

Access Professional Edition – elastyczny system kontroli dostępu, który rośnie wraz z potrzebami Twojej firmy

Access Professional Edition: doskonale rozwiązanie przeznaczone do kontroli dostępu dla małych i średnich firm gwarantujące następujące korzyści:

- Skalowalne, podstawowe rozwiązanie z możliwością rozbudowy w przyszłości
- Szeroki zakres rozwiązań z obszaru kontroli dostępu i bezpieczeństwa przewidziany do różnorodnych zastosowań
- Możliwość umieszczenia nawet 5 kamer przy każdych drzwiach
- Elastyczne przydzielanie uprawnień operatora i posiadacza karty
- Kompatybilność ze standardowymi czytnikami i formatami kart



BOSCH

Technologia bliżej nas

www.boschsecurity.pl

W NUMERZE:

- Nowa norma dotycząca zasilania systemów alarmowych
- Łącza radiowe jako alternatywa dla połączeń kablowych
- Normalizacja w zarządzaniu bezpieczeństwem – nowe spojrzenie
- Miejsce spotkań czy baza danych? Czy nadal chcesz mieć swój profil na portalach społecznościowych?



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

Świat IP coraz bliżej.

SONY



Najnowsze oprogramowanie Real Shot Manager Advanced dostaniesz w prezencie przy zakupie dowolnych 4 kamer IP. Jest to autorskie oprogramowanie Sony stworzone do monitoringu. W połączeniu z kamerami IP Sony dostajecie Państwo gwarancję, serwis oraz Prime Support*. Ponadto łącząc inteligentną analizę wideo, alarmy na żądanie i wiele innych funkcjonalności, Real Shot Manager Advanced zapewnia bezpieczeństwo na najwyższym poziomie oraz daje możliwość wprowadzenia klienta w świat IP.

*Prime Support coś więcej niż gwarancja, zamiana uszkodzonego sprzętu na sprawny w ciągu trzech dni!!!

Chcesz wiedzieć więcej, skontaktuj się z nami:
www.sonybiz.pl

IPELA

Wydarzenia, Informacje4

SSWiN

Nowa norma dotycząca zasilania systemów alarmowych
– *Krzysztof Serafin*24

Sigma 6 i Sigma 12. Najlepsze rozwiązanie do ochrony małych obiektów
– *Janex International*28

Systemy sygnalizacji włamania (część III). Magistrale transmisyjne i metody transmisji danych – *Waldemar Szulc, Adam Rosiński, WSM*30

DVS Visual Software. Oprogramowanie do wizualizacji systemów alarmowych DSC
– *Sylwester Stryjek, AAT Holding*40

Ochrona informacji

Normalizacja w zarządzaniu bezpieczeństwem – nowe spojrzenie
– *Marek Blim*46

Miejsce spotkań czy baza danych? Czy nadal chcesz mieć swój profil na portalach społecznościowych? – *Krzysztof Bialek*54

Bezpieczeństwo IT

Czy VoIP jest bezpieczne?
– *Leszek Winiarski, Interactive Intelligence*56

Monitoring

Bezpieczny Dom – nietypowy monitoring – *CMA*58

Kontrola dostępu

Wideozeryfikacja – najnowsze osiągnięcie firmy Bosch
– *Marcin Ryżko, Bosch Security Systems*60

Systemy zintegrowane

Integracja systemów alarmowych i systemów zarządzających pracą urządzeń w budynku mieszkalnym – *Marcin Buczał, Politechnika Lubelska*64

Nie tylko komunikacja – *Marek Katarzyński, C&C Partners*70

Ochrona przeciwpożarowa

Nowy europejski standard dla zasysających systemów wczesnej detekcji dymu
– *Mariusz Konik, Vision Polska*72

Telewizja dozorowa

Kamery G1 na trudne warunki – nowa generacja kamer dzień/noc marki NOVUS
– *Patryk Gańko, NOVUS Security*76

Łączy radiowe jako alternatywa dla połączeń kablowych
– *Andrzej Walczyk, Altram*80

Inteligentne platformy CCTV – ALL IN ONE – już dostępne w Polsce
– *ISM EuroCenter*86

Karty katalogowe90

Spis teleadresowy96

Cennik i spis reklam106



Nowa norma dotycząca zasilania systemów alarmowych

24



Czy VoIP jest bezpieczne?

56



Integracja systemów alarmowych i systemów zarządzających pracą urządzeń w budynku mieszkalnym

64



Łączy radiowe jako alternatywa dla połączeń kablowych

80



XII Walne Zgromadzenie Sprawozdawczo-Wyborcze Polskiej Izby Ochrony Osób i Mienia oraz 15-lecie Izby

W dniach 15 – 17 czerwca 2009 r. w Kiekrzu k/Poznania obradowało **XII Walne Zgromadzenie Sprawozdawczo-Wyborcze Polskiej Izby Ochrony Osób i Mienia**. W obradach udział wzięło 72 delegatów, dysponujących 94 głosami. Delegaci dokonali podsumowania działalności za lata 2005 – 2009 oraz przyjęli kierunki działania na lata 2009 – 2013. XII Walne Zgromadzenie Sprawozdawczo-Wyborcze dokonało wyboru nowych władz statutowych, czyli Zarządu, Komisji Rewizyjnej oraz Komisji Arbitrów.





W skład nowych władz weszli:

Zarząd Izby:

- Sławomir Wagner – prezes
- Marcin Pyclik – wiceprezes
- Jacek Pachocki – wiceprezes
- Wojciech Stawski – sekretarz
- Andrzej Woźniński – skarbnik
- Tomasz Byjós – członek
- Bogusław Purski – członek
- Andrzej Wieczorek – członek
- Jacek Wieczorek – członek
- Zygmunt Wojdyło – członek
- Zbigniew Wolski – członek

Komisja Rewizyjna:

- Elżbieta Kaszczyk – przewodnicząca
- Tadeusz Paczkowski – wiceprzewodniczący
- Andrzej Kafarski – członek
- Waldemar Stanek – członek
- Konrad Szlępka – członek

Komisja Arbitrów:

- Adam Pleban – przewodniczący
- Lech Oczko – wiceprzewodniczący
- Lech Biernacki – członek
- Andrzej Ławrynowicz – członek

XII Walne Zgromadzenie dokonało **zmiany nazwy Izby**. Od 16.06.2009 Izba nosi nazwę **POLSKA IZBA OCHRONY (PIO)**.

Wieczorem drugiego dnia obrad uczestnicy Walnego Zgromadzenia oraz zaproszeni goście spotkali się na uroczystym bankiecie z okazji **15-lecia Polskiej Izby Ochrony**.

*Bezpośr. inf. Zenon Parchimowicz
dyrektor Biura Zarządu PIO*

Dziękuję za możliwość uczestniczenia w obradach oraz za zaproszenie na uroczystość 15-lecia Izby. Życzę nowo wybranym władzom, aby sprostawały oczekiwaniom wyborców, a wyborcom – aby wspierali zarząd w jego działaniach na rzecz rozwoju naszej branży.

Zapraszam do obejrzenia fotoreportażu z tej uroczystości:
www.zabezpieczenia.com.pl

Teresa Karczmazyk



XV

Walne Zgromadzenie
Sprawozdawczo-Wyborcze
oraz uroczystość
15-lecia PISA – relacja

W dniu 28 maja 2009 r. w hotelu Windsor w Jachrance k. Warszawy odbyły się **obrad XV Walnego Zgromadzenia Sprawozdawczo-Wyborczego Członków Polskiej Izby Systemów Alarmowych (PISA)**, w których udział wzięło 39 przedstawicieli firm członkowskich (czyli 49,36% wszystkich firm – członków PISA).

Jak powiedział dyrektor biura PISA **Henryk Dąbrowski** – *obrad przebiegły zgodnie z przyjętym przez uczestników obrad porządkiem. Walne Zgromadzenie uchwaliło Regulamin obrad i Ordynację wyborczą.*

Jak podaje dyrektor biura, gospodarzami zgromadzenia byli Georgis Bogdanis (Microsystem) i Waldemar Ciesielczyk

(Datel). W skład Komisji Mandatowo-Skrutacyjnej weszli: Jacek Kaczyński (KJ System), Andrzej Krawczyński (Siemens) oraz Wiktor Hajduk (Microsystem), zaś w skład Komisji Uchwał i Wniosków – Maksymilian Majerski (Samax), Włodzimierz Cieślak (Konsalnet System) oraz Piotr Bąchorek (Alpol).

Nowymi ekspertami PISA w zakresie bezpieczeństwa zostali:

- Georgis Bogdanis (Microsystem),
- Piotr Jezierski (Eko Test),
- Marek Warsztan (Eko Test),
- Włodzimierz Cieślak (Konsalnet System),
- Andrzej Wójcik (ES Instal).



Miło nam poinformować, że pani **Agata Brzosko**, asystentka dyrektora biura PISA, otrzymała z okazji 15-lecia Izby okolicznościową statuetkę i list gratulacyjny (pani Agata pracuje w Izbie od początku jej powstania).

W imieniu całego kolegium redakcyjnego składamy nowym ekspertom oraz pani Agacie nasze gratulacje i życzymy powodzenia w dalszej działalności.

Na VI kadencję Walne Zgromadzenie wybrało **Zarząd**, w skład którego weszli:

- Przemysław Jurkowlaniec (Securitas Service),
- Mirosław Krasnowski (Siemens),
- Paweł Leśnodorski (Expert B.C.).

W skład **Rady Nadzorczej** weszli:

- Marek Bielski (Siemens),
- Georgis Bogdanis (Microsystem),
- Maksymilian Majerski (Samax),
- Andrzej Tomczak (ID Electronics).

Na pierwszym posiedzeniu nowo wybrane organy Izby spośród wybranych przez Walne Zgromadzenie członków zarządu ponownie powołały na **prezesa Mirosława Krasnowskiego**, a na **wiceprezesa Pawła Leśnodorskiego**. **Przewodni-**

czącym Rady Nadzorczej tradycyjnie już został **Marek Bielski** (Siemens), a jego zastępcą **Georgis Bogdanis**.

Po zakończonych obradach jego uczestnicy oraz licznie zaproszeni goście udali się na **część oficjalną uroczystości 15-lecia PISA**. Uczestników powitał przewodniczący Rady Nadzorczej **Marek Bielski**, który przypomniał między innymi najważniejsze wydarzenia z historii Izby. Członkom-założycielom wręczono pamiątkowe statuetki, a zaproszeni goście przewodniczącemu Rady wręczyli prezenty i listy gratulacyjne – co



było miłym akcentem kończącym część oficjalną imprezy.

W części artystycznej wystąpiła z recitalem znana i lubiana aktorka filmowa i teatralna – **Hanna Śleszyńska**, której na scenie przez moment towarzyszył **Rafał Bryndal**.

Wieczór zakończył się bankietem, podczas którego goście mogli podzielić się wrażeniami z uroczystości, powspominać dawne dzieje, spotkać dawno niewidzianych kolegów oraz koleżanki.

W imieniu całej redakcji dziękuję za zaproszenie na uroczystość z okazji jubileuszu oraz życzę dalszych osiągnięć, a także wytrwałości w działaniach na rzecz wszystkich członków Izby.

Opracowała Teresa Karczmarczyk



Zapraszamy do obejrzenia fotoreportażu z uroczystości:
www.zabezpieczenia.com.pl

Targi CARTES & IDentification 2009



pod znakiem innowacji



„Biznes, Innowacyjność, Przyszłość” to temat przewodni XXIV edycji targów **CARTES & IDentification 2009**, najważniejszej światowej imprezy w branży zabezpieczeń cyfrowych i inteligentnych technologii, która odbędzie się w **Paryżu** w dniach **od 17 do 19 listopada 2009 r.**

20 tysięcy zwiedzających i 1,5 tysiąca uczestników kongresu, którzy obejrzą ekspozycję produktów wystawianych przez 500 firm goszczących na imprezie, będzie miało okazję zapoznać się z najświeższymi informacjami na temat rozwoju i tendencji na rynku *smart technologies*.

Strong authentication – w kierunku bezpiecznego internetu

Podczas targów **CARTES & IDentification 2009** wystawcy zaprezentują swoje rozwiązania w dziedzinie *Trusted Internet* (internetu zapewniającego użytkownikom wiarygodną identyfikację i bezpieczeństwo). Poruszony zostanie również temat zwalczania cyberprzestępczości.

Zainicjowane w 2007 r. targi **IDentification** stanowią obowiązkowy punkt programu dla osób zainteresowanych zmianami w poszczególnych technologiach gwarantujących pewne uwierzytelnianie. Impreza, która odbędzie się równolegle z targami **CARTES**, zgromadzi producentów oferujących rozwiązania oraz technologie związane z biometrią, zabezpieczaniem transakcji i dokumentów, uwierzytelnianiem, kontrolą dostępu fizycznego i logicznego, kryptografią, technologiami RFID czy procedurami e-Government.

Gościem honorowym imprezy będzie Rosja

Tegorocznym gościem honorowym targów **CARTES & IDentification** będzie Rosja. Od kilku lat dynamicznie rośnie tam liczba stosowanych kart chipowych, a w kolejnych punktach sprzedaży pojawiają się urządzenia niezbędne do korzystania z nich. O ekspansji w tej dziedzinie świadczy z pewnością obecność licznych rosyjskich wystawców na targach.

Jednak ten szybki rozwój wiąże się ze wzrostem rozmaitego rodzaju zagrożeń, takich jak: nieautoryzowane użycie kart, kradzież tożsamości (*trafficking*) i wyludzenie poufnych informacji (*phishing*), co zmusza banki oraz zainteresowane instytucje do poszukiwania nowych rozwiązań w dziedzinie zabezpieczeń. Obecność na targach czołowych przedsiębiorstw wyspecjalizowanych w zabezpieczeniach cyfrowych pozwoli gościom zapoznać się z osiągnięciami i dotychczasowym postępem w tej dziedzinie.

Inne tematy tegorocznej edycji

Wzrost znaczenia transakcji bezdotykowych we Francji

W ostatnich latach wzrost zainteresowania systemami płatniczymi NFC był związany z możliwością wykorzystania i obciążania kart kredytowych za pomocą telefonów komórkowych w celu dokonywania transakcji bezdotykowych [przyp. red. „...do płatności bezdotykowych bardzo dobrze nadaje się telefon komórkowy wykorzystujący technologię NFC (*Near Field Communication*). Wystarczy zbliżyć telefon do specjalnego terminalu w punkcie handlowym czy usługowym (kawiarni, na stacji benzynowej itp.). Transakcja jest sygnalizowana dźwiękiem i komunikatem wizualnym. Na ekranie komórki pojawia się kwota do zapłaty oraz prośba o wprowadzenie za pomocą klawiatury aparatu osobistego kodu właściciela. Po zaakceptowaniu PIN transakcja będzie potwierdzona poprzez kolejne zbliżenie telefonu do terminalu. Płatność w technologii NFC to zarazem najbezpieczniejsza dla klienta metoda regulowania rachunków, bowiem do uwierzytelnienia transakcji wykorzystuje się osobisty kod. Pozwala on na weryfikację użytkownika (w tym przypadku telefonu) i dopiero wtedy dokonywana jest ostateczna autoryzacja. Poza tym telefon komórkowy staje się dla użytkownika swego rodzaju dodatkowym plastikiem, ponieważ numer rachunku karty płatniczej jest zapisywany na SIM telefonu...”. Źródło: www.eservice.com.pl]. Niemniej jednak złożoność zagadnień związanych z wprowadzaniem standardowych i bezpiecznych systemów płatniczych NFC, a także konieczność porozumienia się niektórych podmiotów (operatorów, emitentów kart, stowarzyszeń) w sprawie modelu realizacji usługi, opóźniły wprowadzenie we Francji płatności bezdotykowych na szeroką skalę.

Obecnie rozwiązanie nabiera konkretnego kształtu, zwłaszcza po tym, gdy sieć hipermarketów Carrefour wprowadziła w lutym b.r. bankowe karty bezdotykowe. W marcu część sklepów sieci wprowadziła możliwość dokonywania płatności za zakupy poprzez zeskanowanie ich karty bankowej. Ten pierwszy krok branży dystrybucyjnej dał sygnał do podjęcia szerszych działań w tym zakresie.

Zrównoważony rozwój i proekologiczne podejście

W ramach realizacji haseł związanych z osiągnięciem zrównoważonego rozwoju organizatorzy targów **CARTES & IDentification** podjęli już w ubiegłym roku działania, które pozwalają

A+A 2009

w Düsseldorfie – Targi i Kongres

W dniach od 3 do 6 listopada 2009 w Düsseldorfie zostaną zorganizowane kolejne **Targi i Kongres A+A 2009**. Impreza jest ukierunkowana na ochronę osobistą oraz na zabezpieczenia i bezpieczeństwo podczas pracy. Tematem wiodącym tegorocznej imprezy są „Innowacje w bezpiecznym i zdrowym biznesie”.

Taka tematyka może polskiemu czytelnikowi sugerować, że A+A poświęcone są przede wszystkim zagadnieniom BHP, i tu można się pomylić. Bezpieczeństwo nie tylko podczas pracy, ale i podczas przebywania w firmie jest potraktowane bardzo szeroko. Rozciąga się ono od ochrony osobistych, poprzez bezpieczne warunki pracy, obejmujące oprócz czynników rozumianych tradycyjnie (łącznie z ergonomią stanowiska pracy) również czynną i bierną ochronę przeciwpożarową, ochronę przed innymi zagrożeniami, po zwalczanie kłesk i tematykę zarządzania kryzysowego w firmach, instytucjach publicznych, szpitalach itp. W specjalnie wydzielonych stoiskach zwiedzający będą mogli zapoznać się ze sposobami posługiwania się i manipulowania substancjami niebezpiecznymi.



O rozmiarze imprezy niech świadczy fakt, że stoiska wystawiennicze zlokalizowane są w dziesięciu halach wystawowych, a łączna powierzchnia wystawiennicza przekroczy 50 000 m².

Więcej informacji:

www.messe-duesseldorf.de

<http://www.aplus-a-online.de/>

Redakcja

Źródło: Messe Düsseldorf

zminimalizować wpływ imprezy na środowisko. W tym celu będą zastosowane identyfikatory z PCV (do recyklingu), przyjazne dla środowiska torby na materiały dla zwiedzających, dokumenty promocyjne wykonane przez drukarnie legitymujące się znakiem *Imprim'vert* oraz nadające się do recyklingu nośniki reklamowe. Odbędzie się również selektywna zbiórka odpadów i niektórych materiałów.

CARTES & IDentification” 2009 to również...

Niewątpliwie najważniejszy na świecie kongres branży zabezpieczeń

Trzydniowy kongres, który zgromadzi 1,5 tysiąca uczestników debatujących o najnowszych osiągnięciach technicznych, wyzwaniach marketingowych i strategicznych, to źródło cennych informacji i *know-how* branży. Podczas kongresu odbędzie się około dwudziestu konferencji o tematyce związanej z kartami i identyfikacją. Będą one najlepszym odbiciem tendencji rynku, a także istotnym uzupełnieniem wizyt na stoiskach. Aż 86% uczestników uważa kongres za światowy punkt odniesienia dla tego rynku.

World Card Summit – głos mają giganci przemysłu

Inauguracyjna konferencja **World Card Summit** zgromadzi przedstawicieli czołowych przedsiębiorstw przemysłowych, którzy wymienią poglądy na temat aktualnej sytuacji i wyzwań dla tego sektora w kontekście ogólnoświatowej, trudnej koniunktury gospodarczej.

Weźmie w niej udział około dziesięciu menedżerów najwyższego szczebla, którzy podzielą się swoimi poglądami na temat

przyszłości tej branży. **World Card Summit** – to jeden z najważniejszych punktów programu kongresu, który w ubiegłym roku zgromadził ponad 800 uczestników.

„Sezamy” wyrazem uznania w branży

„Sezamy” – uznane za niepodważalne świadectwo innowacyjności i będące punktem odniesienia dla specjalistów z dziedziny kart chipowych i identyfikacji – zapewniają ich zdobywcom rozpoznawalność w branży oraz gwarantują sukces podejmowanych przedsięwzięć.

Konkurs jest otwarty dla wszelkich innowacyjnych projektów z prezentowanych dziedzin i każdego roku przyciąga coraz więcej kandydatów. W 2008 r. złożono 232 wnioski i wyłoniono dziesięciu laureatów.

„Sezamy” przyznawane są przez jury złożone z ekspertów i wręczane podczas prestiżowej gali organizowanej w Paryżu w przeddzień otwarcia targów „CARTES & IDentification”.

Z produktami zakwalifikowanymi do finału konkursu będzie można zapoznać się na terenie ekspozycji pod nazwą **SESAMES**, która znajdzie się w centralnej części targów.

Najnowsze informacje na temat targów **CARTES & IDentification** są dostępne na stronie internetowej www.cartes.com

Informacje praktyczne:

Termin: 17 – 19 listopada 2009 r.

Miejsce: Parc des Expositions Paris-Nord Villepinte w Paryżu

Bezpośr. inf. **LEWIS PR**

cartes@lewispr.com, <http://www.cartes.com>

System PROTEUS

nowa jakość w działaniach antyterrorystycznych i antykryzysowych

Rusza **PROTEUS** – współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego program budowy zrobotyzowanego systemu wspierającego działania służb ratowniczych, odpowiedzialnych za bezpieczeństwo publiczne.

25 czerwca 2009 roku – **Przemysłowy Instytut Automatyki i Pomiarów (PIAP)** poinformował o rozpoczęciu prac nad nowatorskim na skalę światową projektem **PROTEUS**. Jego celem jest stworzenie systemu, który będzie wspierał koordynację i przebieg akcji ratunkowych prowadzonych wspólnie przez służby odpowiedzialne za bezpieczeństwo publiczne – w tym przez straż pożarną, policję, wojsko i jednostki antyterrorystyczne.

System pozwoli na właściwe rozpoznanie sytuacji, śledzenie jej rozwoju i podjęcie optymalnych działań ratowniczych. Pozwoli to ograniczyć rozmiary zdarzenia, a także zwiększyć skuteczność prowadzonych działań oraz bezpieczeństwo zarówno poszkodowanych, jak i samych ratowników.

Prace nad projektem **PROTEUS** są prowadzone przez konsorcjum złożone z ośrodków i instytucji naukowo-badawczych pod kierownictwem PIAP-u, który jest pomysłodawcą i koordynatorem całego przedsięwzięcia. Realizacja programu jest współfinansowana ze środków funduszu rozwoju regionalnego Unii Europejskiej w ramach „Programu Operacyjnego Innowacyjna Gospodarka na lata 2007 – 2013”. **Program będzie realizowany w latach 2009 – 2013**, a jego wartość wyniesie około 68 mln zł.

– *PROTEUS jest jednym z najbardziej nowatorskich projektów na świecie. Nad podobnymi rozwiązaniami pracuje tylko kilka czołowych ośrodków. Zarówno poszczególne elementy, jak i cały system muszą być na tyle skuteczne, niezawodne i elastyczne, by mogły zastąpić człowieka w najbardziej niebezpiecznych zdarzeniach: pożarach, katastrofach komunikacyjnych i budowlanych czy w sytuacji zagrożenia terrorystycznego – mówi Piotr Szyńkarczyk, kierownik projektu Proteus, Przemysłowy Instytut Automatyki i Pomiarów. – To jedna z tych rzeczy, które trzeba mieć, ale żeby nie trzeba było ich nigdy używać.*

System opracowany w ramach projektu **PROTEUS** będzie składał się z kilku elementów, w tym z Mobilnego Centrum Dowodzenia (MCD), Mobilnego Centrum Operatorów Robotów (MCOR), trzech mobilnych robotów i Bezzałogowego Statku Latającego (BSL). Wszystkie elementy systemu będą wyposażone w spójny system łączności, co umożliwi ich współdziałanie na miejscu akcji nawet w przypadkach, gdy zostaną oddelegowane z różnych jednostek. Każdorazowo będzie go można dostosować do charakteru zagrożenia oraz skali i rodzaju prowadzonych działań dzięki możliwości zestawiania różnych elementów systemu na potrzeby konkretnej operacji.



Wykorzystanie elementów systemu **PPROTEUS** w akcjach ratowniczych znacznie zwiększy bezpieczeństwo osób biorących bezpośredni udział w akcji. W sytuacjach zagrożenia robot w zastępstwie człowieka rozpozna charakter zagrożenia i wykona szczególnie niebezpieczne czynności, takie jak podjęcie ładunku wybuchowego, którego nie da się rozbroić na miejscu, obserwację skażonego terenu czy wejście na teren podmokły. Pozwoli to maksymalnie ograniczyć ryzyko podejmowane przez ludzi.

Podstawowe elementy systemu PROTEUS:

Mobilne Centrum Dowodzenia (MCD)

Zbudowane na podwoziu samochodu ciężarowego centrum gromadzenia, przetwarzania i wymiany informacji przekazywanych przez pozostałe elementy systemu (roboty, BSL).

Mobilne Centrum Operatorów Robotów (MCOR)

Samochód pozwalający na szybki transport robotów w miejsce akcji i sterowanie nimi poprzez przenośne stanowiska operatorów.

Bezzałogowy statek latający (BSL)

Wypożyczony w kamery wizyjne i termowizyjne, przeznaczony do obserwacji miejsca akcji „z lotu ptaka”.

Roboty mobilne

- 1) **Mały robot mobilny (MRM)** – zdalnie sterowany mały i lekki robot przeznaczony do działań inspekcyjnych w trudno dostępnych miejscach. Wypożyczony w kamery wizyjne i termowizyjne oraz innowacyjny układ napędowy pozwalający szybko i łatwo dostać

Samsung Techwin

zdożył nagrodę producenta roku w kategorii telewizji dozorowej

Samsung Techwin zdobył nagrodę producenta roku 2009 w kategorii telewizji dozorowej, przyznaną przez czytelników czasopisma Professional Security Installer.

Ta prestiżowa nagroda została przyznana podczas gali PSI Premier Awards, która miała miejsce 9 czerwca w klubie golfowym Moor Park w Rickmansworth. Wzięło w niej udział ponad 160 przedstawicieli branży zabezpieczeń.

Nagrody PSI Premier Awards są przyznawane jako wyraz uznania dla jakości produktu, obsługi klienta i nowatorskiej myśli. Producenci, którym przyznaje się nagrody, są nominowani i oceniani przez inżynierów instalacji zabezpieczeń.

Komentując przyznanie nagrody, Jake Kim, dyrektor zarządzający Samsung Techwin Europe, powiedział: – *Cieszę się, że tyłu naszych lojalnych klientów zdecydowało się zagłosować na firmę Samsung Techwin. Na konkurencyjnym rynku posiadanie najlepszych produktów nie wystarczy. Ciężko pracowaliśmy, aby upewnić się, że nasza sieć wsparcia jest wystarczająco solidna i przynosi prawdziwą wartość naszym klientom. Nagroda ta jest ukoronowaniem wysiłków wszystkich członków zespołu Samsung Techwin, dostarczających klientom najwyższy poziom usług. Jesteśmy dumni z naszego sukcesu.*



Firma Samsung Techwin oferuje swoim klientom bezpłatne wsparcie techniczne, pomoc w projektowaniu systemów, a także pięciodniowy okres naprawy urządzeń. Wszystkie produkty są dostarczane z trzyletnią gwarancją.

Bezpośr. inf. David Solomons
DRS Marketing

się w miejsca, gdzie człowiekowi trudno jest się poruszać (np. tereny podmokłe).

2) Robot mobilny interwencyjny (RMI) – zdalnie sterowany robot o wadze do 100 kg przeznaczony do zadań rozpoznawczo-interwencyjnych w pomieszczeniach. Jego konstrukcja umożliwi poruszanie się po trudnym terenie oraz wspinanie się po schodach. RMI będzie wyposażony w czujniki wykrywające różne rodzaje zagrożeń, manipulator z wymiennymi szczękami, cztery kamery wizyjne oraz kamerę termowizyjną.

3) Robot mobilny o zwiększonej funkcjonalności (RMF) – zdalnie sterowany bardzo wytrzymały robot przeznaczony do interwencji w trudnych warunkach, takich jak duże pomieszczenia lub teren otwarty. RMF będzie mógł forsować przeszkody terenowe, będzie też wyposażony w czujniki, kamery wizyjne i zestaw do prowadzenia negocjacji. Będzie mógł także podnosić przedmioty o znacznym ciężarze i obsługiwać narzędzia (np. nożyce do cięcia blachy).

Wszystkie elementy wchodzące w skład systemu PROTEUS będą mobilne, co w dowolnym miejscu w ciągu kilku godzin umożliwi ich transportowanie i instalację oraz dostosowanie parametrów systemu do specyfiki konkretnej akcji ratowniczej.

Prace nad projektem będą trwały w latach 2009 – 2013. Obecnie zostały zakończone konsultacje z przyszłymi użytkownikami systemu (m.in. ze strażą pożarną i policją), co pozwoliło zdefiniować funkcjonalność poszczególnych elementów systemu. W drugim etapie prac, który rozpocznie się w połowie roku, zostanie zaprojektowana architektura systemu.

Institucje wchodzące w skład konsorcjum:

- 1) Przemysłowy Instytut Automatyki i Pomiarów – PIAP – wnioskodawca i koordynator projektu
- 2) Centrum Badań Kosmicznych PAN
- 3) Centrum Naukowo-Badawcze Ochrony Przeciwpowodziowej
- 4) Instytut Technologii Materiałów Elektronicznych
- 5) Politechnika Poznańska
- 6) Politechnika Warszawska:
 - Wydział Inżynierii Materiałowej
 - Zakład Automatyki i Osprzętu Lotniczego
 - Zakład Teorii Maszyn i Robotów
 - Instytut Radioelektroniki
- 7) Wojskowa Akademia Techniczna

Bezpośr. inf. PIAP

Samsung Techwin wprowadza na rynek nową wandaloodporną kamerę kopułkową z obiektywem zmiennoogniskowym

Samsung Techwin wprowadza na rynek nową wandaloodporną kamerę kopułkową SVD-4400 odpowiednią do niemal wszystkich zastosowań wewnętrznych i zewnętrznych wszędzie tam, gdzie urządzenie może być narażone na akty wandalizmu.

Łatwy do regulacji obiektyw zmiennoogniskowy 2,8 mm do 10 mm umożliwia kamerze SVD-4400 dostarczanie obrazu w różnych zakresach obserwacji, co pozwala na zwiększenie zakresu jej zastosowań.

Model SDV-4400 ma stopień ochrony IP66 oraz funkcję dzień/noc z wbudowanym filtrem podczerwieni, umożliwiającym efektywne działanie zarówno w warunkach dziennych, jak i nocnych. Wbudowany chipset W4 DSP Samsung Techwin umożliwia dostarczanie obrazu kolorowego o rozdzielczości 580 linii TV oraz obrazu monochromatycznego o rozdzielczości 700 linii TV przy natężeniu oświetlenia 0,001 luksa bez konieczności dodatkowego doświetlania sceny.

Mocna obudowa wykonana z odlewanego ciśnieniowo aluminium stanowi zabezpieczenie przed aktami wandalizmu. W wykonanej z wytrzymałego polikarbonatu osłonie kopuły znajduje się moduł kamery o szerokiej gamie cech i funkcji, takich jak: detekcja ruchu, cyfrowa stabilizacja obrazu (DIS), maskowanie stref prywatności, kompensacja bieli oraz możliwość wyboru metody zasilania.



– SVD-4400 to dyskretna i stylowa wandaloodporna kamera kopułkowa, stanowiąca doskonałe i ekonomiczne rozwiązanie instalacyjne dla szerokiej gamy projektów telewizji dozorowej – mówi Peter Ainsworth, kierownik ds. produktów w dziale ochrony pro-

fesjonalnej firmy Samsung Techwin. – Do imponującej listy funkcji tego modelu należy dodać kompensację tylnego oświetlenia i funkcję kompensacji mocnego światła (HLC), która pozwala kamerze pracować w scenach z ostrymi źródłami światła, umożliwiając na przykład odczytywanie tablic rejestracyjnych samochodów mimo włączonych reflektorów.

Tak jak wszystkie kamery i kopuły Samsung Techwin, model SVD-4400 wyposażony jest w unikatową technologię super redukcji szumów firmy Samsung (SSNR), która w warunkach słabego oświetlenia eliminuje szumy obrazów bez efektu ducha. Eliminując szumy obrazów, technologia SSNR może też zaoszczędzić 70% miejsca na twardym dysku i zoptymalizować szerokość pasma potrzebnego do pracy w sieci (dedykowane oprogramowanie).

Model SVD-4400 może być instalowany wspólnie z akcesoriami firmy Samsung Techwin, które pozwalają na montaż ścienny, narożnikowy oraz sufitowy.

Bezpośr. inf. David Solomons
DRS Marketing

Wspólne szkolenie firmy Bosch i CNBOP

Nawet najlepsze produkty gwarantują wysoką jakość systemu tylko wówczas, gdy trafiają w ręce doświadczonych oraz przeszkolonych projektantów i instalatorów. Z tego powodu Bosch Security Systems bierze czynny udział w upowszechnianiu wiedzy z zakresu systemów bezpieczeństwa, organizując liczne szkolenia i seminaria oraz uczestnicząc w nich.

W dniach 22 – 24 czerwca b.r. odbyło się szkolenie dla projektantów, instalatorów i konserwatorów Sygnalizacji Alarmu Pożarowego (SAP), zaś w dniach od 24 do 26 czerwca – szkolenie z zakresu Dźwiękowych Systemów Ostrzegawczych (DSO). Szkolenia prowadzone były przez Centrum Naukowo-Badawcze Ochrony Przeciwpowodziowej oraz firmę Robert Bosch Sp. z o.o.

Podczas części wykładowej szkolenia z zakresu SAP uczestnicy mogli się zapoznać z zasadami wprowadzania do obrotu oraz stosowania urządzeń SAP w Europie i w Polsce, podziałem i własnościami systemów SAP, sposobem użytkowania, zastosowania, zasadami działania i możliwościami rozwiązań konfiguracji. Tematyka szkolenia obejmowała również kwestie dokumentów normatywnych w zakresie SAP, wymagania PSP przy prowadzeniu czynności kontrolno-rozpoznawczych obiektów

budowlanych oraz zasady prowadzenia odbiorów przez organy nadzoru. W ramach szkolenia odbyły się także warsztaty z zakresu konfigurowania i programowania urządzeń.

Innowacyjną formę i bogaty starannie dobrany program miało również szkolenie DSO dla projektantów, instalatorów i konserwatorów dźwiękowych systemów ostrzegawczych. To już kolejne szkolenie organizowane przez CNBOP wspólnie z producentami wyrobów w ramach Konsorcjów Naukowo-Przemysłowych. Szkolenie DSO składało się z części wykładowej, prezentacji badań laboratoryjnych oraz warsztatów praktycznych. Szkolenie poprowadzili eksperci CNBOP oraz firmy Bosch i KG PSP, przedstawiciele wyższych uczelni oraz doświadczeni praktycy, projektanci i rzeczoznawcy. Zaproszeni zostali również goście specjaliści, w tym wiodący eksperci z Holandii.

Po zakończeniu szkolenia przystąpiono do egzaminu sprawdzającego wiedzę. Uczestnicy, którzy uzyskali pozytywny wynik, otrzymali certyfikat kompetencji oraz zaświadczenie o udziale w szkoleniu.

Bezpośr. inf. Bosch Security Systems



Italians Do It Better

ULISSE COMPACT

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

ULISSE COMPACT jest idealnym rozwiązaniem w przypadku wymagających zastosowań zabezpieczających i monitorowania na zewnątrz budynków.



System kontroli dostępu REG-Sentry

Najnowszy zestaw kamerowy REGD1



Seria REG to zestaw kamer zaprojektowanych specjalnie do przechwytywania numerów rejestracyjnych. Kamery REG fotografują numery rejestracyjne poruszających się pojazdów niezależnie od warunków atmosferycznych oraz oświetleniowych. Stosowane są w kluczowych systemach ochrony oraz inteligentnych systemach transportowych (ITS – ang. *Intelligent Transportation Systems*) na całym świecie. Pozwalają uzyskać zdjęcia o wysokim kontraście, potrzebne do automatycznego rozpoznawania numerów rejestracyjnych (ALPR – ang. *Automatic License Plate Recognition*). Najnowszą innowacją jest system kontroli dostępu **REG-Sentry** – elastyczne i przyjazne użytkownikowi rozwiązanie bazujące na systemie ALPR.

Teraz oferta została wzbogacona o kolejny zestaw kamerowy **REGD1**. Dzięki obrazowaniu w technologii DHC (ang. *Definitive High Contrast*) kamera ta zapewnia poprawny odczyt w najtrudniejszych warunkach oświetlenia. Kamery do identyfikacji pojazdów wyróżnia wysoka rozdzielczość 600 TVL 1/2" LXR CCD, kamera poglądowa posiada natomiast rozdzielczość 480 TVL 1/3" LXR CCD. Wysokosprawne

diody LED Metaphase charakteryzują się średnią trwałością przekraczającą pięć lat.

Przy konstruowaniu kamery zastosowano technologię *Ambient Rejection*, która niweluje problem związany ze światłem reflektorów pojazdu oraz poświatą słoneczną. Połączenie tej technologii z nowościami z zakresu optyki i podczerwieni zapewnia spójne i niezawodne przechwytywanie numerów tablic rejestracyjnych w systemie 24/7. W rezultacie identyfikacja pojazdów możliwa jest z 25 metrów przy prędkości do 160 km/h.

Kamery REGD1 znajdują typowe zastosowania w ochronie i kontroli dostępu, w inteligentnych systemach transportowych, automatycznym rozpoznawaniu tablic rejestracyjnych (ANPR/LPR) oraz monitorowaniu ruchu. Rozwiązanie to stosowane jest również na parkingach samochodowych, w bramkach poboru opłat, w portach lotniczych, portach i przystaniach oraz posiadłościach prywatnych i ogrodzonych obszarach mieszkalnych.

Bezpośr. inf. Bosch Security Systems

Lenel i Guardall łączą się

Lenel Systems International z siedzibą w Rochester, New York, oraz **Guardall** z siedzibą w Edynburgu, Szkocja – firmy należące do **UTC Fire & Security** – ogłosiły połączenie i utworzenie **Lenel Systems International**. Obie firmy zachowają swoje dotychczasowe oddziały w USA, Kanadzie, Szkocji, Francji i Włoszech. UTC Fire & Security jest oddziałem United Technologies Corp. (NYSE: UTX).

W okresie przejściowym połączonymi firmami będzie kierował Luis Orbegoso, prezes Lenel, mający swą siedzibę w Rochester. – Łącząc marketing, łańcuchy zaopatrzeniowe, księgowość oraz funkcje obsługi klienta, nowa organizacja będzie lepiej dostosowana i zorganizowana do wspierania rzeszy globalnych klientów, a także do zapewnienia szybszej reakcji i dostarczenia lepszych wyrobów – stwierdził Orbegoso.

Połączenie nie będzie miało wpływu na strategię wprowadzania na rynek produktów Lenel i Guardall. Wyroby Lenel będą nadal rozprowadzane poprzez sieć certyfikowanych przez

Lenel hurtowników. Wyroby Guardall będą nadal rozprowadzane przez certyfikowanych dealerów Guardalla. Zarówno Lenel, jak i Guardall utrzymają odrębne portfele wyrobów oraz oddzielne kanały sprzedaży i dystrybucji.

Na stanowisko wiceprezesa ds. globalnej sprzedaży Guardall został powołany Bill Lozon. Przed przyjściem do organizacji pracował on dla UltraVision, Bosch Security Systems i Honeywell International (Pittway). Tore Braenna i Abdo Melki będą nadal prowadzić sprzedaż wyrobów Lenel w Europie i na Bliskim Wschodzie, pozostając odpowiednimi wiceprezesami ds. sprzedaży regionalnej. Phil Eldridge obejmie stanowisko dyrektora generalnego Lenel Europe & Middle East, nadzorując codzienne zarządzanie infrastrukturą biznesową w tych regionach. Wszyscy podlegają bezpośrednio Orbegoso.

Źródło: www.securityworldhotel.com

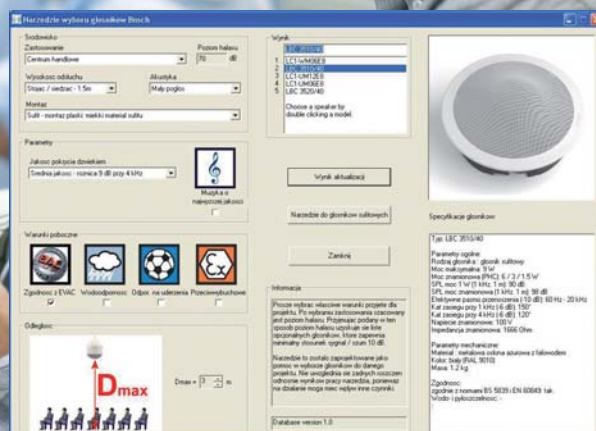
Tłumaczenie: Redakcja

Firma Bosch wspiera pracę projektantów

Firma Bosch zachęca do korzystania z **narzędzia doboru głośników**, które znacząco przyspiesza proces projektowania. Narzędzie to jest dostępne na stronie internetowej **Bosch Security Systems**: <http://www.boschsecuritysystems.pl> w postaci pliku do pobrania w zakładce „Wsparcie techniczne”.

Narzędzie **Dobór głośników** to **użyteczny program wspierający projektowanie**. Do wybranego przez użytkownika zastosowania program podaje poziom hałasu. Następnie generowana jest lista opcjonalnych głośników, które zapewniają minimalny stosunek sygnał/szum 10 dB. Aplikacja jest bardzo łatwa w obsłudze. **Interfejs użytkownika w języku polskim** wspiera nawet mało doświadczonych użytkowników. Program szacuje liczbę głośników niezbędnych do poprawnego nagłośnienia danej powierzchni w przypadku zastosowania głośników na suficie, tj. głośników sufitowych, zwieszanych i nastrogowych.

Bezpośr. inf. Bosch Security Systems



Samsung Techwin

wprowadza do sprzedaży nową generację kamer z wbudowanymi nadajnikami UTP

Samsung Techwin uruchomił nową generację stałych kamer kompaktowych i kopułkowych. Wykorzystał w tym celu ekonomiczne rozwiązania do realizacji transmisji wysokiej jakości obrazów video po nieekranowanym kablu skręcanym.

W rodzinie kamer znajdują się dwie kamery stałe i trzy kopułkowe. Wszystkie one mają **wbudowane nadajniki UTP** dla zapewnienia przesyłu wizji o wysokiej rozdzielczości na odległość do 1,5 km. Dzięki zastosowaniu urządzenia do dystrybucji zasilania, a także sygnału video typu SUJ-800, można również przesyłać zasilanie na odległość do jednego kilometra.

Skrętka nieekranowana jest tańsza oraz łatwiejsza do obróbki niż okablowanie standardowe, szczególnie wtedy, gdy jednym kablem należy przesyłać i obraz, i dane i zasilanie.

Modele te zapewniają najlepsze rozwiązania praktycznie dla każdego zastosowania. W rodzinie kamer pełnią one różne funkcje, choć obie kamery stałe oraz dwie kamery kopułkowe są typu dzień/noc z wbudowanym filtrem wycinania podczerwieni, z detekcją ruchu, kompensacją oświetlenia tła i kompensacją nadmiernego oświetlenia. Wszystkie te pięć modeli



posiada wbudowaną technologię super redukcji szumów firmy Samsung (SSNR), która eliminuje szумы obrazów w warunkach słabego oświetlenia bez efektu ducha. Eliminując szумы obrazów, technologia SSNR może też zaoszczędzić 70% miejsca na dysku twardym i zoptymalizować szerokość potrzebnego do pracy w sieci pasma (dedykowane oprogramowanie).

Bezpośr. inf. David Solomons

DRS Marketing

Tłumaczenie: Redakcja

Przed wszystkim klient

HID Global, dostawca rozwiązań z zakresu bezpiecznej identyfikacji, przedstawił podczas targów IFSEC 2009 swoją inicjatywę „Customer First” (Przed wszystkim klient). Forum jest przeznaczone dla tych wszystkich, którzy chcą podzielić się swymi poglądami i opiniami na temat rynku zabezpieczeń, w tym oczywiście na temat firmy HID Global oraz dostarczanych przez nią produktów i rozwiązań.

Ponad 150 osób, tj. klienci HID i zwiedzający, skorzystało z możliwości podzielenia się z kierownictwem HID swymi przemyśleniami na temat ewentualnych ulepszeń, będących już w ofercie produktów, a także o pomysłach na nowe urządzenia. Przedstawiciele firmy przeprowadzili wiele rozmów handlowych ze swoimi obecnymi i przyszłymi klientami.

– *Imprezy targowe to znakomite miejsce i czas do zaprezentowania nowości przedstawicielom nie tylko firm współpracujących, ale także i tych potencjalnych* – powiedział Paul Naldrett, dyrektor zarządzający HID Global EMEA. – *W tym roku naszym celem było zwiększyć zaangażowanie zwiedzających, zaprosić do rozmów, poznać ich potrzeby i oczekiwania, zademonstrować pełną ofertę wyrobów i rozwiązań z zakresu zarządzania identyfikacją i dostępem. W zamian za podzielenie się pomysłami i przemyśleniami klienci zostali zaproszeni na staroświeckie spotkanie przy lodach.*

Bezpośr. inf. HID Global



ASIS International zorganizował VIII Europejską Konferencję Bezpieczeństwa

VIII Europejska Konferencja Bezpieczeństwa ASIS International odbyła się w dniach 26 – 29 kwietnia w **Centrum Muzyczno-Konferencyjnym w Montreux (Szwajcaria)**.

W 30 sesjach edukacyjnych na najwyższym poziomie, poświęconych tematowi od bezpieczeństwa łańcucha zaopatrzeniowego poczynając, a na zbieżności bezpieczeństwa fizycznego i technologii informatycznych skończywszy, uczestniczyło 312 osób z 44 różnych krajów. Byli to specjaliści do spraw bezpieczeństwa, członkowie zarządów firm, konsultanci i oficjałowie. Choć ze względu na kryzys ekonomiczny liczba delegatów była nieco mniejsza niż w latach poprzednich, nie wpłynęło to na wartość kontaktów towarzyskich i biznesowych zarówno dla delegatów, jak i wystawców.

Konferencję otworzyła dr Sally Leivesley, dyrektor zarządzający NewRisk Limited, organizacji doradczą rządów i firmom w sprawach ryzyka katastrof. Dr Leivesley wymieniła pięć głównych zagrożeń, którym dziś muszą przeciwstawić się specjaliści od zabezpieczeń. Są to: globalna recesja, globalny terror i zagrożenie wojną, dostępność energii, zaufanie publiczne, pandemia. Ze względu na doniesienia o wybuchu świńskiej grypy większość jej wypowiedzi poświęcona była oczywiście temu tematowi.

Następnego dnia Jakob Scharf, szef duńskiej służby wywiadu i bezpieczeństwa (PET), omówił wzrastające, wywołane

opublikowaniem w 2005 r. obrazków proroka Mahometa, zagrożenie terroryzmem w jego kraju.

Kończącym konferencję kluczowym mówcą był Roland Billeter, prezes ADT Continental Europe. Według niego 18 z 27 członków UE pojawia się w czołowej trzydziestce rankingu przestępstw na głowę mieszkańca.

Konferencja obejmowała również zarówno sesje specjalnie przewidziane do omówienia, tworzenia i wdrażania norm, jak i wydarzenia specjalnie przeznaczone dla ludzi z górnej półki profesji *security* – CSO (szefa zabezpieczeń).

Delegaci uczestniczyli również w wydarzeniach towarzyskich takich jak przyjęcie powitalne w pałacu Fairmont Palace Le Montreux czy przyjęcie prezydenckie w historycznym Chateau de Chillon.

ASIS ogłosiło również nazwisko **laureata europejskiej nagrody ASIS International 2009 za Nadzwyczajne Przyczynienie się do Bezpieczeństwa Społeczeństw**. Został nim **ambasador Norwegii, Kai Eide**, nagrodzony za działania na rzecz ustanowienia pokoju i stabilności na Bałkanach Zachodnich.

Bezpośr. inf. Michiel Gen
ASIS International European Bureau
Tłumaczenie: Redakcja



Ogólnopolskie Szkolenie Projektowe Schrack Seconet 2009 – relacja

Dnia 17 czerwca 2009 w Szkole Głównej Służby Pożarniczej w Warszawie odbyło się kolejne **Ogólnopolskie Szkolenie Projektowe firmy Schrack Seconet Polska** – jednego z największych i najbardziej znanych producentów systemów ochrony przeciwpożarowej na świecie.

W szkoleniu wzięło udział 280 osób, głównie projektantów SSP oraz specjalistów z branży zabezpieczeń. Oprócz przedstawicieli firmy Schrack Seconet Polska w gronie autorów wygłoszonych referatów znaleźli się zaproszeni goście: Jerzy Ciszewski i Janusz Sawicki z Instytutu Techniki Budowlanej oraz Antoni Celej z Oddziału Stołecznego Stowarzyszenia Inżynierów i Techników Pożarnictwa. Organizatorzy spotkania umożliwili również firmie Ambient System prezentację urządzeń dźwiękowego systemu ostrzegawczego.

Pierwszą część spotkania rozpoczął prezes zarządu Schrack Seconet Polska, Grzegorz Ćwiek, który powitał uczestników i wprowadził ich w tematykę szkolenia. Następnie dyrektor techniczny firmy – Krzysztof Kunecki – zaprezentował nowości w ofercie Schrack Seconet, m.in. nową generację systemów wczesnej detekcji dymu, tj. system zasysający AirSCREEN ASD 535, nową platformę central B6 (Integral C/C1 Evolution), sygnalizatory akustyczne SBL 501, SBL 502, nowy moduł BX-AIM oraz nowe wersje przycisków MCP 545 oraz liniowej czujki dymu SPB-C.

Jako pierwszy z gości swój referat wygłosił Antoni Celej. Tematy jego wystąpienia to „Koncepcja bezpieczeństwa pożarowego obiektu” oraz „Operat pożarowy”. Z kolei Janusz Sawicki wprowadził uczestników w tematykę „Funkcji scenariusza pożarowego w koncepcji bezpieczeństwa budynku” oraz przedstawił charakterystykę projektów: budowlanego, przetargowego i wykonawczego. W jednym ze swoich wystąpień Antoni Celej poruszył również temat dokumentacji powykonawczej oraz metodyki postępowania Państwowej Straży Pożarnej podczas odbioru obiektu. Po pierwszej części szkolenia uczestnicy zostali zaproszeni na obiad, podczas którego rozpoczęły się pierwsze dyskusje dotyczące aktualności prawnych i kwestii związanych z rzetelnym przygotowaniem projektu zaawansowanych systemów zabezpieczeń budynku.

Drugą część spotkania rozpoczął kierownik ds. produktu Schrack Seconet Polska – Paweł Tomaszewski, sygnalizując jedynie **najnowsze rozwiązania w dziedzinie komunikacji** w obiektach służby zdrowia, takie jak **system przyzywowy** oraz **system komunikacji** Visocall IP. Następnie uczestnicy spotkania zostali zaproszeni na oddzielne szkolenie w tym zakresie.

W tej części spotkania poruszone zostały również tematy

związane z konserwacją i serwisem istniejących już instalacji systemów sygnalizacji pożarowej bazujących na wymogach prawnych, a także procedury audytu systemu bezpieczeństwa pożarowego. Jerzy Ciszewski omówił najnowsze wytyczne w zakresie projektowania systemów sygnalizacji pożarowej.

W drugiej części wypowiedzi przedstawił praktyczne aspekty stosowania coraz popularniejszych obecnie także i w Polsce systemów zasysających. Rozwijając tę wypowiedź, Krzysztof Kunecki szczegółowo scharakteryzował najnowszy **system zasysający Schrack Seconet AirSCREEN ASD 535**. Podczas całodniowego spotkania głos zabierał również Grzegorz Ćwiek, nawiązując do treści poruszanych tematów. Głównym celem jego wystąpień było uświadomienie uczestnikom szkolenia, jak ogromną wagę ma rzetelne przygotowanie projektu zaawansowanych systemów zabezpieczeń. Podkreślał, że nowe podejście do spraw związanych z projektowaniem powinno bazować na bezbłędnym zarządzaniu projektem – od fazy koncepcyjnej, poprzez fazę serwisu, konserwacji, aż po modernizację systemu po latach.

Bardzo duże zainteresowanie wywołało wystąpienie Krzysztofa Kuneckiego na temat **Zdalnego Dostępu do systemu Schrack Seconet** oferowanego w dwóch wariantach: **Integral Remote Control Panel** (dla użytkowników systemu) oraz **Remote Access** (dla firmy serwisującej). Oprogramowanie Remote Access pozwala m.in. na zdalne monitorowanie, obsługę, konfigurację oraz uruchamianie systemu sygnalizacji pożarowej. Praktyczna prezentacja systemu pokazała wiele zalet systemów Schrack Seconet oraz duże oszczędności w ramach kosztów serwisu oraz konserwacji dla ich użytkowników. Na szczególną uwagę gości zasłużyły procedury bezpieczeństwa zdalnych operacji, które w systemie Integral Evolution zostały wdrożone w sposób wyjątkowo dobrze przemyślany.

Uczestnicy spotkania mieli okazję zapoznać się nie tylko z przygotowanymi przez gości Schrack Seconet Polska nowościami dotyczącymi zasad projektowania, ale również z ofertą firmy. W trakcie wystąpień słuchacze mieli również możliwość uzyskania odpowiedzi na pytania związane z najnowszymi wytycznymi i regulacjami prawnymi. Szkolenie zakończył prezes firmy, dziękując uczestnikom za uczestnictwo i zapraszając do dalszej współpracy.

Ogólnopolskie szkolenia Schrack Seconet, które już od ponad 10 lat niezmiennie odbywają się o tej porze roku, są największymi tego typu szkoleniami w branży.

IFSEC 2009 relacja

Na IFSEC 2009, największą na świecie doroczną imprezę z dziedziny bezpieczeństwa, przybyło do NEC Birmingham 25 427 profesjonalistów z zakresu bezpieczeństwa (wg audytu ABC) ze 112 rajów. Pokaz, który odbył się w dniach 11 – 14 maja, otworzył Lord Carlile of Berriew QC, prezes Security Institute i niezależny od rządu ekspert prawodawstwa ds. terroryzmu.

James Blue, dyrektor ds. Fire & Security w UBM Live, organizator IFSEC, powiedział: – *W dzisiejszym klimacie ekonomicznym było dla nas ważne nie spoczywać na laurach, gdy przyszło do organizowania IFSEC 2009. Wykorzystaliśmy okazję do ożywienia przemysłu z dziedziny bezpieczeństwa, przekazując pozytywne sygnały zarówno wystawcom, jak i zwiedzającym. Wprowadzając nowe inicjatywy i cechy, przystosowaliśmy zawartość wystawy do wskazania najpilniejszych zagadnień na rynku zabezpieczeń. Poszerzyliśmy także międzynarodowy charakter wystawy (31% wszystkich obecnych było z różnych krajów) poprzez takie zdarzenia, jak „Spotkaj kupujących”. Po otwarciu imprezy przez księcia Kentu, Michała, powitaliśmy delegację międzynarodowych kupców zabezpieczeń na IFSEC i daliśmy bezprecedensowe okazje handlowe naszym wystawcom z Wielkiej Brytanii.*

IFSEC był ponownie areną pokazową dla wiodących na świecie firm, takich jak: ASSA Abloy, Axis Communication, Bosch, Cisco, Dallmeier, Dedicated Micros, Genie, Gunnebo, HID, Hikvision, IndigoVision, JVC, LG Electronics, Mitsubishi, Panasonic, Paxton Access, Risco, Samsung Techwin, Samsung Opto-Electronics U.K., Sanyo, Satel, Sony, Tyco, Videor i Xtralis.

Po efektownym starcie w roku 2008 konferencja IFSEC powróciła bogatsza i z większą liczbą wykładowców. Konferencja trwała przez trzy dni. Każdy dzień był poświęcony innemu obszarowi bezpieczeństwa. Dzień pierwszy był poświęcony **Ochronie Globalnej, Narodowej i Lokalnej**, dzień drugi koncentrował się na **Zarządzaniu Bezpieczeństwem Korporacji**, a dzień trzeci badał **Innowacje Techniczne w Praktyce**. W ciągu trzech dni seminaria prezentowało 27 ekspertów, w tym:

- Stephen Cooper, szef zabezpieczeń, Zarząd Dostaw Olimpijskich,
- nadinspektor Chris Phillips, naczelnik Krajowego Biura Zabezpieczeń Antyterrorystycznych (NaCTSO),
- Gillies Crichton, naczelnik wydziału HSE, Glasgow International Airport,
- Steve Fowler, CEO, Instytut Zarządzania Ryzykiem.

IFSEC 2009 wprowadził również nową **serię bezpłatnych seminariów szkoleniowych**, skierowanych na zarządzanie bezpieczeństwem podczas recesji ekonomicznej. „Seminaria Biznesowe dla Instalatorów Zabezpieczeń” składały się z szeregu prezentacji prowadzonych przez czołowych przedstawicieli przemysłu.

Kontynuując pomyślny start z poprzedniego roku, powróciło **SMT SELECT**. I znów podczas czterodniowej imprezy ponad tysiąc kluczowych użytkowników w specjalnych łóżach

użytkowników miało okazję spotkać się i wymienić poglądy, a także uzyskać liczne bonusy.

Informacje zwrotne od wystawców na IFSEC 2009 wyraźnie pokazują sukces imprezy:

Paul Browne, dyrektor ds. Business Development w ASSA ABLOY UK, powiedział: – *Jesteśmy pod wrażeniem reakcji osób odwiedzających nasze stoisko na wystawie. Włożyliśmy wiele wysiłku w przygotowanie naszej obecności na IFSEC 09 i odebraliśmy fantastyczną reakcję na nowoczesne wyroby, które wystawiliśmy. IFSEC zapewnił nam idealną platformę do przedstawienia informacji na temat nowości oferowanych przez nas zarówno w dziedzinie kontroli dostępu, jak i na rynku zabezpieczeń mechanicznych.*

Graham Hagger, dyrektor zarządzający Select Manufacturing, dodał: – *IFSEC 2009 okazał się być owocną wystawą dla Select Manufacturing. Uczestniczę w IFSEC od 27 lat i, w mojej ocenie jest ona jedną z najlepszych w branży przemysłu zabezpieczeń. W tym roku było tak samo, a ja już czekam na rok 2010.*

Podczas rozdania nagród **IFSEC Security Industry Awards 2009**, które odbyło się w poniedziałek 11 maja, przemysł zabezpieczeń miał także okazję uczcić najlepsze w branży osoby. Ufundowane wspólnie z Brytyjskim Stowarzyszeniem Przemysłu Zabezpieczeń (BSIA) nagrody uhonorowały ludzi, a także wyroby i postęp technologiczny, które w ostatnim roku odegrały znaczną rolę w rozwoju przemysłu zabezpieczeń.

Alex Carmichael, dyrektor techniczny BSIA, powiedział: – *Co roku nagrody IFSEC Security Industry Awards pokazują proces rozwoju innowacji w naszym przemyśle. Zdobywcy tegorocznych nagród zaprezentowali znakomite wyroby, dobrze świadczyli usługi na rzecz ochrony, a także zacieśnili partnerską współpracę z policją. Zawsze robi na mnie wrażenie poziom kreatywności i zaangażowania w naszym przemyśle. Znalazło to odzwierciedlenie w wyborze tegorocznych laureatów, z których każdy może być dumny ze swych osiągnięć.*

Pełna lista laureatów znajduje się na stronie internetowej: www.protectionandmanagementseries.com.

IFSEC 2010 (razem z wystawami The Facilities Show i Safety & Health Expo) odbędzie się w dniach **od 10 do 13 maja w NEC Birmingham**. Najnowsze informacje znajdują się na stronie www.ifsec.co.uk. Firmy zainteresowane wystawiennictwem na imprezie 2010 powinny skontaktować się z Charlie Cracknell +44 (0) 20 7921 8069 lub charlie.cracknell@ubm.com.

IFSEC South Africa odbył się w dniach 30 czerwca – 2 lipca 2009 r. w Sandton, Johannesburg, South Africa.

IFSEC India odbędzie się razem z Firex India w terminie od 29 do 31 października 2009 r. w Pragati Maidan, New Delhi, India. Więcej informacji i rejestracja na stronie www.ifsecindia.com.

Bezpośr. inf. Guy Melzack

PR & Communications Manager Protection & Management Portfolio

Tłumaczenie: Redakcja

Nedap Security Controller

zdożył nagrodę GIT Security Award 2009



Nedap N.V. Security Management zdobył nagrodę GIT Security Award 2009 w kategorii Locks and Access Control with the Security Controller.

Firma Nedap N.V. Security Management tworzy innowacyjne rozwiązania, oferując użytkownikom maksymalne korzyści przy jednoczesnym obniżeniu kosztów. Otrzymana nagroda po raz kolejny udowadnia, że sprawdza się strategia firmy kładąca nacisk na pionierskie rozwiązania systemów kontroli dostępu. Zdaniem jurorów *To naprawdę imponujące, jak szybko udało się firmie Nedap wypromować nowy produkt oraz zdobyć zaufanie klientów (również w skali międzynarodowej).*

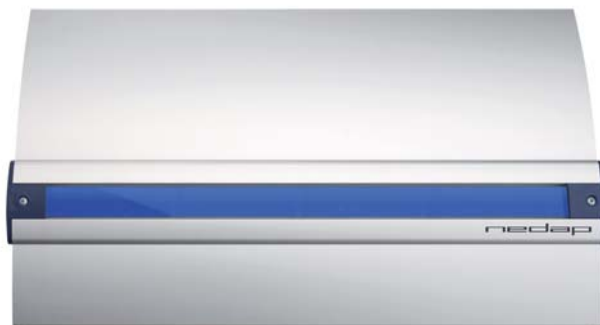
Nedap Security Controller jest pierwszym kontrolerem, który łączy wszystkie funkcje zabezpieczające w jednym urządzeniu. Zastosowanie Nedap Security Controller umożliwia

połączenie funkcji oferowanych dotychczas przez pojedyncze urządzenia kontroli dostępu, takie jak: przechowywanie zapisu wideo, wykrywanie włamań, funkcje PLC czy interkom. Zalety nowego produktu to niewysoka cena oraz niskie koszty instalacji, przy jednocześnie większej funkcjonalności oraz lepszej i łatwiejszej integracji.

Bezpośr. inf. Ilse Peter

Nedap N.V. Security Management

**GIT
SECURITY
AWARD
2009
WINNER**



Firma Honeywell wygrała wart 30 mln USD kontrakt olimpijski



Royal Canadian Mounted Police (RCMP) wybrała firmę **Honeywell** do dostawy **obwodowego systemu sygnalizacji alarmu** dla 18 głównych miejsc, które będą wykorzystywane podczas Zimowych Igrzysk Olimpijskich i Paraolimpijskich Vancouver 2010. W ramach kontraktu Honeywell będzie odpowiadać za instalację, wspomaganie i ewentualny demontaż systemu, który pomoże zabezpieczyć około 27 kilometrów obwodnicy.

System będzie składać się z osprzętu detekcyjnego i oceniającego, zainstalowanego wokół obiektów olimpijskich i paraolimpijskich. W razie zidentyfikowania potencjalnego zagrożenia zostaną zasygnalizowane alarmy pozwalające personelowi ochrony na szybkie zareagowanie. Honeywell zapewni również

całodobową obsługę serwisową, zapewniającą pełne działanie systemu podczas całych igrzysk.

– *Ten kontrakt zapewnia, że na miejscu wokół obiektów, które jesteśmy zobowiązani zabezpieczyć na czas igrzysk olimpijskich i paraolimpijskich 2010, będziemy mieli właściwą infrastrukturę* – powiedział zastępca komisarza Bud Mercer, szef Zintegrowanego Zespołu Zabezpieczeń. – Detekcja naruszenia obwodowego jest ważną częścią wielowarstwowej strategii bezpieczeństwa, a ta informacja potwierdza, że jesteśmy na właściwej drodze.

Źródło: www.securityworldhotel.com

Tłumaczenie: Redakcja



W Zaciszu Borów Tucholskich wcale nie było zacisznie

Tradycją już jest, że od połowy kwietnia w Dziale Marketingu **POLON-ALFA** telefony dzwonią jeszcze częściej niż zwykle, faks nie nadąża z odbiorem wiadomości, a skrzynka mailowa pęka w szwach. Wszyscy pracujący w branży zabezpieczeń zaczynają „zasypywać” firmę pytaniami o konkretny termin i tematykę najważniejszych w Polsce Ogólnopolskich **Warsztatów – Systemy Sygnalizacji Pożarowej ZACISZE**. Chętni,

W tym roku już po raz siedemnasty gościnne progi Ośrodka Doskonalenia Kadr Służby Więziennej przyjęły uczestników warsztatów **ZACISZE 2009**. Impreza zgromadziła blisko 150 osób, które z ogromnym zainteresowaniem przysłuchiwały się wykładom i prezentacjom.

Temat wiodący tegorocznej imprezy to:
Wybrane rozwiązania z zakresu pożarowych instalacji alarmowych

Tematykę tę przybliżyły następujące referaty, z którymi uczestnicy warsztatów mieli możliwość zapoznania się wcześniej:

„Instalowanie czujek pożarowych na sufitach z wykształceniami i podciągami” – Jerzy Ciszewski, ITB Warszawa.

„Czujki wielodetektorowe z członem tlenku węgla jako alternatywa wykrywania pożarów płomieniowych” – Waldemar Wnęk, SGSP Warszawa.

„Wybrane zagadnienia sterowania instalacjami automatycznego gaszenia” – Przemysław Kubica, SGSP Warszawa.

„Kable w instalacjach sygnalizacji pożarowej wg znowelizowanych wymagań warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie” – Janusz Sawicki, ITB Warszawa.

„Współpraca central DSO z centralami sygnalizacji pożarowej w świetle wymagań normy PN-EN 54-16 – Artur Cudowski, ITB Warszawa.

„Rola instalatora w zapewnieniu kompatybilności elektromagnetycznej instalacji stacjonarnych w świetle Dyrektywy EMC 2004/108/WE” – Mariusz Sowiński, POLON-ALFA Bydgoszcz.

„Zasilanie urządzeń alarmowych i automatyki pożarniczej z zasilaczy instalowanych poza centralą sygnalizacji pożarowej” – Dariusz Cygankiewicz, MERAWEX Gliwice.



którzy już uczestniczyli w imprezie, przesyłają zgłoszenia bez żadnych pytań, gdyż wychodzą z założenia, że i tak jak co roku będzie fantastycznie, a nowi... No, cóż – w przyszłym roku oni przyślą zgłoszenia bez żadnych pytań.

„Sygnalizatory głosowe odpowiadające wymaganiom normy PN-EN 54-3” – Włodzimierz Wyrzykowski, W2 Bydgoszcz.

„Optymalizacja wykorzystania wzmacniaczy w systemach DSO na przykładzie systemu PRODAS UNITON” – Krzysztof Kycia, AAT Holding Warszawa.

„Zabezpieczenie przeciwpożarowe magazynu papieru w belach – studium przypadku na przykładzie MONDI ŚWIECIE” – Mariusz Konik, VISION POLSKA Poznań, Jan Misun, Guardtronik Bydgoszcz.

Dla uczestników Warsztatów (jak co roku) przygotowano broszurę z wszystkimi tematycznymi referatami, którą już można zakupić w dziale sprzedaży POLON-ALFA.

Duża dawka wiadomości merytorycznych (czyli coś dla ducha) musiała być jakoś zrównoważona, zadbano więc, by było też coś dla ciała. Pierwszego dnia uroczysta kolacja (z tańcami oczywiście) skończyła się, gdy pierwsze promyki słońca pojawiły się na niebie. W drugim dniu – konkurs dla odważnych, który polegał na... wydojeniu krowy. Ogromne zainteresowanie publiczności, która podziwiała zmagania kilku śmiałków (wśród grona odważnych znalazła się również jedna kobieta), przeszło nasze najśmielsze oczekiwania. Konkurs był międzynarodowy i to właśnie gość zza naszej wschodniej granicy zajął zaszczytne pierwsze miejsce.

Ceremonia wręczenia nagród podczas wieczornego ogniska była ukoronowaniem fantastycznej atmosfery, która panowała wśród wszystkich uczestników warsztatów, bo choć w całej Polsce padał deszcz – w Zaciszu jak zwykle świeciło słońce (no, może z małym wyjątkiem pierwszego dnia).

Za komentarz do tego, że impreza się udała, niech posłużą słowa jednego z pracowników firmy uczestniczącej w Zaciszu po raz pierwszy (ale z pewnością nie ostatni):

„... Sądzę, że wzajemna wymiana doświadczeń oraz informacji z zakresu systemów sygnalizacji pożarowej przyniesie korzyści wszystkim uczestnikom szkolenia. Miła i sympatyczna atmosfera oraz wspaniałe warunki do wypoczynku sprawiły, że obowiązki służbowe idealnie zostały uzupełnione dobrą zabawą i rozrywką...”

Bezpośr. inf. Polon Alfa



REKLAMA

Firma Solid Security w związku z dynamicznym rozwojem poszukuje firm w zakresie

**PODWYKONAWSTWA SYSTEMÓW ALARMOWYCH,
TELEWIZJI DOZOROWEJ I KONTROLI DOSTĘPU**

Oferta dotyczy montażu, serwisu i konserwacji na terenie Pomorza oraz okolic Radomia

Oczekujemy:

- firm dysponujących pracownikami z licencją zabezpieczenia technicznego
- doświadczenia w zakresie instalacji
- listy referencyjnej
- posiadania własnego 24h serwisu

Gwarantujemy:

- atrakcyjne warunki rozliczeń
- ciągłość zleceń

SOLID SECURITY

Oferty zawierające opis i zasięg prowadzonej działalności prosimy składać na adres:

Solid Security Sp. z o.o.
ul. Postępu 17, 02-676 Warszawa
tel. 022 668 60 06

lub e-mailem:
dt.podwykonawcy@solidsecurity.pl

Firma Raytec na targach Ifsec

Zielone światło dla energooszczędnych systemów oświetlenia

IFSEC 2009 - REVIEW
LIGHT MATTERS rayTEC®

Obserwuje się stały wzrost zapotrzebowania na profesjonalne, wysoko-wydajne i energooszczędne systemy oświetlenia dla systemów telewizji dozorowej.

Firma **Raytec** podczas targów **IFSEC 2009** w bardzo ciekawy sposób pokazała zwiedzającym korzyści, jakie można uzyskać, stosując **nowoczesne sposoby oświetlenia**.

Na największym w swej dotychczasowej historii stoisku Raytec zorganizował praktyczną kącik energetyczny, porównując starą technologię oświetlenia z technologią LED i mierząc dokładnie, ile energii i pieniędzy można zaoszczędzić, przechodząc na nowe oświetlacze podczerwone i oświetlacze świecące światłem białym. Nowe oświetlacze Raytec IR i białe



zużywają znacznie mniej energii niż tradycyjne urządzenia oświetleniowe, zapewniając znacznie niższe koszty eksploatacji i konserwacji.

Raytec podczas targów wręczał zwiedzającym darmowy „Kalkulator oszczędności kosztów i energii” ukazujący oszczędności energii i kosztów uzyskiwane po przejściu na oświetlacze LED. Oświetlając swoje stoisko nowymi oświetlaczami niskoenergetycznymi RAYLUX White-Light, Raytec uzyskał oszczędności energii elektrycznej przekraczające 60 procent.

Raytec zaprezentował na targach pierwsze niskoenergetyczne technologie LED w podczerwieni i świetle białym, obejmujące oświetlacze niskonaświetlone FUSION posiadające unikatową funkcję *Adaptive Illumination* (oświetlenie adaptacyjne) oraz nową technologię *Dim and Boost* (ściemnianie i rozjaśnianie).

Bezpośr. inf. Raytec
Tłumaczenie: Redakcja



Darmowe seminaria internetowe organizowane przez firmę Raytec

Specjaliści w zakresie oświetlenia CCTV firmy **Raytec** organizują **darmowe seminaria i szkolenia sieciowe na żywo**. W ten sposób pomagają oni instalatorom i projektantom systemów lepiej zaprojektować systemy zabezpieczeń, aby były jeszcze bardziej skuteczne przy jednoczesnym obniżeniu kosztów.

Program seminariów Raytec (których cztery terminy są już potwierdzone) pozwoli uczestnikom na maksymalizację oszczędności energii i kosztów przy zastosowaniu najnowszej technologii LED (oświetlacze podczerwone lub oświetlacze światłem białym).

Raytec zorganizował w tym roku (początkowo na własne potrzeby) cykl seminariów interaktywnych. Uczestniczyło w nich 70 specjalistów z zakresu zabezpieczeń, którzy podczas oglądania prezentacji on-line mogli się jej przysłuchiwać oraz łączyć telefonicznie.

Aby uczestniczyć w darmowym seminarium Raytec na temat oświetlenia CCTV, po prostu wyślij e-mail do Cat McElroy catherine.mcelroy@rayteccctv.com i zarezerwuj sobie miejsce.

Bezpośr. inf. Raytec
Tłumaczenie: Redakcja



Czy Państwa
system Zarządzania
Bezpieczeństwem
jest przygotowany
na kryzys?

W normalnych okolicznościach system zarządzania bezpieczeństwem pomaga Państwu regulować oraz nadzorować ruch pracowników i odwiedzających. W przypadkach awaryjnych chcieliby Państwo zachować ten sam poziom kontroli. Dzięki AEOS Security Levels firmy Nedap mają Państwo pełną kontrolę nad dostępem do pomieszczeń, nawet w sytuacji kryzysowej. Upoważnienia mogą być zmieniane lub odwoływane za jednym naciśnięciem przycisku dzięki poziomom bezpieczeństwa, które można predefiniować w AEOS. AEOS Security Levels pozwala na szybką reakcję w okolicznościach, które mogłyby poważnie naruszyć Państwa bezpieczeństwo.

Nie ryzykuj. Nedap AEOS. AEOS.

nedap
aeos

NOWA NORMA DOTYCZĄCA ZASILANIA SYSTEMÓW ALARMOWYCH

NIEBAWEM OPUBLIKOWANA ZOSTANIE W JĘZYKU POLSKIM POLSKA NORMA PN-EN 50131-6:2009 SYSTEMY ALARMOWE. SYSTEMY SYGNALIZACJI WŁAMANIA I NAPADU. ZASILANIE. ZASTĄPI ONA NORMĘ PN-EN 50131-6:2000 I WPROWADZI SZEREG ZMIAN.

PRZED W SZYSTKIM BĘDZIE MOGŁA BYĆ STOSOWANA W SYSTEMACH SYGNALIZACJI WŁAMANIA I NAPADU, A NIE JAK JEJ WERSJA POPRZEDNIA TYLKO W SYSTEMACH SYGNALIZACJI WŁAMANIA.



Wprowadzenie

Od momentu wprowadzenia PN-EN 50131-6:2000 przez blisko dziewięć lat występował problem dotyczący tego, w jaki sposób traktować zasilanie i zasilacze w systemach sygnalizacji włamania i napadu. Opublikowana na początku 2000 roku norma jedynie w części dotyczącej zasilaczy do systemów sygnalizacji włamania zastępowała normę PN-93/E-08390/12 Systemy alarmowe. Wymagania ogólne. Zasilacze. Systemy sygnalizacji napadu zostały w PN-EN 50131-6:2000 pominięte. W praktyce oznaczało to, że jeżeli projektowany oraz instalowany system zawierał system sygnalizacji włamania i system sygnalizacji napadu, a takich systemów było i jest najwięcej, należało wybierać z obu norm ostrzejsze zapisy i do nich się stosować. W wielu przypadkach oznaczało to też, że zapisy

PN-EN 50131-6:2000 były z tego powodu martwe, gdyż jako norma bardziej liberalna, zwłaszcza przy określaniu wymagań odnośnie zasilania rezerwowego, nie mogła być stosowana.

Omawiana w artykule norma jest tłumaczeniem Normy Europejskiej EN 50131-6:2008. Aby mogła być ona dokumentem oficjalnym, czyli identycznym z wersją oryginalną, do jej zapisów nie można wprowadzać żadnych zmian ani dodatkowych wymagań. Pojawiające się w normie skrótowce i rysunki również są takie same jak w angielskim tekście normy. Dlatego też do określenia zasilacza systemu alarmowego użyto oznaczenia PS.

Ponieważ przy projektowaniu i instalowaniu systemów sygnalizacji włamania i napadu nie ma obowiązku stosowania tej Polskiej Normy, wszelkie definicje, określenia i regulacje zawarte w normie należy traktować jako zalecenia.

Skrótowce i definicje występujące w normie

I&HAS – system sygnalizacji włamania i napadu

CIE – urządzenia sterujące i obrazujące w tym również centrale alarmowe

podstawowe źródło zasilania – źródło energii elektrycznej umożliwiające długotrwałe zasilanie I&HAS (np. sieć elektroenergetyczna)

dodatkowe podstawowe źródło zasilania (SPPS) – niezależne w stosunku do PPS źródło energii elektrycznej umożliwiające długotrwałe zasilanie energią elektryczną I&HAS (np. generator prądowórczy)

źródło zasilania zewnętrznego (EPS) – zewnętrzne, w stosunku do I&HAS, źródło zasilania energią, niebezprzerwowe

rezerwowe źródło zasilania (APS) – źródło umożliwiające zasilanie energią elektryczną I&HAS w określonym czasie działania w przypadku niemożności korzystania z EPS

czas gotowości APS – czas, w którym APS zasila I&HAS w przypadku braku EPS

bateria (SD) – urządzenie, które magazynuje energię (np. bateria akumulatorów)

zasilacz sieciowy (PU) – urządzenie dostarczające, a także przemieniające i separujące (elektrycznie) energię elektryczną do I&HAS lub jego części oraz do SD, jeśli jest to wymagane

zasilacz (PS) – urządzenie magazynujące, dostarczające, a także przemieniające i separujące (elektrycznie) energię elektryczną do I&HAS lub jego części, zawierające co najmniej PU i SD.

Typ C – zasilacz podstawowy o skończonej pojemności (np. bateria).

Warto tu wyjaśnić, że będący przecież fizycznie istniejącym urządzeniem zasilacz można także traktować jako logiczne rozwiązanie problemu zasilania I&HAS. Przy tej drugiej interpretacji łatwiej jest zrozumieć funkcje i role źródeł zasilania zasilających poszczególne elementy I&HAS, które – jak np. w przypadku SD – mogą być ładowane przez elementy I&HAS, czyli inne zasilacze. Jest to tylko pozorne zapętlenie się definicji, które nie występuje, jeżeli zasilacz lub źródła zasilania są traktowane jak elementy I&HAS (Rys. 1). Powyższa interpretacja ma jeszcze taką zaletę, że umożliwia rozważanie zasilacza o konstrukcji rozproszonej, w którym jego poszczególne elementy są jednocześnie elementami innych części I&HAS.

Powyższy sposób myślenia jest zauważalny w obu normach: PN-EN 50131-1:2007(U) i PN-EN 50131-6:2009. Stopniowo odchodzi się od definiowania poszczególnych urządzeń będących elementami składowymi systemu alarmowego, a wprowadza się charakterystyki funkcjonalne lub narzuca pewne wymagania, nie definiując nawet, gdzie dana funkcjonalność lub właściwość ma być zapewniona. Oczekuje się czegoś od systemu, a nie od jego elementu, bez definiowania, gdzie to ma być realizowane.

Wymagania dotyczące funkcjonalności

Wymagania w odniesieniu do PS są różne dla każdego z czterech stopni zabezpieczenia określonego we wspomnianej już PN-EN 50131-1:2007(U). System alarmowy, jako całość, musi spełniać minimalne wymagania w danym stopniu zabezpieczenia. Do tej pory, zgodnie z PN-93/E-08390/14, używano terminu klasa systemu alarmowego, który niestety nie może być traktowany jako synonim terminu stopień zabezpieczenia. Różnice w tym względzie są widoczne już na przykładzie zasilaczy, a wymagania dla poszczególnych stopni w wielu przypadkach są znacznie zaostrzone.

PS powinien bezprzerwowo dostarczać energię elektryczną do elementów I&HAS. W zależności od stopnia zabez-

Typy zasilaczy

Norma dotycząca zasilania systemów alarmowych odwołuje się do normy PN-EN 50131-1:2007(U) Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe. W normie tej zdefiniowano trzy następujące typy rozwiązań zastosowanych w PS:

Typ A – podstawowe źródło zasilania, np. sieć elektroenergetyczna i rezerwowe źródło zasilania doładowywane z I&HAS, np. akumulator automatycznie doładowywany z I&HAS,

Typ B – podstawowe źródło zasilania i rezerwowe źródło zasilania niedoładowane przez I&HAS (np. bateria niedoładowana automatycznie z I&HAS).

pieczenia oraz typu PS powinien mieć funkcjonalności określone w Tab. 1. Jeżeli zapewniona funkcjonalność określona jest jako opcjonalna dla danego stopnia zabezpieczenia, nie stoi na przeszkodzie, aby również zasilacz ją miał, jednak w przypadku określania zgodności ze stopniem zabezpieczenia urządzenie będzie badane jedynie w zakresie spełnienia obowiązkowych wymagań dla stopnia, dla którego określa się zgodność.

Zasilacze powinny być monitorowane pod kątem zapewnienia ciągłości dostarczania energii elektrycznej do systemu alarmowego. Sygnały monitorowania PS powinny powodować zadziałanie sygnalizacji w CIE. Sygnały te powinny być odporne na zakłócenia, powinny na przykład generować sygnał uszkodzenia nawet w przypadku całkowitego uszkodzenia PS.

Funkcja	Stopień zabezpieczenia	Typ PS		
		A	B	C
Wykrycie braku EPS	1 – 4	M	M	n/d
Wykrycie niskiego napięcia baterii	1 – 4	M	M	M
Wykrycie uszkodzenia baterii	1 – 2	Op	Op	n/d
	3 – 4	M	Op	n/d
Wykrycie niskiego napięcia wyjściowego	1 – 2	Op	Op	n/d
	3 – 4	M	M	n/d
Wykrycie uszkodzenia zasilacza sieciowego	1 – 2	Op	Op	n/d
	3 – 4	M	M	n/d
Zabezpieczenie przed przepięciem	1 – 2	Op	Op	Op
	3 – 4	M	M	Op
Zabezpieczenie przed zwarcie	1 – 4	M	M	M
Zabezpieczenie przed przeciążeniem	1 – 4	M	M	M
Zabezpieczenie przed całkowitym rozładowaniem SD ¹	1 – 2	Op	Op	n/d
	3 – 4	M	M	n/d
Zdalny test	1 – 3	Op	Op	n/d
	4	M	Op	n/d
Ochrona przeciwsabotażowa	1 – 4	M	M	M

¹ Tam, gdzie całkowite rozładowanie może uszkodzić SD. **M** = obowiązkowo, **Op** = opcjonalnie, **n/d** = nie dotyczy

Tab. 1. Funkcje zasilacza

Typy zasilaczy	Stopień 1 (h)	Stopień 2 (h)	Stopień 3 (h)	Stopień 4 (h)
Typ A	12	12	60	60
Typ B	24	24	120	120

Tab. 2. Minimalne okresy gotowości zasilacza rezerwowego

	Stopień 1	Stopień 2	Stopień 3	Stopień 4
Dostęp do wnętrza obudowy	M	M	M	M
Zdjęcie z miejsca zamocowania	Op	Op	M	M
Penetracja do wnętrza obudowy	Op	Op	Op	M

M = obowiązkowo, **Op** = opcjonalnie

Tab. 3. Wykrywanie sabotażu

W przypadku zasilaczy, które są montowane w systemach w 3 i 4 stopniu zabezpieczenia, sygnał uszkodzenia EPS powinien być generowany w czasie do 10 sekund od chwili odłączenia EPS. Jeżeli EPS zostanie podłączony ponownie, sygnał uszkodzenia powinien zaniknąć w ciągu 10 sekund.

To samo dotyczy sygnału uszkodzenia APS, gdzie sygnał ten powinien być generowany w czasie do 10 sekund od chwili wystąpienia niskiego napięcia baterii lub w przypadku wykrycia uszkodzenia baterii.

PS powinien spełniać wymagania dotyczące okresu gotowości źródła rezerwowego. Czasy te są określone w PN-EN-50131-1:2007(U) (Tab. 2).

W przypadku wysyłania sygnałów do alarmowego centrum odbiorczego wartość 60 godzin może być dwukrotnie zmniejszona do poziomu 30 godzin. W tym miejscu warto zacytować kolejny zapis normy PN-EN-50131-1:2007(U), mówiący, że w przypadku zastosowania dodatkowego zasilacza podstawowego, który jest automatycznie uruchamiany w chwili uszkodzenia EPS zasilacza podstawowego, okres gotowości zasilacza rezerwowego może wynosić tylko cztery godziny. Dodatkowy zasilacz podstawowy to np. zasilanie z drugiego transformatora korzystającego z innego przyłącza energetycznego lub agregat prądotwórczy uruchamiany za pośrednictwem układu samoczynnego załączenia rezerwy.

Zasilacz powinien umożliwiać ładowanie baterii akumulatorów po jej rozładowaniu zgodnie z wymaganiami określonymi przez producenta baterii. Bateria akumulatorów powinna być ładowana automatycznie z EPS w czasie 72 godzin dla zasilaczy



Każde niezależne wyjście PS (stopień 1 do 4) powinno mieć zabezpieczenie przed przeciążeniem i przed zwarcieniem.

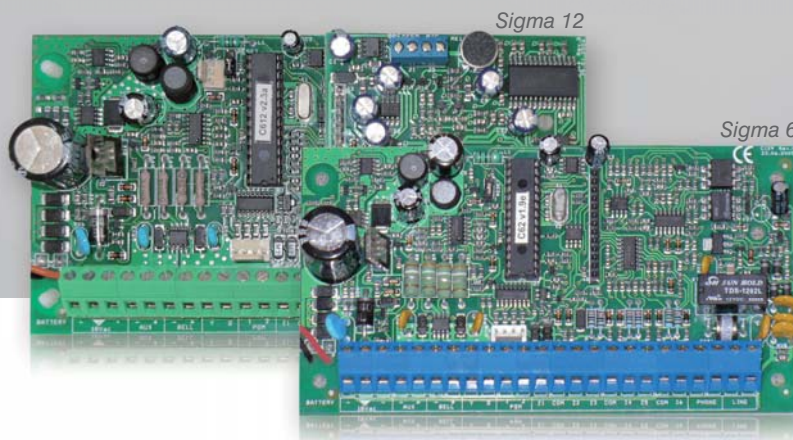
W zależności od stopnia zabezpieczenia sygnał lub komunikat o sabotażu powinien być generowany w przypadku zdjęcia PS z miejsca zamocowania, jeżeli odsunięcie obudowy od miejsca zamocowania przekroczy odległość 10 mm (stopień 1 i 2) lub 5 mm (stopień 3 i 4). Dodatkowo dla PS zaliczanych do stopnia zabezpieczenia 4, nie może być możliwa penetracja do wnętrza obudowy PS przez dostępne powierzchnie metalowym narzędziem powodującym powstanie 4-milimetrowego lub większego otworu bez wygenerowania sygnału lub komunikatu o sabotażu.

Wszystkie elementy, to znaczy śruby regulacyjne i monta-
żowe, są wykonane z nierdzewnej stali.

KT nr 52 PKN ds. Systemów Alarmowych Włamania i Napadu

Sigma 6 Sigma 12

Najlepsze
rozwiązanie
do ochrony
małych obiektów



W niniejszym artykule chcielibyśmy zwrócić Państwa uwagę na centrale alarmowe serii Sigma – Sigma 6 i Sigma 12, które firma Janex International ma w swojej ofercie od kilku lat. Dzięki łatwemu programowaniu, niezawodności oraz niskiej cenie centrale te cieszą się powodzeniem wśród instalatorów systemów alarmowych. Przeznaczone są do ochrony małych obiektów, ale ich możliwości programowe zaskoczą niejednego instalatora.

Płyty central posiadają po sześć zacisków linii; w centrali Sigma 12 funkcje tych linii można podwoić, uzyskując w ten sposób 12 niezależnych linii alarmowych: EOL lub DEOL. System możemy podzielić na dwie niezależne partycje, a każda z tych partycji może być uzbrajana w trybie normalnym lub obwodowym. Na płycie centrali znajdują się dwa wyjścia programowalne PGM, każde o obciążalności maksymalnie 50 mA. W centrali Sigma 12 można je rozszerzyć do sześciu za pomocą modułu rozszerzenia Sigma PGM4.

Jednostka centralna posiada wyjście BELL (o obciążalności 1 A), które służy do sterowania sygnalizatorami.

Centrale z serii Sigma obsługiwane są za pomocą klawiatur LED, a w przypadku central Sigma 12 – również za pomocą klawiatury LCD. Klawiatury systemu Sigma 12 mają dwie linie alarmowe, które można wykorzystać w celu dołączenia czujek alarmowych. Należy jednak pamiętać o tym, aby liczba wszystkich linii w systemie (linie na płycie + podwojone + klawiatury) nie przekroczyła dwunastu.

Maksymalnie może być osiem klawiatur, co pozwala na stworzenie rozległego systemu. Wszystkie manipulatory mają systemowy sabotaż zwiększający bezpieczeństwo systemu.

Istotną cechą centrali Sigma 6 jest duży bufor zdarzeń (400), a w przypadku central Sigma 12 jest to 800 zdarzeń. Z praktyki wiadomo, jak bardzo ważną cechą jest wielkość tego bufora przy ustalaniu przyczyn fałszywych alarmów lub innych zdarzeń zachodzących w systemie. Bufor zdarzeń można odczytać za pomocą klawiatury LCD bądź programu komputerowego SigmaCom. Dzięki oprogramowaniu można

również zaprogramować centralę z komputera w sposób bardziej przejrzysty. Ponadto program pozwala na zapisanie ustawień każdej centrali, dzięki czemu jest możliwość stworzenia bazy klientów.

Każda z central posiada dialer telefoniczny, za pomocą którego wysyłane są raporty na dwa numery stacji monitorowania w jednym z 25 formatów. Do central można podłączyć moduł głosowy, dzięki któremu w przypadku wystąpienia któregoś z 99 zdarzeń w systemie użytkownik będzie o tym powiadamiany głosowo na prywatny numer telefonu. Użytkownik ma możliwość nagrania własnych nazw linii i partycji, co sprawia, że komunikat nadawany przez system jest dla użytkownika jasny i czytelny. Ponadto w celu sprawdzenia stanu systemu istnieje możliwość połączenia się z centralą za pomocą telefonu z wybieraniem tonowym.

System alarmowy może obsługiwać aż 45 użytkowników, którym uprawnienia nadaje nie tylko instalator, ale także właściciel.

Za pomocą szyfratorów LED i LCD system może być przez użytkowników uzbrajany i rozbrajany. Kilkakrotnie wprowadzenie błędnego kodu podczas rozbrajania powoduje zablokowanie klawiatury, co uniemożliwi dalsze próby odgadnięcia hasła przez osoby niepowołane. Uzbrajać i rozbrajać system można również za pomocą pilotów, wykorzystując dedykowany moduł bezprzewodowy KEYFOB-01. Moduł ten umożliwia również dołączenie czytnika kart w formacie Wiegand 26, co pozwala na uzbrajanie systemu także za pomocą karty zbliżeniowej lub breloka. Możliwe jest również zaprogramowanie automatycznego codziennego uzbrajania systemu – jest to przydatne wtedy, gdy klient, opuszczając budynek, notorycznie o tym zapomina.



Ponadto w centralach Sigma 6 i Sigma 12 zaimplementowana jest funkcja automatycznego uzbrojenia również przy braku ruchu – jeżeli w zaprogramowanym przez nas czasie żadna czujka nie będzie naruszona, wówczas system sam się automatycznie uzbroi.

Centrale mają funkcje, które pozwalają na zmniejszenie liczby fałszywych alarmów – możliwość włączenia dla każdej linii niezależnie, wprowadzenie linii alarmowej w stan testu oraz możliwość zaprogramowania linii jako tzw. linii inteligentnej. W przypadku włączenia linii inteligentnej każde pierwsze pobudzenie takiej linii uruchamia odliczanie czasu linii inteligentnej. Alarm będzie wywołany tylko w przypadkach, gdy:

- pobudzenie linii trwa dłużej niż czas linii inteligentnej,
- w trakcie trwania czasu linii inteligentnej linia zostanie pobudzona po raz drugi,
- w trakcie trwania czasu linii inteligentnej zostanie pobudzona inna linia z włączoną funkcją linii inteligentnej.

W przypadku włączenia linii w tryb testowy linia ta nie będzie wywoływała alarmów, ale pobudzenia alarmowe będą zapisywane w pamięci zdarzeń. Jeżeli linia testowa ma ustalone blokowanie po określonej liczbie alarmów, to pobudzenia tej linii będą zliczane. Po osiągnięciu określonej wartości linia ta zostanie zablokowana, a wiadomość o tym zostanie wysłana do stacji monitorowania.

W tym krótkim artykule chcieliśmy przybliżyć Państwu możliwości central serii Sigma oferowanych przez naszą firmę.

Centrale Sigma 6 i Sigma 12 oferują wiele funkcji gwarantujących wysoką użyteczność oraz dających poczucie bezpieczeństwa. Prosta obsługa, opcja powiadamiania głosowego oraz możliwość elastycznego programowania sprawiają, że centrale te znajdują uznanie zarówno wśród instalatorów, jak i wśród użytkowników.

Janex International

Sigma 6
Centrala alarmowa

Płyta + LED 170 PLN*



Sigma 12
Centrala alarmowa

Płyta + LCD 260 PLN*



* - cena do negocjacji, możliwość nadruku loga firmy

JANEX

INTERNATIONAL

JANEX INTERNATIONAL SP. Z O.O. UL. PŁOMYKA 2 02-490 WARSZAWA

TEL.: 022 8636353 FAX: 022 8637423

E-MAIL: JANEX@JANEXINT.COM.PL WWW.JANEXINT.COM.PL

Systemy sygnalizacji włamania

Część 3 – Magistrale transmisyjne i metody transmisji danych

1. Wprowadzenie

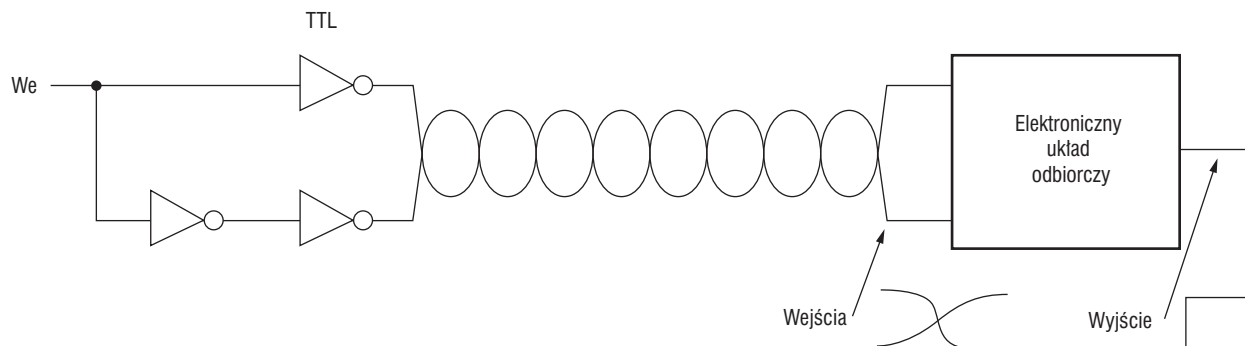
Sygnał alarmu powstaje w wyniku naruszenia określonej czujki bądź czujnika współpracującego z linią dozоровą (ich typy zostały przedstawione w części 2. niniejszego cyklu artykułów). Konfiguracje systemów alarmowych, określające zasady współpracy między modułami a płytą główną centrali alarmowej, były przez autorów opisywane wielokrotnie, ale warto wspomnieć, że szczególne znaczenie mają one przy konfiguracjach mieszanych bądź rozproszonych. Spotykane są jeszcze centrale o charakterze skupionym, łączące się w duże systemy alarmowe o konfiguracjach mieszanych. W takich rozwiązaniach magistrale transmisyjne, wykorzystujące zmodyfikowany interfejs RS232, łączą między sobą kilka central alarmowych (pracujących w tzw. pierścieniu), przez co tworzy się jeden zintegrowany system alarmowy z możliwością centralnego nadzoru, zarządzania i administrowania. Transmisja odbywa się za pomocą czterech przewodów. Ciekawostką była w czasach popularności tego typu systemów izolacja galwaniczna pomiędzy centralami tworzącymi duży system alarmowy uzyskiwana za pomocą transoptorów. Prędkość transmisji (z możliwością programowej regulacji) była niezbyt duża. Współczesne systemy alarmowe o charakterze mieszanym lub rozproszonym mogą posiadać od jednej do kilku magistral transmisyjnych integrujących moduły z jednostką centralną. Spotyka się również systemy z tzw. separatorem magistral transmisyjnych. Poprzez moduły magistral transmisyjne mogą również integrować urządzenia przyłączone do linii wyjściowych, np. sygnalizatory), lub przekazywać alarm zarówno drogami radiowymi bądź komutowanymi, jak również łączami bezpośrednimi. W praktyce spotykane są także systemy mieszane, a więc takie, gdzie transmisja sygnałów odbywa się zarówno przewodowo, jak i drogą radiową. Często stosowane są również konwertery sygnałów z jednego formatu transmisji na inny (np. RS232/RS485 lub RS485/RS232). Należy nadmienić, że bardzo wiele central alarmowych posiada specjalne złącza do nadzoru, programowania, diagnostyki oraz monitorowania, gdzie wykorzystuje się szeregowy format transmisyjny typu RS232. Niestety, nie wszystkie komputery stacjonarne oraz przenośne producent wyposaża w złącze przeznaczone do transmisji szeregowej. Wejścia USB w komputerach (stacjonarnych lub przenośnych) nawet z zastosowaniem konwerterów USB/RS232 sprawiają wiele niespodzianek i kłopotów w trakcie programowania kompletnych systemów alarmowych. W tej części artykułu autorzy przybliżą czytelnikom zagadnienia transmisji informacji dwukierunkowej powszechnie stosowanej w systemach alarmowych. Wiedza ta jest niezbędna do

zrozumienia, w jakim celu stosuje się wynalezione już dość dawno, bo w 1969 roku, szeregowy format transmisyjny (np. standard szeregowy RS232C).

2. Transmisja sygnałów cyfrowych za pośrednictwem kabli

Nie da się przesłać sygnałów cyfrowych z jednego modułu do drugiego za pomocą łączenia tych bloków zwykłymi przewodami. Taki przewód „zbiera” wszelkie zakłócenia z otoczenia (a także sam emituje sygnały zakłócające). Sygnały cyfrowe niosące informacje zwykle przesyła się przewodami współosiowymi (koncentrycznymi), skrętkami dwuprzewodowymi, płaskimi przewodami taśmowymi, wiązkami wieloprzewodowymi oraz obecnie (coraz powszechniej) światłowodami. W niniejszym artykule pokazano sposoby sprzęgania modułów i central alarmowych za pomocą różnych technik. W większości z nich transmisję ułatwiają specjalne układy typu „nadajnik/odbiornik linii”.

Dla względnie powolnej transmisji, wynoszącej kilka tysięcy bitów na sekundę, gdy realizowana jest ona za pomocą zwykłych przewodów (np. wielożyłowych), bardzo przydatny jest nadal popularny standard typu RS232C lub jego nowsza wersja typu RS232D. Standardy te wymagają stosowania napięcia o dwóch polaryzacjach: od ± 5 V do ± 15 V (dla układów nadawczych potrzebne są dwa napięcia zasilające: dodatnie i ujemne). Tego typu wymagania nie obowiązują zazwyczaj dla odbiornika. Po stronie odbiorczej pozwoli to dobierać szerokość pętli histerezy oraz czas odpowiedzi, które to parametry są zależne od poziomu zakłóceń w torach transmisyjnych. Dla przesyłania sygnałów w standardzie RS232 można stosować zwykłe przewody wielożyłowe pozbawione ekranu. Taka opcja jest możliwa, ponieważ linie praktycznie nie sprzęgają się ze sobą ze względu na celowo zmniejszoną prędkość zmian napięcia w liniach do wartości nie większej niż $30 \text{ V}/\mu\text{s}$. Łąca transmisyjne (zwane magistralami transmisyjnymi) pracujące zgodnie ze standardem RS232 są powszechnie stosowane nie tylko w urządzeniach peryferyjnych komputerów, ale również w systemach alarmowych pomiędzy np. płytą główną centrali alarmowej a modułami (dla systemów w wersji rozproszonej lub mieszanej), a także pomiędzy centralami w wersji skupionej (np. w centrali Rankor) pracującymi w pierścieniu. Tego typu magistrale umożliwiają przesyłanie danych (zdarzeń) z kilkoma standardowymi prędkościami w zakresie: od 110 bitów/s do 38,4 kilobitów/s. Istnieją również metody tzw. różnicowego sterowania liniami transmisyjnymi. Przykładem ich wykorzystania jest standard typu RS422, który ma znaczną odporność na



Rys. 1. Transmisja sygnałów TTL metodą różnicową z wykorzystaniem magistrali transmisyjnej (skrętka dwuprzewodowa)

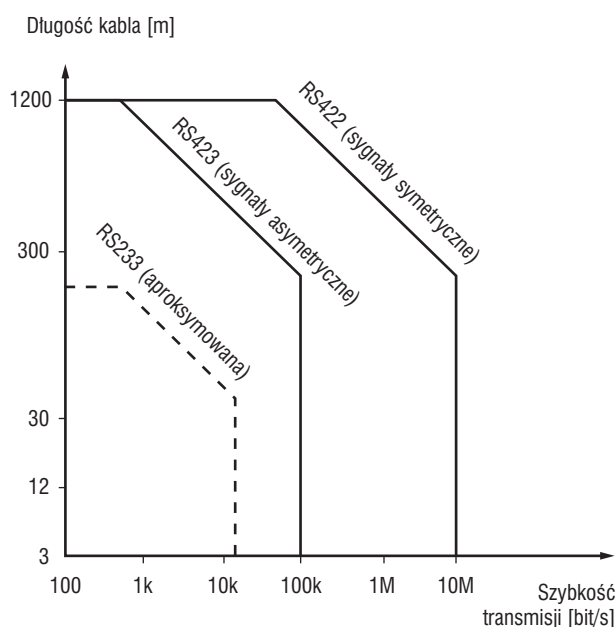
zakłócenia (tak bardzo niepożądane w systemach alarmowych i wywołujące fałszywe alarmy). Transmisja w tym standardzie odbywa się za pomocą skrętki dwuprzewodowej przesyłającej tzw. sygnały komplementarne. Przykład takiego rozwiązania ilustruje rys. 1. Przedstawiono na nim prosty układ dość szybkiej transmisji sygnału TTL (ang. *Transistor Transistor Logic* – technika tranzystorowo-tranzystorowa) metodą różnicową, z wykorzystaniem skrętki dwuprzewodowej jako magistrali transmisyjnej. Taki typ RS422 zesterowaniem różnicowym pozwala na znaczne wydłużenie magistrali transmisyjnej – nawet do 1200 m. Zależność prędkości transmisji za pomocą łącza szeregowego od długości magistrali transmisyjnej dla RS232, RS423, RS422 i RS485 przedstawiono na rys. 2.

Warto nadmienić, że jako nadajniki linii transmisyjnej wybrano układy TTL, a nie CMOS (ang. *Complementary Metal Oxide Semiconductor* czyli – komplementarne układy MOS), ze względu na znacznie większą odporność na zakłócenia powodowane ładunkami statycznymi oraz ze względu na niewystępowanie zjawiska „zatrząskiwania się”, które może pojawić się w układach CMOS jako skutek „odbić” w magistrali transmisyjnej. Układ zapewnia bardzo dobre tłumienie zakłóceń tak niebezpiecznych w systemach alarmowych. Istnieje jeszcze

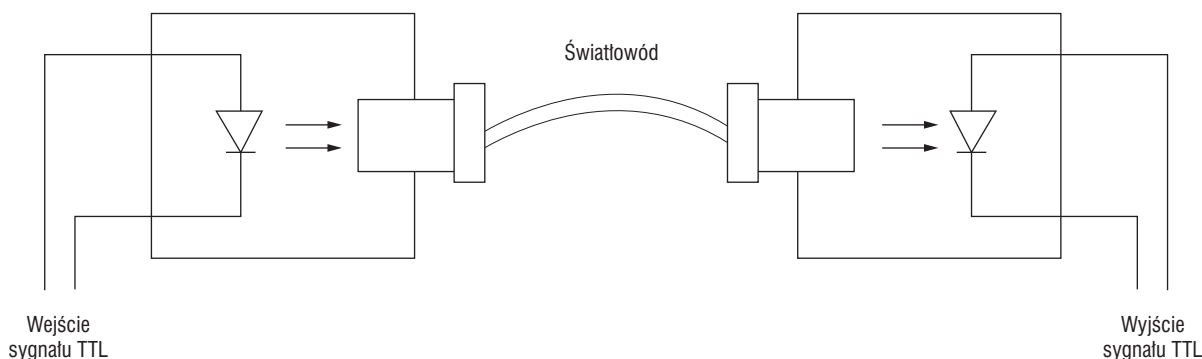
wiele rozwiązań dotyczących transmisji sygnałów pomiędzy nadajnikiem a odbiornikiem, m.in. różnicowy układ prądowy z tzw. dopasowaniem na wejściach odbiornika. Z doświadczeń autorów wynika, że różnicowe nadajniki prądowe zapewniają dużą szybkość transmisji sygnałów. Badania autorów dowodzą, że taki układ transmisyjny jest w stanie przekazywać informacje (zdarzenia) nawet z szybkością 1 Mb/s liniami transmisyjnymi o długości 600 m i szybkością ok. 10 Mb/s na odległość mniejszą, ale przekraczającą znacznie 100 m. Nie jest to tak bardzo istotne przy przekazie informacji pomiędzy centralą alarmową a modułami. Ważna jest natomiast pewność przekazu informacji, a więc występujących zdarzeń dotyczących bezpieczeństwa. Standardy typu RS422/423 zostały opracowane głównie z myślą o przesyłaniu danych, czyli informacji o zdarzeniach, za pomocą skrętek dwuprzewodowych lub przewodów taśmowych (płaskich), które w perspektywie mają wyeliminować nadal bardzo popularny (choć leciwy) standard RS232. Zalecenia tego standardu dotyczą transmisji zarówno magistralami asymetrycznymi (RS423) z maksymalną prędkością 100 kb/s, jak i symetrycznymi (RS422) z maksymalną prędkością 10 Mb/s.

Przebiegi podane na rys. 2. są przebiegami praktycznymi, które poza formatem: RS232, RS423, RS422 uwzględniają standard szeregowy RS485. Będzie o nim mowa nieco później.

Niezmiernie ważnym problemem jest transmisja sygnałów na duże odległości (m.in. w obiektach o charakterze specjalnym). Spotykane są przypadki, gdy chroniony elektronicznie teren jest rozległy. Wtedy klasyczne metody mogą zawodzić. Dodatkowo może dojść do dużych zakłóceń elektromagnetycznych (spowodowanych przez nadajniki radiowe lub stacje radiolokacyjne) lub radioelektrycznych (których przyczyną mogą być źle odłożone systemy sterowania tyrystorów bądź triaków lub inne mocno iskrzące urządzenia elektryczne, trakcja elektryczna i iskrzący zimą pantograf). Wtedy jedynym ratunkiem jest sprzęganie linii transmisyjnych pomiędzy nadajnikiem a odbiornikiem, do czego stosuje się specjalne transformatory z rdzeniami (np. ferrytowymi) o określonym AL, czyli współczynniku przenikalności magnetycznej. Należy jednak pamiętać, że sprzężenie transformatorowe uniemożliwia przesyłanie stałych napięć mających charakter poziomów logicznych. W takiej sytuacji transmitowany sygnał musi być kodowany, np. może być nałożony na tzw. „falę nośną”. Jest to problem dosyć złożony, zwłaszcza gdy w grę wchodzi wymagania dużej prędkości transmisji sygnału.



Rys. 2. Zależność prędkości transmisji od długości magistrali transmisyjnej ($L_{MAG.} = f(v)$, gdzie: $L_{MAG.}$ [m], v [bit/s])



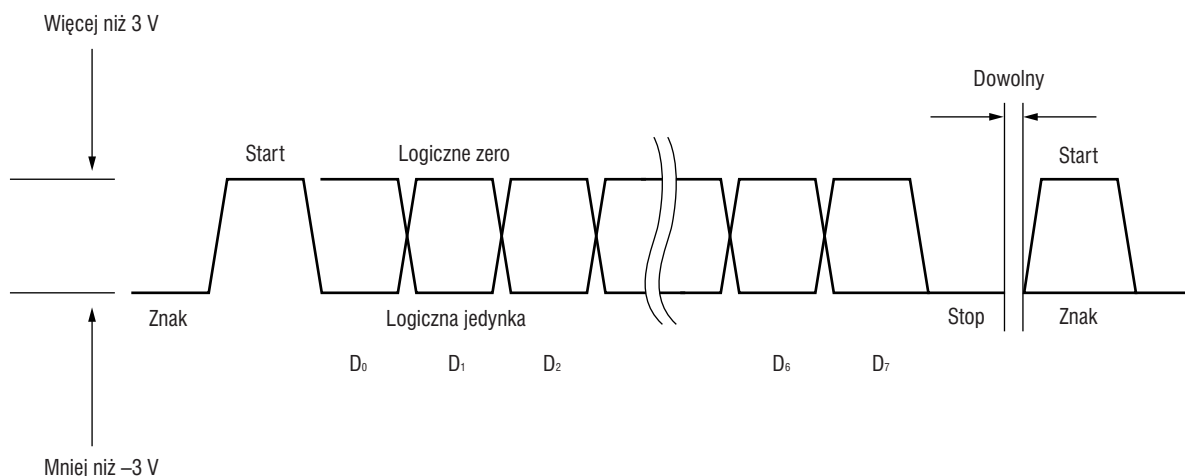
Rys. 3. Proste łącze światłowodowe przeznaczone do transmisji sygnałów na niewielką odległość

3. Transmisja sygnałów cyfrowych za pośrednictwem kabli koncentrycznych.

Kable współosiowe (koncentryczne) zapewniają doskonałą odporność na szkodliwe zakłócenia ze względu na to, że przewody sygnałowe są w pełni ekranowane. Należy również nadmienić, że jednolitość ich średnic i odstępów między przewodem (lub przewodami) sygnałowym a ekranem (często wielowarstwowym) zapewni dużą powtarzalność wartości impedancji falowej Z ($Z = 50 \Omega$, gdy chodzi o sygnały radiowe, i $Z = 75 \Omega$, gdy chodzi o sygnały telewizyjne). Niesie to za sobą doskonałe parametry i właściwości transmisyjne. Z powyższych powodów przewody koncentryczne (jako jedyne) są wykorzystywane do przesyłania sygnałów analogowych w zakresie częstotliwości radiowych. Są one stosowane w radioliniach, które mogą przenosić różne informacje, np. o alarmie. Były i są nadal stosowane w systemach telewizji przemysłowej. Magistrala zawierająca przewody ekranowane była dawniej stosowana w systemach alarmowych mieszanych typu DSC 4000 (gdzie ekran musiał być uziemiany) oraz na przykład w centralach Galaxy (gdzie ekran nie był uziemiany). We współczesnych centralach alarmowych magistralami są inne typy przewodów, które nie są kablami współosiowymi. Kable koncentryczne są powszechnie stosowane jako linie przesyłowe pomiędzy na przykład nadajnikami radiowymi a antenami w systemach monitoringu.

4. Transmisja sygnałów cyfrowych za pomocą światłowodów

Współczesne światłowody znajdują zastosowanie we wszystkich rodzajach sieci telekomunikacyjnych i informatycznych, poczynając od sieci lokalnych LAN (ang. *Local Area Network*), poprzez światłowodowe sieci dostępowe FITL (ang. *Fiber In The Loop*), a na sieciach transmisyjnych dalekiego zasięgu kończąc. Tego typu sieci dostępowe są również stosowane w elektronicznych systemach bezpieczeństwa, gdzie w grę wchodzi problem pewności transmisji oraz bezpieczeństwo transmisji (chodzi o niebezpieczeństwo podsłuchu tam, gdzie coraz częściej systemy alarmowe współpracują z sieciami informatycznymi). Technikę światłowodową zaczęto na szerszą skalę wykorzystywać w sieciach transmisyjnych w latach osiemdziesiątych, zastępując w urządzeniach typu PDH (ang. *Plesiochronous Digital Hierarchy*, czyli plezjochroniczna hierarchia cyfrowa) interfejsy elektryczne interfejsami optycznymi. Burzliwy rozwój (oraz ekspansja) techniki światłowodowej rozpoczął się wraz z budową sieci transmisyjnych opartych na standardach SONET (ang. *Synchronous Optical NETwork* – amerykański standard synchronicznej hierarchii optycznej) oraz SDH (ang. *Synchronous Digital Hierarchy* – synchroniczna hierarchia cyfrowa) i trwa on do dziś. Kable światłowodowe w porównaniu z kablami posiadającymi żyły metalowe mają



Rys. 4. Przebiegi napięć w magistrali transmisyjnej przy przesyłaniu jednego bajta danych łączem szeregowym typu RS232

wiele zalet. Bez wątpienia najważniejsze z nich to szerokie pasmo przenoszenia, małe tłumienie przesyłanego sygnału i duża odporność na zakłócenia zewnętrzne. Ponadto kable światłowodowe cechują się niewielkimi wymiarami i ciężarem, a podsłuch sygnałów w nich przesyłanych jest bardzo trudny. To wszystko spowodowało, że mimo pewnych wad, takich jak na przykład wpływ naprężeń mechanicznych na parametry światłowodu, dominują one we współczesnych sieciach transmisyjnych, a więc i w elektronicznych systemach bezpieczeństwa. Spotyka się je w peryferyjnych elektronicznych systemach alarmowych oraz w budynkach inteligentnych z okablowaniem strukturalnym. Stosowane są w administrowaniu i zarządzaniu wielkimi systemami alarmowymi. Warto nadmienić, że przesyłaniu sygnałów optycznych poprzez światłowody towarzyszą dwa najważniejsze zjawiska, a mianowicie: tłumienie i dyspersja. Od tłumienia światłowodu zależy zasięg transmisji (bez wzmacniania sygnału). Drugim zjawiskiem jest dyspersja światła, od której zależy pojemność kanału transmisyjnego. Emitowane impulsy światła nie są monochromatyczne. Najczęściej światłowody są dostępne w postaci kabli z zewnętrzną warstwą tworzywa sztucznego. Kable wyposażone są w specjalne złącze pozwalające na dołączenie do nich elementów promieniujących światło oraz detektorów światła, które produkowane są specjalnie z przeznaczeniem do współpracy ze światłowodami. Za pomocą światłowodów wyższej klasy można transmitować sygnały zajmujące pasmo o szerokości kilku GHz na odległość dziesiątków, a nawet setek kilometrów, ze stratami nie przekraczającymi ułamka dB/km. Kable światłowodowe można tak zaprojektować, aby ich dyspersja była znikomo mała. W przypadku kabli koncentrycznych nie jest to możliwe. W kablach dyspersyjnych sygnały o różnych częstotliwościach rozchodzą się z różnymi prędkościami i są różnie tłumione. Z tego powodu kształt sygnału na wyjściu jest inny niż kształt sygnału doprowadzony do jego wejścia. Na rys. 3 przedstawiono przykładowe bardzo proste łącze światłowodowe.

Nadajnikiem współpracującym ze światłowodem jest zwykłe dioda elektroluminescencyjna promieniująca w zakresie podczerwieni (a nie dioda laserowa), odbiornikiem zaś może być na przykład fototranzystor (element optoelektroniczny) lub dioda p-i-n.

5. Kody alfanumeryczne i transmisja szeregową

Przy wymianie danych alfanumerycznych pomiędzy średnio szybkimi urządzeniami, a więc np. pomiędzy płytą główną centrali alarmowej a modułami lub pomiędzy komputerem a centralą alarmową, najczęściej używa się 7-bitowego kodu ASCII oraz stosuje się transmisję szeregową bitów po jednej linii. Urządzenia nadawcze przesyłające dane w postaci kodów ASCII zwykle przesyłają jeszcze dodatkowy, ósmy bit, lecz nie jest on częścią kodu ASCII. Zwykle jest to sprzętowy bit parzystości (może oznaczać parzystość lub nieparzystość; najczęściej jego wartość jest zerowana i jest on ignorowany). Jednak czasami stosuje się go jako wskaźnik drugiej połowy rozszerzonego zbioru znaków (dalszych 128 znaków), w którym mogą być umieszczone litery greckie i inne znaki. Znaki te nie są objęte standardem. Szeregowe łącza są tak projektowane, że eliminują ósmy bit (nawet gdy jest on transmitowany), aby odtworzyć na wyjściu tylko kody ASCII, uniemożliwiając tym sa-



**Wyższa Szkoła
Menedżerska
w Warszawie**

Rekrutacja tel.: (22) 59 00 730



WYDZIAŁ INFORMATYKI STOSOWANEJ

Specjalności na studiach inżynierskich

- Technologie Internetowe
- Grafika Komputerowa
- Bezpieczeństwo Obiektów i Informacji
- Zarządzanie Systemami i Sieciami Komputerowymi



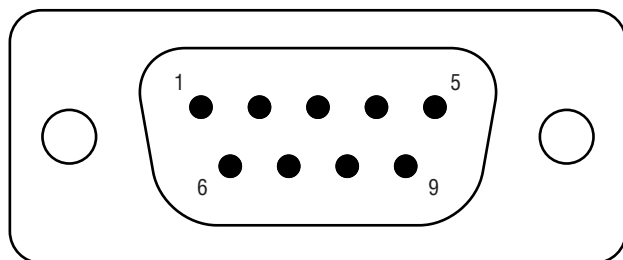
Informacje dodatkowe

Od października 2009 roku zostaje uruchomiona I edycja studiów podyplomowych „Bezpieczeństwo obiektów i informacji” (dwa semestry).

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



www.wsm.warszawa.pl



Rys. 5. Widok złącza (tzw. męskiego) DB-9 od strony wtyczki (stosowanego po stronie komputera) dla RS232

mym wykorzystanie go do przesyłania całego bajta informacji. Kody ASCII mają i inne wady, np. nie uwzględniają indeksów dolnych i górnych, wykładników i znaków greckich. To kłopotliwa sprawa, zważywszy, że symbole: Ω , μ , Π itp. często są używane. Można oczywiście kodem sterującym lub ciągiem takich kodów wskazać zmianę „kroju” czcionki lub alfabetu. Jest to typowy sposób stosowany w programach służących do redagowania tekstów technicznych, gdzie podprogram formatujący odpowiednio interpretuje kody ASCII następujące za kodami sterującymi. Biorąc pod uwagę rozmaitość znaków potrzebnych przy realizacji tekstów technicznych, nawet bardzo liczne, stałe uzupełnienie zbioru kodów ASCII po pewnym czasie okazałoby się niewystarczające. Kody ASCII (jak i inne kody alfanumeryczne) mogą być przesyłane równolegle w postaci grup 8-bitowych, czyli ośmioma oddzielnymi przewodami. Transmisję o średniej lub małej prędkości można zrealizować jako transmisję szeregową, gdyż wymaga ona najprostszego okablowania. Najbardziej popularne prędkości transmisji szeregowej to: 300, 1200, 2400, 4800, 9600 i 19200 Bd. Na rys. 4 przedstawiono zasadę transmisji szeregowej.

Szeregową transmisję kodów ASCII można zrealizować na kilka różnych sposobów. Oryginalna metoda, która powstała wiele dziesiątków lat temu, polegała na przełączeniu prądu o wartości 20 mA (czasem większym) z częstotliwością odpo-

wiadającą wybranej prędkości transmisji. Takie były początki. Obecnie dla średnich prędkości transmisji miejsce poprzedniczki zajął inny sposób transmisji określany jako RS232C (wprowadzony w 1969 r.), a nieco później (wprowadzony w 1986 r.) standard typu RS232D, w którym sygnałami są poziomy napięcie o obu polaryzacjach. Standard RS232 definiuje wymagania stawiane zarówno nadajnikowi, jak i odbiornikowi. Nadajnik musi wytwarzać napięcie o wartości od +5 V do +15 V dla niskiego stanu logicznego oraz napięcie o wartości od -5 V do -15 V dla wysokiego stanu logicznego. Prędkość zmian napięcia nie może być jednak większa niż 30 V/ μ s, a stopień wyjściowy nadajnika musi być odporny na zwarcia z wyjściami innych nadajników. Odbiornik musi być widziany jako obciążenie o rezystancji od 3 k Ω do 7 k Ω . Muszą być również przetwarzane na stan niski napięcia wyjściowe w zakresach od +3 V do +25 V, natomiast napięcie wejściowe o wartości od -3 V do -25 V – na stan wysoki. Przedstawione dane liczbowe dotyczą urządzeń testowych zasilanych napięciem znacznie wyższym niż centrale alarmowe, które jak wiadomo zasilane są napięciem 12 V. Wtedy poziomy napięć będą wyglądały nieco inaczej, ale proporcjonalnie. W standardzie RS232 logiczna „1” reprezentowana jest przez napięcie ujemne (jest to „znak”), a logiczne „0” reprezentowane jest przez napięcie dodatnie (tzw. „odstęp”).

Są także inne standardy łącz szeregowych, o których wspomniano wcześniej, a mianowicie: RS422, RS423, RS485. Kompatybilnym następcą standardu RS232 jest standard RS423, w którym zdefiniowano sposób transmisji za pomocą magistral transmisyjnych asymetrycznych o długościach do 1200 m z użyciem sygnałów bipolarnych przesyłanych z prędkością do 100 kBd. Transmisje magistralami transmisyjnymi symetrycznymi (również o długości 1200 m) pozwalają osiągnąć prędkości sięgające 10 MBd, tak jak i w standardzie typu RS422. Podobny do standardu RS422 jest standard RS485. Zostały w nim zdefiniowane dodatkowe wymagania umożliwiające korzystanie z jednego kabla transmitującego sygnały,

Nr	Kierunek	Oznaczenie	Nazwa angielska	Nazwa polska
1	DCE → DTE	DCD	<i>Data Carrier Detected</i>	sygnał wykrycia nośnej
2	DCE → DTE	RD	<i>Receive Data</i>	odbiór danych
3	DCE ← DTE	TD	<i>Transmit Data</i>	transmisja danych
4	DCE ← DTE	DTR	<i>Data Terminal Ready</i>	gotowość terminala
5	DCE — DTE	GND	<i>Signal Ground</i>	masa
6	DCE → DTE	DSR	<i>Data Set Ready</i>	gotowość „modemu”
7	DCE ← DTE	RTS	<i>Request to Send Data</i>	żądanie wysyłania
8	DCE → DTE	CTS	<i>Clear to Send Data</i>	gotowość wysyłania
9	DCE → DTE	RING	<i>Ring indicator</i>	wskaźnik dzwonka

Tab. 1. Linie sygnałowe złącza DB-9

z kilku nadajników i kilku odbiorników. Prędkości transmisji dla podanych typów RS podano wcześniej na rys. 2. W systemach alarmowych w różnych konfiguracjach zostały zastosowane różne typy transmisji szeregowej pomiędzy centralą alarmową a modułami. Producenci takich systemów podają zwykle stosowane przez siebie typy magistral transmisyjnych oraz ich długości zależnie od zastosowanego standardu RS. Często spotyka się jeden typ transmisji szeregowej. Bywają systemy, w których stosuje się i dwa standardy: RS232 i RS485. Obecnie produkowane komputery (zarówno stacjonarne, jak i przenośne laptopy) zwykle nie są niestety wyposażane w szeregowo złącza typu RS, a przejściówki z USB na RS nie zawsze pracują poprawnie. Trzeba o tym pamiętać.

Na zakończenie tego rozdziału artykułu przedstawiamy typowe złącze RS232 kabla do współpracy pomiędzy komputerem a centralą alarmową, gdzie stosowane jest złącze typu RJ. Taka konwencja współpracy komputera z płytą główną centrali została przyjęta przez firmę Satel z Gdańska.

W tabeli nr 1 podano oznaczenie poszczególnych wyprowadzeń (zwanych potocznie „pinami”) złącza typu DB-9. Nazwa sygnału DSR bywa mylnie tłumaczona jako „wypełniony bufor (gotowość transmisji)”, a DTR – jako „przetworzone dane (gotowość odbioru)”. W rzeczywistości oznaczają one gotowość urządzeń do pracy (czyli, że mają włączone zasilanie i wykonały reset po włączeniu) – angielskie nazwy „Data Set” i „Data Terminal” oznaczają urządzenia, a nie ich stany.

Istnieje wiele innych typów kabli łączy szeregowego typu RS232. Jednak najczęściej stosowany jest kabel z gniazdem przedstawionym na rys. 5. Oznaczenie poszczególnych wyprowadzeń przedstawiono w tabeli 1.

W tabeli nr 1 przedstawiono wszystkie ważne linie sygnałowe. TD i RD to linie transmisji i odbioru danych, RTS i CTS to linie sygnalizujące odpowiednio: gotowość do wysłania danych i gotowość do odebrania danych. DTR, DSR i DCD sygnalizują odpowiednio: gotowość modułu (terminalu), gotowość zbioru danych oraz gotowość łącza do transmisji. Poza tym jest masa sygnałowa (wyprowadzenie 5). Urządzenie typu DTE (ang. *Data Terminal Equipment*, czyli urządzenie końcowe) uaktywnia linie RTS i DTR, gdy jest gotowe do przyjęcia danych. Podobnie urządzenie typu DCE (ang. *Data Communications Equipment*, czyli urządzenie komunikacyjne transmisji danych) w chwili gotowości do przyjęcia danych uaktywnia linie CTS i DSR. Niektóre moduły typu DTE, zanim podejmą jakąkolwiek akcję, również oczekują na uaktywnienie linii DCD. Do przesyłania informacji (danych) liniami sygnałowymi używa się napięć bipolarnych o wartościach zgodnych ze standardem RS232, przy czym linie danych (TD, RD) są aktywne dla napięć ujemnych, natomiast linie sterujące (RTS, CTS, DSR, DTR, DCD) są aktywne dla napięć dodatnich.

Na rys. 6 przedstawiono kilka wybranych systemów alarmowych o konfiguracji mieszanej, w których zastosowano różne formaty transmisji sygnałów oraz różne liczby magistral transmisyjnych. Są to systemy rzeczywiste pracujące w obiektach użyteczności publicznej (wcześniej opisywane w artykułach autorów niniejszego cyklu zamieszczonych w *Zabezpieczeniach*. Na tych rysunkach pokazano transmisję sygnałów w różnych formatach RS.

bpt

MITHO

Ekran dotykowy 16:9
Rozdzielczość 480x272

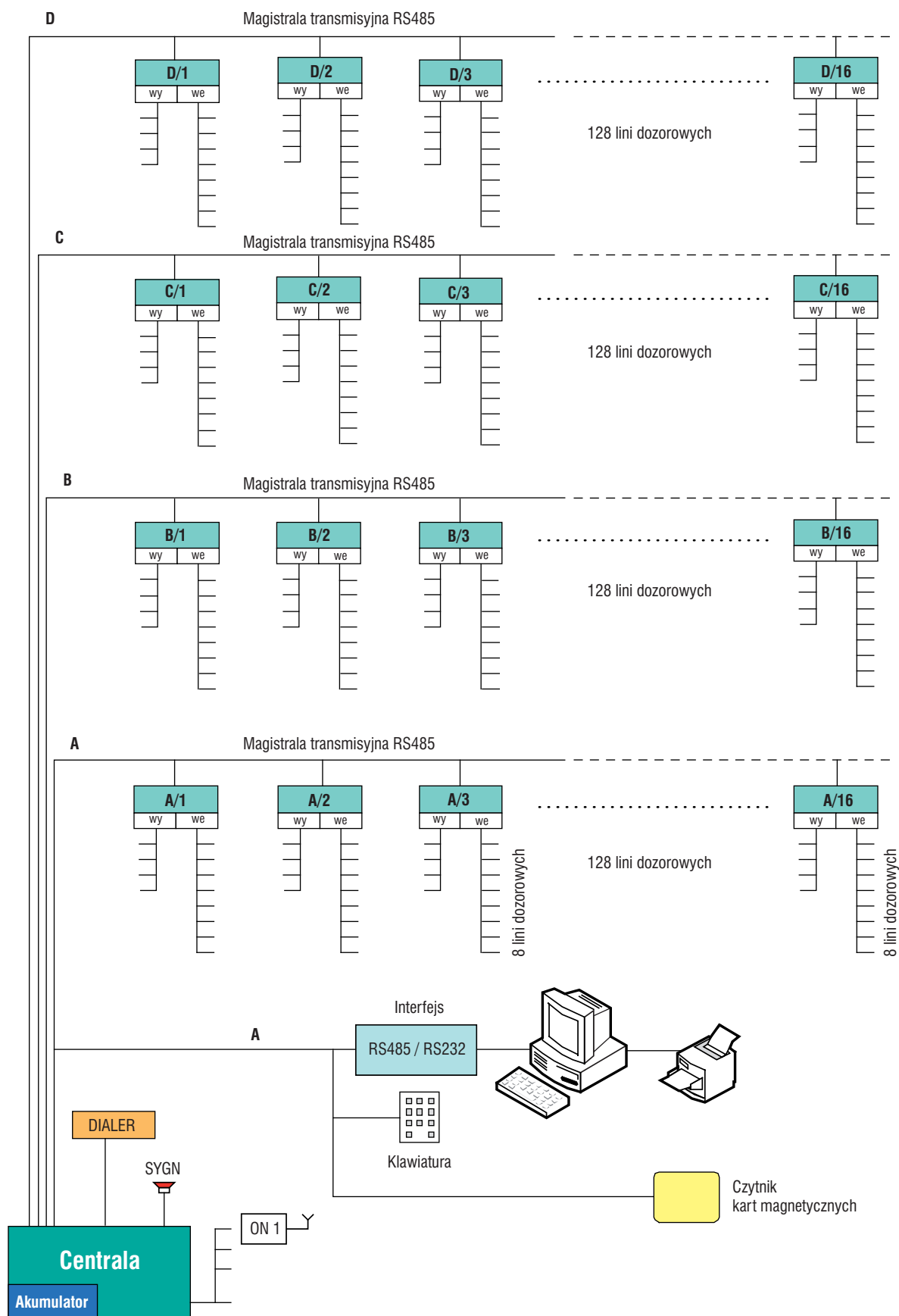
elektro 2008
produkt

3 w 1

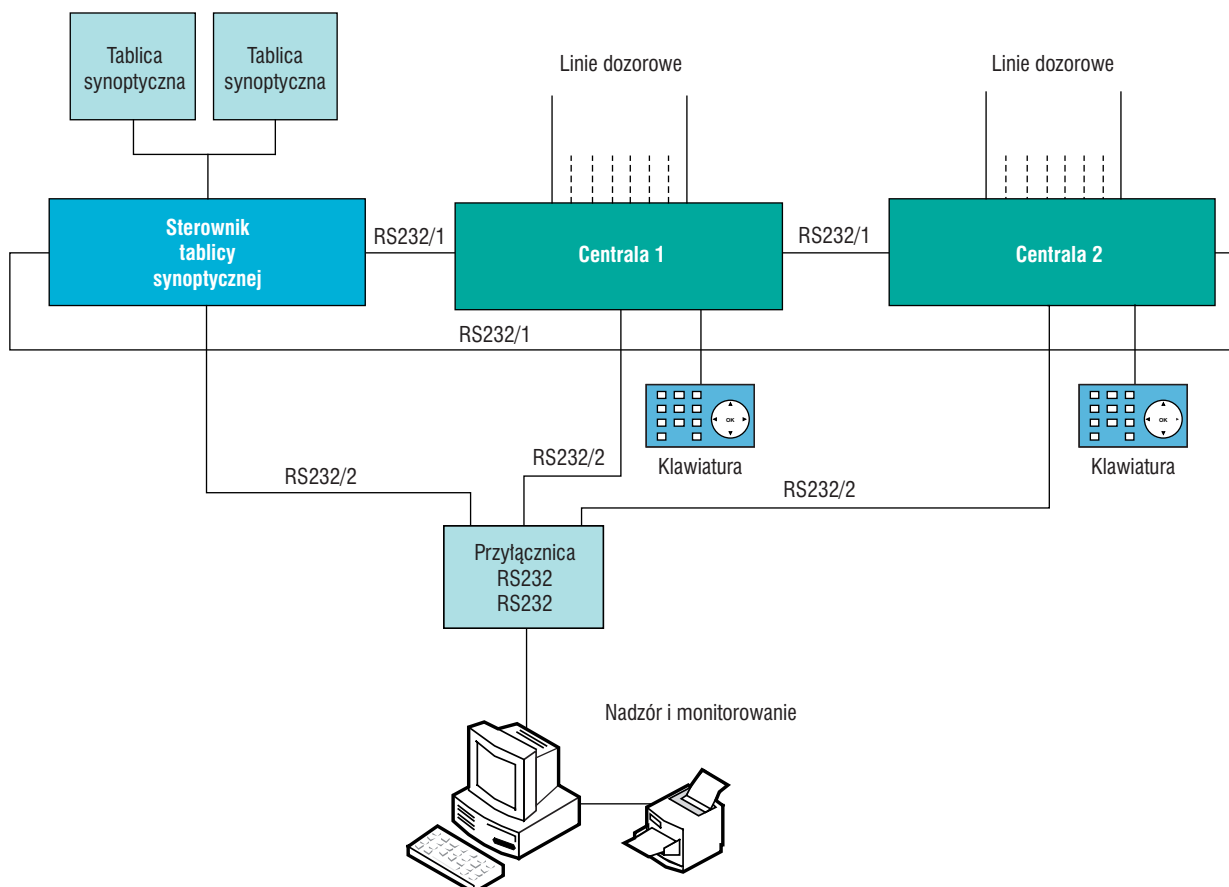
- System wideofonowy
- Inteligentny dom
- System alarmowy

BPT znów zaskakuje

www.bpt.pl



Rys. 6a. Przykładowe rozwiązania różnych wybranych systemów alarmowych, a w nich transmisja sygnałów za pośrednictwem magistral transmisyjnych (wybrane układy)



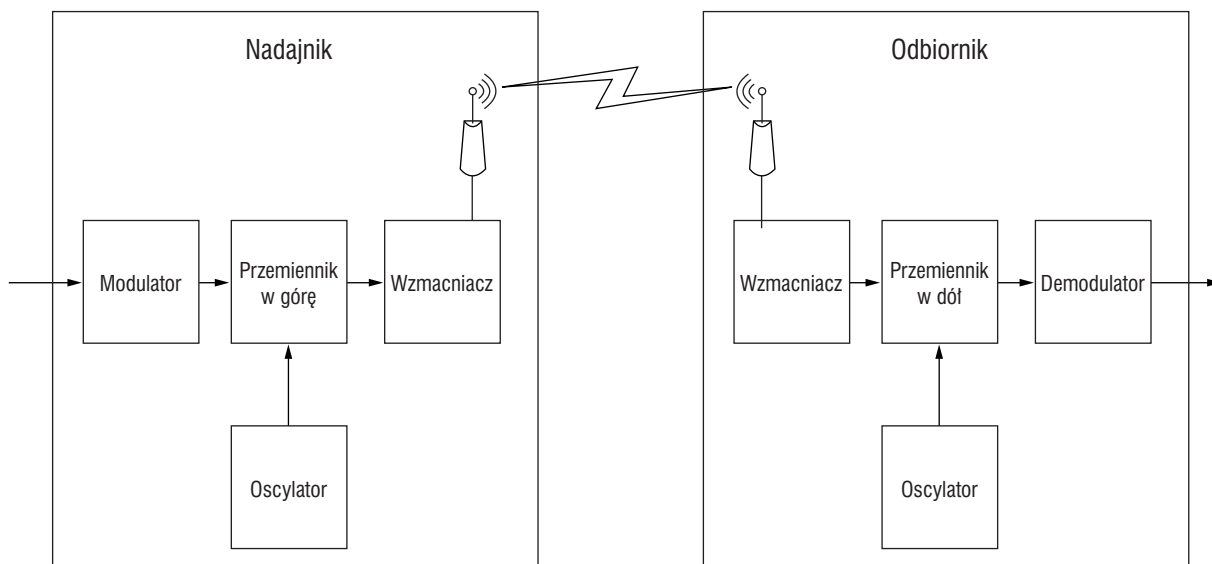
Rys. 6b. Przykładowe rozwiązania różnych wybranych systemów alarmowych, a w nich transmisja sygnałów za pośrednictwem magistral transmisyjnych (wybrane układy)

6. Linie radiowe jako medium transmisyjne

Zastosowanie linii bezprzewodowych stanowi poważny problem ze względu na coraz częstszą konstrukcję systemów alarmowych, gdzie wiele modułów systemu komunikuje się z jednostką centralną drogą radiową (częstotliwość transmisji to m.in. ok. 433 MHz). Podobnie tam, gdzie system alarmowy jest monitorowany, mogą być stosowane nadajniki (o opcjach: offline i online), a więc bez potwierdzenia i z potwierdzeniem. Stosowane są również systemy GSM (coraz powszechniej), gdzie częstotliwość łącza wynosi 900 lub 1800 MHz. Informacje przesyłane są zazwyczaj za pośrednictwem SMS-ów. Bardzo często z linią dozоровą współpracuje radiowe łącze napadowe. Istnieje bardzo wiele takich rozwiązań, jak choćby słynny Nokton pracujący np. na częstotliwości 27 MHz (CB radio) z modulacją kodową do współpracy na przykład dwóch systemów, które trzeba ze sobą połączyć, a droga kablowa jest niemożliwa. Należy pamiętać, że jest to tzw. pasmo obywatelskie. Są i inne częstotliwości urządzeń nadawczo-odbiorczych znacznie bardziej profesjonalnych niż to podane powyżej. Urządzenia tej firmy pracują w pasmach: 40 MHz, 136 MHz do 174 MHz, 400 MHz do 470 MHz z cyfrową modulacją. Ten temat ze względu na swoją złożoność wymaga odrębnego opisu. Istnieją profesjonalne linie radiowe mikrofalowe, które mogą spełniać rolę mediów transmisyjnych. Stosuje się je w systemach alarmowych o specjalnym przeznaczeniu.

Na rys. 7 przedstawiono uproszczony schemat blokowy radio linii mikrofalowej, która umożliwia łączność i transmisję sygnałów na duże odległości (anten-y muszą się „widzieć”).

Podstawowymi elementami składowymi nadajnika są odpowiednio: modulator, przemiennik w górę, oscylator, wzmacniacz i antena nadawcza, natomiast odbiornika: antena odbiorcza, wzmacniacz, przemiennik w dół, oscylator i demodulator. W przypadku zastosowania sieciowego urządzeń ich wyposażenie w dodatkowe bloki, związane z przetwarzaniem sygnałów cyfrowych, zarządzaniem i sterowaniem, jest bardzo zróżnicowane. Ze względów bezpieczeństwa transmisja sygnałów za pośrednictwem radiowych linii mikrofalowych zwykle jest kodowana. Stosowanie linii radiowych jest celowe wszędzie tam, gdzie budowa linii kablowych (w tym magistral transmisyjnych) nie jest uzasadniona ekonomicznie. Na realizację mikrofalowych linii radiowych potrzeba niewiele czasu. Należy jednak pamiętać, że istnieją ściśle określone zasady instalacji tych urządzeń. Na ich drodze nie mogą pojawiać się żadne przeszkody, takie jak budynki, drzewa itp. Wynika to z własności propagacyjnych w pasmach mikrofalowych. Stosowane są one w radiokomunikacji, w systemach telefonii komórkowej (np. w stacjach bazowych), w radiofonii, w systemach bezpieczeństwa, w bezprzewodowych systemach informatycznych: WiFi (ang. *Wireless Fidelity*) i WiMAX (ang. *Worldwide Interoperability for Microwave Access*).



Rys. 7. Uproszczony schemat blokowy radiolinii mikrofalowej

7. Wnioski

W artykule autorzy omówili różne często spotykane formaty transmisyjne, które są stosowane w elektronicznych systemach bezpieczeństwa (od bardzo prostych po złożone). Zdajemy sobie sprawę, że podane tu zostały tylko podstawowe informacje dotyczące sposobów transmisji sygnałów w systemach alarmowych, bez znajomości których budowa i konfiguracja systemów alarmowych byłaby niemożliwa. Nie podano szczegółów dotyczących budynków inteligentnych ani nie omówiono poważnych problemów transmisyjnych z nimi związanych i decydujących o administrowaniu oraz zarządzaniu m.in. systemami alarmowymi. Autorzy nie opisali również problematyki transmisji sygnałów alarmowych za pośrednictwem sieci informatycznych. Naturalnie to zupełnie odrębny i złożony problem, który choćby ze względu na bezpieczeństwo informacji oraz złożoność sieci warto opisać. Wieloletnie doświadczenie autorów – dotyczące problematyki elektronicznych systemów bezpieczeństwa, ich konfigurowania, programowania, diagnostyki oraz badań eksploatacyjno-niezawodnościowych – pozwoliło przybliżyć czytelnikom problemy związane z komunikowaniem się różnych układów wchodzących w skład systemów alarmowych. Informacje przesyłane za pomocą magistral transmisyjnych, a więc komunikowanie się poszczególnych bloków systemów alarmowych, to ważne zagadnienie również w aspekcie zakłóceń radioelektrycznych, bardzo szkodliwych dla poprawnej pracy systemów alarmowych szczególnie rozległych, a więc rozproszonych. Autorzy będą również chcieli w przyszłości przekazać informacje dotyczące tej tematyki, związanej z kompatybilnością elektromagnetyczną. Wiąże się to również z problematyką transmitowania sygnałów za pośrednictwem różnych formatów i mediów transmisyjnych z zachowaniem bezpieczeństwa danych. Ważnym problemem jest transmisja danych w systemach alarmowych chroniących obiekty specjalnego przeznaczenia. Jest to problem, który wymaga sporej wiedzy merytorycznej. Nasuwa się więc jeden zasadniczy wniosek, że magistrale transmisyjne, którymi odbywa się transmisja danych dotyczących systemów alarmowych, stanowią „układ nerwowy” całego systemu bezpieczeństwa.

doc. dr inż. Waldemar Szulc

WSM w Warszawie

Wydział Informatyki Stosowanej

Zakład Bezpieczeństwa Obiektów i Informacji

współpracownik WAT

Wydział Elektroniki

dr inż. Adam Rosiński

WSM w Warszawie

Wydział Informatyki Stosowanej

Zakład Bezpieczeństwa Obiektów i Informacji

Politechnika Warszawska

Wydział Transportu

Zakład Telekomunikacji w Transporcie

współpracownik WAT

Wydział Elektroniki

Bibliografia

1. Haykin S.: *Systemy telekomunikacyjne*. Tom I i II, WKiŁ, Warszawa 2004.
2. Horowitz P., Hill W.: *Sztuka elektroniki*. Tom I i II, WKiŁ, Warszawa 2006.
3. Instrukcje serwisowe central DSC, Satel, Galaxy, Rankor.
4. Kula S.: *Systemy teletransmisyjne*, WKiŁ, Warszawa 2004.
5. Nawrocki W.: *Komputerowe systemy pomiarowe*. WKiŁ, Warszawa 2006.
6. Norma PN-EN 50131-1:2007 *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe*.
7. Szulc W., Rosiński A.: *Problemy eksploatacyjno-niezawodnościowe rozproszonego systemu bezpieczeństwa, „Zabezpieczenia”* Nr 1 (47)/2006, wyd. AAT, Warszawa 2006.
8. Szulc W., Rosiński A.: *Prace własne*, WSM, Warszawa 2006 do 2008.
9. Szulc W., Rosiński A.: *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków (część I – analogowa)*, Oficyna Wydawnicza WSM, Warszawa 2008.
10. <http://pl.wikipedia.org/wiki/RS-232>

Nowoczesny sposób komunikacji

Moduły GPRS-T1, GPRS-T2

GPRS-T1, dzięki funkcji konwersji kodów zdarzeń do postaci transmitowanej przy pomocy technologii GPRS lub do formatu wiadomości SMS, umożliwia projektowanie systemów alarmowych bez konieczności uwzględniania obecności linii telefonicznej. Wykorzystanie technologii GPRS pozwala na obniżenie kosztów związanych z monitoringiem. Urządzenie oferuje ponadto możliwość powiadamiania przy pomocy wiadomości SMS o wystąpieniu wybranych zdarzeń.

Podstawową funkcją modułu GPRS-T2 jest informowanie o zmianie stanu wejść przy pomocy kodów zdarzeń wysyłanych do stacji monitorujących w formie transmisji GPRS lub wiadomości SMS. Funkcjonalność ta pozwala monitorować pracę różnych urządzeń, w tym central alarmowych nieposiadających komunikatora telefonicznego. Dzięki wejściom analogowym moduł może być z powodzeniem stosowany w automatyce.

Nowość



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

DVS

DVS Visual Software

Oprogramowanie do wizualizacji
systemów alarmowych **DSC**



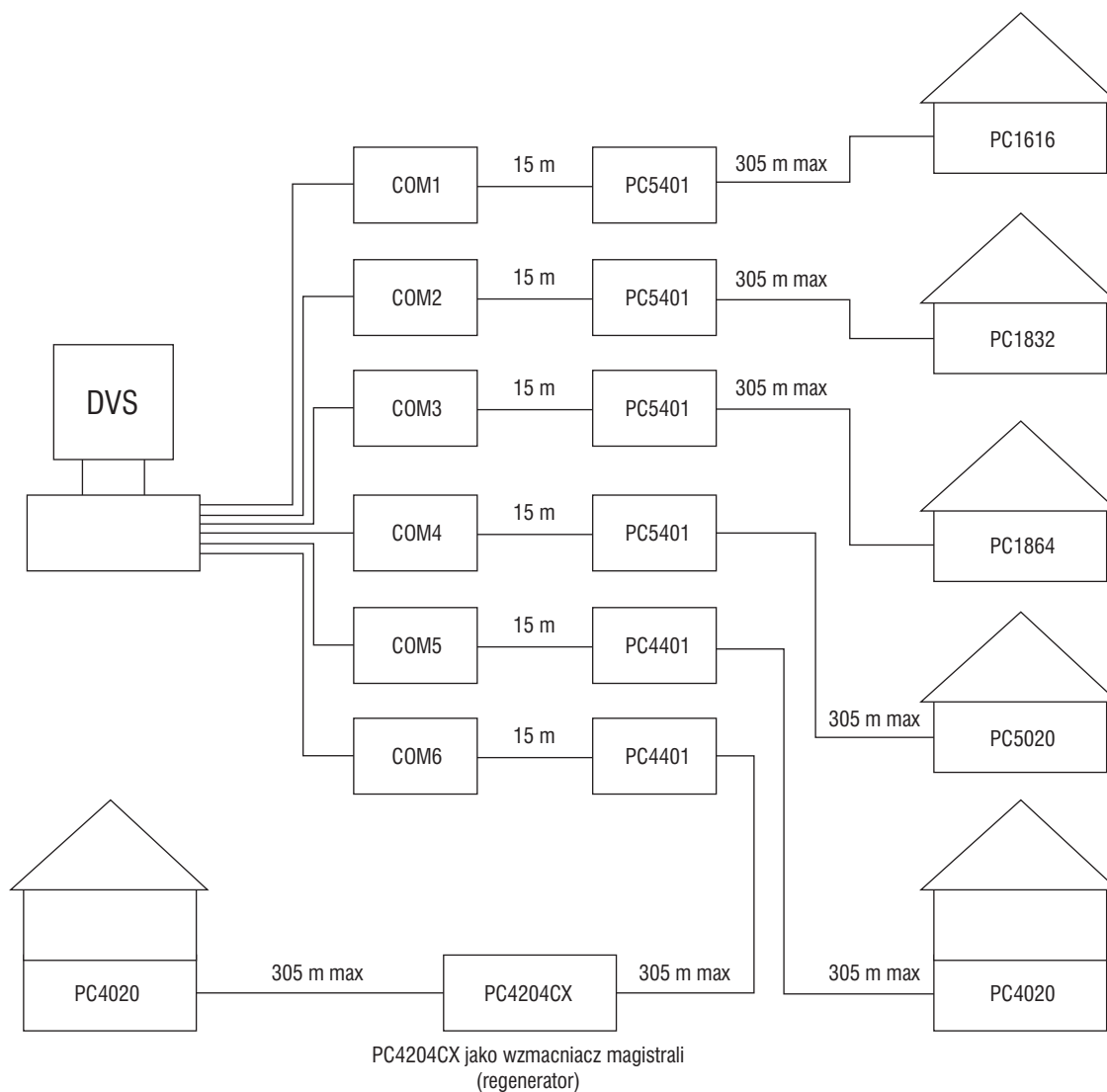
Zabezpieczenia elektroniczne, takie jak systemy alarmowe, kontrola dostępu oraz systemy ostrzegania przeciwpożarowego, często wymagają urządzeń lub oprogramowania umożliwiających wizualizację stanów poszczególnych czujników. W przypadku systemów alarmowych istnieje możliwość odczytania statusu poszczególnych podsystemów oraz stanów linii alarmowych bezpośrednio z klawiatury lub z tablic synoptycznych. Dodatkowym narzędziem obrazującym status danego obiektu jest DVS Visual Software czyli oprogramowanie służące do wizualizacji systemów alarmowych bazujących na centralach DSC.

Program wykorzystuje komunikację z centralami przy użyciu dedykowanych modułów systemowych, wyposażonych w porty szeregowy RS232. Zastosowanie takiego rozwiązania daje następujące możliwości:

- wizualizację stanu wszystkich podsystemów i linii dozorowych w trybie online,
- zastosowanie podkładów map dla poszczególnych pomieszczeń lub całego obiektu, na których istnieje możliwość rozmieszczenia kontrolerek symbolizujących linie dozorowe, podsystemy itp.,
- zebranie kilku map na jednym podkładzie oraz łatwe przełączanie pomiędzy mapami (dzięki zastosowaniu miniatur),
- sterowanie głównymi funkcjami systemu bezpośrednio z komputera, m.in. uzbrajanie, rozbrajanie, ustawianie czasu w centrali, wyzwalanie wyjść PGM, blokowanie linii (tylko MAXSYS),
- sygnalizację usterek systemowych,
- rejestrację zdarzeń odebranych z centrali oraz zdarzeń administracyjnych programu,
- wydruki oraz archiwizację rejestru zdarzeń systemu wizualizacji,

- edycję nazw podsystemów, nazw linii dozorowych, nazw użytkowników oraz nazw wyjść PGM dla poszczególnych obiektów (dzięki czemu do rejestru zdarzeń zapisywana jest także nazwa linii, nazwa podsystemu oraz nazwa użytkownika, którego dotyczy zdarzenie),
- wizualną oraz akustyczną sygnalizację stanów alarmowych, zarówno z wyjścia głośnikowego, jak i z wewnętrznego buzzera komputera.

Teraz kilka słów o sposobie połączenia komputera z zainstalowanym oprogramowaniem DVS Visual Software z centralami alarmowymi. Komunikacja umożliwiająca wizualizację oraz sterowanie posiadanym systemem alarmowym realizowana jest za pomocą modułu PC5401 (w przypadku central serii Power) oraz PC4401 (dla serii Maxsys). Maksymalne odległości transmisji poprzez interfejsy RS232 w linii komputer – moduł wynoszą 15 m. Odległości te można przedłużyć przy wykorzystaniu konwerterów RS232/RS485. Zyskujemy wówczas zwiększenie zasięgu działania do ok. 1200 m. Innym rozwiązaniem może być zastosowanie serwerów portów szeregowych (wirtualne porty szeregowy poprzez sieć komputerową TCP/IP, np. UT-4 [Roger], DE-211, DE-311 [MOXA]). Zaletą tego rozwiązania jest brak konieczności zastosowania przejściówek USB/RS232 oraz



Rys. 1. Przykładowa konfiguracja systemu wizualizacji DVS

tw. hubów do powielenia liczby portów RS232 (w przypadku integracji).

Uwaga: konwertery USB/RS232 (tzw. przejściówki) często mają tendencję do zawieszania portu USB, co może powodować nieprawidłową komunikację komputera z modulem PC4401/PC5401.

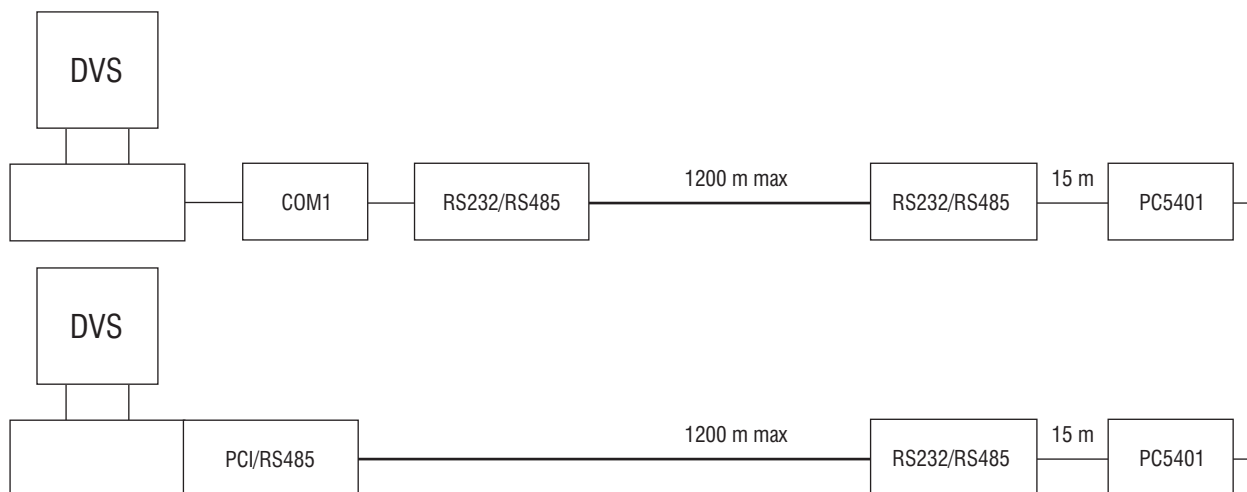
Rys. 1 przedstawia przykładową konfigurację systemu wizualizacji, opartą na programie DVS. Liczba obsługiwanych central uzależniona jest od liczby portów RS232 w komputerze (maksymalnie do 256). W standardzie RS232 dystans 15 m powinien być wystarczający, aby podłączyć komputer z modułami PC5401 lub PC4401. Współpraca centrali alarmowej z modułami realizowana jest za pomocą czteroprzewodowej magistrali COMBUS/KEYBUS. Długość magistrali ograniczona jest do ok. 305 m. Dotyczy to zarówno central serii Power (PC5020, PC1616, PC1832, PC1864), jak i serii Maxsys (PC4020A). W przypadku PC4020A można jednak zastosować zasilacz PC4204CX służący jako regenerator magistrali (patrz rys. 1). Zastosowanie takiego rozwiązania daje możliwość zwiększenia długości magistrali o następne 305 m. Centrala PC4020A może obsłużyć do 16 modułów zasilaczy, co powoduje, że odległość PC4401 od centrali może wynieść nawet ok. 5 km ($305 \text{ m} + 16 \times 305 \text{ m} = 5185 \text{ m}$).

Innym sposobem na zwiększenie odległości pomiędzy centralą a modulem jest zastosowanie konwerterów sygnału RS232 na inny sygnał, np. na RS485, RS422 lub TCP/IP.

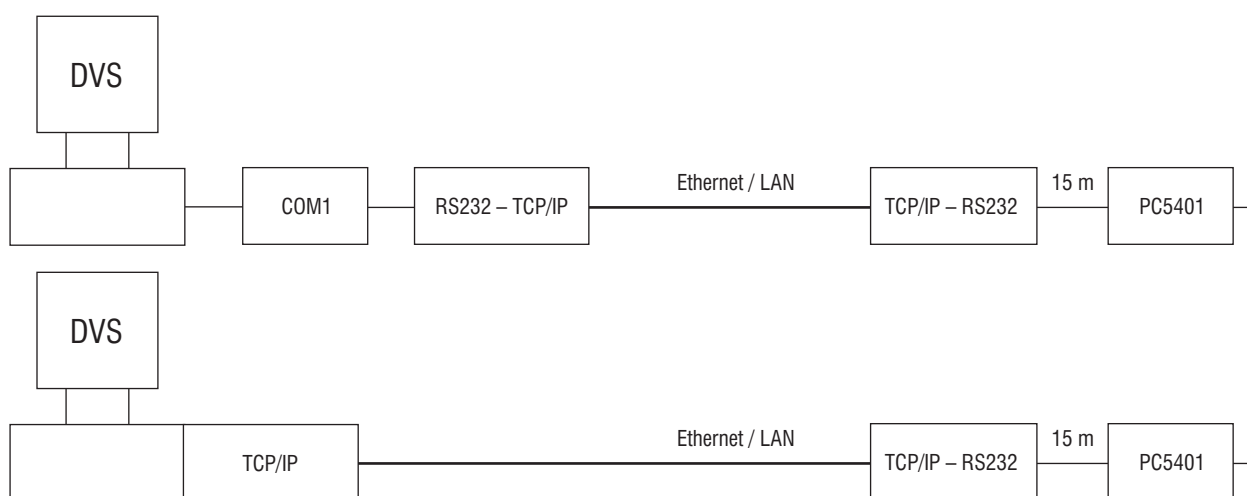
Rys. 2 obrazuje dwa sposoby wykorzystania konwerterów RS485. W pierwszym przypadku konwerterami mogą być dwa identyczne urządzenia, takie jak VC-485 (Kantech), UT2 (Roger) lub inne. W drugim przypadku (Rys. 3) konwerterem wyjściowym jest karta wieloportowa PCI/RS485.

Rys. 3 przedstawia dwa sposoby wykorzystania konwerterów sieciowych LAN na sygnały RS232. Pierwszy schemat obrazuje konwersję RS232 na TCP/IP oraz analogicznie TCP/IP na RS232. Można tu wykorzystać urządzenia, takie jak UT4 (Roger), DE-211, DE-311 (MOXA) oraz inne dostępne na rynku. W komputerze konwerter widoczny jest jedynie jako port COM, a cała transmisja sieciowa odbywa się pomiędzy konwerterami, pozostając dla komputera i centrali alarmowej „przezroczystą”.

Ze względów ekonomicznych praktyczniejsze jest zastosowanie konwerterów tylko po jednej stronie sieci LAN. Wystarczy, że komputer podłączony jest do lokalnej sieci, a wówczas po zainstalowaniu odpowiedniego oprogramowania (sterowników) urządzenia sieciowe widoczne są jako porty szeregowo RS232.



Rys. 2. Przykładowy schemat wykorzystania transmisji RS485



Rys. 3. Przykładowy schemat wykorzystania sieci Ethernet/LAN

Lp.	Typ centrali	Wersje
1	PC1616	v.4.1, v.4.2
2	PC1832	v.4.1, v.4.2
3	PC1864	v.4.1, v.4.2
4	PC5020	v.3.0, v.3.2
5	PC4020A	v.3.3, v.3.5

Tab. 1. Zestawienie obsługiwanych central alarmowych

Program DVS Visual Software umożliwia jednoczesną obsługę wielu central alarmowych.

Każdy system alarmowy wymaga podłączenia osobnego portu szeregowego. Rys. 4 przedstawia przykład podłączenia różnych central (mogą być również takie same modele) do jednego komputera z wykorzystaniem sieci Ethernet/LAN. Dzięki wykorzystaniu programu DVS podłączenie to pozwala na kompletną obsługę systemu alarmowego, umożliwiając wizualizację stanu podsystemów, stanu linii dozorowych, usterek, a także dostęp do funkcji włączania i wyłączania z dozoru podsystemów, blokowania linii dozorowych w PC4020A (w serii Power blokowanie linii dozorowych z poziomu programu nie jest możliwe) oraz aktywację wyjść użytkowych PGM (np. do wyzwolenia rygła w drzwiach przy wejściu do recepcji itp.).

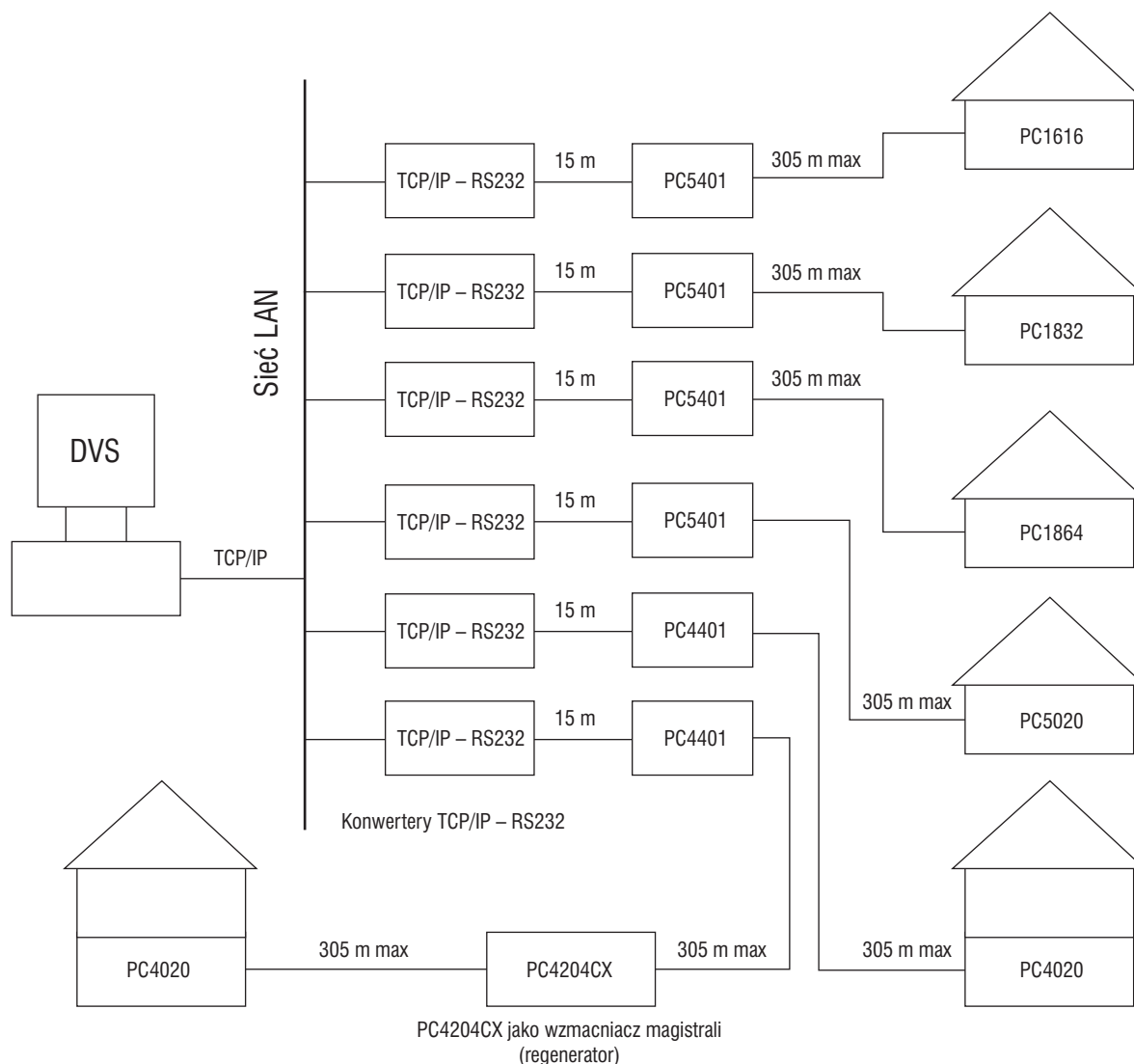
Co jednak z obiektami takimi jak „zamknięte” osiedla?

W tym przypadku nie jest wskazane, aby ochrona miała możliwość wyłączenia z dozoru systemu alarmowego w danym lokalu. Każde mieszkanie może być osobnym, niezależnym systemem alarmowym. Nie ma konieczności monitorowania przez ochronę osiedla wszystkich usterek, wyzwalania wyjść użytkowych oraz stałego nadzorowania, za pomocą którego kodu system został załączony w dozór. W tej sytuacji proponowane jest następujące rozwiązanie: wysłanie najbardziej znaczących sygnałów z każdej centrali i odebranie ich w jednej centrali zbiorczej.

Z każdego lokalu wyprowadzone są sygnały alarmowe z wyjść programowalnych sterujących przekaźnikami. Styki przekaźników podłączone są w centrali PC4020A do 24-godzinnych linii dozorowych. Ponieważ centrala nie wymaga włączania w dozór i może po kilku alarmach ignorować przychodzące sygnały alarmowe, należy pamiętać, aby wyłączyć liczniki naruszeń dla linii dozorowych.

Zalety przedstawionej konfiguracji

- Każdy system alarmowy w danym lokalu traktowany jest jako odrębny, niezależny system, który może być także monitorowany w CMA (Centrum Monitorowania Alarmów);



Rys. 4. Przykładowa konfiguracja systemu wizualizacji wykorzystująca sieć LAN

- Ochrona osiedla nie ma dostępu do wyłączania z dozoru podsystemów w mieszkaniach;
- W razie potrzeby istnieje możliwość szybkiej reakcji lokalnej ochrony (każda linia umieszczona jest na mapie obiektu oraz opisana, np. numerem lokalu i rodzajem alarmu);
- Sterowanie wyjściami użytkowymi z poziomu komputera, np. w celu otwarcia furtki, bramy lub drzwi do recepcji;
- Śledzenie zdarzeń skupione przede wszystkim na alarmach priorytetowych oraz zdarzeniach z centrali, która zbiera sygnały z poszczególnych mieszkań;
- Brak konieczności zastosowania wielu modułów oraz portów szeregowych.

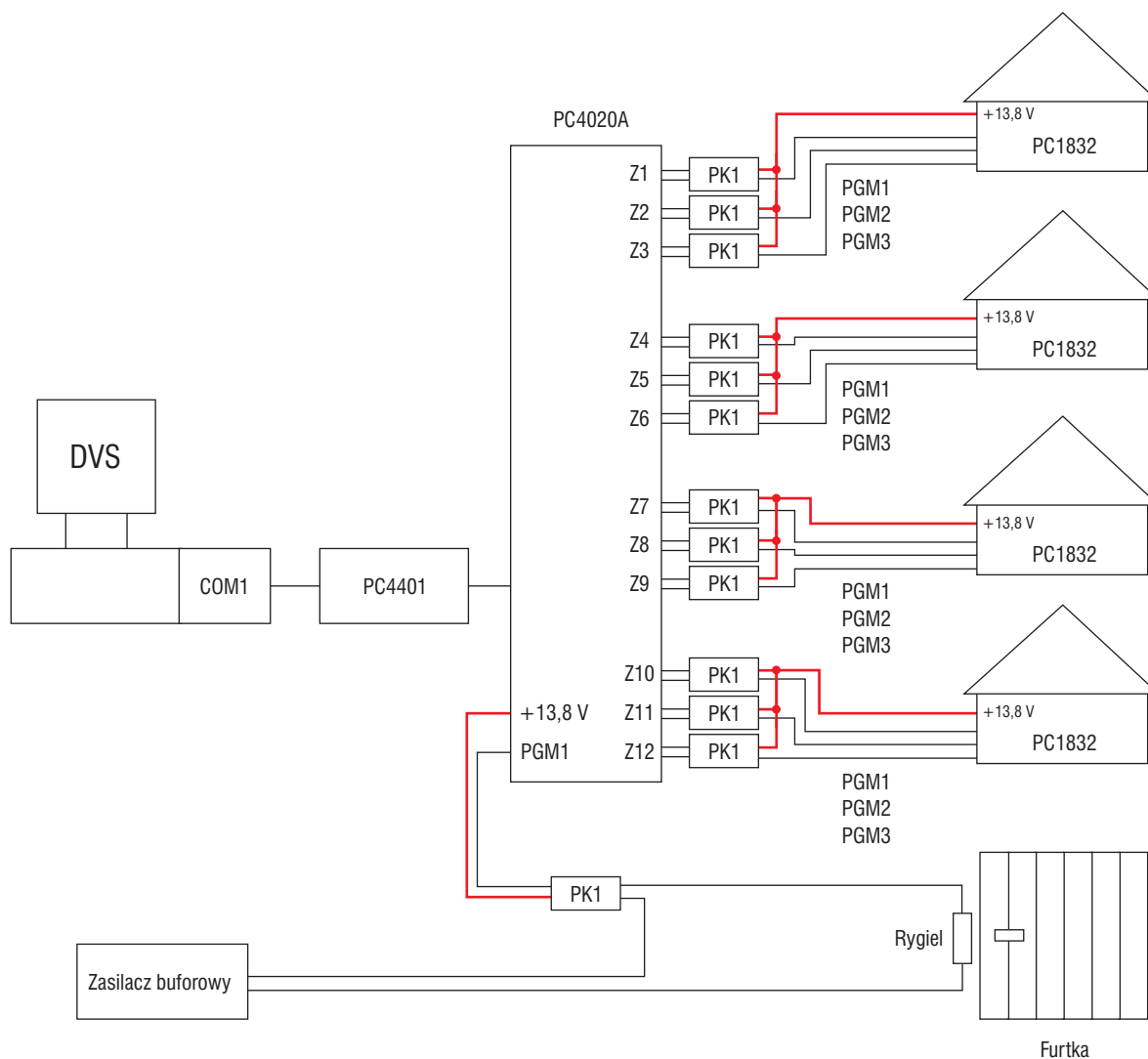
Głównym przeznaczeniem programu DVS Visual Software jest wizualizacja systemów alarmowych w obiektach, czyli odwzorowanie rozmieszczenia linii dozorowych (czujek) na odpowiednich mapach. Mapy mogą zawierać plany budynków, pięter, mieszkań lub całych osiedli oraz obiektów złożonych z wielu budynków. Plan należy wcześniej narysować w dowolnym programie graficznym lub wyeksportować z gotowej dokumentacji, np. z programu AutoCad. Czujki alarmowe naniesione na mapę w odpowiednie miejsca odwzorowują wszystkie możliwe stany (gotowość, naruszenie, sabotaż, usterka, alarm).

Rys. 6 przedstawia przykład rozmieszczenia czujek na podłożonym planie parterowego domu. Kontrolki czujek zaznaczone na czerwono odwzorowują stan alarmowania, podczas którego widoczny jest także sygnalizator oraz dźwiękowa sygnalizacja informująca o zdarzeniu. Klawiatura umieszczona na rysunku umożliwia włączanie oraz wyłączanie podsystemów po wprowadzeniu kodu.

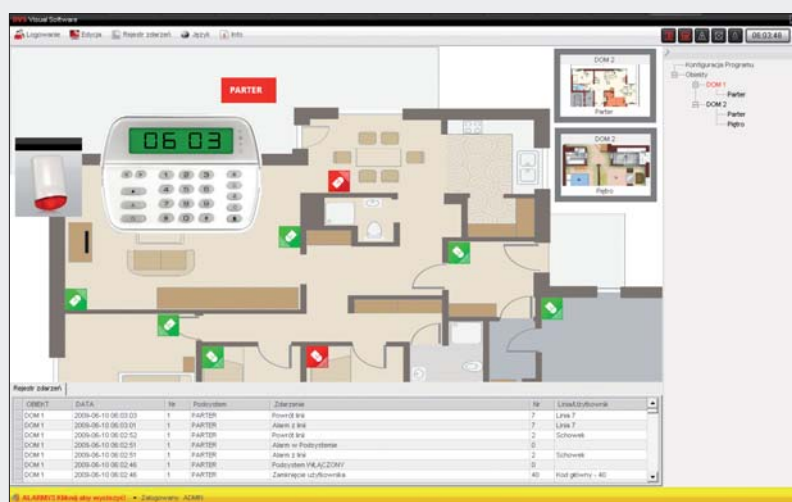
Program DVS zawiera rejestr zdarzeń, w którym zapisane są wszystkie zdarzenia o alarmach, włączeniach przez użytkownika, usterkach, a także zdarzenia systemowe. Przeglądanie rejestru ułatwia filtrowanie rodzaju zdarzeń. Funkcja archiwizacji zdarzeń umożliwia przechowywanie danych w pliku, który można otworzyć za pomocą programu DVS („przeglądarka archiwum”) a następnie wygenerować raport przeznaczony do wydruku. W programie DVS Visual Software dostępne są również funkcje generowania raportów, rozmieszczenia czujek na mapach oraz opisów nazw linii, podsystemów, użytkowników i wyjść użytkowych.

Zalety programu DVS Visual Software

DVS Visual Software jest bezpłatny. Dla zarejestrowanych użytkowników jest on dostępny na stronie internetowej AAT Holding. Program przeznaczony jest do wizualizacji zarówno



Rys. 5. Przykład konfiguracji systemu dla małego „zamkniętego” osiedla



Rys. 6. Widok przykładowej konfiguracji mapy programu DVS

Instalator po zakończeniu procesu instalacji systemu alarmowego może wykorzystać bardzo pomocne narzędzie, tzw. „Test instalacji”. Funkcja ta została stworzona w celu szybkiego i prostego zweryfikowania poprawności działania czujek dozorowych. Dodatkowo instalator lub administrator programu ma możliwość pobierania opisów nazw linii, podsystemów, wyjść użytkowych, a także nazw użytkowników (tylko dla PC4020A). Pobieranie opisów dostępne jest w oknie „Edycja opisów” w zakładce DLS. Operacja pobierania wymaga podłączenia przewodu PC-LINK oraz zainicjowania połączenia (tak jak w programie DLS2002).

małych obiektów bazujących na jednej centrali alarmowej, jak i dla dużych obiektów, wymagających zastosowania wielu central (niekoniecznie tego samego typu). Użytkownikiem programu może być zarówno odbiorca końcowy (osoba prywatna), jak i pracownik ochrony (np. w recepcji) czy instalator.

Serdecznie zapraszamy do zapoznania się z oprogramowaniem DVS Visual Software, dostępnym na stronie www.aat.pl.

Sylwester Stryjek
AAT Holding



DVS Visual Software

Oprogramowanie do wizualizacji systemów alarmowych **DSC**

Wizualizacja on-line Zarządzanie mapami obiektów Sygnalizacja i rejestracja zdarzeń alarmowych



nowość!
2009

DVS Visual Software służy do wizualizacji systemów alarmowych opartych na centralach DSC, przy użyciu dedykowanych modułów systemowych, wyposażonych w porty szeregowo RS-232

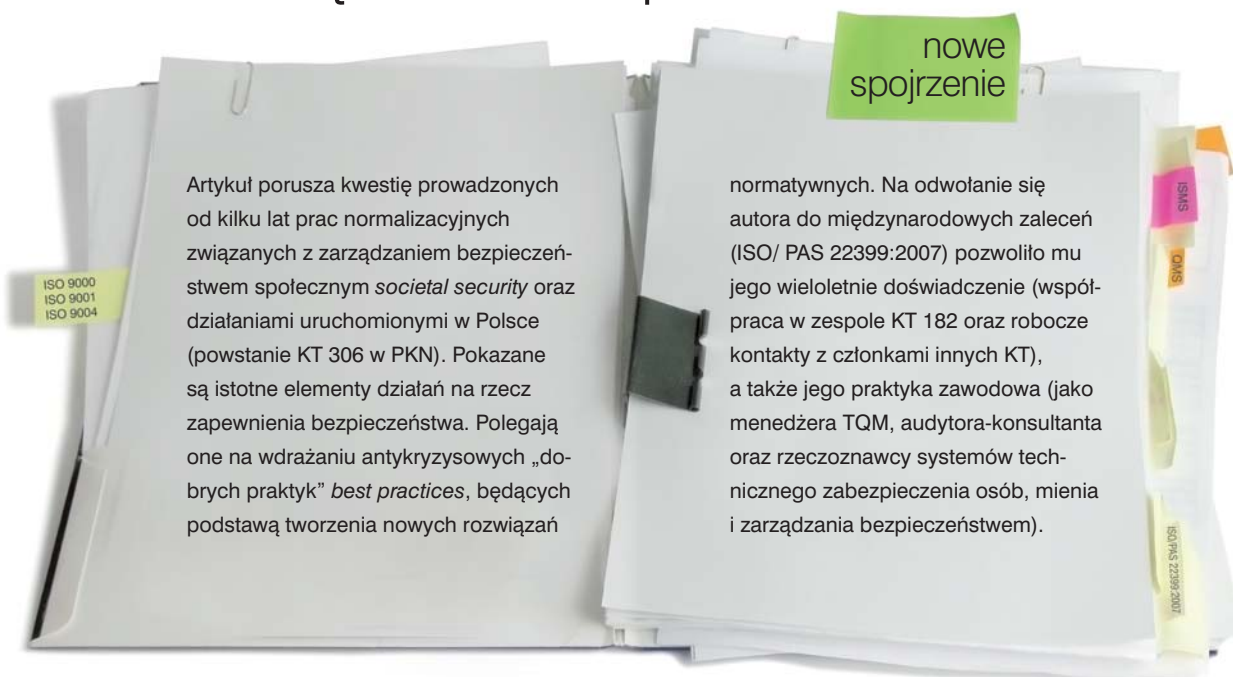
- wizualizacja stanu wszystkich podsystemów i linii dozorowych w trybie on-line
- zastosowanie podkładów map poszczególnych pomieszczeń lub całego obiektu, z możliwością rozmieszczenia kontrolki symbolizujących linie dozorowe, podsystemy, itp.
- obsługa systemu alarmowego bezpośrednio z komputera
- sygnalizacja usterek w systemie
- rejestracja zdarzeń z centrali oraz zdarzeń administracyjnych programu (możliwość wydruku)
- wizualna oraz akustyczna sygnalizacja stanów alarmowych



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

Normalizacja

w zarządzaniu bezpieczeństwem



Artykuł porusza kwestię prowadzonych od kilku lat prac normalizacyjnych związanych z zarządzaniem bezpieczeństwem społecznym *societal security* oraz działaniami uruchomionymi w Polsce (powstanie KT 306 w PKN). Pokazane są istotne elementy działań na rzecz zapewnienia bezpieczeństwa. Polegają one na wdrażaniu antykrzysowych „dobrych praktyk” *best practices*, będących podstawą tworzenia nowych rozwiązań

normatywnych. Na odwołanie się autora do międzynarodowych zaleceń (ISO/ PAS 22399:2007) pozwoliło mu jego wieloletnie doświadczenie (współpraca w zespole KT 182 oraz robocze kontakty z członkami innych KT), a także jego praktyka zawodowa (jako menedżera TQM, audytora-konsultanta oraz rzeczoznawcy systemów technicznego zabezpieczenia osób, mienia i zarządzania bezpieczeństwem).

Kilka słów wprowadzenia...

Wejście ludzkości w XXI wiek jest charakteryzowane bardzo różnie, ale we wszystkich opiniach i ocenach przewija się słowo „bezpieczeństwo”, kojarzone w różny sposób oraz pisane z licznymi odnośnikami. Wrześniowa tragedia WTC z 2001 roku wstrząsnęła światem, uświadamiając nam, że:

- jesteśmy społeczeństwem „III fali” uzależnionym od informacji i jej znaczenia (może być pozytywna-negatywna, budująca-niszcząca, mobilizująca-panikująca);
- działania na rzecz naszego bezpieczeństwa (społecznego, osobistego, środowiskowego, informacyjnego) są wciąż niedoskonałe (często nieracjonalne) i wymagają wielu zmian.

Problematyka badania i oceny naszych działań, widziana i traktowana coraz częściej zgodnie z normami zarządzającymi jako metodyczne odniesienie do zadań organizacyjnych („koło Deminga – PDCA” ↔ „podejście procesowe”)¹ pozostała niejako w tle. Sprawa niebagatelna, bowiem uogólnione „dobre praktyki” (*best practices*) zawarte w normach i dotyczące kwestii bezpieczeństwa stanowią o zgodnym, skutecznym i dającym się wymiennie porównać postępowaniu w odniesieniu do samego problemu bezpieczeństwa w różnych organizacjach, co można stwierdzić i określić poprzez audyt.

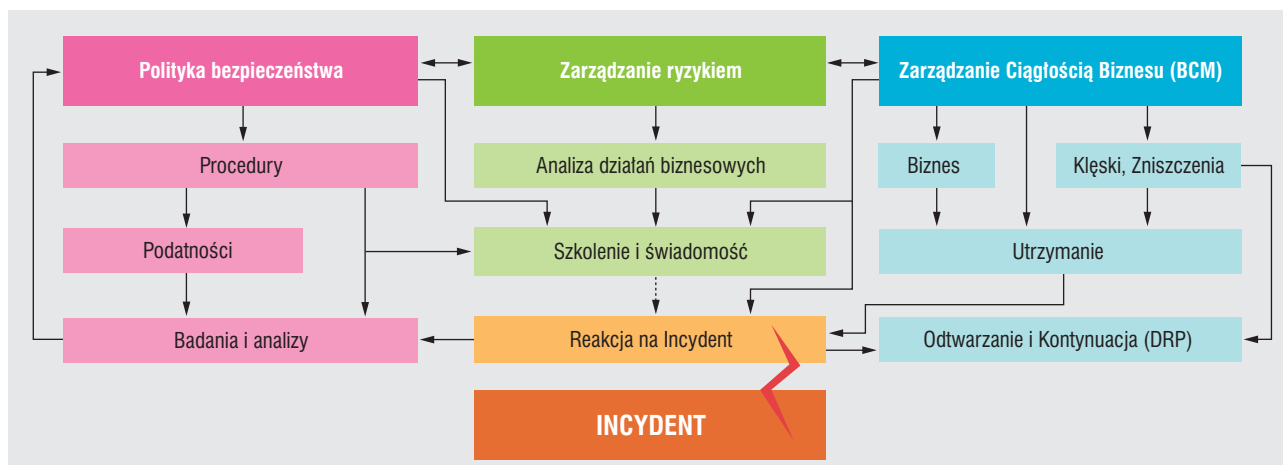
Warto tu podkreślić, że użycie narzędziowe norm zarządzania jakościowego (ISO 9000, ISO 9001, ISO 9004) z całym ich

dorobkiem i skutecznością celową dla potrzeb oceny procesów zapewnienia bezpieczeństwa środowiskowego oraz informacyjnego (ISO 14001, ISO 27001, ISO 27002, ISO 27005) wspiera oraz znacząco podwyższa skuteczność planowanych i prowadzonych działań w zakresie bezpieczeństwa ogólnego.

Normatywny wymóg zachowania nadzoru i zaangażowania kierownictwa w funkcjonowanie wdrożonego w firmie Systemu Zarządzania Bezpieczeństwem Informacji /ISMS/ powoduje przeniesienie wpływów otoczenia (rynek, środowisko) na warunki analizy zagrożeń i oceny ryzyka oraz podejmowane decyzje co do sposobu postępowania z nim („traktowanie ryzyka”)². Należy pamiętać, że każdy prawidłowo zrealizowany audyt bezpieczeństwa (ogólnego, operacyjnego, informacyjnego itd.) w swoich skutkach spełnia podstawowe wymogi w zakresie zachowania jakości zarządzania QMS (*Quality Management System*) zgodnie z zapisem pkt.8.5.3 normy ISO 9001:2008 [*Działania zapobiegawcze – usunięcie przyczyny potencjalnej niezgodności lub problemów, które jeszcze się nie pojawiły*]. W konsekwencji jest to bardzo istotne dla audytowanej firmy, zalecane działania naprawcze (wg QMS) mogą bowiem okazać się droższe niż czynności doskonalące system dla potrzeb bezpieczeństwa (np. dla SZBI/ISMS wg normy ISO 27001). Firma na ogół już realizuje zalecone działania korygujące (QMS – pkt.8.5.2 normy ISO 9001:2008 – *usunięcie przyczyn wykrytych niezgodności lub wykrytych problemów w celu zapobieżenia ich powtórnemu wystąpieniu*) wobec stwierdzonych

1) *Metodyka organizacji oparta na <podejściu procesowym>*, J.M. Chmielewski, K. Waćkowski, *Quality Review* 3-4(55-56) 2008, s. 93-101.

2) *Norma PN-ISO/IEC 27001:2007, ppkt.4.2.1. c) – g)*, s. 11-12.



Rys. 1. Współzależności zarządzania bezpieczeństwem w firmie

Istnieje rozbieżność w rozwinięciu angielskiego akronimu BCM – w języku angielskim BCM to *Bussines Continuity Management*, ale także *Bussines Constancy Management* (czyli Zarządzanie Trwałością Biznesu)

naruszeń systemu bezpieczeństwa. Ale wszystko to, łącznie z tworzeniem planów ciągłości działania i scenariuszami kryzysowymi potencjalnych krytycznych zdarzeń w procesach systemowych (A.14 Zarządzanie ciągłością działania – zał. A normy PN-ISO/IEC 27001:2007), jest wykonywane głównie z myślą o danej firmie/organizacji/korporacji i z tej racji ma bardzo często charakter „czysto biznesowy” (maksimum wysiłku dla minimum strat finansowych). Wdrażane przedsięwzięcia antykryzysowe są ograniczone do „własnego podwórka” i w minimalnym (na ogół) stopniu uwzględniają straty społeczne w samej firmie oraz jej bezpośrednim otoczeniu. W większości firm zarządzanie bezpieczeństwem jest widziane jako przeniesienie świadomości potrzeb zarządzania ryzykiem (we wszystkich jego postaciach) w obszar strategii bezpieczeństwa i zachowania ciągłości działania firmy przy różnorodnych incydentach, mogących prowadzić do zagrożeń kryzysowych (co uwiadcza rys. 1). Poszczególne działania mają zatem prowadzić do zapobiegania i(lub) eliminowania ich skutków (materializacja ryzyk).

A jak się to ma do szerszego kontekstu społecznego w warunkach istniejących oraz wciąż się pojawiających nowych zagrożeń kryzysowych nie tylko biznesowo-rynkowych, ale także naturalnych, technicznych i środowiskowych o zróżnicowanym charakterze, takich jak: zjawiska atmosferyczne/geologiczne z towarzyszącymi im powodzią i pożarami, katastrofy techniczne i komunikacyjne, wielkoobszarowe oddziaływania atmosferyczne (dymy i pyły wulkaniczne, „kwaśne deszcze”, „trujące obłoki”... itp.) przy ich nad wyraz szerokim oddziaływaniu na ludzi, zwierzęta, infrastrukturę, środowisko...?

1. Bezpieczeństwo człowieka – społeczeństwa

Bezpieczeństwo człowieka stało się w ostatnich latach XX wieku domeną działalności naukowej – securitologii, która uwzględnia wieloaspektowość postrzegania i „odczytywania” bezpieczeństwa jako obiektu badań naukowych (z wszystkimi wynikającymi z tego faktu implikacjami, związanymi z zastosowanymi zasadami teorii poznania naukowego).

Pierwsze publikacje podejmujące próbę wyodrębnienia *securitologii* jako dyscypliny naukowej pochodzą z 1989r, co można wyjaśnić nowymi potrzebami i oczekiwaniami, a także

warunkami kształtującymi się po rewolucyjnej zmianie ustrojów społeczno-politycznych w Europie.

Cechą charakterystyczną tych właśnie publikacji jest opisanie i uwzględnienie wielorakich czynników: obiektywnych i subiektywnych, socjopsychologicznych i kulturowych, politycznych i prawnych, przyrodniczych i technicznych, makro- i mikroekonomicznych, które nie tylko warunkują zagrożenia, ale także pozostają z nimi we wzajemnych nierozzerwalnych związkach.

Nauka o bezpieczeństwie (*securitologia*) jest na chwilę obecną widziana dwojako i jest traktowana jako:

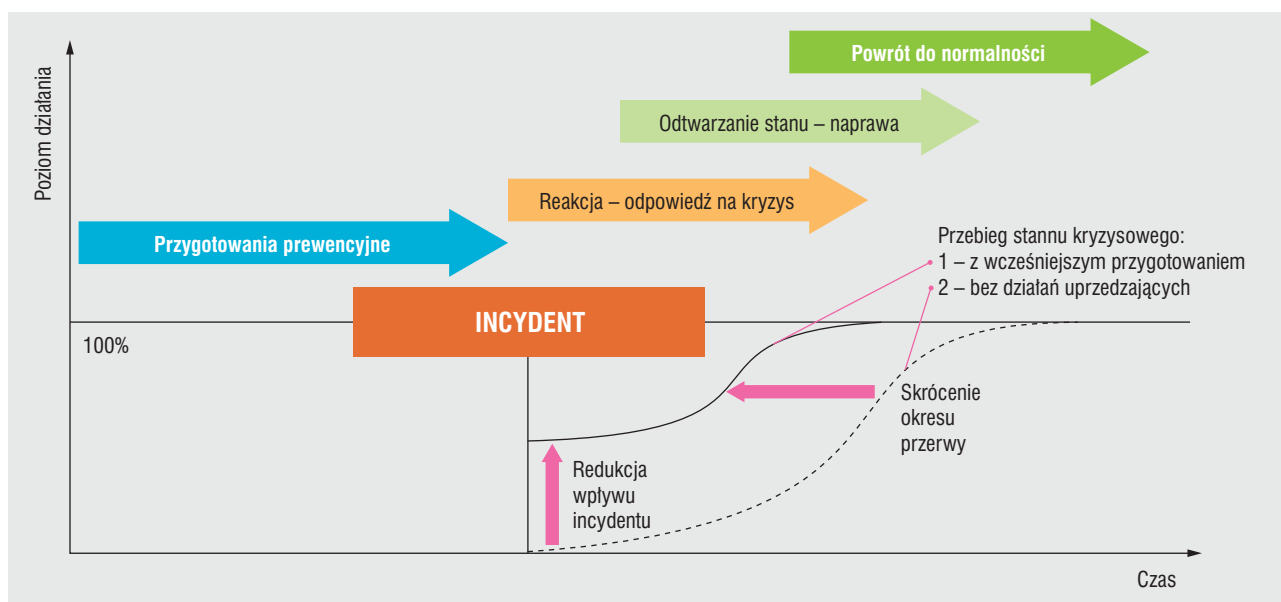
- dyscyplina naukowa w grupie 64 (nauki interdyscyplinarne), tzn. poświęcona badaniom naukowym dotyczącym bezpieczeństwa,
- poddziedzina nauki, ułożona w ramach systematyki odpowiednio: w grupie 3: – nauki ekonomiczne; w dziedzinie 2: – nauki o zarządzaniu, tzn. poświęcona badaniu procesów zarządzania bezpieczeństwem.

W ostatnich latach securitologia zapisała na swym koncie wiele praktycznych osiągnięć w badaniu teorii i praktyki bezpieczeństwa człowieka. Do tego sukcesu przyczynił się również współdział polskiego środowiska naukowego, a także prace popularyzatorskie Stowarzyszenia EAS (*European Association for Security*), które powstało na konferencji krakowskiej 12 maja 2000 r.

Stowarzyszenie EAS (Europejska Federacja dla Bezpieczeństwa) ma osobowość prawną i jest towarzystwem naukowym prowadzącym badania oraz popularyzującym nauki o bezpieczeństwie człowieka. Celem Stowarzyszenia jest edukacja dla bezpieczeństwa ludzi i firm we wspólnej Europie³. Stowarzyszenie wydaje publikacje książkowe oraz (na bieżąco) Zeszyty Naukowe „Securitologia/Securitology/Секюритология” dotyczące nauk o bezpieczeństwie oraz zagadnień z zakresu edukacji dla bezpieczeństwa.

Warto wiedzieć, że Stowarzyszenie to wypracowało podstawę programową, która pozwoliła utworzyć na studiach wyższych nowe specjalności, takie jak: „zarządzanie bezpieczeństwem”, „bezpieczeństwo europejskie”, „administracja

3) Adres, statut, lista członków i inne dokumenty EAS dostępne są na stronie www.eas.krakow.pl



Rys. 2. Obszar korzystnego oddziaływania zaleceń ISO/PAS 22399 (opracowanie własne za www.sail.global: ISO/PAS 22399)

bezpieczeństwem”, a na studiach podyplomowych: „zarządzanie bezpieczeństwem” oraz „edukacja dla bezpieczeństwa”. Powstał również Międzynarodowy Ośrodek Szkoleń Specjalnych. I choć obecnie nie sposób wskazać możliwości ścisłego unormowania (a tym bardziej certyfikowania) bezpieczeństwa społecznego, to jednak trzeba pamiętać, że analizowany problem istnieje i narasta, zwłaszcza w odniesieniu do sytuacji kryzysowych oraz nadzwyczajnych zagrożeń.

1.1. Prace normalizujące – obszar międzynarodowy

Działania w tym zakresie na poziomie międzynarodowym podejmowano dwukrotnie. W ISO opracowano założenia i w 2001 r. powołano komitet „Security people”. Po okresie nieaktywności komitetu dokonano w 2005 r. jego reaktywacji poprzez umieszczenie sekretariatu w szwedzkiej jednostce normalizacyjnej SIS oraz zmianę nazwy na „Societal Security” TC 223. W 2006 r. nowy komitet zorganizował w Sztokholmie pierwsze posiedzenie pod przewodnictwem Pana Ambadora Kristera Kumlina (*Senior Adviser to the Swedish Emergency Management Agency*). W posiedzeniu uczestniczyło 68 przedstawicieli z 30 krajów. Postanowiono wówczas, że praca komitetu będzie koncentrować się na rozwoju zarządzania kryzysowego poprzez usprawnianie sfery technicznej, sfery zarządzania i sfery operacyjnej, a także interoperacyjności (interoperability) w działaniach służb ratunkowych.

Normy i dokumenty normalizacyjne opracowywane w tym komitecie mają wspierać ochronę i ułatwiać reagowanie na kryzysy spowodowane klęskami naturalnymi, wypadkami czy atakami terrorystycznymi niszczącymi naszą codzienną egzystencję. Zostaną wzięte pod uwagę wszystkie fazy zarządzania kryzysowego: przed wystąpieniem sytuacji kryzysowej, w trakcie jej trwania i po jej zakończeniu (Rys. 2).

Pierwszy dokument normalizacyjny TC 223, który zawierał wytyczne dotyczące gotowości na wypadek wystąpienia sytuacji kryzysowych i ciągłości zarządzania w stanach kryzysowych, ukazał się pierwszego grudnia 2007 roku i jest to: *ISO/PAS 22399:2007, Societal security – Guidelines for incident preparedness and operational continuity management*.

Ten bazujący na szerokiej współpracy międzynarodowej dokument zawiera wytyczne dotyczące gotowości i ciągłości w zarządzaniu kryzysowym. Ustala procesy, zasady i terminologię ww. problematyki w kontekście bezpieczeństwa społecznego. Ma on na celu dostarczenie podstaw do rozwoju oraz wprowadzenia gotowości i ciągłości w zarządzaniu kryzysowym w organizacjach, a także zapewnienie zaufania w podobnych sytuacjach pomiędzy organizacjami, społecznościami i biznesem. Wytyczne dostarczają narzędzi, które umożliwiają organizacjom publicznym i prywatnym reagowanie w sytuacjach kryzysowych. Narzędzia te umożliwiają zarządzanie w sytuacji kryzysowej, pokonanie tej sytuacji, a także podjęcie odpowiedniego postępowania w celu zapewnienia ciągłości działania organizacji.

Trzeba pamiętać, że wytyczne oraz sam dokument typu ISO/PAS obowiązują przez okres trzech lat. Po tym czasie w ramach dalszych działań komitetu oraz organizacji normalizacyjnych krajów-uczestników prac powinny one zostać przetworzone do postaci normy (międzynarodowej lub krajowej) lub też powinna być podjęta decyzja o przedłużeniu ważności dokumentu na następne trzy lata. Po tym okresie na jego podstawie można już tylko opracować normę lub wycofać dokument.

Na posiedzeniu w maju 2007 r. TC 223 podjął uchwałę, w myśl której utworzono Grupę Zadaniową nr 2 (*Task Group*). Grupa ta miała za zadanie monitorowanie zastosowania ISO/PAS 22399 oraz przegląd izraelskiej normy dotyczącej bezpieczeństwa i ciągłości systemów zarządzania oraz zastosowania innych dokumentów. Sekretariat TC 223 zwrócił się do wszystkich członków komitetu z prośbą o informowanie o wszelkich istniejących normach i innych dokumentach, jak również o wszystkich pracach prowadzonych w zakresie gotowości i ciągłości, w tym szczególnie o krajowych dokumentach dotyczących specyfikacji i systemów zarządzania. W rozpoczynającym się 2009 roku sekretariat może wskazać następujące zidentyfikowane dokumenty:

– *ISO/PAS 22399:2007, Societal security – Guidelines for incident preparedness and operational continuity management (including the „best of five” documents)*,

- TR 19:2005: *Technical reference for business continuity management* (Singapore),
- BS 25999-2 *Specification for Business Continuity Management* (UK),
- CSA Z1600 *Standard on emergency management and continuity programs* (draft standard from Canadian Standards Association),
- *All Hazards Risk Management Systems Best Practices Standard: Requirements with Guidance for Use: A practical management systems approach to security, preparedness, response, business/operational continuity and recovery for disruptive incidents resulting in an emergency, crisis, or disaster* (draft standard from ASIS International).

W nadchodzących latach prace TC 223 będą nabierały znaczenia, a ich efekty w postaci dokumentów normalizacyjnych umożliwią zainteresowanym opracowywanie procedur i systemów, a jednocześnie dadzą im więcej pewności i przekonania o właściwym przygotowaniu do sytuacji kryzysowych (przy zachowaniu zgodności terminologicznej i operacyjnej).

Gotowość i ciągłość to kluczowe elementy w ochronie życia oraz podczas pomocy w przezwyciężaniu zdarzeń kryzysowych. Kto jest przygotowany do takich sytuacji, ten ma znacznie większe szanse i mniejsze straty, warto zatem zapoznać się z istniejącymi i projektowanymi dokumentami TC:

- 1) ISO/WD 22300 *Societal security – Fundamentals and vocabulary*,
- 2) ISO/NP 22320 *Societal security – Command and control, information, coordination and cooperation for emergency management*,
- 3) ISO/NP 22322 *Societal security – Inter/Intra organisational warning procedures*,
- 4) ISO/NP 22301 *Societal security – Preparedness and continuity management systems – Requirements*,
- 5) ISO/NP **** *Societal security – Video-surveillance Format for Interoperability*,
- 6) ISO/PWI 22397 *Societal security – Public and private partnerships*,
- 7) ISO/PWI 22398 *Societal security – Procedures on exercises and testing*.

Kilka uwag na ten temat:

- problemy zarządzania i współpracy w zakresie wsparcia, pomocy oraz nadzoru nad działaniami wspierającymi związane są z ustaleniami, które wynikają z wymogów prawnych obowiązujących w miejscu ich stosowania;
- wprowadzane procedury ostrzegawcze (międzynarodowe i wewnętrzne) są upowszechniane z uwzględnieniem już obowiązujących zasad ochronnych;
- proponowane i wdrażane procedury testowania oraz ćwiczenia muszą uwzględniać pryncypia środowiskowe (lokalne, religijne itp.) głównie dla zapewnienia łatwości i skuteczności stosowania ich w rzeczywistych działaniach ratowniczo-odtwórczych.

Trzeba przy tym pamiętać, że przedstawiane rekomendacje mają charakter doradczy i są (analogicznie jak i treść norm) przyjmowane oraz stosowane dobrowolnie przez zainteresowane strony, instytucje i osoby.

1.2. Prace normalizujące – obszar krajowy

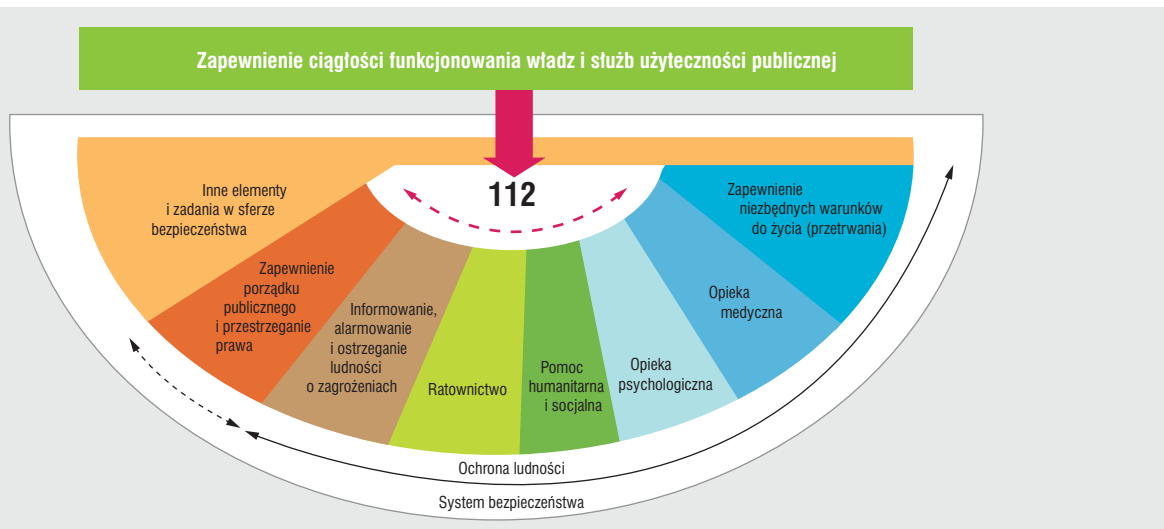
W Polsce kwestie ujmowane jako societal security są (na chwilę obecną) „rozrzucone” w licznych dokumentach ustawowych i normatywnych, przy czym dają się w nich zauważyć znaczne rozbieżności pojęciowe i zakresowe (w części już umocowane prawnie). Trzeba te dokumenty wziąć pod uwagę szczególnie teraz, ponieważ 20 listopada 2008 roku powołano nowy **Komitet Techniczny nr 306** (*Komitet Bezpieczeństwa powszechnego i ochrony ludności*). Powołanie to odbyło się w Polskim Komitecie Normalizacyjnym dzięki inicjatywie takich organizacji ustawowych, jak MSWiA, MON oraz społecznych (POLALARM, PISA, ISACA PL), a także wysiłkowi WSO PKN i jego dyrektora p. Ryszarda Grabca.

W styczniu 2009 r. został powołany Komitet Techniczny 391 i zarazem przestała istnieć dotychczasowa grupa robocza CEN/BT/WG 161 ds. ochrony i bezpieczeństwa ludności. KT 306 będący lustrzanym odbiciem dla obu ww. instytucji ma zapewnić wdrożenie w polskiej praktyce prawnej i zharmonizowanie w naszych normach wskazań dyrektyw UE, związanych z bezpieczeństwem społecznym w warunkach kryzysu i zagrożeń, a wynikających pośrednio z implementacji regionalnej prac ISO/TC 223 „Societal Security”. KT 306 jest sklasyfikowany wg ICS jako: 01.040.03; 01.040.13; 03.080.20; 03.080.30; 03.100.01; 13.060.01; 13.200; 13.310; 13.340.10; 95.020. Jego zakres tematyczny obejmujący ogrom zagadnień niezbędnych do opracowania jest następujący:

- zintegrowane zarządzanie granicami,
- infrastruktura krytyczna (budynki, cywilna infrastruktura inżynierska, bezpieczeństwo zasilania w wodę oraz zasilania w energię),
- ochrona i obrona przed BMR,
- ochrona obywateli przed zjawiskami groźnymi dla życia i zdrowia lub powodującymi straty materialne, a także minimalizowanie ich skutków,
- przeciwdziałanie terroryzmowi,
- bezpieczeństwo łańcucha dostaw,
- zmniejszenie ryzyka popełniania przestępstw z wykorzystaniem produktów i usług,
- służby ratunkowe,
- likwidacja skutków użycia BMR i wystąpienia naturalnych kataklizmów.

KT 306 w zakresie współpracy z CEN/TC 391, CEN/TC 164/WG 15, CEN/TC 379, CEN/TC 384 oraz ISO/TC 223 jest komitetem wiodącym. Na forum międzynarodowym i regionalnym współpracuje z CEN/BT/WG 125, CEN/BT/WG 126, a także CENELEC/TC 79.

W działaniach komitetu KT 306 przewidywana jest szeroka współpraca z powołanym w dniu 25 lutego 2009 roku nowym komitetem CEN/TC 388 – *Systemy ochrony obwodowej* („Perimeter protection”) – pilotowanym przez Holendrów i dążącym do ujednolicenia systemów ochrony bezpośredniej (fizycznej i technicznej). Szczególnie ważnym elementem prac jest planowana szeroka konsultacja w zakresie normalizacji procesów przeciwdziałania rozprzestrzenianiu się terroryzmu [normalizacja statusu upoważnionego przedsiębiorcy (AEO UE – KE C 648/2005; (WE) 1875/2006), działania we współpracy m.in. z instytucjami celnymi i logistycznymi (CT-PAT: Customs Service – USA, Schenker DB – Niemcy/Polska)].



Rys. 3. Dziedziny ochrony ludności. Źródło: KG PSP mat. inf. Biura ds. Ochrony Ludności i Obrony Cywilnej, IV2007

2. Bezpieczeństwo społeczne jako obowiązek państwa

Pytań z zakresu „Societal Security” w stosunku do władz państwowych jest wiele:

- Jak można odnieść się do realizacji audytu systemu bezpieczeństwa społecznego?
- Co wiemy na temat bezpieczeństwa i czego oczekujemy od państwa w tym zakresie?
- W jakich dziedzinach oraz w jak szerokim zakresie prowadzone są działania/czynności rządowe?

Na tak postawione pytania nie ma jednoznacznych odpowiedzi. Ogólne potrzeby i oczekiwania społeczne w zakresie ochrony (różnie artykułowane i realizowane w poszczególnych środowiskach – gminnym, osiedlowym, wielkomiejskim) są powszechnie znane, ale obecnie nie dysponujemy ujednoliconymi wskaźnikami i wymaganiami, nie wspominając o braku norm dla przedstawionego na rysunku systemu bezpieczeństwa społecznego. Trudno jest więc odnieść się do rzetelności przedstawianej publicznie oceny zapewnienia bezpieczeństwa społecznego w rozumieniu spełnienia obowiązku przez państwo (przy zachowaniu warunku oczekiwań samego społeczeństwa).

Istnieje szereg uregulowań prawnych (ustawy i rozporządzenia, zarządzenia i decyzje resortowe oraz przepisy prawa lokalnego), ale problemem zasadniczym jest ich interpretacja. Podobnie dzieje się w procesie rozumienia i wdrażania już istniejących rozwiązań normalizacyjnych, stąd zaangażowanie PKN w wydawanie przez KT w 2009 r. komentarzy do poszczególnych norm⁴.

Odrębnym problemem staje się asymetryczny charakter zagrożeń w przypadku konfliktów zbrojnych, co przekłada się na zagrożenie terrorystyczne dla całego obszaru europejskiego. Jako Europa posiadamy (społecznie nieakceptowalne) doświadczenia z zamachów w Madrycie (11.03.2004 r.) i Londynie (7.07.2005 r.) oraz świadomość udaremnienia zamachów terrorystycznych na lotniska brytyjskie w 2007 r.

Tym bardziej istotne stają się prace KT 306 nad normami z zakresu bezpieczeństwa społecznego oraz zachowanie w tym względzie warunków szerokiej współpracy instytucjonalnej krajowej i zagranicznej (z utrzymaniem wskazanych podstaw interoperacyjności).

3. Audyt bezpieczeństwa w firmie a oczekiwania społeczne

W minionym dwudziestoleciu żadna z ekip rządzących RP (pomimo nagłaśniania sprawy w mediach) nie przedstawiła odpowiednich rozwiązań prawnych dotyczących bezpieczeństwa, w tym polityki społecznej. Powoduje to, że środowisko biznesu III RP traktuje społeczeństwo dwuwymiarowo: jako pracowników – wykonawców oraz nabywców – konsumentów i tylko w tym zakresie czuje się do czegośkolwiek zobowiązane (vide: oceny istniejącego kryzysu światowego).

Audyt bezpieczeństwa w firmach jest z reguły realizowany jako audyt wewnętrzny zarządzania łączący w analizowanych procesach ocenę elementów ZSJ i SZBI (QMS+ISMS).

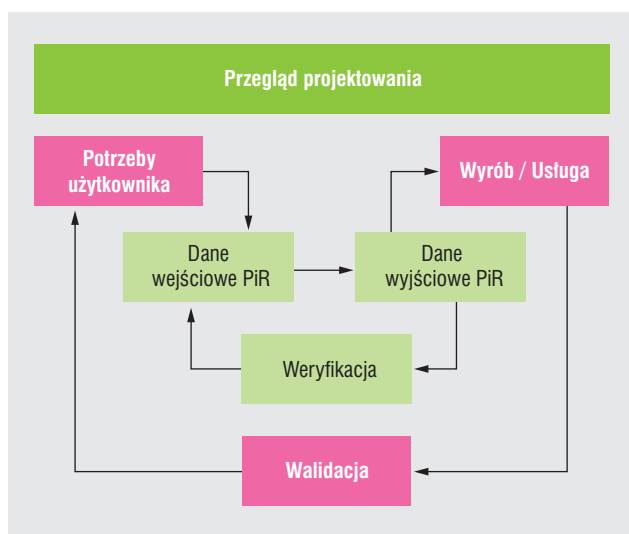
Powody takiego postępowania to:

- konieczność wykrycia i skorygowania niezgodności/zagrożeń/ryzyk dla bezpiecznego funkcjonowania firmy;
- wymaganie norm (ZSJ+SZBI) i przepisów ustawowych (SZBI), w tym deklarowanych odrębnie (SoA ISMS);
- mechanizm sterowania/nadzoru wykorzystywany przez kierownictwo dla potrzeb zapewnienia założonych zysków;
- audyt jako kluczowy element dla zapewnienia skuteczności ZSJ+SZBI,
- skorygowanie błędów/niedoróbek i pomyłek procesowych oraz eliminacja ryzyk dla firmy, zanim zostaną one wykryte przez jednostki zewnętrzne lub (co gorsze) zmaterializują się w postaci kosztów finansowych i środowiskowych.

Zasadniczą rolę odgrywają tutaj cechy podstawowe dla audytu I strony, który to:

- jest robiony u siebie i przez siebie (dla ZSJ, bowiem dla SZBI ciągle jeszcze jest realizowany przez zatrudnionego specjalistę zewnętrznego z powodu obiektywizmu oceny, ponieważ „trudno jest być sędzią we własnej sprawie”, a problematyka bezpieczeństwa obejmuje całość firmy),

4) Ryzyko jest zawsze obecne w naszym życiu, Skalska J., wywiad z prezesem PKN, drem inż. T. Schweitzerem, Wiadomości PKN. Normalizacja, Nr 12/2008, s. 2–5



Rys. 4. Postępowanie w audycie wewnętrznym
(opracowanie własne MB)

- ma zasady ustalane wewnętrznie (ale z zachowaniem zgodności i odpowiedzialności wobec wymogów prawa),
- charakteryzuje się systematyką i niezależnością (co nie zawsze jest spełniane),
- jest przeprowadzany w zakresie i częstotliwości niezbędnej w danych okolicznościach,
- z zasady jest planowany (ZSJ+SZBI), choć bywa doraźny (jako skutek incydentu i/lub zagrożenia zaistniałego w obszarze SZBI).

Na etapie przygotowania i projektowania audytu zgodnie z wymaganiami ISO 9001 zachowane są wymagania procesowe pod względem weryfikacji i walidacji prac (Rys. 4).

Przyjmując „dobro firmy” za zasadnicze, w prowadzonych działaniach podporządkowuje mu się wszystkie inne cele, co czasami prowadzi do kolizji prawnych⁵ o daleko idących skutkach.

Szereg działań przygotowywanych z myślą o sytuacjach kryzysowych w firmie nie uwzględnia potrzeb ludzkich i środowiskowych (w pewnych sytuacjach wręcz obciąża otoczenie swymi skutkami), dlatego tak istotnym staje się wprowadzenie dobrych praktyk społecznych oraz unormowanie obszaru działań ratowniczych i naprawczych – nie tylko zresztą w odniesieniu do firmowych biznesów.

Dla zarządów firm i pracodawców pojawia się tu socjologiczna sprzeczność: trzeba zaufać pracownikom i powierzyć im istotne dane oraz tajemnice firmy, a zarazem liczyć się z koniecznością weryfikacji i walidacji ich pracy. Problem ten musi być rozwiązywany wielopłaszczyznowo: organizacyjnie, personalnie i informacyjnie, przy zachowaniu wymagań ochrony bezpośredniej (fizycznej i technicznej), szczególnie w odniesieniu do zespołów ludzkich zapewniających ciągłość działania firmy i posiadanych przez nich informacji. Nie zapominajmy przy tym, że większość tych osób ma rodziny i otoczenie towarzyskie interesujące się ich pracą.

5) Z praktyki audytorskiej: duża spółka (z udziałem kapitału zagranicznego) w ramach „cięcia kosztów” zlikwidowała swój dział transportu ciężkiego, a potrzeby przeniosła do firmy outsourcingowej, pomijając? zaniedbując? nałożone wcześniej na nią (osoba prawna) ustawowe zobowiązania rzeczowe (obowiązek obronny) wobec Centrum Zarządzania Kryzysowego Wojewody.

GUNNEBO

For a safer world®



Tripody

Bezpieczny stadion



Kołowroty, furty



Gunnebo Polska Sp. z o.o.
62-800 Kalisz, ul. Piwoniczka 4
tel. + 48 (0) 62 768 55 70
fax + 48 (0) 62 768 55 71
www.gunnebo.pl

Podsumowanie

W świetle przedstawionych powyżej faktów certyfikowanie zarządzania bezpieczeństwem nie tylko w firmach dla potrzeb biznesu, ale również dla oceny bezpieczeństwa społecznego jawi się nam niejednolicie i mgliście. Jego uporządkowanie wymaga wiele wysiłku oraz „pracy u podstaw”. Przykładowo – Polska Norma PN-ISO/IEC 27001:2007 dotycząca wymagań dla systemu zarządzania bezpieczeństwem informacji (SZBI/ISMS) dla większości jej potencjalnych użytkowników wydaje się ciągle niezrozumiała – stąd zaawansowane prace w KT 182 nad mającym ukazać się „lada dzień” komentarzem do niej.

To dobry i oczekiwany kierunek działań prospołecznych, ale zainteresowani też powinni sami „uderzyć się w pierś”, bowiem niejedni „biznesmeni” narzekający na normę nie zadał sobie trudu zapoznania się z przywoływanymi w niej dokumentami uzupełniającymi (normami ISO, wytycznymi OECD). Tymczasem wnikliwe przeczytanie drugiej edycji międzynarodowej normy ISO 17799 (PN-ISO/IEC 17799:2007) znakomicie pomaga w rozumieniu istoty wymagań zawartych w załączniku normatywnym A normy PN-ISO/IEC 27001:2007, a stosunkowo niewielki wysiłek włożony w poznanie wytycznych OECD z dnia 25 lipca 2002 r. procentuje w dwójnasób (na stronie www.oecd.org/dataoecd/16/3/15582300.pdf dostępne jest polskie tłumaczenie).

Z żalem należy stwierdzić, że zalecenia ISO/PAS 22399:2007 ciągle jeszcze są przedmiotem rozważań... tylko czy aby potrzebnych i skutecznych, co do ich rezultatów końcowych?

Ksiądz profesor Józef Tischner zwykł być mawiać na swoich wykładach: „...choć prawdą jest stwierdzenie, iż praktyka bez teorii jest ślepa, a teoria bez praktyki mocno kulawa – to należy pamiętać zawsze, że życie jest bogatsze od wszelkich naszych przypuszczeń i przewidywań...”. Na łamach niniejszego artykułu starano się wskazać różnice w podejściu do przedstawionego w tytule tematu.

Świadom ułomności swego pióra autor pragnie ocenę swoich starań pozostawić PT Czytelnikom.

dr inż. Marek Blim

Bibliografia:

1. Anderson S. *Inżynieria zabezpieczeń*, seria TAO, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.
2. *Bezpieczeństwo w biznesie*, pod red. nauk. Wł. Fehlera, wyd. Messenger Service Stolica S.A., Warszawa 2005.
3. Białas A. *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006.
4. Byczkowski M. Blim M., Zawila-Niedźwiecki J., *Założenia TSM - Total Security Management*, opracowanie European Network Security Institute, Warszawa, 2004.
5. Konieczny J. *Wprowadzenie do bezpieczeństwa biznesu*, wyd. Konsalnet, Warszawa 2004.
6. Michalak A. *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, seria MONOGRAFIE, Kantor Wydawniczy ZAKAMYCZE, Kraków 2006.
7. Pipkin D.L. *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, seria TAO, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
8. Polaczek T. *Audyt bezpieczeństwa informacji w praktyce*, Wydawnictwo HELION, Gliwice 2006.
9. Polok M. *Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2006.
10. Yourdon E. *Wojny na bity. Wpływ wydarzeń z 11 września na technikę informacyjną*, seria TAO, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.
11. Zagórski Z., *Socjologiczne portrety grup społecznych*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2002.
12. Strona internetowa ISO – http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?com-mid=295786 z dnia 15-01-2009.
13. Strona internetowa Polskiego Komitetu Normalizacyjnego <http://www.pkn.pl/>, link *Obronność i bezpieczeństwo* w zakładce **DZIAŁALNOŚĆ NORMALIZACYJNA**, z dnia 2009-01-15.
14. Strona internetowa <http://www.sail.global>, link *ISO/PAS 22399* z dnia 2009-01-15.

Wizualizacja i integracja

SPOSÓB NA SZYBKĄ I WŁAŚCIWĄ REAKCJĘ

Integracja produktów firm:

Bosch, Compas, DSC, GE Interlogix, Honeywell, Kantech, Polon Alfa, Siemens, Rokonet, Satel, Unicard.

- ★ Wizualizacja i sterowanie na wielu stanowiskach jednocześnie
- ★ Integracja na poziomie oprogramowania – nie wymaga dodatkowych urządzeń
- ★ Swoboda i prostota dostosowania do potrzeb wyglądu graficznego systemu
- ★ Otwartość systemu
- ★ Wsparcie użytkownika podczas zagrożenia: prowadzenie od planu ogólnego do szczegółowego, automatyczna prezentacja obszarów szczególnie zagrożonych, procedury postępowania

IFTER NA RYNKU OD 1999
www.ifter.com.pl



WYZNACZAMY
NOWE GRANICE
OCHRONY



SYSTEMY ALARMOWE

KABE

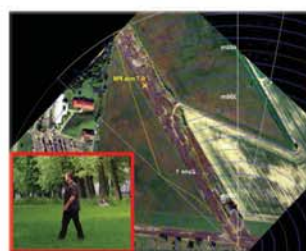
RADARY
NADZORUJĄCE

OCHRONA
ŚWIATŁOWODOWA



Poznaj możliwości zaawansowanych
systemów nadzorujących.

Nie daj się zaskoczyć. Przejmij
kontrolę nad sytuacją.



Namierz intruza zanim dostanie się na
Twój teren.

Śledź każdy jego krok i podejmij
skuteczną interwencję.

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63, 43-190 Mikołów
tel. 032 32 48 900, fax 032 32 48 901
systemy@kabe.pl / www.kabe.pl

Temat: Miejsce spotkań czy baza danych? Czy nadal chcesz mieć swój profil na portalach społecznościowych?

Rozwój technologii i systemów komunikacyjnych pozwala nam na coraz szybszy, łatwiejszy i szerszy dostęp do ogromnych zasobów informacji, których na próżno by szukać w pobliskiej bibliotece. Możemy przeglądać miliony stron internetowych zawierających cenne informacje, komunikować się ze swoimi znajomymi, poznawać nowych ludzi, nawiązać kontakt z osobami, których nie widzieliśmy „całe wieki”, a wszystko to bez konieczności wychodzenia z domu. Nie wszyscy jednak zdają sobie sprawę z tego, że medium to wykorzystują do realizacji swoich nieuczynnych celów również przestępcy...

Gdyby twórcom ARPANET-u – którzy pod koniec lat 60. ubiegłego wieku stworzyli rozległą sieć komputerową łączącą uczelnie w Stanach Zjednoczonych i uznawaną dziś za początki Internetu – ktoś w tamtych czasach opowiedział, jak ich sieć będzie wyglądała po 40 latach (czyli dziś), zapewne nie uwierzyliby swojemu rozmówcy. Początkowo sieć połączonych komputerów, które nie miały centralnego punktu sterowania, ale umożliwiały wymianę danych, miała służyć Departamentowi Obrony USA do skutecznej komunikacji w warunkach wojennych. Obecnie wiele osób nie wyobraża sobie codziennego życia bez Internetu. Bez wychodzenia z domu mamy możliwość dostępu do potężnego zbioru informacji. Ogrom danych, jakie można znaleźć w zasobach globalnej sieci, sprawia, że coraz częściej korzystamy z tego dobrodziejstwa technologicznego podczas szukania aktualnych wiadomości z kraju i ze świata, realizujemy operacje bankowe, rezygnując z wątpliwej przyjemności tracenia swojego cennego czasu na stanie w kolejkach do tradycyjnej kasy, dokonujemy zakupów atrakcyjnych towarów po równie atrakcyjnej cenie, możemy rozwijać swoje hobby, szukając ciekawych informacji z zakresu własnych zainteresowań. Jeśli ktoś ma ochotę, to dzięki odnalezionym w sieci przepisom kulinarnym może uczyć się sztuki kulinarnej, może także zaplanować podróż, korzystając z rozkładów jazdy pociągów czy autobusów komunikacji lokalnej. Coraz większą popularnością – nie tylko w naszym kraju – cieszą się internetowe komunikatory oraz portale społecznościowe, za pośrednictwem których możemy komunikować się ze starymi lub poznanymi właśnie za pośrednictwem sieci znajomymi, „spotkać” dawnych znajomych ze szkoły, wojska, odtworzyć drzewo genealogiczne swojej rodziny.

Dzięki odmiejszczeniu prowadzenia działalności internetowej nie ma znaczenia, w jakim punkcie globu znajduje się użytkownik, ważne by za pośrednictwem kabla, sieci WiFi czy

modemu GPRS lub satelitarnego miał możliwość podłączenia się do jednego z setek tysięcy punktów dostępowych. By prowadzić w Polsce działalność usługową za pośrednictwem internetu, wcale nie trzeba przebywać na stałe w kraju. Co więcej, serwery, na których umieszczone są polskojęzyczne strony, również mogą być zlokalizowane poza granicami naszego państwa. Paradoxem jest jednak to, że medium – u podstaw powstania którego było zapewnienie bezpieczeństwa USA – po kilkudziesięciu latach dynamicznego rozwoju stało się miejscem, w którym swoją działalność prowadzą również przestępcy. Globalny zasięg sieci wielu oszustom daje poczucie bezkarności. Na szczęście organy ścigania posiadają coraz bardziej zaawansowane narzędzia umożliwiające zlokalizowanie osób, które za pośrednictwem internetu dopuszczają się czynów wykraczających poza normy prawa. Obecnie trwa głośna dyskusja wokół zagadnienia związanego z poszerzeniem zakresu uprawnień policji w Unii Europejskiej. W zasięgu ręki są możliwości technologiczne pozwalające na zdalne przeszukiwanie zawartości dysków twardych bez wiedzy użytkownika. By w Polsce skorzystać z nich w majestacie prawa, niezbędna jest pisemna zgoda Prokuratora Generalnego, co mocno wiąże ręce funkcjonariuszom policji. W uzasadnionych przypadkach, gdy inne środki okażą się bezskuteczne, uzyskanie takiej zgody pozwala na przeprowadzanie policyjnych czynności operacyjnych, które najczęściej kończą się zatrzymaniem sprawców przestępstw.

– „Najpierw włamywali się do samochodów. Kradli kołpaki, nawigacje satelitarne, anteny samochodowe do CB. Sprzedawali swoje łupy na jednej z aukcji internetowych. Złodzieje wpadli dzięki monitorowaniu przez policjantów sieci Internet, a także dzięki ich pracy operacyjnej”.

- „O rozważę i ostrożność przed rezerwowaniem miejsc noclegowych za pomocą Internetu apeluje zakopiańska policja. W okresie świąteczno-noworocznym nasilają się oszustwa na „wirtualne noclegi”.
- „37-letniego obywatela Ukrainy Andryia S., podejrzanego o udział w szajce zajmującej się okradaniem przez internet kont bankowych, zatrzymali stołeczni policjanci. Gang wyłudzał informacje o kontach od samych właścicieli poprzez fikcyjne strony internetowe prawdziwych banków”.
- „24-latek uwięził matkę z trójką dzieci w ich domu pod Opolem. Wcześniej poznał kobietę przez internet. Groził rodzinie zabójstwem. Adriana S. ujęli antyterroryści – może spędzić w więzieniu nawet 12 lat”.
- „Krakowska Policja zatrzymała dwudziestodwuletniego pedofila. Swoje ofiary – 12-letnie dziewczynki wyszukiwał w internecie. Zatrzymanemu grozi kara do 10 lat więzienia”.
- „Nastolatka, wykorzystując internet, przez dwa dni nękała groźbami swoje koleżanki. Prerażone dziewczynki o wszystkim powiedziały rodzicom, którzy zawiadomili policję. Prześladowczynią okazała się 16-latka. O jej dalszym losie zadecyduje sąd rodzinny”.
- „Policjanci z Wieruszowa zainteresowali się oferowanymi bardzo tanio przez internet markowymi kosmetykami. Okazało się, że sprzedaje je 22-letni mężczyzna, którego matka prowadzi sklep kosmetyczny. Kobieta nie miała pojęcia, że syn od dwóch lat ją okrada, a kosmetyki sprzedaje przez internet. Mężczyźnie grozi 10 lat więzienia”.
- „Policjanci z Makowa Mazowieckiego zatrzymali 20-letniego mężczyznę, który prowadził uprawę marihuany i przez internet udzielał porad, jak to robić. Dzisiaj odpowie za swoje czyny”.

To tylko kilka nagłówków z policyjnej kroniki, które pojawiły się w ciągu ostatniego roku, ale każdy z tematów dotyczy innego zagadnienia. Z powyższego wynika, że przestępcy wykorzystujący internet do swoich działań celują w różne dziedziny naszego życia, jednak – biorąc pod uwagę fakty świadczące o wykryciu sprawców – nie powinni czuć się bezkarni. Warto jednak zdawać sobie sprawę z tego, że często ofiarami możemy stać się na własne życzenie. Aby ustrzec się przed działaniami przestępczymi, nie wystarczy wyłącznie spełnienie podstawowych warunków, czyli – do znudzenia przypominane na każdym kroku – posiadanie legalnego, na bieżąco aktualizowanego systemu operacyjnego, firewalla oraz oprogramowania antywirusowego. Poruszając się w sieci, powinniśmy zwracać szczególną uwagę na to, czy i jaki ślad pozostawiamy po sobie.

Tak to z mentalnością przeciętnego Polaka jest, że – w odróżnieniu chociażby od Amerykanina – na bezpośrednio zadane pytanie: *Co u Ciebie?* przeważnie w odpowiedzi samo cisnie się na usta: *Stara bieda...* Zupełnie inaczej przedstawia się sytuacja, gdy piszemy sami o sobie w internecie, w szczególności gdy „rozmawiamy” z nieznanymi lub umieszczamy informacje o sobie w profilach portali

społecznościowych. Tutaj chcemy pokazać się z jak najlepszej strony i pochwalić tym, co udało się nam osiągnąć i czym pozytywnym wyróżniamy się na tle innych. A to umieszczamy zdjęcie z wakacji spędzonych w egzotycznym miejscu, a to rodzinne zdjęcie na tle swojego nowego wystrzałowego auta czy pięknego domu. A co! Niech zazdroszczą znajomi!

Od dawna wiadomo, że portale społecznościowe odwiedzane są nie tylko przez naszych znajomych, ale również przez przedstawicieli organów ścigania, firm windykacyjnych, urzędów podatkowych, a ostatnio nawet pracowników opieki społecznej wyszukujących informacji o osobach niesłusznie pobierających zasiłki socjalne. Miejsca, w których można znaleźć informacje o naszym stanie majątkowym, przyzwyczajeniach i naszych znajomych są mekką dla przestępców. Mają tutaj dostęp do podanych na tacy informacji, których zebranie w tradycyjny sposób mogłoby zająć sporo czasu i wymagałoby nie lada umiejętności. Jeśli sami umieścimy w internecie zdjęcie wnętrza swojego mieszkania/domu czy fotografię ukochanego czworonoga podpisaną jego imieniem – pozostawiamy kolejną dawkę informacji o sobie. Lista znajomych to następne potencjalne źródło wiedzy. Bulwersują nas informacje o znalezionych w śmietniku dokumentach zawierających dane osobowe, które wydostały się przypadkiem z banku czy urzędu, a nie mamy oporów przed umieszczaniem informacji o sobie w tak ogólnodostępnym medium, jakim jest internet. Przeciętny internauta odpowie:

„No tak, ale ja nie umieszczam w swoim profilu danych adresowych, więc skąd ktoś mógłby wiedzieć, gdzie mnie odnaleźć”.

Może to i prawda, sami takich informacji zazwyczaj nie umieszczamy w internecie. Ale ktoś da głowę, że któryś z naszych znajomych takich danych nie prześle zainteresowanemu? Zapytanie typu:

„Witam! Jestem starym znajomym Wojtka. Chciałbym mu zrobić niespodziankę i po latach odwiedzić go, ale tak, by go zaskoczyć. Gdzie teraz mieszka? Możesz dać mi aktualny numer jego komórki?” wysłane do dwudziestu osób z listy naszych znajomych przynajmniej w jednym przypadku nie zostanie pozostawione bez pozytywnej – dla przestępcy – reakcji. A stąd już niedaleka droga do pozbawienia nas cennych zasobów, które w pocie czoła gromadziliśmy przez lata.

Nie oznacza to, że musimy zlikwidować swój profil, by czuć się bezpiecznie, ale zwracajmy uwagę, jakie informacje w nim umieszczamy, mając świadomość, że nasze dane mogą być oglądane nie tylko przez sprzyjające nam osoby. Jeśli ktoś ma wątpliwości co do bezpieczeństwa portalu i chce zgłębić wiedzę na temat zagrożeń, jakie niesie za sobą posiadanie na nim swojego profilu, polecam uruchomienie wyszukiwarki internetowej i wpisanie frazy „nazwa portalu oszuści” lub „nazwa portalu przestępcy”, w wyniku czego otrzymamy listę artykułów, które z pewnością podniosą poziom naszej świadomości o potencjalnych niebezpieczeństwach...

Krzysztof Białek



Czy VoIP jest bezpieczne?

Nowe technologie zmieniły świat komunikacji biznesowej. Tradycyjna telefonia odchodzi do lamusa, coraz więcej firm wdraża technologię VoIP. Jednak główną wadą tej technologii, wymienianą przez wielu branżowych ekspertów, jest niższe bezpieczeństwo. Czy telefonia VoIP jest bezpieczna? Jak chronić poufność naszych rozmów? Tradycyjne centrale telefoniczne są o wiele mniej podatne na niektóre typy ataku, takie jak np. zablokowanie sieci. Jednak wprowadzenie telefonii VoIP do firmy nie musi automatycznie oznaczać zmniejszenia bezpieczeństwa komunikacji. Właściwie zarządzana sieć IP, bazująca na systemie wykorzystującym właściwe zabezpieczenia, posiada możliwości ochrony danych nawet bardziej efektywne niż tradycyjna sieć telefoniczna. Dla firm z sektora finansowego, podobnie jak dla instytucji zdrowotnych, agencji rządowych, spółek giełdowych oraz innych organizacji, w których zarządza się danymi poufnymi, zabezpieczenia komunikacji IP są kwestią o najwyższym priorytecie.



Z tego powodu producenci systemów komunikacyjnych klasy IP oraz VoIP wprowadzają najbardziej zaawansowane zabezpieczenia znane branży telekomunikacyjnej. Pierwsze i najważniejsze zabezpieczenie systemu IP stanowi osadzenie na otwartych standardach, z których najbardziej popularnym jest SIP (*Session Initiation Protocol*). Kodowanie bazujące na standardach pozwala korzystać z narzędzi tworzonych przez społeczność deweloperów na całym świecie. Cała ta społeczność zaangażowana jest w tworzenie nowych narzędzi ochrony, przeciwdziałających pomysłowości hakerów. Standard SIP ma również bardzo rygorystyczne wymagania odnośnie uwierzytelniania użytkowników i szyfrowania wiadomości. Wysoki poziom bezpieczeństwa standardu zapewnia i kontroluje organizacja IETF (*Internet Engineering Task Force*), która stale wprowadza, zmienia i ściśle monitoruje specyfikacje zabezpieczeń protokołu SIP, zapisywane w ogólnodostępnych archiwach RFC.

Najpowszechniejsze rodzaje ataków

Wyróżniłbym trzy najczęściej spotykane typy ataków związane z VoIP. Pierwszy z nich to podsłuchiwanie rozmów i przechwytywanie wartościowych informacji, ewentualnie analizowanie danych przepływających w sieci. Możemy mieć tutaj do czynienia zarówno z zewnętrznym podsłuchem i wykradaniem informacji, jak i możliwością nielegalnego użytkowania danych przez pracowników firmy.

Kolejnym rodzajem ataku jest możliwość sparaliżowania komunikacji w firmie, czyli atak typu DoS (*Denial of Services*).

Atak ten, znany od dawna użytkownikom internetu, jest w przypadku komunikacji VoIP o wiele bardziej niebezpieczny. Brak dostępu do strony www może spowodować irytację użytkownika, jednak brak kontaktu telefonicznego z firmą najprawdopodobniej doprowadzi do utraty klienta.

Inny typ ataku, na który komunikacja IP jest bardzo podatna, to wydobywanie poufnych danych dzięki podszyciu się pod rozmówcę (*vishing*, czyli *phishing* poprzez VoIP).

Jak zapobiegać atakom?

Odkąd problemy bezpieczeństwa trafiły do centrum uwagi, eksperci doszli do wniosku, że sama technologia nie wystarczy, aby zagwarantować skuteczną ochronę biura firmy oraz komunikacji przed zagrożeniami. Nawet jeżeli stosuje się w niej „najmocniejsze szyfrowanie na świecie”, może być nieskuteczna, jeśli nie wspierają jej prawidłowe, efektywnie realizowane procesy.

To samo dotyczy planowania i wdrażania procesów bezpieczeństwa oraz integrowania ludzi w organizacji, o ile działania te będą kompleksowe i spójne w obrębie całego przedsiębiorstwa. Wówczas pracownicy mogą wręcz wzmocnić zabezpieczenia. W przeciwnym wypadku mają oni szansę stać się najsłabszym ogniwem. Dlatego najsolidniejszy program bezpieczeństwa łączy nie tylko najlepszą technologię oraz najbardziej surowe procesy możliwe do zastosowania w stosunku do systemów i danych biznesowych, ale i ludzi, którzy rozumieją te procesy i do nich się stosują.

Pracownicy mogą znacząco zwiększyć ryzyko ataku, jeśli nie stosują się do korporacyjnych zasad bezpieczeństwa lub celowo je łamią dla osobistej korzyści. Coraz więcej przedsiębiorców ma świadomość luk w zabezpieczeniach, które w komunikacji IP pojawiają się z powodu czynnika ludzkiego, i stara się im przeciwdziałać. Wśród dobrych praktyk należy tutaj wymienić:

- dokładne sprawdzenie podczas rekrutacji faktów z życia potencjalnego pracownika;
- przypisanie pracownikom w organizacji praw dostępu do poszczególnych funkcji systemu zgodnych z ich pozycją w firmie oraz pełnionymi obowiązkami. Dostęp do serwerowni, gdzie przechowywane są poufne dane, powinien być ograniczony wyłącznie dla pracowników o najwyższych uprawnieniach dostępu do informacji;
- wprowadzenie systemu monitoringu rozmów oraz ekranu pracownika, przydzielenie ścisłych uprawnień do odtwarzania i korzystania z nagrań monitoringu;
- przypisanie pracownikom uprawnień do rozmów zewnętrznych, międzymiastowych oraz międzynarodowych (zależnie od potrzeb).

Za bezpieczeństwo odpowiedzialni są zarówno ludzie, jak i narzędzia systemowe. Mając na uwadze najpopularniejsze typy ataków, skuteczna strategia bezpieczeństwa powinna koncentrować się na następujących obszarach:

- Zapobieganie oszustwom. Konfiguracja systemu komunikacyjnego klasy IP powinna w możliwie maksymalnym stopniu uniemożliwiać podszywanie się lub inne złośliwe działania.
- Zapewnienie ciągłości działania systemu. Jeżeli dojdzie do ataku, wówczas serwery IP, serwery danych, telefony oraz inne urządzenia muszą zachować swoje funkcje, zapewniając wymaganą ciągłość biznesową i umożliwiając funkcjonowanie organizacji oraz pracę pracowników.
- Ochrona poufności. System powinien w możliwie maksymalnym stopniu chronić prywatność zapisów audio oraz wszelkich przechowywanych danych.

Jak chronić się przed podsłuchem

Ataki polegające na przechwyceniu danych podczas ruchu w sieci lub kradzieży zapisanych plików są możliwe głównie wtedy, gdy system komunikacji nie stosuje kodowania wiadomości. Szyfrowanie wiadomości powinno rozpoczynać się już na poziomie urządzenia, czyli telefonu (lub ekranu komputera), i rozciągać się na cały proces transportu wiadomości przez sieć, a także obejmować nagrywanie i przechowywanie informacji.

Zalecaną praktyką konieczną do ochrony rozmów w sieci komunikacyjnej IP jest szyfrowanie wiadomości za pomocą TLS (*Transport Layer Security*) oraz SRTP (*Real-time Transport Protocol*). Innym użytecznym środkiem bezpieczeństwa jest IPsec (*Internet Protocol Security*) – zabezpieczenie protokołu internetowego, tworzące szkielet o otwartym standardzie, na którym wdrażane są procesy bezpieczeństwa kryptograficznego w celu ochrony komunikacji w sieci IP. IPsec umożliwia m.in. uwierzytelnianie terminali użytkowników na poziomie sieci, uwierzytelnienie źródła danych, kodowanie danych dla zachowania poufności oraz ochronę ponownego odczytu. W przypadku telefonii korporacyjnej dostawcy zaawansowanego oprogramowania telekomunikacyjnego bazują na standardzie AES 256. Jest to jeden z najsilniejszych kluczy szyfrowania, który jest potwierdzonym i zalecanym przez wiele międzynarodowych instytucji oraz departamentów bezpieczeństwa standardem bezpieczeństwa.

Wyobraźmy sobie sytuację, gdy klient podaje przez telefon numer konta, co zostaje następnie zmagazynowane w pliku nagraniowym. Rozmowa jest świetnym celem dla złodzieja, zatem możliwość szyfrowania rozmowy, jak również kodowanie monitorowanego nagrania jest niezbędną i najlepszą praktyką ustrzeżenia się przed takimi zagrożeniami. Najlepiej rozmowy równocześnie nagrywać, monitorować i szyfrować.

Leszek Winiarski
Presales Engineer
Interactive Intelligence

MAGICARD

POTRZEBUJESZ DRUKARKI DO KART

ZADZWOŃ! (22) 832 47 44

biuro@acss.com.pl



Bezpieczny Dom

nietypowy monitoring



Komu dedykowany jest Bezpieczny Dom?

Bezpieczny Dom jest usługą, którą firma Centrum Monitorowania Alarmów (CMA) adresuje do Klientów chcących wiedzieć, co dzieje się z ich nieruchomością podczas nieobecności właścicieli, a także chcących mieć pewność, że ktoś czuwa nad ich mieniem i natychmiast powiadomi o zagrożeniu lub problemach technicznych.

To usługa dla:

- lokatora mieszkania w bloku,
- mieszkańca zamkniętego osiedla domków jednorodzinnych,
- właściciela działki,
- właściciela garażu,
- właściciela magazynu,
- zarządcy nieruchomości etc.

W trosce o jak najlepszą obsługę Klienta przygotowany został program współpracy z instalatorami, to oni bowiem mają bezpośredni kontakt z odbiorcą końcowym, znają jego potrzeby i oczekiwania.

Co wyróżnia na rynku usługę Bezpieczny Dom?

Istnieje wiele obiektów, w których interwencja patrolu ochrony jest praktycznie niemożliwa. Trudno bowiem sprawdzić w wysokim bloku czy zamkniętym osiedlu domków, czy ktoś kręci się po mieszkaniu. Do miejsc słabo zamieszkałych lub oddległych ochrona nie ma szans dojechać na czas. Istnieją obiekty, np. domy sezonowe, działki, garaże, dla których standardowa ochrona z przyjeżdżającym patrolom jest zbyt droga. Do ochrony wszystkich tych obiektów CMA dedykuje usługę Bezpieczny Dom.

Są rzeczy, których nie da się kupić za żadne pieniądze – należą do nich spokój i poczucie bezpieczeństwa. Dlatego nawet tam, gdzie nie ma potrzeby lub możliwości korzystania z patrolu ochrony, wskazane jest, aby informacje o zagrożeniach niezwłocznie docierały do klienta.

Interwencja ochrony zazwyczaj kojarzy się z włamaniem, ale włamanie to tylko jedno z zagrożeń pozostawionego bez nadzoru mienia. Usługa Bezpieczny Dom informuje Klienta nie tylko o włamaniu, ale także o innych zagrożeniach, takich jak:

- alarmy techniczne,
- zalanie pomieszczenia wodą,
- ulatnianie się gazu,
- spadek zasilania w monitorowanej instalacji,
- włączenie/wyłączenie monitorowanej instalacji,
- zagrożenie pożarowe,
- ogólne usterki.

Usługa Bezpieczny Dom w ramach stosunkowo niskiego abonamentu pozwala dość dowolnie definiować te sygnały, które są istotne dla właściciela.

Informacje o zagrożeniach powinny niezwłocznie docierać do Klienta, dzięki czemu interwencja ochrony w tych przypadkach jest zbędna.

Jak działa usługa Bezpieczny Dom?

Korzystanie z usługi Bezpieczny Dom ma być w swoim założeniu proste i przyjazne dla odbiorcy. Usługa polega na odbieraniu z nieruchomości różnych sygnałów alarmowych i przekazywaniu ich upoważnionym osobom w postaci SMS-a. Istnieją dwa rodzaje powiązanych ze sobą powiadomień:

1. Powiadomienie automatyczne

Po odebraniu alarmu system klasyfikuje jego typ, generuje go i właścicielowi obiektu wysyła automatycznie SMS-a z treścią zdefiniowaną dla zaistniałego zdarzenia. Po wysłaniu SMS-a system czeka przez trzy minuty na potwierdzenie doręczenia. Jeżeli osoba upoważniona otrzyma SMS, do systemu dociera potwierdzenie tego faktu i procedura powiadamiania zostaje zakończona.

2. Powiadomienie ręczne

Jeżeli w ciągu trzech minut osoba upoważniona nie odbierze wiadomości tekstowej, operator Stacji Monitorowania Alarmów dzwoni na kolejne numery telefonów wskazane

w karcie zgłoszenia obiektu. Jeżeli mimo to powiadomienie się nie uda, operator ponawia próby co 15 minut. Po 4 godzinach operator kończy obsługę alarmu, wpisując raport o niepowodzeniu zgłoszenia o zagrożeniu.

Realizacja umowy na świadczenie usługi Bezpieczny Dom rozpoczyna się tego samego dnia, w którym została podpisana umowa. Po dostarczeniu do CMA dokumentów, w tym stosownych haseł i telefonów, zostają one wpisane do systemu i usługa zostaje uruchomiona.

Jakie zalety posiada korzystanie z usługi Bezpieczny Dom?

- Dzięki technologii GSM/GPRS usługa działa na terenie całego kraju.
- Zapewnia ochronę elektroniczną przez 24 h/7 dni.
- Zniżki w ubezpieczeniach.
- Niski abonament.
- 24-godzinny nadzór nad pracą systemu alarmowego i natychmiastowa reakcja na usterki.
- Stała kontrola łączności z obiektem i natychmiastowa reakcja na usterki.

Kto dostarcza odbiorcy usługę Bezpieczny Dom?

Nad technicznym procesem instalacji czuwa instalator posiadający odpowiednie uprawnienia i rekomendację dostawcy usługi. Teoretycznie jest jedyną osobą, która kontaktuje się z odbiorcą końcowym.

CMA

Powierzając swoje mienie firmom świadczącym usługi szeroko rozumianej ochrony, każdy chce mieć pewność jej wiarygodności i doświadczenia. CMA świadczy usługi w zakresie technicznej ochrony osób i mienia na terenie całego kraju. Firma funkcjonuje na polskim rynku od 1995 roku. Podstawą prawną do działalności jest wydana przez Ministra Spraw Wewnętrznych koncesja Nr L-1836/00. Zaufanie kilkudziesięciu tysięcy Klientów stanowi najlepsze świadectwo i gwarancję wysokiej jakości świadczonych usług. Ważnym etapem rozwoju firmy było przejęcie w październiku 2005 r. Satelitarnego Systemu Pozycjonowania Pojazdów Liberty GPS, co umocniło CMA na pozycji jednej z największych w Polsce firm świadczących usługi ochrony. Znając specyfikę rynku zabezpieczeń, CMA nieustannie weryfikuje wewnętrzne struktury bezpieczeństwa. Mimo posiadania koniecznych zezwoleń i certyfikatów dobrowolnie poddaje się kontroli upoważnionych do tego organów, mając zawsze na względzie bezpieczeństwo danych Klienta. CMA jest członkiem PISA (CMA posiada rekomendację wiarygodności PISA), homologację Ministerstwa Transportu i Budownictwa Nr E20 10R-02 1917, Świadectwo Autoryzacji PIMOT Nr 02A/BLE/SMP/08. Dodatkowo ubezpieczyciele, honorujący systemy zabezpieczeń CMA i udzielający po ich zainstalowaniu znacznych zniżek, są z oczywistych względów gwarantem ich niezawodności i skuteczności.

SZKOŁA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ TECHOM w WARSZAWIE

inż. Bogdana Tatarowskiego

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

zaprasza na

KURSY ZAWODOWE

w zakresie

► Instalowania, konserwacji i eksploatacji systemów alarmowych

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

► Projektowania systemów alarmowych w klasach od SA-1 do SA-4

Dla obiektów cywilnych i wojskowych oraz obiektów z tzw. „listy wojewody”

► Zarządzania bezpieczeństwem obiektu

Bezpieczeństwo teleinformatyczne
Wymogi Prawne i normatywne

► Rzeczoznawstwa

- Systemy Technicznego Zabezpieczenia Osób i Mienia
- Zarządzania Bezpieczeństwem Obiektu

Autoryzacja absolwentów kursów

Dla potrzeb inwestorów
i towarzystw ubezpieczeniowych

Informacja oraz przyjmowanie zgłoszeń:

TECHOM

ul. Marszałkowska 60/27

00-545 Warszawa

tel. 022 625 34 00, 022 625 32 96

tel./faks 022 625 26 75

e-mail: techom@techom.pl

www.techom.com



Wideoweryfikacja

najnowsze osiągnięcie firmy Bosch

Technologia IP, ciągła łączność online, kody PIN, biometria – to standard funkcji, do których Bosch zdążył już nas przyzwyczaić. Teraz czas poznać nową funkcję, czyli wideoweryfikację.

1 lipca 2009 roku odbyła się premiera pakietu Access Professional Edition – najnowszej wersji oprogramowania kontroli dostępu Bosch. Oprócz zwiększenia limitu obsługiwanych czytników oraz użytkowników systemu do najważniejszych zmian należy wprowadzenie funkcji wideoweryfikacji oraz zarządzanie systemem zamków i skrzytek hotelowych

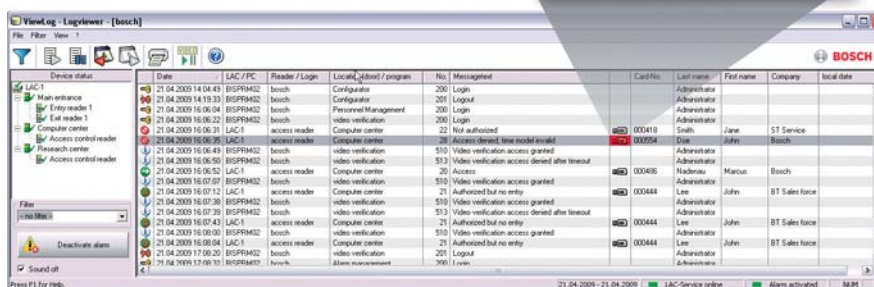
W wersji Access Professional Edition 2.0 (jest to oznaczenie nowego oprogramowania) będzie można zarządzać systemem o wielkości 128 czytników (w poprzedniej wersji były 64 czytniki) oraz bazą danych ludzi wielkości 10 000 użytkowników (do tej pory było 2 000). Co więcej, każdy z użytkowników będzie mógł posiadać przynajmniej trzy różne identyfikatory (karty, breloki, piloty itp.). Rozszerzenia te umożliwią rozbudowę istniejących systemów kontroli dostępu o dodatkowe przejścia lub o nowych pracowników w sytuacjach, gdy nie są potrzebne zaawansowane funkcje oraz zarządzanie z bardziej rozbudowanego systemu Access Engine, a limitem jest tylko liczba parametrów zgromadzonych w bazie.

Jednak prawdziwą rewolucją tworzącą w rozwiązaniu nową funkcję jest zastosowanie **wideoweryfikacji**, i to w systemach o niewielkiej liczbie przejść (do tej pory funkcja ta była zarezerwowana tylko dla systemów integrujących budynkowe systemy bezpieczeństwa). Poprzez sprzężenie z kamerami rozmieszczonymi w obiekcie funkcja ta pozwala znacznie podwyższyć bezpieczeństwo systemu. Na każde przejście można przypisać aż pięć kamer! (Fot. 1) Jedną kamerę do weryfikacji twarzy, dwie do obserwacji przestrzeni przed drzwiami (czy weryfikowana osoba jest sama, czy wnosi ze sobą jakiś pakunek, czy trzyma coś za plecami etc.) oraz dwie kamery po wewnętrznej stronie drzwi, które potwierdzają autoryzowany dostęp uprawnionej

Fot. 1. Przykład sprzężenia systemu kontroli dostępu z systemem monitoringu



Fot. 2. Lista zdarzeń przechowywanych na rejestratorze z wybranym nagraniem zdarzenia



osoby. Obraz twarzy z kamery przy wejściu porównujemy z zapamiętanym w bazie obrazem prawowitego posiadacza karty. Weryfikacja ta może być jeszcze wzmocniona koniecznością podania kodu PIN lub biometrią.

Sprzężenie systemu kontroli dostępu z rejestratorami wideo daje jeszcze jedną bardzo praktyczną funkcję. Mianowicie, przeglądając logi (rejestry, dzienniki – przyp. red.) zdarzeń z kontroli dostępu i klikając myszką na interesujące nas zdarzenie, można mieć natychmiastowy dostęp do nagrania tego zdarzenia, przechowywanego na rejestratorze (Fot. 2). Wyświetlona zostanie scena z kilku- lub kilkunastosekundowym wyprzedzeniem. Można obserwować osobę, która podchodzi do drzwi i przykładając kartę do czytnika dostępu. Następnie widać tę osobę z kolejnej kamery już po drugiej stronie drzwi. Co więcej, materiał wideo może dotyczyć również alarmu wzbudzonego na jednym z wejść przekąźnikowych – a więc można dokładnie prześledzić przebieg siłowego otwarcia drzwi lub naruszenie okna zabezpieczonego kontaktronem. W ten sam sposób może zostać również podłączona czujka ruchu czy czujka zbitcia szkła.

Wykorzystując tę funkcję, bardzo szybko można przejrzeć nagrania na przykład z weekendu, kiedy zazwyczaj liczba osób wchodzących i wychodzących z biura jest niewielka, a zdarzenia te są rozciągnięte w czasie i przejrzanie materiału byłoby czasochłonne. Dodatkowo każde zdarzenie opatrzone jest kompletem informacji dotyczących danych personalnych osoby wchodzącej. W połączeniu z informacją wizualną, która pokazuje, czy jest to osoba uprawniona do wejścia i czy wносиła lub wynosiła ze sobą jakieś przedmioty, jesteśmy w stanie bardzo szybko odtworzyć przebieg zdarzeń.

Wideo weryfikacja zarchiwizowanych zdarzeń może też doskonale sprawdzić się przy weryfikacji pracowników korzystających z funkcji rejestracji czasu pracy (RCP). Położony lub osoba z działu personalnego w każdym momencie może wybrać dowolnego pracownika i sprawdzić, czy w ostatnim czasie wszystkie odbicia jego karty przy wejściu/wyjściu z pracy były dokonane przez niego osobiście, czy też przez kolegę posiadającego jego kartę. W ten sposób można również, oglądając nagrania osób wchodzących do budynku i odbicia ich kart, zweryfikować wydarzenia

dotyczące pojedynczych wejść. Wszystkie potencjalne nadużycia są w pełni udokumentowane i nie pozostawiają wątpliwości. Ponadto taki materiał, ilustrujący naruszenie przepisów możemy wyeksportować do pliku i wykorzystać w dalszym postępowaniu wyjaśniającym bądź karnym. Można zapisywać pojedyncze kadry lub całe sekwencje nagrane na wideo.

Nowa wersja oprogramowania Access Professional Edition zapewni również wsparcie dla systemów hotelowych. System ten będzie współpracował z systemem zamków pracujących w trybie offline, które nie są podłączone do systemu za pomocą tradycyjnego okablowania. Istotne nowości tego systemu to karty dla gości hotelowych programowane w recepcji oraz drzwi do pokoi hotelowych wyposażone w specjalne zamki niewymagające połączenia kablowego z centralą. Jest to niezwykle wygodne rozwiązanie w przypadku budynku wielopokojowego, w którym zebranie informacji ze wszystkich pięter wiązałoby się z założeniem prawdziwej pajęczyny przewodów. Rozwiązanie to sprawdzi się doskonale również w obiektach zabytkowych, gdzie nie wolno stosować przewodów ze względu na charakter budynków. Centralnym punktem systemu jest recepcja, gdzie karty są tak programowane, aby posiadały zakodowany numer pokoju oraz informację, na jaki czas gość ma dostęp

Fot. 3. Przykład wyświetlania

zdjęć i danych osób przechodzących przez dane przejście



do danego pokoju. Za pomocą tradycyjnych czytników system można rozszerzyć w ten sposób, aby uzyskać również dostęp do pomieszczeń personelu, magazynów i wyjść służbowych (gdzie można realizować np. rejestrację czasu pracy i monitorowanie przebywania w strefie). Strukturę takiego systemu – OLS (*Offline Lock System*) – można przedstawić w sposób podany na rys. 1.

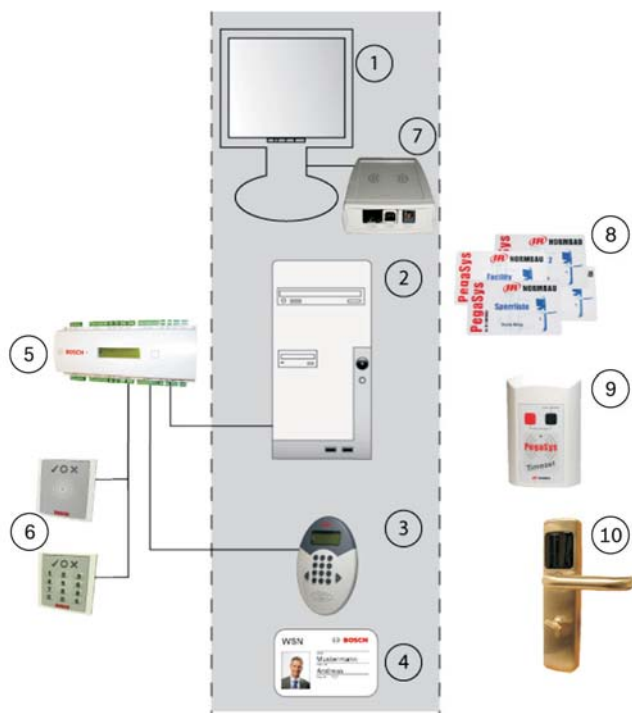
Kolejną bardzo praktyczną funkcją systemu jest „online swipe” (Fot. 3). Funkcja ta umożliwia wyświetlanie i odświeżanie na żywo zdjęć oraz danych ostatnich pięciu osób przechodzących przez dane przejście. Operator siedzący z boku (ochrona czy pracownik recepcji), nie zatrzymując osób przechodzących w tradycyjny sposób przez przejście lub odbijających kartę na czytniku RCP, może na bieżąco porównywać twarze z bazy danych przypisane do kart z ich aktualnymi posiadaczami. W razie wychwycenia niezgodności można szybko zidentyfikować takiego intruza. W przypadku użytkownika, który nie uzyskał autoryzacji, wyświetlone zostanie zdjęcie osoby nieuprawnionej, jej pełne dane osobowe oraz informacja o przyczynie odmowy dostępu (brak uprawnień, nieprawidłowy model czasowy czy np. podwójne użycie karty).

Wszystkie powyżej opisane funkcje dają niezwykle bogatą paletę możliwości zwiększających bezpieczeństwo naszego systemu. Mimo że nowych funkcji jest bardzo wiele, w żaden sposób nie ucierpiała na tym intuicyjność programu. Można nawet stwierdzić, że dodanie elementów wizualnych zdjęć pracowników oraz podglądu wideo ogranicza jeszcze bardziej liczbę parametrów, które trzeba wpisywać, i prezentuje w postaci wizualnej odpowiedź stanu lub oczekiwanych działań. Cały pakiet podzielony został na mniejsze podaplikacje, dzięki czemu poszczególni operatorzy muszą nauczyć się jedynie 10–15% wszystkich opcji systemu, mając jednocześnie pełny dostęp do funkcji wymaganej na ich stanowisku.

W skład pakietu Access Professional Edition wchodzi kilka dedykowanych podaplikacji:

- konfigurator (przeznaczony dla administratora),
- zarządzanie personelem (dla działu personalnego i recepcji),
- przeglądanie dziennika zdarzeń,
- aplikacja do zarządzania alarmami (dedykowana dla pracowników ochrony).

Tak prezentują się nowe funkcje w oprogramowaniu Access Professional Edition 2.0. Jest to kolejny efekt pracy ambitnego i zdolnego zespołu działu badań i rozwoju firmy Bosch. Obecnie trwają prace nad przygotowaniem kolejnej wersji oprogramowania planowanego do wprowadzenia na rynek pod koniec bieżącego roku. Kolejna edycja ma być wzbogacona między innymi o rozszerzenie funkcji alarmowych. Dział R&D (Research and Development – badania i rozwój – przyp. red.) przygotowuje również nową wersję zaawansowanej edycji systemu – Access Engine, która obecnie funkcjonuje w ramach pakietu integracyjnego BIS w wersji 2.2.



Rys. 1. 1. Stacja Robocza, 2. Serwer z aplikacją konfiguracyjną i bazą danych, 3. Czytnik kart z opcją zapisu, 4. Karta – może być wykorzystana w obu systemach (offline i online), 5. Kontroler AMC2, 6. Tradycyjny czytnik kontroli dostępu, 7. Czytnik dialogowy do przypisywania kart, 8. Karty systemowe do OLS, 9. Moduł programowania daty i czasu, 10. Terminal OLS

Marcin Ryżko
Bosch Security Systems



AQAP 2110:2006



firma
ATLine[®]
kompleksowe zabezpieczanie obiektów



BEZPIECZEŃSTWO W KAŻDYCH WARUNKACH

16 lat doświadczenia, profesjonalizm i wysoka jakość oferowanych przez nas usług, gwarantują Państwu pełną satysfakcję. Oferujemy Państwu atrakcyjne ceny, bezpłatne szkolenia i wsparcie fachowców w ramach zakupu. Zapraszamy na naszą stronę www.atline.pl Wszelkie wyceny i propozycje zabezpieczeń przeprowadzamy bezpłatnie.

**16 LAT
DOŚWIADCZENIA**

- wykonywanie kompleksowych dokumentacji technicznych i architektoniczno-budowlanych
- wykonywanie zaawansowanych systemów bezpieczeństwa
- sprzedaż (głównie zewnętrznych systemów ochrony obwodowej)

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

Integracja systemów alarmowych i systemów zarządzających pracą urządzeń w budynku mieszkalnym

W budynkach mieszkalnych już w fazie projektowania instalacji elektrycznych coraz częściej rozważa się możliwość zastosowania autonomicznych układów sterujących i zarządzających pracą poszczególnych grup urządzeń (oświetlenia, ogrzewania) oraz nadzorujących stan obiektu (systemy alarmowe). W artykule zwrócono uwagę na możliwości zastosowania zintegrowanych systemów zarządzających pracą urządzeń w budynkach i jednocześnie realizujących funkcje kontroli nad stanem obiektów. Budowa takich układów umożliwi scalenie pod względem funkcyjnym i sprzętowym poszczególnych autonomicznych, realizujących tylko wybrane cele systemów w jeden zintegrowany system zarządzany centralnie.



1. Wstęp

Zadania stawiane nowoczesnym instalacjom elektrycznym w budynkach nie ograniczają się już tylko do niezawodnego dostarczania energii elektrycznej o wymaganych parametrach. Obecnie oczekuje się, aby wyspecjalizowane układy sprawowały kontrolę nad stanem obiektu i sterowały pracą zainstalowanych w nim urządzeń. W tym celu wyposaża się instalacje w układy sterujące umożliwiające realizację zamierzonych przez użytkownika funkcji i procedur. Takie układy mają realizować założone cele związane z działaniem oświetlenia, ogrzewania, wentylacji, a także spełniać rolę systemów alarmowych oraz systemów informujących użytkownika o stanie obiektu. Dzięki temu często możliwe jest podwyższenie komfortu użytkowania oraz podniesienie bezpieczeństwa przy jednoczesnym ograniczeniu kosztów eksploatacji takich instalacji.

W przypadku systemów zarządzania można wyróżnić dwa ich główne rodzaje:

- system wyspowy, czyli system bazujący na układach autonomicznych. Każdy z nich realizuje jedynie ściśle wyznaczone zadania (np. tylko steruje ogrzewaniem w budynku lub tylko realizuje funkcje systemu alarmowego);
- system zintegrowany, czyli system bazujący na scentralizowanym układzie zarządzania.

Zarówno w systemach autonomicznych, jak i systemach całkowicie zintegrowanych funkcje poszczególnych obwodów są takie same. Od obwodu sterującego ogrzewaniem w dalszym ciągu wymaga się stworzenia użytkownikowi odpowiedniego komfortu cieplnego. Zadaniem elementów systemu alarmowego jest natomiast wygenerowanie sygnału alarmowego

w przypadku wykrycia zagrożenia dla użytkownika lub dla chronionego mienia. Różnica jest taka, że w systemie całkowicie zintegrowanym sygnały pochodzące od wszystkich elementów wejściowych (detektorów, czujek) kierowane są do jednego układu analizującego-decyzyjnego i układ ten steruje pracą poszczególnych elementów wyjściowych.

Celem tego artykułu jest przedstawienie możliwości wykorzystania nowoczesnych systemów zarządzających pracą elementów wyposażenia budynku, bazujących na technologiach EIB (ang. *European Installation Bus*) oraz PLC (ang. *Programmable Logic Controller*), do budowy zintegrowanych systemów realizujących funkcje autonomicznych systemów sterowania. Dodatkowo zostanie przedstawiona rola i możliwości układów, które realizują funkcje stawiane systemom alarmowym w takich zintegrowanych systemach.

Przedstawione w artykule rozwiązania technologiczne będą miały zastosowanie do układów stosowanych w budownictwie mieszkaniowym.

W artykule zwrócono również uwagę na zwiększenie możliwości proceduralnych i funkcyjnych układu odpowiedzialnego za realizowanie zadań systemu alarmowego. W przypadku zastosowania systemu zintegrowanego, gdzie układ decyzyjno-sterujący posiada bieżące informacje o aktualnym stanie wszystkich elementów detekcyjnych występujących w systemie (nie tylko tych związanych z klasycznym systemem alarmowym) oraz historii ich zmienności, możliwa jest realizacja bardziej złożonych funkcji niż w przypadku dysponowania informacjami tylko od typowych czujek systemu alarmowego.

2. Systemy sterujące pracą urządzeń elektrycznych w budynkach mieszkalnych

Pierwsze systemy sterowania pracą urządzeń elektrycznych w budynkach mieszkalnych umożliwiały jedynie załączanie i wyłączanie odbiorników za pomocą łączników. Dzięki postępowi technologicznemu i zastosowaniu układów przekątnikowo-stycznikowych systemy te umożliwiały już realizację bardziej złożonych funkcji, takich jak na przykład cykliczne uruchamianie odbiorników. Kiedy na rynku pojawiły się czujki, układy sterowania mogły zostać połączone z elementami detekcyjnymi i załączać odpowiednie elementy wykonawcze w przypadku zadziałania elementów detekcyjnych lub przekroczenia w nich pewnych wartości granicznych. Wykorzystanie układów cyfrowych umożliwiło zastosowanie w układach sterowania funkcji logicznych. Nadejście technik mikroprocesorowych pozwoliło natomiast na wyposażenie układów sterowania w systemy ekspertowe, bazodanowe, a nawet układy bazujące na technikach sztucznej inteligencji.

W budynkach mieszkalnym można obecnie wyróżnić trzy rodzaje systemów sterujących pracą urządzeń elektrycznych:

- system sterowania ręcznego,
- system realizujący funkcje automatyki budynku,
- system realizujący funkcje inteligentnego budynku.

System sterowania ręcznego to system, w którym wszystkie włączenia i wyłączenia odbiorników odbywają się fizycznie przez użytkownika systemu.

System realizujący funkcje automatyki budynku to system sterujący pracą elementów wykonawczych na podstawie zależności między stanami elementów detekcyjnych. Pierwsze powszechnie wykorzystywane systemy zautomatyzowane to systemy alarmowe: systemy sygnalizacji włamania i napadu (SSWiN) oraz systemy sygnalizacji pożarowej (SSP). W momencie wykrycia zagrożenia umożliwiały one włączanie odpowiednich elementów wykonawczych (sygnalizatorów lub urządzeń) bez ingerencji użytkownika. Mimo znacznej skuteczności i wzrostu wydajności rozwiązanie to miało poważną wadę, ponieważ poszczególne systemy automatyki nie współpracowały ze sobą.

System realizujący funkcje inteligentnego budynku to system, który w sposób celowy i właściwy samoistnie reaguje na występujące w jego otoczeniu zdarzenia i zmieniające się czynniki zewnętrzne [4]. Główną różnicą między systemem realizującym funkcje automatyki budynku a systemem realizującym funkcje budynku inteligentnego jest większe skomplikowanie procedur sterujących oraz powiązanie algorytmu działania z aktualnymi stanami innych niezależnych układów. Zatem w przypadku systemów realizujących funkcje inteligentnego budynku konieczne staje się współdziałanie pomiędzy poszczególnymi układami sterującymi. W systemach tych funkcje bazują na wykorzystaniu w algorytmie działania sprzężeń zwrotnych.

Ponieważ inteligentna instalacja charakteryzuje się nie tylko zautomatyzowaniem procesu sterowania, ale również zintegrowaniem poszczególnych podsystemów, obecnie widoczny jest trend dążący do stosowania central decyzyjno-sterujących. W przypadku małych systemów oraz tych niezagrażonych aktami sabotażu dąży się do zastosowania pojedynczych samodzielných jednostek sterujących. Natomiast w przypadku systemów bardziej rozbudowanych, w których wymagany jest odpowiedni poziom bezpieczeństwa i niezawodności systemu,

a także tych realizujących funkcje systemu sygnalizacji włamania i napadu oraz kontroli dostępu, w których system narażony jest na akty sabotażu, stosuje się sterowanie systemem za pomocą jednostek rozproszonych połączonych w sieć.

3. Integracja autonomicznych układów sterowania

Proces integracji systemu polega na połączeniu poszczególnych instalacji, autonomicznych pod względem funkcji pełnionych w obiekcie, w jeden system realizujący wszystkie zadania stawiane poszczególnym częściom wchodzącym w skład systemu. Systemy zintegrowane sterują wieloma funkcjami i kontrolują wiele urządzeń wykonawczych w budynku. Szczególnie ważne są obwody:

- sterowania oświetleniem,
- sterowania ogrzewaniem,
- sterowania wentylacją i klimatyzacją,
- sterowania pracą systemu alarmowego (włamaniowego i pożarowego),
- sterowania pracą systemu kontroli dostępu.

Ze względu na poziom integracji systemów w budynku wyróżniamy 4 poziomy [1]:

- poziom 1 (każdy system instalacji tworzy odrębną całość),
- poziom 2 (podsystemy zintegrowane są za pomocą łącza szeregowego),
- poziom 3 (poszczególne systemy obiektu połączone są za pośrednictwem sieci LAN),
- poziom 4 (wszystkie systemy podłączone są do wspólnej magistrali systemowej).

Integracja systemów autonomicznych może odbywać się w następujący sposób:

- poprzez wymianę informacji między systemami autonomicznymi (Rys. 1),
- poprzez współdzielenie przez systemy elementów detekcyjnych i wykonawczych (Rys. 2),
- poprzez realizację funkcji przypisanych poszczególnym systemom przez ten sam układ sterujący (Rys. 3).

Integracja systemów poprzez wymianę informacji to najprostszy sposób współdziałania pomiędzy systemami autonomicznymi. Wszystkie systemy działają w sposób autonomiczny, jednak wymieniają się między sobą informacjami o stanach określonych wejść i wyjść. W tym przypadku każdy system autonomiczny wie, jakie stany są w określonych punktach systemu i na podstawie tych informacji może dopasować swój algorytm działania do określonych warunków.

Integracja systemów poprzez współdzielenie elementów polega na podłączeniu elementów, stanowiących część wspólną między systemami, do niezależnych od siebie central zarządzających pracą poszczególnych obwodów. Takie rozwiązanie zwiększa ergonomię użytkownika systemu, umożliwia lepszą jego konfigurację oraz ogranicza koszty instalacji poprzez wyeliminowanie dublowania elementów, które realizują tę samą funkcję, ale współpracują tylko z jednym wybranym autonomicznym układem (np. tylko z systemem SSWiN). Wymaga jednak rozważnego zasilania współdzielonych elementów (szczególnie detekcyjnych) oraz nadawania hierarchii ważności rozkazom przychodzącym ze sterowników (ważne w przypadku elementów wykonawczych).

W przypadku wykorzystania jednego układu sterującego pracą całego systemu znikają problemy związane z systemami autonomicznymi. Wszystkie elementy podłączone są do jednego sterownika. Dzięki takiemu rozwiązaniu występuje tylko jeden układ nadzorujący, który ma dostęp do wszystkich informacji pochodzących z elementów detekcyjnych i w zależności od ustalonego przez użytkownika stanu (trybu)

pracy realizuje założone funkcje. System charakteryzuje się brakiem zdublowanych procedur oraz najszybszym czasem reakcji na rejestrowane zdarzenia. Rozwiązanie takie daje dużo większe możliwości w budowie algorytmu sterującego pracą systemu, jednak zazwyczaj wiąże się z koniecznością poznania języków programowania lub współpracy z wyspecjalizowanym serwisem.

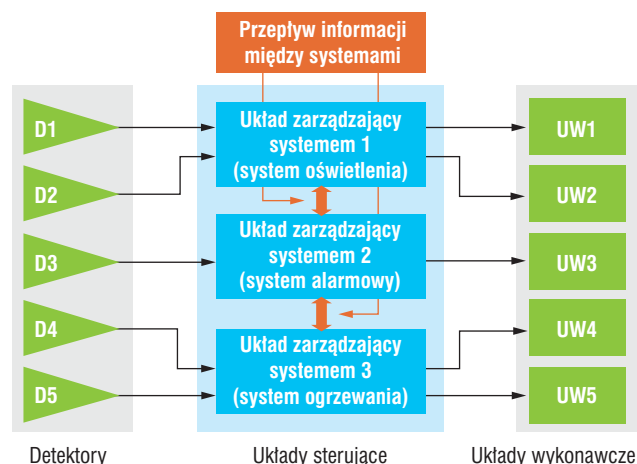
4. Systemy realizujące funkcje inteligentnego budynku

Obecnie występuje wiele rodzajów systemów umożliwiających realizację funkcji inteligentnego budynku. W pracy zostaną opisane dwa podstawowe:

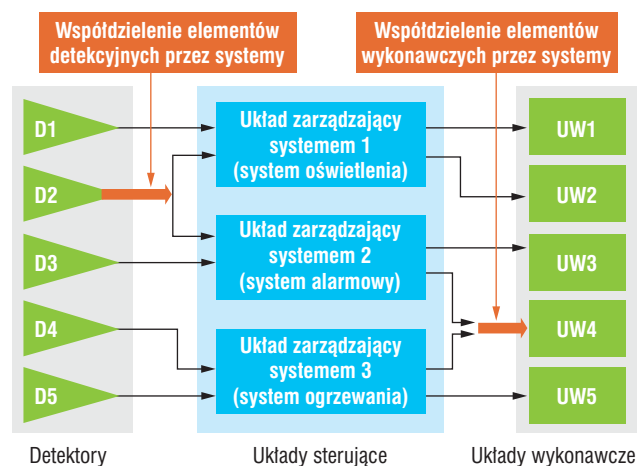
- system bazujący na magistrali EIB (stosowany w przypadku nowych instalacji),
- system bazujący na sterownikach PLC (wykorzystywany przy adaptacji istniejącej instalacji do pełnienia funkcji inteligentnego budynku).

4.1. Systemy oparte na magistrali EIB

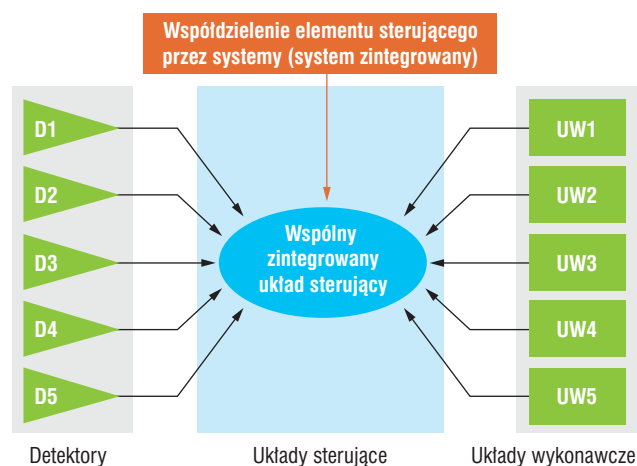
System EIB (ang. *European Installation Bus*) powstał w 1990 r. i służy do załączania, sterowania, regulowania oraz nadzoru urządzeń elektrycznych. Cechą charakterystyczną systemu jest zastosowanie jednego, łączącego wszystkie elementy systemu, przewodu magistralnego na 24 V (napięcie bezpieczne), natomiast urządzenia wymagające 230 V są zasilane bezpośrednio. Z uwagi na brak centralnej jednostki decyzyjnej system jest bardzo elastyczny – wszelkie modyfikacje wymagają jedynie wymiany lub zainstalowania dodatkowych elementów, a przeprogramowanie całego układu nie jest konieczne. Urządzenia komunikują się ze sobą za pomocą telegramów – nadawca (np. czujka ruchu) wysyła informację do wszystkich podłączonych do przewodu magistralnego urządzeń, ale odbiera ją tylko zaprogramowany element, a pozostałe ignorują. Należy pamiętać, że telegram może być zaadresowany do wielu urządzeń (np. jeden przycisk może załączać całe oświetlenie w pomieszczeniu lub budynku), co znacząco zwiększa wygodę użytkowania instalacji w systemie EIB [5]. Schemat blokowy systemu EIB został przedstawiony na rys. 4. Z powodu konieczności ułożenia i podłączenia przewodu magistralnego do wszystkich elementów instalacji system EIB jest wykorzystywany w obiektach nowopowstających lub poddawanych gruntownej renowacji.



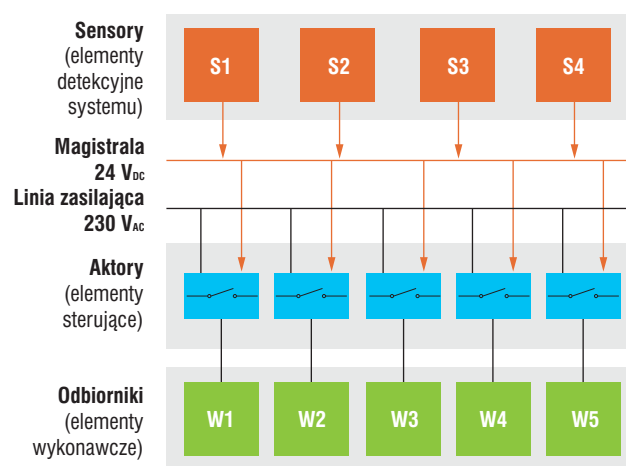
Rys. 1. Integracja systemów poprzez wymianę informacji



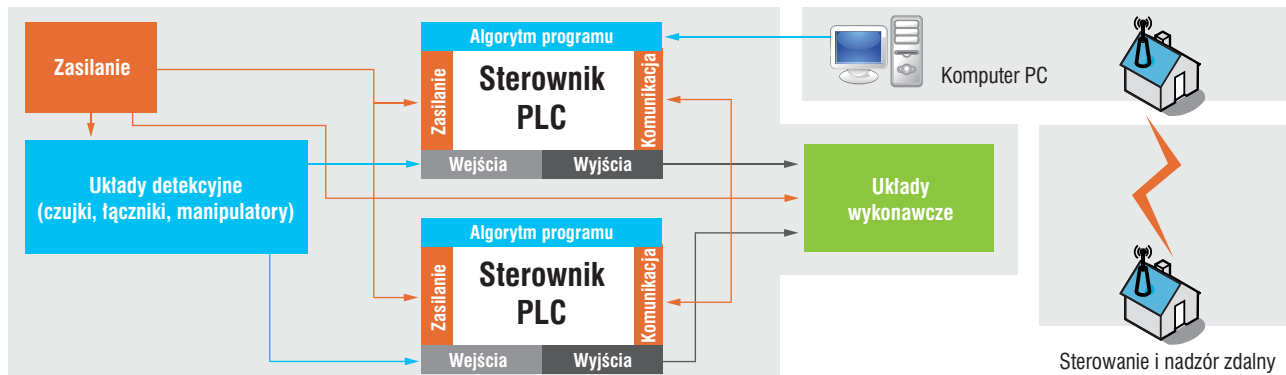
Rys. 2. Integracja systemów poprzez współdzielenie elementów infrastruktury



Rys. 3. System w pełni zintegrowany pod względem sprzętowym i funkcyjnym



Rys. 4. Struktura systemu EIB



Rys. 5. Schemat blokowy zintegrowanego systemu zarządzającego pracą urządzeń w budynku mieszkalnym opartego na wykorzystaniu sterownika PLC jako jednostki zarządzającej

4.2. Systemy bazujące na sterownikach PLC

W przypadku gdy użytkownik istniejącego budynku nie planuje prac remontowych i nie jest możliwe, choćby ze względów estetycznych, ułożenie przewodów magistralnych, preferuje się rozwiązanie pośrednie z wykorzystaniem sterowników PLC. Sterownik PLC to układ mikroprocesorowy przeznaczony do sterowania pracą urządzeń i procesów. Sterowniki PLC spełniają wszystkie funkcje stycznikowych i przekaźnikowych układów sterowania, układów logicznych, programatorów oraz układów przetwarzających sygnały dyskretnie i ciągłe [2]. W systemie zarządzania sterowniki PLC działają na zasadzie scentralizowanego układu nadzorującego, a ich moduły wejść i wyjść mogą dopasować się do aktualnych potrzeb użytkownika. Wadą takiego rozwiązania jest konieczność znajomości specyficznych języków programowania, daje ono jednak możliwość dowolnej konfiguracji i tworzenia bardzo zindywidualizowanych algorytmów sterujących [3]. Schemat blokowy systemu zarządzanego za pomocą sterowników PLC został przedstawiony na rys. 5.

5. Realizacja funkcji systemów alarmowych w systemach zintegrowanych

System alarmowy włamaniowy (system alarmowy) to zespół współpracujących urządzeń (również z instalacją przewodową), który ma na celu wykrywanie zagrożeń mienia spowodowanych włamaniem, a następnie wywołanie alarmu i inicjowanie przedsięwzięć zmierzających do likwidacji takiego zagrożenia. Z opisu tego wynika, że systemy alarmowe wcale nie muszą być działającymi autonomicznie układami. Obecnie budowane systemy alarmowe (centrale alarmowe) umożliwiają zarówno informacyjną, jak i sprzętową realizację funkcji integracyjnych. Coraz częściej systemy alarmowe wyposaża się w dodatkowe, niekoniecznie związane z wykrywaniem zagrożenia w postaci włamania, napadu czy pożaru, czujki (np. czujki zalania montowane w łazienkach). W artykule zostanie przedstawiony proces odwrotny, czyli wyposażenie zintegrowanego systemu zarządzającego w elementy przypisane do systemów alarmowych (czujki, sygnalizatory). Taki proces adaptacji nowych funkcji jest szczególnie istotny w przypadku gwarancji podołania oczekiwaniami i realizacji zadań stawianym systemom alarmowym przez zintegrowane systemy zarządzające, które stanowią

instalacje elektryczne w budynkach mieszkalnych. W dalszej części artykułu zostaną przedstawione przykłady, które ukażą przewagę funkcyjnych możliwości zintegrowanych systemów zarządzających nad rozwiązaniami autonomicznymi.

5.1. Współpraca pasywnych czujek podczerwieni PIR z systemem oświetlenia

W autonomicznym systemie alarmowym czujki PIR spełniają swoją rolę tylko w stanie dozoru, wówczas gdy inicjują proces sygnalizacji naruszenia chronionej strefy w przypadku wykrycia intruza.

W systemie zintegrowanym w stanie dozoru czujki zainicjują proces sygnalizacji naruszenia strefy chronionej, natomiast w innej sytuacji mogą być użyte jako elementy wykrywające obecność użytkownika. Mogą również sterować pracą układu oświetleniowego w danym pomieszczeniu (wykorzystując na przykład dodatkowo funkcje timerów w celu podtrzymania oświetlenia przez założony okres czasu).

5.2. Współpraca czujek kontaktronowych z systemem ogrzewania

W przypadku autonomicznego systemu alarmowego czujka magnetyczna spełni swoją rolę w stanie dozoru, wtedy, gdy nastąpi rozwarcie elementów kontaktronu zamontowanego np. w oknie, lub uniemożliwi uzbrojenie systemu alarmowego, jeżeli wykryje, że elementy kontaktronu nie są umieszczone blisko siebie (co może być oznaką niedomknięcia okna przez użytkownika).

W przypadku systemu zintegrowanego oprócz realizacji wymienionych funkcji rozwarcie elementów kontaktronu będzie skutkowało wyłączeniem ogrzewania w danym pomieszczeniu na czas przewietrzania.

5.3. Współpraca czujników zalania z systemem alarmowym i systemem hydraulicznym

W przypadku autonomicznego systemu alarmowego w momencie wykrycia zalania czujka zainicjuje proces powiadomiania użytkownika.

W przypadku systemu zintegrowanego, oprócz inicjacji procesu powiadomiania użytkownika, dodatkowo zostanie zamknięty zawór wodny sterowany w obwodzie zarządzania hydrauliką obiektu.

5.4. Współpraca czujników temperatury systemu ogrzewania z systemem alarmowym

W przypadku systemu autonomicznego taka funkcja nie będzie realizowana.

W przypadku systemu zintegrowanego wykrycie w pomieszczeniu obszaru o temperaturze zdecydowanie odbiegającej od warunków normalnych wywoła sygnał alarmowy i dodatkowo wyłączy obwody elektryczne w tym pomieszczeniu. Przyczyną takich anormalnych warunków mogą być sytuacje:

- **objaw** – gwałtowny wzrost temperatury w monitorowanym pomieszczeniu – **przyczyna** – w pomieszczeniu może znajdować się silne źródło promieniowania termicznego, np. pożar – **reakcja** – zainicjowanie sygnału powiadamiającego i wyłączenie obwodów elektrycznych w pomieszczeniu;
- **objaw** – temperatura w pomieszczeniu utrzymuje się zarówno powyżej temperatury wody w układzie CO, jak i temperatury otoczenia na zewnątrz budynku – **przyczyna** – w pomieszczeniu może pozostawać włączone źródło ciepła – **reakcja** – w przypadku niewykrycia obecności użytkownika w pomieszczeniu – detektor ruchu – czujka PIR zainicjowanie sygnału powiadamiającego i wyłączenie obwodów elektrycznych w pomieszczeniu).

6. Podsumowanie

Analiza możliwości systemów zbudowanych na bazie elementów EIB i PLC wykazała, że mogą one być użyte do budowy zintegrowanych systemów zarządzających i kontrolujących pracę chronionego obiektu, w skład których będą wchodzić obwody realizujące funkcje stawiane systemom alarmowym (SSWiN i SSP) instalowanym w budynkach mieszkalnych.

Pod względem przejrzystości programu sterującego systemy EIB są bardziej przyjazne dla użytkownika od systemów zbudowanych na bazie sterowników PLC. Jednak pod względem możliwości tworzenia wyrafinowanych funkcji i algorytmów dopasowanych do indywidualnych potrzeb użytkownika systemy oparte na sterownikach PLC dają większe możliwości niż systemy EIB.

Dzięki swojej budowie magistralnej i rozproszeniu elementów systemy EIB charakteryzują się większą odpornością na próby sabotaży niż systemy zbudowane na bazie sterowników PLC.

Sterownik PLC swobodnie może kontrolować wiele podsystemów inteligentnego budynku jednocześnie, pozwalając na pełną integrację funkcji systemu. System zbudowany na bazie sterowników PLC nie ma charakteru skupionego, a dzięki możliwości łączenia w sieć elementów sterujących pracą systemu może być on traktowany jak system rozproszony.

Porównanie cech poszczególnych typów instalacji (autonomicznych i zintegrowanych) przedstawiono w tab. 1.

Jak wynika z tab. 1, jeśli system ma działać w obiektach o niskiej kategorii zagrożenia (Z1 i Z2), proces integracji poszczególnych instalacji jest jak najbardziej słuszny. Zwiększają się dzięki temu poziomy cech, które są istotne dla użytkownika indywidualnego (elastyczność systemu, duży poziom integracji, wymiennosc funkcji, łatwość i intuicyjność obsługi). Cechy te wpływają zasadniczo na wskazanie na system zintegrowany.

Cecha systemu	System autonomicznych instalacji	System zintegrowanych instalacji
Integracja	brak	duża
Elastyczność systemu	niska	duża
Ergonomiczność obsługi systemu	niska	wysoka
Koszt instalacji systemu	duży	średni
Koszt eksploatacji systemu	duży	niski
Możliwość rozbudowy systemu	niewielki	duży
Poziom bezpieczeństwa systemu	duży	średni
Odporność systemu na sabotaż	duża	średnia
Separacja obwodów systemu	duża	mała

Tab. 1. Porównanie cech wybranych typów instalacji elektrycznych

Użytkownik jest w stanie nawet ponieść pewien dyskomfort związany ze zmniejszeniem poziomu bezpieczeństwa systemu i jego odporności na sabotaż. Jednocześnie zdaje sobie sprawę, że środki potrzebne do urzeczywistnienia się zagrożeń w postaci umyślnej ingerencji napastnika w działanie systemu alarmowego w systemie zintegrowanym są dość duże w porównaniu z zabezpieczaniem w obiekcie mieniem.

Mimo dużych możliwości sprzętowych systemów zintegrowanych w przypadku systemów alarmowych stosowanych w obiektach, w których znajduje się mienie o dużej wartości, informacje lub dokumenty o różnej klauzuli tajności, lepiej zastosować dedykowane do ochrony obiektów autonomiczne systemy alarmowe (SSWiN i SSP). Oferują one znacznie większy poziom bezpieczeństwa i odseparowują system alarmowy od instalacji elektrycznej służącej do zasilania zwykłych odbiorników w budynku. W tym przypadku konieczne jest przedłożenie poziomu bezpieczeństwa ponad wygodę użytkownika.

dr inż. Marcin Bucza
Politechnika Lubelska

Katedra Inżynierii Komputerowej i Elektrycznej

Literatura:

1. Antoniewicz B., Koczyk H., Sroczka E., *Nowoczesne wyposażenie techniczne domu jednorodzinnego*, PWRiL, Poznań 1998.
2. Brock S., Muszyński R., Urbański K., Zawirski K. *Sterowniki programowalne*, Wydawnictwo Politechniki Poznańskiej, Poznań 2000.
3. Kasprzyk J. *Programowanie sterowników przemysłowych*, Wydawnictwo Naukowo-Techniczne, Warszawa 2006.
4. Petykiewicz P. *Nowoczesna instalacja elektryczna w inteligentnym budynku*, COSiW SEP, Warszawa 2001.
5. www.eib.pl
6. www.moeller.pl

WEJDŹ NA:

<http://217.28.147.92:8089>

Użytkownik: *demo* Hasło: *demo*

...i zobacz jak działa



DiGiEyes DE-B920N 2.0 Mpx

Digieyes DE-B920N to kamera IP o rozdzielczości 2 Megapixeli zaprojektowana z myślą o telewizji przemysłowej. Połączenie technologii CMOS opartej na przetworniku Micron z bardzo wydajnym procesorem obrazu HiSilicon tworzy doskonale urządzenie do obsługi multimediiów. Wbudowany system operacyjny **Embedded Linux** czyni ją urządzeniem sieciowym w najlepszym wydaniu. Zaawansowana technologia megapixelowa umożliwia wykonywanie wysokiej jakości zdjęć ze zdarzeń alarmowych oraz zapisywanie ich bezpośrednio na karcie SD. Doskonałą jakość obrazu zapewnia kodowanie w rozdzielczości 1600 x 1200 pixeli w czasie rzeczywistym za pośrednictwem algorytmu kompresji H.264. Technologia Plug'n'Play umożliwia prostą i szybką integrację w systemach nadzoru. Dzięki możliwości pełnego zarządzania urządzeniem z poziomu przeglądarki internetowej nie jest wymagana instalacja specjalistycznego oprogramowania. Kamera doskonale sprawdzi się w instalacjach telewizji przemysłowej gdzie potrzebny jest bardzo wysokiej jakości obraz przy niewielkim obciążeniu sieci.

PEŁNĄ OFERTĘ ZNAJDZIESZ NA STRONIE
www.infocam.com.pl

info
CAM

INFO-CAM

09-402 PŁOCK

Al. Kilińskiego 5

tel. (024) 266 97 12

tel./fax (024) 266 97 13

e-mail: handlowy@infocam.com.pl

Nie tylko komunikacja



Ponad 130 lat temu Alexander Graham Bell dokonał rewolucji w dziedzinie komunikacji międzyludzkiej. Od tamtej pory człowiek uzależnił się od uzyskiwania drogą telefoniczną informacji, a także przeprowadzania konsultacji, pogaduszek czy wzywania pomocy. Jednak komunikacja głosowa to nie tylko telefon. Rozwój elektroniki i techniki cyfrowej otworzył nowe możliwości komunikacji. Dotychczas standardowa telefonnia wykorzystywała przy transmisji mowy ludzkiej pasmo 3,4 kHz, natomiast specjalistyczne rozwiązania interkomowe Commend stosowały 7 kHz. Obecnie zmodyfikowane kodeki VoIP pozwalają na szersze wykorzystanie pasma. System komunikacji i zarządzania firmy Commend nie pozostaje w tyle i aktualnie przoduje w systemach łączności interkomowej, stosując pasmo 16 kHz. Firma C&C Partners przedstawi, jak różne wymagania oraz sektory potrafi zaspokoić jeden dostawca.

O tym, jak bogatą i skomplikowaną platformą jest system Commend, firma C&C Partners pisała już kilkakrotnie (w magazynach branży zabezpieczeń oraz w innych czasopismach fachowych, docierających do specjalistów z konkretnej branży). Kilkakrotnie prezentowała swoje systemy na targach (także międzynarodowych). W niniejszym artykule przedstawione zostaną wybrane realizacje, aby uzmysłowić czytelnikom/inwestorom, że interkom w systemie Commend to nie tylko darmowy przekaz głosu.

Jednym z ważniejszych sektorów, w którym produkty firmy Commend znajdują zastosowanie, jest medycyna, a ściślej obiekty służby zdrowia. W szpitalach, domach opieki oraz ośrodkach zdrowia jest stosowana komunikacja głosowa, która obejmuje pielęgniarkę dyżurną i lekarza dyżurnego oraz sale operacyjne/zabiegowe, recepcje/rejestracje. Interkom znajduje zastosowanie także w innych pomieszczeniach szpitalnych, np. w kuchni, pokoju personelu, pokoju socjalnym, w windach, szatniach, na portierni czy nawet w poczekalniach. Nie bez znaczenia jest umożliwienie komunikacji między personelem w części biurowej, dzięki czemu sekretarka, kierownik, oddziałowa i ordynator mogą być w stałym kontakcie. Łączność ta może mieć charakter konferencji, może odbywać się w trybie Simplex lub Open-duplex. W szpitalach ważna

jest także możliwość wykonywania służ, czyli kontroli dostępu z możliwością zdalnego otwierania drzwi z poziomu klawiatury interkomu, a także integracja słuchawki interkomu z telefonią, telewizją dozorową, możliwość nadawania komunikatów do wszystkich/wybranych grup użytkowników czy przełączania się między trybem głośnomówiącym a mikrotelefonicznym. Uzupełnieniem takiego pakietu możliwości jest wizualizacja z funkcjami raportowania. W polskich szpitalach rozwiązania Commend znajdują się w Świnoujściu, Radomiu, Gdańsku, Lesznie, Warszawie i Białymstoku.

Jedną z ciekawszych realizacji jest wyposażenie w system Commend Międzynarodowego Portu Lotniczego w Pyrzowicach. Na terenie tego lotniska znajdują się panele komunikacji SOS (ratowniczej) wykorzystujące interkomu Commend. W sytuacjach alarmowych lub informacyjnych można nawiązać połączenie ze służbami ochrony portu w trybie głośnomówiącym. Wyjście audio z interkomu zostało również sprzęgnięte z pętlą indukcyjną, dając w ten sposób większy komfort odsłuchiwania dla osób z dysfunkcjami słuchu, wyposażonymi w aparaty słuchowe z cewką typu T. W toaletach dla niepełnosprawnych zainstalowane zostały ciągnia, które aktywują alarm, wysyłają komunikat na panel LCD interkomu, uruchamiają sygnalizator optyczny i przekazują informację o miejscu

zdarzenia na wizualizacji. Ze względów bezpieczeństwa wszelkie połączenia głosowe rejestrowane są na serwerze. Wszystko to zbudowane jest na jednej platformie. Innego typu instalacje znajdują się także na lotnisku Ławica w Poznaniu oraz Okęcie w Warszawie.

Innym typem obiektów, w których doskonale sprawdza się Commend, są teatry. W tego typu placówkach ważna jest jakość przekazu oraz niezawodność systemu inspicjenckiego. Nie jest możliwe, aby spektakl został zrealizowany bez ciągłej łączności między inspicjentem, reżyserem, oświetleniowcem czy akustykiem. Commend pozwala dodatkowo na komunikację z garderobami czy integrację z telefonią DECT. Tego typu systemy działają w Warszawie, Łodzi, Szczecinie.

Nietypowym sposobem wykorzystania komunikacji IoIP (ang. *Intercom over IP*) systemu Commend jest realizacja nowego projektu przy współpracy z firmą Thales w Poznaniu. Na terenie stolicy Wielkopolski przy przejazdach kolejowych rozmieszczonych na przestrzeni kilku kilometrów wykorzystano możliwość przesyłu głosu po sieci IP. Na słupach przy przejazdach kolejowych zamontowane zostały kamery, promienniki podczerwieni oraz tuby głośnikowe. Tuby te mają bezpośrednie powiązanie z modułami interkomowymi. W mieście czterech dróżnic wyposażeni są w słuchawki interkomowe pozwalające na nadawanie komunikatów dla wybranych przejazdów, na ostrzeganie oraz informowanie użytkowników dróg i przejeżdżających. System pozwala na pokonywanie hałasu miejskiego przy bardzo dobrej zrozumiałości mowy. Dodatkowo, za pośrednictwem wbudowanych przełączników systemu Commend, pozwala on na załączenie (po wprowadzeniu kodu) promienników podczerwieni (skonfigurowane zostały także wejścia bezpieczeństwa pozwalające na wprowadzenie na przykład sygnału z kontaktronu). Każdy dróżnik ma swój obszar za który odpowiada i nie może nadawać komunikatów na przejazdy, których nie nadzoruje. Dodatkowo pracownicy kolei mają możliwość wzajemnego komunikowania się za pomocą doskonałej jakości sprzętu, wypierającego pocziwe radiotelefony simpleksowe. Interkom (w wydaniu wandaloodpornym) pojawił się również na terenie miasta przy jednym z przejazdów ograniczających wjazd na teren prywatny. I znów jedna platforma spełniła różnicowane oczekiwania (inwestora, integratora, użytkownika oraz prywatnego przedsiębiorcy).

Commend nieprzypadkowo trafił również do przemysłu. Dostarczane są tam sprawdzone rozwiązania pozwalające na pracę w dużym hałasie (bliskim 100 dB). Obudowa o podwyższonej klasie szczelności odporna jest na pył i wilgoć, a tworzywo sztuczne wzmacniane włóknem szklanym sprawdza się także w zakładach azotowych. Interkomy mogą być obsługiwane w rękawicach ochronnych, mogą pracować w trybie simpleks, uruchamiać automatycznie sygnalizator optyczny, mają także programowalne przyciski z podświetleniem LED. Poza tym pozwalają na integrację z innymi systemami. Omawiane tu produkty pracują w Kędzierzynie-Koźlu, Wrocławiu, Olsztynie czy Wykrotach.

Wyjątkowym obszarem zastosowań kompleksowych rozwiązań firmy Commend jest sektor penitencjarny. W zakładach karnych i aresztach potrzebny jest system gwarantujący niezawodność, a zarazem bezpieczny, stabilny, funkcjonalny i intuicyjny. Stosowanie kontroli dostępu i funkcji służ, a także monitoring ciągłości linii, wizualizacja, rozwiązania wandaloodporne, integracja z CCTV, sterowanie oświetleniem – to tylko fragment wykorzystania możliwości tego systemu. Zintegrowany system komunikacji i zarządzania jest wykorzystywany przez skazanych podczas używania radiowęzła. Stosowany jest także do wzywania strażnika oraz pozwala na swobodne i szybkie komunikowanie się pracowników tych fortec.

Austriacka firma Commend wypromowała zintegrowany system komunikacji i zarządzania, stanowiący nieodłączną część budynków inteligentnych. Rozwiązania systemu Commend stanowią platformę integrującą łączność głosową, systemy alarmowe, CCTV, kontrolę dostępu, sterowanie bramami, telefonię, wizualizację itp. Co więcej, Commend nie pozostał obojętny wobec rozwoju technologii IP. Dziś dzięki wykorzystaniu proponowanych rozwiązań możliwa staje się nie tylko komunikacja z ludźmi z całego świata, ale także sterowanie urządzeniami w świecie TCP/IP. Wśród tych, którzy nam zaufali, są zarówno międzynarodowe zakłady produkcyjne, międzynarodowe grupy integratorów systemów automatyki, duże i małe biura projektowe, jak i mali oraz więksi inwestorzy... Sprawdź sam, co przekonało ich do naszego rozwiązania.

Marek Katarzyński
C&C Partners



Nowy europejski standard

dla zasysających systemów wczesnej detekcji dymu



Norma EN-54 jest europejskim standardem określającym jakość produkowanych części składowych systemów sygnalizacji pożarowej. Każdy z obszarów przedstawiony jest w oddzielnym zeszycie.

Co to jest standard produktu?

Standard produktu określa powtarzalność i wytrzymałość produktu, jednakże nie definiuje jego wszystkich możliwości i szczególnych cech funkcjonalnych.

EN-54-20 zasysające systemy detekcji dymu (ASD)

EN-54 część 20 jest europejskim standardem dla zasysających systemów detekcji dymu, określanymi skrótem branżowym ASD (ang. *Aspirating Smoke Detection*), zawierającym nową klasyfikację systemów zasysających (Tab. 1.). Taka klasyfikacja pozwala projektantom i instalatorom na wybranie odpowiedniego systemu dla wymaganej czułości ASD chronionego obszaru.

EN-54-20 jest w pełni uprawomocnionym standardem dla wytycznych konstrukcyjnych. Z początkiem lipca 2009 r. wszystkie produkty wchodzące w skład zasysającego systemu detekcji dymu, oferowanego na terenie Unii Europejskiej, będą musiały być przebadane na zgodność z normą EN-54-20 i muszą odpowiadać jej standardom, aby mogły uzyskać niezbędny znak CE. W Europie jest tylko osiem notyfikowanych laboratoriów badawczych.

Z dniem pierwszego lipca standard 2009 EN-54-20 będzie jedynym obowiązującym dokumentem normatywnym dla systemów zasysających.

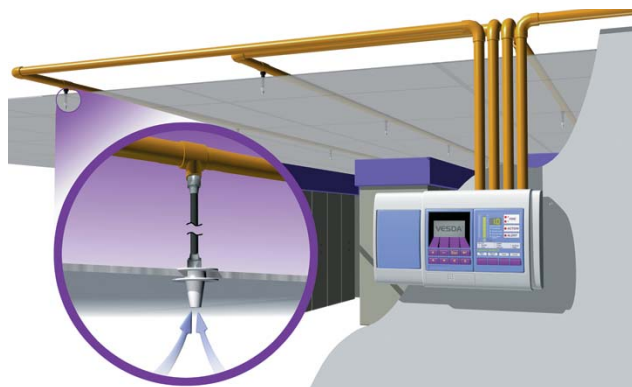
Co nowego?

Norma jest nową klasyfikacją systemów zasysających. Nie jest jednak rodzajem wytycznych projektowych. Określa ona precyzyjnie, jakie parametry minimalne musi spełniać system i co w ramach oferowanych produktów powinien zapewniać

producent. Zauważyć można korzyści bezpośrednio przekładające się na komfort i poziom pracy projektantów. Zgodnie z wytycznymi normy producenci urządzeń są zobowiązani do uzupełnienia dokumentacji wyrobów o informacje, jakiej klasie odpowiada dane urządzenie i przy ilu otworach ssących ta klasa została uzyskana. Producent powinien zapewnić niezbędne narzędzia (oprogramowanie modelowe), służące do symulacji zaprojektowanej instalacji. Narzędzia takie muszą posiadać zaimplementowany moduł obliczający system zgodnie z wymaganiami normy EN-54-20.

Klasa i czułość	Przykłady zastosowania
Klasa A	Bardzo wysoka czułość systemu, która zapewnia najwyższy poziom wczesnej detekcji dymu. Klasa A ma zastosowanie, kiedy ciągłość pracy jest bardzo ważna: Serwerownie, Data Center, Telekomunikacja.
Bardzo wysoka czułość systemu	
Klasa B	Podwyższona czułość systemu dla efektywnej detekcji w wymagającym środowisku oraz tam, gdzie znajduje się ważny i cenny sprzęt.
Podwyższona czułość systemu	
Klasa C	System zapewniający standardową detekcję dymu, która wymagana jest dla większości obszarów i pomieszczeń, nieposiadających niedostępnych przestrzeni.
Normalna czułość systemu. Poziom detekcji w zakresie czujek punktowych	

Tab. 1. Klasy Standardu Normy EN 54-20



Rys. 1. System VESDA

Korzyści wypływające z wprowadzenia normy

Norma adresowana jest do producentów, ale korzyści z jej wprowadzenia czerpią też projektanci i inwestorzy. Taki stan rzeczy wpływa niezwykle pozytywnie na rynek systemów zasysających, bo daje to możliwość ich wiarygodnego porównania. Producenci zgodnie z wytycznymi normy zobligowani są do podawania technicznych parametrów granicznych dla produkowanych wyrobów. Zapis ten wyraźnie wpływa na urealnienie podawanych informacji, które niejednokrotnie były fikcją marketingową. Niepełne czy niewiarygodne informacje mogą być przyczyną niewłaściwego zaprojektowania instalacji bazującej na urządzeniach, które nie spełniają wymaganych parametrów, takich jak chociażby maksymalna liczba otworów, czas transportu zgodnie z wymaganą klasą czy też czułość systemu.

Nieprawidłowości mogące wynikać z niekompletnych informacji bezpośrednio rzutują na kompetencje projektanta i mogą zwiększyć koszty inwestycyjne.

Projektant w łatwy sposób zweryfikuje, czy dane urządzenia mają znak CE, i z wybranych systemów dobierze ten najbardziej optymalny dla chronionego obszaru. Wymagane wsparcie techniczne jest tego gwarantem. Elementem niezwykle istotnym w procesie projektowania są odpowiednie narzędzia, które pozwalają na obliczenie instalacji i określenie kluczowych parametrów.

Inwestorzy mają wówczas pewność, że zastosowane urządzenia będą działały i chroniły ich mienie z najwyższą skutecznością, wpływając tym samym na podwyższenie współczynnika sprawności ciągłości pracy, np. serwera. Dodatkowym argumentem jest możliwość negocjowania stawek ubezpieczeniowych oraz odpowiednie ich obniżanie.

Czego nabywca powinien oczekiwać od systemu zasysającego wczesnej detekcji dymu?

Zgodnie z wymaganiami normy każdy z producentów powinien zapewniać prawidłową pracę oferowanych urządzeń oraz wachlarz dodatkowych korzyści dla nabywcy. Niezbędne cechy tego systemu to:

- przydatność do wymaganej klasy oraz pokrywanej powierzchni,
- posiadanie dodatkowych cech podnoszących jego funkcjonalność,
- możliwość modelowego projektowania instalacji ssącej,
- niskie koszty ruchowe systemu, związane z materiałami eksploatacyjnymi i wymaganiami serwisowymi,
- stabilna kalibracja detektora.

Zastosowanie urządzeń

Obecnie na polskim rynku dostępne są jedynie urządzenia systemu VESDA, które mają certyfikaty CE na zgodność z normą EN-54-20. Produkowane są one przez firmę Xtralis, która jest wiodącą wśród firm produkujących systemy zasysające detekcji dymu. Firma Xtralis uzyskała dla swoich produktów prestiżowy certyfikat CPD – EC Certificate of Conformity, zgodny z normą EN-54-20.

W swojej ofercie posiada całą gamę urządzeń VESDA, na którą składają się detektory z rodziny LaserPLUS, LaserSCANNER, LaserCOMPACT (razem z wersjami przystosowanymi do pracy w sieci MX/ZX, EB&AP), LaserFOCUS oraz urządzenia serii ICAM.

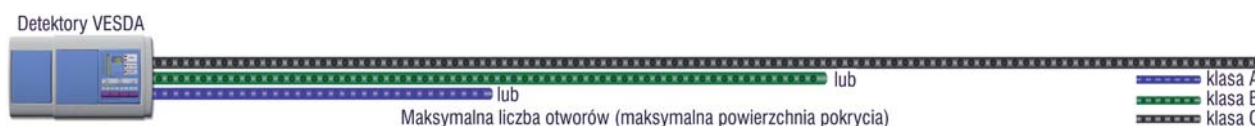
Co to jest system wczesnej detekcji dymu VESDA?

System Bardzo Wczesnej Detekcji Dymu VESDA jest to system zasysający powietrze poprzez otwory ssące w sieci głównych rur oraz kapilar. Tłoczy je do detektora w celu analizy dymu zawartego w badanym powietrzu.

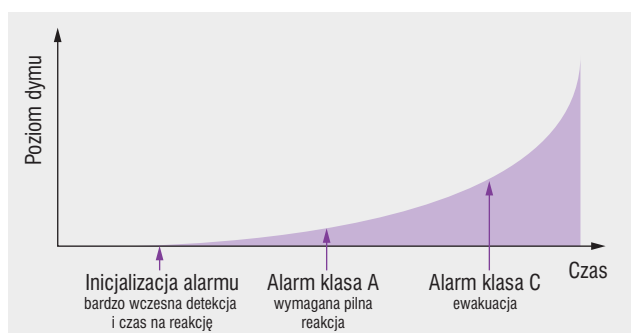
VESDA jest najlepszym produktem nie tylko w swojej klasie, ale we wszystkich klasach. System VESDA zapewnia maksymalną czułość we wszystkich klasach standardu (dla różnych powierzchni i obszarów). Przewyższa inne systemy pod względem dodatkowych cech użytkowych oraz wyjątkowej funkcjonalności, co oznacza, że detektory VESDA są przydatne w najróżniejszych zastosowaniach.

Zastosowanie jednego detektora VESDA do ochrony w wielu klasach

Konfiguracja detektora umożliwia użycie jednego detektora do ochrony w wielu klasach (Rys. 3.). Alarm wstępny (ustawiony na poziomie bardzo wczesnej detekcji dymu) umożliwia szybką reakcję na poziomie dymu niewidocznego, co daje tym samym czas na reakcję obsługi. Kolejny próg alarmowy (w klasie A) wywołuje pilną reakcję obsługi na zaistniałe zagrożenie, zaś próg trzeci (w klasie C) może być sygnałem uruchamiającym procesy automatycznie, takie jak zamknięcie klap ppoż. Kolejne fazy rozwoju zagrożenia można obserwować na wyświetlaczu systemowym lub na ekranie komputera pod kontrolą programu wizualizacyjnego VSM4.



Rys. 2. Detektor powinien spełniać wymogi żądanej czułości i pokrywać duży obszar



Rys. 3. Użycie jednego detektora VESDA do ochrony w wielu klasach

VESDA najczęściej używanym ASD

Jest kilka powodów, dla których VESDA jest najczęściej używanym ASD

- szeroki asortyment produktów, spośród których można wybrać najbardziej odpowiedni produkt dla danego zastosowania,
- szeroki zakres dynamicznej czułości (od 0,005 do 32 %/m).
- filtrowanie powietrza dla ochrony optyki, która utrzymuje sprawność głowicy detekcyjnej,
- stała kalibracja zapewniająca stabilną pracę detektora przez szereg lat,
- stały monitoring powietrza (wykrywanie zmian natężenia przepływu powietrza spowodowanego przerwaniem lub zatkanie rurociągu, a także otworów ssących oraz alarmowanie o tym, utrzymanie stabilności pracy w czystych oraz brudnych środowiskach, obecność czujników monitorujących przepływ powietrza w każdym rurociągu),

- bezkonkurencyjnie pojemna pamięć historii zdarzeń, która jest wykorzystywana przy serwisowaniu i analizie zdarzeń,
- sieć komunikacyjna (VESDAnet) dla obsługi całej gamy urządzeń oraz centralnego systemu monitorowania i diagnostyki,
- profesjonalne wsparcie techniczne i handlowe lokalnych dystrybutorów,
- przejrzyste arkusze danych, aby można było łatwo określić przydatność naszych detektorów według klasyfikacji normy EN-54-20, np. klasa A (30 otworów), klasa B (60 otworów) i klasa C (100 otworów),
- narzędzie modelowego projektowania instalacji ssącej (ASPIRE2) dla wspomagania projektantów.

Na naszych stronach internetowych będziemy przekazywać Państwu praktyczne wskazówki, dotyczące używania tego standardu. Będą to:

- przykłady (np. jak wyrazić wymagania wobec systemu, używając terminologii normy EN 54-20),
- porady (np. jakiej klasy użyć dla zabezpieczenia różnych obszarów),
- rekomendacje (np. jak stosować się do EN-54-20, żeby spełnić wymagania dla wykonania systemu bardzo wczesnej detekcji dymu),
- analizy określonych przypadków instalacji, zamontowania i testowania zgodnych z EN-54-20.

Mariusz Konik

Vision Polska

Polski Kanał Dystrybucyjny Urządzeń VESDA

www.visionpolska.pl



ALARM

4-5.11.2009, Kielce

oraz

X OGÓLNOPOLSKA KONFERENCJA

Bezpieczne Miasto

- Monitoring Wizyjny Miast

Patronat prasowy: **ZABEZPIECZENIA**

Patronat internetowy: **alarmy.com.pl**
GRUPA MARKETEO.COM

NAJWIĘKSZY SERWIS BRANŻY SECURITY
ZABEZPIECZENIA



www.alarm.targikielce.pl

X Konferencja i Wystawa Monitoringu Wizyjnego

Targi Kielce Sp z o.o., ul. Zakładowa 1, 25-672 Kielce,
Szczegółowe informacje: Dyrektor Projektu - Grzegorz Figarski,
tel. 041 365 12 33, fax 041 345 62 61, e-mail: figarski.g@targikielce.pl



SYGNAŁ
BEZPIECZEŃSTWA

Kamery **G1** na trudne warunki

nowa generacja
kamer dzień/noc
marki NOVUS

Wprowadzenie przez producentów kamer kolejnych serii czy generacji urządzeń z reguły wiąże się z nowymi rozwiązaniami technologicznymi wprowadzonymi przez producentów kluczowych podzespołów w kamerze. Dotyczy to przede wszystkim elementów światłoczułych – matryc CCD oraz układów cyfrowej obróbki sygnału DSP. Liczącym się producentów powyższych podzespołów jest zaledwie kilku i to oni są twórcami kolejnych przełomów w dziedzinie kamer. Implementacja tych rozwiązań przez producentów kamer ma już charakter wtórny. W niniejszym artykule chciałbym omówić nową generację kamer serii G1 marki NOVUS, tzn. ich nowe funkcje, a także zalety zastosowanych podzespołów

W ramach serii G1 możemy wyróżnić kamery klasyczne dzień/noc w różnych wersjach zasilania, kamery kopułkowe dzień/noc oraz wandaloodporne kamery kopułkowe dzień/noc (również w wersji z wbudowaną grzałką oraz promiennikiem podczerwieni).

Dla wszystkich kamer serii wykorzystano przetwornik CCD SONY Super HAD drugiej generacji o nazwie ICX639AKA(PAL)/ICX638AKA(NTSC). W porównaniu do

Wartości czułości są trudne do zweryfikowania przez użytkownika/installatora i bardzo często podawane na wyrost. Dlatego najlepszym sposobem ich sprawdzenia jest porównanie znanych nam już modeli kamer w tych samych warunkach oświetlenia. Do przeprowadzenia testu wybraliśmy kamery klasyczne dzień/noc NVC-660DN, NVC-HDN540 oraz NVC-GDN5212C-3 z serii G1. Wszystkie kamery zostały umieszczone w zamkniętej skrzyni ze sterowanym z zewnątrz



Fot. 1. Typy kamer serii G1: kamera kopułkowa dzień/noc, wandaloodporna kamera kopułkowa dzień/noc, kamera klasyczna

poprzedniej wersji przetwornika znacznie poprawiono jego czułość, która jest jednym z najważniejszych parametrów kamer wykorzystywanych w systemach monitoringu. Zwiększenie czułości zostało zrealizowane przy tym samym poziomie szumów (stosunku SNR) oraz nasycenia kolorów. W stosunku do poprzednich modeli przetwornika poprawa czułości jest znaczna i wynosi 7dB. W liczbach bezwzględnych przekłada się to na następującą czułość w kamerach: 0.05 lx/F=1.2 w trybie kolorowym (1/50 s) oraz 0.005 lx/F=1.2 w trybie czarno-białym (1/50 s). Wszystkie modele kamer posiadają dodatkowo funkcję DSS, czyli w warunkach słabego oświetlenia możliwość integracji klatek do 5.12 s i w tych warunkach czułość kamery wynosi nawet 0.00004 lx/F=1.2.

Na poprawę czułości przetwornika (w porównaniu do poprzedniej) wpływają dwa elementy:

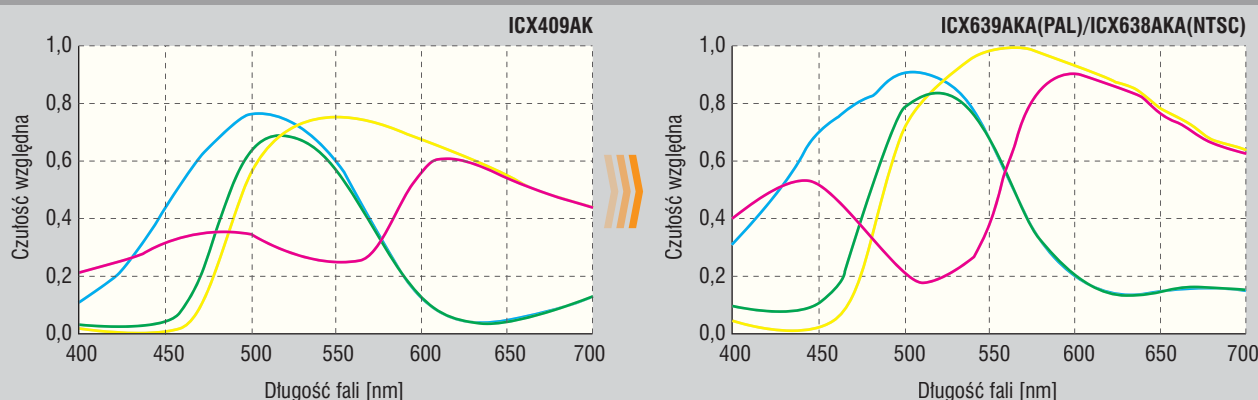
- 1) Zastosowanie komplementarnych barwników w filtrach, co pozwoliło zwiększyć czułość dla krótszych fal (kolor niebieski), natomiast optymalne zbalansowanie czułości spektralnej (nakładanie się wykresów) spowodowało redukcję szumów „kolorów”.
- 2) Wyższa liczba aperturowa mikrosoczewek w górnej strukturze przetwornika, która zapewnia lepsze ogniskowanie promieni światła na fotodiodach, tzn. znaczne zredukowanie obszaru „nieświatłoczułego” pomiędzy poszczególnymi komórkami, co obrazuje rys. 3.

źródłem światła białego. Powyższe źródło światła jest regulowane i w trakcie trwania testu poziom oświetlenia jest płynnie zmniejszany. Dla łatwiejszej oceny czułości obrazów kamery obserwują planszę testową z płynnie poruszającą się wskazówką sekundową. W celu uzyskania łatwych do porównania wyników we wszystkich kamerach wyłączono funkcję DSS, natomiast wartość funkcji AGC ustawiono na minimum. Powyższy test został zrealizowany dla światła widzialnego.

Plik z nagraniem z testu w formacie minibank jest plikiem wykonywalnym z rozszerzeniem .exe. Pozwala na równoczesne odtwarzanie obrazów z wielu kanałów, co jest bardzo wygodne przy dokonywaniu porównań kilku sygnałów wizji. Ponadto plik posiada „wbudowany” odtwarzacz i może być uruchamiany na dowolnym komputerze bez konieczności instalacji dodatkowych kodeków czy programów.

Wszystkie kamery serii G1 charakteryzuje wysoka rozdzielczość: 580 TVL w trybie kolorowym oraz 700 TVL w trybie czarno-białym. Jest ona konsekwencją zarówno dużej liczby efektywnych pikseli w przetworniku CCD (440 k), jak i zastosowania wysokiej klasy procesora DSP.

W dzisiejszych systemach CCTV administratorzy często wymagają funkcji rozpoznawania tablic rejestracyjnych. Jednym z wielu problemów wymagających rozwiązania jest kwestia kompensacji silnego oświetlenia reflektorów samochodowych.



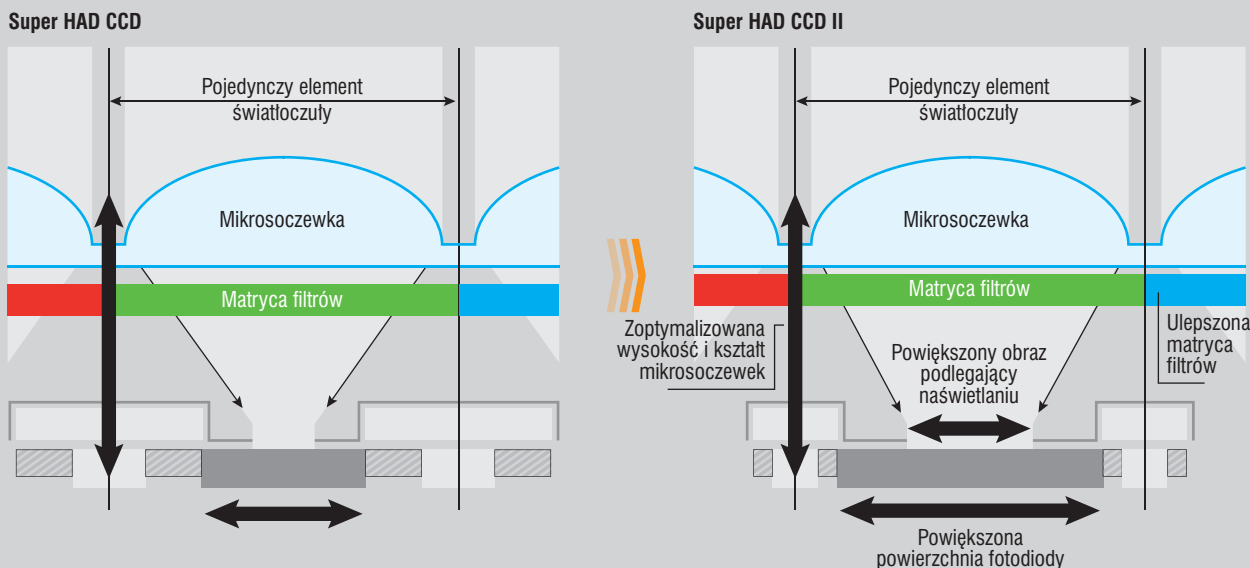
Rys. 2. Porównanie czułości względnej przetworników CCD: poprzedniej generacji ICX409AK (wykres po lewej) oraz ICX639AKA(PAL)/ICX638AKA(NTSC) (wykres po prawej)

Zaimplementowana funkcja HLC (ang. *High Light Compensation*) zapewnia wysoką dynamikę obrazu, znacznie zwiększającą prawdopodobieństwo rozpoznania tablic rejestracyjnych w porównaniu do tradycyjnych kamer z funkcją WDR. Użyteczność powyższej funkcji w takich zastosowaniach doskonale widać na fot. 2.

Włączenie funkcji cyfrowej stabilizacji obrazu (DIS) powoduje uruchomienie zoomu cyfrowego o niewielkiej krotności,

sceny, gwarantując generację klarownego obrazu nawet przy braku jakichkolwiek dodatkowych źródeł światła.

Wszelkie ustawienia kamer mogą być realizowane za pomocą przycisków umieszczonych na tylnych panelach modułów kamerowych w przypadku modeli kompaktowych oraz wewnątrz obudów w przypadku modeli kopułkowych. Ponadto wybrane modele mogą być sterowane za pomocą protokołu Pelco-D poprzez wbudowany port RS485. W ni-



Rys. 3. Porównanie obszaru światłoczułego technologii Super HAD oraz Super HAD II (ICX639AKA(PAL)/ICX638AKA(NTSC))

co użytkownik może zaobserwować jako zmniejszenie rozmiaru wyświetlanego obrazu. Drgania modułu kamerowego są kompensowane przez obróbkę cyfrową w pewnych zakresach ich częstotliwości i amplitudy, poprawiając komfort obserwacji sceny przez operatora. Wszystkie typy kamer posiadają również możliwość określania stref prywatności (do ośmiu) i odpowiedniego ich definiowania w zakresie położenia, wielkości oraz koloru maskowania. Wbudowana detekcja ruchu w kamerze może aktywować wyjście napięciowe i tym samym np. włączyć dodatkowe oświetlenie lub zwiększyć prędkość nagrywania zdarzenia przez rejestrator.

Kamery kopułkowe wandaloodporne mają stopień ochrony IP66 (ochrona przed wnikaniem drobin pyłu oraz wody). Dodatkowo zastosowanie grzałki w niektórych modelach pozwala na bezpieczne ich użytkowanie na zewnątrz przez cały rok. Modele wandaloodporne z wbudowanymi diodowymi promiennikami podczerwieni (36 sztuk) zapewniają efektywny zasięg nawet do 35 metrów oraz równomierne oświetlenie

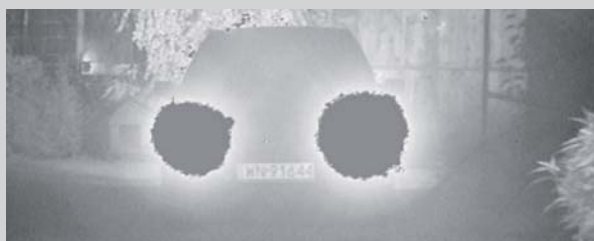
niejszym opracowaniu autor skupił się na najbardziej nowatorskich i przydatnych funkcjach kamer serii G1 z punktu widzenia użytkownika systemu nadzoru wizyjnego, gdyż ramy tego artykułu nie pozwalają na omówienie wszystkich zaimplementowanych funkcji. W celu zapoznania się ze wszystkimi możliwościami kamer autor zachęca do przejrzania zarejestrowanego materiału z omówionego w artykule testu, dostępnego na stronie internetowej Novus Security (http://www.novuscctv.pl/webfm_send/1828) oraz samodzielnego przetestowania kamer i porównania z dotychczas stosowanymi modelami.

Patryk Gańko
NOVUS Security

W artykule wykorzystano informacje zawarte w materiałach promocyjnych producenta podzespołów opisywanego urządzenia, a także wyniki własnych badań i materiały marketingowe.



Wyłączona funkcja HLC



Włączona funkcja HLC

Fot. 2. Działanie funkcji HLC

noVus®

Profesjonalne rozwiązanie dla systemów zabezpieczeń



NOWE kamery dzień/noc serii G1

kamery kompaktowe, kopułkowe i wandaloodporne

- czułość: od 0.00004 lx/F=1.2 (DSS)
- wysoka rozdzielczość: do 700 TVL
- matryca CCD, 1/3" SONY Super HAD II
- mechaniczny filtr podczerwieni
- HLC - funkcja redukująca efekt oślepiania kamery
- 8 stref prywatności
- detekcja ruchu
- oświetlacz podczerwieni: 36 diod LED, zasięg do 35 m (NVC-GDN4212V/IR-2 i HIR-2)
- obudowa o szczelności IP 66 (kamery wandaloodporne)
- protokół sterowania: PELCO-D (NVC-GDN5212C i 4212V)



Wyłączny dystrybutor produktów NOVUS® w Polsce:



AAT Holding sp. z o.o.

ul. Puławska 431, 02-801 Warszawa, tel. 022 546 05 46, faks 022 546 05 01

e-mail: aat.warszawa@aat.pl, www.aat.pl

Łączy radiowe

jako alternatywa

dla połączeń kablowych

W sieciowych systemach telewizji dozorowej obsługujących rozległe otwarte tereny często zachodzi potrzeba transmisji danych cyfrowych na odległości mieszczące się w zakresie od kilkuset metrów do kilkunastu kilometrów. W obiektach, które dopiero powstają, można przewidzieć ułożenie odpowiedniego okablowania sieciowego, co jednak zrobić, gdy dany obiekt już istnieje i nie ma możliwości ingerencji w jego strukturę? Jednym z dostępnych rozwiązań w takim przypadku jest budowa sieci bezprzewodowej.

Jak łatwo zauważyć, we współczesnych systemach teleinformatycznych popularność sieci bezprzewodowych stale rośnie. Jest to związane z niskim kosztem implementacji tego typu systemów, brakiem zależności od infrastruktury kablowej etc. Co prawda sieci bezprzewodowe nie są wolne od wad i ograniczeń, zaś w niechronionych zakresach częstotliwości panuje spory tłok, jednakże w przypadku starannego zaprojektowania instalacji i zastosowania sprzętu odpowiedniej klasy możliwe jest osiągnięcie wysokiego poziomu niezawodności całego systemu.

Dlaczego MikroTik?

Spośród ogromnej gamy urządzeń bezprzewodowych, jaką oferuje nam współczesny rynek, wybierzmy ciekawy, relatywnie mało znany produkt, występujący pod nazwą MikroTik.

Jak podaje Wikipedia, firma SIA Mikrotiks, potocznie zwana MikroTik, jest łotewskim producentem sprzętu komputerowego przeznaczonego do zastosowań sieciowych i bezprzewodowych. Firma MikroTik dostarcza zarówno oprogramowanie sieciowe i urządzenia do łączności radiowej w standardzie 802.11a/b/g, jak i płyty główne ruterów, anteny, kable antenowe, obudowy oraz inne elementy wyposażenia.

W Polsce firma MikroTik ma wielu dystrybutorów, informacje na temat jej produktów są łatwo dostępne w internecie, dlatego w poniższym opisie nie zostaną przytoczone żadne konkretne parametry ani szczegółowe dane techniczne.

Czynnikiem zachęcającym do stosowania urządzeń firmy MikroTik jest ich wysoka jakość oraz relatywnie niska cena. Przeliczony na pojedynczą kamerę koszt systemu transmisji bezprzewodowej nie przekracza 1000 zł, co w przypadku instalacji bardzo rozległych jest szczególnie opłacalne. Tyle tytułem wstępu, a teraz spróbujmy się skupić na wycinku oferty firmy MikroTik, który jest bezpośrednio związany z systemami CCTV.

Przykładowy system CCTV z transmisją bezprzewodową

Wyobraźmy sobie hipotetyczny rozległy obiekt, w którym rozmieszczone są kamery systemu CCTV. Obiektem takim może być parking, hurtownia surowców sypkich, teren rekreacyjny, plac budowy, a nawet obszar osiedla mieszkaniowego czy niewielkiego miasta. O ułożeniu jakichkolwiek kabli transmisyjnych nie może być mowy, dodatkowym utrudnieniem jest konieczność zorganizowania kilku punktów dozorowych, gdyż obiekt ma więcej niż jedno wejście. Jedyne, czym dysponujemy, to instalacja energetyczna, dostarczająca zasilanie do punktów kamerowych.

Przyjmując tego typu założenia, projektowanie systemu rozpoczynamy od rozmieszczania wszystkich kamer. Podstawowym kryterium powinny być względy użytkowe związane z wymaganym polem obserwacji oraz względy praktyczne związane z dostępnością zasilania oraz możliwością montażu urządzeń. Podczas doboru lokalizacji punktów kamerowych należy liczyć się z koniecznością instalacji anten radiowych w sposób zapewniający ich wzajemną widzialność optyczną oraz brakiem przeszkód materialnych w tak zwanej pierwszej strefie Fresnela.

Ograniczenia wynikające z zastosowania transmisji bezprzewodowej

Ze względu na to, że zagadnienia dotyczące propagacji fal radiowych oraz wyjaśnienia, czym jest wspomniana strefa Fresnela, są szeroko dostępne w internecie, w tym artykule ograniczymy się jedynie do przekazania najistotniejszych informacji. Zainteresowanych szczegółami odsyłamy do stron tematycznych.

Mówiąc w uproszczeniu, strefa Fresnela ma kształt wydłużonej elipsoidy obrotowej, łączącej dwie anteny toru radiowego i stanowi obszar odpowiedzialny za przepływ fal radiowych. Jej średnica jest największa w połowie dystansu między antenami i właśnie tam nie powinny występować istotne przeszkody materialne. Innymi słowy, nie wystarczy, by anteny widziały się wzajemnie przez przysłowiową dziurkę od klucza – do poprawnej pracy łącza radiowego niezbędne jest zachowanie wolnej przestrzeni na całej trasie pomiędzy antenami.

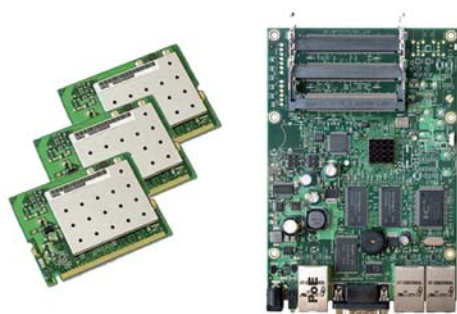
Czynnikiem znacznie pogarszającym niezawodność radiowego systemu transmisji danych jest wszechobecny w całym współczesnym eterze tłok, szczególnie nasilający się w zakresach nie wymagających posiadania licencji na emisję fal radiowych. Jedynie z dala od dużych skupisk ludzkich można liczyć na brak zakłóceń pochodzących od innych użytkowników tych samych częstotliwości. Spośród pasm przydatnych do celu bezprzewodowej transmisji danych, pasmo 5 GHz jest mniej zatłoczone, ponadto odznacza się ono mniejszą średnicą strefy Fresnela i mniejszymi rozmiarami anten niż pasmo 2,4 GHz. Wszystko to razem czyni pasmo 5 GHz dogodnym do zastosowania w systemach CCTV.

Dobór sprzętu radiowego

Bazując na powyższych założeniach, należy odpowiednio dobrać sprzęt radiowy, który ma być użyty w bezprzewodowym systemie CCTV. Firma MikroTik oferuje szeroką gamę modułów radiowych pozwalających na pracę w paśmie 5 GHz. Dokonując wyboru, należy kierować się zarówno względami formalnymi, w tym przypadkiem poziomem mocy wyjściowej oraz zakresem częstotliwości dopuszczonym do nielicencjonowanego wykorzystania na terenie Polski, jak i względami technicznymi, z których najistotniejszym jest maksymalna przepływność planowanej sieci bezprzewodowej. Do dalszych rozważań (nie wdając się w szczegóły) przyjmijmy użycie modułu CM9.

Proponowany moduł CM9 nie jest w stanie pracować samodzielnie. Stanowi on wyposażenie płyty głównej (zwanej z angielska *router board*), będącej w istocie małym komputerem z zainstalowanym na stałe oprogramowaniem sieciowym. W ofercie firmy MikroTik spotkamy wiele modeli płyt głównych, ale do dalszych rozważań przyjmijmy widoczny na zdjęciu typ RB433.

W górnej części płyty głównej RB433 umieszczone są trzy gniazda, zwane także slotami, pozwalające na instalację modułów radiowych (w naszym przypadku modułów typu CM9).



Fot. 1. Moduły CM9 oraz płyta routera RB433

W dolnej części płyty głównej RB433 znajdują się trzy gniazda RJ-45 będące interfejsami Fast Ethernet, przy czym jedno z nich realizuje dodatkowo funkcję PoE.

Tak skompletowany zestaw modułu CM9 i płyty głównej RB433 wymaga umieszczenia w obudowie zewnętrznej oraz podłączenia do anteny przystosowanej do pracy w paśmie 5 GHz.

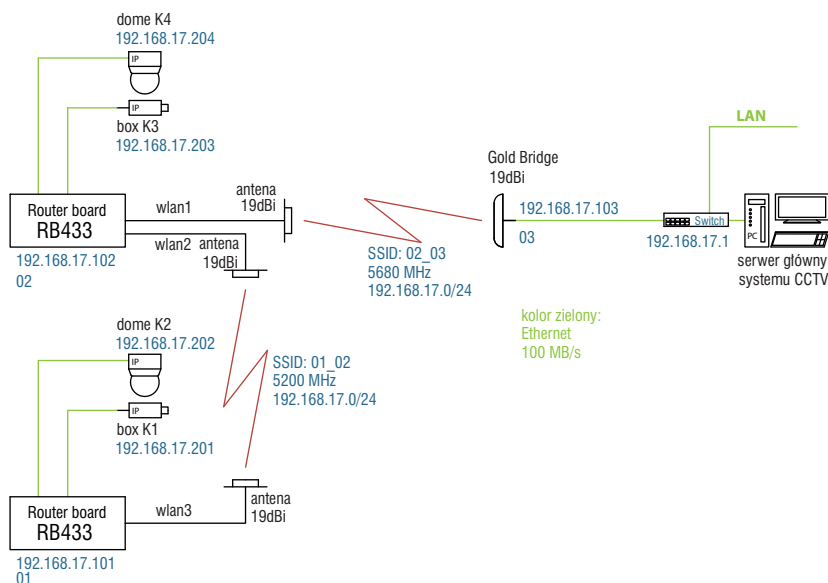
Zarówno obudowy zewnętrzne, jak i anteny są szeroko dostępne na wolnym rynku, mogą one pochodzić od innych producentów, niekoniecznie od MikroTika. Projektant czy instalator systemu CCTV może dokonać wyboru, kierując się własnymi kryteriami. Do dalszych rozważań przyjmijmy zastosowanie anteny panelowej INT-PAN-19-5X-HV o zysku energetycznym na poziomie 19 dBi i o polaryzacji liniowej. Antena ta nie jest produktem MikroTika.

Tak znaczny zysk energetyczny (równy 19 dBi) jest uzasadniony nie tyle wymogami, wynikającymi z bilansu mocy łącza radiowego, co koniecznością ograniczenia obszaru emisji i odbioru fal radiowych. Możliwość ograniczenia tego obszaru wynika z wąskich charakterystyk kierunkowych, typowych dla anten o dużym zysku energetycznym, i przyczynia się do stłumienia zakłóceń, przychodzących z kierunków bocznych. Praktyka wykazuje, że poprawa jakości sygnału w stosunku do anten dookólnych jest znaczna, zaś niedogodności wynikające z precyzyjnego pozycjonowania anten kierunkowych nie są uciążliwe. Jak już wspomniano, anteny dla pasma 5 GHz mają niewielkie rozmiary, co stanowi dodatkowe ułatwienie dla instalatora.

Opisany powyżej zestaw urządzeń został skompletowany i praktycznie wypróbowany przez autora opracowania. Próby zostały wykonane w obiektach, różniących się zarówno wielkością, jak i specyfiką. Maksymalny zasięg omawianych łączy radiowych w terenie otwartym osiąga wartość kilkunastu kilometrów. W terenie miejskim praca na dystansie kilkuset metrów nie stanowi najmniejszego problemu, zaś umieszczenie anten na odpowiednio wysokich masztach lub na dachach wysokich budynków pozwala na uzyskanie zasięgu identycznego jak w terenie otwartym. Warunkiem niezbędnym do uzyskania dużego zasięgu i wysokiej przepływności jest zachowanie niezaburzonej strefy Fresnela (ze szczególnym naciskiem na obszar znajdujący się w połowie dystansu między antenami). Czynnikiem ograniczającym są zakłócenia, które pochodzą od innych użytkowników tych samych częstotliwości. Jedynym rozwiązaniem tego problemu jest znalezienie wolnych kanałów, co nie stanowi problemu jedynie na terenach oddalonych od dużych miast.



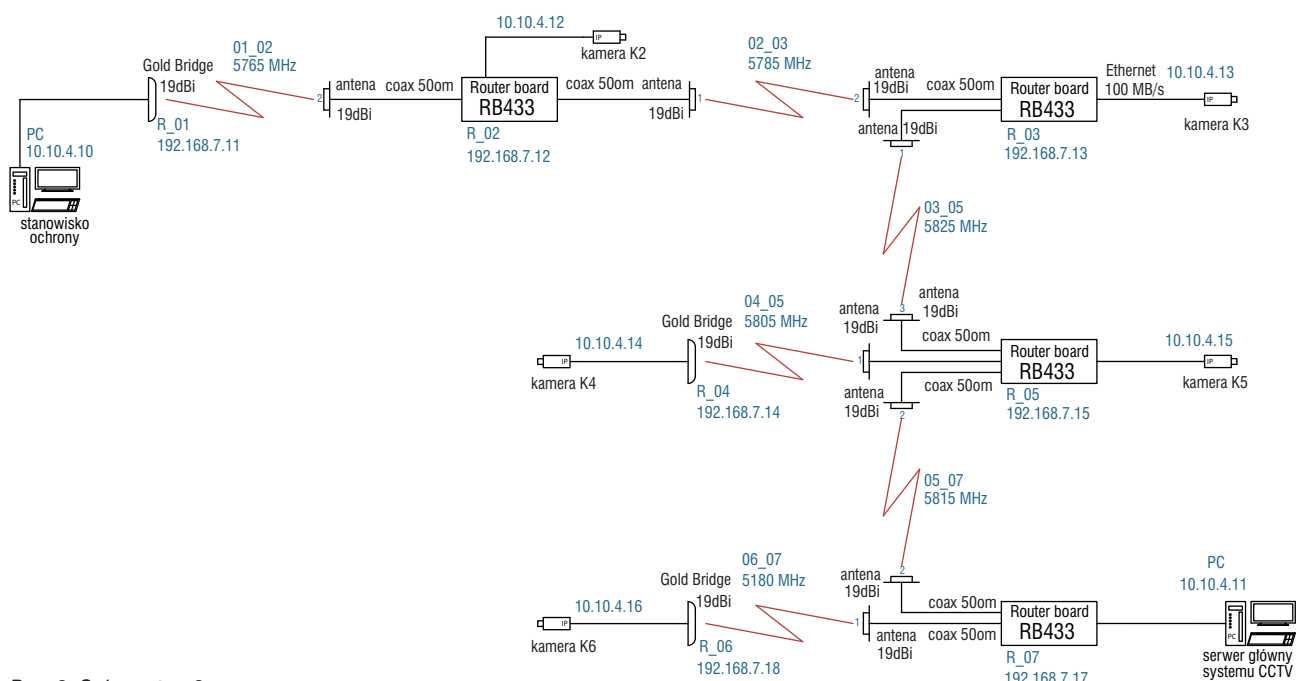
Fot. 2. Antena



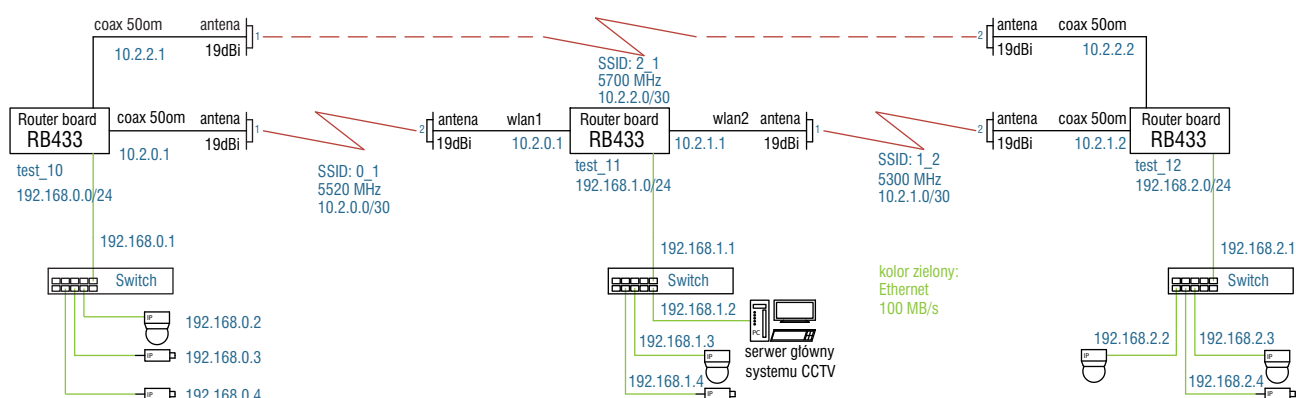
Rys. 1. Schemat nr 1

Przepływność sieci zbudowanych na bazie opisywanych zestawów urządzeń osiąga wartość 54 Mb/s, co znajduje pełne potwierdzenie w praktyce eksploatacyjnej. Zasadniczy wpływ na pogorszenie przepływności mają zakłócenia pochodzące od innych użytkowników tych samych częstotliwości oraz naruszenie strefy Fresnela przez przeszkody materialne. Jeśli jednak podczas instalacji zachowana zostanie odpowiednia staranność w doborze miejsc zamocowania anten, zaś zakłócenia zostaną wyeliminowane przez odpowiedni dobór częstotliwości, łącza będą zachowywać się stabilnie i nie spowodują ograniczeń przepływności.

Zaprezentowane schematy blokowe (Rys. 1, 2, 3) znalazły zastosowanie praktyczne, stanowią więc wiarygodny przykład zastosowania urządzeń firmy MikroTik w realnych warunkach użytkowych.



Rys. 2. Schemat nr 2



Rys. 3. Schemat nr 3

Zagadnienia instalacyjne

Skompletowany na powyższych zasadach sprzęt radiowy stanowi jedynie fragment systemu CCTV. Na całość składają się kamery, rejestratory obrazów, stacje robocze pracowników ochrony etc.

Rys. 1 przedstawia przykładowy schemat blokowy, na którym zostały zaznaczone wzajemne połączenia między elementami systemu.

Jak widać, kamery z płytami ruterów połączone są kablami kat. 5, typowymi dla warstwy fizycznej sieci Fast Ethernet, natomiast anteny z modułami CM9, umieszczonymi w slotach płyt głównych RB433, połączone są kablami koncentrycznymi. Liczba modułów CM9 i anten jest dostosowana do topologii sieci.

Występujący na rys. 1 moduł radiowy, opisany jako Gold Bridge, jest dostępnym na rynku kompletnym zestawem urządzeń, na który składa się prostsza i tańsza płyta główna typu RB411, moduł CM9 oraz antena panelowa. Wszystkie te elementy zamknięte są we wspólnej obudowie zewnętrznej. Jest to bardzo wygodne rozwiązanie techniczne pozwalające na szybką instalację końcowych punktów systemu, które nie wymagają ani dołączania dodatkowych kamer, ani rozgałęziania trasy transmisji.

Zagadnienia sieciowe

Przedstawiony na schemacie blokowym przykładowy system CCTV nie byłby w stanie działać, gdyby wszystkie zastosowane w nim urządzenia nie zostały odpowiednio zaprogramowane. W przypadku tak małych i prostych systemów wystarczająca jest konfiguracja zwana mostem sieciowym, czyli z angielska *bridge*. Bezprzewodowy most sieciowy łączy wszystkie urządzenia należące do danej sieci, tak jakby tego dokonano za pomocą innych nośników, np. przewodów. Innymi słowy, każda kamera i każdy ruter połączony jest z przedstawionym na schemacie przełącznikiem sieciowym, a tym samym z komputerem PC i siecią LAN.

W sensie sieciowym konfiguracja typu *bridge* jest całkowicie przezroczysta, to znaczy transmituje wszystkie pakiety sieciowe niezależnie od ich adresacji. Nie stwarza to problemów w małych i średnich sieciach bezprzewodowych, jednak w dużych instalacjach może stanowić ograniczenie, ponieważ wszystkie transmitowane w sieci dane są dostępne na wszystkich interfejsach niezależnie od tego, czy są potrzebne, czy zbędne. Taka sytuacja powoduje niczym nieuzasadnione zwiększenie ruchu sieciowego oraz pozwala na dostęp do danych z dowolnego punktu sieci, co w pewnych sytuacjach może okazać się niekorzystne.

Na rys. 2 przedstawiony jest schemat większej sieci bezprzewodowej, która także wykorzystuje konfigurację *bridge*.

Uważny czytelnik z łatwością zauważy, że kamery i komputery stanowiące zasadniczy człon systemu CCTV należą do innej sieci niż routery i moduły Gold Bridge. Tęgo typu rozwiązanie pozwala na proste zabezpieczenie przed przypadkową lub celową ingerencją w konfigurację ruterów przez osoby obsługujące system CCTV. Ponieważ routery te należą do osobnej podsieci, nie są widoczne dla komputerów, na których zbudowano serwer systemu CCTV oraz stację roboczą pracownika ochrony. Jest to jednak zabezpieczenie tylko o charakterze podstawowym, dobre dla pracowników ochrony, ale łatwe do pokonania przez osobę biegłą w informatyce.

Dostęp do ruterów

Dostęp do danych konfiguracyjnych każdego z ruterów możliwy jest dzięki prostemu i na dodatek darmowemu programowi o nazwie winbox.exe, który udostępniony jest w internecie na stronach poświęconych urządzeniom firmy MikroTik. W przypadku gdy cały system transmisyjny ma postać mostu sieciowego, uruchomienie programu winbox.exe na dowolnym komputerze, mającym dostęp do dowolnego interfejsu tej sieci, pozwala na nieograniczony dostęp do wszystkich jej składników. Administrator ruterów musi zadbać o bezpieczeństwo danych konfiguracyjnych, stosując logowanie z zabezpieczeniem za pomocą hasła, jednakże nawet w tym przypadku bardzo wyraźnie uwidacznia się niedogodność takiej prostej struktury mostu sieciowego.

Budujemy prawdziwą sieć IP

Poza oczywistą niedogodnością omówionych powyżej mostów sieciowych, która polega na nieograniczonym dostępie do wszystkich danych sieciowych na wszystkich interfejsach, inną wadą jest brak odporności na uszkodzenia fizyczne dowolnego węzła sieci. Gdyby na przykład uszkodzeniu uległ ruter R_07 (przedstawiony na drugim schemacie blokowym), główny serwer systemu CCTV straciłby połączenie ze wszystkimi kamerami, a także ze stacją roboczą pracownika ochrony. Jest to ryzyko znacznie ograniczające niezawodność całego systemu.

Alternatywą jest budowa sieci o strukturze pętlowej wykazującej pewną nadmiarowość, to znaczy pozwalającej na przekazywanie tych samych danych różnymi drogami. Bardzo uproszczonym przykładem takiego systemu o topologii trójkąta jest sieć uwidoczniiona na rys. 3.

W tym przypadku główny serwer systemu CCTV może uzyskać połączenie z oddalonymi kamerami za pośrednictwem dwóch tras: poprzez ruter „test_10” lub poprzez ruter „test_12”. Uszkodzenie lub zablokowanie jednego z łącz radiowych nie powoduje utraty komunikacji w sieci. W bardziej skomplikowanych strukturach (o większej nadmiarowości) poziom niezawodności wzrasta jeszcze bardziej niż w naszym bardzo uproszczonym przykładzie.

W przypadku ruterów typu RB433 zastosowanie struktury pętlowej zmusza do staranniejszego zaprojektowania i programowania całej sieci. Jak wynika z rysunku, nawet w tak prostym przypadku mamy do czynienia z sześcioma podsieciami oraz z rutingiem statycznym lub dynamicznym, które są niezbędne do transmisji danych z wykorzystaniem protokołu IP. Całość instalacji nabiera charakteru typowego dla sieci rozległych WAN.

Duże możliwości konfiguracyjne urządzeń firmy MikroTik pozwalają na łatwe tworzenie skomplikowanych struktur sieciowych, znacznie odbiegających od tych zaprezentowanych na powyższych przykładach. Programowanie ruterów jest typowym zagadnieniem sieciowym, do którego rozwiązania niezbędna jest wiedza informatyczna, jednak w przypadku płyt głównych RB433 jej zakres jest elementarny, możliwy do opanowania w relatywnie krótkim czasie. Dużym ułatwieniem jest pomoc kontekstowa, zawarta w wewnętrznym oprogramowaniu ruterów, udostępniana po uruchomieniu programu winbox.exe.

Realizacja praktyczna

Wszystkie opisane urządzenia są łatwe w instalacji i nie wymagają stosowania żadnych specjalistycznych metod czy narzędzi. Fot. nr 3 przedstawia punkt kamerowy, odpowiadający routowi „02” na schemacie nr 1. Wszystkie urządzenia elektroniczne (wraz z zasilaczem rutera) są zainstalowane wewnątrz aluminiowej obudowy umieszczonej nad kamerami, anteny są przymocowane do masztu i połączone z modułami R-09 za pomocą kabli koncentrycznych.

Na fot. nr 4 przedstawiony jest ruter „R_07”, występujący na drugim schemacie blokowym, stanowiący jedynie pośredni punkt komunikacyjny. Nie jest do niego dołączona żadna kamera. Podobnie jak poprzednio, wszystkie urządzenia elektroniczne znajdują się wewnątrz aluminiowej obudowy, widoczna na zdjęciu dolna puszka stanowi przyłączy energetyczne.

Wnioski

Jak powszechnie wiadomo, każda bezprzewodowa sieć IP (niezależnie od jej charakteru i jakości) odznacza się gorszą niezawodnością i gorszymi parametrami transmisyjnymi od dobrze zaprojektowanej i poprawnie wykonanej sieci kablowej. Także podatność sieci bezprzewodowej na włamanie lub atak typu DoS (celowe zablokowanie) jest znacznie większa niż w przypadku sieci kablowych. Jednakże w wielu przypadkach użycie kabli może okazać się niemożliwe, zaś uwarunkowania ekonomiczne stworzą preferencje dla sieci bezprzewodowych, z natury rzeczy nie obciążonych wysokimi kosztami robocizny związanej z pracami ziemnymi.

Przesadą byłoby twierdzić, że stosowanie łączy radiowych w sieciowych systemach CCTV jest bezproblemowe i pozbawione zawłości, jednakże w przypadku urządzeń firmy MikroTik zagadnienie znacznie się upraszcza. Realizacja małych systemów o strukturze mostu sieciowego leży w zakresie możliwości nawet mało doświadczonych projektantów czy instalatorów.

Rutery oraz moduły radiowe oferowane przez firmę MikroTik pozwalają osobom dysponującym rzetelną wiedzą informatyczną na realizację ambitniejszych zadań, graniczących z budową sieci WAN z routingiem statycznym lub dynamicznym. Biorąc pod uwagę niską cenę i łatwą dostępność tych urządzeń, można stwierdzić, że w cyfrowych systemach CCTV stanowią one realną alternatywę dla rozległych sieci kablowych.

Andrzej Walczyk
ALTRAM



Fot. 3. Punkt kamerowy



Fot. 4. Ruter R_07

G O MEGA



Przedstawiamy nową rodzinę
megapikselowych kamer Sony

ZAPROJEKTOWANE Z MYŚLĄ O BEZPIECZEŃSTWIE

SONY

IPELA

Inteligentna analiza obrazu... bezpieczeństwo dla Ciebie



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

www.sonybiz.pl

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

Inteligentne platformy CCTV

ALL IN ONE

już dostępne w Polsce

Każdy nowoczesny obiekt wymaga zapewnienia bezpieczeństwa na najwyższym światowym poziomie przebywających w nim osób oraz aktywów. Dlatego jednym z krytycznych elementów prawidłowego zabezpieczenia obiektów jest optymalny dobór zastosowanej technologii bezpieczeństwa. Powstające tendencje rynkowe oraz „pokoleniowa” ewolucja systemów CCTV, oddająca coraz więcej pola systemom IP, otwierają przed nami wcześniej nieznane możliwości zarządzania urządzeniami i obrazem. Jednocześnie pozwalają nam dodawać do tych narzędzi w sposób kompleksowy, dobrany do zindywidualizowanych potrzeb klientów, różnorodne narzędzia analityki video.

(W artykule została zachowana oryginalna pisownia – przyp. Red.)

Dopiero połączenie otwartej platformy, integrującej kamery analogowe oraz IP, wyposażonej w cały wachlarz możliwości analitycznych dodawanych do platformy jest funkcjonalnym wzorem dla optymalnie zaprojektowanych systemów zarządzania bezpieczeństwem.

Takie kompleksowe połączenie intuicyjnego współlistnienia otwartej platformy CCTV oraz najważniejszych, oferowanych na światowym rynku możliwości analityki obrazu do niedawna było jedynie oczekiwaniem.

Dziś, dzięki ogromnym możliwościom technologicznym i starannemu doborowi różnych produktów, jest możliwość stworzenia systemu w oparciu o jedno narzędzie integrujące wiele funkcjonalności, niezbędnych do zapewnienia właściwego poziomu bezpieczeństwa każdego obiektu (w zależności od miejsca potencjalnego ryzyka i zagrożenia).

Takim systemem jest otwarta platforma **DIVA** (Digital Intelligent Video Architecture) wraz z wieloma modułami analityki, zaimplementowanymi platformy już przez producenta. Wśród nich możemy znaleźć bardzo zaawansowane i wszechstronne reguły analityki obrazu, system rozpoznający numery rejestracyjne pojazdów oraz moduł służący rozpoznaniu i identyfikacji twarzy. Warty podkreślenia jest też fakt, iż zastosowanie wybranego modułu analityki nie wymaga od użytkownika posiadania specjalizowanych kamer. Wszystkie funkcje wykonywane są przez system na serwerze lub dedykowanych enkoderach.

System **DIVA** składa się z kilku komponentów tworzących skatomizowaną całość, gdzie poszczególne elementy analityki dobierane są w zależności od konkretnych potrzeb i zagrożeń. Każdy z modułów może być w dowolny sposób dodawany do systemu i wykorzystywany w wybranych miejscach na wskazanych kamerach.

Otwarta platforma DIVA

DIVA (Digital Intelligent Video Architecture) to otwarta platforma do integracji i zaawansowanego zarządzania systemami zabezpieczeń obiektów i obszarów, w tym w szczególności rozbudowanych obiektów sportowych wraz z otaczającą je infrastrukturą, oferująca mechanizmy zarządzania obrazem oraz opcjonalnie analityki obrazu najnowszej generacji.

Platforma **DIVA** jest rozwiązaniem skalowalnym, projektowanym pod potrzeby klienta, dającym możliwość wyboru rodzaju pełnionych funkcji oraz obszaru zastosowania.

Interfejs systemu jest w języku polskim.

System może być instalowany na już istniejącej infrastrukturze obiektowych systemów zabezpieczeń lub na nowym sprzęcie, wyposażając w ten sposób nadzorowane obiekty i obszary w dotychczas niestosowane mechanizmy zarządzania, detekcji i analizy zdarzeń.

Platforma **DIVA** integruje wiele typów kamer analogowych lub IP pochodzących od różnych producentów, a także reaguje na sygnały z systemów trzecich, takich jak: kontrola dostępu, system antywłamaniowy, system przeciwpożarowy czy POS.

DIVA charakteryzuje się poniższymi cechami funkcjonalnymi:

- 1) umożliwia przyszłe rozszerzanie swoich funkcjonalności poprzez dodawanie nowych funkcji analizy obrazu – system zatem może być **budowany modułowo**, przez dodawanie kolejnych elementów w miarę powstawania nowych potrzeb,
- 2) współpracuje zarówno z **kamerami analogowymi** jak i **kamerami IP** różnych producentów,
- 3) nie wymaga specjalnie dedykowanych sobie rozwiązań sprzętowych,
- 4) ma **zegar i kalendarz**, przy pomocy których jest możliwa konfiguracja swobodnie wybranej funkcji analizy obrazu, w dowolny sposób, odrębnie dla każdego dnia tygodnia, dla każdego urządzenia oddzielnie lub dla grupy urządzeń – jest to bardzo istotna możliwość z perspektywy różnych potrzeb w tych samych miejscach obiektu w zależności od pory dnia lub tygodnia,
- 5) ma możliwość tworzenia **bazy danych** zdarzeń,
- 6) umożliwia **przeszukiwanie bazy zdarzeń** na podstawie **indywidualnie wybranych parametrów**, np. według tablic rejestracyjnych pojazdów, twarzy ludzkich czy jakiegokolwiek reguły modułu ObjectR we wskazanej przez operatora cezurze czasowej,
- 7) umożliwia tworzenie **makr i procedur postępowania**, realizowanych przez system automatycznie w przypadku zaistnienia zdefiniowanego zdarzenia,
- 8) ma funkcjonalność **automatycznego zapobiegania** zmianą kąta widzenia kamery lub pola widzenia kamery,
- 9) umożliwia swobodne nadawanie przez administratora systemu **hierarchicznych uprawnień** każdej osobie lub grupom osób korzystających z systemu,
- 10) pozwala na **dowolną konfigurację wyświetlanego obrazu z kamer**, pracę z zestawami wielomonitorowymi, monitorami wielkoformatowymi, ścianami wideo,
- 11) ma funkcjonalność **opcjonalnego wyposażenia wybranej kamery w następujące moduły**: detekcja przekroczenia „wirtualnego muru”, detekcja przekroczenia wieloelementowego „wirtualnego muru”, detekcja pozostawienia lub zabrania przedmiotu w określonym obszarze zainteresowania, detekcja przebywania osoby bądź osób na danym obszarze ponad wyznaczony czas, detekcja pojawienia się obiektu w obszarze zainteresowania, detekcja tworzenia się tłumu, detekcja rozdzielania się obiektu, moduł ARTR (automatyczne rozpoznawanie tablic rejestracyjnych), moduł biometriki twarzy 2D,
- 12) ma możliwość nałożenia **wielopoziomowych map** nadzorowanego obszaru obiektu sportowego i umieszczenia na tych mapach punktów kamerowych, ponadto wybranie przez użytkownika „ikony” danej kamery będzie powodować automatyczne uzyskanie obrazu z danej kamery,
- 13) ma funkcjonalność **detekcji ruchu** przydzielanej wybranym kamerom z możliwością regulacji progu czułości w nielimitowanych obszarach pola widzenia urządzenia,
- 14) może **dostosowywać strumień wideo** pomiędzy serwerem a klientem do istniejącego między nimi dostępnego pasma transmisji.

Dodatkowo system DIVA umożliwia:

- 1) dowolne ustawienie pozycji i rozmiaru wyświetlanego obrazu z kamery wideo,
- 2) nadawanie nazw wybranych przez użytkownika systemu poszczególnym źródłom sygnału wideo,
- 3) przeszukiwanie zarejestrowanych materiałów wideo, z podziałem na źródła sygnału i z uwzględnieniem kalendarza w zadanych przez użytkownika przedziałach czasowych,
- 4) współpracę z systemami kontroli dostępu, systemami sygnalizacji włamania i napadu oraz innymi systemami sygnalizacji zagrożeń,
- 5) transmisję danych wizyjnych przy użyciu protokołu TCP/IP,
- 6) przeszukiwanie nagranych materiałów na podstawie funkcjonalności analityki dodanej **post factum** – oznacza to, że istnieje możliwość dodania do obrazu z kamery niewyposażonej w chwili rejestracji w wybraną funkcję analizy obrazu danej funkcjonalności analitycznej i filtracji tego materiału z uwzględnieniem nadanej funkcji,
- 7) tzw. **migrację funkcjonalności** wewnątrz systemu – oznacza to, iż dana funkcjonalność analityki obrazu nie jest przypisana na stałe do konkretnej kamery i w zależności od potrzeby może być dodawana do wybranej przez użytkownika kamery bądź grupy kamer – ta możliwość wynika z bardzo istotnej cechy całego systemu, która **nie wymaga posiadania specjalizowanych kamer** do dodania do nich funkcji analitycznych,
- 8) wyposażanie danej kamery w **więcej niż jedną** funkcjonalność analityczną – np. ta sama kamera ma możliwość realizowania funkcji biometriki twarzy w czasie trwania imprezy masowej, a po jej zakończeniu realizowania funkcjonalności analizy obrazu. Istnieje także możliwość wyposażania wybranej kamery w wybrane funkcjonalności analityczne **realizowane jednocześnie**.

System **DIVA** jest wyposażony w mechanizm tworzenia **dedykowanych procedur postępowania**, które są automatycznie realizowane w przypadku zaistnienia określonego rodzaju zdarzenia. **DIVA** zapewnia skuteczną detekcję i nadzór obiektu lub obszaru eliminując błędy popełnione przez obsługę, przy zagwarantowaniu osiągnięcia najwyższego stopnia bezpieczeństwa.

Platforma **DIVA** może być opcjonalnie wyposażona w trzy moduły analityki wideo:

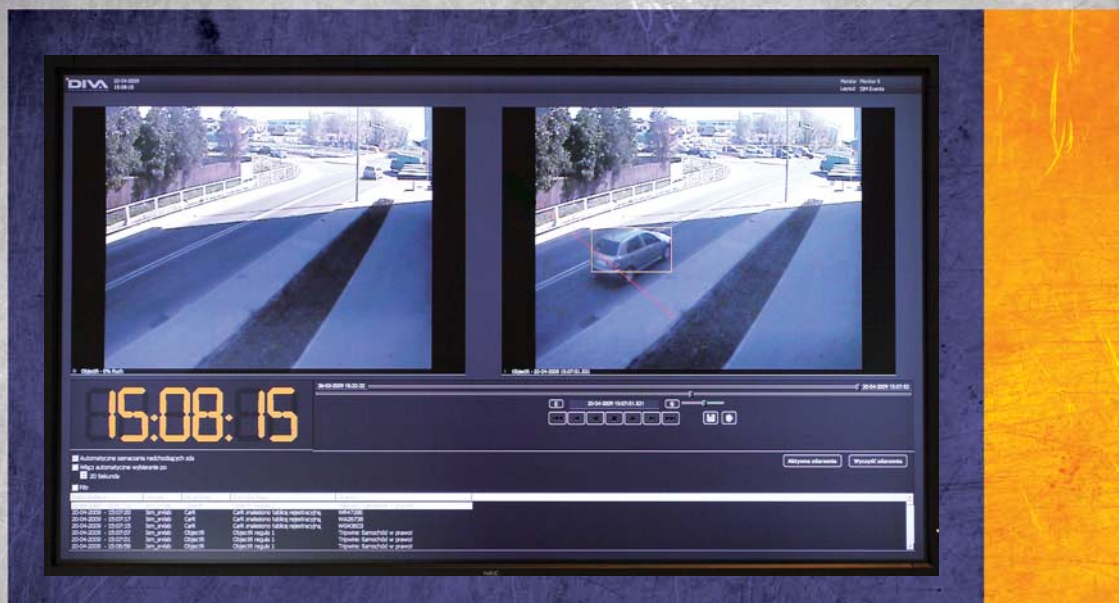
- 1) **ObjectR** – zaawansowana analityka zdarzeń,
- 2) **FaceR** – biometryka twarzy,
- 3) **CarR** – rozpoznawanie numerów rejestracyjnych pojazdów.

Moduł ObjectR – inteligentna analiza video

Algorytmy modułu **ObjectR** wyodrębniają obiekty z obrazu wideo i klasyfikują je według różnych kategorii. System pozwala użytkownikowi tworzyć reguły, których naruszenie powoduje alarm (zdarzenie).

ObjectR reaguje w czasie rzeczywistym m.in. na takie zdarzenia, jak: naruszenie przez obiekt określonego obszaru, nietypowe zachowanie osoby, pozostawienie lub też zabranie przedmiotu.

Dla każdej kamery można ustawić do **5 reguł** (detekcja przekroczenia wirtualnego muru, detekcja pozostawienia/zabrania



Fot. 1. Analizyka obrazu: Przekroczenie wirtualnego muru



Fot. 2. Analizyka obrazu: Śledzenie obiektu w polu kamery



Fot. 3. Moduł FaceR – rozpoznawanie twarzy

przedmiotu, detekcja rozdzielania obiektu, detekcja wejścia w obszar zainteresowania, detekcja tworzenia się tłumu, detekcja przebywania w danym obszarze ponad wyznaczony czas), co w połączeniu z funkcją obsługi zdarzeń i programowanymi makropoleceniami daje wiele możliwości reakcji na potencjalne zagrożenie.

Podstawowe funkcjonalności poszczególnych wariantów algorytmu to:

ObjectR Light

- wykrywanie pojawienia się obiektów w polu widzenia kamery (z możliwością maskowania stref),
- wykrywanie zniknięcia obiektów z pola widzenia kamery (z możliwością maskowania stref),
- wykrywanie pojawienia się lub zniknięcia obiektów bez przekraczania granicy strefy (na przykład wykrywanie osób wsiadających do pojazdów lub z nich wysiadających, bądź przechodzących przez drzwi).

ObjectR Basic

Zawiera funkcjonalności ObjectR Light oraz obsługę jednej, wyznaczonej wirtualnie, kontrolnej granicy strefy, w tym wykrywanie przekroczenia granicy przez obiekty (z możliwością określenia kierunku przekroczenia).

ObjectR Advanced

Zawiera funkcjonalności ObjectR Basic oraz:

- obsługę wielu wyznaczonych kontrolnych granic stref w określonych przedziałach czasu, w tym wykrywanie przekroczenia przez obiekt granicy „strefy”, np. płyty boiska, trybun, innych miejsc,
- wykrywanie pozostawienia lub usunięcia przedmiotu z zaprogramowanej strefy,
- wykrywanie obecności obiektu w nadzorowanej strefie ponad określony czas (nadzorowanie miejsc objętych zakazem parkowania lub przebywania),
- wykrywanie nietypowych zachowań (np. wykrywanie tworzących się kolejek).

Zastosowanie powyższych funkcjonalności w wybranych kamerach dowolnego obiektu radykalnie podnosi skuteczność właściwej detekcji zdarzeń, jednocześnie obniżając koszty zapewnienia bezpieczeństwa w obiekcie.

Moduł FaceR – Identyfikacja i weryfikacja twarzy

System automatycznego rozpoznawania twarzy **FaceR** to rozwiązanie służące do rejestrowania obrazu twarzy i porównywania go, w czasie rzeczywistym, z wzorcami zapisanymi w bazie danych. Dzięki możliwości integracji z systemami kontroli dostępu i istniejącymi systemami nadzoru **FaceR** umożliwia skuteczne zabezpieczenie wejścia do obszarów chronionych.

Moduł **FaceR** może stanowić samodzielny system służący do identyfikacji i weryfikacji osób wchodzących np. na stadion, znajdujących się na lotniskach, dworcach kolejowych, wchodzących do sklepów lub innych istotnych z perspektywy bezpieczeństwa miejsc.

W odróżnieniu od pozostałych technik biometrycznych, takich jak: skanowanie tęczówki oka lub odciski palców, mechanizm **FaceR**

działa w sposób nieinwazyjny i dyskretny. Rejestruje obraz twarzy z określonej odległości, w sposób często niezauważalny dla obserwowanej osoby.

Analiza twarzy 2D dokonywana jest w systemie na podstawie porównania 17 charakterystycznych punktów. Rozpoznanie obserwowanej osoby jest możliwe przy założeniu, że minimalna odległość między oczami rozpoznawanej twarzy wynosi 60 pikseli (przy użyciu kamery analogowej) i 110 pikseli (przy użyciu kamery IP).

System umożliwia płynną regulację parametrów (wartości progowych) rozpoznawania i porównywania twarzy osób pojawiających się w polu widzenia kamery z bazami danych.

System równocześnie wyświetla obrazy twarzy w trakcie rejestracji i obrazy zapisane w bazach danych.

Tworzenie baz danych twarzy odbywa się podczas rejestracji materiału wideo oraz na podstawie fotografii.

Obrazy twarzy można również importować z innych systemów, następnie wybierać i umieszczać na listach w bazie danych, dzięki czemu system **FaceR** może służyć do wykrywania osób poszukiwanych lub niepożądanych. Zidentyfikowanie obrazu twarzy, umieszczonej na czarnej liście, powoduje wygenerowanie sygnału alarmu i wyświetlenie zapisanego w bazie obrazu, dla porównania z obrazem twarzy osoby obserwowanej w chwili zaistnienia zdarzenia.

Moduł CarR - Rozpoznawanie numerów rejestracyjnych pojazdów

Moduł CarR to moduł służący do identyfikacji i weryfikacji pojazdów.

Moduł CarR wykrywa i rozpoznaje numery rejestracyjne pojazdów na obrazach wideo i klasyfikuje je według miejsca pochodzenia (UE, USA, Europa Wschodnia, kraje arabskie).

Zidentyfikowane tablice rejestracyjne są porównywane z listami numerów zgromadzonych w bazie danych (tj. z tzw. „czarnymi” i „białymi listami”). Dopasowanie lub brak dopasowania powoduje zaistnienie tzw. „zdarzenia”. Zdarzenia można wykorzystać do uruchomienia makropoleceń w innych elementach systemu.

W trybie autonomicznym wystąpienie określonego zdarzenia algorytmu CarR może powodować uruchomienie elementu sterującego np. szlabanu czy sygnalizacji świetlnej.

System pozwala ponadto programować profile ryzyka służące do wykrywania pojazdów powracających w to samo miejsce w określonym czasie. CarR może również ponadto wykorzystywany do liczenia pojazdów na parkingach.

Scharakteryzowany system **DIVA** jest już dostępny na polskim rynku. Wyłącznym dystrybutorem tego rozwiązania jest warszawska firma ISM EuroCenter S.A.

ISM EuroCenter



Fot. 4. Moduł CarR - rozpoznawanie tablic rejestracyjnych

Zestaw do zabezpieczenia bankomatu K12/BANK



Ogólna charakterystyka urządzenia

Zestaw zabezpiecza pomieszczenie bankomatu przed dostępem osób niepowołanych oraz umożliwia osobom korzystającym z bankomatu na bardziej komfortowe i bezpieczne pobieranie pieniędzy.

Zestaw do zabezpieczenia bankomatu składa się z dwóch podstawowych elementów:

- zamek do bankomatu K12/bank,
- czytnik kart magnetycznych ACT 1010.

Zamek do bankomatu K12/bank jest wersją kontrolera bibi-K12 przewidzianą do obsługi drzwi wejściowych do bankomatu. Umożliwia wejście do pomieszczenia z bankomatem osobie posiadającej kartę bankową pod warunkiem, że w tym czasie inna osoba nie znajduje się w środku.

Czytnik kart magnetycznych ACT 1010 to standardowy czytnik 2 ścieżki (zgodnie ze standardem ISO dla kart magnetycznych) przeznaczony do pracy w warunkach zewnętrznych.

Zasada działania

Zamek K12/bank pozwala na następującą obsługę drzwi do pomieszczenia bankomatu:

- Po przeciągnięciu karty w czytniku podawane jest napięcie na rygiel - klient może wejść.
- Po wejściu uruchamiana jest blokada zgodnie z zaprogramowanym czasem, aby klient mógł spokojnie pobrać pieniądze z bankomatu.
- Po wyjściu klienta blokada drzwi jest zakończona, nawet jeżeli nie upłynął jeszcze zaprogramowany czas blokady.

Wraz z zamkiem dostarczane są dwie karty serwisowe, które umożliwiają otwarcie drzwi do bankomatu w każdym momencie.

Dane techniczne zamka K12/bank

Kontrola uprawnień karty	
Obsługiwane prefiksy	100
Parametry dodatkowe	„format bankowy”
Karty serwisowe	2 karty umożliwiające zawsze dostęp
Wyjścia tranzystorowe	2 - OC 15 V / 1 A
Sterowanie rygłem	impuls do 25 s
Blokada „bankomat zajęty”	do 4 min
Wejścia sterujące	
Czujnik otwarcia drzwi	styki NO lub NC
Przycisk wyjścia	styki NO
Czujnik obecności	styki NO lub NC
Programowanie	łącze RS485
Napięcie zasilania	12,6 V (11 V do 14 V)
Pobór prądu	100 mA
Wymiary	130 x 130 x 35 mm
Temperatura pracy	od 0°C do +70°C

Dane techniczne czytnika ACT 1010

Odczyt karty	ISO 2 ścieżka
Prędkość odczytu	12 - 170 cm/s
Trwałość głowicy	> 1 000 000 odczytów
Napięcie zasilania	5 V do 12 V
Pobór prądu	20 mA
Wymiary	140 x 44 x 39 mm
Temperatura pracy	od -10°C do +55°C

Instalacja standardowa

Do standardowej instalacji wymagane są następujące elementy:

- zamek K12/bank,
- zasilacz z podtrzymaniem napięcia w razie awarii,
- czytnik kart magnetycznych ACT 1010,
- rygiel elektromagnetyczny,
- czujnik otwarcia drzwi.

Dodatkowo, jako elementy opcjonalne można zastosować:

- przycisk wyjścia,
- sygnalizacja „bankomat zajęty”,
- czujnik obecności (mata aktywna).



Micromade Gałka i Drożdż sp.j.
ul. Wieniawskiego 16
64-920 Piła

tel./faks (67) 213 24 14
e-mail: mm@micromade.pl
<http://www.micromade.pl>

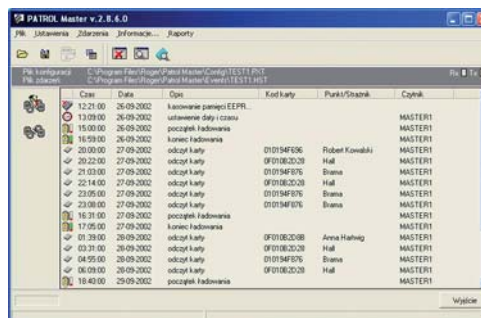
PATROL II LCD – rejestracja pracy wartowników



PATROL II LCD jest przenośnym czytnikiem transponderów zbliżeniowych UNIQUE, przeznaczonym do rejestracji obecności wartownika w wyznaczonych miejscach i o określonych porach. Urządzenie przeznaczone jest do weryfikacji rzetelności pracy wartowników, niemniej może znaleźć zastosowanie wszędzie tam gdzie zachodzi potrzeba kontroli przemieszczania się ludzi pod względem miejsca i czasu. Instalacja systemu polega na rozmieszczeniu w wybranych miejscach obiektu punktów kontrolnych oraz skonfigurowaniu czytnika. Każdemu punktowi kontrolnemu oraz identyfikatorowi użytkownika przypisuje się etykiety co umożliwia później łatwą interpretację historii zarejestrowanych zdarzeń.

Charakterystyka:

- Nieulotna pamięć ostatnich 3500 odczytów
- Sygnalizacja niskiego stanu baterii oraz zapelnienia pamięci
- Zegar czasu rzeczywistego
- Wyświetlacz LCD z podświetleniem
- Złącze USB do transmisji danych
- Ładowanie baterii bezpośrednio z gniazdka USB
- Program PATROL Master II (Windows)



Patrol II LCD:

- Czytnik
- Kabel USB
- Dwa akumulatory AA 1.5V
- Futerał
- Ładowarka baterii



roger®

Roger Sp.j.
Gościszewo 59
82-416 Gościszewo, woj. Pomorskie

tel. (55) 272 0132, faks (55) 272 0133
e-mail: roger@roger.pl
<http://www.roger.pl>

Inteligentny tester akumulatorów GOLD-IBT



GOLD-IBT

inteligentny tester akumulatorów

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

Jak zmierzyć jego pojemność?

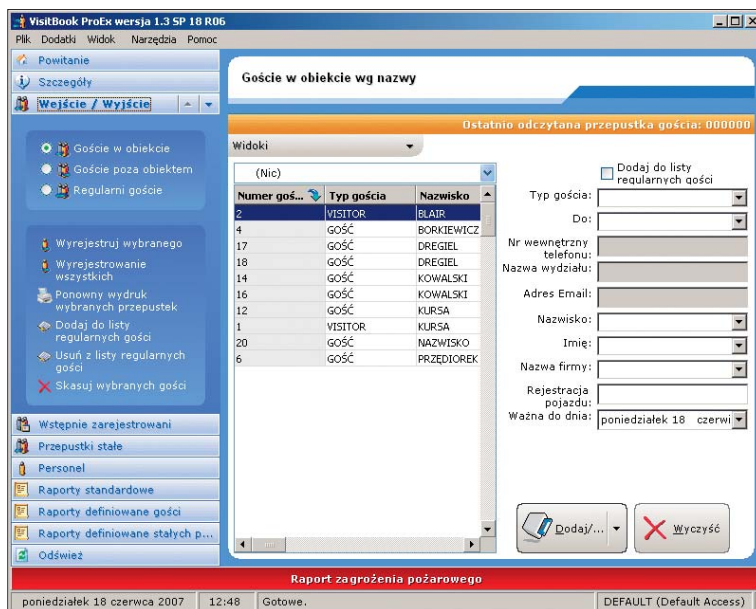
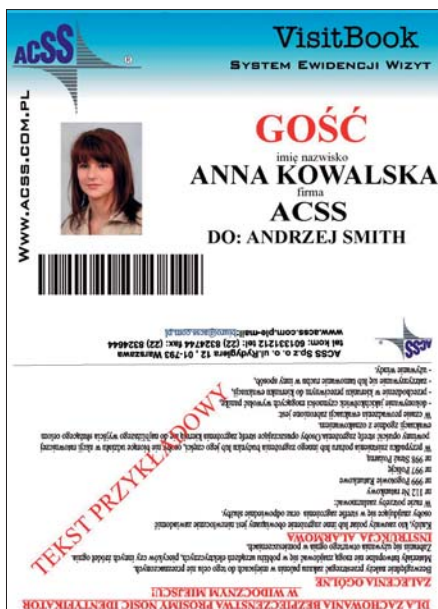
Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora.

Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.

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

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

System rejestracji gości VisitBook



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

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

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

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

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

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

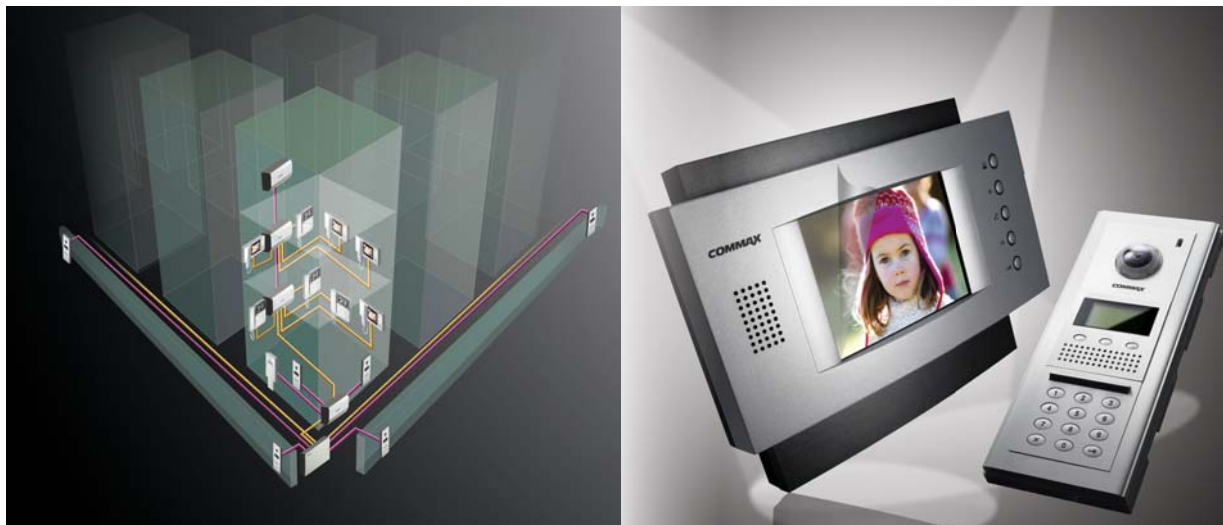
Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera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



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

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

System wieloabonentowy serii 2400



Elementy systemu:

Monitory / Unifony



CAV-51M



APV-4PM



CAV-51AM



AP-5HM

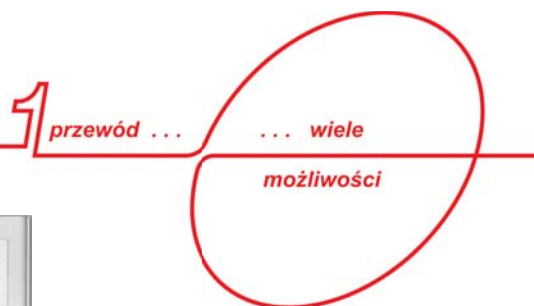
Stacje bramowe

DRC-MSC/MSB
DRC-OSC/OSB

DRC-nSC/nSB

DR-nSB

DR-nMS



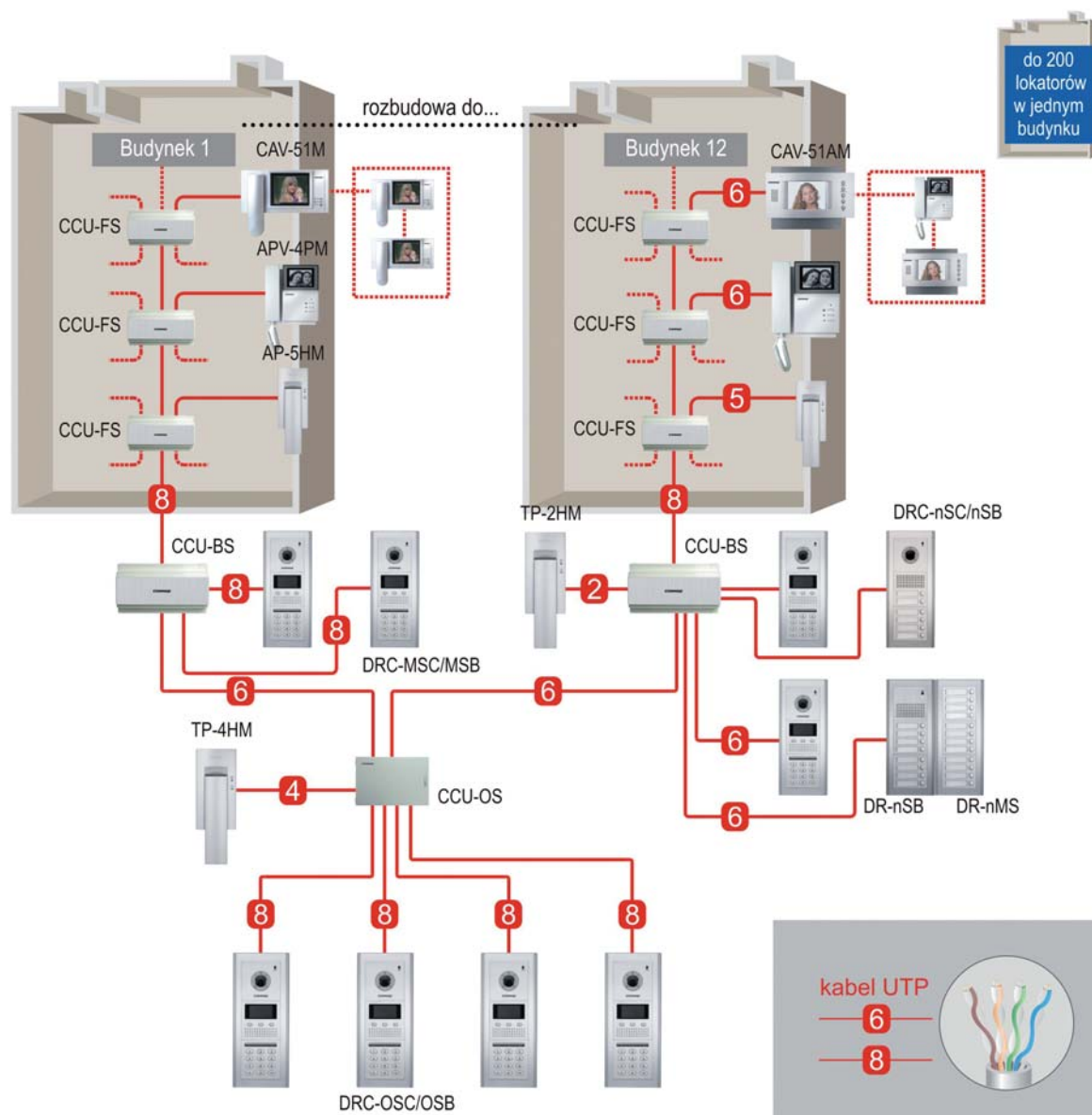
Dystrybutory



CCU-OS

CCU-BS
CCU-FS

System wieloabonentowy serii 2400



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

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

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

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

**2M ELEKTRONIK**

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

**3D****Wielobranżowe Przedsiębiorstwo Sp. z o.o.**

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

**AAT Holding sp. z o.o.**

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

Oddziały:

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

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

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

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

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

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

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

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

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

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

ACSS ID Systems Sp. z o.o.

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

**ADT Fire and Security Sp. z o.o.**

ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 83 01
faks (22) 430 83 02
e-mail: adtpoland@tycoint.com
www.adt.pl

ALARM SYSTEM**Marek Juszczyński**

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

**ALARMNET Sp. J.**

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

**ALARMTECH POLSKA Sp. z o.o.****Oddział:**

ul. Kielnińska 115
80-299 **Gdańsk**
tel. (58) 340 24 40
faks (58) 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

ALDOM F.U.H.

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

**ALPOL Sp. z o.o.**

ul. H. Krahelskiej 7
40-285 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
faks (32) 790 76 61
e-mail: alpol@e-alpol.com.pl
www.e-alpol.com.pl

**Oddziały:**

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

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

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

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

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

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

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

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

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

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

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

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

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

**ALKAM SYSTEM Sp. z o.o.**

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

**AMBIENT SYSTEM Sp. z o.o.**

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

**ANB Sp. z o.o.**

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

**Zakład Produkcyjno-Usługowo-Handlowy ANMA s.c. Tomaszewscy**

ul. Ostrowskiego 9
53-238 Wrocław
tel./faks (71) 363 17 53
e-mail: anma@anma-pl.eu
www.anma-pl.eu

ASSA ABLOY Poland Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
tel. (22) 751 53 54
faks (22) 751 53 56
e-mail: biuro@assaabloy.com.pl
www.assaabloy.com.pl



ATLine Sp. J.
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
handel@atline.com.pl
www.atline.com.pl



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



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



ROBERT BOSCH Sp. z o.o.
ul. Poleczki 3
02-822 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.com.pl



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



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

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



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



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



CBC (Poland) Sp. z o.o.
ul. Krasińskiego 41A
01-755 Warszawa
tel. (22) 633 90 90
faks (22) 633 90 60
e-mail: handlowy@cbcpoland.pl
www.cbcpoland.pl



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



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

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

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

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

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

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

COM-LM
ul. Sciegiennego 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. KEN 96/U15
02-777 Warszawa
tel./faks (22) 855 00 17
e-mail: pk@cs.pl
www.cs.pl



Przedsiębiorstwo Usług Technicznych D-2 s.c.
K. Kolin, B. Czechowska
ul. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85



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



D+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
e-mail: dh-polska@dh-partner.com
www.dhpolska.pl

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

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

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

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

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

ul. Wołczyńska 18, 60-003 Poznań
tel. (61) 863 82 08
faks (61) 866 64 16



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



DELTA BUSINESS SERVICE
Andrzej Bryl
ul. Ciepła 15/50
50-524 Wrocław
tel./faks (71) 367 06 16
e-mail: bok@delta-security.com.pl
www.delta-security.com.pl



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



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



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



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



DYSKRET Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
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. Bronistawa Czecha 59
04-555 Warszawa
tel. (22) 812 05 05
faks (22) 812 62 12
e-mail: office@ebs.pl, j.haschka@ebs.pl
www.ebs.pl



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



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



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



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



ELTCRAC
**Centrum Zabezpieczeń
Systemy Domofonowe**
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60/61, 292 48 70
faks (12) 292 48 62, 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl



ELZA ELEKTROSYSTEMY
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 264 04 60
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl



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

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



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



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

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

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



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



GDE POLSKA
ul. Koniecznego 46
32-040 Świątniki Górne
tel. (12) 256 50 25/35
faks (12) 270 56 96
e-mail: biuro@gde.pl
www.gde.pl



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.pl



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

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

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



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



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

**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

**INSAP Sp. z o.o.**

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

**ISM EuroCenter S.A.**

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

**JANEX INTERNATIONAL Sp. z o.o.**

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

**KABE Sp. z o.o.**

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

**Systemy Alarmowe****KOLEKTOR Sp. z o.o.**

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

KOLEKTOR

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

**P.P.U.H. LASKOMEX**

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

**MAXBAT Sp. J.**

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

**MICROMADE****Gałka i Drożdż Sp. J.**

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

**MICRONIX Sp. z o.o.**

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

**MIWI-URMET Sp. z o.o.**

ul. Pojezińska 90a
91-341 Łódź
tel. (42) 616 21 00
faks (42) 616 21 13
e-mail: miwi@miwiurmet.com.pl
www.miwiurmet.com.pl

NOMA 2**Zakład Projektowania i Montażu Systemów Elektronicznych**

ul. Plebiscytowa 36
40-041 Katowice
tel. (32) 359 01 11
faks (32) 359 01 00
e-mail: systemy@noma2.com.pl
www.systemy.noma2.pl

Oddziały:

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

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

**OBIS CICHOCKI ŚLĄZAK Sp. J.**

ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
faks (71) 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

**OMC INDUSTRIAL Sp. z o.o.**

ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sprzedaz@omc.com.pl
www.omc.com.pl

Przedstawicielstwo:

ul. Grunwaldzka 119, 60-313 Poznań
tel. (61) 657 93 60
poznan@omc.com.pl

**PETROSIN Sp. z o.o.**

Rynek Dębicki 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 Sp. z o.o.**

ul. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.com.pl

**POLON-ALFA****Zakład Urządzeń Dozometrycznych Sp. z o.o.**

ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

**PROFICCTV**

ul. Obornicka 276
60-693 Poznań
tel./faks (61) 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl

**PULSAR K. Bogusz Sp. J.**

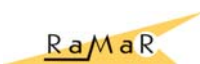
Siedlec 150
32-744 Łąpczyca
tel. (14) 610 19 40
faks (14) 610 19 50
e-mail: biuro@pulsarspj.com.pl
www.pulsarspj.com.pl
www.zasilacze.pl

**PPH. PULSON**

ul. Czernańska 18
00-718 Warszawa
tel. (22) 851 12 20
faks (22) 851 12 30
e-mail: biuro@pulson.com.pl
www.pulson.eu

RADIOTON Sp. z o.o.

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

**RAMAR s.c.**

ul. Modlińska 237
03-120 Warszawa
tel. (22) 676 77 37
faks (22) 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

**ROPAM Elektronik s.c.**

Os. 1000-lecia 6A/1
32-400 Myslenice
tel. (12) 379 34 47
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

**SATEL Sp. z o.o.**

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

**SATIE**

ul. Łączyńska 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 314 69 50
e-mail: info@satie.pl
www.satie.pl

**SAWEL Elektroniczne Systemy Zabezpieczeń**

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

**SCHRACK SECONET POLSKA Sp. z o.o.**

ul. Wołoska 9
02-583 Warszawa
tel. (22) 33 00 620 ÷ 623
faks (22) 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:

ul. Wierzbicice 1, 61-569 **Poznań**
tel. (61) 833 31 53
faks (61) 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-520 **Wrocław**
tel./faks (71) 345 00 95
e-mail: wroclaw@schrack-seconet.pl

**P.T.H. SECURAL Jacek Giersz**

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

**S.M.A.****System Monitorowania Alarmów Sp. z o.o.**

ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

Oddział:

ul. Różyckiego 1 C
51-608 **Wrocław**
tel. (71) 348 04 19, 347 91 91
faks (71) 348 04 19
e-mail: sma@sma.wroclaw.pl
www.sma.wroclaw.pl

**SOFTEX DATA S.A.**

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



stronger together

SOLAR POLSKA Sp. z o.o.

ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: centrala@solar.pl
www.solar.pl www.weblink.solar.pl
www.solar.pl/blueenergy

Oddziały:

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

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

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

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

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

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

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

ul. Przemysłowa 4F, 33-100 **Tarnów**
tel./faks (14) 629 80 20
e-mail: tarnow@solar.pl

ul. Glińki 144 bud. A, 85-861 **Bydgoszcz**
tel. (52) 320 50 88/89
faks (52) 362 01 52
e-mail: bydgoszcz@solar.pl

**SONY POLAND Sp. z o.o.**

ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 24 51
tel. kom. (0) 692 403 272, 600 206 117
faks (22) 520 25 77
e-mail: diana.jesione@eu.sony.com
marta.malecka@eu.sony.com
www.sonybiz.net/nvm

SPRINT Sp. z o.o.

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

Oddziały:

ul. Przemysłowa 15, 85-758 Bydgoszcz
tel. (52) 365 01 01
faks (52) 365 01 11

ul. Budowlanych 64E, 80-298 Gdańsk
tel. (58) 340 77 00
faks (58) 340 77 01

ul. Heyki 27C, 70-631 Szczecin
tel. (91) 485 50 00
faks (91) 485 50 12

ul. Canaletta 4, 00-099 Warszawa
tel. (22) 826 62 77
faks (22) 827 61 21

SPS trading

S.P.S. Trading Sp. z o.o.

ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. (22) 518 31 50
faks (22) 518 31 70
e-mail: warszawa@spstrading.pl
www.aper.com.pl

Biura Handlowe:

ul. Drożyny 6, 80-302 Gdańsk
tel. (58) 624 83 04
faks (58) 668 59 20
e-mail: gdansk@spstrading.pl

ul. Kościuszki 227, 40-600 Katowice
tel. (32) 255 64 27
faks (32) 255 64 52
e-mail: katowice@spstrading.pl

ul. Inflancka 6, 91-857 Łódź
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.pl

ul. Dąbrowszczaków 2 A, 10-541 Olsztyn
tel. (89) 527 92 72
faks (89) 527 92 30
e-mail: olsztyn@spstrading.pl

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

ul. Grudziądzka 176, 87-100 Toruń
tel. (56) 653 99 43
faks (56) 653 90 81
e-mail: torun@spstrading.pl

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

SYSTEM 7

ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
infolinia 0 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.sevenguard.com,
www.system7.pl



TAP Systemy Alarmowe Sp. z o.o.

Os. Armii Krajowej 125
61-381 Poznań
tel. (61) 876 70 88
faks (61) 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl



Biuro Handlowe:

ul. Rzymowskiego 30, 02-697 Warszawa
tel. (22) 843 83 95
faks (22) 843 79 12
e-mail: tap5@tap.com.pl



TAC Sp. z o.o.

Oddziały:

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

ul. Arkońska 6 bud. A2
80-387 Gdańsk
tel. (58) 782 00 00
faks (58) 782 00 04

ul. Rysia 1A
53-656 Wrocław
tel. (71) 711 09 19
faks (71) 711 09 20

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

TALCOMP



TALCOMP SYSTEMY BEZPIECZEŃSTWA

Konrad Talar
ul. Fałęcka 48
30-441 Kraków
tel. (12) 655 85 85, 425 63 67
faks (12) 425 63 68
e-mail: talcomp@talcomp.pl
www.talcomp.pl



TAYAMA POLSKA Sp. J.

ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl



Zakład Rozwoju Technicznej Ochrony Mienia

TECHOM Sp. z o.o.
ul. Marszałkowska 60/27
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 77
Sprzedaż: (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@tpeltech.pl
www.tpeltech.pl

Oddziały:

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

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

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

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

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



W2 Włodzimierz Wyrzykowski

ul. Czajcza 6
86-005 Białe Błota
tel. (52) 345 45 00
tel./faks (52) 584 01 92
e-mail: lukasz.cellari@w2.com.pl
www.w2.com.pl



V4S Sp. z o.o.

ul. Szczecińska 1FA
72-003 Dobra
tel. (91) 421 16 52, 311 33 49
infolinia 0 801 055 075
faks (91) 421 18 05
e-mail: info@v4s.pl
www.v4s.pl



Vision Polska

VISION POLSKA Sp. z o.o.

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



CENTRUM SYSTEMÓW ZABEZPIECZENIA

STRATUS

ul. Nowy Świat 38
20-419 Lublin
tel./faks (81) 743 87 72
e-mail: stratus@stratus.lublin.pl
www.stratus.lublin.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	–	TAK	TAK	TAK	–
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	–	TAK	TAK	TAK	TAK
Alarm System	TAK	–	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Aldom	–	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	–	TAK	TAK	TAK	–
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	TAK	TAK	TAK
AVISmedia	–	TAK	TAK	–	TAK
Bitner Zakłady Kablowe	TAK	–	–	–	–
BOSCH	TAK	–	TAK	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
C&C Partners	–	TAK	TAK	–	TAK
CAMSAT	TAK	TAK	TAK	–	–
CBC Poland	TAK	–	TAK	–	TAK
CCX	–	TAK	TAK	TAK	TAK
CMA	TAK	TAK	TAK	TAK	–
COM-LM	TAK	TAK	TAK	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	–
D-2	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D + H Polska	–	TAK	TAK	TAK	TAK
DANTOM	TAK	–	TAK	–	–
Delta Business Service	–	TAK	–	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	–	TAK
Dyskam	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	–	TAK	–	–
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compile	TAK	–	TAK	–	TAK
EI-Mont	–	TAK	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	–
GDE Polska	–	–	TAK	–	TAK
Gunnebo	TAK	TAK	TAK	TAK	–
GV Polska	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
HSA	–	–	TAK	–	–
ICS Polska	–	–	TAK	–	TAK
Info-Cam	TAK	TAK	TAK	TAK	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	–	TAK	–	–
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	–	TAK	–	TAK	–
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	–	–	–	TAK
Micronix	–	TAK	TAK	–	–
Miwi-Urmet	TAK	–	TAK	–	TAK
Noma 2	TAK	TAK	TAK	TAK	–
OBIS	–	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	–	–	TAK	–	–
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	TAK	–	–
PPH Pulson	TAK	TAK	TAK	–	–
Radioton	–	–	TAK	–	–
Ramar	TAK	–	TAK	TAK	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Sagitta	TAK	–	–	–	–
Satel	TAK	–	–	–	–
SATIE	TAK	–	TAK	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	–	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
SOFTEx Data	–	–	TAK	–	TAK
Solar	–	–	TAK	–	–
Sony	TAK	–	–	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	TAK	TAK	–	TAK
TAC	TAK	TAK	TAK	TAK	TAK
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Techom	–	–	–	–	TAK
Technokabel	TAK	–	–	–	–
TP TELTECH	–	TAK	TAK	TAK	–
W2	TAK	TAK	TAK	–	–
V4S	TAK	–	TAK	–	TAK
Vision Polska	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnienia
2M Elektronik	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	TAK	TAK	TAK	–	–	TAK	–	TAK	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	TAK	TAK	TAK	TAK	–	–	–	–	TAK
ANB	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–
AVISmedia	–	–	–	TAK	–	–	–	–	TAK
Bitner Zakłady Kablowe	kable i przewody do SSWiN, systemów telewizji dozorowej, kontroli dostępu i in.								
BOSCH	TAK	TAK	–	TAK	–	–	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
bt electronics	–	–	TAK	–	–	–	–	TAK	–
C&C Partners	TAK	TAK	TAK	–	TAK	TAK	TAK	–	–
CAMSAT	–	TAK	–	–	–	–	–	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CCX	–	–	TAK	–	–	–	–	TAK	–
CMA	TAK	–	–	–	–	–	TAK	–	–
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Control System FMN	TAK	TAK	TAK	TAK	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D + H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Delta Business Service	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	TAK	–	–	–	–	TAK	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	TAK	–	TAK	TAK	–	TAK	TAK	–	–
EDP Support Polska	TAK	TAK	TAK	–	TAK	TAK	–	TAK	–
ela-compil	–	–	–	–	–	TAK	–	–	–
EI-Mont	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	–	–
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	TAK	TAK	TAK	–	–	–	–	TAK	–
Gunnebo	–	–	TAK	–	TAK	–	–	TAK	–
GV Polska	–	TAK	TAK	–	–	–	TAK	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnienia
HSA	TAK	TAK	TAK	–	–	–	–	–	–
ICS Polska	TAK	TAK	TAK	–	–	–	–	–	–
Info-Cam	TAK	TAK	TAK	–	–	TAK	TAK	–	TAK
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	TAK	–	–	TAK	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Miwi-Urmet	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK	–
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
OBIS	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	–	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	–	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
PPH Pulson	TAK	–	–	–	–	TAK	TAK	–	–
Radioton	–	TAK	–	–	–	–	–	–	–
Ramar	TAK	TAK	TAK	–	TAK	–	TAK	–	–
ROPAM Elektronik	TAK	–	TAK	TAK	–	–	TAK	–	–
Sagitta	–	–	–	TAK	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Softex Data	–	TAK	–	–	–	TAK	TAK	–	–
Solar	TAK	TAK	TAK	TAK	TAK	–	TAK	–	TAK
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	–	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
TAC	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Talcomp	TAK	TAK	TAK	–	TAK	–	–	–	–
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Techom	szkolenia								
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
TP TELTECH	TAK	TAK	TAK	TAK	TAK	–	TAK	–	–
W2	TAK	–	–	TAK	–	–	–	–	–
V4S	–	TAK	–	–	–	TAK	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny

Teresa Karczmarczyk

Redaktor merytoryczny

Stanisław Banaszewski

Dział marketingu i reklamy

Ela Końska

Redaguje zespół:

Krzysztof Białek

Marek Blim

Patryk Gańko

Norbert Góra

Ryszard Sobierski

Waldemar Szulc

Adam Wojcinowicz

Marek Życzkowski

Współpraca zagraniczna

Rafał Niedzielski

Współpraca

Marcin Buczał

Adam Bułaciński

Piotr Czernoch

Marcin Pyclik

Adam Rosiński

Sławomir Wagner

Andrzej Wójcik

Skład i łamanie

Marek Bładoszewski

Korekta

Elżbieta Kaluga

Adres redakcji

ul. Puławska 359, 02-801 Warszawa

tel. (22) 546 0 951, 953

faks (22) 546 0 959

www.zabezpieczenia.com.pl

Wydawca

AAT Holding sp. z o.o.

ul. Puławska 431, 02-801 Warszawa

tel. (22) 546 0 546

faks (22) 546 0 501

Druk

Regis Sp. z o.o.

ul. Napoleona 4, 05-230 Kobyłka

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4200 zł
cała strona, czarno-biała	2200 zł
1/2 strony, pełny kolor	2700 zł
1/2 strony, czarno-biała	1500 zł
1/3 strony, pełny kolor	1900 zł
1/3 strony, czarno-biała	1000 zł
1/4 strony, pełny kolor	1400 zł
1/4 strony, czarno-biała	800 zł
karta katalogowa, 1 strona	900 zł

Artykuł sponsorowany:

indywidualne negocjacje (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł

Spis teleadresowy:

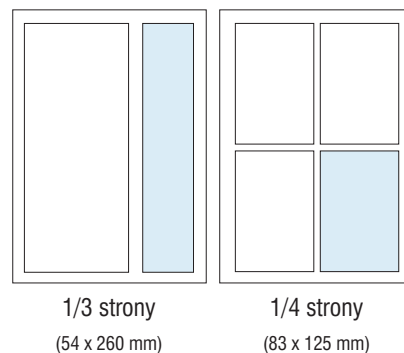
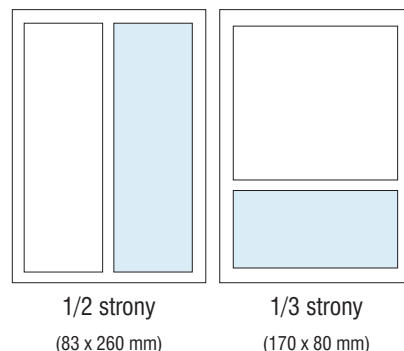
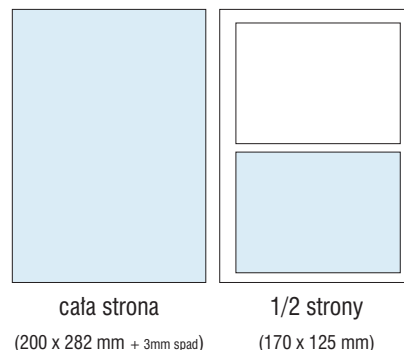
jednorazowy wpis	70 zł
------------------	-------

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji

**W przypadku zamówienia na 12 emisji
10% rabat**

Podane ceny nie uwzględniają podatku VAT (22%)

Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej
<http://www.zabezpieczenia.com.pl>
w dziale **Reklama**



Spis reklam

AAT Holding	45, 79	Kabe	53
ACSS	57	Nedap	23
ADD	35	Polon-Alfa	75
Altram	85	Roger	107
ATline	63	Satel	39
Bosch	1	Solid Security	21
Gunnebo	51	Sony Poland	2
HID	108	Targi Kielce	74
Ifter	52	Techom	59
Info-Cam	69	Videotec	13
Janex International	29	WSM	33

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

ZABEZPIECZENIA
CZASOPISMO BEZPŁATNE | ISSN 1555-9419 | DWUMIESIĘCZNIK NR 4/2009
WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ZABEZPIECZENIA@AAT.PL

Access Professional Edition – elastyczny system kontroli dostępu, który rośnie wraz z potrzebami Twojej firmy

BOSCH
Technologia błądząca nie

W NUMERZE:

- Nowa norma idylogia zasilania systemów alarmowych
- Łączna redukcja kosztów alarmowania dla przegranych budynków
- Nowoczesność w zarządzaniu bezpieczeństwem – nowe aplikacje
- Współpraca czy błąd dzierżby? Czy nadal trzeba mieć swój profil na portalach społecznościowych?

RACS ROGER ACCESS CONTROL SYSTEM

seria radius



Seria Radius

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

W skład rodziny wchodzi czytniki i kontrolery różniące się konstrukcją mechaniczną oraz funkcjonalnością, w zależności od modelu obsługują one karty standardu EM 125 kHz lub 13,56MHz Mifare. Nową kategorię produktu stanowi wandaloodporny czytnik (PRT64EM-VP), w którym przednia część obudowy i klawisze są wykonane w całości z metalu.

Na szczególną uwagę zasługuje kontroler PR602LCD specjalnie zaprojektowany dla systemów rejestracji czasu pracy RCP, do których oferowane jest nowoczesne oprogramowanie RCP Master.

RCP Master

Kompleksowe rozwiązanie RCP firmy ROGER ułatwia zarządzanie czasem pracy oraz wpływa na redukcję kosztów oraz precyzję rozliczania, przyczyniając się pośrednio do wzrostu produktywności w przedsiębiorstwie. RCP Master posiada łatwy w obsłudze, przyjazny interfejs. Program może być użytkowany bezpłatnie w celach ewaluacyjnych przez pierwsze 60 dni. RCP Master oferowany jest z licencją do obsługi 50, 250 lub powyżej 250 pracowników a także w wersji jedno lub wielostanowiskowej, co umożliwia dopasowanie rozwiązania do struktury i wielkości przedsiębiorstwa. Program RCP Master został opracowany w środowisku Microsoft .NET i jest przeznaczony dla systemów operacyjnych Windows XP i Vista.



RCP Master



PR602LCD



roger[®]

www.roger.pl

profesjonalna
kontrola
dostępu



Potrzebuję...

bezpieczeństwa całej firmy,
które jest niezawodne
i najnowocześniejsze

HID oferuje rozwiązania...

na których możesz polegać. Łączą one
bezpieczeństwo i wygodę użycia

HID Global, dostawca ponad 300 mln produktów stał się najbardziej zaufaną marką na rynku.

Bliska współpraca z naszymi klientami gwarantuje, że nawet najbardziej wyszukane potrzeby
zostaną spełnione - dziś, jutro i w przyszłości



H
I
D

Odwiedź naszą stronę hidglobal.com/iwant