

Panasonic
ideas for life

Przetwornik CCD 1,3 Megapiksela, pozwoli Ci zobaczyć więcej



Kamera standardowa



Kamera megapikselowa

**Profesjonalny
sieciowy system
monitoringu wizyjnego
dostarcza doskonałej
jakości obrazów
oraz gwarantuje
wysoką jakość
całego systemu**



Kopułkowa,
megapikselowa
kamera sieciowa
WV-NF302



Megapikselowa kamera
sieciowa typu dzień/noc
WV-NP304

i-Pro Network Surveillance System



<http://panasonic.net/security/>

W NUMERZE:

- Wpływ opóźnień w sieciach IP na skuteczność monitoringu wizyjnego
- Systemy sygnalizacji włamania. Część I. Konfiguracje central alarmowych
- Nocne oświetlanie obiektów monitorowanych przez systemy telewizji dozorowej
- Metodyka SABSA – biznesowe ujęcie kwestii bezpieczeństwa w przedsiębiorstwie

Tak elastyczna, jak Twoje plany

Modułowa centrala sygnalizacji pożaru serii 5000 firmy Bosch



Elastyczność i dostosowanie do potrzeb. Cokolwiek planujesz w zakresie ochrony przeciwpożarowej, modułowa centrala sygnalizacji pożaru serii 5000 firmy Bosch zapewni Ci system sygnalizacji pożaru spełniający najbardziej wyśrubowane wymagania od pojedynczej, samodzielnej centrali po złożoną sieć w pełni wyposażonych central. Dzięki modułowej konstrukcji, możesz dostosować system, kiedy tylko zmienią się Twoje wymagania. Modułowość upraszcza każdy krok: planowanie, instalację, obsługę, szkolenie i rozbudowę. Każdy z tych kroków odkrywa przed Tobą korzyści, jakie niesie nasz system. Więcej informacji można uzyskać na stronie internetowej www.boschsecurity.pl



BOSCH

Technologia bliżej nas

Robert Bosch Sp. z o.o.
Security Systems

ul. Poleczki 3, 02-822 Warszawa

tel.: +48 22 715 41 00 / 01, fax: +48 22 715 41 05 / 06
securitysystems@pl.bosch.com www.boschsecurity.pl

Spis treści

C Z A S O P I S M O
ZABEZPIECZENIA 2/2009

Wydarzenia, Informacje 6

Porady

Nocne oświetlanie obiektów monitorowanych przez systemy telewizji dozorowej
– *Andrzej Walczyk* 22

Publicystyka

Metodyka SABSA – biznesowe ujęcie kwestii bezpieczeństwa
w przedsiębiorstwie – *Mirosław Ryba, Łukasz Ślęzak, Ernst & Young* 26

„Ludwinów” – inteligentny budynek u stóp Wawelu
– *DG Elpro* 30

Telewizja dozorowa

Wpływ opóźnień w sieciach IP na skuteczność monitoringu wizyjnego (część I)
– *Marek Życzkowski, Łukasz Stawicki* 36

Co potrafi kamera telewizji dozorowej?
– *Marta Malecka, Sony Poland* 42

Kamery megapikselowe z Pelco
– *Norbert Góra, TAC* 44

Cyfrowa bezprzewodowa transmisja obrazu wideo Camsat
– *Beata Nadziejko, P.W. Camsat* 46

Ochrona przeciwpożarowa

Systemy sygnalizacji pożarowej marki Bosch – kompletna oferta modułów
wejść/wyjść instalowanych w pętlach dozorowych
– *Bosch Security Systems* 50

Monitorowanie systemu sygnalizacji alarmu pożarowego Panasonic EBL 512
przez Internet – *Rafał Rusiecki, Raj International* 54

Gaszenie gazem obojętnym
– *Rafał Czernicki, ADT Fire and Security* 56

Kontrola dostępu

Biometria z NOVUSA (część II) – *Ryszard Sobierski, AAT Holding* 62

SSWiN

Systemy sygnalizacji włamania (część I). Konfiguracje central alarmowych
– *Waldemar Szulc, Adam Rosiński* 66

Ochrona informacji

Zagrożenia bezpieczeństwa informacji w przedsiębiorstwie (część II)
Kształtowanie zachowań zabezpieczających informacje w małej firmie
– *Marek Jabłoński, Magdalena Mielus* 74

Zarządzanie ryzykiem w działalności gospodarczej (część IV)
– *Anna Słodczyk, Piotr Mąkosa, Risk Management Team Poland* 78

Karty katalogowe 81

Spis teled adresowy 88

Cennik i spis reklam 98



„Ludwinów” – inteligentny budynek
u stóp Wawelu

30



Kamery megapikselowe z Pelco

44



Gaszenie gazem obojętnym

56



Zarządzanie ryzykiem
w działalności gospodarczej

78



IFSEC2009

11 - 14 May 2009
NEC Birmingham

THE MEETING PLACE FOR THE SECURITY INDUSTRY

Security watch.



Finding your way through the economic downturn means using your business acumen to make informed decisions about your future.

IFSEC offers you the ideal platform to **explore your options, analyse resources** and **gather invaluable insight**. Hosting over 800 world leading companies, groundbreaking technologies, a high-profile educational programme and more, IFSEC is the global event of choice for more than 30,000 security professionals.



Supported by:



11 - 14 May 2009, NEC Birmingham
www.ifsec.co.uk

Organised by:



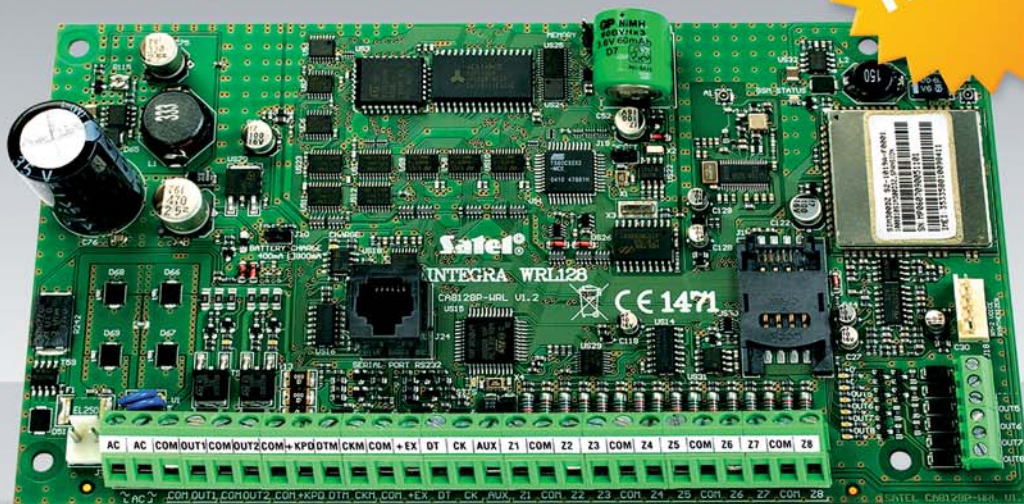
United Business Media

Innowacja w zabezpieczeniach

Centrala INTEGRA 128-WRL

Centrala o możliwościach INTEGRY 128, wyposażona w komunikator GSM/GPRS i technologię dwukierunkową bezprzewodowej łączności z czujkami ABAX. Rozwiązanie dające maksimum korzyści oferowanych przez technologię bezprzewodową z elastycznością i funkcjonalnością tradycyjnych systemów przewodowych.

Nowość



Złoty Medal Targów Poznańskich przyznany centrali za jej innowacyjność, wszechstronność i technologiczne zaawansowanie.

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

Polalarm Cup '09

21–23 maja 2009 r.

Ośrodek Żeglarsko – Wypoczynkowy
„Wichrowe Wzgórze”
w Rynie na Mazurach



Program imprezy

21 maja: Wieczorne hulanki i swawole przy grillu i gitarze

22 maja: 10:00 piracki szlak – do boju żeglarze! Wieczorem wręczenie pucharów, koncert szantowy, pieczenie prosiaka

23 maja: pływanie indywidualne dla chętnych

Zapewniamy:

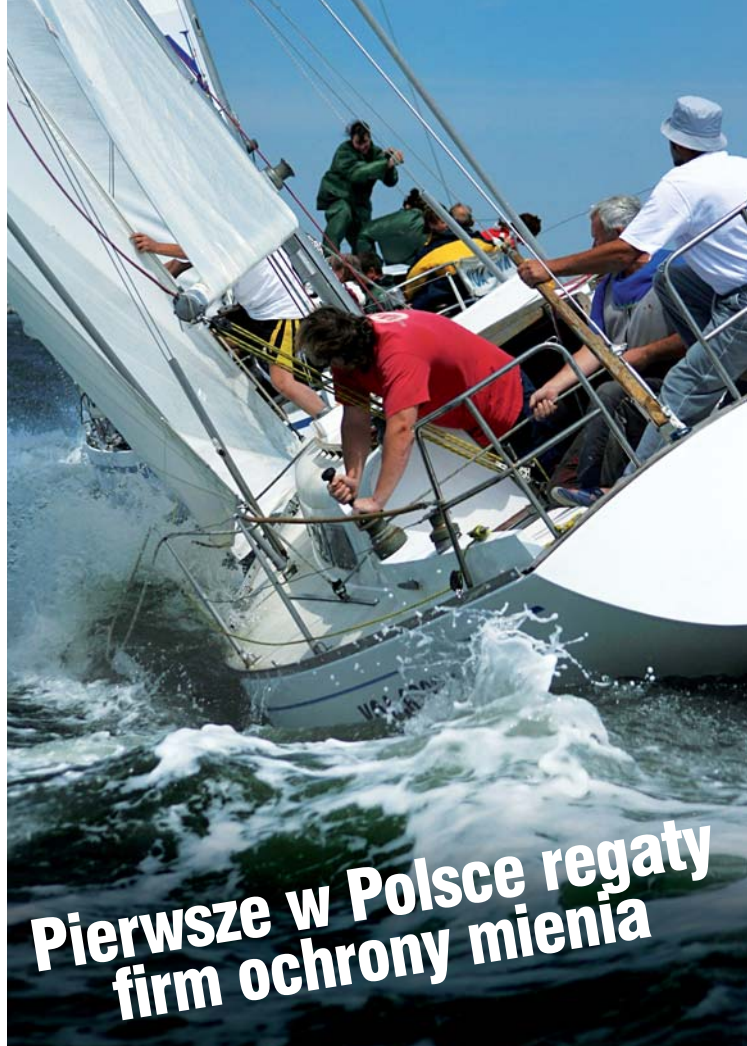
- noclegi,
- wyżywienie,
- łódki,
- opiekę instruktorów,
- profesjonalnie zorganizowane regaty.

Gwarantujemy:

- doskonałą zabawę!

Organizator

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



**Pierwsze w Polsce regaty
firm ochrony mienia**

Szczegółowe informacje i karty zgłoszenia:

www.polalarm.com.pl, polalarm@polalarm.com.pl
tel. (022) 626 90 31, (022) 625 57 43

15 maja 2008 r. **Panasonic System Solutions** świętował osiągnięcie historycznego wyniku sprzedaży **2 milionów sztuk kamery szybkoobrotowej serii Super Dynamic (SD)** od momentu wprowadzenia technologii Super Dynamic w 1997 r.

Technologia **Super Dynamic** została rozwinięta przez firmę Panasonic, aby pozwolić kamerom połączyć jakość obra-

tylko wyjątkowy 128-krotny zakres dynamiki, są one również wyposażone w procesor sygnałowy Super Dynamic, Auto Back Focus, naturalną reprodukcję kolorów, detekcję zmiany sceny oraz automatyczny stabilizator obrazu. Technologię SDIII można odnaleźć zarówno w kamerach analogowych serii WV-CP480 oraz w nagrodzonej serii kamer sieciowych

Kamera szybkoobrotowa Panasonic serii Super Dynamic osiągnęła sprzedaż 2 milionów sztuk



zu dla różnych prędkości migawki i tym samym prawidłowo odwzorowywać sceny o różnym poziomie oświetlenia. Jakość ta jest niedostępna dla kamer standardowych ze względu na ograniczony zakres dynamiki.

Obecnie, w trzeciej generacji, technologia **Super Dynamic III (SDIII)** zapewnia wyjątkowy poziom jakości i „inteligencji” generowanego obrazu. Kamery te wyróżnia nie

i-Pro (w takich modelach, jak WV-NS950 i WV-NW960).

Panasonic System Solutions ma nadzieję, że planowane na najbliższy czas nowe serie produktów powtórzą sukces technologii Super Dynamic, i planuje implementować do nich kolejne ulepszenia tej technologii.

TLUMACZENIE: PATRYK GAŃKO, REDAKCJA

Nowa strona WWW mieszkajbezpiecznie.pl

Każdy z nas instynktownie pragnie poczucia bezpieczeństwa w swoim własnym domu. Aby móc je sobie zapewnić, wyposażamy nasze mieszkania w różne zabezpieczenia. Elektroniczne urządzenia zabezpieczające to przede wszystkim systemy alarmowe, których główną rolą jest przekazanie informacji o wtargnięciu intruza.

Nowa strona internetowa www.mieszkajbezpiecznie.pl to źródło informacji o możliwościach alarmu, podstawowe informacje, które ułatwią poruszanie się w tym obszarze, jak również porady, odpowiedzi na pytania internautów, konfigurator sprzętowy, przykładowe rozwiązania, ciekawe artykuły i inne wskazówki.

Zabezpiecz swój dom – wejdź na www.mieszkajbezpiecznie.pl



Ambient System Sp. z o.o. zaprasza na trzecią już edycję konferencji naukowo-technicznych, w tym roku zatytułowaną:



DŹWIĘK I BEZPIECZEŃSTWO NA STADIONACH I W OBIEKTACH SPORTOWYCH

27 maja 2009, Hotel Gromada, Warszawa

Wśród zaproszonych prelegentów znajdą się przedstawiciele firm branżowych, a także eksperci z zakresu nagłośnienia, ewakuacji oraz zabezpieczeń obiektów sportowych.

Udział w konferencji jest bezpłatny. Liczba miejsc jest ograniczona. Wszystkich zainteresowanych prosimy o przesyłanie zgłoszeń na adres k.odachowska@ambientsystem.pl, więcej informacji znajdą Państwo wkrótce na www.ambientsystem.pl

ZNAMY SIĘ ZE SŁYSZENIA

Firma Bosch powiększa rodzinę modułów serii 420

Bosch Security Systems wprowadza dwa nowe moduły serii 420 do zastosowań w najnowszej, ulepszonej lokalnej sieci bezpieczeństwa (LSN), wykorzystywanej do komunikacji z centralami sygnalizacji pożarowej firmy Bosch.

Moduł FLM-420-I8R1-S, posiadający osiem wejść i jedno wyjście przekaźnikowe, umożliwia, w zależności od potrzeb, monitorowanie maks. ośmiu niezależnych wejść z rezystorami końca linii (EOL) lub bez nich. Posiada również przekaźnik ze stykami przełącznymi, stanowiący wyjście bezpotencjałowe (obciążalność maks. $30 V_{DC}/2 A$). Moduł FLM-420-RLV8-S jest wyposażony w osiem przekaźników ze stykami przełącznymi, stanowiących wyjścia bezpotencjałowe (obciążalność maks. $30 V_{DC}/2 A$).

W przypadku współpracy modułów serii 420 z centralą FPA 5000 możliwe jest wykorzystanie wszystkich nowych funkcji ulepszonej technologii LSN.

Wspólna dla wszystkich modułów serii 420 jest wytrzymała, łatwa w instalacji obudowa zawierająca hermetycznie obudowany układ elektroniczny. Podobnie jak pozostałe urządzenia LSN, moduły są wyposażone w obustronny izolator zwarcia. W przypadku zwarcia lub przerwy w pętli sieci LSN do centrali sygnalizacji pożarowej wysyłany jest komunikat o usterce. Nawet jeśli pętla utrzymuje obwód zwarty, dołączone elementy będą działały prawidłowo.



Nowe moduły interfejsu obsługują również topologie okablowania stosowane w ulepszonej sieci LSN, które mogą zawierać złożone struktury odgałęzień. W tego rodzaju konfiguracjach izolatory zwarcia muszą być stosowane w wybranych punktach odgałęzień.

Moduły serii 420 należą do produktów nowej generacji. W przypadku instalacji natynkowych moduły są dostępne w nowoczesnych obudowach do montażu powierzchniowego.

BEZPOŚR. INF. EMILIA DOBIES
BOSCH SECURITY SYSTEMS

Nowa marka na polskim rynku zabezpieczeń i ochrony przeciwpożarowej

W marcu tego roku dobiegł końca trwający od dwóch lat proces integracji firm ADT Poland oraz Tyco Fire and Integrated Solutions. Obie firmy połączyły się, by stworzyć wspólną, nową markę **ADT Fire and Security** i oferować nową na rynku jakość usług i unikatową ofertę rozwiązań umożliwiających kompleksową realizację nawet najbardziej złożonych i wymagających inwestycji.

Decyzja o połączeniu firm i zmianie marki wynika z globalnej strategii korporacji Tyco International (do której firmy przynależą), która dotyczy budowy jednostki biznesowej ADT Worldwide. Jej zadaniem jest dostarczanie klientom na całym świecie kompleksowych usług w dziedzinie bezpieczeństwa i ochrony życia. Logo, którym dotychczas posługiwały się obie firmy, zostało zastąpione nowym, wspólnym znakiem graficznym. Jest to niebieski ośmiokąt, kształtem nawiązujący do znaku drogowego „Stop”, który symbolizuje dążenie firmy do powstrzymania przestępczości oraz ochrony instytucji, firm, domów, rodzin i osób na całym świecie.

W wyniku integracji obu firm powstała unikatowa na rynku oferta uzupełniających się rozwiązań z zakresu elektronicznych systemów zabezpieczeń, ochrony przeciwpożarowej i sterowania ruchem ulicznym. ADT Fire and Security zapewni klientom kompleksową realizację projektów z zakresu



Fire & Security

instalacji niskoprądowych oraz szeroko rozumianej ochrony przeciwpożarowej, obejmującą zaprojektowanie, realizację, uruchomienie oraz konserwację i serwis dostarczonych rozwiązań.

ADT Fire and Security nadal pozostanie w strukturach grupy Tyco International i będzie korzystać z bogatego zaplecza inżynierskiego, technologicznego i finansowego międzynarodowego koncernu oraz ponad stutrzdziestoletniej tradycji organizacji ADT i Tyco Fire and Integrated Solutions. Ekspertki ADT Fire and Security będą pracować razem, dzieląc się wiedzą i doświadczeniem, a także zapewniając kompleksową realizację projektów na jeszcze wyższym poziomie.

BEZPOŚR. INF. KAROLINA OLECHOWICZ
ADT FIRE AND SECURITY

Nowe normy systemowe EN 50132

Systemy dozoru wizyjnego w całej Europie zapewnią wysoki, jednolity poziom funkcjonalności

Europejski Komitet Normalizacyjny Elektrotechniki CENELEC sformułował pierwszą część „Wymagań systemowych” normy **EN 50132** „Systemy CCTV stosowane w zabezpieczeniach” (**EN 50132-1**). Ustanawia ona ramy dla norm, którym będą podlegać systemy wizyjne. – *Normy oferują znaczące korzyści dla użytkowników oraz producentów systemów bezpieczeństwa. Ich efektem jest stymulacja rynków międzynarodowych do zrównoważonego wzrostu. Niezbędne jest jednakże, aby testy systemów bezpieczeństwa były przeprowadzane zarówno przez producentów, jak i instalatorów* – stwierdzili **Frank Rottmann** z działu **Bosch Security Systems** oraz przewodniczący grupy roboczej CENELEC zajmującej się systemami wizyjnymi. – *Firmy twierdzące, że ich produkty mogą być używane w systemach zgodnych z normą EN 50132-1, przekazują pierwszy komunikat o jakości oraz kluczowych cechach użytkowych* – powiedział Rottmann.

Nowa norma EN 50132-1 wprowadzi w życie ponad 100 podstawowych wymagań, z których wszystkie będą musiały być spełnione przez każdy system dozoru wizyjnego. Zdefiniowane zostaną znormalizowane, podstawowe specyfikacje techniczne systemu bezpieczeństwa, regulujące zapis obrazu, a także powiązane uprawnienia dostępu oraz zasady logowania. Ponad 60 dodatkowych wymagań dotyczyć będzie systemów instalowanych w miejscach o wysokim narażeniu środowiskowym. W celu uzyskania szerokiej akceptacji norm użytkownicy powinni dokładnie zdefiniować wymaganą klasę bezpieczeństwa dla swojego systemu, zaś producenci i instalatorzy powinni projektować, testować oraz opisywać systemy bezpieczeństwa zgodnie z wymaganiami normy EN 50132. Obowiązująca klasa bezpieczeństwa dla systemu jako całości lub poszczególnych elementów będzie mogła być określona przez użytkownika końcowego na podstawie metody szacowania ryzyka lub nadana przez ubezpieczyciela.

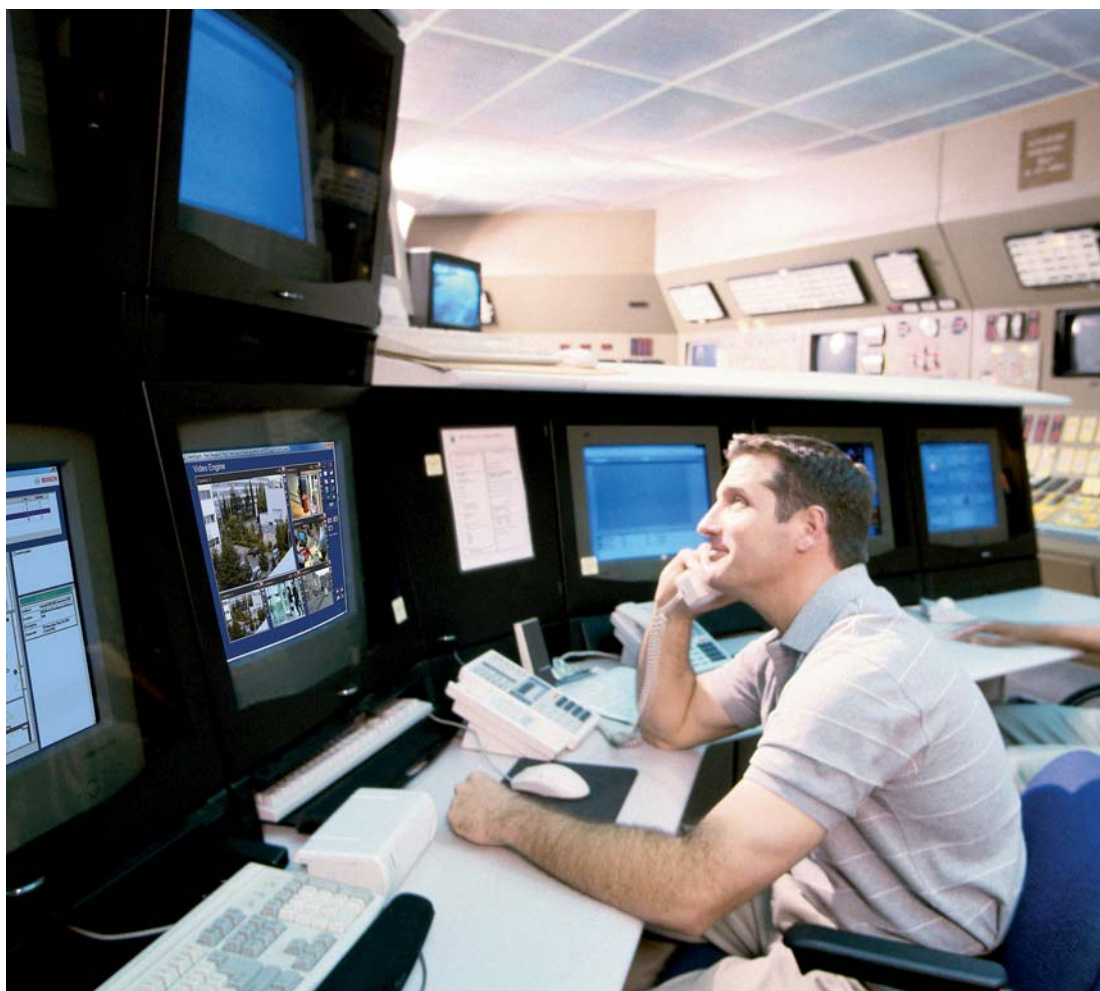
Zakładając szeroką akceptację europejskiej normy EN 50132, firma Bosch przewiduje wysoki oraz wspólny dla wszystkich poziom funkcjonalności systemów bezpieczeństwa w całej Europie dzięki zaledwie jednemu certyfikatowi. Wykorzystując systemy zgodne

z normami EN, nabywcy i osoby odpowiedzialne za bezpieczeństwo będą mieć pewność, że wszystkie zdarzenia są monitorowane, zapisywane i sygnalizowane oraz zadbane o niezawodność systemu, jego prawidłowe działanie i ochronę antysabotażową.

Europejskie normy EN 50132 stopniowo zastąpią istniejące normy krajowe. Będą obowiązywać także w tych krajach europejskich, które nie posiadają własnych uregulowań. W konsekwencji będzie można obiektywnie porównać różne systemy pod kątem jakości oraz funkcjonalności, umożliwiając użytkownikowi skupienie uwagi na wymaganiach operacyjnych już na etapie przetargu.

Nowe wersje normy teletransmisji (część 5) oraz wytycznych stosowania (część 7) na rok 2009 są kolejnymi etapami w procesie normalizacji produktów wizyjnych oraz harmonizacji przepisów europejskich. Frank Rottmann dostrzega dużą szansę na to, że normy EN zostaną przyjęte na poziomie międzynarodowym, a nie tylko w Europie. Cała seria norm jest aktualnie sprawdzana przez **Międzynarodową Komisję Elektrotechniczną (International Electrotechnical Commission – IEC)**.

BEZPOŚR. INF. EMILIA DOBIES
BOSCH SECURITY SYSTEMS



RISCO Group oferuje zintegrowany system wideo

W dniu 28 stycznia 2009 r. **RISCO Group**, wiodący producent zintegrowanych systemów bezpieczeństwa, ogłosił powstanie nowego zintegrowanego systemu telewizji dozorowej. Rozwiązanie to obejmuje systemową platformę zarządzania i bezpieczeństwa budynku **SynopSYS** oraz rodzinę sieciowych urządzeń **DVR**. System umożliwia osobom odpowiedzialnym za bezpieczeństwo obiektów zarządzanie zdarzeniami oraz dozorem wizyjnym w czasie rzeczywistym. Rozwiązania RISCO Group są idealne dla banków, uniwersytetów, różnych instytucji oraz obiektów przemysłowych czy handlowych.

SynopSYS umożliwia operatorowi systemu monitorowanie i kontrolę różnych urządzeń z jednego miejsca, przy użyciu uniwersalnego mechanizmu obsługi zdarzeń w czasie rzeczywistym. Jedną z głównych zalet zintegrowanego systemu RISCO Group jest możliwość połączenia kontroli dostępu i systemu sygnalizacji włamania z urządzeniami Net DVR, dzięki czemu użytkownik otrzymuje kompletny zestaw służący do zabezpieczenia obiektu.

Net DVR, zintegrowany z platformą SynopSYS, przechwytuje krytyczne sygnały wideo w sposób ciągły lub w odpowiedzi na alarmy systemu. Okna z wizualizacją wideo mogą zostać skonfigurowane tak, aby otwierały się automatycznie w momencie wystąpienia wcześniej zdefiniowanych zdarzeń. Istnieje również możliwość odpowiedniego pozycjonowania kamer PTZ w celu oglądania właściwego obszaru skorelowanego z danym zdarzeniem. Operator systemu SynopSYS otrzymuje wszechstronną informację wraz z wizualizacją, co pozwala mu na optymalizację procesu decyzyjnego. Dodatkowo można zdefiniować pewne automatyczne reakcje systemu w następstwie konkretnego alarmu, takie jak np. blokada wszystkich wyjść po nieupoważnionym wejściu. Net DVR pozwala na oglądanie zarejestrowanego lub bieżącego obrazu zarówno lokalnie, jak też zdalnie, poprzez sieć.

Rodzina urządzeń RISCO Group serii Net DVR Plus 7000 & 6000 to zaawansowane sieciowe i cyfrowe rejestratory wideo wykorzystujące technologię H.264. Analogowy sygnał wideo z kamery jest przetwarzany do postaci

cyfrowej z zachowaniem wysokiej jakości (aż 4CIF w czasie rzeczywistym w przypadku użycia algorytmu kompresji typu H.264). Net DVR jest przeznaczony do stabilnego i efektywnego oglądania oraz rejestrowania obrazu z prędkością do 30 (NTSC) lub 25 (PAL) klatek na sekundę dla każdej kamery przy zachowaniu bardzo wysokiej rozdzielczości. Łatwy do zainstalowania i prosty w obsłudze Net DVR pracuje zarówno jako autonomiczny system obsługujący do 16 kamer, jak też jako element rozległej sieci nadzoru.

BEZPOŚR. INF. RISCO GROUP POLAND

RISCO
GROUP Creating Security Solutions with Care.



Konferencja Samsung Techwin Vision Day 2009

relacja

Delegaci przybyli na konferencję **Samsung Techwin Vision Day 2009** wysłuchali oświadczenia dyrektora zarządzającego Samsung Techwin Europe, **Jake'a Kima**, który poinformował, że firma jest na najlepszej drodze do osiągnięcia czołowej pozycji w Europie wśród marek z dziedziny ochrony profesjonalnej. Prezes Samsung Techwin, **Chang Suk-Oh**, jeszcze raz potwierdził natomiast, że ochrona profesjonalna pozostaje podstawowym obszarem działalności firmy.

Obecnym podczas konferencji dystrybutorom i integratorom systemów przedstawiono nową paletę produktów oraz plan dalszego rozwoju firmy Samsung Techwin, zakładający wprowadzenie na przestrzeni kolejnych dwunastu miesięcy dużej liczby nowych produktów i zasadniczych technologii, w tym nowości w dziedzinie kamer sieciowych IP, kamer z kablem UTP oraz kablem koncentrycznym, a także imponującego rozwiązania w zakresie obserwacji automatycznej, jakim jest robot SGR-1.

Dyrektor Kim wyjaśnił, że Samsung Techwin dąży do kompleksowych rozwiązań, a wynikiem tych dążeń jest poszerzenie oferty o dziedzinę kontroli dostępu oraz technikę identyfikacji radiowej RFID. Dodał również, że w związku ze znacznymi inwestycjami Samsung Techwin w badania i rozwój w roku 2009 wprowadzone zostaną innowacje w zakresie technologii zasadniczych, takie jak technologia super-redukcji szumów Samsung (SSNR) trzeciej generacji oraz dwa zaawansowane technicznie zestawy układów scalonych do kamer W-5 i SV-5, które będą dostępne wyłącznie w kamerach i kamerach kopułkowych Samsung Techwin.

Firma Samsung Techwin zebrała w ciągu ostatnich dwunastu miesięcy profesjonalny i wykwalifikowany zespół ds. sprzedaży na Europę, który świadczy usługi przed- i posprzedażowe, tworząc, zdaniem Kima, najlepszy zespół działający obecnie w branży ochrony profesjonalnej. Produkty firmy są dostępne za pośrednictwem szerokiej sieci profesjonalnych dystrybutorów. Dodatkowym wsparciem jest własny, europejski magazyn zapasów. Ponadto wszystkie produkty objęto trzyletnią gwarancją.

Podczas konferencji, która odbyła się w dniach 5–6 marca w hotelu Sheraton na Teneryfie, delegaci mieli możliwość uczestnictwa w praktycznych prezentacjach najnowszych produktów i technologii firmy Samsung Techwin.

Szczegółowe informacje można uzyskać za pośrednictwem poczty elektronicznej, pisząc na adres e-mail STESecurity@samsung.com, lub telefonicznie, pod numerem +44 (0) 1932 45 5308.

Zapraszamy do odwiedzenia strony www.samsungcctv.com.

BEZPOŚR. INF. DAVID SOLOMONS
DRS MARKETING

Redakcja czasopisma *Zabezpieczenia* jeszcze raz serdecznie dziękuje organizatorom za zaproszenie na konferencję Samsung Vision Day 2009. Firmie Samsung Techwin życzymy sukcesów i pełnej realizacji zawodowych planów.



Mikrostrona o Pelco IP



W celu promocji technologii IP wśród swoich klientów **Pelco** stworzyło specjalną mikrostronę internetową, gdzie zebrano informacje o produktach IP znajdujących się w ofercie i nowościach, które zostaną niebawem wprowadzone do sprzedaży. Strona znajduje się pod adresem <http://www.pelco.com/IP> i jest regularnie aktualizowana. Zawiera informacje o stałych i uchylno-obrotowych kamerach IP pracujących w standardowej rozdzielczości (4CIF, 2CIF,

CIF) – Camclosure IP, IP3701H, Spectra IV IP i Spectra Mini IP – oraz o nowych kamerach megapikselowych Sarix, które wejdą do sprzedaży w drugim kwartale 2009 roku. Na stronie znajdują się również informacje o hybrydowych rejestratorach wideo z rodziny Digital Sentry oraz DVR5100.

BEZPOŚR. INF. NORBERT GÓRA
TAC

DS ControlPoint – zarządzaj rejestratorami Pelco

DS ControlPoint wersja 1.5 to nowy, rewolucyjny **graficzny interfejs** użytkownika, który pozwala użytkownikom zarządzać dowolną kombinacją rejestratorów analogowych i IP za pośrednictwem jednego oprogramowania klienckiego. **DS ControlPoint** komunikuje się z rejestratorami serii DX4500, DX4600, DX8000, DX8100 i Integral Digital Sentry, umożliwiając bezproblemową i stopniową migrację od analogowej telewizji dozorowej do IP. Nawigacja i sterowanie na wielomonitorowym stanowisku pozwala użytkownikowi na szybkie przełączanie się między kilkoma przestrzeniami roboczymi. Dostęp do wideo „na żywo” i materiału zarejestrowanego jest możliwy po przełączeniu się do odpowiedniej zakładki. Materiał wideo może być przeglądany



z wielu lokalizacji. Otwarta architektura zapewnia skalowalność, elastyczność i przyszłą integrację zaawansowanych zestawów funkcji.

Karta katalogowa i oprogramowanie do pobrania znajdują się na stronie <http://www.pelco.com>.

BEZPOŚR. INF. NORBERT GÓRA
TAC

7 lutego Automonitoring CMA uniemożliwił kradzież mercedesa Akcja odzyskania pojazdu trwała niecałą godzinę!



15 minut od otrzymania alarmu pracownik stacji **Centrum Monitorowania Alarmów** potwierdził u właściciela pojazdu jego zasadność, a następnie skontaktował się z Komendą Policji w Siemianowicach Śląskich.

Kolejne 30 minut wystarczyło funkcjonariuszom policji na dotarcie do dziupli, odzyskanie i zabezpieczenie pojazdu.

Udana akcja to powód do radości dla wielu osób. Niekwestionowanym zwycięzcą w tej grupie jest właściciel: odzyskał nieuszkodzony samochód, nie musiał tracić czasu na żmudne procedury ubezpieczeniowe i pieniędzy na zakup nowego pojazdu.

Niewątpliwie cieszyć się powinni też policjanci, którzy dzięki szybko podjętej akcji poprawili wykrywalność prze-

stępstw i udowodnili, że są niezastąpieni w takich sytuacjach.

Ubezpieczyciel pojazdu zaoszczędził na wypłacie kwoty ubezpieczenia, która, sądząc po marce, nie byłaby mała.

W grupie zadowolonych są oczywiście pracownicy Centrum Monitorowania Alarmów – dzięki niezawodności **Automonitoringu** mają pracę.

Z przyczyn oczywistych nie możemy podać do publicznej wiadomości większej liczby szczegółów dotyczących akcji, za co bardzo przepraszamy.

BEZPOŚR. INF. MAGDALENA KALINOWSKA
CMA



Aktywna działalność na rynku polskim i zagranicznym, stałe poszerzanie oferty i reagowanie na głosy klientów gwarantują dynamiczny rozwój firmy **SATEL**.

Rok 2008 obfitował w rekordową liczbę targów zagranicznych, w których firma **SATEL** brała czynny udział. Zaprezentowaliśmy aktualną ofertę, w tym wiele nowości, które spotkały się z dużym zainteresowaniem odwiedzających.

Liczba odbiorców naszych urządzeń spoza Polski stale rośnie. Rozwój tej sfery działalności zawdzięczamy umiejętności dopasowywania się do indywidualnych wymagań rynku.

Nasi projektanci pracują nad kolejnymi urządzeniami, które mają za zadanie spełnić oczekiwania stałych i nowych klientów na całym świecie. Dzięki temu oferta przeznaczona na rynek polski i zagraniczny stale się powiększa. Aktualnie wachlarz produktów to już prawie 300 pozycji.

Stały wzrost zapotrzebowania na produkty **SATEL** zaowocował rozbudową budynku przy ul. Budowlanych 66 w Gdańsku. Aktualnie powierzchnia produkcyjna, magazynowa i biurowa wzrosła do 14000 m². Otwarcie nowej części hali odbyło się na początku stycznia 2009 roku

Zasadniczym celem firmy **SATEL** jest tworzenie warunków do dalszego dynamicznego rozwoju eksportu. Eksport traktowany jest jako jeden z podstawowych priorytetów działalności i siła napędowa.

Nowe inwestycje i plany rozwojowe mają pomóc utrzymać tempo rozwoju wbrew trudnej sytuacji gospodarczej na świecie. W obecnych warunkach możliwe jest kilkukrotne zwiększenie potencjału produkcyjnego i znaczące zwiększenie wydajności. Powiększona niemal trzykrotnie powierzchnia magazynowa pozwala na posiadanie większej liczby gotowych produktów, które zaspokoją rosnące zapotrzebowanie na wyroby firmy **SATEL**.

Nasz rozwój zawdzięczamy zaufaniu, jakim obdarzyli nas nasi klienci, za które serdecznie dziękujemy. To państwa uwagi i sugestie powodują, że możemy wprowadzać na rynek nowe produkty, wpływać na rozwój branży zabezpieczeń i być może nadawać jej kierunek nie tylko na rynku krajowym.

BEZPOŚR. INF. AGNIESZKA NOCŃ
SATEL

VERSO POLAR – kamery chronione nawet w arktycznym zimnie

Videotec, producent zewnętrznych rozwiązań dla telewizji dozorowej, proponuje obudowę nadającą się do zainstalowania w temperaturach sięgających **-55 stopni Celsjusza**. Dobrze znana seria obudów **VERSO**, wytworzonych z twardego polimeru technicznego, została poszerzona o **model POLAR**. Jest on wyposażony w wydajny system grzewczy oraz mosiężny, pokryty niklem przepust kablowy. Dzięki temu jest odporny na pracę w najniższych temperaturach.

Boczne otwieranie umożliwia łatwy dostęp do kamery oraz obiektywów i pozwala na łatwe podłączenie kamery. Co więcej, **Videotec** oferuje różne wersje zapewniających ochronę przed wandalami obudów **VERSO POLAR** – zarówno do montażu ściennego, jak i z wewnętrznym przepustem kablowym.

BEZPOŚR. INF. **VIDEOTEC**
TŁUMACZENIE: REDAKCJA

versopolar
SIDE OPENING HOUSING





Uroczyste otwarcie

Zespołu Laboratoriów Systemów Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie

W dniu 6 marca 2009 r. w Sali Senatu Wyższej Szkoły Menedżerskiej (WSM) w Warszawie nastąpiło uroczyste otwarcie Zespołu Laboratoriów Systemów Bezpieczeństwa, którego dokonał rektor WSM prof. zw. dr hab. Brunon Hołyst – światowej sławy naukowiec, specjalista do spraw kryminalistyki, kryminologii, niekwestionowany autorytet w środowiskach kryminalistycznych, a także autor ponad 900 publikacji z dziedziny kryminalistyki i kryminologii.

Architektami i autorami Zespołu Laboratoriów Systemów Bezpieczeństwa, jak również twórcami jednej z czterech istniejących specjalności na Wydziale Informatyki Stosowanej – Bezpieczeństwo Obiektów i Informacji – są doc. dr inż. Waldemar Szulc (Dziekan Wydziału Informatyki Stosowanej i jednocześnie Kierownik Zakładu Bezpieczeństwa Obiektów i Informacji, wieloletni pracownik naukowy Politechniki Warszawskiej na Wydz. Komunikacji, Elektroniki i Wydz. Transportu, a także Wojskowej Akademii Technicznej na Wydz. Elektroniki) oraz dr inż. Adam Rosiński (pracownik naukowy Politechniki Warszawskiej na Wydz. Transportu, Wojskowej Akademii Technicznej na Wydz. Elektroniki i Wyższej Szkoły Menedżerskiej na Wydz. Informatyki Stosowanej).

Podczas swojego krótkiego wystąpienia Waldemar Szulc opowiedział zebranym o tym, jak powstało laboratorium, jak wielkiego nakładu pracy oraz wiedzy wymagało napisanie programu oraz rozbudowa przedmiotów dotyczących miernictwa i elektroniki dla informatyków, a także o perspektywach dalszej rozbudowy laboratorium, czyli o stworzeniu nowych stanowisk służących do kontroli dostępu, systemów sygnalizacji pożarowej, budynków inteligentnych, systemów zintegrowanych oraz biometrycznych.

Projekt laboratorium powstał na przełomie 2007/2008, a jego realizacja nastąpiła w 2008/2009 – w wyniku porozumienia WSM w Warszawie z kilkoma firmami, które zdecydowały się sponsorować to przedsięwzięcie. Jednym z głównych sponsorów jest firma Satel z Gdańska, która wyposażyla laboratorium w aktualnie produkowane urządzenia, które umożliwiły uruchomienie siedmiu stanowisk dydaktycznych dla studentów. Stanowiska te są programowane i zarządzane za pomocą komputerów wyposażonych w odpowiednie oprogramowanie, które również dostarczyła firma Satel.

Firma Sony wyposażyla laboratorium w 21 nowoczesnych kamer telewizyjnych, zarówno analogowych, jak i cyfrowych,

w tym pięć kamer IP. Ponadto Sony przekazało cztery wideoserwery. Powstały cztery stanowiska systemu monitoringu wizyjnego, nadzorowane komputerowo i wyposażone w program Real Shot Manager (licencja dla 32 kamer). Powstało również czterokamerowe klasyczne stanowisko wyposażone w ośmiowejściowy multiplexer (jedna z kamer posiada łącze mikrofalowe pracujące na częstotliwości 2,4 GHz). Warto również nadmienić, że kolejnym stanowiskiem monitoringu wizyjnego jest wysokiej jakości kamera IP wyposażona w szybką głowicę obrotową. Łącznie daje to sześć stanowisk monitoringu wizyjnego.

Kolejny sponsor to firma Altram, która współpracuje z Sony Poland. Firma Altram wyposaża większość analogowych kamer telewizyjnych w obiektywy stało- i zmienneogniskowe.

Podziękowania należą się firmie Astral z Warszawy, która pomogła w logistyce budowy laboratorium, jak również w szkoleniu studentów specjalności Bezpieczeństwo Obiektów i Informacji. Firma Astral pomogła również w kompletowaniu specjalistycznych narzędzi, niezbędnych podczas konfigurowania elektronicznych systemów bezpieczeństwa, które stały się wyposażeniem laboratorium.

Słowa podziękowania należą się również firmie Multisystem.

Wszystkie stanowiska wchodzące w skład Zespołu Laboratoriów Systemów Bezpieczeństwa mają połączenie z zainstalowanym wysokiej jakości rzutnikiem multimedialnym firmy SONY i umożliwiają edycję różnych zdarzeń na ekranie na terenie laboratorium. Cały Zespół Laboratoriów Systemów Bezpieczeństwa jest nadzorowane przez centralny komputer. W trakcie tworzenia Zespołu Laboratoriów Systemów Bezpie-

czeństwa niezwykle ważna była budowa sieci informatycznej oraz przebudowa instalacji energetycznej.

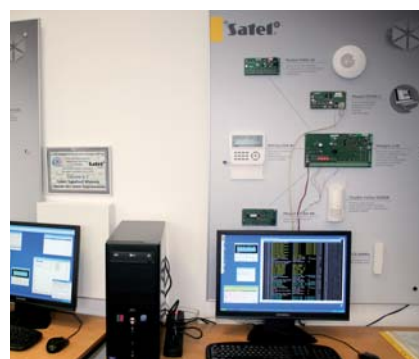
Na zakończenie imprezy głos zabrał rektor WSM – prof. dr hab. Brunon Hołyst, który serdecznie podziękował wszystkim zaproszonym gościom i zaprosił do zwiedzenia laboratorium. Po przecięciu wstęgi zaproszeni goście zwiedzili laboratorium. Doc. dr inż. Waldemar Szulc oraz dr inż. Adam Rosiński oprowadzali zwiedzających i odpowiadali na wszystkie ich pytania. Wszystkie stanowiska laboratoryjne były uruchomione i czynne. Odbył się pokaz działania wszystkich stanowisk dydaktycznych. Wszyscy zwiedzający wyrażali się bardzo pozytywnie o nowo otwartym Zespole Laboratoriów Systemów Bezpieczeństwa i życzyli dalszych sukcesów.

W imieniu całej redakcji życzę powodzenia i wielu sukcesów pomysłodawcom projektu oraz studentom uczelni. Wiedza, jaką studenci zdobędą podczas ćwiczeń w nowo powstałych laboratoriach, z pewnością przyczyni się do lepszego zrozumienia działania urządzeń i całych systemów, co zaowocuje w przyszłej pracy w branży zabezpieczeń.

**OPRACOWAŁA
TERESA KARCZMARZYK**

Pan Waldemar Szulc przesłał do redakcji *Zabezpieczeń* serdeczne podziękowania za pomoc w promowaniu na łamach czasopisma powstałej specjalności Bezpieczeństwo Obiektów i Informacji na Wydziale Informatyki Stosowanej w Wyższej Szkole Menedżerskiej w Warszawie.

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





LOTNISKO 2009 relacja

Zarząd Targów Warszawskich był organizatorem **II Konferencji „Lotnisko 2009”**. W kulisach zorganizowano niewielką wystawę prezentującą ofertę kilku firm, wśród których były firmy reprezentujące naszą branżę, takie jak Gunnebo Polska oraz Kabe Systemy Alarmowe, które w swojej ofercie posiadają między innymi urządzenia mogące mieć zastosowanie np. w ochronie lotnisk.

Tegoroczna edycja konferencji miała na celu promocję i popularyzację zagadnień związanych z planami budowy, modernizacji, a także wyposażenia lotnisk oraz infrastruktury lotniskowej i okołołotniskowej w Polsce.

Swoim zakresem tematycznym impreza objęła trzy panele dyskusyjne:

- **budowa, rozbudowa i modernizacja lotnisk w Polsce** (program budowy i rozbudowy lotnisk w Polsce, nowoczesne technologie wykorzystywane w obsłudze i do modernizacji lotnisk i infrastruktury okołołotniskowej

oraz finansowanie budowy i przebudowy lotnisk),

- **bezpieczeństwo transportu lotniczego podczas organizacji mistrzostw EURO 2012** (analiza bezpieczeństwa ruchu lotniczego, organizacja ruchu lotniczego podczas EURO 2012, nowoczesne systemy wspomagające bezpieczeństwo, zagrożenia terrorystyczne),
- **kadra lotnicza w Polsce** (stan aktualny i perspektywy rozwoju, szkolenia pilotów i kadry lotniczej lotnictwa cywilnego).

Prezes Urzędu Lotnictwa Cywilnego Grzegorz Kruszyński wygłosił referat dotyczący transportu lotniczego w Polsce. Omówił statystyki przewozów pasażerskich w podziale na poszczególne porty lotnicze oraz przewoźników z nich korzystających. Zwrócił uwagę na znacznie większą sezonowość ruchu lotniczego w porównaniu z ogólnym rozwojem gospodarczym kraju oraz widoczny wzrost koncentracji rynku wśród największych operujących w Polsce przewoźników.





Przedstawiciel firmy Kabe – Kazimierz Bulandra – w swoim wystąpieniu przedstawił nowoczesne systemy radarowo-kamerowe, które spełniają wymagania obowiązujących przepisów, mogące mieć zastosowanie w ochronie lotnisk cywilnych. Zastosowanie jednostek radarowych sterujących kamerami nadzoru wizyjnego umożliwia, jak stwierdził Bulandra, dokładne skanowanie całego chronionego obszaru, antycypację wtargnięcia dzięki zautomatyzowanej obserwacji terenu poza ogrodzeniem, a po ewentualnym przekroczeniu przez intruza ogrodzenia – określenie jego aktualnej lokalizacji z dokładnością do pół metra.

Bartłomiej Kędzia z firmy Gunnebo Polska wygłosił referat pt. „Zabezpieczenia antyterrorystyczne lotnisk i kontrola dostępu”.

Marcin Łandwajt z Instytutu Technologii Bezpieczeństwa „Moratex” zaprezentował osobisty zestaw kuloodporny (innowacyjne rozwiązanie służące do indywidualnej ochrony

ciała, przeznaczone dla żołnierzy i funkcjonariuszy wchodzących w skład zespołów pierwszego uderzenia, narażonych na bezpośrednie ostrzeliwanie przy likwidacji grup terrorystycznych), wielofunkcyjną osłonę balistyczną (zabezpieczenie funkcjonariuszy przed działaniem pocisków wystrzeliwanych z broni strzeleckiej krótkiej oraz odłamków urządzeń wybuchowych) oraz sztywną osłonę przeciwybuchową (przeznaczoną do zabezpieczenia niezidentyfikowanych ładunków znajdujących się w miejscach publicznych: na dworcach kolejowych, stadionach, lotniskach, w budynkach administracji publicznej, centrach handlowych itp.).

Zarząd Targów Warszawskich oraz Agencja Lotnicza ALTAIR zapraszają do wzięcia udziału w V Międzynarodowej Konferencji „Nowoczesne technologie dla bezpieczeństwa kraju i jego granic”, która zaplanowana jest na **14 maja 2009 roku**.

REDAKCJA





18 lutego 2009 r. w siedzibie firmy **Sony Poland** odbyła się prezentacja kamer megapikselowych. Pokaz podzielono na dwie części: teoretyczną i praktyczną. Część teoretyczną poprowadziła Marta Małecka (kierownik sprzedaży), która przedstawiła zalety i wady kamer megapikselowych, a także zwróciła uwagę słuchaczy na problemy wynikające z ich zastosowania. Istotnym elementem części teoretycznej było przedstawienie nowych funkcji, jakie pojawiły się w kamerach megapikselowych firmy Sony. Można do nich zaliczyć między innymi połączenie zaawansowanego przetwornika CCD Progressive Scan z technologią ExwavePRO, co zapewnia absorpcję znacznie większej ilości światła niż w standardowych rozwiązaniach. Dzięki temu wzrasta czułość, a dodatkowo uzyskane obrazy charakteryzują się większą ostrością i nasyceniem barw. Kolejna nowość – funkcja Light Funnel – pozwala na czterokrotne zwiększenie czułości kamery bez zwiększania czasu naświetlania (wydłużania czasu otwarcia migawki).

Część praktyczną prezentacji poprowadziła Diana Jesionek (konsultant ds. rozwiązań profesjonalnych). Każdy z uczestników mógł sprawdzić, jak działają nowe funkcje kamer w systemie. Uczestników pokazu zainteresowała prezentacja zwiększenia czułości kamer przy wykorzystaniu funkcji Light Funnel. Każdy z uczestników mógł sprawdzić działanie inteligentnej detekcji ruchu, automatycznie wykrywającej zdefiniowane obiekty przy jednoczesnym ignorowaniu zakłóceń tła. Inteligentna detekcja ruchu umożliwia,

GO Mega show

Prezentacja kamer megapikselowych firmy Sony



oprócz standardowych funkcji, m.in. analizę takich zdarzeń, jak: pozostawienie przedmiotu (np. walizki, torby), detekcja kradzieży (zniknięcie obiektu), przekroczenie określonej strefy (wtargnięcie do chronionego obszaru).

Więcej informacji o produktach firmy Sony znajdą Państwo na stronie internetowej <http://www.sonybiz.pl/>.

BEZPOŚR. INF. REDAKCJA

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



New Security

Relacja z targów w Belgii

W dniach 14–16 stycznia 2008 r. miasto Louvain w aglomeracji Brukseli w Belgii gościło wystawców oraz uczestników targów branży zabezpieczeń **New Security**.

Targi zorganizowano w centrum wystawienniczym Brabantia znajdującym się w południowo-wschodniej części miasta w pobliżu obwodnicy. Sama nazwa centrum nawiązuje do średniowiecznego księstwa Brabancji, obecnie prowincji Brabancja Flamandzka ze stolicą w Louvain. Znakiem rozpoznawczym miasta jest słynny, a zarazem najstarszy w Belgii i krajach Beneluksu Katolicki Uniwersytet Lwański, założony w 1425 roku, z którym związanych było wielu wybitnych Polaków.

Targi New Security odbywają się w cyklu rocznym i mają lokalny charakter. Zdecydowana większość uczestników i wystawców, mimo bliskości granic Holandii, Luksemburga, Francji czy też Niemiec, pochodziła z Belgii.

W targach uczestniczyło 42 wystawców, których oferta obejmowała ściśle techniczne systemy zabezpieczeń.

Pod względem wielkości stoisk i liczby osób obsługujących klientów na targach dominowali najwięksi dystrybutorzy/producenti sprzętu zabezpieczeń: ADI-Gardiner, Norbain, Bosch, JVC.

Pozostałymi uczestnikami targów byli lokalni dystrybutorzy, agencje ochrony, producenci rozwiązań software'owych oraz przedstawiciele prasy branżowej.

Niewielka liczba wystawców–dystrybutorów podczas targów może świadczyć o tym, że, w przeciwieństwie do rynku zabezpieczeń w Polsce, rynek zabezpieczeń w Belgii składa się wyłącznie z kilku dużych firm dystrybucyjnych.

Wśród zwiedzających wystawę najwięcej było przedstawicieli firm instalatorskich.

Wystawcy i dystrybutorzy zabezpieczeń szacują belgijski rynek instalatorski na ok. 600 firm.

Podczas wystawy nie można było spotkać żadnych przypadkowych osób zwiedzających czy też planujących założenie pojedynczego systemu na własne potrzeby. Podobne procesy będzie można zaobserwować w najbliższym czasie na polskim rynku, a nadchodzące spowolnienie gospodarcze może je jeszcze bardziej przyspieszyć.

Ze względu na małą liczbę wystawców i uczestników targi miały charakter salonu – miejsca spotkań i dyskusji znanych sobie osób z branży. Były dobrze zorganizowane (np. każdy z wystawców standardowo posiadał bezprzewodowy dostęp do Internetu).

Na perspektywy rynku zabezpieczeń, który jest bardzo mocno związany z rynkiem nieruchomości, niewątpliwie cieniem kładzie się obecny kryzys. Jego wpływ na sytuację w branży w 2009 r. był jednym z częściej pojawiających się w rozmowach tematów wśród wystawców i instalatorów.

BEZPOŚR. INF. REDAKCJA



GUNNEBO

For a safer world®



Tripody

Bezpieczny stadion



Kołowroty, furty



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

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

Zwiększ swoje możliwości.
Wypredź innych, pracuj z najlepszym
oprogramowaniem na rynku.

Sony wprowadza na rynek telewizji przemysłowej rozwiązanie hybrydowe pozwalające na łatwą integrację nowych sieciowych i starych analogowych rozwiązań po to, aby powstała instalacja, która dziś i jutro będzie zapewniała bezpieczeństwo.

Najnowsza wersja oprogramowania Sony Real Shot Manager – RSM Advanced, przeniesie twoją telewizję przemysłową na wyższy poziom, gdzie będziesz mógł wykorzystywać analizę obrazu w czasie rzeczywistym połączoną z automatyczną detekcją zagrożeń w celu zapewnienia najwyższej ochrony. Dzięki innowacyjnej, Inteligentnej Detekcji Przedmiotów oraz Inteligentnej Detekcji Ruchu automatycznie

włączają się alarmy, uruchamia się oświetlenie, a drzwi otwierają się lub zamykają. Zminimalizowana liczba fałszywych alarmów w połączeniu z aktywną inteligencją, wyszukującą podejrzane obiekty lub osoby, dają doskonały efekt w przypadku realnych zagrożeń – wykrywając je i pozwalając na ich szybkie usunięcie. Podobnie jak w podstawowej wersji doskonale znanego oprogramowania Real Shot Manager, interfejs użytkownika jest niezwykle prosty i intuicyjny, ułatwiający korzystanie ze wszystkich funkcji podglądu, nagrywania, odtwarzania oraz konfiguracji. Oto powody, dla których Real Shot Manager to najlepszy wybór. Aby dowiedzieć się więcej wejdź na: www.sonybiz.pl

Unikalna hybrydowa technologia zaprojektowana z myślą o bezpieczeństwie



SONY

GO ADVANCE

MIGRACJA → ROZWÓJ → ZAPIS → PODGLĄD → OBRAZ

KAMERY ANALOGOWE

GO HYBRID

KAMERY IP

Nocne oświetlanie obiektów monitorowanych przez systemy telewizji dozorowej

Trudno przecenić rolę światła w systemach telewizji dozorowej. Bez jego udziału nie byłoby możliwe wytworzenie jakichkolwiek obrazów. Za sprawą światła świat staje się widzialny, zarówno dla ludzkiego oka, jak i dla przetworników kamer telewizyjnych. Poprawne działanie każdego systemu telewizyjnego zależy od jakości i równomierności oświetlenia obserwowanych scen. Lokalizacja źródła światła oraz jego intensywność decydują o wyglądzie obserwowanych obiektów. W wielu przypadkach przesądza o tym, czy dany obiekt w ogóle będzie widoczny, czy utonie w przysłowiowym mroku

Jak powszechnie wiadomo, widzialny fragment widma promieniowania świetlnego odpowiada długościom fal elektromagnetycznych mieszczącym się w zakresie od 400 nm do 700 nm. Emisje o długościach fal wykraczających poza ten zakres nie są zauważane przez oczy ludzkie, ale mogą być rejestrowane przez kamery telewizyjne. Promieniowanie ultrafioletowe, szczególnie w przypadku długotrwałego naświetlania, może być szkodliwe dla zdrowia ludzkiego, dlatego kamery uczulone na fale krótsze niż 400 nm rozpowszechniły się jedynie w specjalistycznych aplikacjach przemysłowych. Tymczasem promieniowanie podczerwone, nawet bardzo intensywne, nie ma negatywnego wpływu na funkcjonowanie organizmów ży-

wych i między innymi z tego powodu znajduje zastosowanie w systemach technicznej ochrony mienia.

Systemy klasyczne, czyli praca w świetle białym

Osobnym zagadnieniem jest poprawna reprodukcja barw w systemach monitoringu telewizyjnego, którą najprościej osiągnąć, stosując oświetlenie światłem białym. Przez światło białe rozumie się emisję odznaczającą się pewnym charakterystycznym, ciągłym rozkładem energii w całym widmie widzialnym, ale nie jest to zbyt ścisła i jednoznaczna definicja. Światło białe pochodzące z różnych źródeł może mieć pewne cechy indywidualne.



Drastycznym przykładem negatywnym mogą tu być niskociśnieniowe lampy sodowe, masowo stosowane w latarniach ulicznych, których emisja niczym nie przypomina światła białego. Widmo ich promieniowania ma charakter prążkowy, a więc jest pozbawione ciągłości i ma wyraźną żółtą dominantę. W takim oświetleniu szczególnie źle spisują się kamery kolorowe, wymagające do swojej pracy oświetlenia o widmie ciągłym i barwie możliwie zbliżonej do białej.

Użycie oświetlenia, którego barwa znacznie odbiega od bieli, powoduje istotne pogorszenie jakości kolorowego obrazu telewizyjnego. Śmiało można stwierdzić, że każda kamera pracuje na tyle dobrze, na ile pozwala jej jakość oświetlenia obserwowanej sceny.

Systemy pracujące w świetle podczerwonym

Widmo światła podczerwonego nie zawiera żadnego z kolorów składających się na światło białe, co całkowicie wyklucza zastosowanie kamer kolorowych do dyskretnej obserwacji nocnej. Ten zakres emisji może być wykorzystywany wyłącznie przez kamery monochromatyczne lub specjalnie do tego przystosowane kamery z funkcją „dzień – noc”. Obrazy telewizyjne powstające z wykorzystaniem światła podczerwonego są z definicji monochromatyczne, niezależnie od rodzaju użytej kamery.

Ze względów praktycznych w telewizji dozorowej nie stosuje się promieniowania podczerwonego o długości fali przekraczającej 1000 nm. W miarę oddalania się od tej wartości klasyczne kamery telewizyjne wykazują coraz niższą czułość, pojawiają się także problemy z konstrukcją dobrze działających obiektywów. Jako granicę zastosowań praktycznych przyjmuje się fale o długości od 900 nm do 950 nm.

Aspekty praktyczne

Pierwszym problemem, z którym muszą się zmierzyć projektanci systemów telewizji dozorowej, jest konieczność wyboru trybu pracy kamer w warunkach nocnych. Często zdarza się, że użytkownik końcowy preferuje tryb kolorowy, co wiąże się z koniecznością całonocnego oświetlenia terenu światłem białym. W wielu przypadkach, z zupełnie innych względów, światło białe wykorzystuje się jako podstawowe oświetlenie nocne. Jego użycie przyczynia się do wzrostu ogólnego poziomu bezpieczeństwa, a także ułatwia pracę osobom sprawującym nadzór nad danym obszarem. Światło białe stwarza dobre warunki pracy dla kamer telewizyjnych, zarówno monochromatycznych, jak i kolorowych, jednakże musi ono mieć odpowiedni rozkład widmowy, który pozwoli na poprawną reprodukcję barw.

W sytuacjach, gdy oświetlenie światłem białym mogłoby okazać się zbyt natrączywe (w niektórych krajach problem ten jest uregulowany prawnie), a także w sytuacjach, w których wymagane jest zachowanie dyskrecji, użycie światła podczerwonego staje się koniecznością.

W systemach telewizji dozorowej światło podczerwone wykorzystuje się jako dyskretne nocne oświetlenie obserwowanych przestrzeni. Nawet w przypadku użycia źródeł o dużej mocy nie wywołuje ono nieprzyjemnych efektów wzrokowych, typowych dla bardzo jasnego światła białego.

Pomimo tego, że światło podczerwone jest niewidzialne dla ludzkich oczu, bezpośrednia obserwacja promienników podczerwieni stosowanych w systemach telewizji dozorowej może wywoływać pewne wrażenia wzrokowe. Maksimum gęstości widma emitowanego przez te promienniki przypada na zakres niewidzialny, jednakże emitują one pewną



część energii na krańcu widma widzialnego, dlatego stają się widoczne. Z praktyki wynika, że:

- działanie oświetlaczy pracujących w zakresie od 715 nm do 730 nm jest wyraźnie widoczne; w warunkach nocnych efekt jest podobny do działania światła sygnalizacji ulicznej;
- oświetlacze pracujące w zakresie od 815 nm do 850 nm wytwarzają rodzaj delikatnej czerwonej poświaty, jednak nadal, szczególnie w nocy, ich działanie jest wyraźnie widoczne;
- oświetlacze pracujące w zakresie od 940 nm do 950 nm nie wytwarzają żadnej poświaty zauważalnej dla ludzkich oczu.

Przejdźmy teraz do omówienia różnego rodzaju sztucznych źródeł światła, stosowanych w telewizji dozorowej.

Lampy żarowe

W zastosowaniach związanych z telewizją dozorową lampy żarowe wykazują pewne wady. Mają one ograniczoną żywotność, a ponadto są energochłonne. Typowa moc pojedynczego oświetlacza wynosi około 500 W, zaś dla zachowania ciągłości pracy konieczna jest wymiana żarników przeciętnie trzy razy do roku. Z tych względów eksploatacja lamp żarowych jest droga i uciążliwa.

Klasyczne żarówki są relatywnie starym wynalazkiem i odznaczają się bardzo niską sprawnością energetyczną. Około 90% swojej mocy tracą na wytwarzanie ciepła, przez co rozgrzewają się do wysokiej temperatury, co zmusza do stosowania odpowiednich opraw.

Żarówki halogenowe mają wyższą sprawność, lecz nadal tracą około 85% swojej mocy na wytwarzanie ciepła. Są one mniejsze od zwykłych żarówek, ponadto są wypełnione mniej rozrzedzonym gazem, przez co rozgrzewają się do jeszcze wyższych temperatur, stwarzając niebezpieczeństwo poparzenia obsługujących je osób.

Zarówno w przypadku klasycznych żarówek, jak i lamp halogenowych mamy do czynienia z emisją światła odbiegającego swoim rozkładem widmowym od tego, co przyjęło się uważać za światło białe. Występuje tu wyraźna dominanta barw żółtej i czerwonej, jednakże ze względu na ciągłość widma współczesne kamery kolorowe są w stanie skompensować powstałe rozbieżności i poprawnie reprodukcować barwy. Było to niemożliwe w przypadku lamp sodowych, emitujących widmo prążkowe.

Świetlówki

Głównym czynnikiem ograniczającym stosowanie świetlówek w systemach telewizji dozorowej jest uciążliwe zjawisko migotania. Jest ono niemal niedostrzegalne dla ludzkiego oka, lecz wpływa negatywnie na pracę kamer telewizyjnych. Co prawda najnowsze ich modele są na to przygotowane i dysponują opcjami pozwalającymi na redukcję szkodliwego wpływu migotania na jakość wytwarzanego obrazu, niemniej jednak zjawisko nadal istnieje i może na przykład powodować efekty stroboskopowe, utrudniające obserwację obiektów ruchomych. Świetlówki mają przeważnie małą moc i są stosowane do oświetlania przestrzeni wewnętrznej budynków. Ich znaczne rozmiary utrudniają konstrukcję reflektorów ogniskujących światło w wąskim kącie promieniowania.

Zaletą świetlówek jest wysoka sprawność energetyczna, dochodząca do 40%. W porównaniu ze zwykłymi żarówkami

o zbliżonej mocy wytwarzają one znacznie więcej światła i nie rozgrzewają się do tak wysokich temperatur. Jeśli dodać do tego ich wysoką trwałość, trudno się dziwić, że są one masowo stosowane w gospodarstwach domowych jako podstawowe źródło światła elektrycznego.

W sensie widmowym świetlówki emitują światło pozwalające na poprawną reprodukcję barw. Z tego względu mogą być wykorzystywane jako oszczędne źródła światła przy oświetleniu ogólnym o niewielkiej mocy pojedynczego punktu świetlnego. Poza tą funkcją ich stosowanie w systemach telewizji dozorowej jest ograniczone.

Lampy metalowo-halidowe

Popularność tego typu lamp w Polsce była dotychczas niewielka. Przyczyniała się do tego ich słaba dostępność, wysoka cena oraz brak odpowiednich publikacji wyjaśniających ich działanie, jednakże obecnie ogromne zalety eksploatacyjne tego typu lamp powodują wzrost zainteresowania nimi projektantów i instalatorów systemów monitoringu wizyjnego.

Ze względu na swoją zasadę działania lampy metalowo-halidowe należą do grupy lamp wyładowczych. Ich zaletami są: wysoka sprawność energetyczna, odpowiedni rozkład widmowy emitowanego światła oraz duża trwałość, dochodząca do 12 tys. godzin. Wszystko to czyni je wysoce przydatnymi do zastosowań w systemach telewizji przemysłowej.

Sprawność energetyczna lamp metalowo-halidowych zawiera się w przedziale od 60% do 80%. Emitują one światło białe o rozkładzie widmowym pozwalającym na bardzo dobrą reprodukcję barw. W porównaniu z klasycznymi żarówkami lub świetlówkami lampy metalowo-halidowe mają niewielkie rozmiary, co ułatwia konstrukcję opraw i reflektorów.

Oświetlacze wykorzystujące diody LED

W dziedzinie elektrycznych źródeł światła diody LED stanowią obecnie jedną z najszybciej rozwijających się technologii. Tego rodzaju oświetlacze odznaczają się bardzo wysoką sprawnością energetyczną oraz niespotykaną jak dotychczas trwałością. Ponadto są tanie w eksploatacji. Moc pojedynczego punktu świetlnego rzadko kiedy przekracza 100 W, zaś czas bezawaryjnej pracy sięga 10 lat.

Diody LED są elementami półprzewodnikowymi, które z natury rzeczy emitują światło o ograniczonej szerokości widma, co zwalnia z konieczności stosowania filtrów barwnych. W przypadku diod LED nie występują więc straty wynikające z rozproszenia znacznej części mocy na skutek działania filtra podczerwieni, z jakimi mamy do czynienia, gdy źródłem światła są żarówki.

Na rynku oświetleniowym diody LED stanowią relatywnie nowe rozwiązanie, lecz zakres ich zastosowań dynamicznie się rozszerza. Pomimo wysokich cen oświetlacze podczerwone bazujące na diodach LED zyskują sporą popularność, do czego przyczynia się ich wysoka trwałość (do 100000 godzin działania). W przypadku świetlówek ten sam parametr wynosi około 10000 godzin, a w przypadku żarówek tylko 1000 godzin.

Sprawność energetyczna diod LED mieści się w granicach od 80% do 90% i osiąga największą wartość w przypadku diod czerwonych. Tak wysoka sprawność pociąga za sobą niski pobór mocy i niewielki przyrost temperatury podczas pracy. Do kolejnych zalet diod LED należy zaliczyć

natychmiastowy rozruch, wysoką stabilność widmową w całym okresie eksploatacji, odporność na wstrząsy i wibracje, trwałość mechaniczną. W celu optymalnego wykorzystania zdolności emisyjnych diod LED o dużej mocy należy zadbać o ich odpowiednie chłodzenie oraz kontrolować wartość pobieranego prądu.

Sposób na zmniejszenie kontrastu

Przejdźmy teraz do omówienia sposobów wykorzystania sztucznych źródeł światła w realnych warunkach występujących w każdym monitorowanym obiekcie. Jednym z najistotniejszych problemów związanych z nocnym oświetleniem jest jego nierównomierność. Wbrew przysłowiu najjaśniej jest pod latarnią, a w miarę oddalania się od źródła światła poziom oświetlenia szybko spada. Powoduje to bardzo znaczny wzrost kontrastu obserwowanych scen, z czym nie radzą sobie ani oczy ludzkie, ani kamery.

Co prawda pojawiły się już technologie pozwalające na uzyskanie dynamiki zmian oświetlenia w ramach jednego kadru telewizyjnego na poziomie 96 dB, a nawet (szczytowo) 120 dB, jednakże nie zwalnia to projektantów systemów monitoringu z obowiązku dbałości o równomierność oświetlenia obiektów.

Równomierność oświetlenia obserwowanych scen

Możliwość zapewnienia dobrych warunków pracy kamerom telewizyjnym wykorzystywanym w porze nocnej jest związana nie tyle z siłą oświetlenia, co z jego równomiernością. Światło z natury rzeczy nie przenika przez większość przeszkód materialnych, dlatego powstaje problem cieni, nieunikniony nawet w sytuacji zastosowania bardzo silnych oświetlaczy. Dotyczy to w równym stopniu użycia światła białego, jak i podczerwonego.

Jednym z możliwych sposobów poprawy sytuacji jest stosowanie wielu źródeł światła o niewielkiej mocy, rozmieszczonych wewnątrz obserwowanego obszaru, jednakże ze względów praktycznych nie zawsze można przyjąć tego typu rozwiązanie, poza tym trudno poradzić sobie z problemem świecenia wprost w obiektyw kamery. Należy stosować specjalnego typu oprawy oświetleniowe, zaś kamery instalować powyżej źródeł światła. Metoda jest kapryśna i nieprzewidywalna, wiele zależy od topologii obiektu i warunków lokalnych.

Innym często stosowanym sposobem na zmniejszenie nierównomierności oświetlenia jest oddalenie źródła światła od obserwowanego obiektu, co daje dość dobre rezultaty, lecz wiąże się z koniecznością stosowania oświetlaczy o bardzo dużej mocy. Przykładem może być oświetlenie niewielkiego obiektu o strategicznym znaczeniu, położonego w przestrzeni otwartej, obserwowanego przez kamerę obrotową. Błędem jest umieszczenie silnego źródła światła w bezpośredniej bliskości tego obiektu. Lepszym rozwiązaniem jest umieszczenie wąskokątnego reflektora w pobliżu kamery. Poziom oświetlenia będzie co prawda znacznie niższy, lecz nie wystąpi efekt białej plamy, typowy dla oświetlenia lokalnego, z małej odległości.

Oświetlacze adaptowalne

Istnieją także bardziej zaawansowane od opisanych powyżej rozwiązania, które umożliwiają poprawę równomierności sztucznego oświetlenia w porze nocnej. Cel ten może być

osiągnięty przez zastosowanie adaptowalnych urządzeń oświetlających, pozwalających na modyfikację poziomu oświetlenia w poszczególnych fragmentach obserwowanej sceny.

Dotychczas oświetlenie adaptowalne nie zyskało dużej popularności, zarówno wśród projektantów, jak i instalatorów systemów monitoringu. Jest ono objęte zastrzeżeniami patentowymi, zaś szczegółowe dane są chronione przed publikacją. Niewielu producentów dostarcza tego typu oświetlacze.

Jak wiadomo, standardowe punkty świetlne, niezależnie od ich konstrukcji, powodują intensywne oświetlenie centralnych części pola obserwacji, jednakże poziom ten szybko maleje w miarę oddalania się od środka obszaru. Zależność nie jest liniowa, oświetlenie zmniejsza się nieproporcjonalnie w stosunku do wzrostu odległości od źródła światła, co dodatkowo pogarsza sytuację.

Adaptowalne punkty świetlne wyrównują poziom oświetlenia w obrębie obserwowanej sceny. Odbywa się to drogą zmniejszenia zbyt wysokiego poziomu oświetlenia w części centralnej oraz przesunięcia obszarów maksymalnej emisji światła w kierunku granic oświetlanego obszaru, gdzie droga promieni świetlnych jest dłuższa. Tym samym różnice w poziomie oświetlenia punktów bliskich i odległych ulegają znacznemu zmniejszeniu.

Oświetlacze działające na tej zasadzie mają budowę wielosegmentową i składają się z kilku mniejszych oświetlaczy. Każdy z nich może być ustawiony pod innym kątem oraz emitować światło o innej mocy. Stwarza to możliwość budowy oświetlaczy hybrydowych, wykorzystujących zarówno światło białe, jak i podczerwone. Odpowiednia kombinacja tych wszystkich ustawień prowadzi do skierowania większej liczby źródeł światła odznaczających się większą mocą w dalsze obszary obserwowanej sceny, zaś mniejszej liczby słabszych źródeł światła w bliższe obszary. Prowadzi to w efekcie do wyrównania poziomu oświetlenia na całym omawianym obszarze.

Kopułowe kamery szybkoobrotowe a praca w warunkach nocnych

Na koniec warto wspomnieć o popularnych kopułowych kamerach szybkoobrotowych, masowo stosowanych w systemach monitoringu, w przypadku których występują dodatkowe problemy związane z pracą w trybie nocnym. Kamery te są całkowicie ukryte wewnątrz obudów, nie jest więc możliwe łatwe ich sprężgnięcie z obrotowymi oświetlaczami, świecącymi w tym kierunku, w którym w danej chwili zwrócony jest obiektyw kamery. Ponadto chroniące je przezroczyste czasze nie zawsze są całkiem przezroczyste – często, ze względów użytkowych, są wykonane z barwionego materiału, co powoduje zmniejszenie ilości światła docierającego do kamer. Dodatkowo sprawę pogarsza konstrukcja samych kamer, które z różnych względów bywają budowane z wykorzystaniem przetworników o małych rozmiarach, rzędu 1/4" lub nawet 1/6", a to przyczynia się do zmniejszenia ich czułości. W przypadku tego typu kamer szczególnego znaczenia nabiera równomierność oświetlenia obserwowanych scen, a jedną z metod poprawy tej równomierności jest zastosowanie oświetlenia adaptowalnego.

ANDRZEJ WALCZYK

Literatura:

<http://www.rayteccctv.com>

SABSA

Biznesowe ujęcie kwestii bezpieczeństwa w przedsiębiorstwie

Powszechne podejście do kwestii bezpieczeństwa

Wyniki dziesiątego badania Annual Global Information Security Survey¹ wskazują, że najważniejszym czynnikiem motywującym do inwestycji w bezpieczeństwo informacji jest zapewnienie zgodności z regulacjami prawnymi – aż 64% ankietowanych dokonało takiego wyboru. Na kolejnych miejscach znalazły się konieczność zapewnienia prywatności i ochrony przetwarzanych danych (58%) oraz dążenie do osiągnięcia celów biznesowych (45%).

Zmieniające się regulacje prawne powodują, że wymagania wobec przedsiębiorstw są coraz ostrzejsze. Każda firma pragnąca uniknąć sankcji nakładanych przez regulatora podejmuje nowe inicjatywy, aby zarządzać bezpieczeństwem informacji w sposób kompleksowy. Najbardziej popularną techniką podejścia do zapewnienia bezpieczeństwa informacji w przedsiębiorstwie jest stosowanie standardów i norm bezpieczeństwa informacji, takich jak: BS 7799, ISO/IEC 17799, ISO/IEC 27001, ISO/IEC 20000, AS 8018 czy COBIT.

Standardy bezpieczeństwa informacji wdrożyło lub planuje wdrożyć w najbliższym czasie ponad 50% biorących udział w ww. badaniu przedsiębiorstw na świecie.

Stały rozwój tych wytycznych zapewnia pokrycie coraz większego obszaru działalności przedsiębiorstw. Proces wypracowywania zmian i formalnego uaktualniania istniejących standardów nie jest jednak w stanie nadążyć za ciągłymi zmianami biznesowymi czy technologicznymi. Coraz więcej obszarów nie jest objętych działaniami struktur bezpieczeństwa albo wymagania wobec nich nie są adekwatne do wykorzystywanych rozwiązań informatycznych, a przede wszystkim do potrzeb biznesu.

Architektura bezpieczeństwa

Wszelkie standardy i normy idealnie sprawdzają się jako narzędzie audytorskie, stosowane w celu zweryfikowania, czy obszary bezpieczeństwa zostały objęte odpowiednimi działaniami. Sytuacja przedstawia się znacznie gorzej w przypadku

próby wdrażania mechanizmów bezpieczeństwa w przedsiębiorstwie w oparciu o te wytyczne. Zawierają one wymagania odnośnie obszarów, które mają zostać objęte zakresem wdrażania, natomiast nie mówią nic o samym sposobie ani podejściu do ich implementacji. Wynika z nich, co ma lub może być zrobione, natomiast brakuje wskazówek, jak tego dokonać.

Właściwe wdrożenie mechanizmów bezpieczeństwa wymaga podejścia gwarantującego całościowe i szersze spojrzenie na bezpieczeństwo w przedsiębiorstwie. Takie spojrzenie uwzględniać powinno stosowane mechanizmy ochrony wraz z określeniem ich wzajemnych powiązań biznesowych. Dodatkowo koncepcja wdrożenia musi pozwalać na zanalizowanie kwestii bezpieczeństwa przez pryzmat biznesu oraz zmuszać do odpowiedzi na podstawowe pytanie: czym jest bezpieczeństwo dla przedsiębiorstwa, czyli co to znaczy, że „jest bezpiecznie”? Jednocześnie musi być to kompleksowe podejście, które pomoże wyodrębnić wszystkie obszary działalności przedsiębiorstwa, które mogą mieć wpływ na jego bezpieczeństwo.

Przedstawione wymagania są możliwe do spełnienia przez spójną metodykę, która będzie w stanie zapewnić wdrożenie oraz zarządzanie architekturą bezpieczeństwa. Próby poszukiwań takiego rozwiązania podjęli się John Sherwood, David Lynas i Andrew Clark. Wynikiem ich prac była metodyka SABSA (ang. *Sherwood Applied Business Security Architecture*), która z czasem okazała się efektywnym narzędziem do kompleksowego podejścia do architektury bezpieczeństwa, gdyż może być dostosowana do specyficznych wymagań każdego przedsiębiorstwa.

SABSA nie jest kolejną metodyką, która powstała w oderwaniu od istniejących standardów i norm. Pierwotnie sporządzono ją na podstawie międzynarodowego standardu ISO 7498-2 1989: „Systemy przetwarzania informacji. Współdziałanie systemów otwartych (OSI). Podstawowy Model Odniesienia. Architektura zabezpieczeń”. Standard ten przedstawia oderwany od biznesu model składający się z trzech warstw: logicznej (opisującej usługi bezpieczeństwa), fizycznej (przedstawiającej mechanizmy bezpieczeństwa) oraz operacyjnej (wskazującej, jak zarządzać bezpieczeństwem).

1) Coroczne światowe badanie bezpieczeństwa przeprowadzane przez firmę Ernst & Young

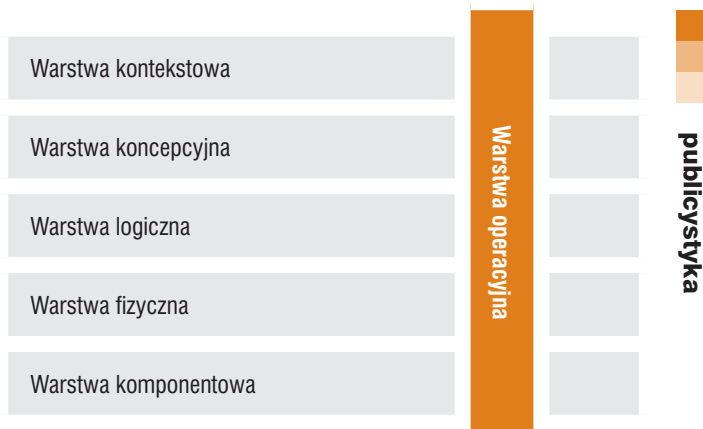
Zespół Johna Sherwooda dodał dwie górne warstwy (kontekstową i koncepcyjną), aby stworzyć model powiązany z biznesem, a także najniższą warstwę komponentową, pozwalającą na pokazanie związku z rzeczywistymi narzędziami.

Równolegle w Stanach Zjednoczonych opracowany został Model Ram Architektonicznych, stworzony przez zespół Johna Zachmana, który służy do całościowego spojrzenia na architekturę przedsiębiorstwa. Zapewnienie spójności metodyki SABSA z Modelem Zachmana wymagało kosmetycznych zmian. John Sherwood wraz z zespołem wprowadził je do swojej metodyki, jednakże oryginalna koncepcja SABSA pozostała prawie niezmienniona.

Koncepcja metodyki SABSA

Jedną z najistotniejszych różnic między metodyką SABSA a powszechnie stosowanymi koncepcjami bezpieczeństwa jest całkowita zmiana filozofii myślenia o bezpieczeństwie, ze zmianą definicji bezpieczeństwa informacji włącznie. SABSA podważa kompletność jednego z fundamentów bezpieczeństwa informacji – zestawu atrybutów zdefiniowanych w normie BS 7799: poufności, integralności i dostępności. Te trzy atrybuty swoim zakresem pokrywają wiele aspektów bezpieczeństwa, ale są zbyt ogólne, przez co istnieje ryzyko zachwiania kompletności podejścia. Twórcy SABSA na swojej drodze do stworzenia metodyki brali udział w wielu projektach w obszarze bezpieczeństwa, podczas których wypracowali listę atrybutów odzwierciedlającą potrzeby przedsiębiorstwa w tym obszarze. Na podstawie swoich doświadczeń opracowali listę 85 atrybutów, które precyzyjnie opisują bezpieczeństwo firmy, a jednocześnie prezentują kontekst biznesowy. Ponadto istnieje możliwość uzupełniania tej listy o kolejne atrybuty charakterystyczne dla poszczególnych przedsiębiorstw.

SABSA ułatwia zrozumienie kwestii bezpieczeństwa poprzez odniesienie ich do faktycznych problemów, z którymi boryka się przedsiębiorstwo i użytkownicy. Robi to, wychodząc od zrozumienia specyfiki działalności przedsiębiorstwa i zachodzących w nim procesów biznesowych oraz wskazując, które spośród zdefiniowanych w SABSA atrybutów są dla przedsiębiorstwa najistotniejsze. Tworzy to płaszczyznę porozumienia pomiędzy biznesem a bezpieczeństwem



Rys. 1. Warstwy modelu SABSA

i pozwala przedstawić wymagania bezpieczeństwa w formie zrozumiałej dla zarządu przedsiębiorstwa. Dzięki spójnemu obrazowi, na którym łączą się ze sobą aspekty biznesu i bezpieczeństwa, członkowie zarządu widzą kontekst biznesowy całego przedsięwzięcia. Pozwala to precyzyjnie określić kluczowe dla przedsiębiorstwa aspekty bezpieczeństwa oraz znaleźć optymalne rozwiązania.

Model SABSA

Całościowe podejście do zarządzania architekturą bezpieczeństwa w przedsiębiorstwie SABSA opiera się na sześciu warstwach (patrz: warstwy modelu SABSA):

- **kontekstowej**, obejmującej umiejscowienie bezpieczeństwa i jego roli w biznesie;
- **koncepcyjnej**, zawierającej wysokopoziomowy opis bezpieczeństwa – strategię bezpieczeństwa;
- **logicznej**, zawierającej model organizacji, model przepływu informacji i politykę bezpieczeństwa;
- **fizycznej**, opisującej procedury, mechanizmy, platformę i infrastrukturę sieciową;
- **komponentowej**, obejmującej bezpośrednie narzędzia wdrożenia bezpieczeństwa – standardy, protokoły, certyfikaty;
- **operacyjnej**, wspierającej pozostałe warstwy w codziennym funkcjonowaniu przedsiębiorstwa – bezpieczeństwo aplikacji, sieci, pomoc techniczną.

	Zasoby (Co?)	Motywacja (Dlaczego?)	Proces (Jak?)	Ludzie (Kto?)	Miejsce (Gdzie?)	Czas (Kiedy?)
Warstwa kontekstowa	Biznes	Model ryzyka biznesowego	Model procesów biznesowych	Organizacja biznesowa i jej powiązania	Geografia biznesu	Zależności czasowe biznesu
Warstwa koncepcyjna	Profil atrybutów biznesowych	Cele kontrolne	Strategia Bezpieczeństwa i warstwy architektury	Model jednostki bezpieczeństwa i struktury zaufania	Model domeny bezpieczeństwa	Czasy życia i terminy związane z bezpieczeństwem
Warstwa logiczna	Model informacyjny biznesu	Polityka Bezpieczeństwa	Usługi bezpieczeństwa	Schemat jednostek i profile uprawnień	Definicje bezpieczeństwa i ich powiązania	Cykl procesów bezpieczeństwa
Warstwa fizyczna	Model danych biznesu	Reguły bezpieczeństwa, praktyki i procedury	Mechanizmy bezpieczeństwa	Użytkownicy, aplikacje i interfejs użytkownika	Platforma i infrastruktura sieci	Czas wykonania struktury kontrolnej
Warstwa komponentowa	Szczegółowe struktury danych	Standardy bezpieczeństwa	Produkty i narzędzia bezpieczeństwa	Tożsamości, funkcje, czynności i ACL	Procesy, węzły, adresy i protokoły	Kolejkowanie kroków bezpieczeństwa
Warstwa operacyjna	Zapewnienie ciągłości organizacyjnej	Zarządzanie ryzykiem operacyjnym	Zarządzanie i wsparcie usług bezpieczeństwa	Zarządzanie i wsparcie użytkowników i aplikacji	Bezpieczeństwo systemów, sieci i platform	Rozkład czynności bezpieczeństwa

Rys. 2. Macierz SABSA

Projektując architekturę bezpieczeństwa zgodnie z metodyką SABSA, należy odpowiedzieć na pytania dotyczące sześciu fundamentalnych aspektów każdej z powyższych warstw.

1. Co?

Trzeba zastanowić się, co próbujemy chronić, czyli jakie aktywa są najważniejsze dla naszego biznesu. Może najważniejsza jest marka, reputacja, znaki towarowe, a może budynki i linie produkcyjne, flota samochodowa. Czy dla naszej organizacji ważne są posiadane informacje i ich źródła?

2. Dlaczego?

Dopiero wówczas, gdy powyższe kwestie są jednoznacznie sprecyzowane, można zastanawiać się, jakie rodzaje ryzyka biznesowego kryją się za zidentyfikowanymi aktywami i celami przedsiębiorstwa. Czy chcemy chronić się przed nadużyciami ze strony klientów? A może to regulator narzuca i egzekwuje pewne formy działania?

3. Jak?

Wiedząc, dlaczego musimy inwestować w bezpieczeństwo, możemy zastanawiać się, w które ważne procesy biznesowe chcemy wpisać idee bezpieczeństwa, jakie działania w obszarze bezpieczeństwa chcemy podejmować, jak chcemy usankcjonować bezpieczeństwo w firmie.

4. Kto?

Rozstrzygnięcie powyższych kwestii pozwoli nam określić rozmieszczenie odpowiedzialności za funkcję bezpieczeństwa w strukturze firmy oraz realizację działań związanych z zapewnieniem bezpieczeństwa. Czy tworzymy dedykowaną strukturę organizacyjną? Czy zlecamy odpowiedzialność za bezpieczeństwo firmie outsourcingowej? A może przenosi odpowiedzialność na klientów?

5. Gdzie?

Kolejnym krokiem jest podjęcie decyzji, gdzie zamierzamy розміścić struktury odpowiadające za bezpieczeństwo, czy tworzymy jedno centrum kompetencji dla całej firmy, czy może przypisujemy zadania związane z zapewnieniem bezpieczeństwa wszystkim jednostkom organizacyjnym.

6. Kiedy?

Następnie należy zdecydować, w jaki sposób zintegrować funkcje bezpieczeństwa z przyjętym modelem biznesowym firmy, kiedy przeprowadzać działania kontrolne tak, żeby były one możliwie transparentne i nie zakłócały funkcjonowania przedsiębiorstwa.

Warstwowy model architektury bezpieczeństwa oraz odpowiedzi na powyższe pytania dla każdej z warstw tworzą macierz przedstawiającą wszystkie aspekty bezpieczeństwa w przedsiębiorstwie – macierz SABSA.

Proces projektowania architektury bezpieczeństwa polega na rozważeniu poszczególnych aspektów dla każdej z wyżej wymienionych warstw macierzy SABSA oraz wypracowaniu rozwiązań bezpieczeństwa adresujących poszczególne obszary. Należy jednak mieć na uwadze to, że opracowanie i wdrożenie architektury bezpieczeństwa nie może pozostać celem samym w sobie. Istotne jest bowiem, aby wdrożone rozwiązania bezpieczeństwa utrzymywać operacyjnie. Służy

do tego warstwa operacyjna, która dekomponowana jest na osobną macierz SABSA – operacyjną macierz SABSA.

Dlaczego SABSA?

Model SABSA sam w sobie jest ogólny i może być użyty jako metoda zapewnienia bezpieczeństwa każdemu przedsiębiorstwu. Jednakże poprzez analizę i dostosowywanie modelu do procesów biznesowych i łańcucha wartości staje się on charakterystyczny dla danego przedsiębiorstwa. Mamy wówczas do czynienia z korporacyjną architekturą bezpieczeństwa, która umożliwia funkcjonowanie biznesu na podstawie proponowanych usług bezpieczeństwa. Architektura bezpieczeństwa gwarantuje, że potrzeby przedsiębiorstwa zostaną całkowicie spełnione i że usługi bezpieczeństwa są zaprojektowane, wdrożone i wspierane jako integralna część biznesu i infrastruktury zarządzania IT.

Dodatkową zaletą metodyki SABSA jest fakt, że nie jest ona komercyjnym produktem, lecz otwartą metodyką, którą można dowolnie wykorzystywać dla potrzeb bezpieczeństwa korporacyjnego.

Warto nadmienić, że SABSA została użyta do wdrożenia i zarządzania architekturą bezpieczeństwa w wielu organizacjach i przedsiębiorstwach na świecie, m.in. przez Ministerstwo Obrony Narodowej Wielkiej Brytanii do stworzenia Architektury Zapewnienia Bezpieczeństwa Informacji. Metodyka ta jest stopniowo rozpowszechniana i rozwijana od czasu jej opracowania w 1995 roku. Obecnie SABSA jest traktowana przez wiele organizacji jako „najlepsza praktyka” służąca do dostarczenia spójnej architektury bezpieczeństwa, m.in. w sektorach bankowości, usług ubezpieczeniowych, administracji rządowej, obronności, chemii, farmacji, cywilnego przemysłu lotniczego, mediów, rozrywki i telekomunikacji.

W Polsce dwie spośród największych spółek na rynku rozpoczęły, we współpracy z Ernst & Young Business Advisory, działania zmierzające do wdrożenia architektury bezpieczeństwa w oparciu o metodykę SABSA². W przypadku obu przedsiębiorstw głównym motywem podjęcia takiej decyzji było dążenie do wkomponowania bezpieczeństwa w model działalności biznesowej, czyli zmiana sposobu myślenia o bezpieczeństwie – odejście od koncepcji zabezpieczania biznesu na rzecz budowy biznesu bezpiecznego.

Dla osób chcących pogłębiać swoją znajomość zagadnień związanych z metodyką SABSA dostępne są szkolenia prezentujące koncepcję oraz informacje nt. szczegółów stosowania metodyki. Dostępna jest również trzystopniowa certyfikacja SABSA. W Polsce do tej pory jedynie pięć osób zdało wszystkie wymagane egzaminy i uzyskało certyfikat SABSA Chartered Foundation (SCF), potwierdzający znajomość metodyki SABSA³.

MIROSLAW RYBA, ŁUKASZ ŚLĘZAK
ERNST & YOUNG BUSINESS ADVISORY

2) Przedsiębiorstwami tymi są Polski Koncern Naftowy ORLEN oraz bank PKO BP – na podstawie *Harvard Business Review*, nr 63, maj 2008.

3) Bez uwzględnienia wyników egzaminu certyfikacyjnego, który odbył się w Warszawie w październiku 2008 r. w ramach szkolenia przygotowującego do certyfikatu SABSA Chartered Foundation (SCF), prowadzonego przez Davida Lynasa. Kolejne szkolenie SABSA w Polsce planowane jest na październik 2009 roku. Szczegóły na stronie <http://www.sabsa.org.pl>



AQAP 2110:2006



firma
ATLine®
kompleksowe zabezpieczanie obiektów



16 LAT
DOŚWIADCZENIA

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.

- 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

LUDWINÓW

inteligentny budynek u stóp Wawelu

W bezpośrednim sąsiedztwie Wzgórza Wawelskiego w Krakowie powstał wyjątkowy budynek – apartamentowiec „Ludwinów” – łączący w sobie atmosferę historycznego Krakowa z nowoczesnością i funkcjonalnością budynku XXI wieku. Budynek położony jest w centrum Krakowa, a równocześnie nieco na uboczu, w widłach Wisły i malowniczej rzeki Wilgi. Z okien swoich apartamentów mieszkańcy „Ludwinowa” będą mogli podziwiać wyjątkowej urody panoramę Starego Miasta, Zamku Królewskiego oraz zabytkowych dzielnic – Kazimierza i Podgórze, a także widok sennie wijącej się pomiędzy zielonymi bulwarami Wisły



Apartamentowiec został zaprojektowany tak, aby mogli w nim wypocząć mieszkańcy o różnych upodobaniach. Dlatego część apartamentów posiada przestronne tarasy, inne wyposażone są w ogrody zimowe, a w jeszcze innych jest dostęp do letnich ogrodów prywatnych.

W apartamentowcu będzie można korzystać z basenu, jacuzzi, sauny, fitness, siłowni i solarium. Dzieci z pewnością chętnie skorzystają z nowoczesnie wyposażonych placów zabaw na dziedzińcu, alejek spacerowych obiegających budynek, a także z placu nad Wilgą i parku położonego po drugiej stronie rzeczki.

Duży wpływ na komfort i bezpieczeństwo mieszkańców budynku będą miały instalacje inteligentnego budynku, które są standardowym wyposażeniem każdego apartamentu oraz części wspólnej.

Najwyższy standard wykończenia budynku oraz wyposażenie go w najnowocześniejsze technologie stosowane w tej klasie budynków to założenia, którymi deweloper kierował się od pierwszego etapu inwestycji.

Zgodnie z tą koncepcją firma DG ELPRO zainstalowała w budynku apartamentowca następujące systemy:

- system automatyki budynkowej w standardzie EIB/KNX, wykonany z wykorzystaniem technologii i urządzeń firmy ABB (obejmujący wszystkie apartamenty),

- system automatyki budynkowej w standardzie LONWORKS, wykorzystujący urządzenia i sterowniki serii XENTA firmy TAC (dla części wspólnej i rekreacyjnej budynku),
- zintegrowane systemy bezpieczeństwa – SSP, SSWiN, SKD, CCTV – firmy General Electric Security,
- cyfrowy system łączności wideodomofonowej i interkomowej firmy GDE-COMMAX,
- okablowanie strukturalne oraz RTV SAT.

Instalacje zostały zintegrowane w ramach systemu BMS, na który składają się dwie niezależne stacje operatorskie realizujące funkcje:

- BAS, czyli Systemu Automatyki Budynku (ang. *Building Automation System*),
- SMS, czyli Systemu Zarządzania Bezpieczeństwem (ang. *Security Management System*).

Firma DG ELPRO, jako wykonawca wszystkich wymienionych instalacji oraz integrator systemów, wykorzystala do integracji systemów automatyki oprogramowanie TAC-VISTA, a do integracji systemów bezpieczeństwa – GE-ALLIANCE. Realizowane na stanowiskach operatorskich tych systemów funkcje zarządzania oraz wizualizacji stanu pracy wszystkich instalacji ułatwiają personelowi obsługi optymalną eksploatację budynku.



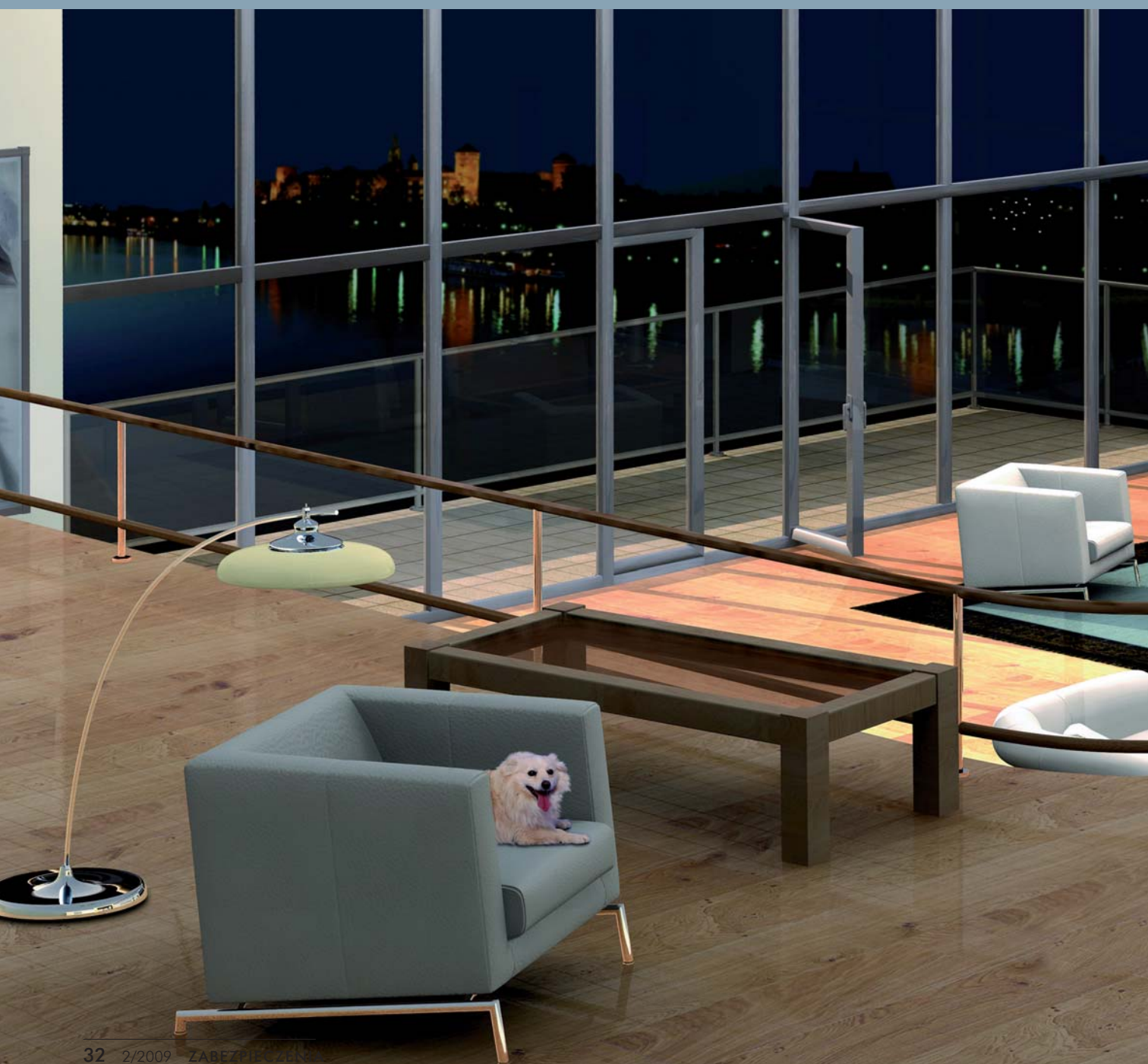
Każdy z apartamentów „Ludwinowa” został wyposażony w indywidualną instalację elektryczną EIB/KNX, system sygnalizacji włamania, instalację okablowania strukturalnego i RTV SAT oraz instalację łączności wideodomofonowej i interkomowej.

Inteligentna instalacja elektryczna, która wykorzystuje nowoczesne systemy magistralne EIB/KNX, umożliwia mieszkańcom realizację wielu funkcji, w tym:

- sterowanie oświetleniem za pomocą cyfrowych wyłączników wieloklawiszowych serii Triton,
- płynną regulację grup oświetleniowych za pomocą ściemniaczy,
- załączanie scen świetlnych,
- sterowanie żaluzjami/roletami i markizami,
- pełne sterowanie ogrzewaniem i klimatyzacją we wszystkich pomieszczeniach,
- realizację funkcji czasowych,

- symulowanie obecności,
- wykorzystanie czujników obecności do sterowania elementami instalacji,
- sterowanie wybranymi elementami instalacji za pomocą pilota,
- zarządzanie instalacją za pomocą kolorowego panelu dotykowego.

W powiązaniu z systemem kontroli dostępu pracuje cyfrowa instalacja łączności wideodomofonowej i interkomowej – system cyfrowy 480 firmy GDE-COMMAX. System umożliwia tworzenie zaawansowanych struktur, łącząc maksymalnie 99 kamer DRC-480L i 480 monitorów APV-480L. Zamiast monitora (lub równolegle z monitorem) może pracować unifon AP-480AL. Wywołanie monitorów/unifonów jest możliwe za pomocą klawiatury numerycznej kamery. Klawiatura ta umożliwia także otwieranie drzwi wejściowych (system indywidualnych kodów PIN). Opcjonalnie zapewniona jest



możliwość otwierania drzwi kartą, odczytywaną przez czytnik kart zamontowany w kamerze. Po zainstalowaniu centrali portierskiej istnieje możliwość kontrolowania przez portiera dostępu osób wchodzących/wychodzących. W systemie tym możliwe jest także nawiązanie bezpośredniej łączności pomiędzy lokatorami (funkcja interkomu).

Instalacja wykonana w apartamentowcu „Ludwinów” obejmuje:

- 31 cyfrowych stacji przywoławczych typu DRC-480L, wyposażonych w kamerę i klawiaturę, umożliwiających komunikację z centralą portierską umieszczoną w recepcji budynku oraz wideodomofonami w poszczególnych apartamentach,
- 200 wideomonitorów APV-480L, zainstalowanych w apartamentach oraz recepcji,
- centralę portierską CDS-480L, zlokalizowaną w recepcji apartamentowca,

- 56 wzmacniaczy/rozdzielaczy wideo VD-104, zlokalizowanych w pomieszczeniach technicznych.

Dzięki takiej konfiguracji zapewniono możliwość kontrolowania wejść na teren posesji i obsługę wszystkich drzwi wejściowych do klatek schodowych budynku oraz przejść z garażu podziemnego do budynku. Zapewniona została również możliwość otwierania wszystkich wejść przez portiera, swoboda połączeń pomiędzy mieszkańcami budynku oraz recepcją. Instalacja wideodomofonowa, podobnie jak system automatyki budynku EIB/KNX, należy do grupy cyfrowych instalacji magistralnych. Kto raz miał okazję przekonać się o korzyściach płynących ze stosowania nowoczesnych systemów magistralnych, nie zechce zrezygnować z tego wyjątkowego komfortu. Ta grupa produktów zapewnia wykonawcom łatwość zarówno wykonania instalacji, jak i jej serwisowania. Klientom daje natomiast gwarancję długotrwałej i bezawaryjnej pracy.

DG ELPRO



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

profesjonalna
kontrola
dostępu

roger[®]

www.roger.pl



IFSEC - 11-14 May 2009 - Birmingham (UK) - HALL 5 - STAND C60

Ulisse IR360 obserwacja bez ograniczeń



System pozycjonowania do pracy w warunkach dziennych i nocnych

Dzięki ciągłości obrotów w płaszczyźnie poziomej, ta wersja pozwala na prowadzenie dynamicznych obserwacji nocnych, w pełnym kącie 360°.

Systemy ULISSE są stosowane i wysoce cenione w tysiącach instalacji, na całym świecie.

Pokrywają one wszystkie wymagania użytkowe, dotyczące zewnętrznych, ruchomych punktów kamerowych, zapewniając maksymalną niezawodność oraz wysoką odporność na ciężkie warunki atmosferyczne.



Wpływ opóźnień w sieciach IP

na skuteczność monitoringu wizyjnego część 1

Szybki rozwój sieci komputerowych spowodował ich szerokie wykorzystanie w wielu dziedzinach techniki. W szeroko rozumianych systemach bezpieczeństwa, a zwłaszcza w monitoringu wizyjnym, wykorzystywane są sieci oparte na technologii Ethernet oraz sieci bezprzewodowe. Posiadając połączenie z Internetem, systemy te dają możliwość przesyłania sygnałów audio/wideo i udostępniania ich stacjom monitorującym lub indywidualnym użytkownikom. Umożliwia to stworzenie struktury o prawie nieograniczonym zasięgu. Przykładem jest zastosowanie telewizji dozorowej IP w monitoringu miasta, zabezpieczeniu lotniska itp.

Chociaż obecnie większość używanych kamer dozorowych to kamery analogowe, stan ten szybko się zmienia. Prawdopodobnie w najbliższym czasie sprzedaż kamer IP przewyższy sprzedaż kamer analogowych. W analogowych systemach dozorowych informacja z kamery przesyłana jest w sposób ciągły, natomiast w sieciowych systemach dozoru wizyjnego obraz jest przesyłany poprzez sieć IP, za pośrednictwem przełączników. Podczas transmisji sygnałów w sieci występują różnego rodzaju utrudnienia. W przypadku potrzeby odczytywania informacji w czasie rzeczywistym, w trakcie którego ważne jest dokładne i wierne określenie zaistniałej sytuacji, mogą one stanowić ograniczenie zastosowania.

Opóźnienia związane z przesyłaniem danych cyfrowych są główną przyczyną tych ograniczeń. Niniejszy artykuł ma za zadanie nakreślić czytelnikom zarys problemów związanych z zastosowaniem transmisji IP w systemach bezpieczeństwa na podstawie badań przeprowadzonych w ramach pracy dyplomowej w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego na kierunku Inżynieria Systemów Bezpieczeństwa Wydziału Elektroniki. Celem wymienionej pracy było zaprojektowanie stanowiska laboratoryjnego, na którym możliwy jest pomiar opóźnień w przesyłanych obrazach sieciowego monitoringu wizyjnego. Przeprowadzenie badań na stanowisku umożliwiło poznanie możliwych źródeł opóźnień i określenie ich wartości.

W pierwszej części artykułu omówiono problematykę monitoringu wizyjnego wykorzystującego sieci IP ze szczególnym uwzględnieniem analizy powstających w takim przypadku opóźnień transmisji.

1. Wymagania użytkowe mające na celu zapewnienie skutecznego monitoringu wizyjnego

System nadzoru wizyjnego jest skutecznym narzędziem poprawy bezpieczeństwa. W ostatnim czasie liczba systemów monitoringu wizyjnego gwałtownie wzrosła. Na przykład w Wielkiej Brytanii jedna kamera dozorowa przypada na 14 osób [4]. W Londynie osoba przebywa w polu widzenia kamer 300 razy dziennie. Światowy rynek urządzeń dozoru wizyjnego IP wzrósł w 2006 r. o 41,9%. Branża telewizji dozorowej dysponuje obecnie szeroką gamą systemów i urządzeń do monitorowania oraz ochrony osób i mienia. Mimo wszystko nadal istnieją wątpliwości dotyczące tego, jak dobrze i skutecznie wykorzystać system nadzoru wizyjnego.

Zgromadzony i podłączony sprzęt nie wystarcza. Po zainstalowaniu musi spełniać zamierzone cele ochrony. Dopiero wtedy będzie to prawdziwy system monitoringu.

W drugiej części artykułu będą przedstawione badania kamer sieciowych, w związku z tym główny nacisk został położony poniżej na sieciowy system wizyjny, często nazywany systemem telewizji dozorowej IP, który umożliwia użytkownikowi monitorowanie i rejestrację obrazów poprzez sieć (LAN, WAN, Internet). Do transferu danych system ten wykorzystuje sieć, a nie bezpośrednie połączenie kablowe, jak w przypadku systemów analogowych. Nie istnieją jeszcze polskie normy dotyczące protokołów i urządzeń wykorzystywanych w systemach wykorzystujących technologię IP. Szybki rozwój tej technologii spowodował, że obowiązujące normy dla telewizji dozorowej odnoszą się na razie tylko do systemów telewizji analogowej. Mimo to stanowią one dla inwestora, projektanta i instalatora niezbędną pomoc przy opracowywaniu wymagań użytkowych i projektowaniu systemów sieciowych telewizji dozorowej IP. W związku z tym, iż nie ma jasno sprecyzowanych wymagań co do samego monitoringu sieciowego, należy również zwrócić uwagę na techniczne aspekty użycia kamer sieciowych oraz podstawowe zasady ich instalacji.

2. Analiza opóźnień w sieciach IP

Głównym środkiem łączności internetowej, umożliwiającym komunikację audio/video za pomocą różnych rodzajów mediów oraz sieci, stał się protokół TCP/IP. Wraz z nowymi metodami komunikowania pojawiły się nowe zagadnienia dotyczące wydajności sieci. Aby dobrze zrozumieć protokół TCP/IP, a zwłaszcza opóźnienia w komunikacji, należy poznać podstawowe zagadnienia telekomunikacyjne.

2.1. Przyczyny i źródła opóźnień w sieci

Rozmiar nagłówka

Przyczyny opóźnienia w przesyłaniu danych przez sieci komputerowe można znaleźć już w samym modelu TCP/IP. Mianowicie do każdej warstwy modelu dodawany jest nagłówek (rysunek 1).

Standardowy rozmiar nagłówka to 20 B. Ich suma wynosi ok. 56 B dla TCP przy maksymalnej wielkości danych równej 1460 B (w przypadku komunikacji przez sieć Ethernet) [1]. Jeśli danych jest niewiele, to jest możliwe, że suma rozmiarów nagłówków przewyższa wielkość danych. Jeśli danych jest więcej, to wykonywany jest podział na ramki, z których każda zawiera nagłówek IP, a tylko jedna nagłówek TCP lub UDP. Liczba ramek zależy między innymi od obciążenia interfejsu sieciowego i procesora. Każdy powstały z podziału fragment może „podróżować” niezależnie od innych fragmentów. Podział może nastąpić u źródła lub przy udziale jednego z ruterów pośredniczących. W miejscu docelowym następuje proces składania fragmentów. Wszystkie te procesy przyczyniają się do dodatkowego opóźnienia, gdyż dodatkowo dochodzi czas odstępu międzyramkowego (ok. 10 μ s) [2], a także czas przesłania znacznika początku ramki.

System operacyjny

Realizacja całego procesu wysyłania i odbierania przez sieć jest możliwa dzięki kartom sieciowym zainstalowanym w hostach.
Typowe opóźnienie przy

przejściu sygnału przez nadajnik/odbiorcę (*transceiver*) karty sieciowej można oszacować jako ok. 0,27 μ s [2].

Obsługa tego sprzętu zajmuje się system operacyjny, który ze względu na możliwość obciążenia go innymi aplikacjami może wpłynąć na szybkość transmisji danych. Opóźnienia te, mimo iż są trudne do wyznaczenia, również powinny być brane pod uwagę w celu całkowitego wyznaczenia ich w sposób dokładny.

Fizyczny nośnik

Kolejna przyczyna opóźnień wynika ze skończonej szybkości przepływu sygnału przez przewody sieciowe. Opóźnienia te niekiedy są znaczne, a ich wartość zależy od użytego nośnika. Nie musi być on identycznego typu w przypadku poszczególnych par nadajnik – odbiorca, które występują na drodze transmisji. Istnieją dwie kategorie nośników: przewodowe i bezprzewodowe.

Powszechnie stosowane w Internecie nośniki transmisyjne to skrętka miedziana, kabel koncentryczny, światłowód oraz kanały radiowe. Najmniejszymi opóźnieniami charakteryzuje się światłowód (0,005 μ s/m) [2]. Światłowody stały się preferowanym nośnikiem transmisyjnym między innymi ze względu na oferowaną szybkość transmisji wynoszącą dziesiątki, a nawet setki gigabitów na sekundę. Ta cecha pozwala na łączenie komputerów z odległą siecią lokalną.

Dla sieci UTP/STP opóźnienie wynosi 0,0057 μ s/m, a dla 10Base2 – 0,00433 μ s/m [2].

Urządzenia sieci

Następną przyczyną opóźnień są urządzenia znajdujące się na drodze przesyłanych informacji. Podobnie jak w przypadku fizycznego nośnika wynika to ze skończonej szybkości przepływu sygnału. Opóźnienia te są trudne do wyznaczenia, gdyż zależą od wielu zmiennych czynników, na przykład od producenta, modelu urządzenia czy obciążenia sieci.

Urządzeniem, które ma największy wpływ na czas przesyłania danych, jest router. Jego głównym zadaniem jest przekierowywanie pakietów między sieciami po odczytaniu adresów IP. Do wyjaśnienia istoty opóźnień posłuży rysunek 2. Gdy pakiet dociera do routera A, jest przez niego identyfikowany (sprawdzanie nagłówka), a następnie kierowany do odpowiedniego łącza wyjściowego (w tym przypadku do łącza B). W routerze A, przed łączem wyjściowym do routera B, znajduje się bufor, czyli kolejka, gdzie pakiety oczekują na transmisję. Przyczyną tego oczekiwania jest to, że:

- szybkość przychodzenia pakietów jest większa od przepustowości łącza,
- pakiety po sprawdzeniu czekają na swoją kolej.

Pakiety są transmitowane bezkolizyjnie, niezależnie, z odpowiednio zachowanym uporządkowaniem, tzn. mogą być przesyłane wówczas, gdy łącze nie przysyła w danej chwili innych danych oraz gdy w buforze nie są przechowywane inne pakiety. Kolejne pakiety ustawiają się w kolejce, czekając na dalszą transmisję. Brak miejsca w buforze (skończona kolejka) powoduje odrzucanie nadchodzących danych, czyli straty w dostarczonej informacji. Utracone pakiety mogą być retransmitowane między węzłami przez system końcowy źródła lub protokół warstwy transportowej.

Wyróżniamy cztery typy opóźnień pakietów w węźle [3] (rysunek 2):

- opóźnienia przetwarzania,
- opóźnienie kolejkowania (oczekiwania),
- opóźnienie transmisji,
- opóźnienie propagacji.

2.2. Rodzaje opóźnień w sieci

W czasie swojej „podróży” pakiet jest transmitowany od jednego węzła do drugiego. Po drodze podlega on kilku typom opóźnień (wymienionych w poprzednim punkcie). Razem tworzą one całkowite opóźnienie węzła.

2.2.1. Opóźnienie przetwarzającego węzła

Opóźnienie to określa czas potrzebny na skierowanie pakietu do odpowiedniego łącza wyjściowego po uprzednim odczycie i sprawdzeniu jego nagłówka. Do tego wliczany jest również czas na sprawdzenie błędów bitowych. Po tym procesie pakiet jest ustawiany w buforze i oczekuje na transmisję. W nowych ruterach opóźnienie przetwarzającego węzła jest mierzone w mikrosekundach.

2.2.2. Opóźnienie kolejkowania

Opóźnienie to określa czas oczekiwania pakietu w kolejce na przesłanie łączem wyjściowym. Wielkość tego opóźnienia zależy od liczby pakietów już oczekujących w buforze. Pusta kolejka oraz brak transmisji innych danych oznacza, iż opóźnienie kolejkowania dla nadchodzącego pakietu będzie zerowe. Jego wartość zwiększa się wraz ze wzrostem liczby oczekujących w kolejce pakietów i może być wyrażona w mikrosekundach lub milisekundach. W przeciwieństwie do innych typów opóźnień kolejkowania może mieć różne wartości w zależności od pakietu. Jeśli będą to pakiety

z kolejki przesyłane w pierwszej kolejności, opóźnienie będzie zerowe lub bardzo małe. Jeśli będą to pakiety z końca kolejki, będzie ono odpowiednio większe. Dlatego do opisu opóźnienia kolejkowania bierze się średnie wartości. Opóźnienie kolejkowania zależy od wielu czynników, z których główne to szybkość umieszczania danych w kolejce, szybkość transmisji łącza, sposób pojawiania się danych w kolejce (cyklicznie, impulsowo).

Istotną rolę w określaniu opóźnienia kolejkowania stanowi **natężenie ruchu**, czyli tzw. współczynnik La/R [3], gdzie:

L – liczba bitów, z których składają się pakiety, długość pakietów (bit),

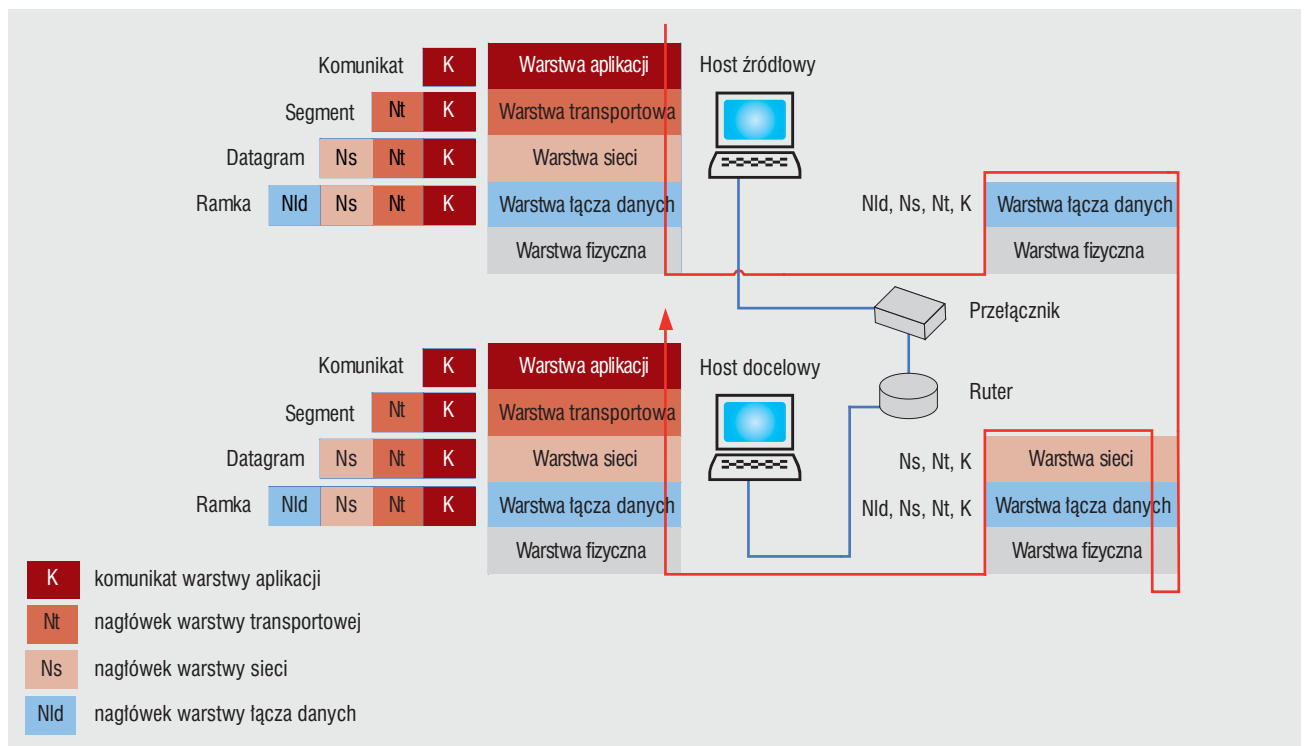
a – średnia szybkość, z jaką pakiety pojawiają się w kolejce (pakiety/s),

R – przepustowość łącza (bit/s),

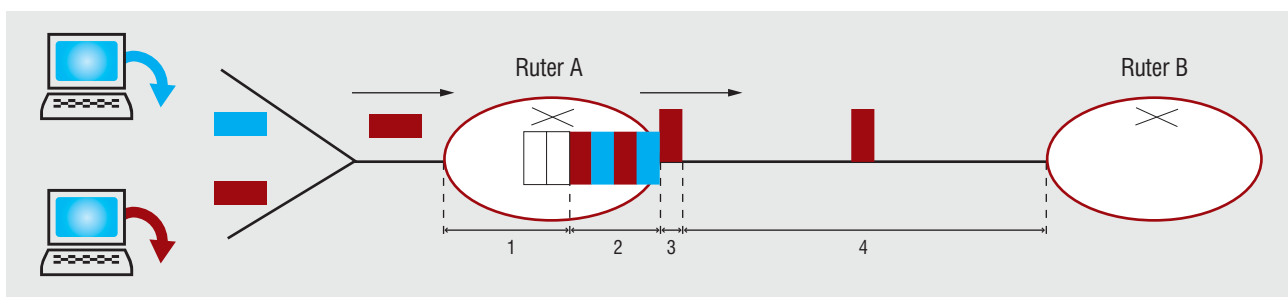
La – średnia szybkość, z jaką bity są ustawiane w kolejce (bit/s).

Jeśli $La/R > 1$, średnia szybkość, z jaką bity są umieszczane w kolejce, przekracza szybkość pobierania z niej bitów, co prowadzi do znacznego powiększania się kolejki. W wyniku tej obserwacji powstała jedna z podstawowych zasad ruchu sieciowego: natężenie ruchu nie może przekroczyć wartości 1.

W przypadku, gdy $La/R \leq 1$, opóźnienie kolejkowania będzie zależało od ruchu sieciowego, tzn. jeśli pakiety będą się pojawiały cyklicznie (jeden pakiet co L/R sekund), wówczas każdy pakiet będzie „wędrował” do pustej kolejki i opóźnienie będzie zerowe, jeśli natomiast pakiety będą się pojawiać okresowo, to tylko pierwszy nie będzie miał opóźnienia. Opóźnienie zwiększy się z każdym kolejnym pakietem. Współczynnik La/R nie ustala jednak dokładnie rzeczywistego opóźnienia kolejkowania. Pakiety z reguły nie pojawiają się w ściśle określony sposób, tylko w różnych odstępach czasu. Zależność ta jest jednak pomocna w zrozumieniu zakresu oddziaływania opóźnienia kolejkowania. Rysunek 3 przedstawia zależność średniego opóźnienia kolejkowania



Rys. 1. Przesyłanie danych



Rys. 2. Opóźnienia węzła w ruterze (białe prostokąty oznaczają wolne miejsca w kolejce, bordowe i błękitne – „podróżujące” pakiety)
1 – opóźnienie przetwarzającego węzła, 2 – opóźnienie kolejkowania (oczekiwanie), 3 – opóźnienie transmisji, 4 – opóźnienie propagacji

od natężenia ruchu [3]. W miarę zbliżania się wartości natężenia ruchu do 1 średnia długość kolejki będzie coraz większa. Przy wartości 1 niewielki procentowy wzrost natężenia ruchu przyczynia się do dużo większego procentowego wzrostu wartości opóźnienia.

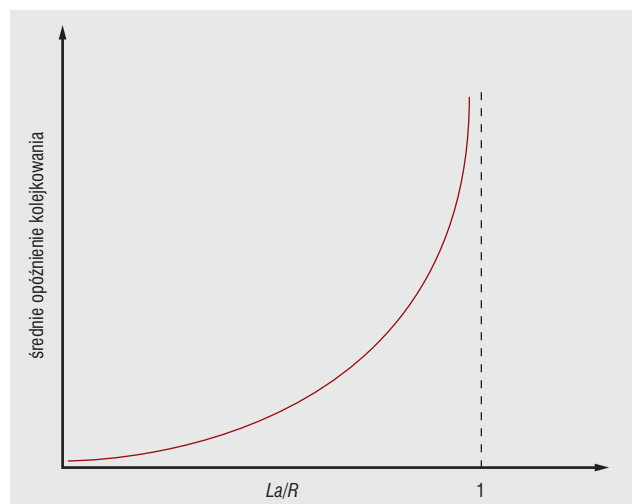
Nateżenie ruchu $\lambda a/R$	Opóźnienie kolejowania
około 0	krótkie lub średnie oczekiwanie w kolejce
bliskie 1	bardzo długie oczekiwanie
> 1	więcej pracy niż można obsłużyć, średnie opóźnienie i kolejka dążą do nieskończoności, w buforze kończą się miejsca, następują straty

Tab. 1. Wpływ natężenia ruchu $\lambda a/R$ na czas oczekiwania w kolejce

W rzeczywistości kolejka przed łączem wyjściowym ma ograniczoną pojemność. Może ona być ograniczona w różny sposób, w zależności od producenta, konstrukcji czy ceny. W związku z tym jeśli natężenie ruchu zbliża się do wartości 1, opóźnienia pakietów nie rosną do nieskończoności. Jeśli kolejka zapełni się, kolejny pakiet zostanie odrzucony przez ruter, co wiąże się z jego utratą. Utracony pakiet może być ponownie przesłany przez aplikację lub protokół TCP.

2.2.3. Opóźnienie transmisji

Opóźnienie to, zwane także buforowym, określa czas potrzebny na wysłanie do łącza wszystkich bitów pakietu. W sieciach z komutacją pakietów dane są przesyłane dopiero wtedy, gdy zostały wysłane wszystkie pakiety, które wcze-



Rys. 3. Zależność średniego opóźnienia kolejkowania od natężenia ruchu [3]

śniej odebrano. Opóźnienie transmisji jest definiowane jako stosunek L/R [3], gdzie:

L – długość pakietu (bit),

R – przepustowość łącza, szybkość łącza wyjściowego (np. dla łącza Ethernet 100 Mb/s wartość R wynosi 100 Mb/s).

Wartość opóźnienia transmisji jest określana w mikrosekundach lub milisekundach.

2.2.4. Opóźnienie propagacji

Opóźnienie to określa czas niezbędny do przesłania bitu z początku łącza wyjściowego do kolejnego ruteru. Definiowane jest jako stosunek odległości między dwoma ruterami do szybkości propagacji d/s [3], gdzie:

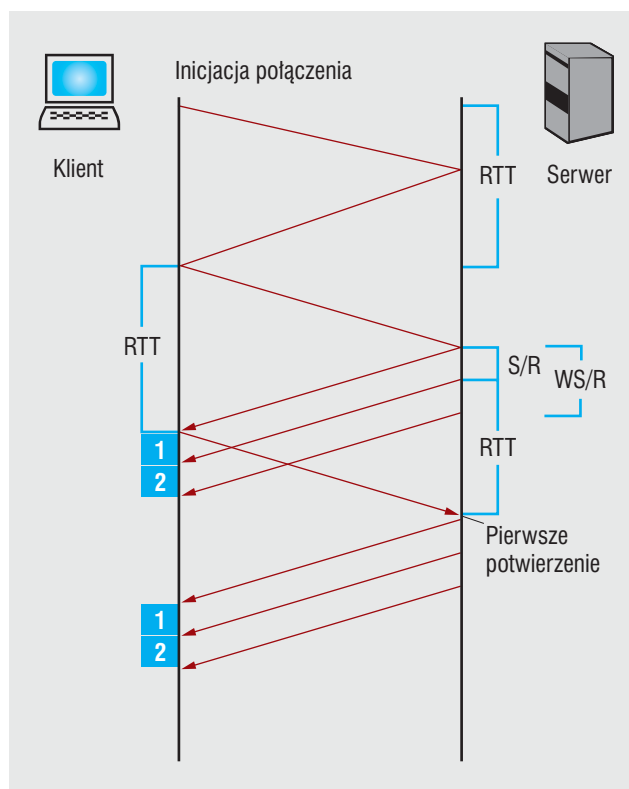
d – długość fizycznego łącza,

s – szybkość propagacji w medium transmisyjnym.

Szybkość ta w zależności od fizycznego nośnika zawiera się w przedziale $2 \cdot 10^8 \div 3 \cdot 10^8 \text{ m/s}$.

Gdy cały pakiet dotrze do kolejnego rutera, zostaje tam zapisany i przekazywany dalej.

Wartość opóźnienia propagacji w sieciach rozległych jest wyrażana w milisekundach.



Rys. 4. Serwer wysyłający wszystkie segmenty okna jeszcze przed odebraniem potwierdzenia dla pierwszego segmentu okna

2.2.5. Opóźnienie całkowite w węźle

Całkowite opóźnienie węzła określa równanie [3]:

$$o_{\text{węz}} = o_{\text{przet}} + o_{\text{kolejk}} + o_{\text{trans}} + o_{\text{prop}} \quad (2.1)$$

w którym:

- $o_{\text{węz}}$ – całkowite opóźnienie węzła,
- o_{przet} – opóźnienie przetwarzającego węzła,
- o_{kolejk} – opóźnienie kolejkowania,
- o_{trans} – opóźnienie transmisji,
- o_{prop} – opóźnienie propagacji.

Poszczególne opóźnienia i ich wkład w całkowitą wartość mogą się znacząco różnić. Jeśli przykładowo rutery znajdują się niedaleko, opóźnienie propagacji będzie bardzo małe, natomiast jeśli rutery będą połączone przy użyciu łącza satelitarnego, opóźnienie propagacji będzie miało znaczną wartość. Wówczas właśnie to opóźnienie może przede wszystkim decydować o wartości całkowitego opóźnienia. Podobnie jest z opóźnieniem transmisji w przypadku przesyłania dużych pakietów za pośrednictwem łącza obsługiwane przez modem telefoniczny.

2.2.6. Opóźnienia pomiędzy węzłami

Między hostem źródłowym a docelowym może znajdować się szereg ruterów. Korzystając z poprzednich punktów, w których omówiono poszczególne opóźnienia, można wywnioskować, iż przy założeniu, że:

- opóźnienie kolejkowania jest pomijalne – sieć nie jest przeciążona,
- opóźnienie propagacji dla każdego łącza jest takie same,
- opóźnienie każdego przetwarzającego węzła i źródłowego hosta jest takie same,
- szybkość wysyłania danych przez rutery i hosta źródłowego wynosi R bitów/s,
- między hostem źródłowym a docelowym znajduje się $N - 1$ routerów

opóźnienie międzywęzłowe ($o_{\text{węz-węz}}$) [3] charakteryzuje zależność:

$$o_{\text{węz-węz}} = N (o_{\text{przet}} + o_{\text{trans}} + o_{\text{prop}}) \quad (2.2)$$

2.3. Przykładowe wyznaczenie opóźnienia

Istnieje wiele modeli umożliwiających przedstawienie i wyznaczenie czasu opóźnienia. Jednym z nich jest model ze statycznym oknem przeciążenia. Chociaż TCP korzysta z dynamicznego okna, to przedstawiony model pokazuje podstawowe procesy i czasy występujące podczas wysyłania danego obiektu. Analiza przeprowadzana jest w kontekście prostej sieci z jednym łączem pośredniczącym. Przyjęto, że sieć nie jest przeciążona, nie mają miejsca retransmisje, bufony odbiorcze są duże, rozmiar przesyłanego obiektu – O bitów, maksymalny rozmiar segmentu (MSS) – S bitów, szybkość transmisji łącza – R bitów/s, czas na zainicjowanie połączenia – RTT [3], niezmienna wielkość statycznego okna przeciążenia – W (gdy serwer odbierze żądanie od klienta, natychmiast odeśle mu W segmentów), dla każdego potwier-

dzenia serwer umieści jeden segment. Poniżej przedstawiony zostanie wariant, w którym serwer wysyła wszystkie segmenty okna przed odebraniem potwierdzenia dla pierwszego segmentu okna. Rysunek 4 przedstawia taką sytuację. Przyjęto, że $W = 2$. Inicjacja połączenia trwa przez czas oznaczony RTT . Klient zaczyna odbierać segmenty po upływie czasu dwukrotnie dłuższego niż RTT . Segmenty są dostarczane z serwera co S/R sekund. Po otrzymaniu każdego segmentu klient wysyła potwierdzenie. Serwer kończy nadawanie segmentów pierwszego okna przed nadejściem potwierdzenia. W związku z tym przechodzi w stan oczekiwania na potwierdzenie. Serwer zacznie wysyłać następny segment w chwili otrzymania potwierdzenia. Kolejne potwierdzenia nadchodzą co S/R sekund. Opóźnienie jest zatem sumą dwóch czasów RTT , czasu potrzebnego na przesłanie obiektu O/R oraz czasu oczekiwania serwera. Jeśli przyjmujemy, że K oznacza liczbę okien danych obiektu, wówczas $K = O/WS$. Okresów oczekiwania serwera będzie $K - 1$, a każdy okres będzie trwał $RTT - (W - 1) S/R$. Zatem opóźnienie wynosi [3]:

$$o = 2 RTT + O/R + (K - 1) [RTT + S/R - WS/R] \quad (2.3)$$

Jeśli serwer otrzyma potwierdzenie pierwszego segmentu pierwszego okna, zanim zakończy transmisję segmentów tego okna, wówczas opóźnienie wynosi:

$$o = 2 RTT + O/R \quad (2.4)$$

Podsumowanie

W pierwszej części artykułu opisano opóźnienia, jakie można napotkać przy zestawianiu sieciowych urządzeń nadzoru wideo, a także przedstawiono wyniki badań opóźnień w transmisji obrazu przykładowych, dostępnych na naszym rynku kamer sieciowych. Po przeanalizowaniu teoretycznych podstaw pracy sieci można stwierdzić, że poszczególne opóźnienia i ich wkład w całkowitą wartość mogą się znacząco różnić. Przykładowo istotnym rodzajem opóźnienia, mającym największy wpływ na całkowitą jego wartość podczas przesyłania dużej liczby pakietów przez ruter, ma opóźnienie kolejkowania. Przy przesyłaniu na dużą odległość najważniejszy jest czas propagacji.

W drugiej części artykułu zostanie przedstawiona koncepcja stanowiska laboratoryjnego do badania opóźnień w sieciach IP, a także zostaną zaprezentowane wyniki przeprowadzonych na tym stanowisku badań.

DR INŻ. MAREK ŻYCZKOWSKI
MGR INŻ. ŁUKASZ STAWICKI

Literatura:

1. Mahbub Hassan, Raj Jain, *Wysoko wydajne sieci TCP/IP*, Wydawnictwo Helion, Gliwice 2004.
2. Sportach M., *Sieci komputerowe. Księga eksperta*, Wydawnictwo Helion, Gliwice 1999.
3. James F. Kurose, Keith W. Ross, *Sieci komputerowe. Od ogółu do szczegółu z Internetem w tle*, Wydawnictwo Helion, Gliwice 2006.
4. http://en.wikipedia.org/wiki/Closed-circuit_television



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

Twoje bezpieczeństwo
jest w jego rękach.

Daj mu najlepsze narzędzia,
pogadaj z SONY.

SONY

www.sonybiz.pl

Inteligentna analiza obrazu... bezpieczeństwo dla Ciebie.

Linia produktów SONY zawiera zarówno najlepsze kamery i rejestratory wizyjne
jak i doskonałej jakości oprogramowanie do zarządzania systemami monitoringu.
Reakcja pracowników ochrony będzie natychmiastowa.

tel. +48 22 520 24 51, www.sonybiz.pl



IPELA

Co potrafi kamera telewizji dozorowej?

Czy wiecie Państwo, że w sieciach handlowych cenne wcale nie są towary na półce, ale sama przestrzeń na tychże półkach? Zabawne, ale zarządcy sieci handlowych nie od dziś uważają, że sprzedają powietrze... powietrze na półkach. Im bardziej uczęszczana jest aleja, w której znajduje się półka, lub im bliżej wysokości wzroku umieszczona jest półka, tym wyższy dla producenta sprzętu/żywności/chemii jest koszt umieszczenia na niej towaru

Wyobraźmy sobie, że możemy zaoferować klientowi rozwiązanie, które nie tylko spełni jego oczekiwania co do poprawy bezpieczeństwa, ale także da mu dodatkowe informacje dotyczące przepływu osób na określonym terytorium. Skoro dla sieci handlowych tak ważna jest powierzchnia i sprzedaż jej w jak najwyższej cenie, zapewne interesujący będzie fakt, że za pomocą instalacji telewizji dozorowej można nie tylko obserwować klientów sklepu, ale także badać ich zachowanie, przepływ, liczbę osób znajdujących się w poszczególnych alejach, w poszczególnych miejscach. Dzięki tym danym zarządcy sklepów mają jeszcze dokładniejsze informacje, które mogą im pomóc lepiej wycenić powierzchnię, ale też zrozumieć zachowanie klientów ich sklepu.

Sony wprowadza na polski rynek kompleksową ofertę skierowaną do tych, którzy chcą wiedzieć więcej o zachowaniu klientów w określonej lokalizacji. W pierwszej chwili na myśl przychodzi wspomniane już sklepy, ale w rzeczywistości wiedza o tym, jak zachowują się ludzie – klienci, zwiedzający, kibice – jest cenna nie tylko w klasycznym handlu.

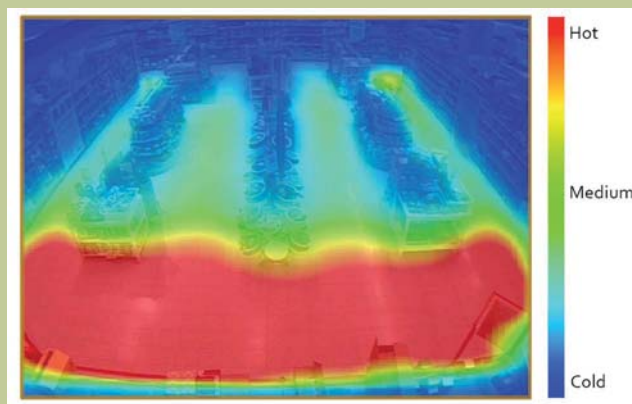
Dzięki zaawansowanej inteligencji zaimplementowanej w kamerach IP Sony możliwe jest wykorzystanie tychże urządzeń w celu zapewnienia bezpieczeństwa oraz równocześnie do generowania danych o przepływie osób. Kamery IP Sony wytwarzają różne strumienie danych. Może być to obraz zakodowany w formacie MPEG-4, H.264, JPEG albo metadane wygenerowane przez kamerę w efekcie analizy obrazu. Funkcja wysyłania podwójnego strumienia danych

umożliwia pracę jednej kamery z dwoma rodzajami oprogramowania.

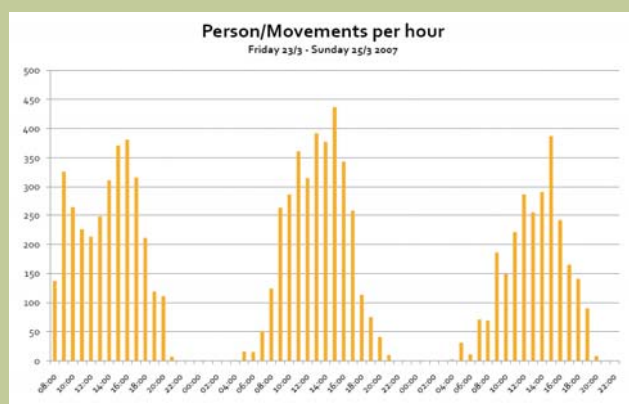
Aby zapewnić bezpieczeństwo osobom przebywającym w określonym obszarze, kamery przekazują przeanalizowany wstępnie obraz, który jest zakodowany w formacie JPEG lub MPEG-4, do programu Real Shot Manager.

Równocześnie kamery przesyłają metadane (informacje o obiektach, ich wielkości, liczbie, pozycji itd.) do oprogramowania zajmującego się zliczaniem osób, rysowaniem linii przepływu obiektów, wskazywaniem tzw. „gorących punktów”, czyli miejsc, gdzie jest największe zagęszczenie osób. Raporty mogą być generowane z dowolną częstotliwością (godzinowe, na zakończenie dnia, tygodniowe, miesięczne) i zawierać dowolnie wybrane dane. Co ważne, działanie jednego systemu nie ma żadnego wpływu na funkcje drugiego. Są one od siebie niezależne, ale zarazem można je umieścić na jednym serwerze. W efekcie mamy dwa różne systemy, które korzystają z tych samych kamer i wykorzystują ten sam serwer. Skutek – rozwiązanie, o którym mówimy, jest bardzo efektywne kosztowo.

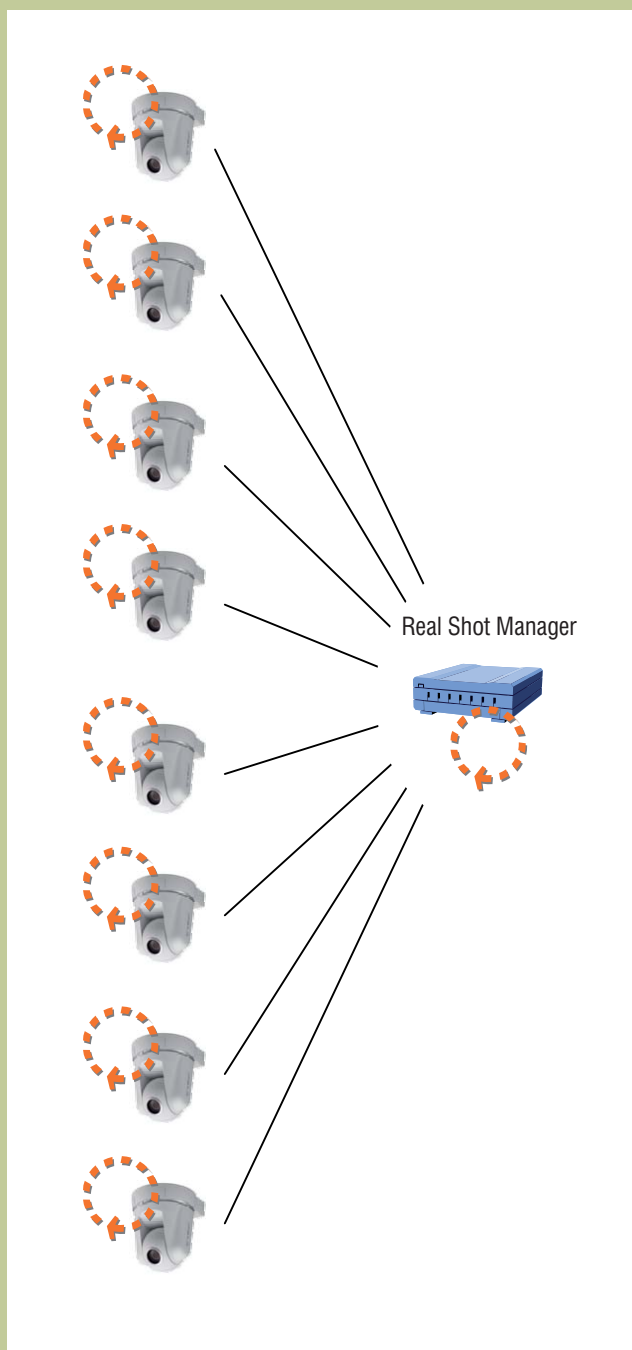
Dzięki zastosowaniu kamer z rozwiniętą detekcją ruchu czy detekcją przedmiotów oraz wykorzystaniu systemu Real Shot Manager systemy telewizji dozorowej wchodzi w nową erę rozwiązań „proaktywnych”. Dostrzeżenie zdarzenia negatywnego czy też podejrzanego nie zależy już tylko od uważnej pracy operatora. Linia kamer IP Sony przekazuje do systemu Real Shot Manager już przeanalizowane dane



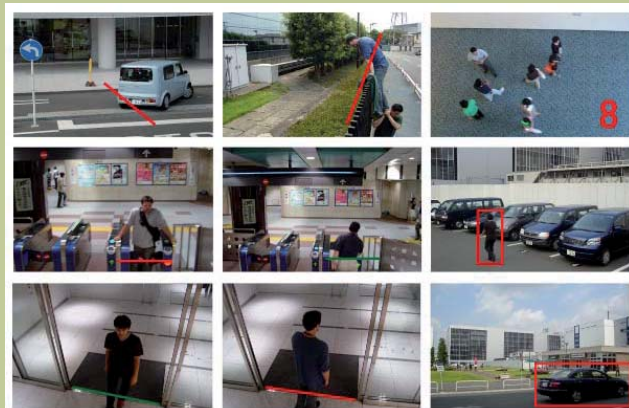
Fot. 1. Mapa cieplna (ang. Heat Map), czyli wskazanie lokalizacji, w których najczęściej pojawiają się ludzie



Rys. 1. Wykres przedstawiający liczbę osób/ruchów na godzinę (piątek 23 marca – niedziela 25 marca)



Rys. 2. Struktura telewizji dozorowej z inteligentnymi kamerami w technologii IP



Fot. 2. Działanie filtrów detekcji zdarzeń w systemie Real Shot Manager

dotyczące tego, co dzieje się na obserwowanym przez nią obszarze. System wykonuje analizę wtórną przekazanego obrazu oraz metadanych.

W przypadku zdarzenia spełniającego określone wcześniej założenia – np. gdy na korytarzu przebywa siedem osób, a alarm jest uruchamiany, kiedy liczba osób przekroczy sześć – alarm generowany jest przez system, w efekcie czego operator dostaje informację dźwiękową o alarmie, okno pokazujące obraz z kamery jest podświetlone, a system może od momentu zdarzenia polepszyć parametry nagrywanego obrazu albo uruchomić nagrywanie obrazu, jeśli wcześniej włączony był tylko tryb podglądu.

Kamery mają zaimplementowane następujące filtry:

- pojawianie się i znikanie obiektów (ludzi, przedmiotów, zwierząt),
- obecność przedmiotów (może być dodany parametr czasu, przez jaki obiekt jest obecny),
- pojemność obszaru (np. liczba osób lub przedmiotów, których obecność może powodować alarm),
- przekraczanie wirtualnych granic,
- nieobecność, usuwanie obiektów.

Spełnienie warunków dowolnego filtra może powodować alarm, rozpoczęcie nagrywania (o ile nie było ono skonfigurowane wcześniej), polepszenie parametrów nagrywanego obrazu, przekazanie informacji (np. do systemu kontroli dostępu), rozpoczęcie nagrywania dźwięku. Co ciekawe, w efekcie zgodności obserwowanej sytuacji z dowolnym filtrem kamera może być – poprzez połączony bezpośrednio z nią głośnik – źródłem ostrzeżeń dźwiękowych zapisanych w pamięci kamery lub też wydawanych bezpośrednio przez operatora.

Kombinacja kamer IP Sony, oprogramowania Real Shot Manager oraz oprogramowania badającego przepływ osób pozwala stworzyć interesującą ofertę nie tylko dla sieci handlowych, choć te oczywiście wydają się być naturalnym użytkownikiem tego rodzaju rozwiązań. Na lotniskach czy dworcach kwestia przepływu osób również wydaje się być nie bez znaczenia. W końcu kluczowa w przypadku rozległych obiektów, przez które przewijają się masy ludzi, jest wiedza o tym, gdzie następuje koncentracja osób. Dzięki takim informacjom można optymalnie zaplanować trasy patroli policji lub ochrony, przez co zwiększy się bezpieczeństwo w niewrażliwych miejscach. Podobnie można zaadaptować to rozwiązanie w obiektach sportowych. Dobrze jest wiedzieć, gdzie zbierają się kibice, gdzie są największe skupiska ludzkie podczas przerw czy też gdzie tworzą się kolejki. Dzięki tej wiedzy można poprawić zarówno bezpieczeństwo, jak i komfort kibiców, klientów czy podróżnych.

Rozwiązanie oferowane przez Sony pozwala wykorzystać zaprojektowaną dla potrzeb bezpieczeństwa instalację telewizji dozorowej w technologii IP do innych celów, nie mnożąc równocześnie niepotrzebnych kosztów. Kamery IP Sony z założenia przejęły znaczną część funkcji systemu telewizji dozorowej i od dawna zajmują się nie tylko dostarczaniem obrazów.

Jeśli chcecie Państwo dowiedzieć się, jak wiele potrafią kamery Sony, zapraszamy do odwiedzenia strony www.sonybiz.pl.

MARTA MAŁECKA
SONY POLAND

Kamery megapikselowe z Pelco

W drugim kwartale 2009 r. firma Pelco wprowadzi do sprzedaży stałe kamery megapikselowe wykonane w technologii Sarix. Celem artykułu jest przedstawienie parametrów i możliwości nowych kamer IP

Technologia Sarix

Sarix to nazwa technologii kamer megapikselowych opracowanej przez konstruktorów Pelco. Będzie ona stosowana we wszystkich kamerach wysokiej rozdzielczości Pelco, jakie zostaną wprowadzone na rynek w 2009 roku. Pierwsze modele kamer wykonanych w tej technologii to rodzina Sarix IX składająca się z ośmiu kamer kolorowych i dzieńno-nocnych o rozdzielczościach 3,1 megapiksela, 2,1 megapiksela, 1,3 megapiksela oraz 0,5 megapiksela. Planowane jest wprowadzenie kolejnych modeli w kolejnych kwartałach 2009 roku. Będą to kolorowe i dzieńno-nocne kamery kopułowe do zastosowań zewnętrznych i wewnętrznych.

Kamery Sarix IX zawierają przetworniki CMOS pracujące ze skanowaniem progresywnym. Czulość, mierzona przy $f/1,2$, 2800 K i $SNR > 24$ dB, dla trybu kolorowego i czarno-białego wynosi odpowiednio 1 luks i 0,20 luksa. W trybie SENS czulość dla trybu kolorowego i czarno-białego wynosi odpowiednio 0,20 luksa i 0,05 luksa.

sarixTM
Mega-Performance Technologies

Podstawowym standardem kodowania jest H.264, dostępny jest też MJPEG. Kamera może wytworzyć dwa strumienie wideo. Liczba obrazów/s w strumieniu wideo zależy od wybranej rozdzielczości i sposobu kodowania. Przykładowo strumień wideo z kamery IXE20 o rozdzielczości 1920x1080 dla kompresji H.264 może zawierać maksimum 15 obrazów na sekundę. Karty katalogowe poszczególnych kamer Sarix IX opisują szczegółowo parametry generowanego strumienia wideo w zależności od wybranej rozdzielczości. Kamery IXS0 mają dodatkowo możliwość wytworzenia strumienia kodowanego MPEG4 o rozdzielczości 4CIF, co



umożliwia zastosowanie ich w istniejących systemach rejestracji obsługujących protokół IP Pelco, takich jak seria DVR5100.

W kamerach IXE20 stosowana jest technologia Sarix EP (*Extended Platform* – poszerzona platforma), dzięki której procesor kamery ma zwiększoną wydajność. Pozwala to uzyskać dużą liczbę obrazów/s dla dużych rozdzielczości oraz stosować w przyszłości oprogramowanie do analizy obrazu. Docelowo klienci będą mogli załadować do pamięci kamery programy analityczne tworzone przez różnych producentów.

Wbudowany czytnik kart pamięci w standardzie mini-SD pozwala na zapis zdjęcia powiązanego ze stanem alarmowym wywołanym na przykład naruszeniem parametryzowanego wejścia alarmowego w kamerze. Oprócz wejścia alarmowego dostępny jest też wyjściowy obwód alarmowy o obciążalności 75 mA przy napięciu stałym 15 V. Dla ułatwienia strojenia kamery Sarix IX są wyposażone w serwisowe wyjścia wideo z analogowym sygnałem PAL.

Obsługiwane są następujące protokoły sieciowe: TCP/IP, UDP/IP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP, RTSP, NTP, IPv4, SNMP, QoS, HTTP, HTTPS, LDAP (klient), SSH, SSL, SMTP, FTP, MDNS (Bonjour).

Interfejs internetowy

Kamery serii Sarix IX mogą być konfigurowane i administrowane zdalnie, przy użyciu przeglądarki internetowej. Kompatybilne przeglądarki to Microsoft Internet Explorer wersja 7.0 lub późniejsza oraz Mozilla Firefox wersja 3.0 lub późniejsza. Użytkownik może oglądać w przeglądarce obraz z maksimum 16 kamer pracujących w tej samej sieci IP. Poprzez przeglądarkę internetową zarządza się także protokołami SSL, SSH i QoS. Z każdą kamerą w trybie „unicast” może połączyć się maksimum 20 użytkowników, natomiast w trybie „multicast” liczba nie jest limitowana.

Systemy rejestracji

Rejestracja obrazów z kamer megapikselowych będzie się odbywać w systemie IP Endura (wersja 2.0), którego

Symbol	Typ kamery	Maksymalna rozdzielczość
IXS0C	Kamera kolorowa, 0,5 megapiksela	800x600
IXS0DN	Kamera dzień-noc, 0,5 megapiksela	800x600
IX10C	Kamera kolorowa, 1,3 megapiksela	1280x1024
IX10DN	Kamera dzień-noc, 1,3 megapiksela	1280x1024
IXE20C	Kamera kolorowa, 2,1 megapiksela	1920x1080
IXE20DN	Kamera dzień-noc, 2,1 megapiksela	1920x1080
IX30C	Kamera kolorowa, 3,1 megapiksela	2048x1536
IX30DN	Kamera dzień-noc, 3,1 megapiksela	2048x1536

Tab. 1. Kamery megapikselowe serii Sarix IX

premiera jest zapowiadana na drugi kwartał bieżącego roku. Drugą platformą rejestracji będzie rodzina rejestratorów Digital Sentry z oprogramowaniem w wersji 1.6 lub późniejszej. Obraz wideo może być wyświetlany i nagrywany także przez oprogramowanie innych producentów z branży. Pelco udostępnia zainteresowanym firmom protokół API umożliwiający wykonanie sterowników do swoich kamer megapikselowych.

Obiektywy

Do kamer megapikselowych oferowana jest nowa seria obiektywów o oznaczeniu 13M, które zapewniają uzyskanie

dobrej jakości obrazu i maksymalne wykorzystanie możliwości kamery nawet przy słabych warunkach oświetleniowych. Obiektywy mają automatyczną migawkę, natomiast ostrość i powiększenie są ustawiane ręcznie. Dostępne są cztery zakresy ogniskowych: 2,2–6,0 mm, 2,8–8 mm, 2,8–12 mm oraz 15–50 mm. Obiektywy serii 13M są przeznaczone do kamer z przetwornikiem 1/3 cala, mocowaniem typu CS i sterowaniem DC. Mogą być stosowane w systemach telewizji dozorowej z oświetlaczami podczerwieni.

Rekomendowane obudowy i zasilacze

Do kamer Sarix IX Pelco poleca obudowy serii EH3512, EH1512 i DF8 (kopuła). Kamery mogą być także mocowane na uchwycie uniwersalnym C10-UM. Masa kamery bez obiektywu to około 500 g. Zasilanie może być doprowadzone poprzez sieć Ethernet w standardzie PoE lub z zewnętrznego zasilacza o napięciu przemiennym 24 V z serii MCS lub WCS. Moc pobierana przez kamerę nie przekracza 7 W.

Kamery megapikselowe Pelco cechują się zaawansowanymi parametrami technicznymi i wyróżniają się wyjątkową estetyką wykonania. Bardzo dobrze prezentują się we wnętrzach nowoczesnych budynków biurowych.

W Polsce produkty Pelco są dostępne w sieci partnerów firmy TAC, która jest wyłącznym przedstawicielem firmy Pelco w Polsce. Więcej informacji o kamerach IP z Pelco można znaleźć na stronie <http://www.pelco.com/IP>. Zapraszamy też na stronę TAC <http://www.tac.com/pl>.

NORBERT GÓRA
TAC



Detekcja:
uderzeń i wybuchów
wiercenia, szlifowania i cięcia mechanicznego
cięcia palnikiem plazmowym
cięcia palnikiem acetylenowym

Certyfikat Techom, klasa S, nr 38/08



VD400
**DETEKTOR
SEJSMICZNY**

www.alarmtech.pl

Nowości 2009

Cyfrowa bezprzewodowa transmisja obrazu wideo



Produkty firmy P.W. Camsat cieszą się nie słabnącym zainteresowaniem i ciągle zdobywają nowe rynki w kraju i za granicą. Popularność, jaką zdobyły bezprzewodowe zestawy TCO 5807H, TCO 5808 i moduły telemetryczne CD 04, a także rosnące zapotrzebowanie na tego typu produkty motywuje nas do dalszej pracy nad konstruowaniem nowych urządzeń. Rozwój technologiczny oraz coraz wyższe wymagania dotyczące jakości transmisji, a przede wszystkim coraz większe zakłócenia przemysłowe, skłoniły nas do wykorzystania w produkcji najlepszych i sprawdzonych technologii, w tym transmisji cyfrowej. Naszym najnowszym produktem, który wraz z nadejściem nowego roku został wprowadzony do sprzedaży, jest cyfrowy system transmisji wideo CDS-5021

Czego możemy oczekiwać, stosując cyfrowy system CDS-5021?

Najczęściej zgłaszanym przez instalatorów problemem przy projektowaniu bezprzewodowej sieci monitoringu są przeszkody, takie jak drzewa, pojedyncze budynki czy też duże zakłócenia ze strony sieci energetycznych (linie wysokiego napięcia, trakcja kolejowa).

Dzięki wykorzystaniu cyfrowej modulacji OFDM systemu CDS-5021 można stosować w dużych aglomeracjach o gęstej zabudowie i silnych zakłóceniach bez konieczności uzyskania stuprocentowej widzialności optycznej anten. W odróżnieniu od systemów analogowych, które gwarantują wysoką jakość transmitowanego obrazu jedynie przy zapewnieniu całkowitej widoczności optycznej anten, w systemach cyfrowych niewielkie przeszkody jedynie zmniejszają zasięg pracy, natomiast nie występuje w nich utrata jakości obrazu. Ponadto system CDS-5021 posiada 21 niezależnych kanałów wideo, co jest bardzo istotne przy dobieraniu sprzętu już na etapie projektowania monitoringu dla dużych obiektów.

Charakterystyka systemów serii CDS-5021:

- rozdzielczość 720×576 (D1) przy prędkości 25 kl/s (pełny PAL),
- częstotliwość pracy ISM 5,2 GHz,
- modulacja OFDM (WiMAX),
- 21 niezależnych kanałów wideo,
- transmisja szyfrowana 128-bitowym kodem,
- kompresja MPEG2,
- dynamiczne dobieranie mocy oraz wolnej częstotliwości pracy,
- bardzo wysoka odporność na zakłócenia, np. z sieci energetycznych oraz WiFi,
- wysoka odporność na krótkotrwałe zaniki oraz odbicia sygnału radiowego,
- bardzo prosty w instalacji i w pełni bezobsługowy.

Bardzo dużym ułatwieniem dla instalatorów jest także niezwykle prosta obsługa systemu cyfrowego firmy Camsat. Uruchomienie systemu CDS-5021 polega wyłącznie na ukięrkowaniu anten i podłączeniu sygnału wideo i zasilania. Nie ma konieczności szukania wolnych częstotliwości czy ustawiania kanałów pracy. W chwili włączenia zasilania w pierwszych sekundach działania urządzenie wyszukuje wolną częstotliwość na danym terenie i zapisuje kanał pracy

na stałe. Nadajnik łączy się wyłącznie z dedykowanym mu odbiornikiem zidentyfikowanym za pomocą indywidualnego kodu, przez co cały system CDS-5021 jest zabezpieczony przed podglądem osób trzecich.

Zestaw zewnętrzny CDS-5021h ma jedno wejście BNC wideo „Composite” z dwoma kanałami audio, natomiast zestaw wewnętrzny CDS-5021 jest dodatkowo wyposażony w wejście S-Video oraz zapewnia transmisję z pilota zdalnego sterowania, tzw. przedłużacza pilota (opcja).

Dzięki zastosowaniu technologii MIMO (technologia zwiększająca przepustowość łącza bezprzewodowego, polegająca na transmisji wieloantenowej zarówno po stronie nadawczej, jak i odbiorczej) uzyskano możliwość szerokiego doboru anten odbiorczych, a co za tym idzie – zwiększenia zasięgów nawet do 5 km. Dzięki ww. technologii uzyskaliśmy również większą odporność łącza na zaniki oraz odbicia sygnału radiowego.

Jednoczesny odbiór zbiorczego sygnału z kilku kierunków pozwala na wykorzystanie systemu CDS-5021 w monitorowaniu wind oraz mobilnych systemach transmisji obrazu.

Cyfrowy system CDS-5021 jest produkowany przez firmę Camsat w trzech wersjach

CDS-5021h – zewnętrzna radiolinia cyfrowa o klasie ochrony IP65 i zasięgu do 2 km (opcjonalnie 5 km) – jest przeznaczona do dużych, profesjonalnych systemów CCTV monitoringu



Fot. 1. Zewnętrzna radiolinia CDS-5021h

miejskiego, gdzie wymagana jest bardzo wysoka odporność na zakłócenia, a także skuteczne zabezpieczenia poprzez kodowanie transmisji. System ten zapewnia transmisję obrazu nawet z 21 kamer na jednym terenie, co w połączeniu z systemami analogowymi (np. TCO5808h) umożliwia budowę monitoringu z użyciem do 29 kamer.

Bardzo wysoka odporność na zakłócenia przemysłowe oraz praca w terenie zabudowanym sprawia, iż system ten świetnie nadaje się do:

- stałych połączeń wideo punkt – punkt w obszarze gęstej zabudowy miejskiej,
- pracy w pobliżu sieci energetycznej,
- pracy w pobliżu dużych sieci internetowych,
- pracy w przypadku częściowego braku widzialności optycznej anten.

CDS-5021 – zestaw wewnętrzny – jest przeznaczony do przesyłu wideo oraz audio z monitoringu wind lub innych obiektów ruchomych wewnątrz budynków na odległość do 100 m (opcjonalnie 2 km). CDS-5021 w wykonaniu wewnętrznym może pracować w środowisku zamkniętym z przeszkodami, umożliwiając np. transmisję pomiędzy pomieszczeniami, pomiędzy piętrami budynku, wykorzystanie go jako nadajnika transmitującego obraz i dźwięk np. z rejestratora DVR, z tunera satelitarnego czy odtwarzacza DVD do odbiorników TV znajdujących się w innych pomieszczeniach. Dodatkowo CDS-5021 można sterować za pomocą pilota, a więc osoba siedząca np. przed odbiornikiem TV może sterować urządzeniem znajdującym się w innym pomieszczeniu.



Fot. 2. Wewnętrzna radiolinia CDS-5021

Przeznaczenie zestawu CDS-5021:

- transmisja z monitoringu wind oraz innych obiektów ruchomych,
- transmisja wideo w obszarach silnie zakłóconych, np. w pobliżu linii energetycznych, sieci trakcyjnej, sieci internetowych WiFi, w kopalniach itp.,
- transmisja obrazów do sąsiednich pomieszczeń w szpitalach, uczelniach oraz salach konferencyjnych,
- transmisja z kamer telewizji przemysłowej CCTV oraz rejestratorów,
- transmisja obrazów z wszelkich źródeł sygnału audio-wideo, np. tunerów satelitarnych, DVD lub komputerów, do sąsiednich obiektów,
- transmisja do telebimów, wyświetlaczy wielkogabarytowych, rzutników oraz projektorów.

CDS-5021 TV – mobilna radiolinia cyfrowa – jest przeznaczona do pracy ruchomej w systemach telewizji profesjonalnej. Umożliwia transmisję obrazu z kamery operatora



Fot. 3. CDS-5021 TV – radiolinia mobilna

poruszającego się np. po scenie, stadionie w czasie imprez masowych lub z kamery umieszczonej w pojeździe przemieszczającym się. Umożliwia przesył wideo oraz audio wewnątrz budynków na odległość do 100 m, a przy wyposażeniu w większe anteny odbiorcze nawet do 800 m.

Niektóre zastosowania CDS-5021 TV:

- transmisja mobilna od poruszającego się kamerzysty do wozu transmisyjnego,
- podgląd mobilnych obrazów na planach zdjęciowych i w studiach filmowych,
- w telewizji kablowej oraz w studiach nagrań,
- mobilne filmowanie ze scen teatralnych oraz imprez masowych,
- kamery telewizji profesjonalnej oraz kamery przemysłowe CCTV,
- rejestratory DVR oraz multipleksery.

Cyfrowe systemy wideo, podobnie jak analogowe, pracują w układzie punkt – punkt, czyli jeden zestaw CDS-5021h jest przewidziany dla jednej kamery.

Przykłady doboru zestawów:

- dla obiektu z 3 kamerami: CDS-5021h x 3,
- dla obiektu z 16 kamerami: CDS-5021h x 16.

TCO 5807m – miniaturowy system wideo 5,8 GHz

Oprócz systemów cyfrowych firma P.W. Camsat wprowadziła systemy analogowe w wersji miniaturowej. TCO 5807m to najnowszy miniaturowy, bezprzewodowy zestaw pracujący w paśmie 5,8 GHz. Współpracuje ze wszystkimi dostępnymi kamerami CCTV oraz rejestratorami DVR, przysyłając obraz na odległość do 200 m z antenami prętowymi oraz



Fot. 4. System TCO 5807m

do 2 km z jedną dodatkową anteną kierunkową. Radiolinia ta została zaprojektowana również w celu zastąpienia urządzeń starej generacji pracujących w paśmie 2,4 GHz. Zapewnia ona dużo lepszą jakość obrazu oraz stabilniejszą pracę odporną na zakłócenia przemysłowe. TCO 5807m charakteryzuje się niewielkimi gabarytami, które umożliwiają montaż nadajnika wewnątrz standardowej obudowy kamery, bardzo prostą instalacją oraz przystępną ceną.

CDS-230 V – transmisja obrazu przewodami sieci energetycznej 230 V

Kolejną nowością zapowiadaną na rok 2009 jest system transmitujący obraz i dźwięk poprzez przewody energetyczne 230 V na odległość do 100 m. Wysokiej jakości transmisję gwarantuje zastosowanie standardu telewizyjnego DVB-T z regulowaną kompresją obrazu MPEG2.

Ten nowatorski system przesyła sygnały pomiędzy gniazdami 230 V w obrębie jednego obiektu niezależnie od tego, która faza jest podłączona. CDS-230 V rozwiązuje szereg kolejnych problemów instalatorów oraz znacząco przyspiesza instalację kamer. Wyjątkowo prosta instalacja systemu polega wyłącznie na podłączeniu kamery do nadajnika CDS-230 V i podłączeniu go do zasilania napię-

ciem prądem przemiennym 230 V. Obraz uzyskujemy z dowolnego gniazdka 230 V poprzez podłączenie odbiornika CDS-230 V. System ten pozwala na bardzo szybkie uruchomienie kamer w dowolnym miejscu budynku, wszędzie tam, gdzie dostępne jest zasilanie 230 V z tej samej rozdzielni (licznika). Zakres zastosowań CDS-230 V jest bardzo szeroki – od przesyłu obrazów z rejestratorów DVR i kamer do odtwarzaczy DVD czy tunerów satelitarnych.

Dzięki urządzeniom wprowadzonym do sprzedaży zdołaliśmy rozwiązać wiele problemów, z którymi spotykają się nasi klienci, nie narażając projektantów i instalatorów na wysokie koszty. Należy jednak pamiętać, iż gwarancję niezawodnego działania daje jedynie użycie oryginalnych urządzeń firmy P.W. Camsat, które posiadają wszelkie certyfikaty zgodności oraz charakteryzują się bardzo niską awaryjnością (poniżej 0,8%).

Serdecznie zapraszamy na naszą stronę internetową www.camsat.com.pl, gdzie znajdziecie Państwo opisy pełnej gamy naszych produktów, certyfikaty oraz deklaracje zgodności, cenniki, a także karty katalogowe urządzeń.

BEATA NADZIEJKO
P.W. CAMSAT

Parametry	Symbol urządzenia							
	TCO 5807h	TCO 5807m	TCO 5808h	TCO 5808	CDS 5021h	CDS 5021 & CDS 5021 TV	CDS 230V	CD04
Częstotliwość pracy	5,8 GHz	5,8 GHz	5,8 GHz	5,8 GHz	5,2 GHz	5,2 GHz	–	869 MHz
Liczba kanałów	7	7	8	8	21	21	1	10
Zasięg	1,5 - 2 km	200 m (opcja 2 km)	3 km (opcja 5 i 8 km)	2 km	2 km	100 m (opcja 2 km)	100 m	6 km
Anteny	kierunkowe zintegrowane	prętowe dookolne	kierunkowe zintegrowane	kierunkowe	kierunkowe	dookolne	–	prętowe dookolne
Moc	< 25 mW	< 25 mW	< 25 mW	< 25 mW	< 100 mW	< 100 mW	–	< 200 mW
Obudowa	IP65	wewnętrzna	IP65	wewnętrzna	IP65	wewnętrzna	wewnętrzna	IP65
Format wideo/danych	PAL lub NTSC	PAL lub NTSC	PAL lub NTSC	PAL lub NTSC	PAL 720×576 (D1) lub NTSC	PAL 720×576 (D1) lub NTSC	PAL (D1) lub NTSC	RS485 & RS232
Wejścia wideo	1 x BNC	1 x przykręcane	1 x BNC	1 x CHINCH	1 x CHINCH	1 x CHINCH (Composite) + 1 x S-Video	1 x CHINCH (Composite) + 3x CHINCH (CVBS)	–
Wejścia audio	2 x przykręcane	2 x przykręcane	2 x BNC	2 x CHINCH	2 x CHINCH	2 x CHINCH	2 x CHINCH	–
Modulacja	FM	FM	FM	FM	OFDM	OFDM	–	FM
Temperatura pracy	–20 +50°C	0 +50°C	–20 +50°C	0 +50°C	–20 +50°C	0 +50°C	0 +50°C	0 +50°C
Zasilanie	12 V _{DC}	12 V _{DC}	12 V _{DC}	12 V _{DC}	12 V _{DC}	12 V _{DC}	230 V _{AC}	12 V _{DC}
Certyfikaty	CE	CE	CE & FCC	CE & FCC	CE	CE	(OEM)	CE

Tab. 1. Porównanie parametrów urządzeń P.W. Camsat



SYGNAŁ
BEZPIECZEŃSTWA

Systemy

sygnalizacji pożarowej marki Bosch

Kompletna oferta modułów wejść/wyjść instalowanych w pętłach dozorowych



Do głównych zadań systemu sygnalizacji pożarowej (SSP) należy wczesne wykrywanie, sygnalizowanie i alarmowanie o pożarze. Współczesne budynki, wyposażone między innymi w skomplikowane urządzenia automatyki, klimatyzacji i wentylacji, stawiają jednak przed systemami sygnalizacji pożarowej również inne zadanie, jakim jest realizacja skomplikowanego scenariusza pożarowego, zapisanego przez projektanta w tabeliysterowań. W rezultacie centrala sygnalizacji pożarowej realizuje liczne funkcje z zakresuysterowań oraz monitorowania urządzeń zewnętrznych. Interfejsem pomiędzy SSP a urządzeniami zewnętrznymi są najczęściej instalowane w pętłach dozorowych moduły wejść i wyjść. Dlatego z punktu widzenia elastyczności systemu niezmiernie ważne jest, aby projektant miał do dyspozycji dużą gamę modułów, które mógłby wykorzystać w celu umożliwienia realizacji nawet najbardziej skomplikowanego scenariusza pożarowego. Celem niniejszego artykułu jest pokazanie, co w tym zakresie ma do zaoferowania Bosch. Zawarte tu informacje jedynie zarysowują możliwości naszych urządzeń i mają charakter wyłącznie poglądowy. Osoby zainteresowane tematem mają możliwość pogłębienia wiedzy podczas regularnych szkoleń technicznych, organizowanych w siedzibie firmy Robert Bosch w Warszawie

Moduły serii 420 cechuje duża różnorodność, którą Bosch osiągnął dzięki podziałowi modułów w zależności od funkcji, jaką mają spełniać, a także sposobu instalacji. W ofercie znajdują się moduły przeznaczone do sterowania, monitorowania, przyłączania linii sygnalizatorów czy innych elementów konwencjonalnych. Jeżeli zastosujemy podział zależny od sposobu instalacji, możemy wyróżnić moduły w obudowie podtynkowej, moduły przeznaczone do szyny DIN lub wybrać montaż ścienny czy wbudowany. Moduły monitorujące i sterujące, wykorzystywane do sterowania różnymi urządzeniami automatyki pożarowej, występują również w różnych konfiguracjach wyjść sterujących i wejść monitorujących, począwszy od modułów jednowyjściowych i dwuwyjściowych, a skończywszy na modułach wyposażonych w osiem dowolnie programowalnych wyjść przekaźnikowych lub osiem wejść monitorujących. Wszystkie moduły, podobnie jak inne urządzenia systemów sygnalizacji pożarowej, posiadają wymagane certyfikaty europejskie CDP lub polskie CNBOP.

Standardem, który obejmuje również moduły serii 420, jest w przypadku SSP marki Bosch wyposażenie wszystkich urządzeń instalowanych w pętłach dozorowych w zintegrowane obustronne izolatory zwarć. Nowe moduły mają również obrotowe przełączniki umożliwiające ręczne adresowanie,

oczywiście przy zachowaniu dostępnej do tej pory możliwości automatycznego adresowania z poziomu centrali. Jest to funkcja ciesząca się dużym uznaniem wśród instalatorów SSP, ponieważ umożliwia dodatkową metodę identyfikacji elementów na pętłach dozorowych. Niewątpliwym atutem jest możliwość stosowania kabla nieekranowanego przy tworzeniu pętli dozorowych (odporność na zakłócenia przetestowana w laboratorium CNBOP), a także zainstalowania do 254 elementów w pętli.

Moduły wejściowe o dowolnie programowalnym kryterium zadziałania wejścia

Rodzinę modułów tej serii zapoczątkował moduł FLM-420-I2. Urządzenie to posiada dwa indywidualnie programowalne wejścia monitorujące stany różnego rodzaju urządzeń zewnętrznych. Często na etapie projektowania systemu trudno jest określić, jakiego rodzaju sygnału (np. NC, NO) czy wartości rezystancji lub napięcia można spodziewać się pomiędzy monitorowanym urządzeniem a modułem wejść. Moduł FLM-420-I2 jest urządzeniem uniwersalnym, bez względu na rodzaj sygnału. Kryterium zadziałania jego wejścia jest dowolnie definiowalne z poziomu centrali sygnalizacji pożarowej.

Moduły wyjściowe o dużej obciążalności styku

Typowe dostępne na rynku rozwiązania zapewniają obciążalność styku wyjściowego w zakresie około 2 A/30 V_{DC}. Najczęściej jest to wartość wystarczająca, lecz zdarzają się równieżysterowania, których realizacja wymaga wykorzystania wyjścia o większej obciążalności. W przypadku oferty firmy Bosch projektant może skorzystać z możliwości modułu FLM-420-RHV, który zapewnia dwa indywidualnie programowalne wyjścia o obciążalności 10 A/230 V_{AC}. Bardzo przydatna w przypadku tego urządzenia jest również funkcjonalność wejścia zwrotnego, pozwalająca na monitorowanie czyysterowanie urządzenia w taki sposób, aby zadziało w przewidywanym czasie, odliczanym od momentu zmiany stanu wyjścia modułu FLM-420-RHV.

Moduły wielowyjściowe i wielowejściowe

Modułem doskonale sprawdzającym się w obiektach, w których występuje bardzo duża liczba sterowań, jest FLM-420-RLV8-S, który posiada osiem indywidualnie programowalnych wyjść przekaźnikowych. Zastosowanie modułu wielowyjściowego pozwala na ograniczenie liczby elementów na pętlach, obniża koszty systemu i oszczędza czas instalatora. W przypadku, gdy konieczne jest monitorowanie stanu dużej liczby urządzeń zewnętrznych, znajduje zastosowanie wielowejściowy moduł monitorujący FLM-420-I8R1-S, posiadający osiem indywidualnie programowalnych wejść i dodatkowo jedno wyjście przekaźnikowe. Kryterium zadziałania jego wejść (np. NC, NO, wartość rezystancji) jest dowolnie definiowalne z poziomu centrali sygnalizacji pożarowej.

Moduł dwóch wejść i jednego wyjścia – najbardziej popularne rozwiązanie

Chyba najbardziej typowe zastosowanie modułów monitorująco-sterujących toysterowanie pojedynczego urządzenia zewnętrznego z możliwością monitorowania jego stanu przy wykorzystaniu dwóch wejść. W ofercie firmy Bosch najczęściej stosowany w tym celu jest moduł FLM-420-RLE, który zapewnia jedno bezpotencjałowe wyjście przekaźnikowe i dwa monitorowane indywidualnie programowalne wejścia. Linie wejściowe mogą być konfigurowane zupełnie niezależnie od linii wyjściowej lub jedna z nich może zostać wykorzystana jako tak zwane wejście zwrotne, umożliwiające

sprawdzenie, czy w zadeklarowanym czasie, liczonym od momentu aktywacji wyjścia, zewnętrzne urządzenie rzeczywiście zadziało.

Moduły zapewniające wyjścia typu „otwarty kolektor”

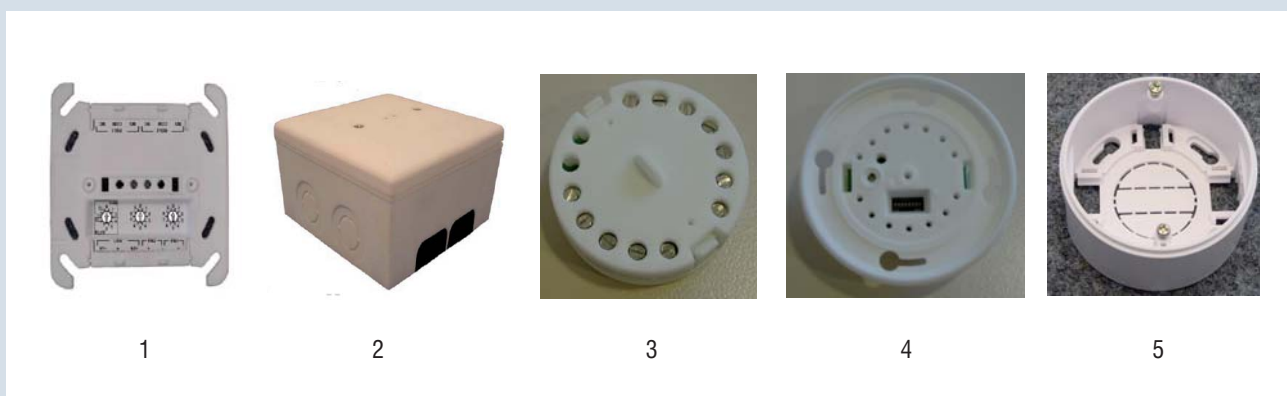
Wszystkie opisane powyżej moduły zapewniają bezpotencjałowe wyjścia przekaźnikowe. Oferta firmy Bosch zawiera jednak dodatkowo szeroką gamę modułów z wyjściami typu „otwarty kolektor” (OC). Jest to wprawdzie rozwiązanie znacznie mniej upowszechnione na rynku polskim, ale może być z powodzeniem stosowane i wydaje się warte spopularyzowania. Wychodząc z tego założenia, poniżej zamieszczamy informacje o dwóch wybranych z dostępnej oferty modułach z wyjściami typu OC.

FLM-420-O8I2 to moduł zapewniający osiem indywidualnie programowalnych wyjść typu OC i dwa monitorowane wejścia. Wyjścia typu OC są tu galwanicznie odseparowane od pętli dozorowej, a ich obciążalność wynosi 700 mA. Dlatego moduł FLM-420-O8I2, podobnie jak FLM-420-RLV8, może być wykorzystywany jako wielowyjściowy moduł sterujący we wszystkich aplikacjach, w których wymagana obciążalność styku nie przekracza 700 mA. Ponadto zaletą tego urządzenia są dwa dodatkowe wejścia, które, podobnie jak w przypadku FLM-420-I2, pozwalają na dowolne definiowanie kryterium ich zadziałania z poziomu centrali sygnalizacji pożarowej.

FLM-420-O1I1 to moduł zapewniający jedno wyjście typu OC i jedno monitorowane wejście. Parametry wejścia i wyjścia są tu identyczne jak w przypadku FLM-420-O8I2. Galwaniczne odseparowanie od pętli dozorowej oraz obciążalność 700 mA sprawiają, że FLM-420-O1I1 znajduje zastosowanie wszędzie tam, gdzie zachodzi potrzebaysterowania pojedynczego urządzenia zewnętrznego i monitorowania jego stanu.

Pętlowe sterowniki sygnalizatorów

Moduły instalowane w pętlach dozorowych systemów sygnalizacji pożarowej to nie tylko wspomniane wcześniej interfejsy wejść i wyjść. Przy zachowaniu określonych zasad projektowania możliwe jest również przyłączanie sygnalizatorów akustycznych i optycznych do sterowników będących elementami pętli dozorowej. Przykładem może tu być

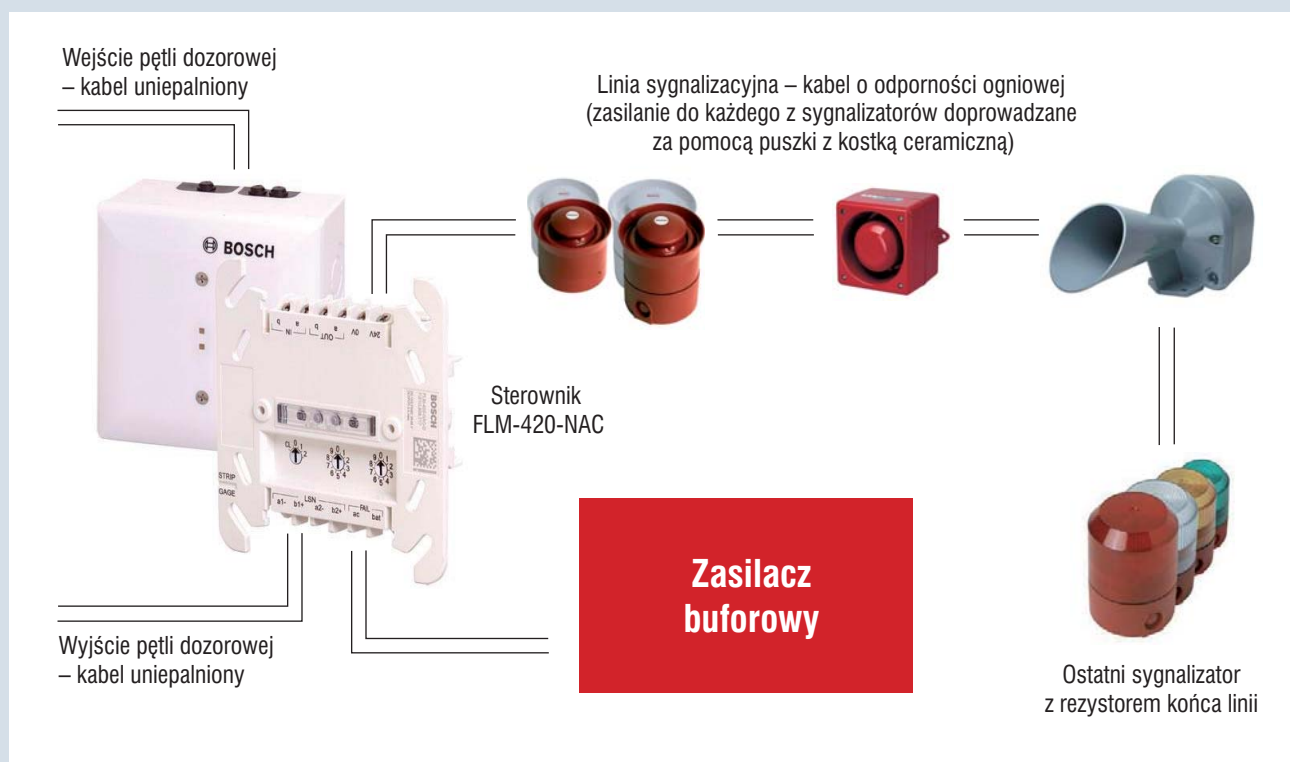


Fot. 1. Różnorodność sposobów instalacji – dostępne wersje instalacyjne modułów serii 420

- 1 – Typ D – wersja umożliwiająca instalację w szynie elektrycznej DIN
- 2 – Obudowa do instalacji powierzchniowej modułów przeznaczonych do szyny DIN
- 3 – Typ E – wersja do instalacji wbudowanej
- 4 – Typ W – wersja do instalacji naściennej
- 5 – Pokrywa modułu do instalacji naściennej

		Typ modułu									
		FLM-420-RLV1	FLM-420-12	FLM-420-RHV	FLM-420-RLV8	FLM-420-18R1	FLM-420-0812	FLM-420-0111	FLM-420-RLE	FLM-420-NAC	FLM-420-CON
Funkcjonalność	Opis	1 wyjście przekaźnikowe bezpotencjałowe	2 wejścia monitorujące	2 wyjścia przekaźnikowe bezpotencjałowe i 2 wejścia zwrotne	8 wyjść przekaźnikowych bezpotencjałowych	8 wejść monitorujących i 1 wyjście przekaźnikowe bezpotencjałowe	8 wyjść OC i 2 wejścia monitorujące	8 wyjść OC i 1 wejście monitorujące	1 wyjście przekaźnikowe i 2 wejścia monitorujące	sterownik sygnalizatorów	moduł przyłączenia 2 linii konwencjonalnych
	Możliwość indywidualnego programowania wejść i wyjść	+	+	–	+	+	+	+	+	+	+
	Bistabilny przekaźnik	+	+	+	+	+	+	+	+	+	+
	Możliwość adresowania z poziomu centrali	+	+	+	+	+	+	+	+	+	+
	Możliwość adresowania ręcznego (przełączniki obrotowe)	+	+	+	+	+	+	+	+	+	+
	Zakres temperatur pracy	od –20°C do +65°C	od –20°C do +55°C	od –20°C do +50°C	od –20°C do +65°C	od –20°C do +65°C	od –20°C do +65°C	od –20°C do +65°C	od –20°C do +50°C	od –20°C do +50°C	od –20°C do +55°C
	Obciążalność styków	maks. 5 A / 30 V _{DC}	–	maks. 10 A / 120 V _{AC} / 230 V _{AC} / 24 V _{DC}	maks. 2 A / 30 V _{DC}	maks. 2 A / 30 V _{DC}	maks. 700 mA / 30 V _{DC}	maks. 700 mA / 30 V _{DC}	maks. 1 A / 30 V _{DC}	–	–
Sposób montażu	E wbudowany	+	+	–	–	–	–	+	–	–	–
	W ścienny	+	+	–	–	–	–	–	–	–	–
	D szyna DIN I, obudowa podtynkowa	+	+	+	–	–	–	+	–	+	+
	S obudowa, montaż natynkowy	–	–	+	+	+	+	–	+	+	+

Tab. 1. Przegląd modułów serii 420 – wybrane parametry oraz dostępne wersje instalacyjne



Rys. 1. Zasada stosowania sterownika sygnalizatorów FLM-420-NAC

moduł FLM-420-NAC. Parametry i możliwości programowania tego urządzenia sprawiają, że zapewnia ono pełną funkcjonalność sterownika sygnalizatorów bez konieczności prowadzenia kabla o określonej odporności ogniowej z centrali sygnalizacji pożarowej aż do miejsca instalacji sygnalizatora. FLM-420-NAC jest bowiem instalowany w sąsiedztwie sygnalizatorów, będąc elementem pętli dozorowej prowadzonej kablem uniepalnionym (np. YnTKSY). Kabel o odporności ogniowej jest w takim przypadku wymagany jedynie na krótkim odcinku pomiędzy zasilaczem a sterownikiem sygnalizatorów oraz pomiędzy sterownikiem a sygnalizatorami. Zgodnie z obowiązującymi wymaganiami linia sygnalizacyjna zapewniana przez FLM-420-NAC jest oczywiście monitorowana ze względu na możliwe zwarcia lub przerwy. Odbyna się to na zasadzie kontrolowania rezystancji linii (rezystor końca linii na ostatnim sygnalizatorze w linii) i aktywacji sygnalizatorów w wyniku zmiany polaryzacji na właściwą w momencie zadziałania. Sposób przyłączenia sterownika FLM-420-NAC i zasadę jego działania w bardziej szczegółowy sposób przedstawia rys. 1.

Warto również wspomnieć o dodatkowej zalecanej sterownik FLM-420-NAC, którą jest synchronizacja dźwięku przyłączonych do nich sygnalizatorów. Instalowane w ramach pętli dozorowej sterowniki, aktywując kolejne linie sygnalizacyjne, synchronizują moment ich załączenia z dokładnością rzędu 3 ms. Jest to unikatowa funkcja, o której zaimplementowaniu wielu producentów niestety zapomina.

Moduły linii bocznych konwencjonalnych

Podstawą systemów sygnalizacji pożaru jest adresowalna pętla dozorowa.

Często w rzeczywistych instalacjach zachodzi jednak potrzeba integracji specjalistycznych systemów detekcji, które produkowane są przez innych producentów. Przykładem mogą być tutaj systemy zasilania i próbkowania dymu lub

liniowe czujki termiczne. Adresowalny system sygnalizacji pożarowej powinien umożliwiać przyłączenie takich urządzeń, zapewniając w tym celu dedykowane i monitorowane wejścia pożarowe. W przypadku oferty firmy Bosch rozwiązaniem jest moduł linii bocznych konwencjonalnych FLM-420-CON. Urządzenie to posiada dwa pożarowe wejścia linii bocznych konwencjonalnych, z których każde jest indywidualnie programowalne. W celu zapewnienia możliwości przyłączenia jak najszerszej gamy systemów konwencjonalnych kryterium zadziałania wejścia jest tu dowolnie konfigurowalne z poziomu centrali sygnalizacji pożarowej. Dzięki temu FLM-420-CON nie tylko umożliwia przyłączenie specjalistycznych systemów detekcji, ale również jest doskonałym rozwiązaniem w przypadkach zamiany w obiektach istniejących już systemów konwencjonalnych na nowe, adresowalne. Z przyczyn ekonomicznych taka zamiana jest często realizowana w kilku etapach obejmujących kolejne części systemu i w okresie przejściowym konieczne jest zapewnienie możliwości współpracy starych urządzeń konwencjonalnych z nowym systemem.

Wiele zintegrowanych specjalistycznych systemów detekcji charakteryzuje się dużym poborem prądu i w związku z tym wymaga doprowadzenia dodatkowego zasilania. Moduł linii bocznej konwencjonalnej FLM-420-CON pozwala na doprowadzenie zasilania do urządzeń za jego pośrednictwem. Takie rozwiązanie umożliwia monitorowanie stanu zasilacza zewnętrznego i wyświetlanie komunikatów o jego ewentualnej awarii na ekranie centrali sygnalizacji pożarowej. Oprócz dwóch wyjść komunikacyjnych do urządzeń konwencjonalnych moduł posiada dwa wyjścia zasilające, każde o wydajności 200 mA (możliwe jest podwojenie tej wartości w przypadku wykorzystania tylko jednego z wyjść).

BOSCH SECURITY SYSTEMS

Monitorowanie systemu sygnalizacji alarmu pożarowego Panasonic EBL 512 przez Internet

Obecnie żyjemy w czasach, gdy jednym z najcenniejszych dóbr jest informacja. Dostarczenie odpowiednich wiadomości na czas pozwala podjąć decyzje szybko i trafnie. Bezpieczeństwo pożarowe jest szczególnym tego przykładem. Czasami nawet ułamki sekundy decydują o ludzkim życiu

Inżynierowie Panasonic Electric Works Fire & Security Technology Europe, udoskonalając swój system sygnalizacji pożarowej, dążą m.in. do dostarczenia użytkownikowi jak największej ilości istotnych informacji w jak najkrótszym czasie.

Jednym z elementów, które wpływają na wyjątkowość systemu sygnalizacji pożarowej EBL 512, jest moduł Web Server 1598. Do tej pory informacje o pracy systemu dostępne były tylko bezpośrednio w centrali lub systemie wizualizacji. Web Server 1598 pozwala na prezentację aktualnego stanu systemu sygnalizacji pożarowej Panasonic EBL 512 na dedykowanym komputerze klasy PC z dostępem do Internetu. Ponadto moduł ma funkcje wysyłania wiadomości e-mail do wybranych użytkowników systemu oraz interfejsu do systemu wizualizacji zdarzeń. Może także współpracować z systemem przywoławczym Asom Tateco oraz służy jako dodatkowa pamięć zdarzeń (do 10000 zdarzeń).

Moduł Web Server 1598 jest to niewielkich rozmiarów skrzynka przystosowana do pionowego montażu na symetrycznej szynie DIN 35 mm. Może być zamocowana zarówno w centrali, jak i w pewnej odległości od niej. Po podłączeniu

modułu do Internetu lub lokalnej sieci LAN i po zalogowaniu się na odpowiedniej zaszyfrowanej stronie internetowej użytkownik otrzymuje dostęp do bazy danych w systemie EBL 512. Wszystkie informacje w bazie są aktualizowane na bieżąco, a strona odświeża się co dziesięć sekund. Jeśli wystąpi niezgodność danych w Web Serverze 1598 i systemie EBL 512, np. po restarcie systemu, centrala automatycznie wymusi synchronizację z modułem. Aktualizacji danych można dokonać także „ręcznie”, poprzez menu centrali lub przez program Win512.

Podstawowym oknem bazy danych o systemie sygnalizacji pożarowej jest „Informacja o systemie”. Użytkownik od razu po zalogowaniu się otrzymuje w formie tabeli następujące dane:

1. **Centrale (control units)**. Podana jest tutaj informacja o wszystkich centralach znajdujących się w systemie. Dostęp do bardziej szczegółowych danych otrzymuje się po kliknięciu na numer danej centrali.
2. **Liczba alarmów (number of alarms)**. Podana jest tutaj informacja o aktualnej liczbie alarmów w systemie (maksymalnie 200).
3. **Liczba alarmów wstępnych (number of pre-warnings)**. Podana jest tutaj informacja o aktualnej liczbie alarmów wstępnych w systemie (maksymalnie 200).
4. **Liczba stref czujek w koincydencji (number of zones/detectors in co-incidence status)**. Podana jest tutaj informacja o liczbie stref i czujek znajdujących się w koincydencji.



5. **Liczba uszkodzeń (*number of faults*)**. Podana jest tutaj informacja o liczbie uszkodzeń w systemie (maksymalnie 200).
6. **Liczba zablokowań (*number of disablements*)**. Podana jest tutaj informacja o zablokowanych elementach w systemie. Nie dotyczy to elementów zablokowanych czasowo.
7. **Liczba alarmów serwisowych (*number of detectors activating service signal*)**. Podana jest tutaj informacja o liczbie alarmów serwisowych.
8. **Liczba otwartych drzwi (*number of open doors*)**. Podana jest tutaj informacja o liczbie otwartych drzwi w centralach.
9. **Liczba stref w teście (*number of zones in test mode*)**. Podana jest tutaj aktualna informacja o strefach znajdujących się w trybie testowania.
10. **Stan połączenia RS232 (*RS232 mode*)**. Podana jest tutaj informacja o aktualnym stanie połączenia między Web Serverem i centralą EBL 512.

Moduł Web Server, oprócz dostarczenia podstawowych informacji o pracy systemu, które są dostępne od razu po zalogowaniu się na stronie, pozwala na uzyskanie dużo dokładniejszych danych o pracy zabezpieczeń przeciwpożarowych.

Menu programu do obsługi Web Servera jest wyposażone w klawisze skrótów, które pozwalają użytkownikowi błyskawicznie uzyskać dostęp do szczegółowych informacji o stanie systemu.

Skróty: „alarmy”, „alarmy wstępne”, „alarmy z czujek koincydencyjnych” oraz „alarm testowy” pozwalają na uzyskanie informacji o liczbie alarmów, dacie i czasie ich wystąpienia, strefie i adresie elementu w stanie alarmu oraz wyświetlenie informacji tekstowej przypisanej danemu zdarzeniu. Poprawna praca systemu sygnalizowana jest zielonym kolorem klawiszy skrótów, a w przypadku testów lub wystąpienia nieprawidłowości kolor zmienia się na czerwony lub żółty. Dodatkowo w przypadku alarmów testowych istnieje możliwość wysłania wiadomości e-mail zawierającej listę tych alarmów.

Informację o aktualnych uszkodzeniach, dacie i czasie ich wystąpienia, opisie oraz statusie (brak potwierdzenia lub potwierdzenie/naprawienie awarii) można uzyskać, wybierając skrót „uszkodzenia”.

Czasem jedynym sposobem zapewnienia prawidłowego funkcjonowania systemu alarmu pożarowego, np. podczas remontu czy innych prac mogących wywoływać fałszywe alarmy, jest zablokowanie poszczególnych elementów detekcyjnych lub sterujących. Jest to funkcja każdej centrali przeciwpożarowej, bez której nie byłoby możliwe użytkowanie wielu obiektów. Web Server umożliwia dokładny podgląd zablokowanych elementów systemu na bieżąco, przez co znacznie zwiększa bezpieczeństwo użytkownika danego obiektu. Po wybraniu zakładki „zablokowania” użytkownik otrzymuje dane o sześciu różnych kategoriach zablokowań: stref, punktów, pętli dozorowych, sterowań z centrali, rodzaju sterowań oraz sterowań z potwierdzeniem (*interlocking*). Informacja ta uzupełniona jest o datę i czas, adres, strefę, sposób zablokowania (ręczny lub w alarmie podczas kasowania) oraz o to, za jakie sterowanie odpowiedzialny był dany element.

Dane niezbędne dla konserwatorów systemu, a także jego użytkowników, dostarcza zakładka „alarm serwisowy”.

Umożliwia ona wyświetlenie listy wszystkich czujek, które sygnalizują konieczność dokonania ich serwisu. Oprócz tego pokazywany jest numer techniczny urządzenia, a także data i czas wystąpienia alarmu serwisowego. Konieczność serwisu jest sygnalizowana zmianą koloru zakładki z zielonego na żółty.

Moduł Web Server pozwala uzyskać na odległość informacje o pracy poszczególnych elementów detekcyjnych. Wybór zakładki „informacja o sensorach” umożliwia uzyskanie szczegółowych danych dotyczących wartości chwilowych, średniej tygodniowej oraz minimalnych i maksymalnych wartości uzyskanych przez sensory optyczne i termiczne. Sposób sortowania zorganizowano w przejrzysty sposób, który umożliwia wyszukiwanie i grupowanie sensorów zgodnie z numerem centrali, numerem linii, adresem oraz numerem technicznym. Użytkownik może stworzyć zgodnie ze swoimi wymaganiami listę elementów detekcyjnych, których pracę chce przeanalizować.

Web Server 1598 umożliwia zapis 10000 zdarzeń. Po wejściu w skrót „log zdarzeń” można wybrać rodzaj interesującego nas zdarzenia. Możliwy jest przegląd wszystkich zdarzeń albo tych, które są związane z centralą, daną strefą, punktem lub numerem technicznym. Zdarzenia wyświetlane są z podaniem numeru, daty i czasu wystąpienia oraz opisem zdarzenia.

W przypadku wystąpienia jednego lub więcej zdarzeń w systemie sygnalizacji pożarowej Web Server 1598 ma możliwość samoczynnego wysłania wiadomości e-mail do czterech wybranych użytkowników. Do wysłania wiadomości pocztą elektroniczną niezbędny jest serwer (SMTP) pracujący w sieci Ethernet LAN. W chwili wystąpienia takich zdarzeń, jak alarm pożarowy, uszkodzenie, zablokowanie, alarm serwisowy, alarm wstępny i alarm testowy, do wybranych użytkowników natychmiast wysyłany jest e-mail. Wiadomość zawiera informację o rodzaju zdarzenia i numerze prezentacyjnym punktu (strefa, adres), opis tekstowy przypisany do danego zdarzenia, numer centrali oraz datę i czas wystąpienia zdarzenia. Obecnie, gdy dostęp do Internetu zapewniają nawet telefony komórkowe, można mieć stałą kontrolę nad systemem sygnalizacji pożarowej.

Kolejną funkcją, jaką może pełnić Web Server 1598, jest praca w charakterze konwertera danych. Można w tym przypadku wyróżnić następujące zastosowania:

- przesyłanie informacji pożarowych do systemu wizualizacji na komputerze PC za pomocą konwertera EBL Talk,
- przesyłanie informacji pożarowych do systemu przywoławczego firmy Asom Tateco za pomocą konwertera Tateco.

W czasach ogólnodostępnego Internetu Web Server 1598 jest narzędziem, które wyznacza nowe standardy w zakresie eksploatacji i serwisu systemów przeciwpożarowych. Pozwala monitorować pracę systemu Panasonic EBL 512 w sposób ciągły i informować o wszystkich zdarzeniach i awariach poprzez wiadomości e-mail.

Zainteresowanych dokładnym poznanieniem tego urządzenia zapraszamy do kontaktu z firmą RAJ International, dystrybutorem systemu Panasonic EBL 512 na terenie Polski (www.raj-international.net).

RAFAŁ RUSIECKI
RAJ INTERNATIONAL



Gaszenie gazem obojętnym

Stałe urządzenia gaśnicze (SUG) to samoczynne instalacje gaśnicze, które umożliwiają automatyczne wykrycie i sygnalizację pożaru oraz rozpoczęcie akcji gaśniczej w chronionych strefach. Stałe urządzenia gaśnicze gazowe są systemami wykorzystującymi jako środek gaśniczy różnego rodzaju gazy, takie jak dwutlenek węgla, mieszaniny gazów obojętnych (np. Inergen) i gazy chemiczne (np. FM 200)



Na systemy te składają się: butle ze środkiem gaśniczym, wyzwalacz zaworu butli pilotowej, kolektor zbiorczy, rurociągi rozprowadzające, reduktory ciśnienia, czujniki przepływu, zawory, węże przyłączeniowe i sterujące oraz dysze.

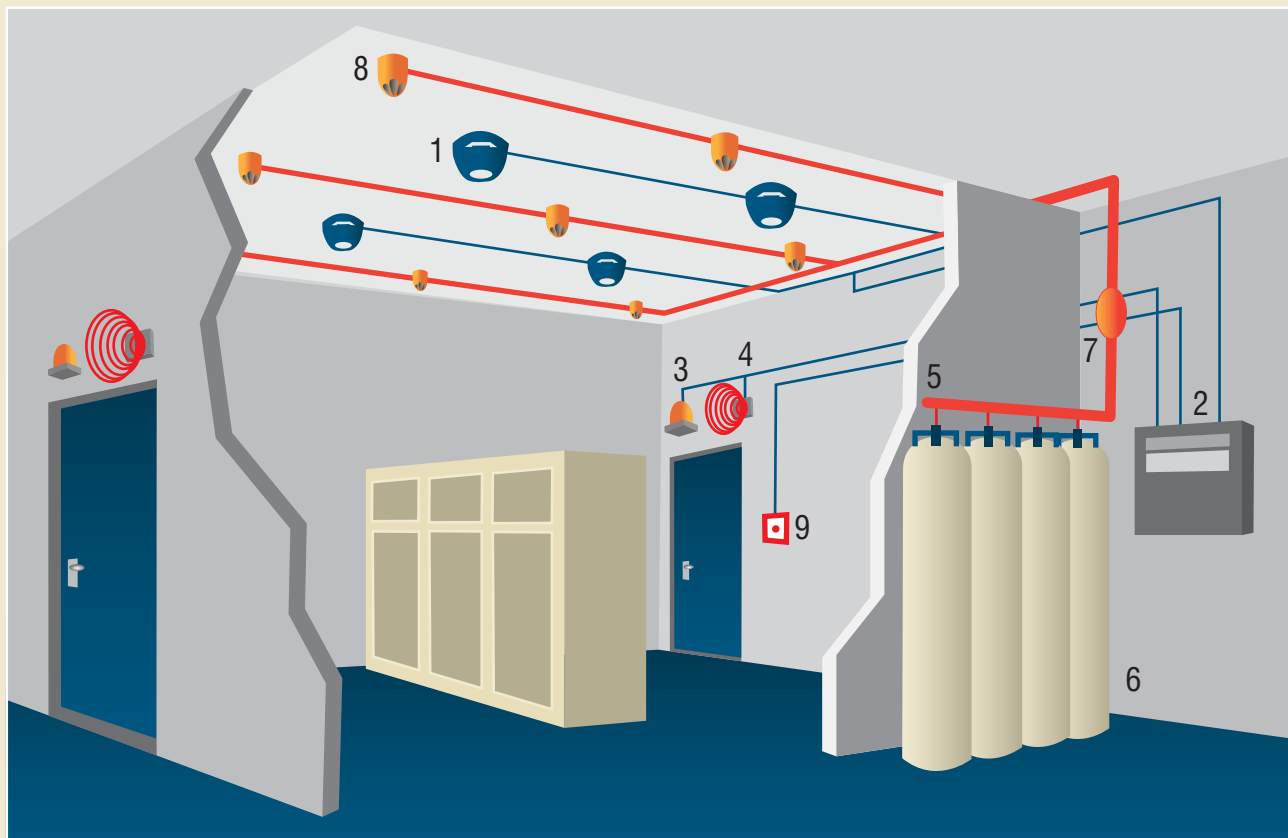
Dodatkowo w skład systemu wchodzi: centrale sterowania gaszeniem, linie dozoru z czujkami pożarowymi, przyciski ręcznego uruchomienia („START”), zatrzymania lub wstrzymania gaszenia („STOP”), różnego rodzaju urządzenia alarmowe (np. sygnalizatory akustyczne, sygnalizatory optyczne) itp. Coraz częściej poza punktowymi czujkami pożarowymi do uruchomienia instalacji gaśniczej stosuje się zasysające systemy detekcji dymu.

Skuteczność stałego urządzenia gaśniczego gazowego zależy od projektu, który należy dostosować do wymagań danego obszaru. Parametry dyszy, rurociągów, reduktorów ciśnienia oraz pozostałych elementów powinny zostać dobrane w taki sposób, aby w przypadku wystąpienia pożaru i uruchomienia instalacji gaśniczej umożliwiły wypełnienie chronionego obszaru gazem gaśniczym o odpowiednim stężeniu w zakładanym czasie. Dodatkowo dzięki właściwemu przygotowaniu chronionego obszaru/pomieszczenia stężenie gaśnicze powinno się utrzymywać odpowiednio długo.

Systemy gaszenia gazem są stosowane w obiektach, w których duże znaczenie ma wartość materialna przedmiotów i niezawodność urządzeń. Do takich pomieszczeń zaliczamy m.in. pomieszczenia komputerowe, serwerownie, centra telefoniczne, centra przetwarzania danych, laboratoria, pomieszczenia podwyższonej czystości (tzw. *clean rooms*), archiwa, sale muzealne, rozdzielnie elektryczne, transformatorownie, stacje przekątnikowe, magazyny cieczy łatwopalnych, magazyny taśm i innych nośników danych, hale pro-

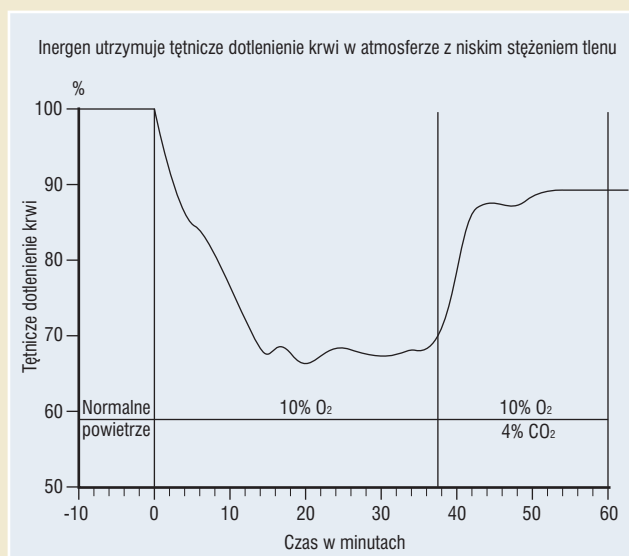
dukcyjne i wiele innych miejsc, w których występuje ryzyko powstania dużych strat lub przerwania nieustannie trwających procesów krytycznych.

Konieczność zapewnienia ochrony przeciwpożarowej takich miejsc, jak wymienione powyżej, motywowała do pracy nad stworzeniem idealnego gazu gaśniczego. Po wielu latach prac wydawało się, iż wynaleziono rodzinę idealnych gazów, zwanych potocznie halonami. Gazy te charakteryzowały się bardzo dobrą skutecznością gaśniczą przy stężeniu kilku procent i nie powodowały szkód wtórnych, jednakże, jak się później okazało, miały negatywny wpływ na środowisko naturalne. Skład strukturalny chemiczny tych gazów powodował, iż wchodziły one w reakcje z ozonem znajdującym się w atmosferze, powodując jego niszczenie. Ponadto niekorzystną cechą tych gazów był czas rozkładu w atmosferze. Mając na uwadze zagrożenie powiększania efektu cieplarnianego oraz tzw. dziury ozonowej, w latach 90. podjęto decyzję o wycofaniu halonów z użycia. Skutkiem tego było stworzenie Protokołu Montrealskiego, ratyfikowanego przez Polskę w 1990 roku. Jego celem było wycofanie halonów z użycia. Lata 90., zarówno w Polsce, jak i w Unii Europejskiej, były okresem, w którym gazy te wycofywano z produkcji i stosowania. Zakazano także sprowadzania ich na teren UE. Definitywny koniec stosowania halonów nastąpił na początku XXI wieku, kiedy weszła w życie Dyrektywa Unii Europejskiej nr 2037/2000. Nakładała ona obowiązek wycofania halonów z istniejących urządzeń gaśniczych do końca 2003 roku. Wyjątek stanowiły tzw. krytyczne odstępstwa od dyrektywy, w przypadku których po tym okresie można było w dalszym ciągu wykorzystywać te gazy. Odstępstwa te dotyczyły lotnictwa oraz zastosowań w pojazdach i obiektach wojskowych.



Rys. 1. Przykładowa jednostrefowa instalacja gaśnicza:

1. Automatyczna czujka pożaru 2. Centrala sterowania gaszeniem 3. Sygnalizator optyczny 4. Sygnalizator akustyczny 5. Elektromagnes zaworu butli pilotowej 6. Zbiorniki z gazem 7. Reduktory ciśnienia 8. Dysza gaśnicza 9. Przycisk uruchomienia ręcznego



Rys. 2. Korzystny wpływ dodatku dwutlenku węgla do atmosfery na dotlenienie mózgu człowieka

System Inergen zainstalowany w pomieszczeniu elektronicznego przetwarzania danych (przykład)

- pojawienie się dymu
- aktywacja pierwszej czujki, uruchomienie akustycznej sygnalizacji ostrzegawczej, przygotowanie do ewakuacji
- aktywacja drugiej czujki, uruchomienie akustyczno-optycznej sygnalizacji ostrzegawczej, zwłoka czasowa (ok. 30 s), przekazanie sygnału o pożarze do centrali SSP i (lub) straży pożarnej, ewakuacja
- koniec zwłoki czasowej, wyzwolenie gazu, po ok. 60 s spadek stężenia tlenu w pomieszczeniu poniżej 13,8% i wzrost stężenia dwutlenku węgla do 2,5%
- początek utrzymywania stężenia gaśniczego, stężenie tlenu na poziomie 12,5%, stężenie dwutlenku węgla na poziomie 3,2%
- koniec opróżniania gazu Inergen z butli po ok. 60 sekundach

Rodzaj gazu	Powietrze	Inergen	Powietrze + Inergen*
Azot	78%	52%	67,3%
Tlen	21%	-	12,5%
Argon	1%	40%	17%
Dwutlenek węgla	0,03%	8%	3,2%

* Trzecia kolumna pokazuje skład mieszaniny powietrza i Inergenu po wyładowaniu do pomieszczenia przy współczynniku wypełnienia 0,51 m³/m³ (stężenie projektowe 40%)

Tab. 1. Porównanie składu gazu Inergen i powietrza

Wycofanie i zakaz stosowania halonów przyczyniły się do wzmożenia prac nad stworzeniem nowych gazów gaśniczych oraz udoskonalaniem i poprawą skuteczności gazów istniejących, które mogłyby skutecznie zastąpić halony. Miały one mieć podobne parametry gaśnicze, a jednocześnie nie wpływać negatywnie na środowisko naturalne. Prace nad znalezieniem równie skutecznych gazów skupiły się wokół gazów chemicznych i obojętnych. Wynikiem tego było opracowanie i rozwój gazów chemicznych, takich jak FM 200 czy Novec. Zespoły badawcze pracowały również nad efektywnym wykorzystaniem gazów obojętnych, które wyróżnia to, że nie biorą one udziału w reakcjach chemicznych oraz są nieszkodliwe dla środowiska naturalnego. W skład mieszanin obojętnych gazów gaśniczych wchodzi tylko naturalnie występujące w atmosferze gazy. Do gazów obojętnych zaliczamy hel, argon, krypton i ksenon. Również inne gazy, takie jak azot i dwutlenek węgla, nie biorące udziału w procesie spalania i nie powodujące powstawania produktów rozkładu, mogą zachowywać się w ogniu jak gazy obojętne.

Przykładem takiego gazu jest Inergen, w skład którego wchodzi jedynie otaczające nas gazy, naturalnie znajdujące się w atmosferze, czyli te, którymi oddychamy. W związku z tym nie jest on szkodliwy dla środowiska naturalnego.

Nazwa Inergen pochodzi z kombinacji słów *inert gas* (gaz obojętny) i *nitrogen* (azot). Inergen jest mieszaniną azotu, argonu i niewielkiej ilości dwutlenku węgla. Gaśnicze działanie Inergenu polega na redukcji stężenia tlenu w powietrzu w pomieszczeniu do wartości pomiędzy 12% a 15%.

W przypadku wybuchu pożaru najważniejsze jest zapewnienie bezpieczeństwa i ewakuacja ludzi. Inergen jest magazynowany w postaci gazowej. Podczas wyładowania do pomieszczenia ogarniętego pożarem jest niewidoczny, więc nie powoduje spadku widoczności, umożliwiając tym samym bezpieczną ewakuację ludzi.

Z uwagi na ewentualne produkty spalania powstające podczas pożaru ludzie powinni być ewakuowani z pomieszczenia gaszonego gazową instalacją gaśniczą, jednakże może się zdarzyć, że z różnych przyczyn pozostaną w takim pomieszczeniu. Niewielka ilość dwutlenku węgla w Inergenie zwiększa poziom CO₂ w pomieszczeniu do ok. 3–4%, dzięki czemu człowiek jest skłaniany do głębszego oddychania, przez co transfer tlenu do tkanek jego organizmu ulega wspomaganii. Krótko mówiąc, Inergen zapewnia dotlenienie mózgu zbliżone do tego, które jest zapewnione przez powietrze o tradycyjnym składzie, a jednocześnie w pomieszczeniu utrzymany jest właściwy skład atmosfery gaśniczej. Rysunek 2 przedstawia proces różnicowania się poziomu tlenu we krwi w normalnej atmosferze, atmosferze z zawartością 10% tlenu bez dwutlenku węgla (w obecności innych gazów obojętnych) oraz z zawartością 10% tlenu i 4% dwutlenku węgla (Inergen).

Aby mógł powstać pożar, wymagane są: ciepło, paliwo oraz tlen. Podczas wyładowania gazu Inergen do pomieszczenia stężenie tlenu spada z poziomu 21% poniżej 15%, powodując zatrzymanie procesu spalania. Azot i argon, jako składniki Inergenu, redukują tlen w powietrzu wypełniającym pomieszczenie. Argon pełni także inną, nie mniej istotną rolę w procesie gaszenia. Za sprawą swojego ciężaru właściwego powoduje, że Inergen ma podobną gęstość do powietrza. W związku z tym stężenie gaśnicze Inergenu można utrzymać w pomieszczeniu przez 10 minut, a nawet

dłużej (w zależności od szczelności pomieszczenia). W przeciwieństwie do innych środków gaśniczych wykorzystujących substancje chemiczne Inergen znacznie dłużej utrzymuje atmosferę gaśniczą w chronionym pomieszczeniu.

Detekcja pożaru odbywa się za pomocą czujek, montowanych z reguły na suficie pomieszczenia. Typ zastosowanych czujek zależy od rodzaju pożaru, jaki może wystąpić. Po wykryciu pożaru czujka wysyła sygnał do centrali sterującej gaszeniem. Kiedy pożar zostanie wykryty przez pierwszą czujkę, uaktywnia się sygnalizator akustyczny zamontowany wewnątrz chronionego pomieszczenia, informując tym samym o konieczności ewakuacji ludzi z zagrożonej strefy. Po wykryciu pożaru przez drugą czujkę rozpoczyna się procedura gaszenia. Urządzenia mogą zostać wyłączone, klapy pożarowe w kanałach wentylacyjnych zostają zamknięte, aby zapobiec dostawianiu się do pomieszczenia świeżego powietrza z zewnątrz, po czym następuje odliczanie czasu zwłoki do wyzwolenia Inergenu.

Instalację gaśniczą Inergen można też uruchomić ręcznie, za pomocą przycisku zamontowanego przed wejściem do chronionego pomieszczenia.



Fire & Security

Firma **ADT Fire and Security** to światowy lider w dziedzinie elektronicznych systemów zabezpieczeń, szeroko rozumianej ochrony przeciwpożarowej oraz sterowania ruchem ulicznym. Powstała z połączenia ADT Poland oraz Tyco Fire and Integrated Solutions – siostrzanych firm międzynarodowego koncernu Tyco International – największego na świecie producenta i dostawcy systemów gaszeniowych oraz elektronicznych systemów bezpieczeństwa. Bezpośredni związek ADT Fire and Security z Grupą Tyco International, pozwala na korzystanie z bogatego zaplecza inżynieryjnego, technologicznego i finansowego międzynarodowego koncernu oraz ponad stu trzydziestoletniej tradycji obu organizacji ADT i TFIS. Ekspert ADT Fire and Security pracują wspólnie, dzieląc się wiedzą i doświadczeniem, jakiej żadna inna firma na rynku nie może zaoferować swoim klientom w jednym miejscu. ADT Fire and Security zapewnia kompleksową realizację rozwiązań – poprzez projektowanie, instalację, uruchomienie, konserwację i serwis, w zakresie systemów kontroli dostępu, systemów nadzoru wizyjnego, systemów wykrywania i sygnalizacji pożaru, dźwiękowych systemów ostrzegawczych, stałych instalacji gaśniczych, systemów sygnalizacji włamania i napadu, elektronicznych systemów przeciwwkradzieżowych, systemów BMS/HMS oraz integracji systemów bezpieczeństwa.

Po zakończeniu odliczania czasu zwłoki zawór na butli pilotowej zostaje otwarty za pomocą wyzwalacza elektromechanicznego. Następnie Inergen z butli pilotowej otwiera poprzez rurociąg sterujący zawory butli gaśniczych, po czym gaz dostaje się do kolektora oraz rurociągów gaśniczych i dysz.

Stale urządzenia gaśnicze gazowe, wykorzystujące jako środek gaśniczy obojętne gazy, ewoluowały od czasu swoich początków. Wieloletnie badania i doświadczenia laboratoryjne, jak również wprowadzony wymóg obligatoryjnego posiadania odpowiednich certyfikatów i dopuszczeń do stosowania (w Polsce – znaku budowlanego B), przyczyniły się do szukania jeszcze nowszych rozwiązań. W wyniku zastosowania odpowiednich materiałów oraz nowoczesnej konstrukcji elementów możliwe stało się przechowywanie tych gazów pod ciśnieniem 300 barów, dlatego współcześnie instalacje nie wymagają już znacznych powierzchni do składowania butli z gazem, przez co zmniejszyły się również koszty samej instalacji. Dzięki niewielkim kosztom ponownego uzupełnienia środka gaśniczego także ich użytkowanie jest dużo tańsze niż eksploatacja instalacji wykorzystującej gazy chemiczne. Należy podkreślić, że odpowiedni dobór mieszanki tych gazów zapewnia obecnie bardzo dobrą skuteczność gaśniczą. Aktualnie stale urządzenia gaśnicze, wykorzystujące jako środek gaśniczy gazy obojętne, spełniają podstawowe wymogi stawiane tego typu instalacjom, tzn. zapewniają bezpieczeństwo ludziom, chronią mienie i środowisko naturalne.

RAFAŁ CZERNICKI
ADT FIRE AND SECURITY

www.MAGICARD.com.pl

Enduro

**Dowolne nadruki na kartach
możesz wykonać sam!**

SPRAWDŹ AKTUALNE PROMOCJE!!!



- Intuicyjny interfejs graficzny w postaci paska ikon stanowiących skróty do najczęściej używanych opcji z menu programu
- Odczyt zdarzeń z kontrolerów w trybie „on-line” i zapis do archiwum na dysku serwera
- Odbiór alarmów i wyświetlanie ich na liście w oknie alarmowym
- Możliwość współpracy poprzez sieć LAN/WAN lub RS-232/422/485 z wieloma kontrolerami - do 2000 urządzeń w systemie
- Współpraca z różnymi typami baz danych: MS Access, SQL, ORACLE

NAM – Novus Access Manager to profesjonalny program nadzorczy umożliwiający zarządzanie systemem kontroli dostępu poprzez sieć LAN/WAN lub RS-232/422/485.

NAM powstał jako przyszłościowa platforma, nieustannie rozwijana, z myślą o integracji nowych kontrolerów oraz rozszerzaniu funkcjonalności systemów kontroli dostępu pracujących pod jego nadzorem.

Aktualnie **NAM** współpracuje z kontrolerami typu NVAC-C300CKF zintegrowanymi z czytnikami biometrycznymi oraz z czytnikami kart zbliżeniowych NVAC-100C/200CK. W przyszłości możliwa będzie również współpraca z bardziej zaawansowanymi kontrolerami, modułami wejść/wyjść sterujących oraz realizacja takich funkcji jak kontrola obecności i rozliczanie czasu pracy (RCP).



Kontroler NVAC-300CKF

komunikacja w systemie z wykorzystaniem technologii IP ■ 11 trybów pracy (kombinacje: palec, karta, kod)
■ możliwość skanowania 2 lub 4 palców ■ możliwość programowania przy pomocy klawiatury i wyświetlacza LCD lub programu NAM z PC ■ współpraca z czytnikami kart zbliżeniowych NVAC-100C/200CK



Czytniki kart zbliżeniowych NVAC-100C/200CK

wyjście Wieganda w formacie 26-37 bitów ■ odczyt kart typu Mifare i iClass HID (13,56 MHz)
lub typu UNIQUE i HID Standard (125 kHz) ■ współpraca z NVAC-300CKF działającym z programem NAM



Skaner linii papilarnych NVAC-FPS

czytnik linii papilarnych administratora programu NAM ■ instalacja i współpraca z programem NAM
poprzez port USB ■ skaner optyczny, rozdzielczość 500 dpi



Czytnik kart zbliżeniowych NVAC-CR/H

czytnik kart zbliżeniowych administratora programu NAM ■ instalacja i współpraca z programem NAM
poprzez port USB ■ odczyt kart na częstotliwości 13,56 MHz typu Mifare i iClass



Moduł bezpieczeństwa NVAC-RM

moduł przekaźnikowy do współpracy z kontrolerem NVAC-300CKF poprzez cyfrowe łącze komunikacyjne
■ bezpieczne sterowanie zamkiem elektrycznym ■ możliwość podłączenia przycisku wyjścia ■ dodatkowy
przełącznik do sterowania syreną alarmową



Przykładowy schemat połączeń

Biometria z NOVUSA

część 2

W numerze 1/2009 *Zabezpieczeń* zaprezentowałem Państwu nowy produkt marki NOVUS – kontroler biometryczny NVAC-300CKF. W przypadku pojedynczego przejścia kontroler ten pracuje w trybie autonomicznym i jego funkcjonalność zawarta w wewnętrznym programie obsługi jest wystarczająca. Gdy system obejmuje kilka lub kilkadziesiąt przejść, niezbędny staje się program nadzorczy zainstalowany na komputerze, który poprzez sieć typu LAN/WAN umożliwia administrowanie kontrolerami i całym systemem



NVAC-FPS

Co to jest NAM?

NAM to skrót nazwy programu – *Novus Access Manager*. Jest to specjalizowany program nadzorczy, który umożliwia zarządzanie siecią kontrolerów NVAC-300CKF.

NAM powstał jako przyszłościowa platforma, nieustannie rozwijana, w celu integracji nowych kontrolerów oraz rozszerzania funkcjonalności systemów kontroli dostępu pracujących pod jego nadzorem.

Aktualnie NAM współpracuje z kontrolerami typu NVAC-C300CKF oraz czytnikami NVAC-100C/200CK. W przyszłości możliwa będzie również współpraca z bardziej zaawansowanymi kontrolerami, modułami wejść/wyjść sterujących oraz realizacja takich funkcji, jak kontrola obecności i rozliczanie czasu pracy (RCP).

Podstawowe cechy programu NAM:

- intuicyjny interfejs graficzny w postaci paska ikon stanowiących skróty do najczęściej używanych opcji z menu programu;
- możliwość współpracy poprzez sieć LAN/WAN lub RS422/485 z wieloma kontrolerami (do 2000 kontrolerów w systemie);
- odczyt zdarzeń z kontrolerów w trybie *on-line* i zapis w archiwum na dysku serwera;
- odbiór alarmów i wyświetlanie ich na liście w oknie alarmowym;
- zdalna konfiguracja parametrów kontrolerów;
- zarządzanie bazą danych użytkowników;
- współpraca z czytnikiem odcisków administratora poprzez port USB;
- współpraca z czytnikiem kart administratora poprzez port COM;
- grupowa aktualizacja parametrów i użytkowników;
- wybór języka menu operatora;
- zdalne operacje na grupach urządzeń;
- selektywne raporty dotyczące urządzeń, użytkowników i zdarzeń;
- możliwość automatycznego (zgodnie z terminarzem) wykonania kopii systemu oraz jej kompresji;
- współpraca z różnymi typami baz danych: MS Access, SQL, Oracle.

Na pierwszy rzut oka, po zainstalowaniu, program może wydawać się bardzo prosty, ale w rzeczywistości zawiera on szereg bardzo użytecznych dla administratora funkcji, co wiadać po bliższym zapoznaniu się z nim. Szczegółowe informacje dotyczące programu zawarte są w instrukcji obsługi, w poniższym artykule zajmiemy się wybranymi, najciekawszymi funkcjami.

Proces instalacji programu przebiega w języku angielskim. Po zakończeniu instalacji i uruchomieniu programu operator ma możliwość wyboru jednego z czterech języków, w jakim będzie wyświetlane menu – w tym oczywiście języka polskiego. Dostęp do programu zabezpieczony jest domyślnym hasłem, które należy zmienić po pierwszym uruchomieniu. Można również ustawić kolejnych operatorów z pełnym lub ograniczonym dostępem.

Przed przystąpieniem do programowania systemu należy również wybrać typ bazy danych, z którym program będzie współpracować. Domyślnym ustawieniem jest baza MS Access. Istnieje również możliwość wyboru takich baz danych, jak:

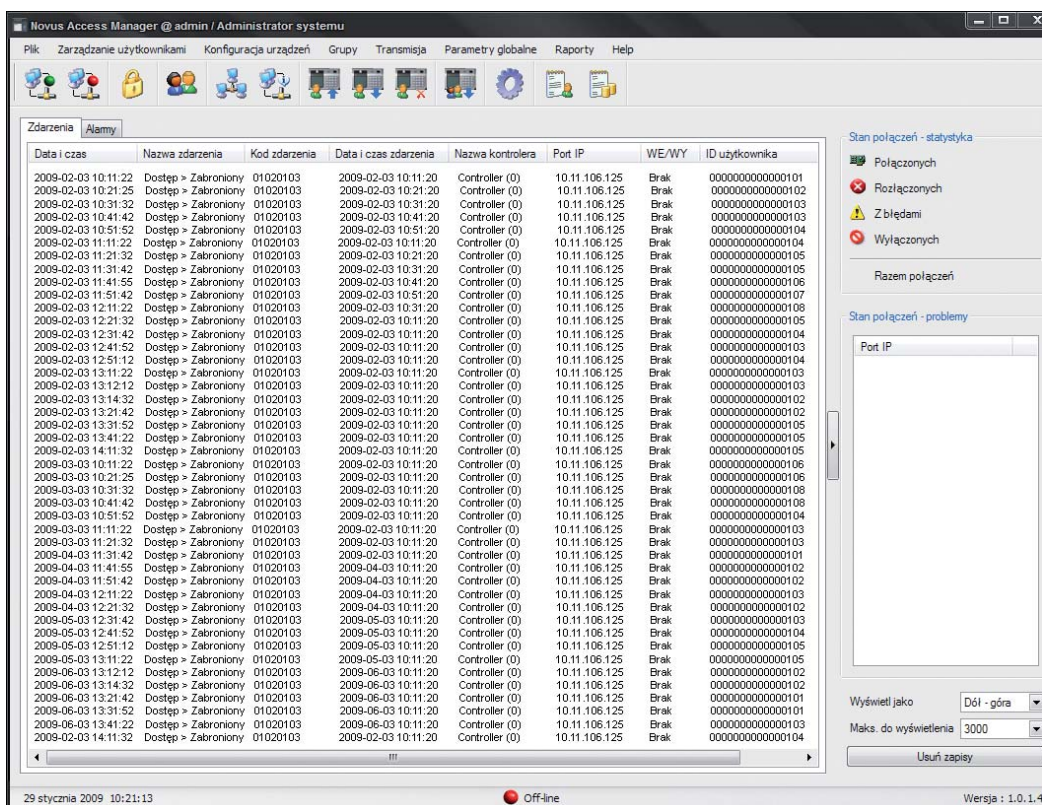
- SQL Server,
- Oracle,
- MySQL.

Warunkiem współpracy z bazą danych jest oczywiście uprzednie zainstalowanie odpowiednich aplikacji. W systemach, które obejmują więcej niż 100 kontrolerów lub ponad 1000 użytkowników, zaleca się współpracę z bazą SQL lub Oracle.

Pulpit operacyjny programu przedstawiono na rys. 1. Główną jego część stanowi okno zdarzeń, które można przełączyć na okno alarmów. Zdarzenia i alarmy wyświetlane w tym oknie odczytywane są na bieżąco poprzez sieć z kontrolerów NVAC-300CKF.

W górnej części ekranu zlokalizowany jest pasek rozwijanego menu, a poniżej znajdują się ikony stanowiące skróty do najczęściej używanych opcji.

Na uwagę zasługuje rozwijana pionowa zakładka z prawej strony ekranu. Umożliwia ona kontrolę komunikacji w całej sieci kontrolerów oraz wykonanie kilku operacji związanych z wyświetlaniem zdarzeń i alarmów.



Rys. 1. Pulpit operacyjny programu NAM

Opcjonalnie stanowisko administratora programu NAM można wyposażać w:

- skaner odcisków palców typu NVAC-FPS, który dołączony jest do portu USB komputera i umożliwia wpisywanie wzorców odcisków bezpośrednio do bazy danych,
- czytnik kart typu *desktop*, który umożliwia odczyt numerów kart i ich zapis w bazie danych.

Pięć najważniejszych funkcji programu, które zostaną przedstawione w dalszej części artykułu, to:

- programowanie struktury sieci systemu,
- definiowanie bazy użytkowników,
- wymiana informacji z kontrolerami,
- monitorowanie stanu sieci kontrolerów,
- archiwizacja zdarzeń i generator filtrowanych raportów.

Programowanie struktury sieci systemu

Rozwój technologii transmisji danych, coraz tańszy sprzęt komputerowy o ciągle rosnących możliwościach obliczeniowych, a także coraz bezpieczniejsze i stabilniejsze sieci komputerowe otworzyły nowe możliwości dla branży zabezpieczeń.

System kontroli dostępu bazujący na IP charakteryzują następujące cechy:

- dzięki sieci komputerowej zarządzanie i monitorowanie może odbywać się z dowolnej lokalizacji;
- łącza internetowe sprawiają, że zasięg systemu staje się teoretycznie nieograniczony – odległość kontrolera od komputera z programem nadzorczym NAM nie jest limitowana zasięgiem transmisji pojedynczego kabla;
- ograniczenie kosztów instalacji oraz uruchomienia i konserwacji systemu dzięki wykorzystaniu okablowania strukturalnego;
- skalowalność – system można rozbudować w prosty sposób, dodając kolejne kontrolery.

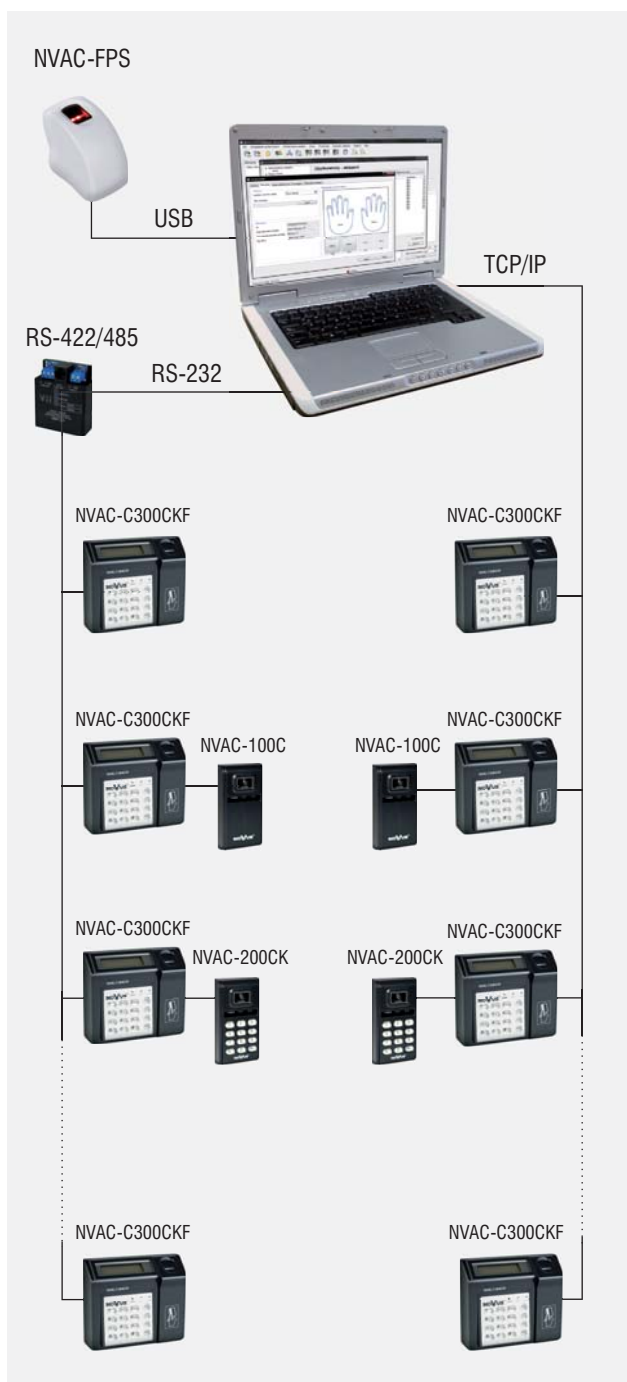
Po zainstalowaniu programu pierwszą czynnością konfiguracyjną powinno być zdefiniowanie struktury sieci kontrolerów. Możliwości systemu w tym zakresie przedstawia schemat blokowy przedstawiony na rys. 2. Cała struktura systemu opiera się na magistralach komunikacyjnych. Każda magistrala może zawierać do 14 kontrolerów. Liczba magistral w systemie nie jest limitowana, ale cały system może objąć maksimum 2000 kontrolowanych jedno- lub dwustronnie przejść. Program automatycznie wyszukuje w sieci kontrolery NVAC-300CKF według adresów MAC. Wyszukane w sieci kontrolery można przypisać do zdefiniowanych uprzednio magistral, a następnie zabezpieczyć hasłem komunikacyjnym. Każdy z kontrolerów może mieć podłączony dodatkowy czytnik (biometryczny lub zbliżeniowy). Taki zestaw umożliwia realizację kontroli wejścia/wyjścia, a z punktu widzenia sieci widziany jest jako jedno kontrolowane przejście. Każdy z elementów sieci (magistrala lub kontroler) może być okresowo wyłączony z monitorowania poprzez zaznaczenie odpowiedniej opcji w formularzu elementu.

Dzięki wykorzystaniu komunikacji poprzez sieć LAN/WAN system może obejmować wiele obiektów zlokalizowanych w różnych budynkach lub miastach. Pozwala to również w wielu przypadkach zaoszczędzić na kosztach instalacji dzięki możliwości wykorzystania istniejącego okablowania strukturalnego.

Definiowanie bazy użytkowników

Baza danych dotycząca użytkowników jest bardzo znaczącym logicznym elementem systemu. W przypadku pojedynczych kontrolerów pracujących w trybie autonomicznym baza taka może zostać utworzona bezpośrednio w pamięci urządzenia. W większych systemach wykorzystujących program NAM baza taka jest tworzona na komputerze, a następnie może zostać rozesłana do kontrolerów. Istnieje również możliwość odczytania bazy z kontrolera, a następnie zapisania jej w programie NAM.

Baza użytkowników zawiera formularze z danymi. Podstawowym parametrem w tej bazie jest unikatowy numer identyfikacyjny użytkownika (ID). Numer może zawierać do 16 cyfr i jest weryfikowany za każdym razem, gdy dodajemy nowego użytkownika, tak, aby uniknąć duplikacji. Do ID przypisane są wszystkie pozostałe dane:



Rys. 2. Schemat blokowy systemu

- nazwisko i imię,
- numer karty,
- wzorce odcisków palców,
- zdjęcie,
- poziom dostępu,
- dział/wydział,
- dane adresowe.

W aktualnej wersji programu dane wpisuje się ręcznie, wypełniając pola w formularzu. W przyszłości dostępny będzie podprogram importujący dane użytkowników z pliku wytworzonego w programie MS Excel.

W celu przyspieszenia zmian wybranych parametrów w formularzach użytkowników w programie NAM dostępna jest funkcja modyfikacji grupowej.

Po zdefiniowaniu operator może przesłać bazę danych użytkowników do kontrolerów w sieci.

Wymiana informacji z kontrolerami

Jest to bardzo istotna funkcja programu NAM. Dzięki niej nie ma potrzeby indywidualnego programowania każdego z kontrolerów.

Pracujące w sieci kontrolery NVAC-C300CKF po przesłaniu do nich danych z programu NAM mogą pracować autonomicznie, ale oczywiście zawsze istnieje potrzeba przynajmniej okresowej wymiany informacji pomiędzy kontrolerami i programem NAM.

Jeżeli kontrolery pracują w trybie sieciowym z włączonym programem NAM, to wówczas wymiana informacji odbywa się w sposób ciągły. Program NAM łączy się kolejno według nadanych adresów IP lub po RS485 z każdym z kontrolerów i odczytuje z ich pamięci zdarzenia. Dzięki temu na pulpicie operatora mamy na bieżąco wyświetlane zdarzenia i alarmy, a w prawej zakładce stan komunikacji z poszczególnymi kontrolerami.

Oprócz odczytu zdarzeń dwukierunkowa wymiana informacji obejmuje również:

- odczyt listy użytkowników z kontrolerów,
- odczyt danych dotyczących użytkowników (numery kart, wzorce),
- przysyłanie danych dotyczących użytkowników do kontrolerów,
- usuwanie danych dotyczących użytkowników z kontrolerów,
- kasowanie zdarzeń z pamięci kontrolerów,
- ustawianie parametrów pracy kontrolerów (daty i czasu, terminarzy, dni świątecznych, stref czasowych i okresów ważności, języka, hasła komunikacyjnego).

Wszystkie te operacje są dostępne wyłącznie dla uprawnionego administratora, który ma przypisane hasło dostępu do programu NAM.

Monitorowanie stanu sieci kontrolerów

Program NAM jako proste oprogramowanie administracyjne nie posiada zbyt rozbudowanej wizualizacji stanu systemu, niemniej jednak umożliwia monitorowanie na bieżąco stanu komunikacji z kontrolerami dołączonymi do obu typów magistral (TCP i RS485). Sumaryczny status komunikacji z podziałem na kontrolery połączone, rozłączone i z problemami wyświetlany jest w prawej rozwijanej zakładce.

Bardziej szczegółowe informacje o stanie komunikacji można otrzymać, klikając na ikonę „Status magistrali”.

Po przejrzaniu całej sieci program wyświetla listę wszystkich kontrolerów skonfigurowanych w systemie. W przypadku kontrolerów, z którymi jest bieżąca komunikacja, wyświetlane są również dane dotyczące adresu, wersji programu producenta (firmware) itp.

Niezależnie od tych informacji komunikaty o utracie lub przywróceniu komunikacji z kontrolerem wyświetlane są w oknie alarmowym.

Archiwizacja zdarzeń i generator filtrowanych raportów

W trakcie pracy systemu generowane są zdarzenia, które są wyświetlane na pulpicie operatora w oknie zdarzeń i alarmów, a następnie zapisywane w archiwum zdarzeń. Zdarzenia są generowane w kontrolerach, jak również w programie NAM. Zarchiwizowane zdarzenia mogą być następnie wykorzystane do wygenerowania raportu.

W praktyce rzadko generuje się raport zawierający wszystkie zdarzenia zawarte w archiwum ze względu na znaczną objętość i utrudnioną analizę. W procesie generowania raportu powszechnie wykorzystuje się filtrację, która umożliwia wydruk raportu zawierającego tylko interesujące nas zdarzenia. Program NAM w opcji „Raporty” zawiera zestaw filtrów, które to umożliwiają.

Najważniejsze filtry to:

- zakres daty i czasu,
- rodzaj zdarzenia,
- kontrolowane przejście,
- nazwisko użytkownika.

Proces generowania raportu sprowadza się do ustawienia poszczególnych filtrów. Następnie raport jest wyświetlany na ekranie i może zostać zapisany w wybranym formacie (xls, doc, pdf) na dysku lub wydrukowany na drukarce.

Oprócz raportu zdarzeń można wygenerować raporty:

- ostatniego użycia kart,
- bazy danych użytkowników,
- bazy danych urządzeń.

Oprócz ww. funkcji NAM zawiera również szereg innych opcji niezbędnych do prawidłowego skonfigurowania i serwisowania systemu, takich jak np. „Parametry globalne” czy „Kopia i odtwarzanie systemu”.

Podsumowanie

Aktualnie oferowana wersja programu NAM jest modyfikowana oraz rozszerzana o nowe funkcje. Najlepiej zapoznać się z programem NAM, zainstalowawszy go na komputerze i połączysz z przynajmniej jednym kontrolerem. Bezpłatna licencja na użytkowanie programu jest dostarczana wraz z kontrolerami NVAC-300CKF.

Niniejszy artykuł nie zawiera oczywiście wszystkich szczegółów funkcjonalnych programu. Zainteresowanych czytelników odsyłam jak zwykle do dokumentacji dostępnej na stronie www.aat.pl lub na CD w siedzibie firmy AAT Holding.

W jednym z kolejnych numerów *Zabezpieczeń* ukaże się artykuł opisujący możliwość wykorzystania kontrolera biometrycznego NVAC-C300CKF oraz programu nadzorczo-go NAM-RCP do rejestracji wejść/wyjść oraz generowania raportów o stanie obecności i rozliczania czasu pracy.

RYSZARD SOBIERSKI
AAT HOLDING

Systemy sygnalizacji włamania

Część 1 – konfiguracje central alarmowych

Systemy alarmowe sygnalizacji włamania zawierają najczęściej następujące części składowe: centralę alarmową, jedną lub więcej czujek, jeden lub więcej sygnalizatorów i (lub) systemów transmisji alarmu, jeden lub więcej zasilaczy. Połączenia pomiędzy elementami systemu powinny spełniać określone wymagania, a zarazem muszą także zawierać się w dopuszczalnych parametrach, określonych przez producenta. Ogólnie można je podzielić na połączenia przewodowe i bezprzewodowe

W cyklu artykułów dotyczących systemów sygnalizacji włamania autorzy przybliżą podstawową wiedzę z zakresu:

- konfiguracji central alarmowych,
- linii dozorowych,
- magistral transmisyjnych,
- linii wyjściowych.

Wiedza ta opiera się na wieloletnim doświadczeniu autorów, zdobytym podczas badań i pomiarów prowadzonych przez autorów w Politechnice Warszawskiej, Wojskowej Akademii Technicznej (tu – w zakresie eksploatacji systemów alarmowych) oraz na Wydziale Informatyki Stosowanej w Wyższej Szkole Menedżerskiej w Warszawie, gdzie powstała specjalność Bezpieczeństwo Obiektów i Informacji. Na łamach *Zabezpieczeń* autorzy publikowali już dane dotyczące konfiguracji i analizy systemów alarmowych w aspekcie wskaźników niezawodnościowo-eksploatacyjnych – tzw. wskaźników gotowości (*Zabezpieczenia* nr 1 (47)/2006, nr 4 (56)/2007).

W niniejszym artykule, stanowiącym pierwszą część cyklu, będą opisane zagadnienia związane z konfiguracjami central alarmowych stosowanych w systemach sygnalizacji włamania, a w następnych – dotyczące analizy linii dozorowych (ich typów i konfiguracji), magistral transmisyjnych z uwzględnieniem przekazu informacji z zastosowaniem formatów transmisji RS232 i RS485 oraz linii wyjściowych.

Nazewnictwo stosowane w normach polskich i europejskich

Norma europejska EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements”, która ma jednocześnie status Polskiej Normy PN-EN 50131-1:2007 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe”, zawiera wykaz definicji i skrótów, które następnie są stosowane w kolejnych rozdziałach tej normy. Wśród nich są m.in. następujące definicje:

- system alarmowy (ang. *alarm system*) – instalacja elektryczna, która odpowiada na ręczne lub automatyczne wykrycie obecności zagrożenia,
- urządzenie sterujące i obrazujące (ang. *control and indicating equipment*) – urządzenie do odbierania, przetwarzania, sterowania, obrazowania oraz transmitowania informacji.

W poprzednio obowiązującej normie europejskiej EN 50131-1:1997 „Alarm systems. Intrusion systems. General requirements”, która miała jednocześnie status Polskiej Normy PN-EN-50131-1 „Systemy alarmowe. Systemy

sygnalizacji włamania. Wymagania ogólne”, przyjęto, że dla określenia urządzenia sterującego i obrazującego będzie stosowany termin „centrala alarmowa”. Należy sądzić, iż większość projektantów, instalatorów i konserwatorów nadal stosuje ten termin (wynika to m.in. z natury ludzkiej – przyzwyczajenia). Dlatego też w niniejszym artykule autorzy będą stosowali termin „centrala alarmowa” z pełną świadomością, że nie jest to zgodne z obecnie obowiązującą normą (należy wyraźnie podkreślić, że projekty elektronicznych systemów bezpieczeństwa powinny być realizowane zgodnie z obowiązującymi normami).

Centrale alarmowe są wyspecjalizowanymi urządzeniami, których zadaniem jest:

- odbieranie sygnałów informacyjnych (analogowych i/lub cyfrowych) od poszczególnych urządzeń,
- przetwarzanie sygnałów informacyjnych zgodnie z wcześniej zaprogramowanymi ustawieniami (instalatora i/lub producenta),
- sterowanie poprzez podanie odpowiednich sygnałów wyjściowych,
- obrazowanie zaistniałych zdarzeń na odpowiednich urządzeniach wchodzących w skład systemu sygnalizacji włamania,
- transmisja informacji do innych systemów, np. alarmowego centrum odbiorczego (w skrócie ARC, ang. *alarm receiving centre*).

Z powyższego wynika, iż systemy sygnalizacji włamania wchodzi w skład systemu sygnalizacji zagrożeń, który można zdefiniować następująco:

System sygnalizacji zagrożeń to zespół środków technicznych i zasad taktycznych mających na celu zapewnienie bezpieczeństwa określonemu obiektowi lub zespołowi obiektów (człowiek i/lub mienie) w przestrzeni i zachowanie jego substancji.

Zadaniem systemu sygnalizacji zagrożeń jest wykrywanie i sygnalizowanie warunków wskazujących na istnienie niebezpieczeństwa. W stanie alarmowym, powstałym w wyniku wykrycia niebezpieczeństwa, system wytwarza sygnał alarmowy. Sygnał alarmu może wystąpić bezpośrednio w dozorowanym obiekcie (najczęściej jest to sygnał akustyczno-optyczny), ale może też być przesłany do alarmowego centrum odbiorczego (i jest to obecnie najczęstszy przypadek). Sygnał alarmu może być przesłany drogą radiową, telefoniczną albo obiema drogami jednocześnie.

Norma PN-EN 50131-1:2007 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe” określa stopnie ryzyka, którym odpowiadają klasy zabezpieczenia oferowane przez poszczególne systemy sygnalizacji włamania. Wyróżniono cztery stopnie:

- stopień 1: ryzyko niskie (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada ograniczoną liczbę łatwo dostępnych narzędzi),
- stopień 2: ryzyko niskie do średniego (zakłada się, że intruz ma minimalną wiedzę na temat systemu alarmowego i posiada ogólnodostępne narzędzia oraz przenośne urządzenia, np. multimetr),
- stopień 3: ryzyko średnie do wysokiego (zakłada się, że intruz zna biegle system alarmowy i posiada złożony zestaw zaawansowanych narzędzi i przenośnego sprzętu elektronicznego),
- stopień 4: ryzyko wysokie (ma zastosowanie, gdy bezpieczeństwo ma priorytet nad wszystkimi innymi czynnikami; zakłada się, że intruz posiada zdolności bądź środki, by szczegółowo zaplanować włamanie, a także posiada zestaw dowolnego sprzętu, łącznie ze środkami do zastąpienia kluczowych elementów elektronicznego systemu alarmowego).

Uwarunkowania projektowe

Określenie klasy zabezpieczenia, jaką system sygnalizacji włamania ma spełniać, jest jednym z pierwszych kroków podczas projektowania systemu sygnalizacji zagrożenia. Następnie dokonuje się wyboru urządzeń, które spełniają założone wymagania. Oczywiście norma nie podaje, jakie elementy muszą być zastosowane. Z tego też m.in. względu spotyka się różne rozwiązania konstrukcyjne central alarmowych. Mogą one spełniać wymagania określonej klasy zabezpieczenia, ale zarazem różnić się między sobą.

Centrala alarmowa stanowi „serce” systemu sygnalizacji włamania. Do niej przesyłane są informacje o stanie poszczególnych linii dozoru (a więc o stanie czujek) i linii wyjściowych (np. dotyczące obciążenia wyjść) oraz wprowadzane są dane (przez użytkownika lub konserwatora systemu, a wcześniej – podczas instalacji systemu – przez instalatora). W zależności od typu centrali alarmowej informacje mogą być przesyłane bezpośrednio do płyty głównej centrali alarmowej lub też do modułów realizujących określone funkcje (np. rozszerzeń wejść, rozszerzeń wyjść, interfejsów drukarek itd.). Obecnie przesyłanie informacji pomiędzy centralą alarmową a poszczególnymi modułami odbywa się najczęściej cyfrowo, z zastosowaniem formatu transmisji RS232, RS485 lub innego (bardzo często jest on opracowany przez producenta urządzeń). Istnieją też rozwiązania systemów sygnalizacji włamania, w których magistrale transmisyjne mogą łączyć:

- kilka central alarmowych ze sobą (pracują one wówczas w tzw. pierścieniu),
- elementy układu sterowania (np. klawiatury sterujące),
- centrale alarmowe z centrum nadzorowania, zarządzania i administrowania zintegrowanym systemem bezpieczeństwa.

Należy tutaj nadmienić, iż większość stosowanych jeszcze kilka lat temu rozwiązań wykorzystywała połączenia przewodowe. Obecnie bardzo wiele rozwiązań oferowanych na rynku umożliwia wykorzystanie transmisji bezprzewodowej, np. typu on-line. W praktyce spotykane są częściej systemy mieszane, a więc takie, w których transmisja sygnałów odbywa się zarówno drogą przewodową, jak i radiową.

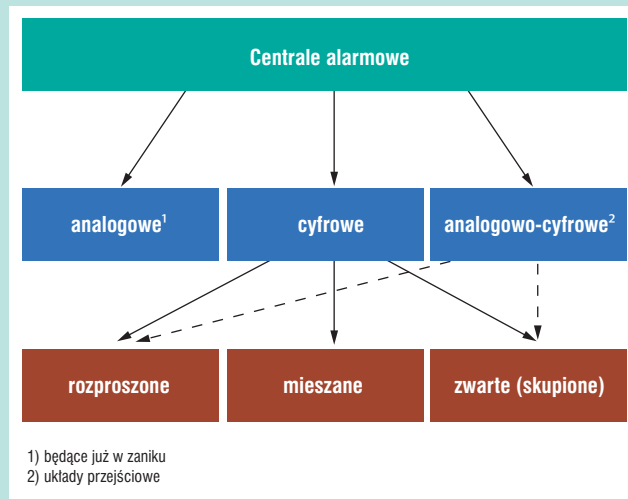
Różne konfiguracje systemów sygnalizacji włamania, które zostaną przedstawione w niniejszym artykule, będą omówione z uwzględnieniem komunikacji pomiędzy centralą alarmową a pozostałymi urządzeniami tworzącymi system, a więc pomiędzy:

- centralą alarmową a czujkami,
- centralą alarmową a urządzeniami wyjściowymi (np. sygnalizatorami),
- centralą alarmową a modułami,
- centralami alarmowymi.

Podział central alarmowych i ich konfiguracje

Centrale alarmowe systemów sygnalizacji włamania można ogólnie podzielić na:

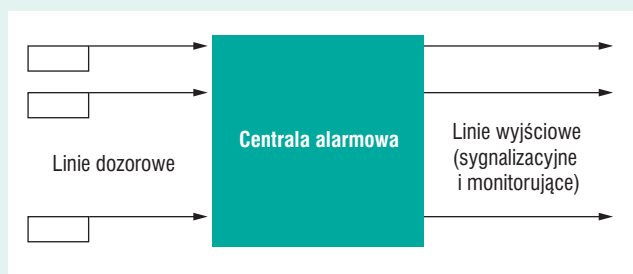
- centrale alarmowe analogowe,
- centrale alarmowe cyfrowe,
- centrale alarmowe analogowo-cyfrowe (podział przejściowy).



Rys. 1. Podział central alarmowych

Obecnie najczęściej spotykane centrale alarmowe to mikroprocesorowe centrale cyfrowe. System sygnalizacji włamania może mieć strukturę zwartą (skupioną), tzn. taką, w której należy doprowadzić wszystkie linie dozoru i linie wyjściowe (sygnalizacyjne oraz monitorujące) wprost do płyty głównej centrali alarmowej. Zostało to przedstawione na rys. 2. Centrale tego typu stosowane są w małych obiektach (np. mieszkaniach, małych biurach), które wymagają kilku-nastu linii dozoru (przeważnie nie więcej niż 16).

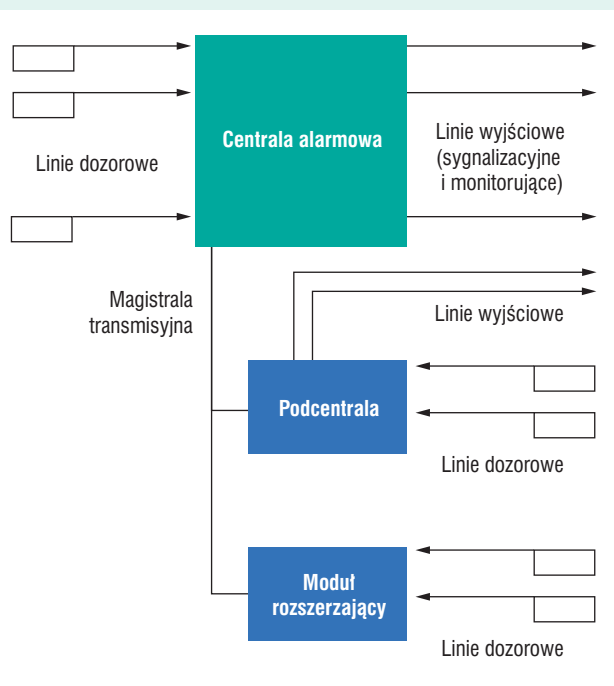
Systemy sygnalizacji włamania typu mieszane posiadają określoną liczbę linii dozoru wprowadzanych do centrali. Mają także możliwość współpracy z innymi centralami poprzez łącza RS232 lub RS485, a także z podcentralami lub modułami za pośrednictwem magistrali transmisyjnej. Na rys. 3 przedstawiono system sygnalizacji włamania w wersji mieszanej. Stosuje się go w obiektach, które wymagają dużej liczby linii dozoru (przeważnie powyżej 16).



Rys. 2. System sygnalizacji włamania o strukturze zwartej (skupionej)

Na rys. 4 przedstawiono system sygnalizacji włamania o strukturze rozproszonej. Centrala jest połączona z modułami za pośrednictwem magistrali transmisyjnej. Do modułów doprowadzone są linie dozоровe i linie wyjściowe. Tęgo typu systemy są rzadko spotykane, ponieważ większość oferowanych na rynku central alarmowych ma na płycie głównej możliwość dołączenia linii dozоровych i są one z reguły wykorzystywane.

Analizując poszczególne typy systemów sygnalizacji włamania, można zauważyć zasadnicze różnice w ich konfiguracji. Na rys. 2 przedstawiono proste rozwiązanie, w którym linie dozоровe są doprowadzane wprost na listwę łączeniową płyty głównej. Zwykle liczba linii dozоровych wynosi od czterech do maks. 64. Linie dozоровe mogą być dwuprzewodowe, np. w przypadku czujek kontaktronowych (magnetycznych) lub przycisków napadowych biernych (bez zasilania), czteroprzewodowe lub sześcioprzewodowe. Szczegóły dotyczące linii dozоровych różnych typów zostaną omówione w kolejnym artykule niniejszego cyklu. Maksymalne odległości pomiędzy czujkami a płytą główną centrali alarmo-



Rys. 3. System sygnalizacji włamania o strukturze mieszanej

wej podaje zwykle producent centrali, ale nie powinny one być większe niż 100 m. Oczywiście dopuszczalne długości linii dozоровych można obliczyć, stosując podstawowe prawa elektrotechniki dla prądu stałego. Nieco inaczej wygląda problem w przypadku adresowalnych linii dozоровych. Przebiegi prostokątne, reprezentujące informacje przesyłane pomiędzy czujką a wejściem do modułu lub centrali,

Wyższa Szkoła Menedżerska w Warszawie

ul. Kawęczyńska 36

Wydział Informatyki Stosowanej

Specjalności na studiach inżynierskich:

- » **Bezpieczeństwo obiektów i informacji**
(zajęcia m.in. w nowo otwartym Laboratorium Systemów Bezpieczeństwa)
- » Zarządzanie systemami i sieciami komputerowymi
- » Grafika komputerowa
- » Technologie internetowe

www.wsm.warszawa.pl

Studia prowadzone są w trybie stacjonarnym i niestacjonarnym

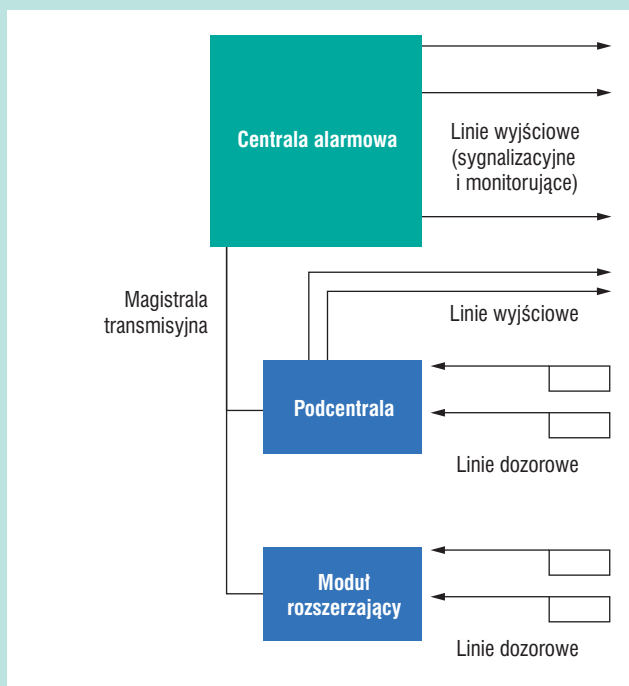
Rekrutacja: tel. (22) 59 00 730, e-mail: rekrutacja@wsm.warszawa.pl

podlegają pewnym zniekształceniom (m.in. ze względu na parametry falowe linii dozоровей, w tym przypadku transmisyjnej), a obliczenia nie są proste.

Na rys. 3 przedstawiono rozwiązanie systemu sygnalizacji włamania w konfiguracji mieszanej. Zwykle kilka linii dozоровей (od czterech do 16) jest doprowadzanych wprost do listwy łączeniowej płyty głównej centrali alarmowej. Zazwyczaj linie te nie są zbyt długie (od kilku do kilkudziesięciu metrów) i łączą czujki usytuowane blisko centrali alarmowej. Pozostałe czujki dołączone są do modułów rozszerzeń wejść, przeważnie o ośmiu wejściach. Linie wyjściowe w tym systemie mogą być dołączone do wyjść płyty głównej lub do modułu rozszerzeń wyjść (najczęściej czterowyjściowego). Jeśli jest to moduł podcentrali, to ma on zwykle do ośmiu wejść linii dozоровей i osiem wyjść.

Na rys. 4 przedstawiono rozwiązanie systemu sygnalizacji włamania w konfiguracji rozproszonej. Linie dozоровей i linie wyjściowe dołączone są do modułów rozszerzających wejścia i wyjścia lub podcentral. Analizując rys. 4, można stwierdzić, że moduły są dołączone do płyty głównej za pośrednictwem magistrali transmisyjnej (zwykle czteroprzewodowej) o długości od kilkunastu metrów do 1300 m. Znane są przypadki długości magistral transmisyjnych sięgających nawet 2500 m przy formacie transmisji RS485 (dla znacznie spowolnionej prędkości transmisji dwukierunkowej). Systemy transmisji szeregowej RS232C, RS232D, RS232A, RS422A i RS485 zostaną szczegółowo opisane w jednym z kolejnych artykułów niniejszego cyklu.

Do bardzo interesujących rozwiązań konfiguracji systemów sygnalizacji włamania należała grupa central, które mogły pracować jako systemy skupione z własną klawiaturą matrycową. Można powiedzieć, że były to pojedyncze systemy, niezależne i autonomiczne. Centrale te dało się w prosty sposób łączyć w duże systemy (nawet do 4096 linii dozоровей). Każdą z tych central należało wyposażyć w moduł RS232. Cały system mógł pracować w tzw. pętli zamkniętej. Wszystkie centrale były kontrolowane systemowo, a ich stan był przedstawiany na ekranie komputera. Warto o tym wspomnieć, ponieważ był to system polski (obecnie już nieprodukowany) – RANKOR. Na rys. 5 przedstawiono zespół różnych central w wersji skupionej, które w wyniku integracji utworzyły system sygnalizacji włamania o strukturze rozproszonej. Każda z central ma niezależną klawiaturę (nie są one przedstawione na rysunku) i została wyposażona w kartę RS232, która umożliwiła połączenie central w duży system alarmowy (na rys. 5 jest to połączenie oznaczone jako „RS232/2”). Poprzez magistralę transmisyjną RS232/1 centrala nr 4 łączy się ze sterownikiem tablicy synoptycznej. Wszystkie bloki systemu alarmowego, a więc centrale o numerach od 1 do 4 oraz sterownik tablicy synoptycznej, są połączone magistralami transmisyjnymi RS232 z przyłącznicą RS232/2, a ta z komputerem nadzorującym pracę całego systemu sygnalizacji włamania. Warto nadmienić, że w skład tego zintegrowanego systemu wchodzi jednostki o różnych wielkościach, a więc o różnej liczbie linii dozоровей (od 18, poprzez 40, do 64 linii dozоровей) oraz o 40 strefach, jakimi dysponuje każda z central. Centrale RANKOR to jedne z nielicznych central, które można



Rys. 4. System sygnalizacji włamania o strukturze rozproszonej

łączyć w duże systemy sygnalizacji włamania. Ważną cechą takich systemów jest możliwość decentralizacji wszystkich central wchodzących w ich skład.

Istotnym problemem, związanym z systemem przedstawionym na rys. 5, była konieczność zachowania wyjątkowej staranności podczas instalacji – zarówno linii dozоровей, jak i magistral transmisyjnych (te ostatnie były

centrumkart.com.pl

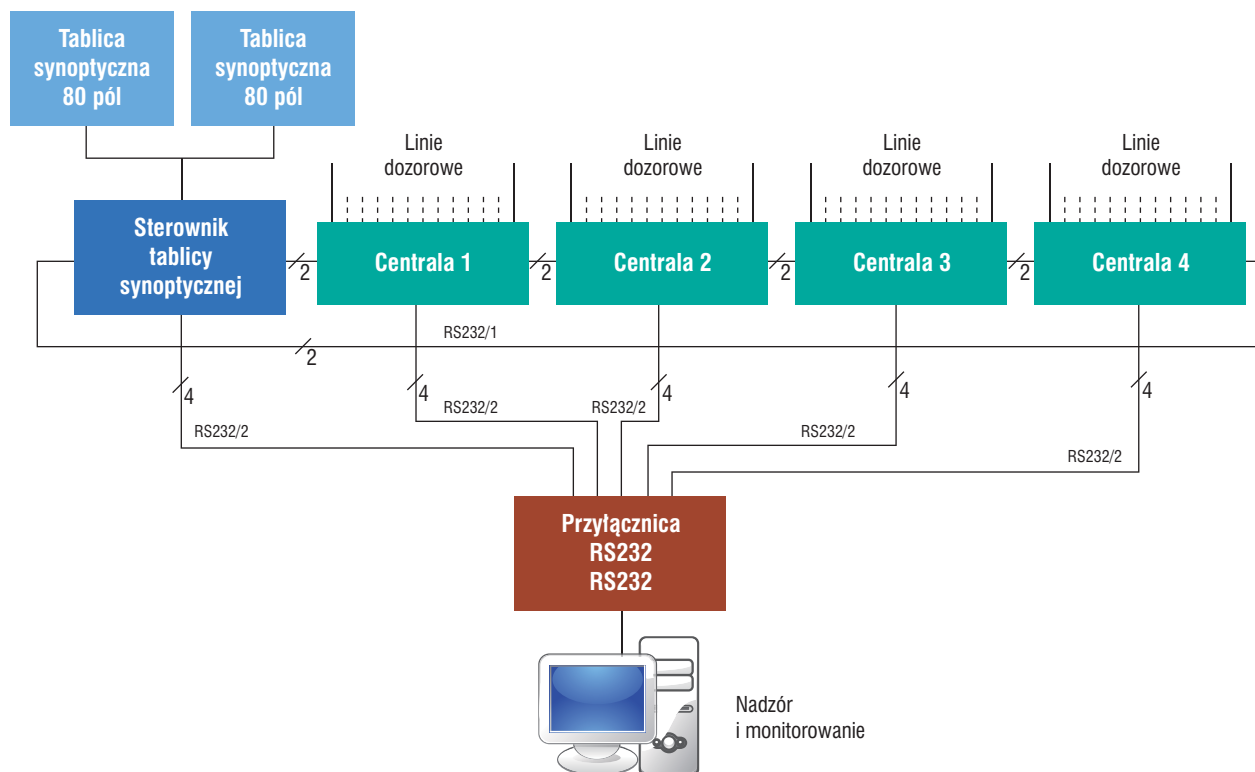
Najlepsze ceny kart i breloków kompatybilnych z systemami:

HID MIFARE ROGER GALAXY SATEL UNIQUE

W ofercie również:

- naklejki na karty zbliżeniowe,
- karty magnetyczne,
- czyste karty PVC w kolorach PANTONE.

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20 C
01-496 Warszawa
tel: +48 22 8324744
biuro@acss.com.pl
www.acss.com.pl



Rys. 5. System sygnalizacji włamania o strukturze rozproszonej, powstały w wyniku integracji czterech central skupionych o różnych wielkościach (od 18 do 64 wejść)

optoelektronicznie izolowane od pozostałej części układu) – gdyż system ten był szczególnie wrażliwy na nieprzestrzeganie zasad związanych z kompatybilnością elektromagnetyczną. Rozwiązanie zaprezentowane na rys. 5 autorzy świadomie przedstawili jako niezmiernie ciekawe. Pozwalało ono na konfigurację systemu sygnalizacji włamania w wersji zdecentralizowanej w praktycznie dowolny sposób.

Na rys. 6 przedstawiono konfigurację systemu sygnalizacji włamania o strukturze mieszanej, w którym zastosowano bezprzewodowe linie dozorowe. Systemy bezprzewodowe stają się ostatnio coraz bardziej popularne ze względu na stosunkowo łatwy montaż. Mogą one pracować m.in. na częstotliwości 433,92 MHz ze specjalnym systemem cyfrowej modulacji. Są to systemy, których linie dozorowe są łączami radiowymi typu on-line o zasięgach ok. 100 m w otwartej przestrzeni. Jeśli jednak ściany obiektu zawierają pręty zbrojeniowe lub metalowe siatki ochronne, pojawiają się kłopoty. Należy bezwzględnie przestrzegać odległości pomiędzy czujkami (beziprzewodowymi) a modułami radiowymi z uwzględnieniem poziomu sygnału radiowego pomiędzy modułem a czujką. Systemy bezprzewodowe nie zawsze mogą więc być stosowane w obiektach specjalnego znaczenia (choćby z powyższych względów).

Przedstawiony na rys. 6 system sygnalizacji włamania stanowi układ mieszany. Część elementów podłączonych do linii dozorowych (np. czujka PIR, czujka magnetyczna, sygnalizator zewnętrzny, sterownik bezprzewodowy) jest połączona drogą radiową ze specjalnym modułem urządzeń bezprzewodowych. Moduł ten jest połączony z płytą główną centrali alarmowej za pośrednictwem przewodowej magistrali transmisyjnej. Pozostała część czujek jest dołączona do płyty głównej za pośrednictwem klasycznych przewodowych

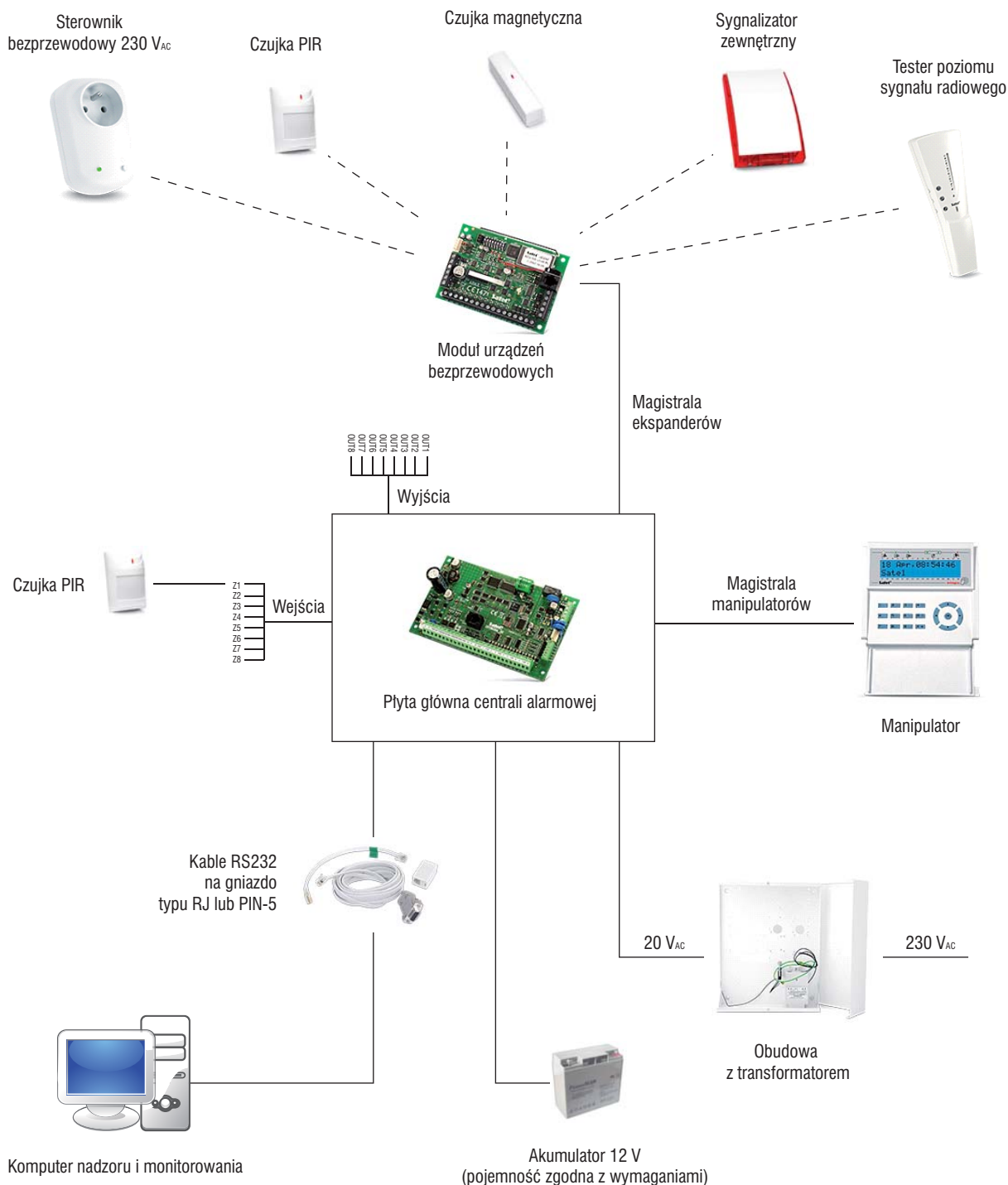
linii dozorowych. Całość systemu sygnalizacji włamania jest programowana i nadzorowana przez komputer za pośrednictwem magistrali z zastosowaniem RS232. Warto nadmienić, że ze względu na warunki propagacyjne radiowych linii dozorowych koniecznością staje się przeprowadzanie pomiaru poziomu sygnału radiowego za pomocą specjalnego testera (pokazanego na rysunku).

Podsumowanie

Niniejszy artykuł dotyczy głównie różnych konfiguracji central alarmowych systemów sygnalizacji włamania. Autorzy zdają sobie sprawę, że przedstawiony materiał obejmuje jedynie niewielki fragment wiedzy na temat projektowania i instalacji tych systemów. Złożoność konfiguracyjna różnych typów central alarmowych, występowanie szkodliwych zakłóceń radioelektrycznych, a więc brak kompatybilności elektromagnetycznej, wadliwość instalacyjna systemów alarmowych oraz nieprzestrzeganie elementarnych przepisów projektowania i montażu pociągają za sobą różne, często kłopotliwe podczas eksploatacji skutki.

DOC. DR INŻ. WALDEMAR SZULC
WYŻSZA SZKOŁA MENEDŻERSKA W WARSZAWIE
(WYDZIAŁ INFORMATYKI STOSOWANEJ,
ZAKŁAD BEZPIECZEŃSTWA OBIEKTÓW I INFORMACJI)
WOJSKOWA AKADEMIA TECHNICZNA
(WYDZIAŁ ELEKTRONIKI)

DR INŻ. ADAM ROSIŃSKI
WYŻSZA SZKOŁA MENEDŻERSKA W WARSZAWIE
(WYDZIAŁ INFORMATYKI STOSOWANEJ,
ZAKŁAD BEZPIECZEŃSTWA OBIEKTÓW I INFORMACJI)



Rys. 6. System sygnalizacji włamania o strukturze mieszanej z zastosowaniem urządzeń bezprzewodowych

Bibliografia:

1. Haykin S., *Systemy telekomunikacyjne*, tom I i II, WKiŁ, Warszawa 2004.
2. Instrukcje serwisowe firm AAT i SATEL oraz dotyczące central GALAXY i RANKOR.
3. Kula S., *Systemy teletransmisyjne*, WKiŁ, Warszawa 2004.
4. Nawrocki W., *Komputerowe systemy pomiarowe*, WKiŁ, Warszawa 2006.
5. Norma: PN-EN 50131-1.
6. Szulc W., Rosiński A., *Analiza niezawodnościowa złożonego systemu bezpieczeństwa dla obiektu o spe-*

cialnym przeznaczeniu, Zabezpieczenia nr 4 (56)/2007, wyd. AAT, Warszawa 2007.

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 2006–2008.
9. Szulc W., Rosiński A., *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków (część I – analogowa)*, Oficyna Wydawnicza WSM, Warszawa 2008.

NOWOŚĆ!



HX-40 HX-40AM

Zewnętrzne czujki firmy

z unikalnym czujnikiem piroelektrycznym



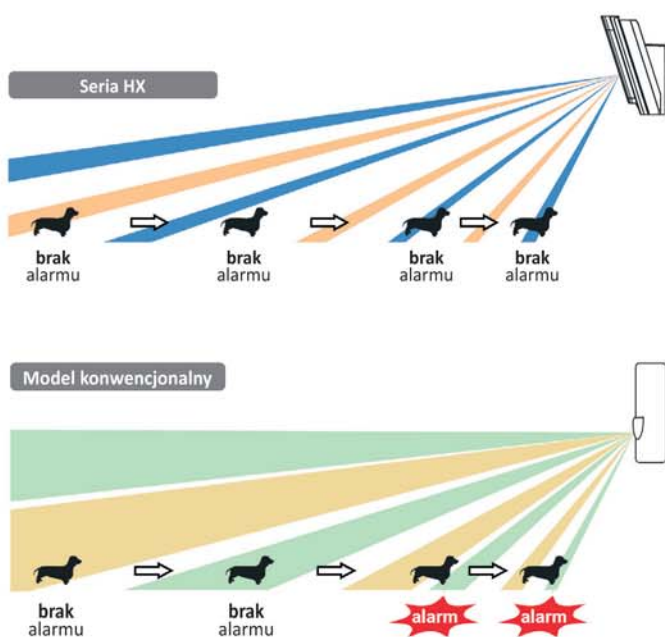
Przeznaczona do wysokiego montażu

Seria HX

W celu uzyskania niezawodności detekcji, firma Optex zaprojektowała niezwykle precyzyjny układ optyczny oraz całkiem nowy piroelement, które razem tworzą strukturę 94 pól detekcji o jednakowej gęstości, zarówno w pobliżu detektora, jak i na krańcach jego nominalnego zasięgu.

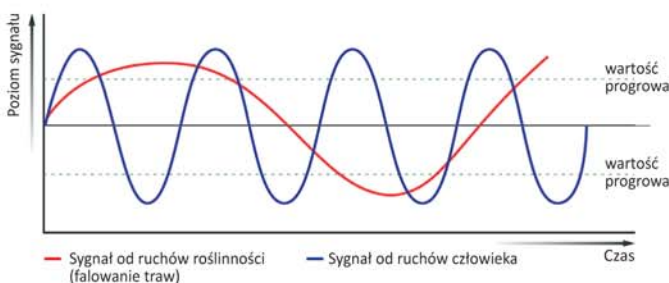
Inteligentna logika AND

Czujki serii HX-40 wykorzystują technologię detekcji AND generując alarm jako efekt sekwencji naruszenia po sobie wyższych i niższych stref detekcji czujki. Pierwotna strefa detekcji czujki została skonfigurowana tak, aby nie wywoływać fałszywych alarmów powodowanych przez niewielkie zwierzęta domowe lub inne małe zwierzęta.



Dyskryminacja sygnałów generowanych przez poruszającą się roślinność

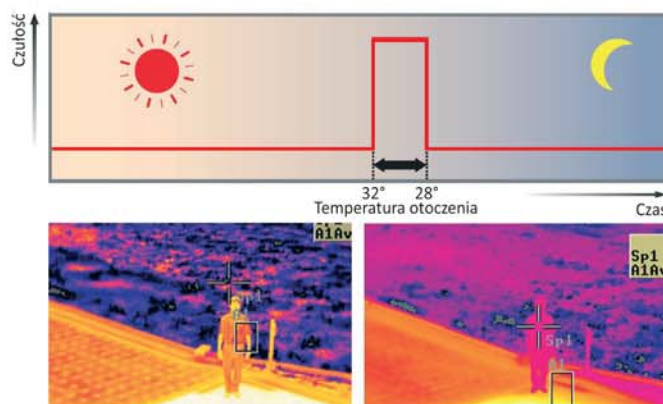
Czujki serii HX-40 przez cały czas swojej pracy monitorują zmiany sygnałów pochodzących z tła. Dzięki zaawansowanym technikom obróbki sygnałów automatycznie ignorują zakłócenia spowodowane kołyszącą się na wietrze roślinnością.



Inteligentna kompensacja temperatury

W trakcie lata, zwłaszcza w porach popołudniowych i wieczornych, w niektórych miejscach obiektów chronionych powstają miejsca, gdzie temperatura ciała człowieka jest praktycznie taka sama jak temperatura otoczenia. W warunkach takich, przy zastosowaniu większości czujek, prawdopodobieństwo braku wykrycia alarmu znacznie wzrasta. Seria czujek HX, dzięki funkcji dodatkowych pomiarów poziomu luminancji podczas zmiany warunków środowiskowych, doskonale eliminuje problem braku wykrycia intruza.

Jednoczesna analiza temperatury oraz stopnia jasności otoczenia wpływa na precyzyjne oszacowanie rzeczywistych warunków środowiskowych i pozwala, by czułość czujki automatycznie zaostbrazała się w przypadku wystąpienia niekorzystnych zmian środowiskowych. Funkcja ta znacznie redukuje potencjalne ryzyko nie wykrycia ruchu w obszarze chronionym przez czujnik.



Cyfrowy antymasking (tylko model AM)

Dzięki zastosowaniu najnowszych osiągnięć w dziedzinie algorytmów samonastrajalnych, funkcja „Antymaskingu” zastosowana w czujkach HX-40AM, adaptuje się do zmiennych warunków otoczenia (poziom promieniowania tła, zakresu temperatur pomieszczenia itp.) zapewniając tym samym niezawodność funkcjonowania.



Wyłączny dystrybutor produktów OPTEX 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

Zagrożenia bezpieczeństwa informacji w przedsiębiorstwie

część 2 – Kształtowanie zachowań zabezpieczających informacje w małej firmie



W pierwszej części artykułu poruszono zagadnienia związane z istotą bezpieczeństwa informacji i klasyfikacją związanych z tym bezpieczeństwem zagrożeń. Część druga jest poświęcona kształtowaniu zachowań zabezpieczających informacje

Zaprezentowane zagadnienia dotyczące bezpieczeństwa informacji organizacji związane są przede wszystkim z jej otoczeniem, które postrzegane jest jako wrogo nastawione do organizacji i realizowanych procesów organizacyjnych. Takie podejście umożliwia projektowanie zestawu instrumentów gwarantujących tworzenie zapór informacyjnych, tak aby istotne z perspektywy zamierzeń strategicznych zasoby in-

formacji znajdowały się poza bezpośrednim i pośrednim wpływem zewnętrznych uczestników gry rynkowej. Instrumenty i różnego rodzaju zabiegi przeciwdziałające wyciekom informacji na zewnątrz organizacji już na etapie ich projektowania spełniają istotną funkcję zapobiegawczą, bowiem kierunkują członków organizacji na przejawianie zachowań utrudniających pozyskiwanie przez otoczenie informacji organizacji. Z kolei ich internalizacja, będąca pochodną uczenia się, może gwarantować, iż podsystem społeczny przedsiębiorstwa będzie reprezentować strategię czuwania, a przez to stanowić najszczelniejszą barierę przeciwdziałającą utraceniu istotnych informacji przedsiębiorstwa. Ważne jest, aby niniejsze podejście nie stało się przyczyną odizolowania podmiotu gospodarczego od otoczenia.

Taka perspektywa wydaje się szczególnie istotna w odniesieniu do małych organizacji, które nie potrzebują skomplikowanych i kapitałochłonnych rozwiązań techniczno-organizacyjnych, a bardziej zainteresowane są prostymi metodami i technikami, które spełnią oczekiwania decydentów. Prostota ta związana jest może nie tyle ze strukturą i zakresem pewnych rozwiązań, ale z tym, iż zarządzanie małymi podmiotami rynkowymi jest przede wszystkim intuicyjne. Dokonuje się w głowie właściciela-menedżera. W rezultacie menedżer organizacji może oddziaływać na ochronę cennych informacji poprzez dawanie innym przykładu swoją osobą, wskazywanie, jakimi informacjami członkowie organizacji mogą i powinni dzielić się z otoczeniem, które ze zbiorów informacji powinni zabezpieczać przed wydostaniem się na zewnątrz organizacji. W takim znaczeniu kluczową sprawą jest wykształcenie w organizacji właściwych zachowań organizacyjnych, które w przypadku małych podmiotów gospodarczych odgrywają istotniejszą rolę w bezpieczeństwie informacji aniżeli środki organizacyjno-techniczne, którymi w większości przypadków organizacje nie dysponują. Właściwe zachowania organizacyjne:

- wzmacniają postawy pracownicze gwarantujące ochronę cennych informacji i udostępnianie odpowiednich treści otoczeniu,
- wzmacniają samokontrolę członków organizacji w sterowaniu przepływami informacji między organizacją a otoczeniem,
- identyfikują działania pracownicze ukierunkowane na poszukiwanie cennych informacji w otoczeniu nie tylko w ramach pełnionych obowiązków, ale także w czasie poza pracą,
- umożliwiają dyfuzję najlepszych praktyk między pracownikami celem dostosowania ich aktualnych potrzeb związanych z ochroną informacji,
- dostosowują działania i praktyki członków organizacji do zmian w otoczeniu, tj. do realizowanych zleceń, zawieranych transakcji, kontrahentów.

Oprócz wymienionych funkcji w obszarze zabezpieczania informacji zachowania pracownicze mają za zadanie promowanie w organizacji i jej otoczeniu praktyk będących pochodną procesów uczenia się na poziomie indywidualnym, grupowym, organizacyjnym i międzyorganizacyjnym (zob. tab. 1). W projektowaniu i upowszechnianiu właściwych zachowań zasadniczą rolę odgrywa właściciel-menedżer organizacji. Jego postawa oddziałuje na podległych pracowników, od niego także rozpoczyna się proces organizacyjnego uczenia się na wszystkich poziomach. Jego postawa warunkuje przebieg procesu uczenia się, może także zahamować ten proces. Nie zostaną poruszone w tym miejscu zagadnienia związane z rolą menedżera w procesie organizacyjnego uczenia się, która służy zabezpieczeniu informacji organizacji, bowiem wymagałoby to uwzględnienia obszarów problemowych znacznie wykraczających poza tematykę niniejszego opracowania, w szczególności dotyczących: przywództwa, zaufania, lojalności, kultury organizacyjnej, stylów kierowania.

Odniesieniem uczenia się pracowników jest bezpieczeństwo informacji. Uczenie się może przebiegać w różnej konfiguracji, w znaczeniu poziomu organizacyjnego uczenia się inicjującego działania i praktyki umożliwiające zabezpieczanie informacji na pozostałych poziomach organizacyjnego uczenia się. Przyjmując jednak, iż zagadnienie ochrony in-

formacji odnosi się do małej organizacji, w której decyzje i działania pracowników nie były bezpośrednio związane z ochroną informacji, można przyjąć, iż proces ten inicjowany jest przez właściciela-menedżera. W pierwszej kolejności zachodzi on na poziomie indywidualnym. Sprowadza się więc do tworzenia, upowszechniania i rozwijania doświadczeń i wyobrażeń członków organizacji, których rezultatem będą metafory identyfikowane przez poszczególnych członków organizacji. Ze zbioru czynników kształtowania zachowań najważniejsze jest promowanie zaangażowania, perspektywiczności myślenia oraz zarządzanie „od dołu”. W stosowaniu tych stymulatorów zasadniczą rolę odgrywa właściciel-menedżer. Bez jego udziału i bezpośredniego zaangażowania szanse na zainicjowanie i skuteczność procesu organizacyjnego uczenia się ukierunkowanego na ochronę informacji są nikłe.

Zdefiniowanie metafor na poziomie indywidualnym umożliwia zachodzenie procesu interpretacji, w którym wzajemne zrozumienie kwestii dotyczących bezpieczeństwa cennych dla organizacji informacji i podejmowanych praktyk w tym zakresie warunkuje nawiązywanie dialogu i konwersacji. Inicjowana w ten sposób komunikacja członków organizacji może zapewnić dyfuzję najlepszych praktyk, uczenie się członków organizacji oraz pobudzanie ich do wzajemnej interakcji celem promowania zrozumienia (*sensemaking*). Na tym poziomie zasadnicze są jednak perswazja i jednolite nacełowanie, przy czym celem procesu interpretacji jest internalizacja istotności kwestii związanych z bezpieczeństwem informacji wśród członków organizacji.

Nawiązywany dialog i konwersacje pomiędzy członkami organizacji stanowią gwarancję kształtowania zachowań pracowników na poziomie grupowym, rozpoczynając proces integracji członków organizacji wokół zagadnień związanych z bezpieczeństwem informacji. Rezultatem tego jest wypracowanie systemu interaktywnego, który stanowi regulator zachowań organizacyjnych. W przebiegu uczenia się zachowań na poziomie grupowym kluczową rolę w odniesieniu do małych firm odgrywa promowanie poczucia zaufania i przynależności grupowej oraz eliminowanie atmosfery współzawodnictwa.

Wskazane powyżej poziomy proces organizacyjnego uczenia się są istotniejsze aniżeli uczenie się na poziomie organizacyjnym i międzyorganizacyjnym, zwłaszcza na etapie początkowym, którego zasadniczym celem jest zwrócenie uwagi członków organizacji na kwestie bezpieczeństwa. Należy także nadmienić, iż realizacja działań zmierzających do kształtowania wspólnego zrozumienia kwestii dotyczących bezpieczeństwa informacji oraz przejawiania właściwych zachowań w przypadku małych firm odbywać się powinna w ramach grup nieformalnych. Związane jest to przede wszystkim z tym, iż małe podmioty gospodarcze nie dysponują wystarczającymi zasobami finansowymi, które pozwoliłyby realizować te działania na specjalnie wyznaczonych w tym celu spotkaniach. Z jednej strony presja czasu i bieżące prowadzenie działalności uniemożliwia prowadzenie tego rodzaju aktywności, z drugiej zaś przekazanie informacji przez właściciela-menedżera, względnie któregoś z pracowników, innemu członkowi organizacji może się odbywać przy okazji przerw w pracy, w trakcie wspólnego dyskusowania zagadnień związanych z realizacją zadań w organizacji.

Poziom organizacyjnego uczenia się	Proces	Nakład	Stymulatory procesu uczenia się i czynniki kształtowania zachowań	Efekt
indywidualny	intuicyjny	doświadczenia, wyobrażenia	rozwijanie ciekawości intelektualnej, opowiadanie (<i>storytelling</i>), traktowanie problemów jak wyzwań, perspektywiczność myślenia, zaangażowanie, zarządzanie „od dołu”	metafory
	interpretacyjny	wzajemne zrozumienie	kult wartości, zachęcanie do podejmowania ryzyka i nauki, dostarczanie jednolitego nazewnictwa, perswazja	konwersacja, dialog
grupowy	integracyjny	wzajemne zrozumienie i dostosowania	eliminowanie barier funkcjonalnych, eliminowanie atmosfery współzawodnictwa, promowanie poczucia zaufania i przynależności grupowej, przyznawanie nagród pracownikom, którzy najsprawniej dzielą się wiedzą, egalitaryzm	systemy interaktywne
organizacyjny	instytucjonalizowania	standardy, systemy diagnostyczne, skodyfikowane doznania i doświadczenia	swoboda organizacyjna, samoorganizacja, fluktuacja kadry między różnymi projektami, bazy danych najlepszych pomysłów, wirtualne grupy zadaniowe	zasady i procedury
międzyorganizacyjny				

Tab. 1. Proces organizacyjnego uczenia się wraz z przykładowymi czynnikami kształtującymi pożądane zachowania pracownicze
Źródło: Opracowanie własne

Osobną kwestią związaną z bezpieczeństwem informacji, odnoszącą się szczególnie do małych podmiotów rynkowych, jest rozstrzygnięcie, w jakim stopniu posiadane informacje narażone są na utracenie, a także, co ważniejsze, wykorzystanie przez potencjalnych konkurentów. W szczególności chodzi o to, jaki rodzaj informacji należy chronić w takich podmiotach. Kwestia ta wydaje się tym istotniejsza, że funkcjonowanie małych podmiotów w przestrzeni społeczno-gospodarczej jest uzależnione od wymiany informacji pomiędzy podobnymi podmiotami gospodarczymi. Biorąc pod uwagę małe zakłady wytwórcze czy usługowe, dostarczające finalnemu konsumentowi produkt czy usługę, można przyjąć, iż dyfuzja informacji sprzyja ich konkurencyjności. Umożliwia ona wymianę praktyk, sposobów nawiązywania relacji z innymi uczestnikami rynkowymi. W wielu przypadkach wzajemna wymiana informacji jest dla takich przedsiębiorstw kluczowym sposobem uczenia się. Z kolei przyjęcie wzorca ochrony informacji powoduje, że organizacje zamykają się na rozwój, ich odizolowanie może znacznie utrudnić ich funkcjonowanie. W takim znaczeniu, o ile kształtowanie zachowań na poziomie indywidualnym i grupowym ma za zadanie wskazywać pracownikom rangę zabezpieczenia informacji przez wydostaniem się jej na zewnątrz przedsiębiorstwa, zarówno na poziomie organizacyjnym, jak i międzyorganizacyjnym proces organizacyjnego uczenia się powinien być ukierunkowany inaczej. Ma za zadanie kształtować postawy i zachowania pracowników zmierzające do dyfuzji informacji w otoczeniu. Tym samym należy promować wśród członków organizacji odmienną postawę wobec otoczenia, nie wroga, lecz przyjazną. Oczywiście nie chodzi tutaj o sprzeczne formułowanie przekazów, ale o to, aby działania podejmowane w organizacji sprzyjały nawiązywaniu relacji z otoczeniem.

Uzasadnieniem takiego podejścia jest przypuszczenie, iż wykształcenie na poziomie indywidualnym i grupowym świadomości pracowników spowoduje, że będą oni przekazywać jedynie te informacje, które nie zagrażają pozycji przedsiębiorstwa na rynku. Zasadniczo chodzi tu o symetrię przepływu informacji między otoczeniem a organizacją. Relacje z otoczeniem w znaczeniu transakcji polegają na wzajemnej wymianie – z jednej strony na przepływie strumieni materialnych, z drugiej zaś niematerialnych. Trudno oczekiwać od partnerów postaw i zachowań altruistycznych (nawet tylko na poziomie deklaracji). Aby uzyskać informacje od innych uczestników gry rynkowej, należy przekazać coś w zamian, z reguły także informacje. Trudno w tym miejscu rozstrzygnąć, które z informacji nadają się do wymiany i udostępniania, brakuje bowiem badań naukowych, które identyfikowałyby zbiory informacji szczególnie ważnych dla małej firmy, których udostępnienie innym podmiotom rynkowym mogłoby zagrozić pozycji rynkowej takiej firmy. Tym samym wnioskiem o charakterze normatywnym, kierowanym do właścicieli-menedżerów małych podmiotów, jest potrzeba zidentyfikowania elementu wyróżniającego firmę w otoczeniu, przy czym bardziej chodzi tu o element behawioralny, związany z miękkimi obszarami zarządzania, tj. łatwość nawiązywania kontaktów, lojalność pracowników, doświadczenia w branży i wprawę w działaniu. Szczególnie w przypadku małych podmiotów rynkowych mniej istotne jest wyposażenie techniczne, maszyny i aparatura, bowiem dostęp do nich jest podobny dla wszystkich. Barierą w ich pozyskaniu jest stopa zwrotu inwestycji i ryzyko z tym związane. Przegląd małych przedsiębiorstw funkcjonujących w poszczególnych sektorach wskazuje, iż dysponują one podobnym wyposażeniem, a konkurują przede wszystkim w oparciu o miękkie

obszary zarządzania. Osobną kwestią jest to, czy element wyróżniający małą organizację w otoczeniu, mieszczący się w sferze niematerialnej, możliwy jest do skopiowania przez innych uczestników rynkowych. Kwestia ta znajduje się jednak poza bezpośrednim zasięgiem tematu niniejszego opracowania.

Kształtowanie zachowań zabezpieczających informacje odbywa się zgodnie z polityką bezpieczeństwa, która jest zbiorem reguł dotyczących wszystkich aspektów bezpieczeństwa¹. Polityka bezpieczeństwa informacyjnego składa się z następujących elementów:

- planowanie zapotrzebowania na bezpieczeństwo,
- analiza metod ochrony,
- analiza ekonomiczna,
- opracowanie zasad postępowania na wypadek katastrofy lub awarii,
- opracowanie dokumentu „polityka bezpieczeństwa”,
- wprowadzenie w życie polityki bezpieczeństwa,
- analiza skuteczności i kontrola systemu,
- korekta polityki bezpieczeństwa².

Podsumowanie

Istnieje wiele podejść i rozwiązań zmierzających do zapewnienia bezpieczeństwa informacji organizacji gospodarczej. Niniejszy artykuł prezentuje podstawy teoretyczne wraz z rozważaniami na temat kształtowania zachowań pracowników małej firmy, które mają wpływ na bezpieczeństwo informacji. Znaczenie bezpieczeństwa, w tym bezpieczeństwa informacji, jest sukcesywnie wzmacniane, szczególnie w obszarze praktyki. Praktyczne znaczenie bezpieczeństwa informacji pozwala uwydatniać i zaktualizować problemy związane z omawianą wartością.

DR MAREK JABŁOŃSKI

UNIwersytet Ekonomiczny w Krakowie

MGR MAGDALENA MIELUS

KRAKOWSKA SZKOŁA WYŻSZA

IM. A. FRYCZA MODRZEWSKIEGO

1) Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000, s. 130.

2) Tamże, s. 131–147.

Literatura:

1. Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.
2. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.
3. Konieczny J. (red.), *Bezpieczeństwo. Teoria i praktyka. Moralne problemy bezpieczeństwa*, czasopismo Krakowskiej Szkoły Wyższej im. A. Frycza Modrzewskiego, numer specjalny, Kraków 2008.
4. Borowiecki R., Kwieciński M., *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze 2003.
5. Ciborowski L., *Walka informacyjna*, Wydawnictwo Marszałek, Toruń 1999.
6. Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kantor Wydawniczy Zakamycze, Zakamycze 2000.
7. Herman M., *Potęga wywiadu*, Wydawnictwo Bellona, Warszawa 2002.
8. Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006.
9. Śmid W., *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.
10. Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Oficyna Współczesna, Poznań 2004.
11. Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000.

Źródła internetowe:

<http://sjp.pwn.pl>

<http://www.cert.pl>





Zarządzanie ryzykiem

w działalności gospodarczej (część 4)

Kontynuując nasz cykl artykułów na temat zarządzania ryzykiem, chcielibyśmy w ostatniej części cyklu przybliżyć Czytelnikom pojęcie szacowania ryzyka. Jak napisaliśmy w części 3, „aby móc zarządzać ryzykiem, w pierwszej kolejności należy je oszacować”. Poniżej podajemy kilka definicji związanych z szacowaniem ryzyka, zaczerpniętych z międzynarodowego przewodnika zawierającego nomenklaturę dotyczącą szeroko pojętego zarządzania ryzykiem ISO/IEC Guide 73:2002 „Risk management – Vocabulary – Guidelines for use in standards”.

Szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka¹

Identyfikacja ryzyka – proces szukania, rozpoznania i opisanie ryzyka²

Analiza ryzyka – systematyczny proces zrozumienia natury ryzyka i wywnioskowania jego poziomu³

Ocena ryzyka – proces porównania rezultatów analizy ryzyka w stosunku do przyjętych kryteriów ryzyka do określenia poziomów ryzyka i przyjęcie akceptowalnych lub nieakceptowanych poziomów ryzyka⁴

Na następnej stronie przedstawiamy graficzną interpretację procesu szacowania ryzyka według dwóch modeli zarządzania ryzykiem, to jest normy ISO/IEC 27005⁵ oraz AS/NZS 4360⁶.

Można oczywiście polemizować na temat różnic w samym modelu zarządzania ryzykiem na przykładzie powyżej przedstawionych schematów, jednak prosimy zwrócić uwagę na zawartość pól w czerwonej ramce. W obydwu modelach powtarzają się procesy wchodzące w skład obszaru szacowania ryzyka. Tak więc widzimy, że pryncypia dotyczące szacowania ryzyka są generalnie takie same w odniesieniu do przedstawionych schematów. Możemy zaryzykować stwierdzenie, że przy analizie innych modeli zarządzania ryzykiem, np. AIRMIC, CRAMM, FERMA itp., odnajdziemy te same elementy, a różnice mogą wynikać z większej lub mniejszej szczegółowości dekompozycji poszczególnych elementów procesu szacowania ryzyka. Należy tutaj zaznaczyć, że cały proces szacowania ryzyka jest procesem subiektywnej oceny przez zespół – ekspertów przeprowadzających poszczególne etapy tego procesu, a wy-

bór metody czy techniki do realizacji poszczególnych działań (identyfikacji, analizy i kryteriów oceny ryzyka) zależy od wielu czynników związanych z profilem działalności organizacji, jej kultury i apetytu na ryzyko. Istnieją jednak uniwersalne techniki i metody, które mogą być wykorzystywane podczas realizacji elementów procesu szacowania ryzyka. Do takich należy macierz ryzyka lub znany w obszarze zarządzania wykres Ishikawy („rybiej ości”). Macierz ryzyka to metoda, od której naszym zdaniem każda firma czy organizacja powinna rozpocząć proces szacowania ryzyka. Powinno się potraktować to jako działanie wstępne. Następnie powinno się rozwinąć szacowanie ryzyka, stosując odpowiednio dostosowane do konkretnego obszaru bardziej skomplikowane metody.

Kluczowe elementy w obszarze szacowania ryzyka to identyfikacja i analiza ryzyka. Od tych elementów w dużej mierze zależy wartość dodana po przeprowadzeniu szacowania ryzyka. Oczywiście nie staramy się pomniejszyć wagi elementu oceny ryzyka, jednak ten element jest subiektywną wykładnią dla każdej organizacji.

Techniki identyfikacji i analizy ryzyka mogą być często takie same (np. przytoczona powyżej macierz ryzyka).

1) ISO/IEC Guide 73:2002 „Risk management – Vocabulary – Guidelines for use in standards”.

2) Tamże.

3) Tamże.

4) Tamże.

5) ISO/IEC 27005:2008 „Information technology – Security techniques – Information security risk management”.

6) The Australian and New Zealand Standard on Risk Management AS/NZS 4360:2004.

Zastosowana technika lub metoda identyfikacji ryzyka bezpośrednio przekłada się na proces analizy ryzyka.

Generalnie metody analizy ryzyka możemy podzielić na:

- **metody jakościowe** (*qualitative risk analysis*), które bazują na ocenie zagrożeń, poziomu ryzyka i wynikających z nich ewentualnych strat, na znajomości analizowanych zagadnień, doświadczeniu i intuicji osoby oceniającej (np. metoda *The Microsoft Corporate Security Group Risk Management Framework* – MCSGRMF);
- **metody ilościowe** (*quantitative risk analysis*), w ramach których próbuje się skwantyfikować i wyrazić

liczbowo, na podstawie danych statystycznych, wielkość potencjalnych strat, prawdopodobieństwo ich wystąpienia, a w efekcie poziom występujących ryzyk (np. metody Courtneya, Fishera, modele Markowa, *risk score*);

- **metody ilościowo-jakościowe**, które łączą obie ww. metody w jedną (np. macierz, FMEA).

Poniżej przedstawiamy kilka wybranych technik analizy ryzyka:

- badania rynku,
- prognozowanie,
- analiza skutków dla działalności,
- diagramy przyczynowo-skutkowe (CCD),
- analiza drzewa zdarzeń (ETA),

- analiza drzewa niesprawności (FTA),
- analiza rodzajów i skutków awarii (FMEA),
- analiza rodzajów, skutków i krytyczności uszkodzeń (FMECA),
- badanie zagrożeń i zdolności do działania (HAZOP),
- modele Markowa etc.

Szczegółowe omówienie którejkolwiek z wymienionych technik czy metod pochłonęłoby znaczną część niniejszego artykułu, a to tylko wybrane przykłady. Nie wspominamy tutaj o metodach stosowanych w obszarze działalności finansowej lub ubezpieczeniowej organizacji.

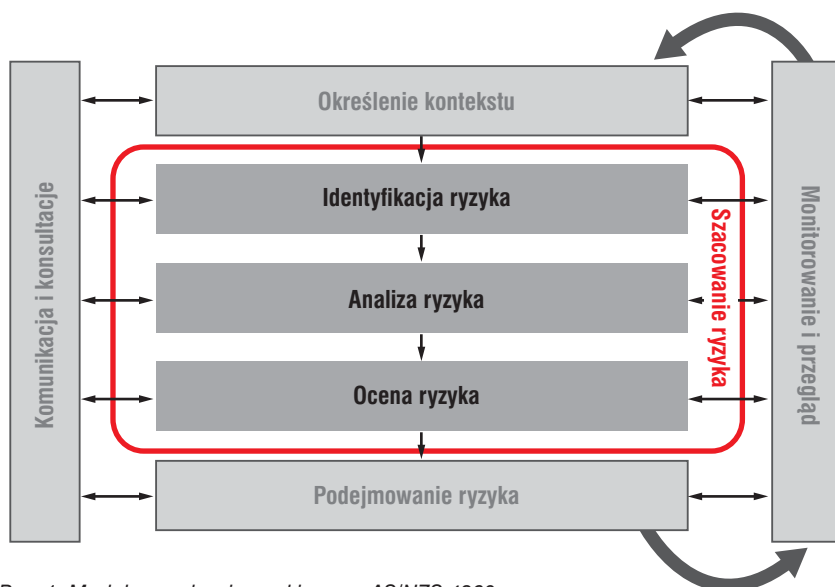
Mamy nadzieję, że poprzez cykl czterech artykułów przybliżyliśmy Czytelnikom podstawy zarządzania ryzykiem i zachęciliśmy do zgłębienia wiedzy z tego zakresu.

Zapraszamy zainteresowane osoby do kontaktu z nami poprzez naszą stronę internetową. Na Państwa życzenie możemy kontynuować tę tematykę, dostosowując interpretacje do określonych branż lub omawiając bardziej szczegółowo różne metodologie.

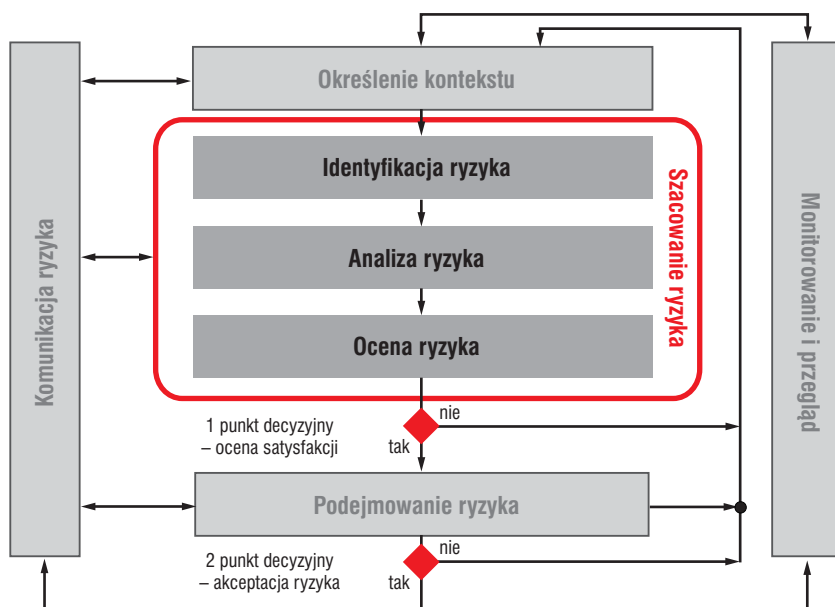
ANNA SŁODCZYK, PIOTR MAKOŚA
RISK MANAGEMENT TEAM POLAND
WWW.ANNASŁODCZYK.COM

Literatura:

1. ISO/IEC Guide 73:2002 „*Risk management – Vocabulary – Guidelines for use in standards*”.
2. ISO/IEC 27005:2008 „*Information technology – Security techniques – Information security risk management*”.
3. The Australian and New Zealand Standard on Risk Management AS/NZS 4360:2004.
4. PN/IEC 27001:2007 „*System zarządzania bezpieczeństwem informacji – wymagania*”.
5. Mirosław Ryba, wykład Ernst&Young pt. *Analiza i zarządzanie ryzykiem systemów informatycznych*.
6. Adam. S. Markowski, *Zapobieganie stratom w przemyśle – część III*, Politechnika Łódzka, 2000.



Rys. 1. Model zarządzania ryzykiem wg AS/NZS 4360



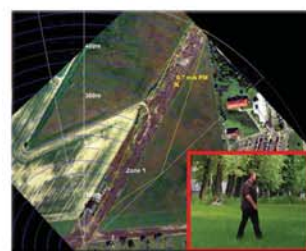
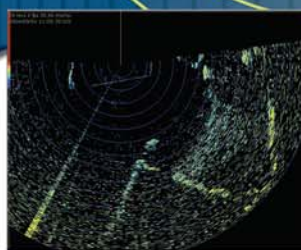
Rys. 2. Model zarządzania ryzykiem wg ISO/IEC 27005



WYZNACZAMY
NOWE GRANICE
OCHRONY



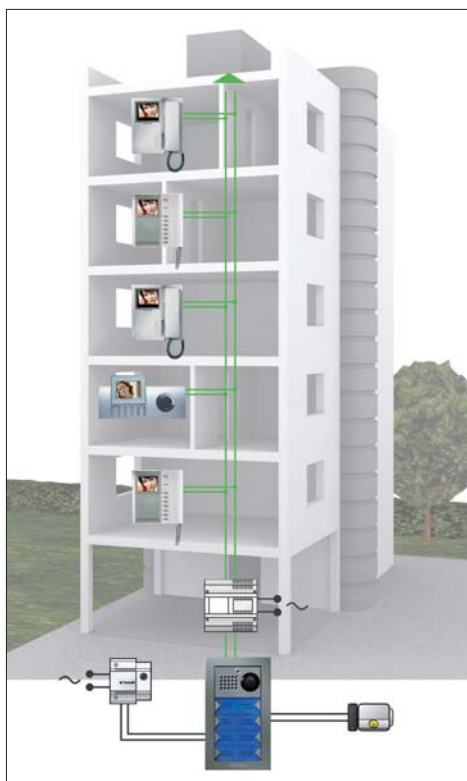
Nasze systemy radarowe wykrywają każde wtargnięcie osób i pojazdów na chroniony obszar, stale monitorując aktualną pozycję intruza. Radary automatycznie sterują zespołem kamer tworząc w pełni zintegrowany system ochrony.



KABE Sp. z o.o.

ul. Waryńskiego 63, 43-190 Mikołów
tel. 032 32 48 900 • fax 032 32 48 901
handel@kabe.pl • www.kabe.pl

2-przewodowy, kolorowy system wideodomofonowy firmy COMELIT



Cechy systemu:

- kolorowe monitory z ekranami LCD;
- 2 przewody łącznie z zasilaniem monitora;
- 4 magistrale na zasilacz (np. 4 piony w budynku mieszkalnym);
- do 8 monitorów z funkcją interkomu na każdy apartament;
- do 240 użytkowników;
- do 600 m maksymalnej odległości pomiędzy panelem wejściowym, a ostatnim monitorem;
- nieograniczona liczba paneli głównych i dodatkowych;
- centralny moduł portiera;
- proste programowanie za pomocą przełączników;
- możliwość tworzenia systemów mieszanych audio i video;
- funkcja dzwonka lokalnego;
- oddalona sygnalizacja wywołania;
- programowalny moduł przekąźnikowy sterowany przyciskiem monitora bądź wybranym zdarzeniem w systemie;
- moduł kamer zewnętrznych;
- interfejs sygnału wideo do postaci analogowej.

Monitory wewnętrzne dostępne w systemie Simplebus Color



GENIUS



BRAVO



DIVA



PLANUX

Panele wejściowe



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



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?

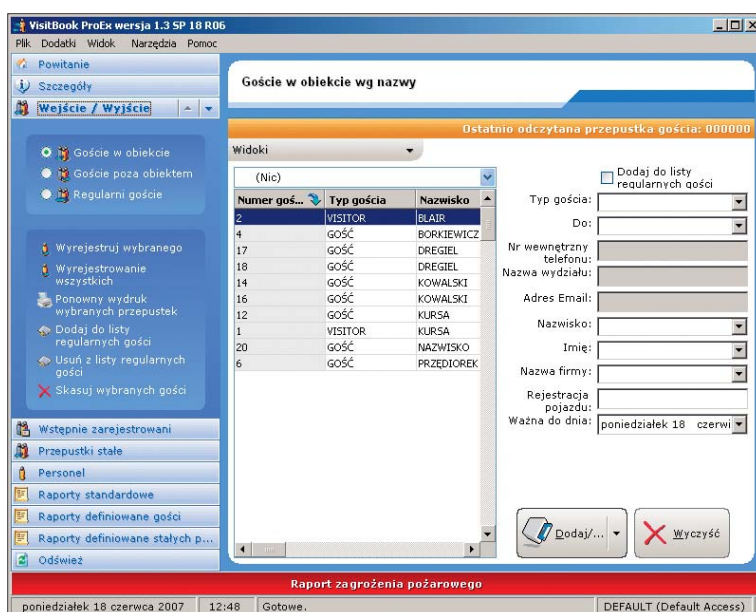
Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora.

Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.

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

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

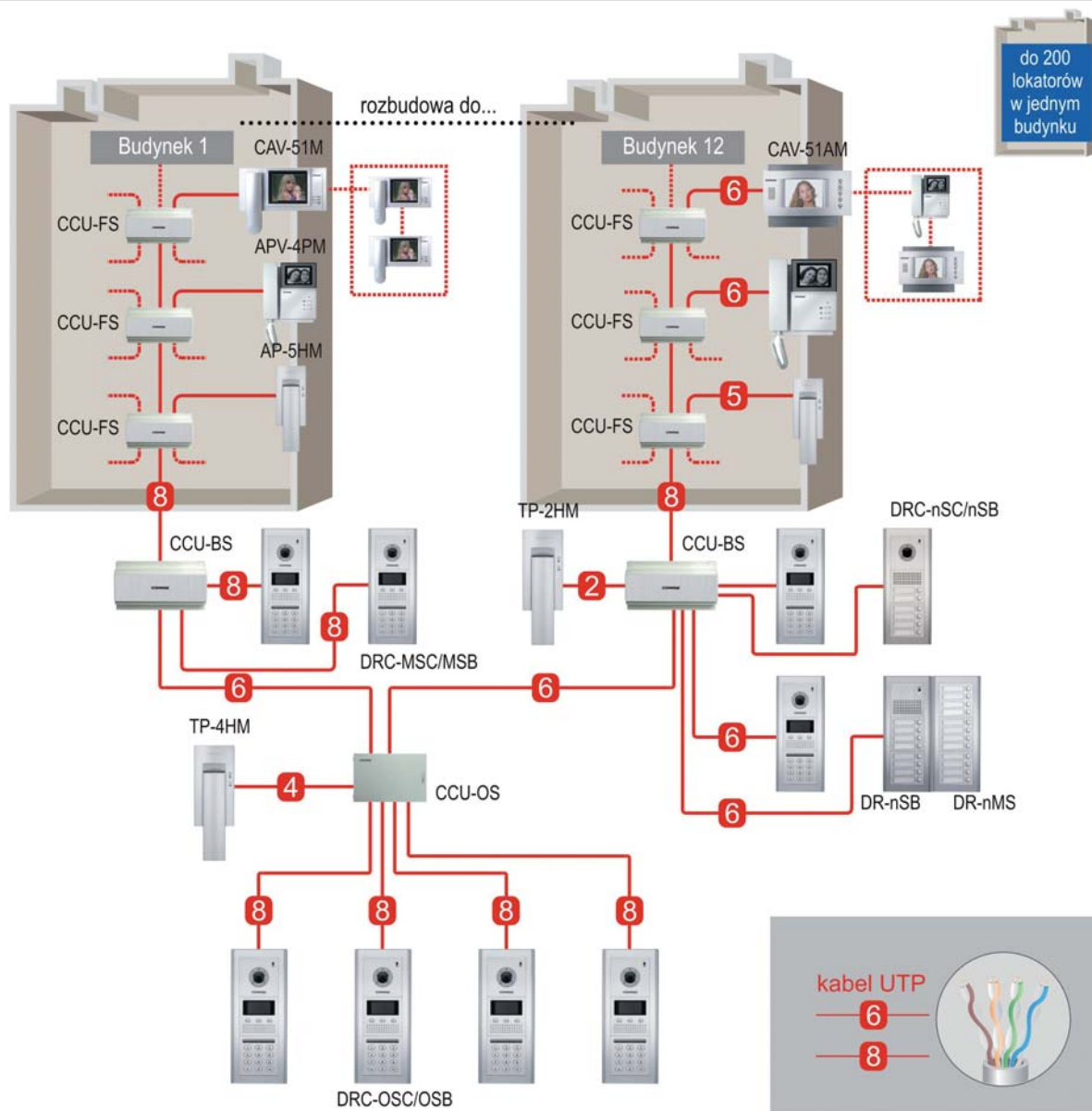
Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera 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



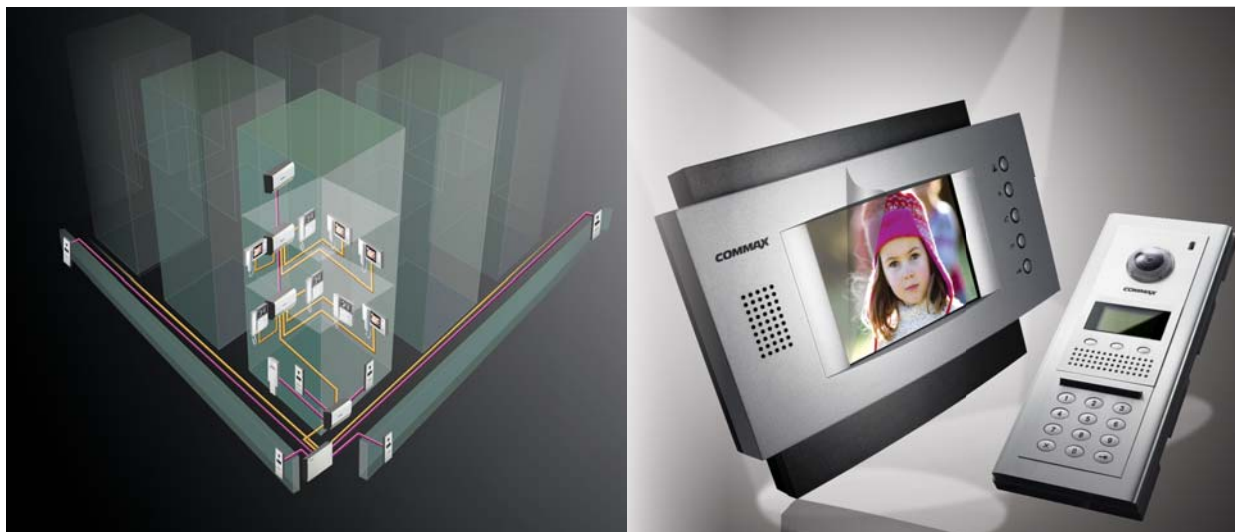
System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna ilość obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

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

1 przewód ...

... wiele
możliwości

Dystrybutory



CCU-OS



CCU-BS
CCU-FS

Kamera Falcon CDN 700F

dzień-noc z mechanicznym filtrem IR

Kamera Falcon CDN 700 F jest najnowszą kamerą w ofercie firmy Factor Security i otwiera nową linię urządzeń Falcon „Red Line”. Urządzenia z tej linii zapewniają wyższe parametry techniczne, większy zakres dostępnych opcji oraz jakość wynikłą ze stosowania w produktach linii „Red Line” japońskich podzespołów. CDN 700F to kamera dzień/noc, z mechanicznie przesuwanym filtrem podczerwieni, który odcinając promieniowanie podczerwone pozwala na prawidłowe odwzorowanie kolorów w dzień. W warunkach nocnych, gdy kamera pracuje w trybie monochromatycznym filtr jest odsunięty w celu wpuszczenia do przetwornika większej ilości światła. Kamera wyposażona została w przetwornik 1/3" SONY Super HAD o rozdzielczości dzień/noc 530/570 TVL oraz czułości 0,5/0,1 lx przy $F=1,2$. Dodatkowo kamera posiada możliwość konfigurowania kompensacji światła tylnego BLC oraz funkcję „sens-up”. Kamera oferowana jest w dwóch wersjach zasilania: 12 V_{DC} lub 230 V_{AC}.



- przetwornik 1/3" Super HAD SONY
- mechaniczny filtr podczerwieni
- funkcje przełącznika DIP
- wysoka rozdzielczość
- zaawansowana kompensacja tylnego oświetlenia
- flickerless

Specyfikacja techniczna	
Przetwornik	1/3" CCD Super HAD SONY
Obróbka sygnału	DSP
Rozmiar matrycy	PAL: 752 (H) x 582 (V) ~440 000 px
Rozdzielczość pozioma	530 TV linii – tryb kolorowy 570 TV linii – tryb czarno-biały
Synchronizacja	Wewnętrzna
Skanowanie	2:1 z przeplotem
Czułość	0,5 lx / F1.2; 30IRE – tryb kolorowy 0,1 lx / F1.2; 30IRE – tryb czarno-biały
Stosunek sygnał/szum	więcej niż 48dB
Automatyczna regulacja czułości	włączona/wyłączona
Automatyczny balans bieli	tak
Kompensacja światła tylnego	tak
Elektroniczna migawka	AI: 1/50 s; AES: 1/50 s do 1/100 000 s
Flickerless	włączone/wyłączone
Długość fali oświetlacza IR	od 700 do 1100 nm
Wyjście wizyjne	1 Vp-p Composite Video, 75 Ω
Montaż obiektywu	C/CS
Ogniskowa obiektywu	DC/VIDEO
Zasilanie	12 V _{DC} lub 230 V _{AC}
Pobór prądu	200 mA
Warunki pracy	od -10°C do + 50°C / wilgotność do 70%
Wymiary / Masa	60 x 53 x 110 mm / 550 g



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
<http://www.factor.pl>

Kompleksowe rozwiązanie RCP firmy ROGER



Kompleksowe rozwiązanie RCP firmy ROGER ułatwia zarządzanie czasem pracy, precyzyjne jego rozliczanie oraz wpływa na redukcję kosztów, przyczyniając się do wzrostu efektywności przedsiębiorstwa.

Program RCP Master został opracowany w środowisku Microsoft .NET i jest przeznaczony dla systemów operacyjnych Windows XP i Vista. RCP Master posiada przyjazny interfejs, jest bezpieczny i łatwy w obsłudze. Program może być użytkowany bezpłatnie w celach ewaluacyjnych przez pierwsze 60 dni po instalacji.

Dla celów rejestracji czasu pracy firma Roger zaleca wykorzystanie kontrolera PR602LCD. Kontroler ten posiada wyświetlacz LCD oraz zestaw czterech programowalnych klawiszy funkcyjnych, które mogą być wykorzystane jako przyciski wyboru rodzaju rejestracji (wejście, wyjście, wyjście służbowe itp.). Kontroler PR602LCD posiada wbudowany bufor zdarzeń i może pracować samodzielnie lub w sieciowym systemie kontroli dostępu typu RACS (Roger).

Charakterystyka RCP Master

Import/eksport danych:

- Import zdarzeń z systemu kontroli dostępu RACS v4.2.5.38 i wyższe
- Import zdarzeń z pliku tekstowego w formacie CSV oraz XML
- Eksport raportów w formacie Adobe Acrobat (.pdf), Microsoft Excel (.xls), Microsoft Word (.doc), Rich Text Format (.rtf) i Crystal Reports (.rpt)
- Eksport raportów czasu pracy w formacie XML

Definicje :

- Dni kalendarza: dzień roboczy, dzień roboczy dodatkowy, święto, dzień wolny itp.
- Typów obecności i absencji: urlop wypoczynkowy, nieobecność nieusprawiedliwiona, przerwa obiadowa itp.
- Maksymalnych i minimalnych czasów przebywania (np. maks. dzienna norma przerw na papierosa, minimalny czas pracy itp.)
- Dodatkowe opcje związane ze spóźnieniami, wcześniejszymi wyjściami, zaliczaniem czasu przed i po godzinach pracy itp.
- Typów przejść: wejście, wyjście, wyjście służbowe itd.
- Wymiarów urlopów i raport stanu ich wykorzystania

Raporty:

- Raporty: grupy pracowników, pracownicy, kalendarze, punkty kontrolne, rejestr zdarzeń RCP, raporty czasu pracy, wymiary urlopów, indywidualne kalendarze itp.
- Możliwość tworzenia dowolnego zestawienia raportów przy pomocy kreatora raportów zarówno zbiorczych dla całej grupy jak i indywidualnych dla poszczególnych pracowników.
- Możliwość automatycznego rozsyłania indywidualnych raportów pocztą e-mail na adres pracownika

Plik Danych:

- Relacyjna, plikowa baza danych typu MS Access
- Praca z lokalną bazą danych lub udostępnioną w sieci komputerowej
- Możliwość ustawiania hasła dostępu do pliku bazy danych
- Możliwość szyfrowania pliku bazy danych
- Kompaktowanie i naprawa pliku bazy danych
- Możliwość operacji na bazie z dowolnego innego programu (np. własna implementacja dopisywania zdarzeń RCP przez system zewnętrzny)

Pozostałe:

- Możliwość korekty i wstawiania brakujących zdarzeń RCP oraz edycja absencji
- Indywidualne kalendarze pracy z możliwością korekty kalendarza dla poszczególnych pracowników np. odpracowywanie, zamiany itp.
- Obsługa zaokrąglania czasu rozpoczęcia i zakończenia pracy
- Obsługa przerw płatnych i niepłatnych
- Obsługa nadgodzin (5 predefiniowanych typów)
- Definiowanie operatorów programu i ich uprawnień
- Rejestracja działań operatorów
- Systemy operacyjne: Windows XP i Vista
- Darmowa aktualizacja w ramach tej samej wersji programu

Wersje licencji:

- Maksymalna obsługiwana liczba pracowników:
 - do 50
 - do 250
 - bez ograniczeń
- Rodzaje licencji:
 - Jednostanowiskowa (pojedyncza instalacja)
 - Wielostanowiskowa (obsługa określonej liczby stanowisk z programem, wymagana instalacja serwera licencji)

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



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



Producent Bezprzewodowych Systemów Transmisji AU / Telenet
Pasmo 2,41 5,8 GHz

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. Łęczyńska 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. Mieszkańska 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 Łakach 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



Fire & Security

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

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

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

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

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

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

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

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

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

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

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

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



ALKAM SYSTEM Sp. z o.o.

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



AMBIENT SYSTEM Sp. z o.o.

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



ANB Sp. z o.o.

ul. Ostrobramska 91
04-118 Warszawa
tel. (22) 612 16 16
faks (22) 612 29 30
e-mail: 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



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 b
31-431 Kraków
tel. (12) 410 85 10
faks (12) 410 85 11
e-mail: saik@saik.pl
www.saik.pl



LEGRAND POLSKA Sp. z o.o.
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.zamkielektyczne.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. Na Niskich Łakach 26, 50-422 Wrocław
tel. (71) 340 0 209
faks (71) 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Raclawska 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

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



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



CONTROL SYSTEM FMN Sp. z o.o.
Al. KEN 96/U15
02-777 Warszawa
tel./faks (22) 855 00 17
e-mail: pk@cs.pl
www.cs.pl



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@dmxpolska.pl
www.dmxpolska.pl

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



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

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

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

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

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



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



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

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



DELTA BUSINESS SERVICE
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.dpkssystem.pl
 www.jablotron.pl



**Przedsiębiorstwo Usług Inżynierskich
 DRAVIS Sp. z o.o.**
 ul. Bukowa 1
 40-108 Katowice
 tel. (32) 253 99 10
 tel./faks (32) 253 70 85
 e-mail: dravisdravis@neostrada.pl
 info@dravis.pl
 www.dravis.pl

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



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



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



ELACOMPIL
 security management solutions

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



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

Oddział:
 ul. Jana Kazimierza 61, 01-267 Warszawa
 tel./faks (22) 836 54 05, 837 75 93
 tel. kom. 0 602 222 516
 e-mail: warszawa@emu.com.pl



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



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

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

ul. Grabiszyńska 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
 GLOBAL DISTRIBUTOR OF ELECTRONICS

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. Piwoniczka 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.
 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

**P.W. IRED**

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

**ISM EuroCenter S.A.**

ul. Wycółki 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. Mikiciuk, R. Rutkowski Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. (58) 553 67 59
faks (58) 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

**KRAK-POŻ Sp. z o.o.**

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

**PP.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**

Galka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks (67) 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

**MICRONIX Sp. z o.o.**

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

**MIWI-URMET Sp. z o.o.**

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

**NOMA 2**

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

Oddziały:

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

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

**NORBAIN POLSKA Sp. z o.o.**

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

Biuro:

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

**OBIS CICHOCKI ŚLĄZAK Sp. J.**

ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
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

**PAG Sp. z o.o.**

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

Oddział:

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

**PANASONIC POLSKA Sp. z o.o.**

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

**PETROSIN Sp. z o.o.**

Rynek 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**

ul. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35, 831 18 97
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.pl



POLON-ALFA

Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
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 Łapczyca
tel. (14) 610 19 40
faks (14) 610 19 50
e-mail: biuro@pulsarspj.com.pl
www.pulsarspj.com.pl



PRH. PULSON

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



RAMAR s.c.

ul. Modlińska 237
03-120 Warszawa
tel. (22) 676 77 37
faks (22) 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl



ROPAM Elektronik s.c.

Os. 1000-lecia 6A/1
32-400 Myślenice
tel. (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. Łączyny 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: office.warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:

ul. Wierzbicę 1, 61-569 Poznań
tel. (61) 833 31 53
faks (61) 833 50 37
e-mail: office.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 86 17
faks (22) 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl



Oddział:

ul. Różycyńskiego 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/blucenergy

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. Glinki 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.jesioneck@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: olsztyn@sprint.pl
www.sprint.pl

Oddziały:

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

ul. Przemysłowa 15

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

ul. Heyki 27c

70-631 Szczecin
tel. (91) 485 50 00
faks (91) 485 50 12
e-mail: szczecin@sprint.pl

ul. Canaletta 4

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

S.P.S. Trading Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. (22) 518 31 50
faks (22) 518 31 70
e-mail: warszawa@spstrading.com.pl
www.spstrading.com.pl

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

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

ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl

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

**CENTRUM SYSTEMÓW ZABEZPIECZEŃ**

STRATUS
ul. Nowy Świat 38
20-419 Lublin
tel./faks (81) 743 87 72
e-mail: stratus@stratus.lublin.pl
www.stratus.lublin.pl

SYSTEM 7
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. Walońska 3-5
50-413 **Wrocław**
tel. (71) 340 58 00
faks (71) 340 58 02

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



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



TAYAMA POLSKA Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, (32) 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl



Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
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 97
Sprzedaż: (22) 516 97 97
faks (22) 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TELCOMP-SERVICE Sp. z o.o.

ul. Annopol 4
03-236 Warszawa
tel. (22) 811 02 59
tel. kom. (0) 662 008 600
e-mail: biuro@telcomp-service.pl
www.centrum-ts.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: tpeltechinfo@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: zbgnew.chodkiewicz@telekomunikacja.pl

TRIKON

32-447 Siepraw 1123
tel. (12) 274 61 27
faks (12) 274 51 51
e-mail: biuro@trikon.com.pl
www.trikon.com.pl

**UNICARD S.A.**

GRUPA FIRM UNICARD

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. (12) 398 99 00
faks (12) 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

Oddziały:

ul. Ratuszowa 11, 03-450 **Warszawa**
tel. (22) 619 22 04
faks (22) 818 64 67

Os. Polan 33, 61-249 **Poznań**
tel. (61) 872 92 08+10
faks (61) 872 96 30



W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. (52) 345 45 00
tel./faks (52) 584 01 92
e-mail: lukasz.cellari@w2.com.pl
www.w2.com.pl

**Vision Polska**

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

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystribucja	instalacja	szkolenia
2M Elektronik	-	TAK	TAK	TAK	-
3D	TAK	TAK	-	-	TAK
AAT Holding	-	TAK	TAK	-	TAK
ACSS ID Systems	-	-	TAK	-	-
ADT Poland	-	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	-
Alarmnet Sp. J.	-	TAK	TAK	-	TAK
Alarmtech Polska	TAK	TAK	-	-	TAK
Aldom	-	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	-
Alpol Sp. z o.o.	-	-	TAK	-	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	-	TAK	TAK	TAK	-
Anma	-	TAK	-	TAK	TAK
Atline Sp. J.	-	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
Cezim	TAK	TAK	TAK	-	TAK
CMA Sp. z o.o.	TAK	TAK	TAK	TAK	-
COM-LM	TAK	TAK	TAK	TAK	-
CONTROL SYSTEM FMN	-	TAK	TAK	TAK	-
D-MAX	-	TAK	TAK	-	TAK
D + H Polska	TAK	TAK	TAK	TAK	TAK
DANTOM	TAK	-	TAK	-	-
DAR-ALARM	-	TAK	TAK	TAK	TAK
Delta Business Service	-	TAK	-	TAK	TAK
DG Elpro	-	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	-	-
DPK System	-	-	TAK	-	TAK
Dravis	-	TAK	-	TAK	-
Dyskret	-	TAK	TAK	TAK	TAK
EBS	TAK	-	TAK	-	-
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compil	TAK	-	TAK	-	TAK
EI-Mont	-	TAK	-	TAK	-
Elproma	-	TAK	-	TAK	-
Eltrac	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
HSA	-	-	TAK	-	-
ICS Polska	-	-	TAK	-	TAK
Info-Cam	TAK	TAK	TAK	TAK	TAK
Insap	-	TAK	TAK	TAK	TAK
Ired	TAK	TAK	TAK	TAK	-

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystribucja	instalacja	szkolenia
ISM EuroCenter	-	-	TAK	-	-
Janex International	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	-	TAK	-	TAK	-
Kolektor MR	-	TAK	TAK	TAK	-
Krak-Poż	-	TAK	-	TAK	-
Laskomex	TAK	TAK	TAK	-	TAK
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	-
NORBAIN Polska	TAK	-	TAK	-	TAK
OBIS Sp. J.	-	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	-	-	TAK	-	-
PAG	TAK	TAK	TAK	TAK	-
Panasonic	-	-	TAK	-	TAK
Petrosin	-	TAK	-	TAK	-
Pointel	-	TAK	-	TAK	-
POL-ITAL	-	-	TAK	-	-
Polon-Alfa	TAK	-	-	-	-
ProfiCCTV	-	TAK	TAK	-	TAK
Pulsar	TAK	-	TAK	-	-
PPH Pulson	TAK	TAK	TAK	-	-
Radioton	-	-	TAK	-	-
Ramar	TAK	-	TAK	TAK	TAK
ROPAM Elektronik	TAK	-	TAK	-	-
Sagitta Sp. z o.o.	TAK	-	-	-	-
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 Sp. z o.o.	-	TAK	-	TAK	TAK
S.P.S. Trading	TAK	TAK	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	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	TAK	-	-	-	-
Telcomp-Service	-	-	-	-	TAK
TP TELTECH	-	TAK	TAK	TAK	-
Trikon	TAK	TAK	-	TAK	-
UNICARD S.A.	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	-	-
Vision Polska	-	TAK	TAK	-	TAK

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy 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 Poland	TAK	TAK	TAK	TAK	-	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	-	-	-	-	-	-
Alarmnet Sp. J.	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 Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Ambient System	TAK	TAK	TAK	TAK	-	-	-	-	TAK
ANB	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
Anma	TAK	TAK	TAK	TAK	-	TAK	-	-	-
ATLine Sp. J.	TAK	TAK	TAK	TAK	TAK	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	-
Cezim	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
CMA Sp. z o.o.	TAK	-	-	-	-	-	TAK	-	-
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Control System FMN	TAK	TAK	TAK	TAK	-	TAK	-	TAK	-
D-MAX	-	TAK	-	-	-	-	-	-	-
D + H	-	-	-	TAK	-	TAK	-	-	TAK
DANTOM	TAK	TAK	TAK	TAK	-	-	-	TAK	-
DAR-ALARM	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Delta Business Service	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	-	-	TAK	-	-	-	-	TAK	-
DPK System	TAK	TAK	-	-	-	-	TAK	-	-
Dravis	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Dyskret	TAK	TAK	TAK	TAK	-	TAK	-	TAK	TAK
EBS	TAK	-	TAK	TAK	-	TAK	TAK	-	-
EDP Support Polska	-	TAK	TAK	-	TAK	TAK	-	TAK	-
ela-compil	-	-	-	-	-	TAK	-	-	-
El-Mont	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Eltrac	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	-	-
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
Ired	TAK	TAK	TAK	-	-	TAK	TAK	-	-

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnienia
ISM EuroCenter	-	TAK	TAK	-	-	TAK	TAK	-	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Krak-Poż	-	-	-	TAK	-	-	TAK	-	TAK
Laskomex	-	TAK	TAK	-	-	-	-	TAK	-
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
NORBAIN Polska	-	TAK	-	-	-	TAK	-	-	-
OBIS Sp. J.	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	-	-	-	-	TAK	-
PAG	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Panasonic	-	TAK	TAK	-	-	TAK	-	-	-
Petrosin	TAK	TAK	TAK	-	-	-	-	-	-
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
POL-ITAL	-	-	TAK	-	-	-	-	TAK	-
Polon-Alfa	-	-	-	TAK	-	-	-	-	-
ProfiCCTV	TAK	TAK	TAK	TAK	-	-	-	-	-
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 Sp. z o.o.	-	-	-	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 Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
STRATUS	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SYSTEM 7	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
Telcomp-Service					szkolenia				
TP TELTECH	TAK	TAK	TAK	TAK	TAK	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	TAK	-	-	-	-	-
Vision Polska	-	-	-	TAK	-	-	-	-	-

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny

Teresa Karczmarzyk
teresa@zabezpieczenia.com.pl

Redaktor merytoryczny

Adam Bułaciński
adam@zabezpieczenia.com.pl

Dział marketingu i reklamy

Ela Końska
ela@zabezpieczenia.com.pl

Redaguje zespół:

Krzysztof Białek

Marek Blim

Patryk Gańko

Norbert Góra

Ireneusz Kryswaty

Paweł Niedziejko

Edward Skiepmo

Ryszard Sobierski

Waldemar Szulc

Adam Wojcinowicz

Marek Życzkowski

Współpraca zagraniczna

Rafał Niedzielski

rafal@zabezpieczenia.com.pl

Współpraca

Marcin Pyclik

Sławomir Wagner

Andrzej Wójcik

Skład i łamanie

Marek Bładoszewski

Korekta

Paweł Karczmarzyk

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:

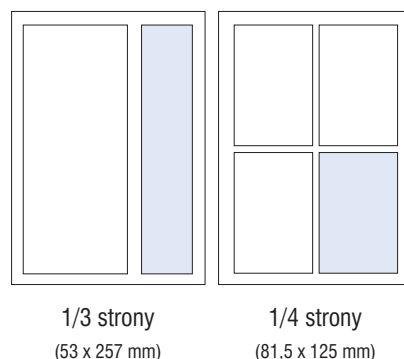
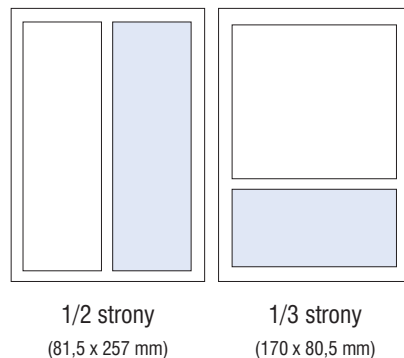
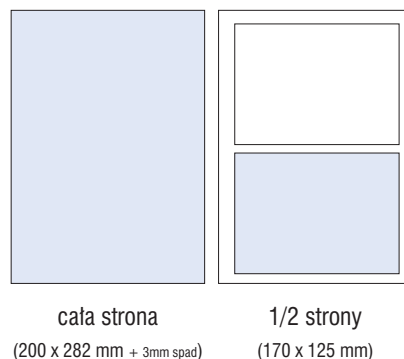
jednorazowy wpis	70 zł
------------------	-------

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	60, 72	Ifter	77
ACSS	59, 69	Kabe	80
Alarmtech	45	Panasonic	1
Altram	21	Polon-Alfa	49
Ambient System	7	Roger	34
ATIline	29	Satel	5
Bosch	2	Sony	41
Camsat	99	Techom	20
Gunnebo	20	Videotec	35
HID	100	WSM	68
IFSEC	4		

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: 1699-5419 • DWUMIESIĘCZNIK NR 2(86) 2009
WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ENER@ZABEZPIECZENIA.COM.PL

Panasonic
Ideas for life

Przetwornik CCD 1,3 Megapiksela, pozwoli Ci zobaczyć więcej

Profesjonalny sieciowy system monitoringu wizyjnego dostarcza doskonałej jakości obrazów oraz gwarantuje wysoką jakość całego systemu

I-Pro Network Surveillance System
<http://panasonic.net/iaq/itp/>

W NUMERZE:

- Wzrosty opóźnienia w sieciach IP na skuteczność monitoringu wizyjnego
- Systemy sygnalizacji włamania. Część I. Konfiguracja central alarmowych
- Nowe sterowniki obiektów monitorowanych przez systemy telewizji dwukolorowej
- Matryca SABA - nowoczesne źródło światła bezpieczeństwa w profesjonalizmie



CYFROWA, BEZPRZEWODOWA TRANSMISJA
OBRAZU VIDEO 5.2GHZ

Nowa generacja systemów bezprzewodowych wideo

**NOWOŚCI
2009 !**

ZESTAW ZEWNĘTRZNY IP65 CDS 5021H

- transmisja do 5 km
- nie wymaga 100% "widzialności optycznej" anten



- rozdzielczość 720x576 (D1)
- prędkość wyświetlania 25kl/s przy D1
- 21 kanałów pracy
- modulacja OFDM (WIMAX)
- częstotliwość pracy 5.2 GHz
- transmisja szyfrowana 128 bitowym kodem
- wysoce odporny na zakłócenia przemysłowe np. z linii wysokiego napięcia, sieci trakcyjnej

MINIATUROWY ZESTAW WEWNĘTRZNY 5.8GHZ

TCO 5807M

- transmisja do 200 m i 2 km
- 7 kanałów pracy
- nadajnik przeznaczony do montażu w obudowach kamer



ZESTAW WEWNĘTRZNY CDS 5021

Przeznaczony do:

- monitoringu wind i obiektów ruchomych
- transmisji obrazów przez ściany oraz kondygnacje m.in. w szpitalach i salach konferencyjnych



PRODUCENT: P.W. CAMSAT; ul. Garbary 5 ; 86-050 Solec Kujawski;
tel. 052 387 3658 tel/fax. 052 387 5466
www.camsat.com.pl camsat@camsat.com.pl

Nasze karty obieghy cały świat.

A teraz poszerzamy
je o szereg nowych
możliwości.

HID

METODY ZARZĄDZANIA DOSTĘPEM I IDENTYFIKACJĄ

Fizyczna Kontrola Dostępu
Logiczna Kontrola Dostępu
Rozwiązania Wspólne
Dystrybucja Kart
Technologia wklejania
dodatkowych elementów

ROZWIĄZANIA TECHNOLOGII IDENTYFIKACJI

Płatność bezgotówkowa
Przemysł i Logistyka
Administracja i Instytucje
Rządowe
Żywność i Zwierzęta

hidglobal.com

HID Global, światowy lider technologii kart i czytników kontroli dostępu, przedstawia nowe spektrum bezpiecznej identyfikacji.

Firma HID rozslawiła się dobrą reputacją opartą o najwyższą jakość, pewność technologii i ciągłą innowacyjność w dziedzinie kart i czytników kontroli dostępu. Teraz postanowiliśmy wzbogacić naszą ofertę produkcji kart o nowe możliwości, poczynając od kontroli dostępu poprzez protokoły Ethernet, aż do rozwiązań wykorzystywanych w transporcie publicznym. Wierzymy, iż przyszłość bezpiecznej identyfikacji należy upatrywać w otwartości na nowości, elastycznych produktach i zbieżności technologii. To jest naszym celem, więc jeżeli szukasz nowych rozwiązań identyfikacji zgłoś się do HID. Twoje oczekiwania mogą już być wykorzystane w naszych kartach.



ACCESS choices.