CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(99)/2014

ZABEZPIECZENIA

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

W NUMERZE:

FUJIFILM
Value from Innovation

Bezpieczeństwo w nowym wymiarze:

4K

Pierwszy obiektyw Fujinon typu Vari Focal

kremer kommunikation

Day Night

Nowy DV2.2x4.1SR4A-SA2L firmy Fujifilm
Doskonała rozróżnialność szczegółów dzięki rozdzielczości obrazu 4K.
Nadający się do użytku 24 godziny na dobę dzięki technologii dzień/noc.
Więcej informacji na stronie www.fujifilm.eu/fujinon lub per scan.
Fujinon. Widzisz więcej. Wiesz więcej.

FUJINON

Spis treści

CZASOPISMO ZABEZPIECZENIA 5/2014

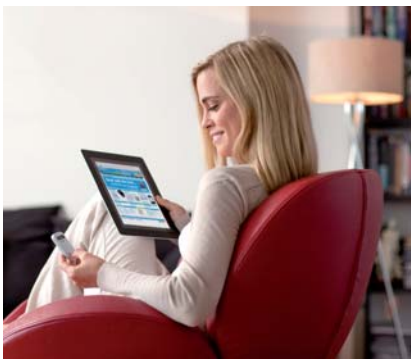
Inteligentnie czy nie? **26**

Sieciowy system trankingowy DMR **56**

Ratunkowe systemy interkomowe **60**

Malware i DDoS – co mają ze sobą wspólnego? **64**

Tokeny firmy HID Global dla klientów korporacyjnych mBanku



mBank (jeden z największych polskich banków) pomyślnie wdrożył tokeny ActivID DisplayCard firmy **HID Global** (czołowego producenta urządzeń przeznaczonych do zarządzania tożsamością) służące do uwierzytelniania wieloskładnikowego. Tokeny zapewnią klientom korporacyjnym mBanku bezpieczny dostęp do bankowości internetowej i mobilnej. mBank to jeden z pionierów bankowości korporacyjnej w Polsce. W 2013 roku został doceniony przez stowarzyszenie Efma i firmę Assencure za innowacyjność, otrzymując nagrodę w kategorii *The Most Disruptive Innovation* za projekty i inicjatywy w dziedzinie finansowych usług detalicznych, które radykalnie zmieniają sposób prowadzenia działalności.

mBank szukał bezpiecznej, wygodnej, nowatorskiej i łatwej do zastosowania metody uwierzytelniania dla swojej bankowości internetowej i mobilnej. Tokeny ActivID DisplayCard firmy HID Global spełniły rygorystyczne wymagania. Ponadto wykorzystują unikalny, opatentowany algorytm HID Global, który jest kompatybilny z wewnętrznym systemem mBanku.

Token ActivID DisplayCard to przypominające kartę kredytową urządzenie uwierzytelniające, które mBank oferuje swoim klientom korporacyjnym. Token ma zintegrowaną klawiaturę dotykową do bezpiecznego wprowadzania numeru PIN. Dzięki niewielkim rozmiarom łatwo mieści się w portfelu. Nie wymaga specjalnego czytnika i jest rozwiązaniem uniwersalnym, opłacalnym i wygodnym dla klientów.

Bezpośr. inf. Jeremy Hyatt
HID Global
Tłumaczenie: Redakcja

Nowe kamery AXIS P39-R

Firma **Axis Communications**, światowy lider w dziedzinie sieciowych systemów dozorowych, informuje o wprowadzeniu na rynek nowych kamer z serii **AXIS P39-R**. Kamery te są przystosowane do pracy w bardzo złych warunkach eksploatacyjnych, odporne na wibracje, wstrząsy, udary mechaniczne i gwałtowne zmiany temperatury, a także zabezpieczone przed przedostawaniem się do ich wnętrza zanieczyszczeń oraz wody. Ponadto zabezpieczono je przed aktywnym sabotażem – sygnalizują próby zasłonięcia obiektywu i zamalowania obudowy farbą w sprayu.

Nowe kamery sieciowe z serii AXIS P39-R mają kompaktową konstrukcję. Są przeznaczone do obserwacji przestrzeni wewnątrz autobusów, pociągów, wagonów metra oraz pojazdów pracujących w trudnych warunkach środowiskowych.

– Kamery sieciowe z serii AXIS P39-R wytwarzają obraz o wysokiej rozdzielczości, zgodny ze standardem HDTV, dokonują obróbki tego obrazu za pomocą procesora sygnałowego i zapewniają możliwość rejestracji materiału wizyjnego na wbudowanej karcie pamięci, dzięki czemu spełniają najbardziej wyrafinowane wymagania klientów – powiedział **Erik Fränlid**, dyrektor do spraw produktów w firmie Axis Communications. *– Podczas projektowania kamer z serii AXIS P39-R wzięto pod uwagę łatwość ich zastosowania w istniejących instalacjach. Dzięki temu klienci będą mogli bez przeszkód modernizować swoje systemy dozorowe. Ponadto, z tych samych względów, w kamerach z serii AXIS P39-R zastosowano ten sam interfejs fizyczny co w znanych i cieszących się dużą popularnością modelach z serii AXIS M31.*

W skład serii AXIS P39-R wchodzą modele AXIS P3904-R o rozdzielczości HDTV 720p, AXIS P3905-R o rozdzielczości HDTV 1080p oraz wzbogacone o funkcje transmisji dźwięku i obsługi dodatkowych wejść/wyjść sterujących modele AXIS P3915-R o rozdzielczości HDTV 1080p. Każdy z tych modeli jest dostępny w wersji ze złączem RJ45 lub ze wzmocnionym złączem M12.

Wszystkie wymienione kamery szybko reagują na zmiany poziomu oświetlenia obserwowanej sceny, dzięki czemu jakość obrazu stale utrzymuje się na wysokim poziomie. Zastosowanie przetwornika obrazowego z progresywnym skanowaniem pozwala na odwzorowanie ruchomych obiektów bez zniekształceń geometrycznych. Specjalny tryb pracy określany mianem *Traffic Light* umożliwia lepsze rozpoznawanie kolorów świateł sygnalizatorów ulicznych w nocy.

Wraz z kamerami z serii AXIS P39-R dostarczane są specjalne narzędzia pozwalające na obrót i wypoziomowanie kulistej części zawierającej obiektyw i przetwornik obrazowy, dzięki czemu montaż tych kamer jest bardzo łatwy. Te same narzędzia mogą być wykorzystane do wymiany obiektywu i regulacji ostrości, gdy zachodzi konieczność zmiany kąta widzenia. Dostarczany jest również kalkulator umożliwiający sprawdzenie, czy przy danym ustawieniu kamery spełnione są wymagania dotyczące liczby pikseli na jednostkę długości obserwowanych obiektów, wynikające ze specyficznych wymogów formalnych.

Kamery z nowej serii AXIS P39-R są już dostępne w sieci dystrybucyjnej firmy Axis.

Bezpośr. inf. Axis Communications
Tłumaczenie: Redakcja

Videotec France przenosi się do Paryża

Mając na uwadze konieczność zapewnienia jak najlepszej obsługi swoim klientom, francuski oddział firmy **Videotec** przenosi się ze swojej dotychczasowej siedziby znajdującej się w pobliżu Rouen w północnej Francji, którą zajmował od 1992 roku, do Parc d'Activité de Courtabœuf – jednego z największych francuskich centrów biznesowych mieszczącego się w południowej części Paryża.

Dostęp do nowej siedziby firmy Videotec będzie dla klientów łatwiejszy niż dotychczas. Ponadto w nowej siedzibie utworzona będzie sala konferencyjna, w której odbywać się będą pokazy urządzeń produkowanych przez firmę Videotec oraz szkolenia wyjaśniające sposób ich wykorzystania.

Nowa paryska siedziba firmy Videotec została otwarta pierwszego sierpnia 2014 r. Wszystkie informacje dotyczące jej lokalizacji oraz numery telefonów i inne dane kontaktowe są dostępne na stronie *videotec.com*.

Poza oddziałem we Francji firma Videotec ma swoje przedstawicielstwa w USA i w Hongkongu oraz liczne biura lokalne na całym świecie. Dzięki temu nabywcy urządzeń wizyjnych przeznaczonych do pracy w trudnych warunkach środowiskowych znajdą pomoc i informacje techniczne na najwyższym poziomie.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

Centrum Handlowe na Placu Unii Lubelskiej w Warszawie z systemami zabezpieczeń firmy Bosch

Nowe centrum na Placu Unii Lubelskiej w Warszawie to kompleks trzech budynków, których łączna powierzchnia wynosi ponad 100000 m^2. Firma **Bosch Systemy Zabezpieczeń** dostarczyła do tego obiektu wszystkie systemy ochrony, m.in. system sygnalizacji pożarowej, system telewizji dozorowej, system kontroli dostępu oraz dźwiękowy system ostrzegawczy.

Kompleks na Placu Unii Lubelskiej w Warszawie, ukończony w maju tego roku, składa się z 23-piętrowego wieżowca oraz dwóch 7-piętrowych łączników w ustawieniu trójkątnym. Kompleks mieści galerię handlową, biura oraz parking. Firma **CORAL**, lokalny partner firmy Bosch, zainstalowała w budynkach wyżej wymienione systemy, wykorzystując wyłącznie rozwiązania technologiczne firmy Bosch. Wszystkie urządzenia są połączone za pośrednictwem sieci IP i działają z wykorzystaniem systemu BIS (Bosch Building Integration System).

– *Połączenie potencjałów dwóch firm, Bosch i CORAL, zaowocowało dostarczeniem klientowi końcowemu zabezpieczeń budynku na najwyższym poziomie* – powiedział **Krzysztof Góra**, dyrektor handlowy działu Bosch Systemy Zabezpieczeń.

W kompleksie znajduje się centrum monitorowania, w którym pracownicy ochrony mogą nadzorować działanie wszystkich systemów bezpieczeństwa. Dzięki ścisłej integracji istnieje możliwość korzystania ze wszystkich kamer telewizji dozorowej w celu natychmiastowej weryfikacji przyczyn alarmów generowanych przez inne systemy, co znacznie skraca czas reakcji i poprawia efektywność ochrony. System sygnalizacji pożarowej ma budowę modułową i składa się z ośmiu central sygnalizacji pożarowej pracujących w sieci, które obsługują ponad 14000 punktów detekcyjnych i sterujących (czujek pożarowych oraz modułów wejść/wyjść sterujących i monitorujących urządzenia zewnętrzne). W przypadku alarmu pożarowego sprawna ewakuacja osób przebywających w różnych strefach obiektu jest zapewniona dzięki komunikatom głosowym emitowanym przez 3200 głośników dźwiękowego systemu ostrzegawczego Praesideo. W normalnych warunkach system jest wykorzystywany do emitowania muzyki oraz reklam w galerii handlowej.

Fot. Archiwum Warbud

System telewizji dozorowej składa się ze 195 kamer, dwóch serwerów z zainstalowanym systemem Bosch Video Management System oraz siedmiu macierzy dyskowych o całkowitej pojemności 110 terabajtów. Wystarcza to do zapisu i archiwizacji danych wizyjnych przez ponad miesiąc, co było wymogiem administratora budynku. System kontroli dostępu obejmuje 240 czytników zabezpieczających drzwi, windy, recepcje, główne wejścia oraz bramki kontrolne.

System został zaprojektowany w taki sposób, by był maksymalnie efektywny, opłacalny i zapewniał najwyższy poziom bezpieczeństwa. Przy wsparciu firmy Bosch firma CORAL stworzyła i zainstalowała kompleksowy system zgodnie z harmonogramem, przed oficjalnym otwarciem budynku.

Bezpośr. inf. Bosch Security Systems

Anna Twardowska objęła stanowisko Nedap Country Manager Poland

Z początkiem września 2014 roku stanowisko Country Manager Poland w firmie **Nedap Security Management** objęła **Anna Twardowska**, która będzie odpowiedzialna za kierowanie polskim zespołem oraz współpracę z obecnymi dystrybutorami i partnerami handlowymi.

Anna Twardowska jest absolwentką studiów magisterskich w Politechnice Poznańskiej. Swoją wiedzę pogłębiała w kolejnych latach w ramach studiów podyplomowych oraz studiów MBA w Uniwersytecie Ekonomicznym w Poznaniu.

Doświadczenie zawodowe zdobyła w firmie Konsorcjum FEN na stanowisku Monitoring IP Business Unit Manager. W ciągu 13 lat swojej kariery zawodowej była odpowiedzialna m.in. za zarządzanie zespołem sprzedaży, stworzenie i rozwijanie sieci partnerów w Polsce oraz za sprzedaż produktów służących do budowy wizyjnych systemów dozorowych.

Bezpośr. inf. Erica Meijer
Nedap Security Management

Axis Communications z nowym koordynatorem ds. marketingu i komunikacji

Pod koniec lipca br. do zespołu **Axis Communications** dołączyła **Justyna Puławska**, która objęła stanowisko Marketing and Communication Coordinator i będzie odpowiedzialna za działania marketingowe na polskim rynku oraz współpracę z dystrybutorami i partnerami handlowymi w tym zakresie.

Justyna Puławska jest absolwentką studiów magisterskich w Wyższej Szkole Przedsiębiorczości i Zarządzania im. L. Koźmińskiego w Warszawie. Swoją wiedzę pogłębiała w kolejnych latach w ramach studiów podyplomowych oraz podczas półrocznego stażu w International Jonkoping Business School w Szwecji.

Doświadczenie zawodowe na rynku systemów zabezpieczeń zdobyła na stanowisku MarCom Managera w dziale Security Systems firmy Robert Bosch. Pracowała również w firmie Cetelem Polska Expansion oraz w Fundacji na rzecz Nauki Polskiej.

– *Cieszymy się, że udało nam się uzupełnić brakujące ogniwo w naszym zespole w Polsce* – mówi **Petr Tošner**, Regional Marketing Manager w Axis Communications. – *Właśnie otworzyliśmy biuro w Polsce i wkrótce podwoimy liczbę pracowników. Jestem przekonany, że dzięki temu będziemy w stanie zintensyfikować nasze działania, a także szybciej i lepiej spełniać oczekiwania naszych partnerów.*

Bezpośr. inf. Axis Communications

Axis Communications z nowym kierownikiem sprzedaży na terenie Polski i krajów bałtyckich

1 września 2014 r. do zespołu **Axis Communications** dołączył **Jakub Kozak**, który objął stanowisko Sales Manager Poland and Baltics i będzie odpowiedzialny za sprzedaż na rynku polskim oraz w krajach bałtyckich, a także za współpracę z dystrybutorami i partnerami handlowymi w tym zakresie.

Jakub Kozak jest absolwentem studiów magisterskich na Uniwersytecie Warszawskim oraz studiów podyplomowych w Szkole Głównej Handlowej. Jest też autorem bądź współautorem artykułów i opracowań dotyczących systemów zabezpieczeń oraz sprzętu wykorzystywanego w walce z terroryzmem.

Od kilkunastu lat jest ściśle związany z branżą zabezpieczeń. Ostatnio był odpowiedzialny za rozwój firmy Nedap w Polsce, a także za sprzedaż i promocję jej produktów służących do budowy zintegrowanych systemów zabezpieczeń.

– *Pojawienie się Jakuba w zespole Axis jest następstwem prężnego rozwoju polskiego oddziału firmy oraz wciąż rosnącego zainteresowania sieciowymi systemami wizyjnymi w tym regionie* – powiedziała **Anna Forsberg**, Regional Director Eastern Europe. – *Niewątpliwie Jakub wesprze zespół, korzystając ze swej wiedzy i doświadczenia, usprawni nasze kontakty z dystrybutorami na terenie Polski i krajów bałtyckich oraz poprawi wyniki sprzedaży* – dodała.

Bezpośr. inf. Axis Communications

AXIS COMMUNICATIONS

Jaka jest różnica między nocą a dniem?

Żadna.

Znakomite obrazy w kolorze uzyskuję również po zmroku.

To dlatego, że kamery sieciowe Axis wykorzystują technologię Lightfinder. Dzięki niej są tak światłoczułe, że zapewniają wyraźny, kolorowy obraz nawet przy bardzo słabym oświetleniu. Znacznie ułatwia to identyfikację osób, pojazdów i przedmiotów o każdej porze dnia i nocy. Jestem kierownikiem ochrony w galerii handlowej i to rozwiązanie stanowi dla mnie ogromny krok naprzód.

Więcej informacji na temat technologii Lightfinder, użyteczności obrazu i różnych rozwiązań do nadzoru można znaleźć w interaktywnym przewodniku firmy Axis dostępnym na stronie
www.axis.com/imageusability

Dahua proponuje innowacyjne rozwiązanie – HDCVI

HDCVI jest skrótem od słów High Definition Composite Video Interface i oznacza analogową technikę przesyłania obrazów telewizyjnych o wysokiej rozdzielczości. Dzięki HDCVI możliwa jest łatwa i szybka modernizacja wizyjnych systemów dozorowych bez konieczności wymiany okablowania. Zespolone sygnały wizyjne są transmitowane na duże odległości za pośrednictwem standardowych kabli koncentrycznych.

Technika HDCVI ma następujące zalety:

Łatwe przejście do rozdzielczości HD
Technika HDCVI umożliwia transmisję obrazów o rozdzielczości zgodnej ze standardem HD 1080p lub 720p z wykorzystaniem modulacji analogowej, co oznacza, że w nowym rozwiązaniu wykorzystane są dokładnie te same metody instalacji i uruchamiania wizyjnych systemów dozorowych co w konwencjonalnych systemach analogowych o standardowej rozdzielczości. Jedyna różnica polega na tym, że HDCVI umożliwia uzyskanie bogatych w szczegóły obrazów o rozdzielczości kilku megapikseli.

Transmisja obrazów na dużą odległość
Dzięki HDCVI można transmitować obrazy na znaczne odległości, wykorzystując standardowe kable koncentryczne, bez stosowania jakichkolwiek urządzeń wzmacniających. Ponadto podczas transmisji nie występują żadne dodatkowe opóźnienia ani zniekształcenia obrazu. W porównaniu z transmisją obrazów metodą HD-SDI technika HDCVI ma znacznie korzystniejsze właściwości. W przypadku HD-SDI maksymalny dystans, na jaki można było przesłać obraz, nie przekraczał 100 metrów, gdy tymczasem w przypadku HDCVI odległość ta wynosi co najmniej 500 metrów. Zastosowanie kabla koncentrycznego typu 75-3 pozwala na ograniczenie do minimum zniekształceń transmitowanego obrazu.

Brak opóźnień
Technika HDCVI jest w bardzo wysokim stopniu niezawodna, gdyż podczas transmisji wykorzystywana jest metoda P2P. Obraz jest przekazywany w czasie rzeczywistym, bez kompresji i bez dodatkowych opóźnień. Dzięki temu jego jakość jest bardzo wysoka, zaś ruch jest przekazywany w sposób płynny.

Transmitowanie trzech sygnałów jednym kablem
Dzięki temu, że jednym kablem koncentrycznym wysyłane są trzy sygnały – odpowiedzialne za fonię, wizję oraz sterowanie – okablowanie wizyjnych systemów dozorowych ulega uproszczeniu, zaś jakość przekazywanych obrazów jest bardzo wysoka. Na te zalety zwrócono uwagę już kilka miesięcy po wprowadzeniu systemów HDCVI do sprzedaży. Dzięki odpowiedniej, podkreślającej niskie koszty tego rozwiązania strategii systemy HDCVI szybko zyskały duży udział w światowym rynku wizyjnych systemów dozorowych. Jednocześnie nową techniką zainteresowali się dystrybutorzy działający na rynku zabezpieczeń elektronicznych. Pojawili się także inni producenci, jednak mimo to, dzięki intensywnym pracom konstrukcyjnym i wdrożeniowym, firma **Dahua Technology** utrzymała swoją czołową pozycję. Tworząc systemy HDCVI, firma Dahua Technology wykreowała nowy trend, który stanowi jednocześnie przełom technologiczny w dziedzinie transmisji obrazów o rozdzielczościach megapikselowych na znaczne odległości, z wykorzystaniem prostych technik instalacyjnych.

Bezpośr. inf. JoJo Li
Dahua Technology
Tłumaczenie: Redakcja

RCP Master 2.1

rejestracja czasu pracy z wykorzystaniem urządzeń mobilnych

Nowa wersja oprogramowania do rejestracji czasu pracy **RCP Master 2.1** ma wiele ulepszeń oraz rozszerzeń. Na uwagę zasługuje zwłaszcza możliwość współpracy programu z mobilnymi urządzeniami z systemem operacyjnym Android. W systemie RCP Master 2.1 funkcję rejestratora może pełnić tradycyjny rejestrator z czytnikiem zbliżeniowym, klawiaturą i wyświetlaczem (PR602LCD) lub – co jest nowością – dowolny tablet z zainstalowanym programem **RCP Point**. Pracownik może logować się tradycyjnie, za pomocą karty zbliżeniowej Mifare, lub za pośrednictwem telefonu komórkowego z funkcją NFC lub Bluetooth. Jeszcze jednym sposobem jest wykorzystanie kodu QR wydrukowanego lub wyświetlonego na ekranie urządzenia mobilnego (tablet, smartfon). Do logowania za pomocą telefonu komórkowego udostępniana jest aplikacja mobilna **Roger Mobile Key**, która wykorzystuje technologię elektronicznych kluczy generowanych przez aplikację RCP Master. Przy każdym logowaniu pracownika mobilny rejestrator może wykonać zdjęcie, co umożliwia późniejsze sprawdzenie, czy osoba posługująca się danym identyfikatorem jest do tego upoważniona. Program RCP Master 2.1 może obsługiwać 8 rejestratorów podłączonych za pomocą Wi-Fi. Zdarzenia zarejestrowane przez mobilne rejestratory mogą być wyświetlane w czasie rzeczywistym na ekranie komputera i mogą stanowić źródło informacji dotyczących obecności i przemieszczania się osób w firmie. Firma Roger oferuje także fabrycznie skonfigurowany tablet przeznaczony do zawieszenia na ścianie (EGTP-1), który można wykorzystać jako rejestrator stacjonarny.

Bezpośr. inf. ROGER
Opracowanie: Redakcja

Security Products SINCE 1991 roger

RACS 4.5

System Kontroli Dostępu

- kontynuacja popularnego systemu RACS 4
- nowa centrala systemu z wbudowanym interfejsem TCP/IP
- bezpieczna komunikacja szyfrowana AES 128 CBC
- współpraca z czytnikiem linii papilarnych RFT1000 (ROGER)
- obsługa zamków mechatronicznych systemu SALLIS (SALTO)
- obsługa zamków bezprzewodowych systemu APERIO (ASSA ABLOY)
- integracja z centralami alarmowymi serii INTEGRA (SATEL)
- integracje CCTV: HIKVISION, DAHUA, GEOVISION

www.roger.pl

Rozszerzono funkcjonalność systemu RACS 4 o możliwość integracji z zamkami bezprzewodowymi APERIO firmy ASSA ABLOY

- obsługa do 16 zamków APERIO oraz do 32 kontrolerów dostępu serii PR (ROGER) w ramach pojedynczej centrali CPR32-NET
- konfiguracja praw dostępu z poziomu oprogramowania zarządzającego PR Master
- bezpłatna obsługa do 2 zamków

Wysoka niezawodność i funkcjonalność potwierdzona w tysiącach wdrożonych z sukcesem instalacji w Polsce i za granicą.

roger®

Gazociąg Gasunie skutecznie chroniony przez system nadzoru wizyjnego GeViScope firmy Geutebrück

Firma **Gasunie** zarządza największym wysokociśnieniowym gazociągiem w północno-zachodniej Europie. Sieć przesyłowa o długości ponad 15000 kilometrów zaopatruje w gaz ziemny Holandię oraz północną część Niemiec. Wzdłuż gazociągu zlokalizowanych jest około 1300 stacji odbiorczych. Kluczowym zadaniem systemu bezpieczeństwa jest ochrona obwodowa, wykrywanie intruzów oraz kontrola dostępu. Praca całego systemu, w którym wykorzystywane są urządzenia i oprogramowanie firmy Geutebrück, jest koordynowana przez centrum ochrony w Groningen w północnej Holandii.

Używany obecnie system dozoru wizyjnego w pełni bazuje na rozwiązaniach IP i wykorzystuje nowoczesną platformę bezpieczeństwa **GeViScope**. Zastosowanie kamer o wysokiej rozdzielczości umożliwiło znaczącą redukcję ich liczby oraz wyraźną poprawę jakości i użyteczności obrazu. – *Podstawową zasadą, jaką kierujemy się podczas instalacji systemów zabezpieczeń, jest umożliwienie jak najszybszej identyfikacji intruzów, najlepiej już na obrzeżach strzeżonego obiektu* – wyjaśnia **Reiner Woldring**, doradca ds. bezpieczeństwa w firmie Gasunie. System zabezpieczeń działa przez 24 godziny na dobę i jest koordynowany przez centrum w Groningen. Transmisja danych z odległych miejsc zawsze była dużym wyzwaniem. – *Ograniczona przepustowość łącza pomiędzy centralą a niektórymi stacjami pozwala przekonać się o efektywnym wykorzystaniu dostępnego pasma sieciowego* – twierdzi **Koen Pelle**, dyrektor krajowy Geutebrück w Holandii. W przypadku wystąpienia awarii w Groningen wszystkie zadania może natychmiastowo przejąć drugie centrum, które jest zlokalizowane w utajonym miejscu na terenie kraju.

System dozoru wizyjnego jest w pełni zintegrowany z systemem kontroli dostępu. W niektórych lokalizacjach weryfikacja tożsamości użytkowników przeprowadzana jest zdalnie, z centrum kontroli, co wymaga zastosowania kamer. Pracownicy ochrony mogą sprawdzić, czy wizerunek na karcie dostępu odpowiada osobie, która się nią posługuje.

System firmy **Geutebrück** skutecznie chroni wszystkie odległe lokalizacje gazociągu Gasunie. – *Nie musimy już prowadzić ciągłej analizy zarejestrowanego materiału wizyjnego* – powiedział Reiner Woldring. – *Postawiliśmy na sprawdzoną metodę dozoru wizyjnego, cyfrowy przesył danych, kamery o wysokiej jakości, możliwość zapisu i archiwizacji obrazów oraz intuicyjną obsługę systemu. W przypadku wtargnięcia niepowołanej osoby na teren obiektu po prostu powiadamiamy policję lub ochronę.*

Dystrybutorem produktów Geutebrück w Polsce jest firma **Arpol**.

Bezpośr. inf. Arpol
tel.: 61 84 62 100
e-mail: cctv@arpol.pl
www.arpol.pl

Wideodomofon w smartfonie

Nowoczesne urządzenia stają się nieodłącznym elementem naszej codzienności. Coraz częściej nowe technologie przekraczają próg naszego domu. Dobrze dobrane i odpowiednio skonfigurowane urządzenia mogą pozytywnie wpłynąć na nasze życie, zwiększając jego komfort i podwyższając poziom bezpieczeństwa.

Mając na uwadze te tendencje, firma **VIDOS** wprowadziła na rynek nowoczesny produkt, który zupełnie zmienia znaczenie słowa „wideodomofon". Chodzi o **moduł MS02**, w którym wykorzystana jest bramka IP umożliwiająca przekierowanie rozmowy z analogowego wideodomofonu marki VIDOS lub Competition do dowolnego urządzenia mobilnego z systemem operacyjnym Android lub iOS.

Moduł MS02 umożliwia prowadzenie rozmowy, obserwację obrazu w czasie rzeczywistym i otwieranie furtki za pomocą smartfonu w dowolnym miejscu na świecie, w którym jest dostęp do Internetu. Po telefonicznym nawiązaniu połączenia bramka IP automatycznie zapisuje dwudziestosekundowe nagranie obrazu i dźwięku. Możliwe jest też rejestrowanie zdjęć podczas połączenia. Bramka IP współpracuje z analogowym wideodomofonem i nie wymaga specjalnego okablowania. Można ją podłączyć do już istniejącego systemu bez konieczności jego przebudowy. Wystarczy podłączyć bramkę IP do domowego routera i wideodomofonu.

Użytkownik MS02 nie ponosi żadnych dodatkowych kosztów związanych z jego użytkowaniem. Wszystkie połączenia za pomocą wideodomofonu realizowane są za pośrednictwem sieci.

Producent udostępnia darmową aplikację COM viewer dla każdego użytkownika AppStore i PlayStore. By skorzystać z aplikacji, należy założyć darmowe konto na serwerze producenta.

Prosta czterostopniowa instalacja umożliwia samodzielne podłączenie i skonfigurowanie sprzętu. Użytkowników bramki IP nie dotyczy problem zmiennych adresów IP. Moduł ma stały, unikatowy adres MAC, który jest wykorzystywany do komunikowania się z serwerem.

VIDOS udowadnia, że wideodomofon – nawet w smartfonie – nie jest zbędnym luksusem. Wideodomofon sieciowy powinien być prosty w konfiguracji i intuicyjny w obsłudze. Bramka IP spełnia te kryteria.

Więcej informacji można znaleźć na stronie *www.vidos.com.pl*

Vidos
friendly technology

Bezpośr. inf. VIDOS

Obrazy ze skanerów X-ray w rozszerzonej serii rejestratorów G-Scope firmy Geutebrück

Nowe, kompaktowe rejestratory sieciowe firmy **Geutebrück** z serii **G-Scope** (modele 1106 oraz 1206) umożliwiają zapis sygnału RGB ze skanerów X-ray z wykorzystaniem jednego lub dwóch wejść VGA/DVI-I. Dla wejść RGB system zapewnia maksymalną rozdzielczość obrazu równą 2048x1536 pikseli. Rejestrator ma sześć kanałów wejściowych, a kupując odpowiednie licencje, można przystosować go do współpracy z czterema lub pięcioma kamerami różnych producentów. Interfejs TACI, port szeregowy oraz osiem wejść alarmowych i cztery wyjścia przekaźnikowe umożliwiają dalszą integrację rejestratora z systemami zewnętrznymi. Dzięki temu możliwe jest szybkie i efektywne wdrożenie zaawansowanego, zintegrowanego systemu dozoru wizyjnego. Rejestratory obsługują kamery i kodery IP współpracujące z kodekami H264CCTV, H.264 oraz M-JPEG.

Aktualna lista kompatybilnych produktów jest dostępna na stronach producenta. W systemie można zdefiniować zdarzenia alarmowe, stworzyć rozbudowane harmonogramy czasowe, umiejscowić okna podglądu na wielu monitorach, uruchomić funkcje eksportu i automatycznej archiwizacji obrazów. Możliwe jest uruchomienie algorytmów podstawowej i zaawansowanej (licencjonowanej) detekcji aktywności dla wszystkich obsługiwanych kanałów wizyjnych. Przeglądając i filtrując listę zdarzeń alarmowych, można szybko i wygodnie wyszukiwać wybrane fragmenty nagrań.

Omawiane modele rejestratorów stanowią rozszerzenie wprowadzonej w ubiegłym roku serii urządzeń kompaktowych G-Scope. Urządzenia te wykorzystują sprawdzoną, niezawodną i wypróbowaną technologię przetwarzania obrazu i zarządzania nim, która jest znana z innych produktów firmy Geutebrück wchodzących w skład platformy GeViScope oraz rejestratorów re_porter i net_porter. Wszystkie rejestratory są w pełni kompatybilne z oprogramowaniem zarządzającym GeViSoft oraz oprogramowaniem stacji podglądu – GSCView oraz G-SIM.

Dystrybutorem produktów Geutebrück w Polsce jest firma **Arpol**.

Bezpośr. inf. Arpol
tel.: 61 84 62 100,
e-mail: cctv@arpol.pl
www.arpol.pl

W rankingu IHS 2014 Dahua zajmuje drugie miejsce na światowym rynku wizyjnych systemów dozorowych

Dahua Technology z siedzibą w Hangzhou, światowy lider w dziedzinach produkcji i dystrybucji urządzeń służących do budowy wizyjnych systemów dozorowych, z dumą zawiadamia, że zgodnie z tegorocznymi wynikami rankingu IHS firma zajmuje obecnie drugie miejsce na rynku systemów dozorowych i czwarte miejsce na globalnym rynku kamer sieciowych, zaś jej rejestratory DVR zajmują w tym rankingu coraz wyższe miejsca.

W porównaniu z wynikami rankingu IHS ogłoszonymi w roku 2013 firma Dahua Technology zrobiła duży krok naprzód, przesuwając się z miejsca szóstego na drugie, i obecnie zajmuje 5,6% światowego rynku wizyjnych systemów dozorowych, obok takich firm jak Axis, Samsung czy Bosch. **Fu Liquan**, prezes firmy Dahua Technology, spytany o przyczyny tak gwałtownego skoku, wyjaśnił, że stało się to możliwe dzięki intensywnej pracy w dziale konstrukcyjnym oraz dzięki dobrej polityce marketingowej.

Każdego roku firma Dahua Technology inwestuje ponad 10% zysków z bieżącej sprzedaży w prace prowadzone w dziale konstrukcyjnym, dzięki czemu opracowywane są innowacyjne produkty o wysokiej jakości i bardzo dobrych parametrach użytkowych. Jako jeden z czołowych graczy w branży firma Dahua Technology stworzyła światową sieć sprzedaży swoich produktów. Zadbała również o serwis i marketing. Jej produkty znalazły liczne zastosowania w wielu krajach. Zostały wykorzystane do budowy wizyjnych systemów dozorowych w takich obiektach jak elektrownia wodna Three Gorges, siedziba Six-Country Summit, stadiony olimpijskie, tereny Shanghai World Expo, Kreml, londyńskie metro i wiele innych.

Początkowo firma Dahua Technology produkowała wizyjne karty przechwytujące i rejestratory DVR, co stanowiło podstawę jej egzystencji. Obecnie asortyment oferowanych przez nią produktów jest bogaty, obejmuje zarówno sprzęt, jak i oprogramowanie i należą do niego kamery, urządzenia transmitujące, rejestrujące i wyświetlające obrazy telewizyjne, urządzenia sterujące, inteligentne urządzenia wykorzystywane do sterowania ruchem ulicznym, a także urządzenia do zastosowań domowych.

Zgodnie z wynikami rankingu IHS firma Dahua Technology zajęła w tym roku czwarte miejsce na światowym rynku w kategorii kamer IP. Ta linia produktów będzie rozwijana ze szczególnym naciskiem na tworzenie nowych produktów, m.in. urządzeń o rozdzielczości 4k, kamer o szerokim polu widzenia oraz kamer o bardzo wysokiej czułości. Ponadto intensywnie rozwijana będzie linia produktów Dahua HDCVI.

– Działamy na rynku wizyjnych systemów dozorowych od ponad 20 lat. W tym czasie nastąpił znaczny rozwój tej gałęzi przemysłu i my także mieliśmy w tym swój udział – informuje **Fu Liquan**. *– W najbliższych latach, a dokładnie do roku 2016, dzięki ciągłemu rozwojowi naszych produktów oraz otwarciu się na zamorskie rynki, zyski firmy Dahua Technology powinny osiągnąć wartość 1,6 miliarda USD. Będziemy kontynuować prace konstrukcyjne, dążąc do tworzenia innowacyjnych rozwiązań technologicznych. Będziemy nie tylko nadążać za obowiązującymi trendami, lecz także sami wytyczać linie rozwoju tej gałęzi przemysłu.*

Bezpośr. inf. JoJo Li
Dahua Technology
Tłumaczenie: Redakcja

Data Center For Business Symposium – relacja

W dniach 25–26 czerwca 2014 r. w Hotelu Windsor w Jachrance odbyło się pierwsze spotkanie z cyklu **Data Center For Business Symposium**.

Na sympozjum goście mogli zdobyć wiedzę dotyczącą centrów przetwarzania danych, możliwości ich wykorzystania oraz najnowszych trendów i wymagań. Rozmawiano o biznesie, technologiach, bezpieczeństwie i ekologii.

– Serdecznie dziękuję za udział w Data Center For Business Symposium wszystkim uczestnikom oraz partnerom, dzięki którym zaprezentowaliśmy szerokie spektrum rozwiązań i możliwości realizacji projektów DC. Jako główny partner merytoryczny przedstawiliśmy specyfikę realizacji projektów DC w szerszym ujęciu. Partnerzy uzupełnili przekaz szczegółowymi informacjami dotyczącymi produktów i technologii, a także mówili o doświadczeniu, jakie zdobyli podczas tworzenia tego typu obiektów na całym świecie. Dzięki temu goście mogli dowiedzieć się, jakie rozwiązania są dostępne, na co przede wszystkim należy zwrócić uwagę, jakie są możliwe błędy oraz dobre praktyki podczas planowania i realizacji inwestycji – powiedział Michał Piechulek, dyrektor Biura Projektów BKT Elektronik.

Merytoryczną część spotkania wzbogaciły panele eksperckie. Lilia Severina z Uptime Institute mówiła o certyfikacji. Na temat bezpieczeństwa transmisji danych wypowiedział się Walter Affeltranger, członek komitetów normalizacyjnych ISO/IEC SC 48 oraz CENELEC TK 215. Zagadnienia dotyczące finansowania projektów centrów przetwarzania danych z Funduszy Europejskich omówiła Justyna Wieprzkowicz z Centralnego Punktu Informacyjnego Funduszy Europejskich. Robert Berliński, promujący właściwe testowanie infrastruktury krytycznej centrów przetwarzania danych, mówił

o tzw. Green IT. Poruszone tematy zachęciły uczestników do dyskusji, które kontynuowano w sali biznesowej.

Formuła spotkania, łączącego panele merytoryczne z równolegle trwającymi rozmowami biznesowymi, spełniła oczekiwania zarówno partnerów, jak i uczestników spotkania. Goście wymienili się swoimi spostrzeżeniami dotyczącymi etapu planowania inwestycji, tworzenia centrów przetwarzania danych i ich użytkowania.

Szczegółowe informacje dotyczące partnerów, prelegentów oraz programu Data Center For Business Symposium znajdują się na stronie *www.dc4business.pl*.

Informacja o BKT Elektronik

BKT Elektronik jest czołowym dostawcą technologii wykorzystywanych w budowie regionalnych i ponadregionalnych sieci szerokopasmowych w Polsce oraz innowacyjnych technologii przeznaczonych dla centrów przetwarzania danych. BKT Elektronik jest polską firmą produkcyjno-handlową, działającą w branży IT, elektrotechniki i automatyki nieprzerwanie od 1998 roku.

Oferta firmy obejmuje dostawy kompletnych systemów okablowania strukturalnego, komponentów do budowy sieci LAN/WAN, szaf i obudów teleinformatycznych i telekomunikacyjnych, różnego rodzaju okablowania optycznego i miedzianego. Dynamika wzrostu obrotów w ostatnich latach stawia BKT Elektronik w szeregu firm o mocnej i ugruntowanej pozycji w sektorze IT w Polsce i Europie. Więcej informacji można znaleźć na stronie *www.bkte.pl*.

Bezpośr. inf. Magdalena Skórkiewicz-Foltyn
Lockus
Fot. Locus
Opracowanie: Redakcja

Nowe otwarte standardy w systemach kontroli dostępu

Pavel Dolezal

Branża kontroli dostępu skłania się ku otwartym standardom, które są zgodne z wieloma produktami dysponującymi ulepszonymi funkcjami i podnoszącymi poziom bezpieczeństwa. Dzięki otwartym standardom modernizacja istniejących rozwiązań jest łatwa, można wykorzystać nowe technologie i aplikacje, a koszty inwestycji zwracają się. Do ostatnio ustanowionych standardów należą protokoły Open Supervised Device Protocol (OSDP) oraz Secure Channel Protocol (SCP), które przynoszą znaczne korzyści. Zapewniają one dwukierunkową komunikację pomiędzy czytnikami i kontrolerami lub innymi elementami systemów zarządzania bezpieczeństwem oraz umożliwiają jej szyfrowanie. Tak zintegrowane urządzenia mogą obsługiwać zaawansowane aplikacje wykorzystujące szyfrowanie danych podczas transmisji między komponentami. Komunikacja dwukierunkowa jest szczególnie korzystna, gdyż umożliwia użytkownikom komunikację z czytnikami i zmianę ich konfiguracji z poziomu systemu centralnego, co zmniejsza koszty eksploatacji przez uproszczenie czynności związanych z konfiguracją i usprawnienie serwisowania czytników.

W przeciwieństwie do wcześniej stosowanych protokołów jednokierunkowych, obsługujących interfejs Wiegand dla czytników RFID oraz interfejs typu clock-and-data używany w czytnikach kart z paskiem magnetycznych, protokół OSDP zapewnia stałe monitorowanie stanu czytnika. Błędy odczytu, uszkodzenia czytników oraz akty sabotażu są natychmiast sygnalizowane. Wszystkie sygnały są transmitowane poprzez dwuprzewodową linię ze wspólnym uziemieniem, co obniża koszty instalacji w porównaniu z interfejsem Wiegand. Do zasilania czytnika oraz wysyłania i odbioru danych można użyć

Fot. 2. Nowa platforma iClass

kabli czterożyłowych (wcześniej konieczne było użycie kabli sześciożyłowych).

Ogłaszając w listopadzie 2011 r. projekt utworzenia standardu OSDP, prezes ds. standardów SIA, Steve Van Till, powiedział: „Uważamy, że istnieje wyraźne zapotrzebowanie na tego typu rozwiązanie. Obecnie brakuje standardowego protokołu umożliwiającego łączenie czytników z innymi elementami systemów fizycznej kontroli dostępu, innego niż protokół Wiegand, który nie pozwala na realizację zaawansowanych operacji, które są potrzebne w przypadku infrastruktury klucza publicznego (PKI)". Zgodnie z tą opinią oczekuje się, że protokół OSDP z SCP zastąpi interfejs Wiegand w wielu zastosowaniach wymagających transmisji dużej ilości danych, komunikacji dwukierunkowej lub szyfrowania, m.in. w trakcie wdrożeń kart inteligentnych, w federalnych

Fot. 1. Nowa linia produktowa czytników i kart iClass

Fot. 3. Pavel Dolezal, Area Sales Manager, HID Global Physical Access

systemach z infrastrukturą klucza publicznego (PKI) oraz w aplikacjach do zarządzania tożsamością. Dzięki zastosowaniu protokołów SCP i OSDP uwierzytelnianie transmitowanych danych jest bardziej wiarygodne, a komunikowanie się urządzeń bezpieczne i poufne. Protokół SCP był używany przez wiele lat i rozwijany przez GlobalPlatform – organ normalizacyjny działający w różnych branżach w zakresie identyfikacji, rozwoju i publikowania specyfikacji, wspomagający wdrażanie rozwiązań związanych z bezpieczeństwem i interoperacyjnością oraz zarządzanie wieloma wbudowanymi aplikacjami wykorzystującymi technologię Secure Chip. Podczas tworzenia połączeń z wykorzystaniem protokołu SCP następuje wzajemne uwierzytelnianie klienta i serwera, zaś dla każdej sesji ustanawiane są oddzielne zestawy kluczy szyfrujących. W przypadku wykrycia błędu protokół SCP powoduje zamknięcie bezpiecznego kanału transmisji danych, a klucze wykorzystywane w danej sesji są niszczone.

Firma HID Global miała znaczny wkład w specyfikację OSDP i jako pierwsza umożliwiła obsługiwanie protokołów OSDP i SCP przez oferowane przez nią czytniki iCLASS SE. Dzięki temu możliwa jest centralizacja obsługi systemów, która przyspiesza i ułatwia czynności związane z ich konfiguracją i serwisowaniem, a także obniżenie kosztów operacyjnych. Obsługa protokołów OSDP i SCP przez czytniki iCLASS SE podwyższa poziom bezpieczeństwa systemu, ponieważ każde z urządzeń wykorzystuje bezpieczny kanał transmisji danych i ryzyko sabotażu zostaje znacznie zmniejszone. Do instalacji czytników iCLASS SE można wykorzystać kable dwużyłowe (oprócz zasilania, które wymaga również dwóch żył) zamiast pięcio- lub sześciożyłowych i dzięki temu zaoszczędzić. W tym przypadku dwukierunkowe przesyłanie danych oraz sterowanie sygnalizatorami (akustycznym i wizualnym LED) odbywa się za pomocą tej jednej pary.

Protokół OSDP i SCP, a także inne standardy branżowe będą nadal odgrywać ważną rolę w systemach kontroli dostępu, podwyższając poziom bezpieczeństwa i stwarzając nowe możliwości, a koszty poniesione przez użytkowników zwrócą się z nawiązką dzięki adaptowalnym rozwiązaniom, które ewoluują wraz z rozwojem firmy.

Pavel Dolezal
Area Sales Manager, HID Global Physical Access

iCLASS SE®
Najnowocześniejsza platforma kontroli dostępu

Technologia przyszłości zapewniająca bezpieczeństwo danych identyfikacyjnych do szerokiego zakresu zastosowań (od kontroli dostępu po zabezpieczenie danych). Ewolucja w kwestiach bezpieczeństwa, użyteczności i wydajności.

Technologia HID i niezależna od nośnika platforma iCLASS SE®, przygotowana do zastosowań mobilnych, stanowią rozwiązanie bezpiecznej identyfikacji dla kontroli dostępu fizycznego oraz największego asortymentu aplikacji i środowisk. W celu osiągnięcia maksymalnej interoperacyjności platforma iCLASS SE wspiera najwięcej technologii kart dostępu, umożliwiając efektywne kosztowo i bezproblemowe unowocześnienie systemu i zwiększenie poziomu bezpieczeństwa oraz wydajności. Platforma iCLASS SE jest przystosowana do obsługi technologii przyszłości, w tym dostępu za pomocą urządzeń mobilnych w technologii NFC, zapewniając wygodny dostęp oraz bezprecedensowy poziom bezpieczeństwa.

Aby dowiedzieć się więcej, odwiedź witrynę hidglobal.com/iclass-se-platform-zab

Bezprzewodowe systemy kontroli dostępu Aperio

Zastosowanie okuć mechatronicznych ASSA ABLOY w nowej lub istniejącej infrastrukturze zabezpieczeń

Kamil Targalski

Nowoczesne systemy kontroli dostępu zapewniają bezpieczeństwo użytkownikom obiektu, a także zwiększają zakres możliwości jego administratora. Większość obiektów rządowych, biurowych oraz handlowych jest zabezpieczona elektronicznie, jednak tylko w pewnym stopniu. Najczęściej kontrolą dostępu są objęte tylko najbardziej zagrożone strefy. Pozostałe przejścia są zabezpieczane zamkami mechanicznymi lub autonomicznymi czytnikami, które nie są sieciowo połączone z bazowym systemem. Ograniczenia skali systemów wynikają przede wszystkim z wysokich kosztów skomplikowanej instalacji lub jej pominięcia na etapie projektu. Jak w łatwy sposób zabezpieczyć budynek i rozbudować system kontroli dostępu? Jak usprawnić wymianę zamków na mechaniczny klucz na systemy, w których wykorzystuje się karty zbliżeniowe RFID? Jakich zabezpieczeń elektronicznych można użyć w przypadku szklanych drzwi?

Najprostszym i najbardziej tradycyjnym sposobem objęcia dodatkowych drzwi kontrolą dostępu jest dołączenie ich do istniejącego systemu poprzez montaż zamka elektrycznego (lub innego elementu wykonawczego tego typu) oraz czytnika kart zbliżeniowych, a następnie połączenie tych elementów ze sterownikiem drzwiowym. Konieczne jest również doprowadzenie zasilania. Trzeba w związku z tym przeprowadzić dodatkowe kable, co jest kłopotliwe, czasochłonne i drogie. Estetyczny montaż elektrozaczepu czy zamka elektrycznego jest skomplikowany – instalator musi wykazać się doświadczeniem i wysoką kulturą pracy. Dodatkowe koszty są związane także z pracami remontowymi – z naprawą i malowaniem ścian uszkodzonych podczas tego typu instalacji. Tradycyjne rozwiązanie nie do końca sprawdza się również w przypadku drzwi szklanych, które często montuje się w obiektach biurowych.

Mniej kłopotliwą metodą zastępowania zamków mechanicznych urządzeniami elektronicznymi jest instalacja lokalnego systemu kontroli dostępu pracującego w trybie autonomicznym. Rozwiązanie to wymaga jednak niezależnego zarządzania. Instalacja zawierająca zarówno urządzenia pracujące w trybie sieciowym, jak i urządzenia autonomiczne jest niewygodna w zarządzaniu i użytkowaniu.

Funkcje i zalety platformy radiowej

Nowoczesną alternatywą dla przedstawionych wyżej rozwiązań jest bezprzewodowa platforma zamków mechatronicznych Aperio oferowana przez ASSA ABLOY. Drzwi, które nie zostały wcześniej uwzględnione w planach systemu kontroli dostępu, mogą zostać do niego w łatwy sposób dodane dzięki wyposażeniu ich w elektroniczne okucia, cylindry lub zamki elektroniczne komunikujące się ze sterownikami drzwiowymi za pośrednictwem anten radiowych. Gdy użytkownik budynku chce otworzyć drzwi zabezpieczone urządzeniem Aperio, cylinder, okucie lub zamek przesyła dane zawarte na jego karcie zbliżeniowej zaszyfrowanym sygnałem do pobliskiego odbiornika radiowego. Następnie odbiornik kontaktuje się z systemem kontroli dostępu w celu sprawdzenia, czy dany użytkownik jest upoważniony do wejścia. Dzięki temu osoby zarządzające obiektami mają do czynienia z jednym integralnym systemem bezpieczeństwa i są w stanie zmieniać uprawnienia dostępowe online, w czasie rzeczywistym. Zasięg w przypadku tego typu transmisji mieści się w przedziale od 5 do 30 metrów, w zależności od typu zastosowanej anteny. Łączność odbywa się w paśmie 2,4 GHz, w standardzie IEEE 802.15.4. Wszystkie dane są szyfrowane z wykorzystaniem algorytmu AES (128 bitów). Anteny mogą komunikować się z systemem kontroli dostępu za pomocą jednego z trzech wykorzystywanych przez ASSA ABLOY protokołów: Wiegand, RS485 lub TCP/IP. Liczba urządzeń połączonych bezprzewodowo z jedną anteną wynosi od jednego do ośmiu – w zależności od stosowanego modelu.

Szeroka gama urządzeń oraz dostępnych technologii RFID

Wykorzystanie komunikacji radiowej do rozbudowy istniejącego systemu umożliwia kontrolę wybranych przejść w obiekcie za pomocą stosowanego dotychczas oprogramowania. Administrator budynku może więc monitorować jeden integralny system bezpieczeństwa, który obejmuje wszystkie przejścia obsługiwane kartami zbliżeniowymi. Co ważne, technologia bezprzewodowa umożliwia rozszerzenie systemu bez modyfikacji stolarki drzwiowej. Dzięki temu instalacja jest mniej kłopotliwa i tańsza niż alternatywne rozwiązania. Zużycie energii oraz koszty utrzymania również są niższe niż w przypadku wykorzystania tradycyjnych rozwiązań bazujących na zastosowaniu pełnego okablowania.

Okucia, cylindry oraz zamki są zasilane bateriami litowymi CR2, CR123A lub AA FR6 – w zależności od typu urządzenia. Instalację można wykonać na niemal wszystkich

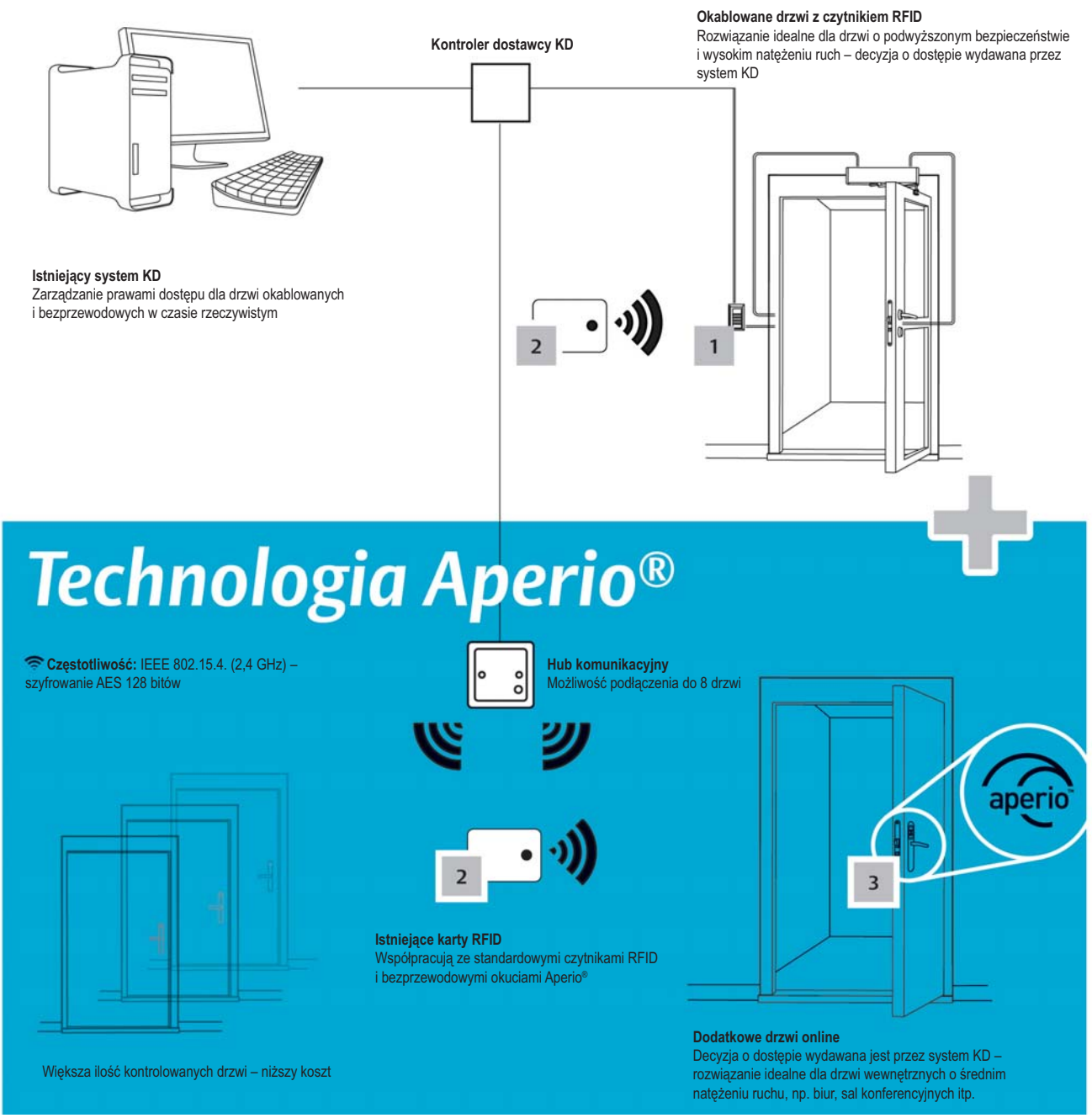
rodzajach drzwi. Do dyspozycji są trzy rodzaje elementów wykonawczych:

– czytnik kart zbliżeniowych zintegrowany z podłużnym szyldem klamkowym, opcjonalnie w wersji z klawiaturą PIN;
– czytnik kart zbliżeniowych zintegrowany z wkładką cylindryczną;
– czytnik kart zbliżeniowych zintegrowany z zamkiem elektromechanicznym, w którym wykorzystano elementy zamków elektrycznych serii EL460/560 marki Abloy.

ASSA ABLOY, przodująca firma na rynku zabezpieczeń mechanicznych, przykłada dużą wagę do bezpieczeństwa oraz norm związanych z ewakuacją. Wszystkie urządzenia wykonawcze Aperio są przystosowane do obsługi przejść z kontrolą jednostronną. Platforma gwarantuje możliwość wyjścia z pomieszczenia w dowolnym momencie – trzeba użyć klamki (norma EN179) lub dźwigni ewakuacyjnej (norma EN1125 dot. zamków elektromechanicznych).

W sytuacjach awaryjnych szyldy klamkowe oraz zamki można bezpiecznie otworzyć kluczem mechanicznym. Zastosowane są zabezpieczenia na wypadek utraty łączności odbiornika z kontrolerem lub uszkodzenia kontrolera. Do pamięci każdego urządzenia Aperio możemy wprowadzić dziesięć kart lub kodów bezpieczeństwa PIN, które są akceptowane przez urządzenie niezależnie od stanu komunikacji ze sterownikiem. Moduł elektroniczny oraz śruby mocujące znajdują się po wewnętrznej, bezpiecznej stronie szyldu, uniemożliwiając nieautoryzowane otwarcie drzwi poprzez demontaż czytnika lub całego zamka.

Duży wybór modeli czytników kart zapewnia kompatybilność z istniejącymi kartami zbliżeniowymi – nie trzeba ich wymieniać ani wprowadzać dodatkowego nośnika dla pracowników obiektu. Platforma Aperio wykorzystuje przodujące technologie zbliżeniowe, takie jak iCLASS SE, Seos, MIFARE, MIFARE DESFire, a także technologie



Rys. 1. Architektura systemu kontroli dostępu wykorzystującego technologię Aperio

Fot. 1. Bezprzewodowy zamek elektromechaniczny Aperio L100

wykorzystujące niskie częstotliwości (125 kHz HID PROX/ EM410x).

Otwarta architektura systemu

Platforma Aperio zapewnia klientom dodatkowe korzyści. Bazując na otwartym oprogramowaniu typu SDK (Software Development Kit) umożliwia elektroniczną kontrolę stanu drzwi dotychczas zabezpieczonych zamkami mechanicznymi. To rozwiązanie jest dostępne na całym świecie – dostawcy i integratorzy systemów są w stanie realizować międzynarodowe lub międzykontynentalne projekty. Bezpłatne zestawy do testów umożliwiają łatwe oraz sprawne dodanie produktów Aperio do swojej oferty przez dostawców systemów kontroli dostępu. Producenci urządzeń mogą zintegrować protokół komunikacyjny ASSA ABLOY z własnym oprogramowaniem oraz przetestować platformę radiową w realnych warunkach pracy. Jeżeli firmy decydują się na współpracę z nami, oferujemy specjalne szkolenia, materiały marketingowe oraz długoterminowe relacje partnerskie. Zapewnimy wszelkie informacje na temat korzyści płynących z programu partnerskiego wszystkim zainteresowanym producentom oraz integratorom systemów kontroli dostępu. Aktualnie ponad 90 globalnych producentów produktów służących do kontroli dostępu wykorzystuje platformę Aperio. Lista integratorów oferujących to rozwiązanie na rynku polskim jest dostępna na stronie internetowej *www.assaabloy.com.pl/aperio.*

Kamil Targalski
Electronic Access Control Product Manager

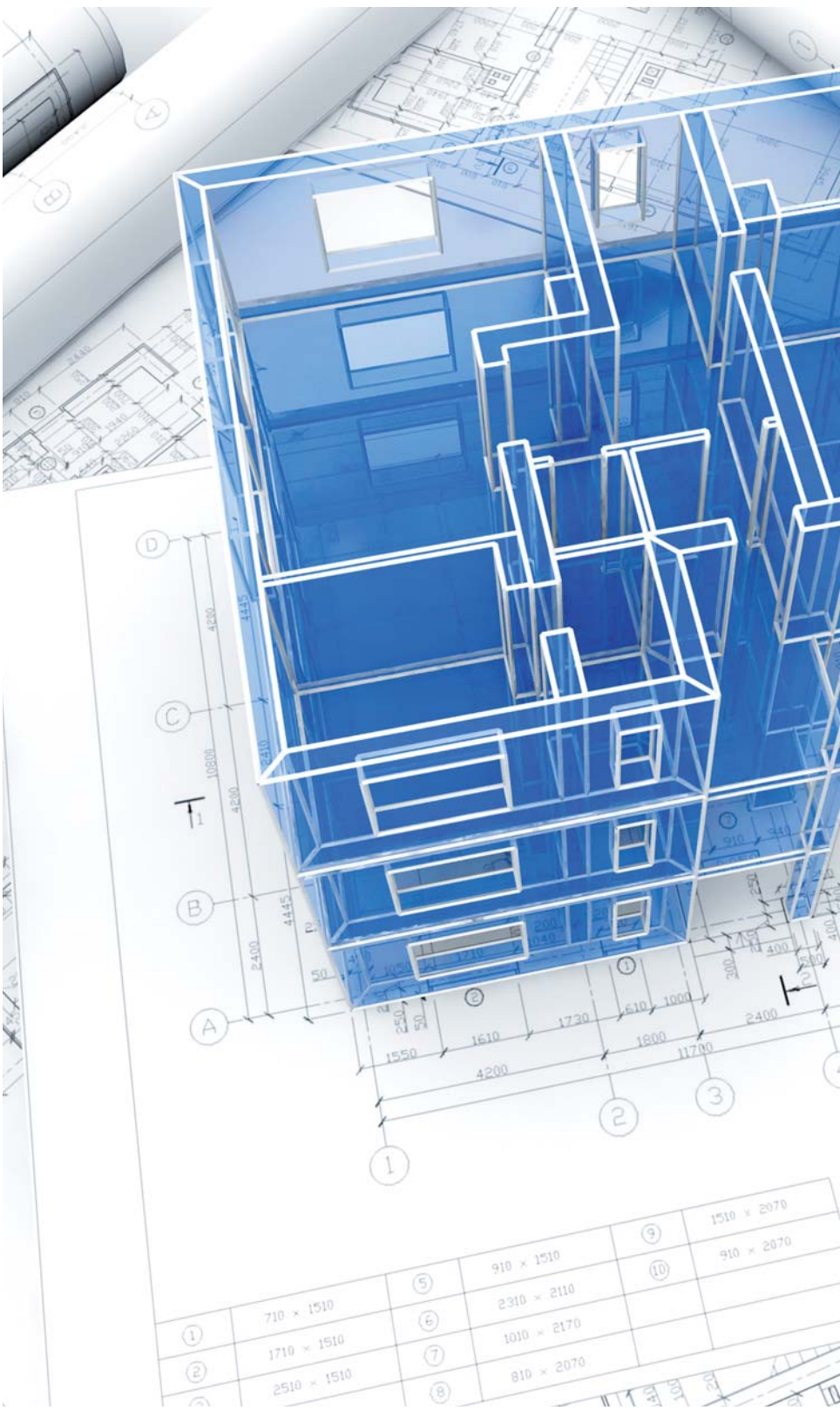
ASSA ABLOY Polska
www.assaabloy.com.pl

AC2000 Lite

Przyszłościowy, ekonomiczny system kontroli dostępu

CEM Systems

CEM AC2000 Lite jest przyszłościowym, ekonomicznym systemem kontroli dostępu przeznaczonym do pracy w instalacjach, w których liczba kontrolowanych przejść nie przekracza 128. Jego podstawowe właściwości użytkowe są zbliżone do właściwości znanego i cenionego na całym świecie systemu AC2000. Jego zastosowanie jest doskonałym rozwiązaniem w przypadku małych i średnich systemów kontroli dostępu, w których wymagane jest zachowanie wysokiego poziomu bezpieczeństwa



System AC2000 Lite zawiera pełny zestaw aplikacji dostępnych w wersji AC2000, spełnia wysokie wymagania dotyczące bezpieczeństwa i może wykonywać skomplikowane zadania. Na przykład aplikacja AC2000 Alarm Event Display (AED) umożliwia tworzenie wizualnych i tekstowych reprezentacji alarmów i innych wydarzeń zachodzących w systemie, a także wyświetlanie ich na specjalnie przygotowanych mapach, co pozwala operatorom systemu na stałą kontrolę nad sytuacją panującą w obiekcie. Aplikacja AC2000 AED nie tylko dostarcza informacje statusowe na temat stanu kontrolowanych przejść, ale także stanowi platformę, dzięki której inne zintegrowane systemy zabezpieczające, takie jak wizyjny system dozorowy czy system sygnalizacji włamania i napadu, uzyskują dodatkowe informacje na temat wydarzeń zachodzących na terenie chronionego obiektu.

System AC2000 Lite jest dostępny w wersji serwerowej lub wirtualnej. Pakiet AC2000 Lite Software Only Virtual Kit nie wymaga stosowania oddzielnego serwera, tak jak wersja AC2000 Lite, dzięki czemu małe systemy kontroli dostępu mogą być budowane bez konieczności angażowania dużych środków finansowych. Virtual Kit umożliwia także łatwą i szybką instalację oprogramowania klienta AC2000 Lite.

W systemie AC2000 Lite mogą być wykorzystane wszystkie urządzenia składowe należące do przemysłowej serii CEM, w skład której wchodzą inteligentne czytniki kart, rozwiązania mobilne, biometryczne, wsparcie dla technologii PoE+ i wiele innych.

System AC2000 Lite został zastosowany w wielu obiektach na całym świecie, m.in. w centrach akademickich, obiektach handlowych, szpitalach, bankach i siedzibach wielu znanych firm.

AC2000 Lite w praktyce – Distribution Center 24 na Białorusi

Distribution Center 24 jest obiektem mieszczącym się na terenie Białorusi, przez który codziennie przewija się wielu pracowników oraz gości odwiedzających różne wydziały. Przez teren obiektu, na którym znajdują się liczne biura, magazyny oraz obszerne parkingi, przejeżdża także wiele pojazdów. Tak duży ruch sprawia, że wymagania dotyczące bezpieczeństwa są wysokie. Dobrze prosperujący biznes wymaga sprawnej ochrony. Dzięki swej elastyczności system AC2000 Lite, zainstalowany przez lokalnego autoryzowanego dystrybutora CRM, czyli przez firmę Unibelus, doskonale sprawdził się w tych trudnych warunkach eksploatacyjnych.

W części rdzeniowej system AC2000 Lite bazuje na oprogramowaniu AC2000 firmy CEM. Oprogramowanie w wersji AC2000 Lite jest jego modyfikacją przystosowaną do pracy w małych lub średnich instalacjach. Dlatego zastosowany

Fot. 1. AC2000 Lite jest wysoce funkcjonalnym i ekonomicznym systemem kontroli dostępu przeznaczonym do zastosowania w małych oraz średniej wielkości obiektach

Fot. 2. AC2000 Lite zainstalowany w Distribution Center 24 zabezpiecza ponad 40 najważniejszych przejść

w Distribution Center 24 system AC2000 Lite oferuje użytkownikom wyrafinowane funkcje, normalnie dostępne jedynie w dużych instalacjach. Dzięki temu duży ruch pieszych i samochodów, z jakim mamy do czynienia na terenie tego obiektu, nie jest utrudniony.

Wydajne oprogramowanie

W zainstalowanym na terenie Distribution Center 24 systemie kontroli dostępu wykorzystano aplikacje, które są standardowymi składnikami pakietu AC2000 Lite, takie jak AC2000 VIPPS (Visual Image and Pass Production Software) i AC2000 Visitor Management. Aplikacja AC2000 VIPPS umożliwia pracownikom służb ochrony obiektu profesjonalne przygotowanie szablonów graficznych kart dostępu, które mogą zawierać informacje tekstowe, zdjęcia użytkowników, obrazy, kody paskowe i inne elementy graficzne. Przygotowane w oparciu o te szablony karty dostępu mogą być wykorzystywane w systemie kontroli dostępu, a dodatkowe oznakowanie ich kolorowymi paskami umożliwia szybką identyfikację wizualną w wydzielonych obszarach obiektu. Dzięki aplikacji AC2000 Visitor Management możliwa jest łatwa i szybka kontrola przemieszczania się osób czasowo przebywających na terenie obiektu. Rejestrowane są informacje na temat okazicieli tymczasowych kart identyfikacyjnych, takie jak dane personalne, cele wizyty oraz godziny umówionych spotkań.

Na wszystkich stacjach roboczych, które są obsługiwane przez pracowników służb ochrony obiektu Distribution Center 24, zainstalowane jest oprogramowanie klienckie AC2000 Lite. Stacje robocze pracują w czasie rzeczywistym i dostarczają informacji na temat stanu całego systemu kontroli dostępu. Dzięki temu możliwe jest szybkie reagowanie na alarmy oraz sygnały dotyczące niebezpiecznych wydarzeń.

Wersje językowe

Wszystkie produkty firmy CEM z serii AC2000, w tym system AC2000 Lite, są dostępne w wielu wersjach językowych, m.in.

Fot. 3. AC2000 Lite zainstalowany w Distribution Center 24 zapewnia szeroki zakres funkcji i nie utrudnia ruchu ludzi i pojazdów

Fot. 4. AC2000 Lite może zostać w prosty sposób zaktualizowany do pełnej wersji systemu zarządzania bezpieczeństwem AC2000, która umożliwia w zasadzie nieograniczoną rozbudowę systemu bezpieczeństwa

w języku polskim, niemieckim, rosyjskim, włoskim, arabskim i uproszczonym chińskim. Na terenie Distribution Center 24 zainstalowano rosyjskojęzyczną wersję systemu AC2000 Lite, dzięki czemu jego obsługa jest prosta zarówno dla personelu, jak i dla gości biznesowych odwiedzających ten obiekt.

Inteligentne urządzenia

Firma CEM wyposażyła Distribution Center 24 nie tylko w swoje oprogramowanie spełniające najwyższe wymagania przemysłowe, ale także w inteligentne urządzenia umożliwiające obsługę wielu punktów dostępowych. W Distribution Center 24 rozmieszczono ponad 40 punktów dostępowych, w których zainstalowano sieciowe kontrolery drzwiowe typu eDCM 300 (Ethernet Door Control Module). Każdy z kontrolerów eDCM 300 jest wyposażony w wewnętrzna bazę danych, dzięki czemu może prowadzić walidację kart identyfikacyjnych oraz zachować zdolność do podejmowania decyzji nawet wówczas, gdy połączenie z serwerem systemowym zostanie przerwane. Zainstalowane na terenie Distribution Center 24 kontrolery eDCM 300 mogą współpracować z czytnikami kart identyfikacyjnych innych producentów. Jest to wykorzystywane podczas obsługi szlabanów parkingowych, kołowrotków oraz rygli elektromagnetycznych kontrolujących ruch osób na terenie obiektu.

Funkcje wykraczające poza klasyczną kontrolę dostępu

System zainstalowany na terenie Distribution Center 24 stanowi jawny dowód na to, że produkty firmy CEM z serii AC2000 Lite mogą nie tylko realizować standardowe funkcje związane z kontrolą dostępu, ale także usprawniać pracę na terenie chronionych obiektów, ułatwiając wytyczanie oznakowanych tras, obsługę gości oraz realizując wiele innych funkcji.

Spojrzenie w przyszłość

W miarę wzrostu wymagań towarzyszącemu rozwojowi Distribution Center 24 system AC2000 Lite może zostać uaktualniony i osiągnąć możliwości systemu zarządzania bezpieczeństwem AC2000 w jego najnowszej wersji. Możliwości wprowadzania kolejnych zmian w oprogramowaniu są praktycznie nieograniczone.

W celu uzyskania dokładniejszych informacji należy skontaktować się z firmą CEM Systems.

CEM Systems

System komunikacji wewnętrznej VoIP

Inteligentny terminal dotykowy

Zdalne aplikacje

Kontroler i czytnik IP

emerald™

Świat możliwości na wyciągnięcie ręki

emerald™ to wielofunkcyjny inteligentny terminal dostępowy rewolucjonizujący przemysł zabezpieczeń.

Dzięki eleganckiej konstrukcji i specjalnie zaprojektowanemu nowoczesnemu ekranowi dotykowemu urządzenie emerald stanowi wydajny czytnik kart i kontroler w jednym, oferujący w pełni zintegrowany system komunikacji wewnętrznej Voice over IP (VoIP) oraz asortyment zdalnych aplikacji, zapewniających różnorodne możliwości kontroli dostępu. System emerald otwiera świat niezliczonych możliwości umieszczając system kontroli dostępu CEM w awangardzie przyszłości.

emerald™ — najbardziej wielofunkcyjny inteligentny terminal dostępowy w branży.

Jeśli potrzebujesz więcej informacji, prosimy o kontakt:
T: +44 (0)28 9045 6767
E: cem.info@tycoint.com
lub odwiedź nas na stronie www.cemsys.com/emerald

CEM SYSTEMS
From Tyco Security Products

Inteligentnie czy nie?

Sławomir Janiso

W latach 80-tych XX wieku jeden z tematów omawianych na zajęciach plastycznych w szkołach podstawowych brzmiał następująco: „Jak będzie wyglądał świat w 2000 roku?”. Rysunki wykonane przez dzieci zazwyczaj skupiały się na wątkach komunikacyjnych, wszędzie widać było latające samochody, w tle wznosiły się niewiarygodnie wysokie budowle. Jak widzimy, świat nie nadąża za dziecięcą wyobraźnią i nadal jeździmy zwykłymi samochodami z czterema kołami i bez skrzydeł

W2005 roku napisałem artykuł, w którym zadałem pytanie, czy widok instalatora systemu telewizji dozorowej z notebookiem na kolanach będzie równie częsty jak tego trzymającego śrubokręt. Czas pokazał, że mamy do czynienia raczej z ewolucją niż rewolucją. Kamery analogowe nadal trzymają się mocno, chociaż rynek CCTV IP ciągle rośnie. Z 2005 roku pamiętam również zachwyt nad możliwym wykorzystaniem tego, co już wtedy nazywano inteligentną analizą obrazu. Co zostało z zachwytu po dziewięciu latach?

Dziedziny, w których zaawansowana analiza obrazu może być szczególnie przydatna, są od wielu lat takie same. Należą do nich:

– transport publiczny: porty lotnicze, stacje kolejowe i przystanki metra, terminale autobusowe, porty morskie;
– monitoring miejski: ochrona obszarów wysoce zurbanizowanych;
– infrastruktura krytyczna: elektrownie atomowe, rafinerie, zakłady chemiczne, stacje telekomunikacyjne;
– transport i komunikacja: autostrady, drogi szybkiego ruchu, skrzyżowania;
– budynki i obszary rządowe i wojskowe;
– handel detaliczny.

Lista wykrywanych zdarzeń i zadań systemu również pozostała niezmienna. Oto one:

– poruszanie się osoby po danym obszarze, przekroczenie linii przez osobę, zatłoczenie, nieuprawnione wejście po osobie poprzedzającej do chronionych stref, wałęsanie się po danym obszarze, gromadzenie się, zliczanie ludzi (również w podstrefach);
– poruszanie się pojazdu po danym obszarze, przekroczenie linii przez pojazd, zatrzymanie się pojazdu, nieuprawniony wjazd za pojazdem poprzedzającym (szlaban), zliczanie pojazdów;
– pojawienie się lub zniknięcie obiektu;
– rozpoznawanie twarzy, płci, wieku i zainteresowania produktem.

Cześć algorytmów zaawansowanej analizy obrazu pełni przede wszystkim funkcje pomocnicze w systemach zabezpieczeń obiektów (detekcja przekroczenia linii, zgromadzeń, długiego przebywania na danym obszarze). Dzięki nim uwaga operatorów systemów monitoringu jest zwracana na te obszary, w których może dojść do działań niepożądanych. Na w pełni zautomatyzowane systemy, których nie musi obsługiwać człowiek, trzeba jednak poczekać. Interpretacja zdarzenia i rodzaj reakcji są nadal uzależnione od oceny sytuacji przez operatora. W tym zakresie ostatnie dziewięć lat nie przyniosło wielkich zmian – dobry pracownik centrum monitorowania jest nadal bezcenny.

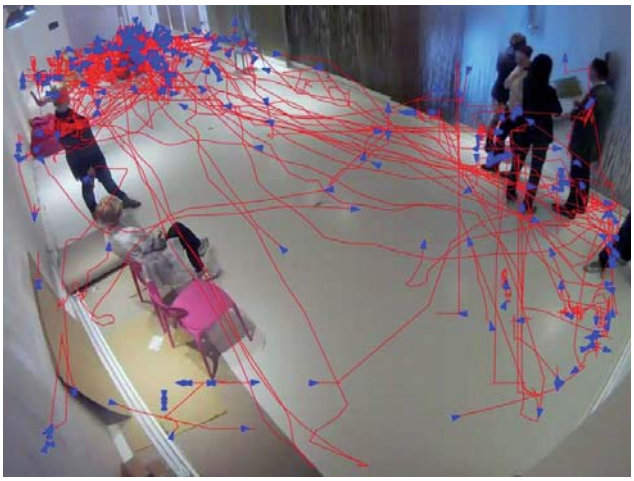
Ciekawym trendem jest wykorzystywanie inteligentnej analizy obrazu co celów innych niż ochrona. Kamery bywają instalowane przy autostradach, drogach oraz w obiektach handlowych. Są źródłem wielu pożytecznych informacji. Są też wykorzystywane w organizowaniu ruchu drogowego w miastach – korki przynoszą straty finansowe, powodują zwiększenie zanieczyszczenia środowiska, w związku z czym wykorzystuje się wszelkie możliwe środki do ich minimalizowania. Jedną z metod jest analiza obrazów z kamer, która umożliwia:

– zliczanie pojazdów w celu uzyskania informacji o obciążeniu danych fragmentów dróg czy skrzyżowań;
– wykrywanie zatłoczenia na drogach;
– analizę ruchu pieszych i pojazdów.

Inteligentną analizę obrazu można wykorzystać w działalności handlowej. Pracownicy ochrony mogą być ostrzegani o zdefiniowanych wcześniej zdarzeniach i wysyłani dokładnie tam, gdzie wymagana jest interwencja. Dzięki temu mogą szybko reagować. Można uzyskać materiał dowodowy w postaci nagrań i gromadzić materiały dotyczące sprawców wykroczeń. Dział marketingu uzyskuje dane dotyczące mocnych i słabych stron obiektu handlowego, skuteczności reklamy itp. Może też porównać swoje wyniki z wynikami konkurencji. Działowi zarządzania łatwiej ustalić wysokość opłat czynszowych, które będą uiszczać najemcy lokali w danym obiekcie, gdyż dzięki kamerom łatwiej jest określić natężenie ruchu klientów. Z analizy obrazu mogą też skorzystać najemcy lokali.

Dzięki inteligentnej analizie obrazu istniejące lub nowe systemy dozoru wizyjnego mogą mieć nowe funkcje:

– zliczanie klientów w czasie rzeczywistym, analiza wejść z rozróżnieniem kierunku ruchu,



Fot. 1. Ścieżki ruchu pokazujące trasy, po których poruszają się klienci

Fot. 2. Mapa cieplna powstała na podstawie ścieżek ruchu

– połączenia z innymi systemami (np. POS – badanie korelacji miedzy klientem odwiedzającym sklep a kupującym),
– analiza ruchu, czyli oznaczenie obszarów o różnych natężeniach ruchu oraz pokazanie często uczęszczanych tras w formie raportu graficznego lub mapy cieplnej,
– sygnalizowanie zatłoczenia, np. przy bankomatach (jako funkcja ochrony) lub przy kasach (jako sygnał dla obsługi).

Powyższe funkcje są niezwykle cenne – umożliwiają ocenę zachowań klientów i zwiększenie przychodów.

Decydując się na wykorzystanie inteligentnej analizy obrazu, musimy wziąć pod uwagę jej ograniczenia. Zatłoczenie obserwowanego miejsca może uniemożliwić detekcję pozostawionych przedmiotów. Kamera o zbyt niskiej rozdzielczości lub złym kącie widzenia może nie policzyć precyzyjnie klientów. Każde zastosowanie inteligentnej analizy obrazu w systemie telewizji dozorowej wymaga dobrego pomysłu, prawidłowego wykonania i rzetelnej analizy zebranych materiałów. Dziś mamy więcej możliwości. Możemy zrobić wszystko szybciej, lepiej, uzyskiwać większą rozdzielczość, ale nadal człowiek jest nieodzownym elementem systemu. Jest inteligentnie, ale nie automatycznie.

Sławomir Janiso

KAMERA IP 1.3 MPX

do całodobowej ochrony terenów wokół budynków

[f=7 ~ 22 mm]

Skupiona na detalach

Megapikselowy obiektyw ze zmienną ogniskową gwarantuje szczegółowy obraz, odpowiednie proporcje i kształty elementów obserwowanej sceny oraz optymalne dopasowanie pola widzenia kamery do miejsca pracy

[IR LED 50 m]

Wydajna praca w ciemności

Działanie funkcji dzień/noc w kamerze jest dodatkowo wspomagane przez pracę wbudowanego promiennika podczerwieni, który umożliwia oświetlenie obszaru w odległości do 50 m

[-40°C ~ 50°C]

Odporna na mrozy i upały

Kamera pracuje w temperaturze od -40°C do 50°C i ma szczelną obudowę o klasie ochrony IP 66, dlatego doskonale sprawdza się na zewnątrz. Uchwyt montażowy, pozwala na instalację na ścianie lub suficie

NOVUS IP | NMS Compatible | ONVIF | 3000 SERIA IP | NOVUS 3 lata gwarancji

Kamera sieciowa NVIP-1DN3040H/IR-1P

z detekcją ruchu i strefami prywatności

Więcej informacji o produktach NOVUS® znajdziesz na:
www.novuscctv.pl

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

System GEMOS
zapewnia bezpieczeństwo w Porcie Lotniczym Poznań-Ławica

Ela-compil

Systemy zarządzania doskonale sprawdzają się wszędzie tam, gdzie o bezpieczeństwo trzeba zadbać w sposób szczególny – między innymi w portach lotniczych. Ochrona tych obiektów to sprawa największej wagi państwowej. Codziennie przez każdy z nich przewijają się dziesiątki tysięcy osób. Zadaniem zarządców jest przede wszystkim zapewnienie maksymalnego bezpieczeństwa przebywającym tam osobom (zarówno pasażerom, jak i obsłudze lotniska), a w razie zagrożenia życia – możliwie jak najszybsze i bezkolizyjne wyprowadzenie ich z obiektu

Fot. 1. Port lotniczy Poznań-Ławica (materiały prasowe portu Poznań-Ławica)

Zadanie to wiąże się z ogromną odpowiedzialnością. Nic więc dziwnego, że osoby odpowiedzialne za bezpieczeństwo lotnisk chętnie sięgają po nowoczesne rozwiązania. Jednym z nich jest elektroniczny system wspomagający działanie Służby Ochrony Lotniska, policji i Straży Granicznej. System ten kontroluje dostęp do stref chronionych, zapewnia interakcję systemów standardowo ze sobą niepowiązanych oraz dostarcza wielu cennych informacji o stanie systemów technicznych.

Podstawowym warunkiem, jaki musi spełnić system bezpieczeństwa portu lotniczego, jest integracja wszystkich systemów wykorzystywanych przez służby ochrony w ramach jednej platformy, która umożliwia kontrolę stanu bezpieczeństwa obiektu z jednego centrum zarządzania. Zazwyczaj systemy te mają postać wielu niezależnych, samodzielnych urządzeń, które muszą być osobno zasilane i serwisowane. Aby zoptymalizować koszty i zapewnić kompleksową obsługę wszystkich tych urządzeń, stosuje się zintegrowane systemy zarządzania obiektami, takie jak proponowany przez firmę Ela-compil system zarządzania GEMOS. System ten aktywnie wspiera działania zarządcy i operatora, obsługuje oraz nadzoruje systemy automatyki budynkowej, a także utrzymuje najwyższy poziom bezpieczeństwa.

GEMOS jest neutralną platformą służącą do integracji, wizualizacji i sterowania dowolnymi podsystemami technicznymi (SSP, SSWiN, KD, DSO, telewizja dozorowa, automatyka pożarowa itp.), które znajdują się w danym obiekcie. Powstał, by spełnić oczekiwania osób zainteresowanych bezpieczeństwem obiektu – inwestorów, architektów, projektantów, generalnych wykonawców, służby bezpieczeństwa oraz pracowników obsługi technicznej. Dzięki systemowi GEMOS możliwa jest integracja, wizualizacja oraz obsługa wszystkich wymienionych systemów, analiza przyczyn alarmów oraz pełna kontrola w ramach jednego lub kilku centralnych stanowisk.

Kluczową cechą aplikacji GEMOS jest jej neutralność. Z systemem GEMOS można zintegrować wszystkie systemy bezpieczeństwa, łączności czy automatyki budynkowej różnych producentów. Dobierając poszczególne systemy teletechniczne, projektant może kierować się wartościami użytkowymi poszczególnych urządzeń, nie zwracając uwagi na to, kto je wyprodukował. Dzięki zastosowaniu systemu Gemos

zaistnienie w jednym z systemów dowolnego zdarzenia, takiego jak alarm, awaria czy pożar, będzie powodowało określoną, zaprogramowaną wcześniej reakcję innego, dotąd kompletnie niezależnego systemu.

System GEMOS integruje inne systemy dzięki interfejsom programowym oraz sterownikom w postaci kart przeznaczonych do obsługi konkretnych systemów. W każdej instalacji możliwe jest też użycie kart wejść i wyjść oraz certyfikowanych przez CNBOP kart wejść i wyjść przeciwpożarowych. Dzięki temu w dowolnym momencie można podłączyć kolejne urządzenia sterowane i nadzorowane poprzez klasyczne wejście lub wyjście przekaźnikowe (np. klapy oddymiające, wentylatory czy sygnalizatory).

Gemos jest systemem skalowalnym. Oznacza to, że może być dowolnie rozbudowywany i uzupełniany, jeśli zachodzi taka potrzeba. Jest to cecha niezwykle istotna, zwłaszcza w przypadku takich obiektów jak port lotniczy, które podlegają stałym rozbudowom czy okresowym modernizacjom. Dodatkowo zastosowanie systemu zarządzania umożliwia wyeliminowanie większości występujących w obiekcie usterek, co podwyższa poziom stanu technicznego oraz bezpieczeństwa obiektów. Systemy nadzorowane przez GEMOS są kontrolowane w trybie ciągłym, przez 24 godziny na dobę. Skrócenie fazy projektowania oraz możliwość zmniejszenia ilości okablowania realnie wpływa na koszty budowy lub modernizacji budynku.

System GEMOS umożliwia użytkownikowi błyskawiczną reakcję na wszelkie sytuacje alarmowe. Obsługiwany na jednym lub kilku centralnych stanowiskach w pełni umożliwia kontrolę wszystkich systemów technicznych zainstalowanych w obiekcie. Personel obsługujący stanowisko kontrolne otrzymuje pełną informację tekstową i graficzną, towarzyszącą pojawieniu się komunikatu alarmowego. Sytuacja wizualizowana jest na ekranie monitora (możliwe jest również wysłanie sygnału dźwiękowego lub SMS-a). Wraz ze zgłoszeniem alarmu wyświetlane są procedury postępowania, które obsługa powinna zrealizować. Ponadto system automatycznie generuje podgląd tego fragmentu obiektu, w którym czujnik alarmujący zgłasza odchylenie od normy. Dzięki temu można otrzymać spójne dane na planach graficznych budynku.

System GEMOS jest wykorzystywany przez pracowników ochrony i administracji w portach lotniczych w całej Polsce. W listopadzie 2001 roku został wdrożony w Porcie Lotniczym Poznań-Ławica. Na pierwszym etapie zintegrowane zostały systemy bezpieczeństwa obiektu, systemy ogrzewania, klimatyzacji, monitoringu, a także systemy alarmowe i przeciwpożarowe w budynku terminalu pasażerskiego.

Na przełomie lat 2007 i 2008, wraz z rozbudową portu, dokonana została aktualizacja systemu do wersji Gemos 3, co umożliwiło kontrolowanie stanu bezpieczeństwa portu na więcej niż jednym stanowisku. Jednocześnie zwiększono liczbę czujek i przejść objętych systemem kontroli dostępu oraz wprowadzono nowe grafiki umożliwiające wizualizację stanu bezpieczeństwa rozbudowanej części portu.

Wkrótce po zakończeniu prac zakres integracji został rozszerzony o strażnicę Lotniskowej Służby Ratowniczo-Gaśniczej znajdującą się poza głównym budynkiem portu, a także o budynek CARGO.

Trzeci znaczący etap rozwoju systemu Gemos nastąpił podczas ostatniej rozbudowy terminalu pasażerskiego Portu Lotniczego Poznań-Ławica, przeprowadzonej po powierzeniu miastu Poznań organizacji finałowych meczy EURO 2012.

Modernizacja i rozbudowa terminalu pociągnęła za sobą gruntowną przebudowę systemów wpływających na stan bezpieczeństwa obiektu. Wymieniono system kontroli dostępu, system telewizji dozorowej, dźwiękowy system ostrzegawczy, a w nowo dobudowanej części terminalu znalazł zastosowanie również inny niż w „starej" części system sygnalizacji pożarowej. Klapy wentylacji pożarowej wyposażono w siłowniki cyfrowe współpracujące z systemem LSK.

Należy podkreślić, iż tak gruntowne zmiany nie utrudniły działania systemu Gemos – został on jedynie dodatkowo wyposażony w interfejsy służące do obsługi nowo wprowadzonych rozwiązań oraz wzbogacony m.in. w nowe grafiki i maski graficzne obrazujące przebudowany terminal.

Pracownicy lotniska doceniają to, że przez ponad dwa lata system GEMOS stale monitorował i nadzorował przebudowywane i rozszerzane o nowe elementy systemy techniczne, co zapewniało pożądany poziom bezpieczeństwa obiektu oraz komfortowe zarządzanie jego bezpieczeństwem.

Zainstalowanie systemu Gemos w Porcie Lotniczym Poznań-Ławica stanowiło nie lada wyzwanie, zarówno dla producenta, jak i dla integratorów. System musi spełniać nie tylko wymogi bezpieczeństwa, ale także wymagania użytkowe stawiane przez wszystkie służby obecne na lotnisku: Straż Graniczną, Straż Ochrony Lotniska, policję, Służbę Celną, Lotniskową Straż Ratowniczo-Gaśniczą. Każda z tych jednostek ma bowiem własne, ściśle określone procedury bezpieczeństwa i choć ogólny cel jest jeden – ochrona portu i bezpieczeństwo jego użytkowników – to procedury postępowania bywają różne. Warto podkreślić, iż system GEMOS został zainstalowany również na krakowskich Balicach i w porcie lotniczym Copernicus we Wrocławiu.

Fot. 2. Terminal portu lotniczego Poznań-Ławica (fot. Hochtief, materiały prasowe portu Poznań-Ławica)

Ela-compil

ULISSE COMPACT **HD**

RENOMOWANE I NIEZAWODNE URZĄDZENIE PTZ PRZEZNACZONE DO ZASTOSOWAŃ ZEWNĘTRZNYCH, AKTUALNIE DOSTĘPNE W WERSJI FULL HD 1080P!

ULISSE COMPACT HD jest kamerą sieciową PTZ Full HD 1080p, umożliwiającą uzyskanie obrazu wideo doskonałej jakości o wysokiej rozdzielczości. To zintegrowane urządzenie PTZ jest odporne na środowiska ekstremalne, gwarantuje dużą prędkość i dokładność detekcji obiektu w każdych warunkach.

ULISSE COMPACT HD jest idealnym rozwiązaniem przeznaczonym dla skomplikowanych zastosowań nadzoru, takich jak: kontrola ruchu drogowego i autostrad, nadzór graniczny, stadionów i budynków przemysłowych, więzień, instalacji wojskowych oraz nadzór granic obszarów.

IP66
IP67
PROTECTION

IP

WIPER

INFRARED

ONVIF S

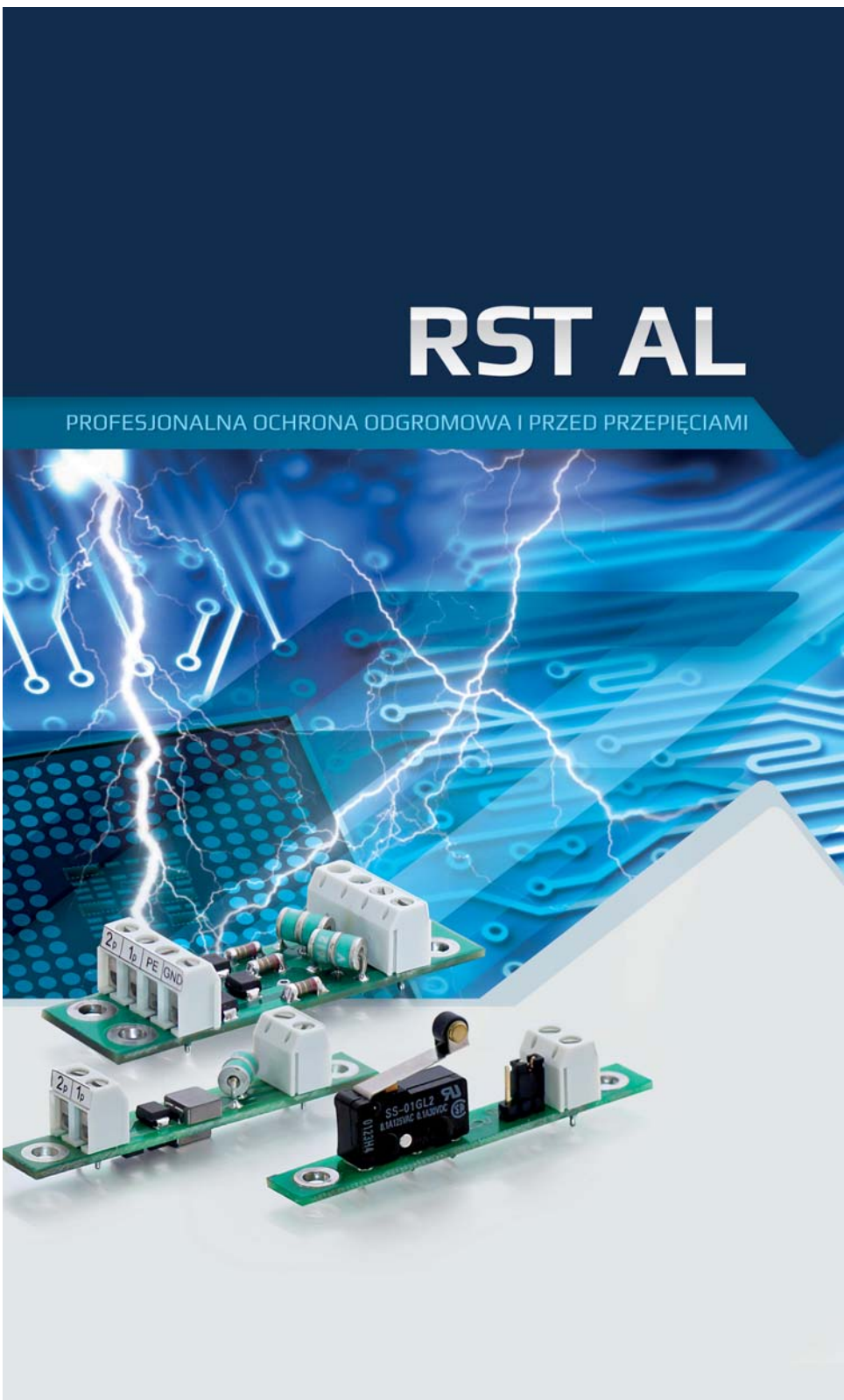
PRODUCTS FOR CCTV | WWW.VIDEOTEC.COM | E-mail: info@videotec.com

VIDEOTEC

Ochrona przed przepięciami systemów sygnalizacji włamania i napadu

Tomasz Maksimowicz

Systemy alarmowe mają na celu zabezpieczenie obiektu przed zagrożeniami, takimi jak pożar lub włamanie. Aby taki system był skuteczny i wiarygodny, powinien być niezawodny w każdych warunkach. Jednym z zagrożeń dla prawidłowego funkcjonowania systemów alarmowych są przepięcia wywoływane zakłóceniami w instalacjach zasilania niskim napięciem oraz oddziaływaniem wyładowań atmosferycznych. W niniejszym artykule przedstawione zostanie zagadnienie ochrony przed przepięciami na przykładzie systemów sygnalizacji włamania i napadu (SSWiN)



1. Zasadność stosowania ochrony

Ochrona przed przepięciami jest zagadnieniem często lekceważonym przez projektantów. Ponieważ w większości przetargów główne kryterium wyboru ofert stanowi cena i nie ma ściśle określonych wymagań technicznych, ograniczniki przepięć (SPD – ang. *Surge Protecting Device*) są traktowane jako źródło dodatkowych kosztów. Potrzeba stosowania ochrony przed przepięciami zauważana jest najczęściej dopiero po wystąpieniu szkód przez nie wywołanych. Jeżeli uszkodzenia będą się pojawiać wielokrotnie w sezonie burzowym, to koszt sumaryczny ich usunięcia w końcu przekroczy koszt całego systemu.

Jeżeli koszt ogranicznika przepięć jest porównywalny z kosztem pojedynczego elementu systemu alarmowego, a zwłaszcza wyższy od niego, to ochrona przed przepięciami jest najczęściej uznawana za nieopłacalną. Taniej jest bowiem wymienić urządzenie, niż zainwestować w ograniczniki przepięć. To przekonanie jednak może okazać się złudne, jeżeli urządzenia będą uszkadzane cyklicznie. Gdy natomiast mamy do czynienia z elementami droższymi, takimi jak np. bariery mikrofalowe łatwiej jest przekonać inwestora do stosowania ochrony przed przepięciami.

Awaria systemu lub jego części wskutek wystąpienia przepięć powoduje nie tylko bezpośrednie straty materialne, ale także utratę części lub całości jego funkcji, co może wiązać się z jeszcze większymi kosztami. Dlatego też należy uwzględnić ewentualne możliwe skutki przerwy w pracy systemu i rozważyć zwiększenie jego odporności poprzez stosowanie SPD. W wielu przypadkach przerwa w działaniu systemu lub jego części nie ogranicza się jedynie do czasu potrzebnego na jego naprawę, ale także (w przypadku obiektów państwowych) obejmuje czas potrzebny do przeprowadzenia procedur przetargowych związanych z zakupem nowego sprzętu lub wyborem wykonawcy robót.

2. Odporność systemów alarmowych

Zgodnie z obowiązującą normą PN-EN 50130-4 dotyczącą kompatybilności elektromagnetycznej systemów alarmowych poszczególne elementy powinny charakteryzować się między innymi określoną odpornością na udary przewodzone. Norma wymaga, aby urządzenia były badane kombinowanym udarem napięciowo-prądowym (kształt napięcia obwodu otwartego: 1,2/50 μs, kształt prądu obwodu zwartego: 8/20 μs). Przyjęte w normie probiercze wartości szczytowe napięć udarowych, które powinny być wytrzymywane przez urządzenia systemów alarmowych, wynoszą:

– dla portów zasilania AC: 1 kV pomiędzy liniami, 2 kV pomiędzy dowolną linią a ziemią;
– dla portów sygnałowych i zasilania DC: 1 kV pomiędzy dowolną linią a ziemią.

Wartościom napięć 1 kV i 2 kV odpowiadają wartości szczytowe prądów zwarcia 0,5 kA i 1 kA. Jak sama norma wskazuje, przyjęte w niej poziomy odporności nie uwzględniają sytuacji krytycznych, do których można zaliczyć oddziaływanie wyładowań atmosferycznych. Wartości prądów udarowych, jakie mogą zostać zaindukowane w liniach sygnałowych wskutek oddziaływania wyładowań atmosferycznych, są znacznie większe. Według informacji podanych w normach odgromowych serii PN-EN 62305 podczas bezpośredniego uderzenia pioruna w budynek w obwodach niskonapięciowych mogą zaindukować się prądy o wartościach szczytowych do 5 kA lub 10 kA, odpowiednio dla założenia IV i I poziomu ochrony odgromowej (LPL – ang. *Lightning Protection Level*). Ponadto jeżeli część obwodów systemu alarmowego znajduje się na zewnątrz obiektu, to mogą do niego przeniknąć także częściowe prądy pioruna o znacznie dłuższym czasie trwania i przenoszące większą energię; dla takich prądów zakłada się udar o kształcie 10/350 μs.

Konstruowanie urządzeń, które bez dodatkowej zewnętrznej ochrony wytrzymają udary o tak dużej energii, nie jest rozwiązaniem zalecanym. Mogłoby to stwarzać dodatkowe zagrożenia dla urządzeń. Ścieżki w standardowych laminatach płytek drukowanych PCB nie wytrzymują przepływu tak dużych prądów, a energia przepięć musi być odprowadzona do ziemi, co wymaga osobnego zacisku uziemiającego. Lepszym rozwiązaniem jest ograniczenie przepięć poza urządzeniem za pomocą specjalistycznego układu SPD i bezpieczne odprowadzenie energii do uziemienia.

Zabezpieczenia takich składników systemu jak czujki i centrale alarmowe powinny ograniczać się jedynie do elementów ograniczających przepięcia – zdolnych do ich pochłonięcia – jednak w takim przypadku należy skoordynować ewentualne zabezpieczenia wewnętrzne z dodatkowymi komponentami SPD.

3. Strefowa koncepcja ochrony odgromowej

Normy odgromowe serii PN-EN 62305 wprowadziły zasady strefowej koncepcji ochrony, która polega na podziale obiektu na strefy ochrony odgromowej (LPZ – ang. *Lightning Protection Zone*). Idea strefowej koncepcji ochrony przed przepięciami została przedstawiona na rysunku 1. Dla każdej strefy LPZ określa się piorunowe środowisko elektromagnetyczne charakteryzujące się założonymi typami i poziomami zagrożeń. W przypadku systemów alarmowych zaleca się wyznaczenie następujących stref:

– LPZ 0_A – strefa na zewnątrz budynku, w której występuje zagrożenie wyładowaniem bezpośrednim oraz oddziaływanie całkowitego prądu pioruna i całkowitego pola magnetycznego; w tej strefie znajdować się mogą zazwyczaj położone w terenie słupy kamerowe czy też bariery mikrofalowe;
– LPZ 0_B – strefa na zewnątrz budynku, w której nie występuje zagrożenie wyładowaniem bezpośrednim, ale możliwe jest oddziaływanie częściowego prądu pioruna lub prądów indukowanych oraz całkowitego pola magnetycznego; strefa ta określona jest poprzez zwody instalacji odgromowej; w tej strefie umieszczone są (zazwyczaj na elewacji budynku) sygnalizatory, kamery, czujki ruchu, manipulatory itp.;
– LPZ 1 – strefa obejmująca wnętrze budynku, w której nie występuje zagrożenie oddziaływaniem ograniczonego prądu pioruna, prądów indukowanych oraz całkowitego lub stłumionego pola magnetycznego; w tej strefie znajduje się większość elementów systemu alarmowego, takich jak czujki ruchu, czujki ppoż., manipulatory, ekspandery, kamery itp.;

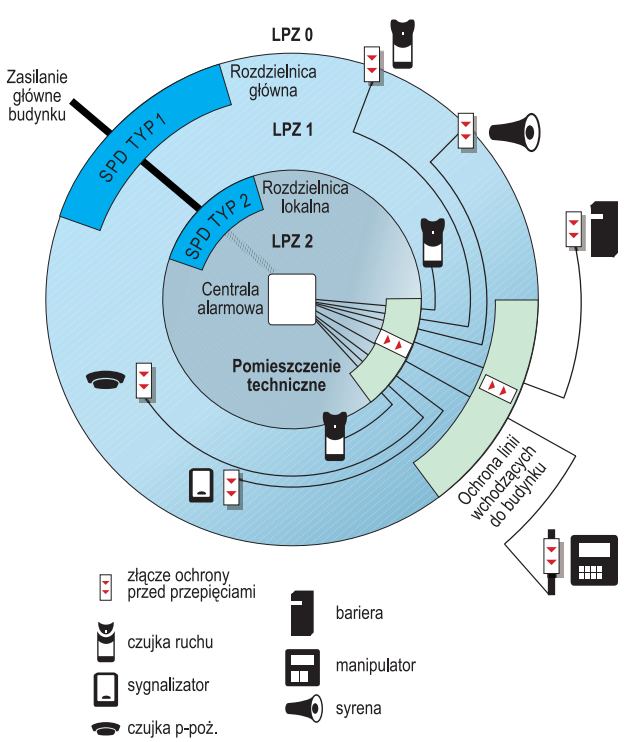
– LPZ 2 – strefa w obrębie LPZ 1 obejmująca wydzielone pomieszczenie techniczne, w którym znajduje się centrala alarmowa; poziomy zagrożeń powinny być ograniczone do bezpiecznych wartości.

Ochrona przed przepięciami powinna być stosowana na granicy poszczególnych stref stosownie do spodziewanych poziomów zagrożeń.

Układy SPD o najwyższej odporności należy stosować na granicy stref LPZ 0/1. Zastosowanie powinny tu mieć jedynie SPD typu 1 wg PN-EN 61643-11 w instalacjach zasilających niskiego napięcia oraz kategorii D1 wg PN-EN 61643-21 w obwodach sygnałowych. Ograniczniki typu 1 i kategorii D1 zapewniają ochronę przed częściowym prądem pioruna, który w strefie LPZ 0 może przeniknąć do instalacji systemu alarmowego. Wszelkie obwody zewnętrzne powinny być w miarę możliwości wprowadzone do wnętrza budynku w jednym miejscu, co pozwala na zabezpieczenie obwodów w jednym punkcie za pomocą złącza ochrony przed przepięciami (ZOP). Jeżeli jest to niemożliwe, obwody do urządzeń umieszczanych na elewacji budynku powinny być zabezpieczone w miejscu wejścia przewodów do budynku.

Zabezpieczenia na granicy stref LPZ 1/2 mają za zadanie zapewnienie ochrony dokładnej przed prądami indukowanymi oraz prądami pioruna ograniczonymi na granicy LPZ 0/1. Dlatego w tym miejscu wystarcza zastosowanie SPD typu 2 i typu 3 w instalacjach zasilających oraz kategorii C2 w obwodach sygnałowych. Zabezpieczenie centrali alarmowej powinno być kompletne, co oznacza, że chronione powinny być wszelkie przyłączone do niej obwody, a nie tylko wybrane, uznane za najbardziej zagrożone.

Oprócz ochrony na granicy poszczególnych stref niekiedy zalecane jest stosowanie ochrony przy wybranych urządzeniach końcowych. Jeżeli długość trasy kablowej wewnątrz budynku między centralą alarmową a danym urządzeniem jest większa niż 30 metrów, to zaleca się zastosowanie ochrony



Rys. 1. Idea strefowej koncepcji ochrony przed przepięciami

bezpośrednio przy urządzeniu. Związane jest to z możliwym indukowaniem się prądów udarowych w pętlach tworzonych przez rozległe okablowanie systemu.

4. Problematyka ochrony systemów alarmowych

Ochrona przed przepięciem obwodu zasilania niskiego napięcia 230 V w systemach SWiN dotyczy praktycznie jedynie central alarmowych zasilanych poprzez transformator; pozostałe elementy systemu zasilane są napięciem stałym z centrali. Ochrona jest ograniczona zwykle do zastosowania ograniczników typu 1 lub typu 1+2 w rozdzielnicy głównej budynku i ograniczników typu 2 w rozdzielnicy lokalnej, z której jest zasilana centrala alarmowa. Istotną kwestią jest dobór ograniczników typu 1 – zaleca się stosowanie ograniczników wykorzystujących iskierniki, które mają znacznie wyższą odporność niż ograniczniki warystorowe.

Bardziej złożona jest kwestia ochrony obwodów sygnałowych SSWiN, w których wyróżnić należy przede wszystkim:

– linie dozorowe,
– linie wyjściowe,
– magistrale transmisyjne.

Obok wyżej wymienionych typów linii spotkać można jeszcze linie telefoniczne i magistrale danych do komunikacji z komputerem.

Ograniczniki przepięć powinny być dobrane na podstawie takich parametrów linii jak maksymalne wartości prądu i napięcia, częstotliwość itp., tak aby nie zakłócać pracy systemu alarmowego.

Linie dozorowe powiązane z wejściami centrali alarmowej przenoszą informacje alarmowe o stanie dozorowanego obiektu lub jego wydzielonej strefy. Obecnie stosowane są linie dozorowe zwykłe, linie parametryczne oraz linie adresowalne. Najpopularniejsze są linie sparametryzowane, które poza informacją o stanie alarmowym czujki mogą jednocześnie przekazać informacje o sabotażu lub zwarciu/rozwarciu linii, co pozwala na uzyskanie bardziej szczegółowych danych przy mniejszej liczbie przewodów. Takie rozwiązanie jest także korzystne z punktu widzenia ochrony przed przepięciami, ponieważ pozwala na ograniczenie liczby SPD. Ograniczniki przepięć są dobierane do napięcia pracy w linii. Typowo napięcie znamionowe w systemach alarmowych wynosi 12 V, ale jego maksymalna wartość może w zależności od producenta wynosić 13,8 V lub nawet 16 V. Maksymalny prąd w liniach dozorowych nie przekracza zwykle wartości kilkudziesięciu miliamperów. Nie ma też wygórowanych wymagań co do pasma częstotliwości.

Linie wyjściowe centrali alarmowej można podzielić na wysokoprądowe i niskoprądowe. Wyjścia niskoprądowe central alarmowych służą do sterowania urządzeniami zewnętrznymi, np. do wyzwolenia sygnalizacji optycznej lub akustycznej. Linie wysokoprądowe odpowiadają z kolei za zasilanie wszelkich urządzeń składowych systemu. Maksymalne obciążenie takich wyjść wynosi 2 A, czasami spotykane są systemy z wyjściami o obciążeniu 3A. Taki prąd jest wystarczający do zasilania sygnalizatorów akustycznych i ewentualnie ładowania umieszczonych w nich baterii akumulatorów. Wyższe wartości prądów nie są spotykane w SSWiN; jeżeli jest potrzeba sterowania przez system w stanie alarmu urządzeniem o wyższym

Fot. 1. Złącze ochrony przed przepięciami centrali alarmowej

poborze prądu, to odbywa się to za pomocą przekaźników sterowanych z wyjść niskoprądowych.

Magistrale transmisyjne zapewniają komunikację z manipulatorami lub ekspanderami wykorzystywanymi do rozszerzenia możliwości systemu. Wykorzystywane są różne standardy transmisji szeregowej, takie jak RS232, RS422, RS485. Transmisja odbywa się za pomocą trzech żył, oznaczanych w różny sposób przez poszczególnych producentów (np. + , – , GND lub DTM, CKM, COM). Wartości napięć zależą od zastosowanego standardu, ale nie przekraczają zwykle ± 15 V.

Na fotografii 1 przedstawiono przykładowe rozwiązanie złącza ochrony przed przepięciami, obejmujące ochronę obwodu zasilania 230 V oraz 26 linii dozorowych i wyjściowych.

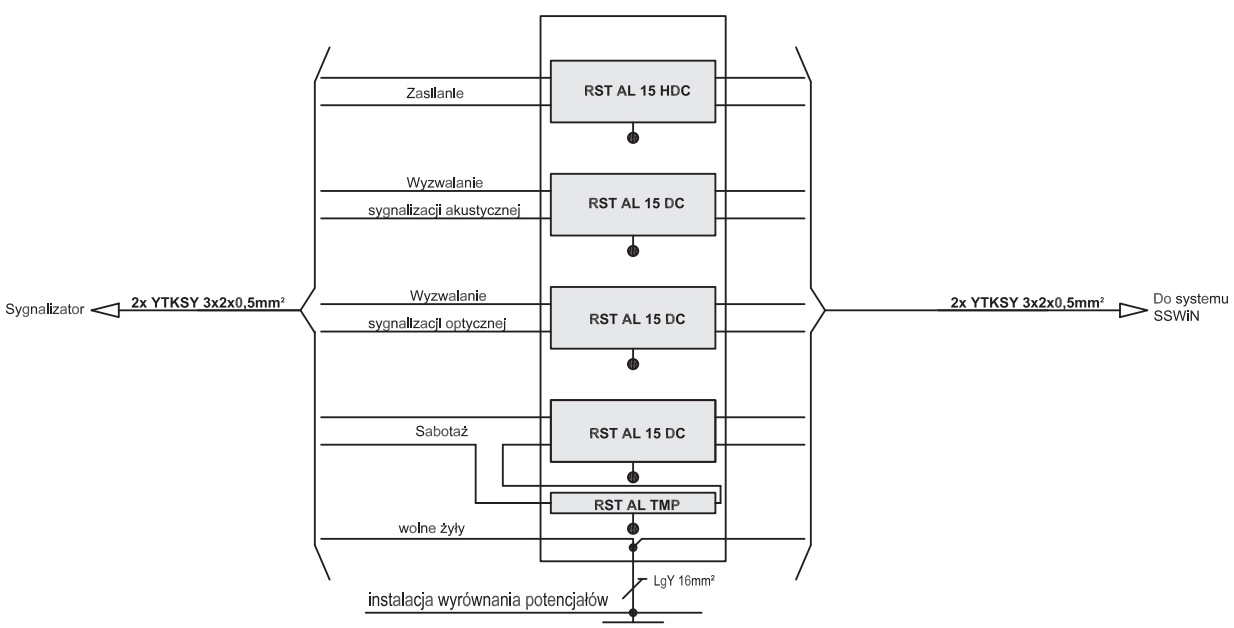
Istotny problem w przypadku ochrony systemów alarmowych stanowi uziemienie ogranicznika przepięć, pozwalające na bezpieczne odprowadzenie energii do ziemi. Zacisk uziemiający ogranicznika SPD, zainstalowanego przy centrali alarmowej, do której transformatora doprowadzono zasilanie 230 V, dzięki czemu jest dostęp do przewodu ochronnego PE, przyłączamy do tego przewodu. Uziemienie układów chroniących poszczególne komponenty, takie jak czujki czy sygnalizatory, może nastręczać trudności. W nowych obiektach, w których ochrona przed przepięciami została uwzględniona już na etapie projektu, możliwe jest wykonanie instalacji wyrównania potencjałów z punktami uziemiającymi ulokowanymi wszędzie tam, gdzie przewiduje się stosowanie SPD. Sytuacja się komplikuje, gdy ochrona ma być wykonana w obiekcie już istniejącym, np. gdy system alarmowy jest dopiero wykonywany lub gdy właściciel obiektu decyduje się na wstawienie ochrony po zaistnieniu szkód spowodowanych przez przepięcia. Jeżeli w obiekcie nie istnieje instalacja wyrównania potencjałów i nie ma możliwości jej wykonania, do uziemienia ograniczników przepięć należy wykorzystać przewody PE instalacji elektrycznej. Uziemienie należy dołączyć do przewodu PE najbliższej puszki łączeniowej lub gniazda instalacji elektrycznej. Zalecane jest umieszczanie ogranicznika przepięć jak najbliżej chronionego urządzenia.

Kolejną kwestią związaną z zabezpieczeniem systemów alarmowych jest sygnalizacja sabotażu. Złącza ochrony przed przepięciami umożliwiają dostęp do poszczególnych linii dozorowych, dlatego należy je również wyposażyć w sygnalizację nieupoważnionej ingerencji. Styki sabotażowe układów zabezpieczających urządzenia końcowe, umieszczone w obudowie złącza z ogranicznikami przepięć, powinny być włączone w obwód sygnalizacji sabotażu chronionego urządzenia. Sygnalizacja sabotażu złącza zabezpieczającego centralę alarmową może stanowić oddzielny obwód wejściowy, jeżeli złącze jest umieszczone w większej odległości od centrali; można je również powiązać z obwodem sabotażowym obudowy centrali.

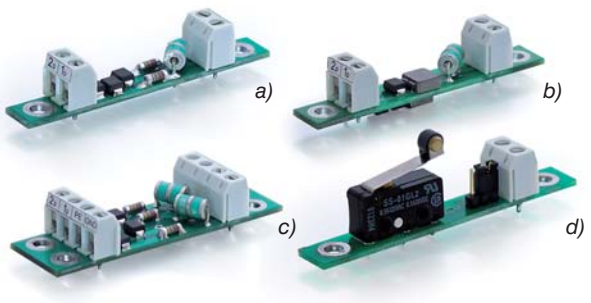
Na rysunku 2 przedstawiono schemat blokowy przykładowego układu ochronnego sygnalizatora ze stykiem sabotażowym RST AL TMP włączonym w obwód sygnalizacji sabotażu sygnalizatora.

5. RST AL – ograniczniki przepięć dedykowane do systemów alarmowych

Seria ograniczników przepięć RST AL produkcji RST została zaprojektowana specjalnie z myślą o ochronie systemów alarmowych. Wszystkie ograniczniki serii wykonane są jako



Rys. 2. Schemat blokowy przykładowego złącza ochrony przed przepięciami sygnalizatora



Fot. 2. Ograniczniki przepięć serii RST AL do ochrony SSWiN: a) RST AL 15 DC, b) RST AL 15 HDC, c) RST AL RS, d) RST AL TMP

miniaturowe moduły przeznaczone do montażu na wydzielonej szynie lub płycie uziemiającej. Wymiary pojedynczego modułu to 10×65 mm, a ich wysokość nie przekracza 15 mm. W porównaniu ze standardowymi ogranicznikami przepięć przeznaczonymi do montażu na szynie TS 35 ograniczniki serii RST AL mogą być umieszczone w znacznie mniejszych obudowach. Dzięki tak małym rozmiarom mogą być montowane w bardziej dyskretnych puszkach łączeniowych zajmujących mniej miejsca.

Podstawowe moduły serii RST AL przeznaczone do ochrony systemów alarmowych to:

– RST AL 15 DC – SPD do zabezpieczenia linii dozorowych i wyjść niskoprądowych (fot. 2a);
– RST AL 15 HDC – SPD do zabezpieczenia wyjść wysokoprądowych (fot. 2b);
– RST AL RS – SPD do zabezpieczenia magistral transmisyjnych (fot. 2c);
– RST AL TMP – moduł do sygnalizacji sabotażu złącza ochrony przed przepięciami (fot. 2d).

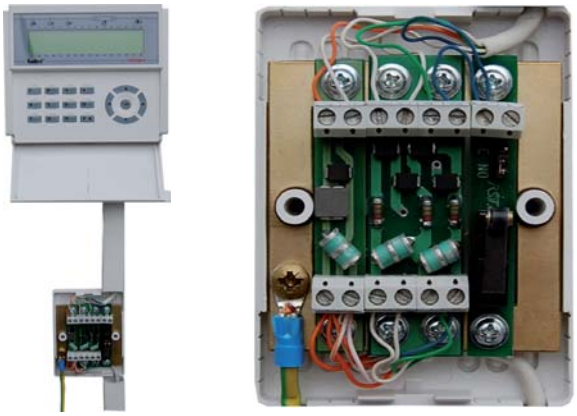
Powyższe ograniczniki charakteryzują się maksymalnym napięciem trwałej pracy U_C = 17 V, tak więc obejmują wszystkie typowe standardy sygnałów stosowanych w systemach alarmowych. Dla innych rozwiązań dostępne są również moduły RST AL 24 DC oraz RST AL 24 HDC, przeznaczone do pracy w systemach o znamionowym napięciu stałym 24 V (U_C = 30 V). Moduły typu DC i HDC różnią się przede wszystkim znamionowym prądem, który wynosi, odpowiednio, 0,5 A i 2,5 A. Z tego względu ograniczniki RST AL 15 DC i RST AL 24 DC są przeznaczone do ochrony linii dozorowych oraz wyjść niskoprądowych, natomiast ograniczniki typu HDC – do ochrony linii wysokoprądowych. Moduł RST AL RS jest przeznaczony do ochrony trzyżyłowych magistral transmisji szeregowej pomiędzy centralą alarmową a manipulatorami lub ekspanderami. Styk sabotażowy RST AL TMP, dostosowany do danego typu obudowy, umożliwia sygnalizację nieautoryzowanej ingerencji w obwody systemu alarmowego.

Ograniczniki RST AL zostały przebadane zgodnie z wymaganiami normy PN-EN 61643-21 dla kategorii wytrzymałości udarowej C2 i D1. Przy małych wymiarach charakteryzują się wysoką odpornością I_{max} = 10 kA na udary indukowane o kształcie 8/20 μs oraz I_{imp} = 2,5 kA na częściowe prądy pioruna o kształcie 10/350 μs. Dzięki kategorii D1 mogą być stosowane także na granicach stref LPZ 0/1. Przy takiej odporności układy te zgodnie z normą odgromową PN-EN 62305-1 mogą być stosowane nawet w obiektach, dla których przyjęto najwyższy pierwszy poziom ochrony LPL I. Dzięki dwustopniowej ochronie opartej na miniaturowych odgromnikach gazowanych i diodach ograniczniki RST AL zapewniają bardzo niski napięciowy poziom ochrony. Podstawowe ich parametry przedstawiono w tabeli 1.

Obudowy dobierane są w zależności od liczby układów i miejsca instalacji złącza ochrony przed przepięciami. Zabezpieczenia pojedynczych urządzeń ograniczają się przeważnie do czterech modułów obejmujących obwód zasilania, linie dozorowe i styk sabotażowy. Przykładowe rozwiązania przedstawiono na fotografiach 3 i 4. Na fotografii 3 przedstawiono przykład zabezpieczenia manipulatora. Układ ochronny składa się z modułu

Parametry techniczne				RST AL 15 DC	RST AL 15 HDC	RST AL RS
Kategoria testowania wg PN-EN 61643-21				D1/C1/C2	D1/C1/C2	D1/C1/C2
Napięcie znamionowe			U_n	15 V=	15 V=	15 V=
Maksymalne napięcie pracy trwałej DC			U_c	17 V=	17 V=	17 V=
Maksymalne napięcie pracy trwałej AC			U_c	12 V~	12 V~	12 V~
Prąd znamionowy			I_N	0,5 A	2,5 A	0,5 A
C1: znamionowy prąd wyładowczy (8/20 μs)/linia			I_n	0,5 kA	0,5 kA	0,5 kA
C2: znamionowy prąd wyładowczy (8/20 μs)/linia			I_n	5 kA	5 kA	5 kA
Maksymalny prąd wyładowczy (8/20 μs)			I_{max}	10 kA	10 kA	10 kA
D1: maksymalny prąd piorunowy (10/350 μs)			I_{imp}	2,5 kA	2,5 kA	2,5 kA
Napięciowy poziom ochrony	linia – linia	przy I_n C1	U_p	24 V	24 V	24 V (48 V*)
	linia – ziemia			24 V	24 V	24 V
	linia – linia	przy I_n C2		33 V	26 V	35 V (58 V*)
	linia – ziemia			33 V	26 V	35 V
Częstotliwość graniczna 3 dB			f	2,3 MHz	1,2 MHz	2,4 MHz
Rezystancja szeregowa na linię			R_{DC}	2,2 Ω	0,2 Ω	2,2 Ω
Prąd upływu przy Uc			I_L	< 1 μA	< 1 μA	< 1 μA
Rezystancja izolacji przy Uc			R_{izol}	100 MΩ	100 MΩ	100 MΩ
Indukcyjność wzdłużna			L	–	22 μH	–
Zakres temperatur pracy			T	−40…+80°C	−40…+80°C	−40…+80°C
Przekrój przewodów			s	0,5…1,5 mm²	0,5…1,5 mm²	0,5…1,5 mm²
Wymiary				10×65 mm	10×65 mm	20×65 mm
Numer katalogowy				**203 015**	**204 015**	**205 015**

*Tab. 1. Parametry techniczne ograniczników przepięć serii RST AL. * Napięciowy poziom ochrony między zaciskami 1_p – GND i 2_p – GND*

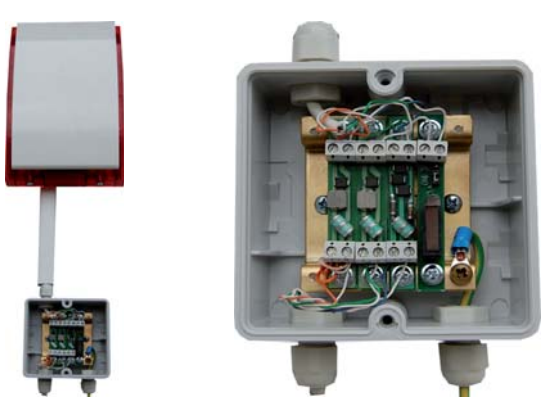


Fot. 3. Złącze ochrony przed przepięciami manipulatora

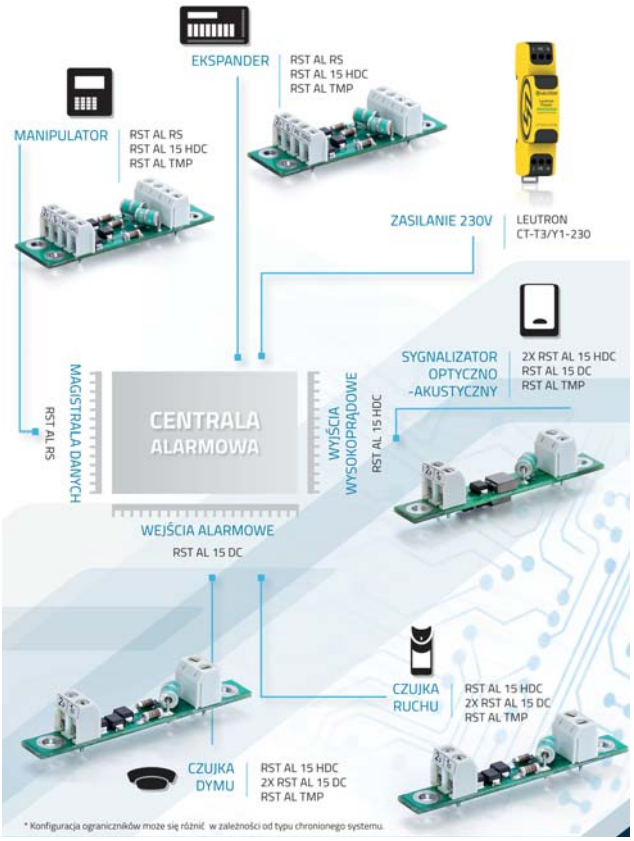
RST AL 15 HDC do zabezpieczenia zasilania urządzenia oraz modułu RST AL RS chroniącego magistralę transmisji danych. Dodatkowo układ wyposażono w moduł RST AL TMP do sygnalizacji sabotażu, włączony do obwodu sygnalizacji sabotażu magistrali. Wszystkie moduły umieszczone są w obudowie o rozmiarze 89×66×30 mm do zastosowań wewnątrz budynku. Na fotografii 4 przedstawiono z kolei przykład zabezpieczenia zewnętrznego sygnalizatora optyczno-akustycznego. Złącze ochrony przed przepięciami składa się w tym przypadku z dwóch modułów RST AL 15 HDC – do ochrony obwodów sygnalizacji akustycznej i sygnalizacji optycznej – oraz jednego modułu RST AL 15 DC, chroniącego obwód sygnalizacji sabotażu sygnalizatora, do którego włączony jest także moduł RST AL TMP. Moduły RST AL umieszczono w tym przypadku w obudowie o wymiarach 98×98×58 mm o podwyższonym stopniu ochrony IP 55 do zastosowań zewnętrznych. Złącza ochrony central alarmowych ze względu na znacznie większą liczbę chronionych linii wymagają już większych obudów. Na fotografii 1 przedstawiono przykładowy układ zabezpieczający centralę zarówno od strony zasilania 230 V, jak i 26 linii SSWiN. Przy tak dużej liczbie chronionych linii zastosowanie serii RST AL pozwala na ograniczenie rozmiarów układu ochronnego. W zależności od złożoności systemu alarmowego obudowa może być dobrana do dowolnej liczby chronionych linii.

6. Podsumowanie

Ochrona przed przepięciami pozwala na zwiększenie niezawodności systemów alarmowych, a tym samym na zwiększenie bezpieczeństwa chronionego obiektu. Prawidłowo zabezpieczony SSWiN zapewnia skuteczną i bezprzerwową pracę na-



Fot. 4. Złącze ochrony przed przepięciami sygnalizatora



Rys. 3. Schemat zabezpieczeń przed przepięciami systemu SSWiN

wet w trudnym środowisku elektromagnetycznym. Aby ułatwić instalację i prawidłowe działanie zabezpieczeń przed przepięciami, ochrona powinna być uwzględniana już na etapie projektowania obiektu.

dr inż. Tomasz Maksimowicz

RST Sp.j. M. Zielenkiewicz, W. Nietupski, A. Wojtkowski
ul. Myśliwska 2
15-569 Białystok
www.rst.pl; rst@rst.pl

Bibliografia

1. PN-EN 50130-4:2012 Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych.
2. PN-EN 62305-1 Ochrona odgromowa – Część 1: Zasady ogólne.
3. PN-EN 61643-21:2004 Niskonapięciowe urządzenia ograniczające przepięcia – Część 21: Urządzenia do ograniczania przepięć w sieciach telekomunikacyjnych i sygnalizacyjnych – Wymagania eksploatacyjne i metody badań.
4. PN-EN 61643-11:2006 Niskonapięciowe urządzenia do ograniczania przepięć – Część 11: Urządzenia do ograniczania przepięć w sieciach rozdzielczych niskiego napięcia – Wymagania i próby.

CA-5 Plus SET

Wygoda i bezpieczeństwo w zestawie

SATEL

Ewolucja jest czymś nieuniknionym, gdy celem jest rozwój. Nic więc dziwnego, że nawet najlepsze wytwory ludzkiego umysłu i ludzkich rąk po pewnym czasie ustępują miejsca nowym technologiom. Zwłaszcza, gdy są one jeszcze lepsze i bardziej innowacyjne od swoich poprzedników, a także mają niedostępne wcześniej funkcje i umożliwiają tworzenie nowych rozwiązań

Nie inaczej jest w przypadku najwyższej jakości urządzeń firmy SATEL, która rozszerzyła swoją ofertę o interesujący produkt. Jest to CA-5 Plus SET, czyli zestaw urządzeń służących do budowy systemu alarmowego, składający się z 7 elementów. Podstawą całej instalacji jest CA-5 Plus, czyli centrala alarmowa i moduł komunikacyjny, a także oprogramowanie przeznaczone dla obu tych urządzeń oraz obudowa. Uzupełnienie zestawu stanowią: czterozakresowa antena, manipulator LCD oraz specjalny kabel do łączenia urządzeń.

Potrójny zestaw korzyści

Innowacyjność CA-5 Plus SET przejawia się w wielu różnych aspektach. Po pierwsze, jest to zestaw, czyli specjalnie skonstruowany pakiet dopasowanych do siebie i idealnie współpracujących ze sobą urządzeń. Takie rozwiązanie znacznie ułatwia instalację systemu, a także programowanie urządzeń wchodzących w jego skład i dostosowywanie ich funkcji do naszych potrzeb.

Po drugie, wszystkie elementy zestawu nie tylko tworzą świetnie działającą całość, lecz każdy z osobna jest najwyższej jakości urządzeniem spełniającym oczekiwania najbardziej wymagających użytkowników. W skład CA-5 Plus SET wchodzą bowiem m.in. udoskonalone wersje uznanych urządzeń marki SATEL.

Po trzecie, CA-5 Plus SET to wygodne rozwiązanie dla osób poszukujących prostego, szybkiego w montażu i niezawodnego systemu alarmowego z rozbudowanymi funkcjami komunikacyjnymi. Dzięki odpowiednio skonstruowanej budowie poszczególnych elementów oraz ich właściwościom idealne sprawdzi się w ochronie małych i średniej wielkości obiektów.

CA-5 Plus SET od podszewki

Jak już wcześniej wspomniano, bazę zestawu stanowi pakiet CA-5 Plus, składający się z m.in. z centrali alarmowej CA-5 P Plus. Jest ona udoskonaloną wersją centrali CA-5 P, znanej i cenionej zarówno przez instalatorów, jak i przez użytkowników. Drugim elementem składowym CA-5 Plus jest moduł komunikacyjny GPRS-T1 Plus, który powstał na bazie GPRS-T1, czyli konwertera sygnałów do systemów monitoringu

Fot. 1. Pakiet CA-5 Plus

Fot. 2. Zestaw CA-5 Plus SET

na komunikaty transmitowane przez GPRS/SMS. Wersja Plus ma nowe funkcje, takie jak np. sterowanie za pomocą SMS.

Do obu nowych urządzeń stworzone zostało specjalistyczne oprogramowanie CA5T1, czyli program do konfiguracji i zarządzania zarówno centralą, jak i modułem. CA5T1 posiada bardzo przyjazną dla użytkownika strukturę danych. Dzięki niej można zaprogramować system alarmowy krok po kroku i nie jest to trudne. Rozwiązania zastosowane w CA5T1 umożliwiają znaczne skrócenie czasu potrzebnego do wykonania wszelkich czynności związanych z programowaniem systemu.

CA-5 Plus składa się z jeszcze jednego, nie mniej ważnego elementu. Jest nim obudowa OPU-4 P, która ma wiele bardzo przydatnych cech, takich jak m.in. podwójne zabezpieczenie antysabotażowe. Co więcej, konstrukcja obudowy umożliwia zainstalowanie w jej wnętrzu urządzeń bezprzewodowych z antenami. Właściwość ta została wykorzystana przez inżynierów firmy SATEL, którzy, tworząc zestaw CA-5 Plus SET, dołączyli do niego także czterozakresową antenę ANT-OBU-Q. Ostatnim umieszczanym w obudowie elementem zestawu CA-5 Plus SET jest specjalny kabel – RJ/PIN3-GPRS. Umożliwia on wymianę danych między centralą alarmową CA-5 P Plus a modułem GPRS-T1 Plus, dzięki czemu zapewnia prawidłową pracę obu tych urządzeń. Co istotne, kabel ten jest dostępny tylko w zestawie.

Żaden system alarmowy nie może być pozbawiony urządzenia umożliwiającego sterowanie i zarządzanie. Z tego powodu wśród elementów składających się na zestaw do budowy systemu alarmowego CA-5 Plus SET jest także funkcjonalny i prosty w obsłudze manipulator CA-5 KLCD-S. Jest on wyposażony w wyświetlacz LCD, na którym prezentowane są komunikaty tekstowe, a także w jasne diody LED informujące o stanie systemu. Dzięki temu możliwe jest intuicyjne i wygodne korzystanie z funkcji centrali. Manipulator został wyposażony również w podświetlenie wyświetlacza i klawiszy. Ponadto sygnalizuje dźwiękowo wybrane zdarzenia w systemie i powiadamia o utracie łączności z centralą.

Fot. 3. Zarządzanie systemem poprzez wiadomości SMS

Zdalne zarządzanie systemem – SMS i nie tylko

Zastosowanie zestawu składającego się z tak wielu najwyższej jakości urządzeń to nie tylko świetny sposób na stworzenie całego systemu alarmowego. Zainstalowanie wszystkich elementów wchodzących w skład CA-5 Plus SET sprawia, że zyskują one zupełnie nowe funkcje. Dzięki wykorzystaniu GPRS możemy np. z dowolnego miejsca na świecie zaprogramować zarówno naszą centralę alarmową CA-5 P Plus, jak i moduł komunikacyjny GPRS-T1 Plus. W ten sposób możemy zdalnie zmienić m.in. czas na wejście lub wyjście, a także numer telefonu, na który wysyłane będą powiadomienia skierowane do klienta. Co więcej, możemy także wygodnie wysyłać informacje o zdarzeniach do stacji monitorowania – poprzez SMS/GPRS albo za pomocą wbudowanego dialera centrali, przez analogową linię telefoniczną (PSTN).

Zestaw CA-5 Plus SET oferuje także inne, dodatkowe możliwości zarządzania centralą CA-5 P Plus poprzez wiadomości SMS. Za ich pośrednictwem możemy zdalnie załączyć lub wyłączyć czuwanie, kasować alarmy, zablokować lub odblokować wybrane wejście oraz – również na odległość – zmienić hasło dostępu. Dzięki Short Message Service można także otrzymywać wysyłane na telefon komórkowy powiadomienia o zdarzeniach i zdalnie kontrolować za pomocą telefonu stan systemu. To jednak nie wszystko – zainstalowanie wszystkich urządzeń wchodzących w skład CA-5 Plus SET sprawia, że informacja o statusie modułu GPRS-T1 Plus może być wyświetlana na wyświetlaczu manipulatora LCD przyłączonego do centrali.

Zastosowanie zestawu CA-5 Plus SET jest świetnym rozwiązaniem dla osób poszukujących prostego i funkcjonalnego systemu alarmowego. Tę bazę możemy rozbudować, dobierając pozostałe wymagane elementy systemu, takie jak transformator, akumulator, czujki, sygnalizatory, i tym samym dopasowując funkcjonalność całej instalacji do danego obiektu i potrzeb jego użytkowników.

SATEL

Fot. 4. Schemat CA-5 Plus SET

Systemy alarmowe **Satel**

CA-5 Plus SET
elastyczny i funkcjonalny

NOWOŚĆ

CA-5 Plus SET to idealna baza do zbudowania solidnego i kompleksowego systemu alarmowego.

Zestaw ten umożliwia zdalne sterowanie centralą, odczytywanie jej stanów, a także monitorowanie poprzez SMS/GPRS. Stanowi dogodne rozwiązanie dla osób poszukujących niezawodnego systemu do zabezpieczania małych obiektów, który można szybko i prosto zamontować.

Umożliwia także wygodną rozbudowę poprzez dodawanie kolejnych elementów z szerokiej oferty produktowej SATEL.

Zestaw
do **budowania** systemu alarmowego

Więcej informacji na
www.satel.pl

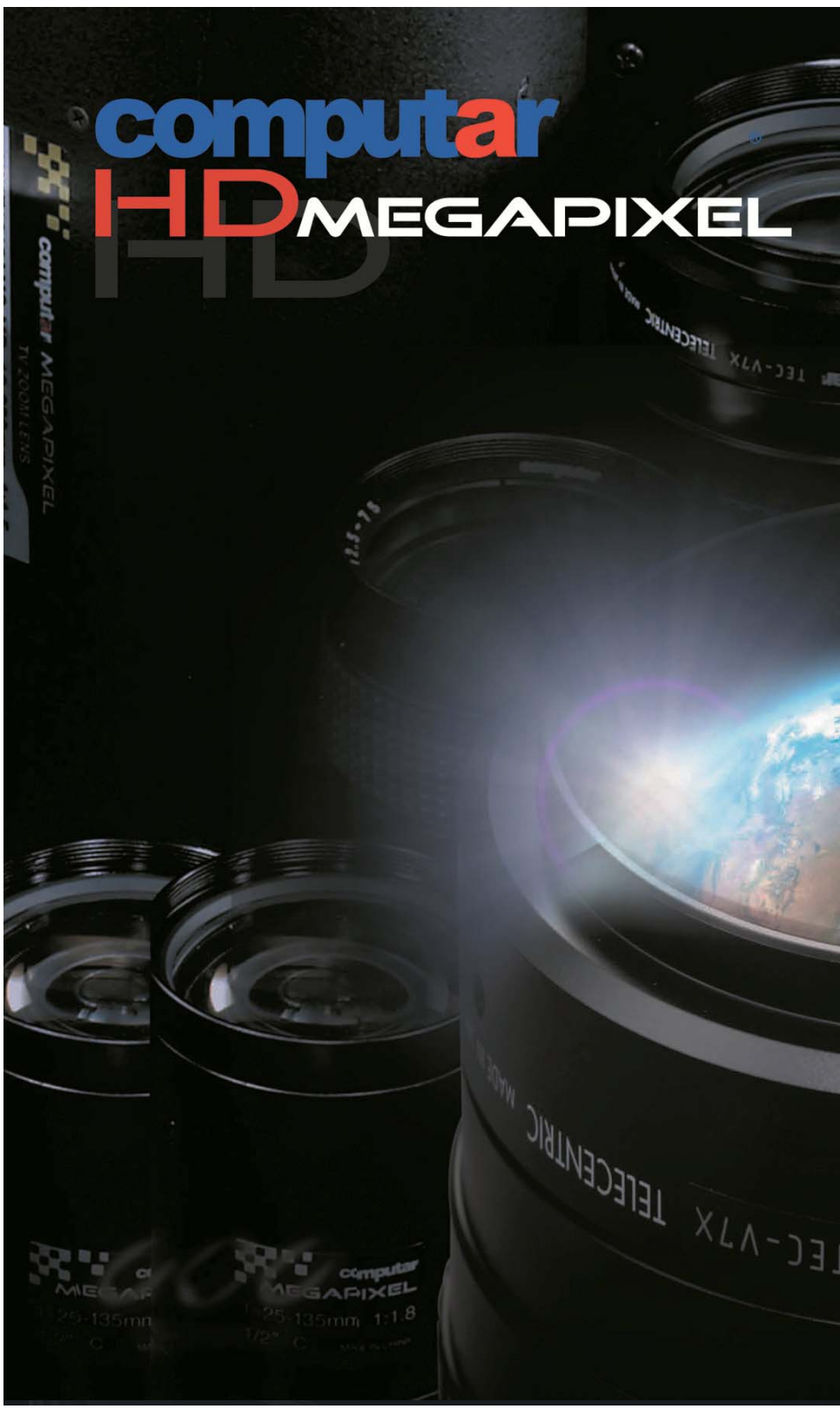
Satel Sp. z o.o.
ul. Budowlanych 66, 80-298 Gdańsk, tel.: (58) 522 66 00, fax: (58) 522 66 94 01,
e-mail: satel@satel.pl, **www.satel.pl**

Satel®

COMPUTAR – 40 lat na rynku CCTV

CBC Group

Od ponad 40 lat urządzenia marki COMPUTAR, należącej do CBC Group, utrzymują czołowe pozycje na świecie w dziedzinie optyki przemysłowej stosowanej w różnych branżach, m.in. w systemach CCTV, w sektorze obronności, w motoryzacji, w przemyśle i kontroli procesów produkcyjnych, w inteligentnych systemach transportowych oraz w wielu innych dziedzinach. Szczególnie w branży CCTV urządzenia COMPUTAR uchodzą za pionierskie rozwiązania z zakresu profesjonalnej optyki przeznaczonej do systemów dozoru wizyjnego. Bez względu na specyfikę i wymagania systemu, w bardzo bogatym asortymencie produktów tej marki można znaleźć obiektyw odpowiedni do każdego zastosowania



Już w 1974 roku japoński koncern CBC Group zaczął produkować profesjonalne urządzenia optyczne, wprowadzając na rynek innowacyjne obiektywy CCTV, które deklasowały konkurencję pod względem jakości i precyzji wykonania. W tym samym roku została stworzona marka COMPUTAR jako zastrzeżony znak towarowy należący do CBC Group. Dzięki solidnym podstawom technologicznym, bazującym na japońskiej inżynierii oraz precyzyjnych maszynach produkcyjnych, w ciągu kilku kolejnych lat marka COMPUTAR stała się doskonale znana na światowym rynku jako synonim najwyższej jakości i precyzji.

W roku 1985 rozpoczęto seryjną produkcję i dystrybucję pierwszych obiektywów COMPUTAR typu motor-zoom, które w niedługim czasie zyskały dużą popularność w tzw. systemach obserwacji dalekiego zasięgu.

W roku 1993 firma COMPUTAR rozpoczęła produkcję i sprzedaż obiektywów o zmiennej ogniskowej regulowanej ręcznie. Już wkrótce, dzięki uniwersalności oraz łatwości w dopasowaniu kąta widzenia do wymagań klienta, ta grupa obiektywów okazała się najpopularniejsza na rynku. Pierwszy na rynku asferyczny, zmiennoogniskowy obiektyw o współczynniku apertury F1.0 (tzw. „superjasny") został wprowadzony właśnie pod marką COMPUTAR.

Obecnie do CBC Group należą cztery fabryki produkujące precyzyjne urządzenia optyczne, w tym obiektywy do CCTV, modele standardowe i megapikselowe, motor-zoom, MFZ, otworkowe oraz termowizyjne.

W ostatnich latach marka COMPUTAR umacnia swoją pozycję również w innych sektorach, m.in. Machine Vision (modele typu makro, telecentryczne), Factory Automation, ITS.

Na szczególną uwagę zasługuje kilka oferowanych nowości, m.in. obiektyw **E24Z1018PDC-MPIR** przeznaczony do systemów CCTV. Jest to 24-krotny motor-zoom z korekcją ostrości w podczerwieni, o ogniskowej regulowanej w zakresie od 10 mm do 240 mm i rozdzielczości 3 megapikseli przeznaczony do kamer z mocowaniem C, o przekątnej przetwornika maks. 1/1.8". Jasność tego obiektywu (min. wartość liczby F) wynosi 1.8, przysłona jest automatycznie regulowana prądem stałym (DC-Iris), a ponadto obiektyw jest wyposażony w układ służący do pomiaru aktualnego ustawienia ogniskowej i ostrości, niezbędny do obsługi funkcji presetów. Obiektyw jest zbudowany z siedemnastu szklanych soczewek. Korpus oraz obudowa są wykonane z metalu.

M5020FIC-MPIR to obiektyw przeznaczony przede wszystkim do systemów ITS. Ma stałą ogniskową równą 50 mm oraz korekcję ostrości w podczerwieni. Rozdzielczość wynosi 5 megapikseli. Obiektyw jest wyposażony w ręcznie regulowaną przysłonę i jest przeznaczony do kamer z mocowaniem C, o przekątnej przetwornika maks. 1/2,5". Jasność tego obiektywu (min. wartość liczby F) wynosi 2,0. Obiektyw jest zbudowany z jedenastu szklanych soczewek. Korpus i obudowa są wykonane z metalu. Masa obiektywu wynosi 155 g, a jego wymiary zewnętrzne to 60×46,5 mm.

M3520-MPW2 to z kolei model o bardzo kompaktowej konstrukcji, przeznaczony m.in. do systemów Machine Vision. Ma stałą ogniskową równą 35 mm oraz rozdzielczość 5 megapikseli. Obiektyw jest wyposażony w ręcznie regulowaną przysłonę i jest przeznaczony do kamer z mocowaniem C, o przekątnej przetwornika maks. 1/2,5". Jasność tego obiektywu (min. wartość liczby F) wynosi 2,0. Obiektyw jest zbudowany z sześciu szklanych soczewek. Korpus i obudowa są wykonane z metalu. Masa obiektywu to zaledwie 60 g dzięki jego bardzo kompaktowym wymiarom (45×28,5 mm).

Asortyment oferowanych obiektywów motor-zoom został wzbogacony w modele megapikselowe, szczególnie cenione w systemach wymagających dużych zbliżeń i zarazem wysokiej jakości obrazu. Do najbardziej złożonych obiektywów należą serie **H21Z1016MP** (10–210 mm, 2 MP, 1/2"), **E24Z1018-MPIR** (10–240 mm, 3 MP, 1/1.8", korekcja IR), **H35Z1015MP** (10–350 mm, 2 MP, 1/2") oraz **H62Z1235-MP** (12,5–775 mm, 2 MP, 1/2"). Ta ostatnia seria została dodatkowo wyposażona w innowacyjną funkcję *fog-through*, dzięki której eliminowane są ograniczające widoczność zakłócenia wywoływane przez takie czynniki jak mgła, zadymienie, śnieg, burza piaskowa itp. Optyka wraz z wbudowanym zespołem filtrów jest sterowana przez procesor służący do analizy obrazu, co nawet w warunkach skrajnie trudnych gwarantuje widoczność nieosiągalną dla konwencjonalnych obiektywów. Są to specjalistyczne obiektywy rekomendowane do obserwacji rozległych obszarów (monitorowanie lasów, granic, lotnisk itp.), z bardzo dużym powiększeniem optycznym.

Asortyment oferowanych obiektywów COMPUTAR jest ciągle powiększany. Produkty są doskonalone z wykorzystaniem najnowszych osiągnięć technologicznych oraz światowej wiedzy inżynierskiej. Aktualna oferta jest przedstawiona na stronie *www.computar-global.com* oraz na stronie polskiego oddziału CBC Group – *www.cbcpoland.pl*.

CBC Group

Jak poznać motywację klienta?

Johan Åkesson

Sieć kamer IP jest czymś więcej niż narzędziem pozwalającym stwierdzić, kto wszedł do sklepu, a kto z niego wyszedł. Z kamerami mogą współpracować inteligentne aplikacje ułatwiające zrozumienie, czym kierują się ludzie na zakupach. Ta wiedza umożliwia poprawę wyników sprzedaży

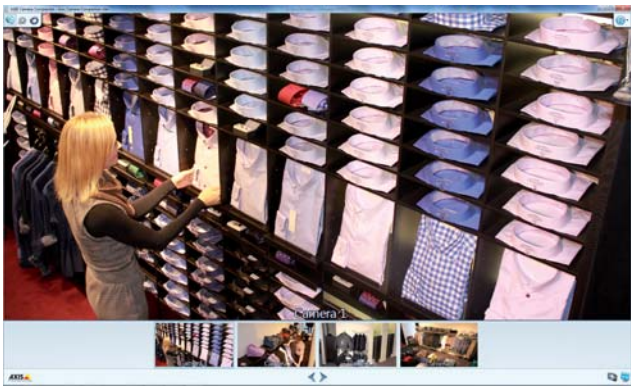
Są sieci handlowe, w których prowadzona jest stała analiza sektora handlu detalicznego pod kątem zachowania się klientów na terenie sklepów, ich świadomych i podświadomych reakcji oraz czynników wpływających na podejmowanie decyzji podczas zakupów. Firmy wykorzystują obrazy z kamer pracujących w wizyjnym systemie dozorowym do kontrolowania sprzedaży określonych produktów oraz do analizy ruchu na wyznaczonych obszarach sklepów. Stwierdzono, że w przypadku takiej działalności decydujące znaczenie ma jakość obrazów dostarczanych przez kamery, ich dostępność oraz możliwość przemieszczania kamer w zależności od potrzeb.

Takie wymagania spełniają kamery IP, które mogą „towarzyszyć" klientom podczas zakupów –w niezauważalny sposób, na całym obszarze sklepu. Na podstawie analizy obrazów z kamer IP można oceniać, jak długo klienci przebywają w pobliżu półek, na których znajdują się dane produkty, stwierdzić, czy klienci czytają informacje zamieszczane na opakowaniach, a także sprawdzić, czy mają problemy z odnalezieniem określonych produktów. Wszystkie te czynniki mogą być brane pod uwagę podczas aranżacji przestrzeni sklepowej i mają znaczny wpływ na wyniki sprzedaży.

W podobny sposób inne aplikacje mogą być wykorzystane do wyznaczania tras, po których najczęściej poruszają się klienci, i tworzenia tak zwanych map cieplnych, które dostarczają czytelnych informacji dla pracowników sklepu i umożliwiają wybór miejsca ekspozycji najbardziej poszukiwanych towarów. Dane uzyskane w wyniku analizy map cieplnych pozwalają na wyznaczenie miejsc na terenie sklepu, w których należy wystawiać towary kupowane przeważnie w pośpiechu, a także miejsc, w których zagęszczenie klientów może być nadmierne (likwidacja takich zatorów także prowadzi do zwiększenia sprzedaży).

Obrazy z kamer IP mogą być przydatne także do kontroli pracy punktów kasowych i rozładowywania kolejek. Najnowsze badania przeprowadzone na terenie Wielkiej Brytanii przez bank Barclays wykazały, że jedna piąta potencjalnych nabywców rezygnuje z zakupów, gdy musi stać w kolejce ponad dwie minuty, a dwie trzecie w ogóle nie robi zakupów, jeżeli kolejka do kasy jest długa. Stwierdzono także, że ponad połowa potencjalnych nabywców nawet nie wchodzi do sklepu, jeżeli już przy wejściu widoczne są

Fot. 1. Axis Camera Companion zapewnia ostry i przejrzysty obraz w standardzie HDTV



Fot. 2. Interfejs graficzny wizyjnego systemu dozorowego Axis Camera Companion

kolejki do kas. Ma to bardzo zły wpływ na ostateczny wynik finansowy w handlu detalicznym.

By usprawnić pracę punktów kasowych, można wykorzystać obrazy z kamer IP oraz aplikacje dostarczające danych na temat długości tworzących się kolejek, średniego czasu oczekiwania oraz czasu poświęcanego na rozliczenie klientów. Na tej podstawie można wyznaczyć optymalną liczbę czynnych punktów kasowych oraz liczbę osób obsługujących klientów. Przekłada się to na realne korzyści finansowe związane ze wzrostem sprzedaży w godzinach największego ruchu. Taki system pracy umożliwia osobom zarządzającym sklepem przewidywanie potencjalnych komplikacji i uniknięcie sytuacji wymykających się spod kontroli.

Kontrola ruchu osób przeprowadzana z wykorzystaniem aplikacji zliczających ludzi widocznych na danym obszarze pozwala pracownikom sklepu na optymalizację procesu obsługi klientów, a także dostarcza narzędzi umożliwiających szybką ocenę skuteczności akcji promocyjnych oraz wysiłków związanych z marketingiem. Informacje na ten temat i inne dane mogą być pobrane z systemu zarządzającego pracą sklepu, pracującego w tej samej sieci co wizyjny system dozorowy, przez co są jednocześnie dostępne dla wielu użytkowników. Dzięki temu nie zachodzi konieczność ręcznej obróbki jakichkolwiek danych. Informacje statystyczne z wielu punktów sprzedaży mogą być sprawdzane i przetwarzane w czasie rzeczywistym w jednostce nadrzędnej, co umożliwia podejmowanie natychmiastowych działań doraźnych lub długoterminowych.

Wskaźnikiem skuteczności działania punktu handlowego jest współczynnik konwersji rozumiany jako stosunek liczby osób odwiedzających daną placówkę handlową do liczby osób, które dokonały zakupów. Obserwacja bieżących wartości współczynników konwersji umożliwia szybką ocenę metod oraz procedur stosowanych w celu zwiększenia sprzedaży w poszczególnych sklepach.

Wykorzystanie różnorodnych aplikacji analizujących obrazy z kamer IP pozwala osobom zarządzającym placówkami handlowymi zrozumieć decyzje klientów. Jest to bardzo skuteczny sposób poprawiania wyników sprzedaży i uzyskiwania wyraźnej przewagi nad konkurencją, która nie stosuje takich metod zarządzania.

Johan Åkesson
Business Development Director Retail
Axis Communications

Seria kamer sieciowych Bosch MIC 7000 HD

Rejestrowanie ważnych szczegółów także w ekstremalnie trudnych warunkach

Michał Biela

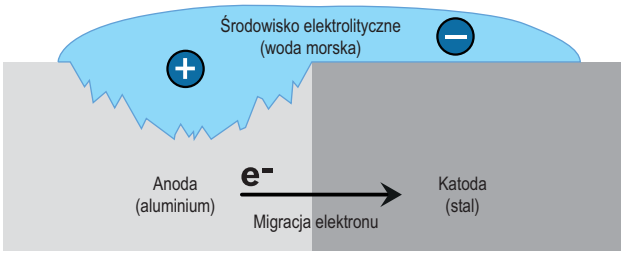
Firma Bosch oferuje nową serię kamer sieciowych PTZ MIC 7000 HD. Dostępne są dwa modele kamer MIC starlight 7000 HD i MIC dynamic 7000 HD. Kamera MIC starlight 7000 HD wytwarza obraz o rozdzielczości HD 720p z prędkością 60 klatek na sekundę. Czułość tej kamery w trybie czarno-białym wynosi 0,01 luksa. To wartość, przy której inne kamery nie mogłyby wytwarzać czytelnego obrazu. Kolorowy obraz o rozdzielczości HD jest wytwarzany przy oświetleniu równym 0,05 luksa. W takich warunkach inne kamery mogłyby wytwarzać tylko obraz czarno-biały. Dokładne odtwarzanie kolorów ułatwia ocenę sytuacji z punktu widzenia bezpieczeństwa. Możliwość obserwacji szybko poruszających się obiektów oraz wysoka jakość obrazu przy bardzo słabym oświetleniu sprawiają, że kamery MIC IP starlight 7000 HD mogą być wykorzystane w najtrudniejszych warunkach oświetleniowych.

Z kolei kamera sieciowa MIC dynamic 7000 HD oferuje rozdzielczość 1080p i wytwarza bogaty w szczegóły obraz zarówno w bardzo jasno oświetlonych, jak i w zaciemnionych miejscach. Duży zakres dynamiki oraz inteligenta kompensacja światła padającego wprost na obiektyw zapewniają optymalne zobrazowanie obserwowanych obiektów i ułatwiają ich identyfikację w zróżnicowanych warunkach oświetleniowych. W celu dodatkowego zwiększenia wyrazistości i podwyższenia jakości obrazu obydwie kamery mają funkcję automatycznego przeciwdziałania efektowi mgły. Dzięki temu możliwe jest dynamiczne dopasowywanie trybu pracy kamery i zapewnienie najwyższej jakości obrazu także w warunkach zamglenia lub zadymienia. Rozpoznawanie istotnych obiektów w całkowitej ciemności umożliwiają dodatkowe oświetlacze MIC. Dysponują one dwoma źródłami światła: emiterami podczerwieni i światła białego. Operator systemu może zmienić rodzaj oświetlenia za pomocą myszki komputerowej. Oświetlacze mają bardzo duży zasięg, który wynosi 175 metrów.

Fot. 1. Kamera MIC z zamontowanymi oświetlaczami

Omawiane kamery są przygotowane do pracy w ekstremalnie trudnych warunkach eksploatacyjnych. Wyróżniają się wysoką jakością obrazu o rozdzielczości HD oraz wytrzymałą obudową, zgodną z normami IP68 i NEMA 6P. Firma Bosch certyfikuje swoje kamery zgodnie z tymi normami. Pierwsza z nich, IP (od *Ingress Protection*), oznacza stopień odporności i jest uznawana praktycznie na całym świecie. Dwie występujące po oznaczeniu „IP" cyfry precyzyjnie oznaczają stopień szczelności danego produktu, który odpowiada określonym warunkom środowiskowym. Pierwsza z nich odnosi się do wnikania ciał stałych do wnętrza obudowy, natomiast druga do przedostawania się wody. „IP68" w przypadku kamery MIC oznacza, że jest ona całkowicie odporna na wnikanie ciał stałych oraz odporna na długotrwałe zanurzenie w wodzie (zgodnie z normą głębokość maksymalna wynosi w tym przypadku 1 m). Testy zgodności według NEMA (National Electrical Manufacturers Association) są popularne w Stanach Zjednoczonych. Oznaczenie „NEMA 6P" jest tożsame z „IP68". Na uwagę zasługuje również fakt, że taki poziom hermetyczności kamery został osiągnięty bez zastosowania obudowy ciśnieniowej. Obudowy ciśnieniowe są czasami wykorzystywane w celu osiągnięcia wysokiego stopnia odporności na wpływy środowiskowe. Taka obudowa jest wypełniona gazem pod ciśnieniem wyższym od ciśnienia panującego na zewnątrz o około 0,3–1,4 bara (zależne od modelu). Najczęściej używanym gazem jest suchy azot. Obudowy ciśnieniowe mają skomplikowaną konstrukcję i wymagają częstych przeglądów konserwacyjnych oraz okresowego uzupełniania gazu, co przyczynia się do wzrostu kosztów eksploatacji. Tych wad nie mają kamery Bosch MIC IP 7000.

Kolejny aspekt to odporność na korozję. Jeśli chce się wybrać kamerę, która może pracować w różnych warunkach środowiskowych, należy sprawdzić, z czego i jak został wykonany dany produkt. W tej klasie kamer znajdziemy produkty zróżnicowane cenowo.

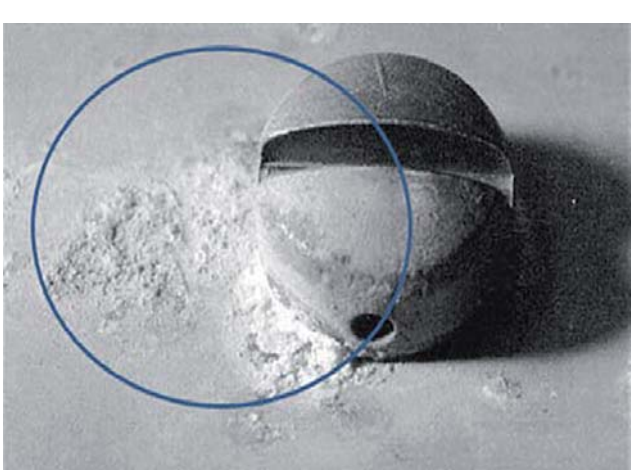


Rys. 1. Proces korozji elektromechanicznej

Kamery pracujące na zewnątrz budynków muszą być skonstruowane z materiałów o odpowiedniej jakości oraz wytrzymałości. Muszą być dostatecznie odporne na silne podmuchy wiatru, opady atmosferyczne i czynniki powodujące korozję.

Korozja elektromechaniczna to zjawisko, które powstaje wskutek różnic potencjałów na powierzchniach materiałów (obudowy) znajdujących się w danym środowisku. Korozja to fizykochemiczne oddziaływanie między środowiskiem i metalem, w którego wyniku zachodzą niekorzystne zmiany właściwości tego metalu. Dlaczego dochodzi do korozji? Obudowa kamery jest wykonana z materiału, który na etapie produkcji może być zanieczyszczony drobinkami obcego metalu. Przyczynia się to do powstania ogniw galwanicznych, gdzie elektrolitem może być np. skroplona para wodna. Dochodzi wtedy do reakcji z dwutlenkiem węgla zawartym w atmosferze. W wyniku takiej reakcji tworzy się kwas węglowy. Kolejnym przykładem elektrolitu jest rozpuszczony w wodzie dwutlenek siarki, emitowany do atmosfery na skutek spalania paliwa w silnikach samochodowych. Wskutek takiej reakcji tworzy się kwas siarkowy. W wyniku zetknięcia się różnych metali z elektrolitem powstają ogniwa korozyjne, w których materiał o wyższym potencjale zachowuje się jak elektroda dodatnia, czyli anoda. Na takim elemencie będzie zachodziło utlenianie, podczas którego atomy, cząsteczki lub jony będą traciły elektrony. Na fragmentach elementu o niższym potencjale zostaje wytworzona elektroda ujemna zwana katodą, gdzie będzie dochodziło do procesu redukcji, podczas którego atomy, cząsteczki lub jony będą pobierały elektrony.

Nie zawsze powodem korozji musi być zanieczyszczony metal. Takie zjawisko może również powstać na skutek połączenia dwóch metali, np. śrub mocujących obudowę wykonanych ze stali nierdzewnej, połączonych z aluminiowym korpusem. Zjawisko to nosi nazwę korozji stykowej. Pomiędzy dwa metale, które mają zróżnicowane potencjały, wdziera się woda i jako roztwór różnych elektrolitów tworzy ogniwo galwaniczne, co powoduje przepływ prądu i utlenianie elementu o wyższym potencjale.



Fot. 2. Skutki korozji stykowej

Rysunek 1 pokazuje migrację elektronu z metalu o wyższym potencjale (anody), np. stali, do metalu o niższym potencjale (katody), np. aluminium. W tym przypadku woda morska jest elektrolitem.

Fotografia 2 przedstawia skutki korozji stykowej. Na jednym elemencie będą występowały ubytki materiału, natomiast na drugim może pojawiać się warstwa obcego metalu. Jednym z przykładów ochrony przed korozją jest dobranie odpowiedniego, mało podatnego na korozję materiału do produkcji kamery. Walcząc z korozją, można również wybierać stopy danego metalu lub też zabezpieczać metal zewnętrzną powłoką antykorozyjną.

Podsumowując powyższe rozważania, należy stwierdzić, że w wyniku korozji następuje pogorszenie działania kamery, a w skrajnych przypadkach całkowite jej uszkodzenie.

Kamery MIC IP 7000 HD zostały starannie zaprojektowane i zbudowane z użyciem materiałów wysoce odpornych na korozję. Do produkcji obudów tych kamer został użyty stop aluminium. Dodatkowo każda część metalowa została pokryta specjalnym środkiem, powszechnie stosowanym w motoryzacji, stanowiącym dodatkową powłokę antykorozyjną.

Obudowa kamery jest wykonana ze stopu odpornego na korozję, jednak nie eliminuje to opisanego powyżej zjawiska korozji elektromechanicznej powstającej na styku dwóch metali. Kamera wykonana ze stopu, przymocowana do podłoża np. stalowymi śrubami, mogłaby ulec korozji elektrochemicznej.

Aby temu zapobiec, na etapie produkcji zastosowano następujące środki zapobiegawcze:

– użyto stopu cynku wysoce odpornego na działanie korozji elektrochemicznej,
– każda aluminiowa część w kamerze jest pokryta specjalną zewnętrzną warstwą ochronną, dzięki czemu podczas instalacji kamery poszczególne części będą skutecznie odizolowane od metalu drugiego typu.

Dodatkowo kamery MIC IP 7000 zostały przetestowane na zgodność ze standardem ASTM B117. Poddano je badaniom w komorze solnej. Próba trwała dwa tysiące godzin. Wynik testu odzwierciedlał bardzo wysoką odporność na korozję. Niemniej w środowiskach narażonych na działanie takich czynników jak roztwory soli Bosch zaleca stosowanie produktów wykonanych ze stali nierdzewnej.

Kamery MIC 7000 HD są przeznaczone przede wszystkim do zastosowań zewnętrznych. Oferują najwyższej jakości obraz i można je wykorzystywać m.in. do monitorowania centrów miast oraz elementów infrastruktury o znaczeniu krytycznym. Kamery są optymalnie przygotowane do pracy w bardzo trudnych warunkach środowiskowych, np. w temperaturach od -60 do +60 stopni Celsjusza oraz przy wilgotności dochodzącej do 100%. Są całkowicie odporne na deszcz, śnieg, pył, uderzenia wiatru i silne wstrząsy.

Michał Biela
Bosch Security Systems

Uchwyć nawet najdrobniejszy szczegół z **30-krotnym** zoomem optycznym

Inteligentne śledzenie obiektów w ruchu 24 godz/dobę. Kamery AUTODOME IP 7000 STARLIGHT oraz DYNAMIC zapewniają ciągłą ochronę niezależnie od warunków oświetleniowych, pory dnia czy dynamiki sceny. Technologia starlight dostarcza użyteczny obraz w sytuacji, gdy inne kamery nie rejestrują obrazu w ogóle. Model dynamic umożliwia identyfikację sceny zawierającej obszary ciemne jak i jasne. Technologia C-BIT (Content Based Imaging Technology) zapewnia inteligentne, adaptacyjne śledzenie obiektów poruszających się oraz doskonałe odwzorowanie sceny. Pozwala zredukować koszty archiwizacji i obciążenie sieci bez wpływu na jakość obrazu.

www.boschsecurity.pl

BOSCH
Technologia bliżej nas

Sygnalizatory zewnętrzne W2

Ta sama obudowa, różne możliwości

Szymon Ratajski

Nowe zewnętrzne akustyczno-optyczne sygnalizatory firmy W2, SGO-Pgz2 oraz SAOZ-Pk, spełnią oczekiwania wielu projektantów i instalatorów. Sygnalizatory te mają nowoczesną konstrukcję i estetyczny wygląd

Sygnalizatory SAOZ-Pk (sygnalizator akustyczno-optyczny) oraz SGO-Pgz2 (sygnalizator akustyczno-optyczny umożliwiający komunikowanie słowne) są z tej samej linii wzorniczej i na pierwszy rzut oka użytkownik nie jest w stanie odróżnić obu wyrobów (fot. 1). Pomimo tej samej obudowy urządzenia te zdecydowanie różnią się możliwościami, jakie oferują użytkownikowi.

Sygnalizator SAOZ-Pk, czyli „prosta" sygnalizacja akustyczno-optyczna

SAOZ-Pk to sygnalizator akustyczno-optyczny przeznaczony do sygnalizowania pożaru zarówno w wewnętrznych, jak i w zewnętrznych systemach sygnalizacji pożarowej. Jest wyposażony w przetwornik piezoceramiczny i lampę z palnikiem ksenonowym. Układ elektroniczny sygnalizatora jest umieszczony w obudowie wykonanej z niepalnego tworzywa sztucznego. SAOZ-Pk może być przyłączony do dowolnej centrali sygnalizacji pożarowej dostarczającej napięcia w zakresie 16–32,5 V_{DC}. Przyłączenie napięcia do zacisków sygnalizatora powoduje rozpoczęcie emisji sygnału akustycznego oraz impulsowego sygnału optycznego. Sygnalizator umożliwia emitowanie czterech różnych sygnałów alarmowych. Ponadto ma dwustopniową regulację głośności (próg 1: ok. 100 dB, próg 2: około 110 dB). Warto zwrócić uwagę na możliwość tworzenia sieci sygnalizatorów pracujących synchronicznie. Funkcja ta ma zasadnicze znaczenie w przypadku nagłaśniania większych obszarów lub pomieszczeń, w których sygnalizatory mogą oddziaływać na siebie akustycznie. W momencie uruchomienia alarmu dźwięk sygnalizatorów synchronizowanych jest czysty, wyraźny, odróżnialny od innych sygnałów akustycznych występujących w obiekcie. W przypadku zastosowania sygnalizatorów niezsynchronizowanych dźwięk jest mniej wyraźny i z powodu wzajemnego oddziaływania na siebie sygnalizatorów mogą wystąpić dudnienia. Tworzenie sieci sprowadza się do wykonania połączenia dodatkową żyłą synchronizującą oraz zmiany ustawień mikroprzełącznika znajdującego się w sygnalizatorze (tryb pracy *master*/*slave*). Synchronizowana jest tylko część akustyczna. Ciekawą opcją jest możliwość synchronizowania sygnalizatorów SAOZ-Pk z sygnalizatorami wewnętrznymi: akustycznym SA-K5N oraz akustyczno-optycznym SA-K7N. Utworzona sieć sygnalizatorów może być połączona z wyłącznikiem pożarowego sygnału dźwiękowego WSD-1. Wyłącznik może działać w dwojaki sposób: wyłączać całą sieć lub wybrane sygnalizatory (zgodnie z zasadą jeden sygnalizator – jeden wyłącznik WSD-1).

Sposób wyłączenia zależy od miejsca przyłączenia wyłącznika WSD-1 (przyłączony do sygnalizatora *master* wyłącza całą sieć, przyłączony do sygnalizatora *slave* – tylko jeden sygnalizator).

Sygnalizator SGO-Pgz2, czyli coś dla bardziej wymagających

SGO-Pgz2 to sygnalizator akustyczno-optyczny, który umożliwia odtwarzanie

Fot. 1. Sygnalizatory SAOZ-Pk oraz SGO-Pgz2

komunikatów głosowych – maksymalnie czterech komunikatów o łącznym czasie trwania 90 s. Należy pamiętać, że jako komunikat traktowany jest dowolny dźwięk.

Sygnalizator pracuje zgodnie z sekwencją opisaną w normie PN-EN 54-3/2003+A2:2007 *Systemy sygnalizacji pożarowej. Część 3: Pożarowe urządzenia alarmowe. Sygnalizatory akustyczne*. Jako źródło dźwięku zastosowano głośnik, dzięki czemu uzyskano wyraźny, czysty dźwięk o wysokiej jakości. Oprócz komunikatu słownego użytkownik ma do wyboru jeden z 15 sygnałów dźwiękowych (lub brak sygnału).

Niewątpliwą zaletą sygnalizatora jest możliwość prostego adresowania komunikatów. Użytkownik ma do dyspozycji zaciski sygnalizatora oznaczone jako +1, +2. Przyłączenie napięcia z zakresu 16–32,5 V_{DC} do odpowiednich styków powoduje uruchomienie emisji komunikatu (tab. 1).

Dzięki zastosowaniu tego typu rozwiązania możliwe jest tworzenie komunikatów „wielojęzycznych".

Parametry pracy sygnalizatora oraz treści komunikatów mogą być programowane za pomocą urządzenia nagrywającego UN-2 lub UN-3. W przypadku urządzenia UN-3 możliwe jest wgranie komunikatów bezpośrednio z pendrive'a, natomiast w przypadku urządzenia UN-2 – nagranie ich za pomocą wbudowanego mikrofonu lub zaczerpnięcie z zewnętrznego źródła sygnału (gniazdo jack 3,5 mm).

Sygnalizatory SGO-Pgz, podobnie jak SAOZ-Pk, umożliwiają tworzenie sieci sygnalizatorów pracujących synchronicznie. SGO-Pgz2 mogą współdziałać w ramach jednej sieci z wewnętrznymi sygnalizatorami głosowymi SG-Pgw oraz wyłącznikiem WSD-1.

Stan wejść	Komunikat
„+1": 24 V_{DC}, „+2": nie podłączony	Komunikat 1
„+1": nie podłączony, „+2": 24 V_{DC}	Komunikat 2
„+1": 24 V_{DC}, „+2": 24 V_{DC}	Komunikat 3

Tab. 1. Wybór komunikatu w zależności od stanu wejść

Nowe sygnalizatory a normy

SAOZ-Pk i SGO-Pgz2 spełniają wymagania zarówno normy PN-EN 54-3/2003+A2:2007 *Systemy sygnalizacji pożarowej. Część 3: Pożarowe urządzenia alarmowe. Sygnalizatory akustyczne*, jak również normy PN-EN 54-23:2010 *Systemy sygnalizacji pożarowej. Część 23: Pożarowe urządzenia alarmowe. Sygnalizatory optyczne* dotyczącej pożarowych sygnalizatorów optycznych. W obu urządzeniach zastosowano identyczny układ optyczny. Oba należą do kategorii O, dzięki czemu można je zamontować nie tylko na ścianie (mimo iż robi się tak najczęściej). Układ optyczny obu sygnalizatorów generuje sygnał optyczny o czasie rozbłysku ~0,5 ms i częstotliwości 0,57 Hz. Zgodnie z wymaganiami Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. z 2007 r., nr 143, poz. 1002) i Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2010 r. zmieniającego rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. z 2010 r., nr 85, poz. 553) sygnał optyczny jest koloru czerwonego. Kolor obudowy również jest czerwony, a na widzialnej części sygnalizatora naniesiony jest napis „POŻAR" koloru białego. Sygnalizatory uzyskały Certyfikat CPR oraz Świadectwo Dopuszczenia wydane przez CNBOP-PIB (SAOZ-Pk – Certyfikat CPR numer 1438-CPR-0366, Świadectwo Dopuszczenia nr 2013/2014; SGO-Pgz2 – Certyfikat CPR numer 1438-CPR-0367, Świadectwo Dopuszczenia nr 2014/2014).

Szymon Ratajski
W2
www.w2.com.pl

Światło i dźwięk
dla bezpieczeństwa

SYGNALIZATOR ZEWNĘTRZNY

DO SYGNALIZACJI POŻARU Z DOKUMENTAMI CNBOP-PIB

SAOZ-Pk
(SYGNALIZATOR AKUSTYCZNO-OPTYCZNY)

SGO-Pgz2
(SYGNALIZATOR GŁOSOWO-OPTYCZNY)

NOWOŚĆ W OFERCIE W2

Ta sama obudowa różne możliwości

www.w2.com.pl

W2, ul. Czajcza 6, 86-005 Białe Błota
Tel: +48.52.345.45.00
Tel/Fax: +48.52.584.01.92

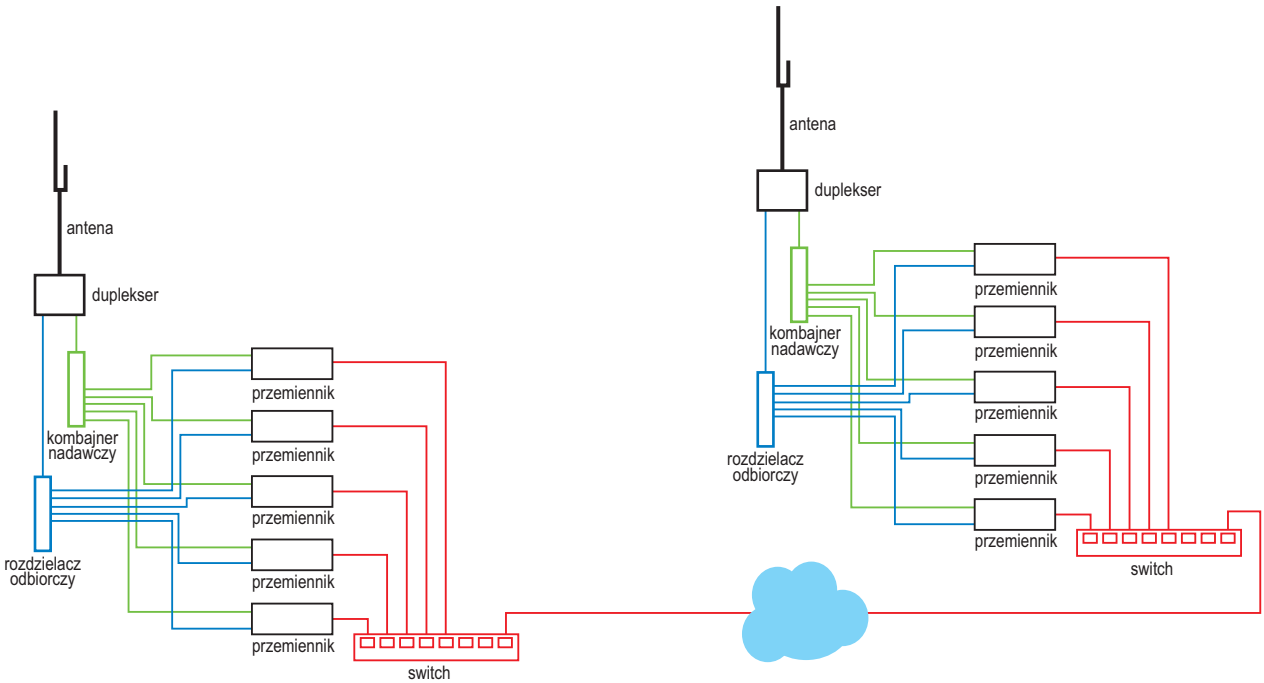
Sieciowy system trankingowy DMR

Andrzej Walczyk

Na bazie urządzeń zgodnych ze standardem DMR można budować złożone systemy radiokomunikacyjne, w tym systemy trankingowe, z których może jednocześnie korzystać wielu użytkowników. W ten sposób rozwiązywany jest problem ograniczonej pojemności systemów konwencjonalnych, jednak zasięg nie ulega poprawie

W systemach radiokomunikacyjnych wykorzystywanych przez służby ochrony i ratownictwa używane są fale radiowe z zakresu VHF lub UHF. Umownie przyjmuje się, że zakres VHF odpowiada częstotliwościom od 30 MHz do 300 MHz zaś zakres UHF częstotliwościom od 300 MHz do 3 GHz. Posługując się uproszczonym modelem propagacji fal radiowych, można przyjąć, że rozchodzą się one po liniach prostych, ulegają odbiciom od przeszkód materialnych oraz słabną z drugą potęgą odległości. W tym sensie są one podobne do światła, które również rozchodzi się prostoliniowo, odbija od przeszkód materialnych i słabnie w miarę oddalania się od jego źródła. Dzięki temu porównaniu łatwo sobie wyobrazić, że w miejscach, w których nie można zobaczyć anteny stacji bazowej, siła odbieranego sygnału będzie niska. Na podobnej zasadzie nie jesteśmy w stanie zobaczyć latarni morskiej, gdy wejdziemy za zasłaniający ją budynek.

W klasycznym systemie trankingowym wykorzystana jest pojedyncza stacja bazowa, w skład której wchodzi od kilku do kilkunastu przemienników radiowych. W ten sposób pojemność systemu, rozumiana jako zdolność do jednoczesnej



Rys. 1. Schemat blokowy sieciowego systemu trankingowego składającego się z dwóch stacji bazowych

obsługi wielu rozmówców, zostaje zwiększona, lecz jego zasięg nie ulega poprawie. Co prawda można zwiększyć zasięg dzięki zastosowaniu lepszych anten oraz umieszczeniu ich na większej wysokości, jednakże i ten pomysł nie jest całkowicie skuteczny. Po pierwsze, można napotkać problemy natury administracyjnej, związane z zakazem budowy lub wykorzystania wysokich konstrukcji wsporczych. Po drugie, zwiększanie wysokości jest skuteczne jedynie do pewnego stopnia – tą metodą nie można dowolnie zwiększać zasięgu.

Podstawowym czynnikiem ograniczającym zasięg łączności radiowej jest krzywizna ziemi. Najłatwiej przekonać się o tym, oglądając horyzont, poza który nie jesteśmy w stanie zajrzeć, nawet jeśli użyjemy silnej lornetki. Co prawda w przypadku fal radiowych występują pewne zjawiska umożliwiające nawiązywanie połączeń pozahoryzontalnych, jednak w zakresach VHF i UHF nie możemy na nie liczyć. Praktyczny wzór, za pomocą którego można wyznaczyć przybliżony zasięg łączności radiowej w przestrzeni otwartej, pozbawionej przeszkód materialnych (określający na przykład zasięg łączności dwóch okrętów znajdujących się na pełnym morzu), ma następującą postać:

$$D[km]=3{,}6*\left(\sqrt{h1[m]}+\sqrt{h2[m]}\right)$$

gdzie symbole h1 i h2 oznaczają wysokości zamocowania anten obu korespondujących stacji nad poziomem gruntu. Wysokości zamocowania anten h1 i h2 powinny być wyrażone w metrach, zaś wynik D jest podawany w kilometrach.

Z interpretacji tego wzoru wynika, że dziesięciokrotne podwyższenie miejsca instalacji jednej z anten powoduje zaledwie trzykrotne zwiększenie zasięgu łączności. Dlatego budowa bardzo wysokich masztów antenowych nie prowadzi do osiągnięcia celu, jakim jest zapewnienie niezawodnej łączności na dużym obszarze.

Praktycznym rozwiązaniem umożliwiającym niemal nieograniczone zwiększenie zasięgu w trankingowym systemie łączności jest zastosowanie wielu stacji bazowych i połączenie ich za pomocą sieci IP. W ten sposób powstaje rozproszona sieć radiowa umożliwiająca prowadzenie rozmów osobom znajdującym się w znacznej odległości od siebie. Schemat blokowy sieciowego systemu trankingowego składającego się z dwóch stacji bazowych jest przedstawiony na rysunku.

W praktyce można zastosować od kilku do kilkunastu stacji bazowych. Pod względem sposobu użytkowania taki system będzie podobny do systemu trankingowego opisanego w poprzednim artykule, lecz będzie obejmował swoim zasięgiem znacznie większy obszar. Jego użytkownicy będą mogli przemieszczać się w nieskrępowany sposób, zaś łączność nawiązać zawsze, gdy tylko znajdą się w zasięgu co najmniej jednej, niekoniecznie tej samej stacji bazowej. Tego typu systemy są obecnie wykorzystywane zarówno przez służby mundurowe, jak i przez organizacje cywilne.

Czym to się różni od telefonii komórkowej? Odpowiedź jest prosta. Właściciele rozproszonych systemów łączności radiowej są jednocześnie ich administratorami i konserwatorami. Odpowiednio skonfigurowane systemy radiokomunikacyjne nie zawiodą w sytuacjach krytycznych, podczas klęsk żywiołowych lub w trakcie incydentów o charakterze terrorystycznym. Nie ulegną również zablokowaniu na skutek nadmiernego obciążenia spowodowanego przez użytkowników w przypadku paniki spowodowanej nagłym wypadkiem.

Także podczas normalnej, codziennej eksploatacji wydzielone systemy łączności są bardziej niezawodne od połączeń komórkowych. Przykładowo, wysłanie jakiejkolwiek wiadomości z podgórskiej miejscowości wypoczynkowej w noc sylwestrową jest niemal niemożliwe, bo wszyscy wysyłają życzenia noworoczne i przeciążają lokalne stacje BTS dostosowane do znacznie mniejszego ruchu. Taka sytuacja nie może zaistnieć w wydzielonym systemie łączności radiowej dostosowanym do potrzeb jego użytkowników.

Andrzej Walczyk

KAMERA IP 3 MPX
do dyskretnego monitoringu

[Ø 10 cm]

Kompaktowa konstrukcja

W miejscach takich jak bary, restauracje czy kawiarnie goście nie powinni czuć się skrępowani obecnością monitoringu. Dzięki stylowej obudowie oraz niewielkim wymiarom, kamera bardzo dobrze wtapia się w wystrój pomieszczeń i nie przykuwa uwagi klientów.

[IR LED 6 m]

Wydajna praca przy słabym oświetleniu

W salach restauracyjnych często dominuje przygaszone światło i nastrojowy półmrok. Kamera ma funkcje dzień/noc (filtr IR), DSS oraz wbudowany oświetlacz podczerwieni, więc generuje wysokiej jakości obraz, nawet gdy w pomieszczeniu panuje ciemność.

[micro SD]

Szereg użytecznych funkcji

Funkcja stref prywatności pozwala na wyłączenie z monitoringu wybranych obszarów. Detekcja ruchu automatycznie wykrywa ruch w polu widzenia kamery. Kontrolę zdarzeń alarmowych ułatwia funkcja powiadamiania o zdarzeniach na e-mail i zapis na serwery FTP, NAS lub kartę pamięci.

NOVUS IP | NMS Compatible | ONVIF | 5000 SERIA IP | NOVUS 3 lata gwarancji

Kamera sieciowa NVIP-3DN5000V/IR-1P
z wandaloodporną obudową o klasie szczelności IP 66

Więcej informacji o produktach NOVUS® znajdziesz na:
www.novuscctv.pl

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

Ratunkowe systemy interkomowe

Leszek Schmidt

Jak wynika z danych statystycznych, ponad połowa ludności świata mieszka w miastach i w ich okolicach. Biorąc pod uwagę fakt, że miasta zajmują jedynie niewielki fragment powierzchni kuli ziemskiej, łatwo wywnioskować, że gęstość zaludnienia na ich terenie jest bardzo duża. W takich warunkach zaczyna obowiązywać prawo wielkich liczb, z którego wynika, że w danej chwili zawsze znajdzie się ktoś, kto poszukuje informacji albo wzywa pomocy. I tu zastosowanie znajdują ratunkowe systemy interkomowe

W miastach są miejsca, w których szybka komunikacja głosowa nabiera szczególnego znaczenia, takie jak lotniska, dworce kolejowe i autobusowe, stacje metra, publiczne parkingi, przejścia podziemne, tunele drogowe. Często zdarza się, że panuje tam spory ruch, co wiąże się z dużym natężeniem hałasu. Podobnie może być poza terenami miejskimi, na przykład na autostradach i innych ruchliwych drogach publicznych, gdzie nagromadzenie pojazdów, a tym samym ludzi, jest bardzo duże i gdzie występują stałe zagrożenia – nie tylko zagrożenie zwykłym wypadkiem drogowym, ale także zagrożenie bandytyzmem czy atakiem terrorystycznym.

Gdy trzeba ratować ludzkie życie i liczy się każda sekunda, szybka komunikacja głosowa odgrywa kluczową rolę. Od publicznych systemów interkomowych wymaga się łatwej obsługi oraz bardzo wysokiej niezawodności. Ich działanie powinno być niezależne od warunków pogodowych, zaś całodobowa obsługa, zapewniana przez odpowiedni personel, powinna być szybka, by rozmówcy nie musieli długo czekać na zgłoszenie się operatora. W większości przypadków w instalacjach interkomowych wykorzystywane są połączenia kablowe.

Współczesne standardy dotyczące jakości dźwięku transmitowanego za pośrednictwem publicznych interkomów są bardzo wysokie. Przykładowo, szerokość pasma kanału dźwiękowego wynosi 16 kHz, co przekłada się na bardzo dobrą zrozumiałość mowy oraz komfortową komunikację głosową. Korzystanie ze stanowisk informacyjnych czy punktów sprzedaży biletów staje się łatwe i wygodne. Ponadto dobra zrozumiałość mowy operatora przekazującego informacje może oddziaływać uspokajająco na zdenerwowaną osobę.

Spróbujmy dokładniej przyjrzeć się dziedzinom, w których zastosowanie publicznych systemów interkomowych nabiera szczególnego znaczenia.

Dworce kolejowe i lotniska

Na dworcach i lotniskach panuje duży ruch i jest duży hałas. Komunikaty dotyczące odjazdów pociągów czy odlotów samolotów mieszają się z reklamami i muzyką dobiegającą ze sklepów i restauracji. Podróżni są często zdezorientowani, towarzyszy im stres wynikający z dużego nagromadzenia bodźców. W takich okolicznościach czytelna komunikacja głosowa nabiera szczególnego znaczenia. Z pomocą mogą przyjść łatwo dostępne, czytelnie oznakowane, proste w obsłudze punkty informacyjne, rozmieszczone w wielu miejscach. Przez naciśnięcie tylko jednego przycisku podróżni mogą połączyć się z operatorem systemu, uzyskać niezbędne informacje lub nawet wezwać pomoc.

W przypadku dużych obiektów, takich jak dworce kolejowe i lotniska, wymagania dotyczące publicznych systemów interkomowych są szczególnie wysokie. Punkty informacyjne powinny być na tyle liczne, by nie tworzyły się przy nich kolejki. W związku z tym potrzebne są duże centra dyspozytorskie, obsługiwane przez całą dobę przez wielu operatorów. Wszystkie zastosowane urządzenia muszą być niezawodne w działaniu, nawet w sytuacjach awaryjnych, co wiąże się z koniecznością zapewnienia ciągłości zasilania zarówno stacji interkomowych, jak i centrum obsługi pasażerów. Jak już wspomniano, w przypadku tej klasy systemów stosuje się wyłącznie połączenia kablowe, co gwarantuje ich niezawodne działanie.

Metro

W metrze proste w obsłudze, czytelnie oznakowane interkomowe punkty informacyjne są rozmieszczane na peronach, a także wewnątrz wagonów. Pasażerowie mogą więc uzyskać niezbędne informacje lub poprosić o pomoc w nagłych wypadkach.

Parkingi samochodowe

Na zurbanizowanych obszarach wielopiętrowe parkingi samochodowe można znaleźć w bardzo wielu miejscach. Stanowią one nieodłączne składniki galerii handlowych, centrów biznesowych, dworców lotniczych i kolejowych. Spotyka się je nawet na osiedlach mieszkaniowych. Publiczne sieci interkomowe na parkingach mogą służyć do komunikacji z administratorami. Można je wykorzystywać także do powiadamiania o nagłych wypadkach i do wzywania pomocy.

Osiedla mieszkaniowe, parki logistyczne i biurowce

W takich obiektach przeważnie instalowane są systemy kontroli dostępu, w których wykorzystuje się karty identyfikacyjne, jednak w praktyce często zachodzi potrzeba wpuszczenia na teren obiektu osób nie dysponujących takimi kartami. Może to być użytkownik, który zgubił swoją kartę albo zapomniał zabrać jej ze sobą. Może to być gość albo osoba świadcząca jakieś usługi. We wszystkich tych przypadkach zachodzi konieczność skontaktowania się z portierem lub osobą pełniącą dyżur w pomieszczeniu ochrony. W tradycyjnych systemach interkomowych jakość dźwięku była stosunkowo niska i w związku z tym często wpuszczano na teren chronionego obiektu osoby, które nie powinny się na nim znaleźć. Współczesne głośnomówiące systemy interkomowe są wolne od tej wady, więc komfort obsługi oraz poziom bezpieczeństwa użytkowników obiektu mogą znacznie wzrosnąć.

Przejścia podziemne i tunele

Są to obszary typowe dla wielkich miast. Krzyżowanie się linii komunikacyjnych zmusza do budowy przejść podziemnych dla pieszych i tuneli drogowych dla samochodów. Długie korytarze czy tunele są miejscami szczególnie niebezpiecznymi. W wielu przypadkach nie działają tam telefony komórkowe. Mogą w nich być zainstalowane kabiny telefoniczne lub stacje interkomowe umożliwiające skontaktowanie się z operatorem systemu lub wezwanie pomocy. Z zasady w tego typu instalacjach stosowane są połączenia kablowe, które gwarantują niezakłóconą komunikację głosową w każdych warunkach eksploatacyjnych.

Drogi publiczne i autostrady

Są to miejsca odznaczające się dużym ruchem kołowym. Panujący tam hałas bardzo utrudnia, a często uniemożliwia skorzystanie z telefonów komórkowych. Wzdłuż dróg i autostrad co kilka lub kilkanaście kilometrów znajdują się zjazdy. Są tam umieszczane stacje interkomowe, często oznakowane jako telefony SOS, co z góry określa ich funkcję. Kierowcy, którzy potrzebują pomocy lub byli świadkami wypadku drogowego czy innego wydarzenia wymagającego natychmiastowej interwencji, mogą skontaktować się z operatorem systemu.

Bramki na autostradach

Bramki na autostradzie są typowym miejscem zastosowania interkomów. Ze względu na duży hałas oraz pośpiech towarzyszący przekraczaniu bramek użycie niezawodnych interkomów emitujących głośne komunikaty głosowe staje się koniecznością.

To oczywiście nie wszystkie możliwe zastosowania interkomów publicznych, a jedynie przykłady. W każdym z opisanych przypadków cechą wyróżniającą jest czytelna komunikacja głosowa oraz wysoka niezawodność zastosowanych urządzeń. Firma C&C Partners jest wyłącznym partnerem systemów interkomowych COMMEND. Są to produkty austriackiej firmy Commend International GmbH założonej w 1971 roku. Specjaliści z firmy C&C służą pomocą podczas projektowania i instalacji publicznych systemów interkomowych. Na terenie Polski urządzenia COMMEND zainstalowano już w wielu miejscach. Zainteresowanych odsyłamy do załączonej listy referencyjnej.

Szczegółowe dane na temat systemów COMMEND można znaleźć na stronie *http://www.ccpartners.pl*.

Leszek Schmidt
Kierownik ds. Produktu
C&C Partners

Lista referencyjna

Lotniska i dworce kolejowe:
- Port Lotniczy Poznań-Ławica,
- Port Lotniczy Wrocław,
- Port Lotniczy Gdańsk im. Lecha Wałęsy,
- Port Lotniczy Łódź im. Władysława Reymonta,
- Mazowiecki Port Lotniczy Warszawa-Modlin.

Dworzec autobusowy:
- Międzygminny Związek Komunikacji Pasażerskiej w Tarnowskich Górach.

Środki komunikacji publicznej:
- parkingi strategiczne „Parkuj i Jedź" w Warszawie.

Parkingi samochodowe:
- Poznań City Center (ZCK),
- Arkady Wrocławskie.

Parki logistyczne i biurowce:
- biurowiec spółki Polski Koks w Katowicach,
- biuro Okrąglak & Kwadraciak w Poznaniu.

Przejścia podziemne, przejazdy kolejowe i tunele:
- droga ekspresowa S69 – tunel Szare-Laliki,
- tunel trasy tramwajowej os. Lecha-Franowo,
- przejazdy kolejowe w Poznaniu.

Drogi publiczne i autostrady:
- stacje interkomowe wzdłuż autostrad A2 i A4 w PPO.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

UNIWERSALNA CENTRALA STERUJĄCA
UCS 6000

Ponad **20 wersji** od 4 A do 64 A
Dowolna konfiguracja
Współpraca z **dowolnym SSP**

INNOWACYJNA FUNKCJA ACOM 6.0

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

Malware i DDoS – co mają ze sobą wspólnego?

Krzysztof Białek

Jeszcze 15 lat temu w Polsce Internet wykorzystywany był przez ograniczone grono użytkowników. Korzystały z niego głównie uczelnie i firmy informatyczne. Obecnie trudno nam sobie wyobrazić życie bez dostępu do tego medium. Możliwość niedrogiego, szybkiego komunikowania się ludzi z całego świata, dostępu do informacji, zamawiania usług, robienia zakupów bez wychodzenia z domu, dostępu do konta bankowego, podglądu obrazu z kamer zainstalowanych w odległych miejscach nie jest już dobrodziejstwem dla wybranych. To część naszego codziennego życia. To, co jeszcze dwie dekady temu wydawało się niemożliwe, dziś już nikogo nie dziwi

Któż z nas uwierzyłby kilkanaście lat temu w to, że możliwe będzie regulowanie przez Internet temperatury w domu, gdy akurat przebywa się poza nim. Obecnie jest stosunkowo niewiele istotnych ograniczeń technicznych. Liczy się pomysł i zasobność portfela. Razem z rozwojem sieci i coraz większą jej dostępnością pojawiły się niestety także nowe zagrożenia. W ostatnim czasie głośno było o masowej, spreparowanej korespondencji e-mail. Treść wiadomości łudząco przypominała oryginalne informacje wysyłane przez dostawców usług telekomunikacyjnych, pocztowych czy bankowych, a załącznikiem do nich było złośliwe oprogramowanie (ang. *malware*). Otwarcie takiego załącznika infekuje komputer ofiary (uruchamia złośliwe oprogramowanie) i umożliwia przejęcie nad nim kontroli. Możliwa jest kradzież danych uwierzytelniających dostęp do konta bankowego. Wiele osób dało się nabrać przestępcom. Najlepszym sposobem na sprawdzenie, czy nasz komputer nie jest zainfekowany, jest pobranie odpowiedniego – nawet darmowego – oprogramowania typu antimalware (np. MalwareBytes, K7 UltimateSecurity) i uruchomienie skanowania. Efekty takiej weryfikacji mogą naprawdę zaskoczyć. Po usunięciu złośliwego oprogramowania lub upewnieniu się, że nasz komputer był wolny od tego typu zagrożenia, możemy ze spokojem zalogować się do swojego konta bankowego, żeby sprawdzić, czy nasze oszczędności nie wyparowały.

Każdego dnia tysiące użytkowników bankowości elektronicznej, użytkowników portali zakupowych czy osób korzystających z możliwości zdalnej weryfikacji stanu central alarmowych w swoich domach łączą się poprzez przeglądarkę internetową ze stroną WWW usługodawcy. Wydajność infrastruktury technicznej oraz przepustowość łącza internetowego są szacowane na podstawie liczby klientów lub zakładanej liczby użytkowników serwisów internetowych. Jeśli jednak w tym samym momencie z dostępu do danej strony internetowej będzie chciało skorzystać kilkaset razy więcej użytkowników niż zwykle, mogą pojawić się kłopoty z wydajnością infrastruktury sieciowej lub serwerów WWW. Objawia się to zazwyczaj wydłużeniem się oczekiwania na wyświetlenie treści lub wyświetleniem komunikatu o braku możliwości połączenia ze stroną. Taka sytuacja może zostać spowodowana przez rzeczywistych użytkowników, np. chcących zalogować się do portalu firmy, która ogłosiła akcję promocyjną: „Dla pierwszych 100 osób, które zalogują się do swojego konta w naszym portalu w piątek trzynastego o godzinie 10^{00} i zarezerwują zabieg kosmetyczny, czekają nagrody". Zwielokrotniony ruch wygenerowany przez internautów chcących skorzystać z promocji może doprowadzić do braku dostępności strony WWW. Do podobnego zdarzenia może dojść na przykład wówczas, gdy na pasku wiadomości znanego telewizyjnego kanału informacyjnego pojawi się informacja o kłopotach finansowych biura podróży – wielu klientów tego biura w tej samej chwili będzie chciało sprawdzić, czy podobna

informacja jest na jego stronie internetowej, i znaczna liczba jednoczesnych prób wyświetlenia strony może doprowadzić do jej niedostępności. Identyczna sytuacja może wystąpić jednak nie tylko w wyniku świadomego działania użytkowników.

Stacje robocze zainfekowane złośliwym oprogramowaniem (o którym wspomniano wcześniej) najczęściej komunikują się z serwerami atakujących, którzy wcześniej wysłali spam z plikami infekującymi komputery – są to serwery Command & Control, zwane w skrócie C&C. Złośliwe oprogramowanie może nie tylko wysyłać do serwera C&C dane wykradzione z komputera (np. dokumenty, zdjęcia, filmy, loginy i hasła wykorzystywane w bankowości elektronicznej lub portalach pocztowych), ale również „oczekiwać na rozkazy" wydawane przez C&C. Komputery zainfekowane przez oprogramowanie typu malware i komunikujące się z tymi samymi C&C stanowią tzw. botnet – sieć komputerów będących pod kontrolą atakujących. W ten sposób za pomocą danego komputera, bez wiedzy jego właściciela mogą być wysyłane wiadomości e-mail na adresy określone przez atakujących, a także nawiązywane połączenia z dowolnymi stronami WWW. Gdy botnet liczący setki tysięcy komputerów – a znane są i takie, które liczą ich miliony – otrzyma „rozkaz" otworzenia w tym samym czasie strony WWW należącej do jakiegoś banku, bankowa infrastruktura sieciowa i (lub) aplikacyjna może nie wytrzymać tak ogromnego obciążenia i dostęp do zasobów bankowych będzie niemożliwy. Jest to atak typu DDoS (ang. *Distributed Denial of Service*). Dynamiczną mapę bieżących ataków DDoS można obejrzeć m.in. na stronie *http://www.digitalattackmap.com.*

W jakim celu dokonywane są takie ataki? Po pierwsze, dosyć częstą praktyką jest grożenie zablokowaniem strony WWW i żądanie pieniędzy za zaniechanie ataku. Po drugie, taki atak może zostać przeprowadzony na zlecenie niezadowolonego klienta. Jeszcze kilka lat temu tego typu ataki były stosunkowo trudne do zrealizowania i kosztowne. Dziś, z uwagi na setki milionów komputerów i serwerów podłączonych do sieci Internet, kilkuminutowy atak DDoS można „zamówić" i „zakupić" już za kilka dolarów. Reklamę takiej usługi można obejrzeć np. na stronie *http://ddosservices.blogspot.com*.

Atak może zostać przeprowadzony również na zlecenie konkurencji. Niczym wyjątkowym nie są również ataki na użytkowników gier internetowych – przypuszczenie ataku DDoS na adres IP gracza powoduje jego czasowe wyeliminowanie z rozgrywki, co może wiązać się z określonymi korzyściami dla zlecającego atak.

Każda firma umożliwiająca swoim klientom dostęp do usług poprzez sieć Internet może stanąć pewnego dnia przed dylematem, jak się obronić przed tego typu atakiem. Brak dostępności usług może wpłynąć negatywnie na reputację firmy i spowodować straty finansowe. Wiele organizacji – w szczególności tych o dużych przychodach – stosuje zabezpieczenia sieciowe, które mają zapobiegać włamaniom do sieci wewnętrznych. Jednak w pojedynkę mogą one nie chronić dostatecznie przed wolumetrycznymi atakami typu DDoS. Może to być związane z ograniczeniami przepustowości łączy internetowych. Dla przykładu, jeśli przy normalnym ruchu użytkowników serwisu WWW danej firmy wykorzystywane jest pasmo 50 Mbps (megabitów na sekundę), a firma wykorzystuje łącze o przepustowości 100 Mbps, to przy ataku DDoS o wolumenie 500 Mbps dostęp do strony WWW dla rzeczywistych użytkowników będzie ograniczony albo niemożliwy, nawet pomimo zastosowania wewnętrznych zabezpieczeń DDoS. Rzeczywisty ruch po prostu nie dotrze do serwerów usługodawcy. Innymi słowy ograniczona przepustowość łącza będzie wąskim gardłem – będzie hamować rzeczywisty, poprawny ruch. Poza tym profesjonalne i skuteczne rozwiązania minimalizujące wpływ ataków DDoS są zbyt kosztowne, by ich zakup był opłacalny dla niewielkich firm.

Trendy, jakie można było zaobserwować w drugim kwartale 2014 roku[1].

Liczba ataków DDoS o wolumenie powyżej 100 Gbps (gigabitów na sekundę) wzrasta z roku na rok. Co prawda zdarzają się wyjątki, w drugim kwartale 2014 maksymalny wolumen ataku spadł z 325 Gbps (w pierwszym kwartale) do 154,7 Gbps, ale generalny trend polegający na przekroczeniu 100 Gbps nadal jest zachowany. Wzrasta czas trwania ataków DDoS – średni czas ataku to 98 minut. Jeszcze dwa lata temu średni czas ataku na strony WWW w Polsce wynosił kilka, kilkanaście minut. W ubiegłym roku odnotowano już wiele ataków trwających kilka, a nawet kilkanaście godzin. Tylko w pierwszej połowie 2014 roku liczba ataków DDoS o wolumenie powyżej 20 Gbps była przeszło dwukrotnie wyższa niż w całym 2013 roku.

1) www.cnet.com/news/ddos-attacks-intensified-in-first-half-of-2014/

Co można zrobić, by uchronić się przed wpływem ataków DDoS? Można zakupić usługę przeciwdziałania atakom DDoS u operatora telekomunikacyjnego. Dzięki temu, że operatorzy mogą udostępniać taką infrastrukturę zabezpieczającą większej liczbie klientów, koszt jej zakupu i utrzymania rozkłada się na większą liczbę partycypujących. Ponadto operatorzy dysponują łączami internetowymi o ogromnych przepustowościach, z których tylko część udostępniają swoim klientom. Poszczególne ataki DDoS swoim wolumenem nie są w stanie zablokować łącz będących do dyspozycji dużych operatorów telekomunikacyjnych. Jaką przepustowość łącza powinna zamówić firma, która chciałaby być niezależna i na własną rękę stworzyć infrastrukturę zabezpieczającą, by chronić swoje zasoby przed atakami DDoS? Jeszcze dwa lata temu obserwowano ataki DDoS o wolumenie rzędu kilkuset megabitów na sekundę. Wartości te z roku na rok wzrastają z powodu powiększania się liczby komputerów/serwerów podłączonych do sieci Internet (wykorzystywanych do ataków po infekcji złośliwym oprogramowaniem), spadku cen szerokopasmowego dostępu do Internetu i związanego z tym wzrastającego popytu. Dziś największe ataki wolumetryczne osiągają wartość kilkuset gigabitów na sekundę. Ze względu na to, że większość firm serwujących usługi poprzez Internet (np. banki) posiada dziś łącza o przepustowości od kilkudziesięciu do kilkuset megabitów na sekundę, wzrost kosztów związany z wykorzystaniem łącza o dużo większej przepustowości, np. kilkusetgigabitowego, byłby po prostu nieopłacalny.

Krzysztof Białek

KAMERA IP 5 MPX

do dokładnej wideoweryfikacji zdarzeń i osób

Żaden szczegół nie umknie uwadze

[2592 x 1944]

Bezpieczeństwo na dworcach jest kwestią priorytetową, dlatego pracujące tam kamery muszą dostarczać materiał wideo w wysokiej jakości. Dzięki 5-megapikselowej matrycy 1/2,5" CMOS, kamera NVIP-5DN5040V/IR-1P generuje ostry i bogaty w detale obraz. Wbudowany oświetlacz IR pozwala na wydajną pracę nawet w warunkach słabego oświetlenia

Możliwość wygłaszania komunikatów

[audio I/O]

Kamera posiada wejścia i wyjścia audio, które po podłączeniu głośników i mikrofonu, umożliwiają odsłuch dźwięku oraz komunikację głosową. Komunikat (np. upomnienie, ostrzeżenie), będzie słyszalny tylko w miejscu zainstalowania kamery, czyli tam, gdzie faktycznie doszło do zdarzenia

Montaż na suficie, ścianie, słupie i narożniku

[IP 66]

Kamery na dworcach są narażone na próby celowego zniszczenia. Wandaloodporna obudowa chroni przed fizycznym uszkodzeniem. Klasa szczelności IP 66 zapewnia odporność na zalanie wodą. Kamerę można zainstalować na suficie, jak również na ścianie, narożniku i słupie za pomocą dostępnych akcesoriów montażowych

NOVUS IP · NMS Compatible · ONVIF · 5000 SERIA IP · NOVUS 3 lata gwarancji

Kamera sieciowa NVIP-5DN5040V/IR-1P

z obiektywem o zmiennej ogniskowej f=3.3 ~ 12 mm

Więcej informacji o produktach NOVUS® znajdziesz na:
www.novuscctv.pl

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

DH-HAC-HFW2200E

Kamera HDCVI w wodoodpornej obudowie tulejowej, z oświetlaczem IR, o rozdzielczości 2 megapikseli, obraz w formacie 1080p.

Dane techniczne

- Przetwornik 1/3" CMOS
- 25/30 kl./s przy1080p, 25/30/50/60 kl./s przy 720p
- Transmisja obrazu na dużą odległość w czasie rzeczywistym
- Możliwość pracy w trybie Full HD i standardowym
- Menu z OSD, sterowanie za pośrednictwem kabla koncentrycznego
- Funkcje Dzień/Noc (ICR), AWB, AGC, BLC, 3D-DNR
- Obiektyw o stałej ogniskowej 6 mm (opcjonalnie 2,8 mm, 3,6 mm, 8 mm)
- Zasięg oświetlacza IR 20 m z funkcją Smart IR
- Stopień szczelności IP66
- Zasilanie 12 V_{DC}

Model	DH-HAC-HFW2200EP
Dane techniczne	
Przetwornik obrazu	1/3" CMOS
Liczba aktywnych pikseli	1920×1080
Migawka elektroniczna	regulowana w zakresie od 1/3 s do 1/100,000 s
Liczba klatek na sekundę	25/30/50/60 przy 720P; 25/30f przy 1080P
Synchronizacja	wewnętrzna
Czułość	0,05 lx przy F1,2 (AGC włączone), 0 lx przy włączonym oświetlaczu IR
Wyjście wizyjne	jedno wspólne złącze BNC dla HDCVI przy wysokiej rozdzielczości i CVBS przy standardowej rozdzielczości, z możliwością przełączania trybu pracy kamery
Zasięg oświetlacza IR	20 m z funkcją Smart IR
Funkcja Dzień/Noc	automatyczne przełączanie między trybem kolorowym a czarno-białym
Redukcja szumów	2D/3D
Menu z OSD	jest
Obiektyw	
Ogniskowa	stała wartość 6 mm (opcjonalnie 2,8 mm, 3,6 mm, 8 mm)
Rodzaj zamocowania	M12
Inne dane	
Zasilanie	12 V_{DC} ± 10%
Pobór mocy	maks. 4,5 W
Warunki środowiskowe	Temp. od -30°C do +60°C/ Wilgotność 95% R bez kondensacji
Transmisja obrazu	na odległość 300 m z użyciem kabla koncentrycznego 75-3
Klasa szczelności	IP66
Wymiary zewn. (W×D×H)	178,4 mm×69,9 mm×70,0 mm
Masa	0,5 kg

Producent:

Dahua Technology Co., Ltd.
1199' BinAn Road, Binjiang District
Hangzhou, China

tel.: +86-571-87688883, faks +86-571-87688815
e-mail: overseas@dahuatech.com
www.dahuatech.com

bibi-C25

Rejestrator czasu pracy z kolorowym ekranem dotykowym i czytnikiem transponderów Mifare

Rejestrator **bibi-C25** jest urządzeniem przeznaczonym do ewidencji czasu pracy z wykorzystaniem identyfikatorów zbliżeniowych RFID typu Mifare. Pracuje w systemach kontroli dostępu i rejestracji czasu pracy bibinet-2.

Rejestrator może komunikować się z węzłem systemu bibinet-2 zarówno wewnątrz sieci lokalnej jak i poprzez rutery i sieć Internet. Transmisja jest szyfrowana. Do jednego węzła systemu bibinet-2 można podłączyć wiele rejestratorów. Wykorzystanie rejestratorów w sieci Internet umożliwia połączenie rozproszonych obiektów (np. sieci sklepów) w jeden system rejestracji czasu pracy (i kontroli dostępu przy wykorzystaniu innych urządzeń systemu bibinet-2). Takie właściwości pozwalają na zbudowanie dużego systemu zarządzanego z jednego miejsca.

Instalacja

Dzięki zasilaniu poprzez kabel Ethernet (*Power over Ethernet*) instalacja rejestratora może być wykonana w oparciu o okablowanie strukturalne obiektu. Adapter PoE i zasilacz montujemy w miejscu instalacji przełącznika sieciowego. W czasie instalacji konfigurację urządzenia można wykonać z menu instalatora wyświetlanego na ekranie dotykowym lub przez przeglądarkę internetową wykorzystując wbudowany serwer WWW.

Rejestracja zdarzeń

Czytnik rejestratora odczytuje identyfikator (UID) kart Philips Mifare o standardowej długości kodu równej 4 bajty oraz o długości kodu równej 7 bajtów (charakterystycznej dla kart Ultralight i DESFire). Karty (breloczki) tego typu są powszechnie stosowane jako karty miejskie (np. bilety komunikacji miejskiej) czy legitymacje studenckie. Można je dodatkowo wykorzystywać jako identyfikatory w systemie rejestracji czasu pracy. W rejestratorze jest wbudowany zegar czasu rzeczywistego, który jest synchronizowany za pomocą danych pobieranych z serwerów czasu w Internecie.

Wybór rodzaju rejestrowanego zdarzenia dokonywany jest w oparciu o klawisze wyświetlane na ekranie dotykowym. Na ekranie tym standardowo wyświetlany jest czas i trzy klawisze: wejście, wyjście oraz klawisz funkcyjny bibi. Dotknięcie tego klawisza rozwija menu udostępniające więcej opcji.

Oprogramowanie

Rejestrator bibi-C25 współpracuje z oprogramowaniem do rejestracji czasu pracy i kontroli dostępu bibinet-2. Oprogramowanie to pozwala na konfigurację urządzenia i automatyczne zbieranie zarejestrowanych danych. Przygotowuje wiele indywidualnych i zbiorowych raportów. Umożliwia pracownikom podgląd tych raportów przez przeglądarkę internetową. Pozwala na eksport zarejestrowanych danych do innych programów kadrowo-płacowych oraz eksport raportów do arkuszy kalkulacyjnych. Program jest licencjonowany.

Dane techniczne

- Wyświetlacz: kolorowy 3,5"
  - rozdzielczość: 320×240
  - panel dotykowy: rezystancyjny
- Typ kart: Philips Mifare, 13,56 MHz
- Odczytywana informacja: identyfikator karty (UID)
- Zasięg odczytu kart: typowo 5 cm
- Pojemność kart: 10 000
- Bufor zdarzeń: 65 000
- Protokół transmisyjny: Ethernet TCP/IP, 10/100 Mb/s
- Zasilanie: PoE, 12-24 V_{DC}, 2 W
- Warunki pracy: +5°C…+40°C, stopień szczelności IP 40
- Wymiary: 155×150×37 mm
- Dostępne kolory: lava, jasnoszary

Producent:

MicroMade

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

tel./faks 67 213 24 14
e-mail: mm@micromade.pl
http://www.bibinet.pl/bibic25

Rejestrator IP INVR-16A

MAZi to nowa, europejska marka na rynku CCTV. MAZi – w języku greckim μαζι – znaczy „razem". Oddaje to przesłanie towarzyszące powstaniu tej marki oraz współpracy z naszymi partnerami. Wprowadzając produkty MAZi chcemy rozwijać naszą ofertę poprzez dostarczanie urządzeń do wizyjnych systemów dozorowych, cechujących się wysoką jakością i niską ceną.

MAZi to pełna oferta urządzeń monitoringu wizyjnego, zawierająca:
- kamery i rejestratory analogowe i hybrydowe (do kamer analogowych oraz IP),
- kamery i rejestratory IP,
- kamery i rejestratory HD-SDI,
- akcesoria do urządzeń MAZi.

Charakterystyka

- Maksymalny strumień odbierany 80 Mb/s
- Maksymalny strumień wysyłany 240 Mb/s
- Obsługa maksymalnie16 kamer o rozdzielczości do 5 Mpx
- 4 HDD
- 1 port eSATA
- 1 port LAN 1 Gb/s
- Obudowa typu rack 2U
- Konfiguracja kamer z poziomu rejestratora
- Możliwość pracy samodzielnej – obsługa za pomocą monitora i myszy podłączonych bezpośrednio do rejestratora
- Tryb dwumonitorowy

Dane techniczne

Wizja
- Maks. strumień: 80/160 Mb/s
- Liczba kanałów: 16×5 Mpx
- Rozdzielczość: HDMI/VGA 1920×1080P/60 Hz, 1920×1080P/50 Hz, 1600×1200/60 Hz, 1280×1024/60 Hz, 1280×720/60 Hz, 1024×768/60 Hz
- Tryb dwumonitorowy: wyjście HDMI/VGA oraz BNC, istnieje możliwość niezależnego wykorzystania wyjścia BNC oraz wyjść HDMI/VGA (za pośrednictwem tych wyjść transmitowany jest ten sam obraz)

Rejestracja
- HDD: 4×SATA HDD do 4 TB + 1×eSATA
- Tryb rejestracji: ciągły, harmonogram, detekcja ruchu

Porty i złącza
- Sieć Ethernet: 1×RJ-45 Gigabit Ethernet
- Wyjścia wizyjne: HDMI, VGA, BNC
- Wyjścia dźwiękowe: 2×BNC
- Złącza USB: 3×USB 2.0
- Porty RS: 1×RS485, RS232
- Złącza alarmowe: 16×wejście, 4×wyjście

Praca sieciowa
- Zarządzanie: wbudowany web-serwer, obsługa za pomocą przeglądarki IE, Firefox lub innej
- Oprogramowanie: program VMS-A1

Parametry fizyczne
- Zasilanie: 12 V_{DC} ± 5%, 6,3 A
- Chłodzenie: radiator i wentylator
- Certyfikacja: CE, RoHS
- Wymiary: 445×390×90 mm
- Masa: 4 kg

Dystrybucja: GDE POLSKA
GDE Polska
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel./faks 12 256 50 35, 256 50 25
faks 12 270 56 96
e-mail: biuro@gde.pl

Kamera IP SICH-2030

Kamera szybkoobrotowa **SICH-2030** wyróżnia się rozdzielczością 2 Mpx oraz obiektywem zmiennoogniskowym o bardzo szerokim zakresie regulacji ×30. Kamera jest również dostępna w wersji z prostszym obiektywem, o zakresie regulacji ×20. W tym przypadku ma ona symbol SICH-2020.
Kamera ma nowoczesny przetwornik CMOS o rozmiarach 1/2,8" i może wytwarzać obraz o rozdzielczości 1920×1080 pikseli z prędkością 25 lub 30 kl./s.

Obiektyw o ogniskowej regulowanej w zakresie od 4,3 mm do 129 mm (×30) pozwala na precyzyjne dostosowanie pola obserwacji kamery do wymagań użytkownika oraz obserwację nawet bardzo odległych obiektów. Funkcje WDR, HLC oraz BLC poprawiają jakość obrazu w trudnych warunkach oświetleniowych.
Do mocowania kamer szybkoobrotowych dostępna jest pełna gama uchwytów: do ściany, sufitu, słupa, uchwyt narożny. Dostępna jest również klawiatura sterująca.

Charakterystyka

- Progresywne skanowanie – z prędkością 25 kl./s gwarantuje płynność ruchu bez smużeń czy zniekształceń wyglądu obserwowanych obiektów
- Dwa strumienie wizyjne: pozwalają na obsługę klientów o różnych wymaganiach jakościowych i wykorzystanie łącz o różnych przepustowościach, w tym także komunikację z urządzeniami automatyki budynkowej, np. Fibaro
- Zgodność z ONVIF
- Obsługa za pomocą przeglądarek Internet Explorer, Firefox i innych
- Dwukierunkowa komunikacja głosowa
- Analogowe wizyjne wyjście serwisowe – pozwala na równoczesne udostępnianie obrazów z kamery zarówno w sieci IP jak poprzez wyjście analogowe
- Możliwość zaprogramowania 255 presetów, 8 tras patrolowych
- Możliwość rejestracji obrazu na karcie mikro SD o pojemności do 32 GB
- Możliwość rejestracji obrazów na serwerze FTP oraz sieciowej pamięci NAS
- Podgląd obrazu przez smartfony
- Zabezpieczenie przeciwprzepięciowe
- Obudowa o stopniu szczelności IP66

Dane techniczne

- Kamera IP: szybkoobrotowa, do zastosowań zewnętrznych
- Rozdzielczość: 1920×1080
- Przetwornik: CMOS o rozmiarach 1/2,8"
- Obiektyw: ogniskowa od 4,3 mm do 129 mm, DC Iris
- Czułość: 0,05 lx przy F1,6 (kolor); 0,01 lx przy F1,6 (B/W)
- Filtr IR: mechanicznie odsuwany filtr podczerwieni TDN
- Wymiary: Ø220×305 mm (Ø8,66"×12,02")
- Masa: 5 kg
- Obudowa: stopień szczelności IP66
- Zasilanie: 24 V_{AC} maks. 22 W

EGTP-1
Rejestrator RCP z ekranem dotykowym

EGTP-1 jest to terminal służący do rejestracji czasu pracy zbudowany w oparciu o tablet z 7-calowym ekranem dotykowym (ASUS) i umieszczony w obudowie przeznaczonej do zawieszenia na ścianie.
EGTP-1 jest fabrycznie skonfigurowany i ma zainstalowaną aplikację RCP Point (ROGER). Dzięki wbudowanej kamerze rejestrator może wykonywać zdjęcia rejestrującym się osobom. W ten sposób rozwiązany został podstawowy problem występujący w systemach rejestracji czasu pracy, bazujących na nośnikach nie zawierających danych biometrycznych. Aplikacja RCP Point jest darmowa i może być zainstalowana na dowolnych tabletach z systemem operacyjnym Android, jednak nie jest wtedy zabezpieczona przed nieuprawnionym wyłączeniem lub nawet odinstalowaniem i dlatego ten wariant pracy nie jest zalecany.

Charakterystyka

- 7-calowy ekran dotykowy o rozdzielczości 1280×800 WXGA
- Obudowa umożliwiająca powieszenie urządzenia na ścianie
- Proste intuicyjne menu oraz wysokiej jakości obraz
- Rejestracja pracownika poprzez karty zbliżeniowe Mifare oraz kody QR
- Możliwość rejestracji za pomocą telefonu komórkowego z łączem Bluetooth i/lub NFC
- Rejestracja zdjęć logujących się osób
- Wyświetlanie nazw trybów RCP
- Szybki wybór z maks. 250 trybów RCP
- Komunikacja przez sieć Wi-Fi

Producent: roger®

ROGER Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

Czytniki zbliżeniowe 13.56MHz ISO14443A i MIFARE serii QUADRUS

Czytniki **PRT82MF** i **PRT84MF** są kontynuacją serii czytników zbliżeniowych przeznaczonych do zastosowania w systemie kontroli dostępu RACS 4. Urządzenia zostały opracowane wg modnych obecnie trendów wzorniczych charakteryzujących się estetyką zbliżoną do smartfonów i tabletów. Stylistyka obudowy sprawia, że mogą się dobrze komponować zarówno w budynkach nowoczesnych jak i tradycyjnych. Czytniki te mogą być również podłączane do kontrolerów innych producentów, o ile kontrolery te akceptują format danych w standardzie Wiegand 26..66 bit.

Charakterystyka

- Odczyt kart ISO 14443A i MIFARE
- Odczyt numerów: CSN, SSN i MSN(*)
- Zasięg odczytu do 7 cm
- Formaty wyjściowe: RACS CLK/DTA oraz Wiegand 26..66bit
- Trzy wskaźniki LED
- Wejście sterujące głośnikiem BUZZER
- Wejście sterujące wskaźnikiem LED
- Głośnik sygnalizacyjny
- Regulacja poziomu głośności oraz poziomu podświetlenia klawiatury
- Dwa klawisze funkcyjne (PRT84MF)
- Klawiatura dotykowa (sensoryczna)
- Czujnik otwarcia obudowy oraz oderwania od ściany
- Konfiguracja z komputera (program RogerVDM)
- Praca w warunkach wewnętrznych
- Biała i czarna wersja kolorystyczna
- Znak CE

(*) - sektor SSN i MSN odczytywany jest w kartach MIFARE Classic

Producent: roger®

ROGER Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

Monitory wideodomofonowe M270B/M270W

M270B/M270W-S1

Monitory wideodomofonowe są przeznaczone do pracy w systemach obsługujących od 1 do 8 abonentów. Głośnomówiący monitor został wyposażony w słuchawkę dając użytkownikowi wybór sposobu prowadzenia rozmowy.

Monitor ma kolorowy ekran panoramiczny TFT LCD o przekątnej 7" z możliwością regulacji jego parametrów (jasność, nasycenie koloru). M270 obsługuje 2 wejścia (2 stacje bramowe lub 1 stacja + 1 kamera CCTV). Przy zastosowaniu odpowiedniego modułu zyskujemy możliwość obsługi dodatkowego wejścia. Funkcja podglądu z dodatkowej kamery CCTV jest przydatna szczególnie w sytuacji niedostatecznej widoczności otoczenia wejścia głównego. Obrazy z kamer można przełączać sekwencyjnie z poziomu monitora.

Dużym udogodnieniem jest możliwość podglądu obrazu z kamery, rozpoczęcia rozmowy i otwarcia elektrozaczepu bez konieczności uzyskania wywołania z zewnątrz.

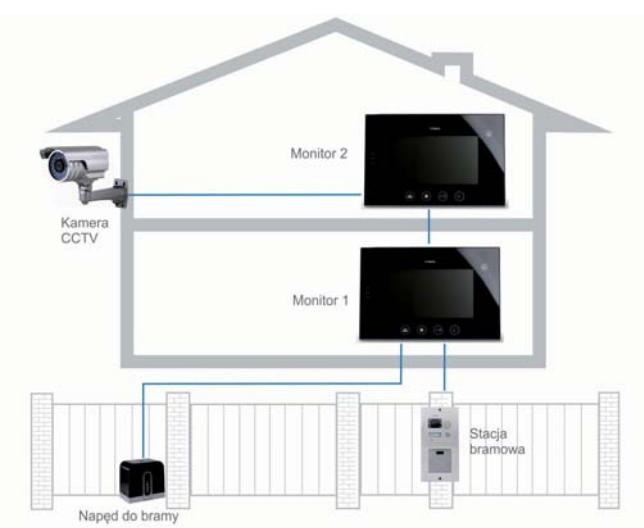
System można rozbudować o dodatkowe trzy monitory lub unifony. Mogą to być dowolne urządzenia marki VIDOS lub Competition.

M270W-S1 jest dodatkowo wyposażony w moduł pamięci zdjęć. Po przyciśnięciu przycisku dzwonka, osoba przed kamerą zostaje sfotografowana, a obraz jest zapisywany w pamięci, która pomieści 100 zdjęć.

Monitory mają funkcję sterowania bramą automatyczną za pośrednictwem osobnego przycisku umiszczonego na panelu.

Dane techniczne

- Monitor głośnomówiący z dodatkową słuchawką
- Panoramiczny, kolorowy ekran TFT LCD o przekątnej 7"
- Obsługa dwóch stacji bramowych (lub jednej stacji i 1 kamery CCTV)
- Funkcja interkomu pozwala na komunikację głosową między urządzeniami wewnętrznymi
- Dotykowy, podświetlany panel sterowania
- Sterowanie elektrozaczepem i bramą automatyczną
- Wbudowana pamięć 100 zdjęć (model M20W-S1)
- Regulacja parametrów monitora (głośność dzwonka, głośność rozmowy, jasność, kolor)
- Podgląd z możliwością włączenia dźwięku i otwarcia furtki
- Instalacja: czteroprzewodowa
- Możliwość rozbudowy o trzy dodatkowe monitory lub unifony
- Zasilanie 14,5 V_{DC}. Zasilacz na listwę DIN w komplecie
- Wymiary 282×135×23 mm
- Współpracuje ze wszystkimi stacjami bramowymi VIDOS i Competition



Producent: wena
WENA
Al. Jerozolimskie 311
05-816 Reguły
tel. 22 837 02 86, 817 40 08
e-mail: wena@wena.biz

KARTA KATALOGOWA

Seria kompaktowych stacji bramowych S600 z panelem ze stali szlachetnej

Wychodząc naprzeciw zmieniającym się trendom w elektronice, VIDOS wprowadza nową serię kompaktowych paneli zewnętrznych ze stali szlachetnej, które zachwycają swoją estetyką i funkcjonalnością. Wyjątkowy design, precyzja wykonania i komfort użytkowania – to najważniejsze cechy tego sprzętu. Wbudowany zamek szyfrowy lub czytnik kart umożliwia otwieranie furtki kodem PIN lub kartą zbliżeniową. Nowością jest stacja bramowa z wbudowanym czytnikiem biometrycznym obsługującym do 900 użytkowników.

Stacje bramowe zostały wyposażone w kolorową kamerę, zamocowaną tak, by możliwa była regulacja kąta nachylenia obiektywu w poziomie i w pionie w zakresie kilkunastu stopni. Standardowe mini obiektywy są wymienialne i w razie konieczności można zastosować inne o szerszym kącie widzenia (2,8 mm/2,5 mm). Atutem modeli z wbudowanym zamkiem szyfrowym jest możliwość podłączenia dodatkowego przycisku wyjściowego oraz timera określającego czas otwarcia rygla.

Niewielkie wymiary wyróżniają serię 600 spośród innych urządzeń na rynku. Szerokość wszystkich paneli to 10 cm. Pozwala to na instalację domofonu w miejscach, gdzie mamy do dyspozycji małą przestrzeń (np. wąski słupek). Możliwość montażu natynkowego poprzez zastosowanie puszki D600 otwiera szeroki wachlarz zastosowań.

Do każdej stacji bramowej można podłączyć maksymalnie 4 monitory bez konieczności stosowania dodatkowych modułów. Mogą to być dowolne monitory z oferty firmy VIDOS lub Competition.

Wszystkie stacje bramowe współpracują ze wszystkimi monitorami i unifonami VIDOS i Competition w dowolnej konfiguracji.

Dane techniczne

- Stacja bramowa do wideodomofonu 1/2/3/6 abonentowa
- Przetwornik obrazu 1/3" CCD kolor
- Kąt widzenia obiektywu ok. 60°
- Rozdzielczość 420 linii
- Obiektyw o ogniskowej 3,6 mm
- Regulacja ustawienia obiektywu w pionie i poziomie ±10 stopni
- Podświetlenie diody LED IR (podczerwień)
- Sterowanie elektrozaczepem z regulacją czasu otwarcia 1-99 s (regulacja czasu w modelach S601A/S601D/S601Z/S603A/S603D)
- Podświetlana klawiatura i szyld na nazwisko (kolor błękitny)
- Wandaloodporny przedni panel ze stali szlachetnej
- Stopień szczelności IP65
- Montaż podtynkowy lub natynkowy z osłoną D600B1/D600B2/D600B3
- Otwieranie furtki za pomocą kodu PIN (S601D/S603D)
- Otwieranie furtki za pomocą karty zbliżeniowej (S601A/S603A)
- Otwieranie furtki przy użyciu czytnika biometrycznego (S601Z)
- Zasilanie kamery z monitora
- Zasilanie szyfratora/czytnika RFID/czytnika biometrycznego z zewnętrznego zasilacza 12-15 V_{DC}

Wymiary panela natynkowego

- 100×110×38 (model S601)
- 100×195×38 (modele S601A/S601D/S601Z/S602/S603)
- 100×280×38 (modele S603A/S603D/S606)

Wymiary puszki podtynkowej

- 96×105×50 (model S601)
- 96×190×50 (modele S601A/S601D/S601Z/S602/S603)
- 96×275×50 (modele S603A/S603D/S606)

Producent: wena

WENA
Al. Jerozolimskie 311
05-816 Reguły

tel. 22 837 02 86, 817 40 08
e-mail: wena@wena.biz

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. Koniczynowa 2A, 03-612 **Warszawa II**
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

ul. Łęczycka 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. Mieszczańska 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 606/610, 81-855 **Sopot**
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

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

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

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44
faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

AGIS FIRE & SECURITY Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
faks 22 430 83 02
e-mail: agisfs.pl@agisfs.com
www.agisfs.pl

ALARMNET Borkiewicz 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 sprzedaży i marketingu
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40
faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.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

ALPOL Sp. z o.o.
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 56
faks 32 790 76 61
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

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

ul. Łęczycka 55, 85-737 **Bydgoszcz**
tel. 32 720 39 67
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

ul. Sandomierska 105, 25-324 **Kielce**
tel. 32 720 39 82
faks 32 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Opolska 18 klatka C parter, 31-323 **Kraków**
tel. 32 790 76 46
faks 32 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Nowodworska 23, 59-200 **Legnica**
tel. 32 750 30 66
faks 32 750 30 67
e-mail: legnica@e-alpol.com.pl

ul. Grenadierów 13, 20-331 **Lublin**
tel. 32 790 76 50
faks 32 790 76 74
e-mail: lublin@e-alpol.com.pl

ul. Senatorska 31, 93-192 **Łódź**
tel. 32 790 76 25
faks 32 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. Oleska 99, 45-222 **Opole**
tel. 32 750 30 36
faks 32 750 30 38
e-mail: opole@e-alpol.com.pl

ul. Odolanowska 49a, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
e-mail: ostrow@e-alpol.com.pl

ul. T. Kutrzeby 16G/112, 61-719 **Poznań**
tel. 32 790 76 37
faks 61 826 63 36
e-mail: poznan@e-alpol.com.pl

ul. Zbrowskiego 100, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. 3 Maja 59, 81-850 **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. Rzymowskiego 34, 02-697 **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

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

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 41 00
faks 22 715 41 05
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.pl

P.W.H. BRABORK-LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. 22 619 29 49
faks 22 619 25 14
e-mail: brabork@braborklab.pl
www.braborklab.pl

bt electronics sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 429 36 16
faks 12 410 85 11
e-mail: saik@saik.pl
www.saik.pl

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
Tulipan Hause
02-672 Warszawa
Infolinia 801 133 084
faks 22 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
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. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
faks 22 633 90 60
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

CMA MONITORING
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888
faks 22 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

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

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 342 03 78
faks 71 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. 12 260 13 96
faks 12 260 13 95
e-mail: info@cma.com.pl

ul. Nowy rynek 2, 62-002 **Suchy Las k/Poznania**
tel. 61 861 40 51
faks 61 861 40 51
e-mail: poznan@cma.com.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel. 58 345 23 24
e-mail: sopot@cma.com.pl

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17
faks 22 546 19 78
e-mail: biuro@cs.pl
www.cs.pl

D-MAX Polska Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel./faks 61 822 60 52
e-mail: biuro@dmaxpolska.pl
www.dmaxpolska.pl

DAHUA TECHNOLOGY Co., Ltd.
No. 1199, Bin an Road, Bin jiang District
Hangzhou
P.R. China
P.C. 310053
e-mail: overseas@dahuatech.com
www.dahuasecurity.com

DG ELPRO
Z. Durlak, K. Durlak, J. Golonka Sp. J.
ul. Wadowicka 6
30-415 Kraków
tel./faks 12 263 93 85
e-mail: biuro@dgelpro.pl
www.dgelpro.pl

DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Mazowiecka 131
30-023 Kraków
tel. 12 423 31 00
faks 12 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00
faks 22 518 84 99
e-mail: sales@ebs.pl
www.ebs.pl

EL-MONT
ul. Wyzwolenia 15
44-200 Rybnik
tel. 32 423 07 28, 422 38 89
faks 32 423 07 29
e-mail: el-mont@el-mont.com
www.el-mont.com

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. 22 398 96 53
faks 22 398 96 54
e-mail: elproma@elproma.pl
www.elproma.pl

EUREKA SOFT & HARDWARE
ul. Rynek 13
62-300 Września
tel. 61 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
Al. Jerozolimskie 133 lok. 13
02-304 Warszawa
tel./faks 22 115 71 50
e-mail: kontakt@estpolska.pl
www.estpolska.pl

FES Trading Sp. z o.o.
ul. Schuberta 100
80-171 Gdańsk
tel. 58 340 00 41 ÷ 44
faks 58 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 35
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

GORKE ELECTRONIC Sp. z o.o.
ul. Staromiejska 31 B
43-200 Pszczyna
tel. 32 326 30 70
faks 32 447 73 30
e-mail: biuro@gorke.com.pl
www.gorke.com.pl

ICS POLSKA
ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38
faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.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

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

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92
faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

KOLEKTOR
K. Mikiciuk i R. Rutkowski Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel./faks 58 553 67 59
e-mail: info@kolektor.pl
www.kolektor.pl

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

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
faks wew. 28
e-mail: info@micronix.pl
www.micronix.pl

NOVATEL Sp. z o.o.
ul. Turystyczna 1
43-155 Bieruń
tel. 32 201 17 04
faks 32 201 15 11
e-mail: novatel@novatel.pl
www.novatel.pl

NUUXE RADIOTON Sp. z o.o.
Siedziba w Krakowie:
ul. Olszańska 5H
31-513 Kraków
tel. 12 393 58 00, 417 36 77
faks 12 393 58 02
e-mail: nuuxe@nuuxe.com
www.nuuxe.com

Biuro:
ul. Polska 43
81-337 Gdynia
tel. 58 621 55 21
faks 58 621 55 21
e-mail: gaszenie@nuuxe.com

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel./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. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@omc.com.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks 61 657 93 60
e-mail: poznan@omc.com.pl

ul. Różyckiego 1c, 51-608 **Wrocław**
tel./faks 71 347 91 91
e-mail: wroclaw@omc.com.pl

POINTEL Sp. z o.o.
ul. Fordońska 199
85-739 Bydgoszcz
tel. 52 371 81 16
faks 52 342 35 83
e-mail: biuro@pointel.pl
www.pointel.pl

POL-ITAL Sp. z o.o.
ul. Irysowa 11
02-660 Warszawa
tel. 22 831 15 35
faks 22 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łapczyca
tel. 14 610 19 40
faks 14 610 19 50
e-mail: norbert@pulsar.pl
www.pulsar.pl

RISCO GROUP POLAND Sp. z o.o.
ul. 17 Stycznia 56
02-146 Warszawa
tel. 22 500 28 40
faks 22 500 28 41
e-mail: sales-pl@riscogroup.com
www.riscogroup.com

POLON-ALFA
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61
faks 52 363 92 64
e-mail: polonalfa@polon-alfa.pl
www.polon-alfa.pl

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

ROPAM Elektronik s.c.
Os. Tysiąclecia 6A/1
32-400 Myślenice
tel. 12 341 04 07
faks 12 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl
www.ropam.eu

PROFICCTV Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl
www.dmaxcctv.pl
www.samsungcctv.pl

RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel. 22 632 72 22
faks 22 833 09 07
e-mail: biuro@rettpol.pl
www.rettpol.pl

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16
faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

SAMSUNG TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Marynarska 15
02-674 Warszawa
tel. 22 205 07 77
faks 22 205 07 63
www.samsung-security.pl

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
tel. 58 320 94 00
faks 58 320 94 01
e-mail: satel@satel.pl
www.satel.pl

SAWEL
Systemy Bezpieczeństwa
ul. Lwowska 83
35-301 Rzeszów
tel. 17 857 80 60
faks 17 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Konstruktorska 12
02-673 Warszawa
tel. 22 511 82 00
faks 22 511 82 02
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.pl

Oddziały:
ul. Galaktyczna 36A
80-299 **Gdańsk**

ul. Muchoborska 18
54-424 **Wrocław**

Budynek KBP100
ul. Krakowska 280
32-080 **Zabierzów**

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44A
02-672 Warszawa
tel./faks 22 33 00 620, 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
Al. Grunwaldzka 82, 80-244 **Gdańsk**
tel./faks 58 767 70 10
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17 (wejście od ul. Stawowej)
31-358 **Kraków**
tel. 12 637 11 74
krakow@schrack-seconet.pl

ul. Wierzbięcice 1, 61-569 **Poznań**
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 **Wrocław**
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

PRZEDSIĘBIORSTWO TECHNICZNO- HANDLOWE
SECURAL Jacek Giersz
ul. Gen. K. 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

SEVITEL Sp. z o.o.
ul. Leopolda 29
40-189 Katowice
tel. 32 705 73 00
faks 32 705 73 99
e-mail: sevitel@sevitel.pl, handel@sevitel.pl
www.sevitel.pl

SMA Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

Oddziały:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@sma.biz.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks 61 657 93 60
e-mail: poznan@sma.biz.pl

ul. Różyckiego 1C, 51-608 **Wrocław**
tel. 71 347 91 91
tel./faks 71 348 04 19
e-mail: sma@sma.wroclaw.pl

SPS Electronics Sp. z o.o.
ul. Krakowiaków 80/98
02-255 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.pl
www.spselectronics.pl

Biura Handlowe:
ul. Drożyny 6, 80-302 **Gdańsk**
tel. 58 624 83 04
faks 58 668 59 20
e-mail: gdansk@spselectronics.pl

al. Roździeńskiego 188a, 40-203 **Katowice**
tel. 32 255 64 27
faks 32 255 64 52
e-mail: katowice@spselectronics.pl

ul. Polska 60, 60-595 **Poznań**
tel. 61 852 19 02
faks 61 825 09 03
e-mail: poznan@spselectronics.pl

pl. Gen. Wróblewskiego 3a, 50-413 **Wrocław**
tel. 71 348 44 64
faks 71 348 36 35
e-mail: wroclaw@spselectronics.pl

Biuro Partnerskie SPS Partner
ul. Przybyszewskiego 199/205, 93-120 **Łódź**
tel. 42 617 00 32
e-mail: lodz@spspartner.pl

ul. Szosa Chełmińska 217A, 87-100 **Toruń**
tel. 56 653 99 43
faks 56 653 90 81
e-mail: torun@spspartner.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

UNICARD S.A.
ul. Łagiewnicka 54
30-417 Kraków
tel. 12 398 99 00
faks 12 398 99 01
e-mail: zapytania@unicard.pl
www.unicard.pl

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

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. 61 674 62 00
faks 61 674 62 01
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

ZBAR PHU
ul. Krakowska 60
94-214 Łódź
tel. 42 611 12 97
faks 42 611 12 98
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

PTK5507 - dotykowa klawiatura serii POWER

DSC

- Nowoczesny design • 7” dotykowy wyświetlacz o wysokiej rozdzielczości (800 x 480) • Intuicyjne menu
- Możliwość personalizacji ekranu głównego • Wbudowany slot kart SD • Funkcja ramki elektronicznej
- Funkcja wirtualnej klawiatury • Diody LED sygnalizujące stan systemu
- Kompatybilna z centralami PC1864, PC1832, PC1616

Z dotykową klawiaturą PTK5507 obsługa systemu alarmowego jest jeszcze prostsza. Intuicyjne ikony menu oraz przesuwany ekran pozwalają łatwo zarządzać systemem. Aby uruchomić wybraną funkcję, wystarczy jedno dotknięcie ekranu palcem!

Klawiatura jest elegancką ozdobą każdego pomieszczenia. Zintegrowana ramka elektroniczna umożliwia wyświetlanie na ekranie klawiatury zdjęć z karty pamięci.

Wyłączny dystrybutor produktów DSC w Polsce:

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS FIRE & SECURITY	–	TAK	TAK	TAK	TAK
Alarmnet	–	–	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	TAK	TAK	–	TAK
ASSA ABLOY	–	–	TAK	–	–
BOSCH	TAK	–	–	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC (Poland)	TAK	–	TAK	–	TAK
CMA	TAK	TAK	–	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	–
D-MAX	–	–	TAK	–	–
DAHUA TECHNOLOGY	TAK	TAK	TAK	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	–
Dyskret	–	TAK	TAK	TAK	–
EBS	TAK	TAK	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
EST POLSKA	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
GORKE	TAK	–	–	–	–
ICS POLSKA	–	TAK	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	–	TAK	–	–
KATON	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Kolektor	–	TAK	TAK	TAK	–
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Novatel	–	TAK	TAK	TAK	TAK
NUUXE RADIOTON	–	TAK	TAK	TAK	TAK
OBIS	–	TAK	–	TAK	TAK
OMC INDUSTRIAL	–	–	TAK	–	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	–	TAK	TAK	–
RISCO	TAK	–	–	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	TAK
Samsung Techwin Europe	TAK	–	TAK	–	–
Satel	TAK	–	–	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schneider Electric Polska	–	–	TAK	–	–
Schrack Seconet Polska	TAK	TAK	TAK	–	TAK
Secural	TAK	TAK	TAK	–	TAK
Sevitel	–	–	TAK	TAK	–
SMA	–	TAK	–	TAK	–
SPS Electronics	–	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	TAK	TAK	–	TAK
UNICARD	TAK	TAK	–	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	–	TAK	–	–
ZBAR	–	TAK	TAK	TAK	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, karty magnetyczne i zbliżeniowe								
AGIS FIRE & SECURITY	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	–	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	TAK	TAK	TAK	–	–	–	TAK	–	–
CBC (Poland)	–	TAK	–	–	–	–	–	–	–
CMA	TAK	TAK	TAK	–	–	TAK	TAK	–	–
CONTROL SYSTEM FMN	–	–	TAK	–	–	–	–	TAK	–
D-MAX	–	TAK	–	–	–	–	TAK	–	–
DAHUA TECHNOLOGY	–	TAK	TAK	–	–	–	–	–	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Dyskret	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EBS	transmitery GSM/GPRS/IP, systemy RFID i GPS, produkcja OEM/ODM, rozwiązania M2M								
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
EST POLSKA	TAK	TAK	TAK	–	TAK	–	TAK	–	–
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
GORKE	TAK	–	TAK	–	–	–	TAK	–	–
ICS POLSKA	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Janex International	TAK	TAK	TAK	TAK	–	–	–	–	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Novatel	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
NUUXE RADIOTON	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	TAK	TAK	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	–	TAK	TAK	–	–	TAK
RETT-POL	TAK	–	TAK	TAK	–	–	TAK	–	–
RISCO	TAK	–	–	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung Techwin Europe	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	TAK	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Schneider Electric Polska	–	TAK	TAK	–	–	TAK	TAK	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Sevitel	–	–	TAK	TAK	–	TAK	–	TAK	–
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Tap – Systemy Alarmowe	TAK	TAK	TAK	–	TAK	TAK	–	–	–
UNICARD	–	–	TAK	TAK	–	TAK	–	–	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	TAK	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik

Skład i łamanie
Tomasz Kaczmarczyk

Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. 22 546 0 951, 953
faks 22 546 0 959
www.zabezpieczenia.com.pl

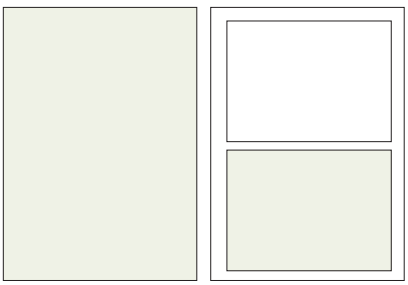
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4600 zł
cała strona, czarno-biała	2400 zł
1/2 strony, pełny kolor	2900 zł
1/2 strony, czarno-biała	1600 zł
1/3 strony, pełny kolor	2000 zł
1/3 strony, czarno-biała	1100 zł
1/4 strony, pełny kolor	1500 zł
1/4 strony, czarno-biała	900 zł
karta katalogowa, 1 strona	1000 zł

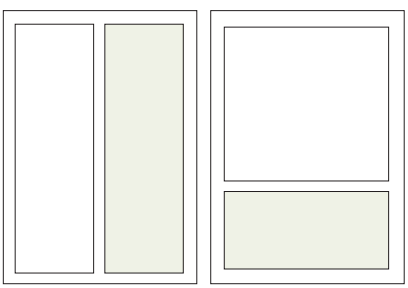


cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1600 zł (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)



1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

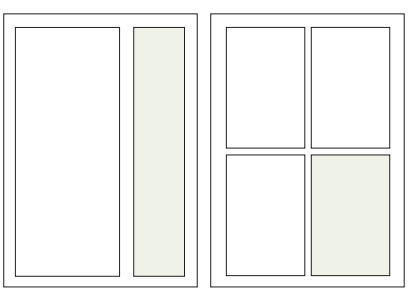
Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5200 zł
przedostatnia strona	5200 zł
ostatnia strona	5200 zł

Spis teleadresowy:

jednorazowy wpis	70 zł

Redakcja przyjmuje zamówienia na 6 kolejnych emisji



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Podane ceny nie uwzględniają podatku VAT (23%)

Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej **http://www.zabezpieczenia.com.pl** w dziale **Reklama**

Spis reklam

HDCVI – pierwszy analogowy system dozoru wizyjnego o rozdzielczości HD

Łatwy i tani sposób modernizacji standardowego systemu CCTV i uzyskania obrazu o rozdzielczości HD

- Liczba klatek na sekundę – 25/30/50/60 przy 720p, 25/30 przy1080p
- Transmisja sygnału przy użyciu kabla koncentrycznego:
  — 500 m dla kabla RG59/700 m dla kabla RG6
- Transmisja sygnału przy użyciu kabla sieciowego:
  — 200 m dla kabla UTP
- Dostępne trzy tryby pracy - HDCVI, IP, analogowy
- Transmisja trzech sygnałów (wizja, dźwięk, sterowanie) jednym kablem
- Zgodność ze standardem HDcctv AT 2.0

Recomendowane modele:

wodoodporne kamery HDCVI o rozdzielczości 720p/1080p
HAC-HFW2100S/2200S

kopułkowe, wodoodporne kamery HDCVI o rozdzielczości 720p/1080p z oświetlaczem IR
HAC-HDW2100S/2200S

trzysystemowy rejestrator wizyjny 4/8/16 kanałów (tryb HDCVI, IP i analogowy), wysokość 1.5U
HCVR7404/7408/7416L

trzysystemowy rejestrator wizyjny4/8/16 kanałów (tryb HDCVI, IP I analogowy), wysokość 2.0U
HCVR7804/7808/7816S

kopułowa kamera szybkoobrotowa PTZ HDCVI o rozdzielczości 1.3Mp
SD63120I-HC

kopułowa kamera szybkoobrotowa PTZ HDCVI o rozdzielczości 1.3Mp z oświetlaczem IR
SD6C120I-HC

CE FC RoHS ISO 9001:2000

SECURITY ESSEN 2014
23–26 Sep 2014 Essen, Germany
Booth: 2.0-104, Hall 2

DAHUA TECHNOLOGY CO., LTD.
No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com
www.dahuasecurity.com

OPTEX
Sensing Innovation

BARIERA PODCZERWIENI

Seria Smart Line™

MODELE PRZEWODOWE

MODELE ROZBUDOWANE

SL-200QDM : 60m
SL-350QDM : 100m
SL-650QDM : 200m

MODELE STANDARDOWE

SL-200QDP : 60m
SL-350QDP : 100m
SL-650QDP : 200m

MODELE PODSTAWOWE

SL-200QN : 60m
SL-350QN : 100m
SL-650QN : 200m

MODELE ZASILANE BATERYJNIE

MODEL STANDARDOWY

SL-350QFR : 100m

MODEL PODSTAWOWY

SL-350QNR : 100m

www.optex.com.pl