CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(77)/2011

ZABEZPIECZENIA

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

W NUMERZE:

Pomóż przedsiębiorstwom **skoncentrować się na wynikach.**

Dobry system nadzoru wizyjnego daje więcej niż tylko nagrywanie zdarzeń. Zwiększa on zdolność do zapobiegania niepożądanym zdarzeniom i ich kontroli-pozwalając skoncentrować się na bieżących sprawach biznesowych.

Połącz nową linię kompaktowych, ekonomicznych sieciowych kamer Axis z serii M z oprogramowaniem AXIS Camera Station lub rozwiązaniem do zarządzania materiałem wizyjnym któregoś z naszych partnerów, by stworzyć prawdziwie efektywny system nadzoru HDTV.

Łatwy do zainstalowania i obsługi, system sieciowego nadzoru Axis dostarcza jakość obrazu, która może stanowić dowód w sprawie, jak też elastyczność i skalowalność potrzebną by uwzględniać zmieniające się potrzeby. Możemy więc spokojnie postawić na wybór bezproblemowego nadzoru wizyjnego, który pozwala koncentrować się, na tym co rzeczywiście jest dla nas ważne.

Przyjmij punkt widzenia Axis. Bądź zawsze o krok do przodu. SKONCENTRUJ SIĘ z Promocją dla Partnerów Axis ! Odwiedź www.axis.com/pl/

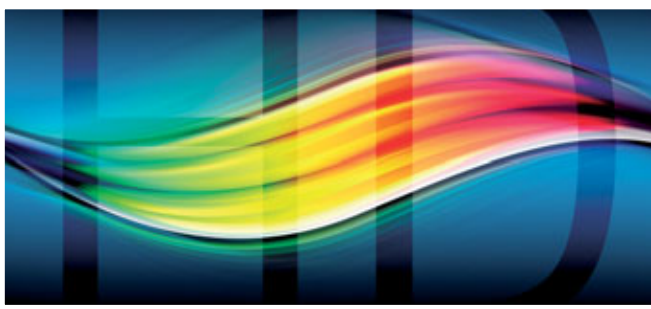
www.axis.com/focus
Kamery sieciowe AXIS M11, AXIS M32 i AXIS M10, w połączeniu z oprogramowaniem AXIS Camera Station dostarczają kompletne rozwiązanie sieciowego nadzoru wizyjnego do 50 kamer ze wsparciem HDTV,H.264 i Power over Ethernet.

AXIS COMMUNICATIONS

Spis treści

CZASOPISMO ZABEZPIECZENIA 1/2011

Rynek nie znosi pustki **18**



Kamery HDTV firmy Axis Communications w nowoczesnych systemach dozoru wizyjnego **36**

Co z tym XXI wiekiem? **50**

Instalacje wykrywania pożaru w przestrzeniach zagrożonych wybuchem (Część I) **54**

Zdjęcie: NCS / J.Kośnik

Bezpieczeństwo podczas EURO 2012

Systemy DSO i SAP firmy Bosch na Stadionie Narodowym

Dokonano już wyboru dostawcy **dźwiękowego systemu ostrzegawczego** (DSO) oraz **sygnalizacji alarmu pożarowego** (SAP), które mają być zainstalowane na Stadionie Narodowym. Dostawcą tym będzie firma **Bosch Security Systems**.

System DSO będzie bazować na Praesideo oraz głośnikach do emisji komunikatów informacyjnych, ostrzegawczych i ewakuacyjnych. Praesideo to sztandarowe rozwiązanie firmy Bosch, które zostało niejednokrotnie sprawdzone w wielu obiektach wielkopowierzchniowych. W pełni cyfrowy system Praesideo daje praktycznie nieograniczone możliwości wdrożenia wielostrefowego i sieciowego. Połączenie z systemem alarmu pożarowego zapewnia szybką ewakuację widzów z zagrożonych obszarów w przypadku wybuchu pożaru. Wysoka jakość dźwięku umożliwia nadawanie wyraźnych komunikatów głosowych kierujących ludzi do dróg ewakuacyjnych.

System sygnalizacji pożarowej na Stadionie Narodowym będzie bazować na nowatorskiej, modułowej centrali **FPA5000**. Łatwa rozbudowa, bezproblemowa adaptacja do warunków lokalnych i przepisów prawnych, przejrzysty i prosty interfejs użytkownika to tylko część zalet centrali FPA5000. Centralę można też łatwo obsługiwać już po krótkim przeszkoleniu, co minimalizuje liczbę błędów popełnianych przez operatora. Możliwość przyłączenia do centrali FPA5000 innych systemów zabezpieczeń firmy Bosch pozwala stworzyć całościowy system ochrony, który zapewni bezpieczeństwo kibicom na stadionie. Warto przypomnieć, że centrala FPA5000 została również niedawno wybrana na stadion Loftus Versfeld w Pretorii w Republice Południowej Afryki, gdzie rozgrywał się Mundial 2010.

Stadion Narodowy w Warszawie jest przygotowywany do Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012. Zostaną na nim rozegrane trzy spotkania grupowe, mecz otwarcia wraz z oficjalną ceremonią, jeden ćwierćfinał i jeden półfinał. Trybuny stadionów pomieszczą 55 tys. kibiców.

Za budowę areny i przygotowanie wyposażenia służącego do zarządzania kompleksem sportowo-biznesowym odpowiada Narodowe Centrum Sportu – spółka Skarbu Państwa powołana przez Ministra Sportu i Turystyki. Stadion Narodowy w Warszawie został zaprojektowany przez firmy: Konsorcjum JSK Architekci, GMP International oraz Schlaich Bergermann und Partner. Generalnymi wykonawcami budowy Stadionu Narodowego w Warszawie są: Konsorcjum ALPINE BAU DEUTSCHLAND, ALPINE BAU, ALPINE Construction Polska, Hydrobudowa Polska i PBG.

Bezpośr. inf. Bosch Security Systems

Nowe urządzenia pamięci masowej **Bosch serii DLA 1200 i DLA 1400**

Firma **Bosch** wprowadza na rynek **urządzenia pamięci masowej do sieciowych systemów monitoringu wizyjnego serii DLA 1200 i DLA 1400**. Są to proste, scentralizowane, wielofunkcyjne systemy zarządzania pamięcią masową z obsługą odpowiednio 64 lub 128 kanałów. Te inteligentne urządzenia pamięci masowej IP eliminują potrzebę stosowania osobnego sieciowego rejestratora wizyjnego (NVR) z serwerem i urządzeniem pamięci masowej. Może to obniżyć całkowity koszt eksploatacji systemu nawet o 45%, a także zmniejszyć łączne zapotrzebowanie na moc zasilania.

Urządzenia te oferują przestrzeń pamięciową o pojemności do 4 TB (seria DLA 1200) lub 8 TB (seria DLA 1400). Wraz z oprogramowaniem Video Recording Manager (VRM) stanowią idealne rozwiązania pamięci masowej dla małych i średnich instalacji sieciowego monitoringu wizyjnego. Ich zwarta konstrukcja, niewymagająca pracochłonnych zabiegów konserwacyjnych, łączy w sobie funkcje serwera NVR oraz inteligentnego archiwum wizyjnego, co zmniejsza liczbę potencjalnych punktów mogących ulec awarii. Instalacja typu Plug and Play i rejestracja za pośrednictwem sieci sprawiają, że są to doskonałe urządzenia dla klientów, którym nieobce są zagadnienia informatyczne w systemach sieciowego monitoringu wizyjnego.

Urządzenia z serii DLA 1200 mają kompaktową obudowę typu wieża, charakteryzują się wyjątkowo cichą pracą i umożliwiają wymianę dysków w miejscu instalacji. Pozwalają nagrywać obrazy z maksymalnie 32 sieciowych urządzeń wizyjnych (z opcjonalną licencją na rozbudowę do obsługi 64 urządzeń). Dodanie bezpłatnego oprogramowania Bosch Video Client (BVC) zmienia urządzenie z serii 1200 w niezwykle tani 16-kanałowy system IP do zarządzania rejestracją obrazów. Dodatkowe licencje na kamery BVC umożliwiają rozbudowę systemu do pełnych 64 kanałów. BVC umożliwia użytkownikom równoczesne oglądanie obrazów z kamer o różnych rozdzielczościach, w tym HD (1080p i 720P) lub SD. Dodatkową pojemność archiwum można uzyskać przez połączenie kilku urządzeń z serii 1200.

Seria DLA 1400 umożliwia rejestrację nawet 64 kanałów IP na jednym urządzeniu (a w przypadku opcjonalnej licencji na rozbudowę – do 128 kanałów). Ma obudowę stelażową o wysokości 1U (z 4 wnękami) lub 2U (z 8 wnękami). Jest wyposażona w dyski, które można wymieniać podczas pracy, oraz mechanizm ochrony danych RAID-5, co zapewnia długi czas pracy systemu bez przestojów. W połączeniu z oprogramowaniem Bosch VMS Lite staje się kompletnym systemem zarządzania rejestracją obrazów z maksymalnie 64 kamer. Użycie większej liczby urządzeń z serii 1400 i oprogramowania Bosch VMS Professional Edition pozwala uzyskać skalowalność do 512 kamer.

Urządzenia pamięci masowej z serii DLA 1200 i DLA 1400 są bardzo proste w instalacji, użytkowaniu i zarządzaniu. Wspomaganie przez kreator i scentralizowana konfiguracja skracają czas instalacji nawet o 50%. Wszystkie części składowe systemu są dostarczane w stanie wstępnie zainstalowanym i skonfigurowanym. Po podłączeniu do sieci i włączeniu zasilania urządzenia są gotowe do rozpoczęcia rejestracji.

Bezpośr. inf. Bosch Security Systems

Co to znaczy ONVIF i dlaczego jest tak ważne?

Coraz większy udział w rynku mają cyfrowe systemy obserwacyjne, wykorzystujące transmisję przez sieć IP. Niestety wzajemne łączenie i dopasowywanie kamer i rejestratorów DVR różnych marek nie jest tak proste, jak było w systemach analogowych. W cyfrowych systemach wizyjnych podstawowe elementy składowe, jak kamery IP i sieciowe rejestratory wizyjne, są często (w przeciwieństwie do systemów analogowych) niestandardowe, a przez to niekompatybilne z oprogramowaniem do zarządzania obrazami (VMS).

W praktyce okazało się, że każdy producent kamer cyfrowych stworzył oddzielny interfejs komunikacyjny. Wprawdzie wykorzystuje się standardowe metody kompresji (H.264, MPEG-4) i transmisji strumieniowej (RTSP), ale interfejsy do przesyłania sygnałów sterujących nie są jeszcze standaryzowane, dlatego producenci oprogramowania VMS i rejestratorów NVR muszą stworzyć oddzielne interfejsy dla kamer różnych producentów.

Mimo że wiodący dostawcy oprogramowania VMS zaimplementowali setki kamer i koderów na swoich platformach, nadal zdarza się, że oprogramowanie obsługuje niektóre funkcje jednej kamery, ale już nie innej.

W celu rozwiązania tego problemu powstało ONVIF (*Open Network Video Interface Forum*) – Forum Otwartych Interfejsów Sieciowych Systemów Wizyjnych. W ramach ONVIF podjęto próbę znormalizowania interfejsów dla cyfrowych systemów obserwacji wizyjnej pracujących w sieciach IP, w tym: konfiguracji urządzeń, obsługi zdarzeń, sterowania kamer PTZ itp. Oznacza to, że wyroby z certyfikatem ONVIF mogą ze sobą współpracować.

Bezpośr. inf. Tom Brigham
BRIGHAM SCULLY
Tłumaczenie i opracowanie: Redakcja

Samsung wprowadza szybkoobrotową kamerę IP z 43-krotnym zoomem optycznym

Nowa **szybkoobrotowa kamera IP SNP-3430H** firmy **Samsung** posiada 43-krotny zoom optyczny, pozwalający operatorowi rozpoznawać szczegóły znacznie oddalonych osób lub obiektów.

Porty lotnicze i morskie, parkingi i stadiony sportowe – to typowe miejsca stosowania kamery, pozwalające na pełne wykorzystanie jej funkcjonalności, a zwłaszcza szerokiego zakresu zmian ogniskowej: od 3,2 do 138,5 mm. SNP-3430H umożliwia operatorowi obserwowanie obiektów z rozdzielczością 600 linii telewizyjnych w trybie kolorowym.

– *Użytkowe cechy kamery SNP-3430H wywierają wrażenie na każdym, kto miał z nią do czynienia* – twierdzi **Peter Ainsworth**, główny kierownik produktu firmy Samsung Techwin Europe. – *W praktyce zakres zmian ogniskowej od 3,2 do 138,5 mm oznacza, że w odległości 10 m od kamery operator widzi scenę o szerokości 5 m i wysokości 4,5 m, natomiast przy ogniskowej 138,5 mm w odległości 100 m od kamery dokładnie widać postać ludzką.*

Kamera SNP-3430H, o klasie szczelności obudowy IP66, jest wyposażona w szeroki zakres funkcji, w tym cyfrową stabilizację obrazu (DIS – *Digital Image Stabilization*) niwelującą drgania wywołane działaniem silnego wiatru na kamerę zamontowaną na słupie lub wysokim budynku. Kamera z procesorem DSP A1 wykorzystuje technikę skanowania progresywnego (*Progressive Scan*), zapobiegającą nieostrościom podczas odtwarzania obrazów szybko poruszających się obiektów, oraz posiada funkcję rozszerzania zakresu dynamiki (WDR – *Wide Dynamic Range*), która selektywnie dostosowuje jasność obszarów o różnym poziomie oświetlenia.

Inteligentna analiza obrazu (IVA – *Intelligent Video Analytic*) obejmuje wykrycie przekroczenia linii, kierunku przemieszczania się oraz pojawiania się lub znikania obiektu w obserwowanej scenie. Zaimplementowana analiza obrazu obejmuje również detekcję sabotażu takiego jak zamalowanie kopuły kamery, jej zasłonięcie lub przemieszczenie poza dotychczasowe pole widzenia.

Kamera SNP-3430H może w czasie rzeczywistym przesyłać sygnał wizyjny o rozdzielczości do 4CIF (704×576) z kompresją H.264 lub MPEG-4. Może też jednocześnie przesyłać wysokiej jakości obrazy MJPEG.

Do innych jej istotnych cech należą:

– dwukierunkowa transmisja dźwięku umożliwiająca komunikację interaktywną między kamerą SNP-3430H a dyspozytornią;
– system zasilania HPoE (*High Power over Ethernet*), obniżający koszty instalacji przez użycie jednego kabla sieciowego zarówno do zasilania, jak i przesyłania sygnału wizyjnego/fonicznego;
– 12 definiowanych przez użytkownika programowalnych wielokątnych stref prywatności;
– wielojęzyczne menu ekranowe;
– gniazdo na kartę pamięci SD do lokalnego zapisu lub przechowywania kopii zapasowej obrazu zapisanego w trybie alarmowym;
– wbudowany harmonogram umożliwiający zaprogramowanie sześciu procedur działania
– bezpłatne oprogramowanie do centralnego zarządzania i podglądu NET-I Viewer;
– bezpłatne oprogramowanie do czterokanałowego zapisu obrazu NET-I.

Kamera SNP-3430H jest dostępna z szerokim wyborem uchwytów do montażu ściennego, sufitowego i narożnego.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung Techwin Europe mianuje kierownika zespołu przedsprzedaży dla Polski i krajów bałtyckich

Kierownikiem zespołu przedsprzedaży **Samsung Techwin Europe**, obsługującego klientów w Polsce i krajach bałtyckich, został mianowany **Piotr Rogalewski**. Będzie on odpowiedzialny za świadczenie wsparcia przedsprzedażowego dla instalatorów, integratorów systemów i dystrybutorów działających w Polsce i krajach bałtyckich (Litwie, Łotwie i Estonii).

Piotr Rogalewski przeszedł do grupy Samsung z firmy ADI Global Distribution, gdzie pracował przez ostatnie sześć lat. Jego doświadczenie w branży elektronicznej obejmuje także cztery lata pracy w firmie Honeywell.

– *Jestem bardzo zadowolony, że mam możliwość pracy w firmie Samsung w czasie, gdy staje się ona dostawcą kompletnych rozwiązań w zakresie zabezpieczeń* – powiedział **Piotr Rogalewski**. – *Na przykład wzbogacenie oferty o system kontroli dostępu jest widocznym znakiem dążenia Samsunga do oferowania produktów i technologii z różnych grup produktowych, integrujących się w sposób dający rzeczywiste korzyści końcowemu użytkownikowi. Pragnę świadczyć klientom firmy porady w zakresie projektowania systemów w celu umożliwienia im idealnego dobrania produktów dla danego projektu lub zastosowania.*

Z Piotrem Rogalewskim można się skontaktować za pomocą poczty elektronicznej: piotr.rogalewski@samsung.com.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung wprowadza odporną na czynniki atmosferyczne kamerę z 37-krotnym zoomem optycznym ze zintegrowaną obudową

Kamerę **z 37-krotnym zoomem optycznym** i ze zintegrowaną obudową **SCO-2370** można określić mianem „wszystko w jednym", ponieważ jest dostarczana z obudową, uchwytem montażowym, grzałką, wentylatorem i osłoną przeciwsłoneczną oraz z kablem o długości jednego metra wyposażonym w odpowiednie złącza, co pozwala instalatorom zaoszczędzić czas oraz zmniejszyć koszty inwestycji.

W kamerze zastosowano procesor DSP W-V firmy **Samsung** do przechwytywania wysokiej jakości kolorowych obrazów o rozdzielczości 600 linii TV i obrazów czarno-białych o rozdzielczości 700 linii TV.

Stacje benzynowe, szkoły, sklepy i budynki gospodarcze to przykładowe miejsca zastosowań kamery z 37-krotnym zoomem optycznym. Obudowa kamery SCO-2370 o stopniu ochrony IP68 umożliwia jej stosowanie w trudnych warunkach środowiskowych, jak na przykład w portach morskich. Inne funkcje kamery to: osiem stref detekcji ruchu, dwanaście stref prywatności oraz technologia redukcji szumów trzeciej generacji *Samsung Super Noise Reduction* (SSNRIII).

Możliwość sterowania za pomocą kabla koncentrycznego zapewnia dostęp do menu ekranowego (czternaście wersji językowych) z poziomu dyspozytorni, poprzez kompatybilny, cyfrowy rejestrator obrazu DVR, np. z najnowszej serii rejestratorów SRD.

Inną użyteczną funkcją kamery jest *Highlight Compensation* – eliminacja silnych, punktowych źródeł światła umożliwiająca operatorowi oglądanie bardzo kontrastowych obrazów. Kamera SCO-2370 posiada również funkcję rozszerzania zakresu dynamiki *Samsung Super Dynamic Range* (SSDR), która selektywnie wyrównuje jasność obszarów o różnym poziomie oświetlenia. Dzięki temu obszary ciemne stają się lepiej widoczne, co umożliwia operatorowi oglądanie obiektów niedostatecznie oświetlonych.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Nowy czterokanałowy cyfrowy rejestrator obrazu popularnej klasy **DVR H.264** firmy **Samsung**

Firma **Samsung** wprowadziła na rynek czterokanałowy cyfrowy rejestrator obrazu (DVR – *Digital Video Recorder*) popularnej klasy, przeznaczony dla systemów monitoringu małych sklepów, biur i mieszkań.

Chociaż jest oferowany po niskiej cenie, **małogabarytowy rejestrator obrazu SRD-450** nie ustępuje jakością innym produktom. Wyposażono go w szereg interesujących funkcji, m.in. możliwość zapisu obrazów z rozdzielczością CIF w czasie rzeczywistym we wszystkich kanałach, możliwość zapisu obrazów z rozdzielczością 4-CIF w wybranych kanałach oraz jednokanałowy zapis dźwięku.

Rejestrator SRD-450 umożliwia zdalne oglądanie obrazów telewizyjnych w trybie „na żywo" oraz obrazów pochodzących z rejestracji. Można je przeglądać przez Internet, za pomocą przeglądarki, a nawet na smartphonie. Dzięki zastosowaniu kompresji H.264, znacznie wydajniejszej od innych technik kompresowania, SRD-450 wykorzystuje większość dostępnego pasma sieciowego do transmisji obrazów. Ponadto zastosowanie kompresji H.264 maksymalizuje ilość danych wizyjnych, jakie można zapisać na wewnętrznym dysku twardym rejestratora SRD-450 o pojemności 500 GB (z możliwością rozbudowy).

W celu lepszego wykorzystania wewnętrznego dysku twardego można tak zaprogramować rejestrator SRD-450, aby zapisywał obraz tylko po wykryciu aktywności przez funkcję wykrywania ruchu *Motion Detection*, a kopię zapasową zapisanych obrazów związanych z ważnymi zdarzeniami można łatwo wykonać za pomocą portu USB.

Rejestrator SRD-450 zaprojektowano z myślą o łatwej obsłudze, co uzyskano dzięki zaledwie pięciu zestawom przycisków na przednim panelu i łatwemu do zrozumienia menu ekranowemu. Przykładowo, zdalny dostęp do materiału wizyjnego przez Internet uzyskuje się przez wpisanie w przeglądarce internetowej adresu IP rejestratora DVR oraz nazwy i hasła użytkownika.

Konstrukcja rejestratora SRD-450 zapewnia dobre chłodzenie podczas pracy, eliminując konieczność stosowania wentylatora, co czyni rejestrator SRD-450 idealnym w zastosowaniach domowych, gdzie hałas może być uciążliwy dla użytkownika.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Nowość w ofercie szkoleniowej PISA

Nowe regulacje normatywne i zmiany w przepisach prawa dotyczące systemów alarmowych wygenerowały – zarówno po stronie inwestorów i administratorów zabezpieczeń technicznych, jak i wykonawców tego rodzaju usług – zapotrzebowanie na uzupełnienie wiedzy w tym zakresie oraz konieczność podniesienia specjalistycznych kwalifikacji. **Polska Izba Systemów Alarmowych** (PISA), odnotowując rosnące zainteresowanie własnymi inicjatywami szkoleniowymi i odpowiadając na te wyzwania, przygotowała nową propozycję szkoleniową: seminarium kwalifikacyjne **„Określanie poziomów ryzyka i stopni zabezpieczenia technicznego w świetle najnowszych uregulowań normatywno-prawnych”**.

Zajęcia seminaryjne będą prowadzić eksperci i wykładowcy Ośrodka Szkoleniowego PISA biorący aktywny udział w pracach nad polskimi projektami nowoczesnych europejskich norm technicznych oraz nad projektem nowego rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.

PISA dedykuje program seminarium wszystkim, którzy są zainteresowani:

– uzyskaniem poszerzonej specjalistycznej wiedzy niezbędnej do określania poziomu ryzyka i stopni zabezpieczenia technicznego w ochronie osób i mienia, w oparciu o nowoczesne wymagania normatywno-prawne;
– zdobyciem umiejętności rozwiązywania problemów związanych z dostosowaniem realizacji zabezpieczeń technicznych do nowych wymagań prawnych i normatywnych;
– udziałem w warsztatach projektowych prowadzonych na bazie scenariuszy systemów zabezpieczeń technicznych stopni 1–4.

Pierwsze seminarium zostanie przeprowadzone w dniach 2–4 lutego 2011 roku. Następne zajęcia będą organizowane w każdym kolejnym miesiącu.

Absolwenci trzydniowego seminarium legitymujący się świadectwami ukończenia kursów projektowania w dawnych klasach SA1-SA4 otrzymają zaświadczenia o uzyskaniu kwalifikacji do projektowania systemów zabezpieczeń technicznych w stopniach 1–4.

Bezpośr. inf. PISA

PISA zaprasza na kursy i seminaria

Polska Izba Systemów Alarmowych (PISA) organizuje następujące kursy i seminaria:

– kurs pracownika zabezpieczenia technicznego pierwszego stopnia **„Instalowanie i konserwacja systemów zabezpieczeń technicznych stopni 1–4/klas SA–SA4”**,
– kurs pracownika zabezpieczenia technicznego drugiego stopnia **„Projektowanie systemów zabezpieczeń technicznych stopni 1–4/klasy SA4 NO”**,
– kurs pracownika zabezpieczenia technicznego **„Montaż, eksploatacja, konserwacja i naprawa urządzeń i środków mechanicznego zabezpieczenia”,**
– kurs inwestorów i administratorów systemów zabezpieczeń technicznych,
– kurs audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji (SZBI) WG ISO 27001,
– seminarium kwalifikacyjne **„Określanie poziomów ryzyka i stopni zabezpieczenia technicznego w świetle najnowszych uregulowań normatywno-prawnych”,**
– kurs kosztorysowania systemów zabezpieczeń technicznych,
– kurs ekspertów i doradców w zakresie bezpieczeństwa,
– kursy specjalistyczne,
– seminaria dokształcające dla ekspertów i doradców.

Absolwenci kursów i seminariów otrzymują wystawione **bezterminowo** dokumenty:

– zaświadczenie o ukończeniu kursu (druk MEN),
– dyplom Ośrodka Szkoleniowego PISA.

Bezpośr. inf. OS PISA

HID Global
wprowadza system naklejek do bezpiecznych płatności bezstykowych i identyfikacji

HID Global zapowiedział wprowadzenie wygodnych w użyciu i wytrzymałych naklejek na karty do płatności i identyfikacji bezstykowej. Naklejki ułatwiają przystosowanie istniejących systemów do realizacji bezstykowego automatycznego poboru opłat lub identyfikacji osób w systemach kontroli dostępu. Mogą również być przyklejane do telefonów komórkowych dla ułatwienia realizacji np. płatności Pass Payment.

Naklejki mają wewnętrzną warstwę ferrytową chroniącą przed zakłóceniami w razie naklejenia na metal (np. na telefon komórkowy). Można na nie nadrukować informację klienta (numery telefonów, kody, logo itp.). Działają w systemach kompatybilnych z MIFARE, MIFARE DESFire i iCLASS.

Dostępne są w ilościach handlowych i jako wzorce. Można je zadrukować u klienta (HID Global ułatwi to zadanie).

Dokładniejsze informacje można uzyskać u przedstawicieli handlowych HID Global.

Bezpośr. inf. Jeremy Hyatt
Global Public Relations
Tłumaczenie: Redakcja

HID Global wspomaga
adaptację e-paszportów i e-dowodów osobistych w Europie

Czytniki bezprzewodowe HID odgrywają coraz większą rolę w rozbudowie infrastruktury systemów do odczytu e-paszportów, e-wiz i e-dowodów osobistych na świecie

HID Global zapowiedział, że technika **czytników bezprzewodowych do odczytu dokumentów tożsamości** (paszportów, dowodów osobistych) jest obecnie wdrażana we Francji, Niemczech, Włoszech, Holandii i Hiszpanii. W pierwszej połowie 2011 roku firma będzie upowszechniać tę technikę za pośrednictwem wiodących integratorów systemowych w dwóch kolejnych krajach.

Moduły czytników HID oferują najszybsze rozwiązanie do biometrycznego odczytu paszportów i pozwalają na zastosowanie ich w systemach podstawowej oraz rozbudowanej kontroli dostępu. Wkładki do dowodów i paszportów HID, czytniki i drukarki są wykorzystywane przez ministerstwa spraw wewnętrznych i spraw zagranicznych w ponad 27 programach paszportowych i 31 programach obsługi dowodów osobistych, ułatwiając życie ponad 120 milionom posiadaczy e-dokumentów.

System podstawowej kontroli jest stosowany do urzędowej identyfikacji tożsamości, w meldunkach hotelowych, automatycznej rejestracji w liniach lotniczych, kupowaniu usług telefonii komórkowej itp. System kontroli rozbudowanej jest wykorzystywany do biometrycznej emisji e-dokumentów oraz automatycznego przekraczania granic, łącznie z lotniskami, w Finlandii, Francji, Niemczech, Portugalii i Wielkiej Brytanii. Ponieważ ponad 30 krajów w Europie przeprowadziło migrację e-paszportów do systemu rozbudowanej kontroli dostępu, a tylko część z nich posiada odpowiednią infrastrukturę do ich odczytu, należy oczekiwać gwałtownego wzrostu zastosowań tych czytników.

Bezpośr. inf. Jeremy Hyatt
Global Public Relations
Tłumaczenie: Redakcja

Wszystko o HDTV – podsumowanie

24 listopada 2010 roku w salach konferencyjnych hotelu Intercontinental firma **AXIS Communications**, której główna siedziba znajduje się w Lund (Szwecja), zorganizowała **seminarium pod tytułem „Wszystko o HDTV”**.

Firma AXIS Communications specjalizuje się w produkcji i dostawie sieciowych systemów telewizji dozorowej. Program dostaw omówiła przedstawicielka firmy **Agata Majkucińska**. Gama oferowanych produktów rozciąga się od kamer stałopozycyjnych, tradycyjnych i kopułkowych, poprzez kamery PTZ (ruchome z możliwością zdalnego sterowania ogniskową obiektywu) i kamery kopułkowe PTZ, aż po kamery termowizyjne o czułości poniżej 100 mK.

Do budowy systemów hybrydowych firma dostarcza również szeroką gamę koderów i dekoderów wizyjnych.

Szczególną uwagę poświęcono rozwojowi systemów HDTV, zapewniających rozdzielczość 1920×1080 pikseli. Stwierdzono, że systemy HDTV pracują w formacie 16:9, ponieważ najbardziej odpowiada on naturalnej percepcji wzroku ludzkiego.

Systemy sieciowe poza znacznymi oszczędnościami na okablowaniu umożliwiają precyzyjne sterowanie kamerami, ich identyfikację w systemie i lokalizację stwierdzonych zagrożeń.

W drugiej części seminarium inżynier **Nadir Yilmaz** przedstawił sposoby doboru i rozmieszczania kamer telewizyjnych w zależności od konfiguracji obiektu i potrzeb klienta. Prelegent zaprezentował możliwość wykorzystania oprogramowania firmowego AXIS, dostępnego dla partnerów tej firmy na stronach internetowych AXIS do projektowania rozmieszczenia i doboru kamer. Optymalny dobór kamer, ułatwiony dzięki temu oprogramowaniu, pozwala wykorzystać właściwości kamer i obiektywów (nie zawsze i nie wszędzie potrzebne są kamery o największej czułości lub najbardziej wyśrubowanych parametrach).

Redakcja

Niecodzienne zadanie postawione przed kamerą **Axis Communications**

Niecodzienne zadanie postawione przed kamerą związane było z badaniem atmosfery realizowanym przez szwedzki ośrodek **Esrange Space Center**, należący do firmy **Swedish Space Corporation**. Wypuścił on na wysokość 35 tys. metrów specjalny balon przeznaczony do lotów na dużych wysokościach i wyposażony w narzędzia badawcze służące do analizy stanu atmosfery. Po przeprowadzeniu testów wypełniony gazem balon o objętości 100 tys. metrów sześciennych ściągnięto na Ziemię przy użyciu trzech spadochronów. Umieszczenie w jednym z nich kamery **AXIS Q6034-E**, która w czasie rzeczywistym przesyłała materiał wizyjny wysokiej rozdzielczości, pozwoliło naukowcom kontrolować na bieżąco proces lądowania. Ostatecznie balon wylądował w północnej Finlandii, co wymagało, aby kamera przesyłała obraz z odległości czterystu kilometrów, korzystając z sieci bezprzewodowej.

– Przeznaczone do zewnętrznego nadzoru wizyjnego kamery sieciowe Axis tworzone są z myślą o ekstremalnych warunkach pogodowych, dlatego zawsze gwarantują niezawodne działanie. Jesteśmy dumni z tego, że nasza kamera przez ponad trzy godziny przesyłała wysokiej jakości obraz w temperaturze –73°C, przy czym najniższa temperatura, w jakiej AXIS Q6034-E pracował w trakcie tego badania, wynosiła –90°C – powiedział **Erik Fränlid**, dyrektor ds. zarządzania produktami w firmie Axis Communications.

Badacze z ośrodka Esrange Space Center również chwalą wyniki testów. – *Możliwość obserwowania na bieżąco przebiegu badania i lądowania w połączeniu z rejestracją wyników pomiarów to zalety nie do przecenienia, kiedy spadochrony nie działają*

właściwie lub gdy nie wiadomo, gdzie wylądują. Taka obserwacja pozwala na prawidłowe zinterpretowanie sytuacji i zabezpieczenie balonu przed niepomyślnymi lądowaniami w przyszłości – wyjaśnił **Per Baldemar**, kierujący zespołem odpowiedzialnym za badania z wykorzystaniem systemów rakietowych i balonowych w firmie Swedish Space Corporation.

Bezpośr. inf. Katarzyna Wójcik
Grayling Poland

Dobre prognozy dla polskiego rynku ochrony i zabezpieczeń dzięki Euro 2012

Ożywienie w sektorze budowlanym spowodowane przygotowaniami do mistrzostw Euro 2012 oraz ostatnie działania konsolidacyjne na rynku firm ochroniarskich wpływają pozytywnie na zmiany w strukturze polskiego rynku ochrony i zabezpieczeń. Ponadto zarówno gracze na rynku, jak i użytkownicy coraz bardziej doceniają znaczenie zabezpieczenia technicznego.

Według najnowszego raportu globalnej firmy doradczej **Frost&Sullivan**, pt. *Rynek ochrony i zabezpieczeń w Polsce*, sektor ten w 2009 roku wygenerował przychody na poziomie 1648,5 mln euro. Co więcej, szacuje się, że w 2015 roku sięgną one nawet 2925,9 mln euro. W raporcie uwzględniono następujące technologie: wykrywanie włamań (w tym monitoring), monitoring wideo (telewizja dozorowa i IP) oraz kontrolę dostępu.

Wraz ze spowolnieniem gospodarczym nastąpił spadek inwestycji w sektorze budowlanym, co z kolei negatywnie wpłynęło na rozwój rynku ochrony i zabezpieczeń. Po tegorocznym ożywieniu największa poprawa spodziewana jest w latach 2011–2012, kiedy zakończy się realizacja projektów rozpoczętych w 2010 roku. Wiele z tych inwestycji obejmuje budowę hoteli, stadionów i miejsc użyteczności publicznej, które są przygotowywane z myślą o mistrzostwach w piłce nożnej Euro 2012.

– *Ożywienie działalności budowlanej jest kwestią niezwykle istotną dla rozwoju polskiego rynku ochrony i zabezpieczeń* – zauważa **Emilia Jeleńska**, analityczka z warszawskiego oddziału Frost & Sullivan. – Spowoduje to przywrócenie zdrowego tempa wzrostu wśród producentów oryginalnego sprzętu (OEM) i dystrybutorów, jak również wśród dostawców usług powiązanych z tymi produktami.

Poprawa sytuacji w budownictwie sprawiła, że dla uczestników rynku ochrony fizycznej niezwykle ważne jest rozszerzanie oferty rozwiązań w zakresie elektronicznych systemów zabezpieczeń. Koszty takich systemów są niższe od kosztów usług świadczonych przez pracowników ochrony. Taka zmiana sprawi, że rynek ten stanie się lepiej zorganizowany i bardziej rozwinięty, podobnie jak w Europie Zachodniej.

– *Rozwój rynku jest stymulowany przez niższe ceny zabezpieczeń elektronicznych oraz konsolidację rynku ochrony fizycznej* – stwierdza Emilia Jeleńska. – Systemy monitoringu i technologie IP dostarczają obecnie nowatorskie rozwiązania, które w dłuższej perspektywie mogą stanowić bodziec do zmian na rynku ochrony, polegających na stopniowym odchodzeniu od usług ochrony fizycznej na rzecz rozwiązań technicznych.

Na rozwoju systemów monitoringu i technologii IP skorzystają najbardziej integratorzy systemów, którzy są w stanie najszybciej zaspokoić potrzeby rynku ze względu na dotychczasowe doświadczenie w branży IT i praktykę biznesową. Agencje ochrony oraz firmy instalacyjne wdrażają wśród użytkowników systemy wykrywania włamań oraz systemy telewizji dozorowej (CCTV) – te dwie technologie generują 90% całkowitych przychodów rynku.

– *Konsolidacja rynku usług ochrony fizycznej, wraz ze wzmocnieniem obecności na nim integratorów systemów, to dwie tendencje, które mogłyby ułatwić rozwój usług zorientowanych w większym stopniu na rozwiązania* – podsumowuje Jeleńska. – *Spowodowałoby to również uporządkowanie sytuacji w rozdrobnionym obecnie sektorze.*

Rynek ochrony fizycznej osób i mienia w Polsce jest częścią programu Rozwoju Usług Partnerskich w Sektorze Automatycznej Identyfikacji i Ochrony, który obejmuje również badania w następujących obszarach rynkowych:

– możliwości rozwoju na światowym rynku mobilnego nadzoru wideo,
– analiza analitycznych aplikacji wideo na rynku EMEA,
– europejski rynek kamer do nadzoru wideo,
– światowy rynek biometryczny,

a także

– europejski rynek konwergencji bezpieczeństwa.

Wszystkie usługi badawcze włączone do programu zapewniają szczegółowe analizy możliwości rynków i trendów w branży, poddane wnikliwej ocenie po przeprowadzeniu obszernych wywiadów z uczestnikami rynku.

Bezpośr. inf. Joanna Lewandowska
Frost&Sullivan

Cooper przejmuje Hernis Scan Systems

Cooper Safety, spółka zależna **Cooper Industries plc**, zakończyła przejmowanie **Hernis Scan Systems AS** po otrzymaniu zgody regulatora oraz uzyskaniu zgody udziałowców Vislink plc.

Wstępną umowę przejęcia Hernis Scan Systems AS od firmy macierzystej Vislink plc podpisano w listopadzie 2010 roku. Wymagała ona zgody udziałowców Vislink plc oraz zgody regulatora. Hernis jest norweskim producentem sprzętu do systemów telewizji dozorowej (CCTV), przeznaczonych do stosowania w środowiskach trudnych i niebezpiecznych. W szczególności specjalizuje się w produkcji sprzętu do systemów telewizji dozorowej w wykonaniu antywybuchowym do zastosowania w lądowych i morskich instalacjach petrochemicznych i gazowych na całym świecie.

– *Będzie to już czwarte przejęcie, którego dokonaliśmy w ciągu ostatniego roku w branży sprzętu przeznaczonego do pracy w trudnym i niebezpiecznym środowisku zagrożonym wybuchem. Pokazuje nasze dążenie do rozszerzenia oferty o nowe technologie i możliwości. Hernis stanowi strategiczne uzupełnienie istniejącej oferty sygnalizatorów optycznych i akustycznych antywybuchowych Cooper Safety oraz wiodącej oferty oprzyrządowania Cooper Crouse-Hind do środowisk trudnych i niebezpiecznych* – stwierdził **Kirk S. Hachigian**, prezes i dyrektor generalny Cooper Industries. – Ponadto to strategiczne przejęcie wspomoże naszą inicjatywę globalizacyjną, ponieważ Hernis jest silnie obecny na europejskim i azjatyckim rynku systemów telewizji dozorowej w środowiskach zagrażających wybuchem.

Bezpośr. inf. www.securityworldhotel.com
Tłumaczenie i opracowanie: Redakcja

POLVISION wprowadza
kolejne modele kamer megapikselowych

Firma **POLVISION** wprowadziła do oferty kolejną serię kamer megapikselowych, w których wykorzystano wydajną kompresję H.264. Są to niewielkie kamery dzienno-nocne, wyposażone w mechaniczny filtr podczerwieni, przeznaczone do zastosowań zewnętrznych i wewnętrznych:

– GV-BX120D Low Lux – 1280×1024, 30 kl./s, obiektyw 2,8–12 mm F1.4, 0,04 luksa
– GV-BX220D – 1920×1080, 30 kl./s, obiektyw 2,8–8,5 mm F1.4, 0,1 luksa
– GV-BX320D – 2048×1536, 20 kl./s, obiektyw 3,1–8 mm F1.2, 0,1 luksa

Warto podkreślić, że ze względu na wysoką czułość kamery megapikselowej GV-BX120D nadano jej przyrostek Low Lux, ponieważ ten model doskonale sprawdza się w **trudnych warunkach oświetleniowych**. Wraz z tą serią do sprzedaży trafiają inne specjalizowane modele kamer wysokiej rozdzielczości:

– GV-BL110 – kamera zintegrowana z obudową o klasie szczelności IP66, z promiennikiem podczerwieni o zasięgu 15 m, do zastosowań zewnętrznych i wewnętrznych;
– GV-FE111 i GV-FE421 – kolorowe kamery minikopułkowe, dookolne, 360 stopni (tzw. hemisferyczne) do zastosowań wewnętrznych.

Kamery zasilane są ze źródła prądu stałego 12 V_{DC} lub metodą PoE. Mają wbudowane wejścia i wyjścia alarmowe, a także **gniazdo na karty pamięci** (mini lub mikro SD/SDHC). Udostępniają dwa niezależnie konfigurowane strumienie wizyjne, kompresowane metodami H.264, MPEG-4 ASP lub MJPEG. Dwukierunkowa komunikacja dźwiękowa może być realizowana za pomocą wbudowanego lub zewnętrznego mikrofonu i głośnika.

Kamery są dostępne w atrakcyjnych cenach i objęte trzyletnim okresem gwarancyjnym.

Oprócz obiektywu dostarczana w zestawie jest **bezpłatna polska wersja 32-kanałowego zaawansowanego oprogramowania GV-NVR**.

Firma POLVISION planuje wkrótce wprowadzenie do oferty ponad **30 modeli kamer megapikselowych** różnego typu o rozdzielczościach od 1,3 MPix do 10 MPix.

Bezpośr. inf. Tomasz Polus
POLVISION

Rejestratory i stacje monitorujące POLVISION zgodne z ONVIF i PSIA

Wszystkie rejestratory hybrydowe i sieciowe oraz stacje monitorujące dostarczane przez firmę **POLVISION** uzyskały zgodność ze światowymi standardami ONVIF i PSIA. Dotyczy to również starszych modeli, pod warunkiem zaktualizowania w nich oprogramowania.

Zgodność z ONVIF i PSIA oznacza, że do urządzeń można podłączyć kamery sieciowe i serwery wizyjne wybrane spośród 600 modeli różnych producentów. W przyszłości można się spodziewać zwielokrotnienia tej liczby, ponieważ wszyscy producenci kamer sieciowych będą produkowali sprzęt zgodny z obowiązującymi standardami.

Bezpośr. inf. Tomasz Polus
POLVISION

POLVISION dostarcza
bezpłatne oprogramowanie NVR

Firma **POLVISION** udostępniła **bezpłatne 32-kanałowe, zaawansowane oprogramowanie NVR** przeznaczone do obsługi kamer i wideoserwerów firmy **GeoVision**. Obsługa kamer innych producentów oraz kamer zgodnych ze standardami ONVIF/PSIA jest możliwa po odpłatnym rozszerzeniu licencji. Łącznie jest to około 600 modeli kamer i wideoserwerów IP.

Oprogramowanie GV-NVR przewyższa funkcjonalnie większość rozwiązań dostępnych na rynku, oferując m.in.:

– liczne funkcje inteligentnej analizy obrazu,
– obsługę zaawansowanych, wielomonitorowych stacji operatorskich,
– aktywne i pasywne zwielokrotnianie strumieni IP za pomocą bramek wizyjnych,
– automatyczne kopiowanie nagrań na zewnętrzne dyski sieciowe zgodnie z ustalonym harmonogramem i przydziałem pasma sieciowego,
– rozbudowany system uprawnień z możliwością przechowywania bazy kont użytkowników na centralnym serwerze uwierzytelniającym,
– automatyczne zmniejszanie rozmiarów nagrań i poprawianie ich jakości poprzez redukcję szumów,
– automatyczną kontrolę pasma sieciowego – skalowanie wielkości strumieni wizyjnych do rozmiarów okien,
– tworzenie własnego interfejsu użytkownika.

Możliwości integracji oprogramowania GV-NVR z innymi systemami są prawie nieograniczone dzięki zgodności z popularnymi standardami plików wizyjnych i baz danych oraz dostępności bezpłatnego zaawansowanego pakietu SDK i wielu urządzeń dodatkowych.

Bezpośr. inf. Tomasz Polus
POLVISION

Gdziekolwiek jesteś – pełna kontrola nad alarmem **MobileKPD2 firmy Satel**

Aplikacja **MobileKPD2** firmy **Satel** zmienia telefon z ekranem dotykowym w zdalny manipulator do obsługi systemu alarmowego bazującego na centrali INTEGRA, wyposażonego w moduł ETHM-1. Dzięki MobileKPD2 możemy zdalnie sterować alarmem w dowolnej chwili, mając dostęp do wszystkich funkcji centrali osiągalnych dla użytkownika. Łączność z centralą – niezależnie od tego, czy nawiązana jest z użyciem GPRS, UMTS (3G) czy WIFI – została zabezpieczona algorytmem AES z użyciem 192-bitowego klucza. MobileKPD2 jest dostępny w dwóch wersjach – wybór jednej z nich zależy od modelu telefonu z ekranem dotykowym. Wersja Java jest przeznaczona dla urządzeń obsługujących środowisko Java J2ME (telefonów z systemem Symbian, Samsung Bada, Windows Mobile). Dla telefonów wyposażonych w system operacyjny Google Android opracowana jest dedykowana wersja aplikacji. Obie wersje można bezpłatnie pobrać ze strony *http://m.satel.pl/*, zoptymalizowanej dla urządzeń przenośnych. Listę telefonów obsługujących aplikację MobileKPD2 w wersjach Java i Android znaleźć można na stronie *www.satel.pl*.

Bezpośr. inf. Agnieszka Nocuń
Satel

Zapraszamy na nowy cykl warsztatów **VERSA**

AKADEMIA Satel ZAPRASZA

Firma **Satel** zaprasza na nowy **cykl warsztatów** poświęcony centralom alarmowym **VERSA**. Zapraszamy do wzięcia udziału w zajęciach praktyczno-teoretycznych, podczas których uczestnicy zdobędą umiejętności pozwalające na samodzielne projektowanie i programowanie systemów alarmowych małych i średnich obiektów.

Warsztaty są przeznaczone dla początkujących instalatorów oraz wszystkich zainteresowanych gamą produktów VERSA.

Zapraszamy na stronę *www.szkolenia.satel.pl*.

Bezpośr. inf. Satel

Komentarz przedstawiciela firmy Axis Communications do artykułu „PixelPro – nowa technologia marki GANZ”

Jako reprezentant firmy Axis Communications poczuwam się do obowiązku ustosunkowania się do artykułu zamieszczonego w szóstym numerze dwumiesięcznika „Zabezpieczenia” przez firmę CBC Group, pt. **PixelPro nowa – technologia marki GANZ**. Firma opisuje w artykule nową serię swoich kamer, które wykorzystują technologię sterowania przysłoną P-Iris, oraz podaje informację, że „Rozwiązanie to zostało opracowane przez CBC Group”, co odbiega od prawdy.

Technologia P-Iris została opracowana przez Axis Communications we współpracy z firmą KOWA – producentem obiektywów – i oficjalnie ogłoszona w maju 2009 roku. Po raz pierwszy zastosowaliśmy ją w naszej trzymegapikselowej kamerze AXIS P1346. Dzięki sterowaniu P-Iris kamery sieciowe osiągają nowy poziom jakości obrazu. Wprowadzając tę funkcjonalność, mieliśmy świadomość, że jest to przełomowe usprawnienie, które wywoła rewolucję w branży. Oczekujemy, że P-Iris stanie się standardem, który z czasem zastąpi obiektywy z przesłoną DC. Jak widać, proces już się rozpoczął – co nas cieszy. Producentów implementujących tę technologię w swoich urządzeniach proszę o rzetelne i oparte na faktach informowanie rynku.

Agata Majkucińska
Key Account Manager Poland
Axis Communications

Jubileuszowa sesja zorganizowana przez POLALARM

W dniu 19 listopada 2010 r. stowarzyszenie **POLALARM** zorganizowało **uroczystą sesję jubileuszową z okazji XXX-lecia** rozwoju technicznej ochrony osób i mienia w Polsce. Uroczystość ta była doskonałą okazją do przyznania szczególnie zasłużonym dla naszej branży osobom odznaczeń, wyróżnień, dyplomów i okolicznościowych medali. Z tej okazji zarząd stowarzyszenia POLALARM wystąpił do wojewodów o przyznanie odznaczeń państwowych dla najaktywniejszych działaczy. Większość wniosków, pozytywnie zaopiniowanych przez wojewodów, czeka na rozpatrzenie w Kancelarii Prezydenta RP. Trzy odznaczenia zostały przyznane przed uroczystością i wręczone na sesji. Srebrny Krzyż Zasługi otrzymał Andrzej Jurek z Łodzi, a Złote Medale za Długoletnią Służbę – Mirosław Kozyra i Jan Mróz.

Za szczególne przyczynienie się do rozwoju technicznej ochrony mienia powołana przez zarząd Kapituła Nagród pod przewodnictwem Andrzeja Ryczera przyznała Nagrody XXX-Lecia. Diamentowy Pionier – LIDER Krajowego Rozwoju Technicznej Ochrony Osób i Mienia w Polsce przypadł w udziale **Bogdanowi Tatarowskiemu**. Diamentowego Pioniera przyznano **Stefanowi Kopczyńskiemu**, **Maksymilianowi Majerskiemu**, **Alojzemu Pawelczakowi**, **Włodzimierzowi Paupie** oraz **Jackowi Szewczykowi**. 36 osób otrzymało Złotego Pioniera, a Pioniera przyznano 30 osobom.

Nagrody Specjalne, Dyplomy Uznania i Medale XXX-Lecia Rozwoju Technicznej Ochrony Osób i Mienia w Polsce przyznano (w różnych kategoriach) 92 osobom.

Wręczono także jedną Diamentową oraz osiem Złotych i Srebrnych Honorowych Odznak NOT, trzy Złote Honorowe Odznaki KIG oraz 20 Złotych Honorowych Odznak POLALARM (pełną listę nagrodzonych oraz fotorelację znajdą państwo na stronie *www.polalarm.org*).

Sesję poprowadzili prezes zarządu Bogdan Tatarowski, przewodniczący rady stowarzyszenia Włodzimierz Kuczkowski oraz wiceprzewodniczący rady Alojzy Pawelczak.

Referat *Uwarunkowania XXX-letniego rozwoju technicznej ochrony osób i mienia w Polsce* wygłosił prezes zarządu Bogdan Tatarowski.

Patronami honorowymi sesji byli prezes FSNT – NOT, prezes KIG, prezes PKN, patronami medialnymi – czasopisma *Zabezpieczenia, Systemy Alarmowe, Ochrona Mienia i Informacji, Twierdza* oraz *Przegląd Techniczny*. „Złotymi" sponsorami były firmy AAT Holding, Compas, Juwentus, Noma 2, HERTZ Systems.

Gośćmi sesji byli m.in. reprezentanci patronów honorowych, władz państwowych, polscy naukowcy, reprezentanci współdziałających instytucji, organizacji samorządowych oraz patronów medialnych.

Uroczystość uświetnił koncert Królewskiej Orkiestry Symfonicznej przy Pałacu w Wilanowie, podczas którego można było usłyszeć znane pieśni w wykonaniu solistów teatrów operowych. Była to wspaniała uczta dla ducha. Aby zaspokoić potrzeby ciała, przygotowano wytworny bankiet, podczas którego licznie przybyli goście mieli wreszcie okazję spotkać się, powspominać, podzielić się doświadczeniami.

Z okazji pięknego jubileuszu redakcja czasopisma *Zabezpieczenia* składa prezesowi stowarzyszenia POLALARM Bogdanowi Tatarowskiemu i wszystkim nagrodzonym najserdeczniejsze gratulacje i wyrazy uznania za dotychczasowe osiągnięcia, a także życzy dalszych sukcesów przyczyniających się do rozwoju całej naszej branży. Przy okazji redakcja pragnie podziękować za przyznaną red. naczelnej Teresie Karczmarzyk Nagrodę Specjalną – Dyplom Uznania i Medal XXX-Lecia Rozwoju Technicznej Ochrony Osób i Mienia w Polsce za aktywny udział w propagowaniu wiedzy o zabezpieczeniach osób i mienia dla rozwoju technicznej ochrony osób i mienia w Polsce.

Opracowanie: Redakcja

Fotoreportaż na stronie: www.zabezpieczenia.com.pl

Szeroki asortyment kamer Sony

Linia produktowa kamer **Sony** z przetwornikiem **Exmor,** o rozdzielczości od 1,3 Mpix do 3 Mpix, została uzupełniona o miniaturowe modele, plasujące się w bardzo atrakcyjnym przedziale cenowym. Przykładem mogą być wandaloodporne kamery kopułkowe SNC-RH210T, generujące obraz o maksymalnej rozdzielczości 2048×1536 pikseli.

Kamery z tej serii są wyposażone w stałoogniskowe obiektywy szerokokątne i dysponują opcją *solid PTZ*, czyli możliwością cyfrowego powiększenia dowolnego fragmentu obrazu. Jest to szczególnie przydatne w systemach ochrony obiektów handlowych. Warto zaznaczyć, że opcja *solid PTZ* jest dostępna nawet w przypadku przeglądania nagrań archiwalnych, a wynikowa rozdzielczość nigdy nie spada poniżej poziomu 4CIF.

Kamery z tej serii są dostępne w wykonaniach standardowych i wandaloodpornych oraz w kilku wersjach kolorystycznych.

Bezpośr. inf. Altram

Coraz większa popularność przetwornika Sony Exmor

Strzałem w dziesiątkę w 2010 roku okazał się **nowy przetwornik CMOS Exmor firmy Sony**. Jego doskonałe parametry, w tym duża dynamika i niski poziom szumów, sprawiły, że znajduje coraz więcej zastosowań.

Wykorzystywany jest nie tylko w licznej grupie produktów z rynku profesjonalnych kamer telewizyjnych, konsumenckich kamer HD i aparatów fotograficznych z serii „α", lecz także w dwudziestu sześciu modelach kamer sieciowych **Sony Ipela**, o rozdzielczościach od 1,3 Mpix do 3 Mpix.

Przewaga przetwornika Sony Exmor nad starszymi rozwiązaniami jest tak duża, że różnicę w jakości obrazu widać gołym okiem. Czynnikiem wyróżniającym jest wysoka dynamika kamery zbudowanej w oparciu o ten typ przetwornika, dochodząca do 125 dB.

W praktyce przejawia się to zdolnością kamery do czytelnego odwzorowania scen odznaczających się bardzo nierównomiernym oświetleniem. Przykładowo, z taką sytuacją mamy do czynienia podczas nocnej obserwacji terenów miejskich, gdzie jednocześnie występują silne odblaski od latarni ulicznych i świateł samochodowych oraz głębokie cienie. Dzięki temu przetwornikowi uzyskujemy czytelny obraz we wszystkich tych obszarach.

Bezpośr. inf. Altram

Nowe rozwiązanie w dziedzinie kamer IP PTZ

W odpowiedzi na zapotrzebowanie firma **Altram** wprowadza na rynek **zintegrowaną kamerę IP** o rozdzielczości 3 Mpix z możliwością pracy w standardzie Full HD (1080p), z obiektywem zmiennoogniskowym o krotności ×22, dysponującą funkcją autofocus, mechanicznie odsuwanym filtrem IR oraz opcją stabilizacji obrazu. Kamera jest przeznaczona do pracy w sieciowych systemach ochrony imprez masowych i monitoringu przestrzeni publicznych.

Wykorzystana w tej konstrukcji głowica uchylno-obrotowa pozwala na nieograniczony obrót wokół osi pionowej oraz możliwość pochylania kamery pod kątem +/– 90 stopni. Rozwiązuje to problem obserwacji obiektów znajdujących się poniżej lub powyżej miejsca instalacji kamery, występujący w klasycznych kamerach szybkoobrotowych.

Bezpośr. inf. Altram

SONY
make.believe

Sony Poland poszukuje pracownika na stanowisko:

Kierownik ds. Kluczowych Klientów w Kanale Kamer Dozorowych

Channel Account Manager Video Security PSE

Sony Poland sp. z o.o.
ul. Ogrodowa 58 . 00-876 Warszawa
www.sony.com

Zadania:

- Rozwój kanału sprzedaży kamer dozorowych oraz rozwiązań związanych z zabezpieczeniami na lokalnym rynku.
- Planowanie strategii sprzedaży.
- Realizacja planów sprzedaży zdefiniowanych dla rynku i dla poszczególnych klientów.
- Budowanie silnych i trwałych relacji we wszystkich kanałach sprzedaży i z klientami.

Wymagane umiejętności:

- Doświadczenie w zakresie sprzedaży kamer dozorowych oraz rozwiązań związanych z zabezpieczeniami.
- Umiejętność w zakresie planowania, prowadzenia negocjacji z partnerami handlowymi oraz realizacji zdefiniowanych celów sprzedażowych.
- Efektywna współpraca z zespołem technicznym i działem marketingu w celu realizacji sprzedaży.
- Wysoki poziom efektywności osobistej i motywacji do pracy.
- Duża proaktywność w proponowaniu rozwiązań mających na celu usprawnienie współpracy z klientami i zwiększenie wielkości sprzedaży.
- Nastawienie na samodzielne rozwiązywanie problemów.
- Bardzo dobra znajomość języka angielskiego.
- Bardzo dobre zdolności komunikacyjne.

Osoby zainteresowane prosimy o przesłanie życiorysu wraz z listem motywacyjnym na adres e-mail:

SonyPoland.Rekrutacja@eu.sony.com

Prosimy o dopisanie w liście motywacyjnym następującej klauzuli:

Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych w mojej ofercie pracy dla potrzeb niezbędnych do realizacji procesu rekrutacji, zgodnie z ustawą z dn. 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. Ust. nr 133 poz. 883.

Brak powyższej klauzuli uniemożliwi nam rozpatrzenie Państwa oferty.

Odpowiemy tylko na wybrane oferty.

www.sony.com

Rynek nie znosi pustki

Andrzej Walczyk

Chcąc sensownie odnieść się do tematu zawartego w tytule artykułu należy zacząć od zacytowania odpowiednich aktów prawnych. Paragrafy Dziennika Ustaw nigdy nie stanowiły pasjonującej lektury, dlatego ograniczymy się jedynie do kilku z nich. Ogłoszona w Dzienniku Ustaw Nr 62 z dnia 21 kwietnia 2009 r. Ustawa 504 z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych głosi:

„Art. 77. Dotychczasowe przepisy wykonawcze wydane na podstawie ustawy, o której mowa w art. 79, zachowują moc do czasu wydania przepisów wykonawczych na podstawie niniejszej ustawy, nie dłużej jednak niż przez 6 miesięcy od dnia jej wejścia w życie.

Art. 79. Traci moc ustawa z dnia 22 sierpnia 1997 r. o bezpieczeństwie imprez masowych (Dz.U. z 2005 r. Nr 108, poz. 909 oraz z 2007 r. Nr 99, poz. 663 i 665).

Art. 80. Ustawa wchodzi w życie z dniem 1 sierpnia 2009 r., z tym że art. 13 ust. 1 – w zakresie dotyczącym meczów piłki nożnej organizowanych poza ramami ligi zawodowej – wchodzi w życie z dniem 1 sierpnia 2010 r."

Wraz z ustawą z 1997 roku tracą moc związane z nią przepisy wykonawcze, o czym można przekonać się, studiując jedną z wielu propozycji (prawdopodobnie najnowszą) nowego rozporządzenia, datowaną 11 sierpnia 2010 r. Znajduje się w niej takie stwierdzenie: „Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 28 października 2004 r. w sprawie sposobu utrwalania przebiegu imprez masowych oraz minimalnych wymagań technicznych dla urządzeń rejestrujących obraz i dźwięk (Dz.U. Nr 243, poz. 2438), które utraciło moc z dniem 1 lutego 2010 r. na podstawie art. 77 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz.U. Nr 2, poz. 504).".

Można analizować te wszystkie paragrafy i zastanawiać się nad interpretacją poszczególnych zapisów, jednakże nie ma najmniejszej wątpliwości, że w chwili obecnej nie obowiązuje żadne rozporządzenie wykonawcze dotyczące bezpieczeństwa imprez masowych, czyli wisimy w przysłowiowej próżni.

Absurdalność sytuacji polega na tym, że wrą prace związane z budową stadionów, hal sportowych i innych obiektów, które mają być wykorzystane podczas mistrzostw Europy w czerwcu 2012 r. Część z tych obiektów została już oddana do eksploatacji. Jeżeli na terenie Polski wszelkie działania gospodarcze muszą być zgodne z obowiązującym prawem, a nie wypada w to wątpić, to w jaki sposób zatwierdzane były projekty i na podstawie jakich kryteriów odbierane były instalacje systemów monitoringu na tych stadionach?

Chcąc zapoznać się z aktualną sytuacją panującą na nowo powstających stadionach, redakcja *Zabezpieczeń* rozesłała krótką ankietę do kilkunastu wiodących klubów należących do Ekstraklasy. W ankiecie były zawarte pytania dotyczące między innymi łącznej liczby kamer pracujących w systemie oraz zgodności realizowanych inwestycji z propozycją rozporządzenia. Pomimo próśb i przypomnień do redakcji przyszły tylko dwie odpowiedzi, w których zawarte były praktycznie same pozytywy. Wyczuwało się, że te kluby nie mają nic do ukrycia, a nawet chcą się pochwalić poprawnością przyjętego rozwiązania i sprawnością posiadanego systemu. Jeden z ankietowanych szczerze wyjawił, że zdaje sobie sprawę, iż jego system może wykazywać pewne mankamenty, jednak oświadczył, że jest gotów ponieść koszty modernizacji, jeśli jej potrzeba będzie wynikać z uprawomocnionego rozporządzenia. Obaj korespondenci nie negowali potrzeby ustalenia jasnych i jednakowych dla wszystkich kryteriów. Czyżby pozostałe kluby nie chciały się wykazać czymś podobnym?

Redakcja *Zabezpieczeń* podjęła także inną próbę uzyskania informacji. Wysłała swojego przedstawiciela na konferencję prasową z udziałem ministra Adama Rapackiego oraz jego doradców, poświęconą funkcjonowaniu ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, zorganizowaną na terenie nowo oddanego stadionu Legii w Warszawie. Można było spodziewać się, że przy tej okazji poruszone zostaną poważne kwestie techniczne i proceduralne, tymczasem większość dziennikarzy była zainteresowana problemem sprzedaży piwa podczas trwania meczów piłkarskich i ten temat zajął niemal cały czas przeznaczony na dyskusję.

Na koniec, gdy delegatowi *Zabezpieczeń* udało się wreszcie dojść do głosu, padło pytanie: jakie kryteria należy stosować podczas projektowania i odbioru systemów monitorowania stadionów i kiedy ukaże się stosowne rozporządzenie? Minister Rapacki wyjaśnił, że propozycje rozporządzenia są od dawna znane inwestorom i na tej podstawie prowadzone są prace, zaś właściwe rozporządzenie ma się ukazać dosłownie na dniach. W odpowiedzi na kolejne pytanie – dlaczego w takim razie do eksploatacji oddawane są obiekty, które nie spełniają wymagań wynikających z propozycji rozporządzenia? – minister Rapacki wyraził duże zdziwienie i ograniczył się do stwierdzenia, że jest to szeroki temat, tymczasem czas, jaki przeznaczył na odpowiedzi, właśnie minął i konferencja prasowa zostaje zamknięta.

Konferencja prasowa potwierdziła widoczny brak jednoznacznych uwarunkowań prawnych, dotyczących minimalnych wymagań sprzętowych i organizacyjnych, związanych z projektowaniem i instalacją systemów monitoringu na stadionach. Rynek nie znosi pustki i w tej sytuacji wszystkie podmioty biorące udział w realizacji takich przedsięwzięć reagują tak, jak im jest najwygodniej. Można zaobserwować **dwa konkurujące ze sobą sposoby działania**.

Pierwszy z nich polega na śledzeniu kolejnych wersji propozycji rozporządzenia, czyli dokumentu, który dopiero w przyszłości ma nabrać mocy prawnej, oraz na dostosowaniu projektów instalacji do jego wymogów. Osoby i firmy postępujące w ten sposób liczą na to, że rozporządzenie ujrzy kiedyś światło dzienne i zacznie obowiązywać – nawet jeśli jego ostateczna treść będzie nieznacznie różnić się od treści propozycji, to ewentualne modyfikacje i poprawki w systemach monitoringu będą nieznaczne.

Przykładem takiego sposobu działania jest realizacja systemu monitorowania stadionu Cracovii w Krakowie. Projekt tego systemu został oparty na jednej z propozycji rozporządzenia, a instalacja ściśle trzymała się projektu. Liczba kamer została dobrana na podstawie wyliczeń zasięgów w poszczególnych kategoriach funkcjonalnych, zgodnie z treścią propozycji rozporządzenia. Przepływności sieci, pojemności dysków pamięciowych i inne właściwości systemu zostały dobrane z uwzględnieniem liczby obrazów generowanych przez poszczególne kamery w ciągu każdej sekundy. Projektanci zadali sobie nawet trud przygotowania procedur częściowego wyłączania systemu na czas, w którym stadion nie jest wykorzystywany, co umożliwia ograniczenie kosztów eksploatacji i ochronę obiektu w przerwach między imprezami.

Drugi sposób radzenia sobie z brakiem uregulowań prawnych to całkowite ignorowanie jakichkolwiek rozporządzeń, zarówno starych, już nie obowiązujących, jak i nowych, jeszcze nie istniejących. W gwarze młodzieżowej takie działanie nazywałoby się *free style*. W tym przypadku projekt instalacji jest uzgodniony lokalnie z władzami klubu, ewentualnie, chociaż nie zawsze, skonsultowany z policją, czyli realizowane jest przysłowiowe widzi mi się. Dostawcy sprzętu oferują po prostu to, czym dysponują, nie zważając na jakiekolwiek aspekty użytkowe. Na dodatek mamią niczego nie świadomych inwestorów rozwiązaniami jak z powieści SF, na przykład użyciem kamer o ekstremalnie dużej rozdzielczości.

Zgodnie z tą koncepcją, mocno lansowaną przez jedną z firm, która monitoringiem wizyjnym zajmuje się dopiero od kilkunastu miesięcy i w związku z tym nie ma w tej dziedzinie ani wystarczającej wiedzy, ani doświadczenia (nie mówiąc już o referencjach), całe sektory trybun miałyby być obserwowane za pośrednictwem jednej kamery o ekstremalnie dużej rozdzielczości. Proponowana kamera wytwarza tylko trzy obrazy na sekundę, czyli jest raczej aparatem fotograficznym robiącym serię zdjęć, a nie kamerą telewizyjną. Pasmo sieciowe wymagane do obsłużenia jednej takiej kamery jest szersze niż 80 megabitów na sekundę. Mało wydajna kompresja JPEG2000 zupełnie nie nadaje się do takich celów. W karcie katalogowej nie są podane żadne istotne dane techniczne kamery. Na koniec – kamera nie ma jednoznacznie określonego typu, czyli podczas realizacji inwestycji pod tą samą nazwą mogą występować urządzenia zupełnie różne od pierwotnie proponowanych.

Nikogo nie obchodzi, że tak zbudowany system będzie bezużyteczny w sytuacji, gdy nad stadionem pojawi się nawet najdelikatniejsza mgiełka lub gdy kibice odpalą świecę dymną i sektor trybun stanie się niewidoczny. Powstały w takich warunkach materiał nagraniowy nie ma wartości dowodowej i zostanie odrzucony przez każdy sąd. Można namówić władze klubu na realizację szalonej koncepcji. Sztuka perswazji słownej i pozawerbalnej jest w stanie przekonać je do wydania dużych sum pieniędzy na ten, a nie inny sprzęt.

Kolejnym elementem, jaki podlega manipulacji, jest łączna liczba kamer w systemie. Propozycja rozporządzenia w jednoznaczny sposób określa, które obszary obiektu powinny być obserwowane, a także precyzuje warunki jakościowe takiej obserwacji. Chcąc sprostać wymaganiom wynikającym z propozycji rozporządzenia, należy odpowiednio rozmieścić kamery w obiekcie. Z tego rozmieszczenia wynika łączna ich liczba, która może nieznacznie się wahać w zależności od przyjętej koncepcji projektowej, jednak żadne rozwiązania techniczne nie są w stanie zmniejszyć jej do połowy czy jednej czwartej.

Na stadionie Cracovii, który spełnia wymagania wynikające z propozycji rozporządzenia, zainstalowano około 250 kamer, gdy tymczasem na stadionie Legii jest ich tylko 170, a na stadionie Lecha – zaledwie 60. Co prawda nie są to identyczne stadiony. Stadion Cracovii mieści 15 tys., Legii – 33 tys., a Lecha – 46 tys. widzów, tyle że to jeszcze bardziej pogłębia dysproporcję. Wnioski co do zgodności (lub braku zgodności) tych instalacji z jakimikolwiek przyszłymi regulacjami prawnymi narzucają się same.

Przejdźmy do innego zagadnienia. W propozycji rozporządzenia jednoznacznie określone są kategorie kamer. Kamery należące do kategorii pierwszej mają umożliwiać rozpoznawanie poszczególnych osób w tłumie kibiców, co stawia przed sprzętem najwyższe wymagania, jest trudne do osiągnięcia i kosztowne. Co ambitniejsze firmy, które próbują dostosować swoje projekty do propozycji rozporządzenia, instalują w każdym z obiektów co najmniej cztery kamery spełniające wymagania typowe dla tej kategorii, gdy tymczasem projekty innych firm tego nie przewidują, tak jakby kategoria pierwsza w ogóle nie istniała. Zgodność z jakimikolwiek propozycjami rozporządzenia nie jest brana pod uwagę.

Kolejnym zagadnieniem jest wymaganie rejestracji dźwięku podczas trwania imprez masowych. Propozycja rozporządzenia podaje konkretne parametry torów fonicznych oraz określa zakres i cel prowadzenia rejestracji dźwięku. Znajdujące się w większości współczesnych kamer sieciowych wejścia mikrofonowe nie spełniają wymagań propozycji rozporządzenia. Firmy, które nie ignorują tych wymagań, oferują specjalne, nierzadko kosztowne rozwiązania, które nie tylko umożliwiają spełnienie wymogów formalnych, ale także poprawiają zrozumiałość mowy ludzkiej w warunkach hałasu panującego na stadionach podczas trwania imprez masowych. Tymczasem ich konkurenci działający na zasadach *free style* nie oferują nic. Niektórzy uważają, że rejestracja fonii jest mało istotna i w praktyce nikt jej nie wykorzystuje. Takie podejście umożliwia znaczne obniżenie kosztów instalacji, oczywiście nie spełniającej wymogów propozycji rozporządzenia, a to z kolei pozwala wygrywać przetargi, w których, jak wiadomo, decyduje wyłącznie cena.

W zasadzie nikogo nie można pociągnąć do odpowiedzialności, bo wobec braku obowiązującego prawa regułą jest brak reguł i żadne, nawet szalone działanie nie może być naganne. Odwlekanie w nieskończoność momentu ogłoszenia ostatecznej, obowiązującej wersji rozporządzenia[1] wykonawczego bulwersuje poważnych i rzetelnych oferentów, a cieszy wszelkiej maści kombinatorów, gdyż stanowi rodzaj milczącej aprobaty działania na własną rękę. Nic tak nie sprzyja kumoterstwu i korupcji, jak brak jasnych kryteriów prawnych. Nawet w obliczu rażących uchybień projektowych nie można rozsądnie reagować, gdyż nie ma wzorca, punktu odniesienia. Brakuje wyraźnych granic postępowania rozsądnego. Wszystko tonie w oparach absurdu.

Andrzej Walczyk

1) Informujemy, że już po przygotowaniu tego numeru Zabezpieczeń do druku, w Dz.U. 2011 nr 16 poz. 73 opublikowane zostało Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 stycznia 2011 r. w sprawie sposobu utrwalania przebiegu imprezy masowej.

Cały świat

w zasięgu wzroku

Zakupy premiowane
Telewizorami
Samsung LCD

kamery Samsung IP

SNB-2000 SNB-3000 SNB-5000 SND-3080 SND-5080

C&C Partners Telecom Sp. z o.o., ul. 17 Stycznia 119, 121, 64-100 Leszno, tel. 65 525 55 55, fax 65 525 56 66
Biura Handlowe: Leszno, e-mail: leszno@ccpartners.pl; tel. 65 525 55 01 / **Gdańsk**, e-mail: gdansk@ccpartners.pl; tel. 58 739 67 80
Katowice, e-mail: katowice@ccpartners.pl; tel. 32 201 78 91 / **Warszawa**, e-mail: warszawa@ccpartners.pl; tel. 22 549 70 00

Systemy zabezpieczeń
obiektów infrastruktury krytycznej

Paweł Kamiński

wprowadzenie

Sir Basil Henry Liddell Hart[1] twierdził, że nie wystarczy strategia militarna, która jest powiązana z planami bitew i działaniami sił zbrojnych. Wielka strategia, w odróżnieniu od węższej – militarnej, koncentruje się na zdolności państwa do koordynowania i kierowania narodowymi zasobami

1) Sir Basil Henry Liddell Hart (1895–1970) – wybitny historyk wojskowości, jeden z najwybitniejszych brytyjskich teoretyków sztuki wojennej.

Potrzeba ochrony obiektów szczególnie ważnych ze względu na bezpieczeństwo państwa została uwzględniona w polskim prawie, w ustawie z 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej[2] oraz w rozporządzeniu z 24 czerwca 2003 roku w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony[3]. Wspomniane rozporządzenie wskazuje na dwie kategorie obiektów. Do kategorii pierwszej, związanej z potencjałem obronnym państwa, należą:

- zakłady produkujące, remontujące, magazynujące uzbrojenie, sprzęt wojskowy i środki bojowe,
- zakłady prowadzące prace badawczo-rozwojowe oraz konstruktorskie w dziedzinie bezpieczeństwa i obronności państwa,
- magazyny rezerw państwowych (np. bazy, składy paliw płynnych, żywności, leków, materiałów sanitarnych),
- obiekty podległe ministrowi obrony narodowej lub przez niego nadzorowane,
- obiekty infrastruktur transportu samochodowego, kolejowego, lotniczego, morskiego, wodnego śródlądowego, drogownictwa, kolejnictwa i łączności,
- ośrodki dokumentacji geodezyjnej i kartograficznej,
- zapory wodne,
- urządzenia hydrotechniczne,
- obiekty należące do jednostek organizacyjnych Agencji Wywiadu,
- obiekty Narodowego Banku Polskiego,
- obiekty Banku Gospodarstwa Krajowego,
- obiekty Polskiej Wytwórni Papierów Wartościowych oraz Mennicy Państwowej,
- obiekty telekomunikacyjne służące nadawaniu programów radiowych i telewizji publicznej,
- obiekty i miejsca, w których produkowane, stosowane lub magazynowane są materiały jądrowe czy też źródła i odpady promieniotwórcze[4].

Do drugiej kategorii zaliczono obiekty związane z właściwym funkcjonowaniem administracji publicznej oraz zapewnieniem odpowiedniego poziomu bezpieczeństwa i porządku publicznego:

- obiekty organów i jednostek organizacyjnych podległe ministrowi spraw wewnętrznych i administracji lub przez niego nadzorowane,
- obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego,
- obiekty policji, Straży Granicznej, Państwowej Straży Pożarnej,
- obiekty będące we właściwości ministra sprawiedliwości, Służby Więziennej oraz jednostek organizacyjnych, które podlegają ministrowi sprawiedliwości bądź są przez niego nadzorowane,
- zakłady, których działalność ma związek z wydobywaniem kopalin podstawowych,
- obiekty (miejsca), w których produkowane, stosowane lub magazynowane są materiały stwarzające zagrożenie pożarem lub wybuchem,
- obiekty, w których prowadzona jest działalność oparta na wykorzystywaniu toksycznych związków chemicznych i ich prekursorów, środków biologicznych i mikrobiologicznych, mikroorganizmów, toksyn i innych substancji powodujących zachorowania u ludzi i (lub) zwierząt,
- elektrownie oraz inne obiekty elektroenergetyczne,
- inne obiekty znajdujące się we właściwości organów administracji rządowej lub też organów jednostek samorządu terytorialnego, formacji, instytucji państwowych, a także prywatnych przedsiębiorców[5].

Także ustawa o ochronie osób i mienia z 22 sierpnia 1997 roku wymienia wiele obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. Zapisy w ustawie precyzują kryteria podziału wspomnianej infrastruktury i dzielą je na związane z obronnością państwa, ochroną interesu gospodarczego państwa, bezpieczeństwem publicznym oraz innymi ważnymi interesami państwa[6].

26 kwietnia 2007 roku weszła w życie ustawa o zarządzaniu kryzysowym[7], która określa infrastrukturę krytyczną jako „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców".

Zdefiniowana została również ochrona obiektów infrastruktury krytycznej. Są to „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie"[8].

Ochrona infrastruktury krytycznej ma dotyczyć obiektów mających związek z systemami:

- zaopatrzenia w energię i paliwa,
- łączności i sieci teleinformatycznych,
- finansowymi,
- zaopatrzenia w żywność i wodę,
- ochrony zdrowia,
- transportowymi i komunikacyjnymi,

2) Dz.U. z 2002 r. Nr 21, poz. 205 z późn. zm.

3) Dz.U. Nr 116, poz. 1090.

4) Rozporządzenia Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, Dz.U. Nr 116, poz. 1090, § 2 pkt 1– 9.

5) Tamże, § 2 pkt 10–19.

6) A. Tyburska, Współpraca policji z innymi podmiotami w zakresie ochrony obiektów ważnych dla bezpieczeństwa państwa, Wydawnictwo Wyższej Szkoły Policji w Szczytnie, Szczytno 2009.

7) Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadkach wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej.

8) Dz.U. z 2007 r. Nr 89, poz. 590.

– ratowniczymi,
– zapewniającymi ciągłość działania administracji publicznej,
– produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (w tym rurociągami doprowadzającymi substancje niebezpieczne).

Organizacja i wykonanie zadań z zakresu ochrony infrastruktury krytycznej należy do wojewódzkich, powiatowych i gminnych organów zajmujących się zarządzaniem kryzysowym[9], które mają obowiązek tworzenia krajowych, wojewódzkich, powiatowych i gminnych planów zarządzania kryzysowego. Mają one zawierać między innymi charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia w infrastrukturze krytycznej. Załączniki funkcjonalne planów mają natomiast określać procedury związane z ochroną infrastruktury krytycznej, zawierać wykaz infrastruktury krytycznej objętej planem oraz podawać zakres ochrony oraz odtwarzania infrastruktury krytycznej.

Zadania z zakresu planowania cywilnego obejmują przygotowanie odpowiednich rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej i powinny uwzględniać zapewnienie funkcjonowania i możliwości odtworzenia infrastruktury krytycznej.

9) Organem właściwym w sprawach zarządzania kryzysowego na obszarze województwa jest wojewoda, na terenie powiatu – starosta, jako przewodniczący zarządu powiatu, a na terenie gminy – wójt, burmistrz lub prezydent miasta.

Ochrona obiektów infrastruktury krytycznej obejmuje swoim zakresem między innymi przygotowanie planów ochrony, ich aktualizacje, stosowanie opracowanych algorytmów postępowania na wypadek wystąpienia zagrożenia obiektów, a także utrzymywanie własnych systemów rezerwowych, podtrzymujących działanie tej infrastruktury do czasu jej całkowitego odbudowania. Zgodnie z zapisami ustawy plany ochrony infrastruktury krytycznej tworzone są na poziomie państwa i województwa[10] i zawierają:

– wykaz obiektów i systemów infrastruktury krytycznej,
– charakterystykę zagrożeń dla infrastruktury krytycznej oraz ocenę ryzyka ich wystąpienia,
– charakterystykę zasobów możliwych do wykorzystania w celu ochrony infrastruktury krytycznej,
– warianty działania w przypadkach zagrożeń lub zakłócenia funkcjonowania infrastruktury krytycznej,
– warianty odtwarzania infrastruktury krytycznej,
– zasady współpracy administracji publicznej z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony, w tym zasady przekazywania informacji,
– wskazanie terminów i trybu aktualizacji planu[11].

Organy administracji publicznej realizują zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym[12]. Współpracują w tym zakresie z organami administracji rządowej właściwymi w tych sprawach, w szczególności z szefem Agencji Bezpieczeństwa Wewnętrznego. Dotyczy to także posiadaczy obiektów, instalacji i urządzeń infrastruktury krytycznej. Są oni zobowiązani do niezwłocznego przekazywania szefowi Agencji Bezpieczeństwa Wewnętrznego będących w ich posiadaniu informacji dotyczących zagrożeń o charakterze terrorystycznym dla tej infrastruktury krytycznej, w tym istotnych z punktu widzenia bezpieczeństwa państwa zagrożeń dotyczących funkcjonowania systemów i sieci energetycznych, wodnokanalizacyjnych, ciepłowniczych i teleinformatycznych.

W 2008 roku utworzono Rządowe Centrum Bezpieczeństwa. Jedną z podstawowych funkcji Centrum, związanych z ochroną infrastruktury krytycznej, jest realizacja zadań planistycznych i programowych z zakresu zarządzania kryzysowego i ochrony infrastruktury krytycznej. Jednocześnie Centrum współdziała z instytucjami i jednostkami organizacyjnymi NATO i Unii Europejskiej oraz innymi międzynarodowymi organizacjami odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej[13].

W 2010 r. Rada Ministrów uchwaliła Narodowy Program Ochrony Infrastruktury Krytycznej, którego celem jest stworzenie warunków umożliwiających poprawę bezpieczeństwa infrastruktury krytycznej. Za najważniejsze uznano zapobieganie zakłóceniom funkcjonowania infrastruktury krytycznej, przygotowanie jej na sytuacje kryzysowe mogące na nią wpłynąć, reagowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz odtwarzanie infrastruktury krytycznej. Ponadto program wyznacza narodowe priorytety, cele, wymagania oraz standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej, a także szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej z uwzględnieniem ich znaczenia dla funkcjonowania państwa i zaspokojenia potrzeb obywateli. Jednocześnie wskazane są instytucje i osoby odpowiedzialne za wspomniane działania[14].

Podsumowując przedstawione informacje o ochronie infrastruktury krytycznej, należy wspomnieć o pojawieniu się nowego rodzaju infrastruktury krytycznej, a mianowicie krytycznej infrastruktury teleinformatycznej państwa. Są to „systemy i sieci teleinformatyczne eksploatowane przez administrację rządową, organy władzy ustawodawczej, władzy sądowniczej, samorządu terytorialnego, a także strategiczne z punktu widzenia bezpieczeństwa państwa podmioty gospodarcze (np. podmioty działające w obszarze telekomunikacji, energii, gazu, bankowości, a także podmioty o szczególnym znaczeniu dla obronności i bezpieczeństwa państwa oraz podmioty działające w obszarze ochrony zdrowia) […]”[15]. Obecnie ustawa o zarządzaniu kryzysowym nie wymienia krytycznej infrastruktury teleinformatycznej oraz roli poszczególnych podmiotów mających udział w systemie ochrony tej infrastruktury, a także nie wyszczególnia ich zadań. W najbliższej przyszłości należy wprowadzić zmiany w polskim prawie, które pozwolą na określenie zasad i form funkcjonowania ochrony krytycznej w państwie. Musi to dotyczyć nie tylko organów administracji publicznej, ale również realizujących zadania publiczne organizacji społecznych, przedsiębiorców i jednostek nieposiadających osobowości prawnej, jeżeli wykorzystują system, obiekt lub instalację wchodzącą w skład infrastruktury krytycznej. Zwiększy to poziom bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa oraz odporność państwa na ataki cyberterrorystyczne.

mgr Paweł Kamiński
Państwowa Wyższa Szkoła Zawodowa
im. Prezydenta Stanisława Wojciechowskiego w Kaliszu

10) W. Lidwa, W. Krzeszowski, W. Więcek, Zarządzanie w sytuacjach kryzysowych, wyd. AON, Warszawa 2010, s. 60–62.

11) Rozporządzenie z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej, Dz.U. Nr 83.7252. 542.

12) Zdarzenie o charakterze terrorystycznym to sytuacja powstała na skutek czynu określonego w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. (Dz.U. Nr 88, poz. 553 z późn. zm.) lub groźba zaistnienia takiego czynu, mogącego doprowadzić do sytuacji kryzysowej.

13) Rozporządzenie z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa, Dz.U. 08.128.821 z dnia 18 lipca 2008 r.

14) Rozporządzenie z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. z 17 maja 2010 r. Nr 83, poz. 541.

15) Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011, MSWiA, Warszawa 2009.

Bezpieczeństwo a normalizacja

E-społeczeństwo i warunki normalizacji (część 1)

Proponujemy Państwu pierwszy artykuł z cyklu „Bezpieczeństwo a normalizacja", dotyczący roli dobrowolnie przyjętych norm w e-społeczności XXI wieku. Na tle zachodzących zmian informacyjnych pragniemy przedstawić użyteczność norm przyjętych w biznesie, skuteczność ich stosowania w sytuacjach kryzysowych oraz innowacyjne działania wynikające z normatywnego podejścia do różnych zdarzeń biznesowych – tych pożądanych oraz niepożądanych i nieoczekiwanych

Marek Blim

Obowiązujące dawniej kanony i reguły kodeksów honorowych zostały we współczesnym świecie zastąpione przez normy. Spowodowało to, że wymogi technologiczne stały się obiektywne, powszechnie znane i zrozumiałe – objęte standaryzacją i certyfikacją

1. Tytułem wstępu

„Oni nie umieli się technicznie dogadać i zrozumieć" – tak mówi się o przyczynach jednego z krytycznych zdarzeń zaistniałych na brytyjskich platformach wiertniczych Morza Północnego, sytuacji o poważnych skutkach gospodarczych. Rzecz dotyczy awarii systemu wydobywczego na jednej z platform BP (w 1997 roku), kiedy to natychmiastowe dostarczenie śmigłowcem części do systemu wiertniczego (jeśliby znajdowały się w magazynie) mogło ograniczyć straty i szkody poniesione w wyniku zaistniałej awarii do kilku tysięcy funtów. Stało się jednak inaczej: urzędnik w centrali BP, od którego zależała decyzja o zakupie nowej części i locie śmigłowca na platformę (koszt rzędu 13 tysięcy funtów), nie zrozumiał powagi sytuacji, o której informował inżynier platformy. „Zaowocowało" to przepychankami formalnymi zakończonymi pożarem na platformie, który spowodował ogromne straty. W wyniku eksplozji zginęło dwóch pracowników, 14 innych zostało poparzonych lub rannych, a platforma uległa zniszczeniu. Straty materialne przekroczyły kwotę dwóch milionów funtów.

Od tamtego czasu znormalizowano komunikację w obszarze BP w relacjach *personel wykonawczy – personel kierowniczy*. Nie ustrzegło to jednak koncernu przed zdarzeniami zaistniałymi ostatnio w Zatoce Meksykańskiej. Wyciek, spowodowany wybuchem na zarządzanej przez BP platformie wiertniczej Deepwater Horizon w kwietniu 2010 roku, wywołał katastrofalne skutki dla środowiska naturalnego. Wypłynęło w sumie 4,9 mln baryłek ropy, zanim – w lipcu – udało się tymczasowo zatamować jej wypływanie. Przyczyną największej w historii USA katastrofy ekologicznej były głównie zaniedbania BP – firmy, która dzierżawiła platformę i prowadziła na niej prace wiertnicze. Zawiodła głowica przeciwerupcyjna i jej obudowa. Winni się też rząd USA, który nie dopilnował, by koncern wprowadził odpowiednie, wymagane normami zabezpieczenia na urządzeniach.

Pojawiające się wątpliwości mają charakter uniwersalny: czy i w jaki sposób można było temu wszystkiemu zapobiec? Na ile można i trzeba uporządkować oraz znormalizować wzajemną komunikację w sytuacjach zagrożeń (zwłaszcza między nacjami różnymi kulturowo i językowo – np. brytyjski personel inżynierski i meksykańscy wykonawcy).

2. Komunikacja i zrozumienie w społeczeństwie „III fali" – e-społeczeństwo

Odwołując się do opisanych przez H. i A. Tofflerów[1] zjawisk rozwoju społecznego (rolnictwo – industrializacja – informatyzacja), pośrednio odnosimy się do materialnych podstaw tego rozwoju. Przyjmujemy za naturalne towarzyszące mu zmiany w systemach komunikacji między ludźmi.

Truizmem wydaje się przypominanie, że bez wspólnego, zrozumiałego wzajemnie systemu sygnałów (prajęzyka) nie byłoby możliwe wspólne polowanie naszych prapraprzodków, a bez uporządkowania zapisów technicznych (normy rysunkowe, normowanie wielkości jednostek miar i wag) ciągle jeszcze mielibyśmy przed sobą perspektywy rozwojowe wieku „węgla i pary" (o rozpowszechnianiu wielu osiągnięć z zakresu techniki użytkowej nie wspomnę).

Zestawienie „kamieni milowych" rozwoju środków komunikacji w życiu społeczności ludzkiej może mieć postać jak w tab. 1.

1) Toffler A., „Trzecia fala", wyd.3, PIW, Warszawa 2001

Kiedy mówimy o rozwoju społeczeństwa XXI wieku, milcząco zakładamy, że większość populacji ludzkiej znajduje się pod względem zrozumienia i stosowania dostępnych rozwiązań ICT[2] w czołowej części fali rozwoju cywilizacyjnego – co wszakże nie jest prawdą. Zróżnicowanie ma postać piramidy wykształcenia – z „jajogłowymi" u szczytu i analfabetami u podstaw.

Analfabetyzm w Polsce (brak umiejętności czytania i pisania w obowiązującym języku państwowym), istniejący w okresie II Rzeczypospolitej oraz w okresie powojennym, był zwalczany wysiłkiem rządowym i społecznym jako czynnik degradujący i uniemożliwiający prawidłowy rozwój państwa, a także jako źródło wykluczenia społecznego licznych grup ludności (napływowej, mniejszości narodowych, ubogich „nizin społecznych") i hamulec rozwojowy.

Obecnie – na początku XXI wieku, będącego zwiastunem epoki e-społeczeństwa wyposażonego w środki nowoczesnego szybkiego komunikowania się, pracy „na odległość", kształcenia i doskonalenia zawodowego bez konieczności fizycznego przemieszczania się – pojawił się nowy rodzaj analfabetyzmu: brak wśród licznej grupy osób umiejętności korzystania ze współczesnych źródeł informacji oraz znajomości zasad posługiwania się dostępnymi systemami informacyjnymi i informatycznymi. Przyczyny rozwarstwienia społeczności informacyjnej w RP są różne, ale zasadniczo sprowadzają się do dwu czynników: zdolności do poznawania i nadążania za zmianami w dostępnych rozwiązaniach ICT[3] (kryterium stanowi tutaj głównie wiek oraz posiadane wykształcenie) oraz dostępu do rozwiniętych technologicznie urządzeń i infrastruktury informacyjnej (decyduje kryterium majątkowe oraz stadium rozwoju krajowej infrastruktury technicznej). Powstają specyficzne enklawy „analfabetyzmu informacyjnego". W praktyce oznacza on wykluczenie społeczne związane z niewydolnością materialną i środowiskową podstawowych komórek społecznych, przy jednoczesnym niedostrzeganiu tego problemu lub pomijaniu jego znaczenia przez instytucje rządowe oraz samorządowe średnich i najniższych szczebli, zajmujące się

2) I&CT – Information and Communication Technology , określenie stosowane dla opisu najnowszych dostępnych rozwiązań komunikacyjnych

3) Przykładem jest „telefon komórkowy dla seniora" będący świadomym regresem w stosunku do wszechobecnych smartfonów, i-podów itp. rozwiązań

Pismo	od 3500 r. p.n.e. (Sumerowie)
Książka	od 1250 r. p.n.e.
Poczta	od 500 r. p.n.e.
Prasa	od 200 r. p.n.e. (Chiny –„gazeta dworu Cesarza")
Druk	1049 r. – czcionki kamionkowe
	1314 r. – czcionki drewniane
	1445 r. – czcionki metalowe
Telegraf	od 1792 r. – optyczny
	od 1832 r. – elektryczny
Fotografia	od 1839 r.
Nagranie dźwięku	od 1857 r.
Telefon	od 1876 r.
Film	od 1891 r. / 1895 r.
Radio	od 1901 r.
Telewizja	od 1907 / 1925 r.
Internet	od 1990 r.

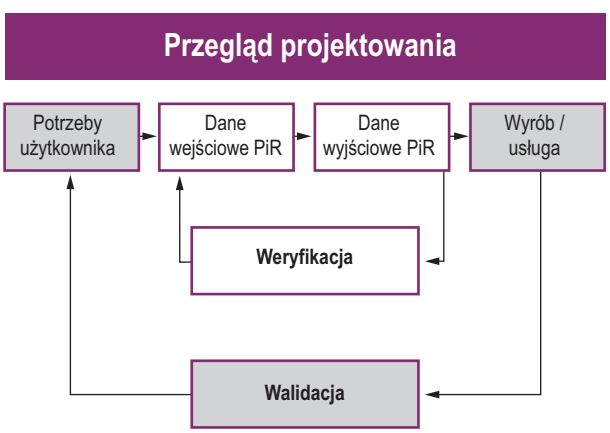
Tab. 1. Rozwój środków komunikacji społecznej

wspieraniem rozwoju społecznego. Nadzieją na zmianę obecnego stanu rzeczy jest nasze uczestnictwo w społecznych programach rozwojowych Unii Europejskiej (EFS), jej wsparcie materialne oraz wymagane formalnie „równanie do przodu" w zakresie stosowania nowoczesnych rozwiązań i technik systemowych wspierających rozwój strukturalny społeczeństwa informacyjnego nowoczesnej Europy. Wiele z tych działań nie byłoby możliwych bez jednoznacznego zrozumienia zaistniałych problemów oraz zastosowania rozwiązań opartych na „dobrych praktykach" wynikających z ujednolicenia wymagań w ramach tak samo rozumianych i dobrowolnie stosowanych wspólnych norm międzynarodowych (ISO/IEC) i regionalnych (EN) oraz krajowych (PN).

3. Czym jest normalizacja i jaką pełni rolę

Normalizacja towarzyszyła ludzkości od zarania dziejów. Pierwsze działania normalizacyjne to przypisywanie znaczenia dźwiękom, tak aby coraz większe grupy ludzi mogły posługiwać się zrozumiałą dla siebie nawzajem mową. Później odnotowane osiągnięcia to normalizacja wymiarowa w branży garncarskiej, poświadczenie miary i wagi. Pierwsze miary i wagi zostały wynalezione przez starożytnych Egipcjan i Babilończyków. Używano ich do obliczania ciężaru zboża, do wytyczania pól uprawnych oraz podczas wymiany handlowej. Miary długości bywały znacznie zróżnicowane, bo zanim doszliśmy do dzisiejszego jarda i metra, stosowano łokcie (pierwszy znany z wzorca to łokieć egipski), stopy (jako wzorcowa – królewska stopa Karola Wielkiego w IX w.), staje i wiorsty. Potrafiono jednak poprawnie przenosić obrazowane przez nie wielkości na obszarach krajów czy też kontynentów. Jednym z pierwszych zachowanych dokumentów związanych z przepisami metrologicznymi w Polsce była ustawa z 1565 roku, ale zanim doszliśmy do wielkości ujednoliconych, bywało różnie – np. ważono w pudach i cetnarach, a widomym dowodem oceny wagi listów jest polski rarytas filatelistyczny w postaci marki pocztowej: *Za łut kopiejek 8*. Mierzono, ważono i płacono od zarania naszych dziejów (stąd prenormy w wymianie pieniężnej i parytety wagowe metali szlachetnych zachowane jako odniesienia).

Opracowanie międzynarodowych wzorców: długości – metr, i wagi – kilogram, umieszczenie ich w Sevres pod Paryżem (w 1875 roku) oraz opracowanie jednolitego systemu jednostek fizycznych to dorobek uczonych europejskich XIX w.



Rys. 1. Zależności ocen współczesnego projektowania wyrobu lub usług (Źródło: A. Białas, materiały XVI Górskiej Konferencji PTI, Szczyrk 2004.)

Dzisiejsza normalizacja to nie tylko zgodność wymiarów i wielkości fizycznych. Uporządkowany świat miar i wag wzbogacił się o pojęcia z zakresu wielkości dotychczas niemierzalnych: jakość zarządzania, bezpieczeństwo środowiska itp. Standaryzacja ocen objęła normalizację, jakość i kodyfikację nie tylko wyrobów, ale także procesów ich projektowania, wytwarzania oraz realizacji licznych usług.

Inżynierowie i projektanci stosują normy na każdym etapie procesu produkcyjnego. Normy są tworzone w kontraktach, w procesach kontroli stosowanych na własne potrzeby producentów, jak również do oceny przez stronę trzecią.

Projektowanie i wykonanie wyrobu lub usługi podlegają dziś nie tylko weryfikacji – czyli sprawdzeniu potwierdzającemu poprawność wykonania i zgodność z przyjętymi normami, ale także objęte są walidacją – czyli upewnieniem się, że jest to działanie pożądane i oczekiwane przez potencjalnego klienta lub użytkownika. Wieki historii potwierdzają tylko, że normalizacja, jako czynnik stymulujący rozwój ekonomiczny, jest na świecie wysoko ceniona. Wskazuje na to również polityka prowadzona współcześnie w tym zakresie, zarówno na szczeblu międzynarodowym, jak i europejskim oraz krajowym.

Kraje, rozwijając się, poszukują dróg rozwoju zapewniających wzrost gospodarczy przy zachowaniu stabilności ekonomicznej, a podstawowy cel, do jakiego dążą, wydaje się bardzo znany. Jest to wzrost zdolności produkcyjnej dóbr i usług, które będą zarówno zaspokajać potrzeby lokalne, jak i odniosą sukces na rynkach międzynarodowych. Aby zrealizować ten cel, niezbędna jest wysoka produktywność oraz zapewnienie konkurencyjności wyrobów i usług. Innymi słowy, trzeba produkować lepiej i więcej – czyli więcej w przeliczeniu na obywatela i lepiej w odniesieniu do światowych cen i standardów jakości. Ogólnie uważa się, że aby sprostać temu zadaniu, należy działać w dwóch kierunkach:

1) W pierwszej kolejności stworzyć takie warunki ekonomiczne, w których promowane będzie inwestowanie w nowoczesne środki produkcji oraz stworzony zostanie system zachęt ekonomicznych dla przedsiębiorstw do eksportowania wytwarzanych przez nie wyrobów. Działania takie pomagają w kreowaniu właściwych warunków i stymulują wzrost gospodarki.
2) Promować transfer technologii, stworzyć wykwalifikowaną kadrę pracowników oraz doskonalić organizację produkcji i marketingu. Kładzie się tu nacisk na budowanie różnego typu infrastruktury: materiałowej, technicznej, naukowej, instytucjonalnej. W tym właśnie obszarze normalizacja odgrywa decydującą rolę w stymulowaniu rozwoju ekonomicznego. Nie jest bowiem możliwe stworzenie w jakiejkolwiek dziedzinie nowoczesnych systemów wytwarzania bez udziału normalizacji.

4. Zależności współczesnej normalizacji

Współczesna standaryzacja działań to nie tylko normalizacja, ale również badania jakościowe i kodyfikacja wyrobów oraz usług. A zaczęło się to od porządkowania w XIX wieku praw dotyczących wymiarów i kształtów maszyn niezbędnych dla potrzeb epoki industrializacji. Jak pisze A. Iwasiewicz: „Pierwsze organizacje normalizacyjne powstały w początkach XX wieku. W 1901 roku powstał jako pierwszy organ normalizacyjny

Komitet Normalizacji Mechaniki, przekształcony w 1918 roku w Brytyjską Organizację Normalizacyjną (BSI). Kolejnymi organami narodowymi były Niemiecki Komitet Normalizacyjny w 1917 r. (obecnie DIN) oraz Komitet Normalizacyjny w Stanach Zjednoczonych w 1918 r."[4]. Pierwszą międzynarodową organizacją normalizacyjną była IEC (*International Electrotechnical Commission*) – Międzynarodowa Komisja Elektrotechniczna powołana w 1904 roku w związku z szybko rozwijającym się przemysłem elektrotechnicznym. Jej zadania dotyczyły wówczas ujednolicania parametrów wytwarzanej energii elektrycznej, jak również korzystających z niej wyrobów.

Powstałe w 1919 roku Stowarzyszenie Elektryków Polskich utworzyło Polski Komitet Krajowy Elektrotechniki, który w 1923 roku został członkiem IEC[5]. W tym samym czasie przy Ministerstwie Handlu i Przemysłu II RP powstał, jako organ państwowy, Komitet Techniczny ds. Normalizacji Wyrobów Przemysłowych – poprzednik powołanego oficjalnie w 1924 roku Polskiego Komitetu Normalizacyjnego (PKN). Wprowadzono zarazem Polską Normę (PN) jako oficjalny dokument do dobrowolnego stosowania[6].

Krajowe organizacje i komitety normalizacyjne powstające na przełomie XIX i XX wieku, w ramach rozwoju współpracy międzynarodowej, powołały w 1926 roku w Szwajcarii Międzynarodową Federację Komitetów Normalizacyjnych, której rolą była przede wszystkim wymiana informacji. Jej działanie zostało praktycznie przerwane przez wybuch II wojny światowej, a w 1942 roku formalnie (decyzja Rady Federacji) zawieszone. Na bazie tej organizacji z inicjatywy Komitetu Koordynacyjnego Norm ONZ powołano w 1947 roku nową jednostkę, Międzynarodową Organizację Normalizacyjną (ISO). Jej zadaniem było tworzenie norm międzynarodowych, do których miały być dostosowywane normy krajowe. Jednym z jej członków-założycieli był reaktywowany w 1945 roku Polski Komitet Normalizacyjny[7]. Obecnie ISO zrzesza ponad 80 jednostek normalizacyjnych oraz przedstawicieli około 30 krajów nie posiadających własnego systemu normalizacyjnego.

Obecnie normalizacja to nie tylko zaspokojenie potrzeb klienta, ale także środowiska – unikanie niepożądanych skutków ubocznych, bezpieczeństwo użytkowania, odpowiednia ochrona informacji i zarządzanie nimi, wysoka niezawodność systemów i procesów. Normy przywoływane są coraz częściej: pomagają w podjęciu decyzji o przyjęciu lub odrzuceniu dostawy, pozwalają dokonać oceny zgodności z przyjętymi powszechnie standardami pod kątem ochrony zdrowia, bezpieczeństwa lub ochrony środowiska. Normy stanowią także wielkie ułatwienie w handlu międzynarodowym, tworząc płaszczyznę porozumienia co do ujednoliconych wymagań, wynikających niejednokrotnie z wieloletnich dobrych praktyk oraz tradycji inżynierskich i kupieckich.

4) A. Iwasiewicz, Zarządzanie jakością, Wydawnictwo Naukowe PWN, Warszawa 1999.

5) „Historia SEP w latach 1919–1999", materiały XXX Nadzwyczajnego Walnego Zjazdu Stowarzyszenia Elektryków Polskich, Warszawa 1999.

6) Pierwsza Polska Norma została opublikowana w 1925 r., patrz: Przewodnik po normalizacji (praca zbiorowa), wyd. PKN, Warszawa 2009.

7) Przewodnik po normalizacji, praca zbiorowa, wyd. PKN, Warszawa 2009.

Uzyskanie potwierdzenia zgodności z normami, w postaci certyfikatu akredytowanej i uznanej na rynku światowym jednostki certyfikującej, buduje stabilną i mocną pozycję danej firmy na rynku. Dotychczasowe, dość powszechnie spotykane certyfikaty zgodności z wymaganiami normy ISO 9001 (kolejne edycje: 1993; 2000; 2008), świadczące o trosce o wysoki poziom jakości zarządzania procesami w przedsiębiorstwie, są coraz częściej uzupełniane w ramach systemów zintegrowanych o wymagania dotyczące środowiska (ISO 14001:2004), bezpieczeństwa warunków pracy (OHSAS 18001 ↔ PN-N-18001:2004) oraz zarządzania bezpieczeństwem informacji (PN-ISO/IEC 27001:2007).

Korzyści ze stosowania tych norm wydają się oczywiste, ale warto je przypomnieć w quasi-dekalogu współczesnych przedsiębiorców:

I. Normy sprzyjają komunikowaniu się i likwidowaniu barier w handlu

Brak jednolitych norm krajowych utrudnia swobodny przepływ dóbr i usług.

II. Normy przyczyniają się do zwiększenia bezpieczeństwa pracy i użytkowania

Odpowiedzialność za zdrowie społeczeństwa, bezpieczeństwo i ochronę środowiska ponoszą organy władzy. Upowszechniana jest więc polityka, aby w europejskim i krajowym ustawodawstwie powoływać się na normy europejskie jako wzorzec zgodności w obszarze regulowanym.

III. Normy są uznawane za gwarancję odpowiedniej jakości

W dyrektywach dotyczących zamówień publicznych wymaga się, aby w ofertach powoływano się na normy europejskie, o ile w danym obszarze takie istnieją. Jest to istotne, ponieważ zamówienia publiczne stanowią około 10% wszystkich przedsięwzięć w Europejskim Obszarze Gospodarczym – EOG (*European Economic Area* – EEA).

IV. Normy przyczyniają się obniżenia kosztów ochrony zdrowia lub środowiska

W wielu dziedzinach tzw. normy zharmonizowane z dyrektywami nowego podejścia pozwalają producentowi zadeklarować zgodność wyrobów z wymaganiami przepisów technicznych bez konieczności powoływania strony trzeciej do wydania stosownego certyfikatu („Deklaracja zgodności" – norma PN-EN 17050).

V. Normy ułatwiają eksport

Dzięki normom europejskim otwiera się dla producentów z obszaru UE rynek ponad 360 milionów konsumentów, na którym koszty amortyzacji badań rozwojowych i wprowadzania nowych wyrobów są znacznie mniejsze niż przy jednostkowym rynku krajowym. Umowy transgraniczne w obszarze Unii Europejskiej są oparte na tym samym poziomie prawnym (umocowania ustawowe, skutki cywilnoprawne).

VI. Normy sprzyjają swobodnemu przepływowi towarów i wpływają korzystnie na poziom ich cen

Dzięki normom europejskim wzrasta konkurencyjność i wolność wyboru konsumenta w zakresie dóbr i usług oferowanych na rynku.

VII. Normy pozwalają na upowszechnianie postępu technicznego

Dzięki zaufaniu do norm europejskich, definiujących nowe materiały i technologie, możliwy jest rozwój nowego przemysłu w zaawansowanych technologicznie dziedzinach. Tym samym z jednej strony stwarzane są nowe możliwości zatrudnienia, a z drugiej – produkowane nowoczesne wyroby.

VIII. Normy sprzyjają utrwalaniu osiągnięć techniki

Szeroko zakrojona normalizacja europejska, kreując zasadniczo jedynie podstawowe obszary wymagań dotyczących bezpieczeństwa, bez konieczności uzgadniania szczegółów technicznych, pozwala na powstawanie nowych usług, na przykład w zakresie techniki informatycznej (IT – *Information Technology*) lub w usługach telekomunikacyjnych ICT (*Information & Communication Technology*).

IX. Normy ułatwiają eksport globalny

Promując normy europejskie na szczeblu międzynarodowym, a zarazem przyjmując międzynarodowe osiągnięcia normalizacyjne, zachęca się i popiera rozwój normalizacji globalnej oraz powszechne otwarcie rynków dla producentów. Dla wszystkich europejskich wysiłków i działań priorytetem jest rozwój normalizacji na szczeblu międzynarodowym wszędzie tam, gdzie to możliwe.

X. Normy ułatwiają porozumiewanie się i dają gwarancję porównywalnego standardu wyrobów i usług

Kreowanie pewnych, partnerskich relacji między dostawcami i poddostawcami, szczególnie wśród małych i średnich przedsiębiorstw (MŚP), jest podstawą sukcesu w budowaniu przemysłu. Zgodność z normami zarządzania jakością przyczynia się do osiągnięcia tego celu i daje wspaniałe możliwości zademonstrowania możliwości poddostawców. Wdrażane zintegrowane systemy zarządzania jakością i bezpieczeństwem tworzą porównywalne standardy wyższego poziomu produkcji i oferowanych usług.

Warto pamiętać, że w normalizacji krajowej prowadzonej za pośrednictwem Polskiego Komitetu Normalizacyjnego (w oparciu o jego ustawowe i statutowe umocowanie) stosuje się następujące zasady:

– jawności i powszechnej dostępności,
– uwzględniania interesu publicznego,
– dobrowolności uczestnictwa w procesie opracowywania i stosowania norm,
– zapewnienia możliwości uczestnictwa wszystkich zainteresowanych stron w procesie opracowywania norm,
– konsensusu jako podstawy procesu uzgadniania treści norm,
– niezależności od administracji publicznej oraz jakiejkolwiek grupy interesów,
– jednolitości i spójności postanowień norm,
– wykorzystywania sprawdzonych osiągnięć nauki i techniki,
– zgodności z zasadami normalizacji europejskiej i międzynarodowej.

Zasady te nie dotyczą Norm Obronnych – opracowywanych w Wojskowym Komitecie Normalizacyjnym – będących obligatoryjnymi w zastosowaniu i w znacznej swej części niejawnymi dokumentami wdrażającymi zasady i praktyki wynikające z podpisanych sojuszy oraz porozumień wojskowych (STANAG's, AP's[8]). Obszary ich stosowania są objęte ustawowymi klauzulami jakości i kodyfikacji, będącymi praktycznym wdrożeniem Procesu Rządowego Zapewnienia Jakości – GQA (ang. *Government Quality Assurance*). Realizacja tego procesu jest podstawowym elementem porozumienia standaryzacyjnego NATO STANAG 4107 „Wzajemna akceptacja procesu Rządowego Zapewnienia Jakości oraz stosowania publikacji standaryzacyjnych zapewnienia jakości" (AQAP 2070).

5. Podsumowanie

Z zasygnalizowanych powyżej zagadnień wynika jednoznacznie, że potrzeby biznesowe wykorzystują i stymulują działania normalizacyjne, choć dyskusyjny jest zakres i sposób udzielanego wsparcia finansowego (doraźne i celowe – nie zawsze służy szerzej rozumianym celom i potrzebom rynku).

Może warto więc przypomnieć kanon zaleceń przedstawiany przez Williama Edwardsa Deminga[9] jako filozofia sukcesu i wymóg działań jakościowych wobec nowoczesnego przedsiębiorcy:

1) Zapewnij stałość celów przedsiębiorstwa (poprawa jakości wyrobów i usług), mając na uwadze poprawę swojej konkurencyjności i osiągnięcie trwałej pozycji na rynku.
2) Stosuj nową filozofię. Nie można dłużej tolerować powszechnie akceptowanych poziomów opóźnień, omyłek, usterek materiałów nie nadających się do obróbki, ludzi nie potrafiących wykonać dobrze swojej pracy, a bojących się zadawać pytania, przestarzałych metod szkolenia. Zadowolenie klienta jest elementem sterującym wszystkimi działaniami.
3) Nie uzależniaj jakości od działań kontrolnych (jakości nie da się osiągnąć przez kontrolę, jakość musi powstać w całym procesie wytwarzania). Zapobiegaj wadom zamiast je wykrywać.
4) Zerwij z praktyką wybierania najtańszych ofert. Cena niewiele nam powie, jeśli nie ma jasności co do jakości wyrobu. Eliminuj dostawców, którzy nie są w stanie poradzić sobie z udokumentowaniem jakości.
5) Stale doskonal system funkcjonowania firmy. Ujawniaj problemy i ich przyczyny. Udoskonalaj sam proces, a nie tylko jego wyniki (uwzględnij projektowanie, zaopatrzenie, zapewnienie sprawności urządzeń, produkcję, szkolenie itd.). Nadzoruj ten proces i steruj nim.
6) Wprowadź nowoczesne metody szkoleniowe na stanowiskach pracy. Człowiek jest wszędzie decydującym ogniwem każdego procesu, również tego w pełni zautomatyzowanego.
7) Wprowadź nowoczesny, właściwie rozumiany nadzór ze strony kadry kierowniczej. Kierownik powinien zawsze pomagać pracownikowi tak, aby mógł on lepiej wykonywać swoje obowiązki. Oznacza to, że:

*8) STANAG (**STAN**dardization **AG**reement) – porozumienie standaryzacyjne; AP (Allied Publication) – publikacja sprzymierzonych.*

9) William Edwards Deming – żył w latach 1900–1993. Amerykański statystyk, ekspert w dziedzinie kontroli jakości. Wykorzystał statystykę do przebadania procesu produkcji przemysłowej, wyłapania jego błędów i poprawienia jakości produktu. Jego nowatorskie metody jako pierwsi zaakceptowali Japończycy. Zaczęli je stosować w przemyśle, co w znacznym stopniu przyczyniło się do jego odbudowy w latach powojennych, za co Deming był bardzo mocno i głośno krytykowany przez amerykańskie korporacje, które wcześniej lekceważyły jego wyniki badań i propozycje zmian.

– przełożony jest szkoleniowcem i opiekunem swoich pracowników (pełni funkcję lidera, a nie bossa);
– błędy wynikające z systemu nie mogą obciążać pracownika. Kierownictwo musi podejmować natychmiastowe działania w odpowiedzi na raporty dozoru technicznego dotyczące takich problemów, jak: permanentne braki, nie konserwowane urządzenia, złe narzędzia, bełkotliwie sformułowane instrukcje itp.

8) Wyeliminuj atmosferę strachu; wspieraj wzajemne kontakty i inne środki prowadzące do eliminacji strachu w ramach całego przedsiębiorstwa;
– robotnik, bojąc się niewykonania określonej normatywem ilości elementów, przekazuje do dalszej obróbki również części wadliwe,
– kierownik przedkłada dyrekcji „upiększone dane", gdyż boi się, że złe wyniki zostaną złożone na karb jego nieudolności, chociaż rzeczywista przyczyna tkwi w istniejącym systemie,
– dostawca, bojąc się, że nie otrzyma zamówienia, obiecuje dostawy najwyższej jakości, mimo że nie posiada odpowiednich warunków technicznych i organizacyjnych,
– jeśli wady wiążą się z sankcjami, to każdy pracownik robi wszystko, aby tych wad nie ujawniać.

9) Przełam bariery między pionami i działami firmy:
– bariery w strukturach pionowych powodują problemy komunikacyjne na odcinku przełożony – pracownicy,
– bariery w strukturach poziomych powodują problemy komunikacyjne między różnymi działami i ich pracownikami (tymczasem ludzie zatrudnieni przy badaniach, projektowaniu, produkcji i sprzedaży muszą pracować jak jeden zespół, przewidywać i rozwiązywać problemy wynikające z różnych wymagań),
– również w ramach firmy układ między stanowiskami i osobami należy rozpatrywać w aspekcie stosunków klient wewnętrzny – dostawca wewnętrzny.

10) Nie stosuj sloganów i nawoływania pracowników do większej wydajności. Wywołuje to skutek przeciwny. W większości przypadków przyczyna niskiej jakości i wydajności leży w samym procesie i wykracza poza możliwości oddziaływania zwykłego pracownika.

11) Usuń normy pracy narzucające limity ilościowe.

12) Eliminuj wszystko, co kwestionuje prawo każdego pracownika i każdego menadżera do dumy ze swojej pracy. Oznacza to:
– wyjaśnienie pracownikom polityki kierownictwa firmy,
– niedopuszczenie do tego, aby dobra praca trafiała „do kosza albo na złom",
– zrezygnowanie z dorocznych ocen pracowników.

13) Promuj kształcenie. Wprowadzenie innowacji produktowych i procesowych wymaga nowych umiejętności. Dlatego:
– dokształcanie musi dotyczyć wszystkich szczebli, poczynając od najwyższego kierownictwa,
– wiedza o metodach statystycznych, szczególnie o sterowaniu procesem, powinna być przekazana odpowiednio każdemu pracownikowi,
– nakłady na kształcenie należy traktować jako inwestycję konieczną.

14) Traktuj codzienną dbałość o realizację powyższych 13 zasad jako podstawowy obowiązek kierownictwa firmy.

Analizując coraz szerszy zakres wymagań normatywnych i jakościowych funkcjonujący na współczesnym rynku, warto się zastanowić nad zasadami W.E. Deminga.

Opracował: dr inż. Marek Blim

Bibliografia:

1) Europejski oficjalny portal poświęcony ocenie zgodności (certyfikacji): http://www.conformityassessment.org/directory/main.
2) Ganeri A., *Form cubit to kilogram*, tłum. M. Cabaj, Nasza Księgarnia, Warszawa 1998.
3) Karaszewski R., *TQM – teoria i praktyka*, wyd. II, Dom Organizatora, Toruń 2008.
4) Materiały europejskiej organizacji normalizacyjnej CEN: *http://www.cenorm.be/*.
5) Materiały ISO: *http://www.iso.ch/iso/en/ISOOnline.frontpage*.
6) *Przewodnik po normalizacji*, praca zbiorowa, PKN, Warszawa 2009.
7) Rezolucja Parlamentu Europejskiego z 24 maja 2007 r. w sprawie wykorzystania wiedzy w praktyce (*www.euro-lex/service/*).
8) Strona Polskiego Komitetu Normalizacyjnego (PKN): *http://www.pkn.pl/aktualnosci1.htm*.
9) Wawak S., *Zarządzanie jakością. Teoria i praktyka*, wyd. II, Helion, Gliwice 2005.

Możliwości wykorzystania sieci IP w systemach bezpieczeństwa

James Smith

W niniejszym artykule autor – europejski przedstawiciel handlowy firmy Samsung Techwin Europe – zwraca uwagę na pewne zagadnienia, które powinny być rozpatrzone na samym początku procesu tworzenia systemów dozorowych obsługiwanych za pośrednictwem sieci. Autor analizuje także pewne najnowsze opracowania, dotyczące produktów przeznaczonych do pracy w sieciowych systemach dozorowych, stymulujące rozwój gałęzi przemysłu elektronicznego związanej z systemami bezpieczeństwa

Ta gałąź przemysłu przez długi czas była utożsamiana z telewizją dozorową, czyli CCTV – w dosłownym tłumaczeniu: telewizją w obwodzie zamkniętym – i w istocie przez wiele lat była „obwodem zamkniętym". Systemy analogowe, w których do transmisji sygnałów wizyjnych wykorzystywane były kable koncentryczne lub kable z parami skrętnymi, już dawno zyskały możliwość podłączenia do sieci za pośrednictwem odpowiednich urządzeń sterujących. Nawet w przypadku zastosowania najtańszych rozwiązań sprzętowych istnieje możliwość obserwacji obrazów, sterowania kamerami i administrowania systemem za pośrednictwem komputera PC podłączonego do Internetu. Jednak obecnie tendencją wiodącą w telewizyjnych systemach dozorowych jest podłączanie kamer przemysłowych bezpośrednio do sieci. Dzięki temu produkty przeznaczone do budowy sieciowych systemów bezpieczeństwa mają największy wpływ na rozwój rynku zabezpieczeń elektronicznych, gdyż w nowo powstających instalacjach zalety pracy w sieci IP są w pełni wykorzystywane. Poza niskim kosztem instalacji – użytkownicy mogą zaoszczędzić na infrastrukturze kablowej – urządzenia sieciowe oferują wiele trudnych do zignorowania korzyści, dzięki którym systemy sieciowe uzyskują przewagę nad tradycyjnymi systemami analogowymi.

Nikt nie ma ochoty inwestować dużych sum w systemy dozorowe i wielokrotnie powtarzać takich inwestycji. Każdy natomiast klient chciałby kupić rozwiązanie, które nie tylko spełni obecne wymagania, lecz także pozwoli na rozbudowę systemu w przyszłości. Równie ważna jest możliwość jak najlepszego wykorzystania wszystkich istniejących systemów – takich, jak systemy kontroli dostępu, domofonowe, sygnalizacji włamania i napadu, ochrony obwodowej i sygnalizacji pożarowej oraz BMS – przez ich wzajemne połączenie i zmuszenie do współpracy. Oczywiste korzyści użytkowe wynikają z możliwości przekazywania sygnałów wizyjnych, danych sterujących oraz informacji o alarmach pomiędzy poszczególnymi systemami, z których każdy może być zlokalizowany w dowolnym miejscu sieci.

Podstawowe zalety systemów dozorowych, których działanie bazuje na sieci IP:

1) Pozwalają na znaczne obniżenie kosztów okablowania dzięki wykorzystaniu istniejącej sieci, bez konieczności instalacji nowych tras kablowych. Pojedynczy kabel sieciowy może być zastosowany do jednoczesnej transmisji sygnału wizji, fonii oraz danych sterujących i telemetrycznych, a także do zasilania urządzeń metodą PoE (*Power over Ethernet*).
2) Umożliwiają przeglądanie obrazów i sterowanie systemem z dowolnego punktu w sieci, a także połączenie się z systemem z dowolnego miejsca na obszarze całego świata.
3) Wykazują dużą elastyczność: rejestracja obrazów o strategicznym znaczeniu może się odbywać w dowolnym punkcie sieci, a ich odtwarzanie jest możliwe z wykorzystaniem dowolnego komputera PC i może być dokonane przez użytkownika dysponującego odpowiednimi uprawnieniami.
4) Stwarzają użytkownikom możliwość skorzystania z kamer najnowszej generacji, odznaczających się wysoką rozdzielczością, znacznie przekraczającą możliwości, jakimi dysponują klasyczne, analogowe kamery CCTV, które typowo wytwarzają obrazy o rozdzielczości 0,4 megapiksela. Na przykład kamera o rozdzielczości 1,3 megapiksela z odpowiednio dobranym polem widzenia może pełnić rolę kilku kamer analogowych, gdyż pozwala na obserwację dużego obszaru, a w razie potrzeby umożliwia powiększenie fragmentu obrazu (w celu dokładniejszego przyjrzenia się szczegółom odległych obiektów) bez jego widocznej „pikselizacji".
5) Zastosowanie oprogramowania zarządzającego systemem, zainstalowanego na komputerze PC, pozwala na współpracę kamer oraz urządzeń rejestrujących pochodzących od różnych producentów. Jednakże w celu zapewnienia kompatybilności wszystkich składników systemu należy rozważyć zakup urządzeń zgodnych z globalnym standardem ONVIF. Standard ONVIF został opracowany w ramach otwartego forum producentów i stanowi rodzaj interfejsu pozwalającego na łączenie różnych urządzeń.

Kamery wykorzystywane w systemach bezpieczeństwa nie są kamerami internetowymi

Należy podkreślić, że kamery IP przeznaczone do pracy w systemach bezpieczeństwa mają niewiele wspólnego

Fot. 1. SNB-5000

Fot. 2. SND-5080

z kamerami internetowymi. Jedyne podobieństwo polega na zastosowaniu tych samych protokołów komunikacyjnych i transmisyjnych. Większość właściwości i funkcji użytkowych kamer sieciowych najnowszej generacji jest dostosowana do oczekiwań użytkowników tradycyjnych, analogowych kamer CCTV. Dotyczy to takich funkcji, jak poszerzanie zakresu dynamiki (WDR), kompensacja przeciwoświetlenia (BLC) oraz redukcja szumów (NR). Ich celem jest zapewnienie możliwie najwyższej jakości obrazu zarówno w dziennych, jak i w nocnych warunkach oświetleniowych, a także sprostanie innym wyzwaniom, takim jak praca przy kontrastowym oświetleniu słonecznym czy oślepiającym świetle reflektorów samochodowych. Szczególnie istotny jest dobór właściwego typu kamery do pracy w określonych warunkach eksploatacyjnych. Możliwości są w tym zakresie zdumiewająco duże, co pozwala na znalezienie rozwiązania dokładnie spełniającego wymagania specyficzne dla konkretnej lokalizacji kamery. Firmy takie jak Samsung oferują darmowe usługi projektowe, ułatwiając użytkownikom dobór urządzeń najlepiej odpowiadających ich oczekiwaniom.

Kamery megapikselowe – najnowsze osiągnięcie w dziedzinie kamer sieciowych

Standard *High Definition* (HD) stał się powszechnie znany zarówno w naszych domach, jak i w miejscach pracy. Rewolucja cyfrowa stworzyła inżynierom możliwość zaprojektowania kamer sieciowych zdolnych do wytwarzania obrazów o rozdzielczościach, których poziom był niewyobrażalny jeszcze kilka lat temu. Dla użytkowników systemów wynika z tego niebezpieczeństwo mylnej interpretacji żargonowych określeń występujących na stronach internetowych producentów oraz w kartach katalogowych.

Zwyczajowo określa się jako megapikselowe te kamery, które są zdolne do wytwarzania obrazów o rozdzielczościach przekraczających milion pikseli. Na współczesnym rynku dużą popularność zyskały kamery o rozdzielczości 1,3 megapiksela, co jest równoznaczne z wytwarzaniem obrazów mieszczących się w rastrze 1280×1024 piksele.

Jednakże nie wszystkie kamery, które mają zdolność wytwarzania obrazów zawierających co najmniej milion pikseli, mogą być określane jako kamery HD, gdyż pojęcie to dotyczy ogólnie akceptowanego standardu HD, z którego wynikają dodatkowe wymagania. Kamery HD muszą być przystosowane do wytwarzania obrazów o rozdzielczościach 1920×1280 pikseli lub 1280×720 pikseli o proporcjach 16:9 (szeroki ekran). Ponadto kamery HD muszą mieć możliwość pracy w czasie rzeczywistym, to znaczy muszą wytwarzać minimum 25 obrazów na sekundę. Niektóre z tych właściwości nie dotyczą megapikselowych kamer przemysłowych. Podsumujmy: wszystkie kamery HD są kamerami megapikselowymi, ale nie wszystkie kamery megapikselowe są kamerami HD.

Zalety kamer HD

Kamery megapikselowe pozwalają na uzyskanie obrazów o bardzo dobrym odwzorowaniu szczegółów, ale mają również możliwość równoczesnego wytwarzania i transmisji obrazów o niskich rozdzielczościach, włącznie z formatami QVGA (320×240), VGA (640×480) i SVGA (800×600). Pozwala to na transmisję strumieni danych o właściwościach możliwie najlepiej dostosowanych do parametrów urządzeń wyświetlających obrazy. Przykładowo, obrazy mogą być rejestrowane w pełnej rozdzielczości (czyli 1,3 megapiksela) w urządzeniach zainstalowanych w pomieszczeniu technicznym, a jednocześnie przeglądane w rozdzielczości QVGA za pomocą telefonu komórkowego.

Kamery megapikselowe oferują znacznie więcej korzyści, niżby to wynikało z wytwarzania obrazów o znakomitej, „dowodowej" jakości oraz o właściwych proporcjach. Dysponują one wieloma innymi funkcjami użytecznymi dla operatorów systemów dozorowych, pozwalającymi na znacznie skuteczniejsze reagowanie w wymagających tego sytuacjach. Większość tych dodatkowych możliwości jest związana z działaniem układów DSP wbudowanych w kamery. Jednym z nich jest układ WiseNet1 DSP, stworzony przez firmę Samsung w celu maksymalnego wykorzystania zalet wynikających z technologii megapikselowej.

Kolejną zaletą jest możliwość przypisania różnym użytkownikom – o określonych poziomach uprawnień – dowolnie dobranych metod kompresji oraz ustalonych wartości rozdzielczości obrazów. Umożliwia to jednoczesną obserwację obrazów w jednej z lokalizacji, rejestrację materiałów dowodowych w innej lokalizacji, a także przeglądanie bieżących lub archiwalnych obrazów na urządzeniach przenośnych, takich jak telefony komórkowe.

Kamery sieciowe umożliwiają wysłanie zgłoszenia incydentu za pośrednictwem poczty elektronicznej z dołączonymi zdjęciami (skompresowanymi metodą JPEG) oraz jednoczesną dokumentację tego incydentu w postaci ruchomych obrazów zarejestrowanych w trybie prealarmowym i postalarmowym na karcie pamięci SD zainstalowanej wewnątrz kamery.

Inteligentna analiza treści obrazów

Inną istotną zaletą większości kamer megapikselowych jest możliwość inteligentnej analizy treści wytwarzanych przez nie obrazów. Opracowany przez firmę Samsung układ WiseNet1 DSP ma wbudowaną bezpłatną opcję IVA, która poza

Fot. 3. SPE-100 FS2

klasyczną detekcją ruchu pozwala na wykrywanie wtargnięć w obszary ograniczone niewidzialnymi liniami, wykrywanie obiektów poruszających się w określonym kierunku, wykrywanie faktu pojawiania się obiektów w określonym obszarze lub ich znikania z niego. Opcja IVA zawiera także funkcję antysabotażową, pozwalającą na wysłanie sygnału ostrzegawczego w przypadku wykrycia zmiany w obserwowanej przez kamerę scenie, na przykład na skutek zamalowania obiektywu farbą w sprayu lub zmiany pola widzenia kamery w wyniku jej nieautoryzowanego przemieszczenia.

Inne istotne zalety kamer HD firmy Samsung:

1) Dzięki jednoczesnemu wykorzystaniu połączeń przez sieć Ethernet i przez złącze BNC sygnał wizyjny może być transmitowany zarówno przez sieć, jak i przez kabel koncentryczny. Umożliwia to pracę w systemach hybrydowych oraz ułatwia instalację kamer i głowic szybkoobrotowych, gdyż podczas regulacji kamer można posługiwać się standardowymi monitorami telewizyjnymi.
2) Dwukierunkowa, dupleksowa transmisja sygnałów fonicznych pozwala na stworzenie systemu komunikacji głosowej pomiędzy miejscem, w którym zainstalowana jest kamera, a pomieszczeniem kontrolnym. Przykładowo, może zaistnieć potrzeba weryfikacji tożsamości osób próbujących wjechać samochodem na określony teren. Dzięki dwukierunkowej komunikacji głosowej i możliwości jednoczesnej obserwacji obrazów o wysokiej rozdzielczości przedstawiających kierowcę pojazdu zastosowanie kamery HD pozwala na uniknięcie konieczności zatrudniania dodatkowych strażników. Ponadto, dzięki temu, że kamery HD dostarczają obrazy o jakości dowodowej oraz zapewniają możliwość dwukierunkowej komunikacji głosowej, mogą być stosowane do odstraszania nieproszonych gości.
3) Możliwe jest zamaskowanie pewnych fragmentów obrazu jednobarwnymi polami w kształcie wieloboku, co pozwala prowadzić monitoring określonych obszarów bez naruszania prywatności obiektów znajdujących się w sąsiedztwie.
4) Wykorzystanie pamięci SD umieszczonej w złączu znajdującym się wewnątrz kamery pozwala na łatwe tworzenie zapasowych kopii nagrań z wydarzeń o charakterze alarmowym.
5) Kamery mogą być zasilane metodą PoE (*Power over Ethernet*), czyli pobierać energię z istniejącej sieci IP, co obniża koszty okablowania obiektu.
6) Kamery HD są w pełni kompatybilne z niewymagającym licencji oprogramowaniem NET-i *Viewer Centralised Management Software* (CMS), co stwarza możliwość podłączenia wszystkich produktów firmy Samsung do sieci IP zaraz po wyjęciu z opakowania.

Rejestracja obrazów

Użytkownicy pragnący rejestrować obrazy pochodzące z dowolnej z kamer sieciowych będą musieli dokładnie zastanowić się nad tym, gdzie i w jaki sposób chcą przechowywać zgromadzony materiał. Dostępne są zarówno rozwiązania oparte na oprogramowaniu uruchomionym na komputerze PC, jak i rozwiązania sprzętowe w postaci niezależnych jednostek *Network Video Recorder* (NVR).

Metody kompresji wbudowane w kamery o wysokiej rozdzielczości pozwalają na skuteczny zapis i przechowywanie nagrań. Przykładowo, metody H.264, MPEG4, MJPEG i JPEG wprowadzone do układu WiseNet1 DSP stwarzają użytkownikom możliwość jednoczesnej transmisji i rejestracji obrazów z wielu lokalizacji, z różnymi prędkościami, różnymi metodami kompresji oraz w różnych rozdzielczościach.

Technologia redukcji szumów SSNRIII, określana przez firmę Samsung jako *Super Noise Reduction*, ma także swój udział w zmniejszeniu wymagań stawianych urządzeniom rejestrującym oraz przyczynia się do lepszego wykorzystania pasma sieciowego podczas przeglądania obrazów za pośrednictwem sieci IP.

Najprostszym rozwiązaniem problemu zapisu obrazów może być zastosowanie rejestratorów NVR (*Network Video Recorder*), które w sposób oczywisty mogą być umieszczone w dowolnych punktach w sieci. Jeśli jednak w systemie wykorzystana jest znaczna liczba kamer o wysokiej rozdzielczości, najbardziej opłacalnym rozwiązaniem będzie wykorzystanie serwerów rejestrujących obrazy.

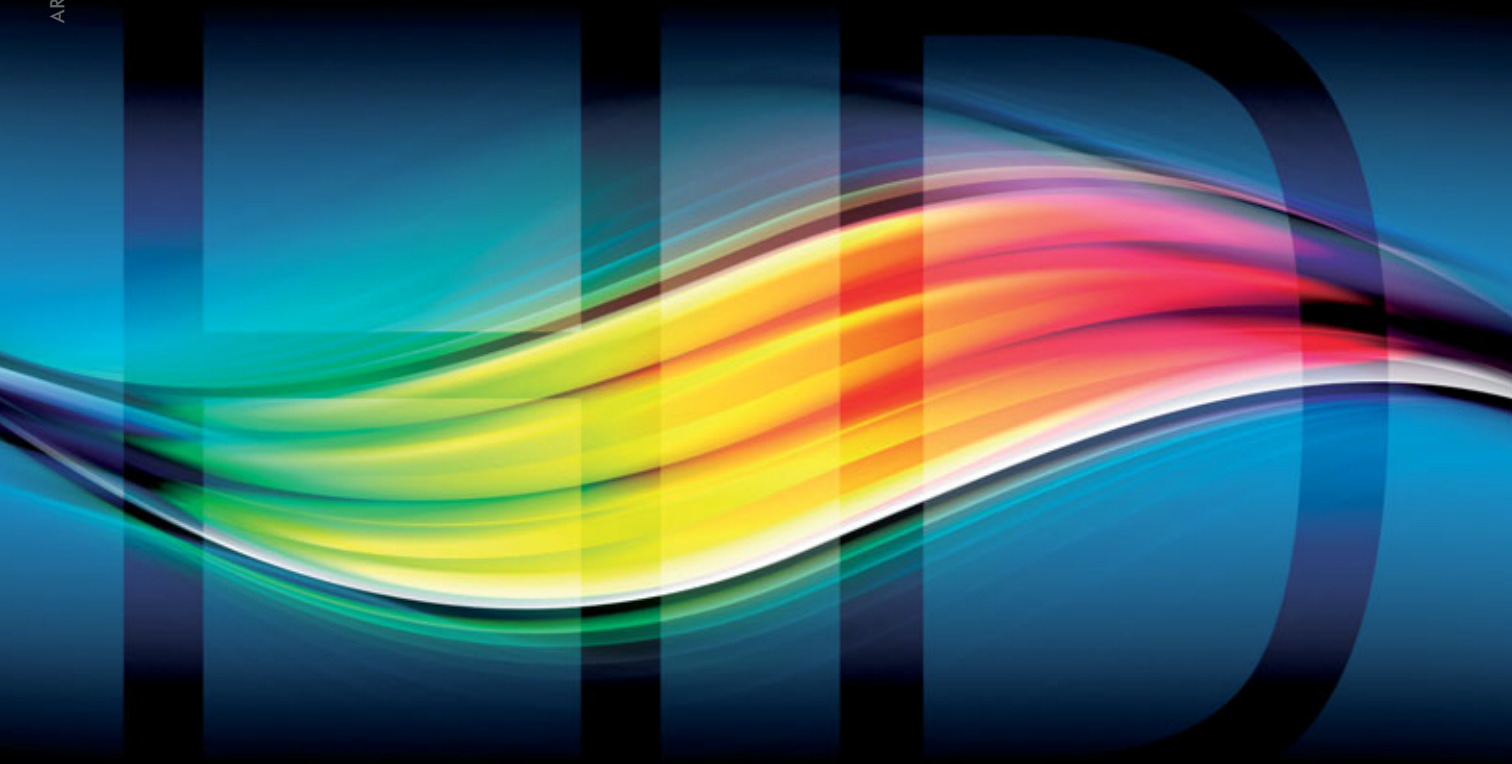
Możliwa jest lokalna rejestracja pewnych wybranych obrazów w układach znajdujących się wewnątrz kamer. Znajduje to na przykład zastosowanie w sytuacjach, w których do operatorów systemu w sposób ciągły wysyłane są jedynie obrazy o niskiej rozdzielczości. Oznacza to, że zarejestrowane w kamerach nagrania o wysokiej rozdzielczości, dokumentujące wykryte incydenty, mogą być w odpowiednim czasie przekazane przez sieć i obejrzane, bez konieczności stosowania transmisji szerokopasmowej.

Szkolenia

Projektanci, instalatorzy i integratorzy systemów, którzy na co dzień nie uczestniczą w projektowaniu technicznych systemów bezpieczeństwa, mogą uznać taką mnogość opcji za przytłaczającą lub mylącą. Z tego powodu producenci, tacy jak Samsung, prowadzą darmowe szkolenia, podczas których w kompleksowy sposób omawiane są wszystkie aspekty analogowych (CCTV) i sieciowych (IP) systemów bezpieczeństwa.

James Smith
Samsung Techwin Europe
Tłumaczenie: Redakcja

Kamery HDTV firmy Axis Communications w nowoczesnych systemach dozoru wizyjnego



Agata Majkucińska

Rynek sieciowych systemów dozoru wizyjnego zmierza w kierunku standardu HD oferującego – w podstawowym wymiarze korzyści – doskonały, wyraźny obraz, który wiernie odzwierciedla kolory i szczegóły. Pięć razy wyższa rozdzielczość w porównaniu z tradycyjną telewizją analogową sprawia, że nie można mieć wątpliwości, że to HDTV jest przyszłością rynku monitoringu wizyjnego

Przytoczę tu wypowiedź Erika Fränlida, zajmującego w Axis Communications stanowisko dyrektora ds. zarządzania produktami. Fränlid tłumaczy fenomen technologii HD następująco:

– Przyczyną wzrostu zainteresowania urządzeniami oferującymi jakość HDTV jest obniżanie się cen telewizorów HD oraz rosnąca liczba programów produkowanych w standardzie HD. Zgodnie z raportem „Globalne prognozy dotyczące urządzeń HDTV"[1], przygotowanym przez Informa Telecoms & Media, pod koniec 2009 roku tylko 5,8% gospodarstw domowych na całym świecie oglądało programy HD. Przewidywania wskazują jednak, że na koniec 2010 roku będzie ich już 21%. Ten sam raport przewidywał również globalną dywersyfikację poziomu implementacji rozwiązań HD. W 2010 roku dwie trzecie światowego zainteresowania technologią HDTV przypada na Amerykę Północną, jednak już cztery lata później odsetek ten będzie wynosił tylko 37%, gdyż wzrośnie udział Azji i Pacyfiku. Przewiduje się, że w 2014 roku region ten zajmie drugie miejsce i osiągnie 31% światowego udziału w rynku. Liderem w Europie jest Wielka Brytania, za którą na drugim miejscu plasuje się Francja.

Cyfrowa czy analogowa?

Pomiędzy systemami telewizji zamkniętej CCTV a systemami sieciowego dozoru wizyjnego istnieje wiele różnic, przy czym z wdrożenia systemów sieciowych wynika szereg korzyści.

Najważniejszą z nich jest możliwość osiągnięcia wysokich rozdzielczości (mierzonych w pikselach), o jakich nie może być mowy w systemach analogowych. CCTV to technologia wywodząca się z rynku telewizyjnego. W drugiej połowie XX wieku zdominowały go dwa standardy: PAL i NTSC.

System PAL (*Phase Alternating Line*) upowszechnił się w Europie i większej części Azji. W Ameryce Północnej i Środkowej, jak również w niektórych częściach Azji, obowiązywał system NTSC (*National Television System Committee*). PAL to system obrazu składającego się z 576 linii pionowych (TVL) przy częstotliwości 50 Hz i prędkości 25 klatek na sekundę (fps), natomiast system NTSC transmituje 480 aktywnych linii pionowych przy częstotliwości 60 Hz i prędkości 30 klatek na sekundę.

Wyższy standard w praktyce

Historia badań nad systemami telewizyjnymi o wysokiej rozdzielczości sięga aż 1958 roku. Pierwsze techniki uzyskiwania wyjątkowo czystego i wyraźnego obrazu opracowało radzieckie wojsko. Jego system telekonferencji o nazwie *Transformer* był zdolny do wytwarzania obrazu składającego się z 1125 linii. Dziesięć lat później japoński publiczny nadawca – NHK – opracował pierwszy system o wysokiej rozdzielczości obrazu przeznaczony do użytku komercyjnego.

Długi proces rozwoju nie był związany z obojętnością lub brakiem popytu. Wręcz przeciwnie, HDTV i perspektywa znacznej poprawy jakości obrazu budziły duże zainteresowanie konsumentów na całym świecie. Przemysł dostrzegł potencjał rosnącego rynku masowego. Pierwszy duży przełom nastąpił na początku lat dziewięćdziesiątych, kiedy wprowadzono standard kompresji MPEG wykorzystujący metody rozpoznawania wzorców, opracowany dla rakiet typu Cruise w Laboratorium Napędu Odrzutowego (*Jet Propulsion Laboratory*) w NASA. W 1993 roku powstał standard MPEG-2, który spowodował dalszy rozwój technologii cyfrowej. Projekt realizowany wspólnie przez MPEG i grupę Video Coding Experts Group z Międzynarodowej Unii Telekomunikacji (*International Telecom Union* – ITU) doprowadził do stworzenia standardu H.264, znanego także jako MPEG-4 Part 10/AVC. Taka technika kompresji nie tylko uczyniła nadawanie HDTV możliwym, ale także opłacalnym.

Jak przekonuje Erik Fränlid, postępujące zmiany wpłynęły również na technologię nadzoru wizyjnego. – *Przejście na technologię HDTV na rynku konsumenckim znacząco wpłynęło na rynek systemów dozorowych, ponieważ klienci wymagali wyższej jakości obrazu także od kamer służących do monitorowania. Choć nagrania o wysokiej rozdzielczości wymagają zapisu znacznie większej ilości danych, kamera sieciowa, która oferuje jakość HDTV i pracuje zgodnie ze standardami SMPTE, a do tego obsługuje format H.264, zapewnia wymaganą rozdzielczość i częstotliwość odświeżania przy jednoczesnej redukcji objętości gromadzonego materiału wizyjnego do akceptowalnych rozmiarów. Dzięki temu można uzyskać obrazy telewizyjne o wysokiej jakości bez nadmiernych kompromisów. Dzięki technologii skanowania progresywnego kamery sieciowe HDTV oferują odwzorowanie rzeczywistych kolorów i wyraźne obrazy nawet w przypadku szybko poruszających się obiektów. Oznacza to, że technologia HDTV staje się bardzo atrakcyjnym rozwiązaniem dla sektora nadzoru, także w miejscach wymagających wyższego poziomu szczegółowości obrazu, na przykład w sklepach detalicznych, na lotniskach, w kasynach lub na autostradach.*

Rozwiązania i korzyści

W 1996 r. firma Axis Communications położyła podwaliny pod nowoczesne systemy dozoru wizyjnego, wprowadzając na rynek kamerę sieciową przeznaczoną do pracy w systemach profesjonalnego monitorowania. Nieustannie poszerzana oferta, w której ważne miejsce zajmują kamery HD, pozwoliła firmie uplasować się na pozycji lidera wyznaczającego nowe trendy w sektorze nadzoru wizyjnego.

W ubiegłym roku firma wprowadziła do oferty pierwszą kamerę HD AXIS Q1755, która wskazała kierunek, w jakim zaczyna zmierzać rynek sieciowych systemów wizyjnych, i jasno określiła pozycję Axisa jako innowatora w tej dziedzinie. Na dzień dzisiejszy w ofercie firmy dostępnych jest ponad dwadzieścia modeli kamer HDTV przeznaczonych do zastosowania w różnych segmentach rynku, takich jak transport, handel, nadzór miast, edukacja etc.

Od grudnia 2010 r. dostępne są nowe kamery HDTV firmy Axis Communications. Zaprezentowane po raz pierwszy na targach w Essen modele AXIS P3346 to stałopozycyjne kamery kopułkowe HDTV z matrycą o rozdzielczości 3 Mpx, które zostały wyposażone w funkcje zdalnej regulacji ogniskowej obiektywu i zdalnej regulacji ostrości obrazu. Kamery AXIS P3346 wyróżniają się także zastosowaniem mechanizmu P-Iris, który umożliwia precyzyjne sterowanie przesłoną. Nowe modele kamer Axis dostępne są w trzech wersjach: do instalacji wewnętrznych (AXIS P3346), odpornej na akty wandalizmu (AXIS P3346-V) oraz przeznaczonej do pracy na zewnątrz (AXIS P3346-VE).

Nowe stałopozycyjne kamery kopułkowe zapewniają obraz o rozdzielczości 3 megapikseli przy poklatkowości wynoszącej 20 obrazów na sekundę albo o rozdzielczości HDTV 1080p przy poklatkowości 30 obrazów na sekundę, dzięki czemu

1) *http://www.informatm.com/marlin/30000001001/MARKT_EFFORT/marketingid/20001772632*

gwarantują klarowny i ostry materiał wizyjny. Mechanizm P-Iris pozwala dostosować ustawienie przesłony do wymaganej głębi ostrości obrazu i umożliwia ustawienie pozwalające na maksymalne wykorzystanie rozdzielczości obiektywu, nie zaniedbując celu podstawowego, jakim jest dostosowanie kamery do zmian natężenia światła w celu zapewnienia niezawodnego nadzoru wizyjnego w każdych warunkach oświetleniowych.

Dodatkowym atutem kamer AXIS P3346 jest możliwość wyselekcjonowania z obserwowanej sceny do ośmiu niezależnych obszarów i transmitowania strumieni wizji z tych obszarów w czasie rzeczywistym (*multi-view streaming*). Ograniczenie transmisji do wybranych obszarów optymalizuje wykorzystanie pasma sieciowego i pamięci masowej. Każdy widok można dodatkowo powiększyć lub przesunąć w poziomie i pionie. Dzięki temu można znacznie zredukować koszty, ponieważ jedna kamera IP o rozdzielczości kilku megapikseli może symulować osiem kamer wirtualnych.

Silną pozycję na rynku wypracowały już sobie kamery AXIS 5534/-E i AXIS Q6034/-E. Modele serii P zapewniają obraz klasy HDTV, są wyposażone w 18-krotny zoom optyczny i 12-krotny zoom cyfrowy z autofokusem. Kamera AXIS P5534 typu PTZ (*pan-tilt-zoom*) jest przeznaczona do instalacji wewnętrznych na lotniskach, stacjach kolejowych, w magazynach, sklepach i szkołach, a model AXIS P5534/-E – do pracy na zewnątrz budynków. Każda z tych kamer wytwarza obraz w jakości HDTV 720p, czyli zgodnie ze standardem SMPTE 296M w rozdzielczości 1280×720 pikseli, przesyła 30 klatek na sekundę, zapewnia wierne odwzorowanie kolorów i proporcje 16:9. Kamera AXIS P5534 może równocześnie wysyłać strumienie wizyjne w formacie H.264 oraz MJPEG, z których każdy jest indywidualnie konfigurowany. Zastosowanie kompresji H.264 optymalizuje wykorzystanie pasma sieciowego i pamięci masowej bez obniżania jakości obrazu, natomiast obsługa formatu MJPEG zwiększa elastyczność i kompatybilność rozwiązania. Dzięki unikalnej funkcji Auto-flip AXIS P5534 obraca się o 360°, co pozwala symulować ciągły ruch poza punktem mechanicznego zatrzymania, a przez to umożliwia nieustanną obserwację nawet szybko przemieszczającego się obiektu. Dzięki mechanizmowi *Advanced Gatekeeper* kamera ta automatycznie obraca się i steruje przybliżeniem po wykryciu aktywności w danym obszarze, a następnie oddala ujęcie po zaprogramowanym czasie.

AXIS P5534

Seria Q6034/-E to najwyższa klasa urządzeń PTZ przeznaczonych do pracy non stop, 24 godziny na dobę przez siedem dni w tygodniu. Przystosowany do takiego działania mechanizm PTZ gwarantuje rzetelny nadzór nawet w bardzo wymagających warunkach zewnętrznych.

Modele AXIS Q6034 (do zastosowania wewnątrz pomieszczeń) i AXIS Q6034-E (stosowany na zewnątrz) oferują wysoki poziom rozróżnialności szczegółów w standardzie HDTV 720p i funkcję 18-krotnego zoomu optycznego, a także szybki obrót/pochylenie (0,05° – 450° na sekundę), pochylenie 220° (20° powyżej linii horyzontu), funkcję Active Gatekeeper, automatyczne śledzenie obiektów i możliwość zasilania przez sieć Ethernet (*High Power over Ethernet*). Doskonale sprawdzają się w zastosowaniach wymagających pokrycia dużego obszaru i wykonywania zbliżeń z zachowaniem szczegółowości obrazu.

AXIS P3346

Na drodze do upowszechnienia HDTV

Firma Axis Communications, pionier i lider rynku w dziedzinie technologii nadzoru wizyjnego IP, niejednokrotnie już decydowała się podzielić swoją wiedzą i doświadczeniem z zakresu nadzoru z wykorzystaniem HDTV. Zainicjowała m.in. wiele warsztatów propagujących zalety technologii HDTV. Jedno z takich spotkań odbyło się w listopadzie w hotelu Intercontinental w Warszawie. Wprowadziliśmy uczestników w świat HDTV, przekonując do korzystania z niezawodnych i najbardziej zaawansowanych technologicznie produktów. Warsztaty były skierowane do dystrybutorów, instalatorów, integratorów oraz użytkowników systemów nadzoru wizyjnego.

AXIS P3346-VE

Dodatkowe informacje na temat rozwiązań Axis Communications wykorzystujących HDTV można znaleźć na stronie www.axis.com/pl.

Agata Majkucińska
Key Account Manager
Axis Communications

STAM-IRS

system monitoringu z wbudowanym mikro serwerem

STAM-IRS jest wszechstronnym rozwiązaniem przeznaczonym dla stacji monitorujących.

Stanowi on połączenie modularnego odbiornika obsługującego monitoring telefoniczny, TCP/IP, GPRS oraz GSM z niezawodnym mikro serwerem pozwalającym na pracę wielostanowiskową. Niezawodność rozwiązania gwarantuje sprawdzony system STAM-2 oraz system automatycznych kopii zapasowych – wszystko po to aby zagwarantować ciągłość pracy w odpowiedzialnym zadaniu monitorowania obiektów.

Nowość

20 1990 2010 | Satel

ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (58) 320 94 00, fax: (58) 320 94 01
e-mail: satel@satel.pl, www.satel.pl

AutoDome Junior HD
Wizja doskonała

Bosch Security Systems

Wzrok jest bardzo surowym jurorem w wielu dziedzinach naszego życia. Aby obraz obiektu obserwowany przez operatora systemu monitoringu spełnił kryteria jakościowe, musi ujmować jak największą liczbę szczegółów przy możliwie najlepszym odwzorowaniu palety kolorów. Dotychczasowa norma PN/EN 50132-7 określa warunki konieczne do spełnienia w przypadku identyfikacji osób. Minimalna rozdzielczość 400 TVL już raczej nikogo nie zachwyca, dlatego projektanci systemów skłaniają się ku rozwiązaniom dającym większe możliwości, a tym samym zapewniającym większą szczegółowość. Aby poradzić sobie z problemem szczegółowości w dotychczasowych systemach monitorowania wizyjnego wykorzystujących kamery o rozdzielczości 4CIF/D1 zwiększano liczbę punktów kamerowych lub wprowadzano dodatkowo kamery PTZ, jednak ze względu na liczbę urządzeń takie systemy wymagają większych nakładów inwestycyjnych

Potrzeba uzyskiwania coraz lepszej jakości przyczyniła się do powstania rozwiązań *High Definition*. Pierwsze kamery pracujące w tym standardzie nie oferowały niestety idealnej czułości, a obraz dynamiczny miał dodatkowe „efekty specjalne" w postaci smużenia. Stopniowy rozwój pozwolił jednak na zminimalizowanie niepożądanych efektów oraz przyczynił się do powstania nowej linii produktów HD firmy Bosch.

Pierwszym reprezentantem tej rodziny jest kamera AutoDome Junior HD. Z uwagi na zastosowany przetwornik CMOS o wielkości 1/2.5 ze skanowaniem progresywnym kamera odznacza się czułością dwóch luksów w trybie dziennym (50IRE). Dlaczego nie zastosowano CCD? Owszem, taka technologia jest dobra dla przetworników o rozmiarze do dwóch megapikseli. Powyżej tej wartości zarówno dynamika, jak i czułość jest lepsza w przypadku zastosowania CMOS. Celowo skonfrontowano tutaj rozdzielczość HD oraz liczbę pikseli. W pierwszym przypadku chodzi bardziej o określenie standardu i korzystanie ze zdefiniowanych rozdzielczości 720P oraz 1080P. W drugim przypadku rozdzielczość wyrażona liczbą pikseli jest głównie określeniem maksymalnej liczby punktów światłoczułych, które będą odpowiedzialne za generowany strumień JPEG czy MPEG.

W każdym z omawianych przypadków niezbędna do transmisji obrazów szerokość pasma sieciowego jest znacznie większa niż w przypadku kamer o standardowej rozdzielczości. Dzięki zastosowaniu kompresji H.264 maksymalna wielkość strumienia danych wytwarzanego przez kamerę Junior HD nie przekracza 10 Mb/s, co w kategorii HD stanowi niezły wynik, jednak wymaga rozsądnego podejścia do problemu zapisu obrazów. W małych systemach, zawierających najwyżej kilkadziesiąt kamer dobrym rozwiązaniem jest zapis metodą iSCSI. Gdy kamer jest więcej, warto rozpatrzyć wariant z inteligentną platformą zapisu nowej serii DLA 1200/1400.

Stanowi ona połączenie technologii iSCSI oraz serwera zarządzającego zapisem w jednej maszynie. Taka platforma będzie umożliwiała zarządzanie systemem zawierającym maksymalnie 128 kamer, natomiast szczytowa prędkość przetwarzania danych będzie wynosić 200 Mb/s. W przypadku małych systemów liczących do 32 kamer doskonale sprawdzi się wersja 1200 wyposażona w cztery twarde dyski, każdy o pojemności 1 TB. Dla największych systemów przewidziano serię 1800, która umożliwia konfigurację woluminu RAID-5 złożonego z ośmiu dysków o pojemności 1 TB każdy. Oprogramowanie nie wymaga dodatkowej licencji i jest gotowe do wprowadzenia konfiguracji inicjalnej. Sam VRM, tak jak w dużych systemach, przydziela kamerom zdefiniowane wcześniej listy adresów zgrupowanych maksymalnie w 128 blokach, w których będzie prowadzony zapis.

Nowością jest zachowanie funkcji, która jest dobrze znana z dotychczasowych wersji Vidos NVR. Mowa oczywiście o ANR – *Automatic Network Replenishment*. Funkcja ta sprawdza się przede wszystkim w systemach o mieszanym zapisie. Jeśli na przykład system wykorzystuje oprogramowanie VRM, macierze iSCSI i jednocześnie kamery z serii NBC200 lub enkodery VideoJet-X40-H008, zapis jest prowadzony bezpośrednio na macierzy. Wbudowana w kamerę pamięć masowa pełni rolę bufora. W momencie braku komunikacji lokalny zapis podtrzymuje ciągłość archiwum. Po odzyskaniu łączności z systemem bazowym oprogramowanie VRM odbudowuje archiwum z nośnika wbudowanego w kamerę lub koder.

Poza danymi dotyczącymi treści obrazów archiwizacji podlegają też metadane pochodzące z mechanizmu VCA (*Video Content Analysis*). Do tej pory inteligentna analiza obrazu była zarezerwowana wyłącznie dla kamer o standardowej rozdzielczości, a rozwiązania HD musiały posiłkować się prostą detekcją ruchu. Kamera AutoDome Junior wyznacza nową klasę rozwiązań ze względu na implementację IVA. Ze względu na rozmiary analizowanej matrycy (1920×1080 pikseli) oraz konieczność detekcji obiektu, którego obraz ma minimalne rozmiary równe 5×5 pikseli zagadnienie mocno się komplikuje. Z pomocą przychodzą wszystkie filtry dotychczas znane z wersji 4.0 funkcjonującej w kamerach o standardowej rozdzielczości. Najciekawszym z nich jest oczywiście filtr służący do detekcji twarzy, równie ciekawym rozwiązaniem jest analiza *Flow Control*.

Dzięki platformie DLA wszystkie dane z uzyskane w wyniku analizy IVA mogą być wykorzystane w przeszukiwaniu archiwów *post factum*. Chodzi oczywiście o funkcję *Forensic Search*. Przykładowo, przeszukiwanie dwugodzinnego archiwum z użyciem podstawowej analizy ruchu może zabrać nawet kilkadziesiąt minut. Nawet w tak krótkim przedziale czasu może mieć miejsce kilka tysięcy zdarzeń, które trzeba zweryfikować. Tymczasem korzystając z *Forensic Search*, operator zadaje precyzyjne pytanie, a odpowiedź otrzymuje w kilkanaście sekund.

Jako interfejs operatora systemu doskonale spisze się oprogramowanie Bosch Video Client. Zapewnia ono nie tylko obsługę kamer HD, ale także pełny zakres rozwiązań dla urządzeń o standardowej rozdzielczości, takich jak kamery Dinion czy enkodery VideJet. Możliwy jest także dostęp do archiwum – niezależnie od tego, czy jest ono zarządzane przez oprogramowanie VRM, platformę DLA czy zostało utworzone na nośniku lokalnym. W dalszej kolejności zostanie wprowadzona obsługa rejestratorów z serii 400, 600, 700 oraz Bosch Recording Station.

Standard *High Definition* dosyć długo umacniał się na rynku, co zaowocowało powstaniem wielu mniej lub bardziej dopracowanych rozwiązań. Jedno jest pewne – czas skutecznych implementacji właśnie nabiera rozpędu. Dzięki pełnej zgodności z ONVIF i możliwości wykorzystania IVA kamera AutoDome Junior HD ma ugruntowaną pozycję w segmencie urządzeń o wysokiej rozdzielczości. Dzięki różnym dostępnym technologiom zapisu już teraz możliwe jest skomponowanie systemu monitoringu na miarę najnowszych wymogów rynku.

Bosch Security Systems

Projektowanie systemów monitoringu IP z firmą SPS

Architektura systemów IP
Elementy systemów IP
Struktura systemu zależnie od jego wielkości

S.P.S. Trading

Na rynku wydawniczym można spotkać wiele publikacji opisujących ogólne zasady projektowania systemów monitoringu wizyjnego oraz sieci niezbędnych do obsługi takich systemów, nie ma więc sensu wracać do tych informacji po raz kolejny. Dlatego też w cyklu artykułów, jakie ukażą się w kolejnych edycjach *Zabezpieczeń* omówione zostaną zagadnienia związane z projektowaniem sieciowych systemów monitoringu wizyjnego, bazujących na konkretnym sprzęcie oferowanym przez firmę S.P.S. Trading. Przyjęto założenie, że współczesne projekty będą realizowane wyłącznie w oparciu o technologię IP (z małymi wyjątkami, dotyczącymi przypadków modernizacji istniejących systemów analogowych, co nie zmienia ogólności dalszych rozważań)

Fot. 1. Centrum zarządzania SeeTec

Tytułem wstępu opisana zostanie architektura typowych, sieciowych systemów monitoringu wizyjnego, w ramach której można wyróżnić dwie zasadnicze grupy urządzeń:

– urządzenia wizyjne, takie jak kamery, rejestratory, serwery, stacje robocze wraz z wyposażeniem niezbędnym do prawidłowego działania tych urządzeń;
– urządzenia stanowiące infrastrukturę sieciową, takie jak przełączniki sieciowe, ewentualnie routery, a także okablowanie niezbędne do połączenia poszczególnych składników systemu.

Kierując się tak przyjętymi kryteriami, urządzenia wizyjne należy podzielić na sieciowe, czyli nadające się do bezpośredniego podłączenia do sieci IP, oraz tradycyjne, nie posiadające interfejsów sieciowych, wymagające zastosowania koderów lub innych urządzeń pośredniczących, łączących je z siecią IP. Wszystkie te urządzenia można znaleźć w ofercie firmy S.P.S. Trading, wraz z rzetelną pomocą przy projektowaniu oraz doborze sprzętu.

Najbardziej wyeksponowaną grupą urządzeń wchodzących w skład sieciowych systemów monitoringu wizyjnego są kamery, zarówno analogowe, jak i sieciowe. W ofercie firmy S.P.S. Trading są one licznie reprezentowane, poczynając od najprostszych modeli stacjonarnych o rozdzielczości SD (PAL), a kończąc na kamerach szybkoobrotowych o rozdzielczości HD. Asortyment tych wyrobów jest na tyle szeroki, że w przeciętnych warunkach nie zachodzi konieczność posługiwania się kamerami pochodzącymi od innych dostawców (choć nie należy tego wykluczać).

W praktyce projektowej często dochodzi do sytuacji, w której konieczna jest rozbudowa istniejącego systemu monitoringu wizyjnego, a ten z natury rzeczy nie zawsze jest zbudowany w zgodzie z najnowszymi trendami. Często jest to system analogowy, wykorzystujący starego typu kamery wytwarzające zespolony sygnał wizyjny w standardzie PAL. W takim przypadku z pomocą śpieszą sieciowe kodery wizyjne, zwane też serwerami wizyjnymi – przekształcają one zespolony sygnał wizyjny na postać strumienia danych cyfrowych, które mogą być transmitowane przez sieć IP.

W systemach analogowych zainstalowanych wiele lat temu, a pracujących do chwili obecnej można jeszcze spotkać rejestratory cyfrowe z wejściami analogowymi wyposażone w interfejs sieciowy, stanowiące przykład tradycyjnych rozwiązań technicznych. Co prawda są to urządzenia przystosowane do pracy w sieci, jednakże ich funkcje sieciowe ograniczają się do podglądu obrazów z kamer i do odtwarzania nagrań archiwalnych. W ramach modernizacji systemu urządzenia tego typu mogą być wyeliminowane i zastąpione koderami wizyjnymi, zapewniającymi sieciowy dostęp do każdej z kamer z osobna. Wszystkie elementy niezbędne do realizacji takich zamierzeń są dostępne w ofercie firmy S.P.S. Trading.

Współczesne systemy monitoringu wizyjnego bazują na megapikselowych kamerach sieciowych oraz cyfrowych serwerach rejestrujących o nowoczesnej konstrukcji, w których w ogóle nie występują analogowe sygnały wizyjne. Wspomniane serwery rejestrujące mogą mieć postać samodzielnych, zamkniętych urządzeń lub komputerów z odpowiednim oprogramowaniem. W większości przypadków pełnią one także funkcje pomocnicze, na przykład pozwalają na sterowanie ruchem kamer sieciowych PTZ, realizują funkcje alarmowe etc. Przeważnie są to urządzenia bezobsługowe, zainstalowane w metalowej szafie umieszczonej w serwerowni lub innym dobrze chronionym pomieszczeniu technicznym (choć zdarzają się wyjątki od tej reguły).

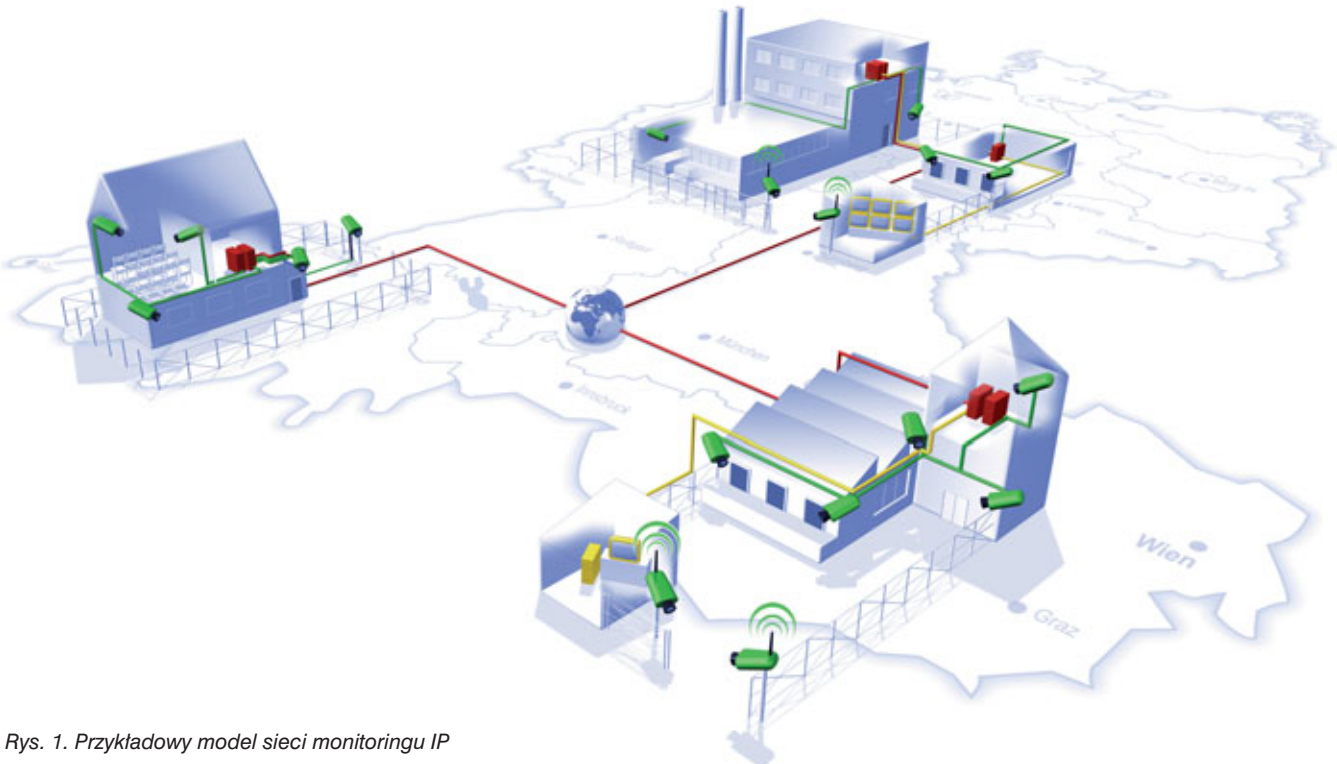
Współczesne systemy monitoringu wizyjnego są obsługiwane za pośrednictwem tak zwanych stacji roboczych. Są to komputery z odpowiednim oprogramowaniem klienckim, wyposażone w karty graficzne pozwalające na podłączenie kilku monitorów, na których wyświetlane są obrazy z kamer. Stacje robocze pozwalają na realizację funkcji sterujących i administracyjnych, tak więc potwierdza się fakt, że w nowoczesnych systemach monitoringu wizyjnego bezpośredni dostęp do rejestratorów lub serwerów systemowych jest zbędny – obsługiwane są poprzez sieć, za pośrednictwem stacji roboczych.

Przykładowym oprogramowaniem, które może być wykorzystane do budowy sieciowego systemu monitoringu, jest pakiet SeeTec, dostępny w ofercie firmy S.P.S. Trading. Jest to nowoczesne, wielofunkcyjne oprogramowanie, którego opisowi zostanie poświęcony oddzielny artykuł; obecnie ograniczmy się jedynie do zasygnalizowania jego istnienia.

Urządzenia należące do drugiej z wymienionych kategorii – czyli przełączniki i ewentualnie routery – stanowiące infrastrukturę sieciową systemu, są urządzeniami uniwersalnymi, nie związanymi ściśle z systemami monitoringu wizyjnego. Ze względów ekonomicznych mogą one stanowić fragment większych sieci realizujących inne zadania, takich jak sieci biurowe czy korporacyjne. Jednak dobrą praktyką jest rozdzielanie funkcji biurowych i funkcji związanych z monitoringiem na oddzielne instalacje.

Przełączniki sieciowe służą do podłączania wielu urządzeń do tej samej sieci IP, pełnią więc rolę inteligentnych rozgałęziaczy, eliminujących kolizje między urządzeniami, które chciałyby jednocześnie skorzystać z dostępu do sieci. Routery sieciowe służą do rozdzielania dużych sieci na mniejsze podsieci, ułatwiając tym samym administrowanie bardzo rozległymi instalacjami. Opis działania tych urządzeń wykracza poza ramy tej publikacji, warto jednak zdawać sobie sprawę z pełnionych przez nie funkcji.

Należy również wspomnieć o bardzo ważnym elemencie składowym każdej sieci IP, jakim jest jej okablowanie. Budowa okablowania jest zależna od wielu czynników, między innymi od wymagań dotyczących przepływności i fizycznej długości poszczególnych odcinków sieci. Przykładowo, na bazie okablowania strukturalnego, dostępnego w większości współczesnych budynków biurowych, możliwa jest budowa sieci określanej jako Fast Ethernet, w której przepływność jest ograniczona do 100 Mb/s, zaś długość poszczególnych odcinków nie może przekraczać 100 m. W rozległych obiektach, takich jak stadiony czy lotniska, konieczne jest stosowanie kabli światłowodowych, nie wykazujących tak drastycznych ograniczeń. Przykładowo, sieć określana jako Gigabit Ethernet zbudowana w oparciu o najtańszy światłowód wielomodowy zapewnia transmisję z przepływnością 1 Gb/s na odcinkach o długości nie przekraczającej 550 m, natomiast użycie światłowodu jednomodowego pozwala na transmisję na odległość rzędu 10 km.



Rys. 1. Przykładowy model sieci monitoringu IP

Jak widać, rodzaj zastosowanego okablowania oraz typ połączenia jest zależny od rozległości sieci oraz od wymagań dotyczących jej przepływności. Należy nadmienić, że w sieciach rozległych często wykorzystywany jest rodzaj rdzenia, czyli części centralnej, która może mieć różną budowę w zależności od lokalnych warunków instalacyjnych.

Problemem, na jaki należy zwrócić szczególną uwagę, jest odległość. Poszczególne urządzenia sieciowe są rozmieszczone w sposób wynikający z pełnionych przez nie funkcji. Zadaniem instalacji kablowej jest połączenie tych urządzeń z siecią IP. Trudno wyobrazić sobie sytuację, w której rozmieszczenie kamer dobiera się pod kątem dostępności połączeń sieciowych. W praktyce jest odwrotnie, to znaczy budowę sieci trzeba dostosować do rozmieszczenia kamer.

Należy pamiętać, że kamery oraz inne urządzenia krańcowe, rozrzucone po obiekcie zgodnie z zamysłem funkcjonalnym, są w większości przypadków wyposażone w interfejsy Fast Ethernet. Oznacza to, że długość pojedynczych odcinków kablowych prowadzących do tych urządzeń nie może przekraczać 100 m. Jest to jeden z istotniejszych problemów, nad którymi musi się zastanowić projektant. W sieci tworzone są punkty węzłowe, do których zbiegają się kable kategorii piątej lub szóstej, stanowiące warstwę fizyczną instalacji Fast Ethernet. Połączenia między tymi punktami stanowią właśnie wspomnianą wyżej część rdzeniową sieci i są wykonywane w innej technologii, pozwalającej na pokonanie większych odległości oraz zapewniającej znacznie wyższą przepływność niż typowy Fast Ethernet.

Do czego jest potrzebna wysoka przepływność części rdzeniowej sieci? Odejdźmy na chwilę od tematu i zastanówmy się nad budową typowej sieci komputerowej w biurze lub w domu.

Fot. 2. Panel tylny kamery sieciowej Sanyo VCC-HD2500P

Fot. 3. Kamera szybkoobrotowa 2Mpx Sanyo VCC-HD5400P

Mamy tam do czynienia z urządzeniami, które w długich przedziałach czasowych nie stwarzają dużego obciążenia dla sieci IP. Z koniecznością szybkiej transmisji danych spotykamy się sporadycznie, na przykład w momencie wydruku wielu stron tekstu na drukarce sieciowej lub podczas przeglądania plików graficznych pobieranych z Internetu. W systemach monitoringu wizyjnego sytuacja wygląda zupełnie inaczej. Obciążenie sieci IP jest duże i utrzymuje się w sposób ciągły. Strumienie danych wytwarzane przez poszczególne kamery dochodzą do punktów węzłowych, a tam podlegają kumulacji, tworząc zwielokrotniony strumień danych, którego dalsza transmisja wymaga użycia sieci o znacznie większej przepływności.

Z tego względu część rdzeniową sieci traktuje się jako wydzielony fragment instalacji, wymagający szczególnego potraktowania. Istnieje wiele różnych topologii części rdzeniowych sieci IP, jednakże w przypadku projektowania systemów monitoringu wizyjnego dominują dwie z nich: gwiaździsta i pierścieniowa.

Jak sama nazwa wskazuje, pierwsza z nich przypomina gwiazdę, z ramionami rozchodzącymi się promieniście od jednostki centralnej do punktów węzłowych. Odcinki sieci tworzące ramiona gwiazdy są przeważnie budowane na bazie kabli światłowodowych i dysponują przepływnością co najmniej 1 Gb/s. W punkcie centralnym, którym może być specjalistyczny, zbiorczy przełącznik sieciowy lub serwer systemowy, następuje dalsza kumulacja strumieni danych, co wiąże się z koniecznością zastosowania technologii o przepływności co najmniej dziesięciu gigabitów na sekundę.

Część rdzeniowa sieci o topologii pierścieniowej ma inną budowę. Poszczególne punkty węzłowe sieci są połączone kolejno, każdy z dwoma sąsiednimi, tworząc zamknięty pierścień. Skumulowane strumienie danych, przychodzących do punktów węzłowych z kamer i innych urządzeń krańcowych, są przekazywane do części rdzeniowej, a stamtąd kierowane do kolejnych punktów węzłowych, by w końcu dotrzeć do jednostki centralnej, także włączonej w ten pierścień. Podobnie jak poprzednio, jednostką centralną może być specjalistyczny, zbiorczy przełącznik sieciowy lub serwer systemowy. Bardzo istotną zaletą topologii pierścieniowej jest jej nadmiarowość, zwana także redundancją. Dane mogą być transmitowane w obrębie pierścienia w dowolnym kierunku, co oznacza, że przerwanie któregoś z odcinków kabla nie powoduje przerwy w transmisji danych.

Jest to dość typowe podejście do tematu, gdyż z punktu widzenia projektanta systemu monitoringu wizyjnego fizyczna realizacja części rdzeniowej sieci może być dowolna, pod warunkiem że spełnia wymagania dotyczące przepływności oraz rozległości sieci. Przeważnie projektowaniem tego fragmentu instalacji zajmują się specjaliści od zagadnień sieciowych, dzięki czemu projektant systemu monitoringu może się skupić na zagadnieniach związanych ze sprzętem wizyjnym.

W kolejnych publikacjach z tej serii opisane będą poszczególne składniki wykorzystywane do budowy sieciowych systemów monitoringu bazujących na konkretnym sprzęcie, oferowanym przez firmę S.P.S. Trading.

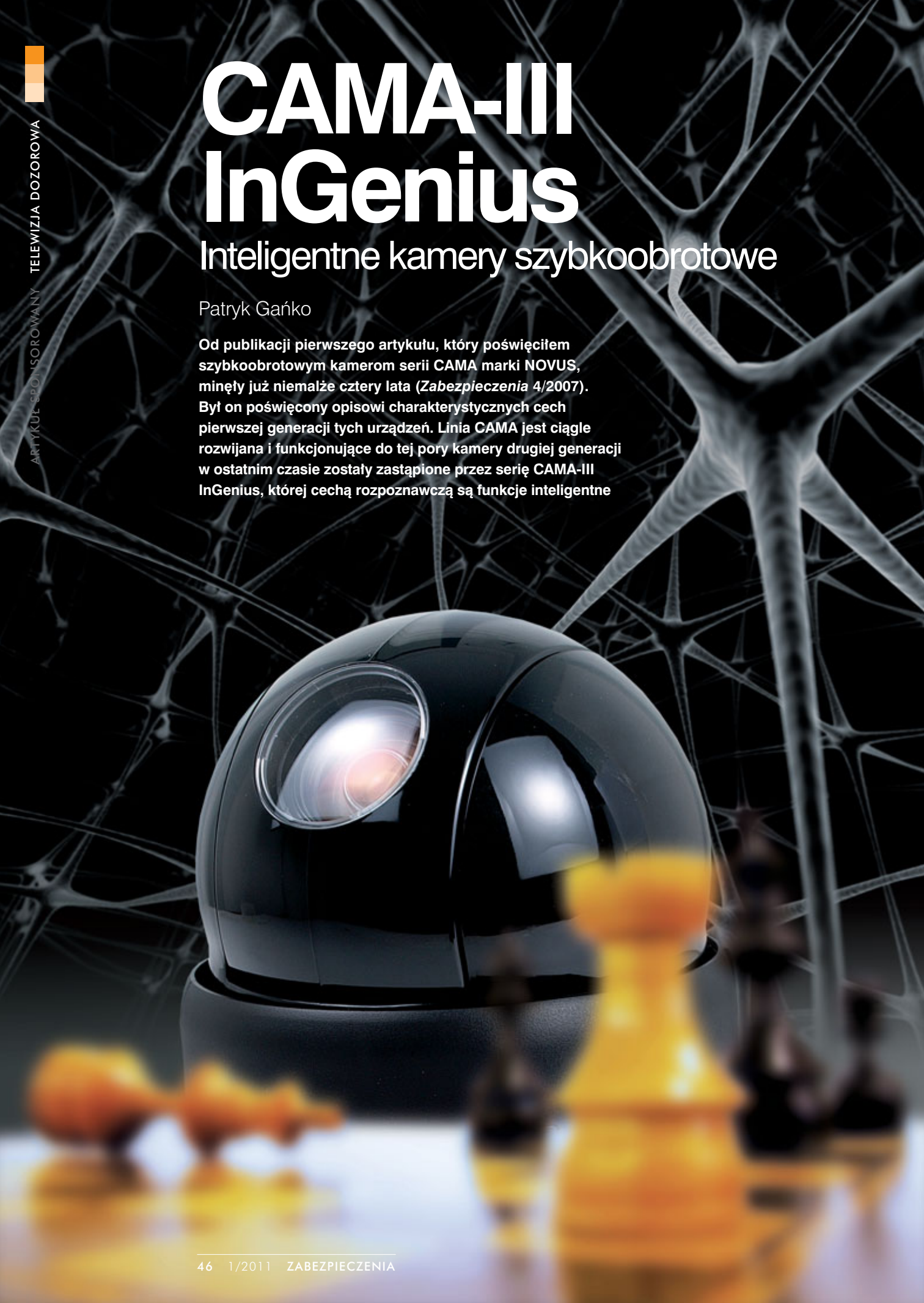
Opracowanie: S.P.S. Trading

CAMA-III InGenius

Inteligentne kamery szybkoobrotowe

Patryk Gańko

Od publikacji pierwszego artykułu, który poświęciłem szybkoobrotowym kamerom serii CAMA marki NOVUS, minęły już niemalże cztery lata (*Zabezpieczenia* 4/2007). Był on poświęcony opisowi charakterystycznych cech pierwszej generacji tych urządzeń. Linia CAMA jest ciągle rozwijana i funkcjonujące do tej pory kamery drugiej generacji w ostatnim czasie zostały zastąpione przez serię CAMA-III InGenius, której cechą rozpoznawczą są funkcje inteligentne



Fot. 1. Kamera serii CAMA-III InGenius

Bardzo ważną zaletą wszystkich kamer CAMA oraz powiązanych z nimi akcesoriów jest ich pełna kompatybilność z poprzednimi generacjami tych urządzeń. Ułatwia to rozbudowę już istniejących systemów monitoringu wizyjnego oraz ich konserwację. Konstrukcja kamery, stosowane typy złącz oraz konstrukcja podstawy instalowanej w obudowie nie uległy zmianie od czasu wprowadzenia pierwszej serii kamer CAMA-I.

W niniejszym artykule chciałbym zaprezentować nowatorskie rozwiązania zastosowane w kamerach serii CAMA-III InGenius oraz pokrótce scharakteryzować szybkoobrotową kamerę z serii CAMA-III mini. Jak mówi znane chińskie przysłowie, jeden obraz wart więcej niż tysiąc słów, co szczególnie odnosi się do będących wzrokowcami mężczyzn, którzy dominują w branży technicznych systemów zabezpieczeń. Dlatego przy opisie poszczególnych funkcji kamer zamieszczę także adresy internetowe, pod którymi będzie można pobrać zarejestrowane strumienie wizyjne uzyskane z wykorzystaniem omawianych funkcji.

Do serii kamer szybkoobrotowych CAMA-III InGenius należą dwa modele – NVC-ISD322DN oraz NVC-ISD336DN z przetwornikiem CCD 1/4" SONY ExView HAD. Powyższe modele wyglądają identycznie i mają te same funkcje. Różnią się jedynie zastosowanym modułem kamerowym, a co za tym idzie długością ogniskowej (do 85,8 mm w NVC-ISD322DN i 122,4 mm w NVC-ISD336DN) oraz ustawieniami automatyki ekspozycji.

GUI

Menu kamery, podobnie jak w rejestratorach, ma charakter graficzny. Zrezygnowano z dotychczas stosowanego menu literowego ze względu na złożoność konfiguracji. Dzięki temu, mimo obecności wielu dodatkowych funkcji oraz rozbudowanego menu, w sposób intuicyjny i szybki można dokonać konfiguracji kamery. Menu kamery jest wielojęzyczne i obejmuje również języki niełacińskie, np. rosyjski.

Harmonogram

Kolejną funkcją spotykaną w rejestratorach wizyjnych i zastosowaną w tych kamerach jest harmonogram działania. Pozwala on na zaprogramowanie do 80 zadań dla kamery, takich jak presety, trasy obserwacji, patrole, automatyczne skanowania, automatyczny obrót dookolny oraz kalibracja w dokładnie zdefiniowanych dniach i godzinach. Wdrożenie harmonogramu było możliwe ze względu na zegar czasu rzeczywistego wbudowany w kamerę. Dzięki temu znacznie wzrosła funkcjonalność kamery, która w określonych przedziałach czasowych może skupiać swoją aktywność na różnych obszarach, np. w godzinach pracy może monitorować parking, a w godzinach nocnych drzwi wejściowe i elewację budynku.

Autokalibracja

Przy długotrwałej pracy kamery z wykorzystaniem jednej z funkcji automatycznej obserwacji może nastąpić przesunięcie położenia kamery względem punktu odniesienia. Wówczas potrafi ona wykryć przesunięcie położenia modułu kamerowego i automatycznie dokonać jego korekty.

Automatyczna ekspozycja dla presetu

Funkcja pozwala na konfigurację ustawień automatyki ekspozycji indywidualnie dla każdego presetu. Kamera obrotowa może monitorować duże obszary, które mogą znacznie różnić się poziomem oświetlenia oraz jego charakterem (źródła punktowe, nierównomierne oświetlenie sceny, oświetlenie padające bezpośrednio w obiektyw kamery). Aby generowany obraz był zawsze najwyższej jakości, dla tych obszarów można indywidualnie zdefiniować m.in. następujące parametry: zwolniona migawka, AGC, jasność, tryb dzień/noc, WDR.

Rejestr zdarzeń

Kamera może zapamiętać do 256 zdarzeń. W przypadku przekroczenia tej liczby najstarsze wpisy będą automatycznie kasowane i zastępowane nowymi. Lista zdarzeń zapisywanych w pamięci obejmuje: alarmy, rozruch (ponowne uruchomienie kamery), ruch (detekcja ruchu), śledzenie (automatyczne śledzenie obiektu), przekraczanie linii, wejście (w zdefiniowaną strefę) oraz porzucenie i zniknięcie.

Inteligentne funkcje

Inteligentne funkcje kamery zostały przyporządkowane do presetów i uaktywniają się po ich wywołaniu. Do każdego presetu może być przyporządkowana jedna funkcja. Funkcje te uaktywniają się również w trybie patrolu, tzn. kiedy kamera przechodzi między kolejnymi presetami. Wszystkie alarmy wykryte przez inteligentne funkcje, w tym również funkcję detekcji ruchu, zapisywane są w rejestrze zdarzeń kamery.

Detekcja ruchu

Po wykryciu ruchu w określonym obszarze i uprzednim zdefiniowaniu siatki detekcji czułości oraz minimalnego i maksymalnego rozmiaru obiektu kamera może aktywować wybrane wyjście przekaźnikowe na określony czas lub wyświetlić ikonę alarmu na tle obrazu. Ponadto w menu można wybrać opcję otaczania wykrytych obiektów ramką oraz rysowania śladu trasy, którą się poruszały. Działanie funkcji detekcji ruchu unaocznia film znajdujący się pod adresem *www.novuscctv.pl/webfm_send/2616*.

Śledzenie

Funkcja śledzenia pozwala na samoczynne obracanie się kamery oraz ewentualne wykonywanie zbliżenia poruszających się obiektów. Poprawia to rozpoznawalność szczegółów, ale również zwiększa prawdopodobieństwo „zgubienia" obiektu, szczególnie jeżeli porusza się on ze znaczną prędkością. Dlatego zbliżenia należy stosować przede wszystkim w przypadku wolno poruszających się obiektów, np. podczas obserwacji osób przemieszczających się pieszo. W przypadku wyjścia obiektu poza obszar możliwej obserwacji kamery lub zdefiniowane uprzednio krańce (prawy, lewy, górny, dolny) po krótkim czasie oczekiwania kamera samoczynnie powróci do punktu początkowego w oczekiwaniu na kolejny obiekt.

Powyższe przypadki i wykorzystanie w nich funkcji śledzenia doskonale pokazują zarejestrowane filmy, które można znaleźć na naszej stronie internetowej (*www.novuscctv.pl/webfm_send/2615*).

W przypadku obserwacji dwóch obiektów poruszających się w przeciwnym kierunku kamera podąży za obiektem dominującym, który wnosi więcej zmian do treści obrazu. Niekoniecznie będzie to obiekt większy, gdyż na przykład jego kolor może zlewać się z kolorem tła.

Fot. 2. Kamery serii CAMA-III mini

Przekroczenie linii

W celu ochrony wybranej strefy w obserwowanej scenie można zdefiniować linię prostą, rozciągniętą między dwoma dowolnymi punktami, której przekroczenie może skutkować podjęciem akcji alarmowej – wyświetleniem ikony alarmu na tle obrazu, włączeniem wybranego wyjścia przekaźnikowego na określony czas lub – co najważniejsze – uaktywnieniem automatycznego śledzenia obiektów. Oczywiście kierunek przekroczenia linii można dowolnie zdefiniować. Wszystkie alarmy wykryte dzięki funkcji przekroczenia linii zapisywane są w rejestrze zdarzeń kamery. Działanie funkcji w rzeczywistości można obejrzeć na zarejestrowanym filmie znajdującym się pod adresem *www.novuscctv.pl/webfm_send/2618*.

Wejście obiektu do określonej strefy

W obserwowanym obrazie możemy zdefiniować obszar w kształcie prostokąta, którego naruszenie może wywołać akcję alarmową. Jest to funkcja szczególnie przydatna w monitorowaniu ruchu w istotnych dla nas miejscach. W materiale filmowym znajdującym się pod adresem *www.novuscctv.pl/webfm_send/2614* pokazano ochronę wybranej strefy parkingu za pomocą tejże funkcji.

Porzucenie obiektu i zniknięcie obiektu

Działanie obu funkcji jest podobne. Po zdefiniowaniu strefy dozorowej kamera zapamiętuje ją, a następnie – w momencie zniknięcia lub pojawienia się jakiegoś obiektu – rozpoczyna proces alarmowania. Warto przy tym zwrócić uwagę na to, że przysłonięcie obiektu (nawet długotrwałe) nie powoduje zadziałania funkcji. Doskonale ilustruje to zarejestrowany film (*www.novuscctv.pl/webfm_send/2617*).

W celu ułatwienia operowania kamerami z poziomu różnych sterowników (klawiatur, programów komputerowych) bezpośrednio z menu można wywołać wszystkie funkcje automatyzacji obserwacji, a ponadto aktywować wyjścia przekaźnikowe. Jest to przydatne, ponieważ protokoły zaimplementowane w różnych klawiaturach są często niekompletne. Oczywiście najnowsze kamery wyposażono w funkcję parkowania, podobnie jak kamery poprzednich serii. Po upływie ustalonego czasu braku aktywności operatora kamera samoczynnie przystępuje do realizacji zaprogramowanej funkcji (preset, patrol, trasa automatycznego skanowania lub trasa obserwacji). Czas, po którym następuje aktywacja wybranej funkcji, może być zmieniany w przedziale od 10 do 240 sekund. Dostęp do ustawień kamery jest zabezpieczony sześciocyfrowym hasłem.

Również kamery szybkoobrotowe serii CAMA-III mini zostały wyposażone w nowe funkcje, charakterystyczne dla kamer szybkoobrotowych w wersji pełnowymiarowej.

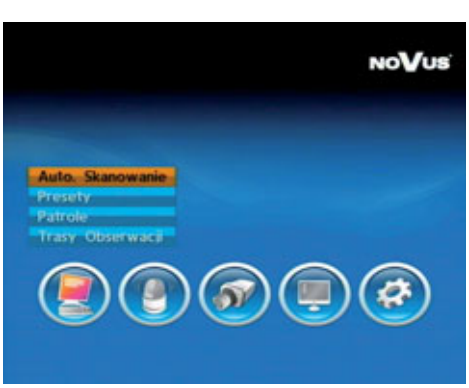
Główną zaletą kamer serii CAMA-III mini jest połączenie cech i funkcji typowych dla zaawansowanych kamer szybkoobrotowych z obudową o niewielkich rozmiarach. Zainstalowana kamera swoim wyglądem nie odróżnia się od typowych kamer kopułkowych, a dodatkowo umożliwia monitorowanie całej otaczającej przestrzeni, duże przybliżenia i obserwację znacznie oddalonych obiektów (identyczny moduł kamerowy jak w modelu NVC-ISD322DN).

Kamera występuje w dwóch wersjach – wewnętrznej oraz zewnętrznej w dodatkowej obudowie z kloszem przeciwsłonecznym i grzałką, co umożliwia pracę w temperaturze do -30°C. Oba modele są wandaloodporne i należą do klasy szczelności IP66, czyli są zabezpieczone przed wnikaniem wilgoci oraz pyłu. Kamery mogą być montowane na ścianie, suficie (również na suficie podwieszanym), maszcie lub w narożniku budynku za pomocą opcjonalnych uchwytów i adapterów.

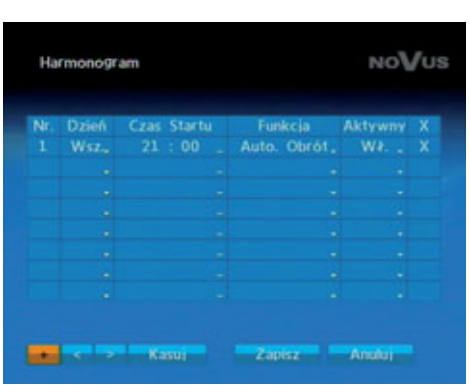
Wydaje się, że znaczenie inteligentnych funkcji w kamerach szybkoobrotowych będzie szybko wzrastać. Trzeba pamiętać, że nie gwarantują one zarejestrowania krytycznych zdarzeń w obrębie danego pola widzenia, ale dzięki nim jest ono znacznie bardziej prawdopodobne. Rozwój funkcji inteligentnych będzie postępował. Już trwają prace nad tworzeniem algorytmów automatycznego wykrywania zdarzeń, takich jak bójka lub uliczne zgromadzenie. W przyszłości, przy rosnącym nasyceniu kamerami, funkcje inteligentne będą powszechnie stosowane i znacznie zwiększą skuteczność pracy operatorów.

Wszystkie filmy, o których wspomniano w artykule, są dostępne na stronie internetowej *www.novuscctv.pl* w zakładce *Marketing/Prezentacje*.

Patryk Gańko
AAT Holding



Fot. 3. Graficzne menu kamer serii CAMA-III InGenius



Fot. 4. Harmonogram działania serii CAMA-III InGenius

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Inteligentne kamery PTZ o wysoce zaawansowanych funkcjach analizy obrazu!

Automatyczne śledzenie obiektów (Auto Tracking)
Pozwala na automatyczne śledzenie przemieszczającego się obiektu, np. osoby lub pojazdu w obrębie monitorowanego obszaru. Funkcja ta jest szczególnie przydatna w bezobsługowym systemie monitoringu wizyjnego, gdy pojawienie się osoby lub pojazdu wymaga szczególnej uwagi.

Wykrywanie przekroczenia określonej linii przez obiekt
Na obrazie z kamery zostaje określona linia „bezpieczeństwa", np. płot, brama, ogrodzenie, przejście służbowe. Naruszenie tej linii przez obiekt (np. osobę, zwierzę, pojazd) wywołuje uprzednio zdefiniowaną akcję, np. rozpoczęcie śledzenia obiektu czy aktywację wybranego wyjścia przekaźnikowego na określony czas.

Wykrywanie pojawienia się/zniknięcia obiektu
Kamera wykrywa pozostawione lub usunięte obiekty z obserwowanej sceny. Analizując obraz, porównuje go z obrazem referencyjnym i uruchamia alarm w momencie zniknięcia lub pojawienia się obiektu. Chwilowe przesłonięcie obiektu nie aktywuje tej funkcji.

NOVUS 3 teraz lata gwarancji

CAMA-III seria

INGENIUS

- Dodatkowe funkcje analizy obrazu: detekcja ruchu, wykrywanie wkroczenia obiektu do określonej strefy
- Mechaniczny filtr podczerwieni
- Rozdzielczość pozioma do 620 TVL
- Czułość: od 0.0008 lx/F=1.6 (DSS)
- WDR - Szeroki zakres dynamiki
- DSS - Wydłużony czas ekspozycji
- DIS - Cyfrowa stabilizacja obrazu
- Zoom optyczny do 36x
- 8 patroli, 17 tras automatycznego skanowania, 8 tras obserwacji (do 500 s), 240 presetów, 8 stref prywatności

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

Co z tym XXI wiekiem?

Grzegorz Ćwiek

„Przed dwudziestu laty podróż z Europy do Stanów Zjednoczonych trwała siedem godzin; kosztem osiemnastu miliardów dolarów skrócono ten czas do pięćdziesięciu minut. Wiadomo już, że dzięki dalszym miliardom ten czas lotu uda się skrócić o połowę. Pasażer, wysterylizowany na ciele i umyśle (żeby nie zawlókł do nas ani azjatyckiej grypy, ani azjatyckich myśli), naładowany witaminami i widowiskiem filmowym z puszki, będzie mógł przenosić się z miasta do miasta, z kontynentu na kontynent, z planety na planetę – coraz pewniej i szybciej, a wizja takiej fenomenalnej sprawności instrumentów opiekuńczych ma zatkać nam usta, byśmy nie zdołali spytać, do czego właściwie te błyskawiczne peregrynacje służą”

Stanisław Lem, Głos Pana (1968)

Mija właśnie dziesięć lat od czasu, kiedy weszliśmy dumnie w XXI wiek. Pamiętacie Państwo, jakie wizje milenium mieliśmy wszyscy w połowie lat dziewięćdziesiątych? A jakie obrazy kuli ziemskiej i życia w latach z „dwójką" na początku mieli reżyserzy filmów nakręconych w latach osiemdziesiątych lub siedemdziesiątych ubiegłego stulecia? Mieliśmy już latać, a nie jeździć, mieliśmy przenikać zamiast przechodzić i teleportować przedmioty w ułamku sekundy zamiast przesyłać pocztą.

Mimo że tak się na razie nie dzieje, a przynajmniej nie w takim stopniu, o jakim marzyli Lem, Spielberg czy Clark, to jesteśmy coraz bliżej całkowitej zmiany zachowań i przyzwyczajeń, właśnie dzięki najnowszej technologii i wynalazkom ostatnich dwudziestu – trzydziestu lat. Chociaż powyższy cytat z powieści Stanisława Lema mógłby odnosić się do czasów przyszłych (dziś jeszcze nie przemieszczamy się z Europy do Ameryki w kilkadziesiąt minut), widzimy, że właściwie od zawsze człowiek snuł bardziej lub mniej prawdopodobne wizje tego, co miałoby go czekać w przyszłości. I co ciekawe, jeśli przyjrzymy się ewolucji, lub nawet rewolucji technicznej nieco bliżej, to okaże się, że zwykle największą przeszkodą dla ludzi w realnym przemieszczeniu się z jednej epoki technologicznej do drugiej były pieniądze. To fakt – wiele z wynalazków to pieniądze zmarnowane lub wydane (wydawałoby się) bez większego sensu, ale większość z nich właśnie generuje naprawdę duże zyski albo prowadzi do uzyskania sporych oszczędności. Czasem przedsiębiorstwa lub osoby prywatne wydają ogromne sumy na pomysły, z których nikt nie korzysta albo korzysta się w niewielkim stopniu. Zespoły marketingowe wielkich korporacji wydają miliardy dolarów rocznie, by przekonać się, dlaczego tak się dzieje. Ich celem jest zbadanie mechanizmu podejmowania decyzji konsumenta lub inwestora. Dlaczego jeden wynalazek się przyjmuje, a inny nie. Wyniki tych badań bywają zaskakujące. Pomijając tak przełomowe wynalazki, jak maszyna parowa, odkrycie właściwości i zastosowań krzemu lub wyprodukowanie pierwszej pralki, okazuje się, że w dużej części ludzie:

– uważają, że nie zawsze potrzebują najbardziej wyrafinowanych wynalazków lub pomysłów,
– nie chcą się uczyć czegoś nowego i wolą pozostać przy rozwiązaniach, które znają,
– z góry uznają, że nowe rozwiązania są na pewno drogie i nie warto ich stosować,
– nie chcą w ogóle wydawać pieniędzy na zmiany (z chęci oszczędzania),
– informacja o użyteczności nowego produktu do nich nie dotarła.

Niestety większość z tych obserwacji jest prawdziwa tylko w krótkim okresie, czyli na początku cyklu życia nowego produktu, pomysłu, wynalazku. Zupełnie inaczej jest w długim okresie: większość innowacji wchłanianych jest z czasem jak gąbka przez większość ludzi (oczywiście w różnym stopniu przez różne kultury, branże etc.). Odnieśmy się jednak do powyższych obserwacji na tle praktyki naszej branży (bezpieczeństwa pożarowego). Dla lepszego zrozumienia problematykę tę powinniśmy analizować w dwu płaszczyznach: technicznej i finansowej.

Z technicznego punktu widzenia: aby nowinki mogły zostać zaakceptowane, muszą być zauważone. W dobie powszechnego dostępu do informacji (Internet) tę sprawę można już coraz częściej pominąć. W przypadku dóbr konsumpcyjnych innowacje są dość trudne do zaakceptowania przez starszych nabywców, a zdecydowanie łatwiejsze do przyjęcia dla młodszych. Ta dość ogólna teza ma częściowe odzwierciedlenie w praktyce naszej branży (choć niezupełnie wśród specjalistów): w szkoleniach, seminariach, warsztatach udział biorą w zdecydowanej większości młodsi inżynierowie. Oni także częściej stosują w praktyce nowe technologie, wprowadzają więcej innowacji do swoich projektów i instalacji (nowoczesne detektory, elementy automatyki, sposoby instalacji, projektowania etc.). Ci starsi z kolei podchodzą do nowinek z większym sceptycyzmem, jakby nie do końca ufając prelegentom, i nieco częściej pozostają przy swoich przyzwyczajeniach lub preferencjach związanych bardziej z ludźmi (przedstawicielami firm) niż z samymi produktami. Efekt tego można także dostrzec w opracowaniach projektowych, gdzie mimo uczestnictwa w szkoleniach i kursach pewna (na szczęście niewielka) grupa bardziej doświadczonych specjalistów nadal wykorzystuje urządzenia i rozwiązania inżynierskie, które przyswoiła sobie kilkanaście lub nawet kilkadziesiąt lat temu. Trochę szkoda, bo oni przecież także kiedyś, czytając Lema czy Clarka, marzyli o lotach w kosmos i wczasach na księżycu lub o tym, by siedząc w zaciszu swego domu, móc np. nadzorować system bezpieczeństwa w innym mieście. Na szczęście, jak już wcześniej wspomniano, wśród starszych specjalistów przeważają tacy, którym siwizna nie przeszkadza w myśleniu innowacyjnym, w dążeniu do spełnienia marzeń, do bycia nowoczesnymi. Ich wielkie doświadczenie życiowe i zawodowe doskonale pozwala odseparować podawane im dzisiaj informacje ważne od nieważnych, rzetelne od nierzetelnych i informacje użyteczne od czczej „marketingowej gadaniny" prześcigających się w zdobyciu ich względów producentów. Choć myślących w ten sposób specjalistów jest niewielu, są to ludzie XXI wieku – w każdym tego słowa znaczeniu.

Ponadto na prawdziwe mentalne i praktyczne przejście w XXI wiek nie pozwala często zwykłe ludzkie lenistwo. To błąd, ponieważ nowoczesne technologie – szczególnie w branży bezpieczeństwa pożarowego – są niezbędne do spełnienia głównego celu wszystkich uczestników tego rynku, a mianowicie: zabezpieczenia ludzkiego zdrowia, życia i mienia – w jak najwyższym stopniu.

Aspekt finansowy z kolei to już poważniejsza sprawa. To także – jak śpiewał Eric Clapton w jednym z największych przebojów – „wielka iluzja" (*Grand Illusion*). Praktyka największych firm w branży wyraźnie pokazuje, że najnowsze technologie stosowane dzięki nowoczesnym wynalazkom, patentom i dużej skali produkcji wpływają nie na podwyższenie cen produktów, lecz na ich obniżenie, a więc na duże oszczędności finansowe. Przykładów w branży jest wiele, między innymi znana doskonale w Polsce i na świecie firma Schrack Seconet, której wysokiej klasy produkty były w połowie lat osiemdziesiątych i na początku dziewięćdziesiątych ubiegłego wieku znacznie, nawet kilkakrotnie, droższe od produktów konkurencyjnych. W ostatnich latach w celu obniżenia kosztów produkcji firma przeniosła zakłady produkcyjne z droższej pod tym względem Austrii do Niemiec (tak, nie do Chin) i dokonała kolejnych cięć cenowych, podnosząc przy tym jeszcze bardziej (sic!) jakość i użyteczność rozwiązań. Najnowszy system wykrywania pożaru Integral IP jest obecnie jednym z najlepiej sprzedających się systemów bezpieczeństwa na świecie! Nie do pomyślenia dwadzieścia lat temu było sprzedawanie najnowszych, interaktywnych czujek multisensorowych (wielokryteryjnych)

w cenie dostępnych powszechnie zwykłych czujek optycznych. Przykładów w branży można by przytaczać dziesiątki, co tylko potwierdza postawioną wyżej tezę, że każda innowacja jest akceptowana przez większą cześć rynku w długim okresie, a także nie oszczędza się pieniędzy na pozostawaniu mentalnie i praktycznie w ubiegłym stuleciu.

A co z chęcią zaoszczędzenia kilku złotych – *oby tylko nie wprowadzać zmian, bo to przecież kosztuje*? Wiek, którego pierwsza dekada właśnie zbliża się ku końcowi, to wiek gwałtownych zmian, częstszych niż w poprzednich latach nagłych i nieoczekiwanych zwrotów akcji i sytuacji rynkowych. To wiek, w którym, jak pisał wielki filozof austriacki Joseph Schumpeter, wieją wichry twórczej destrukcji. Aby była ona twórcza, nie można trzymać się kurczowo przyzwyczajeń z poprzedniej epoki i nie uwzględniać zmian otoczenia. Taniej jest dostosowywać się do nich od razu, bez zbędnej zwłoki. Zdecydowanie więcej oszczędzamy, wprowadzając innowację dziś, niż czekając na moment, w którym będzie ona niezbędna do dalszego funkcjonowania. Dzisiaj mamy wybór i możemy decydować o tym, co i za ile kupimy. Kiedy zmiana stanie się konieczna (np. przy kompletnej degradacji posiadanego systemu bezpieczeństwa po wielu latach jego eksploatacji), rzeczywiście kosztować będzie więcej, bo siła przetargowa kupującego znacząco się osłabi. Dostawca będzie dyktował cenę, trzymając nóż na gardle kupującego. Przykładów na to w naszej branży jest sporo. Dokładnie odwrotnie zachował się Schrack, który jako pierwsza firma w branży i na razie jedyna na rynku opracował specjalne pakiety serwisowe do swoich systemów, mające na celu uaktualnienie zarówno sprzętu, jak i oprogramowania (oferowanego dziesięć, a nawet dwadzieścia lat temu) do rozwiązań najnowszych, skrojonych na miarę XXI wieku. Już dzisiaj inwestorzy i instalatorzy mogą opracowywać plany modernizacji systemu sygnalizacji pożarowej, budżetując na to niewielkie sumy, i dzięki temu uzyskać możliwość znaczącego obniżenia kosztów jego eksploatacji w przyszłości[1]. Dzięki takim rozwiązaniom spadają koszty eksploatacji systemów, serwisu i obsługi pogwarancyjnej. Zmiana przynosi oszczędności, a nie dodatkowe koszty. Aby myśleć w ten sposób, trzeba natychmiast przenieść się w XXI wiek. Dźwigając na barkach odpowiedzialność za życie innych ludzi, a także mając na względzie dobro własnej kieszeni, trzeba przenieść się do… teraźniejszości. Ta teraźniejszość to dawna przyszłość, ale bardziej realna, bo teraźniejsza i dostępna. Co prawda nie wszystko złoto, co się świeci, ale warto dokładnie przyjrzeć się metodom i praktykom XXI wieku – i dzięki nim przenieść się o dwieście lat do przodu… No, dobrze: o sto.

Autor żywi wielką nadzieję, że ten artykuł obudzi w specjalistach z branży ducha rozwoju, innowacji, a także jeszcze bardziej wzmocni potrzebę poznania i wyzwoli w czytelnikach poczucie konieczności dalszego dążenia do urzeczywistnienia marzeń. Nie tylko w sferze postanowień noworocznych i świątecznych życzeń, ale także w codziennej pracy, w służbie na rzecz innych ludzi – bo przecież tym się wszyscy zajmujemy – gorąco zachęcam: wejdźmy śmielej w XXI wiek.

Grzegorz Ćwiek
Schrack Seconet Polska

1) Informacja szczegółowa dostępna w firmie Schrack Seconet Polska.

Kompleksowa oferta produktów HD

Obserwacja bez ograniczeń
oraz bardziej szczegółowe obrazy

Na stadionach i w halach sportowych z powodzeniem wykorzystuje się systemy telewizji dozorowej oraz nagłośnieniowe oparte o technologię Bosch IP. Liczne referencje potwierdzają nasze doświadczenie. Teraz Bosch Security Systems wprowadził kompletną gamę rozwiązań wysokiej rozdzielczości (HD). Odpowiadają one na rosnące zapotrzebowanie w zakresie systemów HD pracujących w sieci IP oraz zapewniają nowy poziom jakości obrazu. Dzięki wyższej rozdzielczości obrazu, operator może rozróżnić drobne szczegóły sceny, co ma istotne znaczenie przy rozpoznawaniu twarzy kibiców i innych podobnych zastosowaniach.

Aby uzyskać więcej informacji, odwiedź naszą stronę internetową
www.boschsecurity.pl

BOSCH
Technologia bliżej nas

Instalacje wykrywania pożaru w przestrzeniach zagrożonych wybuchem (część 1)

Władysław Markowski

Przestrzenie i pomieszczenia, w których są stosowane, produkowane, przetwarzane lub magazynowane substancje mogące wytworzyć z powietrzem lub innymi utleniaczami mieszaniny wybuchowe o objętości co najmniej 0,01 m^3 w zwartej przestrzeni, należy zakwalifikować jako przestrzenie zagrożone wybuchem. Pomieszczenie, w którym może się wytworzyć mieszanina wybuchowa gazów, mgieł lub pyłów, a jej wybuch mógłby spowodować przyrost ciśnienia w tym pomieszczeniu przekraczający 5 kPa, określamy jako pomieszczenie zagrożone wybuchem. Generalnie można założyć, że jeżeli mamy do czynienia z substancjami palnymi, zawsze istnieje prawdopodobieństwo, iż pojawi się atmosfera wybuchowa i znajdujące się w niej urządzenia i instalacje staną się źródłem zapłonu. Zapewnienie bezpieczeństwa, zarówno w odniesieniu do stosowanej technologii, jak i pracy w takich obiektach i wokół nich, jest jednym z najtrudniejszych zagadnień dotyczących bezpieczeństwa technicznego. Jeżeli chodzi o ochronę przeciwpożarową, należy mieć na uwadze, by instalując system wykrywania pożaru, nie spowodować dodatkowego zagrożenia przez wprowadzenie inicjatora wybuchu. Technologie wykorzystujące substancje, które mogą wytworzyć atmosferę wybuchową, dają wiele sposobów zmniejszenia zagrożenia i skutków ewentualnego wybuchu. W pierwszej części artykułu przedstawione zostaną strefy zagrożenia wybuchem oraz rodzaje obudów urządzeń, które mogą pracować w poszczególnych strefach. W części drugiej artykułu (*Zabezpieczenia* nr 2/2011) omówione zostaną zasady doboru urządzeń i projektowania instalacji sygnalizacji pożarowej w przestrzeniach zagrożonych wybuchem

Rodzaje stref zagrożenia wybuchem

Aby właściwie dobrać i zainstalować urządzenia do bezpiecznego stosowania w środowisku, w którym może pojawić się atmosfera wybuchowa, należy dokonać klasyfikacji pomieszczeń i przestrzeni zewnętrznych (stref) zagrożonych wybuchem – uwzględniając rodzaj strefy, grupę wybuchowości i klasę temperaturową w przypadku stref gazowych oraz rodzaj strefy i maksymalną temperaturę na powierzchni urządzenia w przypadku stref pyłowych.

Norma [8] definiuje trzy strefy zagrożenia wybuchem dla mieszanin substancji palnych w postaci gazu, pary lub mgły z powietrzem oraz trzy strefy dla atmosfer wybuchowych w postaci obłoku palnego pyłu w powietrzu.

Strefa 0 i strefa 20 to miejsca, w których atmosfera wybuchowa występuje stale, przez długie okresy lub często, np. wewnątrz pojemników, rurociągów, zbiorników.

Strefa 1 i strefa 21 to miejsca, w których atmosfera wybuchowa może czasami wystąpić w trakcie normalnych działań, np. bezpośrednie otoczenie miejsc napełniania i opróżniania (pojemników, zbiorników, rurociągów itp.) lub nasypywania i wysypywania (materiałów i substancji, które w zawiesinie powietrznej tworzą mieszankę wybuchową).

Strefa 2 i strefa 22 to miejsca, w których atmosfera wybuchowa nie pojawia się w trakcie normalnego działania, a w przypadku pojawienia się trwa krótko (może obejmować miejsca otaczające strefę 0 lub 1 albo miejsca w bezpośrednim otoczeniu urządzeń, np. pomieszczenia z młynami, w których osiada pył).

Klasyfikację stref zagrożenia wybuchem powinny przeprowadzić osoby, które znają właściwości substancji palnych, technologię produkcji i wyposażenie instalacji technologicznej oraz potrafią przewidzieć zachowanie się gazów i cieczy palnych po ich uwolnieniu z potencjalnych źródeł emisji. Przeprowadzona klasyfikacja obszarów niebezpiecznych powinna być zapisana w odpowiednim dokumencie, podpisanym zarówno przez projektanta – technologa, jak i użytkownika, zawierającym m.in. rysunki z poziomymi i pionowymi rzutami, pokazującymi rodzaj i zasięg stref, grupy wybuchowości i klasy temperaturowe.

Projektant instalacji sygnalizacji pożarowej, dobierając urządzenia, korzysta z tak podanej informacji dotyczącej strefy zagrożonej wybuchem.

Urządzenia stosowane w przestrzeniach zagrożonych wybuchem mają w swojej konstrukcji lub sposobie działania odpowiednie zabezpieczenia przeciwwybuchowe, czyli takie, które wykluczają lub znacznie ograniczają możliwość zainicjowania wybuchu przez iskrę lub temperaturę powstające w czasie pracy lub podczas awarii. Urządzenia te będziemy dalej nazywać urządzeniami Ex.

Strefy zagrożenia wybuchem	
substancji palnych: gazu, pary lub mgły z powietrzem	obłoku palnego pyłu w powietrzu
Strefa 0 (dawniej strefa Z0)	Strefa 20 (dawniej strefa Z10)
Strefa 1 (dawniej strefa Z1)	Strefa 21 (dawniej strefa Z11)
Strefa 2 (dawniej strefa Z2)	Strefa 22 (dawniej strefa Z12)

Tab. 1. Strefy zagrożenia wybuchem

Ex	Strefa 1
IIB	T4

Tab. 2. Przykładowe oznaczenie strefy

Klasa temperaturowa	Maksymalna temperatura powierzchni urządzenia [°C]	Temperatura samozapłonu gazu [°C]
T1	450	> 450
T2	300	> 300
T3	200	> 200
T4	135	> 135
T5	100	> 100
T6	85	> 85

Tab. 3. Klasy temperaturowe urządzeń Ex

Podział urządzeń Ex na grupy i podgrupy

Urządzenia elektryczne przeznaczone do stosowania w pomieszczeniach i przestrzeniach zewnętrznych zagrożonych wybuchem (urządzenia Ex) dzieli się [1] na dwie grupy:

- **grupa I** – urządzenia przeznaczone do użytku w kopalniach o zagrożeniu metanowym;
- **grupa II** – urządzenia przeznaczone do użytku w innych miejscach niż kopalnie o zagrożeniu metanowym.

Ten podział urządzeń odpowiada podziałowi atmosfer wybuchowych:

- metan w wyrobiskach podziemnych – grupa I;
- gazy palne i pary cieczy palnych, z wyjątkiem metanu w wyrobiskach podziemnych – grupa II.

Oczywiście projektantów i instalatorów sygnalizacji pożarowej interesować będą wyłącznie urządzenia należące do grupy II, dlatego w dalszej części artykułu ograniczymy się tylko do nich.

Urządzenia przeznaczone do użytku poza kopalniami (grupa II) dzielone są na grupy wybuchowości II (ochrona np. Exe, Exp) i podgrupy wybuchowości **IIA**, **IIB** i **IIC** (ochrona np. Exd oraz Exia/ib/ic) w zależności od właściwości gazów i par w przestrzeni zagrożonej wybuchem, w której będą użytkowane.

Uwaga! Urządzenia podgrupy IIB spełniają wymagania dla urządzeń podgrupy IIA, natomiast urządzenia podgrupy IIC mogą być stosowane zamiast urządzeń podgrup IIA i IIB, gdyż spełniają ich wymagania.

Klasy temperaturowe urządzeń Ex

Urządzenia grupy II klasyfikowane są dodatkowo według klas temperaturowych, określających maksymalną temperaturę osiąganą w czasie pracy przez dowolną część lub powierzchnię urządzenia elektrycznego mogącą zainicjować zapłon otaczającej atmosfery wybuchowej.

Klasyfikację tę ustalono po analizie temperatur zapłonu substancji palnych. Oczywiście urządzenie, które jest oznakowane klasą T6 (co oznacza, że jego obudowa i części nie przekraczają temperatury 85 °C), może być stosowane w atmosferach mających wyższe temperatury samozapłonu.

Urządzenia sygnalizacji pożarowej dla przestrzeni zagrożonych wybuchem zwykle mają klasę temperaturową T6, rzadziej T5 lub T4.

Standardowy zakres temperaturowy pracy urządzeń Ex wynosi od –30 °C do +40 °C. Jeżeli temperatura otoczenia, w którym pracuje urządzenie, wykracza poza zakres standardowy, zakres ten podaje się w oznakowaniu z towarzyszącym symbolem $\mathbf{T_a}$.

Kategorie urządzeń Ex

Wśród urządzeń grupy II wyróżnia się **kategorie 1, 2 i 3.**

Kategoria 1 obejmuje urządzenia tak zaprojektowane, aby mogły poprawnie funkcjonować zgodnie z przeznaczeniem, zapewniając **bardzo wysoki poziom zabezpieczenia**. Przeznaczone są do użytkowania w miejscach, w których atmosfery wybuchowe są obecne stale lub często w długich okresach, a więc w strefach 0 (gazy) i 20 (pyły).

Kategoria 2 to urządzenia tak zaprojektowane, aby mogły działać poprawnie i zgodnie z przeznaczeniem, zapewniając **wysoki poziom zabezpieczenia**. Przeznaczone są do użytkowania w miejscach, w których występowanie atmosfer wybuchowych jest prawdopodobne, a więc w strefach 1 (gazy), 21 (pyły) i 22 (pyły przewodzące).

Kategoria 3 to urządzenia tak zaprojektowane, aby mogły poprawnie funkcjonować zgodnie z przeznaczeniem, zapewniając **normalny poziom zabezpieczenia**. Urządzenia tej kategorii są przeznaczone do użytkowania w miejscach, w których pojawienie się atmosfery wybuchowej jest mało prawdopodobne, a jeżeli się pojawi, to tylko w krótkim okresie – czyli w strefach 2 (gazy) i 22 (pyły nieprzewodzące).

Uwaga! Urządzenia wyższej kategorii (zapewniające wyższy stopień bezpieczeństwa) mogą być stosowane w strefach wymagających urządzeń niższej kategorii, tak więc urządzenie kategorii 1 może być stosowane w przypadku atmosfery gazowej we wszystkich strefach 0, 1 i 2, a w przypadku atmosfery pyłowej w strefach 20, 21 i 22.

Do kategorii przyporządkowana jest litera G w przypadku stref gazowych, a D w przypadku stref pyłowych.

Rodzaje budowy przeciwwybuchowej urządzeń Ex

Zabezpieczenie przeciwwybuchowe urządzeń elektrycznych można osiągnąć poprzez odpowiednią budowę urządzenia, np.:

– osłonięcie obwodów elektrycznych obudowami uniemożliwiającymi przeniesienie wybuchu z obudowy do otoczenia;
– wykonanie obwodów elektrycznych w sposób iskrobezpieczny, wykluczający możliwość, aby urządzenie stało się efektywnym źródłem zapłonu.

Poszczególne rodzaje budowy przeciwwybuchowej urządzeń Ex są objęte normami (międzynarodowymi IEC i europejskimi EN wprowadzonymi do polskich norm PN), szczegółowo określającymi wymagania dotyczące ich konstrukcji i badań elektrycznych. Każdy rodzaj budowy przeciwwybuchowej ma też przypisany jednoznaczny symbol, np.:

– **d** – osłona ognioszczelna,
– **e** – budowa wzmocniona,
– **ia**, **ib**, **ic** – wykonanie iskrobezpieczne o różnych poziomach zabezpieczenia,
– **ma**, **mb** – hermetyzacja o różnych poziomach zabezpieczenia.

Istnieją również inne rodzaje budowy przeciwwybuchowej, jednakże w dziedzinie sygnalizacji pożarowej raczej nie są one używane.

Budowę przeciwwybuchową **d** zapewnia osłona wytrzymująca ciśnienie wybuchu mieszaniny wybuchowej i zapobiegająca przeniesieniu się wybuchu do otaczającej osłonę atmosfery, w przypadku gdyby jakikolwiek zamknięty w niej element mógł wywołać zapłon.

Budowę wzmocnioną **e** zapewniają dodatkowe zabezpieczenia (np. zwiększenie szczelności, zwiększenie odstępów izolacyjnych) przed powstaniem nadmiernej temperatury oraz wystąpieniem łuków i iskier wewnątrz urządzeń elektrycznych i na ich zewnętrznych częściach, normalnie nie wytwarzających iskier i łuków.

Budowę iskrobezpieczną **i** zapewniają bezpieczne wartości napięć, prądów, rezystancji, indukcyjności, pojemności, wartości L/R oraz spełnienie wymogów materiałowych i konstrukcyjnych dotyczących przeciwdziałania powstaniu iskier o energii zdolnej do wywołania wybuchu.

Urządzenia iskrobezpieczne oraz iskrobezpieczne części urządzeń towarzyszących występują w trzech poziomach zabezpieczenia: **ia**, **ib** i **ic**, przy czym poziom zabezpieczenia **ia** jest najwyższy.

Budowę hermetyzowaną **m** zapewnia otoczenie zalewą części urządzenia zdolnych do zapalenia atmosfery wybuchowej wskutek iskrzenia bądź nagrzewania się. Dzięki temu atmosfera wybuchowa nie może zostać zapalona na skutek pracy lub instalowania urządzenia. Urządzenia hermetyzowane mają dwa poziomy zabezpieczenia: **ma** i **mb**, przy czym **ma** reprezentuje wyższy poziom zabezpieczenia.

Zadaniem producenta jest spełnienie wszystkich wymagań norm dotyczących produkowanego urządzenia elektrycznego Ex kategorii 1 i 2 oraz uzyskanie potwierdzającego ten fakt **certyfikatu badania typu WE** (po poddaniu urządzenia badaniom i próbom przez notyfikowane laboratorium z zachowaniem określonych procedur zgodnie z rozporządzeniem [9]). Jednostka notyfikowana na podstawie badań podaje w certyfikacie cechę przeciwwybuchowości urządzenia. Urządzenia elektryczne Ex kategorii 3 zgodnie z obowiązującymi przepisami muszą posiadać deklarację zgodności CE.

Cecha przeciwwybuchowości jest dla projektanta wskazówką, gdzie i w jakiej atmosferze wybuchowej można użytkować dane urządzenie.

Oznakowanie urządzeń Ex

Zgodnie z rozporządzeniem [9], które wprowadziło do polskiego systemu prawnego dyrektywę 94/9/EC, urządzenia przeznaczone do pracy w strefach zagrożonych wybuchem powinny w oznakowaniu zawierać poniższe dane:

a) nazwę (lub znak handlowy) i adres producenta;
b) serię lub typ urządzenia;
c) numer fabryczny (jeżeli jest stosowany);
d) rok produkcji;
e) oznaczenie (cechę) przeciwwybuchowości (według przykładów poniżej);
f) numer certyfikatu badania typu WE, zawierający:
  – nazwę jednostki, która przeprowadziła badanie typu i wystawiła certyfikat,
  – dwie ostatnie cyfry roku, w którym przeprowadzono badanie typu WE,
  – skrót ATEX (z ang. ATmosphere EXplosible),
  – numer przeprowadzonego badania;
g) oznakowanie CE;
h) numer identyfikacyjny notyfikowanej jednostki przy oznakowaniu CE.

Poszczególne elementy oznaczenia (cechy) przeciwwybuchowości urządzenia wyjaśniono na przykładzie w tab. 4.

Przykłady oznakowania urządzeń Ex stosowanych w sygnalizacji pożarowej

1) Uniwersalna optyczna czujka dymu, typ DUR-40Ex:
   Ⓔx II 2G Ex ib IIC T6
   (producent POLON-ALFA, certyfikat nr KDB 05 ATEX 190X)
   – człon **II** – urządzenie grupy **II**, przeznaczone do stosowania w przemyśle poza kopalniami
   – człon **2G** – urządzenie kategorii **2** mogące pracować w strefach **1** i **2** zagrożenia wybuchem, w których występuje atmosfera gazowa **G**
   – człon **Ex ib** – urządzenie o budowie przeciwwybuchowej **Ex**, iskrobezpiecznej **ib**
   – człon **IIC** – w strefach zagrożenia gazami i parami cieczy palnych podgrupa wybuchowości **IIC** (a więc także IIA i IIB)
   – człon **T6** – klasa temperaturowa **T6** (a więc także T1–T5)
2) Czujka płomienia trójpasmowa podczerwieni X3301:
   Ⓔx II 2GD EEx de IIC T5-T6
   (producent DET-TRONICS, certyfikat nr DEMCO 01 ATEX 130204)
   – człon **II** – urządzenie grupy **II**, przeznaczone do stosowania w przemyśle poza kopalniami
   – człon **2GD** – do stosowania w strefach 1 i 2 oraz 21 i 22 zagrożenia wybuchem, w których występuje atmosfera gazowa **G** lub pyłowa **D**
   – człon **EEx de** – urządzenie o budowie przeciwwybuchowej **EEx** (stare oznaczenie), ognioszczelnej **d** i częściowo wzmocnionej (skrzynka zaciskowa) **e**
   – człon **IIC** – w strefach zagrożenia gazami i pyłami palnymi podgrupa wybuchowości **IIC** (a więc także IIA i IIB)
   – człon **T5-T6** – klasa temperaturowa **T5** (a więc także T1–T4) lub **T6** (a więc także T1–T5) w zależności od tego, czy jest wykorzystywany grzejnik

Specjalne oznaczenie zabezpieczenia przeciwwybuchowego	Grupa urządzeń I – do użytku w kopalniach II – do użytku w przemyśle poza kopalniami	Kategoria urządzeń 1 – dla stref 0 i 20 2 – dla stref 1 i 21 3 – dla stref 2 i 22	Atmosfera wybuchowa G – gazowa D – pyłowa
1	2	3	4
Ⓔx	**II**	**2**	**G**
Symbol budowy przeciwwybuchowej	**Symbol każdego rodzaju budowy**	**Grupa lub podgrupa urządzenia**	**Klasa temperaturowa**
5	6	7	8
Ex*)	**ib**	**IIC**	**T6**

Tab. 4. Przykład dla **Ⓔx II 2G Ex ib IIC T6***: poszczególne elementy oznaczenia (cechy) przeciwwybuchowości urządzenia*

**) We wcześniejszym oznakowaniu można znaleźć zapis EEx, oznaczający zgodność z normami europejskimi; obecnie na całym świecie stosowany jest ujednolicony zapis.*

3) Ręczny ostrzegacz pożarowy szeregu BG3:
⟨Ex⟩ **II 1G EEx ia IIC T4**
(producent MEDC, certyfikat nr BAS 00 ATEX 1067X)
– człon **II** – urządzenie grupy **II**, przeznaczone do stosowania w przemyśle poza kopalniami
– człon **1G** – do stosowania w strefach 0, 1 i 2 zagrożenia wybuchem, w których występuje atmosfera gazowa **G**
– człon **Ex ia** – urządzenie o budowie przeciwwybuchowej **Ex**, iskrobezpiecznej **ia**
– człon **IIC** – w strefach zagrożenia gazami palnymi podgrupa wybuchowości **IIC** (a więc także IIA i IIB)
– człon **T4** – klasa temperaturowa **T4** (a więc także T1–T3)

4) Separator, typ 9167/*3-11-00:
⟨Ex⟩ **II (1)GD [EEx ia] IIC/IIB**
(producent STAHL, certyfikat nr BVS 04 ATEX E082X)
– człon **II** – urządzenie grupy **II**, przeznaczone do stosowania w przemyśle poza kopalniami
– człon **(1)GD** – urządzenie towarzyszące urządzeniom przeciwwybuchowym kategorii 1, aby mogły być instalowane w strefach 0, 1 i 2 oraz 20, 21 i 22 zagrożenia wybuchem, w których występuje atmosfera gazowa **G** lub pyłowa **D**
– człon **[EEx ia]** – urządzenie towarzyszące, do pracy poza strefami zagrożonymi wybuchem (symbol **EEx** i symbol rodzaju budowy przeciwwybuchowej w nawiasie kwadratowym), wyposażone w wejście iskrobezpieczne ia do współpracy z urządzeniem pracującym w strefie
– człon **IIC/IIB** – urządzenie podgrupy **IIC**, co oznacza także podgrupy IIB i IIA, lecz wymienienie niezależnie podgrupy **IIB** oznacza inne warunki użytkowania dla tych podgrup (w tym przypadku inne dopuszczalne maksymalne wartości parametrów indukcyjności L_0 i pojemności C_0)
– brak członu określającego klasę temperaturową – w przypadku urządzeń towarzyszących, nie przeznaczonych do instalowania w strefach zagrożonych wybuchem, nie oznacza się klasy temperaturowej

Uwaga! Jeżeli na końcu numeru certyfikatu umieszczony jest symbol **X**, oznacza to, że chcąc bezpiecznie eksploatować dane urządzenie, należy się zastosować do specjalnych warunków użytkowania wskazanych w certyfikacie, np. w przypadku czujki DUR-40Ex chodzi o inny niż standardowy zakres temperatury eksploatacji i parametry obwodu iskrobezpiecznego.

Część druga artykułu, omawiająca zasady doboru urządzeń i projektowania instalacji sygnalizacji pożarowej w przestrzeniach zagrożonych wybuchem, ukaże się w następnym numerze *Zabezpieczeń*.

mgr inż. Władysław Markowski
POLON-ALFA ZUD

Literatura

1) PN-EN 60079-0:2009 *Urządzenia elektryczne w przestrzeniach zagrożonych wybuchem gazów, część 0: Wymagania ogólne.*
2) PN-EN 60079-7:2010 *Atmosfery wybuchowe*, część 7: *Zabezpieczenie urządzeń za pomocą budowy wzmocnionej „e”.*
3) PN-EN 60079-10:2003 *Urządzenia elektryczne w przestrzeniach zagrożonych wybuchem*, część 10: *Klasyfikacja obszarów niebezpiecznych* (oryg)
4) PN-EN 60079-11:2010 *Atmosfery wybuchowe*, część 11: *Zabezpieczenie urządzeń za pomocą iskrobezpieczeństwa „i”.*
5) PN-EN 60079-14:2009 *Atmosfery wybuchowe*, część 14: *Projektowanie, dobór, montaż instalacji elektrycznych* (oryg).
6) PN-EN 60079-17:2008 *Atmosfery wybuchowe*, część 17: *Kontrola i konserwacja instalacji elektrycznych* (oryg).
7) PN-EN 60079-25:2007 *Urządzenia elektryczne w przestrzeniach zagrożonych wybuchem*, część 25: *Systemy iskrobezpieczne.*
8) PN-EN 1127-1:2007 *Atmosfery wybuchowe – Zapobieganie wybuchowi i ochrona przed wybuchem – Pojęcia podstawowe i metodologia* (oryg).
9) Rozporządzenie Ministra Gospodarki z dnia 22 grudnia 2005 r. w sprawie zasadniczych wymagań dla urządzeń i systemów ochronnych przeznaczonych do użytku w przestrzeniach zagrożonych wybuchem (Dz. U. 2005, nr 263, poz. 2203).
10) S. Nowak, *Elektryczne urządzenia Ex*, wyd. II, Automatic Systems Engineering Sp. z o.o., Gdańsk 2009.
11) Praca zbiorowa, *Instalacje elektryczne i teletechniczne,* Dashofer, Warszawa 2010.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

BEZPIECZNY ZAKUP

„POLON-ALFA" Zakład Urządzeń Dozymetrycznych sp. z o.o.

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

ODKRYJ SZYBKOŚĆ INSTALACJI

DSC

WT5500
Bezprzewodowa klawiatura LCD

WT4989
Bezprzewodowy pilot
z wyświetlaczem LCD

WS4904W
Bezprzewodowe czujki PIR

WS4945
Bezprzewodowa
czujka kontaktronowa

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

ALEXOR PC9155

BEZPRZEWODOWY SYSTEM ALARMOWY
O KOMUNIKACJI DWUKIERUNKOWEJ

- Obsługa maksymalnie 32 urządzeń bezprzewodowych i 16 breloków
- Kompatybilność z urządzeniami o komunikacji jednokierunkowej
- Obsługa do 4 sygnalizatorów i klawiatur bezprzewodowych
- Funkcja automatycznego przypisywania urządzeń bezprzewodowych
- Szablony programowania skracające czas instalacji
- 16 kodów użytkownika, 1 kod główny, 1 kod konserwatora
- Funkcja sprawdzania kodu identyfikacyjnego systemu
- Alternatywna komunikacja przez sieć GSM/GPRS lub TCP/IP
- Wbudowany sygnalizator akustyczny o mocy 85dB
- 2 zaciski I/O, które mogą być zaprogramowane jako wyjścia PGM lub przewodowe linie dozorowe
- 200mA obciążalności prądowej wyjścia AUX
- Rejestr 500 zdarzeń
- Podwójne zabezpieczenie antysabotażowe przed otwarciem obudowy lub oderwaniem od ściany
- 24 godzinne podtrzymanie baterii

Pozostałe urządzenia bezprzewodowe kompatybilne z centralą PC9155:

WS4939, PT4
Bezprzewodowy pilot i brelok zbliżeniowy

TL265GS, GS2065
Komunikatory alarmowe wysyłające kody raportujące przez sieć GSM/GPRS i TCP/IP

WT4901
Bezprzewodowy sygnalizator wewnętrzny

WT4911
Bezprzewodowy sygnalizator zewnętrzny

WS4916
Bezprzewodowa czujka dymu

WS4985
Bezprzewodowa czujka zalania wodą

WLS912L
Bezprzewodowa czujka zbicia szyby

WS4975
Bezprzewodowa czujka kontaktronowa

Rynek fizycznej kontroli dostępu

Bilansowanie wartości przez klienta, nowa dynamika

Brad Jarvis

Przez długi czas rynek fizycznej kontroli dostępu charakteryzował się tym, co HID Global nazywał „bilansowaniem wartości przez klienta", czyli znajdowaniem równowagi pomiędzy kosztem, poziomem bezpieczeństwa i wygodą użytkowania systemu kontroli dostępu. Równowaga ta wpływała na dokonywane przez klienta wybory i podejmowane decyzje zakupowe. Ostatnie badania AVISIAN pozwoliły na umocnienie przekonania, że te „działania bilansujące" będą nadal miały miejsce. Jednak na wybory klientów wpłyną także: nowa dynamika rynku, zmieniające się relacje pomiędzy czynnikami „bilansowania wartości przez klienta" oraz nowe dziedziny zastosowań systemów

Wnioski te wynikają z badań rynku fizycznej kontroli dostępu przeprowadzonych przez AVISIAN w 2010 roku. HID Global był gospodarzem związanej z przemysłem grupy docelowej integratorów i doświadczonych konsultantów, której zadaniem było wychwycenie z realnego świata zjawisk, które weterani przemysłu uważają za istotne. Ostatnią podstawą do naszych wniosków były wyniki studium badawczego IMS PAC 2009.

Według wspomnianych badań na rynek fizycznej kontroli dostępu wpływają głównie następujące czynniki:

– wzrost oddziaływań czynników państwowych zarówno w sektorze publicznym, jak i prywatnym,
– nowe technologie (łącznie z bezstykowymi) oraz szybsza ich adaptacja,
– szybkie wprowadzenie inteligentnych kart wielozadaniowych,
– rosnące wymagania co do poziomu zabezpieczeń,
– koszty inwestycji oraz preferowanie rozwiązań o charakterze przyszłościowym.

Zagadnienia te nie są nowe, ale są ważne, ponieważ w świetle specyficznych implikacji rynkowych w istotny sposób wpływają na dokonywany przez klientów bilans wartości. Poniżej znajduje się omówienie roli każdego z tych pięciu czynników.

Czynnik 5. Zwiększone oddziaływanie czynników państwowych

Na jednym ze spotkań grupy stwierdzono, że w ciągu najbliższych trzech lat normy określane przez czynniki rządowe wpłyną na branżę silniej, niż wpływały w ciągu ostatnich trzech dekad. Inicjatywy rządowe sięgają obecnie dalej niż kiedykolwiek poza sektor publiczny, obejmując wiele zastosowań w sektorze prywatnym. Wielu uczestników spotkania sądziło, że większy wpływ czynników rządowych na sektor prywatny spowoduje zwiększenie zainteresowania firm i organizacji sprawami bezpieczeństwa. Wskazywano na fakt, że w przeszłości zabezpieczenia były umiarkowanie kosztowne i nie wymagały szyfrowania, natomiast obecnie rząd zaostrza standardy i plany ochrony prywatności, a nawet wymusza dyrektywy związane z bezpieczeństwem, zwłaszcza w takich dziedzinach życia i gospodarki, jak ochrona zdrowia, przetwórstwo żywności, zaopatrzenie w wodę. Ta tendencja jest także widoczna w przemyśle farmaceutycznym i edukacji. Mimo że infrastruktura cywilna (w USA) jest kontrolowana przeważnie przez sektor prywatny, rząd wywiera na nią ogromny wpływ w sprawach związanych z fizyczną kontrolą dostępu.

Czynnik 4. Nowe technologie, większa szybkość adaptacji

Migracja do nowych technologii, przede wszystkim do połączeń przez IP, wywołuje znaczące zmiany na rynku. Według badań IMS wysokość obrotów kontrolerami z możliwością połączeń przez IP powinna przekroczyć obroty+ kontrolerami z łączami szeregowymi i pod koniec 2013 roku osiągnąć poziom 42,7% udziału w rynku. Dzięki temu zmaleją koszty instalacji i okablowania, a zwiększy się zapotrzebowanie na inteligentne czytniki oraz na poszerzenie funkcjonalności i zbieżność aplikacji.

Badania AVISIAN wskazały trzy najbardziej cenione przez użytkowników cechy technologii związanych z czytnikami:

– możliwość modernizacji czytników i identyfikatorów (włącznie z wgrywaniem zmodernizowanych wersji), pozwalającej na aktywne zwalczanie zagrożeń (cecha oceniana przez 70% respondentów jako wysoce pożądana),
– programowalność czytników oraz możliwość ich równoczesnej pracy z co najmniej trzema typami kart (cecha oceniana jako ważna przez 71% respondentów),
– rozbudowane opcje programowania i konfigurowania oraz uniwersalne narzędzie do konfiguracji programatorów i czytników pozwalające na zarządzanie formatami identyfikatorów, dostępne w wyniku umowy licencyjnej z dostawcą (cecha uznana za pożądaną przez niemal dwie trzecie respondentów).

Respondenci w badaniach AVISIAN stwierdzili również, że chcieliby dysponować generatorem identyfikatorów, wspomagającym definiowanie danych i zabezpieczanie ich na kartach (prawie 60% respondentów), oraz możliwością określania innych typów identyfikatorów, takich jak telefony, breloki do kluczy, naklejki lub żetony. Ponad 70% użytkowników społecznościowych i 80% respondentów z obszaru przemysłu uważało, że ta ostatnia możliwość jest ważna, a obie grupy stwierdziły nieadekwatność obecnych opcji.

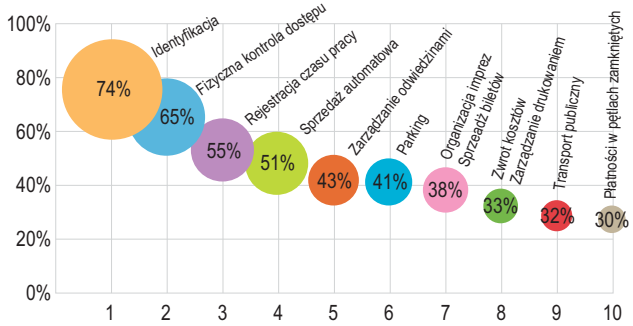
Według badań IMS obroty kartami inteligentnymi stale wzrastają: o 13,5% CAGR w latach 2009–2013, w porównaniu z 2,4% CAGR dla techniki zbliżeniowej w tym samym okresie. IMS sądzi, że liczba instalacji bazujących na kartach inteligentnych zbliży się w 2013 roku do liczby instalacji zbliżeniowych. Jak wspomniano wcześniej, jednym z najważniejszych czynników wzrostu jest dążenie do wprowadzenia pojedynczej karty lub identyfikatora, które mogłyby zmagazynować więcej informacji wymaganych dla dodatkowych zastosowań i bezpieczeństwa.

Czynnik 3. Wiele zastosowań pojedynczej karty

Pragnąc podkreślić ważność kart „wielozadaniowych" na rynku, jeden z respondentów grupy docelowej stwierdził, że główny klient uniwersytecki nie rozważa zakupu, o ile nie zapewni mu się zainstalowania dodatkowych aplikacji w istniejącym systemie kontroli dostępu i identyfikatorach lub rozszerzenia zastosowań istniejących aplikacji na nowe obszary.

W podobnym duchu 64% respondentów stwierdziło, że w ich odczuciu bardzo pożądane jest zapisywanie na pojedynczym identyfikatorze wielu formatów i aplikacji tożsamości, obejmujących identyfikację, fizyczną kontrolę dostępu, rejestrację czasu pracy, sprzedaż automatową i organizację wizyt. Jako pożądane aplikacje wymieniano również parkowanie, organizację imprez i sprzedaż biletów (szczególnie na terenie campusów), a także zarządzanie drukowaniem, transport publiczny oraz systemy płatności w pętlach zamkniętych (rys. 1).

Do środowisk wielozadaniowych przechodzą obecnie szkolnictwo wyższe i służba zdrowia; ich eksplorację rozpoczynają także korporacje. Jednym z przykładów zastosowań korporacyjnych jest fakt, że US Bank ostatnio wprowadził pojedynczą kartę, która może być stosowana do płatności tradycyjnych i bezdotykowych oraz uzyskiwania dostępu do obiektów. Wybrana technologia połączyła aplikację płatności bezdotykowej Visa PayWave z technologią karty inteligentnej HID Global iCLASS



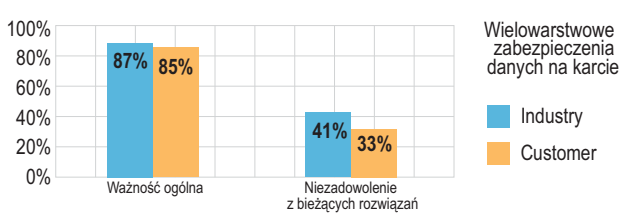
Rys. 1. Wygoda i oszczędność kosztów są zasadniczymi powodami przechodzenia na rozwiązania z pojedynczą kartą

do fizycznej kontroli dostępu . W 2010 roku US Bank, pierwszy w USA emitent kart do pilotażowego programu PayID, otrzymał nagrodę Paybefore za najbardziej innowacyjny program do tego zastosowania.

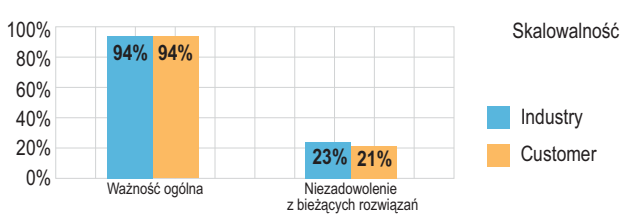
Czynnik 2. Zwiększenie bezpieczeństwa odczytu karty

Obecnie używane karty zawierają znacznie więcej chronionych informacji, są stosowane w większej liczbie aplikacji, wymagają silniejszej ochrony danych osobowych oraz muszą mieć możliwość uwierzytelnienia i zabezpieczenia tożsamości. Spowodowało to konieczność utworzenia wielu warstw zabezpieczeń, między innymi dwuelementowego uwierzytelniania tożsamości i szablonów biometrycznych, które należy zapisać na karcie. Ponad 85% użytkowników uważa, że jest to czynnik bardzo istotny (rys. 2), a ponad jedna trzecia nie odczuwa wystarczającego wsparcia ze strony dostawców (przyznających w tej kwestii rację użytkownikom).

Cecha, którą respondenci uznali za najważniejszą, to możliwość modernizacji zabezpieczeń karty na wypadek złamania obecnych przez hakerów. Uważało tak 91% użytkowników, a ponad 52% było niezadowolonych z obecnie dostępnych opcji. Drugą najbardziej pożądaną cechą karty jest modernizacja oprogramowania w razie pojawienia się nowych zagrożeń – 92% respondentów uznało ją za ważną, a prawie 40% było niezadowolonych z obecnej sytuacji.



Rys. 2. Potrzeba ochrony prywatności, uwierzytelnienia tożsamości i zapobieżenia nieupoważnionemu dostępowi stworzyła konieczność zabezpieczania znajdujących się na karcie danych



Rys. 3. Istnieje rozbieżność pomiędzy żądaniem skalowalności a ofertą przemysłu w tym zakresie

Czynnik 1. TCO i rozwiązania przyszłościowe

TCO (*Total Cost of Ownership* – całkowity koszt posiadania) jest według badań AVISIAN czynnikiem numer jeden wpływającym na rynek fizycznej kontroli dostępu. W coraz większym stopniu klienci przed podjęciem decyzji o zakupie analizują nie tylko koszty instalacji, lecz także całkowity koszt posiadania (TCO) lub obsługi. Do rozważenia jest jeszcze szereg kluczowych kwestii, takich jak oczekiwany czas życia sprzętu, jego deprecjacja w czasie oraz możliwe ścieżki migracji do nowych technologii.

Ekonomika wymusza lepsze uzasadnienie wydatków, a firmy muszą również uwzględnić w kalkulacjach kosztów takie czynniki, jak konserwacja, modernizacje i amortyzacja. Ale czasy życia wyrobów kurczą się, na co wskazuje coraz szybsze wprowadzanie technologii wysokich częstotliwości oraz związane z tym wymagania rządowych standardów i protokołów. Klienci muszą wykorzystać istniejące inwestycje (ponad 90% respondentów stwierdziło, że jest to ważne, a ponad 20% było niezadowolonych z obecnej sytuacji – rys. 3). Respondenci stwierdzili również, że potrzebują łatwości migracji, możliwości przenoszenia tożsamości do nowych modeli zabezpieczeń oraz skalowalności.

Zrównoważenie

Ważnym dla przyszłości zagadnieniem jest również zrównoważenie rozwoju. W przemyśle prowadzone są już badania dotyczące możliwości wykorzystania sterowania nowoczesną automatyką budynków do celów zarządzania energią. Choć jak dotąd implementacje są ograniczone, orientujemy się, co się dzieje, spoglądając na działania liderów branży, pojawiające się normy i oznaki, że bariery kosztowe zaczynają się obniżać. Rządowa Zielona Grupa Zadaniowa ICMA rozważa już, jak „zazielenić" fabryki i wprowadzić „etykietowanie ekologiczne" na poziomie produkcyjnym. Analizuje się możliwości zarządzania energią poprzez kontrolę dostępu i zintegrowania obu systemów. Badając inne gałęzie przemysłu, możemy się dowiedzieć, jak zaadaptowały i wykorzystały standardy LEED (*Leadership in Energy and Environmental Design* – przodowanie w projektowaniu energetycznym i środowiskowym).

Spojrzenie w przyszłość: bilansowanie wartości

Pomimo dynamiki nowego rynku trzy główne elementy bilansowania wartości przez klienta – koszt, bezpieczeństwo i wygoda – nadal są motorem zmian w obszarze fizycznej kontroli dostępu, podobnie jak dążenie do zwiększenia wygody, obniżenia całkowitego kosztu posiadania i wzmocnienia zabezpieczeń nadal dyktują rozwój rynku. Jednocześnie nowa dynamika – na którą wpływają działania rządu, trendy rozwoju techniki, wymagania co do zabezpieczeń, możliwości zastosowania pojedynczej karty oraz wysokość kosztu całkowitego – tworzy nowe możliwości lepszego zaspokajania konkretnych i specyficznych potrzeb klienta, ponieważ pozwala mu na bilansowanie wartości dla systemów fizycznej kontroli dostępu.

Brad Jarvis
HID Global
Tłumaczenie: Redakcja

firma ATLine®

PROJEKTOWANIE KOMPLEKSOWYCH DOKUMENTACJI

- technicznych, architektoniczno - budowlanych wraz z niezbędnymi branżami specjalistycznymi obiektów biurowych i przemysłowych
- innowacyjnych systemów ochrony
- teletechnicznych, elektrycznych i automatyki przemysłowej

WYKONAWSTWO
zaawansowanych technologicznie systemów ochrony i bezpieczeństwa

SPRZEDAŻ
nowoczesnych systemów ochrony

Kompleksowe zabezpieczanie obiektów

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

www.atline.pl

ZSJZ

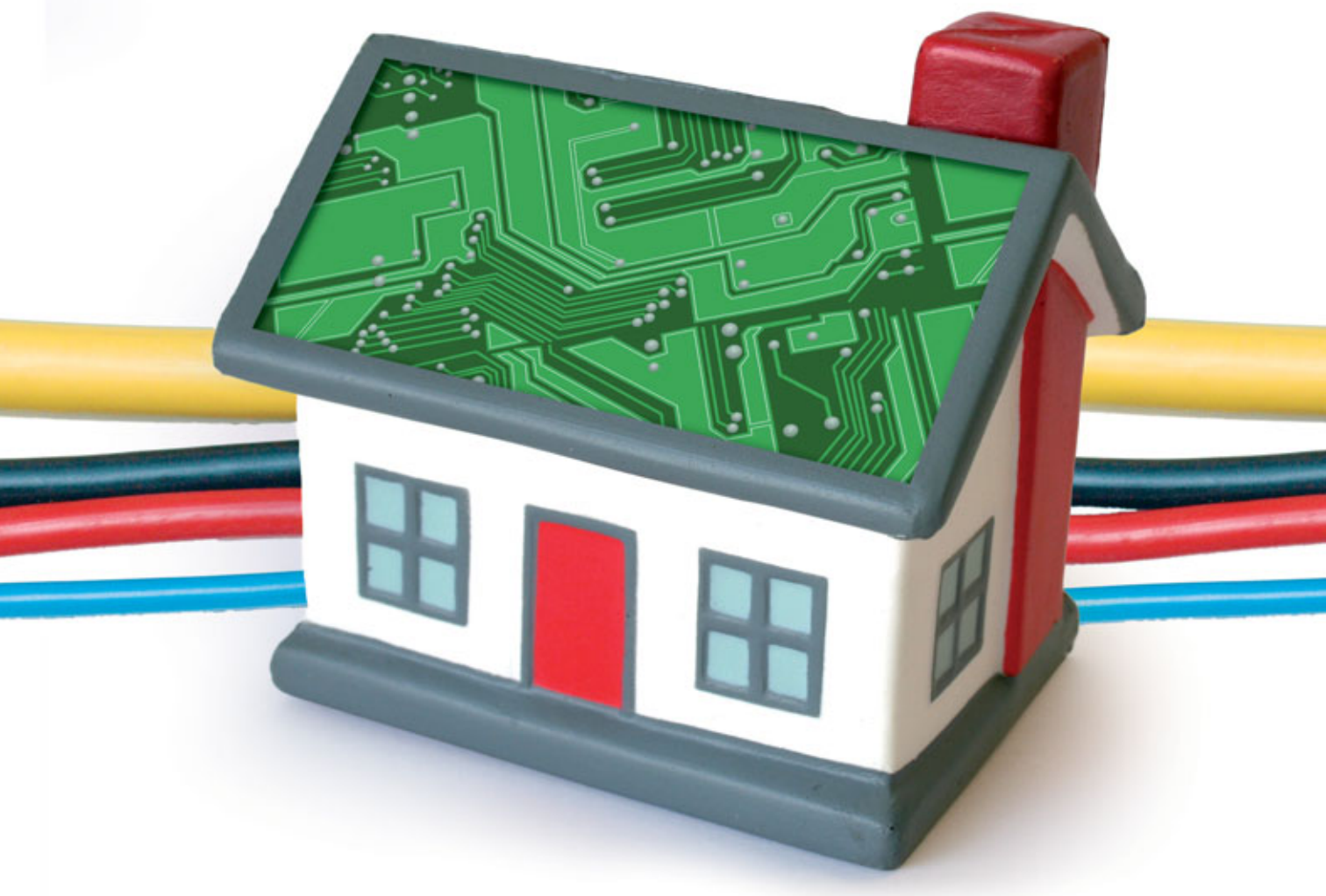
AQAP 2110:2009
ISO 9001:2008

Integracja systemu sygnalizacji włamania i napadu

z urządzeniami infrastruktury technicznej budynku (część I)

Adam Rosiński, Jacek Magiera

Niniejszy artykuł porusza zagadnienia związane z systemami inteligentnego budynku. Prezentuje szczegółową koncepcję integracji systemu sygnalizacji włamania i napadu z urządzeniami infrastruktury technicznej budynku, w tym przypadku domu jednorodzinnego. Jest to przykład, jak dość niewielkim kosztem można taki zintegrowany system wdrożyć w małym budynku mieszkalnym. Ponieważ opracowane rozwiązanie jest skalowalne, istnieje także możliwość jego rozbudowy i zastosowania go w grupie budynków mieszkaniowo-biurowych. Obecnie trwają prace nad wykonaniem zaprojektowanego systemu. Artykuł został podzielony na trzy części. Pierwsza z nich obejmuje wstęp i omówienie protokołów stosowanych w integracji systemów. W części drugiej zostanie przedstawiona koncepcja systemu sygnalizacji włamania i napadu dla domku jednorodzinnego. Część trzecia będzie natomiast zawierała charakterystykę urządzeń infrastruktury technicznej budynku oraz koncepcje integracji systemu sygnalizacji włamania i napadu z urządzeniami infrastruktury technicznej budynku z wykorzystaniem sterowników PLC. Autorzy mają nadzieję, że już jesienią tego roku będą mogli przedstawić spostrzeżenia i wnioski związane z uruchomieniem systemu



1. Wstęp

Pojęcie inteligentnego budynku zostało wprowadzone do terminologii na początku lat siedemdziesiątych ubiegłego wieku. Wówczas w procesach produkcyjnych w sektorze przemysłowym podjęto próby zastąpienia sterowania przez pokręcanie zaworów i przełączanie przełączników sterowaniem bardziej nowoczesnym, jakim jest nadzór komputerowy z wykorzystaniem odpowiedniego oprogramowania. Do sterowania i regulacji służą wtedy klawiatura, mysz i ekran monitora (obecnie również projektory multimedialne). Dzięki gwałtownemu rozwojowi techniki elektronicznej i komputerowej pod koniec lat 80. rozpoczęto przenoszenie koncepcji sterowania różnymi elementami z poziomu komputerów do budynków biurowych, a niedługo później – mieszkalnych. Na początku sterowanie to obejmowało tylko oświetlenie i wentylację (a później klimatyzację). Jednak bardzo szybki rozwój sieci telekomunikacyjnych i Internetu w latach 90. spowodował, że inteligentne budynki zostały podłączone do sieci teleinformatycznych. Dzięki temu możliwe jest sterowanie nimi właśnie poprzez te sieci. Razem z informatyzacją postępowała również integracja różnych systemów – już nie tylko oświetlenia i klimatyzacji, ale również systemów bezpieczeństwa: sygnalizacji włamania i napadu [6], kontroli dostępu, monitoringu wizyjnego, przekazu audio/wideo itd.

Obecnie w większości nowo budowanych budynków o charakterze biurowym już na etapie projektowania przewiduje się system BMS[1] do zarządzania energią (elektryczną, cieplną, chłodniczą) oraz innymi systemami (np. kontrolą dostępu i szeroko rozumianymi systemami bezpieczeństwa). W budynkach biurowych takie „udoskonalenie" jest już postrzegane jako standard, czyli normalne wyposażenie budynku. Brak tego wyposażenia powoduje, że potencjalni klienci (np. nabywcy biur od dewelopera, najemcy) nie zawsze chcą skorzystać z oferty, ponieważ obniża to prestiż firmy.

Zmieniło się też podejście właścicieli budynków mieszkalnych – nie wystarczy wybudować tradycyjny dom, trzeba myśleć m.in. o jego eksploatacji i kosztach utrzymania budynku w przyszłości. Inteligentny system w budynku mieszkalnym – podobnie jak w biurowcach – przestaje być postrzegany jako dobro niekoniecznie potrzebne i zaczyna być obowiązkowym elementem wyposażenia. Dzięki niemu zwiększa się komfort i bezpieczeństwo mieszkańców, a jednocześnie następuje racjonalizacja kosztów eksploatacyjnych domu.

W kolejnych częściach artykułu zostanie przedstawiona praktyczna koncepcja realizacji układu sterowania budynkiem mieszkalnym, odbierającego informacje z systemu sygnalizacji włamania i napadu (SSWiN) [4]. Układ ten opracowano w oparciu o dotychczas zebrane informacje [5,7], dokumentacje oraz wiedzę techniczną i doświadczenie zawodowe autorów. Koncepcję oparto na projekcie domku jednorodzinnego biura projektowego Domus. Zdecydowano się na sterowanie elementami domu za pomocą swobodnie programowalnego sterownika typu PLC[2] firmy Delta Electronics [1] wraz z odpowiednimi modułami wejść/wyjść oraz dwóch paneli dotykowych firmy Weintek (po jednym na każdą kondygnację) [3]. W sterowniku zostanie zainstalowana aplikacja stworzona przez autorów, która powinna spełniać wszystkie założenia wstępne. Układ sterowania ma być prosty, tani i elastyczny na wypadek chęci rozbudowy i wprowadzenia nowych funkcji. Mimo iż istnieją gotowe rozwiązania (które zostaną ogólnie scharakteryzowane w następnej części artykułu), potraktowano realizację takiego układu jako pewnego rodzaju wyzwanie (budowa domu też w pewnym sensie jest wyzwaniem).

2. Protokoły stosowane w integracji systemów

Obecnie na rynku oferowanych jest bardzo wiele różnego rodzaju rozwiązań służących do integracji systemów SSWiN z urządzeniami wyposażenia technicznego budynku. Najbardziej popularnymi, które można zastosować w domu jednorodzinnym, są układy sterowania oparte na protokole LonWorks [9] oraz systemy KNX-EIB [8].

2.1. Protokół LonWorks

Protokół LonWorks (w skrócie LON) został opracowany przez firmę Echelon na początku lat 90. XX wieku. Dość szybko wprowadzono go na rynek i wiele dużych firm wykorzystało go w swoich aplikacjach systemów sterowania. Jeśli jednak w jednym budynku zainstalowano dwa systemy integrujące różnych firm, to wówczas pojawiał się problem z ich integracją (bardzo często występował brak kompatybilności i zgodności protokołów). Dlatego też w roku 1994 zostało powołane stowarzyszenie LonMark International, które do dnia dzisiejszego sprawuje nadzór nad programowaniem urządzeń dołączanych do sieci LonWorks. Dzięki temu każde urządzenie, które posiada logotyp stowarzyszenia, spełnia wymagania „interoperability guidelines".

LonMark International nie testuje fizycznie każdego urządzenia. Cała istota sterowania w sieci LonWorks polega na komunikacji pomiędzy specjalnymi procesorami (Neuron Chips), w które wyposażone jest każde urządzenie. Oprogramowanie tych chipów jest kontrolowane przez stowarzyszenie, dzięki czemu urządzenia mogą współpracować ze sobą. Każdy Neuron Chip posiada niepowtarzalny adres (Neuron ID), który umożliwia nawiązanie komunikacji z konkretnym urządzeniem w sieci. Topologia sieci LON jest bardzo podobna do sieci lokalnej LAN[3]. Przy większych układach sterowania podstawowym elementem sieci jest węzeł, który pozwala podzielić sieć na mniejsze segmenty (np. węzeł – I piętro, węzeł – II piętro itd.). Węzeł z jednej strony jest podłączony do wspólnej sieci z innymi węzłami, a z drugiej do urządzeń wykonawczo-sterujących. Urządzenia te mogą komunikować się z węzłem bezpośrednio poprzez protokół LON lub poprzez moduł wejść/wyjść (oczywiście moduł ten będzie sterowany poprzez LON). Mniejsze układy sterowania można zbudować z pominięciem węzła, poprzez łączenie wszystkich urządzeń w jedną sieć.

Protokół LON jest obecnie używany przez duże firmy zajmujące się automatyką budynkową, takie jak m.in.:

– TAC,
– Siemens,
– Johnson Controls,
– Honeywell.

1) BMS – system zarządzania budynkiem, ang. Building Management System

2) PLC – programowalny sterownik logiczny, ang. Programmable Logic Controller

3) LAN – sieć lokalna, ang. Local Area Network

2.2. Systemy KNX/EIB

Systemy EIB zostały wprowadzone na rynek w latach 90. ubiegłego wieku. W roku 1999 (podobnie jak w przypadku LonWorks) zostało powołane stowarzyszenie, które zajmuje się zarządzaniem tym standardem. „EIB" to skrót angielskiej nazwy *European Installation Bus*, której znaczenie to „europejska magistrala instalacyjna". System EIB składa się z urządzeń zwanych sensorami i aktorami. Sensory są urządzeniami wydającymi polecenia, natomiast aktory – wykonującymi je. Sensory są połączone z aktorami za pomocą jednego kabla magistralnego, przez który są również zasilane. Dodatkowo wymagane jest, by do aktorów doprowadzony był kabel zasilający 230/400 V.

System KNX jest układem zdecentralizowanym. Oznacza to, że nie ma sterownika centralnego. Każdy element systemu (sensor) może sterować każdym innym elementem (aktorem). Ułatwia to ewentualne zmiany w systemie, czyniąc go bardzo elastycznym. Na przykład – jeśli danym włącznikiem nie chcemy już włączać światła w pokoju, tylko w salonie, to wystarczy wprowadzić zmiany w aplikacji. Nie ma potrzeby wymieniać części instalacji elektrycznej systemu, tak jak w przypadku tradycyjnej instalacji.

3. Podsumowanie

W pierwszej części cyklu dotyczącego integracji SSWiN z urządzeniami infrastruktury technicznej budynku przedstawiono zagadnienia związane z inteligentnym budynkiem. Scharakteryzowano dwa bardzo często stosowane protokoły i podano ogólne zasady ich funkcjonowania. Pomimo niewątpliwych zalet tych protokołów autorzy zdecydowali się na samodzielne opracowanie i stworzenie inteligentnego budynku (m.in. z wykorzystaniem sterowników PLC). Będzie można przeczytać o tym w kolejnych częściach.

W części drugiej zostanie przedstawiona koncepcja SSWiN dla domku jednorodzinnego, który posłuży później do integracji systemów jako podsystem składowy.

dr inż. Adam Rosiński
inż. Jacek Magiera

Bibliografia

1) Dokumentacja techniczno-ruchowa urządzeń firmy Delta Electronics.
2) Dokumentacja techniczno-ruchowa urządzeń firmy Satel.
3) Dokumentacja techniczno-ruchowa urządzeń firmy Weintek.
4) Magiera J., *Integracja systemu sygnalizacji włamania i napadu z urządzeniami infrastruktury technicznej budynku*, inżynierska praca dyplomowa, Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej i Technik Bezpieczeństwa, Warszawa 2010.
5) Materiały dydaktyczne Zespołu Laboratoriów Systemów Bezpieczeństwa Wydziału Informatyki Stosowanej i Technik Bezpieczeństwa Wyższej Szkoły Menedżerskiej w Warszawie.
6) Norma PN-EN 50131-1:2009: *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.*
7) Rosiński A., *Koncepcja zastosowania elektronicznych systemów bezpieczeństwa w sterowaniu urządzeniami elektrycznymi*, XXII Międzynarodowa Konferencja Naukowo-Techniczna EKOMILITARIS 2008, Zakopane 2008.
8) Strona internetowa stowarzyszenia EIB (http://www.knx.org).
9) Strona internetowa stowarzyszenia Lonmark (http://www.lonmark.org).

seria radius

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.

RCP Master *PR602LCD*

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

roger®

www.roger.pl

PR402 w obudowie DIN Rail 35mm - wprowadzono do oferty nową wersję zaawansowanego kontrolera dostępu.

Ochrona obwodowa obiektów

Karolina Zasada

Zimbabwe to kraj hiperinflacji i zamurowanego od dwudziestu trzech lat w fotelu prezydenckim osiemdziesięcioszścioletniego Roberta Gabriela Mugabego. W bajecznej scenerii wrześniowej suszy i skwaru poznałam Marcusa – młodego Zimbabweńczyka, który zaprosił mnie do swojej wioski. Zostałam serdecznie powitana, początkowo jako turystka, jednak przy bliższym poznaniu czułam się jak członek jego rodziny, mimo iż byłam „kiła", czyli białym człowiekiem. Ta uboga rodzina wiodła pozornie beztroskie, idylliczne życie wśród natury i dzikiej zwierzyny. Nic bardziej mylnego. Marcus opowiedział mi o reżimie prezydenta, nierespektowaniu praw człowieka, skrajnej biedzie oraz rosnącym poparciu dla opozycji, co z każdym dniem przyczynia się do fali przemocy – prześladowań, pobić, a nawet morderstw zwolenników oporu. Najgorzej wspominał noc, gdy do osady wtargnęła rozbestwiona hałastra wyzutych ze wszystkiego szumowin z maczetami, pałkami i nożami. Zginęły wówczas, śmiertelnie ranne, dwie osoby z jego rodziny. Nie mogę powiedzieć, że znaleźli się w niewłaściwym miejscu o niewłaściwej porze, gdyż byli u siebie. Trawiona nieukojonym pragnieniem szczęścia całej ludzkości, gorączką bezinteresownej i szlachetnej dobroczynności, starłam się z tamtejszą, twardą rzeczywistością. Nie opuszcza mnie jednak wrażenie, że we współczesnym świecie zagrożenie jest częścią życia niezależnie od tego, czy żyjemy w Polsce, czy po drugiej stronie kuli ziemskiej

Historia Marcusa, będąca jednym z przejawów wciąż powszechnego zjawiska terroryzmu, przemocy przeciwko osobom i ich mieniu, sprawiła, że postanowiłam napisać niniejszy artykuł. Jestem przekonana, że każdy z nas choć raz w życiu doświadczył poczucia zagrożenia i przerażenia. Temat jest więc niezwykle istotny, niezależnie od szerokości geograficznej.

Co możemy zrobić, by chronić ludzi i ich mienie? W tym artykule skupię się na ochronie obwodowej obiektów, dzięki której zarówno domy mieszkalne, jak i obiekty użyteczności publicznej mogą być w odpowiedni sposób zabezpieczone przed wtargnięciem napastników.

Po wielu latach doświadczeń w branży zabezpieczeń uważam, że nadrzędne znaczenie ma jak najszybsza informacja o wtargnięciu intruza w chroniony obszar. Po otrzymaniu takiego sygnału mamy jeszcze czas na reakcję, podjęcie decyzji, wezwanie pomocy. Bardzo ważna jest zatem ochrona obszaru wokół budynku lub ogrodzenia i odpowiednio wczesna sygnalizacja obecności nieproszonego gościa, zanim ten znajdzie się w bezpośredniej bliskości chronionych pomieszczeń lub osób.

Elektroniczne systemy ochrony zewnętrznej nadzorują obszar położony na zewnątrz lub wokół chronionego obiektu i sygnalizują zbliżanie się intruza lub wręcz jego wtargnięcie do strefy bezpośrednio przylegającej do tego obszaru. Systemy te można podzielić na trzy podstawowe grupy:

1) systemy pracujące na powierzchni ziemi, takie jak bariery mikrofalowe czy podczerwieni, czujki dualne, laserowe, radary, telewizja dozorowa;
2) systemy montowane na ogrodzeniu, budowane z przewodów mikrofonowych, światłowodowych, czujek wibracyjnych, piezoelektryków;
3) systemy zakopywane, w postaci czujników sejsmicznych, hydraulicznych, kabli światłowodowych, magnetycznych (pasywnych) czy parametrycznych (aktywnych).

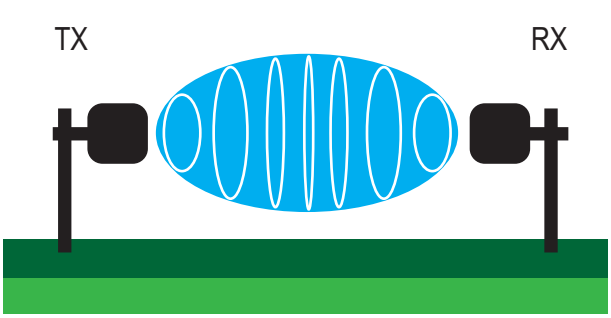
W ochronie obwodowej szczególną rolę odgrywają **bariery mikrofalowe**, czyli czujniki bistatyczne (RX i TX umieszczone naprzeciw siebie), z przestrzenną strefą detekcji.

Urządzenia te instaluje się „na zakładkę" (następna bariera osłania martwą strefę przy nadajniku lub odbiorniku). Bariery pracujące w paśmie X pozwalają na znaczne ograniczenie wielkości owych zakładek, w przeciwieństwie do urządzeń pracujących w mniej korzystnym paśmie K. Długość tzw. martwej strefy w pobliżu barier pracujących w paśmie X wynosi średnio od trzech do pięciu metrów, w zależności od odległości urządzenia od ziemi, zasięgu działania, ustawionej czułości i typu anteny. W barierach wykorzystujących pasmo K należy wziąć pod uwagę, że na konieczne zakładki potrzebujemy znacznie więcej miejsca, zazwyczaj około siedmiu metrów. Ponadto bariery pracujące w paśmie K są częściej narażone na interferencje innych urządzeń, na przykład radarów stosowanych na lotniskach lub w obiektach wojskowych. Nierzadko bowiem inne systemy wykorzystują właśnie to pasmo.

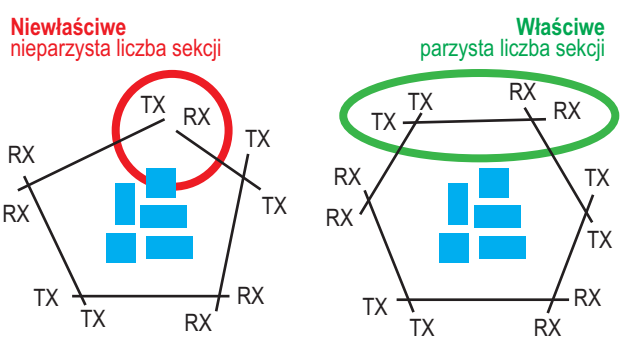
W założeniach projektowych należy uwzględnić parzystą liczbę stref detekcji (zob. rysunek) celem uniknięcia zakłóceń oraz zadbać o dobór takich urządzeń, które posiadają sporą liczbę kanałów pracy o różnych częstotliwościach.

Obecny standard to 16 kanałów pracy do wyboru. Większa liczba dostępnych kanałów modulacji przyczynia się zarówno do zwiększenia odporności na sabotaż, jak i do wyeliminowania ewentualnego wzajemnego zakłócania się barier pracujących na tym samym obiekcie. Aby wyeliminować wzajemne zakłócanie się sąsiadujących ze sobą sekcji układu, preferowana jest instalacja dwóch tych samych modułów bariery obok siebie (RX i RX lub TX i TX). Taki układ jest możliwy dzięki parzystej liczbie stref detekcji, co obrazuje rysunek nr 2. Jeżeli nie ma możliwości zastosowania parzystej liczby stref i w jednym z narożników musimy ustawić przy sobie RX i TX, najlepszym rozwiązaniem jest zmiana polaryzacji w jednej z tych sekcji. Należy jednak pamiętać, że zmiana polaryzacji dotyczy całego kompletu bariery – zarówno nadajnika, jak i odbiornika.

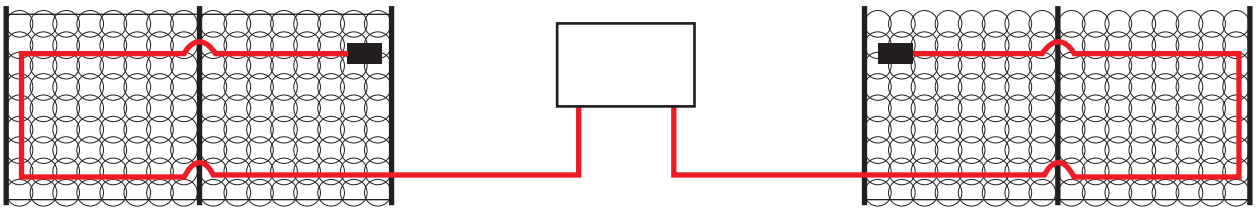
Wysokiej jakości, nowoczesne cyfrowe bariery mikrofalowe są bardzo inteligentne. Mają możliwość porównywania sygnału odebranego z nadzorowanej strefy z zapisanymi parametrami charakteryzującymi typowe wtargnięcie intruza, takimi jak: wielkość, kształt, tempo i sposób poruszania się (próby czołgania, przebiegania etc.). Ponadto we wspomnianych urządzeniach istnieje możliwość odrębnej regulacji czułości jedynie bocznej wstęgi, odległej od centrum strefy detekcji. Dzięki temu urządzenia te są w stanie ignorować zakłócenia pojawiające się na krawędziach strefy, co jest szczególnie pomocne, gdy w pobliżu znajduje się niezbyt stabilne metalowe ogrodzenie, wysoka mokra roślinność, ruchliwa droga lub zbiornik z wodą. Dodatkowo przy barierach, które mają wykryć intruza, najlepiej stosować antenę paraboliczną z polaryzacją liniową (zamiast anteny planarnej z polaryzacją kołową), dzięki której sygnał jest o wiele czystszy, a przy zmianie położenia promiennika o 90° – i tym samym zmianie polaryzacji z poziomej na pionową lub odwrotnie – możemy zmniejszyć część zakłóceń. Bez wątpienia stosowane urządzenia powinny posiadać czujnik sabotażu sygnalizujący demontaż bądź zmianę położenia bariery oraz galwaniczną izolację obwodów, możliwość zdalnej kalibracji i korekcji parametrów, podgląd sygnałów bieżących i archiwalnych. Ogromną zaletą barier



Rys. 1. Strefa detekcji bariery mikrofalowej



Rys. 2. Należy uwzględnić parzystą liczbę stref detekcji



Rys. 3. Przykład instalacji systemu na ogrodzeniu

mikrofalowych jest to, że nie reagują na zakłócenia atmosferyczne, takie jak mgła czy opady. Inaczej jest w przypadku niezwykle czułych **barier podczerwieni** z liniową strefą detekcji (których zwolenniczką nie jestem).

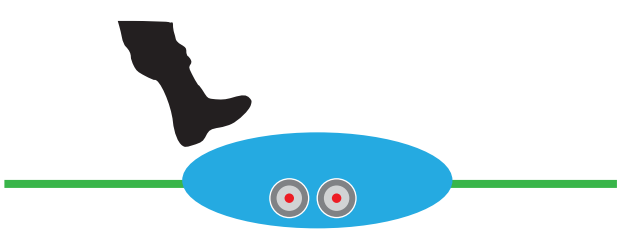
Popularnym rozwiązaniem są również **czujki dualne** (PIR+MW), które doskonale wypełniają martwą strefę, jeżeli zostaną zamontowane na przewidywanej drodze intruza, który będzie się zbliżać do czujki lub od niej oddalać.

Kolejne rozwiązanie to systemy bazujące na **czujkach wibracyjnych**. Analizując je, należy podkreślić, że ogrodzenie, na którym są zainstalowane, musi być stabilne, dobrej jakości, najlepiej nie pokryte tworzywem sztucznym. Czujki te reagują na próbę przejścia ogrodzenia lub jego naruszenia. Na ogrodzeniach wyższych niż dwumetrowe należy stosować więcej niż jedną czujkę. W moim odczuciu rozwiązanie to jest stosunkowo tanie, szczególnie w przypadku rozległych obiektów, jednak technologicznie dość przestarzałe, a ponadto informacja o miejscu naruszeniu strefy dozorowania jest mało precyzyjna i często niewystarczająca. Toteż skuteczniejszym i bardziej uniwersalnym rozwiązaniem jest **system z kablem mikrofonowym montowanym na ogrodzeniu**, a także na **dachu lub ścianie**. Jest on wrażliwy na hałas wywoływany przy próbie naruszenia chronionego obszaru przez intruza – wspinaniu, przedzieraniu się, uszkodzeniu. Przeznaczony jest do instalacji wewnątrz lub na zewnątrz obiektów. System może wyodrębnić niezależne strefy detekcji, posiada również aktywne złącze RS232.

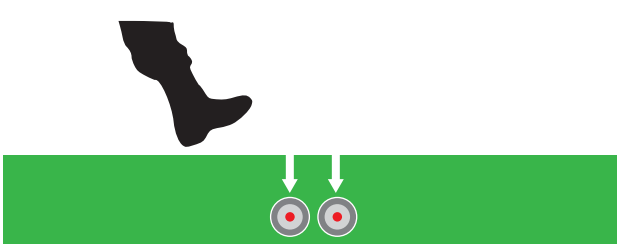
Czujki liniowe, umieszczane pod ziemią, chodnikiem, kostką brukową, betonem, trawą, żwirem, piaskiem lub innego rodzaju podłożem, zwane są **kablami sensorycznymi** lub **parametrycznymi**. Generują sygnał alarmu, gdy pojawienie się intruza w przestrzennej strefie detekcji wywołuje zmianę pola elektromagnetycznego. Integralne części takiego systemu to sterownik oraz kable: nadawczy i odbiorczy, obecnie często umieszczane we wspólnej oponie, co znacznie ogranicza ilość prac związanych z ich instalacją oraz pozwala zawęzić strefę detekcji nawet do dwóch metrów szerokości. Rozwiązanie to nie należy do najtańszych, dlatego niezwykle ważna jest jakość sprzętu, jego możliwości, niezawodność i nowoczesność. Przy jego wyborze warto zwrócić uwagę, czy ma możliwość:

– zdalnej regulacji i zmiany parametrów pracy,
– dezaktywacji dowolnego odcinka,
– automatycznej kalibracji czułości każdego metra niezależnie od zróżnicowanego podłoża, pod którym przechodzi kabel (zapewnia nam to możliwość płynnego przejścia na przykład ze strefy pod trawą do strefy pod kostką brukową),
– lokalizacji miejsca naruszenia strefy do kilku metrów,
– elastycznego wyznaczenia stref detekcji niezależnie od fizycznego rozmieszczenia urządzeń.

W przypadku systemów zakopywanych często jednak poszukujemy rozwiązań bez przestrzennej strefy detekcji, głównie ze względu na ograniczenia terenowe czy warunki środowiskowe. Wówczas idealnym rozwiązaniem są mechaniczne **systemy hydrauliczne**, oparte na różnicach ciśnień wywoływanych przez ruchy intruza (nacisk na grunt). Dwie gumowe rurki wypełnione pod ciśnieniem specjalnym płynem, zakopane na głębokości około 25 cm (w zależności od rodzaju podłoża) w odstępach około 1,3 m, łączą się z zaworem kompensacyjnym i sensorem. Przechodzący intruz wywołuje różnicę ciśnień w pobliżu rurek, a tym samym wywołuje przesunięcie membrany sensora prowadzące ostatecznie do alarmu. Systemy hydrauliczne posiadają również przetworniki, umożliwiające monitorowanie kilku odrębnych stref. Najnowsze wersje są dodatkowo wyposażone w cyfrowy procesor analizujący sygnały w dziedzinie czasu i częstotliwości, określający miejsce przejścia intruza z dokładnością do kilku metrów, a także eliminujący fałszywe alarmy poprzez rozróżnienie standardowych szumów od rzeczywistego naruszenia strefy. W zewnętrznych barierach mikrofalowych transmitowany sygnał jest bowiem narażony na zniekształcenia generowane przez dookolne, nakładające się na niego szumy. Toteż wybierając urządzenie, warto zwrócić uwagę, czy posiada funkcję analizy odbieranego sygnału pod kątem optymalizacji wartości współczynnika stosunku sygnału do szumu (tzw. *Signal to Noise Ratio* – SNR). Warto również podkreślić przy tej okazji, że otrzymywany sygnał jest zdecydowanie czystszy przy polaryzacji liniowej niż przy kołowej. Polaryzacja kołowa jest raczej zalecana do rozłożystych radiolinii o rozległym zasięgu.



Rys. 4. Przestrzenna strefa detekcji nad zakopywanym kablem parametrycznym



Rys. 5. System ciśnieniowy reagujący na nacisk intruza na grunt

Doskonałym rozwiązaniem jest też **podwójny system hydrauliczno-parametryczny**, wykrywający zarówno nacisk intruza na grunt, jak i naruszenie przestrzennej strefy detekcji. Osobiście nakłaniam inwestorów do stosowania systemów zakopywanych, gdyż mają wiele zalet. Przede wszystkim są wydajne przez cały rok, mimo zmiennych warunków atmosferycznych. Są także niezależne od rodzaju podłoża, który ma wpływ jedynie na głębokość zakopania kabli czy gumowych rurek i ustawienie odpowiednich parametrów pracy. Ponadto są całkowicie niewidoczne dla potencjalnego intruza, co stanowi dodatkowy atut w walce z przestępczością. Wkopane tuż przy ogrodzeniu natychmiast zasygnalizują wtargnięcie nieproszonych gości do obiektu. Dzięki cichemu alarmowi mamy czas na podjęcie odpowiednich działań, natomiast głośny alarm z pewnością zadziała odstraszająco.

W przypadku rozległego obszaru lub obiektu podwyższonego ryzyka warto rozważyć zastosowanie podwójnego systemu elektronicznej ochrony obwodowej. Zwiększy to prawdopodobieństwo wykrycia intruza, a tym samym skuteczność systemu. Należy jednak pamiętać, aby łączyć systemy wykorzystujące odmienne zjawiska fizyczne, czyli na przykład ciśnieniowy system zakopywany, wykrywający nacisk intruza na grunt, oraz bariery mikrofalowe z przestrzenną strefą detekcji lub system mikrofonowy na ogrodzenie i kabel sensoryczny. Dodatkowe zastosowanie systemu nadzoru wizyjnego pozwoli zobaczyć ewentualne naruszenie strefy, a tym samym weryfikować wywołany alarm.

Co najmniej dwa niezależne urządzenia lub systemy alarmowe działające w oparciu o różne zjawiska fizyczne należy stosować – zgodnie z Normą Obronną – w strefie zewnętrznej obwodowej obiektów wojskowych I kategorii (takich jak stanowiska dowodzenia szczebla strategicznego i operacyjnego, stanowiska dowodzenia i naprowadzania Sił Powietrznych, baz, składnic oraz składów amunicji, uzbrojenia, materiałów wybuchowych, bomb, rakiet, granatów, torped itp.). Można zastosować na przykład system naziemny i ogrodzeniowy, system ogrodzeniowy i podziemny, system naziemny i podziemny lub dwa systemy naziemne[1].

Panuje przekonanie, że systemy zewnętrzne oddziałują psychologicznie na potencjalnego intruza. Zabezpieczenia elektroniczne widoczne z zewnątrz obiektu – montowane na powierzchni ziemi lub ogrodzeniu – skutecznie odstraszają, natomiast zakopywane (niewidoczne) są dla intruza źródłem zaskoczenia, w efekcie czego zazwyczaj podejmuje on próbę ucieczki. Nieocenione bywają również widoczne rozwiązania mechaniczne, takie jak na przykład zasieki ostrzowe, które zniechęcają do prób wdarcia się na posesję bądź skutecznie je utrudniają. Często jednak ranga obiektu lub aspekty wizualne nie przemawiają za tą formą zabezpieczenia.

Koszmarem niemal każdego użytkownika systemów alarmowych, szczególnie tych źle zainstalowanych, błędnie skonfigurowanych czy niewłaściwie konserwowanych, są tak zwane fałszywe alarmy, czyli takie sygnały o naruszeniu strefy detekcji, które nie zostały wywołane faktycznym wtargnięciem intruza w chroniony obszar. Zjawisko to szczególnie zniechęca użytkowników do eksploatacji systemów zewnętrznych, a co gorsza, z czasem osłabia czujność. Zazwyczaj jednak okazuje się, że te „fałszywe" alarmy generowane są najczęściej na skutek braku wiedzy lub świadomości użytkowników, zaniedbania i beztroski. Niekiedy (o, zgrozo!) ich przyczyną jest montaż urządzeń wykonywany przez osoby z przypadku, tak zwane „złote rączki". Daje to niezwykle krótkotrwałą oszczędność. Pamiętam zabawną sytuację, gdy w obiekcie, w którym zainstalowane zostały zewnętrzne bariery mikrofalowe, imponującej wręcz jakości, użytkownik otrzymywał nieprawdopodobnie wiele alarmów, jak twierdził, fałszywych. Wizja lokalna pozwoliła niezwykle szybko zweryfikować przyczynę owej sytuacji. Bistatyczne urządzenie składa się z dwóch elementów: nadajnika i odbiornika umieszczonych naprzeciw siebie. Bariera została zainstalowana bezpośrednio na ścianie budynku, gdzie znajdowały się również drzwi wejściowe. Właśnie za nimi pomysłowy instalator umieścił odbiornik urządzenia. Każda osoba wchodząca do budynku i wychodząca z niego była traktowana jak intruz wkraczający w strefę detekcji (co właściwie potwierdzało prawidłowe działanie urządzenia). W innych przypadkach sygnały nie pojawiały się w ogóle, gdyż przy kalibracji parametrów w trakcie uruchamiania systemu zewnętrznego czułość została niemalże całkowicie obniżona, podobno ze względu na sporą liczbę poruszających się w pobliżu wiewiórek i innych zwierzątek. Ku mojemu osłupieniu część systemu była zupełnie wyłączona, choć obiekt, w którym miał on funkcjonować, był narażony na duże ryzyko napadu.

Napotykając niestety liczne takie przypadki, uważam, że niezwykle istotną kwestią jest rozważenie kilku zagadnień

1) Na podstawie Normy Obronnej NO-04-A004-1:2010.

mających istotny wpływ na stworzenie prawidłowo funkcjonującego systemu ochrony obwodowej.

Najważniejsze jest indywidualne, staranne rozpoznanie potencjalnych zagrożeń, jakie mogą wystąpić w konkretnym obiekcie. Według tego kryterium można dopasować najwłaściwszy system zarówno pod względem jakościowo-funkcjonalnym, jak i kosztowym. Inaczej zabezpiecza się prywatny dom jednorodzinny, inaczej bank, lotnisko, obiekt wojskowy czy inny obiekt podwyższonego ryzyka. Należy pamiętać również o podstawach: stabilnym ogrodzeniu czy innych utrudnieniach mechanicznych, które znacznie utrudnią potencjalnemu intruzowi wtargnięcie do obiektu lub wręcz go zniechęcą do podejmowania takiej próby. Co więcej, po uruchomieniu systemu ochrony peryferyjnej należy przeszkolić służby ochrony oraz osoby odpowiedzialne za podtrzymanie systemu i jego konserwację. Sama instalacja powinna być wykonana przez wykwalifikowany zespół wyszkolonych, doświadczonych fachowców, a nie osoby trudniące się tym dorywczo.

Czujki pracujące na zewnątrz obiektów narażone są na liczne zakłócenia spowodowane czynnikami środowiskowymi czy atmosferycznymi. Mam tu na myśli wiatr, mgłę, mróz, opady śniegu czy deszczu, burzę, upał, a także zmiany oświetlenia, temperatury, zakłócenia ze strony systemów radarowych, bliskie otoczenie wody, zwierzęta poruszające się w strefie detekcji etc. Toteż siłą rzeczy urządzenia przeznaczone do ochrony peryferyjnej muszą być na nie odporne. Tymczasem obserwując wiele instalacji, odnoszę wrażenie, że warunek ten nie jest brany pod uwagę *a priori*.

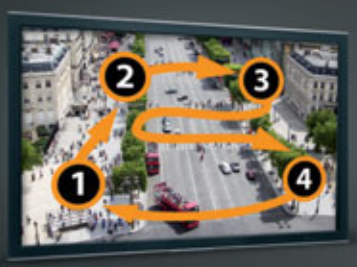
Obecnie dostrzegam ogromne różnice w jakości dostępnego na rynku sprzętu przeznaczonego do ochrony zewnętrznej. Większość urządzeń nie spełnia elementarnych wymogów. Są przestarzałe technologicznie lub stanowią nieudolne podróbki wyrobów renomowanych producentów, a ich jakość, trwałość i niezawodność pozostawiają wiele do życzenia. Jednak „sprzedawcy pudełek" niczym „sprzedawcy marzeń" przekonują usilnie swoich odbiorców – a w tym przypadku raczej swoje ofiary – do zakupu i instalacji tych „nowości", głównie ze względu na niezwykle przystępną cenę. Jestem przekonana, że dzisiejszy inwestor nie jest na ogół zupełnym laikiem w tej dziedzinie. W dobie Internetu, licznej konkurencji i wielkiej ilości łatwo dostępnych informacji przyczyną nietrafnych decyzji inwestycyjnych rzadko bywa całkowity brak wiedzy. Natomiast pośpiech w życiu codziennym i chęć zaoszczędzenia pieniędzy sprawiają, że rzadziej decydujemy się na bezpośredni kontakt ze sprzedawcą, rozmowę z nim, omówienie naszej sytuacji i prezentację produktu, a coraz częściej dokonujemy zakupów zdalnie, co akurat w tej branży nie jest wskazane. Życzyłabym sobie, aby dla każdego producenta i dystrybutora wyznacznikiem jakości i klasy działania systemu lub urządzenia był moment, w którym osiągnięty rezultat jest całkowicie zbieżny z oczekiwaniami klienta. Mimo że taka praca bywa niezwykle trudna, często wyczerpująca i stresująca, daje tym więcej satysfakcji, im więcej wysiłku w nią włożymy.

Karolina Zasada
specjalista ds. ochrony obwodowej obiektów, dystrybucji i marketingu
ZBAR Łódź

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Niewielkie rozmiary, olbrzymie możliwości! Nowa seria kamer szybkoobrotowych



Automatyzacja obserwacji

Automatyzacja procesu obserwacji jest w kamerach realizowana poprzez funkcje automatycznego skanowania, ujęć programowalnych, patroli oraz tras obserwacji. W kamerach CAMA-III mini można zaprogramować: 120 presetów, 4 trasy obserwacji (do 200 s), 4 patrole, 4 trasy automatycznego skanowania. Pozwala to na szybką, sprawną i częściowo zautomatyzowaną obserwację nadzorowanego obiektu.

Instalacja

Niewielkie rozmiary kamer umożliwiają ich montaż w wielu miejscach niedostępnych do tej pory dla standardowych kamer szybkoobrotowych. Kamery posiadają klasę szczelności IP66. Mogą być montowane za pomocą opcjonalnych uchwytów i adapterów do ściany, sufitu (w tym sufitu podwieszanego), masztu lub narożnika budynku. Kamera w wersji zewnętrznej może pracować w temperaturze do -30°C.

Moduł kamerowy

Zastosowanie dzienno-nocnego modułu kamerowego z 22-krotnym zoomem optycznym i 16-krotnym zoomem cyfrowym pozwala na obserwację oraz rozpoznanie szczegółów znacznie oddalonych obiektów z dużą dokładnością (ogniskowa f=3.9 ~ 85.8 mm), nawet przy słabym oświetleniu sceny.

CAMA-III mini seria

- 1/4" SONY ExView HAD CCD
- Mechaniczny filtr podczerwieni
- Rozdzielczość pozioma do 620 TVL
- Czułość: od 0.001 lx/F=1.6 (DSS)
- WDR - Szeroki zakres dynamiki
- DSS - Wydłużony czas ekspozycji
- Zoom optyczny: 22x
- Wbudowana grzałka (NVC-MSD322DN/O)

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

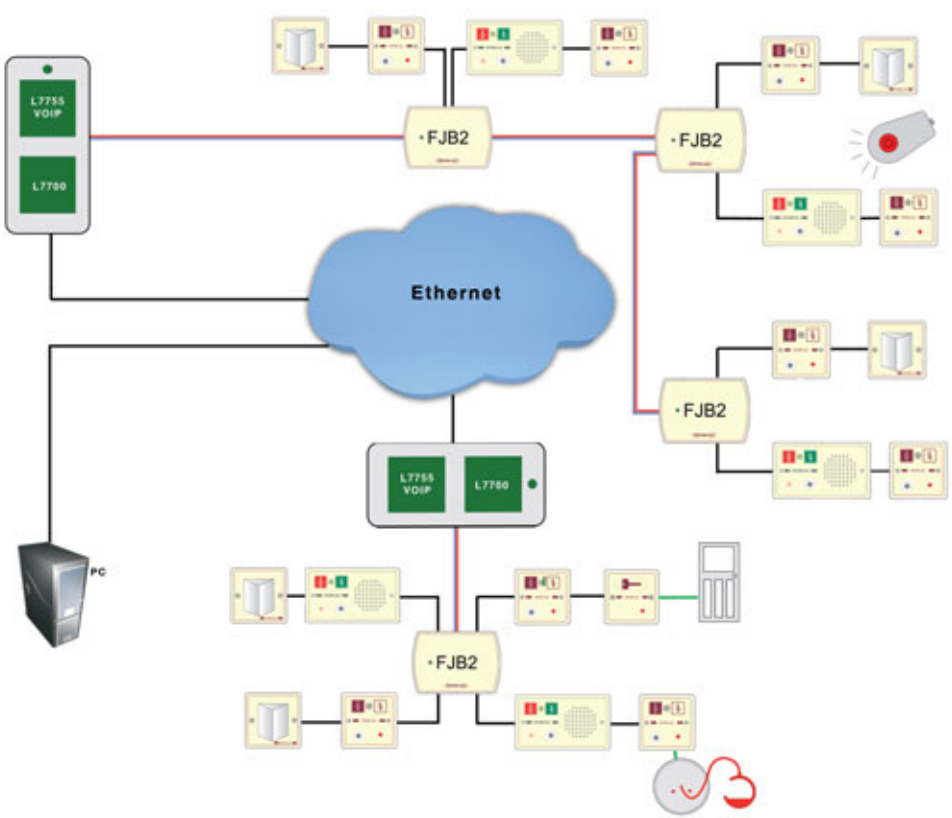
Intercall – szpitalny system przywoławczy

Prosty w instalacji – pomocny dla obsługi – zapewniający bezpieczeństwo pacjenta

Intercall jest najwyższej jakości systemem przywoławczym przeznaczonym dla specjalistycznych placówek opieki zdrowotnej (szpitale, domy opieki, hospicja itp.). Prosty w obsłudze i łatwy w rozbudowie, oferuje wyjątkowe funkcje: komunikację głosową (Intercall 700), rejestrację przywołań, przywołania o różnych priorytetach, czytelną i dokładną informację o rodzaju alarmu oraz miejscu wywołania.

Intercall zapewnia również maksymalnie uproszczony proces instalacji systemu, a dzięki 2-żyłowej magistrali (Intercall 600) pozwala na zastąpienie systemów starszej generacji, bez konieczności wymiany okablowania.

- Nieograniczone możliwości rozbudowy zarówno w zakresie punktów przywoławczych, jak i urządzeń sygnalizacyjnych
- Buforowanie oraz bieżący podgląd zdarzeń
- Dwukierunkowa komunikacja w trybie głośnomówiącym bez użycia słuchawek (Intercall 700)
- Definicja priorytetów zdarzeń alarmowych
- Możliwość bezpośrednich wydruków oraz powiadomienia na pager
- Szeroka gama punktów przywoławczych, w tym maty ciśnieniowe, czujniki moczenia, czujki ruchu, ręczne aktywatory ściskowe, ustne podmuchowe, łazienkowe oraz zdalne nadajniki podczerwieni
- Instalacja czterożyłowa (dwużyłowa przy systemie bez komunikacji głosowej)
- Bezpośrednie i zdalne konfigurowanie urządzeń za pomocą komputea PC



Dystrybucja: alarmnet®

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. (22) 663 40 85, faks (22) 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

Inteligentny Tester Akumulatorów GOLD-PLUS został zaprojektowany do testowania akumulatorów 6-voltowych o pojemności od 1,2 h do 12 Ah oraz 12-voltowych o pojemności od 1,2 Ah do 100 Ah. Zastosowana technologia symulacji pełnego rozładowania skraca normalny test rozładowania z 20 godzin do 20 sekund. Automatycznie wyświetla napięcie akumulatora i aktualną pojemność. Dzięki funkcji kalibracji testera możliwe jest testowanie szczelnych akumulatorów (SLA) wykonanych w technologii AGM, żelowych do pracy cyklicznej oraz akumulatorów samochodowych. Akumulatory można testować wielokrotnie bez przerw pomiędzy pomiarami. Wbudowana dioda LED ostrzega przed odwróceniem polaryzacji.

Wymiana akumulatora jest zalecana, jeżeli jego współczynnik pojemności spada poniżej 65%. Na obudowie umieszczona jest tabela referencyjna wskazująca, kiedy akumulator powinien zostać doładowany lub wymieniony.

Cechy charakterystyczne

- Testuje w ciągu 20 sekund 6- i 12-voltowe szczelne akumulatory (SLA) - AGM i żelowe oraz akumulatory samochodowe,
- automatycznie wyświetla napięcie akumulatora i aktualną pojemność,
- może być skalibrowany do testowania akumulatorów szczelnych, żelowych i samochodowych o pojemności od 1,2 Ah do 100 Ah,
- zabezpieczony przed odwróceniem polaryzacji,
- testuje akumulatory szybko, dokładnie i jest łatwy w użyciu,
- zastosowanie – akumulatory w systemach alarmowych, zasilaczach UPS, samochodach elektrycznych i spalinowych.

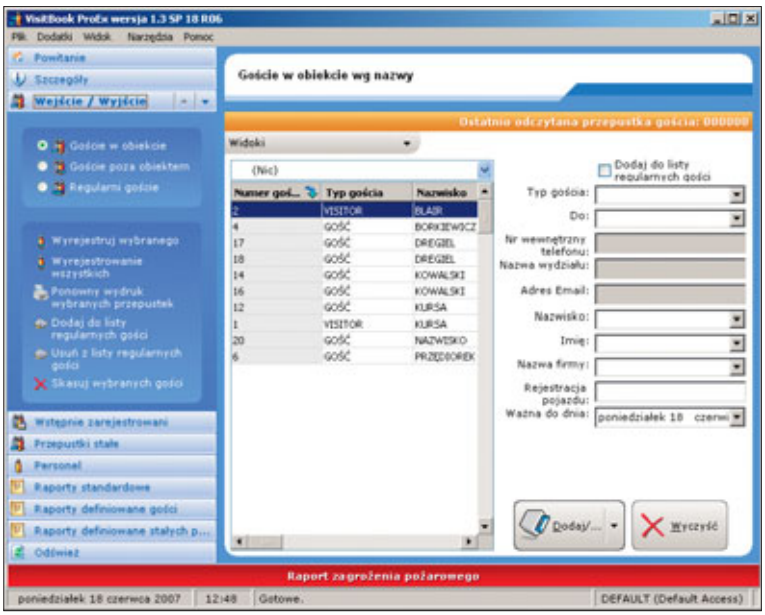
Parametry techniczne	
Model	GOLD- PLUS
Typy akumulatorów	szczelne (SLA) – AGM i żelowe samochodowe akumulatory obsługowe
Pojemność akumulatorów	6 V 1,2 Ah – 12 Ah oraz 12 V 1,2 Ah – 100 Ah
Impulsowe obciążenie akumulatora podczas pomiaru	6 A dla akumulatorów 1,2 Ah – 9,9 Ah, 18 A dla akumulatorów 10 Ah – 100 Ah
Kalibracja Ah	Kalibrowany w pozycji 0 dla nowego, w pełni naładowanego akumulatora SLA o temperaturze 20-25 °C. Regulacja kalibracji w zakresie 00-99 dla akumulatorów żelowych i samochodowych
Wyświetlacz	podświetlany LCD
Ostrzeżenie o odwróconej polaryzacji	czerwona dioda LED
Ostrzeżenie o zbyt niskim napięciu akumulatora	dla 6 V < 5,25 V_{DC}, dla 12 V < 12,0 V_{DC}
Tolerancja pomiaru Ah	+/- 10 % (zależy od konstrukcji i parametrów produkcyjnych)
Tolerancja pomiaru VDC	+/- 2 %
Zabezpieczenie odwrócenia polaryzacji	tak
Zdolność wykonania kolejnych testów	natychmiastowa
Obudowa	ABS
Szczelność	IP54
Wymiary	210 mm × 110 mm × 41 mm
Masa	600 g (w opakowaniu)
Wyposażenie	Przewody testowe, futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

Dystrybucja: alarmnet®

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. (22) 663 40 85, faks (22) 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

System rejestracji gości VisitBook



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

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

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

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

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

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

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

Dystrybucja:

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

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

Pronto – Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

Mała, kompaktowa drukarka o nowoczesnym wyglądzie do zastosowania w każdej firmie i w każdym miejscu. Do szybkiego drukowania identyfikatorów oraz różnego rodzaju kart plastikowych. Drukarka Pronto jest łatwa w konfiguracji i użytkowaniu, posiada instrukcję i sterowniki w języku polskim do Windows 2000, XP, Vista, 7 i zapewnia niezawodne drukowanie kart przez wiele lat. Drukarka Magicard Pronto umożliwia wykorzystanie HoloKote i HoloPatch – opatentowanych zabezpieczeń przed nieautoryzowanym kopiowaniem kart.

Dzięki drukarce Pronto możesz samodzielnie wykonać kolorowe i monochromatyczne nadruki wysokiej jakości.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
- Monochromatyczny wydruk karty w 7 sekund
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1. (kompatybilny z USB 2.0)
- Sterowniki w języku polskim: Windows 2000, XP, Vista, 7
- Rozdzielczość wydruku: 300 dpi
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 270 mm × 215 mm × 233 mm / 4,4 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

Taśmy

- YMCKO 5 paneli nadruk 300 kart (MA300YMCKO)
- YMCKO 5 paneli nadruk 100 kart (MA100YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna zielona nadruk 1000 kart (MA1000K-GREEN)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 × 54) oraz CR-79 (84,1 × 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch i kartach do wielokrotnego zadruku TRW.

Zestaw czyszczący

- 1 szt. rolki czyszczącej dostarczanej z każdą taśmą
- 10 szt. kart czyszczących, 1 flamaster (CK1)
- 5 wałków czyszczących plus wymienna oś wałka

Dystrybucja:

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

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

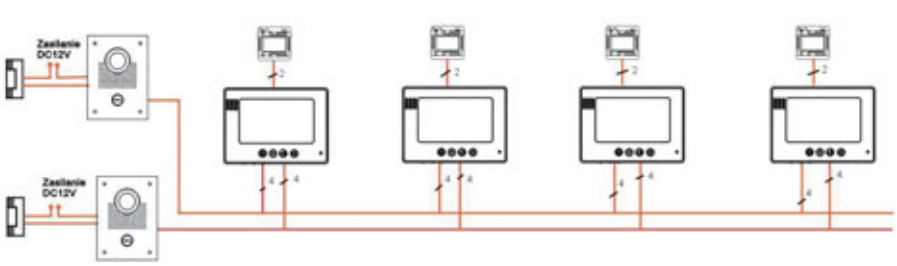
Kolorowy monitor wideodomofonowy MT670C-CK2

Monitor wideodomofonowy MT670C-CK2 firmy Competition to nowoczesna konstrukcja urządzenia spełniająca wymagania najbardziej wymagających klientów, charakteryzuje się unikatowym wzornictwem i różnorodnymi możliwościami rozbudowy. Wyposażony jest w dotykowe przyciski funkcyjne oraz siedmiocalowy kolorowy panoramiczny wyświetlacz TFT LCD.

Monitor przeznaczony jest do użytku w domach jedno lub kilkurodzinnych (do 8 użytkowników), zapewnia pełną regulację parametrów takich jak: głośność, jasność i kolor. Urządzenie umożliwia obsługę dwóch wejść, dzięki czemu możliwy jest kontakt audiowizualny np. z dwoma furtkami i sterowanie elektrozamkiem. Alternatywnie możliwe jest podłączenie zamiast drugiej stacji bramowej, kamery CCTV.

Zestaw wideodomofonowy może być rozbudowany o dodatkowe 3 monitory z serii CK2 lub unifony w pełni zaspokajając potrzeby indywidualnego użytkownika. Funkcja podglądu zapewnia możliwość obejrzenia obszaru w polu widzenia kamery stacji bramowej, jak również obrazu z dołączonej zewnętrznej kamery CCTV. Dzięki takiemu rozwiązaniu otrzymujemy stworzony niskim kosztem prywatny mini-monitoring.

Dane techniczne	
Zasilanie	14,5 V_{DC}
Pobór prądu	300 mA
Ekran	kolorowy 7" LCD TFT
Sygnał wideo	PAL / NTSC
Wymiary	160×240×25 mm



Dystrybutor:

Firma Handlowa Wena
Al. Prymasa Tysiąclecia 66
01-424 Warszawa

tel. (22) 817 40 08 tel./faks: (22) 837 02 86
e-mail: wena@wena.biz
http://www.wena.biz

Stacja bramowa wideodomofonowa z serii CK


SAC5C-CK


SAC35C-CK


SAC50C-CK


SAC551C-CK


SAC551C-CK(8)


SAC561C-CK

Stacja bramowa z serii CK współpracuje z 4-przewodowymi monitorami z serii CK2, wyposażona jest w kolorową kamerę z przetwornikiem 1/3" CCD, oraz oświetlacz LED, dzięki czemu możliwe jest rozpoznanie osób także w nocy. Również korzystanie z klawiatury w nocy jest możliwe dzięki podświetleniu każdego znaku na klawiaturze.

Obiektyw kamery można regulować w pionie i poziomie, co umożliwia dostosowanie stacji do naszych indywidualnych oczekiwań. Obudowy wszystkich stacji są wykonane z metalu i są odporne na akty wandalizmu.

Stacja SAC50C-CK i SAC551C-CK ma wbudowany szyfrator, umożliwiający otwarcie drzwi za pomocą indywidualnego kodu PIN zamiast tradycyjnego klucza. Jest to bardzo wygodne rozwiązanie szczególnie w zimie, gdy nie musimy „wydobywać" kluczy z kieszeni. Stacja posiada także opcję otwierania drzwi ze środka posesji za pomocą zwykłego włącznika. W tym przypadku nie ma konieczności montowania naciskanej klamki do otwierania drzwi. Urządzenie umożliwia sterowanie czasem zwolnienia elektrozaczepu. Podtrzymanie czasowe można ustawić w przedziale od 1 aż do 99 sekund.

	SAC5C-CK	SAC35C-CK	SAC50C-CK	SAC551C-CK	SAC551C-CK(8)	SAC561C-CK
Zasilanie	12V DC					
Przetwornik obrazu	1/3" CCD					
Minimalne oświetlenie	0.05 lx					
Kąt obiektywu	80°					
Podświetlenie	LED światło białe					
Montaż	Natynkowy			Podtynkowy		
Obudowa	Aluminium			Stal nierdzewna		
Wbudowany szyfrator	Nie	Nie	Tak	Nie	Nie	Tak
Wymiary (mm)	58×135×39	97×130×43	78×185×60	150×203×43	150×355×43	120×250×43

Dystrybutor:
wena
Firma Handlowa Wena
Al. Prymasa Tysiąclecia 66
01-424 Warszawa
tel. (22) 817 40 08 tel./faks: (22) 837 02 86
e-mail: wena@wena.biz
http://www.wena.biz

Radiotelefony PMR
rozwiązania komunikacyjne dla instalatorów

PMR-505TX

PMR-121TX

PMR TXL-446

PMR TX-1446P

Radiotelefony typu PMR pozwalają komunikować się ze wszystkimi tego typu urządzeniami pracującymi w ogólnodostępnym paśmie 446MHz. Mogą być one wykorzystywane we wszystkich krajach, gdzie zakres ten został dopuszczony do eksploatacji. Wszystkie modele radiotelefonów PMR marki TTI mogą być użytkowane zarówno przez firmy jak i osoby prywatne. Nie jest przy tym wymagane wnoszenie jakichkolwiek opłat za użytkowanie częstotliwości, a same radiotelefony nie podlegają rejestracji. Ilość radiotelefonów pracujących jednocześnie nie jest limitowana. Każdy z radiotelefonów typu PMR446 posiada minimum 8 kanałów roboczych i 38 kodów selektywnego wywołania CTCSS, co pozwala na pracę bez zakłóceń ze strony innych użytkowników i sprawną organizację sieci łączności. Moc 0,5 W jest wystarczająca do prowadzenia rozmów w zasięgu do 3 km (zależnie od ukształtowania terenu). W ofercie znajduje się kilka modeli radiotelefonów – od prostych kompletów do amatorskiej łączności do bardziej zaawansowanych przeznaczonych dla wymagających instalatorów.

PMR TX-1446P

Konstrukcja jak i funkcje klasyfikują ten model w górnej półce tego typu sprzętu. Inteligentna ładowarka stołowa przedłuża czas użytkowania akumulatora. Standardowy akumulator litowo-jonowy 1000 mAh pozwala na 16 godzin pracy. Za pomocą przejrzystego menu można w prosty sposób dostosować radiotelefon do własnych potrzeb. Radiotelefon z akumulatorem mieści się w niewielkich rozmiarów obudowie ważącej tylko 185 g.

W zestawie:

- Radiotelefon
- Antena
- Ładowarka stołowa
- Akumulator
- Pokrowiec do paska

Parametry:

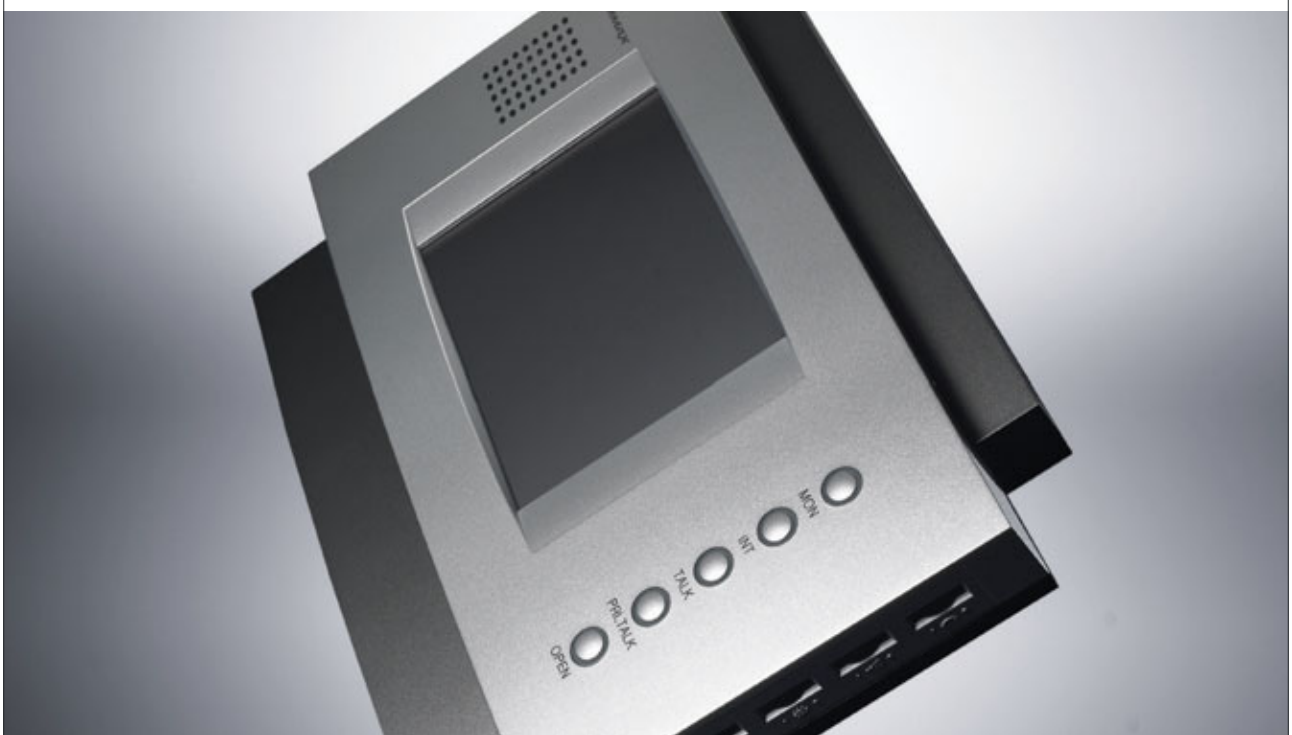
- Moc 0,5 W (wersja eksportowa 4 W)
- Zasięg do 5 km
- Ogólnodostępne pasmo 446 MHz
- 8 kanałów
- 50 kodów CTCSS / 104 kody DCS
- Automatyczne nadawanie/odbieranie VOX
- Funkcja Dual Watch
- Funkcja przeszukiwania SCAN
- Regulowany poziom głośności
- Podświetlany wyświetlacz LCD
- Funkcja klonowania ustawień
- Zasilanie – Akumulator 7,4V Li-Ion 1000 mAh
- Wymiary: 98x63x31 (bez anteny)
- Masa: 185 g

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

Monitor wideodomofonowy CDV-51AM



Monitor COMMAX CDV-51AM to następca modelu CDV-50AM w grupie analogowych systemów wideodomofonowych. Przeznaczony jest do użytku w domach jedno- lub kilkurodzinnych. Ze względu na zastosowanie wysokiej jakości 5-calowego wyświetlacza LCD wyróżnia się bardzo dobrą jakością wyświetlanego obrazu. Menu monitora zaczerpnięte zostało z większego odpowiednika - monitora CDV-71AM. Monitor obsługuje dwa panele wejściowe dzięki czemu możliwy jest kontakt audiowizualny np. z dwoma furtkami (wraz z funkcją otwarcia obu wejść). Zestaw wideodomofonowy może być rozbudowany o dodatkowe monitory z serii CDV-xxx oraz unifony DP-4VH (dostępne w pięciu wersjach kolorystycznych) z funkcją interkomu wewnątrz budynku. Monitor wyposażony jest w moduł pamięci umożliwiający zapis do 128 obrazów (automatycznie lub ręcznie) wraz z datą i godziną. Umożliwia to dodatkową kontrolę odwiedzających (np. podczas nieobecności domowników). Monitor współpracuje z dowolnym panelem wejściowym w systemie 4-żyłowym, dzięki czemu można skonfigurować odpowiedni zestaw dla własnych wymagań. Ponad 40-letnie doświadczenie firmy COMMAX w projektowaniu elementów systemów wideodomofonowych pozwala cieszyć się użytkownikowi doskonałą jakością i bezawaryjną pracą przez długi czas.

Właściwości:

- monitor kolorowy
- wyświetlacz 5" Color TFT-LCD 16:9
- standard sygnału wideo PAL/NTSC
- obsługuje dwa wejścia (dwa panele wejściowe)
- wbudowany moduł pamięci 128 obrazów
- możliwość podłączenia dodatkowego monitora
- współpraca z unifonami DP-4VR, DP-4VH
- komunikacja pomiędzy stacjami
- instalacja czteroprzewodowa + obwód elektrozamka
- współpracuje z kamerami analogowymi czteroprzewodowymi
- zasilanie 230 V
- wymiary: 245x175x45 mm

Dystrybucja:

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

Oprogramowanie klienckie HDxViewer oraz CMS

Program HDxViewer dostarczany jest wraz z rejestratorami firmy CNB, a program CMS wraz z kamerami IP. Oba programy mają taki sam interface oraz takie same możliwości funkcjonalne, jedyna różnica to brak możliwości łączenia się z kamerami IP w HDxViewer. Oba programy są integralną częścią urządzeń.

Kluczowe cechy:

- podgląd do 128 kamer
- obsługa dwóch monitorów
- konwersja nagrań do pliku .AVI
- pełne zarządzanie rejestratorem przez sieć
- możliwość nagrywania
- przeglądanie nagrań zarówno lokalnych jak i zapisanych na dyskach rejestratora
- rozbudowane możliwości przeszukiwania nagrań w tym po zdarzeniach alarmowych (np. ruch) oraz po czasie
- dwukierunkowa komunikacja głosowa między klientem sieciowym a rejestratorem
- wielopoziomowa, hierarchiczna E-mapa
- dodatkowe okna do alarmowego podglądu wybranych kamer wraz z możliwością szybkiego nagrywanie w formacie AVI

Pełna możliwość pracy w sieci oznacza że całość czynności związanych z obsługa rejestratora można dokonać zdalnie. Zaletą jest możliwość zdefiniowania wielu użytkowników o definiowanych prawach dostępu do funkcji systemu.

Program HDxViewer umożliwia połączenie z rejestratorami CNB, natomiast CMS z kamerami IP oraz rejestratorami. Podobnie jak w typowych NVR możliwe jest nagrywanie zarówno z kamer jak i z DVR wielokanałowych.

Program pozwala na obserwację obrazów ze 128 kamer. Dzięki funkcji **Dual Monitor** możliwy jest podgląd 128 równocześnie w układzie 64 kamery + 64 kamery z 16 różnych rejestratorów.

Dual monitor pozwala na pracę dwumonitorową – możemy definiować na którym monitorze pojawi się główne okno programu, okno wyszukiwania nagrań, okno przeszukiwania zdarzeń oraz E-mapa. Takie rozwiązanie umożliwia wygodne zaaranżowanie stanowiska operatorskiego.

Najczęściej na monitorze głównym wyświetlane jest okno główne z podglądem wszystkich kamer, natomiast na monitorze pomocniczym wyświetlamy E-mapę oraz okno wyszukiwania nagrań. E-mapa pozwala na hierarchiczną organizację monitorowanych miejsc oraz na szybki pogląd wybranych kamer.

W obrębie okna głównego możemy przeciągać kamery między oknami, np. ważniejsze kamery umieszczamy w większych polach.

Większość kart graficznych posiada dwa porty DVI-I umożliwiając podłączenie dwóch monitorów. Przy podłączonym jednym monitorze wszystkie okna są wyświetlane na jednym monitorze.

Istnieje możliwość nazwania presetów. Np. kiedy na E-mapie zaobserwujemy ruch na kamerach skierowanych na drogę możemy od razu wywołać wszystkie kamery obserwujące drogę.

CNB TECHNOLOGY Inc.

Zdefiniowany widok może zawierać kamery z różnych urządzeń, w tym kamery z różnych DVR'ów. To, wraz funkcją E-mapy, ułatwia skojarzenie operatorowi systemu gdzie jest dana kamera i jaki obszar obserwuje. Dodatkowo możemy włączyć sekwencyjne wyświetlanie wszystkich presetów, wtedy operator może kolejno obserwować krytyczne obszary w jednym widoku.

Poza sekwencyjnym podglądem obrazów w rożnych trybach podziału, można włączyć sekwencję pełnoekranowych podglądów z kamer.

Wybór widoku polega na wybraniu podziału jaki będziemy obserwować oraz kamer do obserwacji. Stosowanie do potrzeb możemy także rozmieszczać kamery na ekranie, np. kamerę obserwującą wejście do budynku możemy ulokować na większym polu niż pozostałe.

Dostępne jest również oprogramowanie klienta sieciowego dla urządzeń iPhone oraz wyposażonych w system Android.

Oprogramowanie HDxViewer obsługuje wszystkie rejestratory CNB serii HDS.

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 VCM-21VF

Kamera VCM-21VF to wandaloodporna kamera kopułowa o wysokiej czułości i rozdzielczości 600 TVL w trybie kolorowym oraz 650 TVL w trybie B/W, wyróżniająca się wiernym odwzorowaniem kolorów. Kolory są żywe i naturalne, a obraz ostry i wyraźny.

Kamera dedykowana jest do zastosowań wewnętrznych i zewnętrznych wymagających precyzyjnej regulacji pola widzenia.

Kamera posiada funkcję redukcji szumów DNR oraz funkcję kompensacji SBLC (kompensacja jasności zbyt ciemnego obiektu na jasnym tle, rozjaśnia obiekt nie zmieniając jasności tła dzięki czemu unikamy prześwietlenia całego obrazu). W kamerze zastosowano procesor DSP Monalisa.

Cenioną przez instalatorów funkcją jest możliwość zastosowania uchwytu WDB100, dzięki czemu możliwe jest wygodne i estetyczne zamocowanie kamery do ściany. Uchwyt wykonany jest jako solidny metalowy odlew z przepustem kablowym umożliwiającym ukrycie kabli i złączy.

Zaletami kamery są:

- wbudowany obiektyw o zmiennej ogniskowej 2,8÷10,5 mm z automatyczną przysłoną DC.
- dodatkowe serwisowe wyjście wideo
- regulacja położenia modułu kamery w 3 osiach: pion, poziom oraz obrót wokół własnej osi
- SBLC – ulepszona odmiana BLC
- mechaniczny filtr podczerwieni pozwalający na bardzo wierne odwzorowanie kolorów
- możliwość pracy w dzień i w nocy, praca z reflektorami podczerwieni

Kamerą podobną, lecz w plastikowej obudowie kopułkowej oraz bez odsuwanego mechanicznie filtru IR jest DBM-21VD.

Właściwości:

- kamera dzień/noc z mechanicznym filtrem podczerwieni
- przetwornik 1/3" Sony Super HAD II
- bardzo wysoka rozdzielczość 600 TVL oraz w trybie czarno-białym 650TVL
- czułość 0,05 lx (kolor), 0,005 lx (BW)
- obiektyw 2,8÷10,5 mm DC
- OSD
- regulacje jasności oraz koloru
- AGC, SBLC, AWB, DNR, Flickerless, D/N – regulacja przez OSD
- detekcja ruchu, strefy prywatności, funkcja mirror, wyostrzanie obrazu
- zasilanie 12 V_{DC}
- obudowa kopułkowa o średnicy 100 mm, pozwalająca na montaż podwieszany do sufitu oraz w suficie podwieszanym

Model	VCM-21VF
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD II
Rozdzielczość efektywna	752(H)×582(V) 440K
Liczba linii	600 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB
Obiektyw	f=2,8~10,5 mm
Tryb dzień/noc	mechaniczny filtr IR z czujnikiem
Czułość	0,05 lx (kolor), 0,005 lx (B/W)
Menu OSD	angielski, chiński
Cyfrowa redukcja szumu	3 poziomy / wył.
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	SBLC, 3 poziomy / wył.
Redukcja migotania	wł./wył.
Strefy prywatne	4 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Odbicie lustrzane obrazu	w poziomie
Elektroniczna migawka	1/50~1/120 000 s
Ręczna migawka	1/60, 1/250, 1/700, 1/1K, 1/1.6K, 1/2.5K, 1/5K, 1/7K, 1/10K, 1/30K, 1/60K, 1/120K
Stopień ochrony IP	IP65
Zasilanie	12 V_{DC}
Pobór prądu	maks. 180 mA
Wymiary (średnica×wys.)	montaż natynkowy: 100×124,5 mm montaż podtynkowy: 100×111 mm
Temperatura pracy / wilgotność	-10°C~45°C / 30%~80% RH
Masa	1210 g

Czytnik kart zbliżeniowych Mifare AV-G25 Helios

Doskonała jakość, bardzo wytrzymała konstrukcja, praca w każdych warunkach klimatycznych. Najwyższy poziom niezawodności w technologii zbliżeniowej.

Czytnik kart zbliżeniowych Mifare AV-G25 jest czytnikiem inteligentnych kart zbliżeniowych, pracującym w częstotliwości 13,56 MHz. Przeznaczony jest do stosowania w systemach kontroli dostępu, rejestracji czasu pracy, stołówkach i wszędzie tam, gdzie zachodzi potrzeba wykorzystania kart zbliżeniowych.

Czytnik Mifare AV-G25 charakteryzuje się ciekawym wzornictwem i kolorystyką (9 wersji kolorystycznych). Czytniki odczytują każdy rodzaj kart i tagów Mifare (standard, ultralight). Dzięki temu mogą stanowić alternatywę dla obecnie występujących produktów Mifare na naszym rynku.

Czytniki dostępne są w wykonaniu wewnętrznym lub zewnętrznym. Posiadają klawiaturę mechaniczną lub dotykową. Dostępna jest również opcja bez klawiatury. Dodatkowo każdy czytnik posiada wbudowany anty-sabotaż. Opcjonalnie urządzenia mogą być również wyposażone w kontroler, dzięki czemu mogą pracować jako pełny autonomiczny punkt dostępowy. Sygnalizacja stanów alarmowych odbywa się akustycznie i za pomocą kolorowych piktogramów.

Podstawowe cechy drukarki	
Napięcie zasilania	od 9 do 16 V_{DC}
Zasięg odczytu	do 10 cm
Częstotliwość pracy	13,56 MHz
Temperatura pracy	od –35°C do 75°C
Format wyjściowy	Wiegand 26/34, ABATRACK2, ASYNC 9600, N, 8,1
Obudowa (materiał)	poliwęglan UL94
Wymiary	12,50×8,9×3,0 cm
Kolor	czarny, szary, srebrny, niebieski, czerwony, pomarańczowy, biały, zielony, żółty
Instalacja	na każdym podłożu
Sygnalizacja	dioda trójkolorowa i brzęczyk
Transmisja	szyfrowana, klucz 64 bity
Kontrolery	Avanguard, SD-108, IKR, IKR108, SD-660, SD-560
Masa	249,5 g
Wilgotność	5% – 95% bez kondensacji
Pobór prądu	50 / 75 mA przy zasilaniu 12 V_{DC}
Wodoodporny	IP 54

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

chomtech.pl sp. z o.o.
ul. Mieszczańska 5
30-313 Kraków

tel. (12) 421 43 83, 428 12 00
faks (12) 350 40 69
http://www.chomtech.pl

Multimedialne monitory przemysłowe

Prezentujemy Państwu profesjonalną linię monitorów Full HD o przekątnej 17" – 82" wykonanych ze specjalnych podzespołów przeznaczonych do pracy ciągłej

Monitory mają możliwość programowania poprzez wbudowane porty oraz umożliwiają nadzór poprzez sieć LAN. Specjalistyczny wbudowany odtwarzacz multimedialny pozwala na odtwarzanie filmów reklamowych. Monitor posiada inteligentny panel do zarządzania, umożliwiający programowanie sekwencji filmowych według scenariusza przygotowanego przez użytkownika. Dzięki temu można zaprogramować harmonogram wyświetlania materiałów reklamowych. Monitor posiada dysk twardy o bardzo dużej pojemności, dzięki czemu może pracować również w trybie off-line, wyświetlając materiały w kolejności zaprogramowanej przez użytkownika.

Monitory posiadają obudowy wykonane ze stali oraz specjalnie utwardzane szyby o zwiększonej odporności na uszkodzenia mechaniczne. Mogą być używane jako monitory informacyjne w następujących typach lokalizacji: dworce kolejowe, lotniska, centra handlowe (również na zewnątrz), sale koncertowe, puby, fabryki lub stadiony.

Monitory występują również w wersji z bardzo cienką obudową - umożliwiającą budowę ścian wizyjnych, w których odległość pomiędzy sąsiadującymi wyświetlaczami jest minimalna (kilka mm). Osiągane przekątne to wielokrotność modułu podstawowego: 40" (lub większe).

Cechy produktu:

- stalowa obudowa ze specjalnie utwardzanym ekranem, bardzo odpornym na akty wandalizmu,
- wbudowany odtwarzacz multimedialny, pracujący z kartami CF i SD, zamykanymi na klucz w obudowie,
- port USB2.0 high-speed input do wgrywania nowych plików na karty pamięci,
- sygnały wejściowe VGA, YpbPr, HDMI i AV - możliwość zarządzania przez sieć LAN lub internet,
- możliwość zaprogramowania odtwarzania sygnałów z różnych źródeł według harmonogramu,
- możliwość zaprogramowania automatycznego włączania i wyłączania urządzenia,
- rozdzielczość high-definition,
- przekątna ekranu 17" – 82",
- czas pracy panelu ok. 60000 godzin.

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

chomtech.pl sp. z o.o.
ul. Mieszczańska 5
30-313 Kraków

tel. (12) 421 43 83, 428 12 00
faks (12) 350 40 69
http://www.chomtech.pl

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

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

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

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

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

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

ADT Fire and Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 83 01
faks (22) 430 83 02
e-mail: adtpoland@tycoint.com
www.adt.pl

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

ALARMNET 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:
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

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

ALPOL Sp. z o.o.
ul. Ks. F. Ścigały 10
40-208 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
faks (32) 790 76 60
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 65
faks (32) 790 76 85
e-mail: bydgoszcz@e-alpol.com.pl

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

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

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 46
faks (32) 790 76 73
e-mail: krakow@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. Wigury 21, 90-319 **Łódź**
tel. (32) 790 76 25
faks (32) 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. Kutrzeby 16G, 61-714 **Poznań**
tel. (32) 790 76 37
faks (32) 790 76 70
e-mail: poznan@e-alpol.com.pl

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

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

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

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

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

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. (71) 363 17 53, faks wew. 7
e-mail: anma@anma-pl.eu
www.anma-pl.eu

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

ATLine Sp. J.
Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. (42) 657 30 80
faks (42) 655 20 99
e-mail: info@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
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) 410 85 10
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 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
ul. Ogrodowa 2a
86-050 Solec Kujawski /k. Bydgoszczy
tel. (52) 387 36 58, 387 54 66, faks wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

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

Centrum Monitorowania Alarmów Sp. z o.o.
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) 340 0 209
faks (71) 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. (12) 260 13 96
tel. kom. (0) 665 380 677
faks (12) 260 13 95

ul. Palacza 127, 60-279 **Poznań**
tel./faks (61) 861 40 51
tel. kom. (0) 601 203 664
e-mail: poznan@cma.com.pl

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

CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U15
02-777 Warszawa
tel. (22) 855 00 17
faks (22) 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

Przedsiębiorstwo Usług Technicznych D-2 s.c.
K. Kolin, B. Czechowska
ul. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravis@dravis.pl, dravis.czechowska@gmail.com
www.dravis.pl

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

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

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

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

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

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

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

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

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

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

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

DPK System
ul. Piłsudskiego 41
32-020 Wieliczka
tel. (12) 288 14 26 , 288 23 75
faks (12) 278 48 91
e-mail: jablotron@jablotron.pl; biuro@dpksystem.pl
www.jablotron.pl

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

DYSKRET POLSKA Spółka z o.o. 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. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 518 84 00
faks (22) 812 62 12
e-mail: sales@ebs.pl
www.ebs.pl

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

EL-MONT
Adam Piotrowski
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

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

ELZA ELEKTROSYSTEMY
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 264 04 60
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl

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

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

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

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

Przedstawicielstwo we Wrocławiu
tel. kom. 0 693 195 009
e- mail: factor.wr@factor.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
Leszek Mitusiński
ul. Świątnicka 88
Włosań
32-031 Mogilany
tel. (12) 256 50 35
faks (12) 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. (91) 489 41 81
faks (91) 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

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

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

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

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

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

ISM EuroCenter S.A.
ul. Wyczółki 71
02-820 Warszawa
tel. (22) 548 92 40
faks (22) 548 92 82
e-mail: ism@ismeurocenter.com
www.ismeurocenter.com

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

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

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

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

P.P.H. PETROSIN Sp. z o.o.
ul. Rysi Stok 8/2
30-237 Kraków
tel. (12) 266 87 92
faks (12) 266 99 26
e-mail: office@petrosin.pl
www.petrosin.pl

Oddziały:
ul. Fabryczna 22, 32-540 **Trzebinia**
tel./faks (32) 618 02 00, 618 02 02

ul. Chemików 1, 32-600 **Oświęcim**
tel. (33) 847 30 83
faks (33) 847 29 52

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 324 89 00
faks (32) 324 89 01
e-mail: firma@kabe.pl
www.kabe.pl

NAPCO POLSKA
ul. Pszona 2
31-462 Kraków
tel. (12) 410 05 10, 410 05 11
faks (12) 412 13 12
e-mail: napco@napco.pl
www.napco.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

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV 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

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

RAMAR s.c.
U. Drogosz-Niemojewska, W. Niemojewska, M. Niemojewski
ul. Modlińska 237
03-120 Warszawa
tel./faks (22) 676 77 37, 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.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: poland@riscogroup.com
www.riscogroup.com

ROPAM Elektronik s.c.
Os. 1000-lecia 6A/1
32-400 Myślenice
tel. (12) 379 34 47
tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl

SATEL Sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
tel. (58) 320 94 00
faks (58) 320 94 01
e-mail: satel@satel.pl
www.satel.pl

SATIE
Czytniki dalekiego zasięgu
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 314 69 50
e-mail: info@satie.pl
www.satie.pl

SAWEL
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.pl

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Wołoska 9
02-583 Warszawa
tel. (22) 33 00 620 ÷ 623
faks (22) 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

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

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

ul. Mydlana 1, 51-520 **Wrocław**
tel./faks (71) 345 00 95
e-mail: wroclaw@schrack-seconet.pl

P.T.H. SECURAL
Jacek Giersz
ul. 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

S.M.A.
System Monitorowania Alarmów Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

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

SCHNEIDER ELECTRIC BUILDINGS POLSKA Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail:
SEPLBuildings.Poland@buildings.schneider-electric.com
www.schneider-electric.com/pl

ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. (58) 782 00 00
faks (58) 782 00 04

ul. Rysia 1A
53-656 **Wrocław**
tel. (71) 711 09 19
faks (71) 711 09 20

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

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 25 73
tel. kom. (0) 600 206 173
faks (22) 520 25 77
e-mail: marcin.witkowski@eu.sony.com
www.sonybiz.net

SPRINT Sp. z o.o.
ul. Jagiellończyka 26
10-062 Olsztyn
tel. (89) 522 11 00
faks (89) 522 11 25
e-mail: sprint@sprint.pl
www.sprint.pl

Oddziały:
ul. Przemysłowa 15, 85-758 **Bydgoszcz**
tel. (52) 365 01 01
faks (52) 365 01 11

ul. Budowlanych 64E, 80-298 **Gdańsk**
tel. (58) 340 77 00
faks (58) 340 77 01

ul. Heyki 27C, 70-631 **Szczecin**
tel. (91) 485 50 00
faks (91) 485 50 12

ul. Canaletta 4, 00-099 **Warszawa**
tel. (22) 826 62 77
faks (22) 827 61 21

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

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

ul. Kościuszki 227, 40-600 **Katowice**
tel. (32) 255 64 27
faks (32) 255 64 52
e-mail: katowice@spstrading.pl

ul. Drewnowska 48, 91-002 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl

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

ul. Grudziądzka 176, 87-100 **Toruń**
tel. (56) 653 99 43
faks (56) 653 90 81
e-mail: torun@spstrading.pl

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

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

SYSTEM 7
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
Infolinia 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.system7.pl
Internetowa Hurtownia Zabezpieczeń:
www.system7.biz

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: sprzedaz@tap.com.pl
www.tap.com.pl

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. (22) 843 83 95
faks (22) 843 79 12
e-mail: tap5@tap.com.pl

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

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (22) 516 97 97
faks (22) 516 97 91
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

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

W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. (52) 345 45 00
tel./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) 623 23 05
faks (61) 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	–	TAK	–	–
Alarmtech Polska	TAK	TAK	TAK	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	TAK	TAK	TAK
BOSCH	TAK	–	TAK	–	TAK
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	TAK	–	–	TAK
CBC Poland	TAK	TAK	TAK	–	TAK
CMA	–	–	–	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-2	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DANTOM	TAK	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	TAK	TAK
Dyskam	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
ela-compil	TAK	–	TAK	–	TAK
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	TAK	TAK	–
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	TAK	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
HSA	–	–	TAK	–	–

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	–
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	TAK	TAK	TAK	–
NAPCO	–	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	TAK
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	TAK	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	–	TAK	TAK	TAK
RISCO	TAK	–	TAK	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	TAK
SATIE	TAK	–	TAK	TAK	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	TAK	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	–	–	TAK	–	–
Sony	TAK	–	TAK	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	TAK	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	TAK	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	–	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
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	TAK	TAK	–	TAK	–	–	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	–	TAK	–	–	TAK	–	TAK	–	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	TAK	–	–
CMA	TAK	–	TAK	TAK	TAK	TAK	TAK	TAK	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	TAK	TAK	–	TAK	–	–	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EBS	TAK	–	TAK	–	–	–	–	–	–
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	–
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	TAK	TAK	TAK	–
HSA	TAK	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
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	–	–	–	–	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	–	TAK	–	–	–	–
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	konserwacja i serwis zabezpieczeń mechanicznych								
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	TAK	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	–	TAK	TAK	–	–	TAK	–	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	TAK	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	TAK	TAK	TAK	TAK	TAK	–	TAK	–	TAK
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	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
Paweł Karczmarzyk
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz
Marek Życzkowski

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

Skład i łamanie
Marek Bladoszewski

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

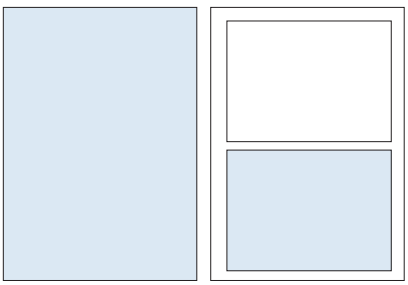
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 0 546
faks (22) 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4200 zł
cała strona, czarno-biała	2200 zł
1/2 strony, pełny kolor	2700 zł
1/2 strony, czarno-biała	1500 zł
1/3 strony, pełny kolor	1900 zł
1/3 strony, czarno-biała	1000 zł
1/4 strony, pełny kolor	1400 zł
1/4 strony, czarno-biała	800 zł
karta katalogowa, 1 strona	900 zł

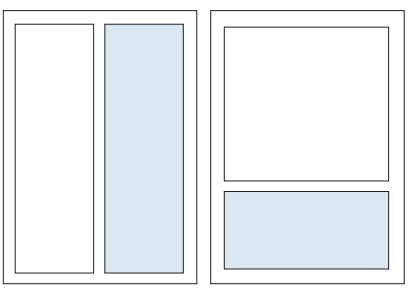


cała strona (200 x 282 mm + 3mm spad) | 1/2 strony (170 x 125 mm)

Artykuł sponsorowany:
indywidualne negocjacje (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

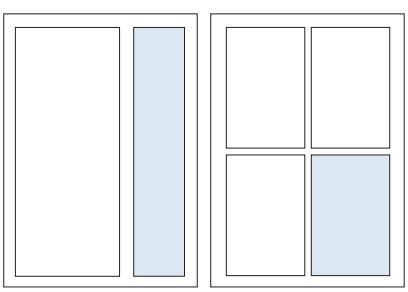
Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/2 strony (83 x 260 mm) | 1/3 strony (170 x 80 mm)

Spis teleadresowy:
jednorazowy wpis 70 zł



1/3 strony (54 x 260 mm) | 1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (22%)

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

Spis reklam

Łączymy się z całym światem

ONVIF
Driving network video through global standardization

Sieciowe rejestratory obrazu (NVR-y) firmy Samsung

Stanowiące fragment sieciowych systemów dozorowych iPOLiS oferowanych przez firmę Samsung, sieciowe rejestratory obrazu SRN są dostępne w wersjach 4-, 16-, 32- i 64-kanałowych, które mogą rejestrować obraz o wysokiej jakości, pochodzący zarówno z sieciowych kamer IP firmy Samsung, jak również z urządzeń innych producentów, które są zgodne ze standardem ONVIF*.

Sieciowe rejestratory obrazu SRN mają wewnętrzne dyski twarde o dużej pojemności. Można również podłączyć do nich zewnętrzne jednostki pamięciowe SVS firmy Samsung. To wszystko umożliwia uzyskanie przestrzeni pamięciowej o łącznej pojemności 40 TB w jednym systemie.

Pełna kompatybilność z oprogramowaniem CMS NET-i firmy Samsung gwarantuje użytkownikom dostęp do sieciowych rejestratorów obrazu z serii SRN za pośrednictwem komputera z każdego miejsca na świecie, umożliwiając im stałą łączność z systemami ochrony niezależnie od miejsca ich instalacji.

Z zastosowania przedstawionych rozwiązań może wynikać wiele nie odkrytych dotychczas korzyści. Skontaktuj się z nami i poznaj pełną ofertę.

* *Zgodność ze standardem ONVIF będzie zapewniona od lutego 2011 r., dzięki możliwości aktualizacji oprogramowania sprzętowego.*

2010 PSI PREMIER AWARDS WINNER

T **+420 222 866 002, +420 602 532 103**
E **STEsecurity@samsung.com**
W **samsungsecurity.com**

Biuro Regionalne:
Samsung Techwin Europe Ltd
Římská 20, 120 00, Praha 2, Czechy

SAMSUNG

Potrzebuję...

drukarki do kart
wspomagającej rozwój
mojej firmy.

HID Global przedstawia nowy model FARGO® DTC4000

Przełom w modułowości, wszechstronności i wygodzie personalizacji kart.

Model FARGO® DTC4000 to niepowtarzalne urządzenie, które zapewnia zwrot inwestycji dzięki wygodzie, jaką daje możliwość dalszej rozbudowy dostępnych funkcji. Dodatkowo oferuje rozszerzoną skalowalność z modułem drukowania dwustronnego oraz podajnikiem na 200 kart. Z myślą o rozszerzeniu bezpieczeństwa dostępny jest system drukowania UV wraz z kilkoma opcjami kodowania. DTC4000 to wygodne i kompaktowe urządzenie dostępne opcjonalnie z podajnikiem/urządzeniem odbierającym z tej samej strony. Dzięki swojej budowie drukarka z łatwością zmieści się w każdym, nawet najciaśniejszym miejscu. Obsługa nie nastręcza żadnych trudności. Urządzenie jest intuicyjne i łatwe w obsłudze, praktycznie nie wymaga przeszkolenia i konserwacji. Dzięki połączeniu najwyższej wszechstronności oraz modułowości DTC4000 stanowi idealne rozwiązanie w zastosowaniach związanych z drukiem wysokonakładowym lub rozbudowanymi opcjami kodowania. FARGO DTC 4000 – wygodne połączenie wszechstronności i modułowości.

HID

Aby dowiedzieć się, jak dzięki HID możesz zrealizować swoje potrzeby związane z personalizacją kart, odwiedź stronę
www.hidglobal.com/fargo-dtc4000-Zab