CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(90)/2013

ZABEZPIECZENIA

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

W NUMERZE:

to już 15 lat Zabezpieczeń

Platforma wymiany informacji

HID iCLASS SE

Otwarta, elastyczna i doskonale zabezpieczona platforma iCLASS SE®, która ułatwia wszystko.

HID®

iCLASS SE® to kolejna generacja platformy kontroli dostępu HID Global, która umożliwia uwierzytelnianie w różnych komercyjnych technologiach przy użyciu kart bezkontaktowych. Bardzo elastyczna rodzina czytników wraz z szeroką gamą kart zbliżeniowych zapewnia wymianę informacji w różnych środowiskach technologicznych. Technologia iCLASS SE może zostać również użyta w telefonach komórkowych (NFC) i innych urządzeniach inteligentnych. Teraz możesz wykorzystać wszystkie możliwości tej technologii do stworzenia idealnego systemu kontroli dostępu. **Aby uzyskać więcej informacji, odwiedź hidglobal.com/path-Zab**

Spis treści

CZASOPISMO ZABEZPIECZENIA 2/2013

Wiosenne nowości firmy SATEL **12**

Komputerowa symulacja elektronicznego systemu bezpieczeństwa **16**

Koszty ponoszone przez posiadacza wizyjnego systemu dozorowego **46**

Dinion HDR – by widzieć więcej **50**

MOBOTIX zdobywcą nagrody GIT Security 2013

Ponad 75000 czytelników zadecydowało o zdobyciu przez **MOBOTIX S14 FlexMount** nagrody **GIT Sicherheit Award 2013** w kategorii C – CCTV.

Pierwsza na świecie podwójna kamera hemisferyczna pokonała wiele innych rozwiązań z branży zabezpieczeń.

Kamera jest dostępna w dwóch wersjach – mono (S14M) oraz dual (S14D). Miniaturowe obiektywy zapewniają elastyczność gwarantującą wiele możliwości zastosowań. Na przykład kamera S14D może być wyposażona w dwa niezależne obiektywy hemisferyczne oraz mikrofon. Moduły peryferyjne są połączone za pomocą kabla z korpusem głównym – obudową. Sprawia to, że możliwa jest obserwacja dwóch pomieszczeń zlokalizowanych obok siebie lub jedno nad drugim za pomocą tylko jednego zestawu S14D. Dzięki płaskiej konstrukcji poszczególnych modułów kamery S14 sprawdzą się w hotelach, bankach i sklepach detalicznych.

Kamera S14 jest zgodna z normą DIN EN 50155, więc odznacza się wysokim stopniem niezawodności, a także doskonale nadaje się do zastosowań mobilnych, np. w autobusie lub pociągu, a nawet w innych ekstremalnych warunkach.

Bezpośr. inf. Linc Polska

System łączności alarmowej na autostradzie

Uruchomienie punktów SOS na A8 – Autostradowej Obwodnicy Wrocławia

W listopadzie 2012 roku firma **Novatel**, wspólnie z lokalnym partnerem **BlueSoft**, zainstalowała system autostradowych telefonów alarmowych. Interkomy rozmieszczono na dystansie 26 km AOW-Zachód, gdzie każdego dnia przejeżdża od 20000 do 27000 pojazdów.

System bazuje na serwerze Alphacom XE7, modułach Turbine TCIS2 i konsoli operatora CRM V firmy STENTOFON Zenitel. Monitoring obejmuje połączenie sieciowe, sygnał audio oraz układ zasilania solarnego każdej stacji. W trakcie połączenia głosowego wykorzystywany jest mechanizm automatycznej redukcji hałasu.

Bezpośr. inf. Novatel

Świadectwo Bezpieczeństwa Przemysłowego w naszych rękach!

Z ogromną przyjemnością informujemy, iż w dniu 22 października ubiegłego roku firma **mvb** uzyskała **Świadectwo Bezpieczeństwa Przemysłowego**. Poświadczenie zostało wydane przez Agencję Bezpieczeństwa Wewnętrznego na podstawie specjalnego postępowania sprawdzającego.

Uzyskanie Świadectwa jest efektem ponad rocznych inwestycji, przeobrażeń i restrukturyzacji firmy mających na celu podwyższenie poziomu ochrony przetwarzanych informacji niejawnych. Aby osiągnąć ten cel, powołano pion ochrony informacji niejawnych oraz wybudowano profesjonalną kancelarię tajną. Jednocześnie utworzono specjalistyczne, autonomiczne stanowisko komputerowe do przetwarzania informacji niejawnych w wersji elektronicznej. Wszyscy należący do kadry odpowiedzialnej za realizację poszczególnych przedsięwzięć oraz pracownicy biorący bezpośredni udział w pracach związanych z ochroną informacji niejawnych odbyli odpowiednie szkolenia oraz uzyskali poświadczenia bezpieczeństwa o wymaganych klauzulach tajności.

Agencja Bezpieczeństwa Wewnętrznego prowadziła postępowanie, które miało na celu sprawdzenie struktury kapitału, sytuacji ekonomicznej, osób zarządzających i kontrolujących, osób działających z ich upoważnienia, systemu ochrony osób,

Grundig CCTV wyłącznie w ofercie C&C Partners

C&C Partners, jeden z największych w Polsce dostawców kompleksowych rozwiązań z dziedziny telekomunikacji, teleinformatyki i zabezpieczeń, rozszerzył swoją ofertę o urządzenia CCTV firmy **Grundig**, wiodącego dostawcy elektroniki użytkowej na rynku europejskim. Na mocy umowy od dnia 1 stycznia 2013 roku C&C Partners ma wyłączność na sprzedaż urządzeń CCTV firmy Grundig wykorzystywanych na całym świecie przez instytucje, przedsiębiorstwa czy w obiektach użyteczności publicznej.

Bazując na swoim kilkudziesięcioletnim doświadczeniu w projektowaniu i produkcji urządzeń audiowizualnych, Grundig oferuje pełną gamę wizyjnych systemów nadzoru i systemów bezpieczeństwa – od kamer i monitorów, poprzez kontrolery i rejestratory, aż po akcesoria. Systemy CCTV firmy Grundig wykorzystują różne metody transmisji sygnału wizyjnego i wszystkie najnowsze osiągnięcia technologiczne przy jednoczesnym zachowaniu wyjątkowej funkcjonalności, niezawodności i jakości, jakiej można oczekiwać od niemieckiej firmy z tak olbrzymim doświadczeniem. W skład bogatego asortymentu produktów Grundig CCTV wchodzą kompaktowe, kopułkowe i szybkoobrotowe kamery do zastosowań zarówno wewnętrznych, jak i zewnętrznych. Uzupełnieniem oferty są różnorodne modele rejestratorów umożliwiające podgląd na żywo oraz szybką i bezproblemową konfigurację systemu.

Grundig jest pierwszym producentem oferującym pełen asortyment urządzeń HD-SDI. Umożliwiają one transmisję nieskompresowanego cyfrowego sygnału wizyjnego w czasie rzeczywistym i zapewniają wyższą jakość obrazu niż rozwiązania IP. Wysoka jakość materiałów zastosowanych w produkcji kamer, monitorów i akcesoriów, a także ich wyjątkowa estetyka i wzornictwo sprawiają, że systemy zabezpieczeń Grundig CCTV znajdują zastosowanie w ekskluzywnych hotelach, nowoczesnych obiektach biurowych, halach produkcyjnych, lotniskach i dworcach kolejowych. Wszystkie produkty firmy Grundig bazują na najnowszych rozwiązaniach opracowanych z myślą o łatwej, intuicyjnej obsłudze.

Systemy CCTV firmy Grundig gwarantują bezpieczeństwo pasażerów na największych francuskich i niemieckich lotniskach, tj. Paris – Charles de Gaulle, Paris – Orly, na lotniskach we Frankfurcie i Düsseldorfie. Firmie Grundig zaufała także Poczta we Francji oraz w Bośni i Hercegowinie, a także firmy z branży spedycyjnej: DHL, DPD i Fedex. Ponadto urządzenia Grundig CCTV są wykorzystywane w wielu placówkach największych światowych banków, m.in. Bank Societe Generale, HSBC, BNP Paribas oraz DZ Bank. Firma Grundig ma także duże doświadczenie w zabezpieczaniu wielkopowierzchniowych obiektów handlowych. Kompleksowe systemy monitoringu działają w sklepach renomowanych europejskich sieci, takich jak Auchan, Carrefour, Decathlon i Lidl. Dużym wyzwaniem było zapewnienie odpowiedniej jakości nadzoru wizyjnego na stacjach benzynowych sieci BP i Total.

– Urządzenia CCTV firmy Grundig doskonale uzupełniają naszą ofertę, w której znajdują się kompleksowe, zintegrowane systemy zabezpieczeń. W tej dziedzinie C&C Partners od lat wiedzie prym na polskim rynku – wyjaśnia Łukasz Jankowski, dyrektor ds. marketingu C&C Partners. Marka Grundig jest doskonale rozpoznawalna w całej Europie i cieszy się niesłabnącym zaufaniem klientów korzystających z różnorodnych rozwiązań z dziedziny elektroniki użytkowej. Niezaprzeczalnym atutem jest fakt, że jest to europejski producent z bardzo dużym doświadczeniem *To ważne dla naszych partnerów, którzy oczekują trwałych i niezawodnych rozwiązań. Co więcej, oferujemy te urządzenia po naprawdę atrakcyjnych cenach – dodaje Łukasz Jankowski.*

Dzięki wprowadzeniu urządzeń CCTV marki Grundig do swojej oferty C&C Partners oferuje teraz jeszcze bardziej kompleksowe i konkurencyjne rozwiązania dla zakładów przemysłowych, biur, a także obiektów użyteczności publicznej, takich jak lotniska, dworce czy szpitale, gdzie najbardziej liczy się niezawodność, trwałość i funkcjonalność urządzeń.

Bezpośr. inf. Łukasz Jankowski
C&C Partners
Agnieszka Stasiewicz-Swinney
Comm Start

materiałów oraz obiektów ze szczególnym uwzględnieniem elementów systemu ochrony informacji niejawnych.

Na podstawie wyników postępowania sprawdzającego przyznano firmie mvb świadectwo stopnia pierwszego, czyli najwyższego z przyznawanych przez ABW. Oznacza to potwierdzenie jej pełnej zdolności do ochrony niejawnych informacji Organizacji Traktatu Północnoatlantyckiego (NATO SECRET i NATO CONFIDENTIAL), Unii Europejskiej (EU SECRET i EU CONFIDENTIAL), jak i krajowych (TAJNE I POUFNE).

Otrzymanie świadectwa jest dowodem rozwoju naszego przedsiębiorstwa. Daje nowe możliwości i zachęca do wdrażania nowoczesnych technologii. Ułatwi nam współpracę z biznesowymi partnerami. Jest gwarancją bezpieczeństwa dla naszych klientów.

Bezpośr. inf. Agata Paciejewska-Strzelska
mvb

Martin Gren zajął pierwsze miejsce w rankingu najbardziej wpływowych osób w branży zabezpieczeń według IFSEC Global

Martin Gren, członek zarządu w firmie **Axis Communications** i jeden z jej współzałożycieli, zajął pierwsze miejsce w rankingu zamieszczonym na stronie internetowej IFSEC Global, w którym znalazły się najbardziej wpływowe osoby związane z branżą zabezpieczeń elektronicznych oraz systemów sygnalizacji pożarowej.

– *Czuję się bardzo szczęśliwy i uhonorowany z powodu przyznania mi tytułu najbardziej wpływowej osoby w światowym przemyśle zabezpieczeń elektronicznych i systemów sygnalizacji pożarowej* – powiedział Martin Gren.

Firma Axis jako pierwsza na świecie wypuściła na rynek kamerę sieciową – w 1996 roku. Obecnie Axis jest liderem na światowym rynku wizyjnych urządzeń zabezpieczających i realizuje plan przebudowy analogowych systemów dozorowych i stopniowego zastępowania ich urządzeniami cyfrowymi.

Per Björkdahl, prezes zarządu organizacji ONVIF, a także dyrektor Działu Strategii i Rozwoju w firmie Axis Communications, zajął w tym samym rankingu trzecie miejsce, a Keith Bloodworth, jeden ze współzałożycieli firmy Axis Communications, a obecnie dyrektor generalny w firmie CNL Software, zajął szóste miejsce.

Na podstawie rankingu IFSEC Global sporządzono ogólnoświatową listę czterdziestu najbardziej wpływowych osób związanych z branżą zabezpieczeń elektronicznych i systemów sygnalizacji pożarowej. Lista ma związek z czterdziestą międzynarodową wystawą IFSEC, która odbędzie się w Birmingham (Wielka Brytania) w dniach 13–16 maja 2013 r.

Bezpośr. inf. Axis Communications
Tłumaczenie: Redakcja

Nowy bezpłatny CMS Mobile dla Windows Phone już do pobrania

CMS Mobile to profesjonalna aplikacja przeznaczona do zdalnego monitoringu wizyjnego z wykorzystaniem urządzeń przenośnych typu smartfon. W nowej wersji wprowadzono wiele usprawnień oraz dodano możliwość nielimitowanych połączeń z wieloma serwerami. Ponadto aplikacja umożliwia sterowanie głowicami PTZ, zdalny dostęp do nagrań archiwalnych i sterowanie urządzeniami podłączonymi do wejść/wyjść alarmowych.

Aplikacja CMS Mobile dla Windows Phone jest w pełni kompatybilna ze wszystkimi produktami **Alnet Systems** – NetStation, NetHybrid oraz NetHybrid HD.

Aplikacja może być pobrana w AppleStore, Play Android Market oraz WindowsStore. Film demonstracyjny jest dostępny na YouTube (*www.youtube.com*).

Bezpośr. inf. Tomasz Kaliński
Alnet Systems

Camsat zaprasza na targi IFSEC

W tym roku mija dziesięć lat działalności firmy **CAMSAT** na rynku telewizji dozorowej. Przez ten czas firma osiągnęła ugruntowaną pozycję w dziedzinie systemów bezprzewodowej transmisji sygnału wizyjnego i danych, zarówno na rynku krajowym, jak i na wielu rynkach europejskich. Już trzykrotnie zostaliśmy wyróżnieni tytułem Przedsiębiorstwo Fair Play.

W tym roku dostrzegliśmy potrzebę zaprezentowania się naszym zagranicznym odbiorcom na **Międzynarodowych Targach Zabezpieczeń IFSEC** w Birmingham, w Wielkiej Brytanii. IFSEC International jest największym wydarzeniem dla branży zabezpieczeń w Europie. Będzie to świetna okazja do zaprezentowania naszych najnowszych produktów. Mamy nadzieję, że na targach

Korzyści finansowe płynące z wyboru centrali FPC-500 firmy Bosch

„Czas to pieniądz" to powiedzenie, którego używamy często, ale raczej nie w odniesieniu do konwencjonalnych central sygnalizacji pożarowej. W ich przypadku o zakupie nadal decyduje niemal wyłącznie cena. Tymczasem warto zwrócić uwagę na łatwość ich instalacji i obsługi, bo właśnie tu mogą kryć się znaczne oszczędności.

Nowa konwencjonalna centrala sygnalizacji pożarowej z rodziny **Bosch 500 Series (FPC-500)** została zaprojektowana tak, aby ułatwić użytkownikowi obsługę i zmniejszyć koszt instalacji. Płyta do obsługi została zaprojektowana w taki sposób, że każdy użytkownik może obsługiwać centralę samodzielnie – specjalistyczna wiedza nie jest już konieczna.

– *Projektantom nowej centrali Bosch Security Systems zależało na skróceniu czasu potrzebnego na jej zainstalowanie. Wystarczy tylko podstawowe, zajmujące mniej czasu i tańsze szkolenie instalatorów, a cały system sygnalizacji pożarowej działa po wykonaniu zaledwie kilku czynności, co skraca czas trwania instalacji i obniża jej koszt* – podkreśla *Krzysztof Kostecki*, Product Manager w Bosch Security Systems.

Aby uzyskać obiektywne opinie na temat nowej centrali sygnalizacji pożarowej, przeprowadzono badanie na niezależnej grupie instalatorów i użytkowników. Udowodniło ono, że obsługa centrali faktycznie jest bardzo prosta, a koszt jej zainstalowania jest niższy niż w przypadku konkurencyjnych rozwiązań.

Testowi poddano grupę niedoświadczonych użytkowników. Porównywali oni centralę FPC-500 z urządzeniami innych marek w ponad 450 przykładowych zastosowaniach. W ramach badania odbył się także test ekspercki, który umożliwił zdobycie indywidualnych ocen doświadczonych instalatorów. Rezultatem badania było uzyskanie jednoznacznego potwierdzenia, że cel projektantów centrali Bosch 500 Series został osiągnięty. Czas całkowitej instalacji centrali był najkrótszy w przypadku FPC-500 – i to bez względu na to, czy instalator miał duże doświadczenie, czy też był amatorem. Niezależni instalatorzy, którzy przetestowali centralę, podkreślali, że jej konfiguracja jest bardzo intuicyjna i łatwa.

– *Instalacja FPC-500 jest tak prosta, że może zająć mi dwie godziny mniej niż zainstalowanie urządzenia innej marki. Ponadto instalacja centrali konkurencji może wymagać obecności dwóch instalatorów. W przypadku centrali FPC-500 wystarczy jeden instalator, o ile prawo nie stanowi inaczej. Obniża to koszty pracy o połowę* – zauważył zawodowy instalator biorący udział w badaniu.

Koszt instalacji systemu przeciwpożarowego to około jednej piątej całkowitego kosztu inwestycji, więc powinien być brany pod uwagę przy wyborze rozwiązania. Łatwiejsza, trwająca ponad godzinę krócej niż zazwyczaj instalacja konwencjonalnej centrali sygnalizacji pożarowej serii 500, a także szybsza konfiguracja może przynieść znaczne oszczędności.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

będziemy mogli także spotkać się z przedstawicielami polskich firm.

Oprócz znanych i docenianych systemów analogowych chcemy zaprezentować nadajnik CAM5816h Multi-Tx i odbiornik CAM5816h Multi-Rx które współtworzą system, na który jest zapotrzebowanie na rynku. System umożliwia przesyłanie czterech sygnałów wizyjnych jednocześnie. Instalatorzy wypowiadają się o nim bardzo przychylnie, gdyż jest to rozwiązanie w dużej mierze zainspirowane ich sugestiami. Wspomniane urządzenia umożliwiają użycie czterokrotnie mniej zestawów do transmisji obrazów i danych w obrębie jednego systemu monitoringu.

Na targach IFSEC zaprezentujemy też urządzenia CDS-5HD do kamer HD-SDI służące do transmisji sygnału wizyjnego o jakości HD z kamer megapikselowych CDS-5IP. Produkty te cieszą się bardzo dużym zainteresowaniem na brytyjskim rynku. Warto zwrócić uwagę także na cyfrowy system CDS5021h(STR). Urządzenia te były już kiedyś produkowane w prostszej wersji. Obecnie zostały wzbogacone o dodatkowy sterownik, który znacznie usprawnił ich pracę. Bezprzewodowe systemy firmy Camsat sprawdzają się nie tylko w telewizji dozorowej. Ciekawym zastosowaniem urządzeń CDS5021(STR) jest zdalny podgląd obrazu z kamery zainstalowanej w helikopterze lub w innej maszynie latającej. Można je używać do obserwacji trybun obiektów sportowych z większych wysokości, a także tam, gdzie trudno dotrzeć operatorowi standardowej kamery. Nasze urządzenia były wykorzystywane podczas mistrzostw Euro 2012 do podglądu obrazu z maszyn latających podczas obserwacji trybun Stadionu Narodowego i do analizy zagrożeń. Ponadto urządzenia CAMSAT uwzględniono w projekcie łazika marsjańskiego, który brał udział w konkursie University Rover Challenge 2012 w Stanach Zjednoczonych.

Bezpośr. inf. Agnieszka Gralak
CAMSAT

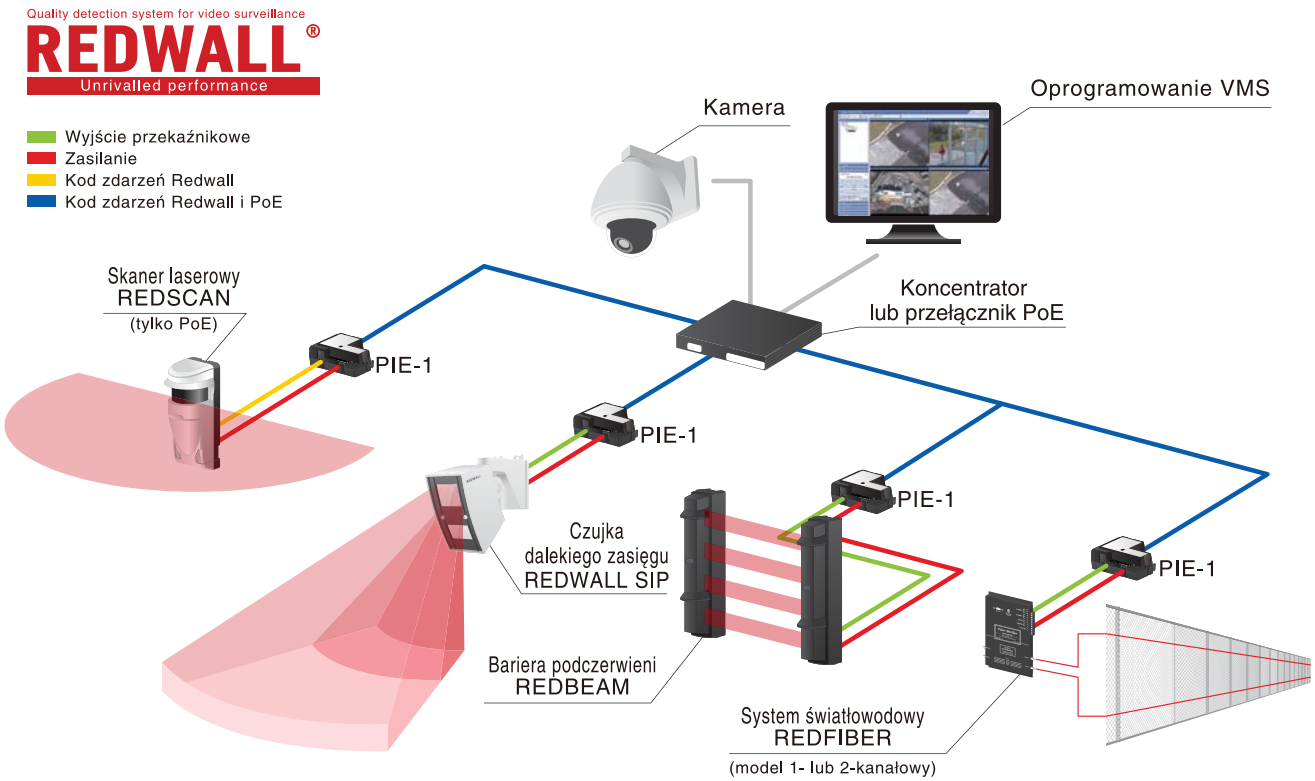
Czujki OPTEX w technologii PoE

Seria zewnętrznych czujek **REDWALL** została uzupełniona o urządzenia, które można bezpośrednio włączyć do systemu nadzoru wizyjnego. W detektorach zastosowano własnej konstrukcji konwerter PIE-1 zamieniający sygnały analogowe na kod ASCII. Każda czujka ma własny adres IP i może być wykorzystana do sterowania kamerami IP (preset) uwzględnionymi w oprogramowaniu systemu nadzoru wizyjnego.

Konwerter PIE-1 opracowano w technologii Power over Ethernet (IEEE802.3 af/at), więc do zasilania czujek można wykorzystać koncentrator lub przełącznik PoE.

Czujki dalekiego zasięgu REDWALL SIP, bariery podczerwieni REDBEAM, skaner laserowy REDSCAN oraz system światłowodowy REDFIBER znajdują się w pakietach urządzeń obsługiwanych przez oprogramowanie Milestone, Genetec, Axxonsoft oraz rejestratory JVC.

Bezpośr. inf. Jacek Wójcik
OPTEX Security



Rys. Zastosowanie technologii PoE w detektorach ułatwia integrację z systemem nadzoru wizyjnego

Integracja systemu kontroli dostępu firmy ROGER z kamerami IP

Oferując system **KD RACS 4.4.12**, firma **ROGER** umożliwia integrację systemu kontroli dostępu z rejestratorami firmy HIK Vision oraz Dahua, a także ich odpowiednikami sprzedawanymi pod markami BCS i Raiden. Zasadniczo integracja została opracowana dla rejestratorów typu BCS0804LE-A oraz DS7204HVI-ST, ale ze względu na zgodność interfejsu programistycznego możliwa jest również obsługa wielu pokrewnych modeli DVR i NVR. System RACS w nowej wersji może współpracować z kamerami IP wyposażonymi w kartę SD (np. kamerą DS-2CD752MF-IFB 2MP firmy HIK Vision). Kamery tego rodzaju mogą być obsługiwane z wykorzystaniem oprogramowania systemu RACS, bez konieczności pośrednictwa rejestratora. Rozwiązanie to obniża koszty integracji z CCTV w tych systemach, w których jest zapotrzebowanie na małą liczbę punktów rejestracji obrazu lub punkty te znajdują się w odległości uniemożliwiającej bezpośrednie podłączenia do centralnego rejestratora.

Dzięki integracji systemu RACS 4 z CCTV można:
– odtwarzać klipy wideo dla wybranych zdarzeń zarejestrowanych w systemie,
– korzystać z podglądu obrazu z kamer w czasie rzeczywistym, bezpośrednio z poziomu programu zarządzającego systemem.

Bezp. inf. ROGER

Bosch pomaga instalatorom uniknąć błędów

Walizka LSN – zaawansowane narzędzie testowe firmy Bosch

Bosch opracował nowe, zaawansowane narzędzie testowe **LSN**, pomocne dla instalatorów systemów przeciwpożarowych i sygnalizacji włamania i napadu. Dzięki niemu można poprawić jakość instalacji, jednocześnie skracając czas jej wykonania i obniżając jej koszt.

LSN umożliwia szybkie sprawdzenie okablowania w trakcie instalacji, a w czasie działania systemu – łatwą identyfikację błędów i usterek. Wykrywa i lokalizuje błędy w ułożeniu okablowania, co zwiększa niezawodność systemu i umożliwia spełnienie wymagań normy EN 54-13.

– Prawidłowa instalacja jest podstawą niezawodnego działania systemu. Dzięki LSN można w ciągu kilku minut upewnić się, że okablowanie i peryferia zostały poprawnie zainstalowane. Do tej pory nie było sposobu na sprawdzenie podczas instalowania, czy okablowanie jest odpowiednio ułożone. Teraz jest to możliwe i łatwe – i to nawet przed zainstalowaniem centrali. Wystarczy tylko połączyć przewody z zaawansowanym narzędziem testowym LSN i nacisnąć przycisk „START". Wszelkie ewentualne błędy i usterki są lokalizowane i pokazywane na grafice przedstawiającej topologię okablowania – wyjaśnia Monika Kołodziejczyk z Bosch Security Systems.

Nowa walizka testowa firmy Bosch umożliwia wykrywanie błędów i usterek w niedostępny do tej pory sposób, zaraz po podłączeniu do linii pętlowej. Identyfikuje ich typ oraz szybko i precyzyjnie je lokalizuje. Efekty pracy urządzenia przedstawiane są bezpośrednio na komputerze. Praca instalatora była dotychczas uzależniona od dostępu do okablowania. Na przykład w hotelach konieczne było uzyskanie zgody na wejście do poszczególnych pokoi w celu zlokalizowania usterek. Dzięki LSN można je wykryć w miejscu zainstalowania centrali, przez co fizyczny dostęp do kabli konieczny jest wyłącznie w sporadycznych przypadkach. Zaletą LSN jest również brak konieczności sprawdzania kabli, np. w przypadku urządzeń peryferyjnych, montowanych bardzo wysoko lub w miejscach trudno dostępnych. Dzięki temu instalator oszczędza czas, zyskuje swobodę i niezależność działania, a także zwiększa komfort swojej pracy.

Najbardziej niebezpieczne są usterki, które nie pojawiają się w czasie normalnej pracy, ale po uruchomieniu alarmu. To właśnie one mogą doprowadzić do tego, że wszystkie urządzenia sygnalizacyjne i urządzenia wyjściowe nie zostaną aktywowane w czasie alarmu przeciwpożarowego. W takim przypadku nie da się zachować bezpieczeństwa, a na szukanie rozwiązań naprawczych będzie za późno. LSN ułatwia serwisantom wykrywanie błędów w okablowaniu oraz lokalizowanie ich we wszystkich trybach obsługi, więc może zapobiec takiej sytuacji. Dzięki temu urządzenie znacząco przyczynia się do spełnienia wymogów dotyczących bezpieczeństwa i niezawodności systemów, które określa norma EN 54-13.

LSN umożliwia również sprawdzanie lokalizacji urządzeń i trasy ułożenia kabla. Sygnalizatory akustyczne i optyczne, a także diody LED detektorów i ręcznych ostrzegaczy pożarowych, mogą być aktywowane pojedynczo lub w grupach. Pojedyncza aktywacja umożliwia szybkie ustalenie położenia każdego urządzenia oraz sprawdzenie jego adresu logicznego. Przy wielokrotnym wyborze detektorów diody LED migają sekwencyjnie, aby instalator mógł sprawdzić drogę ułożenia okablowania.

Przydatną funkcją LSN jest także pomoc w sporządzaniu dokumentacji technicznej, której wykonanie to nie tylko bardzo istotne, ale także czasochłonne zadanie. Wszystkie wyniki i dane, w tym topologia sieci okablowania z lokalizacją usterek i zestawieniem materiałów, mogą zostać zapisane bezpośrednio w dokumencie tekstowym. Informacja o braku błędów i usterek również zostanie zarejestrowana. Wystarczy zatem kilka kliknięć, aby instalator mógł przygotować pełną dokumentację.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Nowy wiceprezes ds. planowania produktów i marketingu strategicznego w firmie Samsung

Jonas Andersson został mianowany na stanowisko Senior Vice President for Product Planning and Strategic Marketing firmy **Samsung Techwin**.

Jonas Andersson, który dołączył do Samsung Techwin 14 stycznia 2013 roku ostatnie 18 lat spędził w Axis Communications, gdzie obejmował wiele kierowniczych stanowisk (był m.in. dyrektorem ds. zarządzania produktami i systemami wizyjnymi, a przez ostatnie pięć lat dyrektorem ds. rozwoju). Od listopada 2008 roku był również przewodniczącym komitetu kierowniczego ONVIF (Open Network Video Interface Forum).

– Jesteśmy bardzo zadowoleni z zatrudnienia kogoś tak znanego jak Jonas Andersson na tym bardzo ważnym stanowisku. Jego duża wiedza o rozwiązaniach wykorzystujących sieć IP oraz niezwykłe zrozumienie rynkowych możliwości będzie miało dla nas ogromną wartość, ponieważ chcemy budować naszą pozycję na sukcesie, jaki dotychczas osiągnęliśmy. Jako przewodniczący komitetu kierującego ONVIF Jonas odegrał kluczową rolę w adaptowaniu wizyjnych urządzeń sieciowych na rynku zabezpieczeń i zapewnianiu wzajemnej kompatybilności między produktami wizyjnymi różnych producentów. Oba te zadania leżą u podstaw naszej Smart Security, która ma zapewnić maksymalne wykorzystanie środków zainwestowanych w nadzór wizyjny – powiedział Hansoo Jung, Senior Vice President firmy Samsung Techwin.

– Spędziłem ostatnie dziesięć lat, pracując dla jednego z wiodących producentów urządzeń IP i jestem bardzo zadowolony z tego, że mogę kontynuować swoją karierę, zajmując to stanowisko w firmie Samsung Techwin. Chcę mieć wkład w działalność młodego zespołu inżynierów oraz specjalistów od sprzedaży i marketingu, którzy wykonali wspaniałą pracę w ciągu kilku ostatnich lat, wprowadzając nowe produkty i technologie, które spowodowały, że Samsung Techwin zyskał miano lidera tego rynku – powiedział Jonas Andersson, komentując swoje zatrudnienie.

Bezpośr. inf. David Solomons
DRS Marketing

UltraLink

nowy wymiar integracji ochrony peryferyjnej

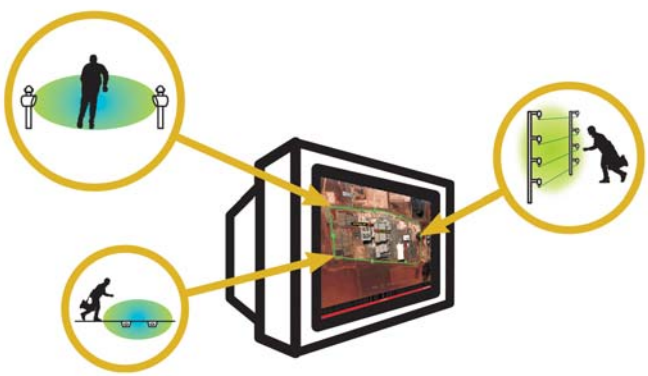
Integracja, zdalne monitorowanie i zarządzanie rozległymi, zewnętrznymi systemami ochrony obwodowej stanowią odwieczne wyzwanie dla projektantów i wykonawców. Szczególnie trudne jest zbudowanie zintegrowanego systemu, składającego się z dużej liczby detektorów wykorzystujących różne technologie wykrywania intruzów. Zestaw produktów **UltraLink** wprowadzony do sprzedaży przez firmę **Senstar** pod koniec 2012 roku pomaga przezwyciężyć te trudności.

System UltraLink składa się z zestawu elementów elektronicznych oraz pakietu oprogramowania sieciowego. UltraLink umożliwia nie tylko zintegrowanie czujek Senstar (takich jak Omnitrax, FlexPS, UltraWave, X-Field), ale również podłączenie dodatkowych czujek dowolnego typu do systemu, bezpośrednie sterowanie kamerami systemu CCTV, a także łatwe połączenie systemu ochrony obwodowej z innymi systemami (np. z nadrzędnym systemem monitoringu). Całość może być monitorowana i zarządzana ze stanowiska operatora, z wykorzystaniem jednej, wspólnej dla wszystkich urządzeń platformy programowej.

Elementy elektroniczne to:

– moduł sterownika, wyposażony w kartę sieciową działającą w standardzie Silver (RS422, MMFiber lub SMFiber), zawiera 8 przekaźników alarmowych, 8 wejść izolowanych galwanicznie, port USB oraz gniazdo do montażu dodatkowych kart rozszerzających,
– karta z 32 przekaźnikami wyjściowymi,
– karta z 32 wyjściami typu „otwarty kolektor”,
– karta z 32 wejściami izolowanymi galwanicznie.

Moduł sterownika może zarządzać maksymalnie 272 wejściami-wyjściami.



Pakiet oprogramowania Network Manager Suite składa się z modułów:

1) Silver Network Manager (SNM). Moduł ten służy do konfiguracji urządzeń i zarządzania siecią. Jest to zestaw programów kontrolno-diagnostycznych (UCM, Plot, Status) wykorzystywanych do konfiguracji wszelkiego typu czujek Senstar. Umożliwiają one pełną zdalną diagnostykę czujek, odczyty logów, rejestracje przebiegów z wykresami sygnałów, programowanie parametrów itp.
2) Software Develompent KIT z pełną dokumentacją API. Jest to narzędzie umożliwiające tworzenie nakładek programowych do integracji TCP/IP lub DLL z innymi systemami.
3) Network Simulator. Umożliwia on tworzenie wirtualnej sieci. To znacznie ułatwia integrację i testowanie połączenia z innymi systemami monitoringu pochodzącymi od innych producentów lub systemami CCTV.
4) Alarm Integration Module (AIM). Jest to oprogramowanie zarządzające wejściami i wyjściami modułów UltraLink oraz wszystkich czujek Senstar, a także umożliwiające prezentację stanu systemu na mapie synoptycznej oraz zarządzanie alarmami przez operatora systemu.

Bezpośr. inf. Karolina Zasada, Krystian Witczak
ZBAR

Videotec wprowadza na rynek nową obudowę z zasilaniem HI-PoE

Najnowsza obudowa zaprezentowana przez firmę **Videotec** została zaprojektowana tak, by mogła spełniać współczesne wymagania rynkowe. Jej konstrukcja łączy w sobie innowacyjną technologię inteligentnego sterowania z nowoczesnymi funkcjami zabezpieczającymi, zapewniającymi niezawodną pracę kamer sieciowych.

Dzięki wdrożeniu innowacyjnego systemu zarządzania mocą IPM (*Intelligent Power Management*) jedynym źródłem zasilania wszystkich zainstalowanych urządzeń jest energia przekazywana przez kabel sieciowy, zgodnie ze standardem PoE lub Hi-PoE. Dzięki temu wzrasta niezawodność sieciowych systemów dozorowych, a ich instalacja ulega uproszczeniu, co z kolei prowadzi do redukcji kosztów.

System zarządzania mocą IPM automatycznie wykrywa wszystkie zainstalowane urządzenia, takie jak grzałki, wentylatory, oświetlacze, i automatycznie dokonuje oceny ich zapotrzebowania na energię, a następnie dokonuje rozdziału dostępnej energii, doprowadzanej przez kabel sieciowy. Taki system zasilania zapewnia poprawną pracę kamer sieciowych przy zmianach temperatury otoczenia w zakresie od -30°C do 60°C. Jednocześnie zachowane są właściwe warunki termiczne wewnątrz obudowy i możliwość zimnego startu (rozruchu kamer przy niskiej temperaturze otoczenia).

System IPM z zasilaniem Hi-PoE może być zastosowany w obudowach HOV i VERSO. Te popularne obudowy są od lat instalowane na całym świecie i spełniają wymagania wynikające z bardzo różnorodnych zastosowań. Zainstalowane w nich kamery są zabezpieczone przed niszczącym wpływem otoczenia, zaś dobre warunki obserwacji są zapewniane dzięki zastosowaniu grzałki podgrzewającej przednią szybkę i wentylacji wnętrza obudowy powietrzem przepuszczanym przez specjalny, podwójny filtr. Dzięki temu nie następuje ani kondensacja pary wodnej, ani gromadzenie się lodu na przedniej szybce obudowy.

Obudowy HOV lub VERSO, które zostały już wcześniej zainstalowane, mogą być wyposażone w system IPM poprzez prostą wymianę układów elektronicznych. Pozwala to na swobodne zastąpienie analogowych systemów dozorowych urządzeniami cyfrowymi bez konieczności ponoszenia dużych kosztów i bez negatywnego wpływu na środowisko.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

MAS i ENAI podpisują umowę o sprzedaży i dystrybucji na terenie Europy

MAS, dostawca oprogramowania do automatyzacji zabezpieczeń, i **ENAI**, dostawca centrów automatyzacji do sterowni i alarmowych centrów odbiorczych, podpisały wzajemne porozumienie o sprzedaży i dystrybucji MASterMind – oprogramowania do automatyzacji nadzorowania alarmowych centrów odbiorczych – na terenie Europy, Bliskiego Wschodu i Afryki.

MASterMind – platforma programowa do profesjonalnego monitorowania – zapewnia możliwość konsolidacji i integracji wielu systemów bezpieczeństwa, w tym systemów antywłamaniowych, cyfrowych systemów telewizji dozorowej, systemów wykrywania pożaru i systemów mobilnych. MASterMind, wdrożona w czołowych stacjach monitorowania i firmach z listy Fortune 500 na całym świecie, charakteryzuje się automatyczną redundancją, sprawdzoną niezawodnością, skalowalnością i dużą mocą przetwarzania.

Firma MAS należy do UTC Climate, Controls & Security, firmy z grupy United Technologies Corp. (na terenie Polski działa firma z tej samej grupy – UTC Fire & Security Polska).

ENAI jest czołowym dostawcą systemów monitorowania alarmów na europejskim rynku zabezpieczeń. Oprogramowanie monitorujące ENAI i wieloprotokołowe odbiorniki RX-8000 sprawdziły się ze względu na prostotę użytkowania, skalowalność, wydajność i niezawodność.

Bezpośr. inf. Stijn van der Heijden
ENAI
Tłumaczenie: Redakcja

Wiosenne nowości firmy SATEL

Michał Konarski

Z początkiem 2013 roku firma SATEL uzupełnia ofertę o nowe produkty. Nowości w asortymencie to wynik nieustannych prac inspirowanych potrzebami i oczekiwaniami klientów oraz własną analizą rynku i zmianami w technologii. Zwiększając liczbę oferowanych produktów, firma SATEL dąży do usatysfakcjonowania klientów poszukujących kompleksowych rozwiązań, a także do ułatwienia codziennej pracy instalatora

Najważniejszą grupą wśród nowości są nowe czujki przeznaczone do tradycyjnych przewodowych instalacji alarmowych. Uzupełniają one dotychczas oferowane detektory.

Miniaturowa cyfrowa czujka ruchu TOPAZ jest wyposażona w zaawansowany układ cyfrowego przetwarzania sygnału. Jej konstrukcja jest efektem wieloletniego doświadczenia firmy SATEL w projektowaniu i produkcji niezawodnych czujek o doskonałych parametrach. Użycie procesora nowej generacji połączonego z pyroelementem wykonanym w technologii SMD oraz zaawansowanego algorytmu przetwarzania sygnałów umożliwiło uzyskanie właściwości, które dotychczas charakteryzowały jedynie urządzenia o znacznie większych gabarytach. Dużym ułatwieniem dla instalatora są wbudowane rezystory parametryczne, dzięki którym nie trzeba dodatkowo przygotowywać czujki do montażu. Wszystko to powoduje, że czujka TOPAZ jest idealna do zabezpieczania pomieszczeń mieszkalnych i biurowych, w których panują standardowe warunki środowiskowe.

Trend miniaturyzacji nie ominął również czujek dualnych, łączących technikę detekcji PIR i mikrofalową. Przykładem jest nowa czujka GREY. Dzięki zminiaturyzowaniu elementów (rozmiar 0402: 1 mm×0,5 mm) oraz zastosowaniu mikrofalowego sensora wykorzystującego częstotliwość 24 GHz czujka mieści się w obudowie tradycyjnej czujki PIR GRAPHITE. Jednak pomimo zewnętrznego podobieństwa ich wnętrza różnią się diametralnie, gdyż czujka GREY technologicznie wywodzi się z uznanej i cenionej czujki dualnej SILVER. Podobnie jak inne zaawansowane detektory firmy SATEL, czujka GREY ma pomocne funkcje zdalnego włączania sygnalizacji testowej LED oraz pamięci ostatniego zadziałania.

Ofertę uzupełnia również nowe pod względem funkcjonalności urządzenie – czujka NAVY z detektorem PIR oraz akustycznym detektorem zbicia szyby. Oba te detektory są zamknięte w zgrabnej obudowie, która nie odbiega pod względem wielkości od standardowych obudów czujek AQUA czy

Fot. 1. Najnowsze czujki firmy Satel: GREY, NAVY, TOPAZ

GRAPHITE. Takie urządzenie jest idealnym rozwiązaniem w przypadku ochrony przeszklonych pomieszczeń, do których można włamać się, wybijając okno. Czujka NAVY ułatwia instalację i eliminuje konieczność zastosowania dwóch odrębnych urządzeń – do wykrywania ruchu oraz do wykrywania zbicia szyby. Oczywiście każdy z torów detekcji posiada oddzielne wyjście sygnalizacji naruszenia, dzięki czemu właściwie skonfigurowana centrala będzie mogła precyzyjnie określić źródło ewentualnego alarmu. Oba te tory detekcji posiadają również odrębną regulację czułości. Tak jak w przypadku pozostałych czujek stłuczenia szyby, specjalistyczny tester akustyczny (tester INDIGO) ułatwia właściwe wyregulowanie toru akustycznego czujki NAVY. Do wykrywania ruchu wykorzystywana jest taka sama technologia detekcji jak w przypadku czujki GRAPHITE, co jest gwarancją poprawnego działania i odporności na fałszywe alarmy. Podobnie jak w tradycyjnych czujkach ruchu firmy SATEL, również w czujce NAVY można zastosować opcjonalne soczewki, dopasowując w ten sposób obszar detekcji do kształtu chronionego pomieszczenia.

Wśród nowości pierwszego kwartału 2013 są także kolejne urządzenia do systemów bezprzewodowych. Linia urządzeń ABAX została uzupełniona o nową magnetyczną czujkę otwarcia drzwi i okien AMD-103. W odróżnieniu od dostępnych dotąd AMD-100 i AMD-101 nowe urządzenie jest zamknięte w zminiaturyzowanej obudowie, którą łatwiej wkomponować w chronione pomieszczenie.

Fot. 2. Czujka magnetyczna AMD-103 przeznaczona dla systemu ABAX

Fot. 3. Czujka magnetyczna MMD-302 i czujka zbicia szyby MGD-300 przeznaczone dla systemu MICRA

Nowości nie ominęły także linii urządzeń bezprzewodowych przeznaczonych dla systemu MICRA. Magnetyczna czujka otwarcia drzwi i okien MMD-302 umożliwia podłączenie zewnętrznych czujek roletowych. Dzięki temu doskonale sprawdzi się w instalacjach, w których pierwszą linię ochrony mechanicznej tworzą przeciwwłamaniowe rolety wyposażone w czujniki podnoszenia. Po włączeniu tych czujek do systemu alarmowego już sam moment wyważania rolety może uruchomić sygnalizację alarmową.

Do linii MICRA należy też nowa czujka zbicia szyby MGD-300, która wykorzystuje cyfrową, wieloczęstotliwościową analizę dźwięku towarzyszącego zbiciu szyby, dzięki czemu prawdopodobieństwo wystąpienia fałszywego alarmu jest mniejsze. Dzięki wprowadzeniu tej czujki asortyment oferowanych urządzeń przeznaczonych dla systemu MICRA obejmuje praktycznie wszystkie główne rodzaje czujek wykorzystywanych w systemach wykrywania włamania.

Firma SATEL wprowadza do swojej oferty także trzy nowe sygnalizatory zewnętrzne. Pierwszy z nich, SP-4004, jest kontynuatorem linii wzorniczej sygnalizatorów serii SP-4000. Od pozostałych sygnalizatorów z tej serii odróżnia się przede wszystkim technologią wykonania. Całkowicie hermetyczna konstrukcja elektroniki wyposażona w sygnalizację akustyczną

Fot. 4. Sygnalizator zewnętrzny SP-4004 spełniający wymagania normy EN50131-4 dotyczące urządzeń stopnia 2

Fot. 5. Sygnalizatory SP-6500 i SD-6000 zostały wyposażone w wiele udogodnień ułatwiających instalację

z przetwornikiem piezoelektrycznym oraz sygnalizację optyczną LED spełnia wymagania normy EN50131-4 dotyczące urządzeń do zabezpieczeń stopnia 2. Dzięki temu sygnalizator ten będzie można zastosować w instalacjach, które wymagają pełnej zgodności z aktualnie obowiązującymi normami europejskimi.

Temu samemu stopniowi zabezpieczenia będą odpowiadać również nowe konstrukcje sygnalizatorów SD-6000 oraz SP-6500. Pierwszy z wymienionych jest wyposażony w dynamiczny przetwornik akustyczny o bardzo donośnym dźwięku, drugi zaś do sygnalizacji akustycznej wykorzystuje przetwornik piezoelektryczny. Oba urządzenia są zamknięte w obudowach z poliwęglanu, z pokrywą mocowaną na zawiasach. Dzięki temu nie trzeba szukać miejsca potrzebnego do odłożenia pokrywy, co może być ułatwieniem podczas montażu sygnalizatora w trudnych warunkach – na przykład wówczas, gdy trzeba skorzystać z drabiny. Ułatwieniem dla instalatora jest też poziomica, wbudowana w każdy z nowych sygnalizatorów, dzięki której łatwiej zadbać o estetykę wykonywanej instalacji. Wszystkie sygnalizatory z nowej serii umożliwiają przyłączenie akumulatora do zasilania pomocniczego, dzięki czemu można je stosować zarówno w trybie zasilania z centrali, jak też jako sygnalizatory z własnym zasilaniem.

Nadrzędnym celem projektantów firmy SATEL jest tworzenie urządzeń spełniających oczekiwania klientów. Aby dogłębnie poznać ich możliwości, warto wziąć udział w warsztatach w ramach Akademii SATEL. Dzięki zdobytej fachowej wiedzy można w pełni wykorzystać potencjał urządzeń firmy i nabyć umiejętności owocujących w codziennej pracy.

Michał Konarski
SATEL

Systemy alarmowe **Satel**

Skuteczna detekcja

Najnowsze czujki, rozszerzające bogatą gamę detektorów SATEL, to efekt ciągłych prac naszych specjalistów w celu osiągnięcia jak najwyższej jakości bazując na oczekiwaniach Klientów i zmianach w technologii komponentów.

GREY – Wykorzystanie zaawansowanej technologii montażu i miniaturyzacji komponentów w połączeniu z użyciem sensora mikrofalowego 24 Ghz umożliwiło stworzenie dualnej czujki ruchu w obudowie od tradycyjnej czujki PIR.

TOPAZ – Użycie procesora nowej generacji w połączeniu z zaawansowanym algorytmem przetwarzania sygnału pozwoliło na uzyskanie właściwości dostępnych dotąd jedynie w urządzeniach o większych rozmiarach, a wbudowanie rezystorów parametrycznych ułatwia instalację czujki.

NAVY – Połączenie w jednej obudowie detekcji ruchu z akustycznym detektorem zbicia szyby to rozwiązanie eliminujące konieczność stosowania dwóch odrębnych urządzeń do kompleksowej ochrony pomieszczeń.

Więcej informacji na
www.satel.pl

Satel®

Satel Sp. z o.o.
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, www.mieszkajbezpiecznie.pl

Komputerowa symulacja elektronicznego systemu bezpieczeństwa

Magdalena Kasprzak
Małgorzata Krawczyk
Robert Chmielewski
Adam Rosiński

W niniejszym artykule przedstawiamy koncepcję wykorzystania programu LabView i języka programowania graficznego G do symulacji elektronicznego systemu bezpieczeństwa. W dalszych badaniach można dokonać symulacji innych urządzeń elektronicznych stosowanych zarówno w systemach zabezpieczeń, jak i w telekomunikacji

Wprowadzenie

Obecnie bardzo często w procesie dydaktycznym, w którym przedmiotem jest wiedza dotycząca elektronicznych systemów bezpieczeństwa, stosuje się metody informatyczne. Metody te można zatem stosować w przypadku rzeczywistych urządzeń i systemów (np. w celu zaprogramowania i zmiany parametrów konfiguracyjnych systemu), ale także po to, by dokonać symulacji ich funkcjonowania. W tym celu można skorzystać z graficznego języka programowania i graficznego środowiska programistycznego LabView (od *ang. Laboratory Virtual Instrument Engineering Workbench*) firmy National Instruments. W dalszej części artykułu zostanie zaprezentowana zrealizowana koncepcja aplikacji symulującej funkcjonowanie systemu zabezpieczającego obiekt o specjalnym przeznaczeniu.

Aplikacja symulująca funkcjonowanie systemu

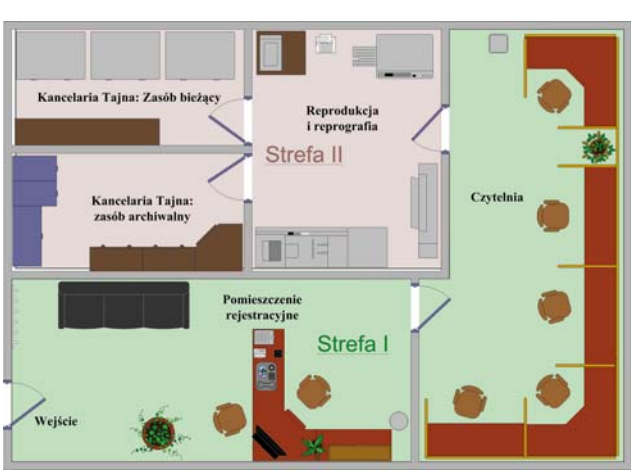
Programy pisane w środowisku LabView są nazywane instrumentami wirtualnymi (ang. *virtual instruments,* w skrócie VI), ponieważ ich wygląd i działanie imituje fizyczne przyrządy, takie jak oscyloskopy czy multimetry.

W środowisku LabView wykorzystuje się graficzny język programowania G. Powszechnie znane języki, takie jak C, C++, Pascal, FORTRAN, PERL, BASIC, COBOL, to języki imperatywne (proceduralne) wysokiego poziomu – dane są przetwarzane przez kolejno przywoływane i wykonywane procedury. Programowanie w języku G polega na logicznym powiązaniu piktogramów, z których składa się program. Do tego celu służą narzędzia umożliwiające zbieranie danych, ich analizę i wizualizację rezultatów.

Nie ma zatem potrzeby pisania jakiegokolwiek kodu źródłowego. Wszystko przedstawiane jest graficznie – za pomocą ikon. Połączone ikony tworzą diagram obrazujący przepływ danych – od źródła informacji, poprzez ich przetwarzanie, do końca obliczeń.

Dane mogą być wprowadzane do LabView ręcznie (przez użytkownika) lub poprzez zewnętrzne urządzenie elektroniczne. Dane wychodzące mogą być wyświetlane na ekranie monitora lub przesłane do zewnętrznego urządzenia.

Dzięki możliwości współpracy programu LabView z urządzeniami zewnętrznymi można traktować komputer jako urządzenie kontrolno-pomiarowo-sterujące. Program znalazł szerokie zastosowanie w wielu dziedzinach nauki, techniki i przemysłu.



Rys. 1. Plan pomieszczeń w chronionym obiekcie

Podsumowując, jest to program umożliwiający szybkie i w miarę dokładne odwzorowanie i zobrazowanie funkcjonowania istniejących bądź dopiero projektowanych urządzeń. Jego główną zaletą jest możliwość sporządzenia symulacji układu, urządzenia lub systemu bez konieczności przyswojenia i użycia skomplikowanych języków skryptowych.

Opis aplikacji

Opracowana aplikacja symuluje funkcjonowanie systemu bezpieczeństwa wykorzystującego centralę alarmową serii INTEGRA firmy Satel. Odwzorowano w niej jedynie podstawowe funkcje centrali, konieczne do zaprezentowania zabezpieczeń obiektu specjalnego przeznaczenia.

Na terenie chronionego obiektu (rys. 1) zostały wyodrębnione dwie strefy bezpieczeństwa:

– pomieszczenie rejestracyjne oraz czytelnia – strefa I,
– właściwa kancelaria tajna z pomieszczeniem do reprodukcji i reprografii – strefa II.

Po uruchomieniu symulacji obie strefy zostają wyłączone z dozoru. Można symulować pojawienie się intruzów w pomieszczeniach (przyciski) lub swobodnie otwierać drzwi do stref (kliknięcie na intruza w drzwiach). Nie spowoduje to uruchomienia alarmu. Okno programu symulacyjnego pokazano na rys. 2.

System można załączyć w dozór na trzy sposoby:

– wpisując na klawiaturze kod 1111# – spowoduje to załączenie tylko strefy I, czyli pomieszczenia rejestracyjnego i czytelni;
– wpisując na klawiaturze kod 4444# – spowoduje to załączenie tylko strefy II, czyli właściwej kancelarii tajnej z pomieszczeniem do reprodukcji i reprografii;
– wpisując na klawiaturze kod 2222# – spowoduje to załączenie obu stref.

Kody wprowadza się, używając symulowanej klawiatury manipulatora. W przypadku pomyłki wprowadzone cyfry można skasować przyciskiem z gwiazdką na symulowanym manipulatorze.

Jeśli dana strefa jest załączona w dozór, to otwarcie drzwi do tej strefy lub symulacja pojawienia się w niej intruza wywoła w niej alarm (obecność intruza jest symbolizowana przez większy symbol postaci – rys. 3) – na manipulatorze włączy się czerwona lampka alarmu i pojawi się informacja, która strefa została naruszona. Jeżeli intruz zostanie wykryty przez czujkę, będzie wiadomo, która czujka go wykryła – włączy się

Rys. 3. Alarm włamaniowy w strefie pierwszej

na niej czerwona lampka. Dodatkowo sygnalizator znajdujący się przy głównych drzwiach wejściowych do kancelarii zmieni kolor na czerwony.

Alarm może zostać uruchomiony również za pomocą przycisku napadowego (kliknięcie na symbol rączki przy biurku w pomieszczeniu rejestracyjnym). W tym przypadku nie ma znaczenia, czy system jest uzbrojony.

Aby wyłączyć alarm, trzeba wpisać kod przyporządkowany do określonej strefy.

System sygnalizacji pożarowej nie wymaga załączenia w dozór – czujki oraz ręczne ostrzegacze pożarowe są ciągle w stanie czuwania. Po uruchomieniu aplikacji kliknięcie ikony pożaru ( ) spowoduje uruchomienie alarmu w danej strefie. Trwający pożar jest reprezentowany przez trzy płomienie (rys. 4). Tak jak w przypadku symulacji systemu sygnalizacji włamania i napadu, na manipulatorze włączy się czerwona lampka, pojawi się informacja, w której strefie wystąpiło zagrożenie pożarowe, a czujka, która wykryła pożar, zmieni kolor na czerwony. Również sygnalizator nad drzwiami głównymi zmieni kolor na czerwony.

Aby wyłączyć alarm, trzeba wpisać kod 3333#, jednak samo wpisanie kodu nie wystarczy – tak jak w rzeczywistym systemie sygnalizacji pożarowej. Należy ponownie kliknąć ikonę symbolizującą pożar, aby poinformować, że zagrożenie zostało zlikwidowane (pożar został ugaszony), i dopiero wtedy wpisać kod na manipulatorze.

Alarm można wywołać również ręcznym ostrzegaczem pożarowym (ROP). Za pomocą przycisków ROP ( ) można natychmiast wywołać alarm pożarowy w strefach, w których są umieszczone. Kliknięcie przycisku jest sygnalizowane zaświeceniem się na żółto znajdujących się na nim strzałek. Aby wyłączyć alarm pożarowy, należy ponownie kliknąć przycisk pożarowy, co symuluje użycie specjalnego kluczyka do wyłączania przycisków ROP, a potem wpisać kod 3333#.

Rys. 2. Okno programu LabView

Podsumowanie

Opisane powyżej przykładowe rozwiązanie umożliwia studentom szybką i prostą analizę powiązań logicznych i porównawczych pomiędzy elementami

Rys. 4. Alarm pożarowy w strefie pierwszej

reprezentującymi wartości wejściowe i wyjściowe danego typu systemu. Dzięki temu mogą oni poznać zasady funkcjonowania języka graficznego G, a jednocześnie zdobywają i wykorzystują umiejętność stosowania go do symulacji.

Możliwe jest także wykorzystanie w symulacji realnych urządzeń zewnętrznych. Można wykorzystać w tym celu interfejsy znajdujące się w komputerze (np. USB, RS232, LAN). Umożliwi to komunikację pomiędzy urządzeniami a systemem, a więc przepływ danych pomiędzy nimi. W dalszych badaniach przewiduje się opracowanie aplikacji symulujących funkcjonowanie innych urządzeń elektronicznych stosowanych zarówno w informatyce, jak i w telekomunikacji.

Można stworzyć symulacje systemów wykorzystujących centrale innych typów (np. MAXSYS firmy DSC czy ProSYS 128 firmy RISCO). Należy tylko zmienić manipulator na odpowiedni, a program zmodyfikować, wykorzystując graficzny język programowania G.

inż. Magdalena Kasprzak
inż. Małgorzata Krawczyk
inż. Robert Chmielewski
dr inż. Adam Rosiński
Politechnika Warszawska
Wydział Transportu
Zakład Telekomunikacji w Transporcie

Bibliografia

1. Buczaj M., *Systemy sterowania i nadzoru szyte na miarę, Zabezpieczenia* Nr 6(88)/2012, Warszawa 2012.
2. Krawczyk M., Kasprzak M., *System Bezpieczeństwa w Składnicy Map i Dokumentów Geodezyjnych o Klauzuli Niejawnej,* praca inżynierska, Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej i Technik Bezpieczeństwa, Warszawa 2011.
3. Norma PN-EN 50131-1:2009: *Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.*
4. Rosiński A., *Programowanie systemów sygnalizacji włamania i napadu*, *13th International Conference Computer systems aided science, industry and transport*, TRANSCOMP 2009, Zakopane 2009.
5. Szulc W., Rosiński A., *Systemy sygnalizacji włamania (Część 1). Konfiguracje central alarmowych, Zabezpieczenia* Nr 2(66)/2009, Warszawa 2009.

Bezpieczeństwo komunikacji radiowej w systemach alarmowych

Krzysztof Adamczyk

Na rynku systemów sygnalizacji włamania i napadu dominują rozwiązania przewodowe, jednak coraz częściej instalatorzy i użytkownicy sięgają po systemy bezprzewodowe. Są one najczęściej montowane w obiektach, w których nie ma instalacji kablowej umożliwiającej zastosowanie urządzeń przewodowych

Wielu producentów systemów zabezpieczeń zaczęło szukać rozwiązania tego problemu, a mianowicie urządzeń alarmowych komunikujących się drogą radiową. Jedną z pierwszych firm, która postanowiła podjąć to wyzwanie, jest Jablotron. Firma powstała w 1990 roku w Czechach, w miejscowości Jablonec. Pierwotnym zadaniem firmy było nadzorowanie wdrażania nowych technologii do urządzeń przemysłowych. Po krótkim czasie postanowiono, że firma będzie tworzyć własne urządzenia zabezpieczające. Głównym założeniem było opracowanie systemu zabezpieczeń wykorzystującego łączność bezprzewodową, gdyż właściciele firmy zauważyli zapotrzebowanie na takie właśnie rozwiązania. Po opracowaniu projektów poprzedzonych dokładnymi badaniami rozpoczęto produkcję urządzeń. Pomysł okazał się strzałem w dziesiątkę. Początkowo prowadzono sprzedaż wyłącznie na rynku czeskim. Później do oferty trafiały coraz to nowe urządzenia, a firma zaczęła się bardzo dynamicznie rozwijać. Przybywało pracowników, poszerzał się rynek zbytu. Produkty Jablotron znajdowały odbiorców w innych krajach europejskich.

Obecnie firma zatrudnia ponad pięciuset pracowników, a swoje produkty eksportuje do ponad siedemdziesięciu krajów w Europie i poza nią.

Początkowe obawy użytkowników i instalatorów dotyczące urządzeń bezprzewodowych stopniowo ustępowały, gdyż dopracowana technologia i jakość zostały potwierdzone poprawnym i bezawaryjnym działaniem przez wiele lat. Wyroby Jablotron trafiły na rynek polski w roku 1996 za sprawą firmy DPK System z Wieliczki, która została autoryzowanym importerem i dystrybutorem czeskiego producenta.

Przy porównaniu urządzeń przewodowych i bezprzewodowych od razu widać różnicę w cenie. Urządzenia bezprzewodowe są droższe. Całkowity koszt inwestycji bywa jednak mniejszy, gdyż okablowanie i ewentualny remont w przypadku instalowania systemu przewodowego wiąże się z dodatkowymi kosztami. Zaletą systemów bezprzewodowych jest również ich mobilność. Na życzenie klienta instalator może bez trudu zmienić lokalizację urządzeń bez większych uszkodzeń elewacji. Najemcy lokali użytkowych mogą „zabrać" system ze sobą w przypadku przeprowadzki.

Pierwszy system bezprzewodowy firmy Jablotron, który trafił na rynek polski, to JA-50. System ten zdobył uznanie odbiorców. Przełomem w branży zabezpieczeń bezprzewodowych okazały się jednak centrale JA-60 – Comfort i Profi, które jako pierwsze komunikowały się radiowo z wykorzystaniem kodów dynamicznych. Ponadto wraz systemem JA-60 firma Jablotron wprowadziła na rynek pierwsze urządzenia komunikujące się dwukierunkowo (manipulator i sygnalizator).

Pięć lat później, w 2006 roku, producent wypuścił na rynek system z serii JA-80 – OASiS. Nowatorskim rozwiązaniem było zastosowanie bezprzewodowego manipulatora LCD z wbudowanym czytnikiem oraz sygnalizatora zewnętrznego. Obydwa urządzenia wykorzystywały komunikację radiową i nie trzeba było zasilać ich z sieci.

Jeśli dla klienta wyższa cena systemu bezprzewodowego nie jest barierą, to mogą pojawić się pytania o bezpieczeństwo systemu i jego odporność na próby sabotażu oraz fałszywe alarmy. Oczywiście nie istnieje idealne zabezpieczenie. Każdy system można „złamać". W przypadku rozwiązań przewodowych wydaje się to trudniejsze, gdyż trzeba dostać się do przewodów, aby to uczynić, a to dopiero pierwszy krok. Aby zrobić następne, trzeba posiadać odpowiednią wiedzę i nadzieję, że instalator nie dołożył wystarczających starań w momencie montażu lub popełnił błędy. W przypadku systemów bezprzewodowych sabotaż może wydawać się łatwiejszy. Może wydawać się, że wystarczy kupić „zagłuszacz" sygnału radiowego za kilkaset złotych, aby zagłuszyć sygnał. Gdyby tak było, systemy bezprzewodowe nie miałyby racji bytu i z pewnością nie mogłyby być przeznaczone do ochrony obiektów. Jeśli system jest zamontowany prawidłowo, to centrala jest zlokalizowana w takim miejscu, że nie ma do niej łatwego dostępu i nie można się do niej zbliżyć na tyle blisko, aby „zagłuszaczem" wpłynąć na jej działanie. Ponadto centrale firmy Jablotron mogą wykrywać próby zagłuszeń. Zapiszą ewentualną próbę w pamięci zdarzeń, zablokują możliwość wyłączenia systemu z dozoru na czas zagłuszania oraz wyślą wiadomość do użytkownika i do stacji monitorowania.

Na szkoleniach prowadzonych przez importera, firmę DPK System, niejednokrotnie pojawiał się temat bezpieczeństwa i odporności urządzeń firmy Jablotron na próby zakłócania. Instalatorzy wielokrotnie testowali systemy pod tym kątem, używając przyniesionych „zagłuszaczy". W żadnym z przypadków nie udało im się osiągnąć celu. Można oczywiście próbować zakłócić komunikację samej bezprzewodowej czujki alarmowej, co wydaje się łatwiejsze, ale produkty Jablotron są wyposażone

Rys. 1. Historia wyrobów Jablotron

w odpowiednie zabezpieczenia. Każda czujka musi co określony czas zgłaszać się do centrali. Jeśli ktoś ją zagłuszy na tyle, że sygnał zgłoszenia obecności nie dotrze do centrali, to zostanie to potraktowane jako próba sabotażu konkretnego urządzenia i użytkownik zostanie o tym poinformowany.

Warto również zaznaczyć, że wszystkie centrale firmy Jablotron wykorzystują dwukierunkową komunikację radiową. W ten sposób komunikuje się również część urządzeń peryferyjnych, np. manipulatory, sygnalizatory, wybrane czujki ruchu i czujki pożarowe. Standardowa czujka ruchu bądź otwarcia nie musi komunikować się dwukierunkowo, gdyż nadzoruje się ją na podstawie sygnałów zgłoszeń wysyłanych przez nią do centrali. Komunikacja zwrotna nie jest potrzebna. Mogłaby być wykorzystana do konfigurowania urządzenia, ale w przypadku urządzeń Jablotron ustawienia czujek i typ reakcji zapisywane są w centrali i nie ma potrzeby wysyłania ich do czujek. Czułość ustawiana jest bezpośrednio w czujce, fizycznie, przełącznikiem *DIP*. Takie rozwiązanie w zupełności wystarcza i nie komplikuje niepotrzebnie komunikacji radiowej systemu. Dzięki temu systemy Jablotron cechują się wysokim poziomem stabilności działania, bardzo niskim poziomem awaryjności, długą żywotnością baterii, a przemyślane rozwiązania bazujące na dwudziestoletnim doświadczeniu firmy są potwierdzone certyfikatami europejskimi stopnia 2. Można je znaleźć na stronie *www.jablotron.pl* przy każdym produkcie.

Dociekliwi mogą zapytać o możliwość skopiowania sygnałów, np. sygnału wysyłanego przez pilota podczas wyłączania z dozoru. Skopiowanie sygnału jest oczywiście możliwe, jednak system nie zareaguje na tak pozyskany kod. Stanie się tak, ponieważ urządzenia wysyłają za każdym razem inny sygnał, co jest związane z dynamicznie zmiennym szyfrowaniem. Centrala zignoruje skopiowany sygnał.

Warsztaty prowadzone w Wieliczce dowodzą również, że systemy Jablotron mogą pracować blisko siebie bez wzajemnego zakłócania komunikacji radiowej. Zajęcia warsztatowe odbywają się w jednym pomieszczeniu, w którym wykorzystuje się cztery centrale z modułami radiowymi, bezprzewodowymi czujkami, manipulatorami i pilotami. Centrale są oddalone od siebie mniej więcej o jeden metr. Zajęcia są prowadzone od trzech lat, średnio dwa razy w miesiącu i nigdy nie zdarzyło się zakłócenie jednego z systemów przez inny. Pomimo tak małych odległości między centralami w tym samym czasie można je niezależnie załączać pilotami, sterować nimi za pomocą bezprzewodowych manipulatorów, a bezprzewodowe czujki mogą generować alarmy odbierane w powiązanych z nimi centralach. Ma to duże znaczenie na przykład wówczas, gdy monitoruje się osiedle domków szeregowych, mieszkania w kamienicach, pawilony handlowe lub inne obiekty, w których zainstalowane są co najmniej dwa systemy bezprzewodowe, a zasięgi ich elementów krzyżują się.

Jablotron stale udoskonala swoje produkty. Wdraża nowe technologie i rozwiązania, które mają podwyższyć poziom bezpieczeństwa, zwiększyć komfort użytkowania i umożliwić prawidłową, stabilną pracę wszystkich elementów, a zwłaszcza central alarmowych. Mam nadzieję, że podane w artykule informacje przekonają sceptyków do bezprzewodowych systemów sygnalizacji włamania i napadu i rozwieją wiele wątpliwości z nimi związanych.

Krzysztof Adamczyk
DPK System

Security Products SINCE 1991 roger

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.
- **INTEGRACJA** z innymi systemami:

RCP CCTV SSWiN

RCP Master *PR602LCD*

roger®

www.roger.pl

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Wprowadzono do oferty **PS-15DR** i **PS-30DR** - moduły zasilające do systemów kontroli dostępu.

Nowoczesne zabezpieczenia w supermarkecie

Karolina Łokietek

Integracja systemów bezpieczeństwa, gromadzenie i analiza danych, wykorzystanie zaawansowanych technologicznie rozwiązań, zwiększanie efektywności prowadzenia działalności biznesowej to tylko wybrane zadania zarządców nowoczesnych obiektów handlowych. Właściciele czy administratorzy supermarketów i hipermarketów, od wielu lat funkcjonujących na polskim rynku i oferujących bogaty asortyment w konkurencyjnych cenach, dbają nie tylko o zapobieganie stratom wynikającym z kradzieży, ale także o wysoką jakość, energooszczędność, skuteczność i estetykę wdrażanych rozwiązań

Jednym z takich obiektów jest hipermarket E.Leclerc zlokalizowany na warszawskim Ursynowie. E.Leclerc funkcjonuje na polskim rynku od 1995 roku i jest najdłużej działającą siecią sklepów w Polsce, a dzięki przywiązaniu konsumentów obecnie liczy ponad sto obiektów w Europie i czterdzieści sklepów w Polsce (zlokalizowanych w trzydziestu sześciu miastach). Najstarszy obiekt sieci to obecnie nie tylko hipermarket, ale także galeria handlowa i budynek biurowy. Aby zapewnić najwyższą jakość usług, jego zarządcy poszukiwali doświadczonego partnera biznesowego oferującego kompleksowy pakiet usług i rozwiązań z dziedziny elektronicznych systemów zabezpieczeń i ochrony przeciwpożarowej. Priorytetem było zapewnienie najwyższego poziomu bezpieczeństwa klientom i przebywającym w obiekcie pracownikom. Nie mniej istotne było zagwarantowanie konsumentom komfortu podczas zakupów. Dbając o koszty prowadzenia biznesu, właściciele ursynowskiego obiektu zwrócili uwagę również na energooszczędność zaawansowanych technologicznie systemów i możliwość ich zintegrowania.

Fot. 1. E.Leclerc Warszawa Ursynów – System UltraExit – rozstaw do 2,4 m – fot. z archiwum AGIS Fire & Security

Wdrożenie przez firmę Agis Fire & Security zabezpieczeń w obiekcie E. Leclerc zostało poprzedzone wnikliwą analizą potrzeb i oczekiwań inwestora. Następnie specjalny zespół czuwał nad odpowiednim zainstalowaniem i uruchomieniem między innymi elektronicznych systemów przeciwkradzieżowych marki Sensormatic (których AGIS Fire & Security jest wyłącznym dystrybutorem), systemów nadzoru wizyjnego z wysokiej klasy urządzeniami firmy American Dynamics, systemów sygnalizacji włamania i napadu, dźwiękowych systemów ostrzegawczych, systemów sygnalizacji pożarowej, a także systemów zarządzania budynkami umożliwiających sterowanie mediami (instalacjami wodnymi, sanitarnymi, oświetleniowymi, centralami wentylacyjnymi, kotłowniami itp.) wszystkich budynków z jednego miejsca. Z myślą o klientach zmotoryzowanych wdrożono również system monitorowania zajętości parkingu i system sterowania szlabanami parkingowymi.

W celu zapewnienia skutecznej ochrony przeciwkradzieżowej w bardzo szerokim wejściu na teren sklepu zainstalowano system Ultra Exit marki Sensormatic o największym na rynku rozstawie bramek sięgającym 2,4 m przy użyciu tylko jednej anteny (największy na rynku rozstaw przy zastosowaniu standardowych zabezpieczeń twardych – klipsów). System ten wykazuje dużą odporność na zakłócenia oraz charakteryzuje się doskonałymi parametrami detekcji i wykrywalności. Można także zintegrować go z takimi systemami zewnętrznymi jak np. system nadzoru wizyjnego, co znacznie usprawnia zarządzanie bezpieczeństwem w sklepie. Bramki przeciwkradzieżowe są także doskonałymi nośnikami reklamowymi.

Swobodny ruch klientów korzystających z wózków sklepowych, a także skuteczną ochronę przeciwkradzieżową przy zachowaniu odpowiedniej widoczności i estetyki zapewniają systemy przeciwkradzieżowe Ultra Lane marki Sensormatic zainstalowane na liniach przykasowych. Ażurowa konstrukcja płaskich i estetycznych bramek pozwala na zachowanie odpowiedniej przestrzeni w przejściu kasowym i nie ogranicza widoczności. Jedna antena systemu Ultra Lane umożliwia zabezpieczenie przejścia po obu stronach, a do obsługi czterech alejek kasowych wymagany jest tylko jeden kontroler, co sprawia, że rozwiązanie jest ekonomiczne, a urządzenia nie zajmują dużej powierzchni.

Nowoczesne systemy przeciwkradzieżowe są nie tylko skuteczne i energooszczędne – posiadają także szereg dodatkowych funkcji, takich jak np. zliczanie klientów (umożliwiające zaplanowanie odpowiedniej obsady personelu sklepowego) czy wykrywanie metali, dzięki któremu obsługa sklepu może być informowana o tym, że do sklepu wchodzi klient wnoszący torbę ułatwiającą kradzież (zdarza się, że złodzieje używają toreb wyłożonych folią aluminiową lub plecaków izotermicznych – w ten sposób starają się „oszukać" bramki przeciwkradzieżowe).

Fot. 2. E.Leclerc Warszawa Ursynów – System UltraLane – fot. z archiwum AGIS Fire & Security

Ułatwia to wykrycie potencjalnych złodziei. Niewątpliwą zaletą systemu jest to, że nie reaguje na takie przedmioty jak klucze czy telefony komórkowe.

System przeciwkradzieżowy powinien być dopasowany do rodzaju prowadzonej działalności. Firma AGIS oferuje swoim klientom fachową radę i pomoc przy wyborze rozwiązania – z uwzględnieniem potrzeb odbiorcy, wystroju wnętrza i dostępnego budżetu. Po zainstalowaniu systemu w punkcie handlowym personel sklepu jest szkolony w zakresie jego obsługi, a pracownicy serwisu technicznego AGIS Fire & Security czuwają nad jego właściwą pracą. Na wypadek jakichkolwiek wątpliwości dotyczących pracy systemu lub jego obsługi pracownicy telefonicznego Centrum Obsługi Klienta AGIS są do dyspozycji użytkowników.

Projekt wdrożenia wymienionych systemów w obiekcie E.Leclerc powierzono firmie AGIS Fire & Security głównie z uwagi na kompleksową ofertę tej firmy, która obejmuje wykonywanie „pod klucz" instalacji niskoprądowych, teletechnicznych i stałych instalacji gaśniczych, a także ze względu na pełny pakiet usług konserwacyjnych i serwisowych oraz bogate doświadczenie w realizacji wielu różnych projektów w zróżnicowanych sektorach rynku. AGIS Fire & Security stale udoskonala swoją ofertę, dbając o to, by oferowane rozwiązania i usługi odpowiadały najwyższym standardom, czego potwierdzeniem są po raz kolejny uzyskane przez firmę certyfikaty ISO 9001:2008 oraz AQAP 2110:2009, przyznane przez Zakład Systemów Jakości i Zarządzania.

Karolina Łokietek
AGIS Fire & Security

TWOJE OCZEKIWANIA NASZE ROZWIĄZANIA!

D-TECT - Zewnętrzne czujniki ruchu

Pewność detekcji oraz duża łatwość i szybkość instalacji

- METALOWE OBUDOWY UŁATWIAJĄCE MONTAŻ
- CYFROWA ANALIZA SYGNAŁU
- PRECYZJA I SZEROKI ZAKRES REGULACJI OPTYKI
- PROGRAMOWANA CZUŁOŚĆ

GJD
DETECT & SECURE

NOWOCZESNE CZUJKI UMOŻLIWIAJĄ PRZEPROWADZENIE INSTALACJI PROŚCIEJ I SZYBCIEJ NIŻ KIEDYKOLWIEK

Od ponad 30 lat brytyjska firm GJD jest oddana procesowi podnoszenia jakości i wydajności swoich produktów. Efektem tych działań jest doskonała linia przewodowych zewnętrznych czujników D-TECT.

Uważne wsłuchiwanie się w potrzeby klientów jest gwarancją ciągłego podnoszenia jakości naszych detektorów.

www.adiglobal.com/pl | tel.: +48 91 485 40 60-69 | info.pl@adiglobal.com

ADI
GLOBAL DISTRIBUTION

Tel.: +48 91 485 40 60-69 / Fax: +48 91 485 40 80
ADI jest marką handlową firmy Ultrak Security Systems Sp.z o.o.

www.adiglobal.com/pl

FAAST i FAAST LT

Czujki zasysające w zastosowaniach specjalnych

Sebastian Nowak
Bernard Sokół

W ochronie przeciwpożarowej obiektów coraz częściej wykorzystuje się czujki zasysające. Jako elementy składowe profesjonalnych systemów sygnalizacji pożarowej są one dosyć nowe, ale stosowano je już na początku lat 80. XX wieku. Do niedawna w Polsce panowało powszechne przekonanie, że są to urządzenia bardzo drogie, po które sięga się dopiero wtedy, gdy nie można zastosować tradycyjnych czujek punktowych ze względu na konstrukcję obiektu, wygląd czy szczególne wymagania dotyczące poziomu zabezpieczenia przeciwpożarowego. W ostatnich latach czujki tego typu zostały udoskonalone. Są wykorzystywane coraz chętniej i bardzo często nie tylko uzupełniają standardowe systemy wykrywania pożaru, ale są fundamentem skutecznego zabezpieczenia obiektu

– Zabezpieczenie pożarowe chłodni często stwarza trudności ze względu na różnice temperatur mogących powodować wysoki stopień kondensacji. Dzięki zastosowaniu dualnego systemu detekcji (podczerwonego lasera i niebieskiej diody LED) czujki FAAST odróżniają dym od cząstek niedymowych, co ogromnie zwiększa skuteczność wykrywania i zapewnia odporność na fałszywe alarmy. Zdalne monitorowanie i „odpytywanie" czujek FAAST za pośrednictwem TCP/IP ułatwia kontrolowanie obiektu w dzień i w nocy. Dostęp do informacji o stanie obiektu, możliwy do uzyskania w dowolnym miejscu, zapobiega niepotrzebnym ewakuacjom lub aktywacjom systemów gaszenia.

Kierownik obiektu w firmie chłodniczej

Zastosowanie czujek zasysających umożliwia efektywną detekcję w miejscach, w których użycie tradycyjnych czujek punktowych jest utrudnione lub wręcz niemożliwe z uwagi na warunki panujące w otoczeniu (np. warunki środowiskowe) lub charakter obiektu (np. obiekt jest zabytkiem objętym ochroną konserwatorską).

Należąca do korporacji Honeywell firma System Sensor opracowała nową generację czujek zasysających FAAST (*Fire Alarm Aspiration Sensing Technology*). Można je stosować nawet w najbardziej skomplikowanych instalacjach i skrajnie trudnych warunkach. Wykorzystano w nich najnowocześniejsze technologie detekcyjne i komunikacyjne.

FAAST – ultraczułe czujki zasysające

Czujka zasysająca FAAST jest ultraczułym urządzeniem do detekcji dymu, odpornym na fałszywe alarmy mogące zakłócać działanie systemu.

Podstawowe cechy systemu FAAST

– **pierwsza tego rodzaju trzystopniowa filtracja**, na którą składa się m.in. tak zwany filtr skrzydłowy (rozwiązanie pochodzi z przemysłu lotniczego) uniemożliwiający wszelkim cząstkom mierzącym więcej niż 25 mikrometrów przedostanie się do komory detekcyjnej, co ogranicza występowanie fałszywych alarmów;

Fakty

– przerwy w ciągłości działania serwerów mogą być przyczyną poważnych strat finansowych i wizerunkowych;
– łączny koszt niedawnych awarii w 41 centrach przetwarzania danych przekroczył 20 milionów dolarów;
– 64% pożarów w budynkach komercyjnych jest spowodowanych awariami układu zasilania lub systemu klimatyzacji (bez których serwerownie nie mogą działać).

– **Dual Vision** – zastosowanie detekcji z wykorzystaniem lasera IR i niebieskiej diody LED oraz użycie zaawansowanych algorytmów odczytu pozwala na odróżnienie cząsteczek dymu od pyłu itp., co uniemożliwia występowanie fałszywych alarmów;
– **ultraczuła detekcja** wykrywająca zadymienie od 0,0015%/m;
– **komunikacja TCP/IP przez Internet** umożliwiająca zdalne monitorowanie oraz zarządzanie systemem z każdego

FAAST zapewnia

– optymalną, stałą ochronę przeciwpożarową;
– większe możliwości zarządzania danymi i sprzętem;
– więcej czasu na przeniesienie danych (nawet dwie godziny);
– ograniczenie zakłóceń lub przerw w działalności firmy;
– uniknięcie konieczności instalowania stałych systemów gaszenia;
– możliwość stałego monitorowania systemu w czasie rzeczywistym – przez Internet (z wykorzystaniem komputera, tabletu, smartfonu itp.).

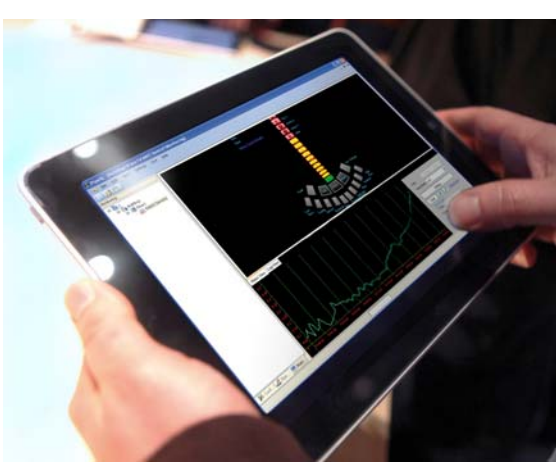
Fot. 1. Czujki FAAST i FAAST LT

miejsca na świecie dzięki możliwości integracji z sieciami lokalnymi oraz rozległymi.

Czujka FAAST doskonale sprawdzi się w obiektach o znaczeniu krytycznym, np. w centrach przetwarzania danych, laboratoriach farmaceutycznych, zakładach produkujących elektronikę przemysłową. W takich obiektach skuteczność tradycyjnych systemów detekcji może być znacznie ograniczona z powodu intensywnej cyrkulacji powietrza wymuszonej przez urządzenia klimatyzacyjne. Aby zapobiec wystąpieniu potencjalnych szkód, należy stosować systemy umożliwiające bardzo wczesną detekcję.

FAAST LT – wykrywanie pożarów w najtrudniejszych warunkach

Są dwie wersje czujki FAAST LT: adresowalna, przeznaczona do użycia na pętli detekcyjnej, pracująca pod nadzorem protokołu System Sensor, oraz konwencjonalna, którą można stosować na linii konwencjonalnej dowolnej centrali pożarowej. Czujka w wersji adresowalnej może być w pełni kontrolowana i zarządzana poprzez centralę sygnalizacji pożarowej. Do detekcji



Fot. 2. Zdalna obsługa czujki FAAST za pośrednictwem TCP/IP

– W procesie produkcji farmaceutycznej generowane są duże ilości bardzo małych cząsteczek kurzu. Zastosowanie standardowego systemu wykrywania pożaru mogłoby prowadzić do wielu fałszywych alarmów, stąd nasza decyzja o wyborze czujek zasysających FAAST. Zastosowana w nich inteligentna technologia rozróżniania cząstek dymu i innych sprawdza się doskonale i daje nam pewność, że ewentualne zagrożenie pożarem zostanie wykryte bardzo wcześnie. Można przyznać, że dzięki temu wzrosła produktywność naszego zakładu.

Kierownik zakładu w znanej firmie farmaceutycznej

dymu wykorzystywany jest optyczny czujnik laserowy. Konfigurację rurek zasysających wspomaga dedykowany program PipeIQ LT. FAAST LT ma podobny do czujki FAAST panel czołowy, bezpośrednio pokazujący status urządzenia.

Czujki FAAST LT zapewniają wysoką czułość detekcji w obiektach, w których zastosowanie czujek punktowych jest utrudnione, niemożliwe lub nieracjonalne. Można je zastosować na przykład w obiektach o dużych powierzchniach, np. w halach produkcyjnych lub atriach, w których dostęp do czujek punktowych w celach serwisowych byłby utrudniony. FAAST LT jest również rozwiązaniem alternatywnym do liniowych czujek dymu instalowanych na przykład w magazynach wysokiego składowania.

FAAST LT jest również doskonałym rozwiązaniem w przypadku w miejsc o dużym zapyleniu (szyby windowe, budynki przeznaczone do hodowli zwierząt, stolarnie, taśmociągi przewożące materiały sypkie, zakłady przemysłu chemicznego itp.). Coraz powszechniejsze jest stosowanie urządzeń FAAST LT w jednostkach penitencjarnych, gdzie tradycyjne czujki punktowe narażone są na złośliwą dewastację. Kolejnym z wielu typowych zastosowań jest montaż w chłodniach, zakładach produkcji artykułów spożywczych lub w miejscach o podwyższonej wilgotności.

Atuty FAAST LT

- czujka laserowa stosowana w kilku generacjach wysokoczułej detekcji dymu;
- ultradźwiękowy pomiar przepływu powietrza umożliwiający szybką identyfikację zablokowanych otworów próbkujących;
- przyjazny interfejs użytkownika obniżający koszty uruchomienia i obsługi;
- łatwy dostęp do komponentów wymiennych, np. filtrów pyłu, czujek typu plug-in;
- klasa szczelności IP65 (elektronika jest zabezpieczona; czujki można zainstalować w miejscach, w których mogą występować duże zanieczyszczenia);
- pakiet oprogramowania PipeIQ LT wspomagający konfigurację rur systemu oraz przygotowujący zestawienie materiałowe;
- na panelu czołowym łatwo sprawdzić kluczowe parametry;
- różne tryby pracy (dzienny, nocny, świąteczny) – pozwalają na dobranie odpowiedniego ustawienia dla rodzaju obiektu;
- możliwość importowania plików z wielu pakietów CAD ułatwiających projektowanie.

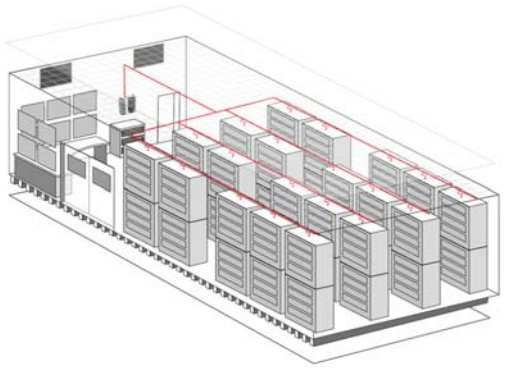
Typowe miejsca, w których stosuje się czujki FAAST LT

– zabytkowe budynki, w których nie można zamontować czujek punktowych (np. ze względu na estetykę);
– obiekty przemysłowe, w których temperatura (wysoka bądź niska) lub zanieczyszczone powietrze uniemożliwiają użycie czujek punktowych (np. zakłady przemysłu spożywczego);
– miejsca, w których może dojść do dewastacji zainstalowanego sprzętu (np. czujek punktowych) – dotyczy to środków publicznego transportu, jednostek penitencjarnych itp.;
– duże obiekty o bardzo wysokich sufitach, w których montaż i serwis czujek punktowych lub liniowych może być utrudniony;
– małe serwerownie (wczesna detekcja klasy A według EN54-20);
– obiekty, w których hoduje się zwierzęta, magazyny itp.

Dobór techniki wykrywania pożaru – wyzwanie dla projektantów i instalatorów

Dobry projekt systemu detekcji pożaru jest często kompromisem – zagrożenia muszą być szybko wykrywane, ale zarazem trzeba ograniczyć ryzyko występowania fałszywych alarmów.

Szczególnie trudne jest projektowanie systemów dla obiektów zabytkowych. Podlegają one specjalnej ochronie konserwatorskiej i bardzo często trudno jest zarazem zachować pierwotną architekturę w nienaruszonym stanie i jednocześnie właściwie zabezpieczyć je przed pożarem.



Rys. 1. Przykładowe zastosowanie czujki zasysającej – sterownia

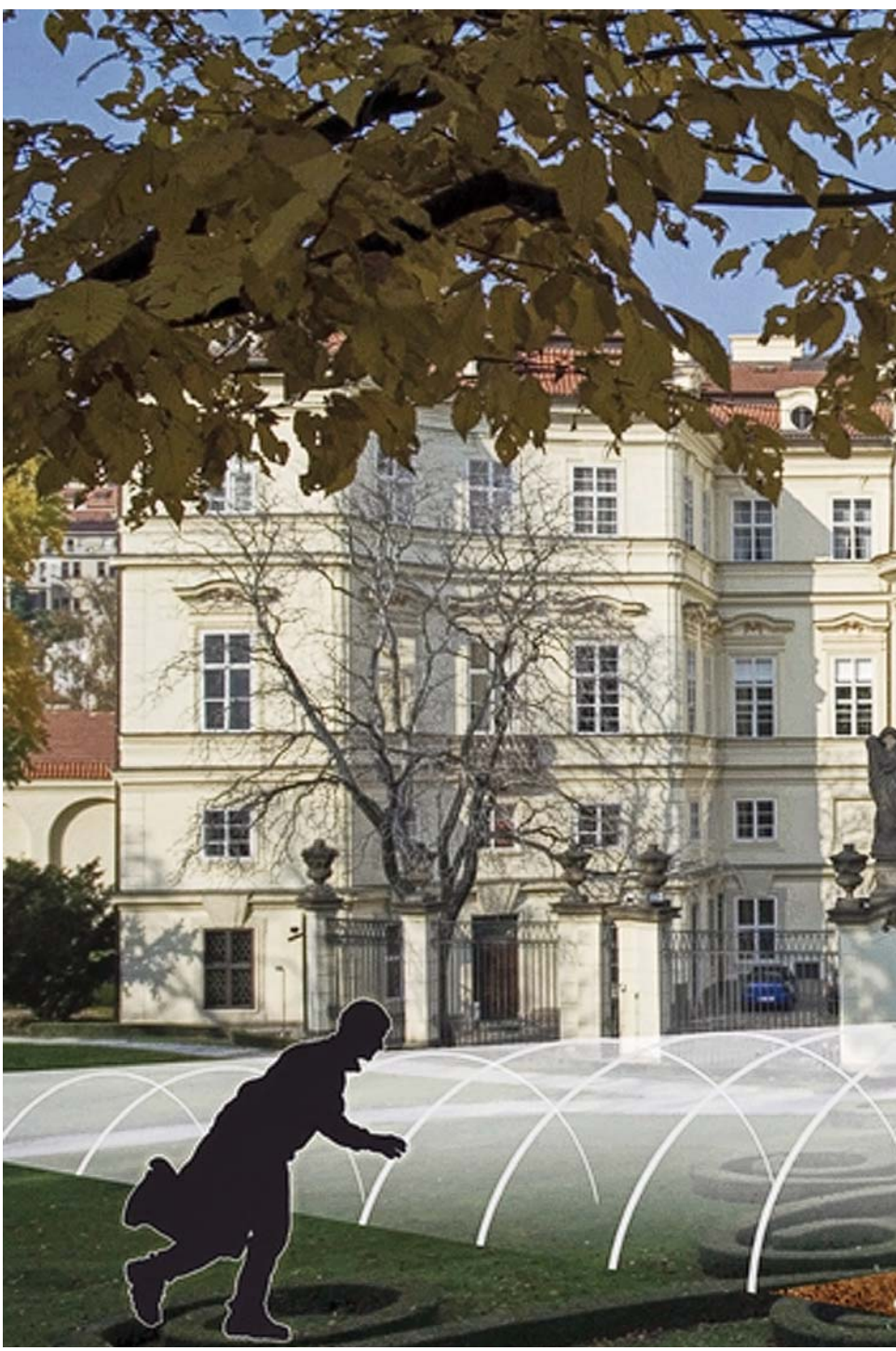
Zastosowanie technologii FAAST umożliwiło zabezpieczenie bezcennych eksponatów w obiektach muzealnych otaczających kompleks Hagia Sophia w Stambule. Dzięki poprowadzeniu instalacji w sposób niewidoczny dla zwiedzających zapewniono pełne bezpieczeństwo obiektu zgodnie z wymaganiami zarówno straży pożarnej, jak i konserwatora zabytków.

Sebastian Nowak
Bernard Sokół

Niewidoczny system ochrony obwodowej nowej generacji

Karolina Zasada

Urządzenia do ochrony obwodowej obiektów są coraz lepsze, jednak wśród „nowości” pojawiają się też urządzenia, w przypadku których nowością jest tylko logotyp i nazwa, natomiast cała reszta jest powieleniem dobrze znanych i dawno stosowanych schematów



Fot. 1. System Omnitrax

Jak zatem testowane są systemy ochrony, zanim trafią na rynek? – *Odwiedziliśmy centrum badawczo-rozwojowe firmy Senstar, która od blisko trzydziestu lat chroni tysiące obiektów w ponad osiemdziesięciu krajach. Jesienią 2006 roku firma wprowadziła na rynek Omnitrax – nowej generacji system przeznaczony do wykrywania wtargnięć intruzów. Jego elementem jest zakopywany kabel koncentryczny z niepełnym ekranowaniem, wytwarzający przestrzenną strefę detekcji. System ten ma dotychczas niespotykane cechy i zalety. Firma Senstar wprowadziła rewolucyjne zmiany technologiczne, które mogą wyznaczyć nowy trend* – mówi Mariusz Popenda, właściciel firmy ZBAR.

Prace badawcze i testy systemu Omnitrax przed jego wielką światową premierą i wdrożeniem do seryjnej produkcji trwały ponad pięć lat. Wykazano między innymi dużą skuteczność wykrywania intruzów – ponad 99% w przypadku osób ważących więcej niż 35 kilogramów.

Bezsporna innowacyjność systemu Omnitrax polega na tym, że system ten monitoruje i niezależnie analizuje stan każdego pojedynczego odcinka kabla sensorycznego, lokalizując obecność intruza z dokładnością do jednego metra. Dzięki temu nie ma licznych ograniczeń systemów poprzednich generacji. Pojedynczy zestaw zabezpiecza odcinek o długości do ośmiuset metrów. Istnieje możliwość programowania i tworzenia wielu dowolnych stref detekcji, które są niezależnie diagnozowane i raportowane, bez względu na fizyczne rozmieszczenie sensorów. Istnieje również niespotykana w innych systemach możliwość kalibracji czułości z dokładnością do jednego metra, która umożliwia kompensację zmian powodowanych ułożeniem kabla sensorycznego w różnych podłożach, na różnej głębokości (np. podłoże piaszczyste może przechodzić w gliniaste, gleba może przechodzić w asfalt itd.). Dzięki temu możemy swobodnie programować wrażliwość wybranych odcinków sensora, a także ich czasową lub stałą dezaktywację.

Kable sensoryczne w systemie Omnitrax mogą służyć do zasilania i przesyłania danych. Nie ma konieczności układania dodatkowego okablowania pomiędzy sterownikami stref. Sygnały alarmowe mogą być odbierane bezpośrednio z przekaźników sterownika lub przesyłane cyfrowo kablami sensorycznymi. Strefy detekcji można dowolnie, wirtualnie rekonfigurować bez konieczności fizycznego przeinstalowywania urządzeń.

Kable sensoryczne Omnitrax mogą być instalowane w większości naturalnych gleb, pod betonem, asfaltem, podłożem utwardzonym za pomocą kruszywa albo kostki brukowej etc. Pole detekcji jest tym silniejsze i większe, im lżejsza jest nawierzchnia, na przykład w lekkich glebach piaszczystych, asfalcie czy betonie. W ciężkim podłożu, takim jak choćby czarnoziem lub glina, pole elektromagnetyczne jest osłabione. Omnitrax umożliwia precyzyjną kalibrację czułości i niwelację różnic poprzez ustawienie odmiennych wartości progowych dla każdego metrowego odcinka aktywnego kabla. Dzięki temu system może działać poprawnie niezależnie od rodzaju podłoża. Kable sensoryczne możemy układać dowolnie, z zachowaniem określonych zasad instalacji, również pomiędzy drzewami.

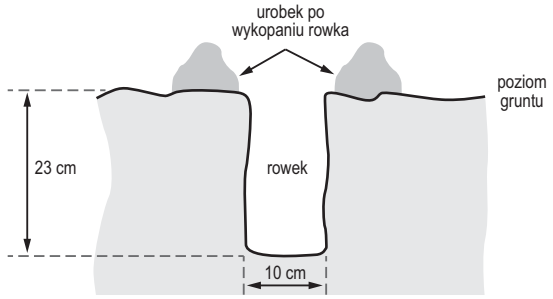
Wszelkie przeszkody w miejscu przebiegu kabli sensorycznych mogą zmniejszać skuteczność detekcji, dlatego producent precyzyjnie określił zasady dotyczące zachowania dopuszczalnych odległości pomiędzy przeszkodami a kablami sensorycznymi.

System Omnitrax zapewnia ochronę przeciwprzepięciową na kablach sensorycznych i na wszystkich dodatkowych wejściach i wyjściach.

Fot. 2. Możliwość ułożenia kabla sensorycznego pomiędzy drzewami

Jest odporny na zakłócenia powodowane przez zjawiska atmosferyczne i nie reaguje na obecność zwierząt.

Instalacja kabli sensorycznych Omnitrax jest tania, łatwa i szybka. Nie wymaga użycia ciężkiego sprzętu ani rozległych wykopów. Wystarczy rowek o szerokości 10 cm i głębokości około 20 cm (w zależności od rodzaju podłoża), który w ciągu kilku godzin można wykopać ręcznie bądź za pomocą małej koparki i zagęszczarki gruntu. Różnice głębokości, na jakiej w danym miejscu będzie znajdował się



Rys. 1. Wymiary rowka na kabel

kabel, zostaną skompensowane poprzez regulację ustawień progowych.

System Omnitrax w niewidoczny sposób dostarcza precyzyjnych informacji dotyczących wtargnięcia intruza na chroniony obszar. Każdą ze stref detekcji można skonfigurować tak, aby idealnie pasowała do naszych wymagań i informowała o wystąpieniu konkretnych sytuacji. W razie zagrożenia system powiadomi nas cichym albo głośnym alarmem, komunikatem lub wykona inną, uprzednio zaprogramowaną czynność.

System Omnitrax charakteryzuje się długą żywotnością i bezawaryjnością. Testy wykazały, że wymiana uszkodzonego bloku elektroniki oraz zaprogramowanie, uruchomienie i skalibrowanie systemu zajmuje nie więcej niż 30 minut. Koszty serwisowania nie są wysokie.

Karolina Zasada
ZBAR

OCHRONA OBWODOWA OBIEKTÓW CCTV

ZBAR

_ CCTV

- kamery laserowe
- kamery termowizyjne
- hybrydowe kamery termowizyjne w technologii laserowej
- systemy transmisji światłowodowej
- rejestratory: DVR, NVR, hybrydowe (DVR/NVR), mobilne DVR
- kamery IP i analogowe
- systemy ścian wideo „video wall"

_ Intelligent Video Analytic
Inteligentna Analiza Obrazu

- tworzenie wirtualnego ogrodzenia
- zliczanie ludzi/pojazdów
- detekcja zniknięcia/pojawienia się obiektu
- klasyfikacja obiektów
- detekcja sabotażu kamery
- rozbudowana detekcja ruchu
- filtr prędkości obiektu

94-214 Łódź, Poland, Krakowska 60
Tel. + 48 **426 111 298**, Fax +48 **426 111 297**
e-mail: zbar@zbar.com.pl

sprawdź pełną ofertę na **www.zbar.com.pl**

Aventura · FFT · Protech · CIAS · SCHRACK SECONET · SENSTAR · GPS STANDARD · IFTER

Środki bezpieczeństwa fizycznego w ochronie informacji niejawnych (cz. 3)

Artur Bogusz
Marek Blim

W ramach podsumowania cyklu artykułów chcemy, odnosząc się do ostatnich kroków postępowania – kwintesencji uproszczonego algorytmu przedstawionego w części pierwszej – nie tylko pokazać problemy i pułapki spowodowane bezrefleksyjną oceną bazującą na tabelaryzowaniu zagrożeń (z pominięciem korelacji stosowanych rozwiązań ochronnych – organizacyjnych, fizycznych, technicznych), ale przede wszystkim odnieść się do praktyki, czyli przewidywanych postaci planu działań na rzecz fizycznego zabezpieczenia informacji niejawnych – praktycznie dostosowanego do potrzeb i związanego z akceptowalnymi kosztami

1. Zasady doboru środków bezpieczeństwa fizycznego

W ramach algorytmu postępowania przedstawionego w pierwszej części artykułu, po przeprowadzonej analizie zasobów, zagrożeń oraz sposobów i obszarów przetwarzania informacji niejawnych (część druga) dochodzimy obecnie do kwestii doboru skutecznych środków bezpieczeństwa fizycznego, czyli próby określenia, gdzie, czym i jak mamy chronić informacje niejawne, aby – spełniając wymogi rozporządzenia[1] – zachować umiar i rozsądek.

Gdzie?

Informacje niejawne chronimy w nakazanych rozporządzeniem strefach ochronnych na terenie własnej jednostki organizacyjnej, czyli na obszarze będącym aktualnie do naszej dyspozycji i pod naszym zarządem (nie musi to być własność fizyczna, wystarczy najem i uprawnienie do użytkowania), umożliwiającym nam swobodny dobór i zastosowanie zalecanych (wskazanych lub wymaganych) środków ochrony fizycznej i technicznej oraz działania personelu bezpieczeństwa.

Czym?

Informacje niejawne chronimy barierami fizycznymi oraz technicznymi (nadzorowanymi przez uprawniony i przeszkolony personel) przede wszystkim przed nieuprawnionym dostępem, ale także przed zaborem oraz zniszczeniem (celowym lub przypadkowym). Bariery fizyczne mają charakter środków ochrony bezpośredniej (trezor, pomieszczenie wzmocnione, sejf lub szafa na dokumenty) lub pośredniej (ściany, stropy, drzwi, okna, ogrodzenia, bramy). Bariery techniczne mają charakter pomocniczy – wspierają realizację procedur bezpieczeństwa (system kontroli dostępu, system sygnalizacji włamania i napadu, system dozoru wizyjnego) lub stanowią części detekcyjno-informacyjne organizacyjnych rozwiązań systemowych służących do nadzoru (np. SMA – stanowisko monitorowania alarmów; LCN – lokalne centrum nadzorcze lub ACO – alarmowe centrum odbiorcze).

Jak?

Informacje niejawne możemy skutecznie chronić, przede wszystkim nie dopuszczając do zaistnienia incydentów zagrażających ich atrybutom bezpieczeństwa (poufność, integralność, dostępność) oraz ograniczając do minimum wszelkie niekorzystne skutki zdarzeń przypadkowych (niezależnie od ich źródeł). Za podstawowe należy uznać przemyślane rozwiązania organizacyjne mające na celu bezpieczeństwo informacji niejawnych w jednostce organizacyjnej widzianej jako całość, z jej rdzeniem (informacjami niejawnymi wymagającymi szczególnej ochrony), wykorzystujące wszystkie dostępne środki fizycznej ochrony.

1) Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 19 czerwca 2012 r., poz. 683).

Z naszej praktyki (w zakresie doboru i oceny środków fizycznej ochrony informacji niejawnych wynika, że na ogół, dla osób planujących ten dobór nie ma najmniejszego znaczenia faktyczna ochrona takich informacji. Zazwyczaj próbuje się tylko spełnić wymagania kontrolujących służb (ABW/SKW)[2], aby dana jednostka organizacyjna otrzymała potrzebne uprawnienia (na danym poziomie zdolności do ochrony informacji niejawnych).

1.1. Zasada generalna – najsłabsze ogniwo

Dobierając poszczególne środki bezpieczeństwa fizycznego, musimy pamiętać, że o wyniku decyduje element o najniższej odporności. Pułapką może być w tym przypadku element, który nie został wzięty pod uwagę w zapisie tabelarycznym przywołanym w rozporządzeniu – np. dostępne z zewnątrz kanały wentylacji grawitacyjnej umożliwiające intruzowi podgląd lub podsłuch pomieszczenia, przechodzące przez to pomieszczenie przewody instalacji wodociągowej, cieplnej lub energetycznej umożliwiające przesłuchy akustyczne czy też podsłuch sygnałów szkodliwej, ujawniającej emisji elektromagnetycznej itp.

1.2. Fałszywe alarmy – korelacja sprzętowa

W przypadku SKD, SSWiN, CCTV, systemów ppoż. i automatyki budynkowej coraz bardziej popularne stają się rozwiązania oparte na wykorzystaniu magistral TCP/IP, dlatego pojawia się problem kompatybilności elektromagnetycznej EMC (*electromagnetic compatibility*) i wzajemnego zakłócania się sygnałów i transmisji danych. Wymagania normy europejskiej EN 50130-4 rozstrzygają kwestię odporności czujek alarmowych (w zakresie 80 MHz–2,7 GHz) na wszelkiego rodzaju sygnały zewnętrzne (np. pochodzące z Wi-Fi i telefonów komórkowych wykorzystujących pasma wysokich częstotliwości), ale pozostaje do rozpatrzenia już istniejący układ połączeń kablowych i radiowych w samym obiekcie Wielokrotnie spotykaliśmy się z tym, że nowi wykonawcy nie uwzględniali zajętości lokalnego spektrum EMF (już wykorzystywanych pasm częstotliwości), rozbudowując system ochrony technicznej lub dobudowując kolejny – stąd fałszywe alarmy, konieczność obniżania poziomów sygnałów lub przekładania tras łączy alarmowych.

1.3. Współpraca w ochronie – korelacja systemowa

Wielość systemów technicznego wsparcia ochrony i bezpieczeństwa może znacznie podwyższyć ogólny poziom bezpieczeństwa. Mówimy tu o iloczynie poszczególnych potencjałów ochronnych, a nie tylko ich prostym sumowaniu. Warunkiem jest umieszczenie wszystkich urządzeń monitorujących we wspólnym pomieszczeniu LCN (lokalnym centrum nadzoru) i bezpośrednia współpraca operatorska (przykładowo – wykorzystanie kamery CCTV do podglądu pomieszczenia i ustalenia przyczyny alarmu czujki pożarowej pozwoliło, w tym konkretnym przypadku, zlokalizować źródło dymu – tlący się kosz, szybko zareagować oraz uniknąć ewakuacji kilkupiętrowego biurowca). Niezbędne szkolenia personelu LCN/SMA oraz przemyślane scenariusze działań ochronnych i kryzysowych wyraźnie podwyższają poziom ochrony obiektu.

2) „Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych" (Dz. U. z 2011 r., nr 93, poz. 541).

Długoletnia praktyka audytorska autorów jednoznacznie wskazuje na to, że systemy zabezpieczeń działają coraz gorzej w miarę upływu czasu. Można powiedzieć, że system zabezpieczeń działa poprawnie w początkowej fazie (planowanie-projektowanie-uruchomienie). Następnie przychodzi czas przygotowania do audytu, czyli okres, w którym system jest nadmiernie kontrolowany i sprawdzany (wiele osób chce się po prostu wykazać). Na końcu nastaje okres normalnego użytkowania. W większości przypadków po roku od momentu wdrożenia system nie działa prawidłowo. Jeżeli system już na początku nie spełniał wszystkich swoich zadań, to po pewnym czasie może być zupełnie nieskuteczny. Nie mówimy o jego sprawności technicznej, która jest uwarunkowana sprawnością poszczególnych elementów składowych, ale właśnie o skuteczności i utrzymaniu odpowiedniej funkcjonalności ochronnej (zależnej od tego, czy był wykorzystywany poprawnie od początku eksploatacji).

2. Tabelaryzacja rozwiązań ochronnych – pułapy i pułapki

Przedstawiona w drugiej części załącznika do rozporządzenia RM tabela punktowa podstawowych wymagań dotyczących bezpieczeństwa fizycznego w sposób enumeratywny określa obowiązkowe i dodatkowe kategorie ochrony, adekwatnie (zdaniem jej autorów) do wskazanego poziomu zagrożeń.

Wskazanie cząstkowych środków bezpieczeństwa należących do różnych kategorii oraz odwoływanie się do norm czy też wymagań normatywnych wydaje się zrozumiałe, ale jest tylko mocno uproszczonym trybem postępowania, a mianowicie jedynie obliczaniem wpływu wskazanych i użytych środków bezpieczeństwa fizycznego danej kategorii ochronnej na podstawie opisu zawartego w załącznikach. Obowiązuje wskazany w tabeli (cz. II) wymagany przez ustawodawcę poziom zagrożeń (niski, średni, wysoki) – adekwatnie do połączonych obowiązkowych kategorii (patrz – suma K1+K2+K3 oraz K4+K5) w przypadku najwyższej klauzuli tajności informacji przetwarzanych w jednostce organizacyjnej.

Pułapy wymagań są zatem oczywiste, a gdzie są pułapki? Tkwią one w niepozornych indeksach podtabelowych, które wyraźnie wpływają na określenie kategorii w stosunku do różnych klauzul.

Przypomnijmy zatem znaczenie poszczególnych kategorii, wprowadzonych w rozporządzeniu jako obowiązkowe do stosowania:

1) **K1 – szafy do przechowywania informacji niejawnych.** Techniczne zabezpieczenia/środki należące do tej kategorii to odpowiednia konstrukcja samych szaf oraz zamontowanych w nich zamków.
2) **K2 – pomieszczenia.** Do kategorii tej należą pomieszczenia, w których informacje niejawne przechowywane są w szafach opisanych w kategorii K1, i nie dotyczy to pomieszczeń wzmocnionych, o których mowa w § 5 ust. 3 rozporządzenia[3]. O zaklasyfikowaniu pomieszczenia do danego typu kategorii decyduje jego najsłabszy element (np. ściana, podłoga, strop, drzwi, okna) oraz zamek do drzwi pomieszczenia.
3) **K3 – budynki.** O zaklasyfikowaniu budynku do danej kategorii środka bezpieczeństwa w związku z poziomem jego technicznego zabezpieczenia decyduje jego najsłabszy element zewnętrzny.
4) **K4 – kontrola dostępu**, w tym (jako środki zabezpieczenia techniczne) elektroniczny, automatyczny system kontroli dostępu pracowników oraz system organizacyjny do kontroli i nadzoru nad interesantami.
5) **K5 – personel bezpieczeństwa i systemy sygnalizacji włamania i napadu**, w tym personel własny i zewnętrzny (outsourcing usług) oraz system SSWiN spełniający określone wymagania normatywne.

Ponadto ustawodawca wprowadza kategorię uzupełniającą do obowiązkowych:

6) **K6 – granice** – ogrodzenie obiektu, wraz z systemami do dozoru nad nim (kontrolowane punkty wejścia/wyjścia, nadzorowanie naruszenia stanu ogrodzenia), oświetlenie i dozór wizyjny.

K1–K5 to kategorie główne, a K6 to kategoria dodatkowa.

2.1. Wymagania związane z klauzulą „ściśle tajne"

Dla obowiązkowej sumy ocen kategorii K1+K2+K3 dopuszcza się fakt (indeksacja „*"), że tylko jedna z wartości może być równa 0 (zero punktów), ale co to oznacza? Oto nasza interpretacja:

- **K1=0** – nie ma szaf i sejfów, za to mamy wzmocnione pomieszczenie (K2) lub wręcz trezor bankowy[4] w solidnym budynku (K3);
- **K2=0** – nie ma pomieszczenia, natomiast odpowiednie sejfy lub szafy (K1) są ulokowane we wzmocnionym budynku lub bunkrze (K3);
- **K3=0** – nie ma budynku, informacje są przechowywane w odpowiednich sejfach lub szafach (K1) ulokowanych we wzmocnionym ruchomym pomieszczeniu (K2) lub kontenerze, dodatkowo nadzorowanym i zabezpieczonym w przypadku jego polowego wykorzystywania; ewentualnie samo pomieszczenie (K2) jest częścią ruchomej jednostki wojska (okręt, pociąg pancerny, latające SD itp.).

Dla obowiązkowej sumy ocen kategorii K4+K5 indeksacja „**" „wymaga", żeby żadna z wartości nie była mniejsza niż 2 (dwa punkty), co oznacza że:

- **K4≥2**, czyli praktycznie jest to (K4=K4S1+K4S2 – patrz załącznik II do rozporządzenia) funkcjonowanie systemu kontroli dostępu nadzorowanego przez personel bezpieczeństwa (K4S1=2 punkty dla typu 2) oraz możliwość pominięcia kwestii systemu identyfikacji własnych pracowników i interesantów z zewnątrz (K4S2=0, co jest logicznym absurdem);
- **K5≥2**, czyli minimum to system ochronny, realizujący nadzorowanie patrolowania obszaru chronionego (przez pracowników z zewnątrz lub personel własny).

Pułapki bezpośrednio przyjętej tabelaryzacji i wprowadzonej punktacji są tu oczywiste – decyduje bowiem szczegółowe określenie potencjalnych zagrożeń, dokładna analiza ryzyka i wskazanie wszystkich dodatkowych środków bezpieczeństwa fizycznego, bo te podstawowe (wykazane już w poszczególnych kategoriach) mogą okazać się niewystarczające nawet dla przyjętego wcześniej niskiego poziomu zagrożeń (20 punktów).

2.2. Wymagania związane z klauzulą „tajne"

Wymagana minimalna suma punktów dla kategorii K1+K2+K3 wymusza odpowiednie składowe środki bezpieczeństwa dla

3) §5 ust. 3 cytowanego rozporządzenia dopuszcza przechowywanie dokumentów niejawnych jako bezpośrednio dostępnych – poza szafami i sejfami – w odpowiednio wzmocnionym pomieszczeniu w strefie.

4) Norma PN-EN 1143-1:2005 – „pomieszczenia monolityczne skarbcowe, skarbce pow. IX kl. odporności".

wskazanych kategorii (szafy, pomieszczenia, budynki), a ponadto indeksacja „***" dla obowiązkowych kategorii K4+K5 wyklucza możliwość przyjmowania wartości 0 (zero punktów) przez dowolną z kategorii składających się na tę sumę, co oznacza że:

– **K4=2**, jeżeli K4=K4S1+K4S2, czyli teoretycznie oznacza to istnienie i poprawne funkcjonowanie systemu kontroli dostępu nadzorowanego przez personel zajmujący się bezpieczeństwem (K4S1=2, bo K4S1=1 jest dopuszczone tylko w przypadku klauzuli „poufne") oraz możliwość braku systemu przepustowego (K4S2=0), co w rzeczywistości jest absurdem, skoro nie jest wymagana identyfikacja własnego personelu (zatem w oparciu o co funkcjonuje system kontroli dostępu – K4S1?);
– **K5=1**, jeżeli K5=K5S1+K5S2, czyli teoretycznie oznacza to istnienie i poprawne funkcjonowanie (K5S1=1 punkt w przypadku środka typu 1 działalności osób – strażników pracujących sporadycznie jako personel zajmujący się bezpieczeństwem lub poprawnie funkcjonującego systemu SA3 (K5S2=1 punkt w przypadku środka typu 1).

Pułapką jest – w tym przykładzie – konieczność przekonania typowego „oszczędnego KJO" (czytaj: skąpego i nie rozumiejącego istoty fizycznej ochrony informacji niejawnych kierownika jednostki organizacyjnej) przez pełnomocnika do spraw ochrony informacji niejawnych, że myślenie „punktowo-tabelowe" przyczynia się do stwarzania dodatkowych zagrożeń. Zwłaszcza wówczas, gdy decyduje on, że minimum 16 punktów dla poziomu niskiego przy klauzuli „tajne" uzyska dzięki dodatkowemu wzmocnieniu ogrodzenia i punktów dostępu, poprawieniu oświetlenia i skorzystaniu z usług dozoru wizyjnego najtańszej firmy zewnętrznej (K6≥5 pkt), która deleguje strażników nieuprawnionych do wstępu na teren obiektu.

2.3. Wymagania w przypadku klauzuli „poufne"

Podobnie jak w przypadkach wyższych klauzul są tu określone kategorie wymagane (K1–K5) i dodatkowa (K6), ale trzeba zwrócić uwagę na możliwość obniżenia do wartości jednego punktu ocen poszczególnych środków bezpieczeństwa w kategoriach K1–K2 (wartość punktowa kategorii jest iloczynem ocen czynników składowych) oraz pominięcia poszczególnych środków bezpieczeństwa kategorii K4–K5 (wartość punktowa kategorii jest sumą ocen czynników składowych), co przy stosunkowo niskich oczekiwaniach adekwatnie do poziomu zagrożenia – niskiego albo średniego, albo wysokiego – wartość wymagana to 11 albo 14, albo 16 punktów) widoczny jest związek z uproszczonym sposobem oceniania i brakiem wnikliwej analizy rzeczywistego potencjału posiadanych środków bezpieczeństwa.

Przykładową pułapką może być punktowa ocena drzwi jako środka bezpieczeństwa technicznego fizycznej ochrony. Dlaczego? Ponieważ drzwi do pomieszczenia wzmocnionego, objętego kontrolą dostępu, powinny zapewniać wzmocnione blokowanie w obu osiach (x i y) poprzez opory przyzawiasowe i mieć wzmocnione rygle zamka głównego połączone z blokadą prętową „góra-dół" zabezpieczoną dodatkowo zamkiem szyfrowym. W przypadku drzwi do pomieszczenia kancelarii tajnej wejście w godzinach pracy powinno być w układzie śluzy kontrolnej (możliwość obsługi przez zworę i wideodomofon), a po godzinach – objęte systemem kontroli dostępu i zabezpieczone mechanicznie. W przypadku doboru drzwi do pomieszczenia, w którym przechowuje się materiały niejawne, powinno się brać pod

uwagę najwyższy wskazany stopień niejawności (klauzula) i ilość tych materiałów. Także w przypadku drzwi do erygowanego na podstawie odrębnych przepisów[5] archiwum niejawnego odgrywa rolę najwyższy stopień niejawności i ilość archiwizowanych informacji, a także sposób ich przygotowania i przechowywania.

Należy podkreślić, że cały czas odnosimy się do wymagań narzuconych w przypadku klauzuli „poufne" lub równoważnych wobec niej klauzul sojuszniczych lub układowych[6], zatem wszystkie te kwestie mogą być kłopotliwe i mieć różne implikacje w przypadku zbytniego uproszczenia oceny. Jako rzeczoznawcy i praktycy zachęcamy do zapoznania się nie tylko z normami cywilnymi z tego zakresu, ale także z normami obronnymi[7] oraz podpisanymi przez RP porozumieniami z NATO (np. z *Umową między Stronami Traktatu Północnoatlantyckiego o ochronie informacji*[8], AD 70-1. Dyrektywa bezpieczeństwa ACE).

2.4. Wymagania w przypadku klauzuli „zastrzeżone"

Kategoriami wymaganymi są K1–K3. Pozostałe (K4–K6) są traktowane jako dodatkowe, ale nie wolno zapominać o tym, że ustawodawca w treści §9 rozporządzenia narzuca kierownikowi jednostki organizacyjnej nie tylko obowiązek zatwierdzenia planu ochrony, ale także obowiązek odniesienia się w nim do wskazanych rozwiązań organizacyjnych i technicznych (na pułapie minimalnym), co wymusza ich stosowanie w stopniu i trybie podstawowym[9]. Rozproszenie miejsc, w których przechowywane są dokumenty z klauzulą „zastrzeżone", w związku z brakiem obowiązku posiadania kancelarii tajnej zagraża bezpieczeństwu tych dokumentów.

5) Uprawnienia do wydania „Aktu utworzenia oddziału Archiwum Państwowego" posiada Naczelny Dyrektor Archiwów Państwowych – niezależnie od klauzuli archiwizowanych dokumentów.

6) Agencja Bezpieczeństwa Wewnętrznego, „Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi", Warszawa, 31 grudnia 2010 r.

7) „Norma Obronna NO-04-A004 Obiekty wojskowe. Systemy alarmowe. Części: 1-9", Decyzja Nr 169/MON z dnia 10 maja 2010 r.

8) „Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji sporządzona w Brukseli dnia 6 marca 1997 r." (Dz. U. z 2000 r., nr 64, poz. 740).

9) Część III załącznika do rozporządzenia – „Klasyfikacja środków bezpieczeństwa fizycznego".

Rys. 1. Współzależności systemowe budowy projektu planu bezpieczeństwa informacji

Według nas wprowadzenie obowiązkowej tabelaryzacji i dodatkowych kategorii ochrony jest skuteczne, ale bardzo trudne do praktycznej realizacji. Skąd pełnomocnik do spraw ochrony ma wiedzieć, że wybrane czy posiadane zabezpieczenia spełniają wymogi określone w stosownej tabeli? Ustawodawca nie określił, czy ocena jest w tym przypadku arbitralna i należy do pełnomocnika do spraw ochrony, czy jednak będzie podlegała jakiejś weryfikacji dodatkowej, np. dokonywanej przez audytorów ABW. W praktyce dobór zabezpieczeń fizycznych jest weryfikowany i oceniany każdorazowo podczas audytu systemu ochrony informacji niejawnych jednostki organizacyjnej. Każde wybrane zabezpieczenie jest weryfikowane oraz oceniane przez audytorów zewnętrznych.

W tym miejscu nasuwa się jeszcze jedna wątpliwość. W jaki sposób i z wykorzystaniem jakiego narzędzia kierownik jednostki organizacyjnej, który decyduje o zastosowaniu fizycznych zabezpieczeń i przeznacza na nie odpowiednie środki finansowe, ma sprawdzić, czy zostały one prawidłowo dobrane? To trudne pytanie, które pozostawiamy bez odpowiedzi.

Pułapką jest w tym przypadku konieczność umiejętnego (akceptowalnego dla ABW/SKW) wytłumaczenia się przez KJO z przyjętych założeń, pominiętych zabezpieczeń i wprowadzonych ograniczeń organizacyjno-użytkowych, zapisanych w zatwierdzonym planie.

3. Plan ochrony informacji niejawnych

Zgodnie z §9 rozporządzenia wszystkie działania na rzecz zabezpieczenia (nie tylko fizycznego) informacji mają być przewidziane w zatwierdzonym przez KJO planie ochrony informacji niejawnych.

3.1. Systemowe podejście do projektu planu ochrony informacji

Rysunek 1 jest graficznym odwzorowaniem systemowego podejścia do problemu bezpieczeństwa informacji. Czynniki wpływające na bezpieczeństwo informacji w konstrukcji tego planu są następujące:

- w obszarze dalszego otoczenia systemowego dla planowanych działań istnieje:
  - znajomość istniejącego stanu rzeczy oraz przydatnych, już sprawdzonych nowych rozwiązań teoretycznych (eksperymenty naukowe),
  - znajomość zastosowanych rozwiązań standardowych,
  - obowiązujące przepisy prawa i zobowiązania wspólne (sojusznicze, układowe, kontraktowe),
  - status organizacyjny i prawny jednostki organizacyjnej,
  - wyniki analizy zagrożeń oraz zebrane oceny potencjalnego ryzyka i rzeczywistego stanu bezpieczeństwa jednostki organizacyjnej,
- w obszarze bliższego otoczenia systemowego dla planowanych działań:
  - założone cele końcowe,
  - znajomość „dobrych praktyk" normatywnych/branżowych,
  - zdolność i gotowość personelu jednostki organizacyjnej do zastosowania niezbędnych środków bezpieczeństwa oraz ich zabezpieczenie logistyczne,
  - zgromadzone siły (fachowy personel) i środki (technika, systemy, finanse).

Warunki zabezpieczenia posiadanych i przetwarzanych zasobów informacji niejawnych na wymaganym poziomie są podane w tabeli w cz. II załącznika rozporządzenia Rady Ministrów (Dz. U. z 2012 r, poz. 683).

Sugerujemy zapoznanie się z *Kodeksem zarządzania bezpieczeństwem informacji* bazującym na brytyjskiej normie BS 7799-1:1997 i dostępnym obecnie jako polska norma PN – ISO/IEC 17799:2007, która jest polskim tłumaczeniem normy ISO/IEC 17799:2005 (ed. 2), tożsamym z obowiązującym międzynarodowym wydaniem normy ISO/IEC 27002:2005. Niektóre z zawartych w tym kodeksie/tej normie zaleceń zostały przeniesione do omawianego załącznika rozporządzenia jako wymogi, niestety bez podania materiałów źródłowych.

3.2. Ustawowe podejście do planu ochrony informacji

Opublikowane w Dzienniku Ustaw RP z 19 czerwca 2012 roku pod poz. 683 rozporządzenie Rady Ministrów z dnia 29 maja 2012 r ma moc prawną obowiązku ustawowego w zakresie i czasie podanym w jego treści. Świadomość tego faktu powinny mieć wszystkie osoby pełniące funkcję kierownika jednostki organizacyjnej (KJO[10]) – odpowiedzialnego za ochronę informacji niejawnych (zorganizowanie jej i zapewnienie jej funkcjonowania) w posiadanych/przetwarzanych/archiwizowanych zasobach informacyjnych. Jest to zgodne z wymogiem przedstawionym w art.14 ust. 1 ustawy o ochronie informacji niejawnych. Przypominamy, że pełnomocnik ds. ochrony informacji niejawnych odpowiada za przestrzeganie przepisów i procedur (wymóg art. 14 ust. 2 ustawy) w ramach uprawnień przyznanych mu przez KJO.

Aby uniknąć wszelkich nieporozumień przytaczamy odpowiedni fragment tekstu:

§ 9. 1. Kierownik jednostki organizacyjnej zatwierdza plan ochrony informacji niejawnych, który zawiera:

1) opis stref ochronnych, pomieszczeń lub obszarów, o których mowa w § 7 ust. 4, w tym określenie ich granic i wprowadzonego systemu kontroli dostępu;

2) procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefach ochronnych;

3) opis zastosowanych środków bezpieczeństwa fizycznego uwzględniający certyfikaty, o których mowa w art. 46 pkt 4 ustawy, oraz poświadczenia, o których mowa w § 4 ust. 6;

4) procedury bezpieczeństwa dla strefy ochronnej I, strefy ochronnej II oraz specjalnej strefy ochronnej, określające w szczególności:

a) klauzule tajności informacji niejawnych przetwarzanych w strefie,

b) sposób sprawowania nadzoru przez osoby uprawnione w przypadku przebywania w strefie osób nieposiadających stałego upoważnienia do wstępu oraz sposób zabezpieczania przetwarzanych informacji niejawnych przed możliwością nieuprawnionego dostępu tych osób,

c) w przypadku specjalnej strefy ochronnej, sposób akceptacji umieszczania linii komunikacyjnych, telefonów, innych urządzeń komunikacyjnych, sprzętu elektrycznego lub elektronicznego, znajdujących się w strefie;

5) procedury zarządzania kluczami i kodami dostępu do szaf, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne;

6) procedury reagowania osób odpowiedzialnych za ochronę informacji niejawnych oraz personelu bezpieczeństwa w przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych;

7) plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych.

2. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych plan, o którym mowa w ust. 1, może zawierać dodatkowe elementy.

Jak wynika z cytowanej treści, jest tu dużo więcej kwestii niż w załączniku do rozporządzenia. Znacznie dokładniej opisana jest organizacja (plany awaryjne, scenariusze sytuacji kryzysowych, stany nadzwyczajne), o czym wspominaliśmy już w poprzednim artykule.

4. Podsumowanie

Poruszając w cyklu artykułów kwestie bezpieczeństwa informacji w sposób dogłębny (analiza ryzyka w części drugiej), ale zarazem nieco przewrotny (pułapy i pułapki),

10) funkcja KJO – kierownik jednostki organizacyjnej według art. 2 ust. 14 ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2010 r., nr 182, poz. 1228).

Rys. 2. Zintegrowane zarządzanie bezpieczeństwem (mat. szkoleniowe ENSI, 2004 r.)

chcemy przede wszystkim zwrócić uwagę na indywidualność każdej jednostki organizacyjnej, w której konieczna jest ochrona informacji. Wszystko jest inne – lokalizacja, personel, rozwiązania organizacyjne, oddziaływania otoczenia.

Tak naprawdę to sami decydenci (KJO) w danej jednostce organizacyjnej muszą zdecydować, czy należy wprowadzić zmiany, a jeśli tak, to jakie i kiedy należy to uczynić aby zapewnić odpowiedni poziom ochrony wszystkich (nie tylko niejawnych) zasobów informacyjnych. Przed podjęciem decyzji należy zapoznać się z obowiązującymi dokumentami ustawowymi oraz zalecanymi normami, ale także skorzystać z istniejących rozwiązań *open source* opracowanych w polskim European Network Security Institute (*www.ensi.net*), dostępnych na zasadach licencji GNU. Opracowane i wdrożone w ramach zintegrowanego zarządzania bezpieczeństwem TSM (*Total Security Management*) poszczególne metodyki (TISM i TSM-BCP) są wysoce użytecznymi i wielokrotnie sprawdzonymi w polskim środowisku biznesowym narzędziami doskonalącymi zarządzanie bezpieczeństwem.

Omawiane w naszym cyklu rozporządzenie[11] nakazuje oraz wymaga, a rozsądek i możliwości osobowo-finansowe (różne dla każdej jednostki organizacyjnej) podpowiadają, konieczność przeprowadzenia dokładnej analizy planowanych działań, gdyż ta formalna, punktowo-tabelowa może nie wystarczyć. Wszyscy decydenci (KJO) i pełnomocnicy do spraw ochrony powinni wziąć to pod uwagę.

Każdy pełnomocnik do spraw ochrony, a tym bardziej każdy kierownik przedsiębiorstwa (KJO) powinien dobrze przemyśleć zastosowanie danego zabezpieczenia, gdyż – po pierwsze – kosztuje, po drugie – może być nieskuteczne, po trzecie – może nie zostać zaakceptowane przez audytorów zewnętrznych.

Artur Bogusz
Marek Blim

Bibliografia

1. Agencja Bezpieczeństwa Wewnętrznego (jako Krajowa Władza Bezpieczeństwa), *Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi*, Warszawa, 31 grudnia 2010 r.
2. Anzel M., *Nowa ustawa i jej zmienione uwarunkowania*, materiały szkoleniowe ZG OSPOIN, Warszawa 2010.
3. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.
4. Blim M., *Bezpieczeństwo obiektów. Poradnik techniczny*, ZRTOM – TECHOM, Warszawa 2012.
5. *Decyzja Nr 362/MON z dnia 28 września 2011 r. w sprawie wprowadzenia do użytku „Wytycznych Ministra Obrony Narodowej w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą »poufne« i »zastrzeżone«*", Dz. Urz. MON z 2011 r., nr 20, poz. 302.
6. PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*
7. ISO Guide 73:2009 *Risk management – Vocabulary (Zarządzanie ryzykiem – Słownictwo*, przekład nieautoryzowany przez PKN).
8. Krawiec J., Stefaniak A., *System Zarządzania Bezpieczeństwem Informacji w praktyce. Zasady wyboru zabezpieczeń,* PKN, Warszawa 2012.
9. Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu,* Konsalnet S.A., Warszawa 2004.
10. Materiały informacyjne z *Forum oddziału wart cywilnych i pracowników wojska (www.owc.com.pl/forum*).
11. Ministerstwo Obrony Narodowej, *Wytyczne w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne*, zał. do Decyzji Nr 362/MON z dnia 28 września 2011 r.
12. *Norma Obronna NO-04-A004 Obiekty wojskowe. Systemy alarmowe, części 1–9,* ostatnia aktualizacja – *Decyzja Nr 169/MON z dnia 10 maja 2010 r.*, Dz. Urz. MON z 2010 r., nr 10, poz. 110.
13. *Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych,* Dz. U. z 2011 r., nr 93, poz. 541.
14. *Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych z załącznikami,* Dz. U. z dnia 19 czerwca 2012 r., poz. 683.
15. *Rozporządzenie Ministra Obrony Narodowej z dnia 2 listopada 2011 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych MON lub przez niego nadzorowanych*, Dz. U. z 2011 r., nr 252, poz. 1519 z późn. zm.
16. Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, Wydawnictwo LexisNexis, Warszawa 2011.
17. *TSM (Total Security Management) – metodyka zintegrowanego zarządzania bezpieczeństwem organizacji,* materiały szkoleniowe ENSI, Warszawa 2004–2010.
18. *Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji sporządzona w Brukseli dnia 6 marca 1997 r.*, Dz. U. z 2000 r., nr 64, poz. 740.
19. *Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, tekst jednolity*, Dz. U. z 2005 r., nr 145, poz. 1221 z późn. zm.
20. *Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych*, Dz. U. z 2010 r., nr 182, poz. 1228.

11) „Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych" (Dz. U. z 19 czerwca 2012 r., poz. 683).

ZASIĘG AŻ DO 240 METRÓW

TECHNOLOGIA LED SMD

ŻYWOTNOŚĆ: 11 LAT

WYDAJNOŚĆ: +20%

OSZCZĘDNOŚĆ ENERGII

NISKIE KOSZTY

5 LAT GWARANCJI

GEKO PEŁNA GAMA OŚWIETLACZY LED

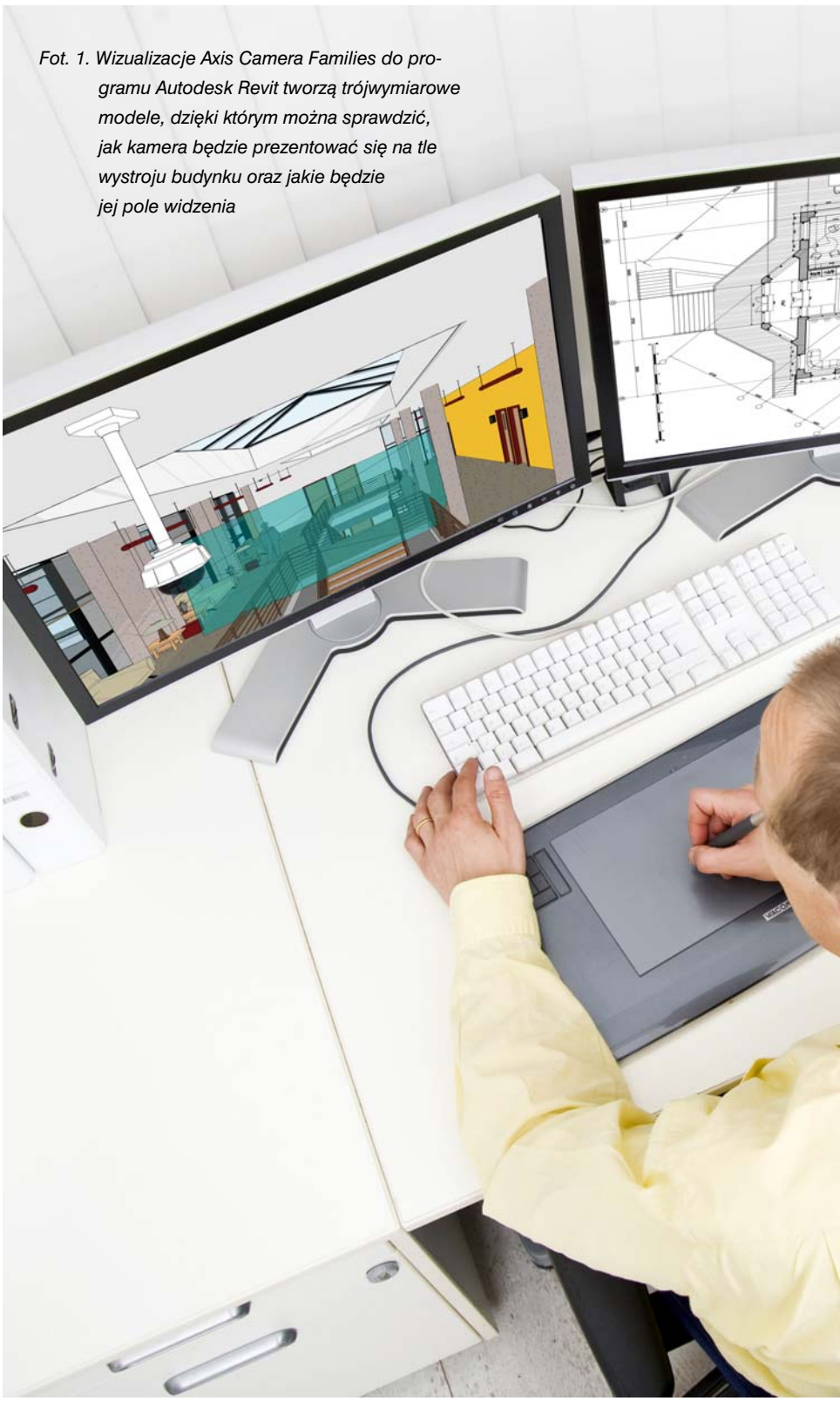
Linia GEKO reaguje na wymagania doskonałego oświetlenia zapewniającego wyraźny obraz CCTV w warunkach nocnych. Zastosowaliśmy w urządzeniach najwyższej jakości komponenty, a ich innowacyjną architekturę zaprojektowaliśmy ze szczególną starannością. Dlatego możemy dać pełną gwarancję na optymalne osiągi, wysoką wydajność, maksymalną trwałość oraz niskie koszty naszych oświetlaczy.

VIDEOTEC

Axis wprowadza trójwymiarowe wizualizacje swoich kamer do oprogramowania Autodesk Revit

Agata Majkucińska

Innowacyjne wizualizacje kamer z serii Axis Camera Families dla oprogramowania Autodesk Revit zawierają trójwymiarowe modele kamer umożliwiające ocenę ich wyglądu i pola widzenia w realnych warunkach eksploatacyjnych. Trójwymiarowe modele zostały zaprojektowane z myślą o projektantach systemów bezpieczeństwa, którzy mogą tworzyć takie systemy już na etapie projektowania budynków, z użyciem pakietu Autodesk Revit 3D CAD



Fot. 1. Wizualizacje Axis Camera Families do programu Autodesk Revit tworzą trójwymiarowe modele, dzięki którym można sprawdzić, jak kamera będzie prezentować się na tle wystroju budynku oraz jakie będzie jej pole widzenia

Axis Communications, światowy lider w dziedzinie sieciowych wizyjnych systemów dozorowych, wprowadza na rynek wydajne narzędzie dla projektantów systemów zabezpieczających. Modele kamer z serii Axis Camera Families zawierają szczegółowe metadane wykorzystywane w procesie modelowania budynków – Building Information Modelling (BIM). Trójwymiarowe modele umożliwią projektantom systemów zabezpieczających także wizualizację pola widzenia kamer, dzięki czemu można optymalnie zaplanować rozmieszczenie poszczególnych składników systemu dozorowego.

– Dobór zabezpieczeń elektronicznych powinien być integralną częścią procesu projektowania wszystkich nowych budynków – wyjaśnia Peter Friberg, dyrektor Działu Systemów i Instalacji w firmie Axis Communications. *– By uzyskać możliwie najlepszy poziom bezpieczeństwa i wyeliminować martwe pola, które mogą stanowić potencjalne źródła zagrożeń, systemy zabezpieczające powinny być projektowane w tym samym czasie co inne istotne media, takie jak instalacje elektryczne czy hydrauliczne.*

Mając do dyspozycji nowe, trójwymiarowe modele kamer z serii Axis Camera Families, projektanci systemów zabezpieczających mogą wskazywać rozmieszczenie sieciowych kamer Axis bezpośrednio na planach budynków sporządzonych w oprogramowaniu CAD oraz modelować pola widzenia tych kamer. Dzięki oprogramowaniu można sprawdzić, jak kamera będzie prezentować się na tle wystroju budynku, oraz określić, gdzie znajdą się obszary zasłaniane przez kolumny czy ścianki działowe, co umożliwia wyeliminowanie martwych pól. Oznacza to, że systemy zabezpieczające można teraz projektować na etapie projektowania budynków, gdyż niezbędne do tego narzędzia są zintegrowane z tym samym pakietem oprogramowania, który jest wykorzystywany do tworzenia pozostałych części budynków. Użytkownicy systemów CAD mogą także uzyskać informacje projektowe dotyczące każdej z kamer, takie jak oznaczenie typu i modelu, pobór mocy, rozdzielczość obrazu, typ i rodzaj akcesoriów służących do mocowania.

– Używaliśmy wizualizacji kamer z serii Axis Camera Families podczas projektowania systemów CCTV dla naszych klientów. Rzeczywiste, trójwymiarowe modele kamer dały nam możliwość symulacji realnych warunków panujących w budynku, wykrycia niedociągnięć projektowych oraz przeszkód mechanicznych, a także uniknięcia konfliktów pomiędzy systemem dozoru wizyjnego a innymi systemami instalowanymi w tym samym budynku, takimi jak instalacje elektryczne i hydrauliczne. Dzięki temu uniknęliśmy błędów podczas doboru pola widzenia kamer. Wizualizacje Axis Camera Families są bardzo przydatne także dla naszych klientów, którzy mogą zobaczyć, jak będzie wyglądał ich dom po zakończeniu wszystkich prac budowlanych i instalacyjnych. Ponadto otrzymujemy dane dotyczące rozróżnialności szczegółów, mierzonej liczbą pikseli na jednostce długości obserwowanej sceny. Pozwala to na uzyskanie rozdzielczości i jakości rejestrowanych obrazów, która odpowiada oczekiwaniom naszych klientów – powiedział Todd Kotlaba, Project Manager w TLC Engineering for Architecture, który pobrał pierwotne wersje wizualizacji kamer z serii Axis Camera Families.

Zgodnie z koncepcją procesu Building Information Modeling informacje o wszystkich składnikach budynku, np. o układzie ścian, położeniu drzwi, rozmieszczeniu elementów instalacji hydraulicznej, zostają umieszczone w bazie danych oprogramowania CAD i dają pełny obraz każdego szczegółu konstrukcyjnego budynku. Ta sama baza danych jest wykorzystywana nie tylko podczas projektowania i wznoszenia budynku, lecz także w całym okresie jego eksploatacji, co ułatwia zarządzanie obiektem i jego konserwację.

Wizualizacje z serii Axis Camera Families do oprogramowania Autodesk Revit są bezpłatnie dostępne dla wszystkich partnerów firmy Axis. Obecnie przedstawiają one większość kamer sieciowych firmy Axis i są na bieżąco uaktualniane.

Agata Majkucińska
Axis Communications

Koszty ponoszone przez posiadacza wizyjnego systemu dozorowego

Peter Ainsworth

„Niemądrze jest płacić zbyt dużo, lecz równie niemądrze jest płacić zbyt mało. Gdy płacisz zbyt dużo, tracisz pewną sumę pieniędzy, to wszystko. Gdy płacisz zbyt mało, czasami tracisz wszystko, gdyż przedmiot, który nabyłeś, nie jest w stanie pełnić swoich funkcji. Zgodnie z prawami obowiązującymi w biznesie nie można zyskać dużo, gdy płaci się mało. Po prostu nie jest to możliwe. Jeśli wchodzisz w układ z osobą oferującą najniższą cenę, będziesz musiał przewidzieć pewne dodatkowe wydatki na pokrycie kosztów ryzyka, a to oznacza, że masz wystarczająco dużo pieniędzy, by zapłacić za coś lepszego.” – John Ruskin – dziewiętnastowieczny publicysta i poeta

Nie można narzekać na brak konkurujących ze sobą producentów wizyjnych systemów dozorowych, którzy starają się oferować swoje wyroby po możliwie niskich cenach. Konkurencyjność stanowi siłę napędową dla rynku, na którym pojawiają się coraz nowsze i coraz doskonalsze urządzenia o funkcjach, których pojawienia się jeszcze kilka lat temu nie mogliśmy przewidzieć. Ta sama siła powoduje obniżanie cen, dzięki któremu nabywcy mogą oczekiwać szybkiego zwrotu kosztów związanych z wdrażaniem wizyjnych systemów dozorowych.

Jednakże w obecnej, trudnej sytuacji ekonomicznej mamy do czynienia z koniecznością ograniczania wydatków i często zwrot kosztów inwestycji (ROI) związanych z systemami bezpieczeństwa staje się natychmiastowym lub krótkoterminowym celem ekonomicznym, a nie jest rozpatrywany jako długoterminowy proces zwrotu całkowitych kosztów posiadania systemu dozorowego, rozkładających się na długie lata jego eksploatacji.

Przy obliczaniu całkowitego kosztu systemu należy uwzględnić zarówno koszty jednorazowe, związane z jego zaprojektowaniem, kupnem urządzeń i ich instalacją, jak i koszty związane z eksploatacją i konserwacją, opłaty za usługi telekomunikacyjne, a także koszty związane z jego ewentualną rozbudową. Gdy weźmie się pod uwagę wszystkie te czynniki, okazuje się, że opcja, która wydawała się najtańsza, wcale nie jest opłacalna. Najtańsza kamera może doskonale prezentować się w ulotce reklamowej, z pozoru może idealnie spełniać wymagania inwestora, jednak podczas eksploatacji okaże się, że trzeba ją wymienić na inną znacznie wcześniej niż zakładano, a kamera droższa zaledwie o kilkadziesiąt złotych mogłaby okazać się znacznie trwalsza.

Jak dowiodły badania przeprowadzone przez niezależne firmy badawcze, Samsung jest w Europie postrzegany jako jedna z trzech najlepszych firm produkujących sprzęt zabezpieczający. Do niedawna Samsung był utożsamiany z technologią analogową, jednak obecnie ma w swojej ofercie wiele rozwiązań sieciowych. Wszystkie te produkty są bardzo konkurencyjne cenowo, mają zapewnioną dobrą obsługę gwarancyjną i – co najważniejsze – zostały zaprojektowane z uwzględnieniem potencjalnych przyszłych potrzeb użytkowników. Z tego powodu Samsung nie obawia się konkurencji ze strony producentów tańszych urządzeń, których dostępność stanowi ogromną pokusę dla projektantów, instalatorów i użytkowników końcowych.

Tak więc niniejszy artykuł stanowi obiektywny opis aktualnej sytuacji rynkowej, zaś jego celem jest uwypuklenie kluczowych

Fot. 1. Cyfrowy rejestrator wizyjny Samsung SRD-1673D wykorzystujący technologię 960H

czynników, które powinny być brane pod uwagę podczas oceny długoterminowych korzyści wynikających z wdrożenia wizyjnych systemów dozorowych.

Uczelnia Manchester Metropolitan University może stanowić doskonały przykład tego, w jaki sposób organizacja publiczna dokonała właściwej oceny sytuacji w celu zagwarantowania maksymalnych korzyści, zarówno natychmiastowych, jak i długoterminowych, wynikających z zainstalowania wizyjnego systemu dozorowego. Nowa Szkoła Biznesu, otwarta na tej uczelni we wrześniu 2012 r., mieści się w budynku, którego rozwiązania architektoniczne kosztowały 75 milionów funtów, zlokalizowanym na terenie kampusu University All Saints. 4000 studentów i 1000 doktorantów może korzystać z nowoczesnych rozwiązań, które w nim zastosowano, co wpływa na komfort studiów i poziom badań naukowych prowadzonych we wszystkich dziedzinach biznesu i zarządzania.

– *Pomieszczenia dydaktyczne i sale wykładowe w nowej Szkole Biznesu są wyposażone w najnowszy sieciowy sprzęt audiowizualny* – powiedział Mark Shutt, Security Manager w Manchester Metropolitan University. – *W związku z tym musimy podjąć wysiłki w celu wykrycia potencjalnych złodziei, mogących pokusić się o kradzież cennego sprzętu, w który zainwestowaliśmy w celu zapewnienia możliwie najlepszych warunków do nauki. Oprócz kosztów związanych z wymianą przedmiotów, które mogłyby zostać skradzione lub uszkodzone, mamy do czynienia z nieuniknionymi kosztami związanymi z przerwami w procesie nauczania. Zamierzamy również prowadzić politykę zerowej tolerancji w odniesieniu do zachowań antyspołecznych.*

W nowych budynkach zainstalowano kamery kopułkowe firmy Samsung, w tym 95 stałopozycyjnych kamer typu SNV-3080 i 15 szybkoobrotowych kamer typu SNP-3301 z obiektywami zmiennoogniskowymi, zapewniającymi trzydziestokrotne optyczne powiększenie obrazu. Pozwala to operatorom systemu na dokładną obserwację obiektów lub ludzi przebywających w znacznej odległości od kamer. Oba z wymienionych modeli mają funkcję automatycznej zmiany trybu pracy – z dziennego na nocny i odwrotnie – oraz funkcję rozszerzania zakresu dynamiki obrazu (WDR). Dzięki temu kamery mogą pracować w miejscach, w których oświetlenie jest zmienne lub bardzo kontrastowe. Ponadto oba modele kamer mogą wytwarzać wiele strumieni wizyjnych z odpowiednio dobraną metodą kompresji obrazu, w tym MJPEG, MPEG-4 i H.264, co umożliwia transmisję obrazów do różnych lokalizacji jednocześnie, z poklatkowością dochodzącą do 25 ramek na sekundę i ze zróżnicowaną jakością i rozdzielczością. Dzięki temu obrazy z kamer mogą być obserwowane przez wielu autoryzowanych użytkowników systemu. Przykładowo – pracownicy służb ochrony uczelni mogą obserwować obrazy z kamer w pomieszczeniach kontrolnych i jednocześnie te same obrazy mogą być rejestrowane w celach dowodowych przez urządzenia umieszczone w innym miejscu. Te same obrazy mogą być także rejestrowane na lokalnych kartach pamięci SD i, jeśli to jest wymagane, wysyłane pocztą elektroniczną i przeglądane na urządzeniach przenośnych, takich jak smartfony. Obrazy ze wszystkich 110 kamer są przesyłane do pomieszczenia pracowników ochrony uczelni, mieszczącego się w budynku Manchester Metropolitan University Cambridge South Hall. Pracujący w tym pomieszczeniu operatorzy systemu mogą przeglądać bieżące obrazy lub analizować te, które zostały zarejestrowane podczas incydentów, w czym pomocne jest oprogramowanie firmy Samsung umożliwiające odtwarzanie materiału archiwalnego na jednym z sześciu monitorów.

Fot. 2. Kompaktowa, płaska kamera sieciowa LiteNet o rozdzielczości 1,3 megapiksela

Co na temat tego systemu mają do powiedzenia jego projektanci? – *Wysłuchaliśmy uwag wielu osób, a także prowadziliśmy własne badania, gdyż chcieliśmy stworzyć system dozoru wizyjnego, który nie tylko spełniałby dzisiejsze wymagania, lecz także mógłby być unowocześniony i rozbudowany w przyszłości. Nie mieliśmy nieograniczonego budżetu, dlatego początkowo kusił nas pomysł zbudowania tradycyjnego systemu analogowego. Nie mieliśmy jednak wątpliwości, że system sieciowy jest najlepszym rozwiązaniem ze względu na jego elastyczność, która będzie potrzebna, jeżeli zmienią się wymagania użytkowników. Zwróciliśmy uwagę na właściwy dobór kamer. Doszliśmy do wniosku, że możemy zaufać firmie Samsung i ich kamerom szybkoobrotowym, które zapewniają najlepszą z możliwych proporcję między jakością a ceną.*

Co należy wziąć pod uwagę, jeśli planuje się zastosowanie wizyjnego systemu dozorowego? Oto kilka sugestii:

1) Podczas doboru sprzętu nie należy polegać jedynie na ulotkach reklamowych. Należy żądać od instalatorów pisemnych zapewnień, że zaoferowane kamery, rejestratory wizyjne i inne urządzenia będą spełniać konkretne wymagania danego użytkownika końcowego.
2) Należy sprawdzić, czy producent sprzętu świadczy darmowe usługi projektowe. Mimo iż projektant czy instalator może mieć bardzo dobrych doradców, to właśnie przedstawiciel producenta wie najlepiej, które kamery i inne składniki systemu będą najbardziej odpowiednie.
3) Należy sprawdzić, jak długo będą trwały prace związane z instalacją i uruchomieniem systemu. Oprócz kosztów związanych z robocizną należy brać pod uwagę straty związane z utrudnieniami w działalności własnego przedsiębiorstwa.
4) Należy sprawdzić, czy producent określił przybliżony czas bezawaryjnej pracy oferowanych urządzeń. Ma to szczególne znaczenie w przypadku urządzeń

Fot. 3. Wandaloodporna kamera kopułkowa Samsung SNV-7082

zawierających części ruchome, takich jak kamery szybkoobrotowe.

5) Należy oszacować koszty związane z konserwacją zainstalowanych urządzeń w całym przewidywanym okresie ich eksploatacji.
6) Należy sprawdzić, czy dostępne są aktualizacje oprogramowania dla użytkowanych urządzeń. Przykładowo – kamery najnowszej generacji mają oprogramowanie fabryczne, które może być uaktualniane zawsze wtedy, gdy na rynku pojawią się nowe opcje czy funkcje użytkowe.
7) Należy sprawdzić, czy oferowane urządzenia są i będą kompatybilne z pozostałymi składnikami systemu.
8) Należy sprawdzić, czy producent oferuje darmowe oprogramowanie służące do zarządzania systemem dozoru wizyjnego. Jeśli nie, to należy sprawdzić, jakie są koszty nabycia licencji i wdrożenia takiego oprogramowania.
9) Należy sprawdzić, czy producent zadbał o kompatybilność swoich kamer, rejestratorów wizyjnych i innych urządzeń z platformami oferowanymi przez wiodące, niezależne firmy tworzące oprogramowanie systemowe. Jest to bardzo ważne, gdyż zgodność z powszechnie używanym oprogramowaniem może mieć duży wpływ na koszt eksploatacji i możliwość rozbudowy systemu w przyszłości, gdy wymagania wobec niego ulegną zmianie. Mimo iż wiodący producenci sprzętu, tacy jak Samsung, mogą zapewnić wszystkie elementy niezbędne do zbudowania kompletnego systemu, trzeba mieć możliwość zastosowania sprzętu pochodzącego od innych dostawców. Twórcy oprogramowania VMS, tacy jak Axxon, Aimetis, Digifort, Griffid, Ipronet, Exacq, Genetec, ISS, Milestone, Mirasys, ONssi i Seetec mogą oferować otwarte platformy programowe ułatwiające integrację urządzeń i systemów pochodzących od różnych producentów. Oczywiście funkcje programów oferowanych przez różnych dostawców nie będą identyczne, lecz niezależnie od doboru platformy programowej można oczekiwać poprawnej obsługi kamer i rejestratorów wizyjnych pochodzących od różnych producentów, a także możliwości integracji z innymi urządzeniami i systemami, takimi jak analizatory treści obrazów, systemy kontroli dostępu oraz urządzenia przenośne.
10) Należy sprawdzić, jakie są przybliżone koszty energii zużywanej przez system dozorowy oraz przez jego poszczególne składniki. Dane dotyczące zużycia energii mogą być bardzo zaskakujące dla użytkowników. Na szczęście większość współczesnych kamer sieciowych korzysta z zasilania metodą PoE i odznacza się niskim zużyciem energii.
11) Należy sprawdzić, czy zaproponowane kamery mogą pracować w zmieniających się warunkach oświetleniowych. Jeśli nie, należy przeanalizować koszty instalacji i eksploatacji dodatkowego oświetlenia.
12) Jeśli głównym celem inwestora jest podwyższenie poziomu bezpieczeństwa w danym obiekcie, należy wyjaśnić, czy system ma służyć jedynie do weryfikacji przebiegu zaistniałych incydentów, czy też ma dostarczać materiału dowodowego, który można wykorzystać w sądzie.
13) Ze względu na to, że w chwili obecnej większość wizyjnych systemów dozorowych wykorzystuje technologię sieciową, już na etapie projektu należy dowiedzieć się, jakie będą koszty eksploatacji sieci IP i koszty jej ewentualnej rozbudowy.

Fot. 4. Modułowy system rejestratorów wizyjnych Samsung

14) Należy podać wszystkie wymagania w pisemnej umowie, która ma określać, czego przyszły użytkownik oczekuje od systemu, z jakimi warunkami środowiskowymi należy się liczyć podczas jego eksploatacji, czy planowane jest rozbudowanie go w przyszłości itd. Istnienie takiego dokumentu umożliwi uniknięcie wielu nieporozumień na wszystkich etapach realizacji inwestycji.

Peter Ainsworth
Samsung Techwin Europe

Peter Ainsworth jest zatrudniony w firmie Samsung Techwin Europe jako Senior Product Manager od sierpnia 2009 r. Przedtem przez trzynaście lat pracował w firmie Norbain, w której przez ostatnich osiem lat pełnił funkcję Vista Product Managera.

Dinion HDR

By widzieć więcej

Paweł Piekut
Radomir Dębek

Systemy dozoru wizyjnego są coraz częściej postrzegane jako równie ważne jak dźwiękowe systemy ostrzegawcze czy systemy sygnalizacji pożarowej. W dobie walki o coraz wyższą liczbę pikseli oferowanych przez współczesne przetworniki zapomniano o tym, co jest w systemie dozorowym najważniejsze, czyli o użyteczności obrazu dla operatora. Nieco mniejsze znaczenie ma tutaj obraz bieżący – najważniejsze jest wykorzystanie odtwarzanego materiału

Firma Bosch Security Systems wprowadziła na rynek nową kamerę Dinion HD 1080p HDR (*High Dynamic Range*) charakteryzującą się szerokim zakresem dynamiki, dzięki czemu uzyskuje się dobrą rozróżnialność szczegółów zarówno na jasnych, jak i ciemnych obszarach obrazu. Dzięki adaptacyjnemu przetwarzaniu obrazu można stosować kamery Dinion HD 1080p HDR w bardzo trudnych warunkach oświetleniowych. W celu uzyskania szerokiego zakresu dynamiki obrazu wykorzystana została znana już z kamer Dinion 2X technologia podwójnej ekspozycji. Proces tworzenia pojedynczej ramki obrazu jest podzielony na dwa etapy mieszczące się w oknach czasowych 20 ms. Złożenie obrazów składowych umożliwia uzyskanie obrazu wynikowego odznaczającego się dobrą rozróżnialnością szczegółów zarówno w mocno oświetlonych, jak i w zacienionych częściach. Na uwagę zasługuje również funkcja automatycznej ekspozycji (iAE), która umożliwia śledzenie poruszających się obiektów nawet na bardzo jasnym albo bardzo ciemnym tle.

Nowa kamera Dinion HDR dostępna jest także w wersji z IVA (*Intelligent Video Analysis*). Ten model kamery dokonuje analizy treści obrazu i dostarcza informacji niezbędnych do wygenerowania zróżnicowanych alarmów. Technologia IVA umożliwia realizację dodatkowych funkcji, takich jak wykrywanie ruchu, gromadzenia się tłumu, przekroczenia wirtualnego ogrodzenia, wykrywanie pozostawionych lub usuniętych obiektów. W oprogramowaniu układowym w wersji 5.50 wprowadzono wiele zmian mających związek z działaniem IVA. Administratorzy systemów docenią nową, znacznie prostszą procedurę kalibracji kamer i przystosowywania ich do pracy w danych warunkach eksploatacyjnych. Najnowsza wersja oprogramowania pozwala też na zliczanie osób przebywających w miejscach detekcji zdefiniowanych przez użytkownika.

Dzięki inteligentnym funkcjom możliwe jest znacznie ograniczenie wymagań dotyczących pasma sieciowego oraz ilości pamięci masowej potrzebnej do przechowywania materiału archiwalnego. Algorytm dynamicznej redukcji szumów (iDNR) skutecznie usuwa szumy z obrazu, dzięki czemu wzrasta poziom kompresji strumienia wizyjnego. Kamera w inteligentny sposób dostosowuje jakość obrazu do dostępnego pasma sieciowego.

Nowe oprogramowanie układowe umożliwia również wskazywanie obszarów obrazu, które wymagają szczególnej uwagi. Obszary te można powiększać, odseparowywać i przesyłać osobnymi strumieniami wizyjnymi, dzięki czemu można obserwować jednocześnie całą scenę i osiem wybranych obszarów.

Poprawiono także parametry sieciowe – administrator systemu ma do dyspozycji wiele narzędzi pozwalających na dostosowanie systemu do potrzeb klienta świadomego dostępnych technologii IT. Zarządzanie ruchem w sieciach współdzielonych wymagało dotychczas stosowania specjalnych znaczników w nagłówkach pakietów TCP/IP w ramach konkretnego VLAN. Obecnie usługa QoS (*Quality-of-Service*) jest dostępna w oprogramowaniu układowym, co upraszcza konfigurację systemu. Transmisja obrazów w formacie HTMLv5 upraszcza sposób wysyłania danych do urządzeń mobilnych oraz do urządzeń, w których ze względów bezpieczeństwa nie

powinno się uruchamiać sterowników ActiveX. Implementacja technologii ABR (*Adaptive Bit Rate*) pozwala na skuteczną optymalizację strumienia wizyjnego, którym przesyłane są obrazy przeznaczone do podglądu na żywo lub materiały archiwalne. Należy wspomnieć o zgodności kamer Dinion HD 1080p HDR ze specyfikacją *Profile-S* ONVIF (*Open Network Video Interface Forum*).

Kamera jest wyposażona w intuicyjny interfejs użytkownika, który ułatwia szybką konfigurację. Kreator automatycznego ustawienia ostrości umożliwia instalatorowi precyzyjną regulację ostrości kamer w realnych warunkach roboczych oraz korektę ustawienia w przypadku zmiany trybu pracy kamer z dziennego na nocny albo odwrotnie. Wszystkie funkcje kamer Dinion HD 1080p HDR można skonfigurować za pośrednictwem przeglądarki internetowej.

Kamery Dinion HD 1080p HDR mogą wytwarzać cztery strumienie wizyjne. Trzy z nich to strumienie skompresowane metodą H.264 (strumień HD 1080p30, strumień o obniżonej rozdzielczości i strumień HD, który zawiera tylko ramki referencyjne), natomiast czwarty strumień jest skompresowany metodą M-JPEG. Zastosowanie czterech strumieni umożliwia wyświetlanie obrazu, rejestrowanie go w optymalnych warunkach oraz integrację z urządzeniami wizyjnymi innych producentów.

Kamery Dinion HD 1080p HDR współpracują z systemem zarządzania zapisem BVRM (*Bosch Video Recording Manager*), który przydziela przestrzeń z macierzy iSCSI w sposób dynamiczny, a jednocześnie zapewnia awaryjne przełączenie w przypadku uszkodzenia jednej z macierzy. Kamery Dinion HD 1080p HDR mogą zapisywać strumienie wizyjne bezpośrednio na macierzach iSCSI, bez wykorzystania jakiegokolwiek oprogramowania zarządzającego. W trybie alarmowym strumienie wizyjne mogą być zapisywane na kartach pamięci MicroSD umieszczonych w kamerach. Wykorzystanie kart umożliwia włączenie funkcji automatycznego zapisu w trybie ANR. Jeżeli któraś z kamer utraci połączenie sieciowe z docelowym urządzeniem rejestrującym, np. macierzą SCSI, zacznie zapisywać strumień wizyjny na lokalnej karcie pamięci. Po przywróceniu połączenia sieciowego zarejestrowany materiał zostanie automatycznie przeniesiony na macierze dyskowe.

Obrazy wytwarzane przez kamery Dinion HD 1080p HDR można oglądać, korzystając z przeglądarki internetowej, oprogramowania Bosch Video Management System oraz bezpłatnego oprogramowania Bosch Video Client obsługującego szesnaście kamer IP. Oprogramowanie BVC ma niezwykle przyjazny interfejs użytkownika, który już w kilka chwil po instalacji może być użyty do zarządzania systemem zawierającym nawet 128 kamer. Obsługa takich funkcji jak podgląd obrazu na żywo, odtwarzanie materiału archiwalnego i eksport materiału jest bardzo prosta.

Paweł Piekut
Radomir Dębek
Bosch Security Systems

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Stacjonarne kamery IP 5 Mpx

Kamera standardowej rozdzielczości

Kamera IP 5 Mpx Full HD marki NOVUS®

Rozdzielczość 5 Mpx

fotograficzna jakość obrazu

Praca w trybie czterostrumieniowym

Obiektyw typu „rybie oko"

poziomy kąt widzenia obiektywu: 180°

NVIP-5DN2021D/IR-2P

NVIP-5DN5001C-1P

obiektyw należy do wyposażenia dodatkowego

NOVUS IP

NMS Compatible

ALNET Compatible

Oprogramowanie NMS (Novus Management System) do monitoringu wizyjnego IP w komplecie!

- Matryca CMOS, 1/2.5" ■ 5 megapikseli (2592x1944) ■ Szeroki zakres dynamiki (WDR) ■ Wydłużony czas ekspozycji (DSS) ■ Cyfrowa redukcja szumu (DNR)
- 5 stref prywatności ■ Kompresja H.264 lub M-JPEG ■ Prędkość przetwarzania do 25 kl/s (HD 1080p) ■ Praca w trybie czterostrumieniowym
- Funkcje przed-alarmu i po-alarmu ■ Nagrywanie wideo w formacie AVI ■ Funkcja harmonogramu ■ Sprzętowa detekcja ruchu ■ Obsługa kart SD/SDHC

NVIP-5DN5001C-1P

- Mechaniczny filtr podczerwieni
- Czułość: 0.02 lx/F=1.2
- Dwukierunkowa transmisja audio
- Montaż obiektywu: C/CS
- Zasilanie: 12 VDC/PoE

NVIP-5DN2021D/IR-2P

- Mechaniczny filtr podczerwieni
- Wbudowany oświetlacz podczerwieni
- Czułość: 0 lx, IR wł.
- Obiektyw typu „rybie oko", f=1.05 mm
- Poziomy kąt widzenia obiektywu: 180°
- Dwukierunkowa transmisja audio
- Wbudowany mikrofon i głośnik
- Zasilanie: 12 VDC/24 VAC/PoE

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

Zobacz więcej!

Nowe kamery IP marki NOVUS

Patryk Gańko

Sercem analogowego systemu monitoringu wizyjnego był rejestrator cyfrowy. Głównie on decydował o ostatecznej jakości zapisywanego obrazu, zależnej od typu procesora DSP (cyfrowej obróbki sygnału) i tym samym algorytmu kompresji oraz wybranej przez administratora rozdzielczości i jakości obrazu. W telewizji IP ta odpowiedzialność za jakość obrazu została przeniesiona na peryferie systemu, czyli do kamer. Oprogramowanie odpowiedzialne za przechwytywanie strumieni wizyjnych zapisuje surowy strumień bezpośrednio na twardym dysku jednostki serwerowej lub wyświetla w oknie wizyjnym za pomocą procesora graficznego. Bardzo rzadko stosowana jest rekompresja takiego sygnału, np. w celu zmniejszenia użytecznej przepływności i przesyłania go w sieciach komórkowych do urządzeń mobilnych. Wynika to z możliwości współczesnych kamer IP, których specjalistyczne procesory potrafią generować równocześnie cztery strumienie wizyjne o różnych parametrach. Mogą być one wykorzystane do zapisu (przy maksymalnej rozdzielczości i jakości), podglądu pełnoekranowego (z maksymalną częstotliwością odświeżania), podglądu w podziale (z maksymalną częstotliwością odświeżania i rozdzielczością D1) oraz retransmisji do urządzeń mobilnych (w niskiej rozdzielczości i z niską częstotliwością odświeżania). W związku z powyższym niniejszy artykuł poświęcę charakterystyce nowych modeli kamer IP kompatybilnych z aplikacją NMS (Novus Management System) obsługującą systemy monitoringu wizyjnego IP. Temat wart jest omówienia również ze względu na różnorodność typów wprowadzanych kamer i stosowanych rozwiązań technologicznych

Kamera kopułkowa NVIP-5DN2021D/IR-2P

Wśród instalatorów kamera jest nazywana rybim okiem (ang. *fish-eye*). Nazwę tę zawdzięcza możliwości dookolnej obserwacji dzięki zastosowanemu obiektywowi o długości ogniskowej f=1,05 mm. Kamera świetnie nadaje się do monitorowania dużych zamkniętych pomieszczeń, holi, recepcji etc. Jedna centralnie umieszczona kamera może monitorować całą przestrzeń pomieszczenia. Wysoka jakość generowanego strumienia i związana z nią zdolność do rozpoznawania szczegółów wynika z rozdzielczości zastosowanej matrycy

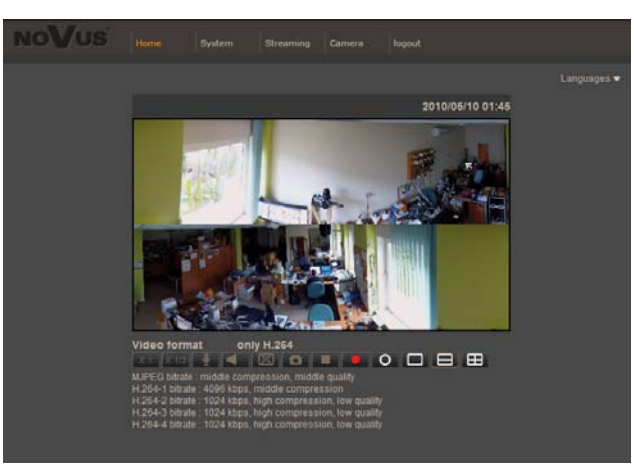
Fot. 1. Kamera kopułkowa NVIP-5DN2021D/IR-2P

CMOS (5 megapikseli) o rozmiarze 1/2,5" i progresywnego skanowania. Należy pamiętać, że ze względu na brak możliwości ustawienia pola widzenia (stała ogniskowa) całkowita rozdzielczość przetwornika rozkłada się na duży obszar. Są cztery tryby wyświetlania strumienia wizyjnego: rybie oko, standardowy, podwójna panorama oraz quad. Dla trybów tych dostępna jest funkcja cyfrowego PTZ umożliwiająca przemieszczanie powiększonego fragmentu obrazu, podobnie jak w typowych kamerach PTZ.

O dostępnych w aplikacji NMS trybach wyświetlania oraz sposobach odtwarzania powyższego strumienia napiszę w kolejnym numerze *Zabezpieczeń*.

Kompaktowa kamera NVIP-5DN5001C-1P

Jest to druga z serii kamer o rozdzielczości przetwornika CMOS 5 megapikseli, wytwarzająca obraz w formacie 4:3 – kamera klasyczna o funkcjach zbliżonych do funkcji kamery Full HD NVIP-2DN5001C-1P przedstawianej już na łamach tego czasopisma. Kamera jest przeznaczona do pracy w trudnych warunkach oświetleniowych. W trybie czarno-białym, bez funkcji wydłużonej migawki jej czułość wynosi 0,02 lx. W najwyższej dostępnej rozdzielczości 2592×1944 kamera generuje do 10 obrazów na sekundę, a w pozostałych rozdzielczościach, także w rozdzielczości FullHD, kamera generuje 25 obrazów na sekundę na żywo. Nową godną uwagi funkcją jest ROI (*Region of Interest*). Dzięki niej można zaznaczyć fragment obrazu, który będzie następnie powiększony/rozciągnięty i utożsamiony z wybranym strumieniem. Kamery mają tryb automatyki ekspozycji z automatycznie regulowanym czasem otwarcia migawki i ustawianym przez administratora progiem. Umożliwia to uzyskanie klarownego obrazu szybko przemieszczających się obiektów w trudnych warunkach oświetleniowych. W menu *sabotaż* można ustalić reakcje kamery na jej zasłonięcie lub zaślepienie.



Fot. 2. Tryb podwójnej panoramy

Fot. 3. Kompaktowa kamera NVIP-5DN5001C-1P

Wandaloodporna kamera NVIP-3DN4010H/IRH-1P

Jest to druga w ofercie 3-megapikselowa kamera marki NOVUS wytwarzająca obraz o proporcjach 4:3. Maksymalna dostępna rozdzielczość strumienia wizyjnego wynosi 2048×1536 przy częstotliwości odświeżania 15 obrazów na sekundę, niezależnej od rozdzielczości. Wbudowany asferyczny obiektyw o zmiennej ogniskowej, regulowanej w zakresie od 3 do 10 mm, zapewnia poziomy kąt widzenia w zakresie 28°~90°. Promiennik podczerwieni ma zasięg do 40 m. Kamera pracuje w trybie trójstrumieniowym. Istnieje możliwość definiowania kompresji, rozdzielczości, prędkości i jakości niezależnie dla każdego strumienia.

Do montażu ściennego kamery stosowany jest uchwyt z puszką przyłączeniową w podstawie, która służy do instalacji zasilacza i realizacji połączeń kablowych. Puszka przyłączeniowa i podstawa kopuły montażowej są zamocowane na zawiasach, co umożliwia łatwy montaż kabli i akcesoriów.

Kompaktowa kamera motor-zoom NVIP-2DN5018CZ-2P

W przypadku wielu obiektów ważna jest możliwość obserwacji szerokiego planu i przybliżenia jego centralnej części. Typowym przykładem jest monitorowanie bramy wjazdowej z przybliżeniem fragmentu centralnego w momencie wjeżdżania samochodu. Wykorzystywanie do tego kamery obrotowej jest rozwiązaniem nieekonomicznym. Należy użyć kamery ze zdalnie regulowaną ogniskową obiektywu. Opisywany model ma obiektyw, w którym ogniskową można zmienić 18-krotnie, w zakresie od 4,7 do 84,6 mm. Wbudowany przetwornik CMOS o rozdzielczości 1920×1080 generuje strumień wizyjny z maksymalną prędkością 25 obrazów na sekundę. Kamera może pracować w trybie czterostrumieniowym. Istnieje możliwość definiowania kompresji, rozdzielczości, prędkości i jakości niezależnie dla każdego strumienia. Dodatkowo, do celów serwisowych oraz w celu integracji z istniejącymi systemami analogowymi, kamera została wyposażona w analogowe wyjście BNC. Pobiera 6 W mocy i może być zasilana przez zewnętrzny zasilacz 24 V_{AC} lub 12 V_{DC} a także przez gniazdo sieciowe RJ45, z wykorzystaniem technologii PoE. W celu ułatwienia operatorowi pracy z kamerą oraz zautomatyzowania procesu obserwacji kamera ma funkcje presetu oraz sekwencji. Preset umożliwia ustawianie oraz zapisywanie pewnych zaprogramowanych ujęć, a sekwencja – wybranie serii cyklicznie zmieniających się ujęć o określonym czasie trwania.

Fot. 4. Wandaloodporna kamera NVIP-3DN4010H/IRH-1P

Fot. 5. Kompaktowa kamera motor-zoom NVIP-2DN5018CZ-2P

W poprzednim numerze *Zabezpieczeń* scharakteryzowałem system sieciowego monitoringu wizyjnego ipGO. Zwracałem uwagę na jego hermetyczność i autonomiczność. W takim systemie nadal mogą pracować jedynie urządzenia z rodziny ipGO, jednak wszystkie kamery są teraz zgodne z systemem NMS w wersji 1.25. Kamery NVIP-2C2001D-P/GO oraz NVIP-2C5005CZ-P/GO zostały opisane w poprzednim artykule. Poniżej chciałbym scharakteryzować trzy nowe modele kamer z rodziny ipGO.

Kamery ipGO: NVIP-2DN2001D/IR-2P/GO (kopułkowa), NVIP-2DN4001V/IR-2P/GO (wandaloodporna), NVIP-2DN3001H/IRH-2P/GO (w obudowie)

Kamery są potocznie określane mianem Full HD. Generują dwa niezależne strumienie o częstotliwości 25 obrazów na sekundę, w rozdzielczości 1920×1080 (obraz ma proporcje 16:9). Wyposażono je w obiektyw z możliwością trzykrotnej zmiany ogniskowej (w zakresie 3–9 mm) oraz z automatyczną regulacją przysłony i ostrości. Regulacja ogniskowej jest czasochłonna i w powyższych kamerach służy jedynie do ustawienia pola widzenia, a nie do ciągłej pracy jak w przypadku modelu NVIP-2DN5018CZ-2P. Kamery mają wbudowany odsuwany mechanicznie filtr podczerwieni. Ponadto zostały wyposażone w 18 lub 40 diod LED o maksymalnym zasięgu, odpowiednio, 10 m i 30 m oraz kącie świecenia 38°. Model wandaloodporny jest umieszczony w obudowie i charakteryzuje się stopniem szczelności IP66. Dzięki zastosowaniu grzałki zakres temperatur, w których działa, wynosi -40°C~50°.

Wszystkie opisane powyżej kamery mają wbudowane przetworniki o rozdzielczościach co najmniej 2 Mpx. Ze względów ekonomicznych wielu inwestorów oczekuje również tanich kamer o niższych rozdzielczościach: D1, 1 Mpx czy 1.3 Mpx. Jest to racjonalne oczekiwanie, zwłaszcza że nie wszystkie obszary obiektu wymagają obserwacji przez kamery o wysokiej rozdzielczości. Co więcej, urządzenia IP umożliwiają równoczesne stosowanie wielu strumieni wizyjnych o różnej jakości. W przyszłości można oczekiwać wprowadzenia na rynek kamer o wspomnianych rozdzielczościach D1, 1 Mpx czy 1.3 Mpx.

Patryk Gańko
AAT Holding

Fot. 6. Kamery ipGO: NVIP-2DN2001D/IR-2P/GO (kopułkowa), NVIP-2DN4001V/IR-2P/GO (wandaloodporna), NVIP-2DN3001H/IRH-2P/GO (w obudowie)

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Stacjonarne kamery IP Full HD

Doskonała jakość obrazu, duża funkcjonalność!

Full HD

Rozdzielczość 2 Mpx Full HD

Kamera standardowej rozdzielczości

Kamera IP Full HD marki NOVUS®

Praca w trybie czterostrumieniowym

SWITCH/ROUTER

Typowa kamera megapikselowa

Kamera IP Full HD marki NOVUS®

Bardzo wysoka czułość

porównywalna z czułością kamer analogowych

obiektyw należy do wyposażenia dodatkowego

NOVUS IP

NMS Compatible

ALNET Compatible

Oprogramowanie NMS (Novus Management System) do monitoringu wizyjnego IP w komplecie!

- Matryca CMOS, 1/2.7" ■ 2 megapiksele (1920x1080) ■ Wydłużony czas ekspozycji (DSS)
- 5 stref prywatności ■ Kompresja H.264, M-JPEG ■ Prędkość przetwarzania do 30 kl/s (HD 1080p)
- Praca w trybie czterostrumieniowym ■ Funkcje przed-alarmu i po-alarmu
- Nagrywanie wideo w formacie AVI ■ Funkcja harmonogramu
- Detekcja ruchu ■ Obsługa kart SD/SDHC

NVIP-2C2011D-P
- Elektroniczna funkcja dzień/noc
- Czułość: 0.1 lx/F=1.5
- Wbudowany mikrofon
- Wbudowany obiektyw f=4 mm
- Zasilanie: PoE

NVIP-2DN2001D-2P
- Mechaniczny filtr podczerwieni
- Czułość: 0.02 lx/F=1.2
- Dwukierunkowa transmisja audio
- Wbudowany obiektyw f=3-9 mm
- Zasilanie: 12 VDC/24 VAC/PoE

NVIP-2DN4001V/IRH-2P
NVIP-2DN3001H/IR-2P
- Mechaniczny filtr podczerwieni
- Wbudowany oświetlacz podczerwieni
- Czułość: 0 lx, IR wł.
- Dwukierunkowa transmisja audio
- Wbudowany obiektyw f=3-9 mm
- Klasa szczelności: IP 66
- Zasilanie: 12 VDC/24 VAC/PoE

NVIP-2DN5001-1P
- Mechaniczny filtr podczerwieni
- Czułość: 0.02 lx/F=1.2
- Dwukierunkowa transmisja audio
- Montaż obiektywu: CS
- Zasilanie: 12 VDC/PoE

NVIP-2DN5018CZ-2P
- Mechaniczny filtr podczerwieni
- Czułość: 0.02 lx/F=1.2
- Dwukierunkowa transmisja audio
- Obiektyw motor-zoom: x18, f=4.7-84.6 mm
- Zasilanie: 12 VDC/24 VAC/PoE

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

Optymalne rozwiązania

Przedsiębiorstwo
Usług Specjalistycznych mvb

W nowoczesnych obiektach wykorzystuje się wiele urządzeń działających w ramach systemów. Odpowiednie zaplanowanie inwestycji, dobry projekt, właściwy dobór urządzeń, współdziałanie systemów i odpowiednie zarządzanie nimi sprawi, że obiekt będzie należycie spełniał swoje funkcje

Dobry projekt kluczem do sukcesu

Aby dobrze zaprojektować dany obiekt, należy wziąć pod uwagę przede wszystkim jego funkcje, potrzeby przyszłych użytkowników oraz możliwość jego ewentualnej rozbudowy. Wielkość budynku, jego wyposażenie, instalacje oraz systemy zabezpieczeń muszą być dostosowane do jego funkcji. Szkolna sala sportowa nie musi być wyposażona tak samo jak areny międzynarodowych mityngów. Z drugiej strony – przygotowując projekty szkolnych obiektów, musimy pomyśleć o ewentualnych zawodach wyższej rangi (ma to wpływ na rozmiary boisk, zaplecze, zegary, mobilne trybuny) i innych imprezach, które mogą się w nich odbywać (możliwość instalacji dodatkowego oświetlenia, nagłośnienia, sprzętu informatycznego). Trzeba być na to przygotowanym już na etapie planowania. Błędne założenia projektowe mogą uniemożliwić wiele rozwiązań, między innymi zastosowanie zintegrowanych systemów bezpieczeństwa czy sieci teleinformatycznych. Uwzględnienie wszystkich elementów projektu – architektury, technologii budowlanych, wyposażenia, automatyki, instalacji – jest jednym z warunków bezpiecznego i sprawnego funkcjonowania infrastruktury.

Ograniczenie kosztów i maksymalizacja korzyści

Ważne jest zastosowanie możliwie najnowocześniejszych urządzeń oraz najnowszych wersji oprogramowania. Wśród technologii związanych z bezpieczeństwem najszybsze zmiany następują w dziedzinie teleinformatyki. Określone rozwiązania inżynieryjne (budownictwo, wentylacja, ogrzewanie) są stosowane przez wiele lat, a nowinki i zmiany w systemach bezpieczeństwa pojawiają się co kilka miesięcy. Ta tendencja zdecydowanie będzie się utrzymywać.

Jeśli najbardziej zaawansowane technologie stają się dostępne dla szerszego grona odbiorców, koszty budowy i wyposażenia obiektu wyraźnie maleją. To oczywista korzyść dla inwestora. Rachunek ekonomiczny jest jednym z podstawowych wyznaczników zakresu i formy inwestycji. Centrum rekreacyjne, pływalnia, hala sportowa czy wystawiennicza musi na siebie zarabiać. Nie chodzi tylko o przedsięwzięcia czysto komercyjne, ale również o lokalne imprezy finansowane przez gminę, związek sportowy lub władze oświatowe. O walorach użytkowych, kosztach utrzymania i wyposażeniu myśli każdy właściciel i administrator…

Pełna integracja – większe korzyści

W świadomości większości użytkowników sprzętu elektronicznego sieć teleinformatyczna to komputery, monitory, kamery, ewentualnie telefony, czujniki i urządzenia alarmowe. Jest to jednak tylko część urządzeń, które funkcjonują w obiekcie.

W inteligentnych budynkach w ramach jednego systemu działa klimatyzacja, wentylacja, oświetlenie, szeroko pojmowana automatyka. Urządzenia mają wspólne okablowanie, a do ich kontrolowania i zarządzania nimi służy jedno oprogramowanie. Właśnie to najpełniej oddaje ideę technologicznej integracji.

Celem podstawowym jest więc sprawna integracja urządzeń elektrycznych, elektronicznych i mechanicznych oraz wszelkiego rodzaju instalacji. Powinny one być jak najlepiej skomunikowane, wydajne i łatwe w obsłudze.

Optymalne rozwiązania

Bardzo ważne jest dostosowanie urządzeń do specyfiki danego obiektu. Wybieramy optymalne rozwiązania, korzystając z wieloletnich doświadczeń w projektowaniu, wykonawstwie i użytkowaniu systemów. Współpraca z wieloma firmami i kooperantami skutkuje znajomością branży. Przywiązanie do jednego dostawcy czy producenta może znacznie utrudnić realizację projektu i zwiększyć koszty. Optymalizację wydatków ułatwia również odpowiednie zarządzanie systemami, właściwe ich skonfigurowanie i wykorzystywanie. Ważne jest wybranie sprawnego integratora systemów, takich jak system zarządzania budynkiem, SAP, DSO, system gaszenia gazem i wykrywania tlenku węgla, CCTV, KD, SSWiN, system teleinformatyczny, multimedialny i inne. W obiekcie sportowym czy rekreacyjnym warto wykorzystać również system ułatwiający zarządzanie, taki jak Sanator SPA lub Sanator ESOK. Użytkownicy tych dwóch systemów mogą korzystać z prostego, intuicyjnego interfejsu odpornego na błędy obsługi. Oprogramowanie to umożliwia wygodną rezerwację biletów, prowadzenie pełnej statystyki oraz raportowanie wewnętrzne i zewnętrzne. Wprowadzane dane są kontrolowane i uzupełniane, a całość wykorzystywana jest w tworzeniu statystyk oraz rozliczeń finansowych, niezbędnych do sprawnego zarządzania bazą rekreacyjną, zabiegową czy też hotelową.

Fot. 1. Dozór kołowrotów przy wejściach/wyjściach

Fot. 2. Monitorowanie płyty stadionu

Powtórzmy to jeszcze raz: dobry projekt obiektu uwzględnia możliwość późniejszego wykorzystania nowszych rozwiązań bez skomplikowanego przekształcania istniejących struktur. Architektura budynku, zastosowane materiały oraz technologie powinny umożliwiać rozbudowę instalacji. Przykładem może być stadion miejski imienia Sebastiana Karpiniuka w Kołobrzegu, który został gruntownie zmodernizowany. Firma mvb, jako partner głównego wykonawcy, odpowiadała za wykonanie wydzielonego systemu zasilania, infrastruktury LAN, systemu nagłośnienia i wykorzystującego kamery IP systemu monitoringu wizyjnego całego obiektu. Wszystkie wymienione systemy i technologie mają wpływ na bezpieczeństwo sportowców, pracowników i kibiców. Na terenie obiektu zainstalowano system CCTV z kamerami IP firmy Axis, które zapewniają najwyższą jakość obrazu. Umożliwiają one podgląd obrazu w czasie rzeczywistym, efektywny dozór w nocy i zdalne zarządzanie systemem. Monitorowane są wszystkie strefy stadionu, między innymi bramki wejściowe i kołowroty, pozostałe wejścia i wyjścia, ciągi komunikacyjne, pomieszczenia socjalne, parkingi, płyta stadionu i trybuny. Najważniejszą funkcją systemu nadzoru na stadionie jest zwiększenie bezpieczeństwa przebywających na nim osób oraz umożliwienie identyfikacji sprawców wykroczeń i aktów wandalizmu.

Fot. 3. Trybuny pod czujnym okiem kamer

Przedsiębiorstwo Usług Specjalistycznych mvb

PTK5507 - dotykowa klawiatura serii POWER

DSC

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

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

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

Wyłączny dystrybutor produktów DSC w Polsce:

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

Zmiany w obowiązujących przepisach

dotyczących ochrony danych osobowych na podstawie projektu rozporządzenia unijnego

Monika Brzozowska
Agnieszka Dymek

W ostatnim czasie Komisja Europejska zaplanowała szereg zmian dotyczących regulacji związanych z ochroną danych osobowych. Zmiany mają ujednolicić zasady posługiwania się danymi osobowymi w Unii Europejskiej oraz poprawić ochronę prywatności użytkowników Internetu. Regulacje te należy traktować przede wszystkim jako odpowiedź na niezwykle szybki rozwój technologiczny w ostatnich latach oraz globalizację

Obowiązująca obecnie dyrektywa 95/46/WE z dnia 24 października 1995 r., dotycząca ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, ma zostać zastąpiona rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Planowana zmiana przepisów ma nastąpić w 2014 roku. Projekt rozporządzenia wprowadza szereg zmian. Poniżej przedstawione zostaną jedynie najważniejsze nich.

Jedną z najistotniejszych zmian zawartych w projekcie rozporządzenia jest zwiększenie odpowiedzialności, jaką będzie ponosić administrator danych w związku z naruszeniem postanowień dotyczących ochrony danych osobowych. Na mocy art. 79 projektu rozporządzenia każdy organ nadzorczy będzie uprawniony do nakładania sankcji administracyjnych. Sankcje te mogą dotyczyć w szczególności uchybień związanych z wyznaczeniem inspektora ochrony danych i utrudnianiem mu wykonywania jego zadań. W przypadku nieumyślnego naruszenia będą udzielane jedynie pisemne ostrzeżenia – gdy osoba fizyczna przetwarza dane osobowe nie tylko w celach handlowych lub przetwarzanie danych osobowych przez przedsiębiorstwo lub organizację zatrudniającą mniej niż 250 osób ma jedynie charakter poboczny w stosunku do głównej działalności. Rozporządzenie określa wiele potencjalnych naruszeń, na skutek których na administratora danych mogą zostać nałożone kary administracyjne. Projekt określa trzy rodzaje kar finansowych:

– maksymalnie 250000 euro, a w przypadku przedsiębiorstwa maksymalnie 0,5% jego rocznego światowego obrotu;
– maksymalnie 500000 euro, zaś w przypadku przedsiębiorstwa maksymalnie 1% jego rocznego światowego obrotu;
– maksymalnie 1000000 euro, a w przypadku przedsiębiorstwa maksymalnie 2% jego rocznego światowego obrotu.

Nakładanie kar będzie wchodziło w zakres obowiązków Generalnego Inspektora Ochrony Danych Osobowych. Zgodnie z projektem rozporządzenia sankcja administracyjna ma być w każdym indywidualnym przypadku skuteczna, proporcjonalna oraz odstraszająca.

Kolejna zmiana jest związana z rozszerzeniem zakresu obowiązków administratora danych. Będzie on zobowiązany między innymi do poinformowania Generalnego Inspektora Danych Osobowych o naruszeniu przepisów w ciągu doby od momentu otrzymania informacji o naruszeniu. Administrator byłby zatem zobowiązany do prowadzenia rejestru naruszeń zawierającego informacje o incydentach zagrażających bezpieczeństwu danych osobowych. Tym samym nowe obowiązki będzie mieć również Generalny Inspektor Danych Osobowych, w którego gestii będzie reagowanie na zgłoszenia o naruszeniach. Generalny Inspektor Danych Osobowych będzie mógł także skontrolować administratora danych. Celem wprowadzenia tej zmiany jest zobowiązanie administratorów do jak największego ograniczenia liczby naruszeń zasad ochrony danych osobowych.

Art. 35 ust. 1 projektu rozporządzenia narzuca obowiązek wyznaczenia inspektora ochrony danych osobowych. Owa regulacja dotyczy administratorów zatrudniających więcej niż 250 osób lub będących podmiotem publicznym, a także tych, których główna działalność polega na przetwarzaniu danych, które ze względu na swój charakter, zakres lub cele wymaga regularnego i systematycznego monitorowania podmiotów danych. Jeżeli administrator lub podmiot przetwarzający jest organem lub podmiotem publicznym, inspektor ochrony danych może być wyznaczony dla jednostek organizacyjnych z uwzględnieniem struktury organizacyjnej danego podmiotu. Wyznaczenie inspektora ochrony danych następuje na podstawie jego kwalifikacji zawodowych, specjalistycznej wiedzy z zakresu prawa dotyczącego ochrony danych, praktyki i zdolności do wykonywania zadań wynikających z wymogów projektu rozporządzenia. Zgodnie z art. 35 ust. 5 projektu rozporządzenia niezbędny poziom specjalistycznej wiedzy ustalany jest w szczególności zgodnie z rodzajem przetwarzania danych oraz wymaganą ochroną danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający.

Projekt wprowadza rozwiązanie nazywane punktem kompleksowej obsługi. Zmiana jest związana z podkreśleniem roli siedziby administratora danych osobowych oraz przetwarzającego. Działalność organów ochrony danych w państwie członkowskim, w którym administrator danych osobowych ma siedzibę, nie będzie wykluczała współudziału organów ochrony danych innych państw członkowskich w podejmowaniu decyzji. Nierzadko – na mocy obowiązujących przepisów – usługodawcy, których działalność była prowadzona na terytorium kilku państw członkowskich, musieli rejestrować swoje bazy danych w każdym z tych państw. Zgodnie z nowymi przepisami wystarczy dokonać zgłoszenia jedynie w urzędzie tego kraju, w którym znajduje się główna siedziba danego usługodawcy.

Nowością jest także rezygnacja z obowiązku rejestracji zbioru danych. W zamian za to konieczne będzie prowadzenie bardziej rozbudowanej dokumentacji, gdyż zgodnie z art. 28 rozporządzenia administrator danych oraz przetwarzający dane mają obowiązek przechowywać dokumentację dotyczącą zbioru, która musi być ujawniona organowi ochrony danych na jego żądanie. Na usługodawcach i usługobiorcach będzie

ciążył obowiązek opracowania raportów zawierających ocenę skutków przetwarzania danych oraz informacje o przewidywanych środkach i gwarancjach mających zapewnić ich ochronę. W raportach należy również wykazać zgodność zastosowanych procedur z rozporządzeniem.

Projekt rozporządzenia przewiduje także zmiany tzw. wiążących reguł korporacyjnych (*Binding Corporate Rules – BCRs*) dotyczących przekazywania sobie danych osobowych przez podmioty z różnych krajów należące do tej samej grupy korporacyjnej.

Projekt rozporządzenia zawiera również przepisy dotyczące zgody osoby, której dane mają być przetwarzane. Chodzi przede wszystkim o przetwarzanie tych danych, których nie można przetwarzać bez uzyskania zgody osoby, której te dane dotyczą. Art. 8 mówi także o zgodzie rodzica lub opiekuna jako warunku dostępu dzieci do usług o charakterze informacyjnym. W rozporządzeniu została określona także zgoda jako podstawa prawna profilowania i transferu danych oraz instytucja odmowy zgody.

Na mocy projektu rozporządzenia Komisja Europejska będzie mogła w większym stopniu bezpośrednio wpływać na zasady ochrony danych osobowych w systemach krajowych, wydając tzw. akty delegowane. Jako przykład można tutaj podać wprowadzenie ujednoliconego w całej UE formularza służącego do komunikacji administratorów i podmiotów przetwarzających dane.

Projekt przewiduje także wspólną odpowiedzialność wobec osoby, której prawa zostały naruszone, w razie istnienia wielu administratorów i podmiotów przetwarzających, co ma ogromny wpływ na poprawę ochrony danych. Podmioty, których dane są chronione, będą zatem uprawnione do domagania się pełnego odszkodowania od każdego z administratorów lub podmiotów przetwarzających dane, lub od wszystkich jednocześnie. Warto zwrócić uwagę także na to, że organizacje społeczne, których statutowym celem jest ochrona danych osobowych, będą mogły występować w postępowaniu sądowym w imieniu grupy poszkodowanych podmiotów.

W projekcie rozporządzenia zawarte zostały także zapisy dotyczące m.in. prawa do usunięcia danych (tzw. prawa do bycia zapomnianym), przenoszenia danych, regulacje związane z profilowaniem oraz zapisy dotyczące zmiany struktury dokumentacji związanej z obowiązkiem informacyjnym.

Skutkiem zastąpienia dyrektywy rozporządzeniem będzie bezpośrednie obowiązywanie przepisów dotyczących ochrony danych osobowych w krajach członkowskich Unii Europejskiej. Nie będzie konieczności wydawania aktów prawnych wprowadzających je do prawa krajowego. Rozporządzenie wejdzie w życie prawdopodobnie na początku 2015 r.

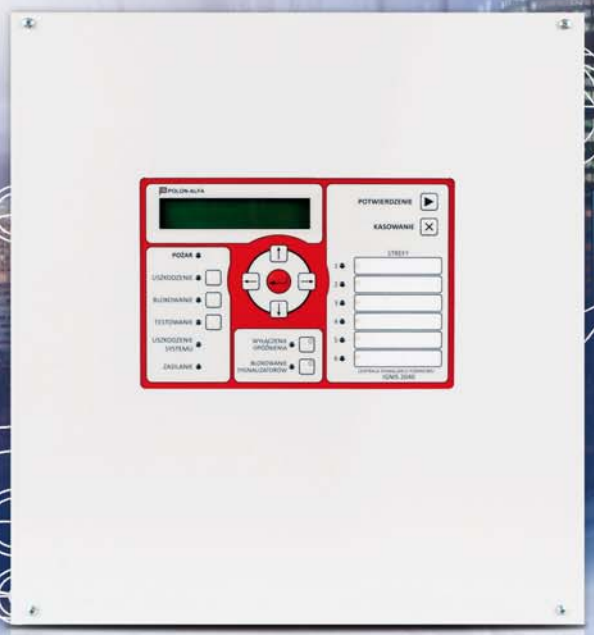
Monika Brzozowska
dyrektor Departamentu Danych Osobowych
w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy,
ekspert Instytutu Sobieskiego

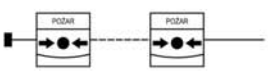
Agnieszka Dymek
aplikant adwokacki
w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

IGNIS 2040

OCHRONA PRZECIWPOŻAROWA MAŁYCH OBIEKTÓW



WEJŚCIA	IGNIS 2040	WYJŚCIA
 do 32 czujek punktowych		→ przekaźniki alarmu i uszkodzenia
 do 10 ręcznych ostrzegaczy pożarowych		→ zasilanie urządzeń zewnętrznych (24 V)
 czujka liniowa		→ linie sterujące sygnalizatorami
 czujki iskrobezpieczne	• od 4 do 6 linii dozorowych • 2 linie sterujące sygnalizatorami (zamiennie z liniami dozorowymi) • 5 lat gwarancji	→ odczyt pamięci zdarzeń

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

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

Depozytor na klucze systemowe SAIK LOCK

Depozytor SAIK LOCK służy do bezpiecznego przechowywania, wydawania i przyjmowania kluczy. Każdy klucz znajdujący się w szafce jest chroniony i dostęp do niego mają tylko uprawnione osoby.

Klucze deponowane są w sposób uniemożliwiający podgląd ich profilów w trakcie przechowywania. W szafkach typu SAIK LOCK istnieje możliwość zastosowania systemów klucza generalnego dowolnego producenta. Jeśli funkcjonują one już w przedsiębiorstwie, nie ma potrzeby wymiany kluczy.

Wszystkie zdarzenia zachodzące w systemie są przez niego rejestrowane z uwzględnieniem daty, czasu oraz danych użytkownika i umożliwiają tworzenie szczegółowych raportów w oparciu o przyjęte kryteria.

Szafka SAIK LOCK wyposażona jest w duży ciekłokrystaliczny wyświetlacz z panelem dotykowym. Umożliwia to wygodne korzystanie z dodatkowych funkcji systemu - na przykład wbudowanej Rejestracji Czasu Pracy – czy wyświetlanie komunikatów od administratora.

Najważniejsze cechy

- Pobranie klucza tylko przez osoby upoważnione
- Zwrot klucza do dedykowanego otworu chroniącego profil klucza
- Wielkość depozytora dowolnie dostosowana do potrzeb klienta
- Duży, kolorowy wyświetlacz LCD z panelem dotykowym
- Standardowo montowany czytnik kart Mifare lub Unique
- Możliwość współpracy z dowolnym innym czytnikiem kart
- Możliwość współpracy z różnymi systemami kontroli dostępu, alarmowymi lub ppoż.
- Wbudowane akumulatorowe zasilanie awaryjne
- Dołączone oprogramowanie instalowane na dowolnej liczbie komputerów pozwalające na pełną kontrolę nad obiegiem kluczy w firmie
- Możliwość podglądu stanu szafki z poziomu przeglądarki internetowej
- Możliwość wyboru dowolnego koloru z palety RAL
- Możliwość dowolnej rozbudowy systemu
- Współpracuje z depozytorami wyposażonymi w tzw. breloki (typu SAIK KEY)
- Możliwość wbudowania kamery nadzorującej osoby korzystające z depozytora
- Podłączenie szafek do sieci LAN
- Wbudowana rejestracja czasu pracy (RCP)
- Możliwość dostosowania depozytora do potrzeb klienta

Producent:

bt electronics

bt electronics sp. z o.o.
Kraków, ul. Dukatów 10
31-431 Kraków

tel. 12 429 36 16, faks 12 410 85 11
e-mail: kontakt@saik.pl
www.saik.pl, www.bte.pl

SAIK SOFT – elektroniczny system wsparcia portiera

System SAIK SOFT to rozwiązanie dla tych firm i instytucji, które potrzebują łatwo i kompleksowo usprawnić organizację obiegu kluczy używanych przez pracowników.

Osoby odpowiedzialne za wydawanie kluczy wyposażone są w elektroniczny Rejestrator Portiera SAIK SOFT. Za pomocą tego urządzenia każde wydanie i zwrot klucza jest odnotowywane przez dołączone oprogramowanie. Dzięki niemu zawsze istnieje możliwość kontroli nad tym kto, kiedy i jaki klucz pobrał.

Co równie istotne, pracownicy mogą dostać tylko ten klucz, do którego mają uprawnienia i tylko w godzinach określonych przez administratora. Takie rozwiązanie pozwala skrócić do niezbędnego minimum czas potrzebny na pobranie i zwrot klucza, zachowując jednocześnie obowiązujące standardy bezpieczeństwa.

System SAIK SOFT posiada także wbudowany moduł rejestracji czasu pracy (RCP), dzięki temu każde przyłożenie przez pracownika karty do czytnika może określać jego czas pracy. W ten sposób system SAIK SOFT można wykorzystywać dla wszystkich pracowników, lub tylko dla wydzielonej ich części.

Zastosowanie SAIK SOFT całkowicie eliminuje konieczność wypełniania i przechowywania dokumentów, takich jak np. księga ewidencji kluczy, książka wejść-wyjść, zeszyt wyjść służbowych. Dzięki temu przewyższa te rozwiązania funkcjonalnością i ilością gromadzonych informacji.

Zaawansowane oprogramowanie, składające się z części administracyjnej, raportowej i alarmowej pozwala na dostosowanie systemu do indywidualnych potrzeb Klienta. Typ rejestratora, liczba obsługiwanych kluczy oraz inne elementy systemu mogą być dowolnie dopasowane do wymagań obiorcy.

Najważniejsze cechy

- Identyfikacja użytkowników w oparciu o osobiste karty zbliżeniowe
- Do każdego klucza przypięty jest brelok, na którym zaszyfrowane są informacje umożliwiające identyfikację klucza
- Każdy pracownik posiada przypisane do siebie klucze
- Elastycznie definiowane przedziały czasowe dostępu do kluczy
- Akumulatorowe zasilanie awaryjne Rejestratora Portiera
- Łatwa wymiana kluczy, możliwa do wykonania przez administratora
- Archiwizacja wszystkich zdarzeń zachodzących w systemie
- Wielostanowiskowe oprogramowanie systemowe pozwalające na przyjazne administrowanie systemem
- Gwarancja jakości i prawidłowej pracy systemu – produkt polski
- Stała 24 h obsługa techniczna
- Wbudowana rejestracja czasu pracy (RCP)

Producent:

bt electronics

bt electronics sp. z o.o.
Kraków, ul. Dukatów 10
31-431 Kraków

tel. 12 429 36 16, faks 12 410 85 11
e-mail: kontakt@saik.pl
www.saik.pl, www.bte.pl

Monitor wideodomofonowy CDV-70P

COMMAX SmartHome & Security

Oferta firmy wzbogaciła się o nowy model monitora COMMAX CDV-70P. Monitor przeznaczony jest dla domów jedno- i wielorodzinnych oraz niewielkich bloków mieszkalnych. Posiada siedmiocalowy ekran o wysokiej rozdzielczości z podświetleniem diodami LED oraz sensoryczne przyciski służące do obsługi systemu. Monitor może współpracować z dwoma panelami zewnętrznymi (obsługa dwóch wejść) lub z jednym panelem i dodatkową kamerą CCTV (podgląd większego obszaru). Wewnątrz lokalu możliwa jest rozbudowa systemu o dodatkowe urządzenia z serii CDV-xxx oraz unifony DP-4VHP pełniące rolę interkomu. Monitor współpracuje z każdą kamerą COMMAX w systemie czterożyłowym i jest produkowany w dwóch wersjach zasilania: 230 V_{AC} lub 24 V_{DC}.

Właściwości

- Kolorowy monitor
- Wyświetlacz 7" Color TFT-LCD 16:9
- Standard sygnału wizyjnego PAL/NTSC
- Dwa wejścia wizyjne
- Możliwość podłączenia dodatkowego monitora
- Współpraca z unifonami DP-4VHP
- Paging pomiędzy stacjami
- Instalacja czteroprzewodowa + obwód elektrozamka
- Współpraca z kamerami analogowymi, czteroprzewodowymi
- Zasilanie 230 V lub 24 V (wersja DC)

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 IXC-2050IR

IXC2050IR poszerza ofertę **kamer IP XNET** firmy CNB o kamerę kompaktową. IXC2050IR to kamera *all-in-one*, czyli kamera, obiektyw oraz podświetleniem w jednej obudowie przystosowanej do pracy na zewnątrz. Kamera ma rozdzielczość Full HD przy częstotliwości 25 kl./s i tworzy obraz o proporcjach 16:9 zapewniających szersze pole widzenia kamery, przetwornik CMOS jest skanowany progresywnie, co zapewnia wyraźniejszy obraz obiektów ruchomych. Kamera wytwarza dwa niezależne strumienie wizyjne. Dodatkową zaletą jest możliwość zasilania kamery metodą PoE oraz obudowa zewnętrzna o klasie szczelności IP66. To idealna kamera do monitoringu firm i osiedli mieszkaniowych.

Właściwości

- Kolorowa kamera z funkcją dzień/noc
- Rozdzielczość Full HD 1920×1080 px @ 25 kl./s
- Rozdzielczość 1100 linii
- Wbudowany obiektyw f=4mm F1,8 DC Iris
- Podświetlenie w podczerwieni IR LED 850 nm o kącie promieniowania 45°
- Dwukierunkowa komunikacja głosowa
- Analogowe wyjście wizji PAL/NTSC
- Regulacje jasności oraz koloru, AGC, BLC, AWB, redukcja migotania, D/N, DSS
- Zasilanie 12 V_{DC} albo PoE IEEE 802.3af

Do kamery dołączone są bezpłatne programy:
CMS (dwa monitory, 128 kanałów w tym 64 kamery IP, E-mapa, pełna zdalna obsługa kamer), Axxon Smart Start pozwalający na nagrywanie obrazów z 16 kamer z możliwością analizy obrazu, a także Digifort w wersji na 16 kamer.

Ponadto z naszej strony *www.gde.pl* można pobrać następujące programy:

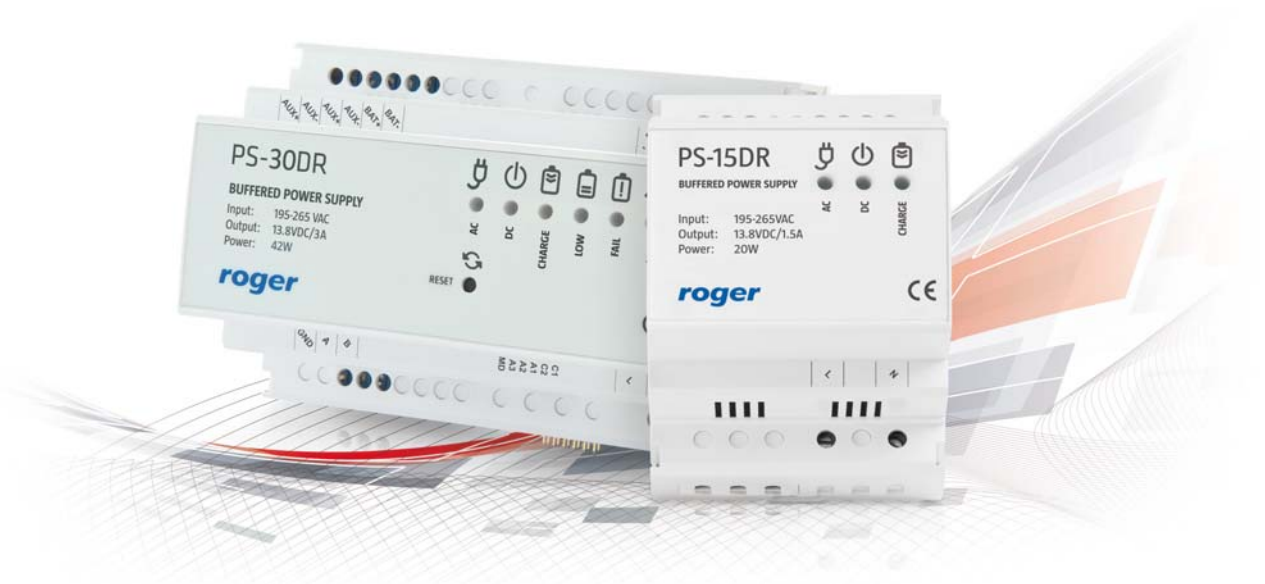
- Multi IP Installer, który pozwala na zbiorcze, automatyczne, równoczesne i szybkie zarządzanie wieloma kamerami, za pomocą jednego programu,
- program NVR CNB , który pozwala na nagrywanie obrazów z 32 kamer bez limitu wielkości bazy danych.

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

PS-15DR i PS-30DR
Moduły zasilające do systemów kontroli dostępu



PS-15DR i PS-30DR to zasilacze impulsowe wyposażone w zaawansowany system zabezpieczeń oraz umożliwiające podłączenie akumulatora awaryjnego. PS-30DR posiada ponadto zintegrowany układ dozoru kontrolujący i przekazujący informacje o pracy urządzenia. Dedykowany jest w szczególności do systemów, w których wymagany jest zdalny bądź lokalny dozór parametrów pracy zasilacza. Oba moduły oferowane są w obudowach z tworzywa sztucznego przystosowanych do montażu na szynie DIN 35 mm.

PS-15DR

- Napięcie zasilania: 230 V_{AC}
- Napięcie wyjściowe: 13.8 V_{DC} (może się zmieniać w granicach od ~11.5 V do 13.8 V w zależności od aktualnego stanu naładowania akumulatora)
- Maksymalny prąd wyjściowy: 1.5 A
- Maksymalny (krótkotrwały) prąd wyjściowy z dołączonym akumulatorem: 2.5 A
- Zabezpieczenia: przeciążeniowe, przepięciowe, termiczne
- Współpraca z akumulatorem ołowiowo-kwasowym (typu SLA lub AGM) o napięciu znamionowym 12 V

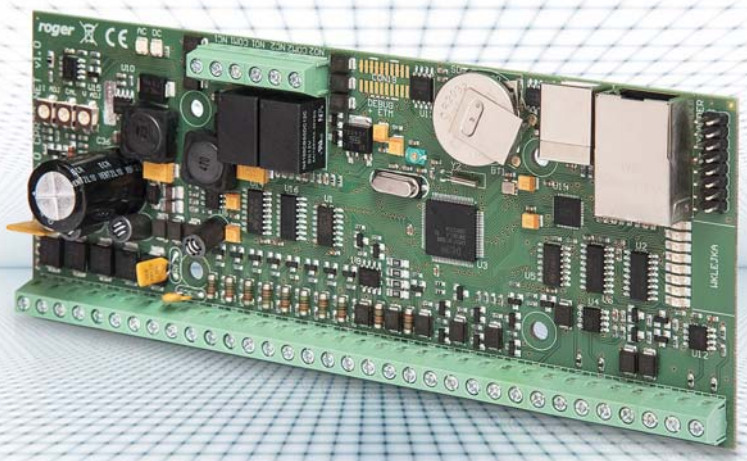
PS-30DR

- Napięcie zasilania: 230 V_{AC}
- Napięcie wyjściowe: 13.8V_{DC} (może się zmieniać w granicach od ~11.5 V do 13.8 V w zależności od aktualnego stanu naładowania akumulatora)
- Maksymalny prąd wyjściowy: 3 A
- Maksymalny (krótkotrwały) prąd wyjściowy z dołączonym akumulatorem: 4 A
- Zabezpieczenia: przeciążeniowe, przepięciowe, termiczne
- Dozór parametrów: zanik napięcia sieciowego, przeciążenie części sieciowej zasilacza, niski poziom napięcia akumulatora, uszkodzony lub odłączony akumulator
- Standardy systemu dozoru: RACS (Roger), autonomiczny (na linach wyjściowych typu OC)
- Współpraca z akumulatorem ołowiowo-kwasowym (typu SLA lub AGM) o napięciu znamionowym 12 V

Producent: roger®
Roger Sp.j.
Gościszewo 59
82-400 Sztum, woj. Pomorskie
tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

Centrala CPR32-NET

Centrala systemu kontroli dostępu RACS 4 z interfejsem IP/Ethernet



Centrala CPR32-NET stanowi kolejną, rozwojową wersję oferowanej od kilku lat centrali kontroli dostępu typu CPR32-SE. Ten nowy produkt realizuje wszystkie funkcje swojego poprzednika, a dodatkowo oferuje szereg nowych możliwości, z których najważniejsze to możliwość programowej integracji z centralami alarmowymi INTEGRA (wymagany jest interfejs INT-RS) oraz możliwość współpracy z zamkami mechatronicznymi serii SALLIS (firmy SALTO). Zrealizowana w centrali CPR32-NET koncepcja integracji z centralami INTEGRA polega na możliwości sterowania uzbrojeniem stref alarmowych, zarówno z poziomu manipulatorów systemu alarmowego jak i czytników systemu kontroli dostępu. Ponadto system kontroli dostępu pobiera i wyświetla w swoim logu zdarzeń pewne krytyczne zdarzenia pochodzące z systemu alarmowego w wyniku czego operator systemu może się ograniczyć do monitorowania jednego wspólnego logu zdarzeń. Nowa centrala oferuje także opcję zapisu zdarzeń na wymiennej karcie pamięci FLASH co powoduje, że zastosowanie odpowiednio dużej karty pamięci może w praktyce zabezpieczyć bufor zdarzeń na kilka lat pracy systemu bez zagrożenia jego przepełnieniem. Komunikacja z nową centralą odbywa się przez sieć LAN/WAN z wykorzystaniem standardu szyfrowania AES 128.

Charakterystyka

- Obsługa systemu złożonego z maks. 32 kontrolerów serii PR
- Osiem wejść parametrycznych
- Sześć wyjść tranzystorowych 15 V_{DC}/1 A
- Dwa wyjścia przekaźnikowe 30 V/1,5 A
- Zarządzanie harmonogramami czasowymi i kalendarzami
- Wbudowany interfejs komunikacyjny IP/Ethernet
- Szybka, szyfrowana transmisja danych pomiędzy centralą a komputerem zarządzającym
- Wbudowany nieulotny bufor pamięci o pojemności 250 tys. zdarzeń z możliwością rozszerzenia o dodatkową kartę pamięci
- Realizacja funkcji globalnych (Strefy Alarmowe, Globalny Antipassback itd.)
- Integracja programowa z centralami alarmowymi Integra (firmy SATEL)
- Integracja programowa z zamkami mechatronicznymi Sallis (firmy SALTO)
- Zasilanie 18 V_{AC} lub 12 V_{DC}
- Wbudowany zasilacz impulsowy z wyjściem 12 V_{DC}/1 A
- Aktualizacja oprogramowania wbudowanego (firmware)

Producent: roger®

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

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

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

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

ALARM SYSTEM
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

ALPOL Sp. z o.o.
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 16
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. Paulinów 10, 67-200 **Głogów**
tel. 32 750 30 78
faks 32 750 30 69
e-mail: glogow@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. Nowodworska 23, 59-200 **Legnica**
tel. 32 750 30 66
faks 32 750 30 67
e-mail: legnica@e-alpol.com.pl

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

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

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

ul. Młodzianowska 75d, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@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. Polna 134/136, 87-100 **Toruń**
tel. 32 750 30 80
faks 32 750 30 73
e-mail: torun@e-alpol.com.pl

ul. Rzymowskiego 34, 02-697 **Warszawa-Mokotów**
tel. 32 790 76 34
faks 32 790 76 69
e-mail: warszawa@e-alpol.com.pl

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

ul. Spółdzielcza 3, 87-800 **Włocławek**
tel. 32 750 30 43
faks 32 750 30 45
e-mail: wloclawek@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

ul. Dekoracyjna 3, 65-722 **Zielona Góra**
tel. 32 750 30 70
faks 32 750 30 71
e-mail: zielona@e-alpol.com.pl

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

FIRMA ATLine Sp. J.
Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. 42 23 13 849, 23 63 019
faks 42 655 20 99
e-mail: handel@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 41 00
faks 22 715 41 05
e-mail: dominika.kolodziejska@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 801 133 084
faks 22 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58
faks 52 387 54 66 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: info@cbcpoland.pl
www.cbcpoland.pl

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

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

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 340 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. 665 380 677
faks 12 260 13 95

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

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

DG ELPRO
Z. Durlak, K. Durlak, J. Golonka Sp. J.
ul. Wadowicka 6
30-415 Kraków
tel. 12 263 93 85-86
faks 12 263 93 85
e-mail: biuro@dgelpro.pl
www.dgelpro.pl

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

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 812 05 05
faks 22 812 62 12
e-mail: sales@ebs.pl
www.ebs.pl

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

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

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

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

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

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

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

GEO-KAT Sp. z o.o.
ul. Taneczna 7
02-829 Warszawa
tel. 22 877 08 80
faks 22 877 08 97
e-mail: info@geokat.com.pl
www.geokat.com.pl

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

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 49 79
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53
faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

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

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

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

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

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

NOVATEL Sp. z o.o.
ul. Turystyczna 1
43-155 Bieruń
tel. 32 201 17 04
faks 32 201 15 10
e-mail: novatel@novatel.pl
www.novatel.pl

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

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel./faks 71 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

OMC INDUSTRIAL Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sprzedaz@omc.com.pl
www.omc.com.pl

Przedstawicielstwo:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks 32 202 55 82
e-mail: katowice@omc.com.pl

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

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

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

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

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

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

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

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

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

SAMSUNG TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Marynarska 15
02-674 Warszawa
tel. 22 205 07 77
faks 22 205 07 63
e-mail: STEsecurity@samsung.com
www.samsungsecurity.com

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

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

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Iłżecka 24
02-135 Warszawa
tel. 22 313 24 15, 511 84 64
faks 22 313 24 10
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.com

Oddziały:
ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. 58 782 00 01
faks 58 782 00 04

ul. Muchoborska 18
54-424 **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

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44a
02-672 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

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

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

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

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

SPS Electronics Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.pl
www.spselectronics.pl

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

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

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

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

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

SECURITY SOLUTION NETWORK Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: ssn@ssn.net.pl
www.ssn.net.pl

TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. 22 516 97 97
faks 22 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

UNICARD S.A.
ul. Łagiewnicka 54
30-417 Kraków
tel. 12 398 99 19
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
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

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

Nowa centrala alarmowa i klawiatura z serii POWER

DSC

PC1404
Centrala alarmowa

- Przeznaczona do stosowania w mieszkaniach, sklepach, biurach itp.
- 4 - 8 linii dozorowych
- Do 4 klawiatur w systemie
- Wbudowany dialer telefoniczny
- Obsługa do 4 numerów telefonów
- 1 podsystem
- Rejestr 128 zdarzeń
- 39 kodów użytkownika
- Elastyczna konfiguracja

PC1404 RKZ
8-liniowa klawiatura LED

- Kompatybilna z centralami PC1404, PC1616, PC1832, PC1864
- Nowoczesny wygląd
- Podświetlone przyciski ułatwiające obsługę
- 4 programowalne przyciski funkcyjne
- Zacisk linii klawiaturowej
- Podwójne przyciski Pożar, Pomoc, Panika
- Podwójne zabezpieczenie antysabotażowe przed otwarciem lub oderwaniem od ściany
- Obsługa 1 podsystemu

Seria POWER to funkcjonalne i niezawodne rozwiązania, dopasowane do indywidualnych potrzeb użytkowników. Wszystkie urządzenia w ramach serii są ze sobą kompatybilne i umożliwiają dowolną konfigurację systemu alarmowego.

Wyłączny dystrybutor produktów DSC w Polsce:

AAT

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS Fire & Security	–	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	–	TAK	–	–
Alarmtech Polska	TAK	TAK	TAK	–	–
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	TAK	–	TAK
ASSA ABLOY	–	–	TAK	–	TAK
FIRMA ATLine	–	TAK	TAK	TAK	–
BOSCH	TAK	–	–	–	–
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC (Poland)	TAK	TAK	TAK	–	TAK
CMA	TAK	–	–	TAK	–
D-MAX	–	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	–
EBS	TAK	TAK	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
EST POLSKA	–	–	TAK	–	TAK
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	–	TAK	–	TAK
GEO-KAT	–	TAK	TAK	TAK	–
ICS POLSKA	–	TAK	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK

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

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, karty magnetyczne i zbliżeniowe								
AGIS Fire & Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	TAK	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
FIRMA ATLine	TAK	–	TAK	–	TAK	TAK	–	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	–	–	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC (Poland)	–	TAK	–	–	–	–	–	–	–
CMA	TAK	TAK	–	–	–	TAK	TAK	–	–
D-MAX	–	TAK	–	–	–	–	–	–	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Dyskam-Ekotrade	TAK	TAK	–	TAK	–	–	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EBS	transmitery GSM/GPRS/IP, systemy RFID i GPS, zabezpieczenia dla bankowości, energetyki, produkcja OEM/ODM								
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
EST POLSKA	TAK	TAK	TAK	–	TAK	–	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
GEO-KAT	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
ICS POLSKA	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Janex International	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
KABE	TAK	TAK	TAK	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
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Novatel	–	TAK	TAK	–	–	TAK	TAK	–	TAK
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	TAK	TAK	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	–	–	–	TAK	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	–	–	–
RISCO	TAK	–	–	–	–	–	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	–	–	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
SSN	–	TAK	TAK	–	–	–	–	–	–
Tap – Systemy Alarmowe	TAK	TAK	TAK	–	–	TAK	–	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
UNICARD	TAK	TAK	TAK	TAK	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

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

Skład i łamanie
Tomasz Kaczmarczyk

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

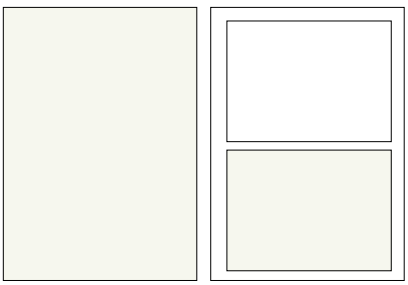
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	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)

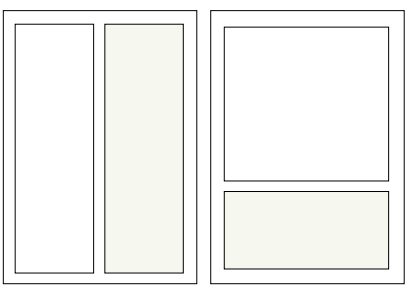
1/2 strony (170 x 125 mm)

Artykuł sponsorowany:

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1500 zł (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)

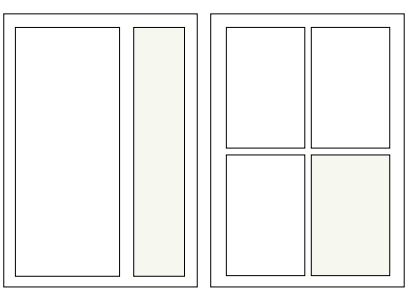
1/3 strony (170 x 80 mm)

Spis teleadresowy:

jednorazowy wpis 70 zł

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

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

Spis reklam

SAMSUNG

Kompaktowe · Stylowe · HD · W przystępnej cenie

LiteNet

Odwiedź: litenet.samsungsecurity.co.uk

Kamery o rozdzielczości 1,3 i 3 megapikseli zapewniają bardzo dobry obraz w przystępnej cenie. Zastosowane technologie: Transmisja wielostrumieniowa, funkcje Smart Codec i Progressive Scan — wszystkie przyczyniają się do rejestrowania wyraźniejszych, ostrych obrazów.

Kamery sieciowe LiteNet firmy Samsung są przeznaczone do instalacji w systemach o dowolnej wielkości.

Niedrogie rozwiązania megapikselowe już dostępne w sieci blisko Ciebie!

E STEsecurity@samsung.com
W samsungsecurity.co.uk

Samsung Techwin Europe Ltd

Axis Communications' Academy

Budowanie kompetencji w dziedzinie sieciowych systemów wizyjnych

Liczba klientów i sukces Twojej firmy zależą od tego, czy dysponujesz najbardziej aktualną i wszechstronną wiedzą w branży. Dzięki szkoleniom w ramach Axis Communications' Academy łatwiej być o krok do przodu przed konkurencją – wiedza z dziedziny sieciowych systemów wizyjnych jest w zasięgu ręki.

Akademia oferuje bogactwo informacji, które umożliwiają budowanie kompetencji w każdej części łańcucha produktów – od interaktywnych narzędzi do projektowania systemów, praktycznych instrukcji „krok po kroku" i specjalistycznych seminariów internetowych po szkolenia stacjonarne i programy certyfikacyjne. Tę wiedzę przekazują przeszkoleni specjaliści Axis. Jest ona dostępna w każdej chwili, w każdym miejscu i w ojczystym języku.

Gdy źródłem Twojej wiedzy jest firma, która opracowała pierwsze sieciowe systemy wizyjne i nadal ustanawia branżowe standardy w zakresie innowacji, świadomi klienci doceniają Twoje doświadczenie co przynosi w konsekwencji wymierne korzyści.

Przyjmij punkt widzenia Axis.
Bądź zawsze o krok do przodu.
Odwiedź www.axis.com/academy

Axis Communications' Academy - globalne centrum wiedzy z dziedziny sieciowych systemów wizyjnych

AXIS COMMUNICATIONS