CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(87)/2012

ZABEZPIECZENIA

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

W NUMERZE:

SAMSUNG

Wybierz SMART.
Wybierz inteligentne rozwiązania z zakresu zabezpieczeń!

Linia SAMSUNG iPOLiS oferuje inteligentne rozwiązania IP, idealnie dostosowane do Twoich potrzed. Doskonałej jakości urządzenia oferowane są z pełnym wsparciem przed- i posprzedażowym, w tym również w zakresie projektowania systemu i bezpłatnego wsparcia technicznego. Całość uzupełnia trzyletnia gwarancja na wszystkie produkty.

Samsung Techwin Europe Ltd

E STEsecurity@samsung.com
W samsungsecurity.com

Spis treści

CZASOPISMO ZABEZPIECZENIA 5/2012

Spaleni słońcem **18**

Nowe spojrzenie na ochronę informacji niejawnych (cz. 3) **52**

Możesz liczyć na Q24 **70**

Wizerunek w sieci – wykorzystywanie cudzego wizerunku w celach komercyjnych oraz popełnianie cyberprzestępstw **78**

Centrala CPR32-NET z interfejsem sieciowym IP

Firma **ROGER** wprowadziła do swojej oferty nowy model centrali – **CPR32-NET**, który stanowi kolejną wersję produkowanej do tej pory centrali CPR32SE. W odróżnieniu od poprzedniej wersji nowa centrala oferuje:

– wbudowany ethernetowy interfejs komunikacyjny,
– możliwość integracji z centralą alarmową serii Integra firmy SATEL,
– możliwość współdziałania z zamkami mechatronicznymi serii Sallis firmy SALTO,
– możliwość buforowania zdarzeń w zewnętrznej pamięci microSD,
– zwiększoną liczbę linii wejściowych i wyjściowych.

Komputer zarządzający łączy się z centralą CPR32-NET przez sieć LAN/WAN. Rozwiązanie to z jednej strony umożliwia znaczne przyśpieszenie transmisji danych, a z drugiej eliminuje konieczność stosowania dedykowanego interfejsu komunikacyjnego pomiędzy centralą a komputerem zarządzającym. Dotychczas urządzenia firmy ROGER zapewniały integrację z systemami alarmowymi dzięki wykorzystaniu odpowiednich linii wejściowych i wyjściowych. Obecnie, dzięki centrali CPR32-NET, możliwa jest integracja z centralami serii INTEGRA firmy SATEL na drodze programowej, z użyciem interfejsu INT-RS. Ogólna koncepcja polega na tym, że strefy alarmowe INTEGRY można załączać w dozór za pomocą czytników kontroli dostępu systemu RACS. Zachowano jednak możliwość niezależnego załączania w dozór za pomocą oryginalnych klawiatur strefowych systemu alarmowego. Zaistniałe w systemie alarmowym zdarzenia są wizualizowane w oknie monitorowania systemu kontroli dostępu, dlatego obsługa nie musi monitorować dwóch systemów jednocześnie.

Bezpośr. inf. ROGER

128-kanałowe serwery rejestrujące

Firma **POLVISION** rozpoczęła produkcję nowych modeli rejestratorów IP. W kieszeniach *hot-swap* można zainstalować jedenaście dysków pracujących w trybie RAID5. Do rejestratorów można też podłączyć macierze dyskowe, w tym produkowaną przez firmę POLVISION macierz PV-RAID rozszerzającą pojemność rejestratora do ponad 80 TB.

Starsze modele rejestratorów sieciowych firmy POLVISION mają bardzo duże możliwości związane z nagrywaniem, wyświetlaniem, analizą materiału wizyjnego, sterowaniem i alarmowaniem, jednak każdy z nich może obsługiwać jedynie trzydzieści dwie kamery. Rejestratory sieciowe z serii **PV-RPNVR** mogą rejestrować i wyświetlać obrazy o rozdzielczości Full HD z trzydziestu dwóch kamer, z sumaryczną prędkością 960 kl./s.

W tym roku rozpoczęto produkcję systemów uzupełniających – zaawansowanych serwerów rejestrujących PV-RPRS, które oferują mniej funkcji, ale umożliwiają podłączenie do jednego urządzenia aż 128 kamer IP o rozdzielczości dochodzącej do 5 Mpx. Serwer rejestrujący ma także możliwość zwiększania liczby sieciowych strumieni wizyjnych do aż 300 połączeń (funkcja tzw. bramki wizyjnej).

Serwer rejestrujący PV-RPRS został przetestowany pod koniec 2011 roku w bardzo dużym systemie rejestrującym materiał wizyjny. Rejestrowano na nim 128 strumieni wizyjnych z kamer GV-FE421 (4.0 Mpx, 15 fps, H.264) o łącznej przepływności dochodzącej do 800 Mbit/s.

Nowe rejestratory i serwery rejestrujące z serii PV-RP są stworzone z myślą o najbardziej wyrafinowanych zastosowaniach, takich jak monitoring miast, stadionów, kasyn, imprez masowych itp.

Bezpośr. inf. POLVISION

Command Centre In-A-Box firmy Aventura Technologies

Amerykańska firma **Aventura Technologies** wprowadziła na rynek system typu „wszystko w jednym", który umożliwia ocenę sytuacji panującej w obiekcie, potrzebuje tylko jednego serwera, nie wymaga skomplikowanej konfiguracji i jest gotowy do użytku zaraz po uruchomieniu. System działa w oparciu o unikalne oprogramowanie zainstalowane na jednym serwerze i pozwala na wyświetlanie informacji z wykorzystaniem technologii Video Wall (*Zabezpieczenia 4/2012*).

System sprzętowo dekoduje sygnały z kamer analogowych, pobiera strumienie wizyjne z kamer IP, a następnie wysyła dane umożliwiające sterowanie ścianami wizyjnymi bez konieczności korzystania z dodatkowego oprogramowania.

Command Centre In-A-Box może pobierać sygnały wejściowe z kamer wiodących producentów poprzez interfejsy HDMI, DVI, RGB, VGA, SDI, S-video, Ethernet i wyświetla obrazy na maksymalnie czterdziestu monitorach obsługiwanych przez jeden serwer.

Producent Command Centre In-A-Box od ponad dziesięciu lat tworzy rozwiązania służące do ochrony obiektów cywilnych, rządowych i wojskowych na całym świecie.

Aventura Technologies jest zwolennikiem otwartych standardów umożliwiających tworzenie własnych aplikacji z wykorzystaniem programowego zestawu uruchomieniowego

pozwalającego klientom zmaksymalizować korzyści płynące z istniejącej infrastruktury.

Więcej informacji na temat systemu Command Centre In-A-Box można uzyskać u wyłącznego polskiego dystrybutora, którym jest firma **ZBAR** z Łodzi (*www.zbar.com.pl*).

Bezpośr. inf. Krystian Witczak, Karolina Zasada
ZBAR

Samsung wprowadza kopułkową kamerę sieciową PTZ Full HD z zoomem optycznym 20×

Lotniska i porty, parkingi, szkoły, centra handlowe, stacje benzynowe oraz stadiony to tylko przykłady miejsc, których administratorzy docenią dwudziestokrotny zoom optyczny zastosowany w modelu **SNP-6200** – nowej sieciowej kamerze PTZ o rozdzielczości Full HD.

Kamera SNP-6200 jest w stanie generować dwumegapikselowe obrazy, które mogą być wyświetlane w formacie 16:9 przy rozdzielczości Full HD 1080p, oraz wykorzystuje technologię skanowania progresywnego, dzięki czemu obrazy ruchomych obiektów i pojazdów zachowują ostrość.

– *SNP-6200 wytwarza kilka strumieni wizyjnych różniących się rozdzielczością i metodą kompresji, a więc ten model może zostać równocześnie użyty do monitoringu w czasie rzeczywistym, monitoringu mobilnego, rejestracji obrazów o wysokiej jakości, nagrywania materiału wizyjnego na kartach SD oraz powiadamiania przez pocztę e-mail* – powiedział **Tim Biddulph**, IP Product Manager z Samsung Techwin Europe**.**

Model SNP-6200 jest zgodny ze standardami ONVIF ma bezlicencyjny system Inteligentej Analizy Obrazu (IVA), obejmującej m.in. funkcję bariery wirtualnej, detekcji wejścia/wyjścia, czy detekcji pojawienia się/zniknięcia obiektu.

Ponadto, technologia Smart Codec firmy **Samsung** oferuje możliwość skanowania wybranych fragmentów kadru z podwyższoną rozdzielczością. Oznacza to, że na przykład obrazy przejść lub okien mogą być rejestrowane w pełnej rozdzielczości, natomiast pozostałe obszary kadru w rozdzielczości zredukowanej, co umożliwia zmniejszenie rozmiaru plików i pozwala użytkownikowi na pełną kontrolę nad przepływnością w sieci.

Kamery SNP-6200 mają wielojęzyczne menu, funkcję WDR, są zasilane metodą PoE i mają wbudowane gniazdo kart pamięci SD służących do lokalnej rejestracji obrazów. Są także w pełni kompatybilne z bezlicencyjnym oprogramowaniem NET-i Viewer firmy Samsung, które umożliwia zdalne przeglądanie obrazów, a także kontrolę oraz zarządzanie jednym bądź wieloma systemami bezpieczeństwa poprzez sieć, w dowolnym miejscu na świecie.

Wersja **SNP-6200H** ma te same funkcje co SNP-6200, jednakże została przystosowana do pracy w niekorzystnych warunkach atmosferycznych – gdy temperatura otoczenia oscyluje pomiędzy -50°C i +50°C. Model ten ma klasę szczelności IP66 i jest wyposażony w aluminiową obudowę z osłoną przeciwsłoneczną, wentylatorem oraz grzałką z termostatem.

Bezpośr. inf. David Solomons
DRS Marketing

SCP-2370RH

nowa kamera kopułkowa firmy Samsug

Dzięki wbudowanym oświetlaczom podczerwieni IR-LED nowa, odporna na trudne warunki atmosferyczne kamera kopułkowa **PTZ SCP-2370RH** z optycznym zoomem 37x jest w stanie generować obrazy o wysokiej jakości zarówno przy dobrym oświetleniu, jak i w całkowitej ciemności. Doskonale sprawdzi się w całodobowym nadzorze parkingów, parków przemysłowych, stacji benzynowych, szkół, szpitali i centrów handlowych.

Kamera SCP-2370RH o klasie szczelności IP66 jest wyposażona w grzałkę z termostatem i doskonale sprawdzi się na lotniskach i w portach.

W warunkach nocnych lub przy niedostatecznym oświetleniu wbudowane oświetlacze pracujące w podczerwieni są aktywowane automatycznie i zapewniają oświetlenie w promieniu 100 m. Co ważne, intensywność tego oświetlenia jest automatycznie dostosowywana do warunków obserwacji i jest zmieniana w zależności od kąta widzenia kamery.

Kamera Samsung SCP-2370RH z serii W-5 jest wyposażona w procesor DSP i może pracować w trybie dzień/noc z wykorzystaniem zintegrowanego filtra podczerwieni. Technologia SSNRIII *Samsung Super Noise Reduction* eliminuje szumy widoczne na obrazie w warunkach niedoświetlenia. Dzięki temu wyeliminowano efekt „ducha" i rozmycia, a także można zaoszczędzić miejsce na dysku podczas rejestracji niedoświetlonych obrazów (nawet 70% przestrzeni dyskowej).

Kamera ma osiem stref prywatności, wykrywa ruch i ma funkcję kompensacji prześwietleń HLC (*Highlight Compensation*), która identyfikuje zbyt silnie naświetlone strefy obrazu, i neutralizuje efekt prześwietlenia, co umożliwia operatorowi dostrzeżenie uprzednio ukrytych szczegółów. Kamera SCP-2370RH jest także wyposażona w funkcję cyfrowej stabilizacji obrazu DIS, która zapobiega negatywnym efektom wstrząsów spowodowanych silnym wiatrem bądź wibracjami konstrukcji mocującej.

Kompatybilność z systemem sterowania telemetrycznego za pośrednictwem kabla koncentrycznego umożliwia kamerze SCP-2370RH wykorzystanie wielojęzycznego menu ekranowego rejestratorów DVR, dostępnego z poziomu centrum kontrolnego. Pozwala to na transmisję obrazu oraz sygnałów telemetrycznych poprzez ten sam kabel koncentryczny, dając tym samym pełny dostęp do ustawień kamery oraz do obsługi funkcji *pan-tilt-zoom* poprzez kompatybilny cyfrowy rejestrator obrazu. Kamerę wyposażono także w tradycyjne sterowanie telemetryczne.

Bezpośr. inf. David Solomons
DRS Marketing

32-kanałowe rejestratory hybrydowe zapewniające wysoką jakość obrazu

Firma **Polvision** rozpoczęła produkcję dwóch nowych modeli rejestratorów hybrydowych, które umożliwiają nagrywanie obrazu i dźwięku z 32 kanałów wizyjnych, zarówno z kamer analogowych jak i sieciowych. Obraz z kamer analogowych jest rejestrowany z sumaryczną prędkością 800 klatek na sekundę i jego jakość jest porównywalna z jakością filmów odtwarzanych z płyt DVD. Materiał wizyjny jest kompresowany sprzętowo, metodą H.264.

Nowe rejestratory, oznaczone symbolami **PV-RADVR32800H** i **PV-RPDVR32800H**, mają duże możliwości funkcjonalne i są stworzone z myślą o najbardziej wyrafinowanych zastosowaniach, takich jak monitoring miast, stadionów, kasyn, imprez masowych itp.

Bezpośr. inf. POLVISION

Hemisferyczne kamery kopułkowe o rozdzielczości 5 Mpx

Firma **POLVISION** wprowadziła do sprzedaży nowe kamery hemisferyczne ze specjalnymi obiektywami typu rybie oko i dużymi przetwornikami CMOS ze skanowaniem progresywnym. Połączenie tych technologii umożliwia rejestrowanie obrazu o wysokiej rozdzielczości (która w przypadku modeli **FE521** i **FER521** dochodzi do 5.0 Mpx – 2048×1944), na którym widoczny jest obszar wokół kamery. Zaawansowane oprogramowanie w wersji polskiej, dostarczane bezpłatnie wraz z kamerą, automatycznie przetwarza obraz dookolny na standardowy. Użytkownik może płynnie obracać i zbliżać widok z kamery tak, jakby była to mechaniczna kamera obrotowa PTZ.

Nowa kamera hemisferyczna FER521 to długo oczekiwany odpowiednik modelu FE521, umieszczony w hermetycznej obudowie o stopniu szczelności IP66 i wandaloodporności IK6. Podobnie jak w przypadku pozostałych kamer dookolnych, dołączone oprogramowanie realizuje funkcje prostowania obrazu (*demorphing*) i śledzenia ruchomych obiektów.

Oba modele kamer mają wbudowany mikrofon i głośnik do dwukierunkowej komunikacji głosowej, wejście i wyjście alarmowe oraz gniazdo na karty pamięci SDHC służące do lokalnego zapisu obrazów.

Istotną przewagą w stosunku do podobnych rozwiązań istniejących na rynku jest to, że każdy z operatorów może korzystać z kamery hemisferycznej niezależnie. Oznacza to, że każdy z nich może uzyskiwać podgląd w dowolnie wybranym układzie ekranu (np. 3600, 2×1800, 4×900 oraz korzystać z funkcji automatycznej panoramy, zoomu, cyfrowego śledzenia obiektu itd.

Bezpośr. inf. POLVISION

Wandaloodporne, szybkoobrotowe kamery o rozdzielczości Full HD, z funkcją WDR

Firma **POLVISION** wprowadziła do sprzedaży nowoczesne kamery szybkoobrotowe z serii **SD200** o rozdzielczości Full HD, odznaczające się szerokim zakresem dynamiki obrazu (WDR – ang. *Wide Dynamic Range*).

Funkcja WDR eliminuje zbyt intensywne tylne oświetlenie obiektu będącego na pierwszym planie. Dzięki temu kamera wykorzystująca funkcję WDR wytwarza jasny obraz takiego obiektu, w przeciwieństwie do kamery bez funkcji WDR, w przypadku której obraz ten będzie ciemny i niewyraźny.

Kamera z serii SD200 oferuje wysokiej jakości obraz skompresowany metodą H.264, o rozdzielczości 2.0 MPx (1920×1080, 30 kl./s). Ma wbudowane cztery wejścia i dwa wyjścia alarmowe, wejście i wyjście foniczne służące do dwukierunkowej komunikacji dźwiękowej oraz gniazdo na karty pamięci SDHC, służące do lokalnego zapisu obrazów. Wersja przeznaczona do zastosowań zewnętrznych jest wyposażona w wandaloodporną obudowę o stopniu szczelności IP66, zasilaną napięciem 24 V_{AC} (pobór mocy: maks. 65 W z włączoną grzałką).

Obiektywy zastosowane w kamerach SD200 umożliwiają osiemnastokrotne lub dwudziestokrotne optyczne powiększenie obrazu, co w połączeniu z wysoką rozdzielczością Full HD pozwala na uzyskanie szerokiego pola widzenia przy zachowaniu poziomu szczegółowości porównywalnego ze szczegółowością, jaką zapewniała starsza kamera SD010 (rozdzielczość D1, obiektyw umożliwiający trzydziestosześciokrotne optyczne powiększanie obrazu). Pozytywnym zaskoczeniem dla testerów nowych kamer okazały się rezultaty prób przeprowadzonych w warunkach nocnych. Przy tej samej szybkości migawki kamera z serii SD200 wyposażona w przetwornik CMOS o rozdzielczości Full HD uzyskiwała jaśniejszy obraz niż starsza kamera SD010 wyposażona w przetwornik CCD o rozdzielczości D1.

Na uwagę zasługuje również bardzo szeroki zakres temperatur pracy (od -40 do +50 stopni Celsjusza) oraz duży wybór uchwytów i adapterów służących do montażu kamer w dowolnej lokalizacji.

W komplecie z kamerami dostarczane jest bardzo zaawansowane technologicznie oprogramowanie NVR dla serwerów i stacji monitorowania, które umożliwia śledzenie obiektów ruchomych.

Bezpośr. inf. POLVISION

Nowe czujki OPTEX są bardziej odporne na starzenie się

Podstawowym założeniem konstrukcyjnym w przypadku detektorów ruchu jest ich niezawodne i bezobsługowe działanie przez długi czas. Doskonale widać to w produktach japońskiej firmy **OPTEX**. Czujki, szczególnie w systemach zewnętrznych, narażone są na silne oddziaływanie czynników środowiskowych wpływające na ich trwałość, niezawodność oraz wygląd zewnętrzny, co może niepokoić użytkowników i konserwatorów systemów alarmowych.

W ostatnich trzech latach na rynek trafiła nowa generacja detektorów ruchu OPTEX charakteryzujących się zwiększoną odpornością na degradujący wpływ czynników środowiskowych.

Dualne, zewnętrzne czujki ruchu **HX-40DAM** są wyposażone w nowoczesny moduł mikrofalowy, zbudowany z wykorzystaniem ceramicznej płyty głównej, którego antenę pokryto warstwą złota. Takie rozwiązania sprawiają, że skuteczność działania części mikrofalowej w długim okresie czasu jest nieporównywalnie wyższa niż w przypadku klasycznych rozwiązań, pomimo oddziaływania wilgoci, utleniaczy oraz wysokiej i niskiej temperatury na elementy elektroniczne. Ten nowoczesny moduł mikrofalowy zastosowano również w nowych wewnętrznych czujkach serii CDX i RXC-DT (IV kwartał 2012 r.) oraz w nowej czujce VX INFINITY – następcy modelu VX-402 (I kwartał 2013 r.).

Kolejna istotna innowacja konstrukcyjna zastosowana przez OPTEX to wykorzystanie tworzyw sztucznych o podwyższonej odporności na oddziaływanie promieniowania UV. Obudowy wewnętrznych czujek serii CDX i RXC wykonano z wysokoudarowego polistyrenu, który odbarwia się znacznie wolniej od powszechnie stosowanego ABS czy PCW.

W czujkach zewnętrznych serii HX, FTN oraz w nowej czujce VXI zastosowano nowoczesne tworzywa sztuczne wykorzystywane również w produkcji pokryć dachowych i motoryzacji. Obudowy tych czujek są wykonane z kopolimeru ASA (kopolimer akrylonitrylu, styrenu i akrylanów), który ma pięciokrotnie większą odporność na odbarwianie niż ABS, co potwierdzają testy starzeniowe wykonywane w warunkach zarówno laboratoryjnych, jak i naturalnych.

Informacje o parametrach czujek wewnętrznych i zewnętrznych oraz barier podczerwieni OPTEX są dostępne na stronie *www.optex.com.pl*.

Bezpośr. inf. OPTEX Security

Bezkompromisowa ostrość obrazu

Bosch oferuje nowe sieciowe kamery dualne **FlexiDome HD 1080p**. Kamery te zapewniają doskonałą jakość obrazu i dużą dokładność odwzorowania barw w trudnych warunkach oświetleniowych.

Elementy układu optycznego FlexiDome HD 1080p odpowiedzialne za powstawanie obrazu, od obiektywu aż po system cyfrowego przetwarzania obrazu, są przystosowane do rozdzielczości HD i gwarantują dużą ostrość obrazu całej obserwowanej sceny, nawet gdy jest bardzo kontrastowa. Dedykowany układ analizy treści obrazu umożliwia wykrywanie określonych zdarzeń. Wysoka rozdzielczość kamery pozwala na identyfikację najdrobniejszych szczegółów obserwowanej sceny.

Kamery **FlexiDome HD 1080p** umożliwiają odróżnienie bardzo podobnych odcieni barw nawet w niekorzystnych warunkach oświetleniowych.

Dzięki nowym kamerom łatwiej wykrywać zagrożenia. Zintegrowana i zoptymalizowana pod kątem HD technologia inteligentnej analizy obrazu IVA (ang. *Intelligent Video Analysis*) pozwala wykryć i wskazać na ekranie każdą sytuację alarmową. Dzięki temu operatorzy nie przeoczą już podejrzanych zachowań. IVA umożliwia wychwycenie wszystkich detali zdarzeń, które można później odszukać za pomocą funkcji Bosch *Forensic Search*.

Sieciowe kamery dualne FlexiDome HD 1080p dostępne są w nowym, praktycznym wzornictwie. Płaskie okno umieszczone przed obiektywem eliminuje tzw. efekt bańki powstający w konwencjonalnych kamerach kopułkowych HD. Operator może

wykonać zbliżenie dowolnego fragmentu sceny bez ryzyka utraty ostrości obrazu. Ułatwia to identyfikację twarzy, obiektów i znaków alfanumerycznych nawet przy znacznych odległościach.

Kamery FlexiDome HD pracują prawidłowo w szerokim zakresie temperatur (od -50°C do +55°C). Dużą odporność na niekorzystne warunki atmosferyczne zapewnia obudowa o klasie szczelności IP66.

Kamery mają czytelny interfejs graficzny ułatwiający ich obsługę. Są łatwe do zainstalowania i uruchomienia, a dzięki funkcji automatycznej regulacji ostrości można uzyskać ostry obraz w bardzo krótkim czasie. Technologia Power over Ethernet (PoE) sprawia, że kamera nie potrzebuje dodatkowego źródła zasilania. Moc niezbędna do zasilania kamer FlexiDome HD 1080p wynosi zaledwie 3,5 W.

Nowe kamery są przeznaczone do nadzoru takich obiektów jak stadiony, lotniska, banki, instytucje finansowe i kasyna. Mogą być także wykorzystane w systemach monitoringu centrów miast oraz do rejestracji przebiegu imprez masowych.

Bezpośr. inf. Robert Bosch

Kamery stworzone do pracy w najcięższych warunkach

Produkty Bosch Security Systems sprawdzają się w przemyśle górniczym

Strefy zagrożone wybuchem, działanie substancji żrących i gazów palnych, skrajne temperatury, zmienne warunki oświetleniowe, duże odległości – to wyzwania dla systemów ochrony w kopalni. Rozwiązania Bosch Extreme pozwalają skutecznie chronić mienie i życie ludzkie w ekstremalnych warunkach.

Specjalna iskrobezpieczna i przeciwpłomieniowa konstrukcja kamer obrotowych serii **MIC** i stacjonarnych serii **EX** umożliwia stosowanie ich w tych miejscach w kopalni, gdzie nagromadzenie łatwopalnych gazów może powodować samozapłon, a następnie wybuch. Obudowa kamery jest tak skonstruowana, aby iskry elektryczne powstające w jej wnętrzu nie miały kontaktu ze środowiskiem zewnętrznym. Technologia bezszczotkowa w kamerach obrotowych dodatkowo minimalizuje ryzyko powstania iskrzenia mogącego być przyczyną wybuchu.

Kopalnia odkrywkowa to rozległy, nieoświetlony obszar, którego ochrona wymaga zastosowania kamer będących w stanie zidentyfikować zagrożenia z dużych odległości. Tylko kamery z obiektywami umożliwiającymi zmianę ogniskowej w bardzo szerokim zakresie mogą patrolować jej teren. Taką kamerą jest **Bosch GVS1000**. Jej zasięg obserwacji dochodzi nawet do pięciu kilometrów. Zastosowanie w tej kamerze oświetlaczy pracujących w podczerwieni pozwala prowadzić dozór kamerowy nawet w całkowitych ciemnościach.

– *W ochronie obwodowej rozległych obszarów, takich jak kopalnie odkrywkowe, często stosuje się kamery z dodatkowym detektorem termowizyjnym. Kamera Bosch MIC widzi przez mgłę, dym, deszcz, śnieg oraz listowie, dzięki czemu jest niewrażliwa na niekorzystne warunki pogodowe czy środowiskowe* – podkreśla **Marek Pyc**, specjalista z Bosch Security Systems.

Kamery Bosch mogą być również wykorzystane jako „dodatkowa para oczu" dla operatora koparki. Osoba obsługująca koparko-ładowarkę często nie widzi, co dzieje się bezpośrednio pod maszyną lub na jej drugim końcu. Mając do dyspozycji kamerę obrotową, operator może spojrzeć okiem kamery w dowolne interesujące go miejsce bez opuszczania kabiny. Kamery obrotowe serii MIC oraz AutoDome doskonale sprawdzają się podczas pracy na maszynach w kopalniach „Turów" i „Bełchatów".

Monitoring wizyjny z wykorzystaniem sprzętu firmy Bosch można również spotkać w kopalni „Bogdanka", gdzie kamery wraz z systemem rejestracji są wykorzystywane na całym obszarze nad ziemią.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Gunnebo przejmuje firmę Hamilton Safe w USA

Mamy zaszczyt poinformować, że w dniu 8 sierpnia 2012 r. **Gunnebo** przejęło **Hamilton Safe** w USA – drugą co do wielkości firmę branży security w tym kraju, dostarczającą zabezpieczeń mechanicznych dla banków i instytucji rządowych.

Zatrudniająca 300 osób firma Hamilton Safe została utworzona w 1967 r., a jej roczna sprzedaż w 2011 r. sięgnęła 70 MUSD. Produkty marki Hamilton Safe są sprzedawane w USA oraz Kanadzie, a odbiorcami są przede wszystkim amerykańskie banki oraz organy administracji publicznej.

Flagowe produkty Hamilton Safe to sejfy, skrytki depozytowe, skarbce i drzwi skarbcowe, systemy kontroli dostępu oraz systemy poczty pneumatycznej. Wszystkie pochodzą z pięciu zakładów produkcyjnych Hamiltona. Sprzedaż odbywa się głównie poprzez rozbudowaną sieć dilerską.

Przejmując firmę Hamilton Safe, Gunnebo podkreśla, że tradycyjne zabezpieczenia mechaniczne są nadal w centrum jej zainteresowania i że jest prawdziwym globalnym liderem w tej branży.

Bezpośr. inf. Jolanta Derbich
Gunnebo Polska

Wandaloodporne, kopułkowe kamery megapikselowe

Firma **POLVISION** wprowadziła do sprzedaży kamery kopułkowe przeznaczone do zastosowań zewnętrznych i mobilnych. Jest to seria kamer **MDR**, która stanowi odpowiednik bardzo popularnych kamer MFD z tą różnicą, że nowe kamery są wyposażone w hermetyczną obudowę o stopniu szczelności IP66 i wandaloodporności IK7. Charakteryzują się one również zwiększoną odpornością na wstrząsy, wilgoć oraz niskie i wysokie temperatury. Posiadają certyfikat zgodności z normą EN50155 standaryzującą sprzęt do zastosowań kolejowych i transportowych.

Kamery oferują wysokiej jakości obraz skompresowany metodą H.264, o rozdzielczości od 1.3 MPx (30 kl./s) do 5 MPx (10 kl./s). Mają wbudowany mikrofon oraz gniazdo na karty pamięci SDHC służące do lokalnego zapisu obrazów. Są montowane w sposób umożliwiający zmianę ich ustawienia w trzech osiach i zasilane metodą PoE (pobór mocy wynosi 3,7 W). Wymiary kamer to Ø 115×59,2 mm, a ich masa wynosi 568 g.

W komplecie z kamerami dostarczane jest bardzo zaawansowane technologicznie oprogramowanie NVR dla serwerów i stacji monitorowania.

Bezpośr. inf. POLVISION

Ochrona i pomiar temperatury w jednym

Kamera termowizyjna FLIR A310 f monitoruje temperaturę instalacji i równocześnie chroni cały obszar

A310 f to stacjonarna kamera termowizyjna marki **FLIR** z najnowszej serii A. Działanie kamery polegające na monitorowaniu temperatury oraz ochronie całego obiektu umożliwia wykrywanie różnego rodzaju zagrożeń i ocenę poziomu ryzyka. Oprócz tego poprawia nadzór, zapobiega przestojom w pracy oraz znacznie poprawia bezpieczeństwo pracowników. Kamera może być jednocześnie wykorzystywana tak jak klasyczna kamera do ochrony obiektów.

Choć w większości przypadków, gdy kamera termowizyjna jest wykorzystywana do ochrony i nadzoru obiektów, nie ma konieczności dokładnego pomiaru temperatury, istnieją instalacje, w przypadku których taki pomiar może przynieść wymierne korzyści.

Typowym przykładem zastosowania kamery z serii A jest zainstalowanie jej w stacji transformatorowej. Kamera termowizyjna pozwala przez cały czas mierzyć temperaturę transformatorów oraz innych urządzeń elektrycznych. W nocy może być dodatkowo wykorzystywana do ochrony perymetrycznej.

Innym przykładem zastosowania kamery A310 f może być zainstalowanie jej przy wysypiskach śmieci lub składach węgla, gdzie może nadzorować obszar, wykryć pożar i alarmować. Możliwych zastosowań jest wiele.

Bezpośr. inf. Linc Polska

Nowa seria produktów Mobotix – functional boxes

Firma **Mobotix** wprowadziła do swojej oferty **functional boxes**. Te niewielkie, wodoszczelne urządzenia zwiększają funkcjonalność systemu wizyjnego. Choć wszystkie wyglądają tak samo, każde z nich kryje w sobie zupełnie inne funkcje.

Jednym z tych urządzeń jest **MX-GPS-BOX**. Zwiększa ono funkcjonalność kamer Mobotix i pozwala znajdować nowe zastosowania. Dzięki GPS-owi kamery Mobotix mogą być wykorzystywane m.in. w monitorowaniu floty pojazdów.

Ponadto MX-GPS-BOX umożliwia aktualizację i synchronizację czasu. Jest to szczególnie pomocne w przypadku monitoringu bez dostępu do Internetu.

MX-GPS-BOX posiada dodatkowe sensory – czujnik oświetlenia i czujnik temperatury, które mogą inicjować różnego rodzaju akcje podejmowane przez kamerę.

Firma Mobotix udostępnia programistom pakiet API, który umożliwia integrację urządzeń z oprogramowaniem innych firm. Oprogramowanie może dostarczać informacje o prędkości, kierunku ruchu, a także aktualnym położeniu urządzeń MX-GPS-BOX. Ponadto wszystkie dane mogą być rejestrowane synchronicznie z odpowiednimi sekwencjami wizyjnymi.

Bezpośr. inf. Linc Polska

Inteligentne śledzenie z kamerą AutoDome serii 700

Obecnie kamery sieciowe są jeszcze bardziej „inteligentne" niż dawniej. **Bosch Security Systems** zwiększył funkcjonalność PTZ **AutoDome serii 700** i wprowadził funkcję *Intelligent Tracking* (inteligentne śledzenie obiektów).

Funkcja *Intelligent Tracking* wykorzystuje oprogramowanie do inteligentnej analizy obrazu IVA (ang. *Intelligent Video Analysis*), którym dysponują kamery AutoDome. W sposób ciągły monitoruje i automatycznie śledzi obiekty poruszające się w polu widzenia kamery.

Kamery AutoDome wyposażone w funkcję *Intelligent Tracking* są niezwykle przydatne w systemach dozoru wizyjnego. Oprogramowanie IVA pozwala na dokładne sprecyzowanie warunków, w których funkcja śledzenia ma zostać uaktywniona. Można na przykład zaprogramować kamerę w taki sposób, że będzie śledziła wszystkie pojazdy poruszające się po określonym obszarze i w konkretnym kierunku. Znacznie ułatwia to pracę służbom ochrony. Ponadto operatorzy systemu mogą w każdej chwili uruchomić funkcję śledzenia obiektu, który wyda im się podejrzany. Aby kamera skupiła się na śledzeniu celu widocznego na ekranie, wystarczy go wskazać kliknięciem.

Podczas śledzenia celu kamera wykorzystuje niezbędne funkcje: obrotu, pochylenia i zmiany ogniskowej obiektywu. Kamery sieciowe AutoDome serii 700 z funkcją *Intelligent Tracking* korzystają z zaawansowanego algorytmu, który sprawia, że znacznie przewyższają funkcjonalnością inne kamery obrotowe. Na przykład jako jedyne mogą automatycznie wznowić śledzenie obiektu, nawet gdy ten czasowo znajdzie się poza granicą maskowanej strefy prywatności lub ukryje się za innym obiektem. Kamera AutoDome powraca do śledzenia celu, kiedy tylko ten pojawi się ponownie w jej polu widzenia lub gdy wykryje ruch wzdłuż tej samej trajektorii.

Kamery sieciowe AutoDome serii 700 mogą obracać się w sposób nieograniczony (pełny kąt obrotu). Dysponują zoomem optycznym 28x lub 36x oraz funkcją progresywnego skanowania obrazów cyfrowych, która gwarantuje doskonałą ostrość, nawet w przypadku poruszających się obiektów. Mają wytrzymałe aluminiowe obudowy o klasie szczelności IP 66, które zapewniają sprawne działanie kamer w środowiskach wilgotnych i charakteryzujących się wysokim stopniem emisji pyłu.

Nowa funkcja *Intelligent Tracking* jest dostępna w oprogramowaniu w wersji 5.51.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Kamera Mobotix S14

Technologia hemisferyczna zastosowana w kamerze Q24 zyskała uznanie klientów. W odpowiedzi na duże zainteresowanie takimi kamerami firma **Mobotix** wprowadziła do swojej oferty dwie nowe kamery z serii **S14** – Mono oraz Dual.

Kamera Mono posiada jeden obiektyw hemisferyczny, który znajduje się bezpośrednio przy kamerze. Obudowa kamery umożliwia jej dyskretny montaż. Kamera Mono może być stosowana wszędzie tam, gdzie liczy się dyskrecja, szeroki kąt widzenia oraz łatwy montaż.

Kamera **S14 Dua**l jest podwójną kamerą hemisferyczną o sumarycznej rozdzielczości 6.2 megapiksela. Jest wyposażona w miniaturowe obiektywy. S14 może zostać wyposażona w dwa moduły hemisferyczne i mikrofon. Każda z kamer może być oddalona o dwa metry od głównego modułu. Dzięki temu tylko jednym zestawem kamer S14 można w pełni zabezpieczyć na przykład dwa pomieszczenia znajdujące się jedno za drugim. Kamera S14 jest bardzo mała, dzięki czemu łatwo ją ukryć i jest praktycznie niewidoczna po zamontowaniu. Jej kolejną istotną cechą jest odporność na warunki atmosferyczne – ma stopień szczelności IP65.

W kamerze S14 zastosowano dwa przetworniki obrazu o wielkości ½" i rozdzielczości 3.1 megapiksela. S14 można wyposażyć w kartę pamięci microSD o maksymalnej pojemności 64 GB, dzięki czemu zapis sekwencji wizyjnych odbywa się wewnątrz kamery.

Bezpośr. inf. Linc Polska

Samsung wprowadza na rynek tanią kamerę sieciową HD

Nowa 1.3-megapikselowa kamera sieciowa **Samsung SNB-5001** została zaprojektowana jako atrakcyjne cenowo urządzenie przeznaczone do zastosowania w systemach nadzoru wizyjnego o rozdzielczości HD.

– Każdego tygodnia na świecie instaluje się setki systemów nadzoru wizyjnego z kamerami HD generującymi obrazy o doskonałej rozdzielczości, pomagające użytkownikom podnieść poziom bezpieczeństwa – powiedział **Tim Biddulph**, IP Product Manager w Samsung Techwin Europe. – *Dotychczas relatywnie wysoka cena kamer HD ograniczała ich wykorzystanie w większości instalacji. Kamera SNB-5001 została wprowadzona na rynek w celu zmiany tego stanu rzeczy, dlatego ma większość funkcji kojarzonych z technologią HD, lecz oferujemy ją w atrakcyjnej cenie.*

Zgodna ze standardami ONVIF kamera SNB-5001 umożliwia kompresję obrazów metodami H.264 oraz MJPEG i równoczesną transmisję obrazów do wielu lokalizacji przy różnej poklatkowości i rozdzielczości, m.in. w formacie 1,3 Mpx 5:4 (1280×1024), HD 16:9 (1280×720), SVGA (800×600), VGA (640×480) oraz QVGA (320×240). Dzięki temu określona liczba autoryzowanych użytkowników jest w stanie monitorować obrazy na żywo w jednej lokalizacji, nagrywać materiał w innej, a także przeglądać obrazy w trybie na żywo lub odtwarzać nagrania za pomocą darmowej aplikacji iPolis zainstalowanej w urządzeniach mobilnych z systemem operacyjnym iOS lub Android.

Funkcja inteligentnej detekcji zmiany pola widzenia kamery SNB-5001 generuje alarm na przykład w przypadku nieautoryzowanej zmiany położenia kamery lub zabrudzenia obiektywu farbą.

Cztery programowalne strefy detekcji ruchu, dwanaście programowalnych stref prywatności oraz zasilanie PoE to tylko niektóre z dodatkowych funkcji modelu SNB-5001. Kamera pracuje w trybie dzień/noc i wytwarza obrazy kolorowe lub czarno-białe w zależności od zmiennych warunków oświetleniowych. Jest w pełni kompatybilna z bezlicencyjnym oprogramowaniem Samsung NET-i Viewer i można ją obsługiwać z wykorzystaniem wielojęzycznego (w tym polskojęzycznego) interfejsu sieciowego, który ułatwia wprowadzenie zmian w konfiguracji.

– Nowy model doskonale sprawdzi się tam, gdzie trzeba użyć wielu kamer HD. Dzięki atrakcyjnej cenie SNB-5001 może zastąpić istniejące kamery analogowe na przykład w recepcjach biur lub przy wejściach do sklepów, gdzie konieczne jest uchwycenie obrazów dobrej jakości – powiedział Tim Biddulph.

Bezpośr. inf. David Solomons
DRS Marketing

Ogólnopolskie Warsztaty Sygnalizacja i Automatyka Pożarowa SAP 2012

20 LAT WARSZTATÓW SAP

Historia

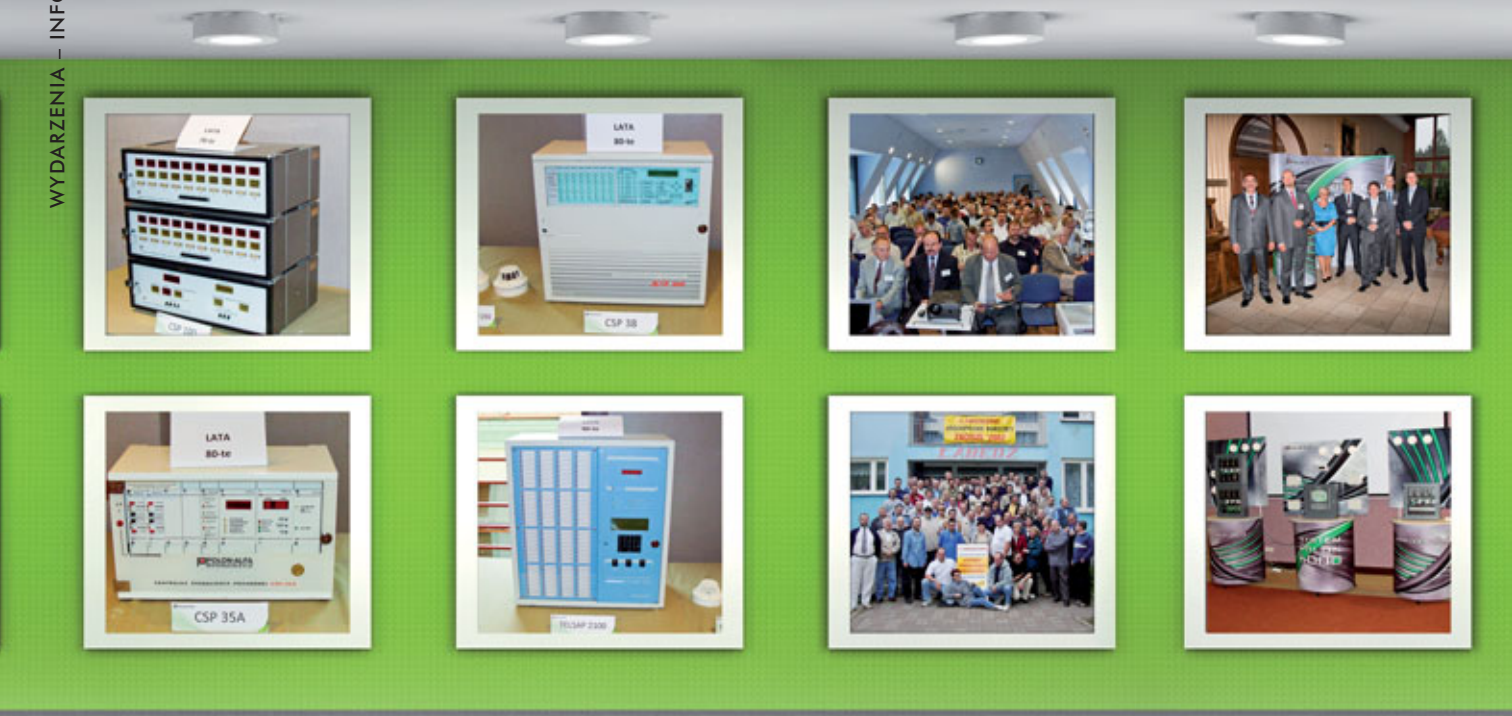
Był rok 1993, gdy po raz pierwszy, na zaproszenie POLON-ALFA, przedstawiciele firm tworzących instalacje sygnalizacji pożarowej i konserwujących je przyjechali na Ogólnopolskie Warsztaty „Systemy Sygnalizacji Pożarowej", które odbyły się w pięknej scenerii Borów Tucholskich w ośrodku Zacisze. Z biegiem lat w warsztatach zaczęło uczestniczyć coraz więcej projektantów instalacji, a także rzeczoznawców ds. ochrony przeciwpożarowej. Rosnąca z roku na rok ranga organizowanej przez POLON-ALFA imprezy sprawiła, że o możliwość uczestnictwa w niej zaczęło ubiegać się coraz więcej firm związanych z szeroko rozumianą branżą zabezpieczeń przed pożarem.

Na pierwszych spotkaniach z instalatorami poruszano głównie sprawy bieżącej współpracy między POLON-ALFA a firmami instalatorskimi i omawiano nowe wdrożenia urządzeń składających się na systemy sygnalizacji pożarowej, przedstawiając ich parametry i funkcjonalność.

Począwszy od 1996 roku każde spotkanie było poświęcone wybranemu tematowi wiodącemu. Tematyka wynikała z bieżących zainteresowań środowiska, potrzeby pogłębienia wiedzy w określonym zakresie i dotyczyła wykrywania pożarów, sygnalizacji, alarmowania oraz sterowania urządzeniami zabezpieczającymi. Referaty drukowane w postaci broszur otrzymywali wszyscy uczestnicy warsztatów. Część nakładu trafiała do bibliotek szkół pożarniczych, między innymi do Szkoły Głównej Służby Pożarniczej w Warszawie, oraz do aktywnych firm i projektantów, którzy z różnych powodów nie mogli uczestniczyć w imprezie.

Przez wiele lat materiały wydawane z okazji warsztatów były jednym z najważniejszych źródeł fachowej literatury dla specjalistów z branży przeciwpożarowej.

Referentami podczas warsztatów były osoby znane i uznawane za autorytety w danej dziedzinie, m.in. przedstawiciele Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej, Instytutu Techniki Budowlanej, Szkoły Głównej Służby Pożarniczej, Komendy Głównej Państwowej Straży Pożarnej, Stowarzyszenia Inżynierów i Techników Pożarnictwa, Państwowej Agencji Atomistyki, Ośrodka Ochrony Zbiorów Publicznych.



Z okazji dwudziestolecia warsztatów chcielibyśmy serdecznie podziękować wszystkim referentom, gdyż to między innymi ich wysiłek złożył się na sukces i prestiż Ogólnopolskich Warsztatów Sygnalizacja i Automatyka Pożarowa SAP.

Modernizacja bazy noclegowej w ośrodku nad Zalewem Koronowskim spowodowała, że w 2009 roku impreza po raz ostatni odbyła się w Zaciszu, które niektórzy do dziś wspominają z rozrzewnieniem (a może to tylko tęsknota za latami młodości?). Nieustający wzrost zainteresowania klientów wymusił zmianę lokalizacji. Od 2010 roku spotykamy się w dużych ośrodkach wypoczynkowo-konferencyjnych. Początkowo było to Centrum Konferencyjno-Rekreacyjne „MOLO" w Smardzewicach, a w 2011 roku – Dolina Charlotty Resort & SPA koło Słupska.

To już dwadzieścia lat

Tegoroczne XX Jubileuszowe Ogólnopolskie Warsztaty Sygnalizacja i Automatyka Pożarowa SAP 2012 odbyły się w dniach 13–15 września w Centrum Kongresowo-Szkoleniowym „Magellan" nad Zalewem Sulejowskim. Impreza zgromadziła blisko 200 uczestników. Swoją obecnością zaszczycili nas między innymi przedstawiciele Biura Rozpoznawania Zagrożeń Komendy Głównej PSP, Kujawsko-Pomorskiej Komendy Wojewódzkiej PSP oraz Łódzkiej Komendy Wojewódzkiej PSP, Narodowego Instytutu Muzealnictwa i Ochrony Zbiorów, Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej, Instytutu Techniki Budowlanej, Zarządu Głównego Stowarzyszenia Inżynierów i Techników Pożarnictwa, Szkoły Głównej Służby Pożarniczej oraz Ministerstwa Kultury i Dziedzictwa Narodowego.

Tematem wiodącym tegorocznej imprezy były *Nowe kierunki w sygnalizacji i automatyce pożarowej*.

Jak co roku do omówienia tej problematyki organizatorzy zaprosili wybitnych specjalistów, którzy wygłosili następujące referaty:

– *Zmiana regulacji prawnych – zastąpienie Dyrektywy CPD rozporządzeniem Parlamentu Europejskiego i Rady UE Nr 305/2011 i wynikające z tego skutki dla procesu certyfikacji* – Barbara Dobosz, Instytut Techniki Budowlanej, Warszawa,
– *Tendencje rozwojowe w konstrukcji czujek pożarowych* – Jerzy Ciszewski, Instytut Techniki Budowlanej, Warszawa,
– *Zaawansowana technika w ochronie przeciwpożarowej zabytków – wybrane elementy* – Piotr Ogrodzki, Narodowy Instytut Muzealnictwa i Ochrony Zbiorów, Warszawa,
– *Integracja systemów bezpieczeństwa – wymagania formalne i podstawy stosowania* – Janusz Sawicki, Instytut Techniki Budowlanej, Warszawa,
– *Nowy projekt normy prEN 54-14:2011 zastępujący specyfikację CEN/TS 54-14:2006 na tle projektu ISO/DIS 7240-14:2012 – bieżący stan prac Komitetu Technicznego KT 264* – Mariusz Sowiński, POLON-ALFA, Bydgoszcz.

Uczestnicy z ogromnym zainteresowaniem wysłuchali referatów, ale też z wielką niecierpliwością czekali na zapowiadaną prezentację pt. *System sygnalizacji pożarowej POLON 6000 – centrala o architekturze rozproszonej*, czyli prezentację nowego systemu wdrażanego do produkcji przez POLON-ALFA.

Powszechne zaciekawienie wzbudził fakt, że centrala ta jako pierwsza w Polsce została zaprojektowana według koncepcji urządzenia modułowego o architekturze rozproszonej, czyli o wielu możliwych obudowach rozmieszczonych w różnych punktach chronionego obiektu, tzw. węzłach, niejednokrotnie znacznie od siebie oddalonych. Takie rozwiązanie umożliwia optymalne dopasowanie urządzeń do chronionego obiektu i jest przełomem w konstrukcji systemów sygnalizacji pożarowej.

Nowy system sygnalizacji pożarowej POLON 6000 jest kompatybilny z obecnie oferowanym systemem POLON 4000. Wszystkie elementy liniowe systemu POLON 4000 mogą współpracować z nową centralą za pośrednictwem programowo definiowanej linii dozorowej typu 4000. Większość elementów liniowych szeregu 4000 oraz wszystkie elementy liniowe nowego szeregu 6000 mogą współpracować z centralą w nowo zdefiniowanym standardzie linii 6000.

POLON 6000 jest odpowiedzią na wymagania klientów oraz wyzwanie, jakie niesie rozwój techniki, w tym nowoczesnych, opartych na najnowszych technologiach urządzeń i systemów sygnalizacji pożarowej. Wkrótce, po przeprowadzeniu badań i certyfikacji, POLON 6000 pojawi się w naszej ofercie handlowej.

Wiedzieliśmy, że POLON 6000 wzbudzi duże zainteresowanie, ale chyba nikt nie przypuszczał, że będzie ono aż takie wielkie. Warto dodać, że od razu przygotowano pełen asortyment modułów i elementów wchodzących w skład systemu. Nowe podejście i charakterystyka systemu POLON 6000 wzbudziły w uczestnikach uznanie dla firmy POLON-ALFA i kierunku jej rozwoju. Firma ta nieustannie ulepsza swoje produkty i utrzymuje pozycję lidera na rynku.

Uczestnicy warsztatów nie kryli zadowolenia, gdyż wiele ich potrzeb i uwag przekazanych przez nich konsultantom POLON-ALFA znalazło swoje odbicie w nowym systemie. Dla wszystkich uczestników przygotowano komplet materiałów informacyjnych, w skład których weszła między innymi broszura zawierająca referaty poświęcone tematowi wiodącemu warsztatów oraz upominek.

Sympatyczni uczestnicy, piękna pogoda i wspaniała atmosfera dwudziestych jubileuszowych warsztatów SAP 2012 upewniły nas o potrzebie organizowania takich spotkań jeszcze przez długie lata.

POLON-ALFA

IX edycja Kongresu Pożarnictwa
podsumowanie

W lipcu br. w Warszawie, w Centrum Nauki Kopernik, odbyło się coroczne spotkanie branżowe specjalistów ochrony przeciwpożarowej. Tegoroczna edycja jednej z największych konferencji w branży zgromadziła ponad 600 uczestników i blisko 50 wystawców oraz spotkała się z szerokim zainteresowaniem osób odpowiedzialnych za projekty i realizacje inwestycji, reprezentujących m.in. budownictwo użyteczności publicznej i mieszkaniowe, budownictwo sportowe, przemysł oraz branże projektowo-wykonawcze. Po raz kolejny **Kongres Pożarnictwa** zgromadził rekordową liczbę uczestników zainteresowanych problematyką bezpieczeństwa. Jest to kolejny sukces organizacyjny firmy **DND PROJECT** realizującej szereg szkoleń i konferencji, m.in. dla tego sektora budownictwa. Patronat medialny nad imprezą objęła m.in. redakcja *Zabezpieczeń*.

Wykłady dotyczyły przede wszystkim ochrony przeciwpożarowej i bezpieczeństwa energetycznego, zapobiegania pożarom i awariom w budownictwie i przemyśle oraz prawidłowego projektowania urządzeń przeciwpożarowych przeznaczonych do zastosowania w obiektach budowlanych. Podczas konferencji wygłoszono 22 referaty poruszające istotne zagadnienia dotyczące bezpieczeństwa obiektów i odnoszące się do aktualnych norm, wymogów i zmian w przepisach. Ekspozycje wystawców zaskoczyły oryginalnością i pomysłowością. Konferencji towarzyszyły również pokazy sprzętu, technologii oraz systemów przeciwpożarowych i elektroinstalacyjnych. Uczestnicy mogli uzyskać praktyczne porady oraz wytyczne projektowe i montażowe od doradców technicznych producentów.

Konferencję uświetniła obecność gości reprezentujących m.in. Kancelarię Prezydenta RP, Ministerstwo Pracy i Polityki Społecznej, Urząd Miasta St. Warszawy, Kierownictwo Komendy Głównej Państwowej Straży Pożarnej oraz komend terytorialnych z całego kraju, Szkołę Główną Służby Pożarniczej, Polskie Radio, NCS, NBP, PLL LOT, a także licznych przedstawicieli uczelni wyższych i przedsiębiorstw budowlanych, projektantów, architektów oraz dziennikarzy prasy i branżowych mediów.

Złotym Sponsorem IX edycji kongresu była firma SVT POLSKA, która w swoim wystąpieniu zaprezentowała bierne zabezpieczenia przeciwpożarowe Pyro-Safe, przeznaczone do konstrukcji stalowych, przepustów i przejść kablowych. Duże zainteresowanie uczestników konferencji, zwłaszcza projektantów, wzbudziła prezentacja reprezentantów firmy CREATIO INDUSTRY, Srebrnego Sponsora kongresu, którzy pokazali, jak skutecznie chronić obiekty za pomocą bezprzewodowych systemów detekcji pożaru.

Na kongresie pokazano m.in. nowoczesne i estetyczne rozwiązania firmy Aluprof, służące do konstruowania ekskluzywnych

i reprezentacyjnych obiektów budowlanych przy zachowaniu pełnego bezpieczeństwa pożarowego, system integrujący DMS 8000 marki Siemens, sposoby zabezpieczeń przed zagrożeniami wybuchowymi i toksycznymi w budynkach, prezentowane przez firmę ALTER, przeciwwybuchowe i specjalne oprawy oświetleniowe firmy Finicom, przeznaczone dla stref zagrożonych pożarem i aktami wandalizmu, okno oddymiające FSP do grawitacyjnego systemu oddymiania marki FAKRO, oświetlenie awaryjne, prezentowane przez firmę AWEX. Dużym zainteresowaniem uczestników konferencji cieszyło się stoisko firmy Top Design Chwaszczyno, która zademonstrowała ewakuację za pomocą fotoluminescencyjnych systemów ewakuacyjnych. Na uwagę zasługuje również zaprezentowany przez firmę RAJ International analogowy adresowalny system wykrywania pożaru. Pokaz silników i łodzi przeznaczonych dla jednostek ratownictwa wodnego OSP i PSP, grup ratownictwa WOPR, jednostek patrolowych straży rybackiej, Straży Granicznej, policji, Wojska Polskiego, RZGW oraz służb zarządzania kryzysowego wzbudził duże zainteresowanie licznie zgromadzonych na konferencji przedstawicieli państwowej i ochotniczej straży pożarnej oraz KG Policji. Zaprezentowane zespoły kablowe podtrzymujące funkcje przez 30 lub 90 minut w warunkach pożaru (E30/E90) i specjalistyczne obudowy elektroinstalacyjne marki Spelsberg Elektro zainteresowały obecnych na konferencji projektantów instalacji elektrycznych i elektroinstalatorów.

Na konferencji omawiano też prawidłowe projektowanie instalacji i systemów pożarowych w nowoczesnych obiektach budowlanych, a także procedury ich późniejszych odbiorów. Uczestnicy kongresu dowiedzieli się m.in., jakie są najczęstsze problemy i błędy popełniane przy projektowaniu i wykonywaniu zabezpieczeń przeciwpożarowych, biernych zabezpieczeń przeciwpożarowych i podczas instalacji, na co zwracać uwagę przy projektowaniu ochrony przeciwprzepięciowej, jak ważne jest zasilanie awaryjne, ochrona odgromowa, właściwe oznakowanie dróg ewakuacyjnych, a także jak stosować polskie normy oraz jakie są wymagania dotyczące zabezpieczenia przeciwpożarowego obiektów użyteczności publicznej, w tym obiektów handlowych. Wykład na ten temat wygłosił mgr inż. Tadeusz Cisek, ekspert rzeczoznawca w dziedzinie ochrony przeciwpożarowej.

O tym, jak istotne są zagadnienia związane z bezpieczeństwem pożarowym i potrzebą dostępu do najnowszych rozwiązań w tej dziedzinie świadczyła frekwencja. Kongres Pożarnictwa już na stałe wpisał się w kalendarz wydarzeń interesujących branżę zabezpieczeń przeciwpożarowych.

Bezpośr. inf. DND PROJECT

Spaleni słońcem

Andrzej Walczyk

„Spaleni słońcem” to tytuł znanego filmu Nikity Michałkowa, jednakże ten artykuł nie ma nic wspólnego z dramatami przeżywanymi przez jego bohaterów, a jedynie opisuje pewne zjawiska fizyczne, które mogą przysporzyć mieszkańcom Ziemi równie wielu kłopotów. U większości ludzi słowo „słońce” wywołuje pozytywne skojarzenia. Jego obecność na pogodnym niebie jest jednoznacznie utożsamiana ze światłem i ciepłem. Wiele osób nie zdaje sobie sprawy z tego, że emitowane przez nie promieniowanie ma wiele składników, z których nie wszystkie są dla nas korzystne

Słońce a technologia

Od czasów prehistorycznych do końca XIX wieku ludzie traktowali słońce jako stały, niezmienny element w ich życiu. Pomimo rozwoju nauki przez stulecia nie podawano żadnego sensownego wyjaśnienia zjawisk zachodzących na Słońcu. Nikt nie zastanawiał się też nad łatwo zauważalnymi fenomenami, choćby takimi jak ciemne plamy pojawiające się okresowo na jego tarczy. Takie plamy zostały po raz pierwszy zaobserwowane w starożytności, zaś w epoce wczesnego renesansu ich naukowymi badaniami zajmował się Galileusz, jednak ich pochodzenie wyjaśniono w zadowalający sposób dopiero w XX wieku. Dopiero w XX wieku postępy w dziedzinie fizyki pozwoliły wyjaśnić, że źródłem energii we wszystkich gwiazdach, w tym także na Słońcu, jest reakcja termojądrowa, zaś jej przebieg wcale nie jest równomierny i niezmienny.

Słońce jest dla nas nie tylko źródłem światła i ciepła. Jego negatywne oddziaływania, które również mają miejsce, mogą utrudnić lub nawet uniemożliwić dalszy rozwój naszej cywilizacji. Wszystkie te negatywne zjawiska występowały od zarania dziejów, jednak przed wiekami ich skutki trafiały w próżnię, bowiem nie istniały żadne urządzenia czy systemy, które wykazywałyby choćby najmniejszą podatność na tego typu oddziaływania. To, co obecnie nazywamy burzami magnetycznymi, powodowało pojawianie się mniej lub bardziej intensywnych zórz polarnych, którym ludy zamieszkujące obszary podbiegunowe przypisywały magiczne właściwości i które były przez nie postrzegane jako zła wróżba. Na tym kończył się negatywny wpływ Słońca na rozwój ziemskiej cywilizacji.

Sytuacja uległa drastycznej zmianie pod koniec XIX wieku, kiedy to na Ziemi pojawiły się pierwsze linie kolejowe i stacje telegraficzne. Zarówno tory kolejowe, jak i druty telegraficzne stanowiły przewodniki o długości dochodzącej do wielu tysięcy kilometrów. W ten sposób powstały pierwsze ziemskie obiekty wykazujące podatność na negatywne oddziaływania Słońca.

W wielu publikacjach można znaleźć opis silnej burzy magnetycznej, która wystąpiła drugiego września 1859 roku. Poprzedziły ją niecodzienne zjawiska na Słońcu zaobserwowane przez angielskiego astronoma-amatora Richarda Carringtona. Analiza opisu tych zjawisk pozwala przypuszczać, że na Słońcu nastąpił wtedy rozbłysk, któremu towarzyszył koronalny wyrzut masy. Tego typu zjawiska są obecnie dobrze znane i podlegają prognozowaniu podobnie jak prognozuje się pogodę, jednakże w tamtych latach były dla astronomów całkowicie zaskakujące. Wyemitowana przez Słońce chmura gorącej plazmy przemieszczała się w kierunku Ziemi z kosmiczną prędkością przekraczającą osiem milionów kilometrów na godzinę i po dwóch dobach dotarła do niej, powodując najsilniejszą ze znanych burzę magnetyczną. Nie oznacza to, że w przeszłości nie występowały jeszcze gwałtowniejsze burze magnetyczne.

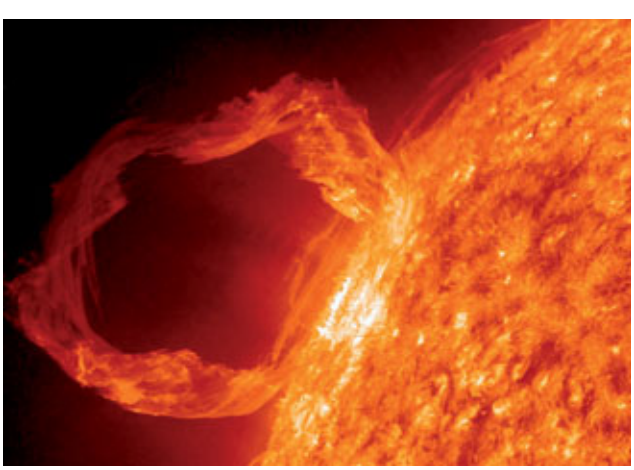
W nocy z 2 na 3 września 1859 roku zorze polarne były tak silne, że rozjaśniły niebo nawet na obszarach podzwrotnikowych, myląc rybaków karaibskich, którzy wypłynęli na morze myśląc, że to już świt. Zmyleni jasnym niebem górnicy w Górach Skalistych także udali się do pracy. Jak widać, jedni i drudzy nie dysponowali jeszcze zegarkami, zaś ich pomyłka nie miała większego znaczenia praktycznego. Jasne zorze były widoczne także w Meksyku, w Afryce i w wielu innych regionach, lecz i tam nie wywołały żadnych poważnych skutków.

Zupełnie inaczej przedstawiała się sytuacja na stacjach kolejowych na terenie Europy i Stanów Zjednoczonych, gdzie zainstalowane były liczne linie telegraficzne. Obecnie wiemy, że burze magnetyczne powodują przepływ prądu stałego o znacznym natężeniu przez wszystkie ciała zdolne ten prąd przewodzić, jednakże tej wiedzy nie mieli ówcześni kolejarze. Obsługa stacji telegraficznych stwierdziła, że telegraf ciągle działa pomimo odłączenia zasilania, zaś przepływającego prądu nie można w żaden sposób wyłączyć. Doprowadziło to do licznych pożarów oraz do porażenia pracowników obsługujących telegraf i nastawnie kolejowe. Tak niecodziennych zjawisk nie można było w żaden sposób wyjaśnić i nikt nie wiązał ich z wybuchem na Słońcu, zaobserwowanym dwa dni wcześniej przez anonimowego angielskiego astronoma-amatora.

Obecnie wydarzenia z drugiego września 1859 roku mogą wydawać się komiczne i mało znaczące, jednak należy zauważyć, że cywilizacja stworzona przez ludzi żyjących w połowie XIX wieku była mało uzależniona od zdobyczy technologii, dlatego silna burza magnetyczna nie stanowiła zagrożenia dla zdrowia i życia mieszkańców Ziemi i nie spowodowała dużych strat materialnych. Ocenia się, że gdyby podobny kataklizm zdarzył się w XXI wieku, jego skutki dla gospodarki światowej byłyby katastrofalne.

We współczesnym świecie najwyższą podatność na burze magnetyczne wykazują sieci energetyczne, a konkretnie transformatory wysokiego napięcia. Przepływ prądu stałego przez uzwojenia takich transformatorów powoduje nasycanie ich rdzeni, a tym samym drastyczny wzrost wydzielania ciepła. Innymi słowy, na skutek silnej burzy magnetycznej większość transformatorów energetycznych na całej Ziemi uległaby spaleniu. Mogłoby się wydawać, że nie powinno to spowodować większych problemów, gdyż łączna liczba tych transformatorów nie jest duża i można byłoby wymienić je na nowe, jednakże tego typu transformatory są produkowane jedynie na zamówienie, a cykl produkcyjny w normalnych warunkach trwa około roku. W nienormalnych warunkach, to znaczy przy braku energii elektrycznej, unieruchomionym transporcie i niedziałających zakładach kooperacyjnych uszkodzone transformatory można byłoby wymienić dopiero po kilkunastu latach. W tym czasie cała Ziemia pozostawałaby bez dostaw energii elektrycznej. Chyba nikomu nie trzeba wyjaśniać skutków takiego stanu rzeczy.

W wielu krajach, między innymi w Stanach Zjednoczonych, prowadzone są prace zmierzające do poprawy tej sytuacji. Sposobem na uniknięcie globalnej katastrofy jest natychmiastowe odłączenie transformatorów wysokiego napięcia od linii energetycznych, jednakże w praktyce jest to trudne i odpowiednie rozwiązania techniczne zostały zastosowane jedynie w niektórych sieciach, zaś system wczesnego ostrzegania praktycznie nie istnieje. Innym

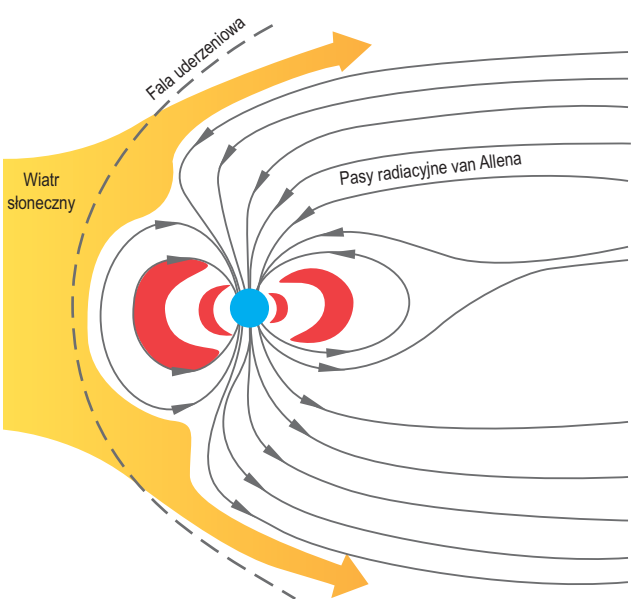


Fot. 1. Koronalny wyrzut masy na słońcu, źródło: NASA/GSFC/Obserwatorium Dynamiki Słońca

sposobem jest modyfikacja sieci energetycznych pozwalająca na odcięcie drogi przepływu prądu stałego przez transformatory, co może być zrealizowane z użyciem odpowiednio skonstruowanych kondensatorów, jednakże ta metoda jest kosztowna i bardzo kłopotliwa w realizacji i nikt nie rozpatruje jej poważnie.

Na zniszczenie na skutek wystąpienia silnej burzy magnetycznej narażone są także systemy zawdzięczające swoje działanie okrążającym Ziemię satelitom. Należą do nich systemy telekomunikacyjne, nawigacyjne a także radiofoniczne, militarne i liczne inne. Chmura cząstek wyrzucanych przez Słońce w chwili rozbłysku koronowego zdmuchuje satelity z orbit podobnie jak silny wiatr powoduje zmianę kursu okrętów na morzu. Słońce cały czas emituje słaby strumień cząstek materialnych zwany wiatrem słonecznym, dlatego wszystkie satelity telekomunikacyjne są wyposażone w silniki korekcyjne stabilizujące ich orbity. W przypadku silnych podmuchów wiatru słonecznego występujących podczas burz magnetycznych silniki korekcyjne nie będą w stanie podołać zadaniu i orbity satelitów ulegną trwałym zmianom, co w konsekwencji spowoduje ich awarię. Ponadto Słońce cały czas emituje strumień innych cząstek materialnych, między innymi neutronów, oraz jest źródłem promieniowania rentgenowskiego, co powoduje zakłócenia w pracy lub nawet uszkodzenia urządzeń elektronicznych znajdujących się w kosmosie. Przykładowo, na skutek promieniowania słonecznego następuje okresowe resetowanie komputerów pokładowych w pojazdach kosmicznych i satelitach telekomunikacyjnych. Podczas burz magnetycznych emisja cząstek materialnych oraz innych szkodliwych promieniowań intensyfikuje się, co w skrajnych przypadkach może całkowicie zablokować komputery pokładowe tych satelitów. Odczuwalne dla nas skutki to między innymi uniemożliwienie jakichkolwiek połączeń telefonicznych, brak dostępu do Internetu i programu telewizyjnego, brak nawigacji satelitarnej.

Promieniowanie korpuskularne emitowane przez Słońce jest szkodliwe dla kosmonautów przebywających w promach kosmicznych i na stacjach orbitalnych. Nie chroni ich ani atmosfera, ani ziemskie pole magnetyczne, dlatego podczas planowania załogowych lotów kosmicznych uwzględnia się prognozy kosmicznej pogody, czyli przewidywaną siłę wiatru słonecznego oraz intensywność innego rodzaju promieniowań, przed którymi kosmonauci nie mogą być chronieni. Skuteczna ochrona wymagałaby zastosowania dużych i ciężkich osłon, których wyniesienie w przestrzeń kosmiczną z użyciem dostępnych środków transportu jest niemożliwe. Jak widać Ziemia z jej atmosferą i magnetosferą stanowi doskonały schron dla istot żywych. Zainteresowanych tym problemem odsyłam do strony www.spaceweather.com, na której można znaleźć szczegółowe dane na temat aktualnego stanu Słońca.



Rys. 1. Wiatr słoneczny i pasy van Allena

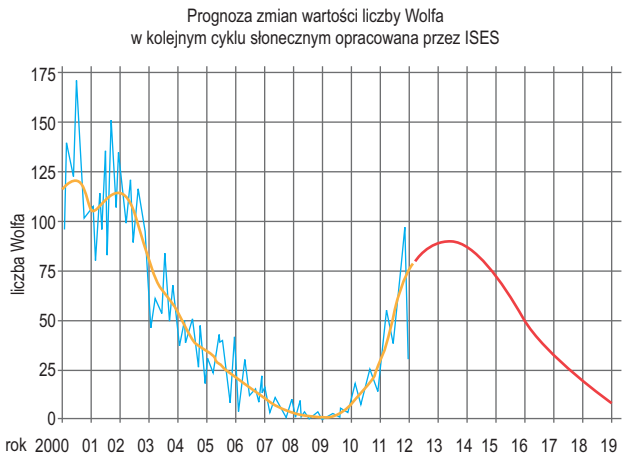
Nie jest to pełna lista strat, z jakimi należy się liczyć w przypadku wystąpienia silnej burzy magnetycznej. Ponadto słabsze burze także stanowią istotne zagrożenie. Przykładowo, na skutek wyrzutu plazmy z korony słonecznej, który miał miejsce dziewiątego marca 1989 roku, w cztery dni później na Ziemi rozszalała się burza magnetyczna, która spowodowała wyłączenie sieci energetycznej w okręgu Quebec w Kanadzie, które nastąpiło w efekcie kaskadowego zadziałania zabezpieczeń. Spaleniu uległy dwa transformatory wysokiego napięcia, zaś awaria na dziewięć godzin pozbawiła prądu sześć milionów ludzi i miała poważne skutki ekonomiczne.

Czym są burze magnetyczne?

Jak wiadomo, na skutek zjawisk zachodzących w płynnym wnętrzu Ziemi powstaje pole magnetyczne, dzięki czemu naszą planetę można porównać do gigantycznego magnesu stałego, którego bieguny są zlokalizowane w pobliżu biegunów geograficznych. Przestrzeń, w której Ziemia porusza się po orbicie wokółsłonecznej, bynajmniej nie jest próżnią. Ta przestrzeń jest wypełniona zjonizowanymi cząstkami materialnymi, głównie rozpędzonymi elektronami i protonami o bardzo wysokich energiach kinetycznych, wchodzącymi w skład wiatru słonecznego. Strumień tych cząstek można traktować jako pewnego rodzaju promieniowanie korpuskularne, którego natężenie nie jest stałe, lecz jest zależne od zjawisk zachodzących we wnętrzu Słońca. Gdyby to promieniowanie docierało bezpośrednio do powierzchni Ziemi, byłoby zabójcze dla większości organizmów żywych, jednakże ulega ono znacznemu osłabieniu po przejściu przez atmosferę ziemską, zaś pole magnetyczne powoduje jego odchylenie w kierunku biegunów.

Planetę obdarzoną polem magnetycznym można porównać do samolotu lecącego z prędkością naddźwiękową, który rozgarnia znajdujące się przed nim powietrze, co powoduje wytworzenie fali uderzeniowej oraz lokalne zmiany ciśnienia. Na podobnej zasadzie poruszająca się ruchem orbitalnym Ziemia rozgarnia cząstki wiatru słonecznego i tworzy falę uderzeniową, układającą się w przestrzeni kosmicznej w tak zwane pasy van Allena. To zjawisko zostało wykryte w 1958 roku przez aparaturę pokładowa satelity Explorer 1.

Intensywność wiatru słonecznego jest zależna od stanu Słońca i w przeciętnych warunkach ustala się równowaga między strumieniem cząstek a ziemskim polem magnetycznym, której nie towarzyszą żadne nadzwyczajne zjawiska fizyczne. Jednakże w okresach, w których aktywność Słońca wzrasta, ta równowaga ulega zaburzeniu. Jeśli gęstość strumienia cząstek emitowanych przez Słońce z jakiegoś powodu wzrasta, ruch tych cząstek oraz ich nagromadzenie w pobliżu biegunów powoduje zmiany ziemskiego pola magnetycznego. Gwałtowne zmiany ziemskiego pola magnetycznego indukują prąd elektryczny przepływający przez wszystkie materiały zdolne do jego przewodzenia, to znaczy przez glebę, wodę morską, a także przez różne wytwory technologii, takie jak linie energetyczne, tory kolejowe, rurociągi naftowe i gazowe. Jeśli w tych konstrukcjach nie zostały



Rys. 2. Aktywność słońca na przestrzeni ostatnich dwunastu lat

zastosowane odpowiednie zabezpieczenia, dochodzi do niekontrolowanego przepływu prądu stałego o dużym natężeniu. I właśnie taki stan nazywamy burzą magnetyczną.

Dwudziesty czwarty cykl słoneczny i jego wpływ na rozwój technologii

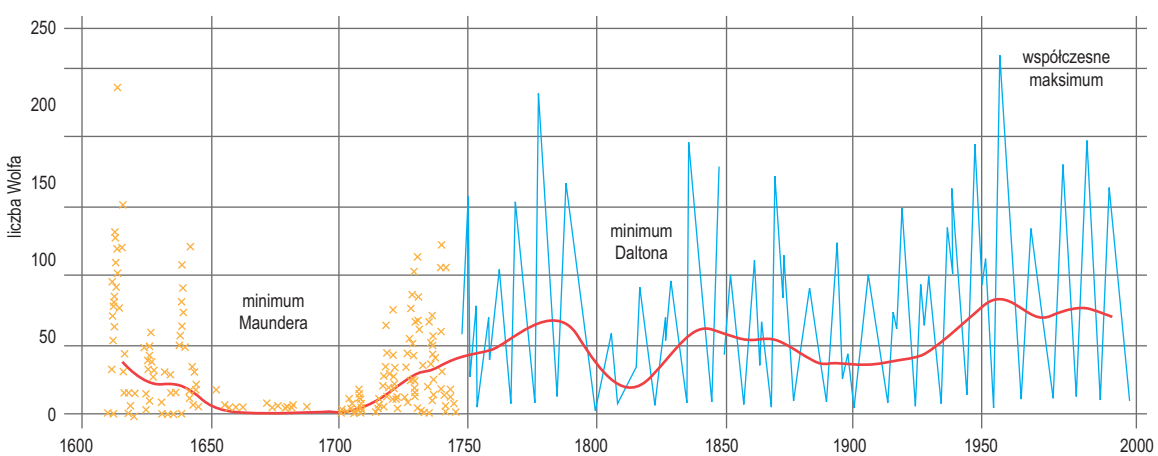
Dane zgromadzone dzięki obserwacjom Słońca prowadzonym przez ostatnie czterysta lat pozwoliły stwierdzić, że aktywność Słońca nie jest stała – podlega cyklicznym zmianom. W 1849 roku szwajcarski astronom i matematyk Rudolf Wolf opracował metodę ilościowej oceny aktywności słonecznej na podstawie liczby i rozkładu plam na Słońcu. Zaproponowana metoda była o tyle dobra, że pozwalała na porównywanie wyników badań uzyskiwanych w różnych obserwatoriach, niezależnie od rodzaju i rozmiarów użytych teleskopów. Od tamtej pory miarą aktywności słonecznej stała się tak zwana liczba Wolfa, zaś jej wykres, sporządzony na podstawie wszystkich dostępnych danych, pozwolił stwierdzić, że od kilkuset lat aktywność słoneczna zmienia się cyklicznie, przy czym długość cyklu nie jest stała – niektóre okresy znacznie różnią się od siebie i zdarzają się nawet kilkudziesięcioletnie anomalie, z jakimi mieliśmy do czynienia w latach 1650–1700. Pomimo tych anomalii przyjęto, że aktywność słoneczna zmienia się średnio co jedenaście lat, zaś poszczególne cykle są liczone od 1600 roku i kolejno numerowane. Obecny cykl słoneczny ma numer dwadzieścia cztery i właśnie zmierza do maksimum, które jest przewidywane na rok 2013.

We wczesnych latach dwutysięcznych aktywność słoneczna była bardzo niska, zaś dwudziesty czwarty cykl słoneczny rozpoczął się z kilkuletnim opóźnieniem. Prognozy mówią, że maksymalna wartość liczby Wolfa, której można się spodziewać pod koniec roku 2013, będzie dwa razy niższa niż w cyklu dwudziestym trzecim. To oznacza, że w początkowych latach XXI wieku wszystkie urządzenia i systemy elektryczne budowane przez ludzi, zarówno te, które zostały zainstalowane na powierzchni ziemi, jak i te, które zostały umieszczone w przestrzeni kosmicznej, nie podlegają i długo nie będą podlegały niszczycielskim wpływom promieniowania emitowanego przez Słońce, gdyż jego intensywność była i będzie bardzo niska. Z jednej strony pozwoliło to na szybki rozwój technologii, lecz z drugiej niesie ze sobą bardzo poważne niebezpieczeństwa.

Zasady ekonomii, którymi kierują się wszystkie firmy budujące rozległe instalacje energetyczne czy telekomunikacyjne, zmuszają do stosowania jak najprostszych rozwiązań technologicznych. Podobnie jest w przypadku konstrukcji satelitów telekomunikacyjnych i innych obiektów umieszczonych w kosmosie. Spokojne Słońce pozwala na potanienie produkcji i na bezawaryjną pracę tych urządzeń, gdyż nie trzeba stosować dodatkowych zabezpieczeń czy gromadzić zapasów części zamiennych. Jeśli aktywność słoneczna w roku 2013 rzeczywiście będzie tak niska, jak mówią prognozy, egzekucja „wyroku" zostanie przesunięta o kolejne jedenaście lat. Nie można jednak wykluczyć możliwości nieoczekiwanego wystąpienia silnej burzy magnetycznej, gdyż wyrzuty zjonizowanej materii z korony słonecznej mają charakter losowy. Zachodzi tu duże podobieństwo do wylewów rzek, które mają różną intensywność, zdarzają się w różnych odstępach czasowych i są trudne do przewidzenia. Mówi się o wodzie dziesięcioletniej i o wodzie stuletniej. Na podobnej zasadzie można prognozować, że umiarkowanie silne burze magnetyczne mogą się zdarzyć co kilkanaście lat, gdyż prawdopodobieństwo ich wystąpienia jest uzależnione od przebiegu jedenastoletniego cyklu aktywności słonecznej, tymczasem silne burze magnetyczne, podobne do tej, która miała miejsce w 1859 roku, mogą wystąpić co kilkaset lat, zaś rządzące nimi mechanizmy nie są dotychczas znane.

Jak się zabezpieczyć przed skutkami burz magnetycznych?

Silnych burz magnetycznych nie można uniknąć, tak jak nie można uniknąć piorunów uderzających w wysokie budynki. Intensywny strumień zjonizowanych cząstek o bardzo wysokich energiach



Rys. 3. Aktywność słońca na przestrzeni ostatnich czterystu lat

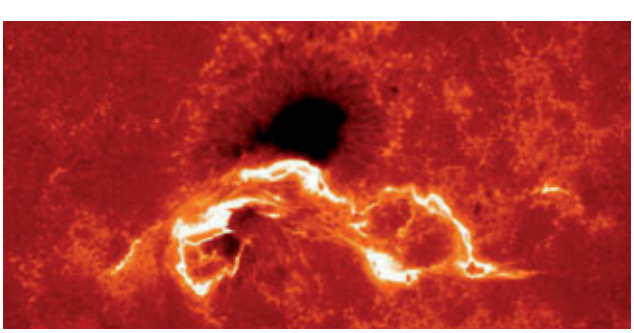
jest w stanie przedrzeć się przez atmosferę i magnetosferę ziemską, powodując przepływ prądu elektrycznego w zewnętrznych partiach skorupy ziemskiej i w instalacjach wytworzonych przez ludzi. Jedynym zabezpieczeniem jest stworzenie bezpiecznej drogi przepływu dla takiego prądu, tak jak w instalacjach odgromowych, gdzie prąd piorunowy jest odprowadzany do ziemi przez system zwodów i jego przepływ nie powoduje poważnych skutków. Wiąże się to z koniecznością przekonstruowania wielu kosztownych urządzeń, choćby takich jak transformatory stosowane w energetyce, a także zmusza do zmian w inwestycjach związanych z nowymi instalacjami. W świecie, w którym jedynym celem rozwoju jest zysk wynikający ze sprzedaży towarów, trudno liczyć na to, że ktokolwiek z własnej woli podejmie tego typu działania.

Na dodatek z długookresowych obserwacji magnetosfery wynika, że ziemskie pole magnetyczne słabnie i za kilkaset lat może dojść do jego zaniku i ponownego odtworzenia, tyle że ze zmienioną biegunowością. Z badań geologicznych wynika, że tego typu przypadki miały już miejsce i Ziemia przez jakiś czas była pozbawiona ochrony wynikającej z istnienia magnetosfery. Te zaniki ziemskiego pola magnetycznego wiąże się z epokami masowego wymierania lądowych gatunków zwierząt.

W przypadku wystąpienia silnych rozbłysków na Słońcu powodujących wyrzut dużej ilości zjonizowanej plazmy nie można zapewnić stabilności orbit i prawidłowego działania aparatury pokładowej satelitów i stacji kosmicznych okrążających Ziemię. Dlatego realnym zagrożeniem jest całkowita, globalna utrata łączności i konieczność odbudowy całej infrastruktury, zarówno naziemnej, jak i kosmicznej. W przypadku całkowitej awarii systemu energetycznego odtworzenie takiej infrastruktury zajmie prawdopodobnie wiele lat. W tym czasie będzie można korzystać z klasycznej jonosferycznej radiokomunikacji i radiofonii, zaś marynarze będą musieli przypomnieć sobie zasady nawigacji z użyciem sekstantu i uwzględnianiem położenia gwiazd, gdyż system GPS przestanie działać.

Co z tego wynika dla osób działających w branży zabezpieczeń?

Jak widać przejście silnej burzy magnetycznej stworzy na Ziemi zupełnie nową sytuację. W ciągu zaledwie kilku godzin warunki życia miliardów ludzi ulegną znacznemu pogorszeniu. Przede wszystkim bardzo szybko wyczerpią się zapasy paliwa, zabraknie energii elektrycznej, staną zakłady pracy, załamie się rynek, zabraknie żywności. W takich warunkach intensyfikują się wszelkie działania bezprawne, zaś zapanowanie nad nimi w warunkach szerzącego się chaosu będzie poważnym wyzwaniem dla zaskoczonych tym stanem służb bezpieczeństwa publicznego. Trudno wyobrazić sobie skalę tego zjawiska, jednakże częściowo można zabezpieczyć się przed jego skutkami.



Fot. 2. Plamy słoneczne, takie jak widoczne na zdjęciu nie pojawiały się w latach 2008 - 2010, przez co w tym okresie słońce zachowywało bardzo niską aktywność (zdjęcie udostępnione dzięki uprzejmości Hinode Mission)

Większości ludzi, szczególnie młodych, pozostaje w dużej zależności od powszechnie dostępnych usług, takich jak GSM, UMTS, HSDPA, GPS, SMS, MMS, GPRS, TCP/IP, VPN, VoIP i wielu, wielu innych, które trudno wymienić. Z biegiem czasu dostępność takich usług staje się dla wszystkich oczywista – jak dostępność powietrza czy przysłowiowego słońca na niebie. Gdy nagle tych zdobyczy zabraknie, przetrwają tylko te systemy, które działają niezależnie od skomplikowanej infrastruktury teleinformatycznej, zarówno naziemnej, jak i kosmicznej, oraz komercyjnie świadczonych usług.

Z tych względów podczas projektowania nowego systemu alarmowego warto zastanowić się, czy zastosowanie archaicznego łącza przewodowego lub własnej, dedykowanej linii radiowej nie jest lepszym rozwiązaniem niż korzystanie z usługi monitoringu alarmów za pośrednictwem telefonu komórkowego i wyspecjalizowanej agencji.

Należy zauważyć, że wszelkie służby o znaczeniu krytycznym decydują się na tworzenie własnych sieci teleinformatycznych w oparciu o mało podatne na zakłócenia linie światłowodowe. Profesjonalne systemy łączności radiowej, takie jak Tetra, także korzystają z własnych stacji przemiennikowych, własnych rezerwowych źródeł zasilania i nie są w żaden sposób zależne od tanich usług komercyjnych. Bynajmniej nie chodzi tu o dostosowanie się do skutków burzy magnetycznej, gdyż mało kto o tym wie i mało kto się nad tym zastanawia. Chodzi o zwyczajną dbałość o pracę systemów w warunkach kryzysowych, podczas powodzi, trzęsienia ziemi czy konfliktu zbrojnego. Tego typu podejście trafia jednak na opór w postaci praw ekonomii rządzących współczesnym światem. Telekomunikacja, ochrona fizyczna, a także cały świat mediów i rozrywki bazuje na tanich, powszechnie dostępnych usługach, zaś tworzenie własnych sieci i rozwiązań działających niezależnie od obcej infrastruktury jest znacznie droższe.

Jak uniknąć tragedii?

Śmiało można zaryzykować stwierdzenie, że prawdopodobieństwo wystąpienia silnej burzy magnetycznej jest niewielkie, jednak takiego zdarzenia wykluczyć się nie da i kiedyś musi ono nastąpić. Ze względu na losowy charakter zjawisk zachodzących na Słońcu silna burza magnetyczna może równie dobrze wystąpić za sto lat jak za dwa dni i z pewnością będzie stanowiła całkowite zaskoczenie dla mieszkańców Ziemi. Uświadomienie tego zagrożenia osobom odpowiedzialnym za wytyczanie kierunku rozwoju gospodarczego mogłoby zaowocować bardzo kosztownymi przedsięwzięciami umożliwiającymi złagodzenie skutków kataklizmu. Trudno jednak liczyć na podatny grunt dla takiej idei w świecie biznesu. Tak więc prognozy nie są optymistyczne – prędzej czy później zostaniemy spaleni słońcem.

Andrzej Walczyk

Nowy cyfrowy rejestrator wizyjny

DVR 670

Gwarancja pełnej kontroli jakości

Advantage Line

DVR 670 to nowe, kompleksowe rozwiązanie do zarządzania sygnałem wizyjnymserii 600. Wykorzystuje wysoce wydajną technologię kompresji H.264, która gwarantuje doskonałą jakość obrazu przy znacznie niższych wymaganiach w zakresie szerokości pasma i pojemności dysku. Bardzo prosta instalacja rejestratora DVR 670 oraz jego intuicyjna obsługa nie wymaga specjalnego szkolenia, a wysoka niezawodność działania obniża ogólny koszt eksploatacji.
To niedrogie rozwiązanie idealnie sprawdza się w małych i średnich instalacjach, takich jak szkoły, sklepy, banki czy hotele.

Infolinia Advantage Line 22 206 4000
AdvantageLine-Support@bosch.com

BOSCH
Technologia bliżej nas

Systemy CEM
inteligentna ochrona lotnisk

Głównym celem kontroli dostępu na lotnisku jest zapobieganie nieuprawnionemu dostępowi do pewnych obszarów oraz zapewnienie bezpieczeństwa podróżnym i personelowi lotniska, jednakże skuteczna kontrola dostępu na lotnisku jest czymś więcej – ogólnie zwiększa skuteczność operacyjną i poprawia funkcjonowanie portu lotniczego. Aby osiągnięcie tego celu było możliwe, wykorzystywana do ochrony lotniska technologia powinna być jak najbardziej nowoczesna, zgodna z aktualnymi wymogami i sprawdzona w działaniu. Ponadto część terminali powinna być przenośna. Właśnie dlatego warto zastosować system CEM.

CEM chroni lotniska na całym świecie, między innymi w Budapeszcie, Keflaviku, Hong Kongu, Dubaju (terminal 3, hala 3), Vancouver, na wszystkich lotniskach BAA. System firmy CEM zastosowany w terminalu 3 lotniska im. Indiry Gandhi w Delhi zwyciężył w kategorii *Best Airport Security System* i otrzymał nagrodę Emerging Markets Award 2011.

AC2000 – bezpieczeństwo teraz i w przyszłości

W największym międzynarodowym porcie lotniczym Węgier – budapeszteńskim BUD – zatrudnionych jest około 10 000 ludzi. Lotnisko to zajmuje obszar 1515 ha i jest drugim pod względem wielkości portem lotniczym na obszarze Unii Europejskiej. System AC2000 firmy CEM ochrania tam personel, podróżnych i mienie od 1995 roku i został zainstalowany przez Bull Hungary – węgierskiego przedstawiciela firmy CEM.

AC2000 na budapeszteńskim lotnisku umożliwia zaawansowaną kontrolę dostępu i zarządzanie budynkami. Na terenie lotniska działa wiele systemów zwiększających bezpieczeństwo. Dla zarządu portu lotniczego najważniejsze było to, by system kontroli dostępu był solidny, niezawodny i umożliwiał realizację zaawansowanych funkcji.

– *System AC2000 okazał się najbardziej niezawodny spośród wszystkich systemów bezpieczeństwa, jakie posiadamy* – powiedział Gábor Tóth, specjalista technologii zabezpieczeń na lotnisku BUD.

Wersja językowa

Na lotnisku w Budapeszcie wykorzystuje się obecnie czytniki CEM S610. Każdy czytnik z tej serii dysponuje bazą danych, na podstawie których karty dostępu są uwierzytelniane w trybie autonomicznym, klawiaturą do uwierzytelniania kodu PIN, ekranem LCD do wyświetlania ważnych komunikatów

Fot. 2. Budynek Sky Court dworca lotniczego w Budapeszcie

skierowanych do użytkownika i obsługuje różne rodzaje kart. Aby ułatwić pracę personelowi lotniska w Budapeszcie, menu interfejsu przetłumaczono na język węgierski.

Zintegrowana biometryczna kontrola dostępu

Czytnik odcisków palców S610f zapewnia dodatkową ochronę zarówno w ogólnodostępnej, jak i w zastrzeżonej strefie terminalu. Ma takie same charakterystyczne właściwości jak standardowy czytnik S610, ale jest dodatkowo wyposażony w moduł biometryczny umożliwiający trzyetapowe uwierzytelnianie (karta, PIN, odcisk palca). Dzięki niemu nie trzeba stosować dodatkowych urządzeń biometrycznych – linie papilarne użytkownika karty są zapisywane równocześnie z jego danymi osobowymi i zdjęciem. Oprogramowanie AC2000 nie zapisuje i nie przechowuje w systemie aktualnego obrazu odcisku palca. Zamiast tego na podstawie zeskanowanego odcisku tworzony jest unikatowy wzorzec identyfikacyjny użytkownika.

Więcej niż kontrola dostępu

System CEM AC2000 umożliwia nie tylko kontrolę dostępu. Dostępne są dodatkowe moduły oprogramowania ułatwiające różne operacje na terenie lotniska (m.in. AC2000 VIPPS i AC2000 Time & Attendance). AC2000 VIPPS (Visual Imaging and Pass Production System) umożliwia łatwe i szybkie projektowanie i tworzenie na miejscu przepustek dla personelu (ze zdjęciem, logo firmy i podpisem).

Fot. 1. Rodzina produktów systemu AC2000 AE

Fot. 3. Czytnik naścienny - "Wstęp dozwolony"

Rozwój systemu

System CEM AC2000 został zainstalowany na lotnisku w Budapeszcie w 1995 roku i przez lata był ciągle modernizowany z wykorzystaniem aktualnych technologii. W 2009 roku na lotnisku rozpoczęto budowę budynku Sky Court o powierzchni 40000 m^2, a także renowację innych obiektów, zajmujących łącznie 55000 m^2. Budynek Sky Court zbudowano, aby połączyć dwa istniejące terminale – 2A oraz 2B – i podwoić przepustowość lotniska. W ramach prac modernizacyjnych rozbudowano system AC2000, instalując ponad 200 dodatkowych czytników S610e i czytników odcisków palców S610f.

Przodująca technologia

Prowadzone przez lata modernizacje i ulepszenia systemu w porcie lotniczym BUD objęły m.in. zastąpienie kart zbliżeniowych wysoce bezpieczną technologią PicoPass Smartcard. Karty PicoPass na lotnisku w Budapeszcie mogą służyć nie tylko do kontroli dostępu. Umożliwiają na przykład handel bezgotówkowy. – *Wraz z rozszerzeniem systemu AC2000 w celu objęcia nim budynku Sky Court zmodernizowano system ochrony lotniska, by spełniał on aktualne wymogi* – powiedział Andrew Fulton, Business Development Manager w CEM Systems. – *Modernizacja objęła dokonane na zamówienie klienta modyfikacje aplikacji AC2000 i wdrażanie wysoce bezpiecznej technologii PicoPass* – powiedział Bela Troszt, konsultant w Bull Hungary.

Dowiedziona skuteczność ochrony

Skuteczność zarządzania kontrolą dostępu za pomocą systemu CEM AC2000 AE (Airport Edition), jedynego na rynku systemu kontroli dostępu stworzonego z myślą o portach lotniczych, została dowiedziona na wielu najważniejszych lotniskach na świecie. Firma CEM współpracuje z lotniskami od 25 lat i stale pracuje nad nowymi technologiami, które odpowiadają wymaganiom związanym z ich ochroną. Przykładem może być przenośny czytnik kart S3030 Portable, czytniki sieciowe z łączem ethernetowym, urządzenia do kontroli otwarcia drzwi wykorzystujące PoE+ czy w pełni zintegrowane biometryczne systemy bezpieczeństwa.

Więcej informacji dotyczących urządzeń zabezpieczających CEM można znaleźć na stronie *www.cemsys.com*, a także uzyskać drogą e-mailową (*cem.info@tycoint.com*) lub dzwoniąc pod numer +44 (0) 28 90456767.

CEM

Visonic
A Tyco International Company

Zapomnij wszystko co wiesz o bezprzewodowych systemach alarmowych!

PowerG oficjalny zwycięzca konkursu Złoty Medal Securex 2012

System PowerG firmy Visonic na nowo definiuje możliwości bezprzewodowych systemów alarmowych.

Innowacyjny. Bezpieczny. Najlepszy.

Stosując system PowerG:

- dostarczasz klientom stabilny i łatwy w obsłudze system alarmowy
- oszczędzasz pieniądze dzięki szybkiej i bezproblemowej instalacji
- chronisz środowisko poprzez stosowanie urządzeń pracujących nawet 8 lat na jednej baterii

Wyłączny dystrybutor produktów Visonic 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

Unicard został oficjalnym dystrybutorem Samsung Access Control w Polsce i krajach bałtyckich

Samsung Techwin Europe

Firma Samsung Techwin Europe ogłosiła, że firma Unicard jest autoryzowanym dystrybutorem systemów kontroli dostępu firmy Samsung na terenie Polski i krajów bałtyckich. Unicard SA jest dystrybutorem systemów kontroli dostępu z siedzibą w Krakowie i ma biura regionalne w Poznaniu i w Warszawie. Z ponad dwudziestoletnim doświadczeniem w dziedzinie projektowania i dystrybucji systemów kontroli dostępu firma Unicard SA stworzyła sieć, w skład której wchodzi ponad czterdziestu partnerów biznesowych mających status autoryzowanych dostawców Unicard

Nowa wersja oprogramowania SAMS

Oprogramowanie SAMS służące do zarządzania systemami kontroli dostępu zostało uaktualnione. Obecnie obsługuje większą niż dawniej liczbę użytkowników i zawiera nowe funkcje.

Uaktualnione oprogramowanie Samsung's Access Control Management Software (SAMS) nie wymaga licencji i obsługuje systemy kontrolujące maksymalnie 40 przejść (80 czytników) i 1000 użytkowników. Dzięki wprowadzeniu nowej funkcji *Muster Reporting* możliwe jest natychmiastowe tworzenie raportów, z których jasno wynika, kto w danej chwili przebywa wewnątrz obiektu. Lista osób jest tworzona automatycznie w przypadku wykrycia zagrożenia pożarowego.

Jedna ze zmian wprowadzonych w najnowszej wersji SAMS dotyczy możliwości tworzenia nadruków na kartach identyfikacyjnych. Oprócz drukowania stałych fragmentów tekstu oraz logotypu firmy nowe oprogramowanie umożliwia dynamiczne tworzenie napisów na podstawie informacji pobieranych z bazy danych.

Oprogramowanie SAMS pozwala także na integrację systemu kontroli dostępu z systemem dozoru wizyjnego. Dzięki temu, że SAMS jest kompatybilne z oprogramowaniem sieciowych rejestratorów wizyjnych Samsung SRN-470D i SRN-1670D, z systemu mogą być pobierane obrazy o wysokiej rozdzielczości, powstające synchronicznie z wydarzeniami odnotowywanymi przez system kontroli dostępu. – *W pierwszej chwili ta funkcja może nie być doceniona i nie zostanie uznana za szczególnie istotną, jednak wiadomo, że przez wiele lat użytkownicy systemów kontroli dostępu mieli problem z ustaleniem, jakim wydarzeniom zgłaszanym przez ten system odpowiadają fragmenty nagrań dostarczanych przez system dozoru wizyjnego, przy czym dotyczyło to zarówno bieżących wydarzeń, jak i tych, które miały miejsce wcześniej i później w stosunku do momentu, w którym powstał dany fragment nagrania* – powiedział Marcin Kucharski, Business Development Manager firmy Samsung Techwin Europe, odpowiedzialny za terytorium Polski, Czech, Słowacji i krajów bałtyckich.

Technologia RFID oraz techniki biometryczne wykorzystywane w systemach kontroli dostępu pozwalają na tworzenie opłacalnych rozwiązań i nowych aplikacji we wszystkich systemach kontroli dostępu, poczynając od najmniejszych, obejmujących swoim zasięgiem pojedyncze przejścia, do wielkich, obejmujących wielopiętrowe budynki lub grupy budynków. Urządzenia składające się na tę ofertę można podzielić na samodzielne sterowniki, działające niezależnie od innych fragmentów systemu, i na sterowniki obsługujące

Fot. 1. SRN-470D – czterokanałowy sieciowy rejestrator wizyjny Samsung

Fot. 2. SRN-1670D – szesnastokanałowy sieciowy rejestrator wizyjny Samsung

od jednego do czterech przejść, wymagające zastosowania oddzielnych czytników i odpowiedniego oprogramowania. Te ostatnie mogą działać niezależnie od siebie lub mogą być połączone za pośrednictwem sieci TCP/IP lub łącza szeregowego RS485.

Funkcje oferowane przez urządzenia Samsung Access Control są na tyle zróżnicowane, że możliwe jest tworzenie konkurencyjnych rozwiązań w projektach dotyczących maksymalnie 128 tysięcy przejść, przy czym czytniki zbliżeniowe mogą być dodatkowo zabezpieczone kodem PIN lub wykorzystywać technologie biometryczne, takie jak rozpoznawanie odcisków linii papilarnych czy twarzy ludzkich. Możliwości oferowane przez czytniki biometryczne firmy Samsung są imponujące. Przykładowo – każdy z nich jest w stanie rozpoznać jeden z 4000 zapamiętanych odcisków linii papilarnych, a na analizę danych potrzebuje zaledwie pół sekundy.

Ze względu na to, że samodzielne sterowniki, działające niezależnie od innych fragmentów systemu, stanowią idealne rozwiązanie w przypadku kontroli pojedynczych przejść, umożliwiono ich łączenie za pośrednictwem sieci i wzajemne przekazywanie informacji biometrycznych pochodzących ze wspólnej bazy danych bez konieczności stosowania oddzielnych komputerów lub dodatkowego oprogramowania.

Konieczność zapewnienia użytkownikom pełnej kontroli nad kompleksowym systemem, zdolnym do monitorowania, zapisu i odczytu danych niezbędnych do ścigania niechcianych gości oraz osób uwikłanych w działania o charakterze kryminalnym, stanowi nie lada wyzwanie. Warto podkreślić, że oprogramowanie Samsung Access Management Software pozwala na tworzenie szczegółowych raportów dotyczących przemieszczania się posiadaczy kart identyfikacyjnych, które mogą być eksportowane do plików w formacie XLS lub PDF w celu dalszej integracji z aplikacjami służącymi do ewidencji czasu pracy, zarządzania zasobami ludzkimi czy rachuby płac. – *Profesjonalna wersja oprogramowania, SAMS PRO, dysponuje tymi samymi możliwościami, a ponadto oferuje dodatkowe funkcje, w tym obsługę zintegrowanych systemów kontroli dostępu i systemów dozoru wizyjnego, co umożliwia operatorom obserwację obrazów związanych z konkretnym użytkownikiem karty identyfikacyjnej. Ponadto status wszystkich czytników i kamer może być monitorowany i pokazywany na specjalnie przygotowanej mapie* – powiedział Marcin Kucharski.

Rozwiązania stosowane w systemach kontroli dostępu Samsung Access Control

Cała oferta jest podzielona na dwie części. Do pierwszej z nich należą samodzielne sterowniki, działające niezależnie

od innych fragmentów systemu. Do drugiej – sterowniki obsługujące od jednego do czterech przejść, wymagające zastosowania oddzielnych czytników i odpowiedniego oprogramowania, przy czym dostępne są wersje umożliwiające łączenie sterowników za pośrednictwem sieci IP lub łączy szeregowych RS485.

Sterowniki działające niezależnie od siebie

Biorąc pod uwagę fakt, że współczesne czytniki inteligentnych kart zbliżeniowych mogą mieć dodatkowe funkcje podnoszące poziom bezpieczeństwa, takie jak potwierdzanie autentyczności karty zbliżeniowej za pomocą kodu PIN, weryfikacja tożsamości użytkownika karty na podstawie analizy odcisków linii papilarnych lub obrazu twarzy, a także mogą dostarczać danych umożliwiających kontrolę czasu pracy, można stwierdzić, że samodzielne sterowniki firmy Samsung, działające niezależnie od innych składników systemu, są najlepszym rozwiązaniem wszystkich problemów występujących podczas kontroli pojedynczych przejść. Opcje pozwalające na wzajemne łączenie tych sterowników stwarzają możliwość kontroli wielu przejść, przy czym możliwe jest wykorzystanie informacji biometrycznych zawartych we wspólnej bazie danych bez konieczności stosowania dodatkowych komputerów i specjalistycznego oprogramowania. Ponadto samodzielne sterowniki firmy Samsung są w pełni kompatybilne z oprogramowaniem służącym do zarządzania systemami kontroli dostępu, dzięki czemu mogą wymieniać między sobą informacje biometryczne dotyczące użytkowników kart identyfikacyjnych. Znacznie ułatwia to pracę administratorom dużych systemów kontroli dostępu.

Sterowniki obsługujące od jednego do czterech przejść

W przypadku sterowników obsługujących pojedyncze przejścia mogą być wykorzystane karty zbliżeniowe w formacie Mifare i w formacie opracowanym przez firmę Samsung. Wybór odpowiedniej opcji może być dokonany zaraz po wyjęciu urządzeń z opakowania, jednakże w przypadku sterowników kontrolujących maksymalnie cztery przejścia należy z góry zamówić urządzenia w odpowiedniej wersji. W każdym z przypadków sterowniki mogą być ze sobą połączone za pośrednictwem sieci IP lub, opcjonalnie, za pomocą łącza szeregowego RS485.

Fot. 3. SSA-S2100 – czytnik kart zbliżeniowych z zabezpieczeniem kodem PIN

Fot. 4. SSA-R2000 – czytnik kart zbliżeniowych z zabezpieczeniem kodem PIN

Sterowniki kontrolujące pojedyncze przejścia mają dwa wejścia służące do podłączania czytników, dzięki czemu możliwa jest realizacja funkcji *anti-passback*. W przypadku realizacji tej funkcji z użyciem sterowników mogących kontrolować maksymalnie cztery przejścia, mających cztery wejścia służące do podłączania czytników, liczba kontrolowanych przejść musi być ograniczona do dwóch, gdyż w każdym z nich muszą być zastosowane po dwa czytniki.

Czytniki

Wszystkie czytniki oferowane przez firmę Samsung są dostępne w dwóch wersjach różniących się formatem obsługiwanych kart zbliżeniowych. Użytkownik może wybrać format Mifare albo format opracowany przez firmę Samsung. Czytniki są produkowane w wersji standardowej lub wandaloodpornej. Mogą także zawierać dodatkowe zabezpieczenia kodem PIN lub realizować funkcje biometryczne, takie jak rozpoznawanie odcisków linii papilarnych lub twarzy ludzkich. To umożliwia instalatorom i integratorom systemów kontroli dostępu elastyczny dobór najlepszej z możliwych konfiguracji sprzętowej, spełniającej wymagania użytkowników końcowych. Wszystkie czytniki inteligentnych kart zbliżeniowych są objęte wieczystą gwarancją firmy Samsung.

Firma Samsung kontynuuje swój program przekształceń mający na celu dostarczanie użytkownikom kompleksowych systemów zabezpieczających. Ciągłe udoskonalanie urządzeń do kontroli dostępu stanowi jawny dowód zaangażowania tej firmy i jej dbałości o klientów. Oferta obejmuje urządzenia i technologie z różnych dziedzin, integrowane w celu zapewnienia użytkownikom końcowym realnych korzyści wynikających z wykorzystania rozwiązań firmy Samsung.

Wszystkie te produkty są oferowane wraz z pełnym serwisem gwarancyjnym oraz wsparciem technicznym ze strony firmy Samsung Techwin Europe. Samsung proponuje bezpłatne projektowanie systemów, doradztwo techniczne oraz udziela trzyletniej gwarancji na urządzenia i wieczystej gwarancji na czytniki.

Samsung Techwin Europe

SSN
Security Solution Network

NAJWIĘKSZY DYSTRYBUTOR

MARKI SAMSUNG W POLSCE PREZENTUJE:

Nowe kamery sieciowe SAMSUNG
SNB-5001 I SNB-7001

SNB-5001 kamera 1,3 Mpixz przetwornikiem 1.3" CMOS

- rozdzielczość maks. 1280x1024
- kompresja MJPEG/H.264
- inteligentna analiza obrazu - działanie sabotażowe
- tryb ONVIF

SNB-7001 kamera 3 Mpix z przetwornikiem 1.28" CMOS

- rozdzielczość maks. 2048x1536
- kompresja MJPEG/H.264
- Smart Codec (ROI)
- tryb ONVIF

DO NABYCIA W SIECI DYSTRYBUCJI NA TERENIE **CAŁEGO KRAJU**

www.ssn.net.pl
www.securitysolution.pl

SAMSUNG TECHWIN

Nowe spojrzenie na stare problemy

Wybrane zagadnienia dotyczące projektowania instalacji SAP

Szymon Ratajski

Niniejszy artykuł ma na celu przybliżenie dwóch wybranych zagadnień dotyczących projektowania instalacji SAP – stosowania sygnalizatorów optycznych oraz stosowania puszki PIP-5A o odporności ogniowej E90 w systemach oddymiania

Stosowanie sygnalizatorów optycznych w instalacjach SAP

Stosowanie sygnalizatorów optycznych w instalacjach SAP jest narzucone przez normę PN-EN 54-14:2006 [1], zgodnie z którą w strefach, w których sygnały akustyczne mogą być nieskuteczne (np. w miejscach, w których personel pracuje w ochronnikach słuchu), jako uzupełnienie sygnałów akustycznych należy stosować sygnalizatory optyczne. Norma informuje nas również o tym, że sygnalizatory optyczne nie powinny być stosowane samodzielnie. Niestety obecnie nie istnieją krajowe wymagania dotyczące sposobu rozmieszczania sygnalizatorów optycznych, natężenia oświetlenia generowanego przez sygnalizatory itp. Często nie przykłada się należytej wagi do sposobu rozmieszczenia sygnalizatorów optycznych, montując je po prostu w sąsiedztwie sygnalizatora akustycznego. W wielu przypadkach projektanci nie zwracają uwagi na parametry sygnalizatora. Wejście w życie rozporządzenia [2,3] w pewien sposób zaostrzyło wymagania dotyczące stosowania sygnalizatorów optycznych – każdy pożarowy sygnalizator optyczny musi spełniać wymagania normy PN-EN 54-23:2010 [4]. Oznacza to, że każdy pożarowy sygnalizator optyczny znajdujący się na polskim rynku powinien spełniać wymagania rozporządzenia [2,3], czego potwierdzeniem jest uzyskanie przez wyrób świadectwa dopuszczenia. Weryfikacja spełnienia przez wyrób wymagań nakładanych przez rozporządzenie odbywa się poprzez przeprowadzenie badań wyrobu. Rozporządzenie informuje o wymaganiach ogólnych dotyczących sygnalizatorów oraz wymaganiach szczegółowych.

W punkcie 11.5.1 rozporządzenia [2,3] (wymagania ogólne dotyczące sygnalizatorów optycznych) znajduje się następujący zapis: „Sygnalizatory optyczne powinny spełniać wymagania aprobaty technicznej lub polskiej normy wyrobu. Spełnienie wymagań powinno być potwierdzone stosownym dokumentem”.

W praktyce oznacza to, że sygnalizatory optyczne powinny spełniać wymagania normy [4].

Punkt 11.5.2. rozporządzenia nakłada również wymagania szczegółowe, które stanowią w pewnym stopniu rozszerzenie wymagań określonych przez normę: „Obudowa sygnalizatora i kolor światła powinien być czerwony. Na widzialnej powierzchni sygnalizatora powinien być umieszczony napis «POŻAR» koloru białego”. „Sygnalizator powinien posiadać oznaczenia i opisy w języku polskim”.

Jaki zatem musi być wyrób spełniający wymagania polskiej normy? Polska norma dotycząca pożarowych sygnalizatorów optycznych określa szereg wymagań dotyczących konstrukcji sygnalizatora, materiałów, z których ma być wykonana obudowa, parametrów części optycznej itd. Poniżej przedstawiam główne wymagania normy, istotne dla projektantów, rzeczoznawców i instalatorów.

Podział sygnalizatorów na trzy kategorie:

1) C – urządzenia montowane na suficie,
2) W – urządzenia montowane na ścianie,
3) O – klasa otwarta.

Sposób określania obszaru pokrycia w zależności od kategorii

W przypadku urządzeń kategorii C należy podać maksymalną wysokość montażu 3, 6 lub 9 metrów oraz średnicę (w metrach) walca, w którym sygnalizator osiąga wymagane natężenie światła[1]. Np. „C-3-6” oznacza, że sygnalizator zamontowany na wysokości trzech metrów zapewnia wymagane natężenie światła w walcu o średnicy sześć metrów i wysokości trzy metry.

W przypadku urządzeń kategorii W należy podać maksymalną wysokość montażu urządzenia na ścianie (minimum 2,4 m) oraz szerokość (w metrach) kwadratowego obszaru, w którym wymagane natężenie oświetlenia jest zgodne z normą. Na przykład „W-2,4-4” oznacza, że sygnalizator zamontowany na ścianie na wysokości 2,4 m zapewni wymagane natężenie światła w przestrzeni o wymiarach 2,4×4×4 m.

W przypadku urządzeń kategorii O należy podać charakterystykę pokrycia (dane określające zasięg działania urządzenia).

Aby wyrób spełniał wymagania normy, producent powinien jasno – za pomocą współczynników (w przypadku kategorii C lub W) lub poprzez podanie kształtu bryły – określić obszar pokrycia. Według normy niedopuszczalne jest np. charakteryzowanie obszaru pokrycia poprzez podawanie energii błysku (w przypadku urządzeń wykorzystujących palniki ksenonowe), jasności sygnalizatora (np. ogólnej wartości 2 cd bez odniesienia do kształtu bryły fotometrycznej) itp.

Wymagania dotyczące części optycznej:

– światło koloru białego lub czerwonego,
– częstotliwość sygnału optycznego w zakresie od 0,5 Hz do 2 Hz,
– minimalna jasność sygnalizatora >1 cd[2],
– maksymalna jasność sygnalizatora nie przekraczająca 500 cd.

Wymagania dotyczące oznakowania sygnalizatora (wybrane):

– numer normy (EN 54-23),
– typ środowiska (A – stosowany wewnątrz budynków, B – stosowany na zewnątrz budynków),

1) Zgodnie z normą natężenie wynosi 0,4 lx.

2) Zgodnie z normą co najmniej 1 cd dla 70% punktów pomiarowych (liczba punktów pomiarowych uzależniona jest od kategorii sygnalizatora, jak również obszaru pokrycia – zasięgu działania sygnalizatora).

– kategoria urządzenia (C, W lub O),
– logotyp CNBOP-PIB[3].

Zakończenie się okresu przejściowego normy [4][4] sprawi, że na rynku pożarowych sygnalizatorów optycznych pozostaną urządzenia wysokiej jakości, które – właściwie stosowane – zapewnią dużą skuteczność ostrzegania o zagrożeniu pożarowym. Zgodnie z normą [4] informacje udostępnione wraz z sygnalizatorem (dotyczące między innymi zasięgu działania urządzenia) są znacznym ułatwieniem dla projektantów systemów SAP. Mimo iż na dzień dzisiejszy nie ma wymagań szczegółowych dotyczących projektowania instalacji z wykorzystaniem sygnalizatorów optycznych, projektant może ustalić z rzeczoznawcą SSP, strażakiem, na przykład wymagane natężenie oświetlenia generowanego przez sygnalizatory w czasie alarmu, a następnie, na podstawie danych dostarczonych wraz z sygnalizatorem, wykonać niezbędne obliczenia.

W przypadku ustalania wymagań lub wykonywania obliczeń pomocne mogą okazać się informacje zawarte w amerykańskiej normie NFPA 72, która określa sposób rozmieszczania sygnalizatorów w zależności od kategorii urządzenia (W, C) oraz kształtu i kubatury pomieszczenia. Norma [5] uwzględnia również pomieszczenia o nieregularnych kształtach. W przypadku pomieszczeń o nieregularnych kształtach wymagane natężenie oświetlenia (pokrycie) to 0,0375 lm/sq. ft, czyli – w przeliczeniu na jednostki europejskie – około 0,4 lm/m^2 (0,4 lx).

Sygnalizator SO-Pd13 – pożarowy sygnalizator optyczny zgodny z normą PN-EN 54-23:2010

Sygnalizator SO-Pd13 spełnia wszystkie wymagania normy, co potwierdza pozytywny wynik badań przeprowadzonych w laboratoriach CNBOP-PIB. Mimo zapewnienia znacznego obszaru pokrycia pobór prądu przez sygnalizator nie przekracza 40 mA[5]. SO-Pd13 należy do kategorii O – jest bardziej uniwersalny niż sygnalizatory kategorii C lub W. Urządzenia należące do kategorii O umożliwiają praktycznie dowolny montaż (sufit, ściana, montaż w narożach). Dokładny opis bryły fotometrycznej umożliwia dokładniejsze obliczenie natężenia oświetlenia podczas procesu projektowania niż w przypadku współczynników (urządzenia kategorii C, W).

Sygnalizator SO-Pd13 jest produkowany w trzech wersjach: SO-Pd13/3m; SO-Pd13/6m oraz SO-Pd13/9m. Wersje różnią się od siebie wysokością montażu oraz kształtem bryły fotometrycznej. Wersja 3m została zaprojektowana z myślą o pomieszczeniach biurowych, pomieszczeniach o małej wysokości. Bryła sygnalizatora ma znaczną średnicę. W przypadku wersji 6m i 9m bryła ma mniejszą średnicę, natomiast większą wysokość, co umożliwia stosowanie tych sygnalizatorów w halach przemysłowych oraz innych obiektach o znacznej wysokości.

Sygnalizatory SO-Pd13 mogą być połączone w sieć i pracować synchronicznie lub z efektem fali (efekt analogiczny do znaków drogowych doświetlających zakręty). Synchronizacja odbywa się z wykorzystaniem linii zasilającej, co umożliwia obniżenie kosztów instalacji (nie jest potrzebny dodatkowy przewód).

Sposób podłączania sygnalizatora do systemu SAP

Sygnalizatory powinny być włączane w linie instalacji SAP poprzez puszki o odporności ogniowej, z wbudowanym bezpiecznikiem. Stosowanie puszek lub izolatorów zwarć zapewnia ciągłość linii zasilającej. Jeśli jeden z sygnalizatorów ulegnie uszkodzeniu, puszka lub izolator zwarć odseparuje uszkodzony sygnalizator od linii zasilającej, nie dopuszczając tym samym do powstania zwarcia na linii zasilania.

W przypadku skorzystania z możliwości synchronizacji pomiędzy wyjściem centrali (lub pomocniczego urządzenia uruchamiającego sygnalizatory) a sygnalizatorami należy włączyć moduł filtra FS-1. Zadaniem modułu jest filtrowanie impulsów synchronizacji i niedopuszczenie do tego, by przedostawały się one do zacisków źródła zasilania.

Komputerowe wspomaganie obliczania natężenia oświetlenia

Aby ułatwić projektowanie instalacji, firma W2 udostępniła na swojej stronie internetowej materiały ułatwiające rozmieszczanie sygnalizatorów optycznych – pliki fotometryczne[6] (opisujące charakterystykę pokrycia) oraz filmy instruktażowe, na których pokazany jest sposób wykorzystania dostarczonych plików w programach do komputerowego projektowania oświetlenia. Dzięki stosowaniu programów Calculux Indoor, Dialux itp. rozmieszczanie sygnalizatorów oraz obliczanie natężenia oświetlenia powierzchni roboczych został znacznie przyspieszony.

Projektant może wykonać zadanie na dwa sposoby. Pierwszym jest ręczne rozmieszczenie sygnalizatorów na podkładzie rysunkowym i obliczenie uzyskiwanego natężenia oświetlenia. Drugim – określenie wymaganego natężenia oświetlenia powierzchni obliczeniowej (np. w nawiązaniu do wymagań normy [5]), a następnie skorzystanie z opcji automatycznego rozmieszczenia sygnalizatorów. Program automatycznie rozmieści sygnalizatory oraz przedstawi wyniki w postaci tzw. isoluxów (krzywych łączących punkty o jednakowym natężeniu oświetlenia). Warto wspomnieć również o tym, że istnieje możliwość wykorzystania podkładu architektonicznego.

Stosowanie puszki PIP-5A w systemach oddymiania

Puszka PIP-5A jest nową puszką o odporności ogniowej E90 w ofercie firmy W2. PIP-5A umożliwia rozgałęzianie przewodów pięciożyłowych o maksymalnych przekrojach 4 mm^2. Głównym przeznaczeniem puszki jest podłączanie przewodów zasilających oraz synchronizujących siłowników klap oddymiających. Jej konstrukcja umożliwia podłączenie

3) Zgodnie z art. 7 ust. 7 ustawy o ochronie przeciwpożarowej z dnia 24 sierpnia 1991 r. „dopuszczony wyrób podlega oznakowaniu przez producenta znakiem jednostki (…) która wydała dopuszczenie”.

4) Okres przejściowy zakończy się 1 marca 2013 r.

5) W wersji SO-Pd13/3m oraz SO-Pd13/6m.

6) Pliki fotometryczne w standardowym formacie IES.

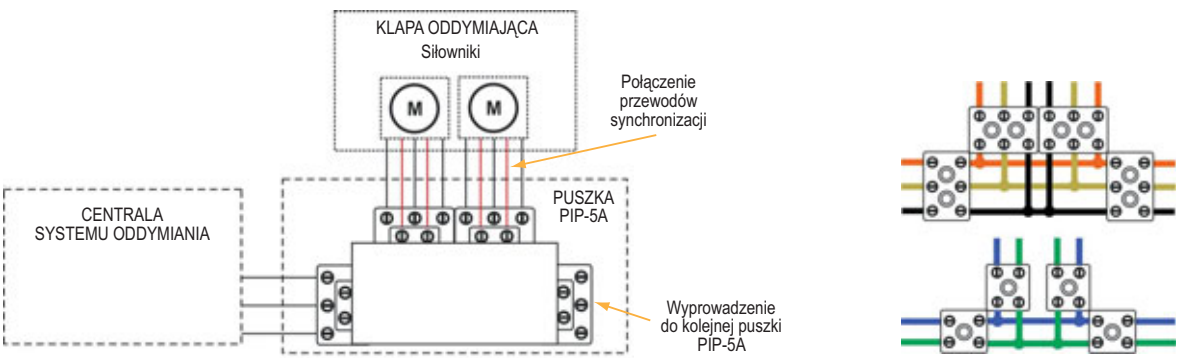
praktycznie dowolnej liczby siłowników. Jedynym ograniczeniem jest przekrój przewodu zasilającego oraz obciążalność prądowa wynosząca 16 A.

Budowa puszki instalacyjnej PIP-5A

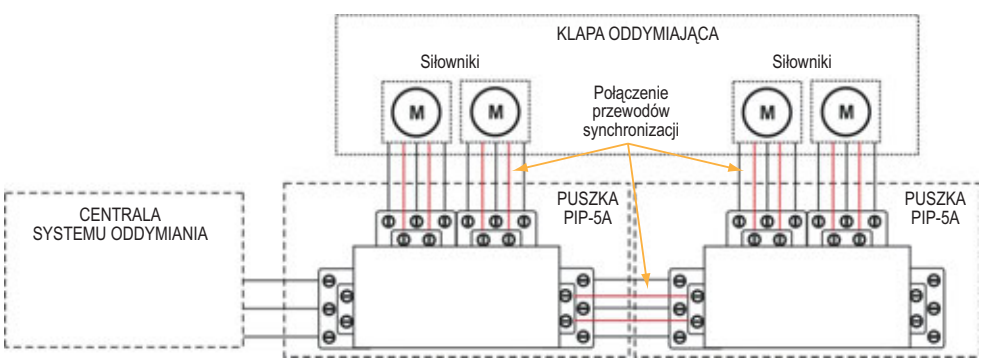
Puszka PIP-5A jest wykonana z blachy stalowej malowanej proszkowo. Wewnątrz niej znajdują się kostki ceramiczne zapewniające odpowiednią odporność na ogień. Kostki ułożone są piętrowo w celu maksymalnego uproszczenia podłączenia przewodów. Pomiędzy kostkami (pod metalowymi osłonami) znajduje się ognioodporne połączenie. Przewody połączeniowe można wprowadzać do wnętrza puszki zarówno przez przepusty od strony podłoża, jak i przepusty umieszczone w bocznych ścianach puszki. Maksymalna średnica przewodu, który można wprowadzić do puszki, wynosi 16 mm.

Pojedyncza puszka zastosowana w systemie oddymiania umożliwia podłączenie trzech niezależnych siłowników (trzy klapy z pojedynczym napędem) lub jednej klapy oddymiającej z dwoma siłownikami oraz modułem końca linii (np. firmy D+H).

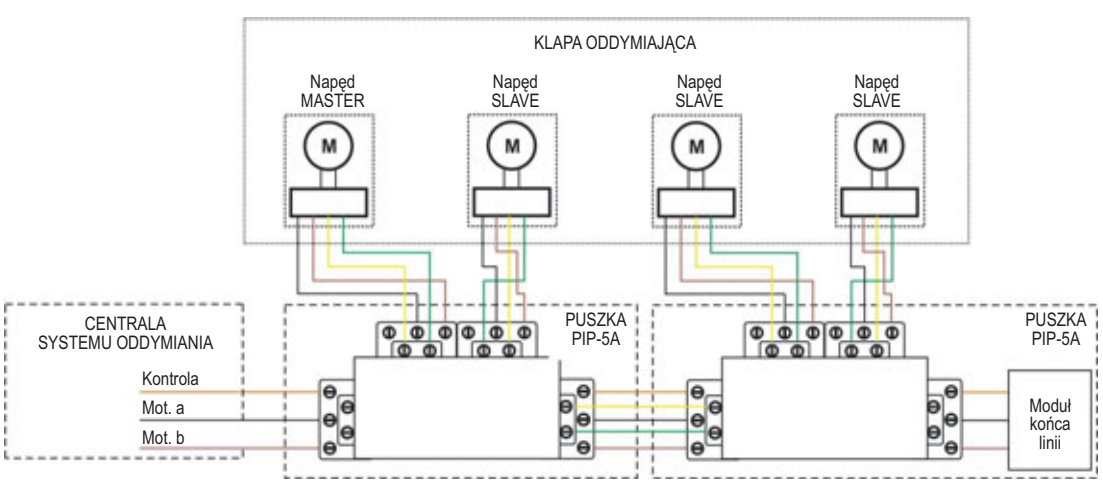
Jak powszechnie wiadomo, w systemach oddymiania w dużych obiektach przemysłowych często wykorzystywane są klapy posiadające więcej niż dwa siłowniki. W przypadku



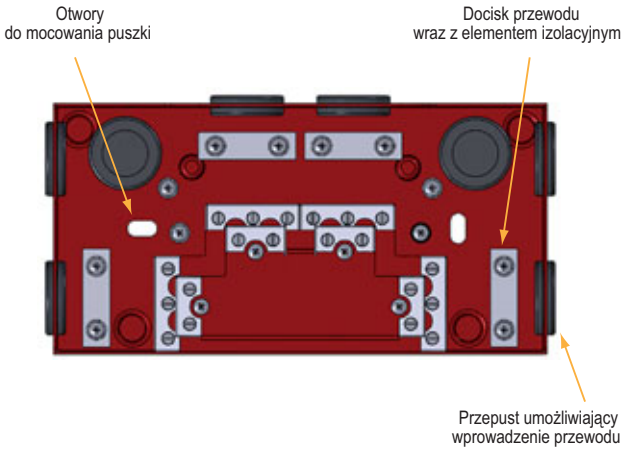
Rys. 1. Schemat podłączenia dwóch siłowników klap oddymiających do puszki PIP-5A



Rys. 2. Schemat podłączenia większej liczby siłowników do puszek PIP-5A



Rys. 3. Schemat podłączenia większej liczby siłowników do puszek PIP-5A z wykorzystaniem systemu oddymiania firmy D+H



Rys. 4. Widok puszki PIP-5A po zdjęciu pokrywy

większej liczby napędów w obrębie jednej klapy konieczne jest łączenie kilku par przewodów synchronizacyjnych. Puszka PIP-5A posiada wyjście przelotowe, co umożliwia zastosowanie dowolnej liczby siłowników.

W celu zapewnienia kontroli ciągłości linii pomiędzy napędami oraz pomiędzy napędami a centralą systemu oddymiania konieczne jest zastosowanie modułów końca linii (np. systemów oddymiania firmy D+H).

Szymon Ratajski
W2

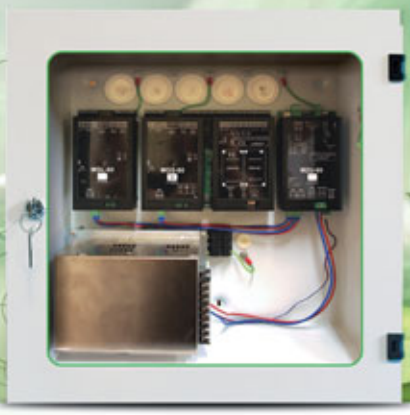
Literatura

1. PN-EN 54-14:2006 *Systemy sygnalizacji pożarowej. Część 14. Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji.*
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. z 2007 r., nr 143, poz. 1002).
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2010 r. zmieniające rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. z 2010 r., nr 85, poz. 553).
4. PN-EN 54-23:2010 *Systemy sygnalizacji pożarowej. Część 23. Pożarowe urządzenia alarmowe. Sygnalizatory optyczne.*
5. NFPA 72 National Fire Alarm Code.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

UCS 6000

UNIWERSALNA CENTRALA STERUJĄCA



WEJŚCIA	UCS 6000	WYJŚCIA
• **praca samodzielna** czujki przyciski oddymiania		• **sterowanie 24 V** klapy z siłownikami dwukierunkowymi 2 lub 3 przewodowymi klapy z siłownikami ze sprężyną sterowanie elektrotrzymaczami itp.
• **praca jako element adresowalny w systemie POLON 4000**		
czujnik deszczu i/lub wiatru przyciski przewietrzające	• ponad 20 wersji • niemal dowolna konfiguracja • dedykowany program konfiguracyjny • 5 lat gwarancji	• **sterowanie 230 V~** wentylatory, kurtyny itp.

WSPÓŁPRACA Z CENTRALAMI SYGNALIZACJI POŻAROWEJ WSZYSTKICH PRODUCENTÓW

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

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

Prawidłowy dobór i montaż czujek w SSWiN

Michał Konarski

Czujki są najważniejszymi elementami systemu alarmowego. Mają zasadniczy wpływ na jego skuteczność i niezawodność. Ich właściwy dobór oraz umiejscowienie zależy od wielu czynników, dlatego te czynności wymagają doświadczenia zawodowego oraz zrozumienia zasady działania stosowanych urządzeń. Rozmaite wytyczne projektowe oraz tzw. „kodeksy praktyki" mogą zawierać jedynie ogólne, podstawowe zasady doboru urządzeń i ich miejsca instalacji. Nie skupiają się one na konkretnych rozwiązaniach technicznych, dlatego podstawowym punktem odniesienia staje się dokumentacja opracowana przez producenta danego urządzenia. Powinna ona zawierać zbiór informacji niezbędnych do zapewnienia prawidłowych warunków pracy urządzenia

Projektowanie systemu alarmowego powinno rozpoczynać się od ustalenia wymagań formalnych, jakie musi spełniać cała instalacja – ze względu na oczekiwania inwestora, uwarunkowania formalno-prawne lub te, które zostają narzucone przez ubezpieczyciela. Obecnie w całej Europie coraz więcej zainteresowanych powołuje się na normy branżowe serii EN50131. Ten zestaw norm określa wymagania wobec całego systemu alarmowego – od wymagań systemowych, poprzez wymagania dotyczące poszczególnych komponentów systemu (w tym czujek), aż po zalecenia dla projektanta i wykonawcy instalacji. Normy z serii EN50131 zawierają czterostopniową klasyfikację systemów alarmowych od stopnia 1 (Grade 1), aż po stopień 4 (Grade 4). Im wyższy stopień zabezpieczenia, tym lepsza skuteczność działania poszczególnych urządzeń i jakość zabezpieczenia przed nieupoważnioną ingerencją (sabotażem). Stojąc przed zadaniem zaprojektowania systemu zabezpieczenia w odpowiednim stopniu, należy pamiętać o ogólnej zasadzie mówiącej o tym, że komponent spełniający wymagania normy właściwe dla najniższego stopnia ochrony narzuci stopień ochrony, jaką zapewni cała instalacja (lub jej część, jeżeli jest wydzielona), będąc jej „najsłabszym ogniwem". Dlatego do wykonania instalacji spełniającej wymagania normy EN50131 dla odpowiedniego stopnia zabezpieczenia należy wybrać elementy spełniające wymagania dotyczące tego lub wyższego stopnia. Oczywiście dotyczy to również czujek.

Fot. 1. Firma SATEL proponuje swoim klientom czujki magnetyczne, zarówno do montażu powierzchniowego, jak i wpuszczanego. Nowością w ofercie są również czujki ze wzmocnioną, hermetyczną metalową obudową, doskonale sprawdzające się w miejscach szczególnie podatnych na mechaniczne uszkodzenia – np. przy bramach garażowych.

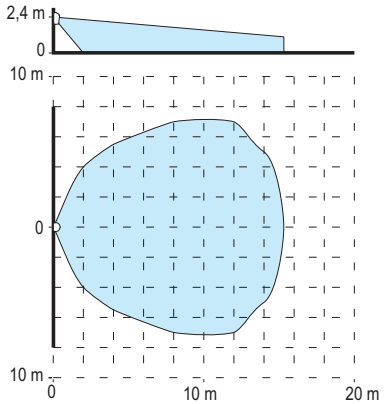
Fot. 2. Czujki ruchu służą do wykrywania obecności włamywacza na obszarze chronionym. Firma SATEL oferuje rozmaite czujki ruchu różniące się designem, wielkością i konstrukcją, co umożliwia dopasowanie ich do konkretnych systemów i wymagań użytkowników

Wybór właściwego rodzaju czujek w zależności od zagrożenia jest jedną z czynności wymagających wyobraźni, doświadczenia oraz wiedzy technicznej. Na tym etapie należy wziąć pod uwagę cały szereg czynników: od położenia chronionego obiektu w terenie po sposób wykorzystywania go na co dzień. Jednak poza specyficznymi przypadkami, wymagającymi zastosowania bardzo nietypowych i niejednokrotnie indywidualnie opracowanych rozwiązań, większość systemów sygnalizacji włamania wykorzystuje typowe i powszechnie dostępne rodzaje czujek.

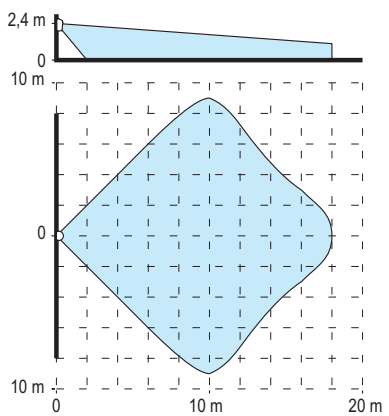
Nawet najprostsze czujki, takie jak kontaktronowe czujki otwarcia drzwi i okien zwane popularnie kontaktronami, wymagają znajomości kilku „sztuczek", jeżeli mają bezawaryjnie pracować przez wiele lat.

Przede wszystkim, należy umieścić elementy czujki w miejscu, w którym nie będą narażone na odrywanie i zgniatanie. Dotyczy to przede wszystkim okien wyposażonych w zawiasy umożliwiające ich uchylanie. Należy także upewnić się, że w pobliżu miejsca montażu czujki nie ma stalowych elementów ramy okiennej. Z biegiem czasu mogłyby one ulec namagnesowaniu i spowodować nieprawidłową pracę czujki (brak reakcji na otwieranie okna).

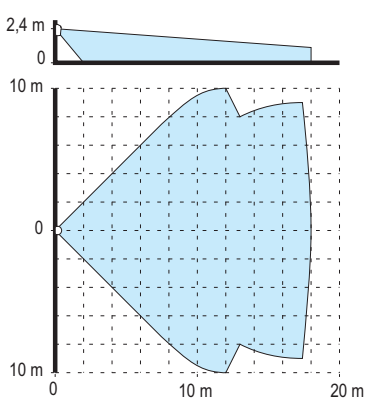
Czujki kontaktronowe mogą także być wrażliwe na mocne udary mechaniczne podłoża. Jeżeli rama drzwi lub okna, na której zamontowana ma być czujka, jest narażona na



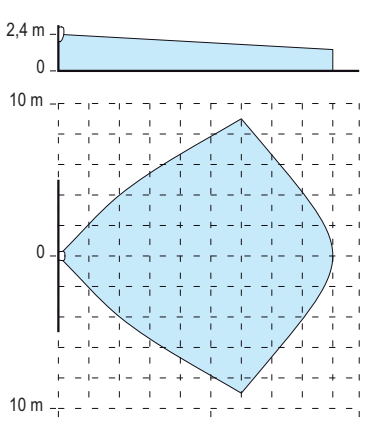
Rys. 1. Obszar wykrywania ruchu przez czujkę AQUA Plus



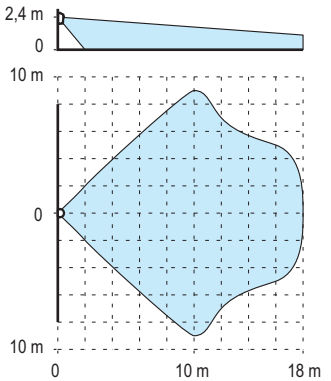
Rys. 2. Obszar wykrywania ruchu przez czujkę GRAPHITE



Rys. 3 Obszar wykrywania ruchu przez czujkę AMBER



Rys. 4. Obszar wykrywania ruchu przez czujkę IVORY



Rys. 5. Obszar wykrywania ruchu przez czujkę SILVER

uderzanie ciężkim skrzydłem, warto zastosować dodatkową elastyczną podkładkę, np. cienką warstwę pianki bądź mikrogumy, która powinna skutecznie stłumić mocne drgania mogące doprowadzić do uszkodzenia szklanego elementu kontaktronu.

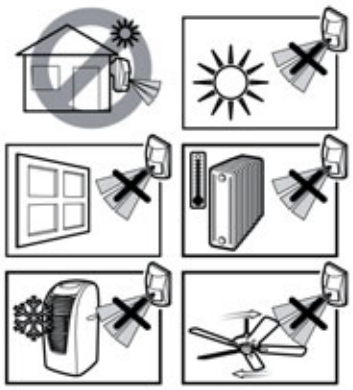
W przypadku wykonywania instalacji zabezpieczającej w stopniu 3 według normy EN50131 może pojawić się konieczność skorzystania z czujek magnetycznych zdolnych do wykrycia próby ich neutralizacji przez przyłożenie „obcego" magnesu. Takie urządzenia mogą wymagać bardziej precyzyjnego niż zwykłe czujki umiejscowienia magnesu względem sensora.

Równie dużą popularnością wśród instalatorów cieszą się pasywne czujki ruchu typu PIR, które są łatwe w montażu, skuteczne i niezawodne.

Należy jednak pamiętać, że tylko właściwie zamontowane czujki PIR zapewnią niekłopotliwą eksploatację oraz skuteczność działania. Chodzi tu zarówno o lokalizację, jak i sposób przyłączenia.

W tym miejscu warto być może przypomnieć podstawowe zasady działania tego typu urządzeń. Wykorzystują one

Rys. 6. Intruz poruszający się w pomieszczeniu emituje promieniowanie z zakresu podczerwieni, które jest odbierane przez czujkę z wykorzystaniem przestrzennego układu wiązek optycznych. Pyroelement zamienia energię promieniowania na sygnał elektryczny analizowany w procesorze sygnałowym, który jest odpowiedzialny za podanie informacji o alarmie.



Rys. 7. Praktyczne wskazówki dotyczące miejsc montażu, które mogą przyczyniać się do niepoprawnego działania czujek ruchu typu PIR

pyrosensor, czyli półprzewodnikowy element przetwarzający natężenie promieniowania podczerwonego na sygnał elektryczny. To promieniowanie podczerwone dociera do pyrosensora za pośrednictwem układu optycznego: soczewek Fresnela lub zwierciadeł, skupiających na powierzchni sensora obrazy fragmentów przestrzeni znajdujących się w polu widzenia czujki. Układ elektroniczny czujki rejestruje szybkie zmiany oświetlenia jej promieniowaniem podczerwonym. Ze względu na zasadę działania całego układu optycznego wraz z sensorem czujki typu PIR są najskuteczniejsze w wykrywaniu ruchu człowieka w kierunku poprzecznym do osi czujki.

Z tego powodu czujka powinna być zamontowana w takim miejscu, aby kierunek ruchu z miejsc najbardziej narażonych na wtargnięcie (drzwi, okna) był prostopadły do osi czujki. Czujki PIR z typową optyką najsłabiej wykrywają ruch wzdłuż osi czujki. Dlatego też jednym z kardynalnych błędów jest umieszczanie ich na wprost przewidywanego miejsca wtargnięcia, na przykład naprzeciw okna.

Oprócz nieoptymalnej skuteczności detekcji takie ustawienie stwarza jeszcze jeden problem. Silne promieniowanie słoneczne, nawet po przeniknięciu przez szybę okna, może zawierać dużo takich składowych podczerwieni, które są rejestrowane przez sensor czujki. Jeśli dodamy do tego ruch przesuwających się po niebie chmur, które mogą przesłaniać i odsłaniać poszczególne fragmenty pola widzenia czujki, powstaje potencjalne źródło trudnych do identyfikacji fałszywych alarmów. Wybierając optymalną lokalizację dla czujek PIR, należy wziąć to pod uwagę.

Innymi potencjalnymi źródłami fałszywych alarmów mogą być wszelkiego rodzaju źródła ruchu masy powietrza o temperaturze innej niż temperatura otoczenia czujki, takie jak na przykład kratki wentylacyjne, wyloty klimatyzatorów czy zwykłe grzejniki. Projektując system, należy uwzględnić te elementy i wybrać takie położenie czujki, które nie narazi jej na oddziaływanie tych czynników.

Tam, gdzie występują wspomniane wcześniej utrudnienia , projektanci i instalatorzy chętnie zastępują czujki PIR urządzeniami dualnymi, łączącymi technologię wykorzystującą podczerwień z detektorem mikrofalowym.

Główną zaletą takiego połączenia jest podwyższona odporność na zakłócenia pochodzące ze wspomnianych źródeł. Typowe czujki dualne alarmują dopiero wtedy, gdy ruch zostanie wykryty za pomocą obu zupełnie niezależnych metod detekcji.

Detektor mikrofalowy wykrywający fale odbijające się od poruszających się przeszkód ignoruje ruch masy powietrza czy bezpośrednie oświetlanie czujki, np. światłem słonecznym. Instalując tego typu urządzenia, trzeba jednak pamiętać, że promieniowanie mikrofalowe jest w stanie przenikać przez cienkie ścianki, np. gipsowo-kartonowe, a więc niewłaściwie wyregulowana czujka może rejestrować (przynajmniej w torze mikrofalowym) ruch zza ściany. Zaskakujące dla niektórych

Fot. 3. Czujki dualne (COBALT, SILVER) warto stosować między innymi w nieogrzewanych garażach, pomieszczeniach gospodarczych, salonach wyposażonych w kominek

Rys. 8. Intruz poruszający się w pomieszczeniu emituje promieniowanie z zakresu podczerwieni, które odbierane jest przez tor podczerwieni czujki z wykorzystaniem przestrzennego układu wiązek optycznych. Jednocześnie ruch ten wykrywany jest przez tor mikrofalowy dzięki wykorzystaniu efektu Dopplera. Oba sygnały, z pyroelementu zamieniającego energię promieniowania na sygnał elektryczny, oraz z toru mikrofalowego trafiają do procesora sygnałowego, który na podstawie algorytmu opracowanego w firmie SATEL podejmuje decyzję o sygnalizacji alarmu.

Fot. 4. Akustyczne czujki zbicia szyby INDIGO są przeznaczone do ochrony obwodowej pomieszczeń zagrożonych włamaniem poprzez rozbicie szyby w oknach lub drzwiach. Dzięki cyfrowej, dwutorowej analizie sygnału są w wysokim stopniu skuteczne i niezawodne. System cyfrowej detekcji wykorzystujący dwie częstotliwości zapewnia skuteczne działanie i odporność na fałszywe zadziałania spowodowane hałasem.

może być też wykrywanie ruchu bezpośrednio za czujką. Wynika to z charakterystyki anten stanowiących element takiej czujki dualnej.

Warto pamiętać także o typowych źródłach sygnału pobudzającego tor mikrofalowy – lampy jarzeniowe lub rury kanalizacyjne umieszczone blisko czujki mogą samoczynnie uruchamiać tor mikrofal, powodując, że cała czujka staje się równie podatna na zjawiska zakłócające jak zwykła czujka PIR.

Do popularnych czujek stosowanych w systemach antywłamaniowych należą także akustyczne czujki wykrywające zbicie szyby. Rolą tych urządzeń jest wykrywanie charakterystycznych dźwięków towarzyszących rozbijaniu szkła.

W zależności od konstrukcji czujki takie mogą reagować na różne parametry dźwięku. Czujki wyższej jakości analizują więcej niż jedną częstotliwość, dzięki czemu są bardziej odporne na typowe hałasy. Z reguły lepiej jednak unikać stosowania czujek akustycznych w pomieszczeniach narażonych na duże natężenie hałasu, np. w halach produkcyjnych czy w okolicach węzłów komunikacyjnych (transport drogowy, kolejowy czy lotniska).

Już na tych kilku przykładach widać, jak wiele czynników należy uwzględnić przy doborze czujek. Wiadomo, że nic nie zastąpi doświadczenia, ale można w miarę szybko i „bezboleśnie” zdobyć cenną wiedzę. W tym celu warto skorzystać ze specjalistycznych kursów, na przykład w ramach Akademii SATEL, które dają wiedzę teoretyczną i dzięki którym można dowiedzieć się o typowych problemach pojawiających się w praktyce, a także o nowoczesnych rozwiązaniach.

Michał Konarski
SATEL

Systemy alarmowe **Satel**

czujki ruchu: **AMBER, AQUA, GRAPHITE, SILVER, IVORY**

Połączenie pasji i zaawansowanej inżynierii pozwoliło firmie SATEL na zaprojektowanie szerokiej gamy czujek - od prostej i niezawodnej czujki **AMBER**, przez czujkę **IVORY** będącą owocem współpracy polsko-japońskiej, po zaawansowaną czujkę **SILVER** zapewniającą najwyższej klasy bezpieczeństwo. Nieustanne dążenie do innowacji zaowocowało m.in. takimi unikalnymi rozwiązaniami jak energooszczędne oświetlenie awaryjne LED zintegrowane z czujką ruchu w urządzeniu **AQUA Luna**.

Wszystkie czujki w ofercie firmy SATEL łączy niezawodność i korzystny stosunek możliwości do ceny - dlatego są tak chętnie wybierane przez profesjonalistów branży zabezpieczeń.

Skuteczna detekcja

- ponad 20 lat doświadczenia
- kontrola jakości na każdym etapie produkcji
- 100% przetestowanych urządzeń

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

JABLOTRON SELF SERVICE

Więcej niż zdalne zarządzanie systemem alarmowym

Krzysztof Bereza

Wraz z pojawieniem się na rynku nowego systemu Jablotron Alarms serii JA-100 producent wprowadził nowe narzędzie do zdalnego zarządzania i monitorowania – JABLOTRON SELF SERVICE. Serwis internetowy umożliwia użytkownikowi samodzielną obsługę systemu i oferuje wiele użytecznych funkcji, które są przydatne dla instalatora. Dostępny jest dla wszystkich urządzeń marki Jablotron (PROFI, OASIS, JABLOTRON-100, AZOR, Autoalarmy ATHOS)

Jablotron Cloud – operacje w chmurze

Serwis wykorzystuje chmurę danych i udostępnia wszystkie usługi bez względu na aktualną lokalizację użytkownika. Instalator uruchamia usługę, rejestrując urządzenie w serwisie przez podanie jego numeru seryjnego i zdefiniowanie toru transmisji (LAN lub GSM). Po weryfikacji poprawności parametrów identyfikacyjnych operator systemu wysyła do urządzenia parametry konfiguracyjne połączenia z chmurą Jablotron i usługa zostaje aktywowana. Instalator nie musi posiadać jakiejkolwiek wiedzy z dziedziny komunikacji sieciowej, jego rola sprowadza się do wypełnienia formularza i przetestowania działania usługi.

Przepływ danych w obrębie serwisu dostępnego dla użytkowników jest zagwarantowany dzięki wykorzystaniu trzech torów transmisji: GSM-SMS, GPRS, LAN. W przypadku braku usługi sieciowej LAN lub GPRS urządzenie automatycznie przełącza się na zapasowy tor SMS. Jeśli urządzenie nie posiada komunikatora LAN, do transmisji służy przede wszystkim GPRS. Do prawidłowego działania usługi konieczny jest aktywny pakiet transmisji danych na karcie SIM z limitem około 10 MB na miesiąc. Jablotron Alarms uruchomił na terenie Polski obsługę GSM-SMS i tym samym koszty transmisji SMS naliczane są według taryfy krajowej.

Chmura Jablotron także dla stacji monitorowania

Zastosowanie technologii operowania w chmurze umożliwia operatorom stacji monitorującej zdalne administrowanie systemami oraz parametrami komunikacji ze stacją. W praktyce oznacza to możliwość uruchomienia usługi monitorowania bez wizyty technika w obiekcie, co znacząco wpływa na koszty działalności firmy.

Prosta komunikacja z użytkownikiem

Serwis umożliwia szybką komunikację z użytkownikiem systemu poprzez wysłanie wiadomości SMS. Wiadomości wysyłane są bezpłatnie, bezpośrednio z serwisu, na przykład w celu poinformowania o zbliżającym się terminie konserwacji systemu.

Wszystko dla instalatora w jednym miejscu

W serwisie nie mogło zabraknąć panelu instalatora. Instalator może znaleźć w nim aktualne oprogramowanie, cennik i instrukcje, a także materiały marketingowe oraz informacje o nowościach i aktualnych szkoleniach.

Najbardziej użyteczna jest jednak możliwość zarządzania kontami klientów obecnych i potencjalnych oraz przygotowania ofert. Oferta może być przystosowana do indywidualnych potrzeb i zawierać logotyp oraz dane kontaktowe firmy instalacyjnej. Istnieje możliwość tworzenia rozbudowanych ofert wariantowych. Tworzy się opis funkcjonalny systemu, dołącza się także fotografie urządzeń oraz referencje firmy. Serwis spełnia funkcje programu CRM. Instalator uzyskuje wgląd do historii kontaktów z klientem.

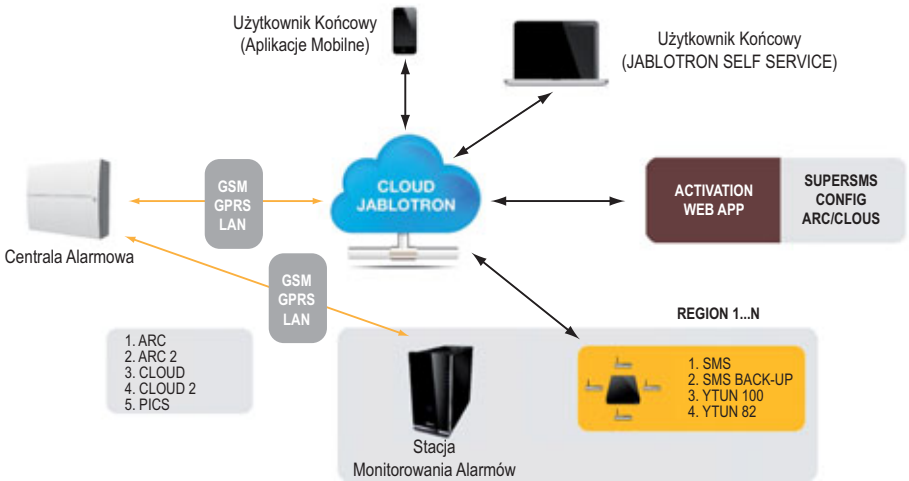
To nie tylko zdalna klawiatura

Usługa JABLOTRON SELF SERVICE pozwala użytkownikowi na zdalną komunikację z systemem alarmowym za pośrednictwem Internetu, za pomocą dowolnego urządzenia, które dysponuje przeglądarką stron WWW. Wkrótce dostępne będą aplikacje dostosowane do systemów operacyjnych iOS, Android oraz RIM.

Po zalogowaniu się w oknie głównym użytkownik widzi aktualny status wszystkich swoich urządzeń i może szybko załączać system w dozór. Po wybraniu urządzenia ma do dyspozycji szereg paneli umożliwiających pełne sterowanie oraz podgląd ostatnich stu zdarzeń wraz z fotografiami z czujek wyposażonych w kamerę cyfrową.

Można sterować systemem za pomocą przycisków z nazwami stref na ekranie głównym i wyjść PG lub za pomocą klawiatury wirtualnej, która jest lustrzanym odbiciem dowolnej klawiatury w systemie.

Fot. 1. Ekran główny panelu użytkownika



Rys. 1. Schemat architektury działania usług w chmurze

Powiadomienie użytkownika jest darmowe

Raporty o alarmach, usterkach, czy uzbrojeniu – SMS-owe oraz wysyłane za pośrednictwem poczty elektronicznej – docierają do użytkownika bezpośrednio z chmury Jablotron. Użytkownik nie płaci za odbierane SMS-y. W przypadku wykorzystania sieci LAN w obiekcie jako podstawowego toru transmisji monitorowanie jest całkowicie darmowe. Darmowe są też powiadomienia o statusie wyjść programowalnych.

Wideoweryfikacja w chmurze

Serwis umożliwia także stały dostęp do wszystkich fotografii wykonanych przez czujki z aparatem fotograficznym (JA-84P, JA-120PC, JA-160PC). Zdjęcia można wykonywać także na polecenie generowane bezpośrednio w panelu użytkownika. Serwis www.jablonet.net automatycznie wysyła do użytkownika wiadomość SMS z linkiem do fotografii oraz wiadomość e-mail z załączonym zdjęciem w formacie JPG. Zdjęcia w chmurze są dostępne w rozdzielczości 320×240 pikseli, natomiast pełna rozdzielczość VGA jest dostępna w wewnętrznej pamięci czujki.

Fot. 2. Panel użytkownika – wirtualna klawiatura

Cała historia zdarzeń dostępna online

Wszystkie zdarzenia zapisane w centrali alarmowej (do siedmiu milionów zdarzeń w przypadku centrali JA-106K) są dostępne online w panelu użytkownika. Istnieje możliwość określenia przedziału czasowego i wygenerowania dokumentu z historią w postaci pliku PDF lub XLS.

Bezprzewodowa klawiatura także w tablecie

Stale powiększająca się grupa użytkowników mobilnych platform komunikacyjnych z pewnością doceni funkcje nowego serwisu JABLOTRON. Daje on możliwość pełnego sterowania systemem z każdego miejsca na świecie. W przypadku wykorzystania transmisji przez sieć LAN użytkownik ma do dyspozycji kolejny bezprzewodowy manipulator w swoim systemie, bez ponoszenia dodatkowych kosztów.

Dopiero najnowszy system JABLOTRON-100 umożliwia pełne wykorzystanie możliwości serwisu jablonet.net. Fabryczne wyposażenie centrali alarmowej w komunikator GSM i LAN pozwala na szybkie uruchomienie usługi i bezpłatną komunikację online. Centrala obsługuje do trzydziestu dwóch wyjść programowalnych, co przy wykorzystaniu timerów i funkcji logicznych umożliwia stworzenie automatyki domowej dostępnej online za pośrednictwem jablonet.net

Przedstawiając syntetycznie zalety nowego serwisu *www.jablonet.net*, można wyróżnić zalety niespotykane u innych producentów: proste uruchomienie usługi przez instalatora, bezpłatne powiadomienie użytkownika SMS -em i pocztą elektroniczną, uruchomienie monitoringu przez stację monitorującą (bez wizyty technika w obiekcie), narzędzie instalatorskie CRM online do zarządzania kontaktami i usługami (wszystkie kosztorysy dostępne online), zaawansowane narzędzie do kosztorysowania. Realizacja usług Jablotron w chmurze pozwala rozszerzać obsługę serwisową o nowe funkcje.

Krzysztof Bereza
DPK System

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 system dostępu i rejestracji dla przedszkoli **SDR Junior.**

PowerG®
Technology for life

zapomnij wszystko, co wiesz
o bezprzewodowych systemach alarmowych

Mariusz Banach

Nieustannie narastające tempo wdrażania technologii bezprzewodowej powoduje coraz większe zagęszczenie przesyłu danych w kanałach komunikacji. Nie bez znaczenia jest także zwiększająca się liczba nadajników działających na tych samych częstotliwościach. W rezultacie skuteczność bezprzewodowych systemów bezpieczeństwa może być zmniejszona z powodu kolizji sygnałów, zakłóceń, których źródłem mogą być warunki panujące w obiekcie, oraz blokady poszczególnych kanałów radiowych, co jeszcze dziesięć lat temu nie stanowiło takiego problemu. Obecnie musimy wdrożyć technologie, które przez kolejną dekadę pozwolą na swobodę rozbudowy i bezpieczne użytkowanie bezprzewodowych systemów bezpieczeństwa. Normy dotyczące bezpieczeństwa są coraz bardziej rygorystyczne. Odporność na zakłócenia oraz docieranie sygnału radiowego do odbiornika musi być zagwarantowane. Ważne jest także lepsze szyfrowanie danych, które mogą interesować potencjalnego włamywacza

Firma Visonic od wielu lat udoskonala bezprzewodowe systemy alarmowe i opracowuje kolejne technologie przesyłu informacji, ochrony sygnału, detekcji sygnałów alarmowych. Na rynku polskim są już dostępne urządzenia wykorzystujące najnowszą technologię PowerG, która stała się podstawą do tworzenia nowych generacji urządzeń bezprzewodowych.

PowerG wykorzystuje rozwiązania pierwotnie przeznaczone dla wojska, między innymi Frequency Hopping Spread Spectrum (FHSS), czyli według definicji nadawanie z przełączaniem fali nośnej między różnymi kanałami w dostępnym paśmie. Mechanizm FHSS umożliwia jednoczesną pracę wielu urządzeń w tym samym paśmie częstotliwości. W tym samym czasie nadajnik i odbiornik zmieniają w zadanej sekwencji częstotliwość nośną. Zapewnia to równomierne rozłożenie sygnału i uodparnia system na próby zakłócenia. FHSS wywodzi się z wojskowej technologii radiowej, która została zastosowana w latach 50. w radiowym sterowaniu torped. Zasadę działania FHSS możemy przyrównać do jazdy samochodem wielopasmową autostradą – jeżeli na jednym lub kilku pasach jest korek, wypadek lub są roboty drogowe, zmieniamy pas ruchu na dostępny i kontynuujemy podróż bez żadnych zakłóceń, bez opóźnień. Dzięki FHSS technologia PowerG eliminuje przypadkowe i zamierzone zakłócenia i umożliwia zastosowanie urządzeń radiowych tam, gdzie kiedyś było to wykluczone.

Time Division Multiple Access (TDMA) to technologia, która umożliwia przyznawanie dostępu do kanału wielu użytkownikom. Kanał transmisji jest dostępny dla poszczególnych użytkowników w odpowiednim, przydzielonym oknie czasowym. Dzięki temu można bezkolizyjnie korzystać z danego kanału. Wśród zalet TDMA można wymienić:

– dynamiczny przydział pasma,
– oszczędzanie energii przez urządzenie, które, znając czas kolejnej transmisji, może lepiej gospodarować poborem prądu,
– zmniejszenie nadmiarowości transmisji poszczególnych sygnałów.

Technologię TDMA wykorzystują m.in. takie systemy telekomunikacyjne jak GSM, UMTS, WIMAX, Bluetooth oraz TETRA. Gdyby wiele osób chciało równocześnie powiedzieć coś jakiejś osobie, niezsynchronizowana komunikacja utrudniłaby dotarcie przekazu do odbiorcy. Korzystanie z TDMA pozwala na wprowadzenie określonego z góry porządku transmisji – jeden nadawca mówi, a pozostali milczą. Dzięki temu do odbiorcy dociera w pełni zrozumiała informacja przy wykorzystaniu mniejszych zasobów.

PowerG korzysta z szyfrowania danych w standardzie Advanced Encryption Standard (AES). Jest to symetryczny szyfr blokowy bazujący na permutacji macierzowej, czyli zamianie

Fot. 1. Centrala Visonic PowerMaster-30 wykorzystująca technologię PowerG

Fot. 2. Centrala Visonic PowerMaster-10 wykorzystująca technologię PowerG

kolumn i wierszy. Wykorzystuje on 128-bitowe bloki wejściowe, a długość klucza może być 128-bitowa (10 rund szyfrujących), 192-bitowa (12 rund szyfrujących) i 256-bitowa (14 rund szyfrujących). Szyfrowanie AES jest powszechnie stosowane w sieciach Wi-Fi czy połączeniach w prywatnych sieciach wirtualnych (VPN)

Do głównych zalet PowerG możemy zaliczyć:

1) Energooszczędność i „inteligencję" urządzeń. Każde urządzenie stale mierzy jakość komunikacji i automatycznie ustawia pobór energii tak, aby zapewnić niezawodną łączność z odbiornikiem, pełną, zsynchronizowaną, dwukierunkową komunikację przy minimalnej zajętości kanału. Żywotność baterii w urządzeniach wykorzystujących technologię PowerG może wynosić nawet osiem lat.
2) Bezpieczeństwo przesyłu informacji. Szyfrowanie AES maksymalnie utrudnia osobom niepowołanym podsłuchanie i zastąpienie oryginalnej informacji podstawioną kopią.
3) Niezawodność łącza radiowego i jego zasięg. Sygnały dynamicznie zmieniające kanały mają dużo większą szansę na eliminację coraz liczniejszych zakłóceń i osiągnięcie większego zasięgu. Umożliwia to zastosowanie systemów radiowych w większych, przemysłowych obiektach o większym stopniu rozproszenia, w instalacjach, w których standardowe rozwiązania bezprzewodowe okazują się niewystarczające.
4) Większa przepustowość. Dzięki PowerG przepustowość kanałów transmisyjnych jest znacznie wyższa, więc można przesyłać dużą ilość danych. Umożliwia to wykorzystanie systemu do takich zadań jak transmisja audio i wideo.
5) Zapewnienie dwukierunkowej łączności z urządzeniami, zdalne pobieranie i wysyłanie danych. Mając dostęp do centrali alarmowej, można zdalnie zmienić ustawienia poszczególnych czujek, pilotów i innych urządzeń peryferyjnych. Dodatkowe narzędzie, jakim jest serwer IPMP, pozwala na zdalne serwisowanie urządzeń, dodawanie lub usuwanie czujek, pełną diagnostykę w trybie on-line.
6) Dodatkowe funkcje dla użytkowników. W najbliższej przyszłości technologia PowerG umożliwi między innymi weryfikację wizyjną stanu systemu, dynamiczny przydział zasobów systemu zależnie od preferencji użytkownika czy dodanie nowych dwukierunkowych urządzeń.

Dzięki technologii PowerG możemy dysponować najlepszymi cechami systemu przewodowego i jednocześnie wyeliminować jego wady, stworzyć bezprzewodowy system nowej generacji.

Mariusz Banach
Visonic

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

ipGO

Nowa rodzina produktów **do monitoringu wizyjnego IP**

Nie jesteś przekonany do technologii IP?

Ten system zmieni Twoje myślenie o urządzeniach sieciowych!

Zero problemów z podłączaniem kamer

100% zadowolenia z doskonałej jakości obrazu

Sprawdź, co potrafi ipGO!

- AUTONOMICZNY SYSTEM
- AUTOMATYCZNA KONFIGURACJA
- OBRAZ Full HD
- PODGLĄD NA SMARTFONACH
- PROSTA OBSŁUGA
- NOWOCZESNY DESIGN

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

Automatyczna konfiguracja całego systemu

ipGO **To takie proste!**

NVIP-NVRA0104/GO
NVIP-NVRA0208/GO

NVIP-2C2001D-P/GO

NVIP-2C5005CZ-P/GO

System ipGO pracuje zgodnie ze standardem Plug & Play, czyli jest gotowy do działania od razu po podłączeniu. Dzięki temu instalacja systemu jest bardzo prosta i zajmuje tyle samo czasu, co zamontowanie systemu analogowego.

1... 2... 3... i gotowe! System działa!

Podłączamy kamerę...

... do odpowiedniego portu w rejestratorze sieciowym ...

... i system jest gotowy do pracy!

Doskonała jakość obrazu Full HD Liczą się szczegóły!

Sceny kamery analogowej

Kamery ipGO

Zdalny dostęp do obrazu z kamer za pomocą urządzeń mobilnych !

iPhone Compatible

Android Compatible

Nowe spojrzenie na ochronę informacji niejawnych (cz. 3)

Artur Bogusz

W niniejszym artykule cyklu pragnę przybliżyć przedsiębiorcom kwestie związane z uzyskaniem i wykorzystywaniem świadectwa bezpieczeństwa przemysłowego (ŚBP) w świetle uwarunkowań prawnych nowej ustawy o ochronie informacji niejawnych. Problematyka ta wciąż wywołuje nieporozumienia – zwłaszcza w przypadkach współpracy przedsiębiorcy z firmami zagranicznymi – co wymaga dodatkowych wyjaśnień z racji ustaleń Krajowej Władzy Bezpieczeństwa co do zobowiązań międzynarodowych

W poprzednich artykułach cyklu omówiłem podstawowe kwestie formalno-prawne. W niniejszym przybliżam przedsiębiorcom wprowadzone przez nową ustawę zmiany dotyczące uzyskiwania i wykorzystywania świadectwa bezpieczeństwa przemysłowego, czyli dokumentu umożliwiającego zawieranie umów i kontraktów biznesowych związanych z dostępem do informacji niejawnych w ujęciu krajowym i międzynarodowym, bowiem warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z umowami albo wykonywaniem zadań wynikających z przepisów prawa jest zdolność do ochrony informacji niejawnych.

Dokumentem potwierdzającym zdolność do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej jest ŚBP wydawane przez ABW albo SKW po przeprowadzeniu postępowania sprawdzającego stan bezpieczeństwa przemysłowego na wniosek przedsiębiorcy.

1. ŚBP – jego rola i znaczenie

Zapisy rozdziału 9. obowiązującej ustawy o ochronie informacji niejawnych, dotyczące bezpieczeństwa przemysłowego, w znaczący sposób zmieniają dotychczasowe zasady wydawania i wykorzystywania ŚBP. Ustawodawca wprowadza analogię do poświadczenia bezpieczeństwa osobowego, które wydawane jest jako dokument potwierdzający dawanie rękojmi zachowania tajemnicy przez osobę. Odpowiednikiem takiego poświadczenia dla przedsiębiorcy (jego firmy jako osoby prawnej) ma być właśnie ŚBP.

1.1. Rola ŚBP w dziedzinie biznesu

ŚBP ma potwierdzać gotowość i zdolność przedsiębiorcy do ochrony informacji niejawnych w ramach realizowanej umowy czy zadania. Można stwierdzić, że jest to dokument potwierdzający jego zdolność do ochrony tychże informacji w jego przedsiębiorstwie – ze wszystkimi tej zdolności konsekwencjami.

Obecnie przedsiębiorca, występując z wnioskiem o przeprowadzenie postępowania bezpieczeństwa przemysłowego, deklaruje jedynie stopień ochrony i klauzulę informacji niejawnych – „poufne" lub wyższą[1] – oraz nie musi go w żaden sposób uzasadniać[2] (był to wymóg poprzedniej ustawy). Jeśli przedsiębiorca zamierza zawierać umowy związane z dostępem do informacji niejawnych o klauzuli „zastrzeżone", świadectwo nie jest wymagane. I jest to w świetle uwarunkowań ustawy o ochronie informacji niejawnych jedyna klauzula, w przypadku której nie jest wymagane ŚBP. Wynika z tego dość jasno, że w chwili obecnej jakakolwiek umowa czy zadanie, w przypadku których wymagany jest dostęp do informacji niejawnych o wyższych klauzulach, nakłada obowiązek posiadania ŚBP. Przepisy rozdziału ustawy o ochronie informacji niejawnych dotyczącego bezpieczeństwa przemysłowego obowiązują także przedsiębiorców będących podwykonawcami umów, jeżeli ich wykonawstwo wymaga dostępu do informacji niejawnych.[3]

W przypadku przedsiębiorstwa jednoosobowego zdolność do ochrony informacji niejawnych jest potwierdzana przez poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli tajności „poufne" lub wyższej, wydawane przez ABW albo SKW, i zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych, wydawane przez ABW albo SKW[4]. W tym przypadku ustawodawca wykonał bardzo głęboki ukłon w stronę przedsiębiorstw jednoosobowych, umożliwiając wykorzystanie poświadczenia bezpieczeństwa osobowego (PBO – dla osoby fizycznej) jako uprawniającego dokumentu tożsamego ze świadectwem bezpieczeństwa przemysłowego (ŚBP – dla osoby prawnej). Praktyka związana jest z całym szeregiem trudności (muszą być one odpowiednio rozwiązane i opisane w „Instrukcji Bezpieczeństwa Przemysłowego załączonej do danej umowy), gdyż z jednej strony mamy brak pełnomocnika ochrony oraz POIN i jego elementów, a z drugiej strony jest uprawnienie do zawarcia umowy, której wykonanie wiąże się z dostępem do informacji niejawnych. Dotyczy to wyłącznie sytuacji i zdarzeń krajowych. Powyższa zasada nie obowiązuje, jeżeli obowiązek uzyskania świadectwa (ŚBP) wynika z ratyfikowanej przez Rzeczpospolitą Polską umowy międzynarodowej lub prawa wewnętrznego strony zawierającej umowę[5].

1.2. Znaczenie ŚBP oraz wyjątki

ŚBP potwierdza zdolność danego przedsiębiorcy/jego firmy (traktowanego jako osoba prawna, funkcjonująca na rynku) do chronienia informacji niejawnych w odpowiednim stopniu. Dotyczy to umów/kontraktów krajowych i międzynarodowych[6].

W Polsce Prezes Rady Ministrów, szefowie Kancelarii: Prezydenta Rzeczypospolitej Polskiej, Sejmu, Senatu albo minister właściwy dla określonego działu administracji rządowej, Prezes Narodowego Banku Polskiego lub kierownik urzędu centralnego, a w przypadku ich braku Szef ABW albo Szef SKW mogą wyrazić pisemną zgodę na udostępnienie informacji niejawnych o klauzuli „poufne" lub wyższej przedsiębiorcy, wobec którego wszczęto postępowanie dotyczące bezpieczeństwa przemysłowego lub postępowanie sprawdzające. Potwierdzoną kopię zgody przekazuje się ABW lub SKW[7]. W szczególnie uzasadnionych przypadkach podmioty, o których mowa wyżej, mogą wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych przedsiębiorcy nie posiadającemu odpowiedniego świadectwa lub poświadczenia bezpieczeństwa (w przypadku przedsiębiorcy, o którym mowa powyżej i wobec którego nie jest prowadzone postępowanie dotyczące

1) Art. 54 ust. 9 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

2) Art. 56 ust. 1 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

3) Art. 54 ust. 6 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

4) Art. 54 ust. 3 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

5) Art. 54 ust. 4 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

6) Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi, Krajowa Władza Bezpieczeństwa, Warszawa, 31 grudnia 2010 r.

7) Art. 54 ust. 7 i 8 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

Rys. 1. Świadectwa bezpieczeństwa przemysłowego poszczególnych stopni

bezpieczeństwa przemysłowego lub postępowanie sprawdzające). Przedsiębiorca, o którym jest mowa wyżej, musi spełnić wymagania ustawy dotyczące ochrony informacji niejawnych o klauzuli „zastrzeżone"(tzn. być dopuszczonym i przeszkolonym), z wyjątkiem wymogu zatrudnienia pełnomocnika ochrony, jeżeli wykonuje umowę/zadanie kontraktowe związane z dostępem do tych informacji. Nie ma on wówczas prawa do przetwarzania uzyskanych informacji w użytkowanych przez niego obiektach.

1.3. Stopnie i klauzule ŚBP

Zgodnie z wnioskiem przedsiębiorcy i w zależności od deklarowanego i potwierdzonego w toku postępowania sprawdzającego stopnia zdolności do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej wydaje się świadectwo odpowiednio:

– pierwszego stopnia – potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji,
– drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, ale bez możliwości ich przetwarzania we własnych systemach teleinformatycznych,
– trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, ale bez możliwości ich przetwarzania w użytkowanych przez niego obiektach[8].

Okresy ważności świadectw potwierdzających zdolność do ochrony informacji niejawnych o klauzuli **„ściśle tajne"** w poszczególnych przypadkach są następujące:

– „ściśle tajne" – 5 lat od daty wystawienia,
– „tajne" – 7 lat od daty wystawienia,
– „poufne" – 10 lat od daty wystawienia.

Okresy ważności świadectw potwierdzających zdolność do ochrony informacji niejawnych o klauzuli **„tajne"** w poszczególnych przypadkach są następujące:

– „tajne" – 7 lat od daty wystawienia,
– „poufne" – 10 lat od daty wystawienia.

Świadectwo potwierdzające zdolność do ochrony informacji niejawnych o klauzuli **„poufne"** jest ważne przez 10 lat od daty wystawienia[9].

8) Art. 55 ust. 1 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

9) Art. 55 ust. 2 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

1.4. Wykorzystywanie ŚBP – jego okres ważności i wygaśnięcie

ŚBP może być wykorzystywane tylko na obszarze RP w okresie swojej ważności (odpowiednio do klauzuli). Stosownie do sytuacji ABW albo SKW wydaje odrębne świadectwa potwierdzające zdolność do ochrony informacji niejawnych o klauzuli stanowiącej zagraniczny odpowiednik klauzuli „tajne" lub „poufne", stosowany przez organizacje międzynarodowe (NATO, UE)[10]. Informacje oznaczone przez NATO lub UE jako *restricted* są uznane za zastrzeżone, natomiast informacje oznaczone jako *unclassified* lub *limited* są przeznaczone wyłącznie do wykorzystania służbowego. Pozostałych informacji pozostających w obiegu międzynarodowym, w którym uczestniczy RP, i wymagających ochrony (np. informacje dotyczące porozumienia z Wassenaar) nie traktuje się jako niejawnych informacji międzynarodowych według ustawy dotyczącej informacji niejawnych.

Ustawodawca przewidział również skrócenie okresu ważności ŚBP – przestaje ono być ważne również wówczas, gdy:

– przedsiębiorca zrzeknie się uprawnień określonych w świadectwie,
– przedsiębiorstwo zostanie przejęte przez inny podmiot lub zlikwidowane[11].

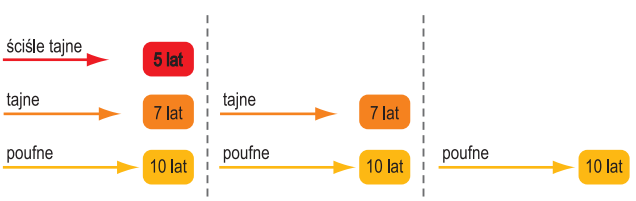
Jako jeden z powodów wygaśnięcia ŚBP ustawodawca podaje „zrzeczenie się uprawnień określonych w świadectwie". Jak należy to rozumieć? Z istoty zapisu wynika, że w przypadku uzyskania ŚBP przedsiębiorca ma obowiązek trwale utrzymywać w gotowości do działania zadeklarowane zasoby (osobowe, techniczne i organizacyjne), jakie wynikają z otrzymanych uprawnień (odpowiednio do stopnia i klauzuli). Jeżeli tego nie czyni, musi liczyć się z możliwością unieważnienia ŚBP, a tym samym z utratą uprawnień, jakie wynikają z faktu posiadania tego dokumentu. Oczywiste jest zatem sukcesywne ponoszenie przez przedsiębiorcę wszelkich niezbędnych kosztów z tego tytułu, pochodnych dla konieczności zachowania ciągłości procesu utrzymywania przyznanych uprawnień zawartych w ŚBP (mogą to być zmiany prawa, kadrowe i inne). Składając wniosek przedsiębiorca powinien w pełni zdawać sobie sprawę z przyjęcia zobowiązań wynikających z faktu posiadania świadectwa (niezależnie od jego bezpośredniego wykorzystania biznesowego).

1.5. Uzyskiwanie ŚBP – postępowanie sprawdzające i jego skutki

Postępowanie dotyczące bezpieczeństwa przemysłowego jest prowadzone na wniosek przedsiębiorcy. Wniosek nie

10) Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi, Krajowa Władza Bezpieczeństwa, Warszawa, 31 grudnia 2010 r.

11) Art. 55 ust. 4 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).



Rys. 2. Okresy ważności świadectw bezpieczeństwa przemysłowego

wymaga uzasadnienia. We wniosku przedsiębiorca określa stopień świadectwa oraz klauzulę tajności informacji niejawnych, których zdolność do ochrony ma potwierdzać to świadectwo. Do wniosku przedsiębiorca dołącza kwestionariusz bezpieczeństwa przemysłowego (KBP) oraz ankiety lub kopie poświadczeń bezpieczeństwa osób określonych w art. 57 ust. 3 ustawy (PBO). Wniosek wraz z kwestionariuszem powinien trafić do ABW. Tylko w nielicznych przypadkach, ściśle wskazanych w ustawie, adresatem jest SKW.

Należy podkreślić wymóg skrupulatnego spełnienia wymagań ustawy (wymagane dokumenty i poświadczenia) oraz poprawnego opracowania danych wpisywanych do KBP (zgodność z realiami w przedsiębiorstwie). ABW albo SKW może wezwać przedsiębiorcę do uzupełnienia braków formalnych we wniosku i jego załącznikach w terminie 30 dni od dnia otrzymania wezwania pod rygorem, że wniosek może nie zostać rozpatrzony[12]. Należy również wspomnieć o konieczności uzupełniania/wyjaśniania poszczególnych pozycji kwestionariusza bezpieczeństwa przemysłowego w toku prowadzonego postępowania sprawdzającego. Brak stosownego uzupełnienia i stwierdzenie tego faktu przez ABW w toku prowadzonego postępowania, może skutkować negatywnym dla wnioskującego rezultatem tego postepowania.

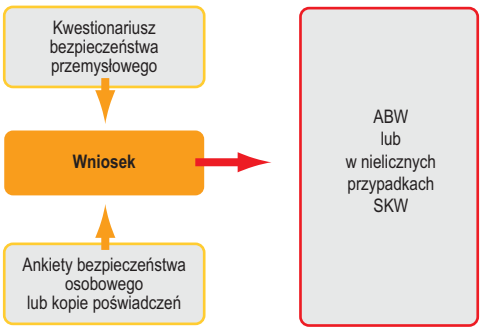
Prowadzone postępowanie kończy się wydaniem przez ABW albo SKW świadectwa zgodnego z wnioskiem przedsiębiorcy lub decyzją o odmowie jego wydania, albo decyzją o umorzeniu postępowania[13].

1.6. Odmowa wydania/cofnięcie wydanego ŚBP

ABW albo SKW może odmówić wydania ŚBP.

Odmawia się wydania ŚBP lub cofa się je w przypadku:

– osób, które zajmują stanowisko KJO, a którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa (wg zgłoszonej w KBP klauzuli),



Rys. 3. Procedura składania wniosku i kwestionariusza bezpieczeństwa przemysłowego

– niemożności ustalenia struktury kapitałowej i źródeł pochodzenia środków finansowych pozostających do dyspozycji przedsiębiorcy,
– niezorganizowania w terminie sześciu miesięcy od daty wszczęcia postępowania kompleksowego systemu ochrony informacji niejawnych w przypadku ubiegania się o świadectwo pierwszego lub drugiego stopnia,
– zatajenia danych w kwestionariuszu lub podania w nim danych nieprawdziwych,
– podania nieprawdziwych informacji o zmianach danych zawartych w kwestionariuszu.

Ustawodawca dość ściśle określił możliwe przyczyny odmowy wydania ŚBP, wskazując określone powinności przedsiębiorcy i rezultaty niespełnienia wymagań.

1.6.1. Przyczyny odmowy/cofnięcia ŚBP

ABW albo SKW może odmówić wydania świadectwa, gdy stwierdzi niezdolność do ochrony informacji niejawnych z powodu:

– ujawnienia w toku postępowania dotyczącego bezpieczeństwa przemysłowego, w wyniku sprawdzenia osób wymienionych w art. 57 ust. 2 pkt 4 ustawy, nie dających się usunąć wątpliwości określonych w art. 24 ust. 2 pkt 1-3 lub 5 lub w art. 24 ust. 3 ustawy,
– niepowiadomienia w ciągu 30 dni o zmianie danych zawartych w kwestionariuszu w trakcie postępowania dotyczącego bezpieczeństwa przemysłowego.

12) Art. 56 ust. 4 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

13) Art. 64 ust. 1 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

Doczekaliśmy się określenia terminu powiadomienia o zaistniałych w przedsiębiorstwie zmianach (albo w toku prowadzonego postępowania sprawdzającego, lub w przypadku posiadania już ważnego ŚBP). Znane sformułowanie „niezwłocznie" zastąpiono 30-dniowym terminem poinformowania o zmianach danych zawartych w kwestionariuszu bezpieczeństwa przemysłowego (zgłoszonym/złożonym KBP). Jak wynika z przedstawionych powyżej wymogów ustawowych, bardzo ważną cechą funkcjonującego w jednostce organizacyjnej systemu ochrony informacji niejawnych jest funkcjonalność informacyjna. Od wywiązywania się przez przedsiębiorcę z obowiązku informacyjnego wobec ABW/SKW zależy uzyskanie, a następnie utrzymanie posiadanego świadectwa. Zorganizowanie w jednostce organizacyjnej mechanizmu informacyjnego jest bardzo ważne. Oczywiście im większe przedsiębiorstwo i im bardziej złożona struktura organizacyjna, tym trudniej stworzyć prawidłowo funkcjonujący system informacyjny.

1.6.2. Struktura dokumentów składających się na ŚBP

Decyzja o odmowie wydania świadectwa oraz decyzja o jego cofnięciu powinny zawierać:

– oznaczenie organu, który wydał świadectwo, unieważnił je bądź odmówił jego wydania,
– wskazanie miejsca i daty wystawienia,
– nazwę przedsiębiorstwa, adres jego siedziby, numer w Krajowym Rejestrze Sądowym i numer REGON,
– podstawę prawną,
– stwierdzenie wydania, odmowy wydania lub cofnięcia świadectwa,
– stopień, klauzulę tajności oraz termin ważności świadectwa (w przypadku jego wydania),
– imienną pieczęć i podpis upoważnionego funkcjonariusza ABW albo funkcjonariusza lub żołnierza SKW.

Decyzja o odmowie wydania oraz decyzja o cofnięciu świadectwa powinny zawierać uzasadnienie faktyczne i prawne oraz pouczenie o dopuszczalności i terminie wniesienia:

– odwołania do Prezesa Rady Ministrów,
– skargi do sądu administracyjnego.

Uzasadnienie faktyczne w części zawierającej informacje niejawne podlega ochronie na zasadach określonych w ustawie o ochronie informacji niejawnych[14].

2. ŚBP a zobowiązania międzynarodowe

Zobowiązania międzynarodowe objęte ustawą o ochronie informacji niejawnych dotyczą NATO oraz Unii Europejskiej[15]. Ponadto mogą być wymagania odrębnie określone (prawo stron umowy/kontraktu) lub przywołane bezpośrednio jako wymóg prawa krajowego (polskie przepisy w ramach realizacji programów sojuszniczych, np. NSIP[16]).

14)Art. 67 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228).

15)"Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi", Krajowa Władza Bezpieczeństwa, Warszawa, 31 grudnia 2010 r.

16) NSIP – NATO Security Investment Programme, realizowany w Polsce przez MON i Min. Gospodarki wieloletni natowski program bezpieczeństwa układowego (m.in. bazy logistyczne i obiekty infrastruktury wojskowej).

2.1. Wymagania NATO

Kwestia bezpieczeństwa przemysłowego w ujęciu wymagań prawnych NATO została opisana w załączniku *G [INDUSTRAL SECURITY]* dokumentu *C-M (2002)49 [SECURITY WITHIN THE NATO]* z dnia 17 czerwca 2002 roku, stanowiącego rdzeń polityki bezpieczeństwa informacyjnego NATO. Jego wykładnią do praktycznego wykorzystania jest wspierająca powyższy dokument dyrektywa *D/2003 [DIRECTIVE ON INDUSTRAL SECURITY]* grupy kadrowej AC/35 CNAD[17].

Inspektorzy Biura Bezpieczeństwa NATO (NOS) co 18 miesięcy sprawdzają, czy wymogi określone w powyższych dokumentach są spełniane.

Zasadnicze wymagania:

1) Przedsiębiorca musi dysponować systemem ochrony zgodnym z wymaganiami NATO, a także podkancelarią lub punktem kontroli dokumentów.
2) Poszczególne osoby z zgłoszonego do prac zespołu muszą posiadać odpowiednie poświadczenia bezpieczeństwa osobowego (certyfikaty NATO) i odbyć szkolenia w zakresie wymagań stawianych przez NATO.
3) W podpisanej umowie lub kontrakcie niejawnym musi być instrukcja bezpieczeństwa – PSI (*Project/Programme Security Instruction*) wraz z przewodnikiem i kontrolnym wykazem klasyfikacyjnym (PSI/SAL).

W procesie ochrony wymienianych w ramach NATO międzynarodowych informacji niejawnych stosuje się następujące akty prawne (wraz z aktami wykonawczymi i dokumentami pomocniczymi):

– ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228),
– umowę między stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzoną w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r., nr 64, poz. 740; akces RP – patrz: Dz. U. z 2000 r., nr 64, poz. 741),
– umowę między stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych, sporządzoną w Paryżu dnia 18 czerwca 1964 r. (akces RP – patrz: Dz. U. z 2001 r., nr 143, poz. 1594),
– memorandum NATO C-M (2002) 49 – *Bezpieczeństwo w ramach Organizacji Traktatu Północnoatlantyckiego* z dnia 17 czerwca 2002 r.

2.2. Wymagania Unii Europejskiej

Kwestia bezpieczeństwa przemysłowego według wymagań prawnych Unii Europejskiej dotyczy głównie zależności wynikających z zobowiązań traktatowych oraz uprawnień Komisji Europejskiej jako ciała wykonawczego. Podstawę wymagań stanowi Decyzja Rady Unii Europejskiej nr 2001/264/EC z dnia 19 marca 2001 roku, uzupełniona w dniu 12 grudnia 2005 roku o sekcję XIII (wspólne minimalne wymagania dotyczące bezpieczeństwa przemysłowego).

17) CNAD – natowska Rada Dyrektorów ds. Uzbrojenia – prowadzi grupy (kadrowe i cywilne) opracowujące dokumenty wykonawcze (w tym dyrektywy) niezbędne dla wdrażania w praktyce memorandów (C-M) organów naczelnych NATO.

Podobnie jak w obecnej ustawie polskiej obowiązuje oświadczenie woli przedsiębiorcy ze wszystkimi konsekwencjami tego faktu (od 14 marca 2003 roku obowiązuje wspólne porozumienie NATO – EU w zakresie ochrony tajemnicy informacji: Dz. UE. L. 80/36 z dnia 24 marca 2003 r.).

W procesie ochrony międzynarodowych informacji niejawnych wymienianych w ramach UE stosuje się następujące akty prawne (wraz z aktami wykonawczymi i dokumentami pomocniczymi):

– ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228),
– traktat akcesyjny podpisany dnia 16 kwietnia 2003 r. (Dz. U. z 2004 r., nr 90, poz. 864 z późn. zm.),
– rozporządzenie Rady Europejskiej Wspólnoty Energii Atomowej (EUROATOM) nr 3 z dnia 31 lipca 1958 r. (Dz. UE. L. z 1958 r., nr 17, poz. 406),
– decyzję Rady Unii Europejskiej nr 2001/264/EC w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa z dnia 19 marca 2001 r. (Dz. UE. L. z 2001 r., nr 101, poz. 1 z późn. zm.),
– decyzję Komisji Europejskiej nr 2001/844/EC w sprawie przyjęcia dla KE przepisów bezpieczeństwa z dnia 29 listopada 2001 r. (Dz. UE. L. z 2001 r., nr 317, poz. 1).

3. Podsumowanie

Mam nadzieję, że udało mi się przedstawić w całym cyklu problematykę ochrony informacji niejawnych oraz bezpieczeństwa przemysłowego w sposób w miarę zrozumiały. Miejscami celowo przejaskrawiłem opis niektórych, może tylko skrajnych zjawisk. Chciałem zasygnalizować Czytelnikom tylko możliwość – a nie konieczność –wystąpienia pewnych problemów, sytuacji formalnie niekorzystnych.

Artur Bogusz

Bibliografia

1. ABW, *Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi, Krajowa Władza Bezpieczeństwa*, Warszawa, 31 grudnia 2010 r.
2. Anzel M., *Nowa ustawa i jej zmienione uwarunkowania*, mat. szkoleniowe OSPOIN, Warszawa 2010.
3. Hoc St., *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. LexisNexis, Warszawa 2010.
4. MON, *Wytyczne w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne*, zał. do *Decyzji nr 362/MON* z dnia 28 września 2011 r.
5. Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. LexisNexis, Warszawa 2011.
6. *Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych*, Dz. U. z 2010 r., nr 182, poz. 1228.
7. *Zestawienie obowiązujących przepisów OIN*, mat. szkoleniowe kursu kierowników KT, ZG OSPOIN, Warszawa 2012.

Cudze chwalicie, swego nie znacie

Rodzima produkcja rejestratorów wizyjnych

Tomasz Polus

Rynek CCTV wypełniają obecnie produkty zaprojektowane i wyprodukowane w Azji. Chyba nie zdołamy już zmienić tej sytuacji na korzyść produktów polskich. Większość naszych instalatorów (a zatem i dystrybutorów) zwraca uwagę na niską cenę urządzeń, często nie dbając o ich jakość oraz poziom lokalnego serwisu i wsparcia technicznego. Na szczęście nie wszyscy zmierzają w tym kierunku, czego najlepszym dowodem jest stale rozwijana oferta firmy POLVISION, która od kilku lat oferuje rejestratory wizyjne i stacje monitorowania produkowane przez polskich inżynierów

W kwietniu 2005 roku rozpocząłem pracę nad pierwszym projektem zaawansowanego cyfrowego rejestratora wizyjnego o roboczej nazwie PV2006. Przez kilka miesięcy prowadziłem sondaże i dokonywałem analizy rynku zaawansowanych rejestratorów cyfrowych, a w międzyczasie testowałem nowoczesne technologie kompresji sygnału wizyjnego, archiwizacji danych, zdalnego sterowania. Skontaktowałem się nawet z Francuzami, którzy pracowali nad bardzo podobnym projektem. Rozważałem możliwość kupna gotowych urządzeń, mimo że były bardzo kosztowne.

Ostatecznie zbudowałem własny prototyp, bazując na doświadczeniach z rynku polskiego. Rejestrator PV2006 nagrywał materiał wizyjny z prędkością100 kl./s, rozdzielczością D1 oraz kompresją Wavelet i MPEG4. Był wyposażony w redundantne zasilacze i osiem kieszeni na dyski twarde. Umożliwiał zbudowanie macierzy RAID5 o pojemności do 3 TB. Zapewniał niespotykanie – jak na tamte czasy – wysoką jakość obrazu oraz wiele możliwości przechowywania nagrań i konfiguracji oprogramowania.

Wówczas był to sprzęt o fascynujących właściwościach, który spełniał wymagania prawie każdego projektu. Niestety – nie sprzedaliśmy wtedy ani jednego z tych rejestratorów. Ludzie oglądali reklamy, dzwonili, pytali, czytali, ale nie kupowali. Dopiero po dwóch latach dostarczyliśmy prototyp kolejnego urządzenia jednej z największych polskich instytucji, której zostaliśmy zarekomendowani. Po przeprowadzeniu testów i niewielkiej modyfikacji rejestratora doszło do pierwszej transakcji. Ostatecznie projekt PV2006 nie przyniósł nam jednak korzyści finansowych, dlatego został wstrzymany.

W pewnym sensie była to dla mnie porażka, ale z drugiej strony niezapomniana lekcja. Po latach zrozumiałem, że brakowało nam wtedy doświadczenia, marki i prestiżu, aby tworzyć sprzęt z myślą o dużych, zaawansowanych projektach CCTV. Na rynku telewizji dozorowej nie kojarzono nas jeszcze wtedy z produkcją rejestratorów, a jedynie z wysokiej jakości urządzeniami do transmisji sygnałów wizyjnych.

Dziś, po siedmiu latach od tamtych wydarzeń, firma POLVISION ma ugruntowaną pozycję na rynku jako producent zaawansowanych rejestratorów cyfrowych. W międzyczasie, w latach 2006–2009, przeżywaliśmy wzloty i upadki. Z braku możliwości produkcyjnych musieliśmy zamawiać zaprojektowane przez nas urządzenia w innych firmach, testowaliśmy swoje oprogramowanie, poprawialiśmy jego kolejne wersje. Mimo licznych problemów zgłaszanych przez naszych odbiorców staraliśmy się zapewniać możliwie najlepsze wsparcie techniczne. Klienci to doceniali – żaden zgłoszony problem nie pozostał bez rozwiązania. Poprawialiśmy oprogramowanie i sprzęt, zdobywaliśmy bardzo cenne doświadczenie i poznawaliśmy rzeczywiste potrzeby naszych klientów.

W latach 2008–2009 sami zwiększyliśmy wymagania wobec naszych urządzeń, głównie w związku z dynamicznym wzrostem sprzedaży naszych megapikselowych kamer IP. Wymusiło to konieczność budowania rejestratorów dysponujących większą pojemnością zainstalowanych dysków, dużą mocą obliczeniową i wydajniejszym systemem chłodzenia. Praktycznie odrzuciliśmy rozwiązania wymagające korzystania z obudów wolnostojących i wykorzystywaliśmy obudowy przeznaczone do montażu w szafach RACK.

W 2010 roku podnieśliśmy poprzeczkę tak wysoko, jak tylko było to możliwe w przypadku tej klasy rozwiązań. Rozpoczęliśmy produkcję serii urządzeń hybrydowych PV-RADVR (RACK DVR) i PV-RPDVR (RACK PRO DVR) oraz stacji monitorowania PV-ECCMS (ECONO CMS) i PV-PRCMS (PRO CMS). Stawiamy na jakość i trwałość naszych rozwiązań, długi okres gwarancji, homogeniczną konfigurację oraz drobiazgowe testy, które pozwalają nam w pełni poznać możliwości sprzętu. Dzięki temu zapewniamy wysokiej klasy wsparcie techniczne i szybki serwis na terenie całej Polski. Na koszty produkcji i związane z nimi ceny naszych urządzeń zwracamy uwagę w mniejszym stopniu, choć nadal nasze systemy rejestrujące uchodzą za atrakcyjne cenowo, chociaż ich możliwości są duże. Wprowadzone w 2010 roku zmiany umożliwiły przede wszystkim obsługę dużych systemów kamer analogowych i megapikselowych z wykorzystaniem nowoczesnej kompresji H.264. Od tej pory rejestratory sieciowe mają możliwość rejestrowania i wyświetlania obrazów z 32 kamer o rozdzielczości Full HD z sumaryczną prędkością 960 kl./s.

Jako jedna z nielicznych firm na rynku polskim opracowaliśmy specjalistyczne oprogramowanie działające na 64-bitowej platformie Windows Embedded, które zapewnia wydajność, bezpieczeństwo i stabilność na poziomie nieosiągalnym dla maszyn bazujących na typowych systemach Windows.

Warto zwrócić uwagę na to, że w przeciwieństwie do większości rejestratorów dostępnych na naszym rynku oferowane przez nas urządzenia potrafią nie tylko zapisywać strumienie wizyjne, ale również inteligentnie je przetwarzać, np. błyskawicznie skalować strumienie IP przesyłane do stacji monitorowania. W rezultacie system doskonale radzi sobie z transmisją poprzez wolne i przeciążone łącza internetowe. Rejestratory te potrafią również analizować obraz w czasie rzeczywistym, m.in. śledzić i zliczać ruchome obiekty, stabilizować obraz, wykrywać sabotaż, redukować efekty mgły, dymu, opadów itp.

Celem przeprowadzonej w 2010 roku modernizacji było również podwyższenie poziomu niezawodności rejestratorów. Ze statystyk firmy POLVISION wynika, że najczęstszą przyczyną przerw w pracy systemów rejestrujących są uszkodzenia dysków twardych. W celu podniesienia poziomu niezawodności, cała seria rejestratorów wyposażana jest w specjalistyczne dyski twarde. Dyski te są zoptymalizowane pod kątem równoczesnego zapisu wielu strumieni wizyjnych i przystosowane do ciągłego działania, a średni czas ich pracy między awariami (MTBF) wynosi około miliona godzin.

Fot. 1. Stanowisko testowania rejestratorów z 2005 roku (prototyp PV2006)

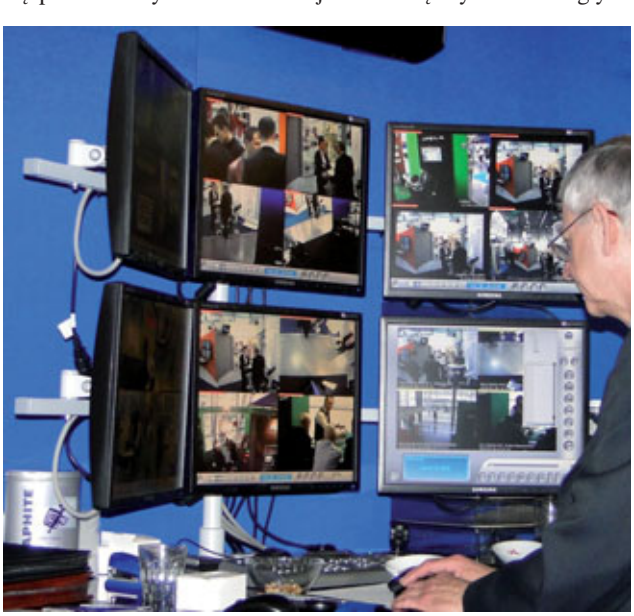
Fot. 2. Aktualne stanowisko testowania rejestratorów hybrydowych i sieciowych (2012)

Na początku 2011 roku wszystkie rejestratory hybrydowe i sieciowe oraz stacje monitorowania oferowane przez naszą firmę zostały formalnie uznane za zgodne ze światowymi standardami komunikacji sieciowej ONVIF, PSIA i RTSP. Niedługo potem zwiększyliśmy pojemność pamięci masowych do 24 TB i wprowadziliśmy obsługę kamer hemisferycznych, które mają pełny kąt widzenia otaczającego je obszaru. Rozszerzenie funkcjonalności o obsługę kamer dookolnych ponownie wymusiło na nas zwiększenie wydajności urządzeń rejestrujących, ponieważ przekształcanie zniekształconego obrazu szerokokątnego na obraz prosty, z możliwością wyboru dowolnego wycinka tego obrazu i śledzenia obiektów – tak jak się to odbywa za pomocą kamer obrotowych – wymaga potężnej mocy obliczeniowej.

Aby dostosować się do rosnących wymagań rynku kamer wysokorozdzielczych, w pierwszej połowie 2012 roku zwiększyliśmy pojemność pamięci masowych do 33 TB. Zbudowaliśmy również własną macierz dyskową PV-RAID w standardzie RAID5, która umożliwia podwojenie pojemności rejestratora.

Mniej więcej w tym samym okresie wprowadziliśmy na rynek dwa nowe modele rejestratorów hybrydowych PV-RADVR32800H i PV-RPDVR32800H, które mają 32 kanały wejściowe i umożliwiają nagrywanie obrazów i dźwięku z kamer analogowych i/lub kamer IP. Jakość rejestrowanego obrazu o rozdzielczości D1 z kamer analogowych jest bardzo wysoka. Obrazy mogą być rejestrowane z sumaryczną prędkością 800 kl./s i kompresją H.264. Należy podkreślić, że w przypadku rozdzielczości D1 pojedynczy strumień wizyjny z każdej z kamer jest niewiarygodnie duży i osiąga 10 Mbit/s. Zazwyczaj wartość ta jest zarezerwowana dla kamer megapikselowych IP o ośmiokrotnie wyższej rozdzielczości.

W naszych rejestratorach wciąż udoskonalamy funkcje nagrywania, wyświetlania, przechowywania nagrań, analizy treści obrazów, sterowania i alarmowania. Nasze konstrukcje są z założenia przeznaczone do najbardziej wymagających zastosowań, takich jak monitoring miast, stadionów, kasyn, imprez masowych itp. Testując nasze rozwiązania, skupiamy się przede wszystkim na funkcjach niezbędnych w rozległych



Fot. 3. Stanowisko testowania centralnej stacji monitorowania

Fot. 4. Rejestrator PV-RPNVR w zestawie z macierzą PV-RAID. Oba urządzenia wprowadzono do produkcji w maju 2012 roku

instalacjach. Podczas prób podłączamy do nich jednocześnie dużą liczbę kamer analogowych i kamer IP, centralne stacje monitorowania i raportowania zdarzeń alarmowych, a także serwery uwierzytelniania służące do centralnego zarządzania kontami i hasłami (*Active Directory*). Uruchamiamy funkcje duplikowania nagrań w różnych lokalizacjach fizycznych, a nawet funkcje duplikowania całych serwerów (*failover*), które gwarantują prawidłowe działanie systemu nawet w przypadku awarii jednej z maszyn. Niejednokrotnie pomagamy klientom zintegrować nasze rejestratory z innymi istniejącymi systemami, np. systemami kontroli dostępu, kasowymi, biletowymi, wagowymi itd.

W drugiej połowie 2012 roku rozpoczęliśmy produkcję systemów uzupełniających – zaawansowanych serwerów rejestrujących PV-RPRS, które oferują mniej funkcji, ale umożliwiają podłączenie do jednego urządzenia aż 128 kamer IP o rozdzielczości dochodzącej do 5 Mpix. Po raz pierwszy serwer rejestrujący PV-RPRS został przetestowany pod koniec 2011 roku w bardzo dużym systemie rejestrującym materiał wizyjny. Rejestrowano na nim 128 strumieni wizyjnych z kamer GV-FE421 (4.0Mpix, 15fps, H.264) o łącznej przepływności dochodzącej do 800 Mbit/s.

Aktualnie pracujemy również nad rozbudową istniejących stacji monitorowania, wprowadzając do nich funkcje wielomonitorowych ścian wizyjnych. Docelowo mają obsługiwać ponad osiem monitorów pracujących w trybie matrycy wizyjnej, sekwencji matryc wizyjnych, okien alarmowych lub podglądowych i map synoptycznych.

Na zakończenie dodam – może nieskromnie – że jestem dumny z produkowanych przez nas rejestratorów i stacji monitorowania. Niezmiernie cieszę się, kiedy nasze produkty chwalą zadowoleni klienci, ponieważ daje mi to dużą motywację do dalszej pracy. Cenię sobie jednak również uwagi krytyczne, które pozwalają spojrzeć na produkt z szerszej perspektywy, dostrzec i wyeliminować jego wady. Jako projektant i jednocześnie kontroler jakości tych urządzeń muszę znać ich wszystkie wady i zalety. Tylko dzięki temu jestem w stanie zagwarantować swoim klientom, że dostarczony im system będzie spełniał wymagania określone w projekcie.

Tomasz Polus
POLVISION
tpolus@polvision.com.pl

Większa rentowność dzięki dyskretnemu i przystępnemu cenowo rozwiązaniu do nadzoru z funkcjami PTZ? **To proste.**

Czy chcą Państwo poprawić bezpieczeństwo w swoim sklepie? A może także zwiększyć efektywność operacyjną i rentowność? Oba te cele pomoże zrealizować rozwiązanie nadzoru wizyjnego.

Kamery Axis z linii M z funkcjami obrót/pochylenie/zbliżenie udostępniają materiał wizyjny jakości HDTV, alarmy w czasie rzeczywistym oraz inne inteligentne i przydatne możliwości. Dzięki nim można między innymi zwalczać kradzieże w sklepach, zapobiegać brakowi towaru na półkach oraz monitorować kolejki do kas.

Ze względu na elastyczne funkcje obrót/pochylenie/zbliżenie, niewielkie rozmiary i prostą instalację kamery AXIS z serii M50 umożliwiają łatwą i dyskretną obserwację wszystkiego, co dzieje się w sklepie.

Niewielka kamera. Wielkie możliwości. Łatwy wybór.

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

Kopułkowa kamera sieciowa PTZ AXIS z serii M50 • Jakość materiału wizyjnego do poziomu HDTV 720p • Funkcje obrotu, pochylenia i zbliżenia oraz ultradyskretna konstrukcja • Zasilanie przez sieć Ethernet • Wbudowany mikrofon • Ochrona klasy IP51 • Gniazdo kart pamięci MicroSD/SDHC

AXIS COMMUNICATIONS

Interesująca propozycja Axis dla sektorów handlu, edukacji, bankowości i przemysłu

Agata Majkucińska

Fot. 1. Małe, odporne na zanieczyszczenia kamery AXIS M30 są przystosowane do szybkiego montażu

Axis wprowadza na rynek niedrogie stałopozycyjne kamery kopułkowe z funkcją inteligentnej analizy treści obrazów i możliwością rejestracji materiału wizyjnego w pamięci wewnętrznej, pracujące z rozdzielczością HDTV, przeznaczone do pracy wewnątrz budynków

Kamery sieciowe z serii AXIS M30 mają małe rozmiary i mogą być stosowane w systemach wykorzystujących oprogramowanie AXIS Camera Companion lub w systemach korzystających z usług hostingowych i AXIS Camera Application Platform. Dzięki temu możliwe jest bardzo znaczne obniżenie kosztów instalacji wizyjnych systemów dozorowych.

Stałopozycyjne kamery kopułkowe z serii AXIS M30 IP mają średnicę około 10 cm i wysokość około 5 cm, przy czym dostępne są modele pracujące w standardach HDTV 720p i HDTV 1080p przystosowane do instalacji wewnątrz budynków. Znajdują one zastosowanie w instalacjach dozorowych w takich obiektach jak galerie handlowe, hotele, szkoły, banki i biura.

– *Kontynuujemy prace zmierzające do zastąpienia przestarzałych analogowych systemów dozorowych nowoczesnymi systemami sieciowymi, przy czym istotne jest to, że oferujemy wysokiej jakości kamery sieciowe w akceptowalnej cenie. Dzięki temu użytkownicy systemów, zarówno małych jak i dużych, mogą korzystać ze wszystkich zalet rozwiązań sieciowych* – stwierdził Fredrik Nilsson, dyrektor firmy Axis Communications.

Nowe kamery Axis z serii M30 mogą pracować w systemach korzystających z oprogramowania AXIS Camera Companion, usług hostingowych i oprogramowania VMS oferowanego przez innych producentów, należących do grupy Application Development Partners, współpracujących z Axis. Takie systemy generują obrazy w standardzie HDTV i mogą być zastosowane wszędzie tam, gdzie niskie koszty mają kluczowe znaczenie.

Dostępne są różne kolory obudów kamer kopułkowych z serii AXIS M30 IP. Dzięki temu kamery te mogą być łatwo dopasowane do otoczenia i nie szpecą pomieszczeń, w których są zainstalowane.

Dzięki zastosowaniu unikatowego sposobu zamocowania obiektywu, którego ustawienie może być regulowane w trzech osiach, kamery z serii AXIS M30 IP mogą być montowane na ścianach, sufitach, a nawet na powierzchniach skośnych

Fot. 2. Mała kamera AXIS M30 przystosowana do montażu wewnątrz pomieszczeń stanowi ekonomiczne rozwiązanie wizyjnego systemu dozorowego w standardzie HDTV

Fot. 3. Dostępne są kolorowe osłony na kamery, pozwalające na ich wkomponowanie w otoczenie

i mogą być wyregulowane w taki sposób, by zapewnić właściwe pole widzenia. Zarówno obiektyw, jak i oprogramowanie zastosowane w kamerze AXIS M30 IP umożliwia korzystanie z funkcji AXIS Corridor Format, która pozwala na obracanie obrazu i jego pionowe ustawienie, co z kolei umożliwia skuteczną obserwację korytarzy, klatek schodowych i innych ciągów komunikacyjnych. Takie ustawienie obrazu pozwala na lepsze wykorzystanie jego powierzchni.

Poziome kąty widzenia stałopozycyjnych kamer kopułkowych AXIS M3004 i AXIS M3005 są równe odpowiednio 80 stopni i 118 stopni, zaś regulacja ostrości nie jest w ogóle wymagana, dzięki czemu czas potrzebny na instalację tych kamer został skrócony do minimum.

Kamery kopułkowe z serii AXIS M30 IP są fabrycznie wyposażone w kabel o długości dwóch metrów i są zasilane metodą PoE. Dzięki temu nie ma potrzeby stosowania dodatkowych kabli zasilających, co z kolei ma wpływ na dalszą redukcję kosztów montażu tych urządzeń.

Dzięki zastosowaniu wydajnej kompresji obrazów metodą H.264 oraz wyposażeniu kamer z serii AXIS M30 IP w gniazda kart pamięci MicroSDHC możliwy jest ciągły zapis obrazu HDTV przez kilka dni z rzędu, bez konieczności przenoszenia zarejestrowanego materiału wizyjnego na nośnik zewnętrzny. Użycie tych kamer w połączeniu z darmowym oprogramowaniem AXIS Camera Companion pozwala na tworzenie tanich i łatwych w obsłudze systemów dozorowych zawierających maksymalnie szesnaście kamer.

Kamery kopułkowe z serii AXIS M30 IP mogą być wykorzystane także w systemach wykorzystujących oprogramowanie AXIS Camera Station lub współpracować z systemami VMS innych producentów w ramach porozumienia Application Development Partner Program. Ponadto kamery te mogą być wykorzystane w systemie AXIS Video Hosting System (AVHS) obok innych urządzeń zgodnych ze specyfikacją ONVIF, których konfiguracja wymaga zaledwie jednego kliknięcia myszką.

Kamery AXIS M3004 i AXIS M3005 będą w sprzedaży w trzecim kwartale 2012 roku.

Agata Majkucińska
Axis Communications

System liczenia osób podczas imprezy masowej na przykładzie Strefy Kibica w Warszawie

CBC Poland
Call.NET.pl

Na każdej imprezie masowej ma zmieścić się przewidywana liczba osób, a obowiązkiem organizatora jest dopilnowanie, aby tej liczby nie przekroczyć. Jeśli na przykład impreza odbywa się na stadionie, na podstawie informacji o sprzedanych biletach oraz danych z bramek wejściowych wiadomo dokładnie, ile osób znajduje się wewnątrz obiektu. Podczas organizowania Strefy Kibica z góry było wiadomo, że liczenie wchodzących osób musi być realizowane inną metodą

Warszawska Strefa Kibica była wydzielonym obszarem o powierzchni 12 hektarów, na który można było wejść poprzez jedną z siedmiu kilkunastometrowych bram. Zrezygnowano z liczenia osób za pomocą kołowrotów, przede wszystkim z powodu zbyt wysokich kosztów (jak na imprezę jednorazową) oraz w celu uniknięcia niepotrzebnego wstrzymywania tłumu podczas opuszczania Strefy Kibica. Liczenie za pomocą czujników diodowych zostało wykluczone ze względu na jego niedokładność, dość kłopotliwą instalację czujników i, wbrew pozorom, dość wysokie koszty związane z dużą liczbą bram.

Wybór padł na system wykorzystujący kamery zawieszone nad bramami, podłączone do specjalistycznych analizatorów obrazu marki GANZ, oraz oprogramowanie serwera raportów, którego producentem jest firma Call.NET.pl – właściciel marki VCN.

Analizatory wizyjne wraz z oprogramowaniem centralnego serwera raportów mają wiele funkcji związanych z liczeniem ludzi na danym obszarze. Możliwe jest też udostępnienie zasobów systemu oraz raportów poprzez przeglądarkę, bez względu na zastosowany system operacyjny (Mac OS, Linux, Windows, Android itp.).

Serwer umożliwia również dostęp do danych za pomocą odpowiednio przygotowanych plików w formacie XLS. Funkcja ta pozwala na łatwe tworzenie samoaktualizujących się raportów. Do ich przygotowania wystarczy podstawowa znajomość języka VBA dostępnego w pakiecie MS Excel. Analizatory wizyjne marki GANZ pełnią funkcję liczników dwukierunkowych, analizując ruch obiektów widzianych na obrazie. Przecięcie umownej linii podczas ruchu obiektu o ściśle zdefiniowanej wielkości w określonym kierunku powoduje zwiększenie stanu licznika. Bieżące stany liczników są przesyłane do serwera raportów poprzez sieć IP w postaci pakietów zawierających metadane. Analizator obsługuje jednocześnie czterdzieści umownych linii na jednym kanale wizyjnym, rozpoznając kierunek ruchu obiektu przecinającego którąś z tych linii. Taka struktura systemu z aktywnymi analizatorami nie obciąża analitycznie serwera raportów, dzięki czemu jeden serwer może obsłużyć z powodzeniem kilkaset pojedynczych liczników. Co więcej, system ten nie obciąża również sieci, gdyż nie ma potrzeby przesyłania strumieni wizyjnych. Dla serwera raportów istotne są jedynie gotowe metadane przychodzące z analizatorów GANZ, zajmujące w sieci niewielkie pasmo.

W opisywanym przypadku Strefy Kibica, ze względu na ogrom przedsięwzięcia (strefa miała pomieścić sto tysięcy osób), jak również jego pionierski charakter, nie dało się uniknąć problemów organizacyjno-technicznych.

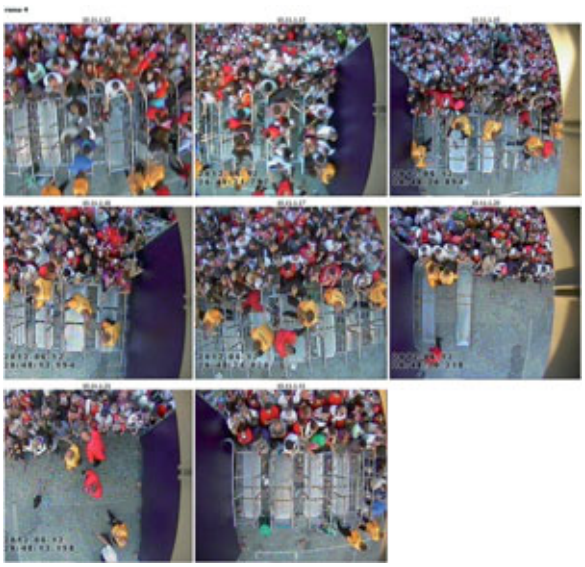
Podczas testów okazało się, że ruch pracowników ochrony, pilnujących wejść do strefy, powoduje, że wynik liczenia jest błędny. Rozwiązaniem problemu było przesunięcie wirtualnych linii zliczania oraz oznakowanie strefy przejścia tak, aby pracownicy ochrony wiedzieli, w którym miejscu następuje zliczanie.

Pewne problemy generowało również właściwe oświetlenie po zapadnięciu zmroku, a dokładniej cienie rzucane przez pojedyncze osoby. W tym przypadku należało inaczej skierować oświetlenie lub dodatkowo doświetlić przejścia z innych kierunków, tak żeby obserwowane obiekty były dobrze widoczne. Skutecznym rozwiązaniem okazała się jednak specjalna funkcja redukcji cienia, którą mają urządzenia GANZ i która sprawia, że cienie występujące w polu widzenia kamery są ignorowane.

Jednym z zadań systemu liczącego było podawanie na bieżąco, ile osób znajduje się w strefie. Zrealizowano to

Fot. 1. Enkoder jednokanałowy GANZ z analityką obrazu VCA

Fot. 2. Interfejs serwera raportów przedstawiający mapę sytuacyjną



Fot. 3. Podgląd weryfikacyjny obrazu z poszczególnych kamer biorących udział w procesie liczenia odwiedzających

poprzez uruchomienie sieciowego procesu sumowania liczby osób wchodzących i odejmowania liczby osób wychodzących ze strefy. Dane były aktualizowane w interwałach jednominutowych.

Specjalnie dla Strefy Kibica przygotowano mapę sytuacyjną, na której oznaczono wszystkie bramy (wejścia/wyjścia) i podawano bieżące informacje, a mianowicie:

– liczbę zliczeń danego dnia (z podziałem na poszczególne wejścia i wyjścia),
– liczbę osób w strefie w danej chwili (ta informacja szczególnie interesowała wszelkie służby w sztabie dowodzenia),
– liczbę wejść przez poszczególne bramki w ciągu ostatniej godziny i ostatnich piętnastu minut.

Specjalnie z myślą o Strefie Kibica stworzono narzędzie do jednoczesnego podglądu obrazów z dużej liczby kamer w jednym oknie. Miało to na celu bieżące weryfikowanie funkcjonowania przejść, to znaczy sprawdzanie, czy układ przejść przez poszczególne bramki nie został zmieniony i czy nie należy zmodyfikować ustawień kamer oraz umownych linii licznikowych.

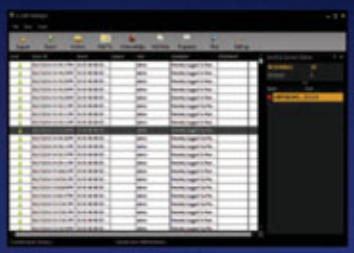
Dane otrzymywane z systemu umożliwiały ustalenie nie tylko liczby osób znajdujących się w danym momencie na terenie strefy, ale również liczby osób przechodzących przez poszczególne bramki i liczby osób odwiedzających strefę w ciągu jednego dnia oraz podczas całej imprezy. Szczególnie istotne jest to, że wszystkie te dane były uzyskiwane na bieżąco i wykorzystywane na wielu stanowiskach jednocześnie (m.in. przez sztab zarządzający, administratorów systemu, specjalistów od marketingu itp.).

Pomimo nieuniknionych zakłóceń pracy poszczególnych urządzeń osiągnięto założoną skuteczność systemu przekraczającą 90%. Była ona obliczana po zamknięciu strefy, na podstawie liczby osób odnotowanej przez system w stosunku do łącznej dziennej liczby odwiedzających, a także na podstawie testów przeprowadzonych przed uruchomieniem systemu.

CBC Poland
Call.NET.pl

OCHRONA OBWODOWA OBIEKTÓW CCTV

ZBAR


CMS

+

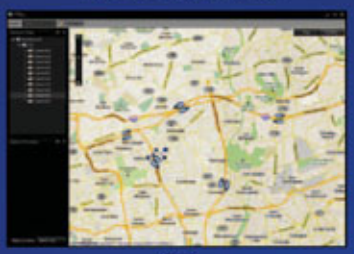

ANALIZA OBRAZU

+

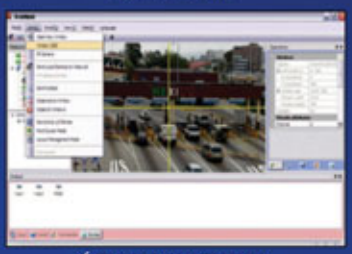

ŚLEDZENIE


DVR

+


GIS

+


ŚCIANA WIZYJNA


POWIADOMIENIA

+


NVR

+


KONTROLA DOSTĘPU

_ 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"

_"Command centre in-a-box"

- pierwszy na świecie system przedstawiający sytuację panującą na obiekcie za pomocą jednego serwera
- inteligentna analiza obrazu
- DVR - kamery analogowe
- NVR - kamery IP
- wspólna platforma operacyjna, która wyświetla informacje przy użyciu technologii Video Wall (do 40 monitorów)
- wspiera otwarte standardy producentów kamer
- posiada m.in. złącza: DVI, HD RGB, VGA, SDI, Ethernet
- możliwość równoległej obsługi przez kilku operatorów

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 · IFTER

DVR 670
nowy rejestrator firmy Bosch

Bosch Security Systems

Bosch rozszerza serię popularnych rejestratorów wizyjnych 600 Advantage Line i wprowadza na rynek model DVR 670, czyli kompleksowe rozwiązanie do zarządzania sygnałem wizyjnym zawarte w jednej kompaktowej jednostce

Rejestrator DVR 670 wykorzystuje wysoce wydajną technologię kompresji H.264, która gwarantuje doskonałą jakość obrazu przy niskich wymaganiach dotyczących szerokości pasma i pojemności dysku. Dzięki temu możliwy jest zapis obrazów z szesnastu kanałów równocześnie w czasie rzeczywistym, w rozdzielczości 4CIF, z szybkością 400 obrazów na sekundę, co daje 25 kl./s z każdego kanału.

Systemem można zarządzać lokalnie, za pomocą klawiatury Bosch IntuiKey, myszy, pilota do zdalnego sterowania lub z panelu przedniego urządzenia. Wszystkie modele rejestratorów DVR 670 (DVR-670-08A000, DVR-670-16A000) są wyposażone w przelotowe złącza klawiaturowe. Dzięki temu za pomocą jednej klawiatury IntuiKey można obsługiwać nawet 16 rejestratorów.

Model DVR 670 oferuje też szereg opcji zdalnego zarządzania (za pośrednictwem sieci Ethernet), które umożliwiają podgląd sygnału wizyjnego, dostęp do archiwum, sterowanie wieloma rejestratorami oraz zdalną konfigurację. Funkcje te są zaimplementowane w darmowym oprogramowaniu Bosch Control Center oraz Bosch Video Client.

Dostęp do urządzenia jest możliwy za pośrednictwem przeglądarki internetowej w której nie trzeba instalować dodatkowych aplikacji. Dostępna jest również aplikacja dostosowana do urządzeń mobilnych, która pozwala na podgląd i sterowanie kamerami PTZ.

W przypadku aktywacji wejścia alarmowego rejestratora DVR 670 istnieje możliwość wysłania 10-sekundowego wideoklipu dodawanego automatycznie do powiadomienia alarmowego przesyłanego pocztą e-mail.

Operatorzy z pewnością docenią także funkcje usprawniające pracę służb ochrony, na przykład inteligentne wyszukiwanie (*Smart Search*), które umożliwia szybkie odnalezienie kluczowych zdarzeń w zarejestrowanym materiale.

Nowy rejestrator DVR 670 chroni wybrane nagrania przed przypadkowym nadpisaniem. Całe nagranie jest oznakowane cyfrowo, co gwarantuje jego autentyczność, a oprogramowanie odtwarzające uwierzytelnione materiały archiwalne umożliwia dostęp do wybranych scen na dowolnym komputerze.

DVR 670 jest dostępny w wersjach różniących się pojemnością pamięci dyskowej. Można też zamówić model z wbudowaną nagrywarką DVD.

Bardzo prosta instalacja rejestratora DVR 670 oraz jego intuicyjna obsługa sprawiają, że użytkownik nie potrzebuje specjalistycznego przeszkolenia. Po podłączeniu urządzenia należy tylko wybrać język, ustawić datę i godzinę, a zapis rozpocznie się automatycznie. Łatwo zauważalną zaletą rejestratora jest wysoki stopień jego niezawodności, który obniża ogólny koszt eksploatacji.

Jak wszystkie produkty linii Advantage Line, rejestrator DVR 670 stworzono z myślą o małych i średnich instalacjach – w szkołach, sklepach, bankach i hotelach. Sprawdzi się także w większych przedsiębiorstwach mających kilka lokalizacji.

Linia produktów Advantage doskonale spełni swoje zadanie w systemach dozoru w relatywnie małych obiektach, takich jak sklepy, restauracje, apteki, stacje benzynowe, szkoły i małe biura. W obiektach tych często brakuje niezawodnych systemów zabezpieczeń. Firma Bosch oferuje kamery cyfrowe i analogowe, cyfrowe rejestratory wizyjne, systemy sygnalizacji pożarowej (centrale sygnalizacji pożarowej, optyczne czujki pożarowe, ręczne ostrzegacze, sygnalizatory) oraz systemy nagłośnieniowe (wzmacniacze, stacje wywoławcze, mikrofony, głośniki kolumnowe, sufitowe i tubowe, regulatory głośności) stworzone z myślą o małych i średnich instalacjach.

Urządzenia należące do Advantage Line są niezawodne, trwałe i charakteryzują się doskonałą jakością. Ich instalacja, konfiguracja oraz obsługa jest prosta i intuicyjna, a wymagania dotyczące serwisowania i konserwacji są minimalne. Inne zalety tego rozwiązania to kompleksowość oferty, atrakcyjna cena oraz dostępność u lokalnych dystrybutorów. To idealna propozycja dla firm poszukujących optymalnego zabezpieczenia.

W sierpniu 2012 została uruchomiona telefoniczna infolinia (+48 22 206 4000), dzięki której można uzyskać informacje na temat serii Advantage Line, dotyczące produktów, nowości i aktualnych promocji, a także wsparcie techniczne. Informacje o Advantage Line można także uzyskać, pisząc na adres *AdvantageLine-Support@bosch.com*. Infolinia działa od poniedziałku do piątku w godzinach 8:00–20:00.

Bosch Security Systems

Możesz liczyć na Q24

Jakub Sobek

Coraz rzadziej urządzenia elektroniczne są przeznaczone tylko do jednego zastosowania – np. telefon już dawno przestał nam służyć tylko do prowadzenia rozmów. Trend ten dotyczy zwłaszcza urządzeń wykorzystujących najnowsze technologie. Firma Mobotix, która do tej pory oferowała kamery przeznaczone przede wszystkim do ochrony obiektów postanowiła umożliwić zupełnie nowe zastosowanie jednego ze swoich flagowych produktów, jakim jest kamera hemisferyczna Q24

Technologia hemisferyczna

Hemisferyczna kamera Mobotix Q24 o kącie widzenia równym 360 stopni tworzy obraz, na którym widoczne jest jej całe otoczenie. Dzięki wysokiej rozdzielczości kamery, obraz utworzony z wykorzystaniem funkcji vPTZ ma wysoką jakość. Możliwy jest podgląd na żywo i przeglądanie już zarejestrowanych sekwencji. W przypadku kamery Mobotix nigdy nie tracimy z oczu żadnego z obszarów obserwowanego pomieszczenia.

Kamera hemisferyczna Mobotix nie jest kolejną kamerą z obiektywem typu rybie oko. Inne kamery megapikselowe, które są wyposażone w obiektyw tego typu, wytwarzają zwykle obraz kiepskiej jakości, a ponadto potrzebny jest bardzo dobry komputer lub serwer, który będzie potrafił dokonać obróbki takiego obrazu.

Oprócz zwykłego procesora sygnałowego DSP w kamerze Mobotix Q24 został zastosowany dodatkowy procesor ARM korygujący perspektywę obrazu oraz przygotowujący strumień danych do transmisji przez sieć. Tak przygotowany obraz nie obciąża komputera, na którym jest dalej przetwarzany. Ponadto dzięki temu jeden komputer może służyć do wyświetlania obrazów z wielu kamer hemisferycznych. Co więcej, w dużo bardziej optymalny sposób wykorzystywana jest przepustowość sieci, ponieważ nie musi być przesyłany oryginalny obraz w formacie RAW.

Wbudowany procesor ARM umożliwia decentralizację systemu monitoringu wizyjnego. Również dzięki temu kamera Mobotix – poza korekcją perspektywy – może także dokonywać analizy obrazu i obróbki strumienia wizyjnego, zarządzać procesem nagrywania, obsługiwać zdarzenia alarmowe i podejmować zaprogramowane akcje, zmieniać stany wyjść, wysyłać e-maile i SMS-y z informacjami itp. Wszystko to odbywa się bez udziału komputera i dodatkowego oprogramowania.

Technologia hemisferyczna tak bardzo spodobała się klientom na całym świecie, że firma Mobotix postanowiła wprowadzić nową linię kamer S14. Kamery S14 są produkowane w dwóch wersjach – Mono oraz Dual. Wersja Mono zawiera jeden obiektyw hemisferyczny znajdujący się bezpośrednio przy kamerze. Od kamery Q24 odróżnia ją obudowa i sposób montażu – kamera może zostać zamocowana w taki sposób, że widoczny jest jedynie jej obiektyw. Kamera S14 Dual składa się z elementu centralnego oraz dwóch przewodów o dwumetrowej długości. Na końcu każdego z przewodów znajdują się niewielkie moduły z przetwornikami obrazu oraz obiektywami hemisferycznymi. Taka konstrukcja kamery umożliwia jej dyskretny montaż, a dzięki długim przewodom za pomocą jednej kamery możemy niezależnie monitorować dwa pomieszczenia.

Analityka obrazu

Duża moc obliczeniowa kamery Q24 pozwoliła firmie Mobotix wprowadzić do niej nowe oprogramowanie oferujące zupełnie nowe analityczne funkcje wizyjne.

Tradycyjne rozwiązania zawsze wymagały stosowania dodatkowego komputera oraz oprogramowania, co ograniczało skalowalność. W przypadku kamery Q24 wszystkie operacje związane z przetwarzaniem danych może wykonywać kamera. Najważniejsze funkcje analityczne kamery Mobotix Q24 to

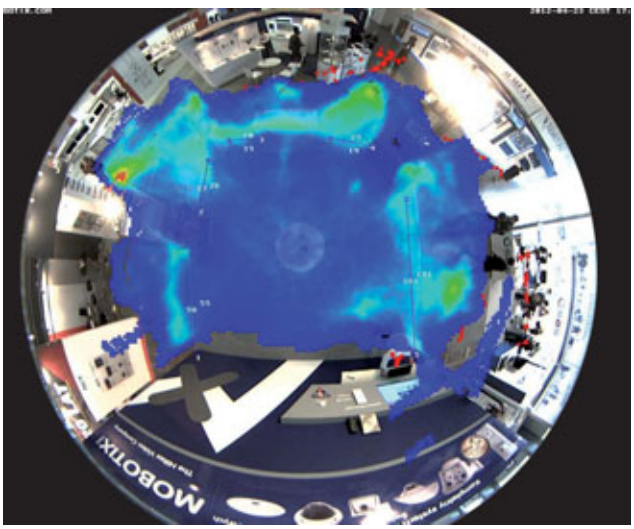
Fot. 1. Kamera hemisferyczna Mobotix Q24

między innymi funkcja zliczania klientów oraz funkcja tworzenia map cieplnych.

Funkcja zliczania osób jest szczególnie przydatna w sklepach czy centrach handlowych, czyli wszędzie tam, gdzie jest duży ruch osobowy i wymagane jest gromadzenie danych dotyczących jego natężenia. Kamera może zliczać osoby przekraczające różne wirtualne linie, np. klientów przechodzących przez kilka bramek w sklepie.

Q24 zbiera wszystkie dane i może je okresowo przesyłać do serwera lub wysyłać na wskazany adres e-mailowy. Dane mogą być przekazywane w formacie HTML lub CSV, co jest szczególnie pomocne, jeśli raporty mają być dalej przetwarzane i obrabiane. Istnieje możliwość zaprogramowania dobowego lub dokładniejszego, godzinowego trybu zliczania klientów.

Konwencjonalne urządzenia do zliczania osób są często montowane we framugach drzwi, przez co zliczanie nie zawsze jest precyzyjne – jeśli trzy osoby przechodzą przez drzwi w tym samym momencie, tradycyjny czujnik odnotowuje tylko jedno przejście. W przypadku zastosowania kamery Mobotix odnotowywane jest przejście każdej osoby. Ważne jest także to, że dla każdej zdefiniowanej wirtualnej linii granicznej można zdefiniować dwa liczniki reagujące na jej przekraczanie w określonym kierunku.



Fot. 2. Mapa cieplna oraz linie zliczające klientów zaprezentowane na obrazie z kamery Mobotix Q24

Funkcja zliczania klientów umożliwia zebranie bardzo dużej ilości danych. Co jednak zrobić, gdy same dane liczbowe nie są dla nas wystarczające lub ich analiza może być zbyt żmudna i czasochłonna? Wówczas pomocna może okazać się kolejna funkcja, tzw. mapa cieplna. Dzięki niej ruch widoczny na obserwowanym obszarze jest ciągle analizowany, a kamera przedstawia w sposób graficzny, w których miejscach ruch osób jest najbardziej intensywny. W przypadku sklepu taka analiza umożliwia sprawdzenie, jakimi ciągami komunikacyjnymi najczęściej poruszają się klienci lub skąd najczęściej oglądane są towary znajdujące się na poszczególnych wystawach. Dzięki temu można dokonać korekty ustawienia regałów i lepiej ułożyć towary, aby zwiększyć sprzedaż w danym punkcie.

Dużą zaletą wprowadzonych nowości jest to, że wszystkie nowe funkcje są dostępne dla klientów, którzy kupili kamerę Q24 z wcześniejszą wersją oprogramowania. Wystarczy zaktualizować oprogramowanie, by nowe funkcje stały się dostępne.

Korzyści wynikające z zastosowania kamer Mobotix Q24 mogą być czerpane przez różne działy przedsiębiorstw – przede wszystkim przez dział ochrony, ale także działy logistyki, marketingu, zarządzania i planowania.

Dzięki kamerze Mobotix Q24 w obiekcie nie trzeba stosować osobnych urządzeń służących do monitoringu i do zliczania osób, z których każde wymaga osobnego oprogramowania – korzystamy z jednego dedykowanego oprogramowania lub przeglądarki internetowej. Dzięki temu można znacznie obniżyć całkowity koszt inwestycji, gdyż redukowane są koszty okablowania, zakupu wielu urządzeń oraz ich zasilania. Istotny jest również fakt, że przy tworzeniu instalacji bazujących na produktach Mobotix zawsze wykorzystywane są standardowe elementy sieciowe. Dzięki temu można wybrać urządzenia sieciowe dowolnej marki.

Fot. 3. Najnowsza podwójna kamera hemisferyczna Mobotix S14D

Podsumowanie

Firma Mobotix nie tylko tworzy coraz doskonalsze i coraz bardziej funkcjonalne urządzenia, ale także stara się udoskonalać produkty będące już na rynku. Najlepszym tego przykładem jest rozszerzenie funkcjonalności kamer Q24. Jest to jeden z powodów, dla których warto tworzyć systemy bazujące na kamerach Mobotix. Mamy gwarancję, że system przez cały czas będzie miał bardzo dobre wsparcie techniczne, dostępne będą aktualizacje i będzie można go rozbudować z wykorzystaniem nowych urządzeń Mobotix.

Bardzo duży nacisk na rozwój produktów, wysoką jakość ich wykonania oraz trwałość sprawia, że firma Mobotix jest liderem w branży kamer IP o wysokich rozdzielczościach. Mamy nadzieję, że już wkrótce będziemy mieli przyjemność poinformować o kolejnych nowościach.

Jakub Sobek
Linc Polska

Mobotix – mity

Rozdzielczość 3.1 megapikseli to zbyt mało w przypadku kamery hemisferycznej!

Taka rozdzielczość kamery hemisferycznej jest w zupełności wystarczająca, aby uzyskać obraz o bardzo wysokiej jakości. Warto zwrócić uwagę na to, że w nowej kamerze został zastosowany przetwornik obrazu o wielkości ½". Dzięki temu kamera ma większą czułość, a obraz jest mniej zaszumiony. Oczywiście sprzedawcy kamer zawsze będą próbować prześcigać się w dziedzinie liczby megapikseli, jednak warto pamiętać, że rozdzielczość nie jest jedyną właściwością wpływającą na jakość obrazu.

Kamery Mobotix są drogie!

Trzeba zawsze porównywać ceny urządzeń tej samej klasy. Kamery Mobotix oferują jakość oraz funkcjonalność, której wielu producentów sprzętu nie potrafi zapewnić. Nie można patrzeć wyłącznie na cenę produktu. Kamery Mobotix pozwalają znacznie obniżyć koszty instalacji, gdyż nie trzeba kupować dodatkowych obudów oraz grzałek. Klient nie ponosi kosztów licencyjnych w związku z zastosowaniem oprogramowania VMS. Znacznie obniżony jest koszt instalacji zasilającej cały system.

Kamery IP o wysokich rozdzielczości wymagają sieci o dużej przepustowości

Wiele kamer innych firm rzeczywiście wymaga sieci o dużej przepustowości, ale kamery Mobotix nie. Dzięki wbudowanemu procesorowi i obróbce obrazu w kamerze nie musimy przesyłać przez sieć całego obrazu, nawet jeśli obraz ten chcemy oglądać na żywo. Kamera przesyła przez sieć obraz zoptymalizowany. Dzięki możliwości rejestracji obrazu na karcie microSD o maksymalnej pojemności 64 GB kamera w ogóle nie musi przesyłać obrazu przez sieć w celu jego rejestracji.

profesjonalne rozwiązania
do cyfrowej rejestracji obrazu

ponad 60 000 instalacji
pracujących na całym świecie

www.alnetsystems.com

ALNET SYSTEMS

sieciowe oprogramowanie do cyfrowej rejestracji obrazu — NS NETSTATION

hybrydowy system do cyfrowej rejestracji obrazu — NET HYBRID

hybrydowy system do cyfrowej rejestracji obrazu HD-SDI — NET HYBRID HD

profesjonalne oprogramowanie klienckie — CMS PROFESSIONAL

oprogramowanie klienckie dla urządzeń mobilnych — CMS MOBILE

blisko 1000 kamer zintegrowanych
z oprogramowaniem Alnet Systems

wybór należy do Ciebie!

ACTi · Arecont Vision · AXIS · BASLER · NOVUS · ETROVISION · GANZ
HIKVISION · iCANTEK · IQinVision · JVC · LILIN · Lumenera · PELCO · MESSOA
Panasonic · SANYO · SAMSUNG · SONY · StarDot · Apeer IP · VIVOTEK · ZAVIO

ipGO sieciowy system typu plug and play marki NOVUS

Patryk Gańko

W dotychczasowych artykułach publikowanych na łamach magazynu *Zabezpieczenia* przedstawiałem zalety wybranych elementów systemu monitoringu wizyjnego: rejestratorów, kamer czy też oprogramowania. W niniejszym artykule chciałbym przedstawić pełny system nadzoru wizyjnego IP składający się z kamer, sieciowych rejestratorów i oprogramowania. Prezentowany system jest autonomiczny i nie może być łączony z dodatkowymi urządzeniami. To ograniczenie implikuje ważną zaletę: prostotę instalacji. Urządzenia są zaprogramowane i przystosowane do natychmiastowego użycia bez żadnej dodatkowej konfiguracji, a ustawienia sieciowych rejestratorów wizji (NVR – Network Video Recorder) są takie same jak w systemach analogowych

Wielu instalatorów obawia się zastąpienia stosowanych dotychczas rozwiązań analogowych rozwiązaniami całkowicie cyfrowymi. Wynika to z wysokich wymagań dotyczących umiejętności konfiguracji i obsługi urządzeń sieciowych. System ipGO jest gotowy do działania zaraz po włączeniu (*plug and play*). Kamery stosowane w systemie nie posiadają własnego interfejsu sieciowego, a ustawień dokonuje się w menu rejestratora – można określać nazwy kamer oraz ustawiać właściwości obrazu, strefy prywatności i strefy detekcji ruchu. Konfiguracja nie obejmuje natomiast żadnych ustawień sieciowych kamer, tzn. wyszukiwania urządzeń w sieci i nadawania im unikalnych adresów IP.

Podczas tworzenia systemu nie trzeba stosować przełączników sieciowych, ponieważ rejestratory NVR mają wbudowane cztero- lub ośmiokanałowe (w zależności od liczby obsługiwanych kamer) przełączniki sieciowe. Dzięki podwójnemu systemowi zasilania (w zestawie znajdują się dwa zasilacze: do rejestratora 12 V_{DC} oraz do kamer PoE 48 V) kamery są zasilane metodą PoE bezpośrednio z rejestratora co znacznie upraszcza instalację kamer.

Łatwość instalacji idzie w parze z bardzo wysoką rozdzielczością i jakością obrazów, nieosiągalną dla systemów analogowych. Rejestratory NVR mogą zapisywać strumień wizyjny w rozdzielczości Full HD (1920×1080) z prędkością do 25 klatek na sekundę dla każdego kanału.

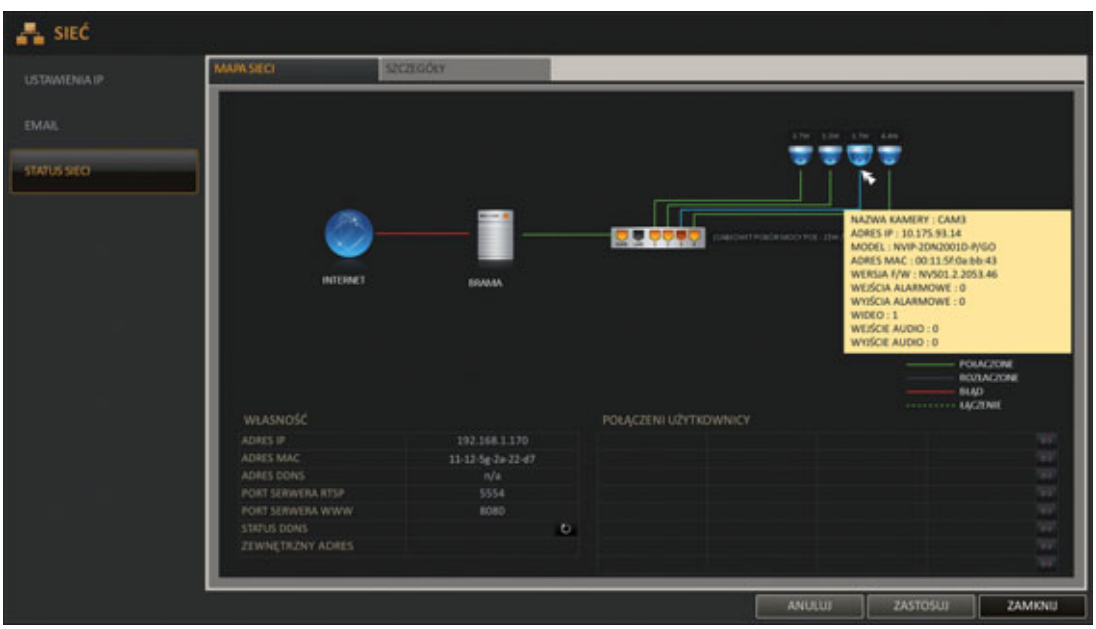
Dostępne są dwa modele kamer przeznaczone do pracy w systemie ipGO: kopułowa NVIP-2C2001D-P/GO oraz klasyczna motor-zoom NVIP-2C5005CZ-P/GO. Oba modele są kamerami kolorowymi z funkcją dzień/noc realizowaną elektronicznie oraz wysoką czułością wynoszącą 0,63 lx. W złych warunkach oświetleniowych automatycznie włączana jest funkcja wydłużenia czasu otwarcia migawki elektronicznej. Dostępność dwóch strumieni wizyjnych pozwala na dynamiczne zarządzanie zasobami sieci i rejestratora. Przy podglądzie pełnoekranowym obraz jest wyświetlany w najwyższej rozdzielczości (Full HD), natomiast w przypadku wyświetlania obrazów na podzielonym ekranie wykorzystywany jest drugi strumień o niższej rozdzielczości równej 640×480. Ogniskowa obiektywu zmienia się w zakresie od 5 mm do 25 mm, co pozwala na pięciokrotne powiększenie obrazu na drodze optycznej.

W kamerach zastosowano przetworniki CMOS umożliwiające generowanie strumienia wizyjnego o rozdzielczości 1920×1080 i prędkości odświeżania do 25 klatek na sekundę (strumień Full HD).

Urządzenia mają wbudowany mechanizm, który dokonuje automatycznej korekcji w przypadku uszkodzenia pojedynczych pikseli. Dla uszkodzonego piksela interpolowana jest wartość sąsiednich pikseli.

Sieciowe rejestratory ipGO wykorzystują system operacyjny Linux i pracują w trybie triplex, zapewniając równoczesny zapis, podgląd na żywo lub odtwarzanie nagrań. W rejestratorach można zamontować do dwóch dysków SATA oraz jeden dysk zewnętrzny eSATA o maksymalnej pojemności równej 2 TB. W związku z wysoką rozdzielczością kamer konieczne było zastosowanie wyjścia monitorowego o odpowiedniej nominalnej rozdzielczości. Rejestrator współpracuje z monitorami cyfrowymi o rozdzielczości 1080p, wyposażonymi w złącze HDMI lub DVI. W przypadku używania monitora z wejściem DVI należy dodatkowo zaopatrzyć się w konwerter HDMI - DVI.

Podczas lokalnego przeglądania zarejestrowanych nagrań można posługiwać się osią czasu i za pomocą myszy wskazywać wybrany fragment materiału archiwalnego, wskazać konkretną datę i czas, wyszukać określone zdarzenia. Istnieje możliwość włączenia trybu szybkiego podglądu. Jest to szczególne przydatne podczas weryfikacji przebiegu zarejestrowanych zdarzeń – można automatycznie przejść do odtwarzania fragmentów cofniętych w czasie o 10, 20, 30 lub 60 sekund. Ponadto fragmenty zarejestrowanego materiału mogą być wyszukiwane na podstawie analizy treści obrazu. W tym celu wyświetlane fragmenty są przesunięte względem siebie o zdefiniowany interwał czasowy. Dzięki temu można łatwo określić, kiedy nastąpiła szukana zmiana w obrazie (np. zniknięcie przedmiotu). Zarówno w przypadku wyświetlania obrazów



Fot. 1. Status sieci

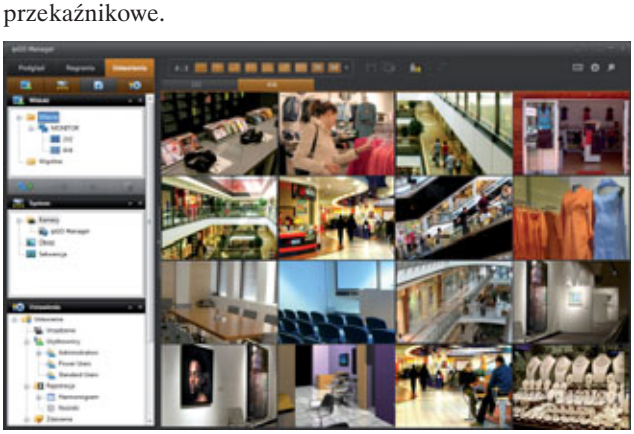
Fot. 2. Urządzenia systemu ipGO

w trybie na żywo, jak i odtwarzania obrazów archiwalnych dostępna jest funkcja zoomu cyfrowego.

Zapisany materiał wizyjny może być kopiowany na zewnętrzną pamięć flash lub dysk przez port USB, może być przenoszony na serwer FTP lub odtwarzany poprzez klienta sieciowego w dwóch formatach: AVI oraz RAW. Format RAW umożliwia równoczesne odtwarzanie wielu kanałów. Materiał zarchiwizowany na zewnętrznych nośnikach może być odtwarzany bezpośrednio z rejestratora. Dane zawierają znak wodny, którego autentyczność jest weryfikowana w rejestratorze.

W przypadku systemu obsługiwanego przez różnych użytkowników (operator, konserwator, instalator, administrator) ważne jest zróżnicowanie uprawnień dotyczących dostępu lokalnego i zdalnego. Zróżnicowanie to dotyczy wyszukiwania i odtwarzania nagrań, archiwizacji nagrań, konfiguracji systemu, konfiguracji parametrów nagrywania, kontroli wyjścia alarmowego i zdarzeń alarmowych, zdalnego logowania do systemu, wyłączania urządzenia oraz ukrywania obrazów pochodzących z wybranych kamer przed poszczególnymi użytkownikami.

W przypadku niektórych zdarzeń (detekcja ruchu, aktywacja wejścia alarmowego, zanik sygnału wizyjnego) system może aktywować wyjście alarmowe zgodnie z ustalonym harmonogramem. Można również ustawić wysyłanie powiadomień e-mail oraz sygnalizację dźwiękową i wizualną. Rejestratory NVR mają dwa wejścia alarmowe i jedno wyjście przekaźnikowe.



Fot. 3. Interfejs graficzny aplikacji ipGO Manager

Użytkownik może otrzymywać informacje o zdarzeniach odnotowywanych w rejestratorze (awaria wentylatora, uruchamianie urządzenia, błąd logowania, przekroczenie zdefiniowanej temperatury, przekroczenie dopuszczalnego poboru energii z zasilacza PoE, przerwanie połączenia z Internetem oraz błąd aktualizacji DDNS) i uruchamiać odpowiednie powiadamianie.

Ostatnim elementem systemu ipGO jest oprogramowanie sieciowe ipGO Manager. Program pozwala efektywnie zarządzać zarówno pojedynczym urządzeniem, jak i rozproszonym systemem sieciowym. Z rejestratorem pracującym w trybie podglądu na żywo lub odtwarzania może połączyć się jednocześnie pięciu operatorów. Dodatkowo możliwa jest zdalna konfiguracja rejestratora.

Aplikacja ipGO Manager może powielać okna z obrazem w zależności od liczby wyjść monitorowych dostępnych w komputerze. W każdym z okien, czyli na każdym monitorze, może być wyświetlany obraz z jednej z 64 kamer. Dla każdego okna użytkownicy mogą definiować zaawansowane rozkłady obrazów z kamer, które dodatkowo dostosowane są do monitorów panoramicznych. Wyświetlane obrazy mogą być przechwytywane i drukowane.

Funkcja sekwencyjnego wyświetlania może również dotyczyć wybranego okna podziału, w którym cyklicznie wyświetlane są obrazy ze zdefiniowanych kamer. Ponadto w niewykorzystanych oknach podziału mogą zostać wyświetlone dowolne materiały graficzne – plany budynku czy firmowe znaki graficzne.

Rozwiązanie ipGO, które zadebiutowało na polskim rynku w lipcu bieżącego roku, jest ciągle udoskonalane. Oferta zostanie w najbliższym czasie uzupełniona o 16-kanałowy rejestrator sieciowy oraz kompatybilne kamery. System ipGO, przeznaczony dla użytkowników niezaawansowanych, łączy zalety systemów cyfrowych, czyli przede wszystkim wysoką jakość i rozdzielczość zapisywanych strumieni wizyjnych, z łatwością instalacji i konfiguracji.

Patryk Gańko
AAT Holding

Ty i Twoi klienci możecie spać bezpieczniej

z systemem PowerMaxExpress!

Wysoce stabilny i **niezawodny**
bezprzewodowy system alarmowy

Oszczędzasz czas i **pieniądze**
dzięki szybkiej i bezproblemowej instalacji!

Visonic
A Tyco International Company

Wyłączny dystrybutor produktów Visonic 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

Wizerunek w sieci

Wykorzystywanie cudzego wizerunku w celach komercyjnych oraz popełnianie cyberprzestępstw

Monika Brzozowska

Wizerunek osoby fizycznej jest dobrem prawnym coraz bardziej dostrzegalnym w społeczeństwie polskim. Wraz z rozwojem gospodarczym i edukacyjnym oraz bogaceniem się społeczeństwa jego członkowie coraz częściej starają się nie tylko zwalczać naruszenia takich dóbr jak własność czy zdrowie, lecz również tych nieco bardziej wysublimowanych, czego doskonałym przykładem jest wizerunek

Wizerunek a regulacje prawne

Problematyka ochrony wizerunku jest uregulowana zarówno na płaszczyźnie konstytucyjnej, jak również ustawowej – w kodeksie cywilnym (wizerunek jest dobrem osobistym) oraz w ustawie o prawie autorskim i prawach pokrewnych.

W związku z rozwojem Internetu, cyberspołeczności i cyberprzestrzeni, w której informacje o ludziach są rozpowszechniane – często bez ich wiedzy i zgody – ochrona wizerunku jest bardzo ważna.

Fundamentalne znaczenie mają normy prawne zawarte w ustawie o prawie autorskim i prawach pokrewnych. Zgodnie z art. 81 ust. 1 ww. ustawy rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W przypadku braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie, przy czym, jak precyzuje ust. 2 przedmiotowego artykułu, zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Z powyższego przepisu wynika wyraźnie, że z zasady na rozpowszechnianie wizerunku należy mieć zgodę osoby prezentowanej na zdjęciu. Nie ma przy tym wymogu otrzymania zgody na piśmie, tak jak w przypadku uwzględniania praw autorskich. Wyrażenie akceptacji na rozpowszechnianie wizerunku może nastąpić w każdy sposób (ustnie, pisemnie, poprzez wiadomość e-mailową lub akceptację postanowień regulaminu). Istotne jest jednak to, że oświadczenie o wyrażeniu zgody powinno mieć jednoznaczny charakter – nie dopuszcza się bowiem tzw. dorozumianej zgody na rozpowszechnianie wizerunku. Takie rozwiązanie ma na celu umożliwienie wyciągnięcia konsekwencji prawnych na przykład w przypadku, gdy zostanie wyrażona zgoda na ograniczone wykorzystanie wizerunku, a mimo to zostanie on wykorzystany w innej formie, miejscu i czasie lub w innych okolicznościach (innym kontekście).

A zatem od zasady zgody na rozpowszechnianie wizerunku istnieją ustawowo przewidziane wyjątki, które zgodnie z zasadą *exceptiones non sunt extendendae* powinny być interpretowane ściśle. Można zatem rozpowszechniać wizerunek osoby powszechnie znanej (tzw. osoby publicznej), a także wizerunek, który stanowi jedynie szczegół większej całości. Można byłoby również uznać, że prośba o zgodę nie jest potrzebna, gdy osoba otrzymuje wynagrodzenie za pozowanie, ale w istocie zgoda jest wymagana, tyle że jej przejawem ma być przyjęcie wynagrodzenia.

Obrona przez naruszeniami prawa do wizerunku

Zarówno przepisy kodeksu cywilnego, według których prawo do wizerunku jest dobrem osobistym, jak i przepisy ustawy o prawie autorskim i prawach pokrewnych zapewniają dość bogaty arsenał środków prawnych na wypadek naruszenia prawa do wizerunku. Nie ma żadnych przeciwwskazań (poza ograniczeniami faktycznymi) do odnoszenia tych roszczeń do wizerunku w cyberprzestrzeni.

Mając na względzie art. 24 kodeksu cywilnego oraz art. 83 w zw. z art. 78 ustawy o prawie autorskim i prawach pokrewnych, należy wskazać, że w razie naruszenia prawa do wizerunku osoba uprawniona może żądać:

– zaniechania dalszego rozpowszechniania wizerunku,
– doprowadzenia do usunięcia skutków naruszenia prawa do wizerunku,
– otrzymania nawet trzykrotności wartości wynagrodzenia za wykorzystanie wizerunku (gdy naruszenie tego prawa ma charakter zawiniony),
– odszkodowania za doznaną krzywdę związaną z naruszeniem,
– przekazania określonej sumy na wskazany przez uprawnionego cel społeczny.

Nie tylko cywilnie!

Wizerunek jest chroniony nie tylko przez prawo cywilne. Od 6 czerwca 2011 roku obowiązuje bowiem art. 190a § 2 kodeksu karnego, który wprowadza do polskiego porządku prawnego przestępstwo tzw. kradzieży tożsamości. Zgodnie z tym przepisem karze pozbawienia wolności do lat trzech podlega ten, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. W kontekście cyberprzestępczości przestępstwo takie może polegać np. na utworzeniu konta w portalu społecznościowym z wykorzystaniem cudzego wizerunku lub opublikowaniu strony internetowej o podobnym charakterze. Istotne jest jednak to, że sprawca w takich przypadkach musi działać intencjonalnie, a jego motywacją musi być wyrządzenie szkody majątkowej lub osobistej pokrzywdzonemu. Działanie sprawcy nie musi być jednak powtarzalne (uporczywe) – jak np. w przypadku nękania (stalkingu).

Ustawodawca, przewidując że kradzież tożsamości może mieć drastyczny charakter i wpływać znacząco na psychikę pokrzywdzonego, wprowadził typ kwalifikowany zabronionego czynu kradzieży tożsamości przez następstwo. Zgodnie z art. 190a § 3 kodeksu karnego surowszej odpowiedzialności (kara pozbawienia wolności do lat dziesięciu) podlega sprawca omawianego przestępstwa, jeśli pokrzywdzony targnie się na własne życie. Nie musi dojść do śmierci w wyniku próby samobójczej, by przestępstwo zostało uznane za dokonane.

Jak to często przyjmuje się w przypadku przestępstw dotykających sfer prywatnych lub nawet intymnych, przestępstwo kradzieży tożsamości ma charakter wnioskowy. Oznacza to, że nie można pociągnąć do odpowiedzialności karnej sprawcy, gdy nie chce tego pokrzywdzony.

Jak pokazuje praktyka, istniało zapotrzebowanie na wprowadzenie art. 190a kodeksu karnego. Przepis ten, zarówno w odniesieniu do stalkingu (§ 1), jak również w przypadku kradzieży tożsamości (§ 2), jest coraz częściej wykorzystywany, przy czym zaangażowanie policji lub prokuratury jest często o wiele skuteczniejsze niż środki cywilnoprawne, gdyż często występują dość poważne trudności w identyfikacji sprawcy naruszenia prawa do wizerunku.

Podsumowując, należałoby stwierdzić, że prawo do wizerunku podlega kompleksowej ochronie prawnej. Nie zmianie to jednak faktu, że duże znaczenie powinny mieć również działania prewencyjno-profilaktyczne uprawnionych, chociażby takie jak niepochopne rozpowszechnianie wizerunku czy zabezpieczenie plików przed ich dostaniem się w niepowołane ręce bądź przed ich nieskrępowaną modyfikacją.

adwokat Monika Brzozowska
kierownik Departamentu Prawa Własności Intelektualnej i Danych Osobowych w kancelarii Pasieka, Derlikowski, Brzozowska i Partnerzy

ZASIĘG
AŻ DO 240
METRÓW

TECHNOLOGIA LED SMD

ŻYWOTNOŚĆ: 11 LAT

WYDAJNOŚĆ: +20%

OSZCZĘDNOŚĆ ENERGII

NISKIE KOSZTY

5 LAT GWARANCJI

VIDEOTEC

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.

Depozytor na klucze systemowe SAIK LOCK

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 ilości 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

SAIK SOFT

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

Kamera SCN-23Z27F

Kamera **SCN-23Z27F** to nowa kamera szybkoobrotowa z rodziny **Xpeed** o bardzo wysokiej czułości wynoszącej 0,0005 lx i rozdzielczości 580 TVL, wyposażona w system DSS – Digital Slow Shutter pozwalający na zwiększenie czułości przy słabym oświetleniu. Zastosowanie sprawdzonego procesora DSP Monalisa II pozwoliło osiągnąć wysoką jakość obrazu, z zachowaniem niskiej ceny kamery.

Wśród zalet kamery warto wymienić możliwość obrotu o 360°, funkcję Auto-Flip, powrót do ustalonego ustawienia w razie bezczynności operatora (parking), albo rozpoczęcie wykonywania zadanej funkcji np. makroinstrukcji, 128 presetów, 8 tras skanowania, 4 makr, 8 stref prywatności. Kamery Xpeed są skonstruowane tak by maksymalnie ułatwić prace instalacyjne, między innymi są zabezpieczone przed upadkiem w czasie montażu. Kamera jest także produkowana w wersji wewnętrznej SBN-23Z27F.

Zaletami kamery są

- Nowoczesny procesor DSP Monalisa II
- Czułość w nocy zwiększa funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 128 ramek
- Odsuwany filtr IR, dzięki czemu uzyskuje się bardzo dobre wierne odwzorowanie kolorów
- Prędkość obrotowa 360°/s
- Zoom optyczny 27x , zoom cyfrowy 10x, zoom całkowity x270x
- 8 stref prywatności
- Łatwa obsługa poprzez OSD
- Sterowanie za pośrednictwem portu RS485, m.in. za pomocą klawiatury SC3100 oraz za pośrednictwem rejestratorów Commax CSD-80/160HA i CNB serii HDx (np. HDE2424E)
- Możliwość mocowania do słupa, ściany, sufitu oraz narożnika
- Obudowa o klasie szczelności IP66

Właściwości

- Kamera z funkcją dzień/noc
- Przetwornik 1/4" Super HAD
- Wysoka rozdzielczość 580 TVL
- Czułość 0,5 lx (kolor), 0,1 lx (BW), 0,0005 lx (BW, DSS x128)
- 127 presetów/8 tras automatycznego skanowania/4 makra /8 stref prywatności
- Grzałka i wentylator
- Zasilanie 24 V_{AC}

Akcesoria

- SSS2000 – osłona przeciwsłoneczna
- SOB2000 – uchwyt do słupa
- SCB2000 – uchwyt narożny
- SPB2000 – uchwyt do sufitu
- SWB2000 – uchwyt do ściany
- SC3100 – klawiatura sterująca
- SOJ-S2324 – zasilacz w obudowie zewnętrznej

Dystrybucja:

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

Nowe monitory serii „Indigo Blue”

COMMAX SmartHome & Security

Ofertę monitorów kolorowych uzupełnia nowa seria wzornicza marki COMMAX – Indigo Blue. Przedni panel monitorów **CDV-35U** i **CDV-70U** jest utrzymany w ciemnoniebieskiej kolorystyce co dobrze komponuje się z szarą obudową. Ten niebanalny wygląd wyróżnia nową gamę produktów marki COMMAX. Monitory przeznaczone są dla domów jedno- i wielorodzinnych oraz niewielkich budynków mieszkalnych. Model CDV-35U jest wyposażony w 3,5-calowy ekran, a model CDV-70U w 7-calowy ekran. Oba ekrany są w wysokiej rozdzielczości z podświetleniem LED. Oba modele są wyposażone w sensoryczne przyciski pozwalające na ich obsługę. Monitory mogą współpracować z dwoma panelami zewnętrznymi (obsługa dwóch wejść) lub z jednym panelem i dodatkową kamerą CCTV (podgląd większego obszaru). Możliwa jest rozbudowa systemu o dodatkowe monitory z serii CDV-xxx umieszczone wewnątrz lokalu oraz unifony DP-4VHP pełniące także funkcję interkomu. Monitory współpracują z każdą kamerą COMMAX pracującą w systemie 4-przewodowym.

Cechy wspólne monitorów

- Przyciski sensoryczne (dotykowe)
- Standard sygnału wizyjnego PAL/NTSC
- Obsługa dwóch wejść
- Możliwość podłączenia dodatkowego monitora
- Współpraca z unifonami DP-4VHP
- Paging pomiędzy stacjami
- Instalacja czteroprzewodowa + obwód elektrozamka
- Współpraca z czteroprzewodowymi kamerami analogowymi
- Zasilanie 230 V

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

ASCD-1

Zewnętrzny zegar z wyświetlaczem matrycowym LED

ASCD-1 to wyświetlacz matrycowy LED z zegarem. Urządzenie stanowi uzupełniający element systemu rejestracji czasu pracy i działa w ramach systemu kontroli dostępu RACS 4 firmy Roger. **ASCD-1** umożliwia wyświetlanie czasu, daty i temperatury.

Wyświetlacz może pracować autonomicznie lub w trybie sieciowym. W trybie autonomicznym aktualna data i czas są odczytywane z zegara wewnętrznego natomiast w trybie sieciowym dane te są pobierane z systemu kontroli dostępu, do którego podłączony jest panel wyświetlacza. Praca w trybie sieciowym jest możliwa w przypadku zastosowania kontrolerów zaawansowanych serii PRxx2 lub centrali CPR32-SE. Obudowa ASCD-1 jest wykonana z profilu aluminiowego lakierowanego proszkowo i posiada uniwersalny system mocowania z możliwością regulacji kąta nachylenia wyświetlacza.

Charakterystyka

- Wyświetlanie daty i czasu z systemu RACS 4 (tryb sieciowy) lub na podstawie własnych wskazań (tryb autonomiczny)
- Wyświetlanie temperatury na podstawie wskazań wbudowanego czujnika
- Możliwość pracy w warunkach zewnętrznych – IP45
- Zasilanie 12 V_{DC}
- Podtrzymanie bateryjne dla wskazań wewnętrznego zegara
- Regulacja kąta nachylenia wyświetlacza
- Wymiary 110×305×55 mm (wys.×szer.×gł.)
- Wysokość wyświetlanego znaku 50 mm

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

PR102DR

Prosty i ekonomiczny kontroler dostępu serii zaawansowanej

Kontroler PR102DR jest nowym, ekonomicznym elementem systemu kontroli dostępu firmy ROGER. Urządzenie to zawiera wszystkie najistotniejsze funkcje i opcje dostępne w serii kontrolerów zaawansowanych. PR102DR może być stosowany samodzielnie lub w ramach systemu kontroli dostępu RACS 4 obejmującego różne kontrolery pojedynczego przejścia.

Charakterystyka

- Uproszczona konfiguracja
- Atrakcyjna cena
- Kontrola jedno lub dwustronna pojedynczego przejścia poprzez dołączenie czytników serii PRT (Roger)
- Obsługa do 4000 użytkowników
- Bufor pamięci na 32 tysiące zdarzeń
- Zasilanie z 12 V_{DC}
- Przekaźnik 5 A/30 V
- Dwie programowalne linie wejściowe NO/NC
- Jedna programowalna linia wyjściowa
- Dostępność w wersji do montażu na szynie DIN 35 mm oraz w postaci modułu elektronicznego
- Możliwość ustawiania adresu urządzenia na zworkach
- Wbudowany zegar czasu rzeczywistego z podtrzymywaniem bateryjnym

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

ABUS SECURITY CENTER
ABUS KEMAZ POLSKA Sp. z o.o.
ul. Wadowicka 8A
30-415 Kraków
tel. 12 640 15 60
faks 12 640 15 61
e-mail: tiglinski@abus-kemaz.pl
www.abus.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 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. Długa 19, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
faks 32 750 30 27
e-mail: ostrow@e-alpol.com.pl

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

ul. Młodzianowska 75d, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. POW 64, 98-200 **Sieradz**
tel. 32 750 30 55
faks 32 750 30 57
e-mail: sieradz@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

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

FIRMA ATLine Sp. J.
ul. Franciszkańska 125
91-845 Łódź
tel. 42 23 13 849÷851, 42 23 63 019
faks 42 655 20 99
e-mail: handel@atline.pl
www.atline.pl

BOSCH

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

Brabork Labs

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

bte bt electronics

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

bticino

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

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 GROUP

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

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

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

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

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

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

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

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 98 44, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

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 11
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 LIMITED
Biuro w Polsce
ul. Postępu 15c
02-676 Warszawa
tel. 22 20 50 777
faks 22 20 50 763
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. 17 857 80 60
faks 17 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. 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. Drewnowska 48, 91-002 **Łódź**
tel. 42 617 00 32
faks 42 659 85 23
e-mail: lodz@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

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. 22 843 83 95
faks 22 843 79 12
e-mail: tap5@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 18
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 98
faks 42 611 12 97
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ABUS	TAK	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS Fire & Security	–	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	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
CMA	TAK	–	–	TAK	–
D-MAX	–	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
Ela-compil	TAK	–	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
GEO-KAT	–	TAK	TAK	–	TAK
ICS POLSKA	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
KATON	–	–	TAK	–	TAK
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	–	–
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	–	–	–	–
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	–	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	–	–
ABUS	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, 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	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
EBS	Transmitery IP/GSM/GPRS, systemy RFID, zabezpieczenia energetyka, bankowość, produkcja OEM/ODM								
Ela-compil	–	–	–	–	–	TAK	–	–	–
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	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	TAK	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	–	–	–	–
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
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	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	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
Sawel	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	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	–	TAK	–	–	–
ZBAR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
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

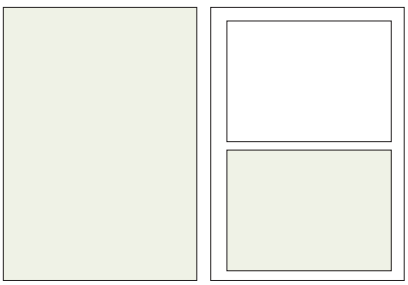
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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)

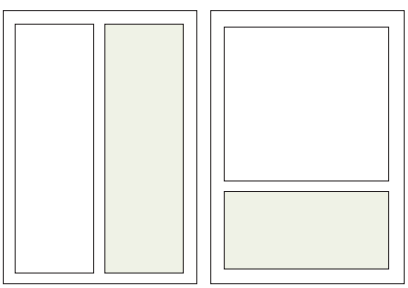
1/2 strony (170 x 125 mm)

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)

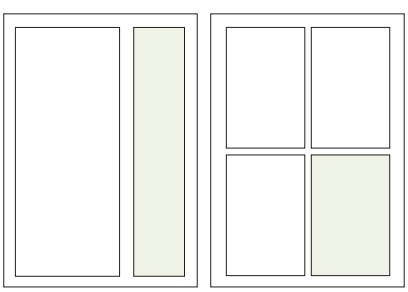
1/3 strony (170 x 80 mm)

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

roger®

PROMOCJA

-25%

Czytniki MIFARE
Wyższy poziom bezpieczeństwa teraz w niższej cenie

Z przyjemnością informujemy o promocji na czytniki zbliżeniowe serii **PRTxxMF** pracujące w standardzie **13.56 MHz MIFARE.**

Promocja obowiązuje **od 16.07.2012 do 31.12.2012.**
W tym okresie wszystkie czytniki serii PRTxxMF dostępne będą w cenie **niższej o 25%**.

Serdecznie zapraszamy do skorzystania z promocji.

Security Products SINCE 1991 roger®

www.roger.pl

Platforma wymiany informacji

twarta, elastyczna i doskonale zabezpieczona latforma 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**