CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(78)/2011

ZABEZPIECZENIA

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

W NUMERZE:

GODZINA 13:15
Jakieś zdarzenia?

Efektywny system zewnętrznego nadzoru wizyjnego chroni to co cenimy najbardziej, ostrzega o niespodziewanych zdarzeniach a nawet uaktywnia konkretne działania. Kamery te muszą wytrzymać intensywne nasłonecznienie , duże opady deszczu i silny wiatr – i zapewnić dobrą jakość materiału wizyjnego.

Kamery do zastosowań zewnętrznych Axis są wyjątkowo proste do zainstalowania, co oszczędza cenny czas i minimalizuje koszty utrzymania. Wytrzymują one ekstremalne warunki pogodowe i zapewniają wyjątkową jakość obrazu. Ponieważ system nadzoru wizyjnego musi dostarczać niepodważalne dowody w formie przejrzystego, wyraźnego materiału wizyjnego- nawet w najcięższych warunkach.

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

Sieciowa kamera kopułkowa AXIS Q6034-E : obudowa klasy IP66 i NEMA 4X, 18x zoom optyczny, HDTV 720p w formacie 16:9, tryb dzień/noc, H.264, zasilanie przez Ethernet, Arctic Temperatur Control i wiele więcej.

AXIS COMMUNICATIONS

Spis treści

CZASOPISMO ZABEZPIECZENIA 2/2011

P2P w świetle prawa autorskiego **18**

Czy jesteś pewien, że Twoje oszczędności są bezpieczne? **22**

Historia z przyszłością. Opowiadanie nie-*science-fiction* **32**

Urządzenia mobilne – znajdujące się w nich cenne dane też możesz stracić **40**

THE INTERNATIONAL SECURITY EVENT

WWW.IFSEC.CO.UK

Do zobaczenia na IFSEC w Birmingham

FSEC to największa na świecie coroczna impreza związana z bezpieczeństwem. Już po raz trzydziesty ósmy odbędzie się w NEC (National Exhibition Centre) w Birmingham, w dniach od **16 do 19 maja 2011 roku.** Przybędą na nią specjaliści ds. bezpieczeństwa z całego świata. Wystawa wielokrotnie zainspirowała opracowanie wielu technologii i wyrobów, a profesjonaliści mieli okazję do zbadania i wypróbowania nowych pomysłów i rozwiązań. Odwiedzający (przedstawiciele wszystkich specjalności z branży zabezpieczeń) mogą podczas tej imprezy odbyć spotkania i rozmowy z ekspertami i czołowymi specjalistami w tej dziedzinie.

Równolegle z wystawą odbędzie się konferencja IFSEC, składająca się z szeregu sesji, podczas których uznani specjaliści ds. bezpieczeństwa podzielą się swoimi spostrzeżeniami na temat najlepszych praktyk i skutecznego stosowania najnowszych technologii między innymi w korporacjach.

W programie konferencji znajdą się:

– cztery moduły specjalistyczne: handel detaliczny, usługi finansowe, usługi techniczno-serwisowe i transport;
– technologia – bezpieczeństwo oparte na protokole IP, telewizja dozorowa, obserwacje termowizyjne, systemy zbiorcze;
– cyberterroryzm – co oznacza dla firmy i jak sporządzić plany uzasadnione ekonomicznie;
– powiązanie fizycznych zabezpieczeń technicznych i bezpieczeństwa IT;
– dyskusja panelowa na temat regulacji branży w świecie post-SIA.

Przewidziano panele dyskusyjne dla menedżerów, dyrektorów i specjalistów branży zabezpieczeń. Będą zorganizowane w taki sposób, by zachęcić uczestników do wzajemnych kontaktów i udziału w dyskusji. Każda sesja jest kierowana przez jedną z czołowych postaci branży zabezpieczeń; należą do nich Brian Sims (wydawca „Security Management Today Online"), Mike Hurst (wiceprezes ds. strategii ASIS UK) i Andrew Mason (kierujący Business Continuity w PricewaterhouseCoopers).

Bogata ekspozycja IFSEC zostanie podzielona na sześć kategorii wyrobów:

– kontrola dostępu,
– telewizja dozorowa,
– systemy sygnalizacji włamania i napadu,
– integracja sieci IP i bezpieczeństwa,
– bezpieczeństwo publiczne,
– rozwiązania techniczne z dziedziny zabezpieczeń.

W bieżącym roku zostanie ponownie zorganizowana Strefa Inteligentnej Integracji (SII, ang. Intelligent Integration Zone – IIZ), przeznaczona dla ludzi odpowiedzialnych za obsługę systemów zabezpieczeń organizacji. Sponsorowana będzie przez Integrated Security Manufacturing (ISM) – specjalistów w zakresie produkcji i rozwoju graficznych systemów zarządzania systemami bezpieczeństwa. ISM wraz z sześcioma partnerami przedstawi własne oprogramowanie do integracji – system Genesys, integrujący ochronę obwodową, obserwację wizyjną, cyfrową rejestrację CCTV, kontrolę dostępu, systemy sygnalizacji włamania i napadu oraz system przeciwkradzieżowy.

Wystawa obejmie wiele pawilonów narodowych, w których zwiedzający będą mogli zapoznać się z najnowszymi urządzeniami i usługami (wydzielone pawilony będą miały m.in. Hiszpania, Belgia, Chiny, Francja, Włochy, Korea, Tajwan i USA).

Kluczowym wydarzeniem towarzyskim stanie się wręczenie nagród IFSEC Security Industry Award 2011 (nagroda branży zabezpieczeń IFSEC 2011), które odbędzie się podczas uroczystej kolacji w hotelu Hilton Birmingham Metropole w poniedziałek, 16 maja 2011 roku.

Przy okazji imprezy IFSEC organizowany jest Konkurs Przyszłości Bezpieczeństwa, ukierunkowany na innowacje w zakresie bezpieczeństwa następnych generacji. Zawodnicy będą rywalizować ze sobą podczas ocenianej na żywo sesji w ramach IFSEC. Konkurs jest przeznaczony dla naukowców, wynalazców i pracowników wyższych uczelni. Uczestnicy muszą przedstawić innowacje technologiczne, które mogą być wykorzystane do poradzenia sobie ze wszelkiego rodzaju incydentami terrorystycznymi i innymi przestępstwami (poprzez zapobieganie, obronę, usuwanie skutków lub inne sposoby).

Równolegle z imprezą IFSEC organizowane będą: International Firex – wystawa na temat bezpieczeństwa pożarowego, Safety & Health Expo – największa w Europie doroczna impreza poświęcona zdrowiu i bezpieczeństwu, oraz Facilities Show (salon wyposażeń) – największa i najszybciej rozwijająca się brytyjska impreza z dziedziny obsługi budynków.

Aby uzyskać więcej informacji o IFSEC 2011 i jej przebiegu lub by zapisać się po darmową wejściówkę, prosimy odwiedzić stronę *http://www.ifsec.co.uk/* lub przyłączyć się do grupy LinkedIn na Twitter @ IFSEC.

Bezpośr. inf. Lina Rudinskaite
UBM Live
Tłumaczenie: redakcja


INNOVATION MOVES ON...
IFSEC IS EUROPE'S FIRST OPPORTUNITY TO SEE NEW SECURITY PRODUCTS BROUGHT TO LIFE
ACCESS CONTROL | CCTV
INTRUDER ALARMS | IP/NETWORK SECURITY
PUBLIC SECURITY | SECURITY SOLUTIONS
REGISTER FOR FREE ENTRY AT
WWW.IFSEC.CO.UK
REGISTRATION CODE
ZPA
IFSEC 2011
16-19 May 2011
NEC Birmingham, UK
THE INTERNATIONAL SECURITY EVENT
IFSEC is part of the Protection & Management Series, uniting security with fire, safety and facilities management professionals.
SUPPORTED BY
CERTIFIED BY
OFFICIAL MEDIA PARTNER
ORGANISED BY
bsia
London First
ADS
ASIS
UK Trade & Investment
US Commercial Service
info4 SECURITY.COM
Security News for the Security Professional
UBM Live

Kto pojeździ terenówką w Grecji?
Konkurs RISCO Group

Pierwsi zwycięzcy w konkursie dla klientów zorganizowanym przez **RISCO Group** to **Sebastian Gudowicz** z Polski i **Alessandro Mantese** z Włoch. Gratulacje! Kolejni zwycięzcy będą losowani na początku każdego miesiąca.

Konkurs trwa do 5 sierpnia 2011 r. Zostań jego zwycięzcą! Dołącz do grupy uczestników z całego świata i wybierz się na wycieczkę krajobrazową do Grecji, kraju fascynującej historii i niezrównanego piękna natury.

– Przejedź się terenowym samochodem po bezdrożach.
– Podziwiaj zapierające dech w piersiach widoki wodospadów, lasów i gór.
– Zwiedź malownicze wioski i spotkaj ich mieszkańców.
– Każdy dzień wycieczki zakończ odpoczynkiem w luksusowym hotelu.

Na opakowaniach konkursowych produktów RISCO (detektorów serii **WatchOUT** oraz aktywnych barier podczerwieni) znajdują się naklejki z numerami seryjnymi. Aby wziąć udział w kolejnych losowaniach, należy zarejestrować numery seryjne produktów biorących udział w konkursie na stronie *http://adventure.riscogroup.com/pl*. Tam też znajduje się regulamin.

Wszystkie szczegóły na temat imprezy, wraz z listą zwycięzców konkursu oraz opisem kolejnych dni wycieczki, będą publikowane na stronie *http://www.facebook.com/RISCOGroup*.

Bezpośr. inf. Norbert Góra
RISCO Group Poland

Dynamiczny rozwój RISCO Group
w Europie Środkowej i Wschodniej

Mimo kryzysu, który dotknął wiele firm z branży elektronicznych systemów ochrony, **RISCO Group** kontynuuje swój dynamiczny rozwój i rozszerza działalność na nowe kraje. Jednym z przejawów rozwoju firmy w naszym regionie jest nominacja **Kazimierza Kacprzyka** na stanowisko **regionalnego menedżera w Europie Środkowej i Wschodniej**. Otwarte zaledwie przed trzema laty biuro RISCO Group Poland w Warszawie staje się regionalnym przedstawicielstwem RISCO Group odpowiedzialnym za sprzedaż produktów firmy w Polsce, Czechach, Słowacji, Litwie, Łotwie, Estonii, Ukrainie i Białorusi.

Risco Group, z siedzibą główną w Izraelu, jest od wielu lat znana na rynku, głównie dzięki marce **Rokonet**. Firma koncentruje się na tworzeniu zintegrowanych rozwiązań z zakresu systemów bezpieczeństwa, pamiętając o potrzebach zarówno klienta korporacyjnego, jak i indywidualnego. W strategii firmy ważnym elementem jest ciągły rozwój technologii systemów bezprzewodowych, programowalnych detektorów adresowalnych oraz urządzeń do transmisji przez sieci GSM/GPRS/IP. Wśród produktów oferowanych przez Risco Group wyróżnia się **SynopSYS** – oprogramowanie do zarządzania i integracji systemów bezpieczeństwa i automatyki budynku, działające lokalnie lub zdalnie przez sieci LAN/WAN.

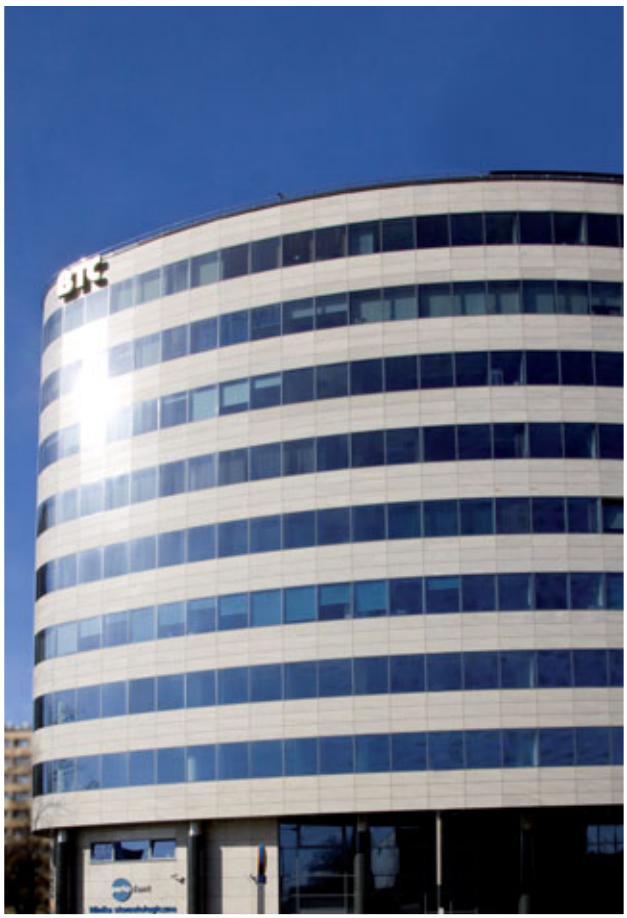
Bezpośr. inf. Norbert Góra
RISCO Group Poland

Nedap Security Management
otworzył biuro w Warszawie

W trzecim roku aktywności na polskim rynku Nedap N.V. Security Management z przyjemnością informuje o otwarciu nowego biura w Warszawie. Pracą biura kieruje Jakub Kozak, nowy *country manager* na Polskę.

Dane kontaktowe:
Nedap Polska
BTC Office Center
Al. Niepodległości 69
02-626 Warszawa
Polska

Jakub Kozak
Telefon stacjonarny: (+48) 22 322 76 74
Telefon komórkowy: (+48) 696 056 977
E-mail: jakub.kozak@nedap.com
Internet: *www.nedap-securitymanagement.com*



Nedap Security Management

Nedap N.V. jest europejskim liderem i pionierem w zakresie zintegrowanych systemów bezpieczeństwa. Sztandarowym produktem firmy Nedap jest **AEOS** – zintegrowana platforma bezpieczeństwa bazująca na inteligentnej architekturze sieciowej. Jest to jedno z najnowocześniejszych rozwiązań tego typu dostępnych obecnie na rynku *security.*

Bezpośr. inf. Nedap Polska

HID Global rozszerza działalność w branży zdalnie odczytywanych identyfikatorów w logistyce

Nowo mianowany specjalista w dziedzinie identyfikacji bezprzewodowej Jason Walden ma zapewnić rozwój branży w Europie

HID Global poinformował o nominowaniu **Jasona Waldena** do kierowania branżą zdalnych identyfikatorów bezprzewodowych w Wielkiej Brytanii, Irlandii, krajach Beneluksu i Skandynawii. Jason Walden będzie odpowiedzialny za wprowadzenie na ten szybko rozwijający się rynek nowych rozwiązań systemowych pozwalających na śledzenie towarów, automatyzację procesów, obsługi medycznej i identyfikację towarów zwracanych. Aktualnie firma HID zajmuje czołową pozycję wśród producentów tego typu rozwiązań.

Jason Walden ma ponadpiętnastoletnie doświadczenie w branży identyfikatorów bezprzewodowych. Obejmuje ono zarządzanie łańcuchami dostaw, systemami zbierania danych, a także technikami pozwalającymi na identyfikację i śledzenie najważniejszych zasobów oraz właściwe ich rozmieszczanie mające na celu zwiększenie efektywności ekonomicznej.

HID oferuje najszerszą paletę identyfikatorów bezprzewodowych sprawdzonych w różnych warunkach przemysłowych. Sprzedał ich już ponad miliard na całym świecie.

Bezpośr. inf. Roland A. Edwards
PR Specialist EMEA
HID Global GmbH

Nowy dyrektor zarządzający w **Samsung Techwin Europe**

Stanowisko nowego dyrektora zarządzającego w firmie Samsung Techwin Europe objął **Lucas Lee**

Lucas Lee w ciągu niemal 20 lat pracy w firmie **Samsung Techwin** zarządzał między innymi sprzedażą zagraniczną aparatów cyfrowych oraz związanymi z tym działaniami marketingowymi. Pracował w Wielkiej Brytanii, Niemczech, Francji oraz Korei. Bezpośrednio przed objęciem obecnego stanowiska zajmował się branżą zabezpieczeń – był dyrektorem sprzedaży zagranicznej i marketingu, odpowiedzialnym za rozwój sprzedaży w Europie oraz Ameryce Północnej i Południowej.

Lucas Lee został przeniesiony do centrali europejskiej Samsung Techwin, zlokalizowanej w Chertsey w Wielkiej Brytanii. – *Jestem bardzo szczęśliwy, że będę zarządzał Samsung Techwin Europe w tak ważnym dla rozwoju firmy okresie. Mamy wspaniały zespół, bogatą ofertę doskonałych produktów i w ciągu ostatnich dwóch lat bardzo się rozwinęliśmy. Jest jednak jeszcze wiele do zrobienia dla realizacji naszego nadrzędnego celu: zostania liderem wśród dostawców rozwiązań z branży zabezpieczeń* – skomentował swój awans Lucas Lee. Zapytany o najbliższe plany firmy, dodał: – *W tym roku skoncentrujemy się na realizacji potencjału w zakresie rozwiązań IP, co przyniesie naszym klientom dodatkowe możliwości rozwoju i dodatkowe korzyści ze współpracy z nami. Chcę, abyśmy zostali prawdziwą siłą napędową rynku. W związku z tym musimy mieć pewność, że zajmujemy się potrzebami naszych klientów w najlepszy możliwy sposób, a to oznacza, że powinniśmy inwestować w dalsze wzmacnianie naszej organizacji. Europejski rynek jest złożony, a wzrost popularności technologii IP oraz zintegrowanych rozwiązań z zakresu ochrony przynosi wiele wyzwań. Będziemy więc w większym stopniu rozwijać własne produkty dla tego rynku. Jedną z pierwszych rzeczy do zrobienia jest stworzenie europejskiego centrum badań i rozwoju, dla zapewnienia długoterminowej kompatybilności i najwyższej jakości naszych produktów. Będziemy również kontynuować rozwój i wprowadzanie na rynek inteligentnych rozwiązań nowej generacji.*

Bezpośr. inf. David Solomons
DRS Marketing

Integracja urządzeń Ulisse

z oprogramowaniem Milestone XProtect Suite

Firma **Videotec** informuje, że linia produktowa kamer sieciowych PTZ, zbudowanych w oparciu o głowice Ulisse, została obecnie zintegrowana z oprogramowaniem **Milestone XProtect**, służącym do obsługi systemów dozorowych.

Videotec jest partnerem handlowym firmy Milestone, dzięki czemu zapewnia pełną integrację funkcjonalną produktów Ulisse IP z otwartą platformą programową XProtect, opracowaną przez Milestone Systems.

Głowice Ulisse IP i Ulisse Compact IP są urządzeniami szybkoobrotowymi (określanymi jako *Ultra Fast Positioning Units*), realizującymi wszystkie swoje funkcje użytkowe przez sieć IP. Są przystosowane do pracy na zewnątrz obiektów, w najbardziej uciążliwych warunkach środowiskowych. Realizują najtrudniejsze zadania związane z dozorem wizyjnym.

Ostatnio oddział Milestone Device Support Team wprowadził na rynek oprogramowanie XProtect Device Pack 5.2, obsługujące również urządzenia z serii Ulisse IP i Ulisse Compact IP. Pozwala to na integrację głowic Ulisse IP PTZ z wieloma urządzeniami sieciowymi i hybrydowymi oferowanymi przez innych producentów. Obecnie operatorzy systemów będą mogli za pomocą oprogramowania XProtect sterować wszystkimi funkcjami głowic Ulisse and Ulisse Compact w wersjach sieciowych, włączając w to obsługę spryskiwacza i wycieraczki przedniej szyby głowicy.

– *Linia produktowa zintegrowanych głowic Ulisse PTZ stała się punktem odniesienia dla innych produktów wykorzystywanych w systemach dozorowych, pracujących na terenach otwartych. Naszą misją jest ciągłe rozszerzanie oferty oraz wprowadzanie innowacyjnych rozwiązań technicznych i marketingowych. Partnerstwo z firmą Milestone jest częścią naszych działań, prowadzących do utrzymania najwyższego poziomu technologicznego tych wyrafinowanych urządzeń* – powiedział **Enrico Dani**, dyrektor działu handlowego firmy Videotec.

Bezpośr. inf. Martina Panighel
VIDEOTEC SpA

Tłumaczenie: redakcja

Badania potwierdzają: **systemy IP tańsze o 13% od analogowych**

Firma **Axis Communications** ogłosiła wyniki niezależnych badań, których celem było porównanie kosztów wdrożenia systemów nadzoru wizyjnego wykorzystujących technologię cyfrową i analogową. Wyniki dowodzą niezbicie, że instalacja systemu opartego na protokole IP jest średnio o 13 procent tańsza niż instalacja jego analogowego odpowiednika.

Badania przeprowadzone przez grupę badawczą Lusax opierały się na ankiecie przeprowadzonej wśród integratorów specjalizujących się w sprzedaży i instalacji profesjonalnych systemów nadzoru wizyjnego, zarówno analogowych, jak i opartych na protokole IP. Respondentów poproszono o sporządzenie ofert dotyczących systemów obydwu typów, obejmujące po 14, 25 i 40 kamer przeznaczonych do zainstalowania w sklepie detalicznym. We wszystkich trzech przypadkach łączny koszt wdrożenia systemu opartego na protokole IP okazywał się niższy niż koszt wdrożenia systemu analogowego.

– Korzyści wynikające z zastosowania nowoczesnej technologii sieciowej opartej na protokole IP są widoczne gołym okiem, kiedy uwzględni się wszystkie elementy systemu, tj. kamery, nośniki do rejestracji i przechowywania obrazu oraz dźwięku, a także konieczność wykonania i utrzymywania instalacji – powiedziała **Bodil Sonesson Gallon**, wiceprezes ds. globalnej sprzedaży w Axis Communications. *– Wyniki podobnych badań przeprowadzonych w roku 2007 wskazały, że system nadzoru oparty na protokole IP jest bardziej opłacalny w przypadku instalacji zawierającej ponad 32 kamery. Teraz widzimy, że również wdrożenie mniejszego systemu tego typu przynosi korzyści* – dodała Sonesson Gallon.

Badania porównawcze systemów nadzoru wizyjnego przeprowadziła grupa badawcza Lusax, działająca przy uniwersytecie w szwedzkim mieście Lund. Jej specjalnością są analizy dotyczące rozpowszechniania się na globalnym rynku zabezpieczeń nowych technologii informatycznych oraz technologii opartych na protokole IP. Wyniki badań nie zaskoczyły profesora **Thomasa Kallinga**, stojącego na czele grupy Lusax: *– Rynek zabezpieczeń opartych na protokole IP rozwinął się bardzo szybko i jest obecnie o wiele bardziej stabilny, niż był jeszcze kilka lat temu. Różnice cenowe powoli się zacierają, zatem klienci zwracają się w dużej mierze w stronę niewątpliwych zalet rozwiązań opartych na protokole IP, to znaczy elastyczności i wyjątkowo wysokiej jakości obrazu. Są to czynniki, które determinują szybki zwrot z poczynionej inwestycji* – dodał prof. Kalling.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Większa widoczność

dzięki oświetlaczowi podczerwieni do zewnętrznych, stałopozycyjnych kamer kopułkowych Axis

Axis Communications rozszerzył ofertę produktów o oświetlacz pracujący w podczerwieni, cechujący się dużą wydajnością, przeznaczony do stosowania z instalowanymi na zewnątrz, stałopozycyjnymi sieciowymi kamerami kopułkowymi serii AXIS P33. Przygotowany do montażu zewnętrznego oświetlacz AXIS T90C IR-LED poprawia widoczność w ciemnościach, zapewniając wysokiej jakości materiał wizyjny w każdych warunkach oświetleniowych. Znajdzie on zastosowanie w systemach dozoru wizyjnego na lotniskach, dworcach kolejowych, a także w miastach, szkołach i kampusach uniwersyteckich.

Zamknięty w eleganckiej i kompaktowej obudowie oświetlacz AXIS T90C IR-LED może współpracować ze wszystkimi kamerami zewnętrznymi z serii AXIS P33. Sterowany jest za pośrednictwem czujnika światła widzialnego, który automatycznie włącza oświetlenie podczerwone po zmierzchu. Aby ułatwić instalację, produkt jest fabrycznie wyposażony w kable i dostępny w dwóch wersjach: zasilanej prądem stałym o niskim napięciu oraz zasilanej przez sieć Ethernet.

– Seria akcesoriów firmy Axis, w tym nowy oświetlacz AXIS T90C IR-LED, została stworzona, by ułatwiać życie naszym klientom – powiedział **Erik Frännlid**, dyrektor ds. zarządzania produktami w Axis Communications. *– AXIS T90C IR-LED, montowany bezpośrednio do kamer AXIS P33, pozwoli uniknąć montażu oddzielnego oświetlacza, umożliwiając wygodniejszą i bardziej estetyczną instalację* – dodał Erik Frännlid.

Oświetlacz podczerwieni Axis jest wyposażony w osiem mocnych i bardzo wydajnych diod LED, które zapewniają strumień światła o szerokim kącie. Dzięki temu w całkowitych ciemnościach zakres widzenia kamery wynosi od 20 do 25 metrów. Pobór mocy w normalnych warunkach eksploatacyjnych oświetlacza AXIS T90C IR-LED wynosi jedynie 15 W. Ponieważ kamery serii AXIS P33 i oświetlacze AXIS T90C IR-LED spełniają wymagania klas ochrony IP66, IK10 oraz NEMA 4X, mogą pracować w trudnych warunkach zewnętrznych i w ekstremalnych temperaturach.

Stałopozycyjny oświetlacz kopułkowy AXIS T90C IR-LED będzie dostępny w pierwszym kwartale 2011 r., w sugerowanej przez producenta cenie detalicznej 299 € (modele AXIS T90C10 oraz AXIS T90C20).

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Nowa kamera **IP 265 HD** firmy Bosch

Wszechstronne rozwiązanie do systemów nadzoru wizyjnego o wysokiej rozdzielczości, stosowanych w biurach i sklepach detalicznych

Firma **Bosch** powiększa innowacyjną i wielokrotnie nagradzaną rodzinę systemów IP serii 200 o kamery HD. Dzięki kamerom IP 265 HD zaawansowana technologia HD zaczyna być stosowana również w przypadku małych firm. Wybór pomiędzy wersją kompaktową i kopułową umożliwia lepsze dostosowanie rozwiązania do konkretnego zastosowania.

Kamera **IP 265 HD** daje wyraźny obraz w standardzie HD 720p i zapewnia najdokładniejsze w swojej klasie odwzorowanie kolorów. Technologia skanowania progresywnego umożliwia utrzymywanie ostrego obrazu poruszających się obiektów. Nasycone szczegółami, panoramiczne obrazy pozwalają wychwycić więcej istotnych informacji niż rozwiązania o standardowej rozdzielczości (SD). Dzięki temu – zależnie od zastosowania – jedna kamera IP 265 HD może nadzorować taki sam obszar jak dwie lub więcej kamer SD.

Oprócz wysokiej rozdzielczości ważnymi zaletami rozwiązań IP 265 HD są wygoda i łatwość użytkowania. Kamera umożliwia rejestrację obrazów natychmiast po jej podłączeniu, bez konieczności używania jakiegokolwiek dodatkowego sprzętu. Gniazdo na kartę microSD/SDHC eliminuje potrzebę używania zewnętrznego rejestratora, a efektywna kompresja H.264 zmniejsza zapotrzebowanie na pamięć nawet o 30% w porównaniu z kompresją MPEG-4. Jeżeli niezbędna jest dłuższa, wielotygodniowa archiwizacja, można ją łatwo uzyskać, podłączając kamerę do rejestratora wizyjnego firmy Bosch lub serwera iSCSI.

Bezpłatne oprogramowanie Video Client (BVC) firmy Bosch umożliwia oglądanie obrazów z wielu kamer na monitorze komputera PC oraz łatwą archiwizację sekwencji wizyjnych. Funkcja inteligentnego wyszukiwania ruchu pozwala szybko zlokalizować ważne zdarzenia przez automatyczne skanowanie zarejestrowanego materiału. Jako że obrazy mają wysoki poziom szczegółowości, można dokładniej zbadać istotne obszary zarejestrowanych scen za pomocą dostępnej w oprogramowaniu BVC funkcji zoomu cyfrowego.

Kamera IP 265 HD ma wbudowane funkcje wykrywania ruchu, wykrywania sabotażu i analizy dźwięku. W przypadku aktywacji tych funkcji kamera automatycznie wysyła powiadomienie (np. przez e-mail) i może włączyć alarm lub zmienić tryb nagrywania. Oprócz alarmu dźwiękowego kamery są wyposażone w dwukierunkowe łącze foniczne, przydatne jako dodatkowy sposób komunikacji. Zgodność ze standardem ONVIF zapewnia kompatybilność z innymi urządzeniami służącymi do nadzoru i pozwala zmniejszyć koszty przyszłej modernizacji.

Bezpośr. inf. Bosch Security Systems

Nowe czujki magnetyczne z certyfikatem EN50131-2-6

Firma **Bosch Security** Systems wprowadziła na rynek **nową gamę czujek magnetycznych** stosowanych w systemach sygnalizacji włamania. Nowa oferta obejmuje szereg czujek do montażu wpuszczanego, powierzchniowego oraz do montażu zewnętrznego. Wszystkie te czujki zostały przetestowane przez niezależne akredytowane laboratorium i uzyskały certyfikat zgodności z normą EN50131-2-6.

Wyróżnikiem czujek magnetycznych firmy Bosch jest duża dokładność wykrywania oraz minimalny wskaźnik fałszywych alarmów przy otwieraniu drzwi i okien. Gama nowych produktów składa się z dwóch serii o różnych parametrach technicznych, w zależności od ich zastosowania. Jedna z serii spełnia wymagania normy EN50131-2-6 stopnia 2, natomiast druga posiada certyfikat potwierdzający stopnia 3.

Czujki do montażu wpuszczanego można z łatwością zamontować w drzwiach, ościeżnicach okiennych i drzwiowych; są całkowicie niewidoczne. Czujki spełniające wymagania dla stopnia 2 mogą być także montowane powierzchniowo, zarówno na powierzchniach metalowych, jak i niemetalowych, natomiast czujki z certyfikatem dla stopnia 3 są przeznaczone tylko do montażu wpuszczanego w środowiskach niemetalowych.

Czujki do montażu powierzchniowego są przeznaczone do montażu we framudze i skrzydle drzwi oraz we framudze i skrzydle okna. Dzięki ich konstrukcji można je dyskretnie zainstalować w każdym właściwie środowisku.

Czujki do montażu zewnętrznego są wykorzystywane do kontroli bram przesuwnych, drzwi żaluzjowych oraz drzwi garażowych.

Nowe czujki magnetyczne zostały opracowane z myślą o łatwej instalacji, aby jak najbardziej uprościć pracę instalatorów. Ważną kwestią była też odpowiednia konstrukcja, która umożliwia dyskretny montaż czujek. Śruby do montażu powierzchniowego są po zainstalowaniu zakrywane, natomiast czujki do montażu wpuszczanego mają ekstremalnie płaskie krawędzie, co pozwala na ich instalację nawet w najszczelniej zamykających się drzwiach.

Duże doświadczenie firmy Bosch w opracowywaniu czujek magnetycznych oraz rygorystyczne i kompleksowe testy produktów pod kątem zgodności z wymaganiami normy EN stanowią najlepszą gwarancję wysokiej jakości wszystkich nowych czujek.

Bezpośr. inf. Bosch Security Systems

Nowe kamery dzienno-nocne **IP Dinion HD i FlexiDome HD 720p** firmy Bosch

Kamery dzienno-nocne **IP Dinion HD 720p** i **FlexiDome HD** to sztandarowe produkty wchodzące w skład nowych rozwiązań do nadzoru HD (*High Definition*) firmy **Bosch**. Kamery zostały wyposażone w najnowszy przetwornik CCD HD z progresywnym skanowaniem i o przekątnej 1/3 cala, dzięki czemu dostarczają ostry i bogaty w szczegóły obraz o rozdzielczości HD.

Sposób przetwarzania obrazu z dokładnością do jednego piksela daje bardziej szczegółowe wyniki niż tradycyjne metody, zatem operatorzy mogą łatwiej spostrzec małe obiekty. Jest to niezmiernie istotne przy rozpoznawaniu twarzy, wypatrywaniu małych przedmiotów czy np. odczytywaniu tablic rejestracyjnych. Ponadto obraz o rozdzielczości HD jest wyświetlany w formacie szerokoekranowym, który ułatwia obserwację monitorowanego obszaru.

Zaawansowane funkcje cyfrowego przetwarzania obrazu wbudowane w dzienno-nocne kamery IP Dinion HD 720p i FlexiDome HD 720p zapewniają wysoką jakość obrazu i dobre odwzorowanie barw, nawet w niesprzyjających warunkach oświetleniowych. Technologia SmartBLC zapewnia automatyczną korekcję oświetlenia tła, a mechanizm SensUp Dynamic zdecydowanie zwiększa czułość kamery przy słabym natężeniu światła (np. przy świetle księżyca).

Kamery obsługują pamięć masową iSCSI. Zastosowanie technologii kompresji H.264 minimalizuje koszty przechowywania obrazu. Dzięki obsłudze potrójnych strumieni wizyjnych można wykorzystać strumień z kompresją H.264 720p do podglądu na żywo i rejestracji, strumień z kompresją H.264 o mniejszej rozdzielczości – do zastosowań w sieciach o ograniczonej przepustowości łączy, a strumień z kompresją JPEG – do łatwej integracji z systemami zarządzania obrazem i nagraniami pochodzącymi z innych źródeł.

Ponadto urządzenia są wyposażone w standardowe funkcje analizy obrazu, takie jak wbudowana funkcja wykrywania ruchu MOTION+. Bardziej zaawansowane modele kamer oferują też funkcję IVA (*Intelligent Video Analysis* – Inteligentna Analiza Obrazu), przeprowadzającą wielopoziomową analizę pikseli, tekstur i kierunków, w których zwrócone są poszczególne obiekty.

Kamery Dinion HD i FlexiDome HD są w pełni zgodne ze standardem ONVIF.

Bezpośr. inf. Bosch Security Systems

Nowy cyfrowy rejestrator wizyjny **serii 600** firmy Bosch

Łatwe w użyciu i przystępne cenowo rozwiązanie do zarządzania procesem rejestracji obrazu

Cyfrowy **rejestrator wizyjny serii 600** to kompletne rozwiązanie służące do zarządzania procesem rejestracji obrazów z maksymalnie ośmiu lub szesnastu kamer. Oferowana przez serię 600 funkcja zdalnego monitorowania pozwala operatorom zarządzać systemami wizyjnymi i systemami rejestracji cyfrowej z dowolnego miejsca za pośrednictwem sieci LAN, WAN lub Internetu.

Instalacja i obsługa urządzeń z serii 600 jest bardzo łatwa, dlatego ich użytkownicy nie muszą przechodzić specjalnego przeszkolenia. Po podłączeniu urządzeń wystarczy wybrać język, w jakim wyświetlane będą informacje tekstowe, a proces rejestracji rozpocznie się automatycznie. Urządzenia mają trwałą, zwartą konstrukcję, dzięki której zakres czynności serwisowych jest zmniejszony do minimum, co obniża koszty utrzymania systemu.

Sterowanie jest realizowane za pomocą klawiatury, myszy, pilota na podczerwień lub bezpośrednio z przedniego panelu urządzenia. Wraz z urządzeniami z serii 600 dostarczane jest bezpłatnie oprogramowanie Control Center PC, umożliwiające połączenie ze sobą kilku urządzeń i ich centralne sterowanie.

Efektywna kompresja H.264 znacznie zmniejsza wymagania dotyczące przepustowości sieci i pojemności pamięci, a jednocześnie zapewnia znakomitą jakość obrazu. Możliwa jest rejestracja w czasie rzeczywistym z rozdzielczością CIF na wszystkich kanałach równocześnie, a w przypadku gdy niezbędne jest wychwycenie drobniejszych szczegółów – także z rozdzielczością 2CIF lub 4CIF.

Proces rejestracji zdarzeń może być inicjowany na zasadzie pobudzania wejść alarmowych lub wykrywania ruchu w obrazie, a powiadomienia mogą być generowane w sposób automatyczny i wysyłane drogą elektroniczną. Funkcja Smart Search (inteligentne wyszukiwanie) umożliwia szybkie odnalezienie ważnych zdarzeń w zarejestrowanym materiale wizyjnym, poprzez wykrywanie zmian w wybranym obszarze. Nagrania o istotnym znaczeniu są chronione przed nadpisaniem i zabezpieczone znakiem wodnym, co gwarantuje wysoką wiarygodność zapisanego materiału.

Cyfrowe rejestratory wizyjne serii 600 stanowią ekonomiczne, wygodne i elastyczne rozwiązanie do zarządzania rejestracją wizyjną. Świetnie nadają się do różnych zastosowań o małej i średniej skali, na przykład w szkołach, sklepach, hotelach i firmach.

Bezpośr. inf. Bosch Security Systems

Samsung wprowadza do swojej oferty sieciową kamerę kopułkową z funkcją zliczania osób

Sieciowa kamera kopułkowa SND-3080C została opracowana głównie w odpowiedzi na potrzeby użytkowników wymagających niezawodnego i prostego w obsłudze narzędzia, służącego do monitorowania natężenia ruchu w celach marketingowych, handlowych oraz związanych z ochroną. Kamera ta może znaleźć szerokie zastosowanie również w transporcie, bibliotekach, muzeach, na parkingach, w obiektach sportowych i ośrodkach rekreacyjnych.

Dostępne w modelu SND-3080C zliczanie osób jest jedną z funkcji zaimplementowanego w kamerze systemu analizy obrazu. Działanie tej funkcji opiera się na wcześniejszym zdefiniowaniu wirtualnej bariery (linii) lub prostokątnego obszaru w określonej części obrazu. Kamera zlicza osoby, które przekraczają linię lub wchodzą w wyznaczony obszar. Następnie dane te mogą być okresowo przesyłane w formacie XML lub CSV do wcześniej zdefiniowanej lokalizacji.

Kamera SND-3080C dzięki mechanicznemu filtrowi podczerwieni doskonale sprawdza się w dziennych i nocnych warunkach oświetleniowych. Zapewnia możliwość rejestracji obrazów w czasie rzeczywistym z rozdzielczością 4CIF (704×576 pikseli). Obsługuje transmisję wielu strumieni wizyjnych, co pozwala optymalnie dobrać metodę kompresji (H.264, MPEG-4 lub MJPEG) do wymagań konkretnego użytkownika oraz dostępnej infrastruktury sieciowej. Wyposażona zarówno w złącze Ethernet, jak i gniazdo BNC, kamera SND-3080C może jednocześnie przesyłać strumień wizyjny przez sieć IP oraz analogowy sygnał wizyjny metodą tradycyjną, przez kabel koncentryczny.

Dostępne są różne sposoby zdalnego przeglądania obrazów rejestrowanych przez kamerę SND-3080C. Użytkownik może skorzystać ze standardowej przeglądarki internetowej, zapewniającej zdalny dostęp do obrazu w czasie rzeczywistym oraz do danych zapisanych w kamerze na karcie SD. Możliwy jest także pełny dostęp do menu OSD kamery. Alternatywnie można wykorzystać nie wymagające licencji oprogramowanie NET-i firmy Samsung, a także wiele platform NVR innych wiodących producentów.

Innymi przydatnymi funkcjami są: PoE (zasilanie przez sieć Ethernet), WDR (szeroki zakres dynamiki obrazu), poligonalne maskowanie stref prywatności oraz technologia skanowania progresywnego. Dupleksowa transmisja sygnałów fonicznych umożliwia dwukierunkową komunikację głosową między miejscem zainstalowania kamery i pomieszczeniem kontroli.

Kamera SND-3080C jest dostępna w wersji do montażu powierzchniowego, a jej bliźniaczy model SND-3080CF został przeznaczony do instalacji w suficie podwieszanym.

Podobnie jak wszystkie profesjonalne produkty firmy Samsung, kamery SND-3080C oraz SND-3080CF są oferowane wraz z pełnym wsparciem serwisowym firmy Samsung Techwin Europe, w tym bezpłatną pomocą techniczną przy projektowaniu systemów oraz pełną trzyletnią gwarancją.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: redakcja

Samsung wyznacza standardy

W lutym prestiżowe brytyjskie czasopismo „Benchmark Magazine", poświęcone testowaniu profesjonalnych produktów z branży zabezpieczeń, przyznało bardzo wysokie oceny dwu produktom firmy Samsung. Były to SRD-1670 i SSA-S3010. Oceny „Benchmark Magazine" opierają się na wynikach całkowicie niezależnych testów produktów wiodących marek, oceniających ich konstrukcję, parametry, własności użytkowe, funkcjonalność oraz łatwość montażu.

SRD-1670 to szesnastokanałowy rejestrator cyfrowy Samsung, pozwalający na zapis obrazu w czasie rzeczywistym (25 kl./s) we wszystkich kanałach, w maksymalnej rozdzielczości 4CIF. Urządzenie uzyskało ocenę ogólną 90% oraz miano „Wyróżniający się". Tak wysokie noty w ciągu ostatnich dwóch lat przyznano zaledwie dziewięciu innym produktom spośród setek testowanych przez „Benchmark Magazine".

Samsung SSA-S3010 to autonomiczny **sterownik do systemów kontroli dostępu** z biometrycznym skanerem linii papilarnych, czytnikiem kart zbliżeniowych, kart typu Smart i klawiaturą do wprowadzania kodu PIN. Otrzymał ogólną ocenę 83% oraz miano „Zalecany przez Benchmark".

– Samsung cieszy się reputacją producenta jednych z najlepszych systemów zabezpieczeń na świecie. Jedną z najistotniejszych przyczyn tego faktu jest stałe, intensywne inwestowanie w działalność badawczo-rozwojową, które zaowocowało wprowadzeniem licznych innowacji o przełomowym znaczeniu – powiedział **Piotr Rogalewski**, kierownik działu przedsprzedaży firmy Samsung Techwin Europe na obszar Polski, Litwy, Łotwy i Estonii. – *Bardzo cieszy nas fakt tak wysokiej oceny dwóch naszych produktów przez „Benchmark Magazine", szanowane brytyjskie czasopismo z branży zabezpieczeń. Wyniki niezależnych testów potwierdzają pozycję firmy Samsung jako lidera w dziedzinie kompleksowych rozwiązań technologicznych.*

Bezpośr. inf. David Solomons
DRS Marketing

Securitas Polska Sp. z o.o.
Dział Zabezpieczeń Technicznych

nawiąże współpracę z firmami instalatorskimi

Wymagania:

- doświadczenie w branży instalacji elektronicznych systemów zabezpieczeń
- uprawnienia SEP – instalacja i eksploatacja
- uprawnienia elektryczne do 1kV
- licencja zabezpieczenia technicznego oraz koncesja
- całodobowa obsługa serwisowa
- praktyczna znajomość urządzeń systemów CCTV, SSWiN, SKD takich producentów jak min.: Bosch, Infortrend, Samsung, Sony, Axis, Aper, Satel, Galaxy, GE Security, Siemens, Roger, C-Cure, Palko, Falcon,
- znajomość zagadnień projektowania systemu zabezpieczeń technicznych w klasie SA1 – SA4 (ukończony kurs w PISA, TECHOM)

Oferujemy:

- stałe zlecenia w zakresie serwisów, konserwacji i instalacji
- podnoszenie kwalifikacji zawodowych w ramach prowadzonych szkoleń
- korzystanie na partnerskich zasadach z know-how, doświadczenia oraz zasobów Securitas
- terminowe płatności

Zgłoszenia prosimy kierować na adres:
zabezpieczenia.techniczne@securitas.pl

SECURITAS

Japońskie akcenty na uroczystej gali **CBC (Poland)**

4 lutego 2010 roku odbyła się uroczysta gala firmy **CBC (Poland)** pod nazwą „Japonia wszystkimi zmysłami".

CBC (Poland) to oddział japońskiej korporacji CBC Co., Ltd. – jeden z wiodących dostawców sprzętu CCTV na polski rynek. W ofercie firmy znajdują się produkty marki **GANZ** i obiektywy **Computar**.

Spotkanie odbyło się w hotelu Lando w Piasecznie pod Warszawą. Wzięły w nim udział firmy współpracujące, a stronę japońską reprezentował **Toru Takezawa** – *financial director* z CBC (Deutschland) GmbH – który dokonał uroczystego otwarcia gali.

Przedstawiciele CBC (Poland) **Joanna Zajączkowska** (*CCTV Sales Team Leader*) i **Marcin Mroczkowski** (*CCTV Technical Team Leader*) w ramach podsumowania i podziękowania za współpracę w 2010 roku przyznali nagrody.

– Liderem Roku 2010 w kategorii sprzedaż obiektywów Computar została firma Alpol.
– Liderem Roku 2010 w kategorii sprzedaż systemowa obiektywów Computar i GANZ została firma Sawel.
– Liderem Roku 2010 w kategorii sprzedaż kompleksowa obiektywów Computar i GANZ została firma Nekma.
– Liderem Roku 2010 w kategorii inicjatywa marketingowa została firma I.T.O.M. Euroalarm.
– W kategorii Sprzedawca Roku 2010 nagrodę otrzymał dział handlowy firmy Nekma.
– W kategorii Business Partner Roku 2010 nagrodę otrzymała firma PPHU SECURITY Marek Kozak.
– Projektantem Roku 2010 została firma ATOM Service.
– Dealerem Roku 2010 została firma DTS.

Po oficjalnej części gali wszyscy uczestnicy mogli wziąć udział w grach i zabawach w japońskim klimacie. Część artystyczną spotkania przygotowała firma Action Group.

Nie zabrakło również tańców japońskich, które wykonały tancerki z Klubu Japonia Matsuri. Firma Allvision zapewniła nagłośnienie i oświetlenie.

Dużym zainteresowaniem cieszył się pokaz przygotowania sushi, zorganizowany przez Sushi Akademie. Wszyscy goście mogli nie tylko obejrzeć sposób wykonania tych japońskich dań, które podbiły cały świat, ale przede wszystkim ich spróbować.

Po tak wybornej kolacji każdy mógł stracić trochę kalorii na parkiecie. Zabawa taneczna trwała do późnych godzin nocnych.

Firmie CBC (Poland) gratulujemy zorganizowania tak udanego spotkania. Dziękujemy raz jeszcze za zaproszenie redakcji *Zabezpieczeń* oraz życzymy samych sukcesów i pomyślności w 2011 roku.

Ela Końka

Fot. CBC Poland

Samsung Vision Day 2011
podsumowanie

W dniach 3 i 4 marca 2011 r. w hotelu Westin Dragonara na Malcie odbyła się międzynarodowa **konferencja Samsung Vision Day 2011**. Celem konferencji była prezentacja nowych produktów CCTV firmy Samsung oraz jej strategii biznesowej w tej dziedzinie na najbliższe lata. Oprócz gospodarzy w spotkaniu uczestniczyli dystrybutorzy sprzętu CCTV firmy Samsung, licznie przybyli z kilkunastu krajów Europy, a także przedstawiciele prasy.

W pierwszej części konferencji wręczone zostały nagrody dla wiodących dystrybutorów i integratorów, którzy w ostatnich latach mogli pochwalić się dużą sprzedażą produktów Samsunga. Przedstawiono także regionalnych reprezentantów handlowych firmy. Kierownikiem zespołu przedsprzedaży Samsung Techwin Europe, obsługującego klientów w Polsce i krajach bałtyckich, został Piotr Rogalewski, odpowiedzialny za rejon Polski i kilku innych krajów Europy Wschodniej.

W dalszej części konferencji firma Samsung jasno określiła swoje plany związane z ekspansją na rynku europejskim, poparte badaniami i prognozami sporządzonymi przez niezależne agencje marketingowe. Plany inwestycyjne, które mają na celu rozszerzenie oferty firmy, obejmują wprowadzenie na rynek nowych modeli urządzeń CCTV, w tym kamer sieciowych o rozdzielczości HD, a także urządzeń pozwalających na tworzenie kompletnych systemów bezpieczeństwa, między innymi systemów sygnalizacji włamania i napadu, kontroli dostępu, a także wielofunkcyjnych systemów domofonowych.

Tak więc w aktualnej ofercie Samsunga znajdują się nie tylko kamery CCTV i rejestratory wizyjne, lecz także kontrolery przejść, czytniki kart identyfikacyjnych, czytniki biometryczne, centrale zarządzające dużymi instalacjami domofonowymi, abonenckie stacje domofonowe a nawet pasywne czujki podczerwieni. Jak widać, jest to bardzo szeroka i kompleksowa oferta, która umożliwia budowę skomplikowanych systemów bezpieczeństwa z wykorzystaniem wyłącznie produktów Samsunga. Urządzenia, które zaprezentowano na wystawie kończącej pierwszy dzień spotkania, cieszyły się dużym zainteresowaniem uczestników konferencji.

W ramach dodatkowych atrakcji zorganizowano bankiet oraz krótką wycieczkę do Valletty – stolicy Malty.

Redakcja

Zapraszamy do obejrzenia fotoreportażu na naszej stronie internetowej (*www.zabezpieczenia.com.pl*).

Redakcja czasopisma *Zabezpieczenia* dziękuje Organizatorom za zaproszenie na Samsung Vision Day 2011. Firmie Samsung Techwin życzymy zrealizowania wszelkich planów i kolejnych sukcesów.


SAMSUNG TECHWIN
Onvif
FULL HD
iPOLiS
SSA-R1000
Proximity card reader
SSA-R2000V
Vandal resistant proximity and PIN reader
SAMSUNG VISION DAY 2011
Norbain SD Ltd
EMEA
NORBAIN

P2P
w świetle prawa autorskiego

Monika Brzozowska, Areta Ochwat

Jeżeli najczęściej oglądacie hity kinowe przed ich polską premierą; jeśli Wasza dyskografia jest niezwykle bogata, mimo że dawno nie kupiliście płyty ulubionego wykonawcy; jeśli kopiujecie cudze teksty do własnej twórczości lub udostępniacie w Internecie pliki muzyczne – to przeczytajcie ten artykuł, bo nieznajomość prawa autorskiego może okazać się… bardzo kosztowna. Ale po kolei…

Przede wszystkim należy obalić mit, że to, co opublikowane w Internecie, możemy swobodnie kopiować, przedrukowywać czy też przerabiać i modyfikować. Jeśli nawet autor wyraził zgodę na rozpowszechnianie w sieci artykułów, fotografii lub filmów, nie oznacza to jego zgody ani na kopiowanie, ani na jakiekolwiek korzystanie z tych utworów poza zakresem tzw. „dozwolonego użytku".

Należy bowiem podkreślić, że to autor lub inna osoba uprawniona (np. wydawca) decyduje o rozpowszechnianiu utworu (np. artykułu czy fotografii). Działania polegające na wykorzystywaniu lub opracowywaniu cudzej twórczości bez zgody podmiotu uprawnionego i poza zakresem dozwolonego użytku należy kwalifikować jako naruszenie prawa autorskiego. Pamiętajmy: prawo autorskie w sieci niczym nie różni się od prawa autorskiego w świecie realnym. Jest to niezwykle istotne, gdyż w dobie globalnej wioski coraz więcej utworów znajduje się w cyberprzestrzeni i coraz częściej dochodzi do różnego rodzaju „kradzieży intelektualnych" w Internecie.

W XX wieku nastąpił szybki rozwój nowych technologii: powstał standard MP3, format DivX, a w końcu zaczęły funkcjonować internetowe sieci wymiany plików *peer-to-peer* (P2P). Początek XXI wieku to eksplozja komunikacji sieciowej i rewolucja w przepływie informacji. Zaczęto coraz częściej stosować programy typu eMule czy Torrent. Systemy te służą do wymiany plików pomiędzy użytkownikami za pomocą łączy internetowych. Owej wymianie podlegają utwory, czyli dobra chronione przez prawo autorskie. Z technicznego punktu widzenia sprawa wygląda następująco: każdy włączający się do tego rodzaju wymiany użytkownik musi zainstalować na swoim komputerze oprogramowanie, które umożliwia pobieranie danych z udostępnionej części twardego dysku innego użytkownika P2P. Oznacza to, że aby uzyskać poszukiwane pliki, należy uruchomić program typu P2P. Tym samym dana osoba nie tylko pobiera utwór z Internetu (ze zbiorów znajdujących się na komputerach innych użytkowników), ale równocześnie wprowadza do obiegu internetowego inne utwory[1]. Czy takie działanie jest legalne? Oto jest pytanie!

Osoby korzystające z tego typu programów powołują się na tzw. dozwolony użytek prywatny. Warto wobec tego przyjrzeć się bliżej pojęciu dozwolonego użytku. Zgodnie z art. 23 Ustawy o prawie autorskim i prawach pokrewnych „wolno nieodpłatnie korzystać z już rozpowszechnionego utworu w zakresie własnego użytku osobistego (…). Zakres własnego użytku osobistego obejmuje krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego".

O ile więc samo pobieranie plików z Internetu nie musi rodzić odpowiedzialności cywilnej czy karnej, o tyle w przypadku pobierania i jednoczesnego udostępniania tych plików innym użytkownikom możemy mówić o przekroczeniu granic dozwolonego użytku prywatnego. Co więcej, nawet jeśli „ściągający" zablokuje dostęp do zasobów na własnym dysku, to już w czasie „ściągania" danego pliku w systemie P2P dochodzi do udostępniania „ściągniętych" dotychczas pakietów – plików

1) H. Szymański, Zarys problematyki prawnej przetłumaczonych list dialogowych, pobranych z wyspecjalizowanych serwisów internetowych, http://prawo.vagla.pl/node/6216 (stan z 20 lutego 2011 r.).

z fragmentami tego utworu. Niektórzy przedstawiciele doktryny próbują argumentować, że marginesowy charakter takiego udostępniania jako pochodna technicznych właściwości systemu może świadczyć na korzyść „ściągającego”[2]. Podkreślić jednak należy, że jest to w zasadzie jedyny argument, którym ów „ściągający” może się bronić.

Niektórzy prawnicy idą jeszcze dalej i kwestionują w ogóle legalność samego „ściągania” plików. Podkreślają bowiem, że korzystanie z dozwolonego użytku prywatnego dotyczy tylko utworów rozpowszechnionych. Zgodnie zaś z definicją ustawową utworem rozpowszechnionym jest utwór, który został udostępniony za zgodą twórcy. Skoro twórca nie wyraził zgody na rozpowszechnienie w Internecie, „ściągający” nie może powoływać się na dozwolony użytek prywatny. Tutaj jednak zaczynają się rozbieżności w interpretacji prawa – część bowiem „liberalnych” prawników podkreśla, że osoba, która np. „ściąga” plik lub ogląda filmy na YouTube, nie musi sprawdzać, czy twórca wyraził zgodę na rozpowszechnienie w Internecie.

Jak wskazują J. Barta i R. Markiewicz, w przypadku utworów rozpowszechnianych w Internecie nie ma normatywnego uzasadnienia dla ograniczania zakresu użytku osobistego i uzależniania jego legalności od tego, czy utwór był rozpowszechniony zgodnie z prawem, skoro taki warunek nie jest stawiany w przypadku utworów rozpowszechnionych w inny sposób.

W odniesieniu do dozwolonego użytku trzeba również pamiętać, że zgodnie z art. 35 Ustawy o prawie autorskim i prawach pokrewnych: „Dozwolony użytek nie może naruszać normalnego korzystania z utworu lub godzić w słuszne interesy twórcy”. Często podkreśla się, że wykorzystywanie i udostępnianie np. plików muzycznych lub filmów godzi w interesy np. producenta i aktorów. Producent filmu inwestuje środki finansowe, by poprzez system licencji uzyskać zwrot nakładów i osiągnąć zysk. Tymczasem rozpowszechnianie filmu przed jego premierą kinową w Polsce, a tym bardziej pojawieniem się w sklepach na płytach DVD, niewątpliwie godzi w słuszne interesy podmiotu uprawnionego z tytułu majątkowych praw autorskich.

Należy zaznaczyć, że w przypadku filmów stanowiących utwory audiowizualne może być wiele podmiotów uprawnionych z tytułu autorskich praw majątkowych i praw pokrewnych. Wystarczy wspomnieć, że współtwórcy utworu audiowizualnego i jego wykonawcy (aktorzy) są uprawnieni do wynagrodzenia za określone w przepisie formy eksploatacji utworu audiowizualnego, niezależnie od przysługujących im majątkowych praw autorskich do utworu. Niewątpliwie zatem ich interesy są naruszane w przypadku rozpowszechniania utworu poza oficjalną drogą dystrybucji. Jeżeli chodzi o kwestię przekroczenia dozwolonego użytku osobistego, to ustawa wyraźnie stanowi: „Zakres własnego użytku osobistego obejmuje krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego”. Udostępnianie plików muzycznych czy filmów w systemie P2P wykracza poza zakres tzw. „stosunku towarzyskiego”. Jak zauważa H. Szymański, użytkownik w systemie P2P nie ma technicznej możliwości kontrolowania, kto pobiera plik, a zatem należy przyjąć, że udostępnia dany plik nieokreślonej grupie odbiorców[3].

Pamiętajmy jeszcze o jednej bardzo istotnej rzeczy. Naruszenie prawa autorskiego wiąże się nie tylko z odpowiedzialnością cywilną (i koniecznością np. zapłaty potrójnego wynagrodzenia, gdy naruszenie jest zawinione). Bardziej dotkliwa może okazać się odpowiedzialność karna. Zgodnie bowiem z prawem autorskim: „Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór (…) podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3” (art. 116). Dodatkowo w razie skazania za ten niecny czyn sąd może orzec „przepadek przedmiotów służących do popełnienia przestępstwa, chociażby nie były własnością sprawcy” (art. 121). Jak zauważa H. Szymański, w tym przypadku wspomnianym przedmiotem jest komputer z oprogramowaniem, a nawet (co może już budzić większe wątpliwości) monitor[4].

Jak wskazują J. Barta i R. Markiewicz, w procesie dotyczącym jednej z pionierskich firm w tej branży – w tzw. sprawie Nepstera – sądy amerykańskie uznały użytkowników Internetu korzystających z usług Nepstera za dopuszczających się bezpośredniego naruszenia praw autorskich i wkroczenie w monopol twórcy już poprzez samo oferowanie plików z utworami, jak również „ściąganie” ich i tworzenie trwałych kopii na własnym komputerze. Natomiast co do usługodawcy uznano, że można mu postawić zarzut co najmniej przyczynienia się do naruszenia prawa autorskiego, jako że tego rodzaju usługi polegają z założenia na organizowaniu działalności prowadzącej do naruszeń prawa autorskiego i praw pokrewnych, a użytek naruszający prawo stanowi w zasadzie regułę. Jak zauważają autorzy, przenosząc te rozważania na grunt prawa polskiego: „nie budzi wątpliwości fakt, iż udostępniający plik muzyczny w Internecie do powszechnego «ściągania» narusza prawo autorskie”[5].

Podsumowując całość powyższych rozważań, można dojść do następujących wniosków: „ściąganie” plików nie musi rodzić odpowiedzialności cywilnej lub karnej. Natomiast udostępnianie plików bez zgody podmiotu uprawnionego już rodzi taką odpowiedzialność.

Podobnie przedstawia się sprawa innych utworów (czyli przejawów działalności twórczej o indywidualnym charakterze). Samo czytanie artykułów znajdujących się w sieci jest oczywiście dozwolone, podobnie jak ich drukowanie na własny użytek. Jeśli jednak ktoś wykorzysta artykuł poza zakresem dozwolonego użytku, na przykład umieści go na swojej stronie internetowej bez podania informacji o jego autorstwie i źródle lub też zasugeruje, iż jest jego autorem, to naruszy przepisy prawa polskiego, a pewnie i boskiego (patrz: VII przykazanie). Zakres „dozwolonego użytku” jest ściśle określony przez prawo i nie każde nasze działanie w cyberprzestrzeni można będzie uznać za legalne. Warto o tym pamiętać.

mec. Monika Brzozowska
Areta Ochwat

2) J. Barta, R. Markiewicz, Prawo autorskie, Oficyna a Wolters Kluwer business, Warszawa 2010, s. 347.

3) H. Szymański, op. cit.

4) Ibidem.

5) J. Barta, R. Markiewicz, op. cit., s. 345–346.

Versa
wszechstronne centrale alarmowe

Nowoczesne centrale VERSA to połączenie intuicyjnej i prostej obsługi z zaawansowanymi możliwościami rozbudowy i wszechstronnymi funkcjami komunikacyjnymi. Dzięki temu są idealnym rozwiązaniem dla zabezpieczania mieszkań, domów i małych obiektów handlowo-biurowych.

AKADEMIA Satel ZAPRASZA

Zapraszamy do Akademii SATEL
na specjalistyczne szkolenia z zakresu:

1. **Instalacji systemów alarmowych opartych na centralach VERSA**
2. Instalacji systemów alarmowych opartych na centralach INTEGRA
3. Programowania i instalacji systemu kontroli ACCO
4. Programowania i obsługi stacji monitorującej STAM-2

Zapisy na stronie
http://www.szkolenia.satel.pl

Satel®

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

Czy jesteś pewien, że Twoje oszczędności są bezpieczne?

Krzysztof Białek

Gdybyśmy trzydzieści lat temu przeprowadzili uliczną ankietę i zadali jedno pytanie: „Czy Twoim zdaniem kiedyś w każdym polskim domu będzie komputer?”, wielu respondentów zapewne popukałoby się w głowę. Dziś wielu z nas nie potrafi sobie wyobrazić pracy, nauki czy rozrywki bez komputera, a w naszych mieszkaniach często znajduje się więcej niż jedna stacja robocza. Dla najmłodszych komputer to tak samo pospolite urządzenie jak telewizor czy telefon. Oczywiste dla naszych milusińskich jest również to, że korzystanie z przepastnych zasobów Internetu nie jest już wyjątkowym dobrodziejstwem, lecz zwykłym, codziennym, ułatwiającym życie zajęciem. W żartach mówi się, że jeśli czegoś nie można znaleźć w Internecie, to rzecz ta po prostu nie istnieje

Stale rosnąca liczba osób korzystających z usług internetowych jest siłą napędową dla pomysłowości przedsiębiorców. Coraz więcej spraw można załatwić, nie wychodząc z domu, dzięki takim możliwościom jak: różne formy komunikowania się (poczta elektroniczna, rozmowy za pośrednictwem VoIP, czaty, fora dyskusyjne, blogi), bankowość elektroniczna, a nawet zakupy za pomocą Internetu. Jeszcze dziesięć lat temu nikt nie sądził, że może powstać coś takiego jak portal społecznościowy. Obecnie liczba aktywnych użytkowników takich portali na świecie przekracza trzysta milionów, a wielu z nas ma więcej „przyjaciół" w swoim profilu niż w prawdziwym życiu. Nie będziemy się jednak skupiać na wpływie Internetu na życie społeczne i psychikę użytkowników, lecz na fakcie, że z rozwoju technologii czerpią korzyści również ci, którzy żerują na ludzkiej naiwności i braku świadomości zagrożeń.

Ponad dwadzieścia lat upłynęło od dnia, w którym w sieci Internet znalazł się „przodek" dzisiejszych wirusów, trojanów i robaków. Był nim samokopiujący się program stworzony przez Roberta Morrisa – pracownika jednej z amerykańskich uczelni. 2 listopada 1988 roku do komputerów korzystających z sieci zewnętrznej Morris wprowadził złośliwy kod, który w dwie godziny od uruchomienia programu uniemożliwił wielu administratorom dostęp do komputerów. W efekcie zainfekowanych zostało – jak oszacowano – przeszło sześć tysięcy maszyn, co w tamtych czasach mogło stanowić nawet jedną dziesiątą wszystkich komputerów podłączonych do sieci Internet. Dopiero po ośmiu dniach przywrócono funkcjonowanie urządzeń do stanu sprzed infekcji.

Tego typu zagrożenia występują także obecnie, ale w odróżnieniu od występku Morrisa – który nie był świadomy, jak duże zamieszanie spowoduje jego program – mamy do czynienia z działaniami nakierowanymi na celowe doprowadzenie do destabilizacji systemów. Również skala działań (liczba zaatakowanych maszyn i wymierne straty finansowe) jest nieporównywalnie większa. Atakującymi mogą być na przykład hakerzy – entuzjaści, którzy chcą w ten sposób zaistnieć w swoim środowisku, ale coraz częściej działania tego typu są prowadzone na zlecenia zorganizowanych grup przestępczych, których celem jest maksymalizacja zysku.

Coraz więcej klientów banków korzysta z możliwości kontrolowania stanu swoich rachunków oszczędnościowych i wykonywania operacji finansowych za pośrednictwem Internetu. Pozwala to na zaoszczędzenie czasu (nie musimy wychodzić do banku, stać w nierzadko długich kolejkach) i pieniędzy (prowizje za samodzielne wykonanie operacji bankowych są najczęściej niższe niż koszt wykonania tych samych czynności przez pracownika banku). Podobnie przedstawia się sytuacja przy robieniu zakupów – sklepy internetowe najczęściej oferują ten sam towar co sklepy tradycyjne, ale po niższej cenie, w dodatku z dostawą do domu. Coraz więcej klientów dokonuje płatności „z góry" za pośrednictwem specjalnych stron oferujących możliwość realizacji bezpiecznych transakcji internetowych. Portale finansowe są odpowiednio zabezpieczone przed atakami i próbami włamań do nich – najsłabszym ogniwem transakcji może okazać się nasz komputer, czy nawet telefon komórkowy. O procederze zwanym phishingiem[1] pisaliśmy już na łamach naszego periodyku. Przypomnijmy tylko, że phishing jest próbą wyłudzenia poufnych informacji (takich jak loginy, hasła, dane osobowe) poprzez podszycie się pod godną zaufania osobę lub instytucję. Najczęściej możemy stać się ofiarami tego typu procederu, gdy np. po otrzymaniu spreparowanej wiadomości e-mail zapraszającej do aktualizacji swoich danych (wiadomości wskazującej na to, że została do nas wysłana np. przez bank czy portal aukcyjny) klikniemy zawarty w niej link. To z kolei może spowodować przekierowanie przeglądarki internetowej do strony, która do złudzenia przypomina portal aukcyjny lub stronę naszego banku, a w rzeczywistości jest formularzem przesyłającym podane przez nas dane wprost do bazy danych przestępców. Jeśli w ten sposób przekazaliśmy swój login, hasło i jeszcze kilka liczb zawartych na karcie kodów jednorazowych umożliwiających autoryzację operacji finansowych, możemy spodziewać się w niedługim czasie kłopotów z dostępnością do funduszy zgromadzonych na koncie bankowym. W tym miejscu należy zwrócić uwagę, że ofiarami phishingu możemy paść nie tylko poprzez uaktywnienie łącza zawartego w otrzymanej, spreparowanej wiadomości e-mail. Również jeśli nasz komputer został zainfekowany wirusem (np. w wyniku instalacji programu pochodzącego z nieznanego źródła lub wskutek uruchomienia załącznika z „zakażonej" wiadomości e-mail), możemy bezwiednie zostać przekierowani na stronę przestępców wyłudzających dane. Pomimo że wpiszemy do przeglądarki adres strony internetowej swojego banku, wirus po wykryciu żądania połączenia ze stroną banku wykona automatyczne przekierowanie na spreparowaną, fałszywą stronę.

Ostatnio rozwinęła się kolejna forma wyłudzeń, umożliwiająca dostęp do środków zgromadzonych na lepiej zabezpieczonych bankowych kontach oszczędnościowych. Do niedawna celem ataków phishingowych byli klienci banków, którzy do zlecania operacji nie musieli podawać dodatkowych – poza loginem i hasłem – danych autoryzacyjnych bądź wykorzystywali do autoryzacji karty kodów jednorazowych. Do wyłudzenia powyższych danych służyły właśnie spreparowane wiadomości e-mail oraz podrabiane przez przestępców strony internetowe. Obecnie na baczności muszą się mieć również klienci korzystający z bardziej zaawansowanej formy zabezpieczenia operacji bankowych, polegającej na losowo generowanych hasłach autoryzacyjnych, przesyłanych na ich telefony komórkowe. W skrócie mechanizm działania przestępczego jest następujący. Klient będący celem ataku phishingowego zostaje przekierowany na spreparowaną stronę internetową, wyłudzającą poufne dane umożliwiające dostęp do konta bankowego (login i hasło). Dodatkowo klient jest proszony o aktualizację danych dotyczących telefonu, na który bank wysyła wiadomości SMS służące do potwierdzania dokonania operacji (podaje numer telefonu, a nawet nazwę producenta i typ aparatu telefonicznego). Na numer telefonu podany przed chwilą w formularzu przez klienta przesyłana jest wiadomość z linkiem zapraszającym do

1) Phishing (spoofing) – w branży komputerowej, oszukańcze pozyskanie poufnej informacji osobistej, jak hasła czy szczegółów karty kredytowej, przez udawanie osoby godnej zaufania, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej (źródło: Wikipedia – przyp. red.).

pobrania na telefon „certyfikatu bezpieczeństwa". W rzeczywistości ściągana aplikacja nie ma nic wspólnego z certyfikatem bezpieczeństwa, lecz jest wirusem (np. Trojan Zeus/Zbot), który przechwytuje m.in. wiadomości SMS z kodami autoryzacji otrzymywanymi z banku i wysyła je niepostrzeżenie do systemów kontrolowanych przez cybernetycznych gangsterów. Przestępcy, posiadając komplet danych – login i hasło dostępu do konta wyłudzone wcześniej na spreparowanej stronie, a teraz dodatkowo hasło autoryzacyjne przesłane SMS-em na telefon komórkowy – mogą dokonać nieuprawnionego przelania pieniędzy na własne konta, tzw. „konta muły".

O tym, że padliśmy ofiarą przestępstwa, dowiadujemy się czasem dopiero wtedy, gdy nasze konto zostaje wyczyszczone. Zwykle dalszy scenariusz jest podobny: kontakt z bankiem, zgłoszenie reklamacji wykonanej operacji, a potem złożenie na policję doniesienia o podejrzeniu popełnienia przestępstwa. Nikogo nie trzeba zapewne przekonywać o tym, że czynnościom takim towarzyszyć muszą zdenerwowanie oraz niepewność, czy uda nam się odzyskać skradzione pieniądze.

Biorąc pod uwagę opisane wcześniej mechanizmy wyłudzania danych – a w konsekwencji wyłudzania pieniędzy – można mieć wątpliwości, czy pomimo szerokiej dostępności usług bankowości elektronicznej korzystanie z nich jest bezpieczne. Odpowiedź brzmi: TAK, ale pod warunkiem że mamy świadomość istnienia zagrożeń i sposobów obrony przed nimi. I tak:

1) Trzeba pamiętać, że cyberprzestępcy wykorzystują przede wszystkim możliwości występujące po stronie klienta. Instytucje finansowe z reguły mają bardzo dobrze zabezpieczone połączenia z Internetem, a ich działalność antyphishingowa skupia się przede wszystkim na uświadamianiu klientom zagrożeń, a także na współpracy z organizacjami wyszukującymi w sieci spreparowane strony internetowe. W przypadku wyłudzeń najczęściej nie dochodzi do bezpośredniej komunikacji klienta z prawdziwymi systemami banku, lecz z podstawionymi stronami wyłudzającymi dane.
2) Recepta na spokojny sen jest prosta:
   – Nie korzystaj – o ile to możliwe – z dostępu do konta bankowego za pośrednictwem komputerów publicznych (np. w kawiarniach internetowych), użyczonych przez nieznajomych oraz gdy (jeśli nawet używasz własnego laptopa) dostęp do Internetu nie jest szyfrowany lub nie masz co do tego pewności (np. sieci bezprzewodowe nie zawsze są zabezpieczone).
   – Korzystaj z legalnego systemu operacyjnego i legalnego oprogramowania narzędziowego, aktualizuj je na bieżąco.
   – Zainstaluj i aktualizuj na bieżąco program antywirusowy oraz firewall.
   – Pamiętaj, że Twój bank nigdy nie prosi o aktualizację poufnych danych umożliwiających autoryzowanie operacji bankowych.
   – Jeśli masz wątpliwości lub podejrzewasz, że stałeś się ofiarą ataku, skontaktuj się z pracownikiem banku.

Krzysztof Białek

RACS 4

System Kontroli Dostępu

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

RCP Master *PR602LCD*

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

roger®

www.roger.pl

20 YEARS 1991-2011

Wprowadzono do oferty EMR-1-LT oraz EMR-1-SDC - moduły czytników zbliżeniowych EM 125 kHz dedykowane do zabudowy w urządzeniach innych producentów.

BEZPIECZEŃSTWO A NORMALIZACJA

CZYLI INNOWACJE W NORMALIZACJI Z WOJSKIEM W TLE

(CZĘŚĆ 2)

Marek Blim

Artykuł będący kolejnym w cyklu odnosi się do kwestii komunikacji w e-społeczności oraz związanego z nią przenoszenia (lub przenikania) do środowiska cywilnego rozwiązań normalizacyjnych opracowanych w wojsku i na potrzeby wojska. Podaje przykłady otwartego dostępu do technik i technologii o charakterze militarnym, obecnie powszechnie użytkowanych w społeczeństwie. Omawia innowacyjność w stosowaniu norm, propagowaną przez Unię Europejską, oraz niektóre kwestie normalizacji rynku zamówień i usług sektora obronnego w ramach UE i NATO

Truizmem będzie stwierdzenie, że nie można mówić o społeczeństwie informacyjnym bez sprawnej komunikacji – tej bezpośredniej (tu i teraz) i szeroko rozumianej, dalekosiężnej, możliwej w obszarze całego świata dzięki łączom radiowym i przewodowym. Przypomnę zatem, że zgodnie z decyzją przywódców państw podjętą w listopadzie 2005 roku w Tunisie podczas Światowego Szczytu Społeczeństwa Informacyjnego oraz postanowieniami konferencji Międzynarodowego Związku Telekomunikacyjnego (ITU), która odbyła się w 2006 roku w Antalyi (w Turcji) postanowiono obchodzić dzień 17 maja jako „Światowy Dzień Telekomunikacji i Społeczeństwa Informacyjnego". Data ta upamiętnia utworzenie 17 maja 1865 r. w Paryżu Międzynarodowego Związku Telegraficznego (ITU – *International Telegraph Union*). Był on poprzednikiem obecnie funkcjonującego Międzynarodowego Związku Telekomunikacyjnego – wyspecjalizowanej organizacji Narodów Zjednoczonych obejmującej obecnie 191 państw (Polska jest członkiem ITU od 1921 roku). Głównymi zadaniami związku są standaryzacja i zarządzanie pasmem radiowym – mamy więc do czynienia z normalizacją „w eterze", nad wyraz istotną, bo bezpośrednio związaną z wykorzystywaniem poszczególnych zakresów na potrzeby obronności i porządku publicznego.

1. Nowe inicjatywy informacyjne – udział technik militarnych

Opisując w poprzednim artykule różnego rodzaju uwarunkowania oraz historię dokonań normalizacyjnych, zasygnalizowałem, że funkcjonujące na polskim rynku Normy Obronne (NO) odbiegają od znanych wszystkim Polskich Norm (PN), głównie ze względu na swoją obligatoryjność stosowania oraz niejawny (w większości) charakter ujętych w nich treści. Obecnie, w ramach wspólnych działań cywilno-wojskowych w warunkach kryzysów i zagrożeń (CIMIC – *CIvil & MIlitary Cooperation*), sytuacja ta się zmienia. Przykładem mogą być obchody Światowego Dnia Telekomunikacji i Społeczeństwa Informacyjnego w Polsce w 2010 roku – pod hasłem ITU: „Techniki informacyjne i komunikacyjne katalizatorem lepszego życia w mieście" („Better city, better life with ICTs").

13 maja 2010 roku w Sali Kolumnowej Sejmu RP odbyła się z tej okazji XI Konferencja Okrągłego Stołu (KOS) pod nazwą „Polska w drodze do Społeczeństwa Informacyjnego; techniki informacyjne i komunikacyjne katalizatorem lepszego życia w mieście". Pokazała ona możliwości normatywnie zastosowanych nowoczesnych technik informacyjnych.

Swoistym novum XI KOS był przekaz multimedialny w postaci wideokonferencji z wirtualnymi ośrodkami studyjnymi oraz transmisji internetowej na żywo (w obradach KOS wzięli udział goście oraz prelegenci obecni w studiu wirtualnym Przemysłowego Instytutu Telekomunikacji oraz w studiach terenowych – w Gdańsku, Wrocławiu i Szczecinie).

Szczególnie pragnę zwrócić uwagę Czytelników na zrealizowany w ten sposób panel główny konferencji, który przebiegał pod hasłem: „Cywilizacja technik militarnych na rzecz poprawy warunków życia w mieście". Uczestniczyli w nim przedstawiciele grupy BUMAR i PIT S.A.

Prelegenci przedstawili przykłady zastosowania technik wojskowych w rozwiązaniach cywilnych. Ich wystąpienia były uzupełnione o panel branżowy, zrealizowany pod hasłem: „Polityka Regulatora katalizatorem rozwoju społeczeństwa informacyjnego i poprawy warunków życia", oraz panel akademicki, pod hasłem: „Inicjatywy środowisk naukowych na rzecz rozwoju społeczeństwa informacyjnego". W pierwszym z nich znalazł się bardzo ciekawy referat prof. Aleksandry Monarchy-Matlak z Uniwersytetu Szczecińskiego, dotyczący związku między pojęciem społeczeństwa informacyjnego a informatyzacją sektora publicznego w obszarze poprawy życia mieszkańców miast (wygłoszony w studiu wirtualnym w Szczecinie).

W panelu głównym tej cywilnej konferencji po raz pierwszy w Polsce tak jednoznacznie pokazano militarny rodowód stosowanych już powszechnie technik ICT[1]. Ale jeśli już mówimy o telekomunikacji, czym byłyby dzisiejsze telefony komórkowe bez uwzględnienia rozwiązań przejętych ze zminiaturyzowanej (noszonej na hełmie) taktycznej radiostacji pola walki?

Normalizacja niejawna istniała już w II RP. Tajne dokumenty dotyczące zasad budowy elektromechanicznych „bomb kryptologicznych"[2] na potrzeby odtwarzania ustawień klucza niemieckiej Enigmy powstały w 1938 roku w Biurze Szyfrów Sztabu Głównego RP jako matematyczny model autorstwa Mariana Rejewskiego i zostały przekazane konstruktorom z zakładu „AVIA" przy ul. Stępińskiej w Warszawie[3]. Zespół pracujący pod kierownictwem inż. Antoniego Pallutha opracował znormalizowane rozwiązanie praktyczne bazujące na polskich kopiach Enigmy (wykonano sześć sztuk tych urządzeń). Dokumentację techniczną „bomb kryptologicznych", wykonaną z wykorzystaniem niejawnych polskich norm, przekazano w sierpniu 1939 roku przedstawicielom Anglii i Francji wraz z egzemplarzami kopii samych maszyn[4]. Pierwsze urządzenia „bomb" w angielskim Bletchley Park pracowały na bazie polskich norm wojskowych w połączeniu z polskimi wzorami „płacht Zygalskiego"[5].

Współczesne Normy Obronne to domena Wojskowej Komisji Normalizacyjnej oraz byłych biur: Wojskowego Biura Standaryzacyjnego MON (1993–1998) oraz Biura Wojskowej Służby Normalizacyjnej MON (1998–2002), a obecnie Wojskowego Centrum Normalizacji, Jakości i Kodyfikacji MON. Wsparcie w zakresie prowadzenia badań jakościowych i audytowania rezultatów stanowił do 31 grudnia 2010 roku samodzielny Zakład Systemów Jakości i Zarządzania MON, powołany decyzją nr 3/MON z 8 stycznia 2002 roku. Obecnie jest on pozbawiony samodzielności zarządczej oraz finansowej i od 1 stycznia 2011 roku funkcjonuje jako ZSJiZ – laboratorium Wydziału Mechanicznego Wojskowej Akademii Technicznej. Wypada przypomnieć, że samodzielny zakład budżetowy MON jako jedyny organ w Polsce posiadał uprawnienia w zakresie prowadzenia certyfikowanych szkoleń i audytów na zgodność z natowskimi wymaganiami zawartymi w AQAP.

2. Innowacyjna rola norm we współczesnym świecie

Kwestie zarządzania jakością oraz bezpieczeństwem środowiska i informacji mają w dzisiejszym świecie biznesu charakter uniwersalny. Dlatego popularyzacja norm (zarówno cywilnych, jak i wojskowych) jako kwalifikowanych dobrych praktyk jest dla większości osób z personelu zarządczego (kierowniczo-technicznego) czymś oczywistym, niezależnie od specyfiki działania danej firmy. Z perspektywy Polski normy mają znaczenie strategiczne w przypadku wchodzenia naszych towarów na rynki europejskie.

Warto pamiętać, że w ramach strategii UE mającej na celu wzrost gospodarczy i wzrost zatrudnienia Komisja Europejska oraz Rada Unii Europejskiej uznały normalizację za kluczowy instrument pobudzania innowacyjności. Rada ds. Konkurencyjności w swych zapisach z 4 grudnia 2006 roku podkreśliła potrzebę udoskonalenia europejskiego systemu normalizacyjnego[6] oraz wezwała Komisję do przedstawienia propozycji działań, jakie powinny podjąć zainteresowane strony, aby zreformować i usprawnić ten system. Parlament Europejski w swej rezolucji w sprawie strategii innowacyjnej[7] również podkreślił znaczenie wkładu norm w politykę innowacyjną.

Komisja Wspólnot Europejskich w wyniku podjętych prac, po szerokich konsultacjach i uwzględnieniu uwag Europejskiego Komitetu Społeczno-Ekonomicznego, opublikowała 11 marca 2008 roku komunikat dla Rady i Parlamentu Europejskiego[8], podkreślając w nim rolę i charakter podejmowanych na rynku europejskim działań.

1) ICT lub I&CT – akronim używany dla skróconego opisu technologii informatycznych i telekomunikacyjnych

2) Nazwę bomba dla agregatu kryptologicznego Rejewskiego przypisuje się jako pomysłodawcy Jerzemu Różyckiemu; za: Wł. Kozaczuk, W kręgu Enigmy, wyd. Książka i Wiedza, Warszawa 1979, s. 100.

3) Zakład „AVIA" realizował w dziale produkcji specjalnej szereg niejawnych zamówień na rzecz Ministerstwa Spraw Wojskowych II RP.

4) Wł. Kozaczuk, W kręgu Enigmy, wyd. Książka i Wiedza, Warszawa 1979, s. 111.

5) Tamże, s. 208.

6) http://www.eu2006.fi/news_and_documents/conclusions/vko50/en_GB/1165932111543/.

7) Rezolucja Parlamentu Europejskiego z 24 maja 2007 r. w sprawie wykorzystania wiedzy w praktyce: szeroko zakrojona strategia innowacyjna dla Europy.

8) Ku zwiększeniu wkładu normalizacji w innowacje w Europie, COM(2008)133(Final) z 11.03.2008 r.

Strony zainteresowane, czyli europejski przemysł, biznes, organizacje normalizacyjne i stowarzyszenia zawodowe Europejskiego Obszaru Gospodarczego (EEA) z francuskim A2AP na czele, angażują się w normalizację zarówno na płaszczyźnie formalnej, jak i nieformalnej. Normalizacja formalna przebiega na trzech poziomach, obejmujących: krajowe organy normalizujące (KON), trzy europejskie organizacje normalizacyjne (EON[9]) oraz organizacje międzynarodowe[10]. Warto wiedzieć, że w celu skupienia polityki normalizacyjnej UE na innowacjach Komisja Europejska w przywołanym wcześniej komunikacie określiła dziewięć następujących kluczowych zadań przedmiotowych:

1) Potwierdzić zobowiązanie do prowadzenia **normalizacji** zorientowanej na rynek oraz do dobrowolnego stosowania norm. Specyficzna wartość dodana normalizacji w wyznaczaniu specyfikacji technicznych wynika bowiem z dobrowolnej współpracy między podmiotami prywatnymi i publicznymi.
2) Uznać **znaczenie zarówno formalnych, jak i nieformalnych norm** dla innowacji. Formalny proces normalizacji, przeprowadzony w pełnym poszanowaniu zasad otwartości, integracji, przejrzystości i spójności oraz prowadzący do konsensusu między wszystkimi krajowymi stanowiskami i, w razie potrzeby, wszystkimi zainteresowanymi stronami jest niezbędny.
   [*Inne normy, opracowane przez uznane organizacje normalizacyjne i inne organizacje, są bardziej otwarte na technologie innowacyjne, w związku z czym odgrywają ważną rolę w przyspieszaniu uznawania norm przez rynek. By móc czerpać korzyści z obu rodzajów norm, zachować spójność europejskiego systemu normalizacji oraz zoptymalizować wpływ dostępnych ekspertów, należy ułatwić sprawną koordynację działań pomiędzy formalnymi i nieformalnymi organami normalizacyjnymi. W związku z tym za dobrą praktykę powinna zostać uznana praktyka ETSI na poziomie europejskim oraz ISO i IEC na poziomie międzynarodowym, polegająca na włączaniu do współpracy wielu nieformalnych forów normalizacyjnych*].
3) Zająć się w szczególności **opracowywaniem norm dla rynku światowego**. Europejski przemysł potrzebuje norm, które umożliwiają dostęp do globalizujących się rynków. Ważne jest, by przemysł europejski brał od samego początku udział w wyznaczaniu norm dla rynków światowych[11].
   [*Komisja zachęca strony zainteresowane normalizacją europejską do większego zaangażowania w normalizację międzynarodową, do nawiązywania współpracy w zakresie działań i polityk normalizacyjnych poszczególnych regionów, a w szczególności do wzmocnienia roli EON w zwiększaniu europejskiego wkładu w międzynarodową normalizację*].
4) Ułatwiać **integrację nowej wiedzy w normach**, w szczególności wiedzy pochodzącej z finansowanych ze środków publicznych programów w dziedzinie badań i innowacji, w tym ze wspólnotowego programu ramowego w zakresie Badań i Rozwoju Technologicznego (BRT) oraz programu ramowego na rzecz konkurencyjności i innowacji (CIP).
   [*Komisja zachęca organizacje normalizacyjne do ułatwiania społeczności badawczej dostępu do opublikowanych norm, a EON zachęca się do przygotowania wspólnej propozycji rozpoczęcia działań monitorujących rozwój technologii oraz do ustanowienia punktów kontaktowych skupiających się na ułatwianiu transferu wyników programów ramowych BRT i CIP do normalizacji*].
5) Ułatwić **dostęp do normalizacji wszystkim zainteresowanym stronom, w szczególności małym i średnim przedsiębiorstwom (MŚP)**, ale również użytkownikom/konsumentom i badaczom. Normalizacja jest potężnym narzędziem umożliwiającym upowszechnianie stanu wiedzy wśród MŚP, a poprzez uczestnictwo konsumentów również ułatwianie przejmowania innowacji przez rynek. UE wspiera reprezentację sektora MŚP w działaniach normalizacyjnych na poziomie europejskim.
6) Polityka UE musi przyczynić się do sprawniejszego znoszenia przeszkód hamujących **wdrażanie i skuteczne stosowanie norm**, takich jak niedostateczna widoczność norm, ich skomplikowany charakter, niepewność co do zgodności z normą lub istnienie norm konkurencyjnych.
   [*Komisja wzmocni swe wsparcie dla koordynowania integracji norm w innowacyjnych produktach i praktykach handlowych poprzez normalizacyjne sieci Europe Innova*].
7) Zarówno **prawa własności intelektualnej (IPR)**, jak i normalizacja pobudzają innowacyjność oraz ułatwiają upowszechnianie technologii. Jednak, ponieważ przyczyniają się one do realizowania wspólnych celów na różne sposoby, należytą uwagę należy poświęcić wzajemnym powiązaniom między IPR a normalizacją.
   [*Komisja jest zdania, że normy powinny być ogólnodostępne i możliwe do wdrażania przez wszystkich, a prawa własności intelektualnej związane z daną normą powinny być brane pod uwagę w procesie normalizacji. Pozwoliłoby to osiągnąć równowagę między interesem użytkowników norm a prawami właścicieli własności intelektualnej. EON zobowiązały się do zagwarantowania, że normy, ze wszystkimi IPR, jakie mogłyby zawierać, będą mogły być wykorzystywane przez podmioty gospodarcze na zasadach uczciwych i rozsądnych (FRAND)*].
8) Silny europejski system normalizacyjny stanowi ogromną wartość dla przemysłu, rządów i obywateli Europy. **EON pełnią podstawową rolę w europejskim procesie normalizacji, a będący w toku proces ich reformy** zasługuje na szczególną uwagę.

9) EON to: CEN dla większości sektorów, CENELEC dla elektrotechniki, ETSI dla telekomunikacji.

10) IEC w elektrotechnice, ITU w telekomunikacji oraz ISO w większości pozostałych dziedzin, ale także Międzynarodowa Organizacja Lotnictwa Cywilnego, Kodeks Żywnościowy „Codex Alimentarius" itd.

11) Europejskie zadanie: osiągnąć sukces w epoce globalizacji, COM (2007) 581 z 03.10.2007 r.

[*Komisja zachęca EON do kontynuowania wysiłków i wyznaczania ambitnych celów reformy, w szczególności w celu jeszcze większego przyspieszenia procesu normalizacji, zagwarantowania proaktywnego wyznaczania priorytetów do realizacji, opartych na potrzebach przemysłu i użytkowników, oraz określenia rodzaju produktów, jakie powinny powstać w wyniku tego procesu. Komisja zachęca EON oraz KON, by regularnie przyznawały pierwszeństwo nowym działaniom normalizacyjnym na poziomie europejskim, unikając w ten sposób ewentualnych opóźnień wynikających z prac przygotowawczych na poziomie krajowym*].

9) **Główne cele europejskiej normalizacji muszą nadążać za rozwijającymi się potrzebami gospodarki i społeczeństwa europejskiego** oraz drastycznymi zmianami na międzynarodowej scenie politycznej oraz w środowisku gospodarczym.
[*Komisja zachęca wszystkie strony zainteresowane normalizacją do współpracy we wdrażaniu środków zaproponowanych w niniejszym komunikacie. Jednocześnie również obecne i przyszłe wyzwania wymagają dogłębnej analizy co do zakresu i roli europejskiej normalizacji w nowym kontekście światowym oraz ewentualnej aktualizacji jej istniejącej podstawy prawnej*].

Komisja Europejska, publikując niniejsze zasady, oczekiwała i nadal oczekuje, że europejskie organy normalizacyjne, przemysł oraz wszystkie strony europejskiego obszaru gospodarczego EOG/EEA (*European Economic Area*) zainteresowane normalizacją rozważą wszystkie wymienione środki oraz podejmą stosowne działania. Dotychczasowe obserwacje potwierdzają słuszność tego kierunku działania.

Dyskusyjne pozostają działania quasi-normalizacyjne szeregu stowarzyszeń międzynarodowych, które publikując przygotowane i popularyzowane przez siebie opracowania, bardzo często uzyskują dla części z nich szerokie zastosowania międzynarodowe. Niektóre rozwiązania są traktowane jako standardy faktyczne pomimo braku formalnych norm. Podobną rolę pełnią porozumienia sprzymierzonych podpisywane jako uzupełnienia i wymogi w ramach istniejących sojuszy wojskowych (np. natowski AQAP). Stąd też dodatkowym elementem wpływającym na coraz szersze stosowanie rozwiązań normatywnych lub stowarzyszeniowych w procesach biznesowych są celowe działania Unii Europejskiej na rzecz inicjatyw utworzenia jednolitego logistycznie rynku uzbrojenia.

3. Normalizacja wojskowa na rynku europejskim – zamówienia obronne

Podstawą normalizacji wojskowe są polityczne ustalenia UE wskazujące konieczność zmian w europejskich strukturach obronnych (EUMS, EDA, ENISA[12]). Podstawą takiego działania są funkcjonujące od lat rozwiązania będące implementacją w sektorze obronności oraz porządku publicznego „dobrych praktyk UZE" (*best practices WEU*) zapisane w dokumentach III Filaru Traktatu WE (Maastricht 1997).

Podjęte zamierzenia to:
- elektroniczny system ofert w ramach Europejskiej Agencji Obrony jako propozycja dla średniej i małej przedsiębiorczości w poczynaniach obronnych Europy,
- możliwość udokumentowania w sporze prawnym lub procesie odszkodowawczym (na drodze niezależnej oceny), że wojskowy użytkownik zachował warunki korzystania z produktu/usługi wymagane/rekomendowane przez cywilnego dostawcę zgodnie z wymaganiami przywołanych norm, będące istotnymi elementami wprowadzanego przez EDA w UE jednolitego systemu logistycznego[13] zabezpieczeniu dostaw obronnych.

Podobne zjawisko rynkowe występowało już wcześniej w ramach działań NAMSA (Natowskiej Agencji Zaopatrzenia i Utrzymania Sprzętu)[14] i udziału w NSIP (wieloletnim programie podwyższenia obronności nowych członków sojuszu)[15] polskich przedsiębiorstw posiadających NCAGE (natowski numer referencyjny)[16] lub realizujących programy w dostawach uzbrojenia NATO. Jednak z racji wprowadzonych wcześniej ustaleń nie było w tym obszarze zdarzeń o charakterze konfliktów cywilnoprawnych na linii przedsiębiorca – agencja. Rozstrzygnięcia wprowadzające oferowane produkty lub usługi polskich przedsiębiorców na listy preferencyjne NATO były generalnie oparte na rezultatach przetargów realizowanych według zasad NATO lub na wynikach konkursów wewnętrznych NATO.

Działania podjęte przez Europejską Agencję Obrony to przede wszystkim próba zmniejszenia dystansu Europy wobec USA na drodze „efektywnej integracji" europejskich armii. Ścieżkę prowadzącą w tym kierunku wyznacza zastosowanie się państwa członkowskiego do Kodeksu Dobrych Praktyk oraz Kodeksu Postępowania (*Code of Conduct*) w zakresie Zamówień Obronnych EDA[17]. Patrząc przez pryzmat historycznych uwarunkowań techniki oraz technologii (stosowanie nowoczesnych rozwiązań głównie w sektorze wojskowym oraz przenoszenie ich „z poślizgiem"

12) *ENISA (European Network and Information Security Agency) – Europejska Agencja Bezpieczeństwa Sieciowego powołana przez Komisję Europejską UE Rozporządzeniem z dnia 19 listopada 2003 r., funkcjonująca od 1 stycznia 2004 r. (więcej informacji: www.enisa.eu.int lub www.mnii.gov.pl oraz www.cert.pl).*

13) *EBB EDA – dr Stavros Kyrimis, zastępca dyrektora Dyrektoriatu ds. Rynku i Przemysłu Obronnego EAO, materiały Seminarium SEA „Obronność w sieci", Warszawa 21.02.2006 r.*

14) *NAMSA – NATO Maintenance an Supply Agency (Natowska Agencja Zaopatrzenia i Utrzymania Sprzętu) - więcej informacji: http://www.namsa.nato.int lub www.dostawy.wp.mil.pl.*

15) *NSIP – NATO Security Investment Programme, wieloletni program podwyższenia obronności w sektorze nowych członków.*

16) *NCAGE – NATO Commercial and Government Entity Code, natowski numer referencyjny przypisany przedsiębiorstwu spełniającemu warunki Podmiotu Gospodarki Narodowej, w trybie obligatoryjnym lub fakultatywnym przez Narodowe Biuro Kodyfikacyjne państwa-członka NATO (43NCB Poland) - więcej informacji: www.wcnjk.wp.mil.pl/wcnjk_kod_ncage_warunki.*

17) *Konkurencja w zbrojeniówce, „Polska Zbrojna", 02.04.2006 r.*

do środowiska cywilnego), trzeba zdawać sobie sprawę z roli KE dążącej do aktywnego połączenia biznesowego środowisk wojskowych i cywilnych.

Charakterystycznym zjawiskiem jest szerokie wykorzystanie dla potrzeb wojska artykułów z rynku cywilnego (*towary z półki – COST*), a w zasadach ich użytkowania przywołuje się cały szereg wytycznych OECD[18]. Wytyczne te funkcjonują od lat w obszarach związanych z bezpieczeństwem informacji, bezpieczeństwem danych osobowych oraz kryptografią stosowaną dla potrzeb biznesu. Wskazują na zasadność oraz ważność działań podejmowanych dla ogólnoświatowego społeczeństwa informatycznego (OECD *Towards a Culture of Security* – W kierunku kultury bezpieczeństwa[19]).

Dokumenty OECD, łącznie ze wskazaniami EDA, wiążą się ściśle z już funkcjonującymi europejskimi strukturami ENISA, które znaczną część prowadzonych działań opierają na doświadczeniach cywilnych OECD (patrz: – CICCP)[20] oraz zaleceniach wojskowo-cywilnych agend NATO. Wypracowane dokumenty odnoszą się również w sposób bezpośredni do wzajemnej weryfikacji skutków działań. Można i należy je uznać za *standard faktyczny* w zakresie działań, których dotyczą.

Aktualną wykładnią wieloletniej współpracy wojskowo-obronnej UE – NATO są wdrożone do codziennej praktyki dokumenty:

– *European Handbook* (otwarta macierz tematyczna oraz powołane grupy eksperckie, odpowiednio EG1 – EG8)[21],
– *Initial Handbook* (dokumenty dot. obronności UE – ponad 130 000 pozycji) oraz prace powołanej struktury doradczo-technicznej BT/WS10[22].

Trzeba tu wspomnieć o coraz szerszym zjawisku „absorpcji" rozwiązań *stricte* militarnych do środowiska biznesowego z zachowaniem zmieniających się wciąż wymogów *e-commerce security*. Problem bezpieczeństwa biznesowego we współczesnym społeczeństwie dotyczy bowiem nie tylko samego kontraktu handlowego, ale wiąże się z ochroną fizyczną, techniczną oraz zachowaniem bezpieczeństwa informacyjnego jego uczestników.

Przywołując cywilną praktykę wzajemnego zaufania i kontroli opartej na normach oraz ich sprawdzaniu w drodze realizacji audytów „drugiej strony" w warunkach europejskich dostaw wojskowych (co samo w sobie stanowi w Polsce novum), trzeba wskazać, że wiąże się ona ze ścisłym spełnieniem warunków opisanych i przyjętych we wspomnianych wcześniej dokumentach EDA: Kodeksie Dobrych Praktyk oraz Kodeksie Postępowania w zakresie Zamówień Obronnych.

Różnicowanie jest istotne, ponieważ NATO, działając w ramach STANAG 4107, czyli rządowego programu zapewnienia jakości, funkcjonuje wyłącznie u dostawcy (poprzez nadzór inspektorów QAR). Natomiast EDA, rozwijając idee i intencje KE, dąży do szerokiej formuły stosowania audytu jako oceny zdolności procesowych dla przyjętych zobowiązań oraz ich realizacji zarówno u wytwórcy – przedsiębiorstwa, jak i u odbiorcy – jednostki wojskowej.

4. Podsumowanie

Przedstawione powyżej fakty historyczne oraz sygnalizowane obecnie kierunki działań KE wskazują na coraz szerszą współpracę sektora obronnego z firmami cywilnymi – współpracę bazującą nie tylko na kontraktach, ale również na niezależnych audytach zewnętrznych dotyczących jakości zarządzania i bezpieczeństwa. Analizując szczegółowo zmiany w zakresie przyjętej Dyrektywy Nowego Podejścia we Wspólnotach Europejskich oraz przenoszenie ich na elementy struktur wojskowych (UZE – NATO – EUMS – EDA), można z całą odpowiedzialnością stwierdzić, że innowacyjna rola norm propagowana w ostatnich latach przez Komisję Europejską istnieje w strukturach wojskowych NATO (MAC/NSA) od ponad dziesięciu lat w postaci przyjętych do praktyki rozwiązań stowarzyszeniowych oraz porozumień i publikacji sprzymierzonych. Omówienie przenikania tych idei i ich skutków biznesowych będzie tematem kolejnych artykułów tego cyklu.

Opracował: dr inż. Marek Blim

Bibliografia:

1) Komunikat KE UE *Ku zwiększeniu wkładu normalizacji w innowacje w Europie*, COM(2008)133 (*www.euro-lex/service/*).
2) Komunikat KE UE *Europejskie zadanie: osiągnąć sukces w epoce globalizacji*, COM(2007)581 (*www.euro-lex/service/*).
3) Kozaczuk Wł., *W kręgu Enigmy*, Książka i Wiedza, Warszawa 1979.
4) Materiały archiwalne miesięcznika PKN „Normalizacja" za lata 2004–2009
5) Materiały autora (z prac realizowanych na rzecz WKN, BWSN MON, WCNJiK MON)
6) Materiały informacyjne OECD (*www.oecd.pologne.net*).
7) Materiały informacyjne NC3A (*www.nc3a.nato.int*).
8) *Polska normalizacja – jaka jest?*, PKN, Warszawa 2009.
9) Weidenfeld W., Wessels W., *Europa od A do Z. Podręcznik integracji europejskiej,* wyd. IV, Wydawnictwo „Wokół nas", Gliwice 2004.

18) *OECD (Organisation for Economic Co-operation and Deveploment) – Organizacja Współpracy Gospodarczej i Rozwoju powołana na mocy Konwencji Paryskiej z 14 grudnia 1960 r. Polska jest jej członkiem od 11 lipca 1996 r. (Dz. U. z 1998 r. nr 76, poz. 490) - więcej informacji: www.oecd.org lub www.oecd.pologne.net.*

19) *Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych – Zalecenie Rady OECD z 1037 sesji z 25 lipca 2002 r.; za: „Przegląd OECD" 2003 (wersja polska).*

20) *OECD Committee for Information, Computer and Communications Policy – Komisja ds. Polityki Informatycznej, Komputerowej i Komunikacyjnej OECD. - więcej informacji: www.oecd.org lub www.oecd.pologne.net.*

21) *J. Krawiec, Europejska inicjatywa w zakresie normalizacji obronnej – EUROPEAN HANDBOOK, „Normalizacja" (miesięcznik PKN) nr 6/2005 s. 3.*

22) *Cz. Dziedzic, Rola i zadania normalizacji w zakresie obronności i bezpieczeństwa państwa, materiały seminarium PKN i Instytutu Lotnictwa, „Normalizacja" (miesięcznik PKN) nr 3/2005 s. 25.*

UTC Fire & Security

Nowa Platforma
Advisor Advanced

Prosty wybór bogatych możliwości!

- Różne tryby zazbrajania i rozbrajania przy pomocy karty i/lub kodu PIN
- Zazbrajanie po 3-krotnym użyciu karty
- Parametryzowane linie dozorowe do obsługi czujek z układem wykrywania maskowania (Anti-masking) i czujek inercyjnych
- Podział na niezależne obszary (4/8) z możliwością stosowania zazbrajania częściowego w każdym z nich.
- Bogaty wybór interfejsów komunikacyjnych i możliwość sterowania oraz raportowania przez komunikaty SMS
- Dostępne wersje z interfejsem IP (Ethernet) na płycie
- Szeroki wybór czujek przewodowych i bezprzewodowych oraz innych urządzeń peryferyjnych

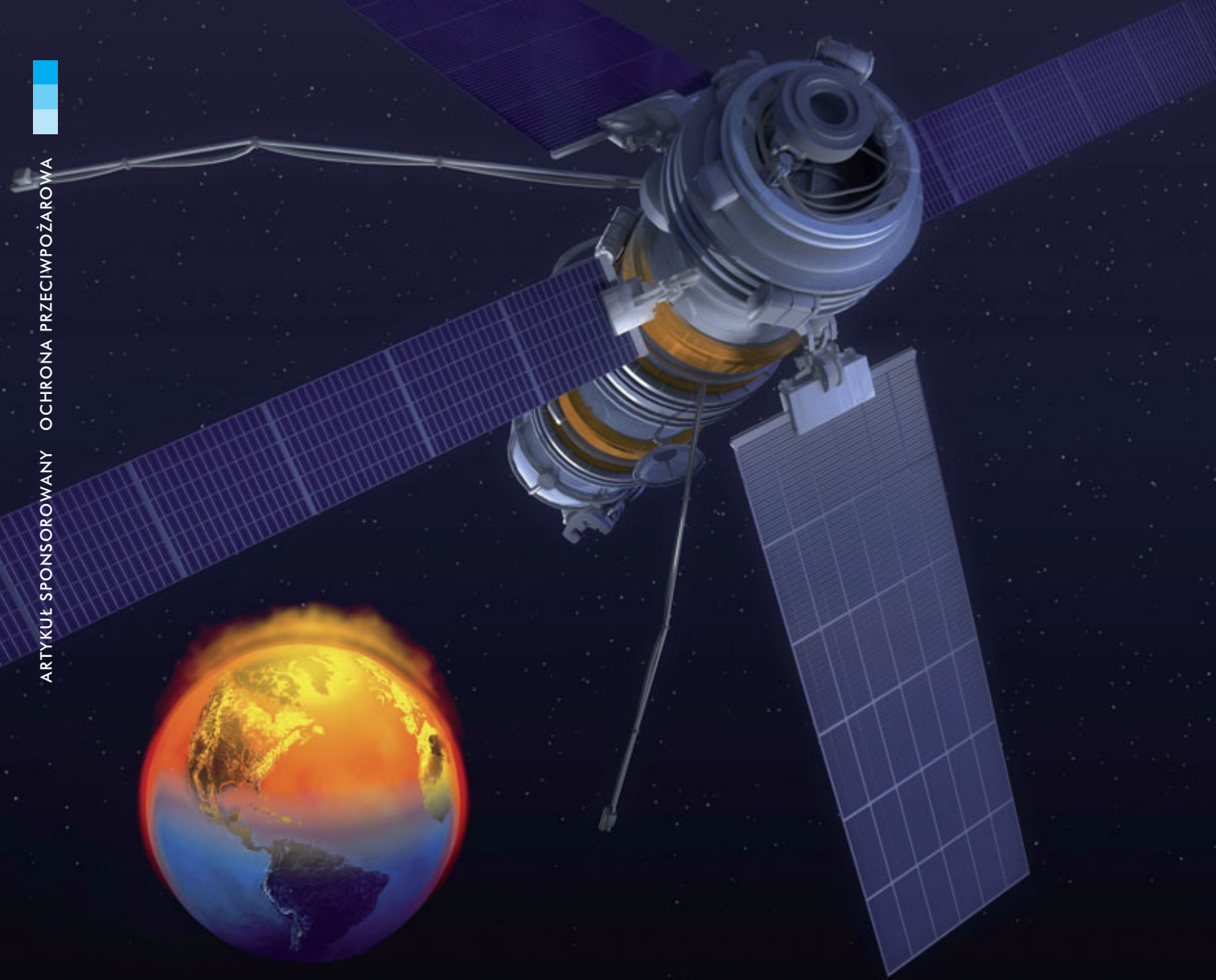
SPEŁNIA WYMAGANIA NORMY EN50131: 2009

UTC Fire & Security
A United Technologies Company

Centrala UTC Fire & Security Polska Sp. z o.o.
ul. Sadowa 8
80-771 GDAŃSK
tel.: (58) 301 38 31, (58) 760 64 80
fax: (58) 301 14 36

Oddział w Warszawie
Al. Stanów Zjednoczonych 59
04-028 WARSZAWA
tel.: (22) 810 00 03
fax: (22) 810 10 55

Oddział w Poznaniu
Oś. Na Murawie 11/2
61-655 POZNAŃ
tel.: (61) 821 35 66
tel./fax: (61) 821 31 94



Historia z przyszłością

Opowiadanie nie-*science-fiction*

Grzegorz Ćwiek

Jest rok 2211. Zebranie sił prewencyjnych międzygalaktycznej straży pożarnej na 12. planecie układu Małego Mesha w gwiazdozbiorze S-1. Sala spotkań w kwaterze BMZ-6. Szósty poziom platformy A.

– Udzielam panu głosu, kapitanie.
– A zatem coś przeczytam.
– Dobrze, słuchamy. Oby to miało sens…
– Proszę wysłuchać cierpliwie fragmentów, które przygotowałem:

W ciągu ostatnich czterech lat system sygnalizacji pożarowej **Integral** przeszedł gruntowną modernizację. W dostępnych dzisiaj na rynku systemach **Integral IP** zastosowaliśmy całkowicie nowe rozwiązania w zakresie przesyłu danych i zarządzania komunikacją – zarówno wewnętrzną w systemie, jak i z użytkownikami. Od początku procesu tworzenia nowego systemu było dla nas jasne, że musimy spełnić dwa, w zasadzie sprzeczne, wymogi rynku. Pierwszy dotyczył obiektów wysokich i wysokościowych oraz rozproszonych i tych o dużej kubaturze – obiektów biurowych, handlowych, stadionów, hal sportowych i lotnisk. Musiał powstać system, który mógłby w łatwy sposób – i to bez wsparcia dodatkowych systemów zewnętrznych – przetworzyć przeogromną liczbę zarówno informacji z zakresu wykrywania pożaru, jak i sygnałów sterująco-monitorujących. Drugi wymóg – w teorii sprzeczny z pierwszym, według założeń nie tylko inżynierów ze Schrack Seconet, ale wszystkich w branży – mówił o tym, by system nie był drogi. Dokonaliśmy jednak cudu...

– STOP! Miał pan, kapitanie, zabrać głos w ważnej sprawie, a tymczasem czyta nam pan jakieś marketingowe opowiastki z dalekiej przeszłości.

– Panie generale! Nad rozwiązaniem naszego problemu myślałem przez ostatnie pięć lunarmiesięcy. Tunele teleportacyjne między naszą planetą a planetami numer 11, M113, C Alfa 8 i prowadzącą do naszej galaktyki gwiazdostradą Tera-Gral-62 są zablokowane każdego dnia o określonych godzinach oraz w czasie anomalii magnetycznych związanych z oddziaływaniem śmieci kosmicznych emitowanych z komety Novarion-G0, czy tak?

– Zgadza się.

– Utrudnia nam to nie tylko normalną pracę, a więc przesyłanie informacji za pomocą naszych łączy komunikacyjnych, ale także zakłóca dostawy żywności, środków gaśniczych, narzędzi, w ogóle wszystkiego, prawda?

– Niestety tak. Myśleliśmy, że nasze najnowsze roboty gaśnicze SUG-REX 10 i SUG-REX 21, wykorzystujące napęd plazmotronowo-refrakcyjny, poradzą sobie z tym problemem, ale i one nie mogą się przebić. Może udałaby im się ta sztuka, gdyby nie były tak duże i tak wolne. Pan wie, kapitanie, ile kosztuje nas strata cennego czasu, zniszczenia i straty w sprzęcie, a przede wszystkim – brak możliwości poprowadzenia akcji ratowniczej dokładnie wtedy, kiedy jest potrzebna? Każde pięć lunarminut opóźnienia w dostarczeniu pakietu danych lub robota gaśniczo-ewakuacyjnego może zagrozić życiu całej planety, nie tylko załogi pojedynczego obiektu latającego czy podstacji teleportacyjnej… Sytuacja robi się niecieka-wa. Galaktyczni inspektorzy nadzoru nie szczędzą nam przykrości, nie mówiąc już o Międzyplanetarnej Unii Bezpieczeństwa Pożarowego ITBCNBOPVDSNFPAB-SIiTD…

– Wiem, panie generale. Szczególnie ci z Unii są nieugięci… ale jestem pewien, że mam rozwiązanie!

– Od lat nikt nie wie, co z tym zrobić. Lepiej, żebyśmy nie tracili więcej czasu, kapitanie. Jeżeli ma pan jakieś rozwiązanie, zamieniamy się w słuch – tylko niech pan już nie cytuje tych marketingowych opowiastek z XXI wieku, do rzeczy!

– Panie generale: jako dziecko uwielbiałem lekcje historii. Jak pan wie, mój pradziadek był wykładowcą na jednej z najlepszych akademii ochrony przeciwpożarowej, jaka powstała na Marsie po migracji ludności z naszej praplanety Ziemi w roku 2112. Jak pan pamięta, stało się to dokładnie sto lat po ostatnim wielkim wydarzeniu sportowym w historii naszej ziemskiej ojczyzny – Polski. Pan też jest kibicem starballu i na pewno pamięta pan, co wydarzyło się wtedy w naszym prakraju?

– A kto z nas mógłby tego nie pamiętać? Polacy zdobyli wtedy mistrzostwo Europy w piłce nożnej po raz pierwszy w historii – i niestety ostatni. Zaraz potem, aaa… szkoda gadać. Ale nie zabrał pan przecież głosu tylko po to, żeby porozmawiać o wydarzeniach, o których przeczytał pan w starych książkach historycznych? Do rzeczy!

– Nnnie... oczywiście, że nie. To znaczy... tak. To znaczy nie… yyy...

– Niechże pan wreszcie powie, o co chodzi, kapitanie!

– Otóż chodzi o to, że dokładnie dwieście lat temu, w roku 2011 – czyli na rok przed tym sportowym wydarzeniem, które tak dobrze pamiętamy z lekcji historii, miało miejsce inne, bardzo dla nas dzisiaj istotne. Otóż pradziadek mojego pradziadka, który wykładał na Marsie, a o którym wspomniałem wcześniej, prowadził w owym czasie wykłady na jednej z ziemskich akademii, właśnie w Polsce. Z materiałów, do których dotarłem, wynika, że były to wykłady z nowej – jak na owe czasy – technologii związanej z wykrywaniem pożaru i układami sterowania elementami mechanicznymi. W początkach XXI wieku rozwiązania, które prezentował, były niezwykle zaawansowane. Oni nie mieli tam ani robotów gaśniczych, ani droidów ewakuacyjnych, ani nawet molekularnych transponderów antymaterii! Urządzenia, którymi dysponowali, były jednak na tyle dobre, że podczas owych mistrzostw zostały użyte na prawie wszystkich stadionach piłkarskich w naszym prakraju, a do tego w setkach innych obiektów różnego przeznaczenia. Do tego…

– Dość! Działa mi już pan na nerwy, i wszystkim tu zebranym chyba także. Jest pan młodym człowiekiem i jeszcze nie nazbyt doświadczonym. Naszą zasadą jest mówienie o konkretach. My nie mamy wolnych całych lunarcykli czasu, ani nawet lunarsekund. Jeżeli pan pozwoli, przerwiemy teraz pański historyczny wywód i zostawimy go sobie na wspominkowy wieczór gdzieś około świąt Bożego Narodzenia. To jeden z tych wieczorów, który nam został z całej tradycji naszego prakraju i praplanety, która… eeech, dość. Po prostu dość. Jeżeli nie znajdziemy natychmiast jakiegoś nowego sposobu komunikacji z naszymi odległymi bazami, to wydarzy się coś złego. Pogadankę o starodawnych detektorach dymu, które dziś zostały zastąpione przez molekularne transpondery antymaterii, musimy definitywnie odłożyć. Dzisiaj moc pożarów bywa tysiąckrotnie większa niż kiedyś na Ziemi, a eksperymenty z gaszeniem gazami

obojętnymi są dobre na lekcje zajęć praktyczno-technicznych, które prowadzi się dla młodych humanodroidów w przedszkolu…

– Panie generale proszę... Proszę jeszcze o minutę uwagi. Jeżeli to, co teraz powiem, nie będzie dość konkretne – przerwie mi pan, a ja do końca zebrania nie odezwę się ani słowem. Nie jestem zbyt dobrym mówcą, więc przeczytam coś, co wygrzebałem z archiwów pradziadka. O komentarz poproszę także panów zebranych w sali.

– Ma pan ostatnią szansę. Włączam detry… yyy… jak to się kiedyś mówiło? Ach, no tak, stoper! Włączam stoper…

– Dziękuję za szansę. Tekstu jest dużo, toteż przeczytam tylko część. Proszę mi wybaczyć, jeżeli tekst nie będzie zbyt spójny, ale wybrałem tylko fragmenty z całości. Mimo wszystko będę kontynuował od momentu, w którym przerwałem. To wypowiedź jednego z przedstawicieli firmy, która wymyśliła ten system:

Pomysł, choć trudny w realizacji, okazał się znakomity. Polega na tym, że zaprojektowaliśmy system, w którym zastosowaliśmy zwielokrotnione połączenia pomiędzy poszczególnymi węzłami sieci oraz istotnie zwiększyliśmy liczbę torów komunikacyjnych wewnątrz samych central SAP. Dzięki zastosowaniu **sieci kratowych** rozkazy i dane przesyłane dotychczas pojedynczymi kanałami transmisji (w zdublowanych pierścieniach podcentral[1]) mogą być od tej pory przesyłane różnymi obwodami w tym samym czasie. Po dotarciu na miejsce docelowe pakiety danych podróżujące różnymi torami są dzięki inteligencji systemu składane znowu w ciągi logiczne, a następnie wykorzystywane we właściwy sposób przy znacznie krótszym czasie dostępu. Nie dość, że zwiększono w ten sposób przepustowość kanałów komunikacyjnych, to jeszcze zagwarantowano znacznie większe bezpieczeństwo i stabilność pracy samego systemu. Nawet siedem uszkodzeń w połączeniach (zablokowanie lub zerwanie kanałów transmisji) nie spowoduje utraty komunikacji między centralami. Dane zawsze znajdą drogę, którą będą mogły się przedostać do celu. W pogotowiu bowiem znajduje się zapasowe oprogramowanie, gotowe do zastąpienia tego podstawowego w całości lub części – w każdym przypadku stwierdzenia przez układ autokontroli jakiejkolwiek nieprawidłowości w jego działaniu. Na przykład może się to zdarzyć w razie potężnego zakłócenia elektromagnetycznego w obiekcie przemysłowym, wojskowym, czy nawet szpitalnym.

Integral LAN jest...

– Ciekawe…

– Proszę? Czy mam czytać dalej, panie generale?

– Jak się nazywał ten produkt? Integral IP?

– Tak. Wprowadziła go na rynek austriacka firma Schrack Seconet w 2011 roku. Oni wcześniej...

– Wiem. Nieważne. Nie mamy czasu na rozmowy o firmach. Unia Międzygalaktyczna zniosła nazwy firm i krajów. Dzisiaj jest tylko jedno przedsiębiorstwo, które produkuje sprzęt przeciwpożarowy i nie ma żadnej nazwy. Wszystkie inne upadły albo zostały przez nie wchłonięte. Niech pan czyta dalej.

– Tak jest.

W najnowszym **Integralu IP** istnieje całkowita dowolność wyboru topologii sieci systemu. O ile w detekcji stosuje się nadal pętle dozorowe do nadzoru i wykrywania zagrożeń, to różnica pomiędzy nowym a starym Integralem jest taka, że w nowym dzięki technice **X-LINE** można zamiast 128 elementów pętlowych zastosować ich aż 250, a zamiast pętli o długości 2000 metrów możemy zastosować pętle do 3500 metrów. Wszystkie elementy peryferyjne zostały wzbogacone o nowe funkcje. Podstawowy element detekcyjny – wielosensorowa czujka interaktywna **Cubus MTD 533X (TF1 – TF9)** – podobnie jak inne elementy z indeksem **X** pobiera dzisiaj znacznie mniej prądu, dzięki czemu cały system jest bardziej przyjazny środowisku.

– Dalej! Niech pan czyta dalej o tej komunikacji. My tu nie budujemy pętli dozorowych, tylko mamy problem z prędkością transmisji i pozatykanymi kanałami przesyłowymi.

– Tak, wiem. Ale ten opis nowych funkcji systemów Schrack Seconet z 2011 roku jest tak obszerny, że żal pominąć niektóre kwestie. O! Jest następne zaznaczenie:

W technologii **Integral LAN** mamy do dyspozycji różne media komunikacji sieciowej: RS485 (*high speed*), modemy światłowodowe, DSL. W przypadku transmisji danych przez Ethernet możemy osiągnąć prędkość do 100 Mb/s. Dzięki temu możliwe jest zdalne nadzorowanie pracy systemu on-line lub aktualizacja oprogramowania całego systemu sieciowego z dowolnego miejsca na świecie, i to „w locie" – bez konieczności zatrzymania systemu!

– A, cha, cha, cha, cha! Z dowolnego miejsca na świecie… a to dobre! Nie dziwię się, że z taką prędkością transmisji, jaką mieli, nie potrafili polecieć na Marsa! Ziemia była ich całym światem, nie to, co dzisiaj. Ale fakt: pamiętam z historii. 100 Mb/s? W tamtych czasach to szok! Żaden inny producent systemu przeciwpożarowego nie dawał takich możliwości. Ale nie to mnie zaciekawiło. Chyba wiem, co pan odnalazł w tych lekcjach historii sprzed 200 lat... Niech pan czyta dalej.

Dalsze odcinki opowiadania z przyszłości – o **Integralu IP** i losach międzygalaktycznej straży pożarnej – znajdą Państwo w następnych numerach *Zabezpieczeń*.

Grzegorz Ćwiek
Schrack Seconet Polska

1) Zdublowane pierścienie połączeń między centralami to stosowana dotychczas przez Schrack Seconet technika łączenia central (systemów) w sieć. Do momentu wprowadzenia sieci kratowych była to najbezpieczniejsza, redundantna topologia sieciowa stosowana w systemach sygnalizacji pożarowej. Aby uzyskać więcej informacji, najlepiej kontaktować się z biurami lub autoryzowanymi partnerami Schrack Seconet w Polsce.

Kup produkt zewnętrznej ochrony RISCO i WYGRAJ Niezapomnianą Przygodę

RISCO
riscogroup.com

Outdoor Adventure

Zapewnij swoim klientom najlepszą ochronę przed włamaniem…
a sobie możliwość przeżycia wspaniałej przygody!

Produkty biorące udział w kampanii Niezapomniana Przygoda:

Bariery Podczerwieni

przewodowe i bezprzewodowe aktywne bariery podczerwieni RISCO to zaawansowane rozwiązanie dla zewnętrznej ochrony obwodowej w budynkach mieszkalnych oraz komercyjnych.

WatchOUT™

Wyposażona w unikalne technologie detekcji, wielokrotnie nagradzana linia produktów WatchOUT zapewnia niezawodne wykrycie intruza w środowisku zewnętrznym.

Dwuwiązkowe bariery podczerwieni

zapewniają niezawodne i ekonomiczne zabezpieczenie z równoczesną odpornością na występowanie fałszywych alarmów

*Opakowania produktów konkursowych posiadają naklejkę "Outdoor Adventure"

www.adventure.riscogroup.com

RISCO GROUP

Creating Security Solutions. *With Care.*

riscogroup.com

Instalacje wykrywania pożaru w przestrzeniach zagrożonych wybuchem (część 2)

Władysław Markowski

W pierwszej części artykułu (*Zabezpieczenia* nr 1/2011) przedstawiono charakterystykę i podział stref zagrożonych wybuchem oraz rodzaje obudów urządzeń mogących pracować w poszczególnych strefach. W niniejszej części artykułu omówione zostaną zasady doboru urządzeń i projektowania instalacji sygnalizacji pożarowej w przestrzeniach zagrożonych wybuchem

Dobór urządzeń Ex

Zadaniem projektanta instalacji sygnalizacji pożarowej (ISP) jest właściwy dobór urządzeń do sklasyfikowanej strefy zagrożonej wybuchem. Od tego zależy bezpieczna praca urządzeń w wykonaniu przeciwwybuchowym.

Lokalizacji i klasyfikacji stref zagrożonych wybuchem dokonuje (i przedstawia na piśmie) inwestor w porozumieniu z projektantem procesu technologicznego lub użytkownikiem. Informacja ta jest podstawą prac projektanta ISP.

Projektant ISP w oparciu o otrzymane dane, a także rozeznanie co do potencjalnych źródeł pożaru określa, jakiego rodzaju czujki pożarowe (dymu, ciepła, płomienia) należy zastosować. Poszukuje więc określonego rodzaju czujek wśród mających certyfikaty badania typu WE, mogących pracować w danej strefie.

Projektant ISP powinien też brać pod uwagę warunki środowiskowe w zagrożonej wybuchem strefie, które mogą wpływać na czujkę: temperaturę otoczenia, wilgotność, korozję, promieniowanie UV, osiadanie pyłu, oddziaływanie chemiczne.

Dobór urządzeń odpowiedniej kategorii i podgrupy w zależności od sklasyfikowanej strefy i grupy wybuchowości atmosfery przedstawiają tab. 1 i 2.

Klasę temperaturową urządzenia należy dobrać tak, aby maksymalna dopuszczalna temperatura powierzchni lub jakiejkolwiek części urządzenia (element oznakowania na poz. 8 wg tabeli 3[1]) była co najwyżej równa temperaturze samozapłonu substancji palnej.

1) Część I art. w czasopiśmie Zabezpieczenia Nr 1/2011).

W poradniku [11] można znaleźć wykaz 270 substancji i ich parametrów fizykochemicznych mających wpływ na powstanie zagrożenia wybuchowego oraz na dobór instalacji i urządzeń elektrycznych.

Instalacje wykrywania pożaru są najczęściej projektowane dla stref 2 i obszarów przyległych. Rzadko montuje się je w strefach 1, a jeszcze rzadziej w strefach pyłowych. W strefach 0 zwykle nie występują.

Urządzenia Ex stosowane w sygnalizacji pożarowej

Do wykrywania pożaru w strefach i pomieszczeniach zagrożonych wybuchem stosowane są:

– czujki pożarowe, głównie dymu i płomienia,
– ręczne ostrzegacze pożarowe,
– sygnalizatory alarmowe.

Jeżeli są to urządzenia w wykonaniu iskrobezpiecznym i, to do połączenia ich z centralą sygnalizacji pożarowej, instalowanej zwykle w strefie bezpiecznej, niezbędne są:

– bariery iskrobezpieczne,
– lub separatory iskrobezpieczne.

Ograniczają one energię (prąd i napięcie) w obwodzie iskrobezpiecznym do wartości bezpiecznych, tj. takich, przy których ewentualny łuk elektryczny nie jest w stanie spowodować zapłonu atmosfery wybuchowej.

Bariery to proste elementy bierne, w których wyjściowe obwody iskrobezpieczne są chronione przez diody Zenera, rezystory i bezpieczniki.

Zalety barier:

– stanowią stosunkowo tanie rozwiązanie,
– mają małe wymiary,

Klasyfikacja strefy	Odpowiadająca kategoria urządzenia	Kategorie urządzenia możliwe do zastosowania
Strefa 0 lub strefa 20 (pył) (najbliżej źródła emisji)	Kategoria 1 (bardzo wysoki poziom zabezpieczenia)	–
Strefa 1 lub strefa 21 (pył) lub strefa 22 (pył przewodzący) (pomiędzy strefą najbliższą i najdalszą)	Kategoria 2 (wysoki poziom zabezpieczenia)	Kategoria 1
Strefa 2 lub strefa 22 (pył nieprzewodzący) (najdalej od źródła emisji)	Kategoria 3 (normalny stopień zabezpieczenia)	Kategoria 1 Kategoria 2
Pozycja elementu oznakowania urządzenia wg tab. 3.[2]	Poz. 3	Poz. 3

Tab. 1. Dobór urządzeń odpowiedniej kategorii w zależności od sklasyfikowanej strefy wybuchowości atmosfery

2) Część I art. w czasopiśmie Zabezpieczenia Nr 1/2011).

Grupa wybuchowości atmosfery	Odpowiadająca podgrupa urządzenia	Podgrupa urządzenia możliwego do zastosowania
IIA	IIA (normalny poziom zabezpieczenia)	IIB, IIC
IIB	IIB (wysoki poziom zabezpieczenia)	IIC
IIC	IIC (bardzo wysoki poziom zabezpieczenia)	–
Pozycja elementu oznakowania urządzenia wg tab. 3.[3]	Poz. 7	Poz. 7

Tab. 2. Dobór urządzeń odpowiedniej podgrupy w zależności od sklasyfikowanej grupy wybuchowości atmosfery

3) Część I art. w czasopiśmie Zabezpieczenia Nr 1/2011).

– są proste w montażu,
– nie wymagają zasilania.

Wady barier:
– wymagają uziemienia – bezpieczeństwo jest uzależnione od jego jakości i poprawności,
– są bardzo wrażliwe na błędy montażu,
– trudno jest dobrać odpowiedni typ bariery,
– nie posiadają izolacji galwanicznej między obwodami wejściowym i wyjściowym.

Uziemienie bariery powinno być wykonane w ten sposób, aby rezystancja połączenia pomiędzy barierą a uziemieniem głównym była mniejsza niż 1 Ω.

Separatory są elementami aktywnymi, w których obwody iskrobezpieczne uzyskuje się poprzez:
– oddzielenie obwodu wejściowego za pomocą transformatora separującego,
– zastosowanie ogranicznika prądu (rezystory) oraz ogranicznika napięcia (diody Zenera).

Zalety separatorów:
– izolacja galwaniczna między wejściem, wyjściem i zasilaniem,
– brak konieczności uziemienia,
– łatwość doboru izolatora,
– odporność na interferencje,
– prosty montaż.

Wady separatorów:
– wyższy koszt niż w przypadku barier,
– większe wymiary (w porównaniu z barierami),
– niekiedy konieczne zewnętrzne zasilanie.

Zarówno bariery, jak izolatory powinny być instalowane w obszarze bezpiecznym i w obudowach zapewniających odpowiedni stopień ochrony IP.

Urządzenia o budowie iskrobezpiecznej **ia** lub **ib** są zwykle instalowane wewnątrz pomieszczeń zagrożonych wybuchem: w strefach niebezpiecznych na wolnym powietrzu przeważnie są instalowane urządzenia w obudowie ognioszczelnej **d**.

Okablowanie instalacji w przestrzeniach zagrożonych wybuchem

W instalacjach sygnalizacji pożarowej, stosowanych w przestrzeniach zagrożonych wybuchem, „spotykają" się obwody zwykłe, instalowane w części bezpiecznej obiektu, oraz obwody pracujące w strefach 1 lub 2 (zagrożonych wybuchem). Dlatego oprócz wymagań podstawowych, stawianych obwodom „normalnym", należy uwzględnić wymagania dodatkowe, zapewniające pożądany poziom bezpieczeństwa instalacji w strefie zagrożonej wybuchem.

Kable urządzeń „i" w strefach 1 i 2

W instalacjach z obwodami iskrobezpiecznymi dla stref 1 i 2 urządzenia iskrobezpieczne i towarzyszące im dodatkowe urządzenia zawierające elementy iskrobezpieczne powinny należeć przynajmniej do kategorii bezpieczeństwa **ib**.

Urządzenia towarzyszące, zawierające elementy (głównie wyjścia) iskrobezpieczne, powinny być zainstalowane poza strefą zagrożoną wybuchem.

Elementy oraz okablowanie urządzeń iskrobezpiecznych i urządzeń towarzyszących (np. barier iskrobezpiecznych) powinny być umieszczone w obudowie zapewniającej ochronę przynajmniej na poziomie IP20.

Przewody w iskrobezpiecznej części instalacji powinny być prowadzone tak, aby nie były narażone na działanie zewnętrznych pól elektrycznych lub elektromagnetycznych (np. wytwarzanych przez przebiegające w pobliżu przewody wysokiego napięcia). Można to osiągnąć przez używanie kabla ekranowanego i (lub) skręcanego bądź poprzez zapewnienie odpowiedniego odstępu od źródeł pola elektrycznego lub elektromagnetycznego.

Dodatkowo kable (zarówno w części iskrobezpiecznej, jak i nieiskrobezpiecznej) powinny spełniać jedno z następujących wymagań:
– obwody iskrobezpieczne powinny być oddzielone od nieiskrobezpiecznych,
– obwody iskrobezpieczne powinny być zainstalowane tak, aby nie były narażone na uszkodzenia mechaniczne,
– obwody iskrobezpieczne i nieiskrobezpieczne powinny być ekranowane, w pancerzu lub w osłonie metalowej.

Obwody iskrobezpieczne i nieiskrobezpieczne nie mogą być prowadzone w jednym kablu. Dodatkowo kable z obwodami iskrobezpiecznymi i nieiskrobezpiecznymi nie powinny być prowadzone w tej samej wiązce lub rurce, chyba że są

Fot. 1. Przykłady czujek w wykonaniu iskrobezpiecznym
Czujka pożarowa PUO-35Ex firmy POLON-ALFA Ex II 2G Ex Ib IIC T6
Czujka pożarowa DUR-40Ex firmy POLON-ALFA Ex II 2G Ex Ib IIC T6

oddzielone przegrodą z materiału izolacyjnego lub uziemioną przegrodą metalową.

Jeżeli obwód iskrobezpieczny izolowany od ziemi (ze względu na zastosowany separator) jest prowadzony w kablu ekranowanym, ekran powinien być podłączony do ekwipotencjalnego systemu uziemiającego w jednym punkcie. Uziemienie należy wyprowadzić z obudowy, w której znajduje się separator. Część linii dozorowej normalnej (sprzed separatora) należy uziemić przy centrali.

Kable pozostałych urządzeń Ex

Połączenia kablowe w strefach Ex powinny być realizowane poprzez dodatkowe elementy połączeniowe (wpusty), przystosowane do danego kabla. Powinny one zapewnić bezpieczeństwo obudowy na poziomie **e**, dla osiągnięcia odpowiedniego stopnia ochrony tej obudowy (IP minimum 54). Może być również potrzebne użycie dodatkowych elementów uszczelniających (np. dławików) w miejscach wprowadzenia kabli do urządzeń Ex.

Wszędzie tam, gdzie jest to konieczne, należy stosować zabezpieczenia przewodów przed uszkodzeniami mechanicznymi, oddziaływaniem niekorzystnych temperatur, korozją czy też środkami chemicznymi. W sytuacji kiedy nie da się zastosować odpowiedniej osłony mechanicznej, należy poprowadzić okablowanie w rurkach albo zastosować kabel zbrojony, ekranowany, izolowany przy użyciu aluminium bez szwu, izolowany izolacjami mineralnymi lub półsztywnymi osłonami.

Tam, gdzie występują wibracje, należy użyć kabla, który jest na nie wytrzymały i w dłuższym czasie nie ulegnie uszkodzeniu.

W instalacjach należy stosować tylko izolowane kable miedziane, w których napięcie testowe (którym badane są przewody) uziemienia, ekranu wynosi przynajmniej 500 V_{AC} lub 750 V_{DC}.

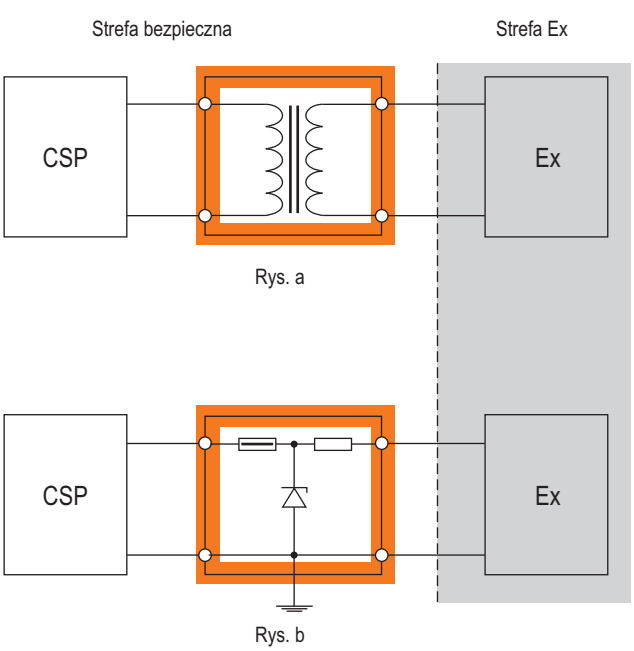
Parametry elektryczne kabli (*pojemność i indukcyjność* lub *pojemność i współczynnik indukcyjność/rezystancja*) powinny być wyznaczane według jednego z poniższych warunków:

a) najbardziej obciążonego parametru elektrycznego podawanego przez wytwórcę kabla,
b) parametru elektrycznego wyznaczonego podczas badania próbki kabla,
c) pojemności kabla 200 pF/m i: 1 μH/m lub 30 μH/Ω, kiedy połączenie obejmuje dwie lub trzy żyły zwykłego kabla (z ekranem lub bez).

Jeżeli w instalacji używa się przewodów ekranowanych, ekran należy uziemić w jednym punkcie (w przypadku przestrzeni bezpiecznej linię dozorową przy centrali).

Jeżeli obwód iskrobezpieczny izolowany od ziemi jest prowadzony w ekranowanym kablu, ekran powinien być podłączony do ekwipotencjalnego systemu uziemiającego w jednym punkcie.

mgr inż. Władysław Markowski
POLON-ALFA ZUD



Rys. 1 Poglądowy schemat separatora a) i bariery b) iskrobezpiecznej

Literatura

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

Urządzenia mobilne – znajdujące się w nich cenne dane też możesz stracić

Paweł Odor

Niemal każdy z nas ma na co dzień przy sobie telefon komórkowy, przenośną pamięć czy aparat cyfrowy, które wykorzystywane są w pracy bądź na wakacjach. Coraz więcej osób używa także popularnych smartfonów, których sprzedaż w Polsce z roku na rok systematycznie rośnie. Choć pod względem ochrony danych nie traktujemy tych urządzeń tak poważnie jak komputery, musimy pamiętać, że niekiedy są to nośniki danych równie ważne jak dyski naszych pecetów. W takim samym stopniu – a nawet większym z powodu mobilności tych urządzeń – możemy tracić z nich ważne cyfrowe pliki. Właśnie wtedy trafiają one do specjalistycznych laboratoriów, które odzyskują dane nawet ze spalonych lub niemal całkowicie zalanych urządzeń przenośnych. Jak wygląda proces odzyskiwania danych z naszych przenośnych maszyn i których dotyczy w szczególności?

Jak wynika ze statystyk polskiego oddziału Kroll Ontrack, największej na świecie firmy zajmującej się odzyskiwaniem danych oraz informatyką śledczą, ok. 5% wszystkich przypadków utraty danych jest związane z urządzeniami mobilnymi. Wśród nich przodują pamięci flash, które montowane są w telefonach komórkowych (również w smartfonach), pendrive'ach czy aparatach fotograficznych. W większości przypadków zapisane na nich dane są tracone nie tylko w wyniku przypadkowego skasowania (np. sformatowania karty), lecz także w przypadku zalania, spalenia czy uszkodzenia karty w wyniku zbyt wysokiej lub zbyt niskiej temperatury. Mimo tak ekstremalnych warunków utraty informacji większość z tych problemów można rozwiązać. Zajmują się tym specjaliści od odzyskiwania danych, zarówno pracujący za granicą, jak i w Polsce. Co jednak istotne, tylko największe firmy zajmujące się odzyskiwaniem danych stworzyły tak zaawansowane technologie, że są w stanie odzyskać dane zapisane w urządzeniach mobilnych. Jak więc wygląda proces odzyskiwania danych z tych urządzeń w profesjonalnym laboratorium największej na świecie firmy zajmującej się przywracaniem utraconych plików do życia?

Pamięci flash

Małe, wygodne w użyciu i coraz tańsze – to niepodważalne zalety bardzo popularnych już pamięci flash. Na wykorzystujących powyższą technologię kartach pamięci aparatów cyfrowych, pendrive'ach czy dyskach SSD przechowywane są coraz istotniejsze dane. Niestety, podobnie jak w przypadku nośników tradycyjnych (takich jak dyski twarde), ryzyko ich utraty nadal istnieje. Dlatego też inżynierowie odzyskiwania danych stworzyli technologię, która pozwala użytkownikom pamięci flash i dysków SSD odzyskać dane nawet w najtrudniejszych, nierozwiązywalnych dotychczas przypadkach.

Wraz ze wzrostem popularności urządzeń korzystających z technologii flash wyraźnie wzrosła także liczba przypadków utraty przechowywanych na nich plików. W USA i krajach azjatyckich do laboratoriów Kroll Ontrack – największej na świecie firmy odzyskującej dane – trafiło o 70% więcej zleceń odzyskania danych z tych nośników niż w 2006 roku.

Pamięci flash to obecnie kluczowa technologia, która w przyszłości pozwoli na tworzenie innowacyjnych produktów przeznaczonych dla przedsiębiorstw oraz klientów indywidualnych. Należy jednak pamiętać, że rozwiązania te oraz ulepszenia technologii (większa pojemność, zróżnicowane aplikacje oraz zwiększona wydajność) nie pozwalają uchronić pamięci flash oraz dysków SSD przed utraceniem zapisanych na nich informacji. Pamiętajmy, że urządzenia wykorzystujące opisywaną technologię również są narażone na utratę danych, podobnie jak nośniki tradycyjne, w przypadku których pliki giną w wyniku awarii dysku bądź błędu człowieka.

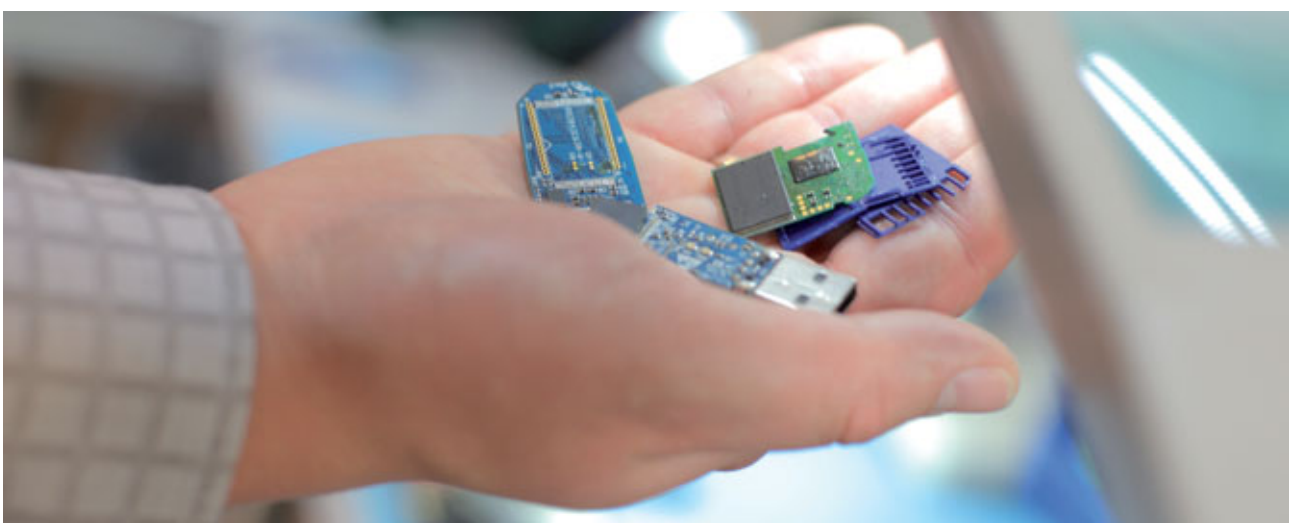
Użytkownicy indywidualni wykorzystują technologię flash do zapisu zdjęć w aparatach cyfrowych oraz plików w pamięciach przenośnych. Firmy natomiast, choć w głównej mierze nadal korzystają z tradycyjnych „twardzieli", coraz częściej decydują się na zastąpienie ich dyskami SSD bazującymi na technologii flash. Odzyskanie z nich danych jest możliwe zarówno w przypadku uszkodzeń mechanicznych (np. zalania, roztrzaskania, spalenia), jak i logicznych (np. przypadkowego skasowania danych).

Proces odzyskiwania danych

W pierwszym etapie procesu odzyskiwania danych z urządzeń mobilnych specjaliści zapoznają się telefonicznie z konkretnym przypadkiem i pomagają dopasować najlepsze rozwiązanie pod względem czasu reakcji i kosztów. Po dostarczeniu nośnika do laboratorium (osobiście przez właściciela bądź przez kuriera) eksperci przeprowadzają szczegółową analizę uszkodzenia, co pozwala ocenić stan danych, zakres uszkodzenia oraz szacowany czas przywrócenia informacji.

Wynikiem ekspertyzy jest najczęściej raport Verifile, który pozwala klientowi na zapoznanie się z możliwą do odtworzenia strukturą plików i danych, jeszcze przed rozpoczęciem procesu ich odzyskiwania. Na tym etapie specjaliści w laboratorium sporządzają także kalkulację kosztów odzyskania danych. Komplet informacji jest następnie przekazywany klientowi.

Proces odzyskiwania danych rozpoczyna się niezwłocznie po otrzymaniu akceptacji wyników ekspertyzy. Specjaliści dokonują odzyskania i naprawy struktur logicznych danych przy użyciu ponad 120 różnego rodzaju urządzeń specjalistycznych oraz szerokiej gamy oprogramowania. Po odzyskaniu dane zwracane są klientowi na wybranym przez niego nośniku



Fot. 1. Uszkodzone karty pamięci przygotowane do odzyskania danych w laboratorium Kroll Ontrack

(np. na karcie pamięci). Kopia bezpieczeństwa danych jest przechowywana na firmowym serwerze przez 30 dni, a następnie bezpowrotnie usuwana, zgodnie z procedurą bezpieczeństwa.

Specjaliści wyszczególniają dwa typy uszkodzeń nośników:

– **uszkodzenia logiczne (software'owe)** – polegające na naruszeniu integralności struktury logicznej danych, a nie na uszkodzeniu samych nośników. Czasem w tego typu przypadkach pomagają standardowe narzędzia, jednak często problem jest na tyle poważny, że w celu odzyskania danych z dysku konieczna jest ingerencja specjalisty pracującego w laboratorium *data recovery*.
– **uszkodzenia sprzętowe (fizyczne)** – gdy nośnik danych ulega uszkodzeniu mechanicznemu (np. zalaniu bądź spaleniu). W tego typu sytuacjach nie jest możliwe zastosowanie oprogramowania do samodzielnego odzyskiwania danych.

W przypadku uszkodzeń fizycznych odzyskiwanie danych (głównie z dysków) jest wykonywane w sterylnym środowisku, gdzie nośniki są rozmontowywane, testowane i naprawiane. W przypadku uszkodzeń logicznych zawartość nośnika jest kopiowana, a struktury danych odtwarzane na nowym nośniku. Próba dokonania tej operacji samodzielnie lub przez niedoświadczonego dostawcę usługi grozi postępującym niszczeniem nośnika, a w efekcie całkowitą utratą zapisanych danych.

Zjawisko sezonowości utraty danych w przypadku urządzeń mobilnych

Jedną z ciekawostek w przypadkach urządzeń mobilnych jest zjawisko sezonowości utraty danych. Ze względu na swoją specyfikę urządzenia te w zdecydowanej większości są dużo bardziej narażone na różnego rodzaju wstrząsy, niskie i wysokie temperatury czy upadki.

W szczególności dotyczy to lipca, sierpnia i września – te miesiące są wyjątkowo pracowitym okresem dla specjalistów pracujących w laboratoriach. W czasach gdy niemal każdy posiada już cyfrowe urządzenia do zapisywania zdjęć, rośnie też liczba przypadków ich uszkodzeń. Jest to szczególnie widoczne w okresie wakacyjnym, gdy liczba zapisywanych przez urlopowiczów danych jest w stosunku do pozostałych miesięcy wyjątkowo wysoka, a zarazem wzrasta liczba okazji do uszkodzenia urządzeń.

Jak wskazują specjaliści, mimo zdarzających się stosunkowo często awarii urządzeń najczęstszą przyczyną utraty plików z popularnych „cyfrówek", pendrive'ów, komórek i odtwarzaczy MP3 jest właśnie niefrasobliwość użytkownika. Najczęściej więc urządzenia te lądują np. w ogniskach lub basenach, zdarza się także przypadkowe skasowanie zdjęć lub sformatowanie karty.

Zagrożenia dla firm

Niestety używanie coraz bardziej zaawansowanych smartfonów wiąże się także z możliwością utraty zapisanych na nich danych. Pamiętać o tym muszą przede wszystkim polskie firmy, zaopatrujące swoich menedżerów i innych pracowników w tego typu telefony, na których zapisanych jest coraz więcej kluczowych firmowych dokumentów, baz danych oraz innych zastrzeżonych informacji.

Przyczyn utraty danych w przypadku tego typu urządzeń jest wiele, wśród nich są także przypadki kradzieży lub po prostu zgubienia urządzeń. Według statystyk Komendy Głównej Policji każdego roku w Polsce kilkanaście tysięcy osób pada ofiarą kradzieży telefonów komórkowych lub je gubi. Poza tradycyjnymi informacjami, jak numery telefonów, adresy czy treści SMS-ów, w komórkach znajdują się także dane firm, które coraz częściej używają smartfonów przystosowanych do edycji i zapisywania dokumentów przesyłanych na pocztę e-mail. Przedsiębiorcy powinni pamiętać, że utrata tych danych może grozić poważnymi konsekwencjami finansowymi nie tylko dla samej firmy, ale także jej klientów i kontrahentów.

Urządzenia wykorzystujące technologię flash, z jakich eksperci największych na świecie laboratoriów odzyskują dane, to najczęściej:

– BlackBerry,
– CompactFlash,
– Memory Stick,
– PC Cards (PCMCIA),
– SD Media,
– kieszonkowe PC/WinCE,
– karty pamięci SmartMedia,
– dyski USB „Key",
– xD Media,
– palmtopy,
– aparaty cyfrowe.

Fot. 2. Specjaliści Kroll Ontrack podczas odzyskiwania danych w laboratorium

Fot. 3. Uszkodzony dysk przygotowany do procesu odzyskiwania danych w laboratorium Kroll Ontrack

Fot. 4. Spalony aparat z którego odzyskano zdjęcia w laboratorium Kroll Ontrack

Najciekawsze przypadki utraty danych z urządzeń mobilnych

Najgłośniejszy w Polsce przypadek utraty zdjęć cyfrowych jest związany z himalaistą Krzysztofem Wielickim, który w 2004 roku stracił dokumentację jednej ze swoich wypraw po tym, jak tragarz, siadając, uszkodził urządzenie do archiwizowania zdjęć, na którym ta dokumentacja się znajdowała (zdjęcia zostały odzyskane).

Inne oryginalne przypadki utraty danych z całego świata to między innymi:

1) „Sprawa żołądkowa" – przestępca, którego zatrzymali policjanci, połknął kartę SIM swojego telefonu. Były na niej zapisane godziny rozmów oraz książka adresowa, w której mogły znajdować się osoby podejrzane o popełnienie przestępstwa. Kiedy policyjnym lekarzom udało się odzyskać kartę, nieco uszkodzona trafiła do laboratorium odzyskiwania danych.
2) „Kość niezgody" – pies jednego z klientów firmy odzyskującej dane potraktował pamięć przenośną pozostawioną na biurku jak zabawkę do gryzienia. Specjaliści odzyskali wszystkie dane, pomimo licznych pogryzień urządzenia, których sprawcą był rodzinny pupil.
3) „Kochanie, wypiorę twoje spodnie" – zrozpaczony mężczyzna zwrócił się do specjalistów odzyskiwania danych po tym, jak przekazując żonie spodnie do prania, nie wyciągnął z kieszeni swojej pamięci przenośnej. Żona wybrała tryb z wirowaniem i suszeniem. Wszystkie dane zostały klientowi zwrócone.
4) „Szukając Nemo" – użytkownik wodoszczelnego aparatu wrócił z podróży życia na Barbados. Chciał obejrzeć zdjęcia, które robił pod wodą podczas nurkowania. Niestety aparat nie okazał się tak szczelny jak w reklamie. Inżynierowie odzyskali jednak wszystkie zdjęcia kolorowych rybek, które uwieczniał nurek-fotograf.
5) „Halo! Wyprane dane" – do laboratorium odzyskiwania danych zadzwoniła pewna osoba z informacją, że wyprała wszystkie swoje dane. Jej pamięć USB trafiła do pralki, a usuwanie danych trwało cały cykl z płukaniem. Niestety danych nie można było odzyskać. Podobny przypadek miał miejsce w Polsce w 2005 roku.
6) „Córeczka tatusia" – pewien mężczyzna po pracy spieszył się do domu, gdzie czekała na niego córeczka. Tego dnia to on miał przygotować dla niej obiad. Wychodząc z pracy, wrzucił pamięć przenośną do kieszeni koszuli. Jakiś czas później karmiąc córkę, nachylił się i wtedy pamięć z kieszeni wylądowała w ciepłym, apetycznym, ale dość rzadkim i klejącym jabłkowym puree (dane zostały odzyskane).
7) „Spalony na węgiel" – po pożarze jednego z mieszkań strażacy odnaleźli zwęglony aparat fotograficzny. Właściciele zlecili odzyskanie zdjęć ze spalonego urządzenia. To jedyne, co udało się uratować po pożarze.
8) „Zawiódł spadochron" – producent spadochronów postanowił nagrać na wideo testy nowego modelu. W tym celu do obciążenia spadochronu wyrzuconego z samolotu dołączono kamerę. Niestety test wypadł niepomyślnie. Ładunek wraz z kamerą rozbił się o ziemię i rozpadł na wiele kawałków. Ekspertom udało się złożyć kartę pamięci kamery i odzyskać nagranie.
9) „Dane za burtą" – wyjątkowa podróż dookoła świata mogła zakończyć się dramatem, gdy statek, którym płynął podróżnik, zatonął. Wraz z nim pod wodą znalazł się aparat fotograficzny ze wszystkimi zdjęciami z kończącej się właśnie wyprawy. Na szczęście wizyta w laboratorium odzyskiwania danych przyniosła oczekiwane skutki i 100 procent danych z „wyprawy życia" udało się odzyskać.
10) „Bestia czy dwulatek?" – specjaliści Kroll Ontrack otrzymali kartę SD (pochodzącą z aparatu fotograficznego) z widocznymi śladami zębów. Właściciel karty, przynosząc ją do laboratorium odzyskiwania danych, uporczywie twierdził, że dostała się w paszczę „dzikiego zwierzęcia" podczas jednej z jego podróży. W rzeczywistości groźnym zwierzęciem okazał się jego dwuletni syn.
11) „Wymiecione dane" – standardowe sprzątanie jednego z domów przerodziło się w „sprzątanie danych", gdy pendrive został wciągnięty przez odkurzacz piorący. Na szczęście z zalanego urządzenia udało się odzyskać wszystkie dane, a sprzątaczka nie straciła pracy.
12) „Spełniona obietnica" – po powrocie z jednej z wypraw pewien znany podróżnik przypadkowo skasował wszystkie zdjęcia zapisane na karcie SD. Strata okazała się tym większa, że na karcie znalazła się zapierająca dech w piersiach fotografia napotkanego turysty, którą podróżnik obiecał przesłać na jego e-mail po powrocie z wyprawy. Zdjęcie ostatecznie dotarło do turysty.
13) „Zaklinacz koni" – wyścigi konne mogą być groźne nie tylko dla ludzi, lecz także dla danych. Podczas jednej z gonitw upadł jeździec, który miał zamontowaną na toczku kamerę. Choć toczek spełnił swoje zadanie i ochronił głowę dżokeja, kamera nie przetrwała upadku i roztrzaskała się wraz z kartą pamięci, na której znajdował się zapis gonitwy. Zapis wyścigu odzyskano dopiero za trzecim razem, gdy sprawą zajęli się eksperci od odzyskiwania danych.

Paweł Odor
Główny specjalista polskiego oddziału Kroll Ontrack, największej na świecie firmy zajmującej się odzyskiwaniem danych i informatyką śledczą

Usługi monitoringu wizyjnego w agencjach ochrony

Daniel Kamiński

Rozwój technologii informatycznych oraz obniżenie kosztów teletransmisyjnych powodują, że klienci coraz częściej pytają o usługi monitoringu wizyjnego. W przypadku dużych obiektów klienci korzystają z systemów nadzoru wizyjnego polegającego na stałej obserwacji obrazów za pomocą zainstalowanych tam kamer. Ma to na celu zmniejszenie miesięcznych koszów ochrony fizycznej oraz zwiększenie efektywności systemu ochrony. Natomiast uruchomienie monitoringu wizyjnego w takiej postaci dla klientów indywidualnych jest bardzo trudne do wykonania. Obiekty, które miałyby być chronione, są rozproszone, koszt nadzoru wizyjnego przekracza możliwości domowych budżetów, a instalowane systemy wymagają nadzoru. Stanowi to spore wyzwanie dla firm świadczących usługi w zakresie ochrony. Rozwiązaniem może być potraktowanie rozproszonych klientów jako jednego systemu sieciowego i stworzenie usługi polegającej na zdalnym monitoringu zdarzeń wizyjnych w sytuacjach alarmowych

Zarówno ochrona fizyczna, jak i systemy nadzoru wizyjnego są przeznaczone do ochrony obszarów i obiektów o średnim i wysokim poziomie zagrożenia. Połączenie obu rozwiązań podnosi poziom bezpieczeństwa i pozwala na elastyczne dostosowanie procedur do potrzeb chronionego obiektu. Niestety wyposażenie, eksploatacja i obsługa takich systemów ochrony stanowią dla zwykłego śmiertelnika spory wydatek.

Na łamach prasy branżowej często omawiane są rozwiązania pozwalające na budowanie złożonych systemów ochrony bazujących na CCTV i zarządzanych za pomocą aplikacji typu VMS (*video management system*). W artykułach przedstawia się sposoby zabezpieczania obiektów najtrudniejszych do nadzorowania i stawiających największe wymagania: systemy ochrony stadionów, centrów handlowych, linii metra i monitoringu miejskiego. Opisy te przenoszą czytelników w świat najnowszych technologii obserwacji.

Bardzo rzadko natomiast pojawiają się opisy rozwiązań przeznaczonych do ochrony mniejszych obiektów, czyli dla klientów indywidualnych oraz małego biznesu. W pewnym sensie to zrozumiałe, ponieważ temat nie jest tak medialny, a prasa branżowa jest kierowana przede wszystkim do innej grupy odbiorców – dużych inwestorów, projektantów, integratorów itp. Przyczyny można szukać w tym, że grupa klientów nazywana często klientem masowym nie jest w stanie zainwestować znacznej kwoty w system bezpieczeństwa składający się z ochrony fizycznej oraz systemu nadzoru wizyjnego. Jeśli jednak spojrzymy na małe obiekty (w których zainstalowano najwyżej po cztery kamery) z innej perspektywy i potraktujemy je jako duży obiekt sieciowy w rozproszonej lokalizacji, to system znacząco się komplikuje i stanowi inżynierskie wyzwanie. W takim systemie największym problemem do pokonania będzie przyjęcie i przetworzenie danych wizyjnych z tysięcy kamer.

Usługi realizowane za pomocą takiego rozwiązania również będą się różniły od usług charakterystycznych dla większych obiektów. Przy dużej liczbie kamer oraz małym poziomie zagrożenia na jednego operatora systemu będzie przypadać więcej obiektów do nadzorowania. W takiej sytuacji zmienia się sposób pracy: zamiast ciągłej obserwacji monitorów operator czeka na zdarzenie alarmowe, w wyniku którego:

a) otrzymuje obrazy z chronionego obiektu w celu ich weryfikacji wizyjnej,
b) łączy się z monitorowanym obiektem na czas obsłużenia zdarzenia.

Stworzenie systemu dla dużej liczby rozproszonych obiektów stanowi spore wyzwanie. Z tego względu artykuł jest poświęcony systemom łączącym w sobie zalety ochrony fizycznej i monitoringu wizyjnego, przeznaczonym dla klienta masowego. W artykule omówione zostaną systemy weryfikacji wizyjnej alarmów oraz zdalnego monitoringu zdarzeń wizyjnych, wspierane przez mobilne załogi interwencyjne.

nadzór wizyjny – usługa stałego nadzoru poprzez obserwację kamer w obiekcie

zdalny monitoring zdarzeń wizyjnych – usługa zdalnego nadzoru kamer w wyniku zadziałania wyjścia alarmowego (na czas obsługi zdarzenia)

Inne spojrzenie – monitoring wizyjny dla mas

Na naszym rynku usługi ochrony dla klientów masowych świadczą głównie agencje ochrony. Firmy te wyspecjalizowały się w monitorowaniu alarmów, czyli usługach dla klientów poszukujących kompromisu pomiędzy ceną i poziomem bezpieczeństwa, gdzie w przypadku alarmu do chronionego obiektu wysyłana jest załoga interwencyjna. Koszt tej usługi to niewielki abonament oraz opłata za każdą interwencję.

W przypadku monitoringu wizyjnego dla klientów masowych główny problem stanowią ograniczenia związane z kosztami, skalowalnością oraz zasadami licencjonowania stosowanych rozwiązań. Obecnie nawet największe centra handlowe czy systemy monitoringu miejskiego liczą mniej niż 1000 kamer. Stąd zbudowanie systemu obsługującego 50 tys., 250 tys. czy 1,5 mln kamer stanowi spore wyzwanie. A przy obsłudze klienta masowego musimy wziąć pod uwagę takie liczby.

Przy standardowym założeniu, że serwer obsługuje do 64 strumieni wizji, uruchomienie systemu obsługującego 50 tys. kamer w trybie obserwacji ciągłej wymagałoby wybudowania olbrzymiego centrum przetwarzania danych zawierającego ponad 750 serwerów, zapewnienia łącza o przepustowości ponad 20 GB/s (30 Mb/s na serwer), zatrudnienia 5000 operatorów (1500 na zmianie) oraz zapewnienia 1500 TB przestrzeni dyskowej (przy miesięcznej archiwizacji).

Podane liczby wskazują, że uruchomienie usługi według standardowych kryteriów nie byłoby zasadne, ponieważ jej koszt w przeliczeniu na kamerę byłby za duży, aby zainteresować klientów.

Jeżeli zatem rozważamy objęcie klienta masowego usługą zdalnego monitorowania wizyjnego, musimy zrezygnować z założenia, że operator przez 24 godziny obserwuje obraz z każdej kamery. Należy przyjąć, że operator obserwuje obraz tylko w chwili zdarzenia alarmowego, i to przez czas potrzebny do podjęcia decyzji, którą procedurę uruchomić.

Doświadczenia z systemów monitorowania alarmów włamaniowych pokazują, że:

1) Obiekty klientów indywidualnych generują średnio 2–3 alarmy w roku, natomiast klienci biznesowi generują

Fot. 1. Przykład centrum nadzoru wizyjnego (dzięki uprzejmości firmy Netwatch z Irlandii)

1–2 alarmy w miesiącu. Stosunek liczby klientów indywidualnych do biznesowych obsługiwanych przez dane centrum obsługi wynosi z reguły 60:40.

2) Obsługa sygnału alarmowego przez operatora (wraz z powiadomieniem klienta) zajmuje średnio 2–3 minuty. Można więc przyjąć, że operator może obsłużyć ok. 15 sygnałów alarmowych na godzinę.
3) Przy tych danych wyjściowych oraz uwzględnieniu godzin „szczytu" na jednego operatora przypadnie ok. 5000 klientów (liczba wynika z praktyki centrum monitorowania alarmów), więc do obsłużenia sygnałów alarmowych z 50 tys. obiektów potrzebnych będzie dziesięciu operatorów.

Jeżeli zatem rozważamy objęcie klienta masowego usługą zdalnego monitorowania wizyjnego, musimy zrezygnować z założenia, że operator przez 24 godziny obserwuje obraz z każdej kamery. Należy przyjąć, że operator obserwuje obraz tylko w chwili zdarzenia alarmowego, i to przez czas potrzebny do podjęcia decyzji, którą procedurę uruchomić.

Korzystając z powyższych założeń, możemy oszacować liczbę personelu potrzebną do obsługi zdarzeń wizyjnych. Przy 50 tys. obiektów należy się spodziewać około 140 alarmów wizyjnych na godzinę. Przy założeniu, że obsługa zdarzenia wizyjnego zajmie maksymalnie 5 minut, uzyskujemy następujące dane:

– operator może obsłużyć do 10–15 alarmowych sygnałów wizyjnych na godzinę, zatem do obsługi 50 tys. kamer potrzeba 15 operatorów na zmianie (100 razy mniej niż przy nadzorze wizyjnym),
– do obsłużenia tej liczby alarmów wizyjnych wystarczy dziesięć serwerów wizyjnych (jeden serwer obsłuży do 5000 kamer).

Zmiana założeń umożliwia przygotowanie danych pozwalających na wycenę usługi skierowanej do klienta masowego.

Różne zastosowania monitorowania wizyjnego

W agencjach ochrony wzrasta zakres usług związanych z wizyjną weryfikacją alarmów oraz wizyjnym monitorowaniem zdarzeń. Jest to wywołane coraz większą liczbą pytań klientów, którzy chcą mieć zdalny dostęp do systemów bezpieczeństwa zainstalowanych w swoich obiektach poprzez przeglądarkę internetową lub smartfony. Za pomocą tych usług klienci chcą samodzielnie sprawdzić, jak opiekunka zajmuje się dzieckiem, kontrolować pracowników, weryfikować stan obiektu, upewniać się, że członkowie rodziny wrócili do domu itp.

Drugim poszukiwanym przez klientów rodzajem usług są wirtualne patrole, czyli zdalne sprawdzanie, czy w chronionym obiekcie nie ma sytuacji zagrożenia. Usługi są szczególnie przydatne w sieciach handlowych, w których zredukowano liczbę pracowników ochrony. Operator centrum monitorowania łączy się cyklicznie kilka razy dziennie ze sklepami i w przypadku zaobserwowania kradzieży informuje obsługę obiektową oraz wysyła załogę interwencyjną.

Fot. 2. Przykład aplikacji do obsługi strumieni wizyjnych (fot. Milestone).

Powodem wzrostu popularności usług wizyjnych wśród agencji ochrony jest obniżenie kosztów działalności załóg interwencyjnych. Jest to obecnie najbardziej skuteczny sposób weryfikacji fałszywych alarmów, szczególnie generowanych przez zewnętrzne systemy ochrony. Operator centrum monitorowania w przypadku otrzymania sygnału alarmu uzyskuje automatycznie połączenie wizyjne z chronionym obiektem. Na podstawie obserwacji zdarzenia w obiekcie podejmuje decyzję o wysłaniu załogi interwencyjnej. Dzięki takiemu wsparciu załogi interwencyjne rzadziej jeżdżą do nieuzasadnionych alarmów, co bezpośrednio wpływa na zmniejszenie się liczby interwencji spóźnionych.

Przegląd dostępnych rozwiązań

Na rynku jest dostępnych kilka rodzajów rozwiązań, na bazie których można przygotować system zarządzania zdarzeniami wizyjnymi odbieranymi z dużej liczby obiektów.

Przykładowymi rozwiązaniami przeznaczonymi dla stacji monitorowania są systemy zdalnego monitorowania wizyjnego firm AdPro (Xtralis), Heitel i OzVision. Systemy są dostępne na rynku europejskim od kilkunastu lat. Każdy z producentów sprzedał ponad 50 tys. urządzeń transmisyjnych. Rozwiązanie takie jest oparte na nadajnikach wizji korzystających z sieci transmisyjnych o niskich przepustowościach. Główną jego zaletą jest możliwość fizycznego odseparowania od lokalnego rejestratora wizji. Przy tym rozwiązaniu klient ma pewność, że operatorzy centrum monitorowania nie będą naruszali jego prywatności, ponieważ do stacji monitorowania są przekazywane tylko sygnały z wyjścia alarmowego rejestratora. Każde z powyższych rozwiązań jest przygotowane do obsługi wielu tysięcy kamer.

Drugim sposobem tworzenia rozwiązań dla stacji monitorowania jest wykorzystanie programów zarządzania strumieniami wizji, takich producentów jak: Griffid, IndigoVision, Milestone, Mirasys, SeeTec, Verint i innych. Systemy te są przeznaczone do obsługi kamer IP i wideoserwerów IP. Część z nich potrafi integrować również obrazy z rejestratorów popularnych producentów. Rozwiązania bazujące na kamerach IP/IP WIFI są szczególnie przydatne w obiektach, w których nie ma systemów CCTV.

W przypadku obu typów systemów elementem, który musi być wzięty pod uwagę, są opłaty licencyjne. Producenci rozwiązań wykorzystywanych do budowania systemów monitoringu wizyjnego wyceniają swoje aplikacje serwerowe w odniesieniu do liczby przyłączonych kamer. W przypadku usług zdalnego monitorowania zdarzeń wizyjnych rozliczenie w zależności od liczby kamer nie jest korzystne, gdyż opłaty są skalkulowane

Fot. 3. Przykład aplikacji do zdalnej analizy zarejestrowanych zdarzeń (fot. Heitel).

przy założeniu całodobowego nadzoru wizyjnego, a nie kilkuminutowego dostępu do kamery. Należy mieć nadzieję, że w przyszłości opłaty te zostaną dostosowane do specyfiki pracy agencji ochrony i że dla usług zdalnego wizyjnego monitorowania zdarzeń wprowadzone zostaną licencje uzależnione od liczby serwerów lub od liczby aktywnych połączeń.

Analityka w celu redukcji liczby fałszywych alarmów

Systemy zdalnego monitorowania wizyjnego stosuje się do weryfikacji zdarzeń alarmowych, aby zredukować liczbę interwencji na skutek alarmów fałszywych. W przypadku dużej liczby kamer pojawia się potrzeba automatycznego odfiltrowania obrazów, na których nie stwierdzono obecności intruza. Do tego celu stosuje się cyfrową analizę obrazu.

Warto przypomnieć, że fałszywe alarmy powodują 95% interwencji podejmowanych przez agencje ochrony. Podgląd wizyjny pozwala na znaczące ograniczenie liczby interwencji, a dzięki temu na uzyskanie dużych oszczędności. Zmniejszenie nakładu pracy niezbędnej do przeglądania odbieranych obrazów dzięki zastosowaniu analizy cyfrowej pozwala na zmniejszenie liczebności personelu wymaganego na stacji monitorowania, a przez to wprowadzenie dodatkowych oszczędności.

Analiza obrazu jest realizowana na dwa sposoby. Sygnały są analizowane na serwerze po odebraniu nagranego materiału z kamery albo sama kamera jest wyposażona w odpowiedni układ do analizy i wykonuje ją bezpośrednio podczas obserwacji. Pierwsze rozwiązanie umożliwia dodatkową weryfikację zdarzenia przez człowieka; drugie nie daje takiej możliwości, ale zdecydowanie mniej obciąża łącze komunikacyjne.

Podsumowanie

Usługodawca nie może zakładać, że operator będzie całą dobę obserwował kilka kamer. Należy założyć, że obiekt klienta jest wyposażony w system wykrywania i sygnalizacji alarmu, a zadaniem operatora systemu obserwacji jest podejmowanie decyzji, którą procedurę należy uruchomić po wizualnej weryfikacji zdarzenia w obiekcie. Dzięki takiemu podejściu skuteczność systemu rośnie, a usługa nabiera nowego charakteru; co najważniejsze, jej cena stanie się akceptowalna dla klienta.

Rozwiązania bazujące na opisanym modelu są obecne w Europie od kilku lat, ale niestety nie ma jeszcze wypracowanych w tym zakresie standardów. Największe stacje posiadają nawet 400 tys. klientów i obsługują do 5000 obiektów wyposażonych w kamery. Mamy więc szansę wpłynąć na rozwój tych usług i współtworzyć nowe standardy.

Daniel Kamiński
OCHRONA JUWENTUS

System Kontroli Dostępu

KaDe

Kontrolery zintegrowane z czytnikami kart zbliżeniowych

Wizualizacja systemu poprzez elektroniczne mapy z aktywnymi ikonami, zdjęciami użytkowników i obrazami wideo „na żywo"

Intuicyjne oprogramowanie nadzorcze

Komunikacja TCP/IP i RS-485

Integracja z systemem CCTV

C-70 C-60 C-10 C-20 KZ-1000

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

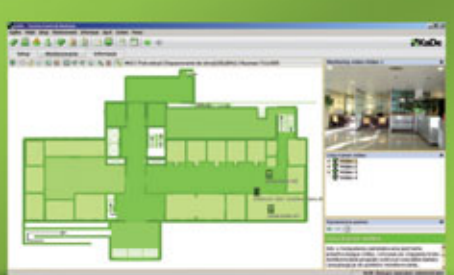
Kontroler KZ-1000	Kontroler przejścia integrujący: moduł kontrolera 1 przejścia, czytnik kart zbliżeniowych 125 kHz UNIQUE, klawiaturę do wprowadzania kodu PIN i przycisk dzwonkowy, sygnalizator optyczny i akustyczny, czujnik antysabotażowy

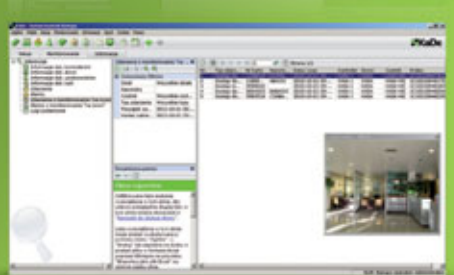
Czytniki kart zbliżeniowych typu UNIQUE (125 kHz):

C-10 C-60 C-70	Czytniki do instalacji wewnątrz i na zewnątrz pomieszczeń, różniące się między sobą jedynie obudową i kolorystyką, co umożliwia optymalne dopasowanie urządzenia i sposobu montażu do każdego wnętrza
C-20	Czytnik identyczny z powyższymi pod względem parametrów, dodatkowo wyposażony w klawiaturę kodową
C-ADM-U	Czytnik administratora przeznaczony do wprowadzania dużej liczby kart do bazy danych programu nadzorczego KaDe. Istnieje możliwość wykorzystania urządzenia do innych zastosowań, np. do współpracy z dowolnym edytorem lub polami edytowalnymi w różnych aplikacjach

Akcesoria

Konwerter RS232/485	Konwerter służy do połączenia magistrali kontrolerów z programem nadzorczym w komputerze poprzez port COM. Urządzenie umożliwia konwersję protokołu RS-232 na RS-422/RS-485
Konwerter TCP/RS485	Konwerter służy do połączenia magistrali kontrolerów z programem nadzorczym w komputerze poprzez sieć Ethernet. Urządzenie umożliwia konwersję protokołu RS-422/RS-485 na protokół sieciowy TCP/IP
Konwerter USB/RS485	Konwerter służy do połączenia magistrali kontrolerów z programem nadzorczym w komputerze poprzez port USB
Karty AST	System współpracuje z kartami zbliżeniowymi AST: AST-U-1001, AST-U-1002, AST-U-1003, AST-U-1004





INTERFEJS OPERATORA

- konfiguracja parametrów elementów fizycznych systemu
- definiowanie elementów logicznych
- monitorowanie stanu systemu „on-line" poprzez system graficznych map obiektów i komunikatów
- wyświetlanie zdjęć użytkownika
- integracja z systemem CCTV poprzez wbudowaną w PC kartę przechwytującą wideo lub zewnętrzny DVR/IP, kamery przypisane do kontrolowanych przejść lub czujek
- generowanie filtrowanych raportów zdarzeń i zapis w formacie *.xls

Funkcje specjalne realizowane przez system KaDe

- dostęp po użyciu 2, 3 lub 4 kart
- pierwsze otwarcie kontrolowanego przejścia przez tzw. pierwszą kartę ze specjalnymi uprawnieniami
- dostęp po potwierdzeniu przez operatora

Prosty i funkcjonalny system KaDe

Ryszard Sobierski

Badania rynkowe oraz opinie uzyskane od instalatorów i klientów wykazują wzrastające zapotrzebowanie na proste i funkcjonalne systemy kontroli dostępu przeznaczone do obiektów, w których potrzebne są tylko funkcje podstawowe, a jednym z ważniejszych kryteriów wyboru systemu jest cena. Tendencja ta jest bardzo ważną wskazówką dla producentów, importerów i dystrybutorów elektronicznych systemów zabezpieczeń. Parafrazując wieszcza, można powiedzieć, że w ślad za systemami alarmowymi trafia pod strzechy również kontrola dostępu

System kontroli dostępu oferowany pod marką KaDe jest przeznaczony dla małych i średnich obiektów, w których potrzebna jest prosta, ale skuteczna kontrola dostępu za przystępną cenę. Mam tu na myśli zwłaszcza obiekty użyteczności publicznej finansowane z budżetu państwa (szpitale, przychodnie, urzędy administracji miejskiej), które, jak powszechnie wiadomo, dysponują najczęściej skromnym budżetem na tego rodzaje wydatki. Zarazem jednak ze względu na charakter obiektu (dużą liczbę interesantów) powinny być zabezpieczone przed dostępem tych osób do miejsc przeznaczonych tylko dla pracowników.

System KaDe spełnia te warunki. Jest prosty i szybki w instalacji, łatwy w obsłudze i posiada intuicyjny interfejs dla administratora. Również instalacja urządzeń nie powinna sprawiać kłopotów. W artykule tym zostaną przedstawione elementy systemu KaDe oraz jego najważniejsze funkcje.

Program nadzorczy KaDe-Soft V1

Program nadzorczy KaDe-Soft V1 jest przeznaczony do współpracy ze zintegrowanymi kontrolerami typu KZ-1000 w trybie

sieciowym. Praca w takim trybie znacznie zwiększa funkcjonalność systemu kontroli dostępu opartego na wspomnianych kontrolerach w porównaniu z kontrolerami w trybie autonomicznym.

Program jest bardzo prosty w instalacji i posiada przyjazny interfejs graficzny dla operatora. Przystosowany jest do pracy w środowisku Windows 2000/2003/XP/Vista i współpracuje z domyślną bazą danych Microsoft Access. Możliwa jest również współpraca z bazą SQL. Bardzo przydatną funkcją jest możliwość importu danych użytkowników z pliku (np. z programu kadrowego). Na uwagę zasługują również wyświetlane na pulpicie operatora okna „dynamicznej pomocy", czyli podręcznej instrukcji. Po kliknięciu dowolnego pola w oknie pulpitu wyświetlany jest opis tej pozycji i metoda definiowania lub konfiguracji danego elementu systemu.

Program nadzorczy KaDe-Soft V1 przeznaczony jest do małych i średnich systemów kontroli dostępu. Interfejs operatora umożliwia między innymi:

– konfigurację parametrów fizycznych elementów systemu,
– definiowanie elementów logicznych,
– monitorowanie stanu systemu „na żywo" poprzez system graficznych map obiektów, zdjęć, obrazów z kamer i komunikatów,
– wyświetlanie zdjęć użytkownika po użyciu karty,
– integrację z CCTV poprzez kartę przechwytującą wideo (wbudowaną w PC lub rejestrator DVR) oraz kamery przypisane do kontrolowanych przejść,
– operacje na elementach systemu (kontrolery, drzwi) z menu kontekstowego,
– rejestrację i kasowanie alarmów – automatyczne lub przez operatora,
– generowanie filtrowanych raportów zdarzeń i zapis w formacie *.xls.

Program KaDe-Soft V1 oferuje szereg funkcji, które umożliwiają spełnienie różnych nietypowych wymagań stawianych przez administratora systemu, takich jak: dostęp po użyciu dwóch, trzech lub czterech kart, pierwsze otwarcie kontrolowanego przejścia przez tzw. „pierwszą kartę" ze specjalnymi uprawnieniami lub dostęp po potwierdzeniu przez operatora.

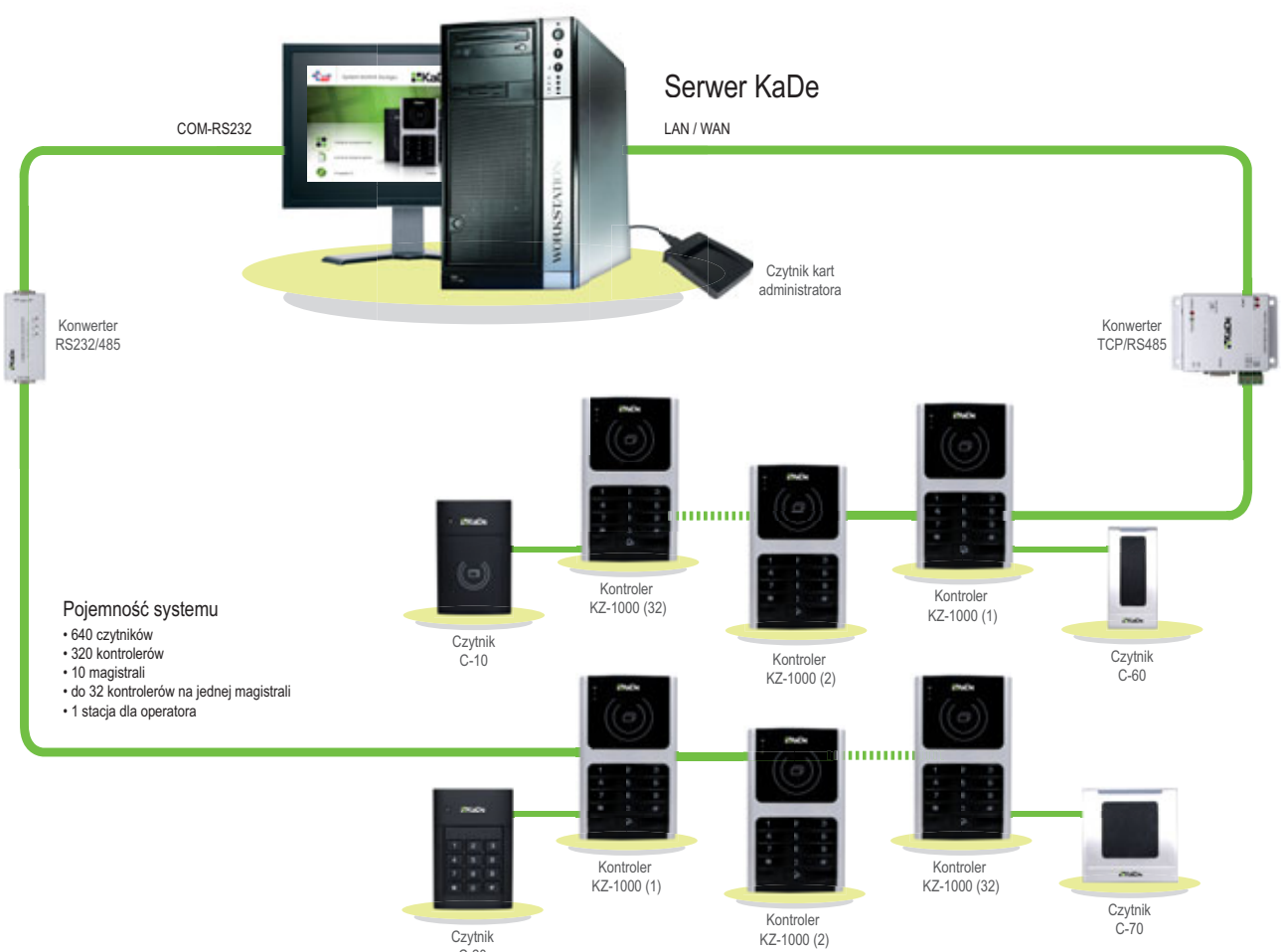
Magistrale kontrolerów wykorzystujące protokół RS485 mogą być połączone z programem nadzorczym na komputerze poprzez konwerter RS485/232 lub poprzez konwerter RS485/TCP. Program może obsłużyć do dziesięciu magistral, po 32 kontrolery każda.

Pojemność systemu czyli liczba użytkowników kart, jakich może on obsłużyć, jest uzależniona od modelu kontrolera. W przypadku kontrolera KZ-1000 wynosi ona 3000 kart.

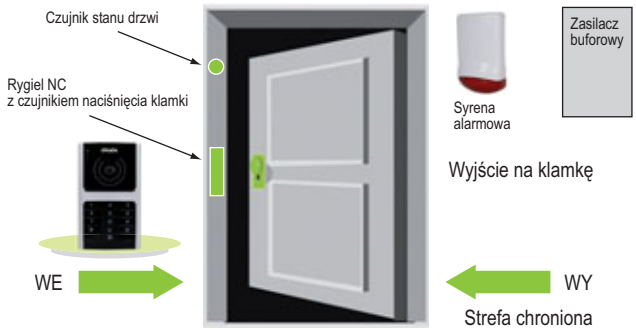
Elementy systemu – kontroler zintegrowany KZ-1000

Kontroler zintegrowany typu KZ-1000 jest przeznaczony do pracy w systemie kontroli dostępu KaDe. Jest to kontroler jednego przejścia. Przejście to może być kontrolowane jedno- lub dwustronnie. Aby zrealizować kontrolę dwustronną, należy dołączyć do portu kontrolera drugi czytnik.

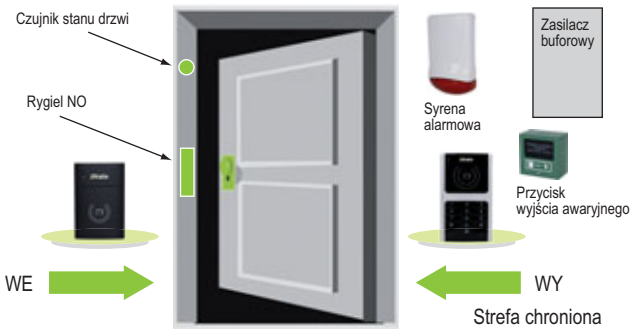
Kontroler KZ-1000 może pracować w trybie autonomicznym (programowanie za pomocą klawiatury) lub sieciowym



Rys. 1. Schemat systemu KaDe



Rys. 2. Przejście kontrolowane jednostronnie

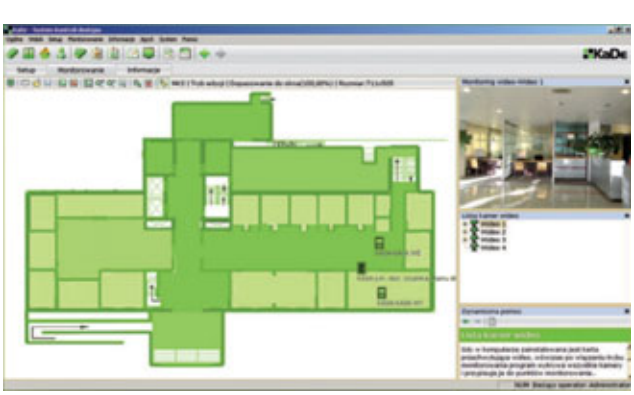


Rys. 3. Przejście kontrolowane dwustronnie

(pod kontrolą programu nadzorczego KaDe-Soft V1 na PC). W trybie sieciowym przy braku komunikacji z programem zdarzenia związane z dostępem oraz alarmy są zapisywane w pamięci kontrolera. Pojemność bufora to 8200 rekordów z funkcją kasowania najstarszych pozycji. Identyfikacja użytkownika odbywa się przez prezentację karty lub przez przedstawienie karty i wprowadzenie kodu PIN. Uprawnienia związane z dostępem mogą podlegać ograniczeniom poprzez zdefiniowanie poziomów dostępu oraz terminarzy tygodniowych i dni świątecznych.

Urządzenie integruje w sobie następujące elementy:

– moduł kontrolera jednego przejścia,
– czytnik kart zbliżeniowych w standardzie 125 kHz ISO UNIQUE,
– klawiaturę do wprowadzania kodu PIN i programowania oraz przycisk dzwonkowy,
– sygnalizator optyczny (diody LED) i akustyczny (brzęczyk),
– czujnik antysabotażowy.
– Moduł kontrolera zawiera:
– zaciski do podłączenia zasilania (+12 V, 110 mA),
– port komunikacyjny typu RS232 do bezpośredniego połączenia z programem nadzorczym na komputerze,
– port komunikacyjny typu RS485 do podłączenia magistrali komunikacyjnej,
– port drugiego czytnika do kontroli dwustronnej (format: 26 bitów, Wiegand),
– wejście linii dozorowej do podłączenia czujnika stanu drzwi,
– wejście linii dozorowej do podłączenia przycisku wyjścia,
– wyjście przekaźnikowe do sterowania zamkiem elektrycznym,
– wyjście przekaźnikowe do sterowania sygnalizatorem alarmowym,
– zestaw mostków do ustawiania trybu komunikacji.



Rys. 4. Pulpit operatora systemu KaDe w trybie monitorowania

Wszystkie wymienione elementy zamontowane są w estetycznej obudowie. Kontroler KZ-1000 przeznaczony jest do instalacji wewnątrz pomieszczeń. Jeżeli kontrolujemy wejście z zewnątrz budynku, należy do kontrolera podłączyć czytnik w wykonaniu zewnętrznym (np. C-10). Zainteresowanych bardziej szczegółowymi informacjami o parametrach kontrolera odsyłam do jego instrukcji.

Elementy systemu – czytniki

Seria czytników kart zbliżeniowych obejmuje następujące modele:

– C-10,
– C-20,
– C-60,
– C-70.

Modele te różnią się obudowami, ale są identyczne pod względem parametrów elektrycznych. Zróżnicowanie obudów umożliwia dopasowanie wybranego modelu do miejsca i sposobu montażu oraz do kolorystyki wnętrza. Model C-20 wyposażony jest w klawiaturę kodową. Wszystkie modele przystosowane są do montażu wewnątrz i na zewnątrz pomieszczeń. Odległość czytnika od kontrolera nie powinna przekraczać 60 metrów. Zasięg odczytu z kartami standardowymi wynosi do 10 cm. Wszystkie wyżej wymienione modele mają standardowy 26-bitowy format wyjściowy Wieganda, co umożliwia zastosowanie ich również do innych kontrolerów i w innych systemach, obsługujących ten format. Posiadają wbudowane sygnalizatory (optyczny – LED, i akustyczny – brzęczyk); tymi sygnalizatorami steruje kontroler w przypadku wystąpienia zdarzeń związanych z dostępem lub alarmem.

Zamierzamy nadal rozwijać system KaDe, wprowadzając do oferty wersje oprogramowania z rozszerzoną funkcjonalnością oraz nowe kontrolery standardowe do kontroli jednych, dwojga lub czworga drzwi, obsługujące czytniki identyfikatorów w dowolnej technologii (Mifare, iClass, biometryczne). Dużym zainteresowaniem będą się z pewnością cieszyły kontrolery z portami IP.

Polecam ten system firmom instalacyjnym i klientom, którzy szukają prostego i taniego systemu kontroli dostępu. Radzę również odwiedzić naszą stronę www.aat.pl, gdzie dostępna jest bezpłatna, pełna wersja instalacyjna programu KaDe oraz dokumentacja. Pozwoli to zainteresowanym na bardziej szczegółowe zapoznanie się z tym systemem.

Ryszard Sobierski
AAT Holding

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Rejestrator cyfrowy do zastosowań mobilnych

HDD 2.5" SATA i karta SD

Rejestrator posiada jeden dysk SATA 2.5" umieszczony w wyjmowanej kieszeni. Mocowania dysku twardego oraz samego rejestratora zostały wykonane z wykorzystaniem nowoczesnej, absorbującej wibracje i uderzenia technologii. Dodatkowo kieszeń dysku została wyposażona w gniazdo mini USB umożliwiające bezpośrednie podłączenie dysku twardego do komputera PC, w celu odtwarzania lub kopiowania nagrań zawartych na nośniku. W niskich temperaturach otoczenia, wykraczających poza zakres pracy dysku twardego, rejestracja odbywa się na kartę SD.

Odbiornik GPS

Wbudowany odbiornik GPS, z dołączoną anteną zewnętrzną, pozwala na zapisywanie aktualnych koordynat położenia, a tym samym śledzenie i rejestrację prędkości obiektu. System korzysta z dedykowanej do rejestratora aplikacji E-Viewer oraz serwisu Google Maps, precyzyjnie obrazujących przebytą trasę i prędkość pojazdu.

Czujnik przeciążeń (G-sensor)

Wbudowany czujnik przeciążeń umożliwia wywołanie alarmu rejestratora w przypadku zderzenia, stłuczki czy gwałtownego hamowania. Dzięki jego zastosowaniu, powyższe zdarzenia drogowe mogą zostać zarejestrowane według parametrów zdefiniowanych dla nagrywania alarmowego.

E seria

E-Viewer Compatible

- Quadrupleks: równoczesny zapis, podgląd „na żywo"/odtwarzanie nagrań, kopiowanie nagrań i połączenie sieciowe
- Prędkość nagrywania do 100 obr/s
- Algorytm kompresji H.264
- Rozdzielczość nagrywania: 720x576, 720x288, 360x288
- Funkcje przed-alarmu i po-alarmu
- Funkcja przechwytywania danych tekstowych z urządzeń fiskalnych
- Możliwość rejestrowania do 4 kanałów audio
- Praca w sieci komputerowej, w tym możliwość połączenia z wieloma rejestratorami jednocześnie oraz wysyłanie wiadomości e-mail o sytuacjach alarmowych
- Auto-diagnostyka systemu z automatycznym powiadamianiem
- Menu w języku polskim
- Mocowanie zapewniające ochronę przed wibracjami i wstrząsami
- Zasilanie: 12 ~ 36 VDC

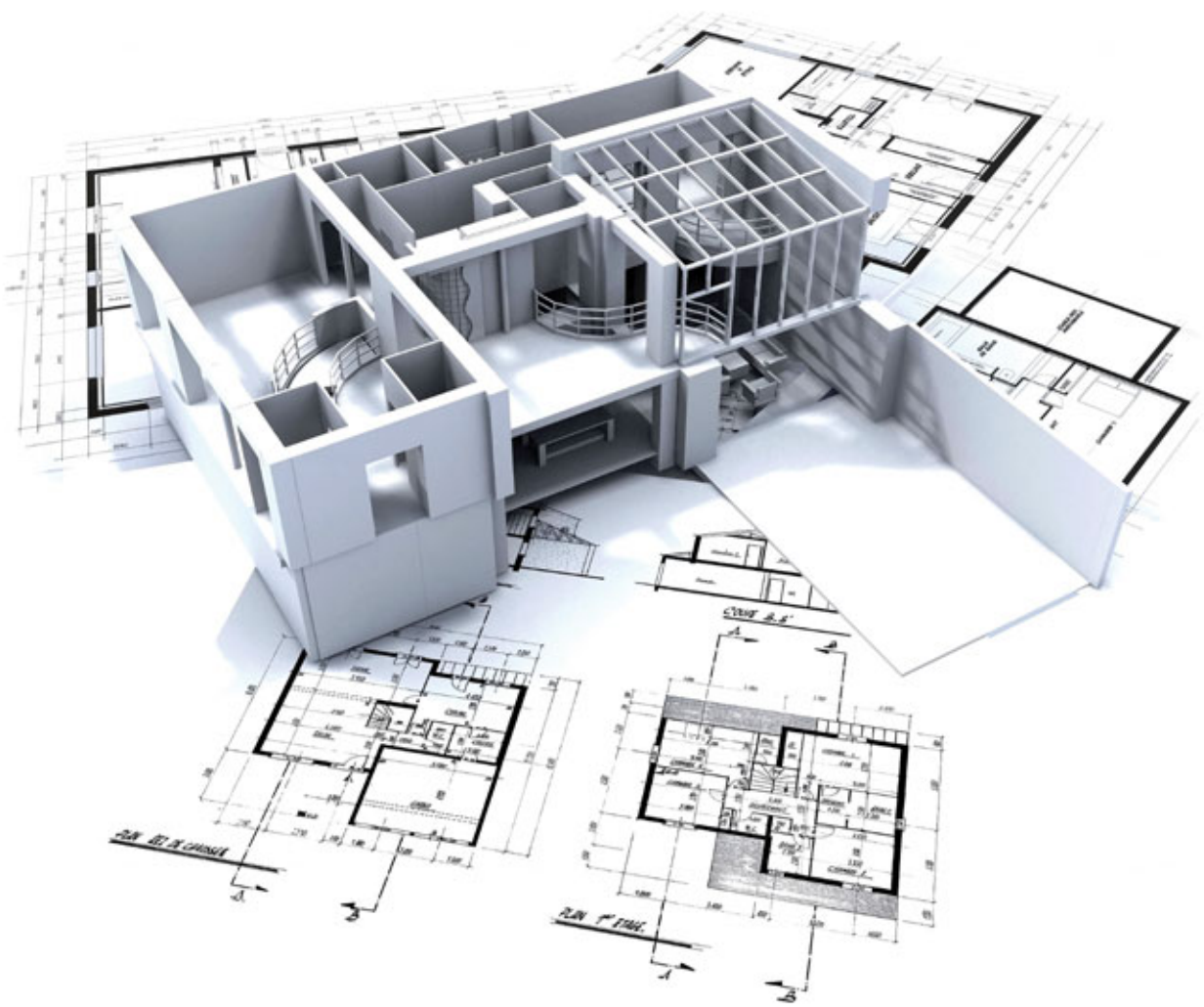
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Integracja systemu sygnalizacji włamania i napadu

z urządzeniami infrastruktury technicznej budynku (część 2)

Adam Rosiński, Jacek Magiera

W drugiej części niniejszego cyklu artykułów przedstawiona jest koncepcja systemu sygnalizacji włamania i napadu dla domku jednorodzinnego. Przedstawiono zarówno wstępne rozmieszczenie zastosowanych urządzeń, jak i konfigurację systemu z wykorzystaniem z wykorzystaniem specjalnego oprogramowania (służącego również do obsługi serwisowej central alarmowych)



1. Koncepcja SSWiN dla domku jednorodzinnego

Jeszcze kilka lat temu profesjonalne instalacje systemów bezpieczeństwa, ze względu na cenę, były montowane tylko w obiektach użyteczności publicznej, biurach dużych firm oraz miejscach zamieszkania bogatych osób. Obecnie wraz z postępem technologicznym cena urządzeń gwałtownie spadła i takie instalacje stały się dostępne dla przeciętnego obywatela. Zamontowanie systemu sygnalizacji włamania i napadu (SSWiN) w domu jednorodzinnym lub mieszkaniu daje użytkownikowi pewne poczucie bezpieczeństwa. Opuszczając miejsce zamieszkania i uzbrajając system, zyskuje on pewność, że pod jego nieobecność nikt niepostrzeżenie nie dostanie się do jego domu. Oczywiście w przypadku wystąpienia zdarzenia alarmowego korzystne jest również powiadomienie odpowiednich służb interwencyjnych (np. agencji ochrony, policji), sąsiada itp.

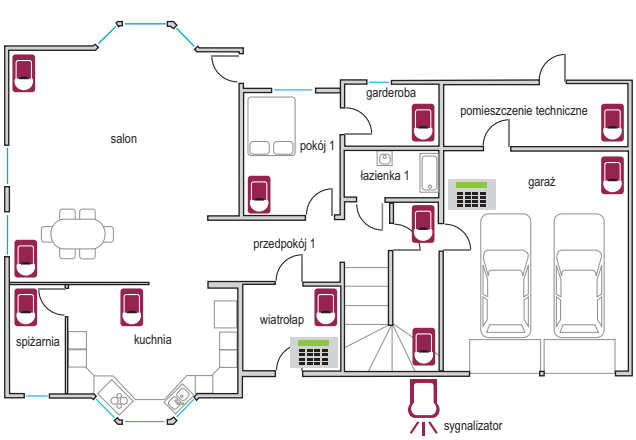
W przyjętym do projektu domu jednorodzinnym przewidziano instalację alarmową w postaci SSWiN. Zdecydowano się na centralę Integra 128 firmy Satel wraz z czujkami i manipulatorami [2]. Urządzenia firmy Satel wybrano przede wszystkim dlatego, że autorzy niniejszego artykułu mają duże doświadczenie w ich stosowaniu. Poza tym Integra 128 jest produktem stosunkowo niedrogim, a producent udostępnia nieodpłatnie aplikacje do programowania central (wszelka dokumentacja techniczna jest dostępna na jego stronie internetowej).

W każdym pomieszczeniu przewidziano co najmniej jedną czujkę ruchu, która sygnalizować będzie obecność w nim ludzi. Każdy otwór okienny i drzwiowy będzie „strzeżony" przez czujnik kontaktronowy. W pomieszczeniach, w których może nastąpić wyciek wody lub gazu, zostaną zainstalowane odpowiednie czujniki. Klawiatury, które umożliwiają użytkownikowi komunikację z centralą, będą zamontowane przy wejściach do domu, tj. w garażu i wiatrołapie oraz na pierwszym piętrze.

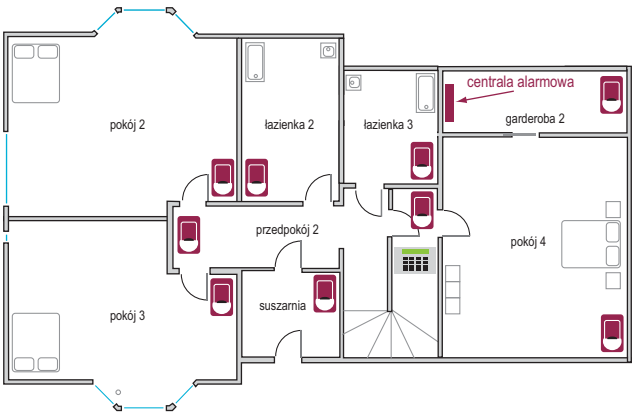
Rozmieszczenie poszczególnych elementów systemu alarmowego w poszczególnych pomieszczeniach przedstawiają rysunki 1 i 2.

Cały system alarmowy będzie się składał z następujących komponentów firmy Satel:

– centrali alarmowej – Integra 128,
– trzech manipulatorów LCD – INT-KLCDR-BL,
– siedmiu ekspanderów wejść – CA-64 E,



Rys. 1. Rozmieszczenie elementów systemu alarmowego – rzut pionowy parteru (źródło: opracowanie własne na podstawie projektu firmy Domus)



Rys. 2. Rozmieszczenie elementów systemu alarmowego – rzut pionowy poddasza (źródło: opracowanie własne na podstawie projektu firmy Domus)

– ośmiu ekspanderów wyjść niskonapięciowych – CA-64 O-OC,
– sterownika radiowego wraz z pilotami – INT-RX z pilotami P-4,
– dwudziestu dwóch dualnych czujek ruchu – SILVER,
– trzydziestu sześciu czujek magnetycznych – do okien K-1, do drzwi K-2,
– czujki gazu ziemnego – DG-1 ME,
– dwóch czujek tlenku węgla (czadu) – DG-1 CO,
– czujki chloroformu (gazu usypiającego) – DG-1 TCM,
– czterech czujek zalania – SD,
– sygnalizatora zewnętrznego optyczno-akustycznego – SP-4001 R,
– obudowy z zasilaczem i akumulatorem.

W wykazie nie uwzględniono agregatu prądotwórczego, który będzie znajdował się na parterze w pomieszczeniu technicznym.

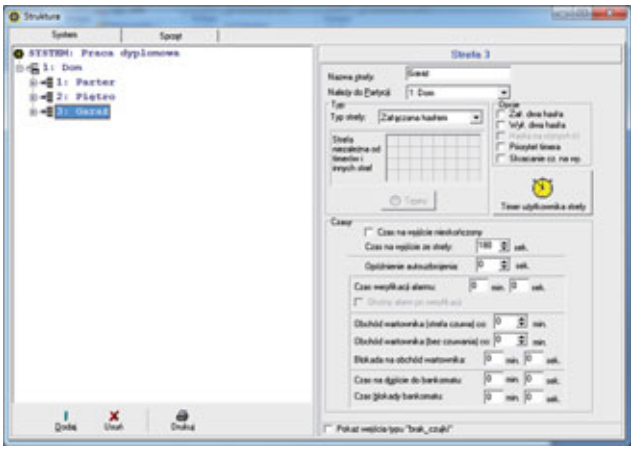
1.1. Konfiguracja SSWiN

Konfigurację całego systemu alarmowego można przeprowadzić za pomocą manipulatora lub komputera z zainstalowanym oprogramowaniem DLOADX firmy Satel, podłączonego do centrali specjalnym przewodem. Ponieważ konfiguracja większego i bardziej rozbudowanego niż standardowy systemu za pomocą manipulatora byłaby kłopotliwa, w naszym przypadku zdecydowano się na wykorzystanie do tego celu komputera PC.

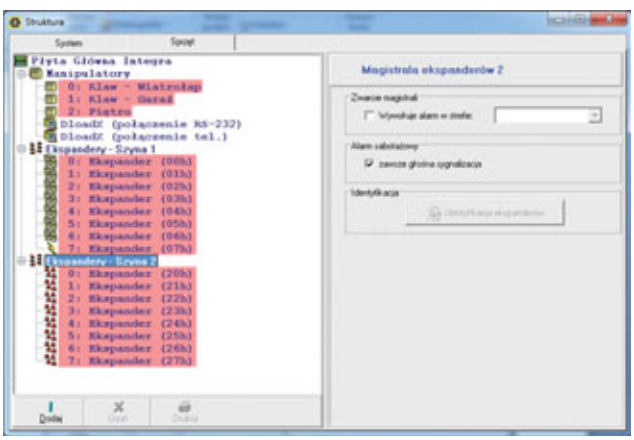
Konfigurację w programie DLOADX (na etapie fazy koncepcji) przeprowadzono „na sucho", tj. bez konieczności posiadania centrali podłączonej do komputera. Po sprawdzeniu wszystkich parametrów konfiguracyjnych można tak przygotowaną bazę danych systemu wgrać do centrali, sprawdzić działanie i wprowadzić ewentualne poprawki, które zaproponowano podczas etapu instalacji urządzeń.

Po uruchomieniu programu konfigurację rozpoczęto od utworzenia partycji głównej oraz dodania do niej trzech stref. Strefy ustalono na podstawie podziału budynku na trzy części (fot. 1), które są od siebie niezależne, czyli:

– garaż,
– parter,
– piętro.



Fot. 1. Widok konfiguracji strefy (źródło: opracowanie własne)



Fot. 2. Lista wszystkich dodanych modułów dodatkowych (źródło: opracowanie własne)

Dzięki takiemu podziałowi uzyskano możliwość zablokowania i odblokowania dostępu tylko do części domu. Na przykład gdy kładziemy się wieczorem do łóżka na poddaszu, możemy załączyć w dozór stref garażu oraz parteru, aby nocą nikt niepostrzeżenie nie dostał się do domu. Na wypadek gdyby zaszła konieczność zejścia w nocy na dół, np. do kuchni, przy schodach na piętrze przewidziano zainstalowanie manipulatora, który umożliwi wyłączenie z dozoru strefy „parter", a po powrocie na górę ponowne jego włączenie. W konfiguracji stref pozostawiono domyślne parametry konfiguracyjne, z wyjątkiem nazw stref oraz czasów opuszczenia stref. Czas opuszczenia strefy po załączeniu jej w dozór oznacza, ile czasu musi upłynąć, aby strefa zaczęła sygnalizować alarm, czyli reagować na naruszenie linii dozorowych. Czasy te ustawiono następująco:

– garaż – 180 sekund,
– parter – 60 sekund,
– piętro – 60 sekund.

Kolejnym krokiem w konfiguracji projektowanego systemu alarmowego jest dodanie wszystkich manipulatorów oraz modułów dodatkowych. Odbywa się to poprzez wybranie opcji „Dodaj" w liście sprzętu i wskazanie odpowiedniego modułu z listy rozwijanej. W naszym systemie dodano:

– trzy manipulatory,
– siedem ekspanderów wejść,
– osiem ekspanderów wyjść,
– jeden moduł obsługi pilotów zdalnego sterowania.

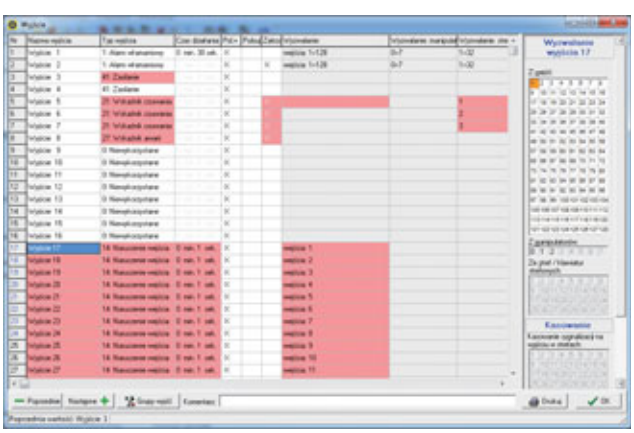
Centrala alarmowa Integra 128 posiada trzy szyny komunikacyjne. Jedna jest przystosowana do obsługi manipulatorów, a dwie kolejne do obsługi modułów rozszerzających. W naszym układzie zastosowano następujący podział (fot. 2):

– do szyny manipulatorów dodano trzy manipulatory,
– do pierwszej szyny ekspanderów dołączono wszystkie urządzenia wejściowe (siedem modułów wejść oraz moduł obsługi pilotów),
– do drugiej szyny ekspanderów dołączono wszystkie urządzenia wyjściowe (osiem modułów wyjść).

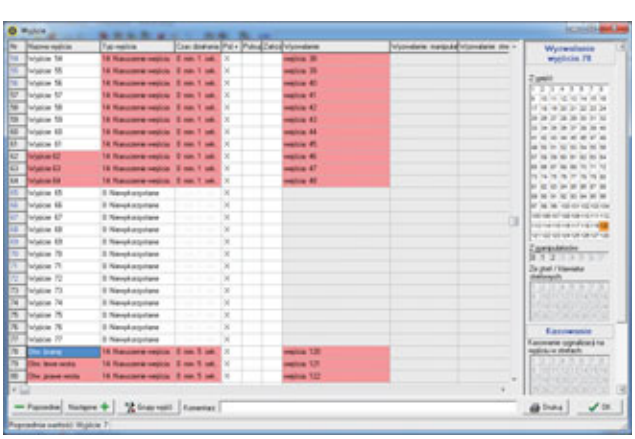
Po dodaniu wszystkich elementów systemu przystąpiono do kolejnego kroku, którym było dodanie i skonfigurowanie wejść w odpowiednich strefach. Wyjścia są dodawane automatycznie po dodaniu modułu rozszerzającego ich liczbę. W naszym systemie zastosowano nazewnictwo wejść wynikające z ich podziału na typy:

– magnes – czujki typu kontaktron,
– ruch – czujki ruchu,
– gaz – czujki gazu.

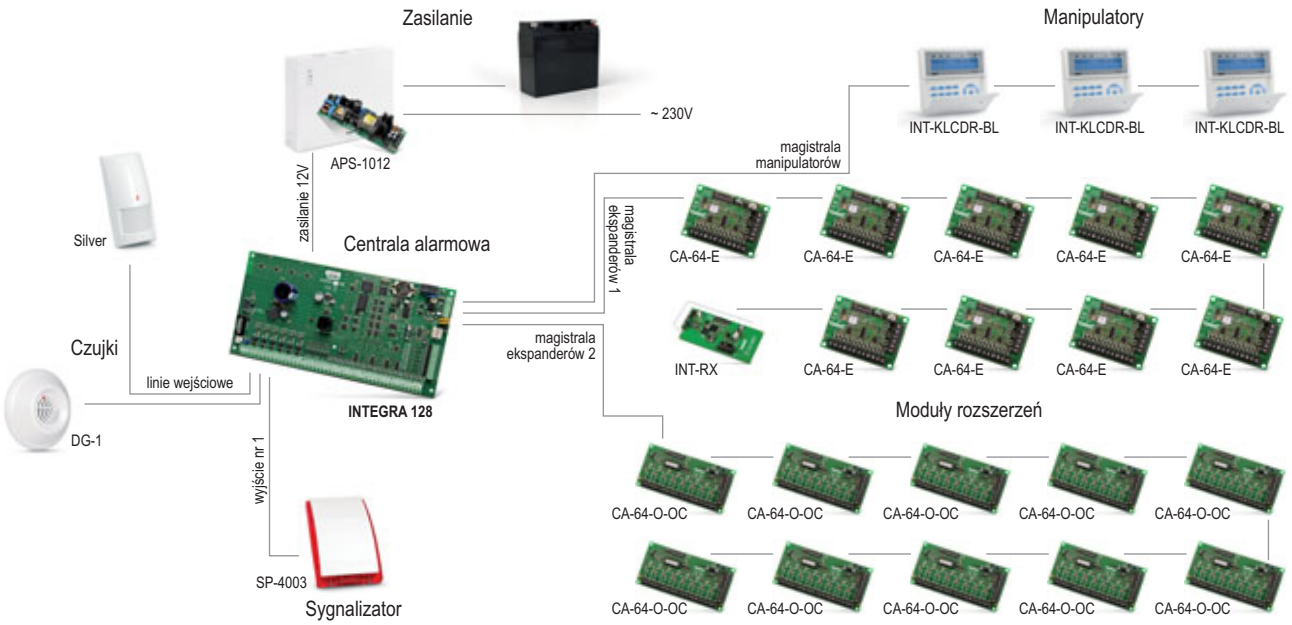
Dodatkowo, w celu usprawnienia diagnostyki całego systemu oraz ułatwienia lokalizacji poszczególnych czujek, zawarto w opisach krótką informację o pomieszczeniu i miejscu, w którym znajduje się czujka . W przypadku czujek zainstalowanych na liniach wejściowych do domu, gdzie trzeba podejść do manipulatora i wpisać kod, określono typ „wejście/wyjście", jednocześnie konfigurując odpowiedni czas na wejście (30 sekund).



Fot. 3. Konfiguracja wyjść z systemu alarmowego, cz. I (źródło: opracowanie własne)



Fot. 4. Konfiguracja wyjść z systemu alarmowego, cz. II (źródło: opracowanie własne)



Rys. 3. Schemat podłączeń urządzeń dodatkowych do centrali alarmowej Satel Integra 128 (źródło: opracowanie własne na podstawie dokumentacji technicznej Satel)

Pozostałe czujki skonfigurowano jako zwykłe, czyli bez żadnej zwłoki. Czujki gazów i wody skonfigurowano jako linie techniczne, działające całą dobę, niezależnie od włączenia dozoru danej strefy.

Czujki ruchu w wiatrołapie i garażu skonfigurowano tak, aby po ich pobudzeniu przy systemie wyłączonym z dozoru we wszystkich manipulatorach rozlegał się przyjemny dla ucha sygnał, zwany gongiem. Gdy wchodzimy, rozlega się gong (lub inny dźwięk) i osoba pracująca w sklepie lub biurze jest informowana o tym, że ktoś właśnie wszedł do środka, nawet jeśli nie widzi bezpośrednio wejścia.

Kolejnym etapem było odpowiednie skonfigurowanie wyjść (fot. 3 i 4). Część z szesnastu wyjść centrali wykorzystano do sygnalizacji włamania, sygnalizacji stanu włączenia dozoru stref oraz sygnalizacji awarii zbiorczej systemu alarmowego. Dla potrzeb integracji ze sterownikiem PLC dalsze wyjścia, począwszy od wyjścia 17 (czyli pierwszego z modułów rozszerzeń), ustawiono jako typ 14 (naruszenie wejścia). Ustalono przyporządkowanie zadziałania kolejnych wyjść do pobudzenia poszczególnych wejść. Jak widać na rysunku, wyjścia 78, 79 i 80 skonfigurowano tak, by działały po pobudzeniu wejść zdefiniowanych wcześniej jako przyciski pilota.

Tak skonfigurowany system po poprawnym podłączeniu wszystkich elementów, wgraniu konfiguracji i uruchomieniu powinien działać prawidłowo. Do jego poprawnej pracy nie jest konieczne skonfigurowanie wszystkich wyjść . Służą one jedynie do integracji systemu alarmowego ze sterownikiem PLC, który steruje instalacjami infrastruktury technicznej budynku (rys. 3).

2. Podsumowanie

W drugiej części niniejszego cyklu artykułów dotyczących integracji systemu sygnalizacji włamania i napadu z urządzeniami infrastruktury technicznej budynku zaproponowano realizację systemu sygnalizacji włamania i napadu. Szczegółowo scharakteryzowano taki system przeznaczony dla domku jednorodzinnego, z uwzględnieniem zastosowania dodatkowych wyjść w celu wykorzystania ich do integracji ze sterownikami PLC.

W części trzeciej zostanie przedstawiona charakterystyka urządzeń infrastruktury technicznej budynku oraz koncepcja integracji systemu sygnalizacji włamania i napadu z urządzeniami infrastruktury technicznej budynku z wykorzystaniem sterowników PLC.

dr inż. Adam Rosiński
inż. Jacek Magiera

Bibliografia

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

Obiekty sportowe pod nadzorem kamer Axis Communications

Agata Majkucińska

Kamery ekip telewizyjnych, dbających o regularne transmisje wydarzeń dla fanów poszczególnych dyscyplin, nie są jedynymi, jakie znajdują się w obiektach sportowych. Obiekty te są bowiem coraz częściej pod całodobowym nadzorem kamer monitoringu, których podstawową funkcją nie jest rejestrowanie zmagań zawodników, lecz zapewnienie bezpieczeństwa kibiców. Co istotne, sukcesywnie wzrasta tu popularność rozwiązań cyfrowych, które w porównaniu z analogowymi gwarantują znacznie wyższą jakość obrazu, szereg funkcji dodatkowych oraz skalowalność. Kamery sieciowe najwyższej klasy, jakie ma w swojej ofercie Axis Communications, są wyposażone również w inteligentne funkcje detekcyjne. Jak dowiodły ostatnie badania przeprowadzone przez grupę badawczą Lusax przy Uniwersytecie w Lund, w przypadku instalacji systemów złożonych z co najmniej 14 kamer rozwiązania cyfrowe są także bardziej uzasadnione ekonomicznie

Jakość HDTV – skok wzwyż

Poziom bezpieczeństwa kibiców na imprezach sportowych zależy w dużej mierze od możliwości ciągłego i szczegółowego monitorowania wszystkich potencjalnie problematycznych obszarów stadionu: trybun, wejść i wyjść, korytarzy oraz dróg ewakuacyjnych. Z reguły problemy powstają wówczas, gdy ograniczona liczba kamer ma za zadanie monitorować duże powierzchnie, a jednocześnie zapis ma być na tyle dokładny, by pozwolił na identyfikację osób w przypadku odnotowania sytuacji niebezpiecznych lub choćby podejrzanych.

Kamery analogowe w odróżnieniu od cyfrowych mają mniejszy zakres zmian ogniskowej obiektywu, dlatego nie są w stanie rejestrować obrazów z wystarczającą dokładnością, a to w obszarze nadzoru wizyjnego ma kluczowe znaczenie. Właśnie dlatego nowoczesne ośrodki sportowe w coraz większej mierze korzystają z rozwiązań HDTV gwarantujących wysoką rozdzielczość nagrywanego obrazu oraz odpowiednią poklatkowość, co umożliwia rejestrację szczegółów, a dzięki temu bezsprzeczną identyfikację postaci i jednoznaczną ocenę zdarzeń. Dzięki pracy w systemie skanowania progresywnego kamery IP wytwarzają wyraźniejsze i ostrzejsze obrazy nawet w sytuacji monitoringu obiektów ruchomych, np. biegnących osób lub jadących pojazdów. Ponadto, dzięki wysokiej jakości obrazu gwarantowanej przez standard HDTV zapewniają wierne odwzorowanie kolorów. Sprawia to, że w dozorze wizyjnym imprez sportowych kamery te sprawdzają się wyjątkowo dobrze.

Kolejną zaletą monitoringu wizyjnego HDTV, jest to, że pojedyncze klatki telewizyjne mogą być używane do sporządzania kopii papierowej w niemal fotograficznej jakości. Może być to decydujące, gdy materiał ma być wykorzystywany np. jako dowód w sądzie.

Fot. 1. AXIS Q1755

Kamery AXIS Q1755-E podnoszą poprzeczkę

AXIS Q1755 to pierwsza kamera sieciowa klasy HD, wprowadzona na rynek w styczniu 2009 r. Jest ona przystosowana do pracy zarówno w dziennych, jak i w nocnych warunkach oświetleniowych. Obecnie w ofercie Axis Communications znajduje się także model AXIS Q1755-E, zaprojektowany z myślą o wymagających instalacjach zewnętrznych i wyposażony w unikalną funkcję Arctic Temperature Control, która umożliwia bezpieczne włączenie kamery nawet przy bardzo niskiej temperaturze otoczenia (do –40°C), np. po awarii zasilania. Kamery AXIS Q1755-E oferują wyraźny, ostry obraz o rozdzielczości HDTV 1080i lub 720p, zgodny ze standardami SMPTE 274M i 296M, które poza rozdzielczością dotyczą jeszcze odwzorowania kolorów, formatu (16:9) i poklatkowości. Dzięki temu świetnie sprawdzają się w ochronie obszarów, które wymagają dużej szczegółowości obrazu, w tym także obiektów sportowych, takich jak hale czy stadiony.

Kamery AXIS Q1755-E, z 10-krotnym zoomem optycznym i 12-krotnym zoomem cyfrowym, dysponują funkcją automatycznej regulacji ostrości. Dzięki temu umożliwiają natychmiastowe uzyskanie żądanego pola widzenia z precyzyjnie ustawioną ostrością. Aby ułatwić przechowywanie materiału wizyjnego i zwiększyć elastyczność instalacji, model ten jest wyposażony w gniazdo kart pamięci SD/SDHC. AXIS Q1755-E obsługuje przesyłanie wielu oddzielnie konfigurowalnych strumieni wizyjnych w formatach H.264 i Motion JPEG. Format H.264 optymalizuje zapotrzebowanie na pasmo sieciowe i pamięć masową bez wpływu na jakość obrazu. Obsługa funkcji *Power over Ethernet* umożliwia zasilanie kamer przez sieć komputerową, eliminując konieczność układania dodatkowych kabli, a tym samym obniżając koszty instalacji.

Co więcej, kamery AXIS Q1755-E mają zaimplementowane inteligentne funkcje detekcyjne, takie jak zaawansowane wykrywanie ruchu, analiza dźwięku oraz wykrywanie prób ingerencji w ich działanie. Są również wyposażone w funkcję „wartownika" (*tzw. gatekeeper*), która automatycznie przybliża obraz w razie wykrycia ruchu w monitorowanym obszarze, po czym oddala go po upływie określonego czasu.

Parma – tylko najlepsi

Z zalet kamer AXIS Q1755 skorzystali już menedżerowie włoskiego klubu piłkarskiego FC Parma, którzy wprowadzili system nadzoru wizyjnego na stadionie Tardini w Parmie. Aby tamtejszy monitoring był skuteczny i pewny, musiał zostać wdrożony na bazie sprzętu najwyższej jakości, dostarczającego wyraźne, ostre obrazy w każdych warunkach. Głównym celem było zagwarantowanie maksymalnie wysokiego poziomu bezpieczeństwa i komfortu w obiekcie, w którym odbywa się większość imprez organizowanych przez klub, począwszy od meczów, aż po spotkania menedżerów drużyny. *Podczas opracowywania projektu dokonaliśmy wyboru najważniejszych parametrów sprzętu, jaki chcieliśmy zainstalować, oszacowaliśmy też odległości na stadionie, aby zapewnić właściwe kąty obserwacji monitorowanych obszarów. Dzięki takim cechom, jak elastyczność i szeroka funkcjonalność, kamery AXIS Q1755 okazały się doskonałym wyborem* – stwierdziły władze klubu.

Transmisja na żywo

Kluczowe i naturalne zadanie systemów monitoringu wizyjnego to podniesienie poziomu bezpieczeństwa danego obiektu. Inną rolą, zyskującą obecnie na znaczeniu, jest umożliwienie zdalnego udziału w rejestrowanych wydarzeniach osobom, które nie mogą ich oglądać na żywo. Coraz częściej bowiem wdrożenie systemu monitoringu wizyjnego ma na celu nie tylko zapewnienie bezpieczeństwa i porządku, lecz także udostępnienie transmisji wydarzeń w czasie rzeczywistym w Internecie. Niejednokrotnie ułatwia to promowanie imprez sportowych, które dotychczas nie cieszyły się zbyt dużym zainteresowaniem, były dostępne tylko dla niewielkiej grupy kibiców lub o których niewiele osób wiedziało. Wdrażanie systemu nadzoru wizyjnego daje więc podwójną korzyść: pozwala nie tylko zwiększyć bezpieczeństwo, ale również transmitować i promować wydarzenie

Fot. 2. Konstrukcja stadionu w Kijowie

Fot. 3. Stadion w Parmie

na szeroką skalę, bez ponoszenia dodatkowych kosztów związanych z zatrudnieniem specjalistów, operatorów kamer i montażystów.

Tenis live

Zalety stosowania monitoringu wizyjnego opartego na technologii IP oraz transmitowania wydarzeń sportowych w Internecie doskonale obrazuje przykład turnieju tenisowego Gemax Open. Jego organizatorzy zdecydowali się na instalację systemu składającego się z kamer sieciowych HDTV Axis, oprogramowania zarządzającego materiałem wizyjnym Netavis Observer oraz urządzenia NVR Neteye. Rozgrywki tenisowe transmitowano na żywo za pomocą kamer sieciowych AXIS Q1755 HDTV z kompresją H.264.

Szczegóły widoczne z dystansu

Najnowsze rozwiązania z zakresu nadzoru sieciowego są projektowane tak, by spełniały indywidualne oczekiwania klientów reprezentujących różne branże i mających zróżnicowane wymagania. Stąd bardzo ważne jest określenie zadań, jakie system ma realizować, oraz dopasowanie modelu kamer i ich funkcjonalności do miejsca, w którym mają być zainstalowane. Kamery megapikselowe i HDTV oferują rozbudowane funkcje nadzoru wykorzystujące kilkunasto- czy nawet kilkudziesięciokrotne powiększenia optyczne, umożliwiające np. odczytanie numerów rejestracyjnych samochodów z odległości kilkuset metrów. Zatem takie modele jak AXIS P1346 czy AXIS P5532 najlepiej sprawdzą się na parkingach bądź w długich korytarzach prowadzących na trybuny lub murawę. Pozwolą też obserwować szczegóły przebiegu rozgrywek nawet ze znacznych odległości.

AXIS P5532 – rekord pobity

Sieciowa kamera kopułkowa AXIS P5532, wyposażona w funkcję PTZ (*pan-tilt-zoom*), 29-krotny zoom optyczny i 12-krotny zoom cyfrowy z automatycznym ustawianiem ostrości, świetnie sprawdza się w instalacjach wymagających wysokiej wydajności, doskonałej jakości obrazu i zaawansowanego zarządzania zdarzeniami. Dzięki stopniu ochrony IP-51, zabezpieczeniu przed pyłem i wodą oraz zasilaniu w systemie *High Power over Ethernet* kamera AXIS P5532 może zostać łatwo zainstalowana w miejscach, w których konkurencyjne modele nie spełniałyby swoich funkcji.

Dzięki zastosowaniu automatycznie usuwanego filtra podczerwieni kamera AXIS P5532 zapewnia doskonałą jakość obrazu zarówno w dziennych, jak i w nocnych warunkach oświetleniowych. Opcja *Auto-flip*, dostępna w modelu AXIS P5532, pozwala na stałe śledzenie obiektów przemieszczających się bezpośrednio pod kamerą, z zachowaniem pola obserwacji w zakresie 360°.

Unikatowa funkcja „wartownika" – *gatekeeper* – sprawia, że kamera może automatycznie ustawić się w konkretnym położeniu, aby odczytać np. treść tablic rejestracyjnych pojazdu lub rozpoznać twarz osoby po wykryciu ruchu w określonym obszarze, a następnie – po zdefiniowanym czasie – powrócić do pierwotnego położenia.

Profesjonalne wdrożenie na Euro 2012

System nadzoru wizyjnego Axis, oparty na technologii IP, sprawdza się doskonale nie tylko w bieżącym rejestrowaniu przebiegu imprez sportowych czy też zapewnianiu bezpieczeństwa kibicom zgromadzonym na trybunach. Na ciekawe jego wdrożenie zdecydowano się podczas budowy Stadionu Narodowego w Kijowie, wznoszonego na potrzeby Mistrzostw Europy w Piłce Nożnej. Aby pokazywać postępy w budowie obiektu, na placu budowy zainstalowano kamery sieciowe AXIS Q1755, dysponujące kompresją H.264, które przesyłają obrazy przez wewnętrzną sieć UNTC do dedykowanego serwera wizyjnego. Serwer ten przekształca następnie strumienie materiału wizyjnego i retransmituje je na potrzeby zamieszczenia w Internecie. Dzięki temu każdy internauta może w dowolnym momencie odwiedzić stronę WWW z transmisją i sprawdzić postępy w budowie stadionu na Euro 2012. Wdrożenie spotkało się z bardzo dużym zainteresowaniem – w ciągu zaledwie trzech miesięcy stronę z materiałem transmitowanym na żywo odwiedziło ponad milion osób.

System na medal

Wdrażanie w obiektach sportowych systemów nadzoru wizyjnego bazujących na technologii IP spotyka się z coraz większym uznaniem, zarówno wśród sportowców i pracowników, jak i wśród kibiców. Ukraińska inicjatywa pokazywania na żywo postępów w budowie jednego ze stadionów spotkała się również z aprobatą ze strony specjalistów ukraińskich i europejskich, a także otrzymała liczne nagrody, np. EEBC Highlight 2009 Awards w kategorii „Najlepsze rozwiązanie technologii bezprzewodowych".

Agata Majkucińska
Key Account Manager
Axis Communications

full internet control.

ULISSE NETWORK-CAM

System PTZ dla **kamer sieciowych IP** - idealne rozwiązanie obserwacji wideo w aplikacjach zewnętrznych.

www.videotec.com

VIDEOTEC

Czy już czas,
by na poważnie rozpatrywać wykorzystanie sieci IP?

James Smith

Piotr Rogalewski, kierownik zespołu przedsprzedaży dla Polski i krajów bałtyckich firmy Samsung Techwin Europe, stawia w artykule pytania, które zwykli sobie zadawać użytkownicy systemów dozorowych w początkowej fazie planowania swoich instalacji. Czy architektura wizyjnego systemu dozorowego powinna bazować na czysto sieciowej strukturze IP, czy też konwencjonalna technologia analogowa jest nadal zdolna dostarczyć wszystko to, czego oczekuje użytkownik?

Dalsze pytania, dalsze odpowiedzi

Pytanie, z którym moi koledzy i ja spotykamy się najczęściej, to: „Powyżej jakiej progowej liczby kamer warto rozważać wykorzystanie systemów bazujących na rozwiązaniach sieciowych, a nie na konwencjonalnej strukturze analogowej?”. Część osób twierdzi, że jest to dwanaście kamer, część uważa, że trzydzieści; jednak w rzeczywistości nie ma prostej odpowiedzi na tak postawione pytanie. Istnieje wiele czynników, które powinny być wzięte pod uwagę, a większość z nich jest zależna od wymagań stawianych przez użytkownika.

Celem tego artykułu jest zasugerowanie pewnych pytań, które projektant systemu musi sobie postawić, zanim podejmie decyzję dotyczącą wyboru sieciowej lub niesieciowej struktury systemu. Pytania są następujące:

– Czy system będzie obsługiwany przez wielu operatorów w trybie całodobowym, a jeśli tak, to czy wszystkie stanowiska obserwacyjne będą umieszczone w tym samym pomieszczeniu kontrolnym?
– Czy poza personelem zgromadzonym w pomieszczeniu kontrolnym inni użytkownicy, w ramach swoich uprawnień, będą korzystać z zewnętrznego dostępu do bieżących obrazów z kamer lub do zarejestrowanych nagrań?
– Czy system dozorowy będzie wykorzystywany do innych celów, nie związanych z bezpieczeństwem obiektu, na przykład do kontroli przestrzegania zasad bezpieczeństwa i higieny pracy, kontroli ruchu pieszego i samochodowego itp.?
– Czy w szczególnych przypadkach, wymagających dokładniejszej obserwacji, niezbędny będzie dostęp do obrazów o bardzo wysokiej rozdzielczości, umożliwiających rozpoznanie lub nawet identyfikację osób na całym obserwowanym obszarze, czy też wystarczające okażą się obrazy o jakości pozwalającej jedynie na stwierdzenie zaistnienia danego zdarzenia?
– Czy wymagana będzie ciągła rejestracja obrazów ze wszystkich kamer (24 godziny na dobę, siedem dni w tygodniu)?
– Czy wymagane będzie przechowywanie nagrań przez tydzień, miesiąc, dłuższy okres?
– Jaka jest przepustowość istniejącej sieci IP?
– Czy administrator sieci zezwoli na wykorzystanie części dostępnych zasobów sieciowych do transmisji danych niezbędnych do obsługi systemu dozorowego?

Fot. 2. SND-5080

– Czy oczekuje się, by system dozorowy współdziałał z innymi systemami bezpieczeństwa, takimi jak system kontroli dostępu, sygnalizacji włamania, ochrony obwodowej itp.?

Po uzyskaniu odpowiedzi na te oraz inne pytania, specyficzne dla wymagań dotyczących działania systemu, projektant dysponuje danymi pozwalającymi na zasugerowanie struktury systemu spełniającej te wymagania.

Rozwiązania

Systemy dozorowe bazujące na technologii IP mają następujące zalety:

– Obniżenie kosztów okablowania, w tym możliwość wykorzystania istniejącej sieci. Pojedynczy kabel sieciowy może służyć do transmisji wizji, fonii, danych telemetrycznych oraz do zasilania urządzeń metodą PoE *(Power over Ethernet)*.
– Możliwość sterowania systemu i monitorowania go z dowolnej lokalizacji dysponującej dostępem do sieci.
– Elastyczność – nagrania obrazów o strategicznym znaczeniu można przechowywać w dowolnych lokalizacjach, a odtwarzać za pomocą komputerów PC, obsługiwanych przez wielu użytkowników dysponujących odpowiednimi uprawnieniami. Możliwość utworzenia wielu stanowisk, w których prowadzona jest jednoczesna rejestracja i archiwizacja obrazów, zapewnia osiągnięcie wysokiej nadmiarowości systemu.

Fot. 1. SRD-1670D

– Korzyści wynikające ze stosowania kamer sieciowych najnowszej generacji, odznaczających się wysoką rozdzielczością.

Najczęściej jednak najbardziej opłacalne i najlepiej dostosowane do celu, jakiemu mają służyć, są systemy hybrydowe, wykorzystujące zalety obu technologii. Systemy hybrydowe pozwalają na jednoczesne wykorzystanie kamer sieciowych i analogowych oraz sterowanie nimi za pośrednictwem tych samych urządzeń. Nowe kamery mogą być wprowadzane do systemu bez konieczności układania długich tras kablowych.

Postęp technologiczny w dziedzinie konstrukcji kamer i rejestratorów wizyjnych, z jakim mamy ostatnio do czynienia, faworyzuje hybrydowe podejście do budowy systemów dozorowych. Przykładowo układy DSP z serii WiseNet1, stosowane w wielu powszechnie dostępnych kamerach analogowych, wykorzystują technologię idealną dla systemów hybrydowych. Dotyczy to tych właściwości kamer, które pozwalają na zaoszczędzenie czasu i kosztów związanych z ich instalacją – np. jednoczesne udostępnienie wyjść BNC i Ethernet umożliwia transmisję sygnału wizyjnego zarówno przez kable koncentryczne, jak i przez sieć.

Metody kompresji H.264, MPEG4, MJPEG i JPEG, którymi dysponują układy DSP z serii WiseNet1, stwarzają użytkownikom możliwość jednoczesnej transmisji obrazów do różnych lokalizacji, z różnymi poklatkowościami i rozdzielczościami, włączając w to formaty obrazu: 1,3 megapiksela (1280x1024), HD (1280x720), QVGA (320x240), SVGA (800x600) i VGA (640x480).

Możliwość swobodnego wyboru z tak różnorodnego zestawu metod kompresji oraz rozdzielczości obrazów sprawia, że wielu różnych użytkowników, zgodnie ze swoimi uprawnieniami, może jednocześnie przeglądać bieżące obrazy z kamer w jednej z lokalizacji, rejestrować te same obrazy w innej lokalizacji, a także przeglądać zarówno bieżące obrazy z kamer, jak i zarejestrowane nagrania z użyciem smartfonu. Nieruchome obrazy w formacie JPEG, składające się na dokumentację jakiegoś wydarzenia, mogą być dołączane e-maili stanowiących powiadomienie o alarmie; w tym samym czasie możliwy jest zapis ruchomych obrazów w trybie prealarmowym i postalarmowym na karcie pamięci SD zainstalowanej wewnątrz kamery.

Jedną z najbardziej efektownych właściwości układów DSP z serii WiseNet1 jest inteligentna analiza treści obrazu, obejmująca wykrywanie znikania lub pojawiania się obiektów, przekraczania wirtualnych linii, a także wchodzenia i wychodzenia osób. Układy te dysponują również funkcją wykrywania prób sabotażu na podstawie analizy zmian sceny obserwowanej przez kamerę. Dotyczy to takich działań, jak zamalowywanie przedniej soczewki obiektywu farbą w sprayu lub ręczne obracanie kamery, przez co zmienia się jej pole widzenia.

Fot. 3. SPE-100 FS2

Fot.4. SNB-5000

Kamery wyposażone w układy DSP z serii WiseNet1 DSP są przeważnie zbudowane w oparciu o przetworniki CMOS o rozmiarach 1/3" z progresywnym skanowaniem obrazu. Pozwala to na uniknięcie zniekształceń w odwzorowaniu szybko poruszających się obiektów (rozmycia ich krawędzi), typowych dla kamer CCTV ze skanowaniem międzyliniowym.

Dwukierunkowa transmisja dźwięku stwarza możliwość interaktywnej komunikacji głosowej pomiędzy obszarem, w którym zainstalowana jest kamera, a pomieszczeniem kontrolnym.

Hybrydowa rejestracja cyfrowa, dostosowana do zastosowań sieciowych

Rejestratory DVR i NVR najnowszej generacji są głęboko osadzone w hybrydowych rozwiązaniach systemów dozorowych. Dysponując wydajną kompresją H.264, zapewniają wysoką jakość rejestrowanych obrazów, z jednoczesnym ograniczeniem wymagań dotyczących niezbędnej przestrzeni dyskowej i pasma sieciowego.

Dostępne są modele rejestratorów czterowejściowych, ośmiowejściowych lub szesnastowejściowych, przy czym każdy z nich oferuje pełną listę właściwości przyjaznych dla instalatora i użytkownika, pozwalających na dobór typu urządzenia najlepiej dostosowanego do wymagań użytkowych. Przykładowo dane tekstowe przechwytywane z urządzeń ATM, POS lub kontroli dostępu mogą być zapisywane wraz z materiałem wizyjnym i w dowolnym momencie odtwarzane.

Wykorzystanie podwójnych kodeków pozwala na wytworzenie odrębnych strumieni wizyjnych, umożliwiających rejestrację obrazów o wysokiej jakości oraz optymalizację strumieni wizyjnych przeznaczonych do transmisji. Wbudowany w kamerę serwer sieciowy realizuje funkcje przeglądania bieżących obrazów i odtwarzania nagrań z możliwością wyszukiwania wydarzeń alarmowych za pomocą standardowej przeglądarki internetowej.

James Smith
Samsung Techwin Europe
Tłumaczenie: Redakcja

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

BEZPIECZNY ZAKUP

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

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

Bosch HD
Ewolucja, a nie rewolucja

Jan T. Grusznic

Rozdzielczość jest i zawsze była wyznacznikiem jakości w telewizji dozorowej. Choć o jakości obrazu decydują także inne wartości, jak dynamika i głębokość bitowa (liczba bitów wykorzystanych do zakodowania informacji o barwie i o odcieniu szarości), to właśnie rozdzielczość jest uznawana przez rynek za wartość zapewniającą lepszą lub gorszą rozróżnialność szczegółów. Dotychczas ciągły rozwój technologiczny w systemach analogowych powodował zwiększanie wartości tego parametru zarówno w kamerach, jak i w wizyjnych systemach zapisu – wszystko po to, aby obraz był zniekształcony w jak najmniejszym stopniu. Gdy osiągnięto granicę możliwości rozwoju technologii analogowej, rozpoczęły się poszukiwania wyższych rozdzielczości w dziedzinach przetwarzania obrazu cyfrowego

Narodziny kamer megapikselowych (Mpix) w telewizji dozorowej miały zmienić postrzeganie CCTV jako rozwiązania zamkniętego w ujęciu fizycznym i logicznym. Scentralizowana analogowa struktura przetwarzania i wizualizacji obrazu narzucała na ogół konieczność prowadzenia dozoru wizyjnego tylko z jednego punktu. Wszelkie próby decentralizacji skutkowały relatywnie dużym wzrostem kosztów przy jednoczesnym niewielkim stopniu rozproszenia systemu. Dodatkowo każde wydłużenie i przekształcenie toru transmisji sygnału powodowało dalszą degradację rozdzielczości. W ujęciu *stricte* cyfrowym bezpośrednia digitalizacja obrazu bez zbędnego przejścia w sygnał analogowy gwarantowała lepszy obraz bez niepotrzebnych strat jakości, jakie następują podczas konwersji obrazu w układzie kamera – enkoder. Wykorzystanie sieciowych metod transmisji zapewniało uzyskanie powtarzalnych wyników w dziedzinie rozpoznawalności szczegółów obrazu, niezależnie od lokalizacji pomieszczenia kontrolnego, nawet znacznie oddalonego geograficznie od chronionego obiektu. Brak wyraźnych ograniczeń technologicznych w wytwarzaniu przetworników o większej liczbie elementów światłoczułych powodował, że obraz o bardzo wysokiej rozdzielczości przestał być fikcją. *De facto* w tym okresie powstała nowa gałąź CCTV, wykorzystująca konstrukcję aparatów fotograficznych dopasowaną do wymagań telewizji dozorowej. Gdy zatem na targach IFSEC w 2006 roku zobaczyłem po raz pierwszy kamerę HD w otoczeniu mocno już wtedy zarysowującej się konkurencji kamer megapikselowych, nie dawałem jej dużych szans na przetrwanie. Właściwie byłem przekonany, że rozwiązania megapikselowe wchłoną takie wynalazki jak kamery o rozdzielczości HD ze względu na ograniczenia, jakie z definicji stawia ta technologia. Trudno jest bowiem porównywać obraz o wymiarach 1920×1080 pikseli z obrazem z kamery o rozdzielczości 8 megapikseli. Z perspektywy pięciu lat już wiem, w jak wielkim byłem błędzie.

Rozwiązania określane jako megapikselowe nie mają zdefiniowanego standardu dotyczącego rozmiarów i proporcji boków obrazu; od początku swojego istnienia stanowią niezależny i zarazem specyficzny kierunek w rozwoju wizyjnych systemów dozorowych, na ogół bez możliwości integracji z istniejącymi systemami CCTV. W niektórych kamerach megapikselowych stosowana jest mało wydajna kompresja JPEG wymagała stosowania dużo większych pojemności dyskowych do archiwizacji materiału niż w systemach

analogowych lub SD[1] IP. W warunkach niedostatecznego oświetlenia oraz w przypadku scen o dużych zmianach natężenia oświetlenia słabe parametry kamer megapikselowych – w porównaniu z kamerami SD – wzbudzały poważne wątpliwości co do zasadności ich stosowania w systemach zabezpieczeń. Z drugiej strony istniał wymóg korzystania z wyższych rozdzielczości.

Uruchomienie w 2004 roku telewizji programowej nadawanej w technologii HD zainicjowało działania na rzecz jej wykorzystania w systemach zabezpieczeń[2]. Płynny obraz o poprawnej reprodukcji kolorów, wysokiej dynamice stanowił poważną alternatywę dla kamer megapikselowych, które w zasadzie nie wytwarzały ruchomego obrazu, lecz serię następujących po sobie zdjęć. Standaryzacja formatu HD zapewniała dostosowanie pozostałych technologii zapisu i wizualizacji do parametrów ustanowionych w 2002 roku przez ITU-R (*International Telecommunication Union – Radiocommunication Sektor*, czyli Międzynarodowy Związek Telekomunikacji – Sektor Radiokomunikacji)[3]. W efekcie branża zabezpieczeń zainteresowała się rozwiązaniami HD, co stanowiło naturalną ewolucję wizyjnych systemów dozorowych, nie zaś rewolucję w postaci gwałtownego zwiększenia liczby pikseli, błędnie utożsamianego z poprawą jakości obrazu.

Synergia technologii SD i HD

Implementacja standardu HD w systemach Boscha była poprzedzona analizą dotychczasowych doświadczeń. Kamery Boscha są od lat kojarzone z wysoką jakością wykonania i wzorową reprodukcją obserwowanej sceny. Ciągle rozwijana technologia XF Dynamic, wykorzystująca 15-bitowe przetwarzanie sygnału, gwarantuje prawidłowe odwzorowanie barw i skali szarości oraz poprawną obserwację miejsc o dużej rozpiętości tonalnej (fot. 1). Rozwiązanie to jest doceniane w trudnych i uciążliwych warunkach oświetleniowych, gdzie w kadrze znajdują się jednocześnie miejsca bardzo jasne i bardzo ciemne. Poprzez wydłużenie czasu naświetlania przetwornika (funkcja SensUp) usprawniany jest dozór w nocy, w słabych warunkach oświetleniowych – bez nadmiernego wzrostu zaszumienia obrazu. Wieloletnie doświadczenia w dziedzinie tworzenia obrazu o wysokiej jakości Bosch powiązał z technologią zapewniającą wysoką rozdzielczość. Synergia takiego powiązania zaowocowała powstaniem rozwiązań Bosch HD, gwarantujących reprodukcję poprawnego obrazu o rozdzielczości 720p oraz 1080p niezależnie od warunków oświetleniowych.

Utrzymanie niezmienionej, wysokiej jakości obrazu dostarczanego przez kamery HD oferowanych przez Boscha jest możliwe dzięki wykorzystaniu kompresji H.264 Main Profile, znacznie obniżającej wielkość wyjściowego strumienia wizyjnego bez widocznego wpływu na jakość obrazu. Standard H.264 stanowi innowację wywodzącą się z popularnych standardów kodowania sygnału wizyjnego MPEG-2 oraz MPEG-4. Każdy detal obrazu jest kompresowany bez żadnego uszczerbku na częstotliwości odświeżania. Jest to o tyle ważne, że przy wykorzystaniu formatu HD 720p60 (60 klatek prezentowanych w ciągu sekundy) każda, nawet chwilowa zwłoka spowodowałaby zauważalne zubożenie jakości prezentowanego obrazu. Bosch, wykorzystując kompresję H.264 MP, zredukował wielkość zapisywanego pliku wizyjnego o ponad 80% w porównaniu z formatem Motion JPEG oraz o około 50% w porównaniu z tradycyjnym standardem MPEG-4 Part 2.

Inteligentne wspomaganie

Wysoka rozdzielczość obrazu zwiększa ilość informacji wymagających przetworzenia. Z jednej strony pozytywne jest to, że dzięki rozwiązaniom HD pole dozoru zostało poszerzone. Z drugiej strony w obecnych systemach analogowego dozoru wizyjnego istnieje problem przeciążenia personelu, które wpływa na efektywność jego pracy. Operatorzy systemów CCTV uważają, że liczba monitorów, jaką są w stanie efektywnie kontrolować, to szesnaście lub mniej. Ponad połowa operatorów twierdzi natomiast, że maksymalna liczba waha się od jednego do czterech[4]. Dane uzyskane w wyniku przeprowadzonych doświadczeń wskazują, że wraz ze wzrostem liczby nadzorowanych kamer maleje efektywność pracy obserwatorów próbujących wykryć określone cele (dotyczy to monitoringu w centrach miast). Wnioski te idą w parze z wynikami badań Ticknera i Poultona, którzy porównywali efektywność pracy przy zwiększającej się liczbie monitorów. Przy czterech, dziewięciu i szesnastu monitorach pokazujących bardzo ruchliwe obszary miejskie skuteczność działań operatorów przy wykrywaniu postaci wyniosła odpowiednio 93%, 84% i 64%.

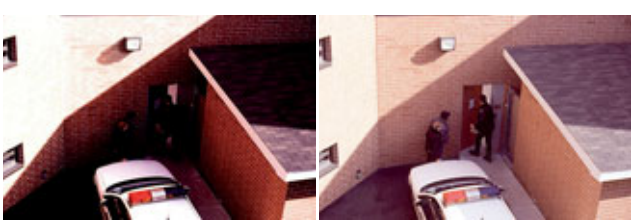
Starając się rozwiązać problem przeciążenia personelu, Bosch kilka lat temu wyposażył swoje kamery w funkcję inteligentnej analizy obrazu – IVA (*Intelligent Video Analysis*). Obecnie dostosował ten algorytm do nowych rozdzielczości, przyczyniając się w ten sposób do skuteczniejszego wykrywania określonych zachowań. Wbudowany w kamery Bosch algorytm IVA jest zdolny nie tylko do detekcji ruchu, ale także do wykrywania określonych obiektów (takich jak porzucony bagaż), kierunku ruchu, a nawet podejrzanych zachowań, np. pozostawania w jednym miejscu przez długi czas. Wszystko analizowane jest w czasie rzeczywistym. Analiza przeprowadzana w kamerach Boscha, w przeciwieństwie do analogicznej analizy przeprowadzanej przez ludzki mózg, działa bez przerwy – kamera nigdy się nie rozprasza, nie nudzi i nie bierze dnia wolnego. Ponadto jest na tyle inteligentna, aby zauważyć modele działań, które niekiedy umykają uwadze nawet najbardziej czujnego operatora, a mogą być interpretowane jako potencjalnie podejrzane.

1) SD – Standard Definition – określenie, które pojawiło się po wprowadzeniu rozwiązań HD i oznacza obraz o rozdzielczości PAL lub NTSC.

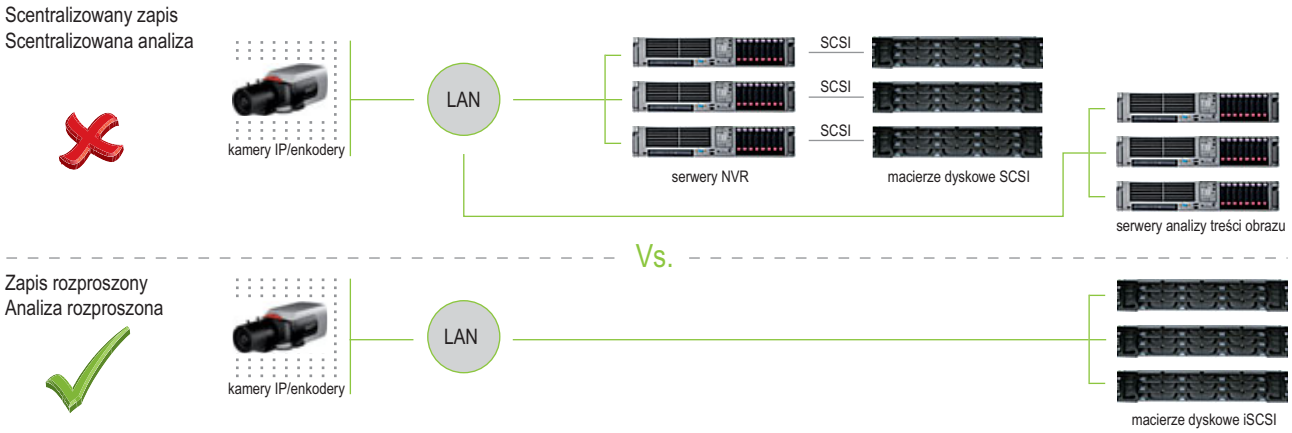
2) 1 stycznia 2004 roku belgijska korporacja Euro1080 uruchomiła kanał HD1, na którym transmitowała koncert noworoczny filharmoników wiedeńskich. Ten dzień przyjęto jako datę oficjalnego wprowadzenia telewizji HD na starym kontynencie.

3) Rekomendacja ITU-R BT.709-5 (04/2002).

4) Mary Lynn Garcia, The design and evaluation of physical protection systems, Butterworth-Heinemann 2001.



Fot. 1. Porównanie efektu dwóch technologii przetwarzania obrazu. Po lewej obraz przetworzony przez filtr 8-bitowy, po prawej – przez filtr 15-bitowy



Rys. 1. Schemat przedstawiający porównanie scentralizowanych i rozproszonych technologii analizy i zapisu obrazu wizyjnego

Są to na przykład: poruszanie się w kierunku odwrotnym do normalnego kierunku ruchu podczas podchodzenia do stanowiska kontroli na lotnisku lub ciągłe powracanie do tego samego miejsca. W takich przypadkach odpowiednia konfiguracja zaawansowanych algorytmów analizy obrazu może powodować wyzwalanie alarmu. Prócz tego dane cyfrowe generowane przez systemy IVA są również zapisywane celem ich późniejszego wykorzystania jako materiału dowodowego. Analiza IVA już teraz redukuje ilość materiału wizyjnego, który musi być przeszukany, ale mimo to proces wyszukiwania jest pracochłonny, jeśli przeprowadza się go ręcznie. Aby ułatwić wyszukiwanie, bardziej zaawansowane algorytmy IVA oferują funkcje zarządzania obrazami. Automatycznie generowane metadane są przesyłane razem z obrazem na nośnik zapisu. Metadane to ciąg znaków składający się zwykle z kilku, słów kluczowych opisujących określone scenariusze zdarzeń,, ,wspomniane modele zachowań oraz informacje na temat obserwowanych obiektów, takie jak proporcje, barwa, inne cechy związane z wyglądem, a ponadto metadane zawierają informacje na temat daty i godziny wystąpienia zdarzenia. Dzięki temu pliki z metadanymi są znacznie mniejsze niż pliki z obrazem. Przeszukanie metadanych za pomocą inteligentnych funkcji (podobnych do tych, które są dostępne w wyszukiwarkach sieciowych) umożliwia znalezienie właściwego obrazu w ciągu kilku sekund, co w przypadku ręcznego wyszukiwania zajęłoby całe dnie, a nawet tygodnie. Wyniki wyszukiwania, ograniczone do określonej liczby trafień, są wyświetlane wraz z przypisanym materiałem wizyjnym, z możliwością dokładnego sprawdzenia pod kątem ich przydatności do dalszych działań.

Cloud computing w CCTV

Analiza obrazu dokonywana przez kamerę umożliwia decentralizację systemu poprzez wykorzystanie mocy obliczeniowej kamer, a nie serwerów z wbudowanym oprogramowaniem analitycznym. Obecnie rozwiązania bazujące na oprogramowaniu przechwytującym strumienie wizyjne są coraz częściej wypierane przez innowacyjne technologie analizy, takie jak IVA. To samo dotyczy systemów zapisu. Innowacje proponowane przez firmę Bosch są związane przede wszystkim z przeniesieniem inicjatora zapisu z punktu centralnego do urządzenia brzegowego (kamery) w myśl trendu zwanego cloud computing. W takim systemie można wyróżnić punkt kamerowy oraz punkt archiwizacji. Nie jest wymagany dodatkowy serwer ani oprogramowanie. System bazujący na takiej technologii wysyła strumień wizyjny z kamery bezpośrednio do pamięci masowej (iSCSI) dostępnej w sieci LAN. Pozwala to na ograniczenie kosztów rejestracji i skrócenie łańcucha urządzeń bezpośrednio zaangażowanych w proces rejestracji. Z klasycznego schematu: kamera IP, serwer, specjalistyczne oprogramowanie i macierz, usunięte zostają serwer i oprogramowanie. Zwiększa to także bezawaryjność całego rozwiązania.

HD według Boscha

Wykorzystanie przedstawionych technologii, sprawdzonych przez instalatorów i użytkowników, spowodowało, że naturalne stało się zaadaptowanie wyższych rozdzielczości do obecnych rozwiązań, a nie odwrotnie. Korzystając z dotychczasowych doświadczeń, Bosch nie zapomniał o masowym wykorzystaniu rozwiązań SD I przygotował bogatą ofertę nowych produktów HD, w pełni kompatybilnych z wykorzystywanymi obecnie technologiami, dzięki czemu możliwe jest czerpanie korzyści ze wszystkich tych standardów, bez konieczności jakichkolwiek kompromisów.

Jan T. Grusznic
CCTV&Video IP Product Manager
Robert Bosch

Fot. 2. Sekwencja ukazująca działanie IVA. Na obraz nałożone zostały metadane w formie graficznej. Kolor żółty oznacza działanie analizy, lecz obiekt nie spełnił warunku (przekroczenie linii ogrodzenia). Kolorem czerwonym oznaczony jest obiekt, który spowodował uruchomienie alarmu. Zielona linia ukazuje trajektorię poruszania się obiektu

125 Bosch 1886–2011

Wizja bez kompromisów

Zarejestruj wszystkie szczegóły z dzienno-nocną kamerą IP - Dinion HD

Do naszej oferty produktów o wysokiej rozdzielczości (HD) dołączyła dzienno-nocna kamera IP - Dinion HD 720p. Dzięki połączeniu rozdzielczości HD i wydajności, z której są znane produkty z serii Dinion, możliwe jest rejestrowanie wyraźnego, szczegółowego obrazu pozwalającego zidentyfikować najmniejsze detale. To łatwe w użyciu, inteligentne urządzenie zapewnia wysoką jakość obrazu, a nowatorska funkcja „Quad Streaming" umożliwia współdziałanie z oprogramowaniem innych firm. Kamera wspiera technologie multicast, transmisję IP wielostrumieniową i zapis na urządzeniach iSCSI. **Z pełną ofertą rozwiązań firmy Bosch w technologii HD, obejmującą kamery obrotowe i stałopozycyjne, oprogramowanie oraz platformy rejestrujące, można zapoznać się pod adresem www.boschsecurity.pl**

BOSCH

Technologia bliżej nas

HDCCTV
Czy czeka nas kolejna rewolucja?

Tomasz Kaliński

Podstawową wadą analogowych systemów CCTV jest niska rozdzielczość, ograniczona standardem PAL. Jedyną drogą do poprawy jakości obrazu okazały się megapikselowe kamery IP, które w opinii wielu ekspertów miałyby stać się powszechne w ciągu kilku najbliższych lat. Jeszcze do niedawna taki pogląd nie podlegał dyskusji, ale dziś można już zastanawiać się nad tym, czy marsz w kierunku megapikselowych kamer IP nie zostanie spowolniony. Przyczyną tego może być nowy standard telewizji, który pojawił się na rynku w ubiegłym roku – HDCCTV. Już w 2011 roku można się spodziewać wprowadzenia na rynek wielu kamer w tym standardzie

Czym jest standard HDCCTV?

HDCCTV został stworzony specjalnie dla systemów telewizji dozorowej. Bazuje na standardzie telewizyjnym HDTV opracowanym przez stowarzyszenie SMPTE (*Society of Motion Pictures and Television Engineers*). W ramach SMPTE powstało wiele standardów przeznaczonych do transmisji obrazu TV w systemie HD, ale najbardziej odpowiedni dla telewizji dozorowej okazał się SMPTE 292M, zwany powszechnie HD-SDI. Jest to właściwie szeregowy interfejs cyfrowy, który pozwala na przesyłanie nieskompresowanego obrazu HD za pomocą popularnych przewodów koncentrycznych RG-59 na odległość do 100 m przy szybkości transmisji do 1,485 Gb/s. Stosując przewody lepszej jakości, np. RG11/U, można zwiększyć dystans o 20–30%. Generalną zasadą jest, aby przewód przy częstotliwości sygnału 1 GHz nie miał większego tłumienia niż 20 dB na odcinku 100 m.

Obecnie standard HDCCTV w wersji 1.0 pozwala na przesyłanie obrazu w dwóch rozdzielczościach: 720p (1280×720) oraz 1080p (1920×1080). Skanowanie progresywne sprawia, że obraz jest najwyższej jakości, porównywalnej z tym, jaki uzyskujemy z Blu-ray DVD. Wersja 2.0, nad którą obecnie prowadzone są prace, zapewni zwiększenie dystansu transmisji do 300 m bez użycia wzmacniaczy, a dodatkowymi atutami będą dwukierunkowa transmisja dźwięku i danych (sterowanie PTZ, wejścia/wyjścia) oraz zasilanie kamery w sposób przypominający do PoE w systemach sieciowych.

Co może przemawiać na korzyść HDCCTV?

HDCCTV to rozwiązanie, które łączy wszystkie najlepsze cechy telewizji analogowej oraz sieciowej (IP). Jakość obrazu z kamery HDCCTV jest dużo lepsza niż oferowana przez kamery IP o podobnych rozdzielczościach. Zastosowane trzy rozwiązania – obraz nieskompresowany, transmisja niepakietowana i niewykazująca opóźnień – sprawiają, że obraz jest krystalicznie czysty i płynny, nawet gdy pochodzi z kamer PTZ znajdujących się w ruchu.

Instalacja kamer HDCCTV wymaga takiej samej wiedzy jak w przypadku kamer analogowych. Nie ma potrzeby przeprowadzania dodatkowych treningów i szkoleń w zakresie LAN, gdy tymczasem wśród instalatorów CCTV niewystarczająca wiedza w zakresie budowy sieci IP jest jednym z czynników hamujących rozwój technologii kamer sieciowych. Ten argument może przekonać wielu integratorów do zastosowania rozwiązań HDCCTV.

Do instalacji kamer HDCCTV można używać takich samych przewodów jak w istniejących analogowych instalacjach CCTV. W wielu przypadkach modernizacja systemu, mająca na celu poprawienie jakości obrazu, nie będzie już wymagała użycia kamer IP oraz budowania niezbędnej sieci LAN, co nie zawsze jest opłacalne i możliwe. Znacznie prostsza budowa kamer HDCCTV sprawia, że są one tańsze od kamer IP, a z czasem będzie można spodziewać się dalszego spadku cen.

Jak rejestrować obraz w HDCCTV?

Do rejestracji obrazu w HDCCTV jest oczywiście niezbędny dedykowany rejestrator, np. NetHybrid HD firmy Alnet Systems. Jest to pierwsze rozwiązanie na rynku pozwalające rejestrować obraz w trzech technologiach (CCTV + IP + HDCCTV) w jednym urządzeniu. Daje to spore możliwości modernizacji oraz rozbudowy każdej instalacji.

Fot. 1. Interfejs aplikacji NetHybrid HD

Rejestratory NetHybrid HD są typu PC Based, czyli pracują jako serwery komputerowe, a obraz jest przechwytywany za pomocą kart. Rejestrator NetHybrid HD występuje w wersjach z czterema, ośmioma, dwunastoma i szesnastoma wejściami HDCCTV. Dodatkowo do każdej z powyższych konfiguracji można dodać kamery IP (cztery, osiem, dwanaście lub szesnaście) oraz karty z wejściami analogowymi (cztery, osiem lub szesnaście). Maksymalna liczba kamer współpracujących z jednym serwerem nie może przekroczyć trzydziestu dwóch. Możemy na przykład skonfigurować system NetHybrid HD 8 AVC 16/400/4IP, który posiada osiem wejść w standardzie HDCCTV, szesnaście wejść analogowych (D1 – 25 kl./s) oraz cztery wejścia IP. Możliwości konfiguracyjne są naprawdę duże i pozwalają precyzyjnie dostosować projekt do wymagań klienta.

Obraz z kamer HDCCTV jest przechwytywany i wyświetlany na monitorze w postaci nieskompresowanej, co daje krystaliczną jakość i płynność niespotykaną w innych rozwiązaniach. Podczas rejestracji karty przechwytujące kompresują sprzętowo obraz HD do standardu H.264, a to zapewnia optymalną zajętość dysku przy wysokiej jakości obrazu.

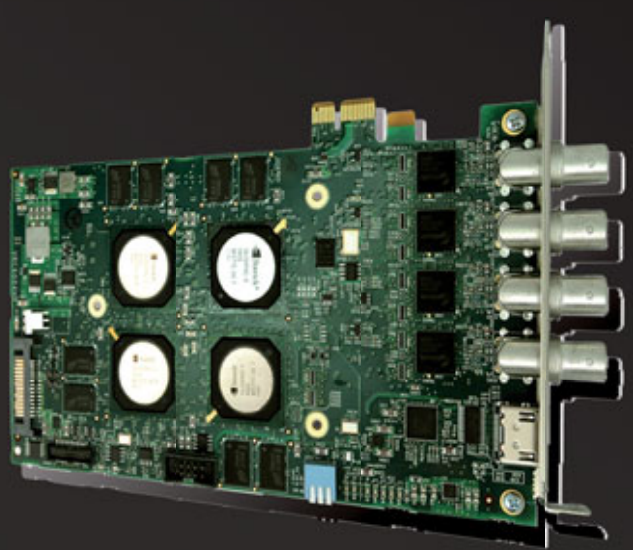
Do rejestracji obrazu z kamer analogowych stosowane są znane z poprzednich wersji NetHybrid karty przechwytujące serii AVC z kompresją sprzętową H.264. Mając tak szerokie możliwości konfiguracji wejść wizyjnych, jesteśmy w stanie prosto i szybko zbudować instalację łączącą trzy technologie wizyjne. Przy budowie serwera należy odpowiednio dobrać płytę główną, tak aby zawierała wystarczającą liczbę gniazd PCIe; na pewno warto przy tym pomyśleć o jednym gnieździe rezerwowym w związku z potencjalną rozbudową. Pojedyncza karta przechwytująca o rozdzielczości HD zawiera cztery wejścia BNC, co oznacza, że system obsługujący szesnaście kamer pracujących w standardzie HD wymaga czterech gniazd PCIe. Jeśli chodzi o obsługę wejść analogowych, mamy do wyboru trzy różne karty: AVC 4 (cztery wejścia), AVC 8 (osiem wejść) oraz AVC 16 (szesnaście wejść). Seria AVC oferuje obraz jakości D1 przy 25 kl./s dla każdego kanału z kompresją sprzętową do formatu H.264. Każda z kart serii HD/AVC ma dodatkowo możliwość dołączenia modułu wejść/wyjść, który standardowo zawiera również interfejs RS485 do sterowania głowicami PTZ.

Do zarządzania rejestratorem zastosowano doskonale znane oprogramowanie używane w systemach NetHybrid/NetStation, a zdalny dostęp zapewniają bezpłatne aplikacje CMS Professional oraz CMS Mobile. Oprogramowanie serwerowe stosowane przez NetHybrid HD to zaawansowane narzędzie do zarządzania obrazem z kamer pracujących we wszystkich dostępnych standardach, nadające się do użycia w instalacjach o dowolnej skali. Pełna skalowalność zapewnia możliwość rozbudowy systemu oraz jego precyzyjne dostosowanie do wymagań klienta. Zaawansowane zarządzanie wyświetlaniem obrazów z kamer na wielu monitorach, rozbudowany harmonogram zadań oraz profesjonalne archiwum to tylko niektóre elementy systemu NetHybrid HD. Intuicyjny interfejs użytkownika pozwala na taką konfigurację systemu, aby był łatwy w codziennej obsłudze nawet dla niezaawansowanego operatora. Opcje zarządzania zdalnymi połączeniami sprawiają, że system doskonale nadaje się do monitorowania rozproszonych obiektów, takich jak placówki bankowe, stacje benzynowe czy sieci sklepów.

Oprogramowanie przeznaczone do obsługi stacji klienckich pracujących w systemie Windows to aplikacja CMS Professional. Na jednym komputerze możemy uruchomić dowolną liczbę takich aplikacji, co zapewnia możliwość zdalnego monitorowania nawet rozległych obiektów wyposażonych w setki kamer. Jeden program kliencki pozwala połączyć się z szesnastoma różnymi serwerami i dostarczać obraz w sumie z 512 kamer. Za pomocą wielomonitorowej karty wizyjnej możemy łatwo, szybko i tanio zrealizować centrum monitoringu o rozbudowanych możliwościach.

Zaawansowane opcje e-mapy zapewniają sprawne zarządzanie dużą liczbą kamer na rozległym obszarze. Dodatkowo funkcje sprawdzania połączeń on-line ze zdalnymi serwerami daje gwarancję, że stale otrzymujemy aktualny obraz ze wszystkich serwerów.

Pakiet CMS Mobile to prostsza aplikacja kliencka przeznaczona do pracy w urządzeniach mobilnych wyposażonych w systemy operacyjne Android, Windows Mobile, iOS lub BlackBerry. Najnowsze aplikacje przeznaczone do pracy w telefonach iPhone oraz tabletach iPad w wersji HD zapewniają doskonały obraz oraz pełną obsługę wyświetlaczy typu *multi-touch*. Pakiet CMS Mobile, podobnie jak jego „duży" odpowiednik – CMS Professional, pozwala łączyć się z kilkoma serwerami i monitorować różne obiekty w tym samym czasie. Dostępne jest sterowanie głowicami PTZ, wejściami/wyjściami cyfrowymi oraz zdalny dostęp do archiwum. Dopełnieniem jest funkcja cyfrowego powiększania fragmentu obrazu, niezwykle przydatna w przypadku megapikselowych kamer IP lub kamer HDCCTV. Rozwiązania mobilne są niezwykle przydatne w sytuacjach, gdy istnieje potrzeba stałego kontaktu z monitorowanym obiektem, np. gdy grupa agentów ochrony pracuje w terenie.



Fot. 2. Karta przechwytywania obrazu w standardzie HDCCTV

Jaka będzie przyszłość standardu HDCCTV?

Poznamy ją prawdopodobnie już w tym roku. Można by zapytać, dlaczego standard HDCCTV pojawia się dopiero teraz i czy to nie jest zbyt późno. Gdyby został wprowadzony kilka lat temu, byłby dziś bez wątpienia powszechny, a rozwój telewizji sieciowej (IP) na pewno nie przebiegałby tak dynamicznie jak obecnie. HDCCTV jest bacznie obserwowany przez producentów oraz użytkowników systemów telewizji na całym świecie. Bezsprzecznie to nie zalety tego standardu przesądzą o jego sukcesie rynkowym – wszystko zależy od tego, ilu czołowych producentów zdecyduje się wejść do gry. Poczynione w ostatnich latach spore inwestycje w technologie IP sprawiają, że nowy standard niekoniecznie zostanie wdrożony przez wielkich graczy, takich jak Panasonic, Sony czy Bosch. Obecnie gotową ofertę w zakresie HDCCTV przedstawili EverFocus, Speco, Comart i Webgate, a wkrótce zamierza to zrobić CNB. Wielki chiński producent CSST zapowiada, że w 2011 roku „zaleje rynek" tanimi kamerami HDCCTV o wysokiej jakości. Są one prostsze w produkcji niż megapikselowe kamery IP, a przede wszystkim nie wymagają integracji z oprogramowaniem typu *open platform*, co zdecydowanie przyspiesza ich wejście na rynek. Wszystkie te sygnały zapowiadają, że nowy standard wkrótce zajmie przynajmniej pewną niszę w ofercie CCTV na całym świecie. Trudno powiedzieć, czy będzie stosowany masowo w nowych instalacjach, ale na pewno jest to doskonałe rozwiązanie do modernizacji istniejących systemów analogowych, polegającej na wyposażeniu ich w kamery dostarczające obraz o jakości HD. Ogromny rynek gotowych instalacji analogowych jest łakomym kąskiem dla integratorów.

Z badań przeprowadzonych przez organizację HDCCTV Alliance wynika, że w 2013 roku na 40 milionów wszystkich sprzedanych kamer 30% będą stanowiły kamery w standardzie HDCCTV, 55% – kamery analogowe, a pozostałe 15% – kamery IP. Biorąc pod uwagę szereg zalet standardu HDCCTV, można się zgodzić, że zaprezentowany scenariusz w dużym stopniu może się sprawdzić. Dotychczasowe doświadczenia pochodzące z rynku CCTV jasno wskazują, że kluczem do sukcesu jest zaoferowanie dobrej jakości za rozsądną cenę. Pozostaje bacznie przyglądać się temu, co oferuje nowy standard HDCCTV, który jest w stanie spełnić te kryteria.

Tomasz Kaliński
ALNET SYSTEMS

ALNET SYSTEMS

profesjonalne rozwiązania do cyfrowej rejestracji obrazu

ponad 60 000 instalacji na całym świecie

www.alnetsystems.com

NET HYBRID HD

NOWOŚĆ !

NetHybrid HD jedyny na rynku !

System łączący trzy technologie w jednym rejestratorze.

HDcctv + IP + CCTV

Doskonała jakość obrazu HD bez kompresji i opóźnień.

720p/1080p

NS NETSTATION – sieciowe oprogramowanie do cyfrowej rejestracji obrazu

NET HYBRID – hybrydowy system do cyfrowej rejestracji obrazu

CMS PROFESSIONAL – profesjonalne oprogramowanie klienckie

CMS MOBILE – oprogramowanie klienckie dla urządzeń mobilnych

Projektowanie systemów monitoringu IP z firmą SPS

Wielostrumieniowość w systemach telewizji dozorowej IP opartych na oprogramowaniu SeeTec i kamerach Sanyo

S.P.S. Trading

Artykuł, który ukazał się w poprzednim numerze *Zabezpieczeń*, zawierał informacje ogólne dotyczące budowy i działania sieci IP wykorzystywanych w sieciowych systemach monitoringu wizyjnego. Obecnie przechodzimy do zagadnień szczegółowych, związanych z praktycznym wykorzystaniem sprzętu oferowanego przez firmę SPS, w tym kamer Sanyo i oprogramowania SeeTec

Duży przepływ danych we współczesnych systemach telewizji dozorowej IP stawia wysokie wymagania urządzeniom sieciowym i sprzętowi komputerowemu. Nowoczesne metody kompresji, takie jak H.264, są dość złożone obliczeniowo i bez względu na implementację będą powodowały znaczne obciążenie procesora, zarówno podczas kodowania, jak i dekodowania. Wysoka rozdzielczość przesyłanego obrazu wiąże się z większą przepływnością strumienia wizyjnego i zajęciem szerszego pasma sieciowego. Dzięki wykorzystaniu produktów Sanyo i SeeTec można wyjść naprzeciw tym wyzwaniom. W niniejszym artykule zostaną przedstawione faktyczne korzyści, jakie daje wielostrumieniowość, ze szczególnym uwzględnieniem dużych instalacji.

Jedną z najważniejszych funkcji wykorzystywanych w monitoringu IP jest wielostrumieniowość. Tym mianem określa się zdolność systemu do pracy z kilkoma jednocześnie strumieniami wizyjnymi o różnych parametrach, wysyłanymi z tej samej kamery. Do parametrów tych należą:

– format (MJPEG, H.264 – nowsza odmiana MPEG-4),
– rozdzielczość (od 320×180 do 2288×1712),
– poklatkowość (0,1 – 25 kl./s).

Funkcjonalność ta w zależności od przyjętych założeń pomaga w ograniczeniu ilości danych przesyłanych przez sieć komputerową oraz w zredukowaniu obciążenia procesora. Musi być ona realizowana zarówno po stronie kamer, jak i oprogramowania. Do zastosowań związanych z telewizją dozorową w zupełności wystarcza, aby kamera generowała dwa strumienie wizyjne. Tak jest w przypadku podstawowej kamery z serii HD – Sanyo VCC-HD2100P. Bardziej zaawansowane modele, takie jak Sanyo VCC-HD2500P, wytwarzają dodatkowe strumienie wizyjne, które mogą być wykorzystane również poza systemem telewizji dozorowej, np. na stronie internetowej, lub przetwarzane przez inne oprogramowanie. Ilość możliwych zastosowań jest niemalże nieograniczona.

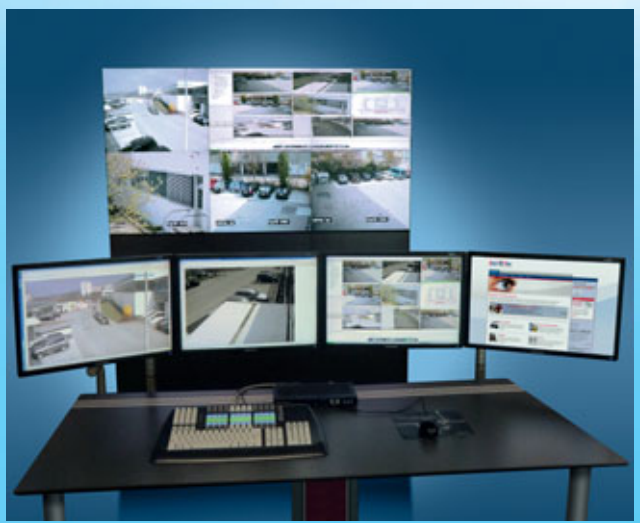
Skupmy się jednak na telewizji dozorowej. W dużych instalacjach najczęściej występuje konieczność prowadzenia podglądu przy użyciu kilku monitorów, z których każdy najczęściej obsługuje kilka kamer (fot. 1).

Rozważmy następujący przypadek: obraz z szesnastu kamer Sanyo VCC-HD2100P jest wyświetlany na monitorze w trybie podziału ekranu na części. Kamery i monitor pracują w rozdzielczości Full HD, czyli 1920×1080 pikseli. Obraz z kamer jest jednak skalowany w celu dopasowania go do rozmiarów odpowiedniego fragmentu ekranu monitora, w wyniku czego jego wysokość i szerokość są zmniejszone czterokrotnie. Otrzymany w ten sposób obraz ma wymiary ok. 480×270 pikseli. Staje się oczywiste, że przesyłanie i dekodowanie klatek o rozmiarach odpowiadających rozdzielczości Full HD traci sens, ponieważ widoczny obraz i tak jest znacznie mniejszy. W takich sytuacjach zastosowanie znajduje wielostrumieniowość.

W przeprowadzanych dalej testach podstawowym trybem pracy każdej z szesnastu kamer będzie rozdzielczość Full HD i poklatkowość 12 kl./s (rys. 1), co jest więcej niż wystarczające dla większości zastosowań praktycznych. Rozważymy również drugą konfigurację, która będzie się różniła jednym elementem – każda kamera będzie generowała dodatkowy strumień wizyjny w formacie MJPEG o niższej rozdzielczości, równej 640×360 pikseli, ale z identyczną poklatkowością (rys. 2). Rozdzielczość taka jest wystarczająca do wyświetlenia obrazów w trybie podziału ekranu monitora na części. Co się stanie, gdy operator będzie potrzebował dostępu do strumienia wizyjnego o wysokiej jakości, żeby mógł dostrzec jakiś szczegół, korzystając np. z funkcji powiększenia cyfrowego? Aplikacja kliencka może zostać skonfigurowana w taki sposób, aby zaznaczenie pola obrazu z danej kamery powodowało przełączenie na inny, zdefiniowany wcześniej strumień wizyjny. W ten sposób można uniknąć niedogodności związanych z niską rozdzielczością obrazu.

Zajętość pasma sieciowego

Na pierwszy rzut oka wydaje się, że jeżeli kamera generuje dodatkowy strumień wizyjny, to obciążenie łącza będzie większe. I jest tak w rzeczywistości, ale tylko podczas transmisji w kierunku od kamery do serwera. Za to strumień wizyjny wysyłany z serwera do jednej lub wielu stacji klienckich będzie o wiele mniejszy (rys. 3), co przynajmniej częściowo rekompensuje wspomnianą niedogodność. W zależności od dobranych parametrów całkowita przepływność danych wysyłanych z serwera i do serwera może być niższa. W przypadku



Fot. 1. Wielomonitorowe stanowiska operatorów w centrach monitoringu (źródło: SeeTec)

Rys. 1. Serwer pobierający jeden strumień danych

Rys. 2. Praca w konfiguracji wielostrumieniowej

systemu z pojedynczymi strumieniami wizyjnymi należy się liczyć z dużą przepływnością, która dzięki wielostrumieniowości może zostać zmniejszona. W każdej jednak sytuacji oszczędzane jest pasmo sieciowe przy transmisji na trasie serwer – klient.

Obciążenie procesora[1]

Drugą, i może najważniejszą, zaletą wynikającą ze stosowania wielostrumieniowości jest obniżenie kosztów zakupu sprzętu komputerowego. Podczas obserwacji obrazów na stacji klienckiej możliwość wykorzystania strumienia wizyjnego powstałego w wyniku zakodowania obrazu o niższej rozdzielczości pozwala na znaczną redukcję obciążenia procesora (rys. 4).

W przypadku stacji klienckich służących do wyświetlania obrazów obciążenie procesora na poziomie 60% stanowi wartość graniczną. Większość dekoderów programowych zapewnia obsługę mechanizmów kontroli jakości (QoS), pełniących różnorodne funkcje. W tym przypadku ma to na celu utrzymywanie stałego opóźnienia poszczególnych klatek obrazu, dzięki czemu utrzymywana jest stała prędkość odtwarzania. Zwiększenie obciążenia powyżej pewnego poziomu powoduje zwiększenie czasu dekodowania. W celu utrzymania odpowiedniego tempa wyświetlania obrazów dekoder może pomijać niektóre klatki, co skutkuje zmniejszeniem średniej poklatkowości. Dlatego właśnie tak ważne jest utrzymywanie obciążenia procesora na stosunkowo niskim poziomie.

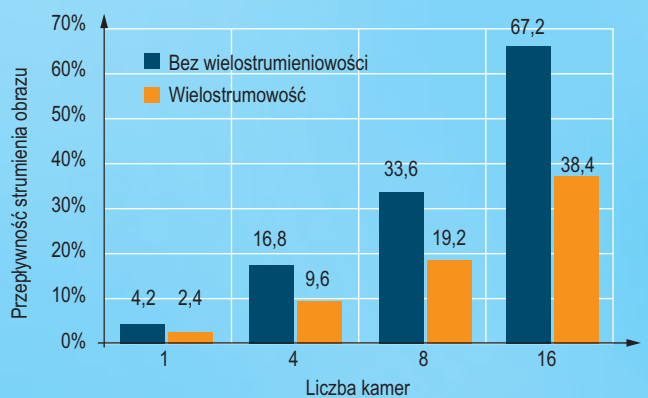
1) Wszystkie testy zostały przeprowadzone na komputerze wyposażonym w procesor Intel Core i7 870 2,93 GHz, 4 GB RAM, kartę ATI Radeon z serii 5700 i 32-bitowy system operacyjny Windows 7.

Niski poziom obciążenia procesora, osiągnięty z wykorzystaniem wielostrumieniowości, pozwala na dołączenie do stacji klienckiej co najmniej jednego dodatkowego monitora i wyświetlenie obrazów z kolejnych szesnastu kamer. W przypadku korzystania z jednego tylko strumienia wizyjnego o wysokiej rozdzielczości nie byłoby to możliwe bez wymiany sprzętu komputerowego na wydajniejszy. Należy również pamiętać o tym, że ceny komputerów nie są związane zależnością liniową z ich wydajnością. Ściślej mówiąc, dwukrotny wzrost wydajności może pociągnąć za sobą wielokrotny wzrost ceny. Bardziej opłacalne w tym przypadku może być po prostu użycie kolejnej stacji klienckiej, co również nie zawsze jest pożądane.

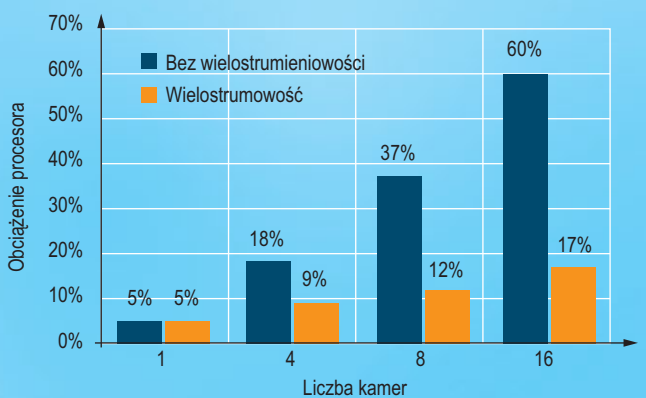
Podsumowanie

Wyniki praktycznych pomiarów przeprowadzonych w systemie SeeTec, współpracującym z kamerami Sanyo, potwierdzają, że zastosowanie wielostrumieniowości umożliwia zredukowanie obciążenia sieci oraz procesora. Funkcjonalność ta pozwala obniżyć wymagania sprzętowe docelowych stacji klienckich lub wyeliminować konieczność zakupu dodatkowych komputerów. Skutkuje to zmniejszeniem całkowitego kosztu realizacji systemu IP, dzięki czemu rozwiązanie takie jest korzystne zarówno w małych, jak i w dużych instalacjach. Nie bez znaczenia jest również możliwość częściowego wykorzystania infrastruktury sieci komputerowej, chociaż dla profesjonalnych systemów dozorowych zaleca się zaprojektowanie i fizyczną realizację osobnej, dedykowanej sieci teleinformatycznej, która zagwarantuje poprawne działanie systemu.

Opracowanie: S.P.S. Trading



Rys. 3. Przepływność strumienia danych wysyłanego z serwera w Mb/s



Rys. 4. Obciążenie procesora stacji klienckiej

firma ATLine®

ZSJZ

www.atline.pl

AQAP 2110:2009
ISO 9001:2008

H-Series

PT- Series

PTZ 35x140 MS

F-Series

SR- Series

D-Series

KAMERY TERMOWIZYJNE

Firma ATLine sp.j. Sławomir Pruski
ul. Franciszkańska 125, 91-845 Łódź,
tel. +48 42 657 30 80, fax +48 42 655 20 99
e-mail: info@atline.pl, handel@atline.pl

FLIR dostrzegą to czego oczy nie widzą

Kamera BBB-31F

BBB-31F to kamera o wysokiej czułości i rozdzielczości (580 TVL w trybie kolorowym, 650 TVL w trybie B/W), wyróżniająca się wiernym odwzorowaniem kolorów. Kolory są żywe i naturalne, a obraz ostry i wyraźny. W kamerze zastosowano procesor Blue-I. W przypadku pracy z promiennikiem podczerwieni należy pamiętać o zastosowaniu obiektywu z korekcją aby uniknąć rozmycia obrazu. Kamera posiada funkcję WDR poprawiającą zdolność do obserwacji scen o różnym poziomie oświetlenia. W odróżnieniu od kamer z elektroniczną funkcją WDR w kamerze BBB-31F stosowany jest WDR z wykorzystaniem funkcji podwójnego skanowania.

Zalety:

- przetwornik Double Scan
- WDR – szeroki zakres dynamiki
- cyfrowa stabilizacja obrazu DIS
- redukcja szumów 3D DNR, w porównaniu ze standardową funkcją 2D DNR zapewnia zmniejszenie smużeń przemieszczających się obiektów
- mechaniczny filtr zapewniający wierne odwzorowanie kolorów
- BLC – kompensacja światła z tyłu
- sterowanie przez port RS-485 – protokół Pelco-D
- funkcja DSS x128, zwiększająca czułość przy niskim poziomie oświetlenia

Właściwości:

- kamera dzień/noc
- przetwornik 1/3" Double-density scan
- wysoka rozdzielczość 580TVL (w trybie bw 650TVL)
- czułość 0,1 lx (kolor), 0,0002 lx (DSS wł., B/W)
- OSD
- AGC, WDR, Eclipsa, BLC, AWB, 3D DNR, DIS, Flickerless, D/N, DZ – regulacja przez OSD
- WDR maks. 72 dB
- detekcja ruchu, strefy prywatności, funkcja mirror w pionie i poziomie oraz obrót obrazu, wyostrzanie obrazu
- sterowanie przez RS-485 (Pelco-D)

CNB TECHNOLOGY Inc.

BLUE-i

Dane techniczne	
Model	BBB-31F
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" Double Scan CCD
Rozdzielczość efektywna	752(H) x 582(V) 440K
Liczba linii	580 TVL (BW 650TVL)
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50dB
WDR	On (3 poziomy, maks. 72dB) /Off
Obiektyw	mocowanie C/CS
Tryb dzień/noc	tak, mechaniczny
Czułość	0,1 lx (kolor), 0,0002 lx (DSS on B/W), F1.2, 30IRE
Menu OSD	angielski, chiński, koreański, rosyjski, hiszpański, francuski
Cyfrowa redukcja szumu	3D DNR, 63 poziomy / wył.
Balans bieli	ATW, ANTI-ROL, push, manual
DSS	do 128 ramek obrazu
Automatyczna regulacja wzmocnienia (AGC)	3 poziomy / wył.
Kompensacja światła tylnego	BLC, 3 poziomy / wył.
Eclipsa	16 stref
Redukcja migotania	wł./wył.
Cyfrowa stabilizacja obrazu	wł./wył.
Cyfrowy zoom	x6,13
Strefy prywatne	8 programowalnych stref
Detekcja ruchu	4 programowalne strefy
Odbicie lustrzane obrazu	w poziomie, w pionie, obrót
Elektroniczna migawka	1/50~1/120 000 s
Ręczna migawka	1/60, 1/250, 1/700, 1/1K, 1/1.6K, 1/2.5K, 1/5K, 1/7K, 1/10K, 1/30K, 1/60K, 1/120K
Zasilanie	12 V_{DC}
Pobór prądu	maks. 3,3W / 270 mA
Wymiary (średnica x wys.)	70 x 64 x 129 mm
Temperatura pracy / Wilgotność	-10°C~50°C / 30%~80% RH
Masa	ok. 324 g

Kamera IP IGC2050F

CNB TECHNOLOGY Inc.

Kamera IP IGC2050F to najnowszy przedstawiciel rodziny kamer IP XNET firmy CNB. Kamera wyróżnia się rozdzielczością Full HD przy częstotliwości odświeżania 25 klatek/s, dwustrumieniowością oraz wbudowanym mikrofonem. Przetwornik CMOS charakteryzuje się progresywnym skanowaniem zapewniającym wyraźniejszy obraz poruszających się obiektów. Dodatkową zaletą jest możliwość awaryjnego zapisu na karcie SD oraz zasilanie PoE. Obraz z kamery cechuje naturalne odwzorowanie kolorów.

Zalety:

- przetwornik CMOS 1/3" z progresywnym skanowaniem
- rozdzielczość Full HD: 1980x1080 @ 25kl./s
- rozdzielczość 1100 linii
- mechaniczny filtr podczerwieni TDN
- dwa strumienie H.264/MJPEG
- dwukierunkowa komunikacja audio
- wbudowany mikrofon
- zapis na kartach SD
- zgodność ze standardem ONVIF

Właściwości:

- kamera dzień/noc
- obiektyw z mocowaniem CS lub C (z dodatkowym pierścieniem pośredniczącym)
- dołączony bezpłatny program CMS (praca dwumonitorowa, 128 kanałów, E-mapa, pełna zdalna obsługa kamery)
- analogowe wyjście wizji PAL/NTSC
- regulacje jasności oraz koloru
- AGC, BLC, AWB, Flickerless, D/N, DSS
- zasilanie 12 V DC albo PoE IEEE 802.3af
- obudowa typu box

Dane techniczne	
Kamera	IGC2050F
System skanowania	16:9 progresywne
Przetwornik	1/3" CMOS
Synchronizacja	wewnętrzna
Liczba pikseli	1920 (H) x 1080 (V) 2,0Mpx
Rozdzielczość efektywna	1100 TVL
Wyjście wideo	NTSC/PAL, 1,0Vp-p (BNC 75Ω, composite - CSWk)
Obiektyw	mocowanie C/CS
Tryb dzień/noc	mechaniczny filtr podczerwieni
Kompensacja światła tylnego	BLC wł. / wył.
Redukcja migotania	wł. / wył.
Wyostrzanie	0~5
Balans bieli	Auto/Manual
Ręczna migawka	NTSC: 1/7,5, 1/15, 1/30, 1/60, 1/120, 1/180, 1/240, 1/300, 1/360, 1/420, 1/480, 1/600, 1/900, 1/1,2K, 1/1,5K, 1/1,8K, 1/2K, 1/3K, 1/4K, 1/6K, 1/8K PAL: 1/7,5, 1/15, 1/25, 1/50, 1/100, 1/150, 1/200, 1/250, 1/300, 1/350, 1/400, 1/500, 1/750, 1/1K, 1/1,25K, 1/1,5K, 1/2K, 1/3K, 1/4K, 1/6K, 1/8K
Elektroniczna migawka	NTSC: 1/7,5 ~ 1/8000 (21 kroków) PAL: 1/7,5 ~ 1/8000 (21 kroków)
Kompresja	H.264 / MJPEG
Liczba kl./s	H.264, MJPEG: PAL 25fps, NTSC 30fps
Rozdzielczość	Full HD (1920 x 1080), SXGA (1280 x 1024), 720P (1280x720), D1(720 x 480 / 720 x 576), VGA (640x480), CIF (352 x 240 / 352 x 288)
Audio	dwukierunkowa (full duplex / ADPCM G.726)
Wejścia audio	liniowe / wbudowany mikrofon
Protokoły	IPv4, HTTP, TCP, RTSP, RTP, RTCP, UDP, SMTP, FTP, ICMP, DHCP, UPnP, Bonjour, ARP, DNS, DynDNS, ONVIF
Obsługiwane serwery DDNS	1. CNB DDNS 2. DynDNS.org 3. kod źródłowy z SDK
Port LAN	Ethernet 10/100 Base-T (RJ-45 Type)
Obsługa PoE	Standard IEEE 802.3af
Prawa dostępu	wielu użytkowników z własnym hasłem i prawami dostępu (administrowanie, podgląd, zarządzanie)
Bezpieczeństwo sieciowe	filtrowanie IP
Detekcja ruchu	tak (maks. 3 obszary)
Złącza alarmowe	1 wejście alarmowe, 1 wyjście alarmowe
Reakcja na alarmy	kopiowanie obrazów JPEG na serwer FTP oraz powiadamianie przez e-mail
Przeglądarka	Internet Explorer 6.0 lub nowszy
Oprogramowanie	XNVR, CNB CMS oraz programy użytkowe (IP-Installer i inne)
Aktualizacja oprogramowania	aktualizacja przez HTTP
Wymiary (szer. x wys. x gł.)	71 x 65 x 143,8 mm
Temperatura pracy	0°~40°
Masa	366 g
Zasilanie	12 V_{DC} maks. 5 W
Pobór prądu	0,4 A

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

Elektrozaczepy SCOT

Elektrozaczep jest elementem wykonawczym kontroli dostępu, tzn. realizuje fizyczne zwolnienie skrzydła drzwi przez system domofonowy, wideodomofonowy, kontroli dostępu lub też prosty przycisk zwierny (tzw. „dzwonkowy").

Elektrozamki SCOT wytwarzane są z wysokiej jakości materiałów, co przekłada się na ich bezawaryjną pracę przez długi okres. Testy producenta nie wykazują nadmiernego zużycia nawet przy setkach tysięcy cykli otwarcia. Pozwala to na objęcie elektrozamka 5-letnią gwarancją. Wraz z elektrozamkiem klient otrzymuje uniwersalną, metalową listwę umożliwiającą montaż elektrozamka w słupku furtki lub w ościeżnicy drzwi.

cecha / model	symetryczny	regulacja języka	napięcie zasilania	standardowy (NC)	rewersyjny (NO)	pamięć	blokada	sygnalizacja
ES-S12AC/DC	+	+	12 $V_{AC/DC}$	+				
ES-S12AC/DC-M	+	+	12 $V_{AC/DC}$	+		+		
ES-S12AC/DC-B	+	+	12 $V_{AC/DC}$	+			+	
ES-S12AC/DC-MB	+	+	12 $V_{AC/DC}$	+		+	+	
ES-S12DCn	+	+	12 V_{DC}	+				
ES-S12DC-R	+	+	12 V_{DC}		+			
ES-S12DC-RS	+	+	12 V_{DC}		+			+
ES-S24AC/DC	+	+	24 $V_{AC/DC}$	+				
ES-S24DC-R	+	+	24 V_{DC}		+			
ES-S24DC-RS	+	+	24 V_{DC}		+			+

Elektrozaczep symetryczny

W przypadku typowych modeli, klient przy wyborze elektrozamka musi określić kierunek otwierania sterowanych nim drzwi (lewy-prawy). Elektrozaczep symetryczny posiada zapadkę (język) umieszczony w jednakowej odległości od obu krawędzi obudowy, co sprawia, że można go montować zarówno w drzwiach lewych jak i prawych. Eliminuje to konieczność doboru konkretnego rodzaju elektrozamka już na etapie projektowania systemu kontroli wejścia.

Regulacja języka zapadki

Pozwala na eliminację szczeliny pomiędzy językiem (zapadką) elektrozaczepu, a zapadką zamka drzwi przez wysunięcie języka elektrozaczepu w zakresie 0 ~ 4 mm od standardowego położenia.

Blokada mechaniczna

Elektrozaczep posiada mechaniczny przełącznik, który umożliwia rezygnację z kontroli otwarcia wejścia. Ma zastosowanie w miejscach, gdzie w ciągu dnia jest duże natężenie ruchu osobowego i nie ma wymogu, aby drzwi były zabezpieczone przed wejściem.

Pamięć

Do otwarcia (odblokowania) zamka wystarczy krótki (chwilowy) impuls elektryczny, który powoduje odblokowanie elektrozaczepu. Po otwarciu skrzydła drzwi elektrozaczep powraca do stanu zamkniętego. Jest to wygodna funkcja w przypadku zastosowania przycisku wyjścia umieszczonego w pewnej odległości od drzwi, gdzie osoba wychodząca nie może jednocześnie nacisnąć przycisku wyjścia i otworzyć drzwi.

Sygnalizacja

Elektrozaczep jest wyposażony w mikroprzełącznik z zaciskami, który całkowicie zastępuje dodatkowe elektromagnesy instalowane w drzwiach. Umożliwia to dodatkowo kontrolę stanu wejścia (np. kontrolę niedomkniętych drzwi), podając sygnał do systemu kontroli lub centrali alarmowej.

Uniwersalne zasilanie

Elektrozaczep został wyposażony w cewkę pozwalającą na zasilanie prądem stałym (z zasilacza prądu stałego) lub zmiennym (z transformatora). Właściwość ta pozwala na montaż elektrozaczepów SCOT w systemach posiadających już zainstalowane źródło ich zasilania.

Elektrozaczep rewersyjny

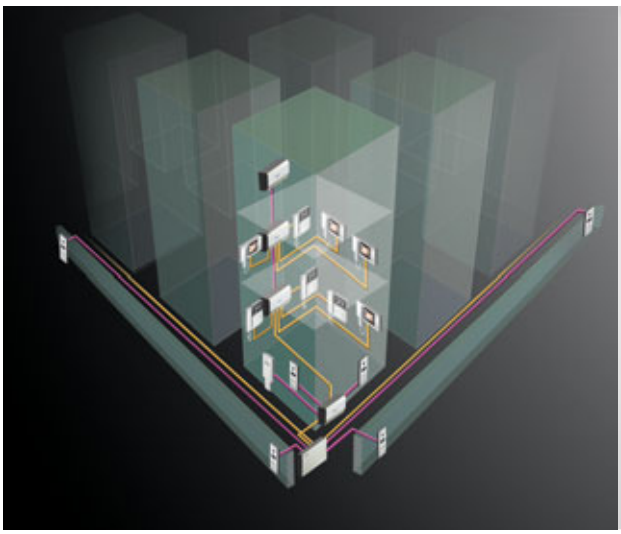
Elektrozamek z odwrotną funkcją otwarcia. Zamek rewersyjny jest po podłączeniu napięcia zasilającego zamknięty (zablokowany). Po odłączeniu zasilania zamek jest otwarty (odblokowany).

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

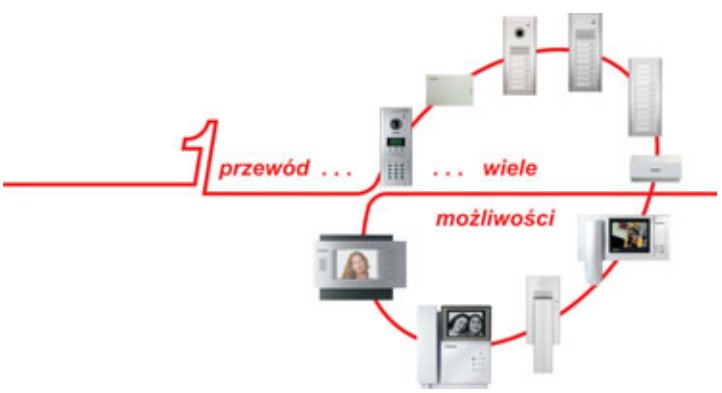
System wieloabonentowy serii 2400

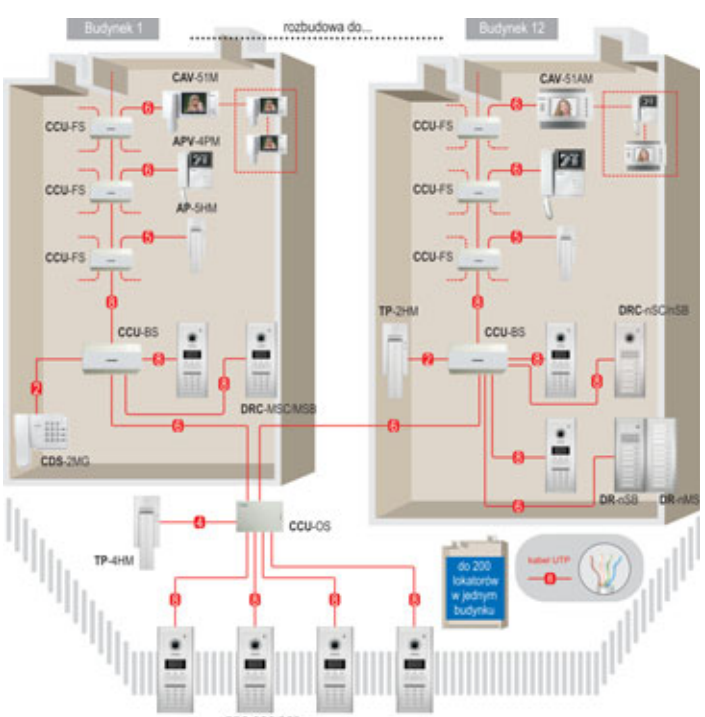


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna ilość obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

Lokator może mieć zainstalowany prosty unifon, umożliwiający kontakt głosowy z osobą odwiedzającą jak i monitor (czarno-biały lub kolorowy), pozwalający także na obserwację wizualną osoby odwiedzającej.

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak wideo - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów). System może być wyposażony w unifon lub stację portierską instalowaną w portierni, przez co lokatorzy oraz osoby ich odwiedzające mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków, jak i całych osiedli zamkniętych, gdzie ogrodzonych może być klikanaście budynków, a całość nadzorowana przez kilku portierów.





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

RioPro – Profesjonalna drukarka do kart identyfikacyjnych

Profesjonalna drukarka zaprojektowana do seryjnego wydruku identyfikatorów. Rio Pro to niezawodna, szybka i łatwa w obsłudze drukarka umożliwiająca w każdym momencie użytkowania szybką zmianę trybu pracy na drukowanie dwustronne. Wbudowane opatentowane funkcje HoloKote i HoloKoteFlex zabezpieczają karty przed nieautoryzowanym kopiowaniem. Funkcje te dają również możliwość personalizacji znaku wodnego zawierającego tekst lub logo firmy. Standardowo, podczas procesu wydruku karta pokrywana jest cienką folią (overlay) zabezpieczającą nadruk przed uszkodzeniem mechanicznym i promieniami UV. Rio Pro i Rio Pro Duo wyposażone są w wyświetlacz LCD z menu w języku polskim informujący o statusie drukarki. Drukarki posiadają 3-letnią gwarancję łącznie z mechanicznymi uszkodzeniami głowicy. Drukarki posiadają certyfikat CE i RoHS.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 23 sekundy
- Monochromatyczny wydruk karty w 6 sekund
- Interfejs do PC: USB i Ethernet
- Menu wyświetlacza w języku polskim
- Sterowniki 32 i 64 bit w języku polskim: Windows 2000, XP, Vista, Windows 7
- Rozdzielczość wydruku: 300 dpi
- Podajnik na 100 kart
- Odbiornik na 70 kart
- Możliwość ręcznego podawania kart
- Zasilanie: 100-240 V / 50-60 Hz
- Wymiary / Masa: 470 mm x 220 mm x 250 mm / 4,9 kg
- Temperatura pracy: od 10°C do 30°C
- 5 wzorów znaków wodnych do wyboru
- Wydruk na kartach wielkości CR-80 oraz CR-79
- Automatyczna regulacja grubości karty
- 3 lata gwarancji z możliwością wydłużenia do 4 lat, łącznie z mechanicznymi uszkodzeniami głowicy

Opcje dodatkowe:

Możliwość aktualizacji do wersji dwustronnej

Możliwość drukowania dwustronnego (Rio Pro Duo)

Możliwość kodowania kart magnetycznych, chipowych i zbliżeniowych

Taśmy

- Kolorowa 5 paneli nadruk 300 kart (MA300YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Kolorowa + czarna nadruk dwustronny 250 kart (MA250YMCKOK)
- Kolorowa 5 paneli nadruk 100 kart (MA100YMCKO)

Karty

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

Zestaw czyszczący

- 1 szt. rolki czyszczącej dostarczana z każdą taśmą
- 10 szt. kart czyszczacych, 1 flamaster (3633-0053)
- 5 szt. wałków czyszczących plus wymienna oś wałka

Dystrybucja:

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

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

Pronto – Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

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

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

Specyfikacja techniczna

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

Taśmy

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

Karty

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

Zestaw czyszczący

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

Dystrybucja:

ACSS

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

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

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

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

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

Cechy charakterystyczne

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

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

Dystrybucja: alarmnet®

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

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

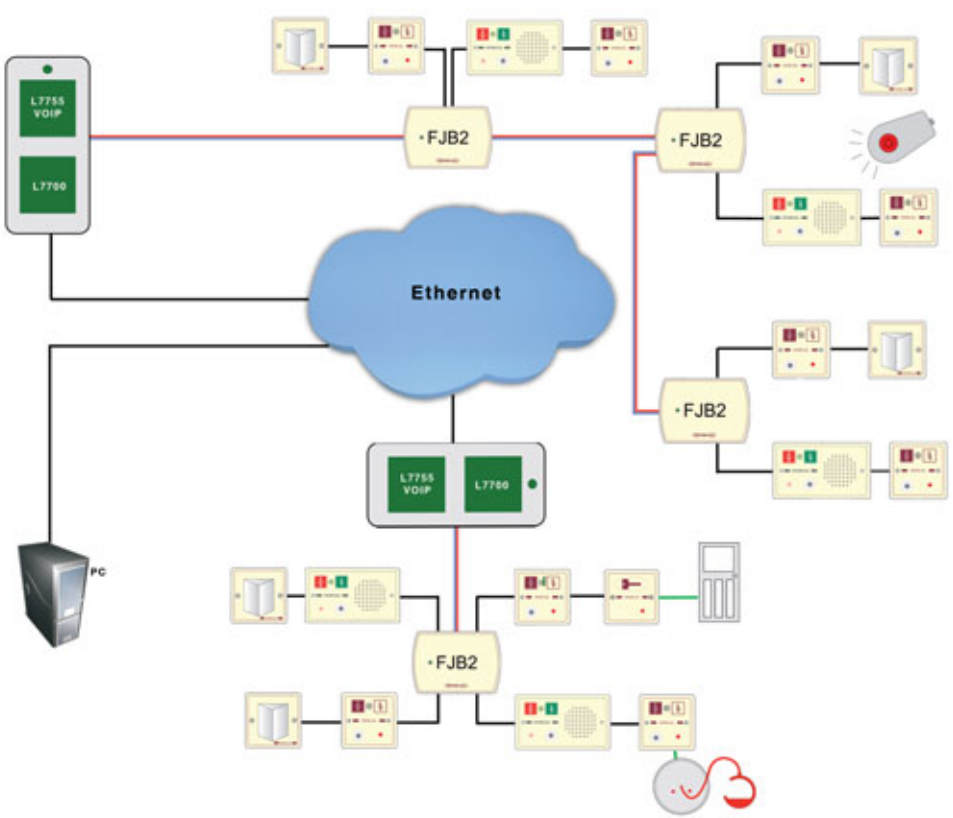
Intercall – szpitalny system przywoławczy

Prosty w instalacji – pomocny dla obsługi – zapewniający bezpieczeństwo pacjenta

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

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

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



Dystrybucja: alarmnet®

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

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

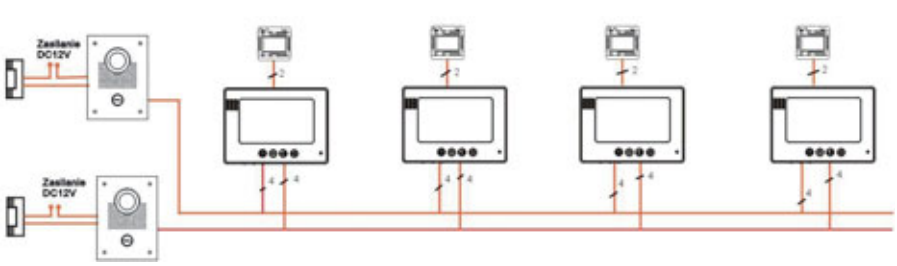
Kolorowy monitor wideodomofonowy MT670C-CK2

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

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

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

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



Dystrybutor:

wena

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

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

Stacja bramowa wideodomofonowa z serii CK

SAC5C-CK

SAC35C-CK

SAC50C-CK

SAC551C-CK

SAC551C-CK(8)

SAC561C-CK

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

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

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

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

Dystrybutor:

wena

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

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

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

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

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

ul. Łęczycka 37, 85-737 **Bydgoszcz**
tel./faks (52) 342 91 24, 342 98 82
e-mail: aat.bydgoszcz@aat.pl

ul. Ks. W. Siwka 17, 40-318 **Katowice**
tel./faks (32) 351 48 30, 256 60 34
e-mail: aat.katowice@aat.pl

ul. Prosta 25, 25-371 **Kielce**
tel./faks (41) 361 16 32/33
e-mail: aat.kielce@aat.pl

ul. Mieszczańska 18/1, 30-313 **Kraków**
tel./faks (12) 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

ul. Energetyków 13a, 20-468 **Lublin**
tel. (81) 744 93 65/66
faks (81) 744 91 77
e-mail: aat.lublin@aat.pl

ul. Dowborczyków 25, 90-019 **Łódź**
tel./faks (42) 674 25 33, 674 25 48
e-mail: aat.lodz@aat.pl

ul. Racławicka 82, 60-302 **Poznań**
tel./faks (61) 662 06 60/62
e-mail: aat.poznan@aat.pl

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

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

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

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

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

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

ALARMNET BORKIEWICZ Sp. J.
ul. Karola Miarki 20C
01-496 Warszawa
tel. (22) 663 40 85
faks (22) 833 87 95
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

ALARMTECH POLSKA Sp. z o.o.
Oddział:
ul. Kielnieńska 115
80-299 **Gdańsk**
tel. (58) 340 24 40
faks (58) 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

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

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

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

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

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

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

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

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 46
faks (32) 790 76 73
e-mail: krakow@e-alpol.com.pl

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

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

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

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

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

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

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

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

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

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

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

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.pl

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

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

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
Tulipan Hause
02-672 Warszawa
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

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

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

Centrum Monitorowania Alarmów Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 0 888
faks (22) 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

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

ul. Zatorska 36, 51-215 **Wrocław**
tel. (71) 340 0 209
faks (71) 341 16 26
e-mail: wroclaw@cma.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DYSKRET POLSKA
Spółka z 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. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 812 05 05
faks (22) 812 62 12
e-mail: office@ebs.pl
www.ebs.pl

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

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

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

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

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

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

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

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

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

Przedstawicielstwo we Wrocławiu
tel. kom. 0 693 195 009
e- mail: factor.wr@factor.pl

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

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

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. (91) 489 41 81, 434 67 38
faks (91) 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

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

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

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. (12) 411 49 79, 411 57 47
faks (12) 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RISCO GROUP POLAND Sp. z o.o.
ul. 17 Stycznia 56
02-146 Warszawa
tel. (22) 500 28 40
faks (22) 500 28 41
e-mail: 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

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 462 30 87
e-mail: info@satie.pl
www.satie.pl

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

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

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

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

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

P.T.H. SECURAL
Jacek Giersz
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. (32) 291 86 17
faks (32) 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. (61) 623 23 05
faks (61) 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	TAK
Janex International	–	TAK	TAK	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	–
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
NAPCO	–	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	–
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	TAK	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	–	TAK	TAK	TAK
RISCO	TAK	–	–	–	–
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	TAK
SATIE	–	–	TAK	TAK	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	TAK	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	–	–	TAK	–	–
Sony	TAK	–	TAK	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	TAK	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	TAK	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	–	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
AGIS Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	–	–	–	TAK	–	TAK	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	TAK	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	–	–	–	–	TAK	–	–
CMA	TAK	–	TAK	TAK	TAK	TAK	TAK	TAK	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	TAK	TAK	–	TAK	–	–	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EBS	Transmitery IP (ethernet), GSM/GPRS/SMS, zabezpieczenia bankowe, sygnalizatory, GPS, produkcja OEM/ODM, R&D								
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	–
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	TAK	TAK	TAK	–
HSA	TAK	TAK	TAK	TAK	–	–	–	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	–	–	–	TAK	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	–	TAK	–	–	–	–
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	TAK
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	konserwacja i serwis zabezpieczeń mechanicznych								
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	TAK	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	–	TAK	TAK	–	–	TAK	–	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	TAK	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	TAK	TAK	TAK	TAK	TAK	–	TAK	–	TAK
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

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

Skład i łamanie
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

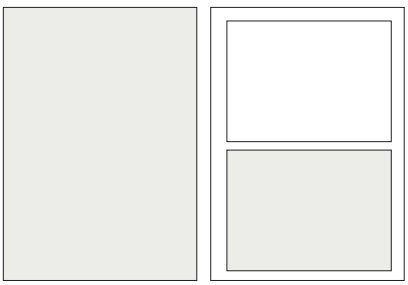
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 0 546
faks (22) 546 0 501

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



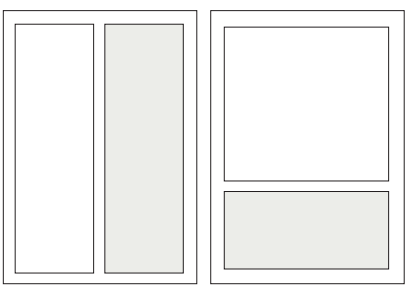
cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

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

Reklama na okładkach:

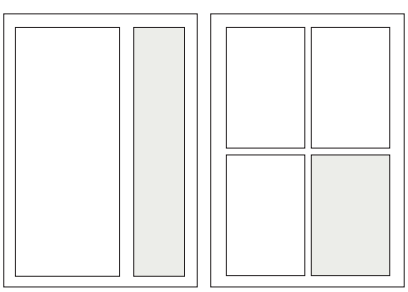
pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Spis teleadresowy:
jednorazowy wpis 70 zł



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)

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

Spis reklam

Chipset WiseNet2 DSP z rozdzielczością Full HD

uchwyć każdy szczegół..

iPOLiS FULL HD ONVIF

WiseNet II

- Kompresja H.264
- Funkcja Smart Codec
- Obsługa rozdzielczości 3 megapiksele (2048 x 1536) oraz Full HD (1920 x 1080p)
- WDR (rozszerzony zakres dynamiki)
- SSNR (Samsung Super Noise Reduction)
- Oprogramowanie klienckie Net-i
- Wyjścia sygnałowe Ethernet i BNC
- Wbudowane gniazdo karty pamięci SD
- Zasilanie PoE
- Skanowanie progresywne

Moduł SNB-7000 wprowadza rozdzielczość Full 1080p High Definition (HD)

Model SNB-7000 jest pierwszą megapikselową kamerą iPOLiS nowej generacji, w której zastosowano procesor sygnałowy WiseNet2 DSP firmy Samsung. Kamera ta generuje obrazy w rozdzielczości Full HD (1080p).

Procesor WiseNet2 DSP oferuje mnóstwo zaawansowanych funkcji dla aplikacji monitoringu, przy jednoczesnej minimalizacji wymagań dotyczących szerokości pasma sieciowego. Na przykład, wykorzystanie kodeków sprzętowych Smart Codec firmy Samsung pozwala określić krytyczne obszary obrazu, które mogą być przesyłane w wyższej rozdzielczości niż pozostała część. W połączeniu z zaawansowaną metodą kompresji H.264 oraz opcją jednoczesnej obsługi strumieni o różnej rozdzielczości, w tym obrazów Full HD (format 16:9) oraz 3MP (format 4:3), użytkownik otrzymuje możliwość pełnej kontroli nad przesyłanymi obrazami.

Funkcja WDR zapewnia doskonały i ostry obraz przy obserwacji scen z tylnym oświetleniem i o małym kontraście. Funkcja redukcji szumów trzeciej generacji, opracowana przez firmę Samsung (SSNRIII), eliminuje zakłócenia powstające przy słabych warunkach oświetleniowych, znakomicie poprawiając jakość obrazu oraz minimalizując wymagania w zakresie szerokości pasma sieci oraz wymaganej przestrzeni dyskowej do rejestracji (mniejsze zakłócenia = lepsza kompresja).

Oprogramowanie NET-i, umożliwiające bezproblemową integrację z autonomicznymi rejestratorami sieciowymi firmy Samsung, nie wymaga opłat licencyjnych. Podobnie jak sama kamera SNB-7000, oprogramowanie to jest kompatybilne ze standardem ONVIF, wspieranym przez wszystkich liczących się producentów kamer IP i systemów NVR na świecie.

IFSEC 2011
16-19 May 2011
NEC Birmingham, UK
SAMSUNG CITY | 5/D130

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

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

SAMSUNG

Potrzebuję...

drukarki do kart
wspomagającej rozwój
mojej firmy.

HID Global przedstawia nowy model FARGO® DTC4000

Przełom w modułowości, wszechstronności i wygodzie personalizacji kart.

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

HID

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