CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3(85)/2012

# ZABEZPIECZENIA

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



## W NUMERZE:

SuperLoLux 2HD

JVC

# kamery, które ożywają nocą

Kamery *wszystkich* wystawców MTP Securex 2012 zostały zaprezentowane przy świetle dziennym.

W ciemności,* *tylko* kamery JVC serii Super LoLux 2HD pokazały, że widzą rzeczy niewidoczne bez konieczności wydłużania czasu migawki.

* Na stoisku firmy Euroalarm zbudowano ciemnię, w której został umieszczony zegar ścienny, w celu pokazania płynnego ruchu wskazówki sekundnika

euroalarm

www.euroalarm.com.pl

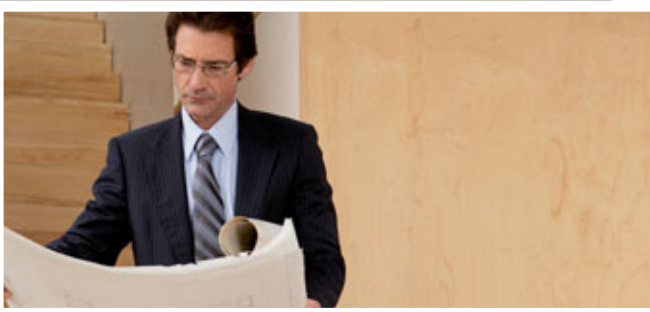
**JVC jest w Poznaniu, Bydgoszczy, Toruniu, Wrocławiu, Gorzowie Wlkp, Koszalinie, Krakowie i Zielonej Górze.**
**Uwaga! Poszukujemy dystrybutorów na terenie Trójmiasta, Warszawy i Katowic.**

# Spis treści

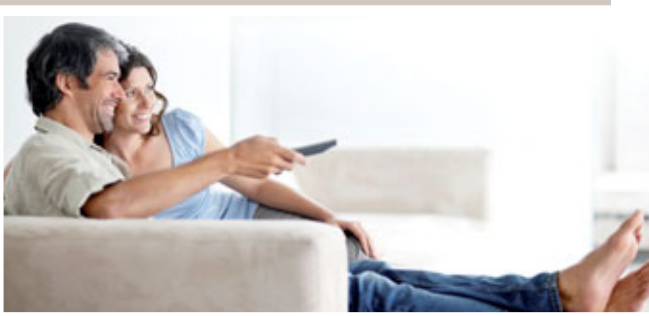



CZASOPISMO ZABEZPIECZENIA 3/2012

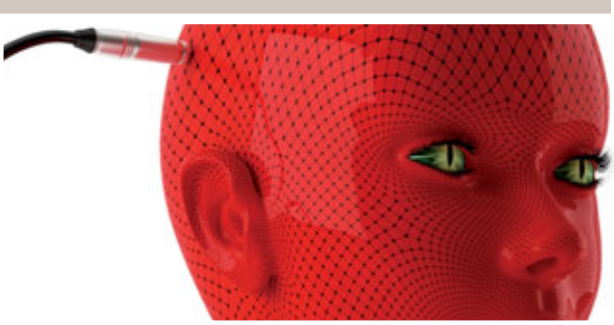

HD-SDI w praktyce **26**



Zasady realizacji projektów **30**



Sterowanie systemem alarmowym **56**



Kradzież tożsamości i stalking – czyli cyberprzestępstwa w nowej odsłonie **60**

# Samsung i Sureview – udana integracja

**Rejestratory DVR z serii SRD** firmy **Samsung** zostały skutecznie zintegrowane z systemowym oprogramowaniem dyspozytorskim **Immix Enterprise** oraz **Immix Cloud** marki **SureView.**

Immix Enterprise to platforma oprogramowania zgodna z BS8418, przeznaczona do odbioru i konsolidacji informacji o zdarzeniach alarmowych oraz nagrań wizyjnych pochodzących z systemów analizy obrazu i kontroli dostępu, systemów automatyki oraz urządzeń GPS. Immix Cloud jest sieciową wersją oprogramowania Enterprise, która umożliwia użytkownikom tworzenie „prywatnej chmury" (*private cloud*) w celu uzyskania dostępu do spersonalizowanych usług poprzez dowolną przeglądarkę internetową lub urządzenie przenośne.

– *Dzięki wprowadzeniu oprogramowania dyspozytorskiego Immix do central alarmowych i ośrodków zdalnego monitoringu wizyjnego w całej Europie klienci firmy Samsung mogą zainstalować dowolny model rejestratora z serii SRD i mieć pewność, że dyspozytorzy będą w stanie w pełni wykorzystać ich możliwości do zapisu obrazów o najwyższej jakości* – powiedział Peter Ainsworth, Senior Product Manager w Samsung Techwin Europe.

Seria rejestratorów SRD firmy Samsung składa się z ponad 20 różnych modeli w wersjach cztero-, ośmio- lub szesnastokanałowych. Wszystkie te modele wykorzystują skuteczną kompresję H.264. Dzięki zastosowaniu podwójnych kodeków możliwe jest tworzenie osobnych strumieni przeznaczonych do zapisu oraz transmisji obrazów. Wszystkie rejestratory SRD mają też ten sam intuicyjny interfejs użytkownika (GUI), co znacznie ułatwia obsługę operatorom, na przykład podczas konfiguracji poszczególnych kanałów mających służyć do zapisu obrazów z różną poklatkowością lub w różnej rozdzielczości.

– *Obecnie, oprócz modeli SRD, także wybrane modele z innych serii naszych rejestratorów mogą wykorzystywać oprogramowanie Immix Enterprise. Nadal współpracujemy z działem rozwoju systemów firmy Sureview, by zintegrować nasze najnowsze rejestratory sieciowe (NVR) z tą aplikacją* – dodał Peter Ainsworth.

*Bezpośr. inf. David Solomons*
*DRS Marketing*

# RXC-ST – nowa czujka OPTEX

„Masz problem? Zawieś RX-40QZ i zapomnij o fałszywych alarmach". Niestety, po wielu latach **OPTEX** zakończył produkcję tej doskonałej czujki pasywnej podczerwieni.

Jej miejsce zajmie nowe urządzenie – **RXC-ST**. „C" w nazwie pochodzi od „CORE" oznaczającego rdzeń, na którym bazują nowe urządzenia. „CORE" oznacza też mikroprocesorową analizę sygnału rejestrowanego przez piroelement.

Przy tworzeniu nowej serii firma OPTEX wykorzystała swoje bogate doświadczenie zdobyte przy produkcji czujek i barier wykorzystywanych do detekcji zewnętrznej. Wykorzystując rozwiązania znane z czujek zewnętrznych serii HX czy FTN, OPTEX wprowadził mikroprocesorową analizę przebiegu sygnału z piroelementu. Sam piroelement jest nową konstrukcją.

Najpopularniejszy algorytm detekcji bazuje na zliczaniu impulsów. OPTEX zrobił duży krok naprzód, uwzględniając analizę kształtu impulsu. Mikroprocesorowa analiza kształtu impulsu pozwala na odróżnienie sygnału charakterystycznego dla człowieka od sygnałów pochodzących od zwierząt, poruszających się roślin, zasłon, spadających z faksu ciepłych kartek papieru itp. W serii CORE nie ma specjalnej wersji czujki odpornej na zwierzęta, bo tę funkcję realizuje mikroprocesor.

Urządzenie zostało wyposażone w oddzielny układ pomiaru temperatury otoczenia celem dopasowania czułości do aktualnych warunków otoczenia.

Czujka nie ma „klikających" przekaźników, co sprawia, że jest niesłyszalna nawet dla najwrażliwszych użytkowników.

*Fot. Nowa czujka RXC-ST odróżnia ludzi od zwierząt*

Instalację ułatwia uchwyt montażowy, który jest standardowo dołączany do czujki.

Obudowę wykonano z wysokoudarowego polistyrenu – tworzywa o dużej odporności na odbarwienia. Diodę sygnalizacyjną umieszczono pod soczewką, więc nie ma przyciągających wzrok elementów kontrastujących kolorystycznie, a czujka wtapia się w otoczenie.

Seria CORE spełnia nowe wymagania dotyczące odporności elektromagnetycznej, które będą obowiązywały od 2014 r. Urządzenia spełniają wymagania klasy 2 normy EN 50131.

*Bezpośr. inf. Jacek Wójcik*
*Optex Security*

# ADI Global Distribution nowym partnerem Axis Communications

Firma **ADI Global Distribution**, obecna na światowym rynku zabezpieczeń od 50 lat, będzie nowym dystrybutorem produktów marki **Axis** w Polsce.

*– Z firmą ADI współpracowaliśmy już wcześniej na innych rynkach, m.in. szwedzkim, czeskim i słowackim. Rozwój sieciowego nadzoru wizyjnego w Polsce i związane z tym zwiększenie podaży skłoniło nas do powiększenia sieci naszych dystrybutorów. Zawarcie umowy z ADI, jednym z największych dystrybutorów systemów zabezpieczeń, jest prostą konsekwencją naszej strategii. Dzięki niemu w znacznej mierze zwiększy się dostępność produktów firmy Axis na rynku polskim* – powiedział Daniel Lesisz, Distribution Channel Manager CEE w Axis Communications.

ADI Global Distribution oferuje swoim klientom systemy zabezpieczeń, a także pomoc ekspertów działu technicznego i grupy przedstawicieli techniczno-handlowych. Dzięki temu jest w stanie zapewnić spersonalizowane rozwiązania w każdym segmencie rynku telewizji dozorowej. Teraz może wykorzystać również produkty firmy Axis.

*– Podpisanie umowy z Axis Communications wzmocni pozycję ADI Polska w segmencie rozwiązań zaawansowanych, jak również powiększy ofertę produktów w kanale dystrybucyjnym, co jest zgodne ze strategią jednoczesnego rozwoju sprzedaży dystrybucyjnej i projektowej naszej firmy* – powiedział Tomasz Kowalewski, Managing Director w ADI Poland.

*Bezpośr. inf. Krzysztof Pietrzak*
*Grayling Poland*

# Seria kamer VGA IP WiseNetS firmy Samsung

**Samsung** ponownie udoskonalił swoje sieciowe systemy nadzoru wizyjnego wykorzystujące IP poprzez wprowadzenie pięciu nowych kamer, w których wykorzystano WiseNetS – najnowszy chipset DSP (*Digital Signal Processor*) firmy Samsung, opracowany specjalnie dla kamer IP o rozdzielczości VGA.

Dzięki WiseNetS DSP każda z nowych, zgodnych z ONVIF kamer kompaktowych VGA umożliwia dodatkowo wielostrumieniową transmisję obrazu przy prędkości 30 klatek na sekundę, wybór metod kompresji (MJPEG lub wydajną H.264), zasilanie przez Ethernet oraz użycie wielokątnych masek prywatności.

Oprócz standardowej funkcji detekcji ruchu wszystkie kamery WiseNetS mają także funkcję detekcji twarzy. Wykrywają obecność osób i informują o niej operatorów, na przykład poprzez e-mail. Można ustalić dzienny albo tygodniowy harmonogram. Nawet twarze ukryte za wielokątną maską prywatności mogą zostać rozpoznane.

Jakość wytwarzanego przez kamery WiseNetS obrazu VGA (640×480) została podwyższona dzięki zastosowaniu przetworników obrazu wykonanych z wykorzystaniem technologii CMOS, natomiast system skanowania progresywnego poprawia jakość obrazu poruszających się obiektów, umożliwiając na przykład odczytanie numerów rejestracyjnych samochodu (nie ma efektu rozmycia obrazu). Wybrane modele zapewniają także dwukierunkową komunikację głosową.

Wśród sześciu nowych urządzeń jest stałopozycyjna kamera SNB-1001, odporna na warunki atmosferyczne i działająca na podczerwień kamera SNO-1080R, stałopozycyjna kamera kopułkowa SND-1011, kopułkowa kamera ze zmiennoogniskowym obiektywem SND-1080, wandaloodporna kamera kopułkowa ze zmiennoogniskowym obiektywem SNV-1080 oraz wandaloodporna kamera kopułkowa ze zmiennoogniskowym obiektywem SNV-1080R z wbudowanymi diodami IR.


Wszystkie modele, za wyjątkiem SNO-1080R, mają wbudowane gniazdo kart pamięci Micro SD/SDHC, na których można przechowywać obrazy dokumentujące zdarzenia alarmowe zarejestrowane bezpośrednio przez kamerę, natomiast modele SND-1080 oraz SNV-1080 oferują dwukierunkową komunikację dźwiękową.

*– Te sześć kamer można zastosować w każdym małym lub średnim systemie w szpitalach, biurach, szkołach, placówkach handlowych czy na parkingach* – powiedział **Tim Biddulph**, IP Product Manager w Samsung Techwin Europe. *– Ponadto kamery te mogą być podstawą kompletnego niskobudżetowego sieciowego systemu nadzoru wizyjnego dostarczającego obrazy w czasie rzeczywistym lub rejestrującego obrazy o wysokiej jakości w przypadku zastosowania tych kamer w połączeniu z naszymi najnowszymi sieciowymi rejestratorami obrazu (czterokanałowym SRN-470D oraz szesnastokanałowym SRN-1670D).*

Co więcej, kamery WiseNetS są w pełni kompatybilne z oprogramowaniem zarządzającym Samsung NET-i Ware, które jest dostępne w wersji 8-, 16-, 32- oraz 64-kanałowej, a także w bezlicencyjnej wersji czterokanałowej do stosowania w mniejszych systemach. Oprogramowanie to zostało stworzone w celu ułatwienia zarządzania, kontroli, monitoringu oraz nagrywania obrazów wytwarzanych przez sieciowe i kopułkowe kamery marki Samsung. Dzięki niemu można nagrywać i odtwarzać obrazy na komputerze PC poprzez sieć, w dowolnym miejscu na świecie i łączyć się z systemem bezpieczeństwa przez 24 godziny na dobę i 7 dni w tygodniu – bez względu na to, gdzie się znajdujemy.

*Bezpośr. inf. David Solomons*
*DRS Marketing*

# Nowy menadżer do spraw marketingu w firmie Samsung

**Dominic Jones** został mianowany na stanowisko **European Marketing Manager** w dziale profesjonalnych zabezpieczeń firmy **Samsung Techwin Europe**. Będzie podlegał dyrektorowi sprzedaży i marketingu Gary'emu Rowdenenowi.

Dotychczas Dominic Jones pełnił funkcję dyrektora marketingu w firmie Sanyo Sales and Marketing Europe, gdzie był odpowiedzialny za promocję kamer Full HD, a także projektorów LCD oraz elektronicznych produktów konsumenckich tej marki.

*– Cieszę się, że mogę poprowadzić jeden z najefektywniejszych zespołów w branży zabezpieczeń elektronicznych. Dla firmy Samsung to niezwykle interesujący okres, w którym koncentrujemy się na promowaniu Smarter Security. Polega ona na udostępnieniu klientom narzędzi, dzięki którym mogą oni łatwo udoskonalać system analogowy, wprowadzając rozwiązania wykorzystujące sieć IP w najdogodniejszy dla swojej firmy sposób. Wkrótce uruchomimy wielojęzyczny serwis internetowy, aby zapewnić klientom z całej Europy dostęp do wszelkich informacji potrzebnych do określenia specyfikacji lub ułatwiających wybór odpowiednich zabezpieczeń marki Samsung* – powiedział Dominic Jones.

*Bezpośr. inf. David Solomons*
*DRS Marketing*

# Zabezpieczenie elektrowni słonecznej

**Videotec** i inne firmy postanowiły zapewnić możliwie wysoki poziom bezpieczeństwa w elektrowni słonecznej pod Turynem.

Prace projektowe trwały około dwóch miesięcy. W ich trakcie odbyły się spotkania z klientami oraz realizatorami. Biorąc pod uwagę odległości od granic chronionego obszaru (około czterech kilometrów) oraz możliwość wystąpienia poważnych zakłóceń elektromagnetycznych wywołanych pracą dwunastu inwerterów zainstalowanych na terenie elektrowni, firma Sicurtel zdecydowała, że należy zbudować sieć Ethernet w postaci zamkniętego pierścienia światłowodowego, z wykorzystaniem technologii O-ring, z dwunastoma przełącznikami sieciowymi rozmieszczonymi w terenie, przystosowanymi do pracy w zakresie temperatur od -40°C do 75°C.

Do tej sieci należy podłączyć dwadzieścia osiem barier mikrofalowych ERMO 482 X PRO Cias, jedenaście punktów kamerowych Ulisse Compact IP i trzydzieści sześć kamer Videotec 110 z oświetlaczami pracującymi w podczerwieni.

Bariery mikrofalowe Cias powinny być podłączone do sieci za pośrednictwem piętnastu konwerterów IB-FMCREP-ETH z wejściami RS485 i sterowane za pomocą serwera IB-SYSTEM IP.

Kamery Videotec, które składają się na wizyjny system dozorowy, są wyposażone w obiektywy o zmiennej ogniskowej i wywierają bardzo niewielki wpływ na poziom oświetlenia w porze nocnej.

Firma Sicurtel doszła do wniosku, że jedyną platformą spełniającą wymagania klienta, która pozwala na pełną integrację wszystkich urządzeń sieciowych zainstalowanych na terenie elektrowni, jest oprogramowanie systemowe Milestone XProtect.

System na bieżąco dostarcza dane dotyczące produkcji energii elektrycznej i przekazuje je użytkownikowi końcowemu. Oprogramowanie XProtect Smart Client umożliwia przekazywanie tych danych do siedziby zarządu firmy. Ponadto stosowane jest oprogramowanie XProtect Mobile, które dla pracowników zajmujących się utrzymaniem elektrowni w ruchu jest szczególnie przydatnym i skutecznym narzędziem. Jest ono wykorzystywane do zdalnej realizacji i weryfikacji wszelkich interwencji, niezależnie od ich rodzaju.

Oprogramowanie Milestone VMS obsługuje pewną liczbę modułów typu I/O IP, co pozwala operatorowi systemu, użytkownikowi końcowemu oraz firmie zajmującej się ochroną obiektu na wykorzystanie oprogramowania Milestone XProtect Smart Client do włączania oświetlenia na obszarze rozciągającym się wzdłuż obwodu chronionego terenu. Dzięki temu w porze nocnej możliwe jest wykrywanie wszelkich anomalii lub sytuacji krytycznych.

Przyjęte rozwiązanie pozwala personelowi technicznemu firmy Sicuretel na przeprowadzanie skutecznych i szybkich interwencji z wykorzystaniem zdalnie obsługiwanych systemów sterujących. W szczególności dotyczy to rutynowych czynności konserwacyjnych oraz interwencji zmierzających do rozwiązania problemów wykrytych przez system, które nie wymagają wymiany lub naprawy urządzeń znajdujących się w terenie. Obsługa wszystkich urządzeń może być także dokonywana przez Internet.

*Bezpośr. inf. Videotec*
*Opracowanie: Redakcja*

**Śp. Jan Mróz**, prezes firmy Janex International Sp. z o.o., urodził się 3 maja 1948 roku jako ósme dziecko w rodzinie. Jego droga życia nie była usłana różami, ale zawsze wierzył, że osiągnie sukces.

Mimo iż pochodził z biednej rolniczej rodziny, ukończył studia na wydziale elektroniki Politechniki Warszawskiej. Swoją karierę zawodową rozpoczynał w Zakładach Elektroniki Przemysłowej Profel Sp. z o.o. w Szydłowcu. Po powrocie z emigracji w 1992 roku, wraz z Joanną Zawadzką-Mróz założył firmę Janex International z siedzibą w Radomiu. Początki działalności były bardzo trudne. Jednak brak kapitału, zła lokalizacja i trudności logistyczne nie zniechęciły początkującego przedsiębiorcy. Przezwyciężył trudności dzięki charyzmie i uporowi w dążeniu do celu. Punktem zwrotnym było otwarcie oddziału w Warszawie w 1996 roku. Dzięki niemu firma rozkwitła.

Jan Mróz odszedł niespodziewanie 8 maja 2012 roku. Zapamiętamy go jako człowieka uśmiechniętego, życzliwego, koleżeńskiego i najlepszego szefa. Po latach ciężkiej pracy i osiągnięciu ogromnego sukcesu nie zmienił się. Dbał o rodzinę i swoich pracowników. Nigdy nikomu nie odmawiał pomocy. Sukces był jego celem, ale nie dążył do niego za wszelką cenę. Cenił przyjaźń bardziej niż pieniądze, mimo iż wielokrotnie się na niej zawiódł. Zawsze można było liczyć na jego pomoc i dobrą radę. Był bardzo mądrym szefem. Doceniał swoich pracowników i był z nimi bardzo związany. Ich los nie był mu obojętny.

Nam wszystkim będzie go bardzo brakowało.

*Zarząd i pracownicy firmy Janex International*

Zarząd AAT Holding oraz redakcja czasopisma *Zabezpieczenia* składa wyrazy współczucia rodzinie i współpracownikom Jana.

# Konferencja SPIN Extra

Podczas specjalnej, wiosennej edycji **Spotkania Projektantów Instalacji Niskoprądowych (SPIN Extra)** w dniach 22–23 marca 2012 roku firma **Lockus** zorganizowała konferencję, na której zaprezentowano m.in. zintegrowane systemy sterowania oświetleniem w nowoczesnych budynkach i biurowcach, nowoczesne rozwiązania dla centrów danych, systemy elektroakustyczne, urządzenia aktywne, systemy kontroli dostępu.

Uczestnikami było ponad 110 osób – projektanci, instalatorzy oraz czołowi dostawcy rozwiązań dla branży niskich prądów.

Podczas dwóch dni wykładów swoje rozwiązania zaprezentowały następujące firmy: 3M, 3LOGIC, Axis Communications, AVAYA, Konsorcjum FEN, Nedap, NETGEAR, Rittal, Romi, TOA Electronics Europe.

Zintegrowane systemy monitoringu i bezpieczeństwa zostały przedstawione przez przedstawicieli firmy Konsorcjum FEN i reprezentantów firmy Axis Communications. Przedstawiciel firmy Nedap omówił systemy kontroli dostępu, telewizji dozorowej oraz SSWiN, a przedstawiciele 3LOGIC przedstawili zintegrowane systemy sterowania oświetleniem i omówili ich zastosowanie w nowoczesnych budynkach i biurowcach.

Poruszono także inne tematy, np. dotyczące telefonii IP i transmisji danych, systemów elektroakustycznych, zasilania gwarantowanego w Data Center (Centrum Danych).

Pozytywny odbiór i duże zainteresowanie konferencją stanowi dla firmy Lockus dowód na to, iż warto kontynuować podjętą inicjatywę także na północy, w centrum i na zachodzie Polski.

Ponadto na jesień zaplanowano tradycyjne, odbywające się w na południu Polski Spotkanie Projektantów Instalacji Niskoprądowych SPIN. Będzie to dziesiąta, jubileuszowa edycja.

*Bezpośr. inf. Edyta Marek*
*Lockus*

# Axis prezentuje AXIS Camera Companion

**Axis Communications** prezentuje **AXIS Camera Companion** – rozwiązanie klasy *entry-level* wykorzystujące sieć IP, przeznaczone do stosowania w małych systemach nadzoru wizyjnego. Zaprojektowano je z myślą o systemach wykorzystujących od 1 do 16 kamer. Idealnie sprawdza się w przypadku małych firm, sklepów, biur, hoteli itp. W skład kompletu wchodzi bezpłatne oprogramowanie klienckie oraz kamery sieciowe AXIS lub kodery wizyjne obsługujące karty SD.

– *Choć w większych instalacjach sieciowe urządzenia do nadzoru wizyjnego w coraz większym stopniu zastępują urządzenia analogowe, mniejsze systemy często bazują na kamerach analogowych i magnetowidach* – powiedział Peter Friberg, dyrektor działu System and Services w Axis Communications. – *Nasza propozycja skierowana jest do tych, którzy dotychczas rezygnowali z sieciowych systemów nadzoru wizyjnego z przyczyn finansowych. AXIS Camera Companion zapisuje cały materiał wizyjny z kamer i koderów, dlatego nasze rozwiązanie jest proste, niezawodne i niedrogie.*

AXIS Camera Companion umożliwia właścicielom małych firm wykorzystanie sieciowych kamer HDTV w celu wykrywania potencjalnych aktów wandalizmu, kradzieży i innych incydentów. Nagranie może być odtwarzane lub podglądane na żywo w dowolnym miejscu na terenie firmy lub zdalnie – przez Internet. System umożliwia wykrywanie ruchu w obrazie oraz sterowanie położeniem kamer czy ogniskową obiektywów. Zarejestrowane obrazy mogą być łatwo przesłane do współpracowników czy służb porządkowych, takich jak straż pożarna czy policja. System umożliwia również wykorzystanie zewnętrznych aplikacji do podglądu materiału wizyjnego – zarówno zarejestrowanego, jak i oglądanego na żywo – na większości nowoczesnych smartfonów i tabletów.

W przeciwieństwie do analogowych instalacji AXIS Camera Companion nie wymaga centralnego urządzenia nagrywającego – cyfrowego czy sieciowego rejestratora, a nawet komputera. Kamery zasilane są przez sieć, dlatego nie ma potrzeby stosowania dodatkowego okablowania. Wszystkie obrazy są zapisywane na typowych kartach SD umieszczonych w każdej z kamer. W związku z tym nawet w przypadku przerwy w działaniu sieci kamery nie przestają nagrywać. Obniża to koszty i upraszcza instalację, zwiększając zarazem niezawodność systemu przez eliminację wielu potencjalnych przyczyn awarii.

AXIS Camera Companion składa się z trzech części: standardowych sieciowych kamer AXIS lub koderów wizyjnych z możliwością zapisu na kartach SD; darmowego oprogramowania klienckiego oraz zewnętrznych aplikacji służących do podglądu materiału wizyjnego; typowego sprzętu sieciowego, takiego jak rutery, przełączniki, karty SD czy urządzenia NAS. Dotychczas wykorzystywane kamery analogowe mogą zostać zintegrowane z systemem dzięki koderom wizyjnym AXIS.

Razem z AXIS Camera Companion można wykorzystać większość sieciowych kamer i koderów wizyjnych Axis z oprogramowaniem w wersji 5.40 lub nowszym.

*Bezpośr. inf. Krzysztof Pietrzak*
*Grayling Poland*
*Opracowanie: Redakcja*

# OPTEX przedstawia nową serię czujek klasy 3 wg EN50131

Dla firmy **OPTEX** rok 2012 jest rokiem nowości. Po nowej serii barier SL i nowej czujce ruchu RXC-ST, zaprezentowanych na targach SCECUREX, przyszedł czas na kolejne urządzenia.

Od kilku lat w ofercie firmy OPTEX znajduje się seria OPTiMAL – zaawansowane czujki ruchu przeznaczone do zastosowań w obiektach komercyjnych. Ich wysoką jakość potwierdzają instalacje w obiektach, w których wymaga się stosowania zabezpieczeń klasy 2 i 3 wg EN501131. Seria OPTiMAL została uzupełniona nowymi czujkami CD-X.

CD-X to trzy nowe urządzenia klasy 3 wg EN50131 – czujki pasywnej podczerwieni: powierzchniowa o zasięgu 15 m×15 m, kurtyna 24 m×2 m oraz czujka dualna 15 m×15 m. Wszystkie mają funkcję wykrywania maskowania na podstawie cyfrowej analizy sygnału aktywnej podczerwieni. Niewątpliwym udogodnieniem dla konserwatora systemu jest funkcja samokontroli czujki. Jest ona realizowana automatycznie, przez układ sterowania urządzenia, w określonych odstępach czasowych, lub uruchamiana ręcznie z poziomu centrali.

Koleją cechą ułatwiającą eksploatację i zwiększającą bezpieczeństwo systemu jest możliwość wyłączania i załączania diody sygnalizacyjnej z poziomu centrali (np. w celu przeprowadzenia testu przejścia), bez konieczności zdejmowania obudowy z czujki. Poza tym potencjalny intruz nie dowie się o zadziałaniu funkcji antymaskingu. Ważnym zabezpieczeniem antysabotażowym jest zintegrowany czujnik oderwania od ściany.

Nowy filtr światła białego i zakłóceń elektromagnetycznych umożliwia bezproblemową eksploatację w warunkach bardzo silnego oświetlenia, często spotykanego w obiektach handlowych.

Nie bez znaczenia jest możliwość ograniczania zasięgu działania części mikrofalowej czujki dualnej, a nawet jej wyłączenia (w systemie wyłączonym z dozoru). Nowością jest zastosowanie skuteczniejszego modułu mikrofalowego wykorzystującego rozwiązania znane z czujek zewnętrznych serii HX-40.

Wygodę instalowania w rozbudowanych systemach zapewniają rezystory końca linii, które w nowych modelach uproszczono i ograniczono do tylko jednej zwory.

Wszystkie te rozwiązania sprawiają, że seria CD-X spełnia wysokie wymagania wobec systemów zabezpieczeń klasy 3 wg EN50131. Zalety nowych czujek OPTEX opiszemy dokładniej w kolejnym numerze Zabezpieczeń.

*Bezpośr. inf. Jacek Wójcik*
*Optex Security*

*Fot. Klasyczny kształt obudowy CD-X kryje zaawansowane technologie detekcji*

# Podsumowanie Międzynarodowych Targów Zabezpieczeń

Tegoroczne Międzynarodowe Targi Zabezpieczeń **SECUREX 2012** były przede wszystkim miejscem omawiania ważnych zagadnień, biznesowych rozmów oraz wymiany doświadczeń. W tym roku patronat objęli: Minister Gospodarki, Minister Spraw Wewnętrznych, Prezes Związku Banków Polskich oraz Komendant Wojewódzki Policji w Poznaniu.

Kwietniowa edycja odbywających się w cyklu dwuletnim targów zgromadziła blisko 250 wystawców z 18 krajów. Niemal 22% stanowili uczestnicy z zagranicy – z Austrii, Belgii, Chin, Czech, Francji, Holandii, Izraela, Kanady, Korei, Litwy, Niemiec, Portugalii, Słowacji, Szwajcarii, Szwecji, Tajwanu oraz Wielkiej Brytanii. Obok wiodących polskich firm w Poznaniu pokazali się uznani w Europie producenci i dystrybutorzy światowych marek. Na targach zadebiutowało ponad 150 nowych produktów. W dniach 23–26 kwietnia SECUREX oraz odbywające się w tym samym czasie targi Instalacje, Wodociągi, Kominki, TCS oraz SAWO odwiedziło **22 591 profesjonalistów** z branży.

Przez cztery dni można było nie tylko zwiedzać ekspozycję wystawców, ale również wziąć udział w licznych konferencjach, wykładach i pokazach zorganizowanych z udziałem znaczących stowarzyszeń branżowych, ośrodków naukowych lub pod patronatem wystawców. Branżowe spotkania dostarczyły wyczerpującej wiedzy na temat polskiego rynku, jego potencjału oraz najnowszych światowych trendów.

## Merytorycznie i fachowo

Blisko pięć godzin trwał finał **III Mistrzostw Polski Instalatorów Systemów Alarmowych** organizowanych przez Polską Izbę Systemów Alarmowych (**PISA**) i Międzynarodowe Targi Poznańskie (**MTP**), pod honorowym patronatem Ministra Spraw Wewnętrznych. Najlepsi w konkurencji związanej z systemami telewizji dozorowej, systemami sygnalizacji włamania i napadu, systemem kontroli dostępu oraz systemami sygnalizacji pożarowej okazali się Mistrzowie Polski – **Paweł Daniszewski i Piotr Podlaski z Agencji Solid Security z Olsztyna**. II miejsce i tytuł wicemistrza zdobyli Jarosław Lester i Daniel Zamłyński z Agencji Solid Security – tym razem ze Szczecina. Łukasz Dorman i Marek Kordiukiewicz z firmy MR Systemy z Warszawy stanęli na III miejscu podium.

Intrygująco rozpoczęła się konferencja na temat **bezpieczeństwa obiektów i zbiorów muzealnych**. Był dym, ostrzał z karabinów maszynowych i sprawna akcja policji. Pokaz w wykonaniu funkcjonariuszy wyspecjalizowanych jednostek policji – Samodzielnego Pododdziału Antyterrorystycznego Policji KWP w Poznaniu, Wydziału Konwojowego KWP w Poznaniu oraz Wydziału Kadr i Szkolenia KWP w Poznaniu – zademonstrował działanie służb podczas napadu na konwój przewożący cenne dzieła sztuki. Akcja policjantów miała związek z tematyką konferencji współorganizowanej przez KWP w Poznaniu oraz MTP. Podczas prelekcji fachowcy dzielili się swoimi doświadczeniami związanymi z ochroną muzeów w czasie przemieszczeń ludności oraz zabezpieczeniem obiektów podczas ewakuacji i wywozu zabytków z kraju. Omówiono także najczęstsze metody włamań oraz sposób przeciwdziałania im.

Dużo emocji wzbudziła debata ***Prawo dla monitoringu wizyjnego?*** poruszająca bardzo ważny problem regulacji zasad monitoringu wizyjnego w Polsce. W dyskusji moderowanej przez Łukasza Kistra wzięli udział Mariusz Cichomski (Naczelnik Wydziału Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej Departamentu Nadzoru), dr Wojciech Rafał Wiewiórowski (Generalny Inspektor Ochrony Danych Osobowych) oraz dr Paweł Waszkiewicz (adiunkt w Katedrze Kryminalistyki Wydziału Prawa i Administracji


Więcej zdjęć na stronie *www.zabezpieczenia.com.pl*


Uniwersytetu Warszawskiego). Publiczność zgromadzona na sali nie szczędziła uczestnikom debaty trudnych pytań dotyczących kontrowersyjnych zagadnień związanych z poprawą efektywności systemów monitoringu wizyjnego w naszym kraju.

Pierwszego dnia targów wręczono nagrody w prestiżowym konkursie **Mistrz Techniki Alarmowej** przygotowanym przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **POLALARM**. Nagrody w konkursie zostały przyznane za wybitne elektroniczne urządzenia oraz systemy przeznaczone do technicznej ochrony mienia, a w szczególności urządzenia systemów sygnalizacji włamania, napadu, pożaru, systemów telewizji dozorowej, kontroli dostępu, monitorowania zagrożeń, elektroniczne wyposażenie agentów ochrony fizycznej oraz zabezpieczenia pojazdów, transportu, ładunków. Spośród zdobywców I miejsc w poszczególnych kategoriach komisja konkursowa wyłoniła Laureata Głównej Nagrody. **Złotą Zbroję otrzymał Helikopter bezzałogowy KBUAV – 01 firmy KABE z Mikołowa**.

Podczas pobytu w Poznaniu można było również dowiedzieć się, jak bezpiecznie korzystać z bankowości internetowej i kart bankowych. Analiza napadów na agencje bankowe na terenie Wielkopolski oraz procedury postępowania podczas napadu były przedmiotem dyskusji podczas konferencji ***Bezpieczeństwo instytucji finansowych***. Bardzo aktualny temat poruszyli przedstawiciele Wydziału Bezpieczeństwa i Zarządzania Kryzysowego WUW podczas seminarium poświęconemu **bezpieczeństwu imprez masowych**. Z kolei o zarządzaniu bezpieczeństwem w praktyce rozmawiali prelegenci zgromadzeni na **II Konferencji Zarządzania Bezpieczeństwem Obiektów i Informacji** (zorganizowanej przez **POLALARM**).

Współcześnie niemal każdy element działalności podmiotów gospodarczych wiąże się z przetwarzaniem danych i systemami informatycznymi. Efektywność działalności i bezpieczeństwo firm zależy od ochrony zasobów przed ich naruszeniem czy utratą. Z myślą o kadrze technicznej i kierowniczej specjaliści z Zespołu Bezpieczeństwa PCSS oraz ITTI przygotowali **szkolenia z zakresu bezpieczeństwa IT**. Podczas spotkań omówiono między innymi metody ochrony serwerów i stacji roboczych, sposoby walki z atakami DDoS, problemy ochrony danych w modelu *cloud computing* i kwestie tworzenia oprogramowania pozbawionego błędów w zabezpieczeniach.

## Złoto dla najlepszych

W tym roku już przed targami poznaliśmy laureatów Złotego Medalu MTP. W tym roku konkurs zorganizowano po raz pierwszy według nowej formuły. Sąd konkursowy w składzie: prof. dr hab. inż. Bogdan Branowski, mgr inż. Wojciech Dąbrowski, dr inż. Jan Uniejowski, prof. dr hab. inż. Marek Domański, mgr inż. Andrzej Tomczak, mgr inż. Paweł Jakimiak, mgr Tomasz Kobierski nagrodził produkty 19 firm. Podczas targów rozpoczął się plebiscyt na najlepszy zdaniem konsumentów produkt spośród tegorocznych zdobywców Złotego Medalu. Zwiedzający targi mieli możliwość głosowania na swojego faworyta za pośrednictwem ekranów dotykowych zlokalizowanych w Strefie Mistrzów w centrum targowej ekspozycji.

Podsumowując, można powiedzieć, że tegoroczne targi SECUREX odniosły sukces. Świadczą o tym nie tylko liczby, ale przede wszystkim ciepłe słowa wystawców i zwiedzających.

Już dziś zapraszamy do uczestnictwa w kolejnej edycji targów SECUREX wiosną 2014 roku.

*Bezpośr. inf. Katarzyna Jardanowska*
*Zespół PR i Promocji Produktów*
*Products PR Team*


securex 2012
DEBATA
"PRAWO DLA MONITORINGU WIZYJNEGO?"
DEBATA
secure


ex 2012


POLON-ALFA
POLON-ALFA


ALNET


8A


Sate


Dream Toget


ULTIMODE


ZABEZPIECZENIA
zapraszamy na poklad


www.ast.pl


KABE


ESSER

secure


GUNNEBO
For a safer world
ARPOL
ZŁOTA ZBROJA
www.zsar.com.pl
www.aat.pl
KANTECH
BOSCH
Advantage Line
New products
camSAT
20 LAT DOŚWIADCZEŃ W OCHRONIE ZEWNĘTRZNEJ
ATLine
FLIR
www.atline.pl
OCHRONA JUWENTUS


maxto
Panasonic
maxto
make it work together
securex
GUNNEBO
alarmnet
www.alarmnet.com.pl
AXIS
roger
Systemy dostępu i rejestracji
ZEBRA
JANEX
ICS
POLSKA
euroalarm
Secure


OPTEX
Sensing Innovation
PROMET
securex
POLON-ALFA
BOSCH
www.aat.pl
fortec
SONY
make.believe
ex 2012


# Polski Mistrz Techniki Alarmowej 2012

## Nagroda honorowa stowarzyszenia POLALARM za publikacje fachowe w prasie branżowej

Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **„POLALARM"** organizuje konkurs *Polski Mistrz Techniki Alarmowej* od 1996 r. W bieżącym roku odbywa się jego XIV edycja.

Początkowo konkurs organizowany był wyłącznie dla polskich producentów (cztery pierwsze edycje w latach 1996–1999). W roku 2000 oceniano zarazem wyroby polskie i zagraniczne, a od 2001 roku wyroby produkcji polskiej i zagranicznej konkurowały już ze sobą bez podziału na grupy. Ta stopniowa ewolucja wprowadziła nas na arenę międzynarodową. Tak więc konkurs *Polski Mistrz Techniki Alarmowej* to wkład stowarzyszenia POLALARM w promowanie postępu technicznego w naszej branży. Wnikliwie oceniamy urządzenia do ochrony osób i mienia wprowadzane na polski rynek. Zgłoszenia do Konkursu ocenia 11-osobowa komisja, która od początku działa w prawie niezmienionym składzie.

Ogłoszenie wyników oraz wręczenie nagród i wyróżnień laureatom wszystkich edycji konkursu odbywa się zawsze w czasie Międzynarodowej Wystawy Zabezpieczeń „SECUREX" w Poznaniu.

W dniu 31 marca 2012 r. Komisja Konkursowa przyznała nagrody w konkursie *Polski Mistrz Techniki Alarmowej 2012* w poszczególnych kategoriach:

**1. Urządzenia i systemy sygnalizacji włamania i napadu**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za Alarm Control dla firmy Ochrona JUWENTUS z Warszawy,
– wyróżnienie specjalne komisji konkursowej za panel kontrolny KBPK–01 dla firmy Kabe z Mikołowa,
– wyróżnienie za klawiaturę dotykową TM 40 firmy Paradox Security Systems dla firmy I.C.S. Polska Hubert Durlik z Warszawy,
– podziękowanie za udział w konkursie i prezentację czujki ruchu BLUE LINE GEN2 dla firmy Robert Bosch.

**2. Urządzenia i systemy sygnalizacji pożarowej**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za system nagłośnieniowy Promatrix PM8000 dla firmy Robert Bosch,
– podziękowanie za udział w konkursie i prezentację konwencjonalnej centrali serii FPC500, FPC500-2, FPC500-4, FPC500-6 dla firmy Robert Bosch.

**3. Urządzenia i systemy nadzoru telewizyjnego i rejestracji obrazów**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za NBN-832 – dualną kamerę sieciową Dinion HD 1080p – dla firmy Robert Bosch,
– wyróżnienie za system sieciowej rejestracji wizji i dźwięku SRN-1670 wraz z oprogramowaniem zarządzającym Net-i Viewer dla firmy Ultrak Security Systems (Dołuje k/Szczecina).

**4. Urządzenia i systemy kontroli dostępu**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za redundantny system kontroli dostępu amerykańskiej firmy PCSC (na bazie urządzeń serii Fault Tolerant) dla firmy VOLTA z Warszawy.

**5. Zintegrowane systemy sygnalizacji zagrożeń**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za bezzałogowy helikopter KBUAV-01 dla firmy KABE z Mikołowa,
– wyróżnienie za zintegrowany system monitorowania bezobsługowych obiektów teleinformatycznych lub energetycznych dla firmy Electronic Power and Market ze Szczecinka,
– Wyróżnienie za NICE Situator – platformę programową klasy PSIM umożliwiającą zarządzanie sytuacją i zdarzeniami – dla firmy ISM EuroCenter z Warszawy.

**6. Urządzenia i systemy transmisji alarmu oraz monitoringu**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za zintegrowany system monitorowania bezobsługowych obiektów teleinformatycznych lub energetycznych dla firmy Electronic Power and Market ze Szczecinka,
– wyróżnienie specjalne Komisji Konkursowej za zintegrowany system monitorowania bezobsługowych obiektów teleinformatycznych lub energetycznych dla firmy Electronic Power and Market ze Szczecinka,
– wyróżnienie za zaawansowany system zarządzania budynkiem Vision BMS dla firmy APA z Gliwic,
– podziękowanie za udział w konkursie i prezentację zdalnej konfiguracji central alarmowych


z użyciem nadajnika LX20G-3C dla firmy EBS z Warszawy.

**7. Inne urządzenia i systemy technicznej ochrony oraz wspomagające ochronę fizyczną**

– I miejsce oraz tytuł Polskiego Mistrza Techniki Alarmowej 2012 za Księgę Wejść/Wyjść dla firmy RegiTech z Wrocławia.

Spośród zdobywców pierwszych miejsc w poszczególnych kategoriach komisja wyłoniła zwycięzcę konkursu i przyznała główną nagrodę – Złotą Zbroję. **Laureatem Złotej Zbroi w konkursie *Polski Mistrz Techniki Alarmowej 2012*, przyznanej za bezzałogowy helikopter KBUAV-01, została firma KABE z Mikołowa.**

## Nagroda honorowa stowarzyszenia POLALARM za publikacje fachowe w prasie branżowej

Od 2003 roku stowarzyszenie POLALARM przyznaje również honorową nagrodę stowarzyszenia za publikacje fachowe w prasie branżowej, by uhonorować dorobek redaktorski autorów najbardziej poczytnych i wartościowych artykułów dla specjalistów branży technicznej ochrony osób i mienia w Polsce. Kapituła Nagrody od samego początku pracuje w niezmienionym 6-osobowym składzie.

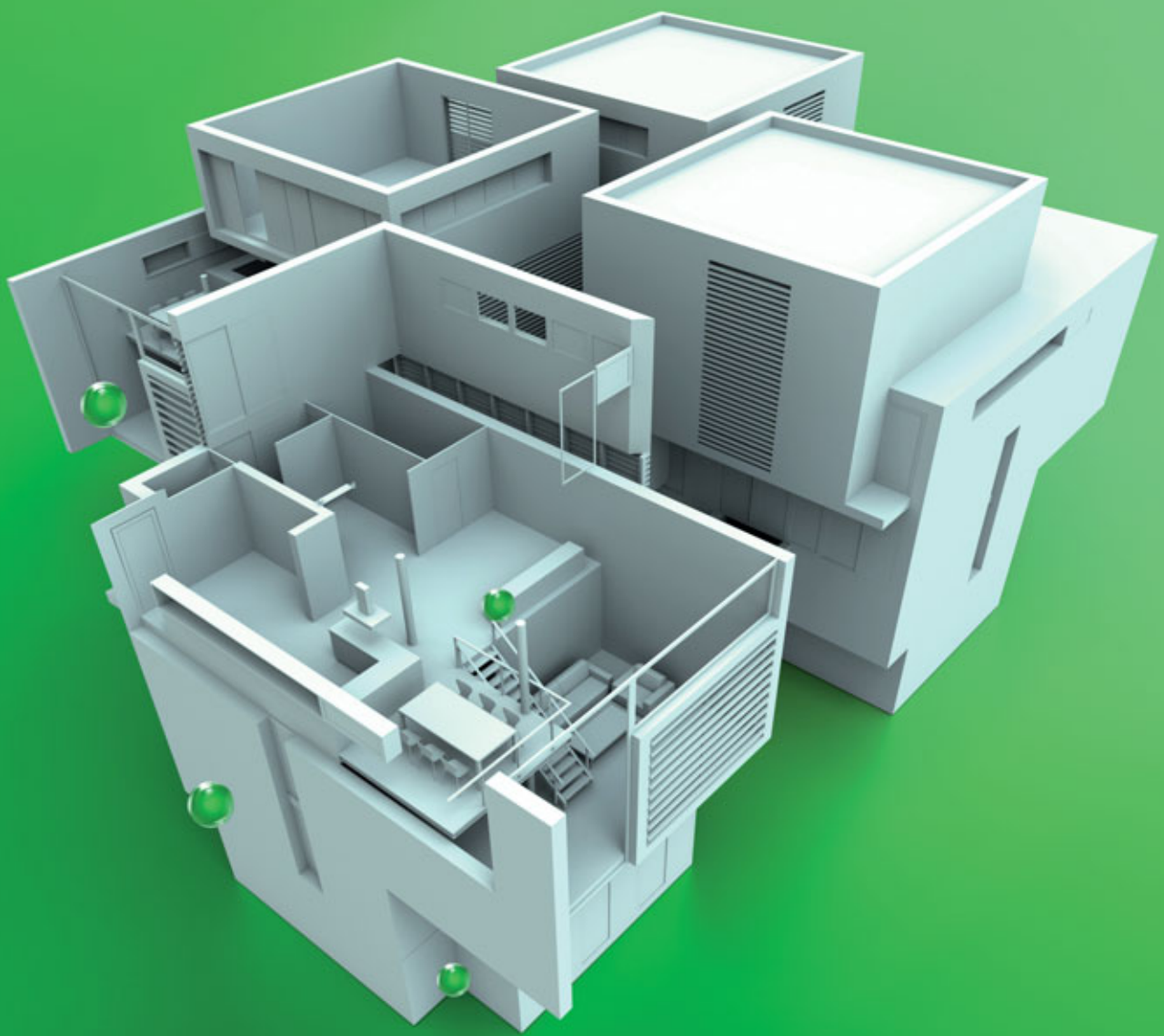
**Laureatem tegorocznej nagrody został Waldemar Fiałka** za rzetelne i bezstronne propagowanie nowoczesnych metod projektowania elektronicznych systemów dozorowych, ciekawy dobór tematów i wnikliwą analizę omawianych zagadnień w artykułach pisanych z pożytkiem dla wszystkich specjalistów branży technicznej ochrony osób i mienia w Polsce.

Praca Komisji Konkursowej i Kapituły Nagrody to również ogromny wkład w promowanie nowych rozwiązań ułatwiających ochronę osób i mienia, a także w popularyzację wybitnie użytecznych osiągnięć technicznych.

*Bezpośr. inf. POLALARM*

Redakcja *Zabezpieczeń* gratuluje wszystkim nagrodzonym i wyróżnionym w konkursie, a panu Waldemarowi Fiałce życzymy jeszcze wielu ciekawych publikacji.

# Alternatywne projektowanie systemów kontroli dostępu



Adam Rosiński, Martyna Balejko

W artykule omówiono zagadnienia związane z systemami kontroli dostępu (KD). Systemy te scharakteryzowano ze szczególnym uwzględnieniem jednostronnej i dwustronnej kontroli dostępu. Przedstawiono także możliwość projektowania indywidualnych systemów KD uwzględniających specyficzne wymagania inwestora (zarówno w aspekcie budowlanym, jak też funkcjonalnym)

## 1. Wprowadzenie

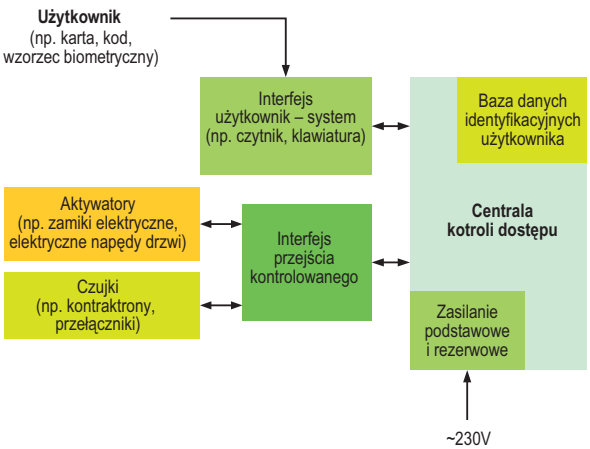
System kontroli dostępu to zestaw urządzeń i oprogramowania mający za zadanie:

a) identyfikację osób albo pojazdów uprawnionych do przekroczenia granicy obszaru chronionego oraz umożliwienie im wejścia/wyjścia,
b) niedopuszczenie do przekroczenia granicy obszaru chronionego przez osoby albo pojazdy nieuprawnione,
c) wytworzenie sygnału alarmowego informującego o próbie przekroczenia granicy obszaru chronionego przez osobę albo pojazd nieuprawniony.

Na rys. 1 przedstawiono uproszczony schemat blokowy systemu kontroli dostępu [4,9]. Użytkownik, który chce przejść przez przejście kontrolowane, musi potwierdzić swoją tożsamość. Może to uczynić np. poprzez przyłożenie karty zbliżeniowej (coś, co mam), podanie kodu (coś, co wiem) lub pozwolenie na odczytanie cechy biometrycznej (kim jestem) [8]. Interfejs przesyła odczytaną informację do centrali kontroli dostępu, gdzie zostaje ona porównana z wcześniej zaprogramowanymi i zapamiętanymi danymi użytkownika. Jeśli jest ona zgodna, to poprzez interfejs przejścia kontrolowanego następuje uruchomienie aktywatorów przejścia (np. otwarcie zamka elektrycznego czy włączenie elektrycznego napędu otwierającego drzwi). Jeśli informacja nie jest zgodna z zarejestrowanymi wcześniej danymi, to użytkownik nie może przejść, ponieważ nie nastąpi uruchomienie aktywatorów przejścia. W systemie kontroli dostępu są także czujki, które określają, czy drzwi zostały zamknięte po przejściu uprawnionej osoby albo czy nie zostały otwarte w sposób niedozwolony (np. siłowy). W systemie może występować także moduł komunikacji z innymi centralami kontroli dostępu i innymi systemami zarządzania bezpieczeństwem budynku (np. systemem sygnalizacji włamania i napadu, systemem sygnalizacji pożarowej, systemem monitoringu wizyjnego itp.).

Systemy kontroli dostępu można podzielić:

– ze względu na funkcję:
  - kontrola obszaru (grupa pomieszczeń),
  - kontrola pomieszczenia,
– ze względu na wyposażenie:
  - przejście kontrolowane jednostronnie,
  - przejście kontrolowane dwustronnie.



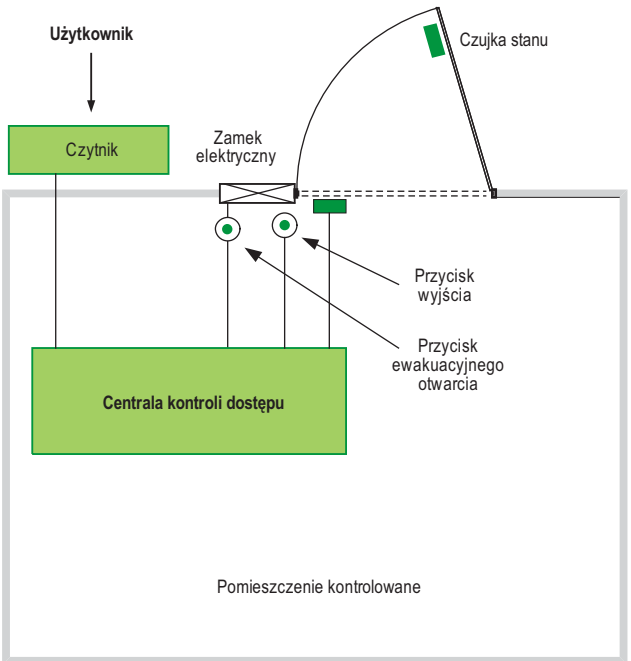

*Rys. 1. Uproszczony schemat blokowy systemu kontroli dostępu*

Przejście kontrolowane zazwyczaj jest wyposażone w:

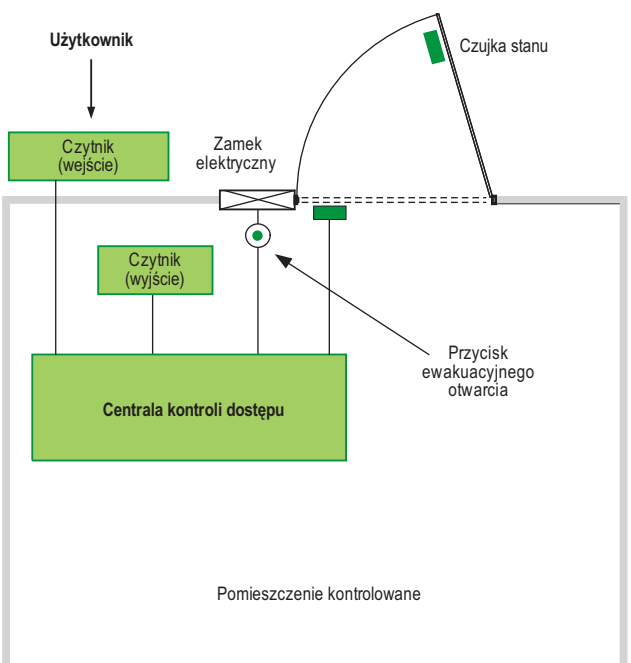
– czytnik (coraz częściej biometryczny),
– czujki stanu skrzydła drzwi,
– przycisk otwarcia,
– przycisk ewakuacyjnego otwarcia drzwi (wymagania ppoż.),
– element ryglujący (np. rygiel, zwora, zamek),
– samozamykacz (jednofazowy lub dwufazowy),
– pochwyt (pochwyty).

Rys. 2 obrazuje wyposażenie przejścia kontrolowanego jednostronnie. Składa się ono z centrali kontroli dostępu, do której podłączone są:

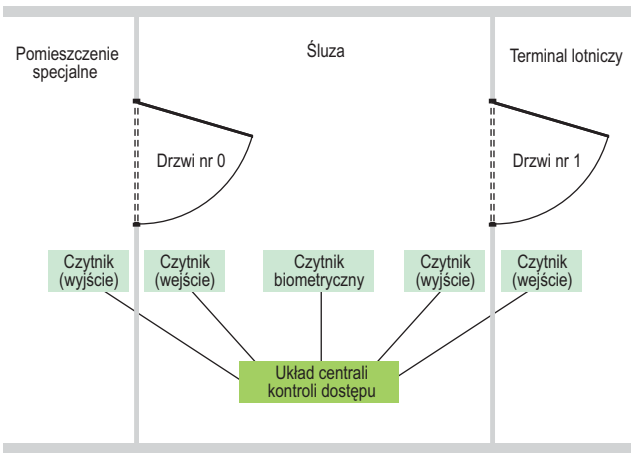
– czytnik (np. kart, kodu, biometryczny),
– aktywator (np. zamek elektryczny, rygiel, elektrozwora),




*Rys. 2. Przykładowe wyposażenie przejścia kontrolowanego jednostronnie*




*Rys. 3. Przykładowe wyposażenie przejścia kontrolowanego dwustronnie*




*Rys. 4. Koncepcja śluzy pomieszczenia specjalnego w terminalu lotniczym*

– czujka stanu zamknięcia drzwi,
– przycisk wyjścia,
– przycisk ewakuacyjnego otwarcia (w przypadku zamka typu NO).

Rys. 3 obrazuje wyposażenie przejścia kontrolowanego dwustronnie. Składa się ono z centrali kontroli dostępu, do której podłączone są:

– czytniki: wejście i wyjście (np. czytnik kart, kodu, biometryczny),
– aktywator (np. zamek elektryczny typu NO, rygiel typu NO, elektrozwora),
– czujka stanu zamknięcia drzwi,
– przycisk ewakuacyjnego otwarcia.

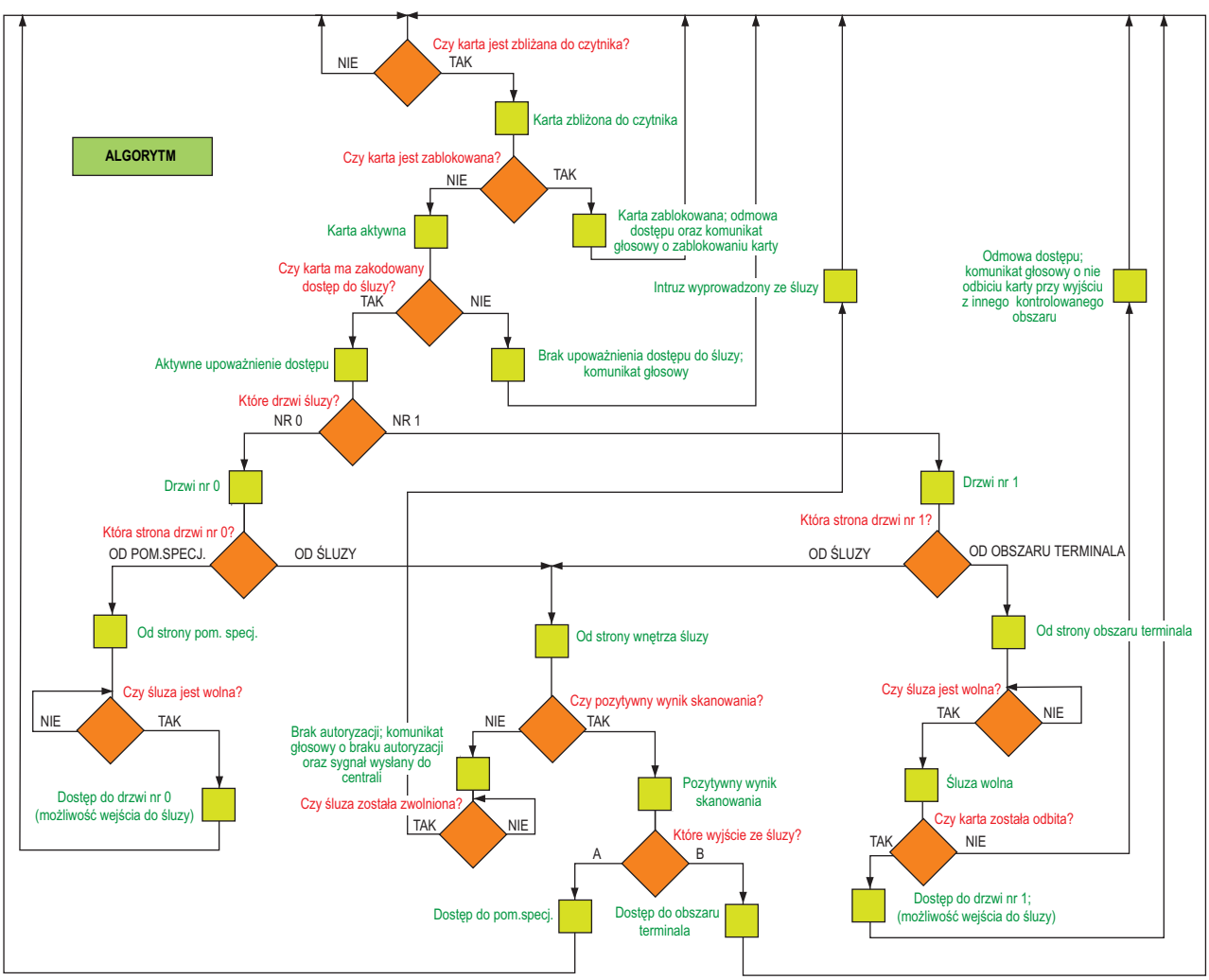
Obecnie w systemach KD coraz częściej stosuje się biometrię [2,10]. Pozwala ona na precyzyjną identyfikację osób dzięki sprawdzeniu ich niepowtarzalnych, charakterystycznych cech anatomicznych. Sprawdzane mogą być m.in.:

– geometria dłoni,
– linie papilarne,
– geometria twarzy,
– geometria ucha,
– geometria ust,
– budowa oka (cechy charakterystyczne tęczówki i siatkówki oka),
– układ żył nadgarstka,
– barwa głosu.

Do cech behawioralnych można zaliczyć m.in.:

– mowę,
– ruch ust,
– ruch gałki ocznej,
– pismo,
– chód.

Czytniki biometryczne znalazły wiele zastosowań. W systemach kontroli dostępu są stosowane już od lat siedemdziesiątych ubiegłego wieku. Początkowo (ze względu na




*Rys. 5. Algorytm autorskiego układu systemu KD*

wysokie koszty) instalowano je tylko w systemach przeznaczonych dla obiektów wymagających specjalnych zabezpieczeń gwarantujących wysoki poziom bezpieczeństwa. Dzięki bardzo szybkiemu rozwojowi technologii mikroprocesorowych układów elektronicznych w ostatnich latach, a przez to tańszym produktom, cena czytników biometrycznych zdecydowanie obniżyła się, a ich precyzja i niezawodność działania bardzo wzrosły. Dzięki temu można stosować je w wielu systemach przeznaczonych dla różnych odbiorców.

## 2. Projektowanie systemów kontroli dostępu uwzględniających wymagania inwestora

Przedstawiamy autorski projekt systemu kontroli dostępu, który uwzględnia niepowtarzalne wymagania inwestora [1].

Projekt obejmuje specjalistyczny układ sterowania dostępem do śluzy znajdującej się w budynku terminalu portu lotniczego (rys. 4). Z uwagi na duże zagrożenie terroryzmem [3] wymagania dotyczące bezpieczeństwa są szczególne. Śluza jest barierą oddzielającą pomieszczenie specjalne o wysokim poziomie kontroli dostępu od pozostałej części terminalu. Wyposażona jest w dwoje drzwi, z których każde jest wyposażone w parę modułów kontrolera przejścia (czytniki). Moduły rozmieszczone są po obu stronach drzwi. Pomiędzy drzwiami jest niewielka przestrzeń, w której odbywa się proces skanowania (potwierdzenia tożsamości) użytkownika, który posługuje się danym identyfikatorem. Weryfikacja przebywającej w śluzie osoby polega na przeskanowaniu tęczówki oka i porównaniu wyników z danymi z bazy danych. W danej chwili w śluzie mogą być otwarte tylko jedne drzwi, a wewnątrz może przebywać tylko jedna osoba.

Zaprojektowany układ sprawdza, czy identyfikator (karta zbliżeniowa) użytkownika jest zbliżany do czytnika. Jeśli tak, to następuje zweryfikowanie, czy karta nie jest zablokowana. W przypadku jej zablokowania generowany jest komunikat głosowy informujący o blokadzie i braku dostępu. Jeśli natomiast nie ma blokady, układ sprawdza, czy w identyfikatorze jest zakodowany dostęp do danej śluzy. Jeżeli nie, to wygenerowany zostanie komunikat głosowy o braku upoważnienia do dostępu do śluzy. W przeciwnym razie układ sprawdza, do której grupy modułów wejściowych (grupa modułów drzwi nr 0 albo nr 1) zbliżany jest identyfikator. Potem sprawdza, do którego konkretnie modułu zbliżana jest karta – czy jest to moduł znajdujący się wewnątrz czy na zewnątrz śluzy. Gdy prośba o dostęp jest skierowana z zewnętrznej strony śluzy, kontrolowana jest jej zajętość. W przypadku prośby od strony pomieszczenia specjalnego dostęp jest umożliwiany automatycznie, po stwierdzeniu nieobecności innego użytkownika wewnątrz śluzy. Jeśli natomiast użytkownik chce uzyskać dostęp od strony terminalu, następuje dodatkowe sprawdzenie, czy dana karta została „odbita" przy wyjściu z innego kontrolowanego obszaru. Jeśli taka czynność nie została wykonana, wygenerowany jest odpowiedni komunikat głosowy. W przeciwnym razie użytkownik uzyskuje dostęp do śluzy. Jeżeli użytkownik znajduje się wewnątrz śluzy, układ kontroluje poprawność skanowania. W przypadku braku autoryzacji wygenerowany

zostaje komunikat głosowy, który powiadamia o tym fakcie, a do centrali wysyłany jest sygnał. Inni użytkownicy mają dostęp do śluzy wyłącznie po wyprowadzeniu intruza przez odpowiednie służby. W przypadku pozytywnego wyniku weryfikacji układ ponownie sprawdza, do których drzwi (ich czytników) zbliżona jest karta i zezwala – odpowiednio – na wejście do pomieszczenia specjalnego bądź na teren terminalu.

Algorytm działania układu realizującego funkcje projektowanego systemu kontroli dostępu pokazano na rys. 5.

Weryfikacja układu w trybie symulacji funkcjonalnej została przedstawiona na rys. 6, natomiast przebieg symulacji czasowej po przeprowadzeniu syntezy i implementacji układu został przedstawiony na rys. 7.

## 3. Zakończenie i wnioski

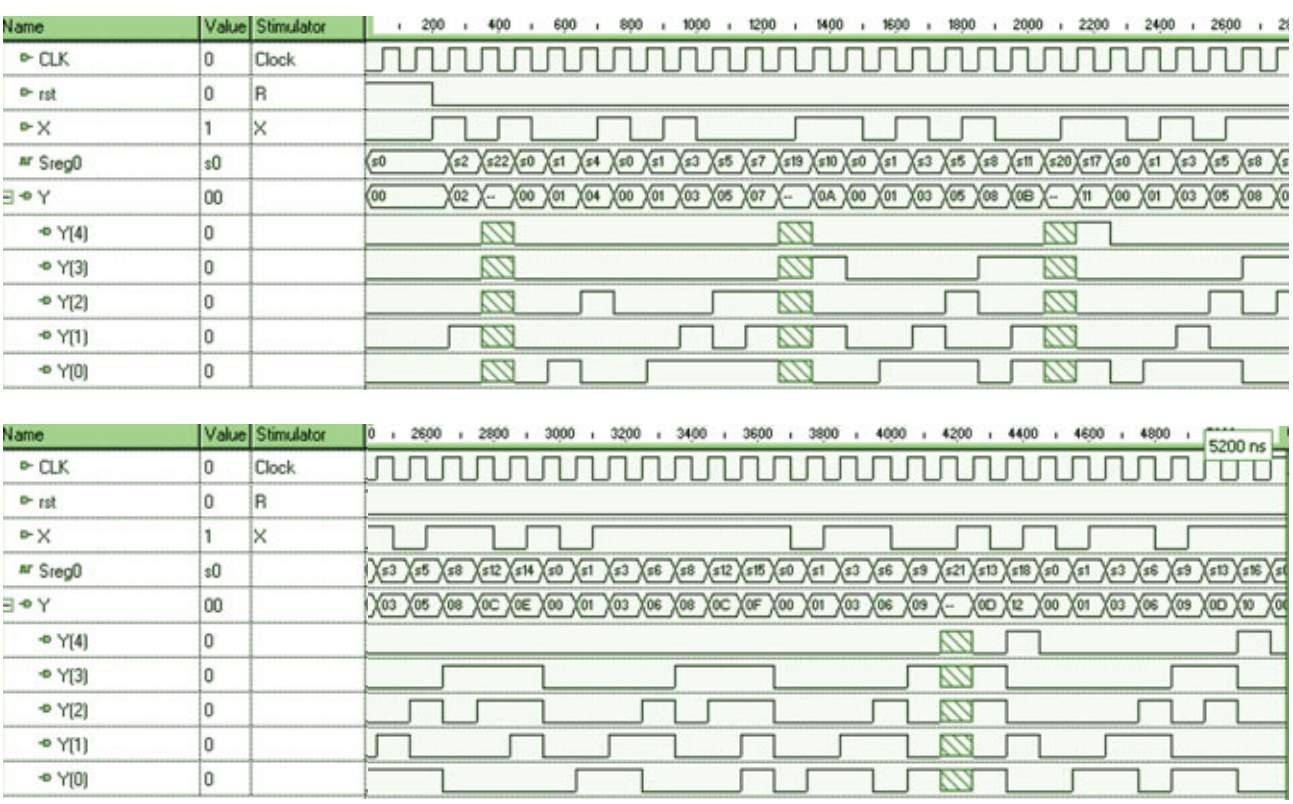
W artykule przedstawiono autorski projekt układu elektronicznego realizującego funkcje systemu kontroli dostępu. Dzięki niemu osiągnięto funkcjonalność, którą trudno było uzyskać w przypadku zastosowaniu standardowych rozwiązań służących do kontroli dostępu, oferowanych przez producentów. Istniała oczywiście możliwość opracowania tego rozwiązania w postaci aplikacji informatycznej, która realizowałaby założone funkcje, jednakże wymagałoby to zastosowania komputera, który mógłby być słabym ogniwem całego systemu. Z tego powodu zdecydowano się na rozwiązanie sprzętowe, które jest bardziej niezawodne i działa znacznie szybciej. Istnieje już kilka analiz dotyczących niezawodności jego funkcjonowania [5,6,7].

Ukazana metodyka projektowania autorskich układów realizujących funkcje systemów kontroli dostępu pozwala stwierdzić, iż istnieje możliwość projektowania systemów bezpieczeństwa, które mogą wykorzystywać autorskie prototypy układów elektronicznych realizujących funkcje niedostępne w rozwiązaniach producenckich. Należy jednak pamiętać, iż nie są one poddane badaniom na zgodność z odpowiednimi normami. Niemniej jednak czasami zachodzi potrzeba zastosowania tego typu rozwiązań.

*dr inż. Adam Rosiński*
*inż. Martyna Balejko*
*Politechnika Warszawska*
*Wydział Transportu*
*Zakład Telekomunikacji w Transporcie*

## Bibliografia

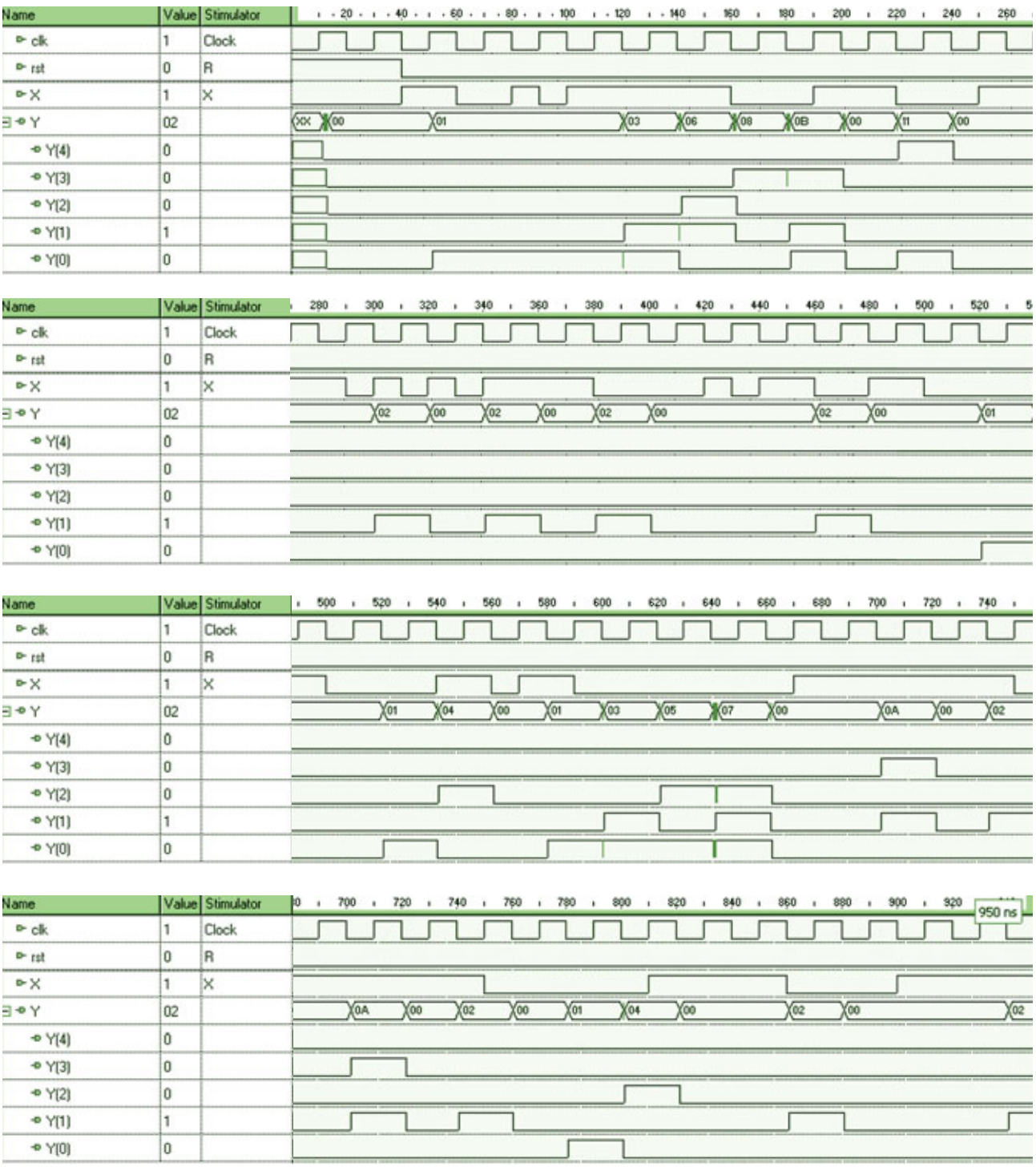
1) Balejko M., *Projekt specjalizowanego układu sterującego dostępem do śluzy*, Politechnika Warszawska, Wydział Transportu, Warszawa 2011.
2) Dunstone T., Yager N., *Biometric System and Data Analysis*, Springer, 2009.
3) Hołyst B., *Terroryzm. Tom 1 i 2*, Wydawnictwa Prawnicze LexisNexis, Warszawa 2011.
4) PN-EN 50133-1:2007 *Systemy alarmowe. Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia. Część 1. Wymagania systemowe.*
5) Rosiński A., *Design of the electronic protection systems with utilization of the method of analysis of reliability structures*, Nineteenth International Conference On Systems Engineering (ICSEng 2008), Las Vegas, USA 2008.
6) Rosiński A., *Reliability analysis of the electronic protection systems with mixed m–branches reliability structure*, International Conference European Safety and Reliability (ESREL 2011), Troyes, France 2011.




*Rys. 6. Przebieg symulacji funkcjonalnej układu systemu KD*

Referat został opublikowany pod tytułem *Reliability analysis of the electronic protection systems with mixed m–branches reliability structure. Advances in Safety, Reliability and Risk Management*, Berenguer, Grall & Guedes Soares, Taylor & Francis Group, London, UK 2012.

7) Rosiński A., *Reliability analysis of the electronic protection systems with mixed – three branches reliability structure*, International Conference European Safety and Reliability (ESREL 2009), Prague, Czech Republic 2009. Referat został opublikowany pod tytułem *Reliability analysis of the electronic protection systems with mixed – three branches reliability structure. Reliability, Risk and Safety. Theory and Applications*. Volume 3, R. Bris, C. Guedes Soares & S. Martorell, CRC Press/Balkema, London, UK 2010.
8) Siergiejczyk M., Rosiński A., *Analiza funkcjonalna systemu kontroli dostępu w aspekcie bezpieczeństwa systemów telematycznych*, XL Zimowa Szkoła Niezawodności, Szczyrk 2012.
9) Szulc W., Rosiński A., *Koncepcja systemu kontroli dostępu w obiekcie specjalnego przeznaczenia*, I Krajowa Konferencja ARCHBUD 2008, Zakopane 2008.
10) Tistarelli M., Li S Z., Chellappa R., *Handbook of Remote Biometrics for Surveillance and Security*, Springer-Verlag, 2009.




*Rys. 7. Przebieg symulacji czasowej układu systemu KD*

# HD-SDI w praktyce

Andrzej Walczyk

Tytuł tego artykułu jest nieco przewrotny, gdyż HD-SDI ma się do praktyki tak, jak przysłowiowa pięść do oka. Jak dotychczas nie spotkałem się z ani jednym wizyjnym systemem dozorowym wykorzystującym tę technologię. Za to w materiałach marketingowych publikowanych przez niedoszłych dystrybutorów urządzeń HD-SDI natrafia się na stwierdzenia, z których jasno wynika, że technologia HDI-SDI cieszy się ogromnym zainteresowaniem instalatorów i administratorów systemów CCTV. Niestety prawda jest taka, że wszystko kończy się na zainteresowaniu

HD symbolizuje telewizję o wysokiej rozdzielczości, zaś SDI oznacza szeregowy interfejs cyfrowy służący do transmisji zakodowanych sygnałów wizyjnych na niewielkie odległości. Interfejs SDI jest masowo wykorzystywany do tworzenia połączeń pomiędzy profesjonalnymi urządzeniami stanowiącymi wyposażenie studiów telewizyjnych lub wozów transmisyjnych. Ze względu na to, że podczas realizacji programu telewizyjnego wykorzystywanych jest wiele różnorodnych urządzeń, zaś odległości między tymi urządzeniami są niewielkie, interfejs SDI operuje strumieniem nieskompresowanych danych cyfrowych. W ten sposób unika się konieczności wielokrotnego kodowania i rozkodowywania tych samych danych przy ich przechodzeniu z jednego urządzenia do drugiego. Brak kompresji powoduje, że przepływność związana z transmisją obrazów o wysokiej rozdzielczości dochodzi do 1,5 Gb/s, jednak w warunkach studyjnych nikomu to nie przeszkadza, gdyż profesjonalne urządzenia telewizyjne są z natury przystosowane do obróbki dużych strumieni danych.

Jak dotychczas stosowanie interfejsu SDI w innych dziedzinach techniki napotykało ograniczenia natury formalnej, związane z obwarowaniami licencyjnymi, przez co ten rodzaj transmisji był wykorzystywany jedynie w profesjonalnym sprzęcie telewizyjnym. Obecnie sytuacja uległa zmianie i na rynku konsumenckim pojawiły się odtwarzacze przeznaczone do pracy w systemach kina domowego, transmitujące dane cyfrowe do monitorów lub projektorów wizyjnych za pośrednictwem interfejsów SDI. Podjęte zostały próby adaptacji interfejsów SDI do pracy w wizyjnych systemach dozorowych.

Zastanówmy się teraz nad tymi cechami technologii HD-SDI, które są uporczywie eksponowane w materiałach marketingowych, i spróbujmy znaleźć odniesienie do realnych warunków pracy urządzeń stosowanych w wizyjnych systemach dozorowych.

## Możliwość stosowania kabla koncentrycznego

Jak wiadomo, w warstwie fizycznej interfejsu SDI wykorzystywane są popularne złącza BNC oraz kable koncentryczne o impedancji falowej 75 Ω. Czy aby na pewno są to typowe kable koncentryczne? Prawda jest taka, że do transmisji danych cyfrowych z przepływnością rzędu 1,5 Gb/s konieczne jest stosowanie specjalnych kabli koncentrycznych i właśnie takie specjalne kable są używane w instalacjach studyjnych.

W materiałach marketingowych promujących stosowanie technologii HD-SDI w wizyjnych systemach dozorowych często powtarzany jest argument, że instalatorzy, którzy zdecydują się na modernizację starych systemów monitoringu wizyjnego, mogą posłużyć się istniejącymi kablami koncentrycznymi, nikt jednak nie wypowiada się na temat rodzaju i jakości tych kabli. Wiadomo, że do poprawnej transmisji danych cyfrowych z przepływnością rzędu 1,5 Gb/s konieczne jest zapewnienie małej tłumienności i płaskiej charakterystyki amplitudowo-fazowej toru kablowego w widmie sięgającym kilkudziesięciu MHz. Takich warunków nie spełniają żadne popularne kable koncentryczne stosowane w analogowych systemach dozorowych. Sytuację pogarsza fakt, że tłumienność starych kabli koncentrycznych, poddanych wieloletniemu działaniu naturalnych czynników środowiskowych, rośnie i osiąga wartości nieakceptowalne nawet w przypadku systemów analogowych. Słowem – stare kable koncentryczne powinny być okresowo wymieniane na nowe. Propozycja ich zastosowania w systemach HD-SDI zakrawa na ironię.

## Jakość obrazu

Często przytaczanym argumentem jest wysoka jakość obrazu przekazywanego przez interfejs SDI związana z brakiem kompresji sygnału wizyjnego. Owszem, jakość obrazu rzeczywiście jest wysoka, ale tylko do momentu, gdy sygnał wizyjny zostanie przetransmitowany do urządzenia końcowego, na przykład do rejestratora. Tam pierwszą operacją jest kompresja obrazu, najczęściej przeprowadzana metodą H.264, bowiem trudno sobie wyobrazić możliwość dalszej transmisji lub rejestracji gigantycznego strumienia danych cyfrowych o przepływności 1,5 Gb/s. Innymi słowy, z nieskompresowanym obrazem, odznaczającym się bardzo wysoką jakością, mamy do czynienia tylko na odcinku między gniazdem wyjściowym kamery a gniazdem wejściowym rejestratora. Tego obrazu nikt nie ogląda, gdyż ma on postać strumienia danych przepływającego przez kabel koncentryczny. Obraz pojawiający się na ekranie monitora systemowego powstaje w wyniku kompresji i dalszej obróbki sygnału doprowadzanego do interfejsu SDI, tak więc jego jakość niczym nie różni się od jakości obrazów uzyskiwanych w sieciowych systemach dozorowych.

Kompresja strumienia danych o przepływności rzędu 1,5 Gb/s wymaga zastosowania bardzo wydajnych procesorów sygnałowych, co z kolei powoduje komplikację konstrukcji rejestratorów i wzrost kosztów ich produkcji. Z tego powodu w tańszych modelach rejestratorów z interfejsami SDI skuteczność kompresji jest ograniczona, a to pociąga za sobą konieczność stosowania rozbudowanych banków dysków twardych, czyli wiąże się ze wzrostem kosztów przechowywania nagrań.

Warto podkreślić, że jednym z sugerowanych zastosowań kamer z interfejsami SDI jest wykorzystanie ich w systemach obserwacyjnych instalowanych w salonach gier i w kasynach. Aktualne przepisy zmuszają administratorów takich obiektów do przechowywania nagrań ze wszystkich kamer przez okres czterech lat. Czy ktoś o zdrowych zmysłach bierze pod uwagę możliwość realizacji tego zadania bez bardzo wydajnej kompresji obrazów dostarczanych przez kamery? Czy argumentacja opierająca się na możliwości uzyskania obrazów o wysokiej jakości przez zaniechanie kompresji sygnału wizyjnego ma w ogóle jakikolwiek sens?

## Niskie koszty inwestycji

Często przytaczanym argumentem jest niska cena kamer HD z interfejsem SDI. Owszem, tego typu kamery mogą być relatywnie tanie, gdyż nie zawierają żadnych układów kodujących, kompresujących ani zamieniających sygnał wizyjny na postać możliwą do przetransmitowania za pośrednictwem sieci IP. Jednakże kamery są jedynym tanim elementem takiego systemu dozorowego. Uwzględniając koszty wynikające z konieczności stosowania specjalnych kabli koncentrycznych, a także koszty związane z zakupem odpowiednich rejestratorów, do ceny każdej kamery należy dodać minimum 600 EUR. Jeśli jeszcze doliczymy do tego koszty związane z kupnem dysków twardych niezbędnych do rejestracji słabo skompresowanych obrazów, koszty systemu wykorzystującego technologię HD-SDI będą porównywalne z kosztami realizacji sprawnego systemu sieciowego o znacznie lepszych właściwościach użytkowych.

## Praca w czasie rzeczywistym

Orędownicy systemów wykorzystujących technologię HD-SDI często powołują się na płynność ruchu obrazu telewizyjnego i jego wysoką poklatkowość. Są to niewątpliwe zalety, istotne w przypadku systemów kina domowego lub podczas oglądania programu telewizyjnego, gdy korzystamy z telewizorów szerokoekranowych. W odniesieniu do pozostałych przypadków taka argumentacja zawodzi. Celem wizyjnych systemów dozorowych jest podnoszenie poziomu bezpieczeństwa na obserwowanych obszarach, dlatego nie zawsze wymagane jest tworzenie płynnych, ruchomych obrazów o wysokiej poklatkowości – często wystarcza prędkość transmisji obrazów mieszcząca się w zakresie od kilku do kilkunastu klatek na sekundę. Ponadto brak możliwości uzależnienia prędkości transmisji obrazów od ich treści prowadzi do wielogodzinnej rejestracji identycznych, nieruchomych scen, co było zmorą analogowych systemów dozorowych. Na koniec warto dodać, że do rejestracji obrazów o stałej, wysokiej poklatkowości, typowych dla kamer HD-SDI, konieczne jest zastosowanie rozbudowanych banków dysków twardych. Wspomnianych wad nie mają sieciowe systemy monitoringu wizyjnego, w których poklatkowość obrazu może być dynamicznie dostosowywana do zmieniających się warunków obserwacyjnych.

## Zapomnij o IP

Często przytaczanym argumentem mającym przemawiać na korzyść kamer z interfejsami SDI jest możliwość projektowania i instalowania systemów dozorowych przez osoby niedysponujące żadną wiedzą na temat budowy i działania sieci IP. Pokrętność takiej argumentacji przypomina próby czynienia cnoty z czyjejś niewiedzy, czego osobiście nie akceptuję, tym bardziej, że o IP i tak nie da się zapomnieć, bo rejestratory z interfejsami SDI prędzej czy później muszą być podłączone do sieci w celu udostępnienia lub archiwizacji zapisanych obrazów.

## Dostępność elementów składowych

W najnowszych publikacjach poświęconych technologii HD-SDI spotyka się stwierdzenia, że odpowiedni sprzęt jest już dostępny na rynku, a jeśli nie jest dostępny, to wkrótce będzie, gdyż ta rewolucyjna technologia zdominuje całą branżę systemów monitoringu wizyjnego. W praktyce nie zauważa się takiej tendencji. Pierwsze kamery HD-SDI opracowane z myślą o systemach dozorowych zostały zaprezentowane na targach IFSEC już w 2009 roku, jednak żaden z liczących się producentów nie uwzględnił ich w swoich rozwiązaniach. Obecnie kamery i rejestratory wykorzystujące interfejsy SDI są oferowane jedynie przez producentów dalekowschodnich i nic nie wskazuje na to, że ta sytuacja ulegnie zmianie.

Asortyment tych wyrobów jest bardzo wąski – przeważnie są to klasyczne kamery stałopozycyjne, rzadziej kopułkowe, zaś szybkoobrotowych kamer PTZ praktycznie nikt nie oferuje. Brakuje przełączników wizji lub krosownic pracujących w tym standardzie, zaś wybór rejestratorów jest niewielki. Przeważnie są to rejestratory czterokanałowe, rzadziej ośmiokanałowe lub szesnastokanałowe, jednak ich wysokie ceny nie stanowią zachęty dla projektantów i instalatorów systemów dozorowych. Najnowszą, ciekawą propozycją rynkową są rejestratory z czternastoma wejściami analogowymi i dwoma interfejsami SDI. Jak widać, producenci próbują uatrakcyjnić swoją ofertę, jednak – pomimo tego – rozwiązania wykorzystujące technologię HD-SDI stanowią absolutny margines.

Jak na ironię, stopniowo odchodzi się od wykorzystania interfejsów SDI do transmitowania sygnałów wizyjnych w profesjonalnym sprzęcie studyjnym. Transmituje się je przez sieć Gigabit Ethernet.

## Konkluzja

Pomimo tak oczywistych wad systemów dozorowych wykorzystujących technologię HD-SDI nie należy całkowicie wykluczać możliwości stosowania kamer z interfejsami SDI w szczególnych, wyjątkowych sytuacjach. Na przykład może to dotyczyć bardzo prostych systemów obserwacyjnych, stanowiących połączenie pojedynczej kamery z monitorem, w których wymagana jest wysoka jakość obrazów, zaś zagadnienia związane z transmisją, rejestracją i archiwizacją tych obrazów nie są istotne. Kamery z interfejsami SDI znajdują zastosowanie w systemach telekonferencyjnych, gdyż są kompatybilne z profesjonalnymi urządzeniami studyjnymi i dzięki temu mogą być wykorzystywane podczas transmisji telewizyjnych z sal obrad. Nie ma to jednak wiele wspólnego z wizyjnymi systemami dozorowymi.

*Andrzej Walczyk*

profesjonalne rozwiązania
do cyfrowej rejestracji obrazu

ponad 60 000 instalacji
pracujących na całym świecie

www.alnetsystems.com

ALNET SYSTEMS


sieciowe oprogramowanie do cyfrowej rejestracji obrazu — NS NETSTATION

hybrydowy system do cyfrowej rejestracji obrazu — NET HYBRID

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

profesjonalne oprogramowanie klienckie — CMS PROFESSIONAL

oprogramowanie klienckie dla urządzeń mobilnych — CMS MOBILE

blisko 1000 kamer zintegrowanych
z oprogramowaniem Alnet Systems

wybór należy do Ciebie!

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

# Zasady realizacji projektów

Daniel Kamiński

W branży zabezpieczeń technicznych wyszczególnić można trzy rodzaje projektów: projekty małe, których czas realizacji wynosi kilka dni, a budżet nie przekracza 50 tys. zł; projekty średnie, których czas realizacji nie przekracza trzech miesięcy, a koszty 1 mln zł; oraz projekty duże, które mogą być realizowane nawet 2–3 lata, a ich koszty sięgają 50 mln zł i więcej

Na rynku zabezpieczeń prowadzonych jest znacznie więcej małych projektów, ale dla wykonania rocznego obrotu rzędu 10 mln zł trzeba ich zrealizować około 400. Taki sam obrót można uzyskać przez wykonanie ok. 25 średnich lub 5 dużych instalacji. Z tego punktu widzenia wykonywanie średnich i dużych projektów wygląda atrakcyjnie, wymaga jednak odmiennego – projektowego – podejścia, ponieważ opóźnienie lub przerwanie realizacji projektu będzie mieć bardzo duży ujemny wpływ na wyniki firmy. Jest to ważne m.in. dlatego, że według statystyk z rynku IT aż połowa projektów jest zawieszana lub porzucana w trakcie realizacji.

Głównymi przyczynami przerywania realizacji projektów lub wycofywania się z nich są: brak wystarczających informacji wejściowych od klienta, źle zdefiniowane jego potrzeby, niewłaściwie postawione zadania, nieefektywne wdrożenia oraz obawy związane z faktycznym i formalnym zakończeniem projektu (rozliczeniami, zakończeniem finansowania, koniecznością usuwania usterek itp.). Zwykle przyczyny te nawarstwiają się, gdy na stanowisko kierownika projektu wybierze się niewłaściwą osobę, która na dodatek nie uzyska wsparcia ze strony zarządu firmy.

Dobór właściwego kandydata na stanowisko kierownika projektu ma kluczowe znaczenie dla realizacji projektu. Przy prawidłowym zarządzaniu projektem można znacząco ograniczyć koszty wykonania, skrócić czas realizacji – zwiększając uzyskiwaną na projekcie marżę – a przy właściwych działaniach marketingowych nawet zwiększyć wartość projektu dzięki pracom dodatkowym nie objętym kontraktem.

Dokumentacja jest zarówno warunkiem, jak i świadectwem dobrego lub złego wykonania projektu. Okazuje się, że około 50% trudności realizacyjnych, a przez to i strat, wynika z nieprawidłowego prowadzenia dokumentacji.

## Etapy projektów

Projektem można nazwać każde zadanie składające się z wielu działań, które muszą być zrealizowane w ustalonym terminie i nie mogą przekroczyć ustalonych kosztów. Wszystkie działania wymagają określonego czasu na realizację. Większość jest ze sobą wzajemnie powiązana, ale część może być realizowana niezależnie od innych. Z tego względu w realizacji projektów wyszczególnia się cztery główne etapy: definiowanie, planowanie, realizację oraz odbiory.

Rozpoczynając prace nad projektem, należy wyjaśnić, jaki jest cel projektu (*Co ma być jego końcowym rezultatem?*) oraz określić wymagane zasoby (*Kiedy należy zakończyć projekt i jaki budżet przeznaczono na realizację?*). Gdy już wiadomo, dlaczego uruchamiany jest projekt, należy określić, co powinno być zrobione oraz w jakiej kolejności. Następnie identyfikuje się zasoby (*Kogo potrzebujemy? Jakie narzędzia są nam potrzebne?*) i przydziela się zadania. Mając te informacje, przystępuje się do opracowywania harmonogramu prac, w którym zostaną graficznie odzwierciedlone wszystkie zadania, terminy ich rozpoczęcia oraz zakończenia, a także dostępne zasoby (ludzie i narzędzia). Zanim harmonogram zostanie zatwierdzony, należy uzyskać odpowiedzi na kilka pytań: *Co może pójść źle? Co zrobić, gdy wystąpi problem? Jak zmniejszyć ryzyko? Jak uruchamiać działania korygujące?* Analiza odpowiedzi na te pytania pozwoli na weryfikację planu.

Uruchomienie projektu jest zależne od tego, czy określony czas i dostępne zasoby pozwolą na jego zrealizowanie. Nie warto uruchamiać projektu, jeśli wiadomo, że nie będzie można go zrealizować, gdyż pochłonie zbyt dużo pieniędzy i czasu. Dlatego tak istotne jest zdefiniowanie zakresu projektu oraz zaplanowanie jego realizacji.

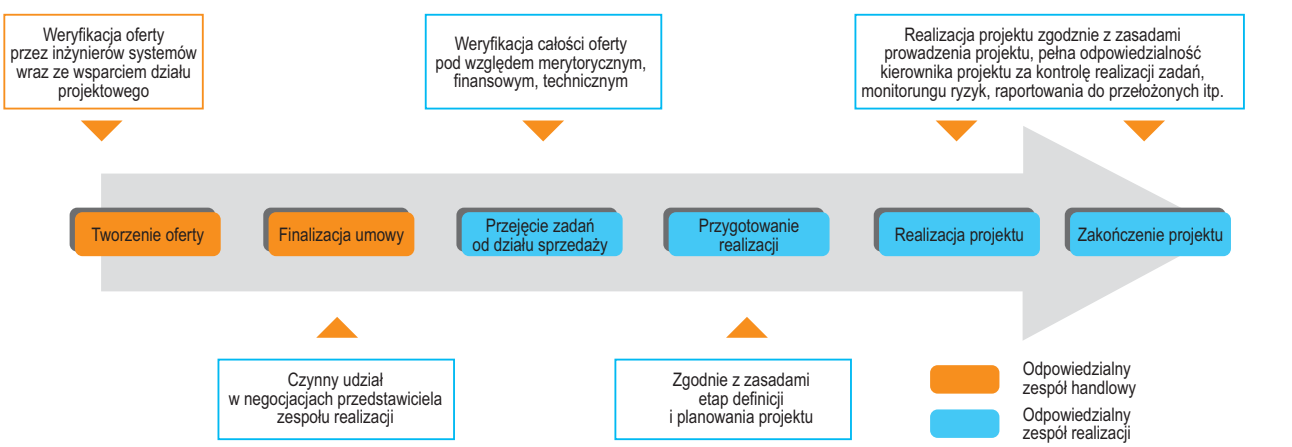
Gdy już wiadomo, że warto projekt realizować oraz że uda się go skończyć w założonym czasie, należy przygotować się do jego uruchomienia, czyli zainicjowania jego realizacji. Najczęściej dzieje się to w trakcie spotkania, na którym omawia się z kierownictwem firmy lub działu oraz członkami zespołu takie kwestie jak rola poszczególnych osób w projekcie, sposób organizacji pracy, dostępne narzędzia oraz harmonogram prac.

Każdy projekt musi być nadzorowany tak, aby można było odpowiednio wcześnie zdiagnozować problemy i wprowadzić modyfikacje do harmonogramu prac. Na bieżąco powinno się weryfikować przestrzeganie harmonogramu oraz reagować zarówno na zagrożenia, jak i na szanse przyśpieszenia prac.

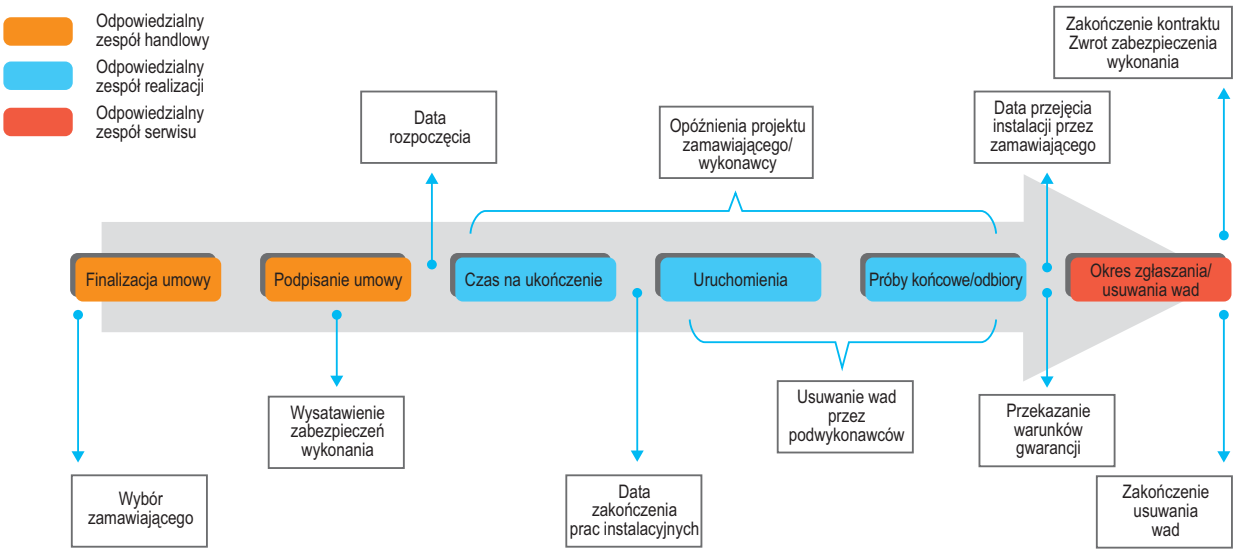
Ostatnim etapem realizacji projektu jest jego zakończenie. Już na samym początku powinno być wiadomo, kto zamknie projekt, kiedy, gdzie i na jakich warunkach. Do zamknięcia projektu potrzebne jest dokonanie odbiorów oraz oceny realizacji. Warto w tym momencie zastanowić się: *Czego się nauczyliśmy?* oraz *Co następnym razem powinniśmy zrobić inaczej?*

## Rola kierownika projektu

Zadaniem kierownika projektu jest takie wykonywanie wszystkich czynności zarządzania projektem, aby umożliwić osiągnięcie celu projektu w ramach założonego zakresu prac oraz założonych kosztów i w założonym czasie.




*Rys. 1. Rozpoczęcie projektu*



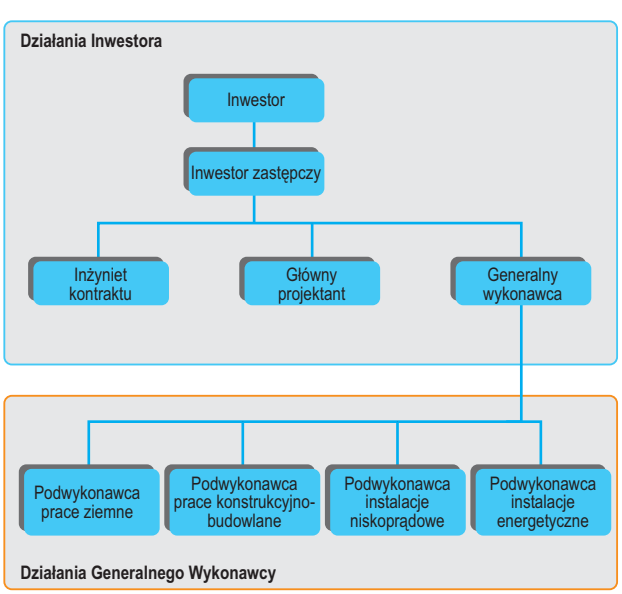

*Rys. 2. Standardowy cykl projektu*

Głównymi obowiązkami kierownika projektu są:
- uczestnictwo w pracach nad przygotowaniem umowy,
- opracowanie harmonogramu realizacji projektu i nadzorowanie jego przestrzegania,
- przekazywanie klientowi i przełożonym rzetelnej informacji dotyczącej stanu projektu, zagrożeń, zagadnień otwartych i ewentualnych wniosków o dokonanie zmian,
- analiza ryzyka, opracowanie działań zapobiegawczych i naprawczych, bieżące monitorowanie i kontrola ryzyka, podejmowanie akcji naprawczych,
- planowanie i organizacja odbiorów poszczególnych fragmentów projektu.

## Dokumentacja projektu

Kierownik projektu zawsze posiada pełną dokumentację projektu do wglądu – zarówno na swoje potrzeby, jak i na potrzeby przełożonego. W skład dokumentacji wchodzą: umowa, projekty techniczne, harmonogram prac oraz korespondencja.

W przypadku średnich i dużych projektów w umowie realizacji powinny być zawarte: zakres prac, sposób komunikacji wykonawcy z zamawiającym, obowiązki zamawiającego, obowiązki wykonawcy, wstępny harmonogram (kamienie milowe), sposób przedłużenia czasu na ukończenie, sposób zgłaszania roszczeń i zmian, sposób obliczania roszczeń (np. cenniki), zasady i termin odbioru prac, sposób płatności, zasady akceptacji kwot częściowych, zasady naliczania odszkodowań i kar, zasady udzielonej gwarancji i sposobu jej realizacji oraz zasady odstąpienia od umowy, wypowiedzenia i rozwiązania jej przez zamawiającego oraz wykonawcę.




*Rys. 3. Typowa struktura na budowie*

Korespondencja powinna być tworzona minimum w dwóch egzemplarzach – w przypadku potwierdzeń osobistych drugi egzemplarz z podpisem przechowuje się w archiwum. Żadne pismo nie może pozostać bez odpowiedzi, należy prowadzić na bieżąco korespondencję z klientem. Otrzymane notatki powinno się weryfikować, porównując ich treść z dotychczasowymi ustaleniami, a w przypadku niezgodności bezwzględnie informować o tym autora notatki. Należy unikać uzgodnień ustnych, w przypadku otrzymania polecenia tą drogą potwierdzić je pisemnie przed wykonaniem.

Najważniejsze sprawy, o których należy powiadamiać zamawiającego, to:
- opóźnienia, które generuje podwykonawca lub sam zamawiający,
- niemożliwość wykonania prac ze względu na opóźnienia nie z naszej winy,
- przesunięcie terminu zakończenia prac, jeśli aktualne problemy związane z naszą realizacją, są niemożliwe do rozwiązania,
- wszelkie zmiany, które generują dla nas dodatkowe koszty lub dodatkowe prace,
- pomysły, które mogą usprawnić realizację, przyspieszyć wykonanie zakresu prac itp.,
- uszkodzenia i zniszczenia efektów naszej pracy,
- wezwania do odbiorów prac częściowych, końcowych, robót zakrytych.

## Zmiany i roszczenia

W trakcie realizacji projektu może się okazać, że ze względu na zewnętrzne okoliczności występuje potrzeba weryfikacji kosztów i czasu realizacji. Dodatkowe koszty mogą dotyczyć wszelkich zmian wpływających na zakres prac, z którymi wiąże się konieczność zakupu dodatkowego sprzętu, wykonania dodatkowej instalacji,

wykonania dodatkowych czynności inżynierskich i projektowych, zwiększenia zaangażowania pracowników itp.

Dodatkowy czas na zakończenie zadania lub całości prac może także wynikać z przestojów z winy zamawiającego, zmiany terminów przez wykonawców innych branż, braku danych koniecznych do wykonania zadania, braku decyzji zamawiającego, braku możliwości wykonania prac itp.

Roszczenia zgłasza się pisemnie. W zgłoszeniu należy wskazać przedmiot roszczenia i wyjaśnić okoliczności jego wystąpienia oraz opisać, jak dany problem (będący przyczyną roszczenia) wpłynie na harmonogram realizacji projektu i jakie koszty poniesie wykonawca w związku z jego rozwiązaniem. Roszczenie kończy się podpisaniem aneksu do istniejącej umowy lub zleceniem na wykonanie prac dodatkowych.

Zadaniem kierownika projektu jest niedopuszczenie do zbędnego przedłużania się rozstrzygnięcia roszczenia; w tym celu monitoruje on dokumentację i korespondencję, a w razie konieczności wysyła przypomnienia lub wezwania, np. do przekazania danych.

Przykłady zmian w projekcie:

– usunięcie skutków zaniedbań, do jakich doszło przed uruchomieniem projektu lub już w trakcie jego realizacji (np. nieprzekazania istotnej informacji),
– uwzględnienie dodatkowych instrukcji zamawiającego,
– wykonanie dodatkowych prac wynikających z ustaleń z zamawiającym,
– wprowadzenie zmian do wytycznych traktowanych jako baza wyceny materiałów i robót,
– zmiana kolejności oraz czasów wykonania prac w odniesieniu do uzgodnionych terminów,
– przeprojektowanie (np. zmiana architektury systemów, zmiany założeń i wytycznych projektowych).

## Zakończenie

Realizacja projektów jest tematem bardzo szerokim i nie może być w całości omówiona w pojedynczym artykule. Autor chciał ukazać zagadnienia kluczowe dla bieżącej pracy projektantów, instalatorów, koordynatorów, serwisantów i innych osób uczestniczących w realizacji projektów.

Zagadnienia zarządzania projektami są bardzo popularne w wielu branżach. Wiedzę z tego zakresu można zdobywać i pogłębiać na dostępnych kursach zawodowych oraz na kilku uczelniach wyższych.

W zarządzaniu projektami oraz ich optymalizacji mogą pomóc dostępne narzędzia i techniki takie jak TQM, LEAN, 6Sigma DMAIC (definiuj, mierz, analizuj, usprawniaj, kontroluj). Osoby posiadające kwalifikacje z tego zakresu są chętnie zatrudniane w firmach produkcyjnych i instalacyjnych.

*Opracował: Daniel Kamiński*
*OCHRONA JUWENTUS*

Materiały źródłowe:


1. Robert Berliński: *Szkolenie dla koordynatorów projektów*
2. *http://www.skutecznyprojekt.pl/artykul.htm?AID=204*
3. *http://www.bankier.pl/wiadomosc/Przyczyny-porazek-projektow-1873102.html*
4. Materiały szkoleniowe Lean SixSigma, poziom Green Belt


# Nadzór wizyjny w transporcie

Agata Majkucińska

**Bezpieczeństwo sektora transportowego, a w szczególności kolejowego, jest uzależnione od możliwości błyskawicznego reagowania na wszelkie incydenty stwarzające potencjalne zagrożenie. Systemy nadzoru wizyjnego wykorzystujące protokół IP dostarczają niezbędnego materiału dowodowego, a także stwarzają możliwość skutecznego zapobieganiu przestępstwom. Zwiększają także efektywność przewozową, a dzięki podglądowi w czasie rzeczywistym umożliwiają kontrolowanie tego, co dzieje się na dworcu czy stacji kolejowej**

Wszędzie tam, gdzie w transporcie publicznym zdecydowano się na wprowadzenie sieciowych systemów nadzoru wizyjnego, odnotowano nie tylko podwyższenie rzeczywistego poziomu bezpieczeństwa. Dzięki lepszemu nadzorowi obniżono koszty związane z zachowaniem ciągłości usług i koszty reakcji na akty wandalizmu. Lepszy nadzór przyciągnął większą liczbę pasażerów, którzy chętniej korzystają ze środków transportu publicznego. Wszystkie przeznaczone do wykorzystania w instalacjach mobilnych kamery Axis Communications mają funkcje antysabotażowe. Dzięki temu nawet po zamaskowaniu obiektywu kamery, np. za pomocą lakieru w sprayu, odpowiednie służby są natychmiast powiadamiane o zagrożeniu, więc mają możliwość błyskawicznej reakcji.

Najnowsze rozwiązania dają jeszcze więcej możliwości. Wprowadzenie na rynek kamer sieciowych pozwalających na uzyskanie materiału wizyjnego o wysokiej rozdzielczości (takich jak np. kamery AXIS M3114) powoduje, że identyfikacja osób jest dużo łatwiejsza. Co więcej, możliwa jest obserwowanie większych obszarów z wykorzystaniem mniejszej liczby kamer. Operator systemu w jednej chwili uzyskuje zdalny dostęp do obrazu przekazywanego na żywo z dowolnego autobusu lub pociągu. Dzięki inteligentnym funkcjom wizyjnym można zliczać pasażerów, ustalać miejsca i trasy środków transportu, które są najbardziej obciążone lub narażone na ewentualne akty wandalizmu lub kradzieży. Integracja systemu nadzoru wizyjnego z systemem GPS umożliwia śledzenie pojazdów na cyfrowej mapie z jednoczesnym wyświetlaniem obrazów z zamontowanych w nich kamer.

*Fot 1. AXIS M3114*

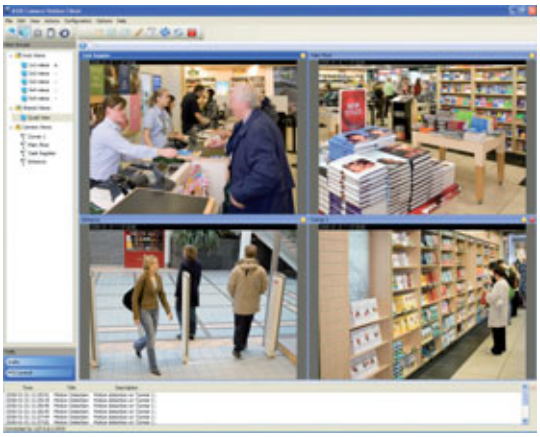
Dzięki pełnej skalowalności i otwartemu oprogramowaniu kamery zainstalowane w pojazdach mogą być łatwo zintegrowane z systemami nadzoru wizyjnego istniejącymi już na stacjach czy w terminalach, nawet jeśli wykorzystano w nich urządzenia analogowe. Dzięki zastosowaniu koderów wizyjnych, również dostępnych w ofercie Axis Communications, możliwe jest włączenie dotychczasowych analogowych kamer do nowoczesnej sieci nadzoru wizyjnego wykorzystującego protokół IP.

Kamery IP świetnie sprawdzają się w dużych, rozbudowanych instalacjach dozorowych. Przykładem wykorzystania protokołu IP w nadzorze wizyjnym środków transportu publicznego jest szybka kolej Waratah w Sydney. Składająca się z 78 pociągów flota została w ostatnich latach wyposażona w nowoczesne kamery IP, dzięki którym podróżni są bezpieczniejsi. W 626 wagonach zamontowano w sumie ponad 7000 kamer dostarczonych przez Axis Communications. Zastosowany model – AXIS 209 MFD-R – charakteryzuje się niewielkimi rozmiarami i odpornością na wstrząsy, zapylenie oraz duże zmiany ciśnienia i temperatur. Co ciekawe, cały materiał wizyjny jest przechowywany lokalnie, w pociągach, a źródłem zasilania wszystkich kamer jest pokładowa sieć Ethernet (dzięki technologii Power over Ethernet – PoE). Ten sam model wykorzystano w norweskich pociągach Intercity, gdzie w ramach instalacji zamontowano ponad 3200 kamer AXIS 209 i AXIS 221. Skorzystały z niego także koleje szwajcarskie – SBB (Schweizerische Bundesbahn) – wykorzystując kamery AXIS 209 MFD-R w systemie nadzoru wizyjnego zastosowanym w 115 pociągach miejskich.

Bezpośredni następca tego modelu – AXIS M31-R, także przeznaczony do użytku w obiektach ruchomych, takich jak pociągi czy autobusy – pozwala na uzyskanie obrazu o rozdzielczości HDTV, a także na obsługę wielu strumieni wizyjnych jednocześnie. Około 6000 kamer sieciowych AXIS M31-R zastosowano we flocie autobusów zarządzanych przez władze Madrytu. Takie same kamery wykorzystano w systemie nadzoru wizyjnego tramwajów i w metra w Monachium (ponad 450 pojazdów) i w sztokholmskiej sieci komunikacji miejskiej (stacje, autobusy i pociągi metra – razem ponad 15000 urządzeń).

Do proponowanych urządzeń Axis, które mogą być zainstalowane na dworcach kolejowych, w terminalach przeładunkowych, tunelach itp., należą kamery termowizyjne, które znakomicie sprawdzają się w nadzorze infrastruktury transportowej, lub urządzenia umożliwiające pracę w bardzo złych warunkach oświetleniowych (np. we wspomnianych tunelach). Należy podkreślić, że seria kamer AXIS Q60-xx sprawdzi się wszędzie tam, gdzie wymagana jest precyzja, identyfikacja szczegółów obrazu, duże powiększenie optyczne, zaawansowana inteligencja. Obudowy kamer skutecznie chronią je przed pyłem, kurzem i wodą, a wzmocniona konstrukcja sprawia, że kamery pokładowe są odporne na wstrząsy, wibracje i gwałtowne zmiany temperatury i wilgotności. Dodatkowe baterie zapewniają nieprzerwaną pracę kamer nawet w przypadku awarii zasilania, a oprogramowanie automatycznie powiadamia operatora systemu o próbach manipulowania, zamalowywania czy niszczenia kamery.

To wszystko jest niezwykle istotne w tak ważnych instalacjach jak sieci transportowe. Od szybkości analizy sytuacji



*Fot 2. Oprogramowanie AXIS Camera Station*

często zależy bezpieczeństwo pasażerów, pracowników, a także taboru i innego mienia. Ponadto, po wypadku czy wystąpieniu aktu wandalizmu, osoby badające zdarzenie mogą zapoznać się z sytuacją niemal natychmiast, bez żmudnego przekopywania się przez dane nagrane na tradycyjnych analogowych nośnikach, takich jak np. kasety wideo. Wykorzystujące protokół IP systemy nadzoru wizyjnego pozwalają też na ocenę rozwoju wydarzeń na żywo, niezależnie od warunków pogodowych, i błyskawiczną, adekwatną do obserwowanej sytuacji reakcję.

Kamery sieciowe ułatwiają ochronę całej infrastruktury, włącznie z kluczowymi elementami linii kolejowych czy zaciemnionymi obszarami dworców. Dzięki technologii termowizyjnej są pierwszą linią obrony przed złodziejami okradającymi torowiska, grafficiarzami czy też zwykłymi wandalami. Kamery termowizyjne proponowane przez Axis Communications potrafią wykryć osobę stanowiącą potencjalne zagrożenie nawet z odległości kilometra. Dzięki detekcji ruchu i cichemu alarmowi operator systemu jest niemal natychmiast powiadamiany o niebezpieczeństwie i może natychmiast zawiadomić odpowiednie służby, takie jak policja czy Służba Ochrony Kolei.

*Fot 3. AXIS Q6035*

*Agata Majkucińska*
*Axis Communications*


# OCHRONA OBWODOWA OBIEKTÓW CCTV

ZBAR

## _ CCTV

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

## _ kamery laserowe:

- opatentowana technologia "searchlight"
- przenikanie przez szkło / okno
- precyzyjna identyfikacja obiektów
- 6km w dzień / 3km nocą
- szeroki zakres regulacji ogniskowej obiektywu (18x-36x)
- stabilizacja obrazu
- regulacja obrotu w pionie i w poziomie

## _ kamery termowizyjne

- widoczność w całkowitych ciemnościach, we mgle, dymie, pyle
- wykrywanie zagrożeń w odległości ponad 2km
- sterowanie PTZ z dużą prędkością
- szeroki zakres dynamiczny
- zobrazowanie cieplne

## _ kamery hybrydowe

- pracuje w świetle widzialnym z funkcją termowizji wspomaganej laserem
- opatentowana technologia "searchlight"
- widoczność w całkowitych ciemnościach, we mgle, dymie, pyle
- 7,5km w dzień / 7km nocą
- automatyczne śledzenie
- wzmocniona konstrukcja

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

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

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

# Sukces Samsunga
## w świecie handlu detalicznego

W obecnych, trudnych warunkach ekonomicznych nie budzi zdziwienia, że sprzedawcy detaliczni szukają sposobów na zwrot kosztów poniesionych na inwestycje związane z instalacją systemów bezpieczeństwa. Na szczęście z pomocą przychodzi technologia i sprzedawcy detaliczni mogą obecnie czerpać korzyści z kamer, które oferują funkcje i wartości o których nie mogło być mowy jeszcze kilka lat temu. Na przykład oprogramowanie służące do detekcji twarzy oraz integracja kamer z systemami kasowymi stwarza możliwości zwalczania konszachtów między personelem a nabywcami i ukrócenie działań prowadzonych „z dobrego serca", podczas gdy technologia WDR (rozszerzająca zakres dynamiki kamer) zastosowana w kamerach najnowszej generacji pozwala na tworzenie obrazów o wysokiej jakości nawet w bardzo niekorzystnych warunkach oświetleniowych, na przykład takich, jakie występują w pobliżu witryn sklepowych

Kamery CCTV są stosowane w przemyśle i w handlu detalicznym od ponad trzech dziesięcioleci i służą do wykrywania działań o charakterze kryminalnym. Technologia CCTV nie pozwalała na stworzenie niczego więcej oprócz zamkniętych instalacji o charakterze lokalnym. Obecnie systemy analogowe, w których do transmisji sygnałów wizyjnych wykorzystywane były kable koncentryczne lub wieloparowe kable symetryczne, można podłączać do sieci IP za pośrednictwem odpowiednich urządzeń kodujących. Nawet w przypadku stosowania najtańszych rozwiązań pojawiła się możliwość obserwacji obrazów i zarządzania systemami za pośrednictwem komputerów PC połączonych z Internetem. Jednakże dopiero możliwość bezpośredniego podłączenia kamer do sieci IP spowodowała, że dalszy rozwój wydarzeń nabrał żywszego tempa. W efekcie produkty służące do budowy sieciowych systemów bezpieczeństwa zajęły dominującą pozycję na rynku wizyjnych systemów dozorowych, zaś w nowych instalacjach można w pełni wykorzystać zalety wynikające z tej koncepcji.

Sieciowe systemy dozorowe pozwalają sprzedawcom detalicznym na czerpanie korzyści ze stosowania najnowocześniejszych kamer o wysokiej rozdzielczości, które mogą zaoferować znacznie więcej niż tradycyjne analogowe kamery CCTV, które generowały obrazy zawierające zaledwie czterysta tysięcy pikseli. Przykładowo – przy odpowiednim doborze kąta widzenia kamera o rozdzielczości 1,3 megapiksela może pełnić rolę kilku kamer analogowych, gdyż umożliwia obserwację dużego obszaru i powiększenie wybranych fragmentów obrazu bez spowodowania pikselizacji.

## Korzyści wynikające ze stosowania megapikselowych kamer HD

Megapikselowe kamery HD oferują znacznie więcej niż tylko obrazy o dogodniejszych proporcjach i jakości umożliwiającej wykorzystanie ich jako wiarygodnych materiałów dowodowych. Mają one inne zalety. Większość z dodatkowych funkcji jest realizowana dzięki procesorom DSP wbudowanym w kamery. Na przykład układy WiseNetI i WiseNetII produkowane przez firmę Samsung zostały zaprojektowane z myślą o maksymalnym wykorzystaniu możliwości megapikselowych kamer HD.

Megapikselowe kamery HD mogą wytwarzać obrazy odznaczające się bardzo dobrą rozróżnialnością szczegółów, które mogą być wykorzystane w lokalnych instalacjach przez służby ochrony obiektów. Możliwa jest jednak jednoczesna transmisja obrazów o znacznie niższej rozdzielczości, odpowiadającej standardom QVGA (320×240), VGA (640×480) i SVGA (800×600), a także kompresja obrazów z wykorzystaniem wielu różnych metod. Dzięki temu obrazy mogą być jednocześnie obserwowane przez użytkowników dysponujących odpowiednimi uprawnieniami, rejestrowane w celach dowodowych i oglądane na smartfonach przez użytkowników przebywających z dala od chronionych obiektów. Obrazy skompresowane metodą JPEG mogą być dołączane do listów wysyłanych pocztą elektroniczną. Ponadto dostępne są funkcje rejestracji ruchomych obrazów na wewnętrznych kartach pamięci SD, w trybie prealarmowym i postalarmowym.

Oczywiście nie zawsze zachodzi potrzeba obserwacji całego chronionego obszaru z najwyższą dostępną rozdzielczością. Podczas realizacji projektów należy kierować się zasadami zdrowego rozsądku i dobierać kamery tak, by spełniały specyficzne wymagania wynikające z przyjętych założeń użytkowych. Megapikselowe kamery HD należy stosować tam, gdzie jest to rzeczywiście wymagane, zaś w pozostałej części systemu, wszędzie tam, gdzie potrzebna jest jedynie ogólna ocena sytuacji, należy stosować kamery o standardowej rozdzielczości.

*Fot. 1. Dom handlowy M&M's World London mieszczący się na Leicester Square*

## Inteligentna analiza obrazu

Inną zasadniczą korzyścią wynikającą ze stosowania megapikselowych kamer HD jest możliwość wykorzystania funkcji inteligentnej analizy obrazu (IVA) pozwalającej na wykrywanie obiektów poruszających się w obserwowanej przestrzeni i naruszających granice strzeżonych obszarów, wyznaczanie kierunku ruchu obiektów, wykrywanie pojawiających się lub znikających przedmiotów oraz analizę innych zjawisk związanych z ruchem obiektów. Ponadto IVA umożliwia wykrywanie aktów sabotażu i emisję sygnałów ostrzegawczych, na przykład w chwili podjęcia nieautoryzowanej próby obrócenia kamery lub gdy obiektyw zostanie zamalowany farbą.

## Spojrzenie w przyszłość

Jeśli przyjrzymy się domowym urządzeniom telewizyjnym, łatwo zauważymy, że większość z nich pracuje w standardzie HD. W ciągu ostatniego roku ceny megapikselowych kamer HD znacznie spadły. Dzięki temu w wielu aplikacjach można czerpać korzyści wynikające z posługiwania się obrazami o wysokiej jakości, zaś na rynku jest konkurencja, co wpływa na wzrost podaży urządzeń. Ostatnio firma Samsung wprowadziła do swojej oferty czterokanałowe i szesnastokanałowe


*Fot. 2. Klawiatura Samsung SPC-6000*

sieciowe rejestratory wizyjne NVR pozwalające na rejestrację obrazów o rozdzielczości HD. Dzięki temu zaistniała możliwość budowy tanich i skutecznych w działaniu sieciowych systemów dozorowych. Dzięki takim tendencjom rynkowym należy się liczyć z coraz częstszym stosowaniem technologii IP w małych i bardzo małych instalacjach dozorowych.

Aby, w obecnej sytuacji ekonomicznej, usprawiedliwić wydatki związane z instalacją systemów dozorowych, od analogowych lub sieciowych systemów dozorowych będzie się oczekiwać wymiernych zysków wynikających z dodatkowych funkcji oferowanych przez te systemy. W wielu przypadkach będą to zyski wynikające z obniżenia kosztów HR, IT oraz kosztów związanych z marketingiem. Będą to także zyski wynikające z wykorzystania danych pochodzących z kamer pracujących w systemach dozorowych przez kierownictwo obiektów handlowych. Technologia wykorzystywana w systemach dozorowych będzie w stanie odpowiadać rosnącym oczekiwaniom użytkowników końcowych, co jest ściśle związane z funkcjami oferowanymi przez megapikselowe kamery HD najnowszej generacji, z ich zdolnością do wytwarzania obrazów o zadziwiająco wysokiej jakości, dzięki czemu możliwa będzie realizacja wielu zadań, nie tylko polegających na obserwacji tego, co dzieje się na terenie chronionych obiektów. Najlepszym przykładem mogą być rozwiązania wykorzystane w sieci handlowej M&M's World.

Dom handlowy M&M's World London, będący własnością Mars Retail Group, jest zarazem największą na świecie cukiernią. Zajmuje powierzchnię równą 35 tysięcy stóp kwadratowych i jest czteropiętrowym budynkiem, w którym klienci mogą nabyć czekoladę M&M oraz inne markowe produkty, takie jak zabawki, naczynia kuchenne, ubrania, bielizna pościelowa, wyroby jubilerskie i wyroby ze szkła. Budynek mieści się na Leicester Square w Londynie i został otwarty jako pierwszy dom handlowy M&M's World w Europie. Znajduje się w nim ściana wykonana z czekolady, gdzie klienci mogą tworzyć swoje własne kompozycje z ponad stu gatunków czekolady M&M.

Daniel Clare jest specjalistą do spraw bezpieczeństwa w obiektach M&M's World. Z racji zajmowanego stanowiska odpowiada on za zespół pracowników, których zadaniem jest demaskowanie złodziei sklepowych oraz innych kłopotliwych gości domu handlowego na Leicester Square. – *Jest to kolorowy, piękny dom handlowy, chętnie odwiedzany przez klientów* – powiedział Daniel Clare. *Nasze główne cele to odstraszanie złodziei oraz zapewnianie bezpieczeństwa klientom i pracownikom, bez wywierania negatywnego wpływu na atmosferę panującą w tym obiekcie.* Kamery dostarczone przez firmę Samsung pracują w trybie 24/7 i są obsługiwane w pomieszczeniu technicznym znajdującym się na terenie budynku, jednakże sieciowe rejestratory Samsung SRD-1670D pozwalają także kierownictwu M&M's World obserwować obrazy z kamer w swojej siedzibie mieszczącej się w USA. – *Jest to wielka zaleta, zwracają się koszty instalacji systemu* – powiedział Daniel Clare.– *Zostały spełnione wymagania związane z bezpieczeństwem obiektu, a handlowcy mogą uzyskać wartościowe informacje dotyczące reakcji klientów na ich działania, nie wychodząc ze swoich biur na terenie USA.*

## Progressive Scan – kolejny krok naprzód

Powszechnie odczuwanym mankamentem powodującym frustrację u sprzedawców detalicznych, którzy zdecydowali się na instalację kamer PTZ, był dotychczas brak czytelności obrazu, a także wyraźny efekt smużenia w chwili, gdy kamera poruszała się. Jeśli kamery PTZ były wykorzystywane do obserwacji obszarów o znaczeniu strategicznym, takich jak lotniska czy porty morskie, nagrania o niskiej jakości przyczyniały się do utraty przekonania użytkowników o przydatności systemów dozorowych do poprawy poziomu bezpieczeństwa tych obszarów. Podobnie było w przypadku parkingów bądź obiektów produkcyjnych lub handlowych, które nie miały znaczenia strategicznego, jednak stanowiły środowiska, w których kamery PTZ znajdowały powszechne zastosowanie. Mało czytelny, smużący obraz miał negatywny wpływ na zdolność personelu obsługującego system dozorowy do poprawnej oceny sytuacji i do podejmowania prawidłowych decyzji w przypadku wykrycia incydentów lub zagrożeń.

*Fot. 3. Szesnastokanałowe rejestratory DVR SRD-1670D firmy Samsung*

Na całe szczęście z pomocą przyszła technologia. Nowa właściwość kamer określana nazwą *Progressive Scan* pozwoliła na uzyskanie obrazów o wysokiej jakości, na których widoczne są wyraźne kontury obserwowanych obiektów. Wynikającą z tego poprawę jakości można najłatwiej zauważyć w przypadku pojedynczych, nieruchomych obrazów, na których można na przykład odczytać numery rejestracyjne przejeżdżających pojazdów.

Firma Samsung zastosowała technologię *Progressive Scan* w najnowszych kamerach szybkoobrotowych. We wszystkich czterech modelach kamer zgodnych z ONVIF, w których wykorzystany jest wysoce ceniony procesor sygnałowy SV-5 DSP, możliwe jest wytwarzanie obrazów o rozdzielczości 4CIF z prędkością 25 klatek na sekundę. Model SNP-3371, przystosowany do pracy w każdych warunkach pogodowych, jest wyposażony w obiektyw zmiennoogniskowy o krotności x37, zaś model SNP-3371TH ma opcję automatycznego śledzenia ruchomych obiektów i jest dostarczany wraz z obudową, co ułatwia jego instalację. Model SNP-3302 jest wyposażony w obiektyw zmiennoogniskowy o krotności x30, zaś jego obudowana wersja SNP-3302H ma stopień szczelności IP66.

Oprócz technologii *Progressive Scan* na zdolność kamer szybkoobrotowych do wytwarzania czytelnych obrazów ma wpływ między innymi praca w dwóch trybach, dziennym i nocnym, możliwa dzięki zastosowaniu przetwornika CCD o rozdzielczości 600 linii telewizyjnych i czułości pozwalającej na pracę w warunkach bardzo słabego oświetlenia. W kamerach wykorzystana jest także technologia rozszerzania dynamiki (WDR), dzięki której problemy z tylnym oświetleniem są rozwiązywane 160 razy skuteczniej niż w przypadku klasycznej kompensacji BLC.

*Samsung Techwin*

*Tłumaczenie: Redakcja*

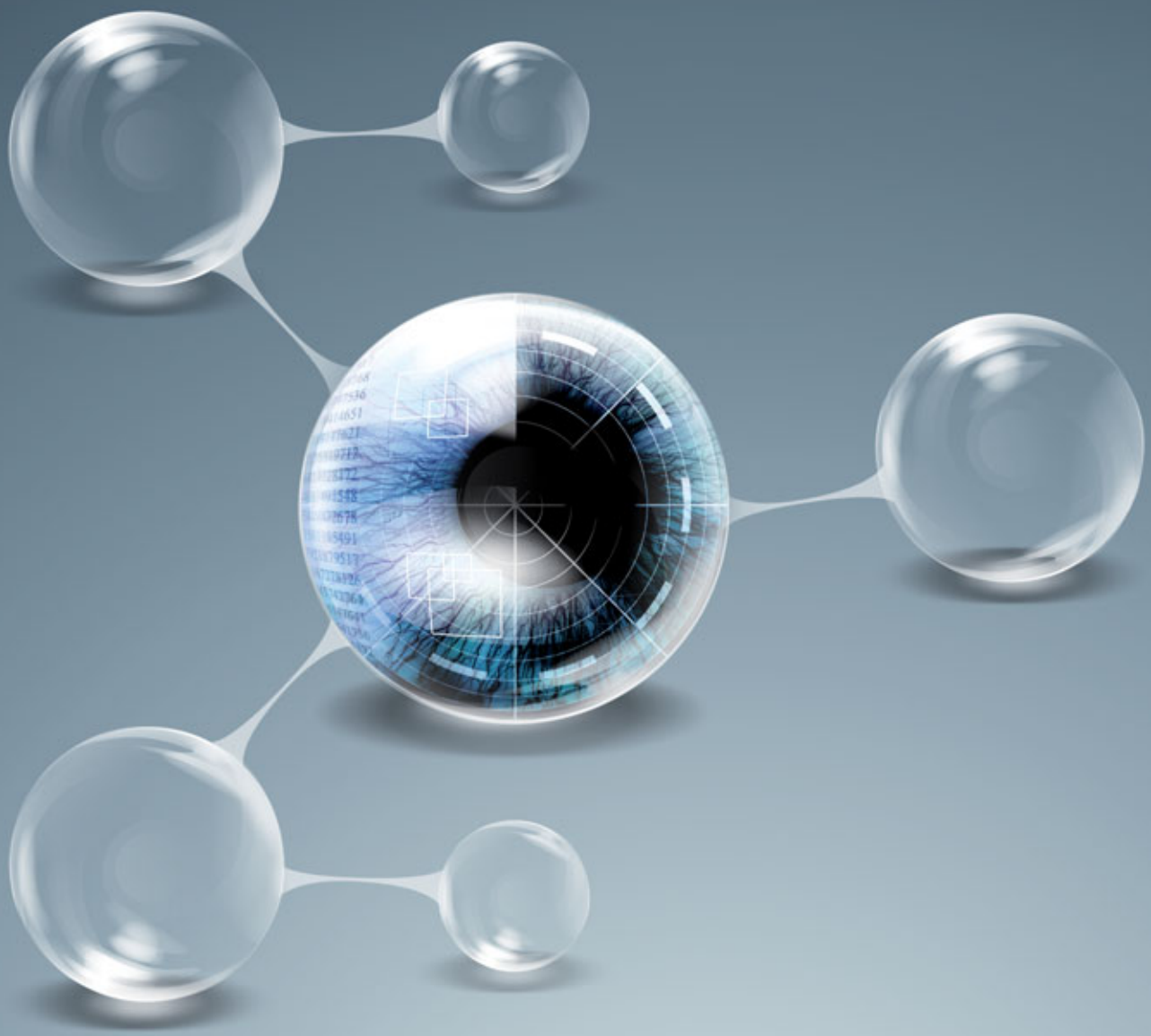
SSN
Security Solution Network

# OFICJALNY DYSTRYBUTOR PRODUKTÓW **FIRMY SAMSUNG**


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

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

SAMSUNG **SAMSUNG TECHWIN**



# Samsung wprowadza serię kamer IP WiseNetS o rozdzielczości VGA

Firma Samsung ponownie rozszerzyła zakres swoich propozycji z dziedziny sieciowych systemów dozorowych i wprowadziła na rynek sześć kamer IP o nazwie WiseNetS, w których wykorzystany został najnowszy cyfrowy procesor DSP, specjalnie przystosowany do obróbki obrazów o rozdzielczości VGA


*Fot. 2. Kamery szybkoobrotowe Samsung SCP-2250 z obiektywem zmiennoogniskowym o krotności x25*

Oprócz redukcji szumów metodą SSNRIII i zwiększenia dynamiki obrazu metodą SSDR użytkownicy sieciowych kamer Samsung o rozdzielczości VGA i kompatybilnych z protokołem ONVIF oczekiwali wprowadzenia do każdej z nich wielu nowych funkcji przynoszących realne korzyści, takich jak możliwość wytwarzania wielu strumieni danych z prędkością 30 klatek na sekundę, możliwość wyboru rodzaju kompresji (MJPEG lub H.264), możliwość zasilania kamer metodą PoE oraz możliwość stosowania wielokątnych masek dla stref prywatnych.

Ponadto, poza standardowymi opcjami detekcji ruchu, wszystkie kamery z serii WiseNetS mają także wbudowane układy pozwalające na detekcję twarzy. Informacje ostrzegawcze mogą być wysyłane pocztą elektroniczną lub innymi metodami, zaś funkcja detekcji twarzy może być uaktywniana zgodnie z harmonogramem dobowym lub tygodniowym. Możliwe jest także wykrywanie ludzkich twarzy ukrytych za wielokątnymi maskami prywatności.

Jakość obrazów o rozdzielczości VGA (640×480 pikseli), wytwarzanych przez kamery z serii WiseNetS, została poprawiona dzięki zastosowaniu przetwornika CMOS ze skanowaniem progresywnym, co umożliwia np. odczyt tablic rejestracyjnych szybko poruszających się pojazdów, bez borykania się z uciążliwym zjawiskiem smużenia występującym w starszych rozwiązaniach. Wybrane modele mogą też dwukierunkowo transmitować dźwięk, co pozwala na skuteczną komunikację głosową. W ofercie znalazło się sześć nowych kamer, w tym stałopozycyjna SNB-1001, wodoodporna SNO-1080R, kopułkowa z obiektywem o stałej ogniskowej SND-1011, kopułkowa z obiektywem typu varifocal SND-1080, wandaloodporna kopułkowa z obiektywem typu varifocal SNV-1080 i wandaloodporna kopułkowa z obiektywem typu varifocal SNV-1080R (ta ostatnia z wbudowanym oświetlaczem pracującym w podczerwieni).

Wszystkie modele kamer (za wyjątkiem SNO-1080R) mają wbudowane gniazdo służące do wprowadzenia karty pamięci Micro SD/SDHC, co ułatwia zapis obrazów w sytuacjach alarmowych, zaś kamery SNB-1001, SND-1080 i SNV-1080 umożliwiają dwukierunkową komunikację głosową. – *Tych sześć kamer pozwala na tworzenie tanich rozwiązań przeznaczonych do wykorzystania w systemach dozorowych monitorujących małe i średnie obiekty, takie jak parkingi, szpitale, biura, szkoły oraz punkty handlu detalicznego* – powiedział Tim Biddulph, IP Product Manager w Samsung Techwin Europe. – *Ponadto, w połączeniu z naszym najnowszym czterokanałowym rejestratorem typu SRN-470D i szesnastokanałowym rejestratorem typu SRN-1670D, o wyglądzie i funkcjach typowych dla większości sieciowych rejestratorów DVR, możliwe jest tworzenie kompletnych, tanich i skutecznych w działaniu systemów dozorowych dostarczających obrazy o wysokiej jakości. Co więcej, te kamery są w pełni kompatybilne z urządzeniami i oprogramowaniem firmy Samsung z serii NET-i Ware, dostępnym w wersjach o liczbie kanałów równej 8, 16, 32 i 64. Oprogramowanie zostało stworzone w celu uproszczenia procesu zarządzania i sterowania systemem zapisującym obrazy wytwarzane przez sieciowe kamery firmy Samsung i pozwala na zapis i odtwarzanie obrazów z użyciem komputerów PC, za pośrednictwem sieci IP, z dowolnej lokalizacji, w której jest dostęp do Internetu, na kuli ziemskiej, umożliwiając utrzymywanie stałego kontaktu między ludźmi obsługującymi systemy bezpieczeństwa przez dwadzieścia cztery godziny na dobę i przez siedem dni w tygodniu, niezależnie od tego, gdzie ci ludzie się znajdują.*

Kamery o rozdzielczości VGA z nowej serii WiseNetS są dostępne u wszystkich dystrybutorów firmy Samsung Techwin Europe. Firma zapewnia trzyletnią gwarancję, usługi serwisowe oraz darmowe konsultacje projektowe i techniczne.

*Samsung Techwin*
*Tłumaczenie: Redakcja*


*Fot. 1. Wandaloodporna kamera kopułkowa SNV-1080R firmy Samsung z wbudowanym oświetlaczem pracującym w podczerwieni*


*Fot. 3. Wodoodporna kamera SNO-1080R firmy Samsung z wbudowanym oświetlaczem pracującym w podczerwieni*

# Koreański D-max
## wkracza na rynek z technologią HD-SDI

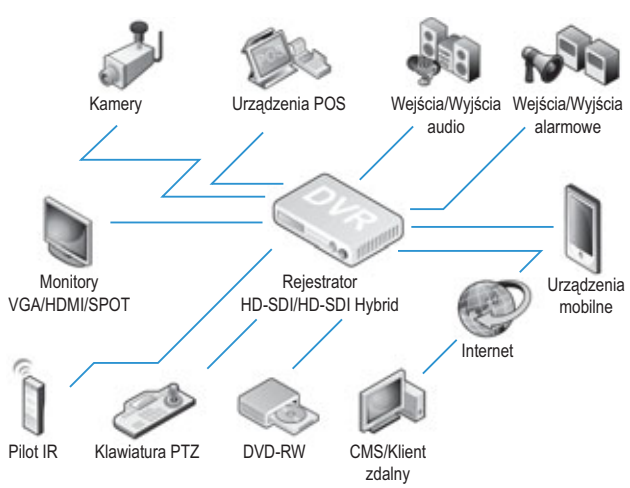
Paweł Mielewczyk

W połowie 2012 roku firma D-max zaprezentuje nową linię rejestratorów pracujących w standardzie HD-SDI. Ich największą zaletą jest możliwość rejestracji obrazów o rozdzielczości Full HD z kamer podłączonych kablem koncentrycznym. Pierwszym rejestratorem, który już można spotkać u dystrybutorów, jest HD-0400SP. Umożliwia on rejestrację 100 kl./s z czterech kamer HD. Zapisywany obraz jest kodowany metodą H.264. Wkrótce w ofercie pojawią się także rejestratory HD-0400S, HD-0800S, HD-1600S. Będą one mogły rejestrować obrazy z 4, 9 lub 16 kamer. Rejestrator HD-0400S umożliwi zapis 60 kl./s w pełnej rozdzielczości, a HD-0800S oraz HD-1600S – 100 kl./s. Wszystkie rejestratory charakteryzują się wyświetlaniem na żywo z prędkością 25 kl./s dla każdej kamery

Technologia HD-SDI wzbudza coraz większe zainteresowanie instalatorów i użytkowników systemów CCTV. Jakość obrazu uzyskiwanego z kamer HD-SDI jest zaskakująco dobra. Obraz z kamer, a także obraz odtwarzany z rejestratora odznacza się bogactwem szczegółów. Warto nadmienić, że obraz przesyłany z kamery do rejestratora nie podlega żadnej kompresji. Takie rozwiązanie eliminuje straty jakości powstałe podczas transmisji sygnału. Opóźnienia wyświetlanego obrazu są dużo mniejsze w porównaniu z systemami IP, które kompresują obraz bezpośrednio w kamerze. Ważną zaletą systemów HD-SDI jest maksymalna odległość, jaką może mieć przewód transmisyjny (BNC) bez dodatkowych urządzeń wzmacniających sygnał. Wynosi ona 200 metrów, co dwukrotnie przewyższa maksymalną długość skrętki stosowanej w systemach IP. Szacuje się, że systemy HD-SDI zyskają co najmniej taką popularność jak systemy IP. Wpłyną na to na pewno opisane wyżej zalety, a także prostota instalacji – instalacja przebiega tak samo jak w systemach analogowych. Najważniejsza jest jednak cena – wyższa niż cena systemów analogowych, lecz porównywalna, a nawet niższa od ceny systemów w standardzie IP. Najdroższy element to rejestrator zgodny ze standardem HD-SDI, którego cena jest wyższa od ceny jego sieciowego odpowiednika. Wynika to z konieczności stosowania procesorów o znacznie większych mocach obliczeniowych, które muszą poradzić sobie z ogromną ilością nieskompresowanych danych wysyłanych przez kamery. Same kamery i infrastruktura kablowa stworzona z wykorzystaniem przewodów koncentrycznych będą jednak tańsze.

W dobie rosnącego zainteresowania nową technologią koreański producent zapowiedział wprowadzenie na rynek jeszcze jednej nowości, to jest rejestratora HD-SDI Hybrid DVR, który ma dwa wejścia HD-SDI oraz 14 wejść analogowych. To doskonałe rozwiązanie, jeżeli istniejący system analogowy trzeba uzupełnić jedną bądź dwiema kamerami o wysokiej rozdzielczości (np. do identyfikacji osób) lub gdy istnieje potrzeba zainstalowania kamery o wysokiej rozdzielczości, a budżet jest ograniczony.

HD-SDI Hybrid DVR to wysokiej klasy rejestrator, który umożliwia zapis do 50 kl./s w rozdzielczości 1080p (2 kanały HD-SDI) i do 350 kl./s w rozdzielczości 720×576. Wyposażony jest w wyjścia VGA, HDMI oraz trzy wyjścia BNC. Posiada również 16 wejść fonicznych, 16 wejść i wyjść alarmowych i można nim sterować przez sieć LAN. Sterowanie odbywać się może także za pomocą panelu przedniego, który jest wyposażony w gniazdo USB pozwalające na podłączenie myszy, pilotem lub za pośrednictwem dodatkowego pulpitu sterowniczego. Rejestrator umożliwia nagrywanie we wszystkich popularnych trybach – ciągłym, inicjowanym wykryciem ruchu, przebiegającym zgodnie z harmonogramem, wyzwalanym zewnętrznym alarmem. Możliwy jest także tryb, w którym nagrywanie jest wymuszane przez operatora. Nagrania mogą być zmagazynowane na pięciu dyskach twardych o pojemności do 2 TB każdy. Rejestrator ma też funkcję, która jest coraz bardziej popularna – czyli zdalny dostęp przez urządzenia mobilne smartfon z systemem operacyjnym iOS, Android, Blackberry, Symbian czy MS Mobile z dostępem do Internetu, umożliwia podgląd i sterowanie kamer z każdego miejsca na świecie.




*Rys 1. Przykładowy schemat systemu dozorowego z wykorzystaniem rejestratora HD-SDI*

Technologia HD-SDI daje nowe możliwości w dziedzinie systemów CCTV. Dzięki niej jakość obrazu może być znacznie wyższa niż w przypadku kamer analogowych, których możliwości rozwoju są ograniczone. Rozdzielczość 1080p jest pięciokrotnie większa od rozdzielczości D1, co przyczynia się do bardzo wyraźnej poprawy jakości obrazu. Zatem technologia HD-SDI oferuje jakość obrazu typową dla sieciowych kamer HD i umożliwia integrację z istniejącymi systemami analogowymi, ponieważ do przesyłania obrazów wykorzystywany jest przewód koncentryczny. Poza jakością obrazu jest to niewątpliwie największa zaleta tego rozwiązania, wpływająca przede wszystkim na obniżenie kosztów inwestycji.

Zaawansowany rejestrator, do którego można podłączyć kamery HD-SDI oraz kamery analogowe, z pewnością spodoba się wielu instalatorom i operatorom systemów CCTV. Rejestratory D-Max są znane ze swojej niezawodności oraz wygodnego interfejsu. Opisane powyżej urządzenia odpowiadają rosnącemu zainteresowaniu odbiorców kamerami i rejestratorami o wysokiej rozdzielczości. Razem z nowymi rejestratorami na rynek wprowadzone zostaną kamery kompaktowe i kopułowe działające w standardzie HD-SDI. Urządzenia te mogą być obsługiwane za pomocą znanej na rynku klawiatury typu DCK-500A i DCK-500B. Uzupełnieniem kompletnego systemu monitoringu w standardzie HD, na który składają się urządzenia firmy D-max, jest 23-calowy monitor LED DLM-23LA. Dewizą firmy D-max Dong Young Unitech jest ciągły rozwój, tworzenie coraz doskonalszych produktów. Jednym z ostatnich osiągnięć koreańskiego producenta jest ciekawe rozwiązanie zastosowane w kamerach analogowych D-max DMS-200Sec, które umożliwia wykorzystanie jednego kabla koncentrycznego do zasilania, sterowania PTZ oraz przesyłania sygnału wizyjnego. Nowa linia urządzeń HD-SDI i ciągłe udoskonalanie systemów analogowych umiejscawia firmę D-max w czołówce producentów urządzeń CCTV. Do zapoznania się z ofertą zaprasza polski dystrybutor – D-max Polska.

*Paweł Mielewczyk*
*Na podstawie materiałów*
*D-max Dong Yang Unitech*

**D-max Polska sp. z o.o.**
ul. Obornicka 276, 60-693 Poznań
tel. +48 61 822 60 52
dmax@dmaxpolska.pl
*http://www.dmaxpolska.pl*

EVIX®

# Zaawansowane rejestratory cyfrowe na każdą kieszeń
## Wysoka jakość, intuicyjna obsługa!

### ER-401, ER-801, ER-1601

- Możliwość instalacji 1 dysku (ER-401, ER-801) lub 2 w przypadku ER-1601
- Prędkość nagrywania odpowiednio: do 100 kl/s, do 200 kl/s i do 400 kl/s w zależności od modelu
- Wyjście SPOT
- 4 kanały audio
- Zdalny dostęp: IE, dedykowane oprogramowanie CMS, oprogramowanie na urządzenia mobilne

### ER-811, ER-1611

- Możliwość instalacji 4 dysków
- Prędkość nagrywania odpowiednio: do 200 kl/s i do 400 kl/s w zależności od modelu
- Wyjście wideo HDMI
- Wyjście SPOT
- eSATA
- 8/16 kanałów audio w zależności od modelu
- Zdalny dostęp: IE, dedykowane oprogramowanie CMS, oprogramowanie na urządzenia mobilne

### ER-421, ER-821, ER-1621

D1 Real-Time RECORDING

- Możliwość instalacji 8 dysków
- Prędkość nagrywania w rozdzielczości 720x576 odpowiednio: do 200 kl/s, 200 kl/s i do 400 kl/s w zależności od modelu
- Wyjście wideo HDMI (oprócz ER-421)
- Wyjście SPOT
- eSATA (oprócz ER-421)
- 4/8/16 kanałów audio w zależności od modelu
- Zdalny dostęp: IE, dedykowane oprogramowanie CMS, oprogramowanie na urządzenia mobilne

Wyłączny dystrybutor produktów Evix® w Polsce:

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

# Zawsze pełna kontrola!

Podgląd obrazu z kamer „na żywo” z telefonu komórkowego

Windows Mobile Compatible | Symbian Compatible | iPhone Compatible | Android Compatible | BlackBerry Compatible

# Funkcjonalność w dobrej cenie

- Quadrupleks
- Prędkość nagrywania do 400 obr/s
- Strefy prywatności
- Kompresja H.264
- Wyjście HDMI*
- Nagrywanie „real-time”, również w rozdzielczości D1*
- Obsługa do 8 dysków SATA
- Dwa niezależne strumienie sieciowe dla każdego kanału

*wybrane modele

CMS Compatible | Internet Explorer Compatible

# Łatwe zarządzanie rejestratorami dzięki oprogramowaniu CMS

- Możliwość jednoczesnego połączenia z wieloma rejestratorami EVIX®
- Możliwość połączenia w trybie podglądu „na żywo” do 64 kamer
- Harmonogram nagrywania lokalnego
- Zdalna konfiguracja rejestratorów, odtwarzanie nagrań, kopiowanie nagrań
- Możliwość tworzenia wielu kont użytkowników z różnymi uprawnieniami
- Moduł zdalnego monitorowania zdarzeń systemowych (detekcja ruchu, aktywacja wejść alarmowych, utrata sygnału wideo)
- Dwukierunkowe połączenie audio
- Zdalna aktualizacja oprogramowania rejestratorów
- Wizualizacja obiektu (mapy)
- Interfejs w języku polskim

# Rejestratory marki EVIX

Patryk Gańko

Obecnie firmy branży CCTV koncentrują się na rozwijaniu segmentu telewizji IP (w tym funkcji inteligentnych) oraz integracji elektronicznych systemów zabezpieczeń: telewizji dozorowej, kontroli dostępu, systemów alarmowych i innych systemów wykorzystywanych do zarządzania obiektami. W przypadku analogowych systemów telewizyjnych (pomijamy kwestie dotyczące telewizji HD SDI), a w szczególności technologii stosowanych w rejestratorach cyfrowych, mamy natomiast do czynienia ze stagnacją. Ta sytuacja spowodowała, że duża liczba producentów rejestratorów CCTV doścignęła renomowanych producentów. I właśnie z tej perspektywy chciałbym przedstawić Państwu zalety rejestratorów marki Evix, które spełniają najwyższe wymagania

Seria rejestratorów Evix obejmuje osiem modeli cztero-, ośmio- i szesnastokanałowych, podzielonych na trzy rodziny. Trzy modele – ER-421, ER-821 oraz ER-1621 – to rejestratory *real-time*, które umożliwiają zapis obrazów z każdego kanału wizyjnego z prędkością 25 kl./s i rozdzielczością D1. Pozostałe modele również zapisują z prędkością *real time*, ale dotyczy to tylko rozdzielczości CIF (360×288).

Duża prędkość zapisu rejestratorów implikuje konieczność stosowania dużych archiwów dyskowych. ER-1621 i ER-821 umożliwiają podłączenie do ośmiu dysków SATA o maksymalnej pojemności 2 TB, co pozwala na zagregowanie do 16 TB przestrzeni dyskowej. Dodatkowo do portów eSATA znajdujących się na tylnym panelu rejestratora można podłączyć dwa dodatkowe dyski do kopiowania zarejestrowanego materiału. Rejestratory umożliwiają kopiowanie materiałów w dwóch formatach – DAT oraz AVI. Do odtworzenia nagrania w formacie AVI konieczna jest wcześniejsza instalacja kodeka udostępnianego przez rejestrator. W trakcie kopiowania do archiwizowanego materiału może zostać dołączony program SuperPlayer służący do odtwarzania nagrań.

Funkcja znaku wodnego umożliwia użytkownikowi sprawdzenie oryginalności pliku wideo. Ponadto możliwy jest lokalny zrzut obrazu (*snapshot*) w formacie JPG z kamery na dysk rejestratora w celu trwałego zabezpieczenia nagrań przed nadpisaniem.

Rejestratory posiadają do 16 liniowych wejść fonicznych, dodatkowe wejście mikrofonowe oraz jedno wyjście foniczne (głośnikowe) do dwukierunkowej komunikacji głosowej. Rejestrator umożliwia też dwukierunkową komunikację głosową pomiędzy rejestratorem a komputerem z przeglądarką Internet Explorer.

Monitory mogą być podłączone do wejść BNC, VGA i – w wybranych modelach – do wyjść HDMI o rozdzielczości 1080p. Wyświetlane na monitorze obrazy z kamer można w dowolny sposób przestawiać za pomocą funkcji *drag and drop* i tworzyć ich własne układy. Również informacje statusowe mogą być wyświetlane w dowolnie wybranym fragmencie obrazu. Na monitorach podłączonych do wyjść pomocniczych (*spot monitor*) wyświetlany jest obraz z wybranego kanału w formacie pełnoekranowym lub wyświetlana jest sekwencja obrazów pochodzących z wybranych kamer.

Urządzenia mogą być obsługiwane z poziomu panelu czołowego za pomocą przycisków, pilota na podczerwień oraz myszy USB. Rejestratorami można sterować za pomocą klawiatur NV-KBD30 oraz NV-KBD70, z wykorzystaniem protokołu N-Control.

Z poziomu rejestratora oraz przeglądarki internetowej lub aplikacji CMS można sterować kamerami szybkoobrotowymi z wykorzystaniem protokołu N-Control, Pelco-D lub Pelco-P.

Funkcja eksportu i importu ustawień oraz ich zapisu na pamięci USB ułatwia zarządzanie dużą grupą rejestratorów.

Dostęp poszczególnych użytkowników do rejestratora może być ograniczony do wybranych zasobów. Poziomy dostępu obejmują m.in. podgląd i odtwarzanie obrazów ze wskazanych kamer, ustawienia systemowe, przeszukiwanie rejestrów, zamknięcie systemu, ustawienia parametrów zapisu na dysku etc. Poziom dostępu nie zależy od sposobu połączenia (połączenie lokalne albo zdalne), a jedynie od przyznanych uprawnień. Informacje o wszystkich użytkownikach, którzy w danym momencie są połączeni z rejestratorem zdalnie, są dostępne w menu rejestratora (*Informacje*), co pozwala kontrolować liczbę zdalnych użytkowników.

Rejestrator powiadamia administratora systemu o pewnej grupie zdarzeń systemowych, takich jak brak miejsca na dysku, wyłączone nadpisywanie, konflikt adresów IP, rozłączenie sieci LAN lub błąd zapisu na dysku, poprzez uruchomienie brzęczyka, wysłanie e-maila z dołączonym zdjęciem lub aktywację wyjścia alarmowego.

Z rejestratorem można łączyć się zdalnie – z poziomu przeglądarki Internet Explorer 7.0 lub nowszej (konieczna jest obsługa formantów ActiveX) – lub z poziomu oprogramowania CMS. Możliwe jest utworzenie maksymalnie dziesięciu równoczesnych połączeń z rejestratorem w trybie „na żywo", jednego połączenia w trybie odtwarzania oraz jednego połączenia w trybie konfiguracji.

W rejestratorze można zdefiniować listę adresów IP, które mogą być wykorzystane do nawiązania połączenia z danym rejestratorem, oraz listę adresów zakazanych, które nie mogą być wykorzystane do utworzenia takiego połączenia.

Cechą charakterystyczną połączenia przez przeglądarkę Internet Explorer jest wielość dostępnych funkcji, takich jak np. podgląd obrazów z kamer w trybie na żywo, zdalne wyszukiwanie i odtwarzanie nagrań, kopiowanie plików z rejestratora, konfiguracja lokalna, zdalna aktualizacja oprogramowania rejestratora, sterowanie kamerą obrotową, lokalne nagrywanie, a przede wszystkim zdalne ustawianie wszystkich parametrów rejestratora.

Dowolne przestawianie obrazów z kamer w trybie podziału jest możliwe zarówno w przypadku obsługi lokalnej, jak i zdalnej, za pośrednictwem przeglądarki IE oraz aplikacji CMS.

Główną różnicą między dostępem do zasobów rejestratora z poziomu aplikacji CMS oraz IE jest możliwość realizacji połączenia typu *multisite*, czyli z wieloma rejestratorami równocześnie, oraz tworzenie map. Definiowane mapy mogą być ze sobą łączone w celu stworzenia wielopoziomowego planu obiektu.

Rejestratory Evix umożliwiają użytkownikom podgląd obrazów z kamer na telefonach komórkowych z systemami operacyjnymi iOS, Android, Symbian, Windows Mobile lub BlackBerry. Można więc powiedzieć, że dostępne jest oprogramowanie dostosowane do większości systemów operacyjnych stosowanych w telefonach komórkowych.

Telefon łączy się z rejestratorem dzięki dostosowanej do jego systemu operacyjnego aplikacji. Oprogramowanie umożliwia nie tylko – jak wiele innych aplikacji – pełnoekranowy podgląd w trybie na żywo. Przykładowo – aplikacja SuperLivePro dla urządzenia iPhone umożliwia także podgląd w trybie podziału ekranu (2×2), zdalne odtwarzanie zapisanego materiału, przechwytywanie i podgląd zdjęć, odsłuch kanału fonicznego, sterowanie kamerami PTZ (z wywoływaniem presetów i tras obserwacji) oraz ustawienia lokalne aplikacji.

Jak widać, rejestratory Evix mogą być wykorzystywane w różnego typu obiektach – również w takich, w których obowiązują najwyższe standardy bezpieczeństwa. Wyróżniają się wieloma funkcjami, których nie mają inne rejestratory. Przykładem może być możliwość zainstalowania do ośmiu twardych dysków w jednym urządzeniu. Utworzenie tak dużej przestrzeni dyskowej innymi metodami wymaga stosowania niezależnych macierzy dyskowych. Również pod względem stabilności, parametrów i bezawaryjnej pracy rejestratory Evix nie ustępują bardziej renomowanym markom, a z ekonomicznego punktu widzenia ich wybór jest korzystniejszy. Proces zrównywania się możliwości technicznych różnych grup rejestratorów będzie postępował. Podobnie będzie w przypadku rozwiązań sieciowych.

*Patryk Gańko*
*AAT Holding*

# Nowe spojrzenie
## na ochronę informacji niejawnych

Artur Bogusz

Niniejszym artykułem pragnę rozpocząć cykl rozważań dotyczących ochrony informacji niejawnych w świetle uwarunkowań prawnych nowej ustawy o ochronie informacji niejawnych. Zmiany w obowiązujących przepisach mają wpływ na sposób pojmowania bezpieczeństwa informacji niejawnych

W dzisiejszym świecie informacja jest cennym towarem. W społeczeństwie informacyjnym zabieganie o nią staje się celem samym w sobie i prowadzi do wykształcenia się grup, które zawodowo zajmują się jej ochroną, zdobywaniem czy handlowaniem. Dotyczy to również informacji niejawnej.

Informacja jest pojmowana i definiowana różnie, ale zasadnicze ujęcia są dwa. Pierwsze można nazwać obiektywnym i wywodzi się z fizyki i matematyki. Według tych nauk informacja stanowi pewną własność fizyczną lub strukturalną obiektów. Zgodnie z ujęciem drugim, subiektywnym (kognitywistycznym), informacja jest tym, co umysł jest w stanie przetworzyć i wykorzystać do własnych celów.

W ujęciu infologicznym (Bo Sundgren 1973) „informacja to treść komunikatu przekazywanego za pomocą danych”[1] .

Ta sama treść może być przekazywana za pomocą różnych danych (znaki, mowa, wykresy). Dlatego też potocznie często używa się ich zamiennie. Informacja natomiast, według twórcy cybernetyki – Norberta Wienera, to relacja niematerialna, zachodząca jednocześnie między trzema elementami:

a) odtwarzanym elementem rzeczywistości społecznej,
b) tezaurusem punktu a,
c) społecznym nastawieniem do a i b.

Wiener zapoczątkował interpretację przyznającą informacji szczególne miejsce jednego z podstawowych elementów wszechświata, formułując w 1948 roku słynne zdanie: „Informacja jest informacją, a nie energią ani materią”[2].

## 1. Rola państwa w ochronie informacji

Współczesne państwo, reagując na kwestie handlu i chęci zaboru informacji przez wszystkie podmioty życia publicznego, kreuje instrumenty bezpieczeństwa, tworząc prawne ramy działania instytucji. Aby efekty tej działalności były pożądane, społeczeństwo musi postrzegać ją jako pożyteczną, służącą dobru publicznemu. Na gruncie ustaleń ogólnych problem wydaje się zatem rozstrzygnięty, jednak refleksja nad współczesną pozycją i rolą państwa, znaczeniem bezpieczeństwa narodowego oraz sposobami jego zapewnienia nasuwa istotne wątpliwości dotyczące słuszności stosowania tradycyjnych instrumentów oceny. Państwo, które niedostatecznie zabezpiecza informacje, to państwo zupełnie nieodporne na zewnętrzne i wewnętrzne działania uderzające w jego praworządność i samodzielność.

Problem ten można zilustrować innym, a mianowicie ujawniającą się względnością wartości chronionych przez państwo. Można go zidentyfikować poprzez wskazanie relacji między ochroną informacji niejawnych a bezpieczeństwem państwa. Pozornie zależność ta nie wydaje się zbyt złożona – ochrona ważnych zasobów informacyjnych jest związana z interesem bezpieczeństwa państwa. Skuteczne działanie wymaga utajnienia części informacji w taki sposób, aby potencjalny przeciwnik nie mógł przeciwdziałać (zaszkodzić) przyjętemu zamierzeniu. Owo utajnienie oznacza jednak – przynajmniej teoretycznie – trafną identyfikację wartości chronionych (określenie zakresu i rodzaju informacji podlegających ochronie). Zbyt szeroki zakres tajności dewaluuje ją. Zbyt wąski naraża na szwank działanie. Przedmiotem pogłębionej analizy powinny być zatem nie tylko formalne aspekty ochrony tajemnic państwowych, ale też ich współczesne pojmowanie w kontekście roli państwa, a ściślej zestawienie tych elementów[3] (tzn. informacji, materiałów, a także systemów kierowania i dowodzenia oraz obronnych – w tym ich części składowych).

## 2. Rozstrzygnięcia ustawowe dotyczące ochrony informacji

W ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r., nr 182, poz. 1228) określono zasady ochrony informacji niejawnych – zasady, które obowiązują w przypadku realizowania usług lub wykonywania zadań, podczas których uzyskuje się dostęp do tych informacji. Potwierdzeniem przestrzegania zasad ochrony informacji niejawnych przez danego przedsiębiorcę jest tzw. świadectwo bezpieczeństwa przemysłowego. Do przyznania takiego świadectwa prowadzi tzw. postępowanie bezpieczeństwa przemysłowego.

Obowiązująca od 1 stycznia 2011 roku ustawa o ochronie informacji niejawnych określa zasady ochrony informacji niejawnych, których nieuprawnione ujawnienie może być szkodliwe dla państwa.

### 2.1. Informacja i zakres jej ochrony

Ustawa określa sposoby:

– klasyfikowania informacji niejawnych;
– organizowania ochrony informacji niejawnych;
– przetwarzania informacji niejawnych;
– kontroli stanu zabezpieczenia informacji niejawnych;
– ochrony informacji niejawnych w systemach teleinformatycznych;
– fizycznego zabezpieczenia informacji niejawnych.

### 2.2. Przepisy ustawowe i ich zakres

Przepisy ustawy dotyczą następujących instytucji, jednostek organizacyjnych czy podmiotów gospodarczych:

– sejmu i senatu;
– Prezydenta Rzeczypospolitej Polskiej;
– organów administracji rządowej;
– organów jednostek samorządu terytorialnego, a także innych jednostek organizacyjnych, które są im podległe lub są przez nie nadzorowane;
– sądów i trybunałów;
– organów kontroli państwowej i ochrony prawa;
– jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
– Narodowego Banku Polskiego;
– państwowych osób prawnych i innych niż wyżej wymienione państwowych jednostek organizacyjnych;
– jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;
– przedsiębiorców zamierzających ubiegać się o zawarcie umów związanych z dostępem do informacji niejawnych,

*1) Sundgren B., „An Infological Approach to Data Base”, SUE&S, Stockholm 1973; za: materiały konferencji PLUG, Kościelisko 2005.*

*2) Wiener N., „Cybernetics or Control and Communication in the Animal and the Machine”, New York 1948; za: Cybernetyka i społeczeństwo, wyd. KiW, Warszawa 1960.*

*3) Zalewski S., „Ochrona informacji niejawnych jako instrument bezpieczeństwa politycznego państwa”, w: „Ochrona informacji niejawnych i biznesowych”. Materiały IV Kongresu, Katowice 2008, s. 43.*

ubiegających się o zawarcie takich umów, związanych takimi umowami albo wykonujących zgodnie z przepisami prawa zadania związane z dostępem do informacji niejawnych.

Przepisy ustawy dotyczące ochrony informacji niejawnych nie kolidują z obowiązującymi odrębnie przepisami ustaw o ochronie tajemnicy zawodowej lub innych tajemnic.

W niniejszym artykule zamierzam zwrócić uwagę na przedsiębiorców, którzy zamierzają zawrzeć albo zawarli umowy mające związek z dostępem do informacji niejawnych lub wykonują (albo zamierzają wykonywać) zadania związane z dostępem do takich informacji.

## 3. Wykładnia formalna pojęć ustawowych

W art. 2 ustawy podano wszelkie istotne definicje i pojęcia, które następnie, w dalszych częściach tekstu ustawy, są wykorzystywane w bardzo istotny sposób. W tym miejscu zwrócę uwagę na kilka spośród nich:

– **rękojmia zachowania tajemnicy** – stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego zdolność osoby do spełnienia ustawowych wymogów w celu zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem;
– **dokument** – każda utrwalona informacja niejawna;
– **przetwarzanie informacji niejawnych** – wszelkie operacje na informacjach niejawnych i związane z informacjami niejawnymi, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
– **kierownik przedsiębiorcy** – jednoosobowy zarząd lub organ zarządzający, a jeżeli organ jest wieloosobowy – cały organ albo członek, albo członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy (z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę); w przypadku spółki jawnej i spółki cywilnej kierownikiem przedsiębiorcy są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd, a w przypadku spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym; kierownik przedsiębiorcy jest kierownikiem jednostki organizacyjnej w rozumieniu przepisów ustawy;
– **zatrudnienie** – powołanie, mianowanie lub wyznaczenie.

Oczywiście to tylko niektóre definicje, jakie pojawiają się w ustawie o ochronie informacji niejawnych. Definicje te są bardzo istotne. Bez zrozumienia podstawowych definicji zgodnie z intencją ustawodawcy nie będzie możliwe właściwe zinterpretowanie zapisów całej ustawy o ochronie informacji niejawnych.

Informacje niejawne mogą być udostępnione wyłącznie osobie gwarantującej zachowanie tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy, pełnienia służby na zajmowanym stanowisku lub wykonywania czynności zleconych[4]. Zasady uwalniania od obowiązku zachowania informacji niejawnych w tajemnicy oraz sposób obchodzenia się z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw i rozporządzeń. Jeżeli przepisy odrębnych ustaw uprawniają organy, służby, instytucje lub ich upoważnionych pracowników do kontroli (w szczególności do swobodnego dostępu do pomieszczeń i materiałów), a jej zakres dotyczy informacji niejawnych, uprawnienia te muszą być zgodne z przepisami ustawy o ochronie informacji niejawnych.

### 3.1. Klauzule ochrony informacji

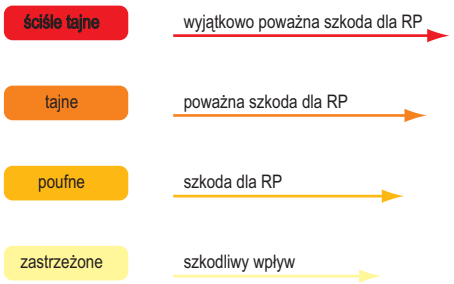
Informacje niejawne opatrza się klauzulą „**ściśle tajne**”, jeżeli ich nieuprawnione ujawnienie spowoduje **wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej** przez to, że:

– zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
– zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
– zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
– osłabi gotowość obronną Rzeczypospolitej Polskiej;
– doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze (jeżeli zagraża to bezpieczeństwu wykonywanych przez nich czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy);
– zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
– zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób im najbliższych, lub świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.), lub osób im najbliższych.

Informacje niejawne opatrza się klauzulą „**tajne**”, jeżeli ich nieuprawnione ujawnienie spowoduje **poważną szkodę dla Rzeczypospolitej Polskiej** przez to, że:

– uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
– pogorszy relacje Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
– zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
– utrudni wykonywanie czynności operacyjno-rozpoznawczych mających na celu bezpieczeństwo państwa lub ściganie sprawców zbrodni przez służby lub instytucje do tego uprawnione;
– w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
– znacznych rozmiarów stratę związaną z interesami ekonomicznymi Rzeczypospolitej Polskiej.

*4) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. z 2010 r., nr 182, poz. 1228.*




*Rys. 1. Zobrazowanie definicji poszczególnych klauzul*

Informacje niejawne opatrza się klauzulą „**poufne**", jeżeli ich nieuprawnione ujawnienie spowoduje **szkodę dla Rzeczypospolitej Polskiej** przez to, że:

– utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
– utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
– zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
– utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za bezpieczeństwo lub podstawowe interesy Rzeczypospolitej Polskiej;
– utrudni wykonywanie zadań organom wymiaru sprawiedliwości i służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwo obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych;
– zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
– niekorzystnie wpłynie na funkcjonowanie gospodarki narodowej.

Informacje niejawne opatrza się klauzulą „**zastrzeżone**", jeżeli nie opatrzono ich powyższą klauzulą tajności, a ich nieuprawnione ujawnienie może mieć **szkodliwy wpływ** na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań mających związek z obroną narodową, polityką zagraniczną, bezpieczeństwem publicznym, przestrzeganiem praw obywateli, wymiarem sprawiedliwości albo interesami ekonomicznymi Rzeczypospolitej Polskiej.

Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem posiadanej klauzuli tajności.

## 3.2. Postępowanie z materiałami objętymi klauzulą niejawności

Jeżeli zrozumiemy i zaakceptujemy zaproponowane przez ustawodawcę definicje poszczególnych klauzul niejawności, musimy zapoznać się z zasadami ich nadawania. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności na zasadach określonych w ustawie. Osoba, o której mowa wyżej, może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności. Zniesienie lub zmiana klauzuli tajności jest możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę wskazaną powyżej albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony. Nie rzadziej niż raz na pięć lat kierownicy jednostek organizacyjnych dokonują przeglądu materiałów w celu ustalenia, czy zgodnie z ustawą wymagają one ochrony. W przypadku informacji niejawnych o klauzuli „ściśle tajne" pisemną zgodę na ten przegląd wyraża kierownik jednostki organizacyjnej, w której materiałowi została nadana klauzula tajności. Po zniesieniu lub zmianie klauzuli tajności zmienia się oznaczenie materiału i informuje o tym odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli. W przypadku rozwiązania, zniesienia, likwidacji, upadłości obejmującej likwidację majątku upadłego, przekształcenia lub reorganizacji jednostki organizacyjnej uprawnienia w zakresie zniesienia lub zmiany klauzuli tajności materiału przechodzą na następcę prawnego. W razie braku następcy prawnego uprawnienia w tym zakresie przechodzą na Agencję Bezpieczeństwa Wewnętrznego (ABW) lub Służbę Kontrwywiadu Wojskowego (SKW) Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności. To oczywiście tylko kilka zasad oznaczania dokumentów klauzulą niejawności, które można by nazwać podstawowymi i wystarczającymi na poziomie początkowym funkcjonowania podmiotów ustawy.

## 3.3. Udostępnianie materiałów – wątpliwości i zastrzeżenia wobec klauzul

Zgodnie z przepisami ustawy informacje niejawne, którym nadano określoną klauzulę tajności, mogą być udostępnione wyłącznie osobie uprawnionej do dostępu do informacji o tejże klauzuli tajności. Można je przetwarzać w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności. Informacje niejawne muszą być chronione odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

W przypadku jakichkolwiek wątpliwości odbiorca materiału, który stwierdzi zawyżenie albo zaniżenie tajności, może zwrócić się do osoby, która nadała klauzulę w danym przypadku, albo do przełożonego tej osoby z wnioskiem o dokonanie stosownej zmiany. W przypadku odmowy lub nieudzielenia odpowiedzi w ciągu 30 dni od daty złożenia wniosku odbiorca materiału może zwrócić się odpowiednio do ABW lub SKW z wnioskiem o rozstrzygnięcie sporu. Spór zostanie rozstrzygnięty w terminie 30 dni od daty złożenia wniosku. Jeżeli stroną sporu, o którym mowa, jest ABW albo SKW, to rozstrzyga go Prezes Rady Ministrów w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu. Ze względu na sposób zdefiniowania poszczególnych klauzul i brak przykładowych informacji, które mogłyby być opatrzone klauzulami danych rodzajów, umożliwione przez ustawodawcę podważanie zasadności klauzuli może być nagminne, np. wówczas, gdy nadanie określonej klauzuli będzie mogło w jakiś sposób uniemożliwić jednej ze stron uczestniczenie w dalszej części postępowania przetargowego. Może to być niebezpieczne, szczególnie dla służb ochrony państwa, gdyż

bardzo trudno wyobrazić sobie komórkę, która będzie odpowiedzialna za rozstrzyganie sporów dotyczących klauzul we wszystkich możliwych przypadkach.

## 4. Funkcjonowanie systemu ochrony informacji

Do tych obowiązków ABW i SKW, które są związane z nadzorowaniem funkcjonowania systemu ochrony informacji niejawnych w podległych im jednostkach organizacyjnych, należy:

– przeprowadzanie kontroli ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;
– realizowanie zadań z zakresu bezpieczeństwa systemów teleinformatycznych;
– prowadzenie postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego;
– zapewnianie ochrony informacji niejawnych wymienianych między RP a innymi państwami lub organizacjami międzynarodowymi;
– doradztwo i organizowanie szkoleń w zakresie ochrony informacji niejawnych.

SKW realizuje zadania dotyczące:

– MON oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
– ataszatów obrony w placówkach zagranicznych;
– żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w jednostkach organizacyjnych podległych MON.

ABW realizuje zadania dotyczące jednostek organizacyjnych i osób podlegających ustawie, których nie wymieniono wyżej.

Aktualny podział kompetencji nie budzi wątpliwości, gdyż dość jasno precyzuje, w jakich sytuacjach właściwą służbą ochrony państwa jest SKW, a w jakich ABW.

### 4.1. Krajowa władza bezpieczeństwa

Szef ABW pełni funkcję krajowej władzy bezpieczeństwa. Krajowa władza bezpieczeństwa jest odpowiedzialna za nadzorowanie systemu ochrony informacji niejawnych w stosunkach RP z innymi państwami lub organizacjami międzynarodowymi i wydawanie dokumentów upoważniających do dostępu do informacji niejawnych NATO, Unii Europejskiej lub innych organizacji międzynarodowych, zwanych dalej „informacjami niejawnymi międzynarodowymi". Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w odniesieniu do podmiotów, o których mowa w art. 10 ust. 2 ustawy, za pośrednictwem Szefa SKW. W zakresie niezbędnym do wykonywania funkcji krajowej władzy bezpieczeństwa odpowiednio Szef ABW lub upoważnieni przez niego funkcjonariusze ABW oraz Szef SKW lub upoważnieni przez niego żołnierze lub funkcjonariusze SKW mają prawo do:

– wglądu do dokumentów związanych z ochroną informacji niejawnych międzynarodowych;
– wstępu do obiektów i pomieszczeń przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
– dostępu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych;
– uzyskiwania wyjaśnień i informacji dotyczących ochrony informacji niejawnych międzynarodowych.

Szef ABW organizuje współdziałanie z Szefem SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa.

### 4.2. Uprawnienia do nadzoru i kontroli

W zakresie niezbędnym do kontroli stanu zabezpieczenia informacji niejawnych, upoważnieni pisemnie funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mają prawo do:

– wstępu do obiektów i pomieszczeń jednostki kontrolowanej, gdzie informacje takie są przetwarzane;
– wglądu do dokumentów związanych z organizacją ochrony tych informacji w kontrolowanej jednostce organizacyjnej;
– żądania udostępnienia do kontroli systemów teleinformatycznych służących do przetwarzania tych informacji;
– przeprowadzania oględzin obiektów i składników majątkowych oraz sprawdzania przebiegu określonych czynności związanych z ochroną tych informacji;
– żądania udzielania ustnych i pisemnych wyjaśnień od kierowników i pracowników kontrolowanych jednostek organizacyjnych;
– zasięgania informacji w jednostkach niekontrolowanych (w związku z przeprowadzaną kontrolą), jeżeli ich działalność pozostaje w związku z przetwarzaniem lub ochroną informacji niejawnych, oraz żądania wyjaśnień od kierowników i pracowników tych jednostek;
– powoływania oraz korzystania z pomocy biegłych i specjalistów, jeżeli ze względu na okoliczności ujawnione w czasie przeprowadzania kontroli wymagane są wiadomości specjalne;
– uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych, a także organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony tych informacji w kontrolowanej jednostce organizacyjnej.

Jeżeli w czasie dokonywania kontroli, o której mowa wyżej, okaże się, że w systemach teleinformatycznych, które nie posiadają akredytacji bezpieczeństwa teleinformatycznego, prawdopodobne lub możliwe jest zdarzenie przetwarzania informacji niejawnych, funkcjonariusze ABW albo funkcjonariusze lub żołnierze SKW mogą żądać udostępnienia tych systemów do kontroli – wyłącznie w celu i zakresie niezbędnym do ustalenia, czy przetwarzanie takie miało miejsce, oraz do wyjaśnienia okoliczności z tym związanych.

*Artur Bogusz*

Bibliografia

1. Anzel M., *Nowa ustawa i jej zmienione uwarunkowania*, mat. szkoleniowe OSPOIN, Warszawa 2010.
2. Hoc St., *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. LexisNexis, Warszawa 2010.
3. Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, wyd. LexisNexis, Warszawa 2011.
4. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych, Dz. U. z 2010 r., nr 182, poz. 1228.
5. *Wytyczne w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne* zał. do Decyzji Nr 362/MON z dnia 28 września 2011 r.


# RACS 4

## System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.
- **INTEGRACJA** z innymi systemami:

RCP CCTV SSWiN

*RCP Master* *PR602LCD*

roger®

www.roger.pl

# Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Wprowadzono do oferty **PR621-CH** - kontroler dostępu z kieszenią do zastosowań hotelowych.


# Sterowanie systemem alarmowym

Jeszcze do niedawna obsługa systemów alarmowych kojarzyła się z manipulatorami pełnymi migających wskaźników i niezrozumiałych skrótów wyświetlanych na ekranie. Firma SATEL, wprowadzając kolejne wersje swoich produktów, przykłada wagę do tego, by korzystanie z systemu na co dzień było ułatwione, a jego programowanie i okresowe testowanie usprawnione. Obecnie, w przypadku nowoczesnych urządzeń, takich jak INTEGRA czy VERSA, obsługa z wykorzystaniem manipulatora to tylko jeden z wielu sposobów sterowania systemem alarmowym. Dzięki funkcjom oferowanym przez dodatkowe moduły centrale te mogą być z powodzeniem obsługiwane z wykorzystaniem pilotów radiowych, kart zbliżeniowych, telefonów komórkowych, tabletów czy komputerów

## Manipulatory

Pomimo wielości urządzeń umożliwiających sterowanie nadal największą popularnością cieszą się manipulatory. Do obsługi systemu za pomocą tych właśnie urządzeń wystarczy użyć hasła wpisywanego przez użytkownika na klawiaturze. Ich dużą zaletą jest też możliwość łatwego dostępu do bardziej zaawansowanych funkcji, takich jak dodawanie nowych użytkowników, programowanie czasu w centrali czy ręczne sterowanie urządzeniami podłączonymi do centrali alarmowej. Z kolei instalatorzy mogą docenić łatwość testowania i zmian w konfiguracji systemu. Dostęp do najczęściej wykorzystywanych funkcji nie wymaga przyłączania komputera ani innych dodatkowych urządzeń, co pozwala oszczędzić cenny czas.

Najbardziej popularne typy manipulatorów to manipulatory LED oraz LCD. Te pierwsze przekazują najważniejsze informacje w sposób uproszczony – sygnalizują stany centrali diodami LED pełniącymi funkcje wskaźników. Manipulatory LCD mają tekstowy wyświetlacz, na którym informacje mogą być podawane w postaci tekstów w języku polskim.

Z reguły konkretne modele manipulatorów są przeznaczone do obsługi określonych central alarmowych. Wybór modelu centrali niejako determinuje wybór manipulatora. Różnice między nimi nie sprowadzają się do wzornictwa. Przykładowo – manipulatory z serii INT-KLCDR, przeznaczone do central INTEGRA, posiadają wbudowany czytnik kart zbliżeniowych ułatwiający obsługę systemu osobom, które nie chcą lub nie mogą zapamiętać haseł dostępu.

Pod wieloma względami szczególnym manipulatorem z oferty firmy SATEL jest INT-KSG. Jest on przeznaczony do obsługi central INTEGRA. Oprócz bardzo atrakcyjnego wyglądu, nawiązującego do współczesnych trendów wzorniczych w elektronice użytkowej, posiada on szereg niepowtarzalnych cech technicznych. Przede wszystkim został wyposażony w pojemnościową klawiaturę sensoryczną, pozbawioną tradycyjnych mechanicznych przycisków. Wyznaczone pola reagują na dotknięcie palcem. Brak mechanicznych styków poprawia jego niezawodność i ułatwia utrzymanie urządzenia w czystości. Kolejną innowacją w INT-KSG jest duży ekran pozwalający dowolnie zaaranżować prezentowane na nim informacje. Takie rozwiązanie powoduje, że użytkownikowi łatwiej zorientować się, czy (i w jakim trybie) system czuwa. Ponadto może np. sprawdzić, jaka jest temperatura w pomieszczeniach z zainstalowanymi odpowiednimi czujkami, czy jednym spojrzeniem sprawdzić stan urządzeń sterowanych przez centralę.

Kolejną funkcję szczególnie docenią ci, którzy konfigurują centrale INTEGRA. Polecenia szybkiego dostępu z funkcjami MAKRO umożliwiają użytkownikowi uruchamiać nawet bardzo złożone sterowanie pojedynczym poleceniem. Przykładowo – uruchomienie scenariusza „seans filmowy" może spowodować opuszczenie rolet zewnętrznych, wyłączenie głównego oświetlenia i ściemnienie świateł pomocniczych w celu oddania nastroju panującego na sali kinowej.

## Piloty i karty zbliżeniowe

Jeżeli system alarmowy ma być obsługiwany przez osoby mogące mieć trudności z posługiwaniem się manipulatorami, dobrym pomysłem może być wyposażenie go w urządzenia

umożliwiające sterowanie pilotami i kartami zbliżeniowymi. Istnieje wiele uniwersalnych zestawów do zdalnego sterowania, które umożliwiają sterowanie praktycznie dowolną centralą alarmową. Takie sterowanie odbywa się dzięki odpowiedniemu połączeniu wyjść odbiornika pilotów z wejściami centrali – niestety w tym przypadku nie ma możliwości zidentyfikowania osoby obsługującej system.

W przypadku central INTEGRA i VERSA z pomocą przychodzi dedykowany moduł zdalnego sterowania INT-RX. Dzięki niemu każdy użytkownik systemu może mieć przypisanego pilota, który umożliwia mu nie tylko podstawowe sterowanie systemem (włączanie i wyłączanie czuwania), ale także np. wezwanie pomocy w razie konieczności czy sterowanie dodatkowymi urządzeniami – bramą garażową czy roletami.

Zamiast pilotów do sterowania można używać kart zbliżeniowych. Takie rozwiązanie jest najprostsze. Na karcie nie ma żadnych przycisków, a obsługa za jej pomocą sprowadza się do zbliżenia jej do odpowiedniego czytnika.

W przypadku sterowania centralami INTEGRA oraz VERSA najlepszym rozwiązaniem jest użycie modułu INT-CR. Pozwala on na zdefiniowanie, które strefy (i w jakiej konfiguracji) mają być załączane kartą użytkownika. Aby wybrać odpowiedni tryb w przypadku sterowania za pomocą INT-CR, wystarczy zbliżyć kartę do czytnika i poczekać na zaświecenie się diody sygnalizującej wybrany tryb pracy systemu.

W przypadku centrali INTEGRA dobrym rozwiązaniem może być też skorzystanie z manipulatora INT-KLCDR wyposażonego we wbudowany czytnik kart. Jest to rozwiązanie uniwersalne. Z jednego miejsca można sterować systemem zarówno w sposób tradycyjny (za pomocą haseł), jak i uproszczony (korzystając z kart zbliżeniowych).

Ze względu na minimalizację ryzyka błędnej obsługi za pomocą kart zbliżeniowych i pilotów taki sposób sterowania jest doskonałym rozwiązaniem w przypadku systemów, które mają być obsługiwane przez osoby starsze czy dzieci.

## Zdalna obsługa systemu

Wszystkie wspomniane metody sterowania można wykorzystać do obsługi lokalnej. Możliwości oferowane przez nowoczesne cyfrowe komunikatory – zarówno GSM/GPRS, jak i Ethernet – pozwalają w pełni sterować systemami INTEGRA czy nawet VERSA zdalnie – nawet z odległych miejsc na globie. Najprostszym rodzajem zdalnego sterowania jest komunikacja za pomocą SMS. Wysyłając wiadomość o określonej treści, można np. włączyć czuwanie systemu lub nawet uruchomić podlewanie ogrodu. Do bardziej „interaktywnego" sterowania przez telefon może służyć moduł głosowy INT-VG – steruje się klawiszami telefonu, wybierając opcje z głosowego menu. Ciekawostką jest sposób rejestrowania komunikatów głosowych. Funkcja automatycznego przetwarzania tekstu na mowę eliminuje konieczność samodzielnego nagrywania odpowiednich wiadomości.

Najbardziej zaawansowanym sposobem zdalnej obsługi jest skorzystanie z aplikacji MobileKPD w telefonie komórkowym lub smartfonie. Takie sterowanie jest możliwe jedynie w przypadku centrali INTEGRA wyposażonej w komunikator TCP/IP ETHM-1. Umożliwia on komunikację z centralą przez Internet. Dzięki aplikacjom MobileKPD oraz MobileKPD2 dla smartfonów z ekranami dotykowymi można sterować systemem w taki sam sposób jak w przypadku manipulatora znajdującego się bezpośrednio przy centrali. Dzięki temu można użyć ich także do obsługi podłączonych do centrali urządzeń automatyki służących do sterowania oświetleniem, podnoszeniem i opuszczaniem rolet czy zraszaniem zieleni. W wersji PRO aplikacja udostępnia także mechanizm makropoleceń, taki jak w przypadku zaawansowanego manipulatora INT-KSG, co jeszcze bardziej ułatwia korzystanie z rozbudowanych możliwości systemów inteligentnych.

Jak widać, jest wiele możliwych sposobów sterowania systemami SATEL. Można dostosować funkcje i sposób obsługi do oczekiwań danego użytkownika. Warto zapoznać się z tymi możliwościami, aby móc przedstawić inwestorowi kompleksową, dopasowaną dokładnie do jego potrzeb i oczekiwań ofertę – w końcu to spełnianie oczekiwań klienta stanowi o sukcesie w dzisiejszych czasach.

*SATEL*

# Systemy alarmowe **Satel**


aplikacja na smartfony **MobileKPD2**
manipulator sensoryczny **INT-KSG-SSW**

Szeroki wachlarz możliwości sterowania w centralach **INTEGRA** staje się szczególnie przydatny przy systemach inteligentnego budynku. Manipulator sensoryczny **INT-KSG** może nie tylko służyć do włączania i wyłączania dozoru, ale oferuje też wygodne rozwiązanie sterowania urządzeniami automatyki systemu **INTEGRA** oraz urządzeniami KNX.

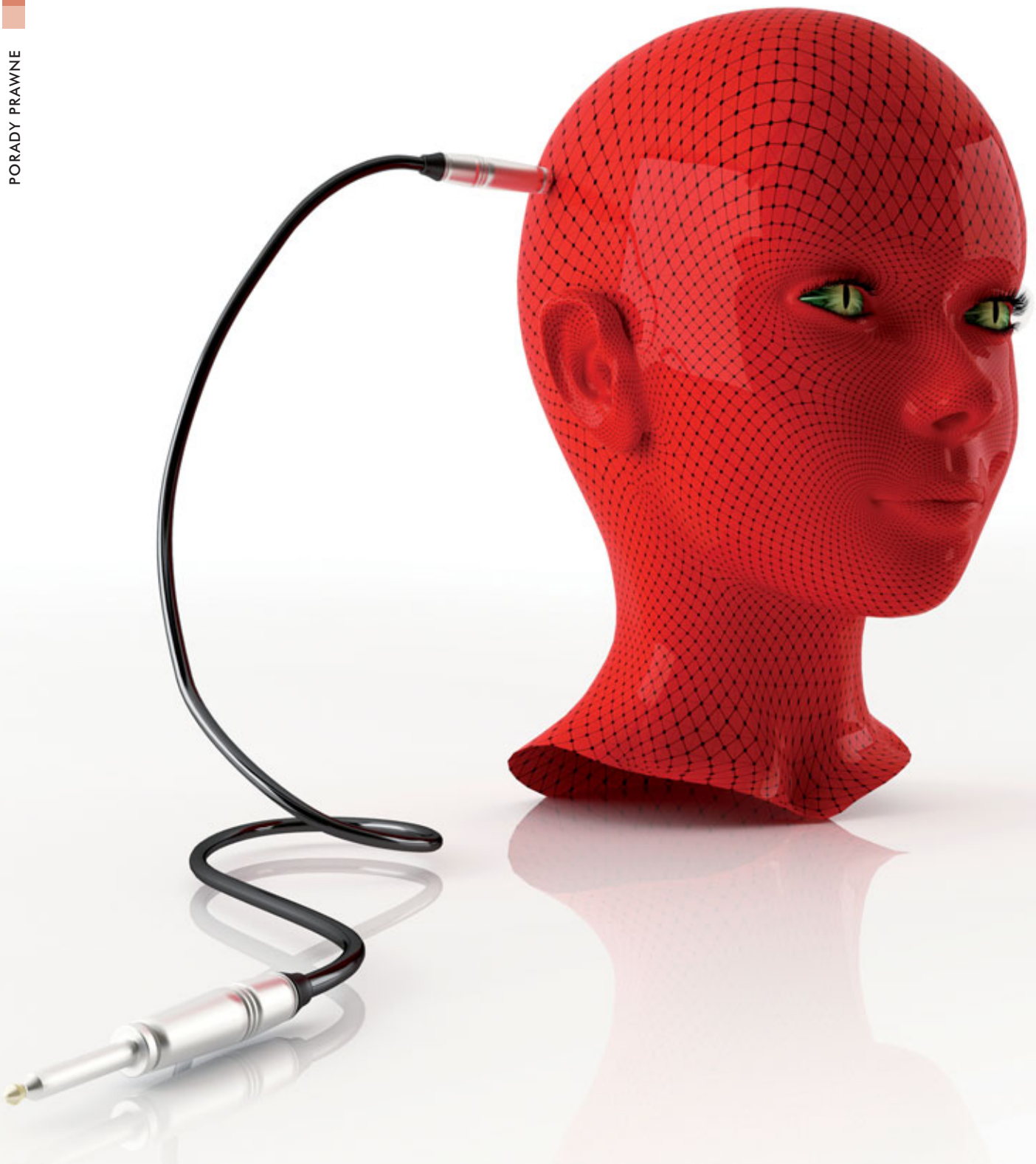
Wyposażona w odpowiedni moduł komunikacji centrala **INTEGRA** pozwala realizować ten sam zakres sterowania za pomocą SMS czy aplikacji dla zwykłych telefonów komórkowych, jak i nowoczesnych smartfonów - iPhone oraz urządzeń opartych o system Android. Możliwe jest też użycie w tym celu laptopa z połączeniem internetowym.

## **Wygodne sterowanie** zdalne i lokalne

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

Satel

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



# Kradzież tożsamości i stalking

## czyli cyberprzestępstwa w nowej odsłonie

Monika Brzozowska

Coraz więcej osób pada ofiarą tzw. kradzieży tożsamości. W potocznym rozumieniu sformułowanie to oznacza wyłudzenie danych osobowych, a następnie ich wykorzystanie do realizacji określonego celu. Często celem tym jest kradzież oszczędności, zaciągnięcie kredytu lub zakup towarów w e-sklepach. Istotą kradzieży tożsamości jest podszywanie się pod inną osobę i przywłaszczenie jej danych osobowych. Ogólnie można ją więc zdefiniować jako uzyskanie cudzych danych osobowych w celu ich przywłaszczenia i wykorzystania

Kradzież tożsamości przez długi czas nie była objęta regulacjami prawnymi, mimo że pojęcie pojawiało się w literaturze, a samo działanie polegające na podszywaniu się pod inną osobę było znane policji i prokuraturze. Trudno jednak było znaleźć przepis, na podstawie którego można było postawić sprawcy zarzuty.

Sytuacja zmieniła się w 2011 r., kiedy to nowelizacją[1] Kodeksu karnego wprowadzono przepis art. 190a § 2 kk, który penalizuje tego typu zachowanie. Zgodnie z jego brzmieniem karze pozbawienia wolności do trzech lat podlega każdy, kto podszywając się pod inną osobę, wykorzystuje jej wizerunek lub dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Dalej kk stanowi, że jeśli następstwem tego podszywania się pod inną osobę jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do dziesięciu lat (art. 190a § 3 kk). W przypadku typu podstawowego przestępstwa kradzieży tożsamości ustawodawca wprowadził tzw. tryb wnioskowy, co oznacza, że ściganie odbywa się na wniosek pokrzywdzonego. Bez wniosku ani policja, ani prokuratura nie podejmą działania. Z oczywistych przyczyn natomiast z urzędu odbywa się ściganie typu kwalifikowanego przez następstwo w postaci targnięcia się przez pokrzywdzonego na własne życie.

Przepis wprowadzono w związku z coraz częstszymi doniesieniami o umieszczaniu przez przestępców w sieci zdjęć i danych osobowych ofiar, zamawianiu na ich koszt towarów, korzystaniu z różnego rodzaju usług, zakładaniu kont na popularnych serwisach (w tym portalach społecznościowych czy tzw. serwisach randkowych).

Co niezwykle istotne, pociągnięcie do odpowiedzialności za podszywanie się pod inną osobę jest niezależne od sposobu, w jaki sprawca pozyskał dane osobowe lub wizerunek. Mógł więc wejść w posiadanie tych danych zupełnie legalnie (np. będąc w związku małżeńskim z przyszłą ofiarą, będąc kolegą/koleżanką z pracy itp.). Osoba, której dane zostały przywłaszczone, mogła je sama przekazać przestępcy, oczywiście nie będąc świadoma, do jakiego celu te dane zostaną w przyszłości wykorzystane.

Częstą metodą wyłudzania danych przez przestępców jest wykorzystanie fałszywej strony banku internetowego, łudząco podobnej do tej, z której korzysta ofiara, logując się do swojego konta bankowego. Dane, które podaje nieświadomy niczego użytkownik (przede wszystkim nazwa użytkownika i hasło), są zapisywane w bazie danych atakującego (phishera, jak określa się osobę, która wyłudza dane w przedstawiony sposób). Następnie użytkownik – aby nie było podejrzeń – jest kierowany na prawidłową stronę banku i logowany do swojego konta bankowego.

Oczywiście może się również zdarzyć kradzież danych osobowych innymi metodami.

Trzeba podkreślić, że kradzież tożsamości, która jeszcze niedawno wydawała się jedynie fikcją, dziś dotyka coraz większej liczby osób. Internet sprzyja tego typu działaniom.

Kradzież tożsamości to nie jedyna przykra rzecz, z którą może spotkać się użytkownik cyberprzestrzeni. W ostatnim czasie mieliśmy do czynienia z doniesieniami prasowymi dotyczącymi rzekomego stalkingu Katarzyny Tusk. Warto więc przybliżyć czytelnikom ten nowy rodzaj przestępstwa, jakim jest stalking (uporczywe nękanie).

Zjawisko stalkingu pojawiło się w latach 80. XX wieku – nie jest więc nowością, choć bez wątpienia nowoczesne technologie mogą sprzyjać tego typu działaniom. Za ofiary stalkingu uznaje się m.in. Johna Lennona czy Agnieszkę Kotlarską (Miss Polski 1991 i Miss International, zamordowaną przez zakochanego w niej fana, którego nękanie ignorowała). Na czym polega stalking? Ogólnie rzecz ujmując, polega na takim działaniu sprawcy, które cechuje się uporczywością i wskutek którego u ofiary występuje poczucie zagrożenia.

W ostatnim czasie coraz bardziej popularny staje się cyberstalking – forma nękania o niezwykle szerokim zasięgu, niewymagająca dużych nakładów finansowych i przede wszystkim sprawiająca trudności w wykryciu sprawcy. Cyberstalking to uporczywe nękanie za pomocą wszelkiego rodzaju działań z wykorzystaniem nowoczesnych technologii (ze szczególnym uwzględnieniem Internetu). Do najczęstszych zachowań cechujących się uporczywością sprawcy (stalkera) można zaliczyć nieustanne wysyłanie SMS-ów, MMS-ów, e-maili, ale również podawanie prawdziwych danych ofiary w fałszywych ogłoszeniach internetowych (np. o charakterze seksualnym), podawanie prawdziwych danych osobowych w fałszywych plotkach publikowanych w Internecie, upublicznianie wizerunków ofiary w Internecie (często naruszające jej dobre imię lub godność).

Przez długi czas w Polsce ofiary stalkingu (których nie brakowało) nie miały podstaw do dochodzenia swoich praw w przepisach Kodeksu karnego. Wybierały więc drogę cywilną (naruszenie prywatności czy miru domowego – na zasadzie ochrony dóbr osobistych przewidzianej przez art. 23 i 24 Kodeksu cywilnego) lub drogę skargi z tytułu wykroczenia, tj. „dokuczenia innej osobie poprzez złośliwe niepokojenie" (art. 107 Kodeksu wykroczeń). Były to jednak procesy albo długotrwałe, albo nieskuteczne. Sytuacja zmieniła się niedawno, gdyż od maja 2011 r. ofiary stalkingu mogą składać zawiadomienia o popełnieniu przestępstwa uporczywego nękania.

*1) Ustawa z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny (Dz.U. nr 72, poz. 381).*

Zgodnie bowiem z art. 190a § 1 kk karze pozbawienia wolności do lat trzech podlega każdy, kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność.

Bardzo istotną kwestią jest tzw. uporczywość. Jednorazowe działanie, np. plotka w Internecie, jednorazowy wpis lub post, nie będzie „uporczywym zachowaniem sprawcy", nawet jeśli wzbudzi w ofierze poczucie zagrożenia. Może jednak nosić znamiona przestępstwa pomówienia – art. 212 § 2 kk (jeśli plotka będzie nieprawdziwa i jednocześnie może poniżyć daną osobę w opinii publicznej), lub przestępstwa znieważenia – art. 216 § 2 kk (jeśli wpis będzie obrażać inną osobę, np. poprzez używanie wulgaryzmów).

„Uporczywy" to zgodnie z definicją „trudny do usunięcia, utrzymujący się długo lub ciągle powtarzający się, nieustanny, uciążliwy"[2]. W orzeczeniach sądowych pojawiają się takie sformułowania jak: „działania trwające dłuższy czas"[3], „wielokrotność zachowań"[4].

Badania psychologiczne pokazują, jakie mogą być (i jakie są) skutki cyberstalkingu. Ofiara cyberstalkera na początku albo odpowiada na działania, albo je ignoruje. Gdy tego typu zachowania nie przynoszą efektu, a stalker działa dalej, ofiara zaczyna odczuwać zagrożenie, np. przestaje wychodzić z domu, zmienia otoczenie, unika kontaktów itp. W skrajnych przypadkach próbuje nawet odebrać sobie życie. W sytuacji gdy następstwem stalkingu jest targnięcie się ofiary na swoje życie, Kodeks karny przewiduje zaostrzenie kary (art. 190a § 3 kk).

Podobnie jak w przypadku przestępstwa z art. 190a § 2 kk, również w przypadku stalkingu pozostaje bez znaczenia sposób, w jaki stalker pozyskał dane osobowe (czy włamał się do komputera ofiary, czy pozyskał je legalnie, np. jako były pracownik lub były małżonek, czy też je wyłudził). Ustawodawca zdecydował się na penalizowanie samego uporczywego nękania, które u ofiary powoduje poczucie zagrożenia lub narusza jej prywatność.

Internet i wszelkiego rodzaju nowe technologie oprócz wielu korzyści niosą również zagrożenia. Coraz więcej osób skarży się na obraźliwe posty, coraz częściej pojawiają się doniesienia prasowe dotyczące pomówień, stalkingu czy kradzieży tożsamości. Ustawodawca zauważył ten problem, zatem tego typu zachowania – od niedawna – stanowią przestępstwa w rozumieniu prawa karnego. Oczywiście praktyka pokaże, jakie będą orzeczenia sądowe w tym zakresie.

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

*2) Uniwersalny słownik języka polskiego, red. S. Dubisz, PWN 2003.*

*3) Np. wyrok SA w Łodzi z 18 stycznia 2001 r., II AKa 241/00, LEX nr 54979.*

*4) Postanowienie SA w Krakowie z 13 grudnia 2000 r., II AKz 289/00, LEX nr 46065.*

# *full internet control.*

ULISSE

ULISSE IR360

ULISSE PLUS

ULISSE MAXI

ULISSE jest pierwszym systemem PTZ stworzonym do aplikacji CCTV z kamerami sieciowymi ONVIF: SD, HD oraz megapikselowymi. Wykorzystując tylko jeden adres IP - wszystkie funkcje PTZ oraz kamery, włączając presety i wycieraczkę, mogą być łatwo sterowane poprzez sieć z poziomu większości dostępnych na rynku Systemów Zarządzania Wideo.

www.videotec.com

VIDEOTEC


# Bariery podczerwieni i czujka 3 x PIR

ATSUMI®

seria NR-TS/NR-TM

seria NR-QS/NR-QM

SIR10S

Wyłączny dystrybutor produktów Atsumi w Polsce:

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

# Red Barrier

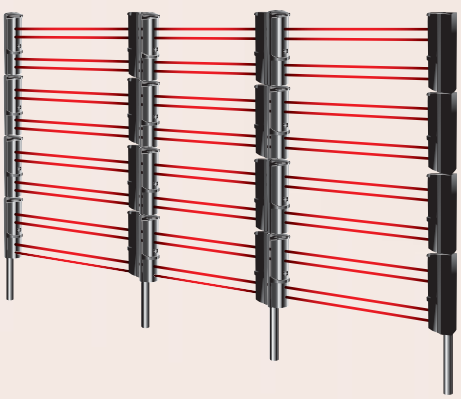
**Zbuduj niewidzialny system detekcji z ATSUMI**

## Zewnętrzne bariery podczerwieni

dwuwiązkowe serii **NR-TS** i **NR-TM**
czterowiązkowe serii **NR-QS** i **NR-QM**

**Bariery podczerwieni ATSUMI posiadają niezawodne, kontrolowane cyfrowo układy, które zapewniają bezawaryjną pracę i doskonałą ochronę nawet w najtrudniejszych warunkach środowiskowych.**

- Sferyczne soczewki Fresnela
- Skuteczna detekcja nawet przy 99% poziomie tłumienia wiązki, podczas pracy w trudnych warunkach atmosferycznych (deszcz, mgła, śnieg itp.)
- Układ automatycznej regulacji wzmocnienia (AGC)
- Podwójna modulacja częstotliwości wiązki i funkcja kontroli mocy sygnału wiązki (NR-QS, NR-QM)
- Obwód EDC (NR-QS, NR-QM)
- Wybór kanału częstotliwości pracy (NR-QM, NR-TM)
- Tryb OR (NR-QM)
- Klasy szczelności IP54 (NR-QS, NR-QM) i IP55 (NR-TS, NR-TM)
- Łatwa instalacja
- Wysoce niezawodna ochrona obwodowa oparta na innowacyjnej technologii - możliwość instalacji do 4 barier w pionie (NR-QM)



## Zewnętrzna pasywna czujka podczerwieni 3 x PIR

**SIR10S**

**Czujka podczerwieni ATSUMI wykorzystuje nowo opracowaną metodę potrójnej detekcji PIR, dzięki czemu zapewnia niezawodną ochronę na zewnątrz obiektów i jednocześnie jest odporna na źródła fałszywych alarmów.**

- Sferyczne soczewki Fresnela
- Zbieranie informacji przez 3 niezależne czujniki PIR
- Filtry światła białego
- Możliwość podłączenia do systemów CCTV lub innych aplikacji
- Klasa szczelności IP55
- Wszechstronność instalacji, możliwość montowania czujek jedna koło drugiej lub naprzeciwko siebie

## Metoda zapobiegania fałszywym alarmom dzięki potrójnej detekcji PIR

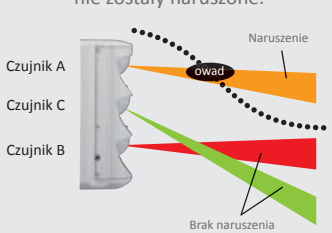
### Bezpośrednie działanie promieni słonecznych

Naruszenie pól detekcji czujników A i B.
Pole detekcji czujnika C
nie zostało naruszone.


Nawet w przypadku, gdy czujniki A i B skierowane są bezpośrednio na działanie promieni słonecznych, czujka nie wchodzi w stan alarmu.

### Owady, ptaki i zwierzęta

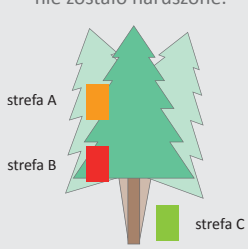
Naruszenie pola detekcji czujnika A.
Pola detekcji czujników B i C
nie zostały naruszone.




Latające ptaki, owady lub spadające z drzew liście nie powodują wejścia czujki w stan alarmu.

### Poruszająca się roślinność

Naruszenie pól detekcji czujników A i B.
Pole detekcji czujnika C
nie zostało naruszone.




Kołysząca się roślinność nie powoduje wejścia czujki w stan alarmu.

# O (S)UFO
## i lotniskach dla nich

Jan Rybczyński

1 grudnia 2011 r. weszło w życie rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 października 2011 r. w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji (Dz.U. 2011 nr 245 poz. 1462). Ponieważ data wejścia w życie jest już zeszłoroczna, można byłoby tylko poinformować o zaistnieniu takiej zmiany, gdyby nie kłopot, jaki sprawiło wprowadzenie słowniczka w tym akcie prawnym (o czym w dalszej części artykułu). Przepisy tego rozporządzenia są jednak ważne same w sobie, gdyż można szacować, że dotyczą, jak mówi jego uzasadnienie, około 1500 firm zajmujących się ochroną posiadających status SUFO. Dochodzą do tego oczywiście wewnętrzne służby ochrony

Dla porządku wskażmy ważniejsze zmiany, istotne w praktyce SUFO.

Z treści rozporządzenia usunięto zbędne od wielu lat (ze względu na art. 29 ust. 1 pkt 1 i 2 Ustawy z dnia 21 maja 1999 r. o broni i amunicji) powtórzenie regulacji dotyczącej ubiegania się o wydanie pozwolenia na broń na okaziciela (do 2003 r. nazywanego świadectwem broni). Istotnie jest to materia ustawowa.

W nowym rozporządzeniu wprowadzono zamknięty katalog broni pozostających na wyposażeniu SUFO. Są to: broń palna bojowa i gazowa w postaci pistoletów i rewolwerów centralnego zapłonu (kal. od 6 do 12 mm), pistolety sygnałowe, pistolety maszynowe, strzelby gładkolufowe powtarzalne (kal. wagomiarowy 12), karabinki (kal. od 5,45 do 7,62 mm) i paralizatory elektryczne (o średniej wartości prądu w obwodzie

przekraczającej 10 mA). W uzasadnieniu projektu zapisano, że katalog ten pozostaje w spójności z ustawą o broni i amunicji, jak również z rozporządzeniem w sprawie szczególnie niebezpiecznych rodzajów broni i amunicji oraz rodzajów broni odpowiadającej celom, w których może być wydane pozwolenie na broń. Uzasadnienie jest zgodne z prawdą, ale jak słusznie zauważa Tomasz Żórawski, zgłaszając do PIO uwagi CSSO DELTA, omawiane rozporządzenie jest aktem wykonawczym do ustawy o ochronie osób i mienia, a nie wyżej wskazanej ustawy o broni i amunicji. Ustawa o ochronie zaś kwalifikuje w art. 38 ust. 2 pkt 6 broń gazową jako środek przymusu bezpośredniego. Dodatkowo zapisy art. 36 – 38 dotyczą tak ważnych kwestii jak podstawy prawne użycia broni palnej lub środków przymusu bezpośredniego, sfery uprawnień pracownika ochrony i obowiązków obywatelskich. Z tego względu przepisy w tym zakresie należy jak najszybciej ujednolicić.

W nowym rozporządzeniu bardziej szczegółowo uregulowano kwestie normatywów amunicji, włącznie z ustaleniem normatywu dla pistoletów sygnałowych (który nie był dotychczas określony) oraz strzelb gładkolufowych powtarzalnych. Określono też rodzaje nabojów do tej broni. Do strzelb gładkolufowych powtarzalnych przewidziano wyłącznie naboje z pociskiem kulowym o kalibrze 12/70 lub 12/76, co wynika z przeznaczenia broni gładkolufowej do konwojowania wartości pieniężnych oraz ochrony obiektów i magazynów wojskowych.

W rozporządzeniu wyraźnie określono zasady wydawania amunicji do zadań ochrony. Zasadą podstawową jest wydawanie połowy normatywu, natomiast pełny normatyw wydaje się do wykonywania ochrony konwojowanego mienia przez grupę interwencyjną (do której definicji powrócimy), w przypadku bezpośredniego zagrożenia napadem na chronione osoby, obszar, obiekt lub urządzenie . Pełny normatyw to: liczba amunicji wystarczająca do pełnego załadowania czterech magazynków pistoletu, pistoletu maszynowego albo karabinka; 24 sztuki amunicji do rewolweru lub strzelby gładkolufowej; 12 sztuk amunicji do pistoletu sygnałowego.

Dodano też określenie sposobu ładowania normatywu amunicji (do magazynków albo urządzeń je zastępujących lub ładownic), co stało się ważne np. dla określenia okoliczności odpowiedzialności firmy za szkodę. Warto na ten pozornie mało znaczący, techniczny przepis zwrócić uwagę w praktyce.

Odnośnie do przechowywania broni ustalono kilka nowych zasad. Magazyn broni odbiera protokolarnie nie organ policji, lecz upoważniony funkcjonariusz. Ustalono pełen zakres informacji przekazywanej do organu policji przez przedsiębiorcę, obligując go do powiadamiania o miejscu przechowywania poszczególnych egzemplarzy broni, jak i zmianie miejsca ich przechowywania (np. przeniesienia z magazynu w siedzibie do obiektu chronionego lub z jednego obiektu do innego). Został na to określony pięciodniowy termin, biegnący od zaistniałego zdarzenia. Każdy sposób przekazania pisemnego zawiadomienia jest przy tym dopuszczony (bezpośrednio, pocztą, faksem lub e-mailem z podpisem elektronicznym).

Poprzez odesłanie do konkretnych Polskich Norm zostały precyzyjniej określone wymogi dotyczące specjalnego zabezpieczenia magazynu broni i jego wyposażenia (w szafy stalowe i sejfy). Pod konkretnymi warunkami dopuszczono przechowywanie broni określonego rodzaju i w określonej liczbie egzemplarzy w innych pomieszczeniach. Warunkiem zasadniczym jest zabezpieczenie miejsca przechowywania za pomocą systemu sygnalizacji włamania i napadu z transmisją sygnału alarmu do uzbrojonego stanowiska interwencyjnego (USI), pełniącego całodobowy dyżur. W przypadku braku wyposażenia pomieszczenia w tę sygnalizację musi być ono objęte całodobową uzbrojoną ochroną. Pojęcie USI zostało wprowadzone w słowniczku tego aktu prawnego i oznacza co najmniej jednego uzbrojonego pracownika ochrony, który po uzyskaniu informacji z urządzeń lub systemów alarmowych sygnalizujących zagrożenie podejmuje decyzję co do rodzaju środków niezbędnych do jego usunięcia. Magazyny broni lub inne pomieszczenia, które zostały dopuszczone do przechowywania broni i amunicji na zasadzie uchylonego rozporządzenia z 1998 r., mogą być nadal wykorzystywane, nie dłużej jednak niż do końca listopada 2014 r. (przez 36 miesięcy od dnia wejścia w życie nowego aktu).

W obecnym rozporządzeniu odstąpiono od obowiązku potwierdzenia przez organ policji kopii dowodu zakupu broni i amunicji, ze względu na istniejący prawnie obowiązek okazania tego dokumentu przy rejestracji broni i powiadomienia policji przez sprzedającego.

Nie zmieniono wzorów książek stanu uzbrojenia i wydania-przyjęcia broni i amunicji. W trakcie opiniowania projektu odrzucona została propozycja Polskiej Izby Ochrony (PIO) o dopuszczeniu formy elektronicznej tych dwóch rodzajów ewidencji (co w końcu nie jest kwestionowane) w tzw. obrocie specjalnym. Dopuszczono zaś dokonywanie w książce stanu uzbrojenia zapisów uwzględniających podział broni według jej rodzajów. Nowe rozporządzenie zawiera wskazanie (którego nie było do tej pory) czasu przechowywania dokumentacji (książek stanu uzbrojenia i wydania-przyjęcia broni i amunicji) przez okres pięciu lat od dokonania ostatniego wpisu.

Powróćmy do intrygującej sprawy słowniczka w tym akcie prawnym. Słowniczek ten oprócz wskazanej definicji USI zawiera definicję przedsiębiorcy oraz grupy interwencyjnej.

Przedsiębiorcą jest podmiot, który uzyskał koncesję na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia (bez zmian) lub kierownik jednostki organizacyjnej, który powołał wewnętrzną służbę ochrony (WSO). Nie uwzględniono poglądu PIO, że objęcie definicją „przedsiębiorca" kierownika jednostki jest niezgodne z art. 2 pkt 8 ustawy o ochronie, motywując, iż definicja została określona jedynie na potrzeby przedmiotowej regulacji. Wskażmy, że w uchylonym rozporządzeniu definicja obejmowała nie kierowników, lecz przedsiębiorców i jednostki organizacyjne, które powołały WSO. W tym kontekście zachodzą wątpliwości, czy stwierdzenie w § 4, że „przedsiębiorca posiada broń na podstawie pozwolenia na broń na okaziciela", a w § 16, że „karty dokumentacji pieczętowane są pieczęcią przedsiębiorcy", przy wieloosobowych organach przedsiębiorców i jednostek organizacyjnych nie będą powodować niejasności co do tego, jakich pieczątek używać, np. zarządu czy imiennej członka zarządu wyznaczonego do kierowania WSO (przy czym osoby takie się zmieniają).

Poważniejszą jednak sprawą jest wprowadzenie w rozporządzeniu definicji *uzbrojonego stanowiska interwencyjnego* (USI) i *grupy interwencyjnej* (GI).

Ponieważ z tego względu cały akt jest narażony na krytykę, należy wskazać dlaczego. Otóż został on wydany na podstawie niekonstytucyjnej delegacji, niezmienionej od 1997 r. Przypomnijmy, że art. 92 Konstytucji RP wymaga, aby rozporządzenia były wydawane na podstawie szczegółowego upoważnienia w ustawie i w celu jej wykonania, a upoważnienie powinno określać zakres spraw przekazanych do uregulowania oraz wytyczne dotyczące treści aktu. Takich wymagań upoważnienie z 1997 r. nie spełnia. Właśnie z takiego powodu nie wydaje się nowego rozporządzenia o dokumentacji w firmach ochrony, uwzględniającego ich formę elektroniczną.

Zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „zasad techniki prawodawczej", tzw. słowniczek ma służyć objaśnieniu określeń i skrótów zastosowanych w rozporządzeniu. Należy zauważyć, że definicji GI użyto tylko wobec powtórzenia w przepisie zapisu o normatywach amunicji. Niestety w tenże okrężny sposób zostały wprowadzone – sposobem pozaustawowym, a więc niekonstytucyjnym – kosztowne obowiązki dla firm ochrony.

A zatem GI to co najmniej dwóch uzbrojonych pracowników ochrony, którzy po uzyskaniu za pośrednictwem USI informacji z urządzeń lub systemów alarmowych sygnalizujących zagrożenie chronionych osób lub mienia wspólnie realizują zadania ochrony osób lub mienia w formie bezpośredniej ochrony fizycznej doraźnej na terenie chronionego obszaru, obiektu lub urządzenia.

I tu ze strony firm ochrony posypały się pytania w rodzaju: czy mając status SUFO z tytułu ochrony tylko jednego obiektu i ochraniając sto innych zwykłych obiektów, muszę zwiększyć wszystkie patrole do dwuosobowych i czy wszystkie patrole muszą być uzbrojone? Czy „uzbrojenie" rozumie się według rozporządzenia, czy według ustawy o ochronie? (O sprzeczności była mowa wcześniej). Czy musimy zmienić stan patroli, ochraniając bez broni obiekty z listy wojewody (definicja nawiązuje przecież do określeń z art. 5 ustawy o ochronie)? Etc., etc.

Oczywiste jest, że wprowadzenie tej definicji, poza skutkami obligacyjnymi, powoduje skutki kosztowe po stronie przedsiębiorców z branży ochrony, o czym nie ma mowy w ocenach skutków regulacji rozporządzenia na etapie projektu. W mojej ocenie, zgodnie z zasadą *Ex iniuria non oritur ius* (prawo nie może powstać z tego, co jest sprzeczne z prawem), niedopuszczalna jest interpretacja, że definicja ta nałożyła na wszystkie firmy mające status SUFO (posiadające pozwolenie na broń na okaziciela) obowiązek dotyczący działania grup interwencyjnych według określenia jak wyżej. Definicja GI nie jest w żaden sposób powiązana z pojęciem ustawowym wykonywania ochrony osób i mienia, realizowanej w formie bezpośredniej ochrony fizycznej doraźnej (art. 3 pkt 1a ustawy o ochronie osób i mienia). Wychodząc od zasady racjonalności prawodawcy, trudno byłoby przyjąć, że racjonalne jest uzbrojenie patroli interwencyjnych (czy mają się od dziś wszystkie nazywać GI?) do ochrony szkół, miejsc publicznych itd. Argumentów zresztą jest wiele.

W tym kontekście można przyjąć, że:

– Obowiązek posiadania GI składającej się z co najmniej dwóch uzbrojonych pracowników ochrony, odnosi się tylko do przypadków ochrony wykonywanej na podstawie uzgodnionego z KWP planu ochrony, który przewiduje wykonywanie tych zadań z bronią. Chodziłoby więc o przypadki określone w art. 7 ust. 2 oraz art. 10 ust. 1 ustawy o ochronie osób i mienia. Poza tymi przypadkami, tam gdzie wykonawca przyjął na siebie obowiązek umowny, działania grup czy patroli interwencyjnych z bronią (np. jedna jednostka), może on, ale nie musi tworzyć GI według definicji rozporządzenia. Kwestię uzbrojenia musi zinterpretować organ policji;
– Wprowadzenie definicji nie łączy się automatycznie z funkcjonowaniem GI w ochronie obiektów z list wojewodów, skoro plan ochrony nie przewidywał uzbrojonej grupy interwencyjnej. Nie ma też w takim przypadku obowiązku tworzenia USI;
– Przy realizacji reszty umów – nie wykonywanych na zasadzie przewidzianego w planie ochrony działania uzbrojonej grupy lub grup interwencyjnych – status SUFO nie obliguje do zwiększania liczebności pracowników w pozostałych grupach patrolowych czy interwencyjnych i ich uzbrajania;
– Status SUFO wymaga stworzenia USI, jeżeli w firmie działa, na podstawie uzgodnionego planu ochrony, choćby tylko jedna GI, gdyż definicja przewiduje łączne działanie GI i USI („wspólnie realizują zadania ochrony").

Obecnie to najważniejsze wątpliwości co do stosowania „definicji" z rozporządzenia; z pewnością życie przyniesie kolejne.

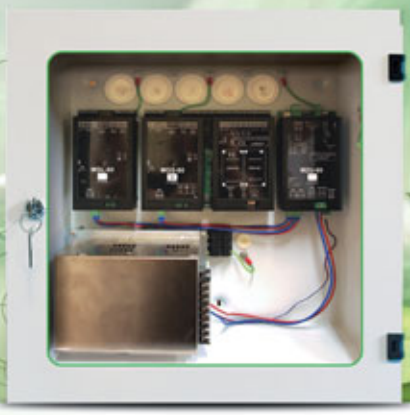
Jeśli chodzi o drugą część tytułu artykułu – lotniska dla SUFO – należy wskazać na wejście w życie, 19 lutego 2012 r., zmiany Ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia. Wynika ona z art. 3 Ustawy z dnia 30 czerwca 2011 r. o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw (Dz. U. 2011 nr 170 poz. 1015). Ustawa ta jest następczą wobec zmiany w samym prawie lotniczym, w jego art. 2 pkt 21. Dodano bowiem nową definicję służby ochrony lotniska, którą objęto wewnętrzne służby ochrony oraz Specjalistyczne Uzbrojone Formacje Ochronne, działające na podstawie ustawy o ochronie osób i mienia, realizujące zadania na rzecz ochrony lotnictwa cywilnego i podlegające zarządzającemu lotniskiem. Mamy tu zatem ustawowy warunek działalności gospodarczej przedsiębiorcy z branży ochrony ubiegającego się o zawarcie umowy na prowadzenie działalności w zakresie ochrony lotnictwa cywilnego w portach lotniczych – warunkiem tym jest posiadanie statusu SUFO. Inne szczegółowe warunki są zawarte w art. 22a ustawy o ochronie osób i mienia i nie ma potrzeby ich tu powtarzać. Można je określić jako warunki dotyczące dokumentacji składanej u zamawiającego oraz polisy ubezpieczenia. Prace nad rozporządzeniem Ministra Finansów w sprawie zakresu ubezpieczenia obowiązkowego, terminu jego powstania oraz minimalnej sumy gwarancyjnej są w końcowej fazie. Dodatkowo art. 22b zawiera warunek, aby przedsiębiorca prowadzący działalność gospodarczą w zakresie ochrony lotnictwa cywilnego w portach lotniczych wykonywał tę działalność samodzielnie – nie ma on zupełnie możliwości powierzania wykonywania czynności z zakresu takiej ochrony innym podmiotom.

*Jan Rybczyński*
*radca prawny*

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

# UCS 6000

## UNIWERSALNA CENTRALA STERUJĄCA



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

**WSPÓŁPRACA Z CENTRALAMI SYGNALIZACJI POŻAROWEJ WSZYSTKICH PRODUCENTÓW**

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

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

# Nowa centrala sygnalizacji pożarowej IGNIS 2040

Patryk Sawicki

W pierwszym kwartale 2012 roku na rynku pojawiła się nowa centrala sygnalizacji pożarowej IGNIS 2040. Urządzenie jest produkowane przez firmę Polon-Alfa, która od ponad 50 lat specjalizuje się w produkcji zaawansowanych systemów sygnalizacji pożarowej. Centrala IGNIS 2040 jest przeznaczona do zabezpieczania niedużych obiektów, gdy inwestorowi zależy na profesjonalnym i niedrogim systemie

*Fot. 1. Centrala IGNIS 2040*

## Przeznaczenie i budowa

Mikroprocesorowa centrala sygnalizacji pożarowej IGNIS 2040 (fot. 1) jest przeznaczona do wykrywania i sygnalizowania zagrożenia pożarowego po odebraniu informacji od dołączonych do niej czujek i ręcznych ostrzegaczy pożarowych. Na liniach dozorowych mogą pracować dobrze znane na rynku konwencjonalne czujki szeregu 40 (optyczne dymu, jonizacyjne dymu, ciepła, dwusensorowe: optyczne dymu i ciepła, ciepła i płomienia oraz czujki liniowe), a także ręczne ostrzegacze ROP-63 i ROP-63H.

Centrala IGNIS 2040 jest standardowo wyposażona w cztery linie dozorowe i dwie linie uniwersalne, fabrycznie skonfigurowane jako linie alarmowe przeznaczone do uruchomienia pożarowych urządzeń alarmowych. Jeżeli linie te nie są wykorzystane

jako alarmowe, można skonfigurować je tak, by działały jako linie dozorowe. W takim przypadku IGNIS 2040 pracuje z sześcioma liniami dozorowymi.

Nowoczesna konstrukcja, estetyczny wygląd, wygodny w użyciu panel operatora (rys. 1), który umożliwia pełną konfigurację i programowanie centrali, to tylko niektóre z charakterystycznych cech nowego produktu.

Duży alfanumeryczny wyświetlacz LCD (2×20 znaków), podświetlany, o barwie jasnozielonej, zapewnia instalatorowi komfort pracy w trakcie programowania centrali i odczytu sygnalizowanych zdarzeń.

Centrala IGNIS 2040 ma cztery poziomy dostępu, wybierane przy użyciu kodów, umożliwiających korzystanie z odpowiednich funkcji w zależności od wykonywanych czynności i przeszkolenia operatora.

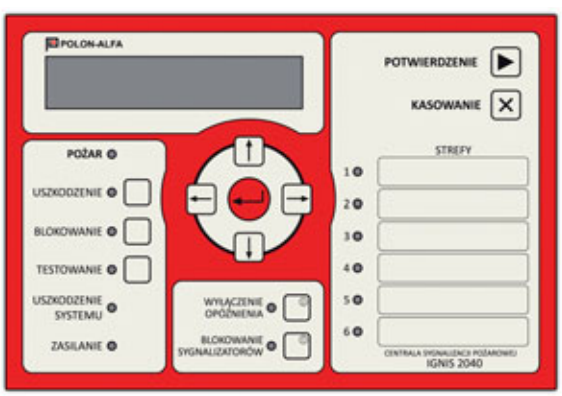
Ważnymi elementami każdej centrali systemu sygnalizacji pożarowej są przekaźniki wyjściowe. Oprócz przekaźników alarmu ogólnego i uszkodzenia w centrali IGNIS 2040 znajduje się sześć programowalnych przekaźników wyjściowych, które można zaprogramować w taki sposób, by możliwe były różne warianty ich działania. Ich główne zastosowanie to sterowanie dodatkowymi urządzeniami zabezpieczającymi uruchamianymi podczas alarmu pożarowego. Można je przypisać do różnych stref alarmowania, a także wybrać stopień alarmu mającego aktywować wybrany przekaźnik. Programowalne przekaźniki mogą pracować jako przekaźniki kasujące, co jest bardzo przydatną funkcją. Funkcja ta polega na przełączeniu styków wybranego przekaźnika na określony czas wyłącznie w momencie kasowania stanu alarmu w centrali. Takie działanie umożliwia powrót zewnętrznego urządzenia współpracującego z systemem sygnalizacji pożarowej do stanu dozorowania.

IGNIS 2040 ma także wyjście do zasilania urządzeń zewnętrznych (o wydajności 400 mA/24 V), uruchamianych np. z wyjść przekaźnikowych. Do komunikacji centrali z komputerem służy złącze USB. Umożliwia ono odczytanie pamięci zdarzeń przy użyciu odpowiedniego programu dostępnego na stronie internetowej firmy Polon-Alfa.

## Stany pracy centrali

Centrala IGNIS 2040 może sygnalizować różne stany pracy. Są to:

1) **Stan dozorowania.** W tym stanie centrala prowadzi dozór w obiekcie.
2) **Stan alarmowania.** W tym stanie następuje rozpoczęcie procedury sygnalizowania alarmu pożarowego zgodnie z przyjętym scenariuszem pożarowym. W zdecydowanej większości przypadków od personelu wymagane jest potwierdzenie „przyjęcia alarmu do wiadomości" i udanie się do obiektu w celu zweryfikowania rzeczywistego stopnia zagrożenia pożarowego. Centralę IGNIS 2040 wyposażono w algorytmy umożliwiające automatyczną weryfikację sygnału alarmowego odbieranego z ostrzegaczy. Istnieje możliwość zaprogramowania następujących wariantów alarmowania dla każdej z linii dozorowych:
   – alarmowanie jednostopniowe zwykłe,
   – alarmowanie dwustopniowe zwykłe,
   – alarmowanie jednostopniowe ze wstępnym kasowaniem,
   – alarmowanie jednostopniowe ze współzależnością (koincydencją) liniową,
3) **Stan uszkodzenia.** Jest on sygnalizowany wówczas, gdy układy kontrolne centrali wykryją awarię jednego lub kilku elementów systemu. Stan ten oznacza nieprawidłową pracę systemu i powinien zostać jak najszybciej zdiagnozowany doraźnie przez obsługę, a w najbliższym możliwym czasie przez przeszkolonego serwisanta.
4) **Stan blokowania.** Jest on sygnalizowany w przypadku blokowania linii dozorowych lub przekaźników. W stanie blokowania wybrane linie dozorowe oraz wybrane przekaźniki są wyłączone.
5) **Stan testowania.** Umożliwia on sprawdzenie elementów sygnalizacyjnych centrali oraz elementów pracujących na liniach dozorowych. W trakcie testowania poszczególnych elementów zgłaszany jest alarm testowy. Po zakończeniu testowania należy przełączyć centralę w stan dozorowania.




*Rys. 1. Panel operatorski centrali IGNIS 2040*


*Rys. 2. Podświetlany wyświetlacz LCD (2×20 znaków)*

## Podsumowanie

Nowy produkt jest bardzo ciekawą propozycją z grupy konwencjonalnych central sygnalizacji pożarowej. Wysoka jakość, przystępna cena, bogate wyposażenie i pięcioletnia gwarancja producenta to niewątpliwie atuty nowej centrali. Wyposażenie centrali w rozbudowane układy diagnostyki i samokontroli gwarantuje długotrwałą i niezawodną eksploatację. IGNIS 2040 jest przeznaczony do zabezpieczania małych obiektów, takich jak magazyny, sklepy, biura, wyniesione obiekty, tj. kontenery telekomunikacyjne, rozdzielnie elektryczne itp. Centrala ma niezbędne certyfikaty umożliwiające sprzedaż i stosowanie produktu w instalacjach ochrony przeciwpożarowej.

*Patryk Sawicki*
*POLON-ALFA*

# Nowa drukarka do kart identyfikacyjnych

**Drukarka Enduro+** dostępna jest w wersji jedno- i dwustronnej. Wersja drukarki do nadruków jednostronnych może zostać w dowolnym momencie zaktualizowana przez użytkownika do wersji dwustronnej. W razie potrzeby użytkownik może również w prosty sposób rozbudować swoją drukarkę o port komunikacyjny Ethernet. Enduro+ wyposażona jest w podajnik kart wykorzystywany przy wydrukach seryjnych. Posiada również funkcję ręcznego podawania kart wygodną podczas wydruków pojedynczych. Drukarka umożliwia wydruk na zwykłych kartach PVC, kartach magnetycznych, zbliżeniowych, stykowych oraz kartach wielokrotnego zadruku i kartach samoprzylepnych. Obsługiwane są dwa formaty kart: CR-79 oraz CR-80.

## Kluczowe cechy drukarki

- Jednostronny lub dwustronny nadruk od krawędzi do krawędzi
- Podajnik na 100 kart, odbiornik na 30 wydrukowanych kart
- Możliwość aktualizacji z drukarki jednostronnej do dwustronnej
- Możliwość ręcznego podawania kart
- Profil ICC (udoskonalane odwzorowanie kolorów)
- Kolorowy wyświetlacz LCD z przyciskami funkcyjnymi
- Możliwość drukowania na kartach do wielokrotnego zapisu
- Możliwość samodzielnej rozbudowy o port Ethernet

## Zabezpieczenia

- HoloKote w standardzie 4 znaki wodne
- Wydruk na kartach HoloPatch (złoty kwadrat na powierzchni karty)
- Koder pasków magnetycznych (opcja)
- Koder kart stykowych, zbliżeniowych: MIFARE, DESFire, IClass (opcja)

## Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 s
- Monochromatyczny wydruk karty w 7 s
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1., USB 2.0 z opcją Ethernet
- Możliwość rozbudowy do wersji dwustronnej
- Menu wyświetlacza w języku polskim
- Sterowniki w języku polskim: Windows 2000 Proffesional (SP4), XP, Vista i 7 (32/64 bity), Windows Server 2003 R@SP2, Server 2008 (32/64 bity)
- Rozdzielczość wydruku: 300 dpi
- Podajnik na 100 kart
- Odbiornik na 30 kart
- Możliwość ręcznego podawania kart
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 453×233×206 mm/ 5,5 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

## Taśmy

- Taśma kolorowana na 300 wydruków XXMA300YMCKO
- Taśmy monochromatyczne na 1000 wydruków: czarna, biała, niebieska, zielona, czerwona, srebrna, złota MA1000K

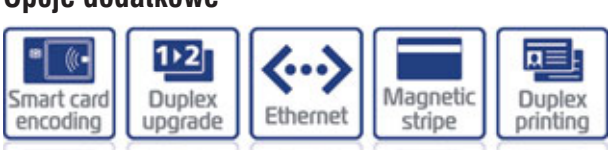
## Karty

Drukuje na wszystkich standardowych kartach PCV ISOCR-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, kartach do wielokrotnego zadruku TRW.

## Zestaw czyszczący

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

## Opcje dodatkowe




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
www.acss.com.pl, www.magicard.com.pl

# Profesjonalna drukarka do nadruku na kartach PVC o większej długości

Rio PRO Xtended

Ultra ELECTRONICS | MAGiCARD

**Magicard Rio Pro Xtended** pozwala drukować na standardowych kartach ISO oraz na kartach o takiej samej szerokości, ale większej długości. Daje to możliwość umieszczenia większej ilości informacji na powierzchni karty. Karta dzięki temu staje się bardziej czytelna. Obszar zadruku wynosi do 110×54 mm w pełnym kolorze, oraz 140×54 mm przy wydruku monochromatycznym. Drukarka obsługuje również karty predrukowane o długości do 140 mm. Wydruk zabezpieczany jest przeźroczystą warstwą Overlay, na której użytkownik ma możliwość wydruku spersonalizowanego znaku wodnego HoloKote lub HoloFlex.

## Specyfikacja

- Typy wydruków: wydruk kolorowy i monochromatyczny na kartach standardowych oraz na kartach o większym formacie
- Gwarancja: 3-letnia gwarancja Ultra CoverPlus obejmująca mechaniczne uszkodzenia głowicy oraz drukarkę zastępczą na czas naprawy
- Dostępne porty: USB i Ethernet w standardzie
- Sterowniki: Windows 2000 Professional (SP4), XP, Vista i 7 (32/64 bity), Windows Server 2003 R@SP2, Server 2008 (32/64 bity)
- Podajnik i odbiornik: Podajnik na 100 kart Xtended o wymiarach 86×140×54 mm, odbiornik na 70 kart Xtended o wymiarach 140×54 mm
- Masa: 4,95 kg
- Zasilanie: 100-240 V / 50-60 Hz
- Wymiary: 612×220×250 mm (wymiary obejmują podajnik i odbiornik)
- Prędkość nadruku: Wydruk karty w kolorze od krawędzi do krawędzi, 150 kart na godzinę
- Monochromatyczny nadruk karty 1000 kart na godzinę
- (Prędkość druku zależy od projektu graficznego karty)
- Temperatura pracy: od 10°C do 30°C

## Powierzchnie wydruków

- Jednorazowy wydruk kolorowy 86×54 mm/86×50 mm
- Podwójny wydruk kolorowy 110×54 mm/110×50 mm
- Monochromatyczny 140×54 mm/140×50 mm

## Zabezpieczenia kart

Możliwość wydruku znaku wodnego HoloKote. Do wyboru 4 standardowe znaki wodne, oraz znak wodny HoloFlex drukowany w dowolnym miejscu i dowolnym rozmiarze na powierzchni karty. Zarówno znak HoloKote i HoloFlex mogą być spersonalizowane w postaci dowolnego logo klienta.

## Taśmy

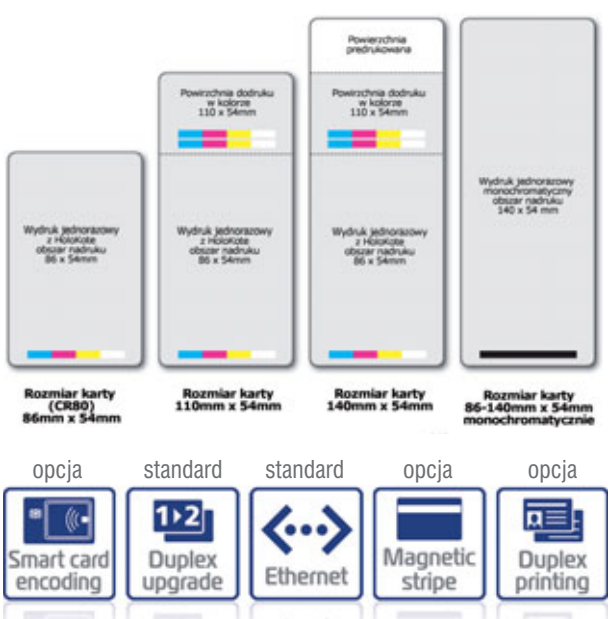
- YMCKO taśma kolorowana na 300 wydruków XXMA300YMCKO
- Taśmy monochromatyczne na 1000 wydruków: czarna, biała, niebieska, zielona, czerwona, srebrna, złota MA1000K

## Zestaw czyszczący

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

## Typy kart/grubości:

Wszystkie karty PVC ISO CR80/CR79, karty Xtended

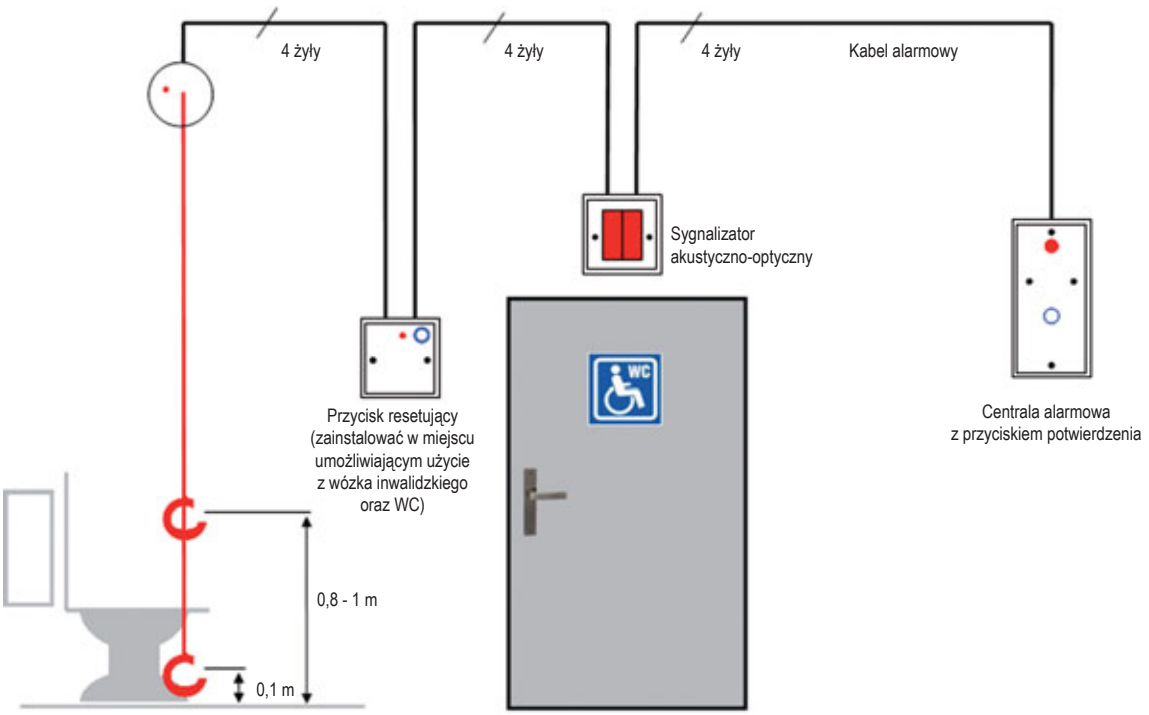



Dystrybucja:

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
www.acss.com.pl, www.magicard.com.pl

# Zestaw alarmowo-przywoławczy do toalet firmy Intercall




Przywoławczy zestaw do toalet jest prostym w instalacji i użytkowaniu oraz niezawodnym w działaniu systemem przywoławczym dla osób niepełnosprawnych. Przeznaczony do instalacji w toaletach i łazienkach umożliwia użytkownikom szybkie i proste wezwanie pomocy.

Zestaw zawiera wszystkie niezbędne urządzenia do zbudowania w pełni funkcjonalnego autonomicznego systemu przywoławczego. Dodatkowo do dyspozycji jest alarmowe wyjście przekaźnikowe NC umożliwiające integrację z innymi systemami. Centrala wyposażona jest w awaryjne zasilanie bateryjne zapewniające około 24 godziny pracy bez zasilania podstawowego. Istnieje możliwość rozbudowy zestawu o 2 dodatkowe przełączniki sufitowe.

Stan przywołania, aktywowany przy użyciu przełącznika sufitowego, sygnalizowany jest za pośrednictwem sygnalizatora akustyczno-optycznego przed wejściem do toalety oraz na panelu centralki alarmowej. Przywołanie może zostać skasowane za pomocą przycisku resetującego wewnątrz pomieszczenia. Zależnie od konfiguracji przywołania mogą być resetowane bądź potwierdzane za pomocą przycisku na centralce alarmowej. Jeżeli w czasie 120 sekund od potwierdzenia przywołania na centrali nie zostanie ono zresetowane za pomocą lokalnego przycisku resetującego wówczas centralka ponownie zasygnalizuje stan „alarm-przywołanie".

## Cechy

- Wbudowany moduł zasilacza
- Wyjście przekaźnikowe
- Załączona bateria awaryjna
- Sygnalizacja dźwiękowa oraz świetlna
- Funkcja potwierdzenia przywołania
- Załączanie/Wyłączanie przycisku Reset
- Funkcja *self-test*
- Zdejmowane kostki połączeniowe
- 2 uchwyty typu G

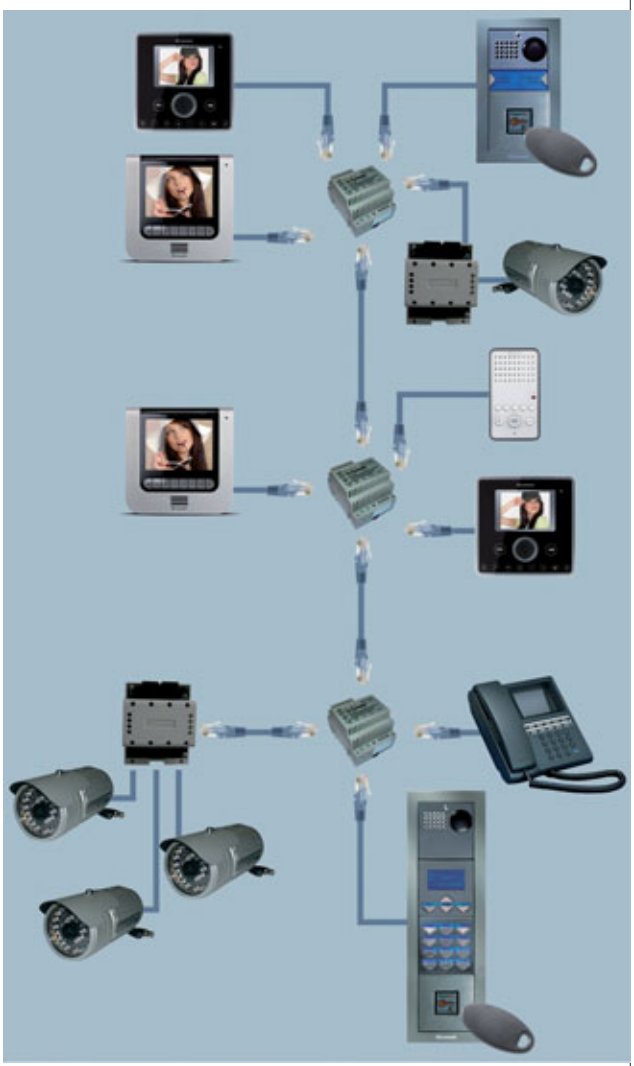
INTERCALL® SECURE SYSTEMS

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

# VIP – system wideodomofonowy IP
# Połączenie nieograniczonych możliwości z prostotą instalacji



System wideodomofonowy Comelit VIP jest funkcjonalny, elastyczny i niezawodny. Prosty w instalacji i uruchomieniu.

Wykorzystanie technologii IP w każdym fragmencie systemu zapewnia niespotykane dotąd możliwości w tego typu aplikacjach.

W praktyce technologia ta daje projektantom i instalatorom wielką elastyczność i swobodę podczas projektowania, instalacji i późniejszej rozbudowy systemu.

Użytkownicy otrzymują już nie tylko narzędzie służące do rozmowy z gościem i otwarcia mu drzwi, lecz nowoczesny system komunikacji audiowizualnej o dużej funkcjonalności, a w przyszłości również możliwości integracji z innymi aplikacjami za pośrednictwem sieci LAN (np. TVIP, VIOP, PC, czy SmartPhone).

## Wybrane funkcje i możliwości systemu VIP

- Technologia Plug & Play
- Brak limitu odległości pomiędzy urządzeniami
- Brak limitu liczby paneli głównych, lokalnych, central portierskich oraz monitorów wewnętrznych
- Wielka elastyczność. Brak narzuconej architektury połączeniowej. Każde urządzenie w systemie dołączane jest w ten sam sposób w dowolne miejsce na Switch'u
- Nieograniczona ilość równoległych rozmów. W systemie VIP całkowicie wyeliminowane zostało zjawisko zajętości
- Swobodne połączenia interkomowe. Możliwość komunikacji wewnętrznej pomiędzy wszystkimi użytkownikami systemu
- Proste programowanie. Podstawowe umiejętności obsługi komputera są wystarczające do uruchomienia systemu
- Możliwość zdalnej diagnostyki i obsługi systemu
- Wykorzystanie dedykowanej bądź istniejącej sieci LAN
- Monitory z pamięcią wideoklipów oraz możliwością nagrania komunikatu nieobecności
- Możliwość podglądu obrazu z kamer zewnętrznych oraz przekazania obrazu z kamer własnych do systemu CCTV
- Kontrola dostępu z czytnikami kart zbliżeniowych

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

# Wideodomofon jednoabonentowy CDV-35A/DRC-4FC


COMMAX SmartHome & Security

Zestaw wideodomofonowy składa się z monitora CDV-35A oraz kamery DRC-4FC.
Monitor COMMAX CDV-35A przeznaczony jest dla domów jedno- i wielorodzinnych oraz niewielkich bloków.
Posiada 3,5-calowy ekran wysokiej rozdzielczości w podświetleniem LED oraz sensoryczne przyciski służące do obsługi systemu. Monitor może współpracować z dwoma panelami zewnętrznymi (obsługa dwóch wejść) lub z jednym panelem i dodatkową kamerą CCTV (podgląd większego obszaru). Wewnątrz lokalu możliwa jest rozbudowa systemu o dodatkowe monitory z serii CDV-xxx oraz unifony DP-4VHP wraz z obsługą funkcji interkomu. Monitor współpracuje z każdą kamerą w systemie 4-żyłowym.
Najnowszym modelem kamery jednoabonentowej jest DRC-4FC. Kamera przystosowana jest do montażu w puszce podtynkowej. Posiada regulację położenia optyki oraz doświetlenie światłem białym. Metalowy panel w uniwersalnym, szarym kolorze pozwala dopasować się kolorystycznie do większości ogrodzeń.

## Dane techniczne

**Monitor CDV-35A**

- Monitor kolorowy
- Wyświetlacz 3,5" Color TFT-LCD z podświetleniem LED
- Przyciski sensoryczne (dotykowe)
- Standard sygnału wizyjnego PAL/NTSC
- Obsługa dwóch wejść
- Możliwość podłączenia dodatkowego monitora
- Współpraca z unifonami DP-4VHP
- Paging pomiędzy stacjami
- Instalacja czteroprzewodowa + obwód elektrozamka
- Współpracuje z kamerami analogowymi czteroprzewodowymi
- Zasilanie 230 V

**Kamera DRC-4FC**

- Kamera kolorowa
- Panel metalowy
- Montaż podtynkowy
- Kąt widzenia w pionie: 55 stopni, w poziomie: 68 stopni
- Standard sygnału wizyjnego PAL
- Pełna regulacja kąta widzenia (pion - poziom: 12 stopni)
- Doświetlenie diodami emitującymi światło białe
- Instalacja czteroprzewodowa plus obwód elektrozamka
- Współpracuje z monitorami czteroprzewodowymi
- Wymiary puszki podtynkowej 168/100/40 mm (wys./szer./gł.)
- Wymiary panela czołowego 183/124/18 mm (wys./szer./gł.)

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

# DRC-nAC2/nAB2 – rozszerzona linia wieloabonentowych, analogowych paneli wideodomofonowych


Wychodząc naprzeciw zapotrzebowaniu klientów firma COMMAX wzbogaciła ofertę o kilka produktów – między innymi o panele wieloprzyciskowe dla systemów analogowych. Panele umożliwiają podłączenie standardowych monitorów analogowych (dostępnych jest kilkanaście modeli), dzięki czemu każdy użytkownik ma możliwość indywidualnego dopasowania wyglądu i funkcji monitora do własnych potrzeb. Nowa linia obejmuje panele z kamerami czarno-białymi lub kolorowymi, przeznaczonymi do instalacji od 4-abonentowej aż do 16-abonentowej (dotychczas maksymalna liczba abonentów obsługiwanych przez jeden panel wynosiła 8). Możliwy jest montaż zarówno podtynkowy (wraz z zalecaną osłoną/daszkiem) jak i natynkowy (również w odpowiedniej osłonie). Prosty montaż oraz brak dodatkowych elementów systemu (bezpośrednia komunikacja kamery z monitorem) to dodatkowe oszczędności dla instalatorów i klientów końcowych.

## Dane techniczne

- Panel wideodomofonu 4/6/8/10/12/14/16 – przyciskowy z kamerą
- Panel metalowy
- Montaż podtynkowy
- Standard sygnału wizyjnego: PAL (kolor)/CCIR (b/w)
- Zasilanie 12 V (zasilacz RF-1A)
- Kąt widzenia w pionie: 55 stopni, w poziomie: 68 stopni
- Pełna regulacja ustawienia kąta widzenia (pion - poziom: 12 stopni)
- Współpracuje z monitorami analogowymi (czarno-białymi lub kolorowymi w standardzie PAL)
- Wymiary puszki podtynkowej (wys./szer./gł.) :
  - 209/115/50 (DRC-4AB2/6AB2, DRC-4AC2/6AC2)
  - 295/115/50 (DRC-8AB2/10AB2/12AB2/14AB2, DRC-8AC2/10AC2/12AC2/14AC2)
  - 383/109/50 (DRC-16AB2, DRC-16AC2)
- Wymiary panela natynkowego (wys./szer./gł.) :
  - 233/123/18 (DRC-4AB2/6AB2, DRC-4AC2/6AC2)
  - 315/123/18 (DRC-8AB2/10AB2/12AB2/14AB2, DRC-8AC2/10AC2/12AC2/14AC2)
  - 400/123/18 (DRC-16AB2, DRC-16AC2)

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

# PR621-CH
# Kontroler dostępu z kieszenią na kartę


Kontroler dostępu PR621-CH znajduje zastosowanie w systemach hotelowych oraz wszędzie tam, gdzie wymagane jest załączanie poszczególnych urządzeń, oświetlenia lub zasilania w pomieszczeniu za pomocą identyfikatora w postaci karty zbliżeniowej. Do załączania napięcia sieciowego 230 $V_{AC}$ wymagane jest zastosowanie standardowego zwiernego przekaźnika monostabilnego sterowanego napięciem 12 $V_{DC}$.

## Charakterystyka

- Możliwość załączania poszczególnych wyjść tak długo, jak karta obecna jest w kieszeni
- Załączanie wyjść przez dowolną kartę danego standardu lub kartę o określonym numerze seryjnym
- Ustawienie opóźnienia w zwalnianiu wyjścia czytnika po wyjęciu karty z kieszeni w zakresie od 3 s do 99 min.
- Pełna funkcjonalność standardowego kontrolera PR621, w tym m.in.:
  - wbudowany czytnik zbliżeniowy EM 125 kHz,
  - możliwość dołączenia dodatkowego czytnika zewnętrznego,
  - 2 programowalne wyjścia tranzystorowe 15 $V_{DC}$/1 A,
  - 1 programowalne wyjście przekaźnikowe 30 V/1.5 A,
  - 3 programowalne wejścia NO/NC,
  - komunikacja przez RS485,
  - programowanie manualne lub z poziomu komputera z programem PR Master,
  - zasilanie 12 $V_{DC}$.

Producent: roger®

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

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

# PR411DR-SET & PR402DR-SET
## Zestawy kontroli dostępu


Akumulator widoczny na zdjęciu nie wchodzi w skład zestawu

**PR411DR-SET** i **PR402DR-SET** są zestawami złożonymi z kontrolera dostępu PR411DR lub PR402DR oraz zasilacza sieciowego PS-10ACDR (18VA) osadzonych fabrycznie w obudowie metalowej mogącej pomieścić akumulator awaryjny 7Ah/12V. Obudowa metalowa jest wyposażona w łącznik ochrony antysabotażowej oraz posiada wizjer do podglądu wskaźników statusowych zainstalowanych w niej urządzeń. Zestaw jest dedykowany do realizacji kontroli dostępu pojedynczego przejścia z jedno- lub dwustronną identyfikacją. Uzupełnieniem zestawu mogą być czytniki serii PRT produkcji ROGER lub inne czytniki pracujące w jednym z popularnych standardów, takich jak Wiegand.

### Zalety stosowania zestawów w rozwiązaniach kontroli dostępu

- Atrakcyjna cena zestawu
- Kompletność rozwiązania – zestaw zawiera wszystkie (oprócz terminali) elementy potrzebne do realizacji punktu kontroli dostępu
- Możliwość instalacji na suficie
- Bezpośredni podgląd stanu pracy kontrolera dostępu dzięki wbudowanemu w obudowę wizjerowi
- Estetyczna metalowa obudowa
- Łatwa i szybka instalacja dzięki wyposażeniu w akcesoria montażowe

### Zawartość zestawu

- Kontroler dostępu PR411DR lub PR402DR
- Karta Master
- Komplet zworek do programowania adresu kontrolera
- Zasilacz transformatorowy PS-10ACDR
- Obudowa metalowa z wizjerem, łącznikiem antysabotażowym i szyną DIN 35mm
- Komplet wkrętów mocujących
- Opaski zaciskowe do zamocowania akumulatora
- Komplet przewodów do podłączenia akumulatora
- Instrukcje obsługi

Producent: roger®

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**ABUS SECURITY CENTER**
**ABUS KEMAZ POLSKA Sp. z o.o.**
ul. Wadowicka 8A
30-415 Kraków
tel. 12 640 15 60
faks 12 640 15 61
e-mail: tiglinski@abus-kemaz.pl
www.abus.pl

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

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

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

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

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

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

**ALPOL Sp. z o.o.**
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 16
faks 32 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

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

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

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

ul. Paulinów 10, 67-200 **Głogów**
tel. 32 750 30 78
faks 32 750 30 69
e-mail: glogow@e-alpol.com.pl

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

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

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

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

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

ul. Długa 19, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
faks 32 750 30 27
e-mail: ostrow@e-alpol.com.pl

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

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

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

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

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

ul. Polna 134/136, 87-100 **Toruń**
tel. 32 750 30 80
faks 32 750 30 73
e-mail: torun@e-alpol.com.pl

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

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

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

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

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

**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

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

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

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

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

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

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

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

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

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

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

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

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

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

**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

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

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

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

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

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

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

**PHU ELPROMA Sp. z o.o.**
**Biuro Handlowe:**
ul. Syta 177
02-987 Warszawa
tel. 22 312 06 00
faks 22 312 06 02
e-mail: elproma@elproma.pl
www.elproma.pl

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

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

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

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

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

**GEO-KAT Sp. z o.o.**
Al. Prymasa Tysiąclecia 145/149
01-424 Warszawa
tel. 22 877 08 80
faks 22 877 08 97
e-mail: info@geokat.com.pl
www.geokat.com.pl

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

**INSAP Sp. z o.o.**
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 98 44, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**SAMSUNG TECHWIN EUROPE LIMITED**
**Biuro w Polsce**
ul. Postępu 15c
02-676 Warszawa
tel. 22 20 50 777
faks 22 20 50 763
e-mail: STEsecurity@samsung.com
www.samsungsecurity.com

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

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

**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**
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. 32 291 86 17
faks 32 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl

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

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

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

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

**SCHNEIDER ELECTRIC POLSKA Sp. z o.o.**
ul. Rzymowskiego 53
02-697 Warszawa
tel. 22 313 24 10
faks 22 314 24 11
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.pl/buildings

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

ul. Muchoborska 18
54-424 **Wrocław**
tel. 71 711 09 19
faks 71 711 09 20

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

**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

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

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

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

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

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

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

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

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

**P.P.H.U. SUMA Sp. z o.o.**
ul. Panewnicka 109
40-761 Katowice
tel. 32 258 05 97
faks 32 258 05 98
e-mail: biuro@suma.com.pl
www.suma.com.pl

**Biuro Handlowe:**
ul. Makuszyńskiego 22a/23, 31-752 **Kraków**
tel. 12 684 00 23
e-mail: krakow@suma.com.pl

**TAP- Systemy Alarmowe Sp. z o.o.**
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: 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**
**Robert Prandota, Henryk Prandota, Krystyna Prandota Spółka Jawna**
ul. Słoneczna 4
40-135 Katowice
tel. 32 258 22 89
faks 32 357 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 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

**UNICARD S.A.**
ul. Wadowicka 12
30-415 Kraków
tel. 12 398 99 18
faks 12 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

**W2 Włodzimierz Wyrzykowski**
ul. Czajcza 6
86-005 Białe Błota
tel. 52 345 45 00
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

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

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

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

| Nazwa firmy | systemy sygnalizacji włamania i napadu | systemy telewizji dozorowej | systemy kontroli dostępu | systemy sygnalizacji pożarowej | systemy ochrony peryferyjnej | integracja systemów | monitoring | zabezpieczenia mechaniczne | systemy nagłośnień |
|---|---|---|---|---|---|---|---|---|---|
| **AAT Holding** | TAK | TAK | TAK | TAK | – | TAK | TAK | – | – |
| **ABUS** | TAK | TAK | TAK | TAK | – | TAK | TAK | TAK | – |
| **ACSS ID Systems** | drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe | | | | | | | | |
| **AGIS Fire & Security** | TAK | TAK | TAK | TAK | – | TAK | TAK | – | TAK |
| **Alarm System** | TAK | TAK | TAK | TAK | – | TAK | – | – | – |
| **Alarmnet** | – | TAK | TAK | – | – | TAK | – | – | – |
| **Alarmtech Polska** | TAK | – | – | – | – | – | – | – | – |
| **Alkam System** | TAK | TAK | TAK | TAK | – | TAK | – | – | TAK |
| **Alpol** | TAK | TAK | TAK | TAK | TAK | TAK | – | – | TAK |
| **Anma** | TAK | TAK | TAK | TAK | – | TAK | – | – | – |
| **ASSA ABLOY** | – | – | TAK | – | – | – | – | TAK | – |
| **FIRMA ATLine** | TAK | – | TAK | – | TAK | TAK | – | TAK | – |
| **BOSCH** | TAK | TAK | TAK | TAK | – | TAK | – | – | TAK |
| **P.W.H. Brabork-Laboratorium** | TAK | TAK | TAK | TAK | – | – | – | – | TAK |
| **bt electronics** | – | – | TAK | – | – | TAK | – | TAK | – |
| **CAMSAT** | – | TAK | – | – | – | – | TAK | – | – |
| **CBC Poland** | – | TAK | – | – | – | – | – | – | – |
| **CMA** | TAK | – | TAK | – | – | – | TAK | – | – |
| **D-MAX** | – | TAK | – | – | – | – | – | – | – |
| **D+H Polska** | – | – | – | TAK | – | TAK | – | – | TAK |
| **DG Elpro** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK |
| **Dyskam-Ekotrade** | TAK | TAK | – | TAK | – | – | TAK | – | – |
| **Dyskret** | TAK | TAK | TAK | TAK | – | TAK | – | TAK | TAK |
| **EBS** | Transmitery IP/GSM/GPRS, systemy RFID, zabezpieczenia energetyka, bankowość, produkcja OEM/ODM | | | | | | | | |
| **Ela-compil** | – | – | – | – | – | TAK | – | – | – |
| **El-Mont** | TAK | TAK | TAK | – | – | TAK | TAK | TAK | TAK |
| **Elproma** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | – | TAK |
| **Eureka** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | – | – |
| **Factor Polska** | TAK | TAK | TAK | TAK | TAK | – | – | TAK | TAK |
| **FES** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | – | TAK |
| **GDE Polska** | – | TAK | TAK | – | – | – | – | TAK | – |
| **GEO-KAT** | TAK | TAK | TAK | TAK | – | TAK | – | – | TAK |
| **ICS POLSKA** | TAK | TAK | TAK | TAK | TAK | – | – | – | – |
| **Insap** | TAK | TAK | TAK | TAK | – | TAK | TAK | – | TAK |
| **Janex International** | TAK | TAK | TAK | TAK | TAK | TAK | – | – | TAK |
| **KABE** | TAK | TAK | TAK | TAK | TAK | TAK | – | TAK | TAK |

| Nazwa firmy | systemy sygnalizacji włamania i napadu | systemy telewizji dozorowej | systemy kontroli dostępu | systemy sygnalizacji pożarowej | systemy ochrony peryferyjnej | integracja systemów | monitoring | zabezpieczenia mechaniczne | systemy nagłośnień |
|---|---|---|---|---|---|---|---|---|---|
| **KATON** | – | TAK | TAK | – | – | TAK | – | – | – |
| **Kolektor** | TAK | TAK | TAK | TAK | TAK | TAK | – | TAK | TAK |
| **Legrand Polska** | – | – | TAK | – | – | – | – | – | – |
| **MicroMade** | – | – | TAK | – | – | – | – | – | – |
| **Micronix** | TAK | TAK | TAK | – | – | – | – | TAK | – |
| **Novatel** | – | – | – | – | – | TAK | – | – | TAK |
| **Nuuxe – Radioton** | – | TAK | – | TAK | – | – | – | – | – |
| **OBIS** | TAK | TAK | TAK | TAK | – | – | – | – | TAK |
| **OMC INDUSTRIAL** | TAK | TAK | TAK | TAK | – | – | – | TAK | TAK |
| **Pointel** | TAK | TAK | TAK | TAK | TAK | TAK | – | – | TAK |
| **POL-ITAL** | – | – | – | – | – | – | – | TAK | – |
| **Polon-Alfa** | – | – | – | TAK | – | – | – | – | – |
| **ProfiCCTV** | TAK | TAK | TAK | TAK | – | TAK | – | – | – |
| **Pulsar** | TAK | TAK | TAK | – | – | – | – | TAK | – |
| **Ramar** | TAK | TAK | TAK | TAK | TAK | – | – | – | – |
| **RETT-POL** | TAK | TAK | TAK | TAK | – | – | – | – | – |
| **RISCO** | TAK | – | TAK | – | – | TAK | – | – | – |
| **ROPAM Elektronik** | TAK | TAK | TAK | – | – | TAK | TAK | – | – |
| **Samsung** | – | TAK | TAK | – | – | – | – | – | – |
| **Satel** | TAK | – | TAK | – | – | – | TAK | – | – |
| **Sawel** | TAK | TAK | TAK | TAK | TAK | TAK | – | – | – |
| **Schrack Seconet Polska** | – | – | – | TAK | – | – | – | – | – |
| **Secural** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK |
| **SMA** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK |
| **Schneider Electric Buildings Polska** | – | TAK | TAK | – | – | TAK | TAK | – | – |
| **Sprint** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK |
| **SPS Electronics** | TAK | TAK | TAK | TAK | – | – | TAK | – | – |
| **STRATUS** | TAK | TAK | TAK | TAK | TAK | TAK | – | – | – |
| **SUMA** | – | TAK | – | – | – | – | – | – | – |
| **Tap – Systemy Alarmowe** | TAK | – | TAK | – | – | – | – | – | – |
| **Tayama** | – | TAK | TAK | – | – | – | TAK | – | – |
| **Technokabel** | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK | TAK |
| **UNICARD** | TAK | TAK | TAK | TAK | – | TAK | – | TAK | – |
| **W2** | TAK | – | – | TAK | – | – | – | – | – |
| **Vision Polska** | – | – | – | TAK | – | TAK | – | – | – |
| **ZBAR** | TAK | TAK | TAK | TAK | TAK | TAK | – | TAK | TAK |

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

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

Skład i łamanie
Tomasz Kaczmarczyk

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

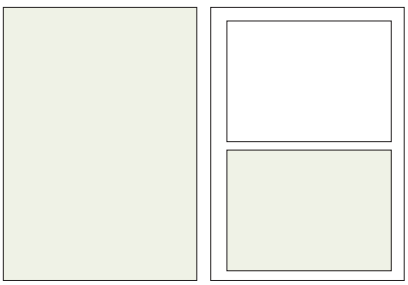
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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


# Cennik reklam

**Reklama wewnątrz czasopisma:**

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



cała strona (200 x 282 mm + 3mm spad)

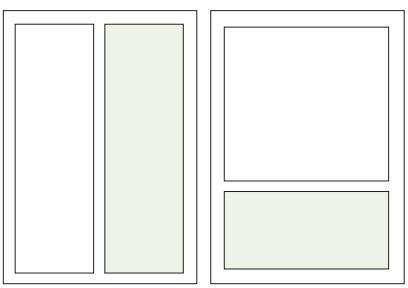
1/2 strony (170 x 125 mm)

**Artykuł sponsorowany:**

Cena za stronę artykułu sponsorowanego w czasopiśmie to 1500 zł (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

**Reklama na okładkach:**

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



1/2 strony (83 x 260 mm)

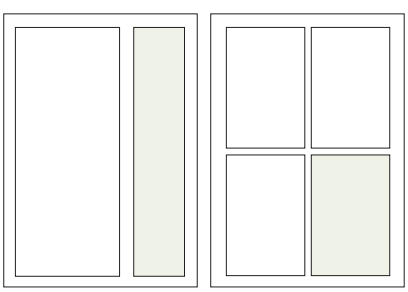
1/3 strony (170 x 80 mm)

**Spis teleadresowy:**

jednorazowy wpis 70 zł

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

**Podane ceny nie uwzględniają podatku VAT (23%)**



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

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

# Spis reklam

# ZOBACZ


# ZAPISZ

# POKAŻ

# ZŁAP

**iPOLiS**

Rozwiązania sieciowe firmy Samsung

| Obraz w rozdzielczości Full HD | Inteligentna Analiza Obrazu | Skalowalna rejestracja | Zdalny podgląd i sterowanie |
|---|---|---|---|
| FULL HD |  |  |  |

**Rozwiązania Samsung HD network security generują nawet pięciokrotnie więcej detali obrazu w porównaniu z systemem o standardowej rozdzielczości. Generowanie obrazu HD, rejestrowanie oraz wyświetlanie połączono w jednym systemie bezpieczeństwa, pozwalającym uzyskać niewiarygodnie wysoki poziom odwzorowania szczegółów obrazu.**

Kamery HD oraz monitory generują obrazy w formacie 16:9 i pozwalają operatorom określić z maksymalną dokładnością specyficzne obszary zainteresowania do bliższego zbadania – bez strat rozdzielczości i bez efektu „pikselacji" przy obserwacji. A dzięki zapisowi w rozdzielczości HD na materiale zarejestrowanym można wszystko zobaczyć z tą samą jakością.

Z pełnym zestawem kamer, wyborem opcji sprzętowych lub oprogramowania oraz monitorami HD, możesz stworzyć system bezpieczeństwa idealnie dopasowany do twoich potrzeb.

**Sieciowe rozwiązania bezpieczeństwa Samsung HD.**
**Inteligentniejsze bezpieczeństwo.**

E **STEsecurity@samsung.com**

**Samsung Techwin Europe Ltd**
Address: Postępu 15 C, 02-676 Warszawa
Tel: +48 222 050 777
Fax: +48 222 050 763

SAMSUNG

# Wykorzystaj nowe możliwości uwierzytelniania


**Model Secure Identity Object firmy HID:**

- **Zmienia każde urządzenie umożliwiające komunikację bliskiego zasięgu (NFC) w bezpieczne urządzenie uwierzytelniające**
- **Działa ze wszystkimi najpopularniejszymi kartami inteligentnymi**
- **Bezpieczne uaktualnienia ułatwiają migrację i zwiększają żywotność**

Przedstawiamy rozwiązanie iCLASS SE® z modelem danych Secure Identity Object (SIO).

Dowiedz się o SIO. hidglobal.com/sio lub zeskanuj kod przy użyciu czytnika QR

**Bezpieczne i działające niezależnie od technologii nowe rozwiązanie iCLASS SE® pozwala zamienić telefony i inne urządzenia inteligentne w kartę identyfikacyjną.**

HID®

Rozwiązanie iCLASS SE® umożliwia ochronę tożsamości przy użyciu wielowarstwowej, odpornej na złamanie technologii z bezpiecznym systemem zarządzania kluczem. Rozwiązanie to jest bardzo elastyczne — obsługuje technologie MIFARE®/DESFire®, EV1 oraz Indala, a także iCLASS®, umożliwiając przekształcenie każdego urządzenia obsługującego model danych SIO w bezpieczne urządzenie uwierzytelniające. Wybierz technologię i zaprogramuj nośnik uwierzytelnienia, aby już dziś stworzyć idealne rozwiązanie kontroli dostępu — następnie przeprogramuj czytnik, gdy zmienią się Twoje wymagania. Technologia iCLASS SE jest wszechstronna i elastyczna, została zaprojektowana z myślą o wysokiej wydajności. iCLASS SE to kontrola dostępu nowej generacji.

**Więcej informacji można znaleźć w witrynie hidglobal.com/unleash-zab**