

Czujka zewnętrzna OD850 technologia TriTech Niezawodna ochrona obwodowa



Prezentujemy jedną z najbardziej niezawodnych technologii wśród systemów antywłamaniowych.

- Detektory TriTech serii OD850 są przeznaczone do zastosowań zewnętrznych, w niesprzyjających warunkach fizycznych.
- Działanie czujek opiera się na kombinacji wykrywania za pomocą pasywnej podczerwieni (PIR) i promieniowania mikrofalowego (MV) z zaawansowanymi technologiami przetwarzania sygnałów.
- Dzięki skutecznej, zewnętrznej ochronie, intruz jest wykrywany na terenie, przed włamaniem do domu, co zapewnia dłuższy czas na interwencję.
- Liniowy pomiar przemieszczających się obiektów, które w konsekwencji nie zmieniają swojego położenia. Zapobiega to wywołaniu alarmu przez obiekty, które wprawdzie się poruszają, ale nie przemieszczają, takie jak gałęzie drzew czy wiszące szyldy.
- Możliwośćysterowania dodatkowego przełącznika, dzięki czemu może być włączane oświetlenie oraz sygnalizator akustyczny lub optyczny.
- Możliwość sprawdzenia działania czujki nawet przy silnym oświetleniu, dzięki diodzie LED o podwyższonej jasności.
- Obszar pokrycia 15x15m

Robert Bosch Sp. z o.o.
Security Systems
ul. Poleczki 3, 02 822 Warszawa
tel.: +48 22 715 41 00 / 01, fax: +48 22 715 41 05 / 06
securitysystems@pl.bosch.com www.boschsecurity.pl

 **BOSCH**
Technologia bliżej nas

W NUMERZE:

- Monitorowanie oprogramowania
- Matryce w kamerach telewizji dozorowej
- Obiektywy w systemach telewizji dozorowej. Dobór obiektywu – podstawowe pojęcia
- System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Cz. 1. Wprowadzenie



Zgodny z: PN-EN 60849

dźwiękowy system ostrzegawczy MCR-Venas



- Pełna zgodność z normą **PN-EN 60849** i certyfikat **CNBOP**
- **Dopuszczone certyfikatem: możliwość konfiguracji w systemie sieciowym oraz dowolność lokalizacji mikrofonów strażaka i komercyjnych poza pomieszczeniem centrum alarmowego**
- przyjazne oprogramowanie w języku polskim
- unikatowa funkcja nadawania komunikatów głosowych w przypadku awarii mikroprocesora
- jedyny system DSO z dowolnością wyboru metody nadzoru linii głośnikowych: impedancyjnej lub tonowej
- jedyny system DSO z wszechstronnym sterowaniem:
 - z pulpitów mikrofonowych
 - przez wejścia sterujące
 - za pomocą programatora z planowaniem dziennym, tygodniowym, miesięcznym i rocznym
- wyjątkowo szybkie i łatwe uruchamianie systemu przez każdego instalatora
 - nie wymaga specjalistycznego sprzętu

NOWOŚĆ

Ambient System Sp. z o.o., ul. Sucha 25, 80-531 Gdańsk, tel. +48 58 345 51 95, fax +48 58 344 45 95
marketing@ambientsystem.pl, www.ambientsystem.pl

SECUREX
ZAPRASZAMY
NA TARGI

Na targach Securex
gościmy na stoisku firmy Schrack Seconet
Hala 3, stoisko I 28.
Zapraszamy!!

WYDARZENIA INFORMACJE 4

MONITORING

Monitorowanie oprogramowania, *Krzysztof Białek* 16

SYSTEMY ZINTEGROWANE

RISCO Group prezentuje zintegrowany system bezpieczeństwa
ProSYS, RISCO Group 20

SSWIN

Inteligentne czujki serii Professional z wielopunktowym
antymaskingiem, *Krzysztof Kosteki, Bosch Security Systems* 30

Wielowiązkowe bariery podczerwieni REDNET,
Jarosław Gibas, Optex Security 36

TELEWIZJA DOZOROWA

Obiektywy w systemach telewizji dozorowej. Dobór obiektywu
– podstawowe pojęcia, *CBC (Poland)* 41

Najnowsze systemy bezprzewodowe do monitoringu wizyjnego
firmy P.W. Camsat, *Agnieszka Gralak, P.W. Camsat* 51

Nowe systemy kamerowe Pelco (cz. 2),
Norbert Góra, Pelco Europe 56

Matryce w kamerach telewizji dozorowej,
Marcin Gierszner, Alpol 60

Kamery obrotowe Novus – II generacja,
Patryk Gańko, Novus 65

OCHRONA INFORMACJI

System Zarządzania Bezpieczeństwem Informacji zgodny
z ISO/IEC 27001. Cz. 1. Wprowadzenie,
Andrzej Wójcik 68

Cyfrowa kasa pancerna,
Opracowano na podstawie literatury firmy TX Eastern Europe 77

KONTROLA DOSTĘPU

Wielkie możliwości dwóch przewodów. System domofonowy
i wideodomofonowy BTicino, *Legrand Polska* 78

Zabezpieczenia kart elektronicznych – nadruk UV – EDIsecure,
Janusz Sałaciński, EDP Support Polska 82

System inteligentnego domu HOASIS firmy BPT,
Andrzej Grodecki, Maciej Krzyczkowski 83

KARTY KATALOGOWE 87

SPIS TELEADRESOWY 100

CENNIK REKLAM 110

SPIS REKLAM 110



16

Monitorowanie
oprogramowania



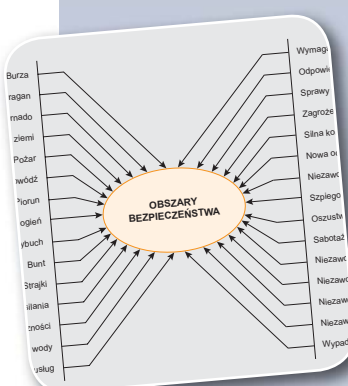
41

Obiektywy
w systemach
telewizji
dozorowej.
Dobór obiektywu
– podstawowe
pojęcia



60

Matryce
w kamerach
telewizji
dozorowej



68

System
Zarządzania
Bezpieczeństwem
Informacji
zgodny
z ISO/IEC 27001.
Cz. 1.
Wprowadzenie



MicroMade ma już 20 lat!

Firma MicroMade, polski producent urządzeń elektronicznych, obchodzi w tym roku dwudziestolecie swojej obecności na rynku. Została założona w 1988 roku przez dwóch braci, Piotra Gałka i Pawła Gałka, absolwentów Politechniki Gdańskiej (PG). Pierwszymi produktami były programatory i symulatory pamięci EPROM z serii Piccolo. W 1992 roku do spółki dołączył jeszcze jeden absolwent PG, Jerzy Drożdż, który w Pile zbudował dział handlowo-produkcyjny firmy. Wszystkie produkowane przez MicroMade urządzenia są opracowywane we własnym Biurze Konstrukcyjnym w Gdańsku.

Obecnie firma produkuje urządzenia elektroniczne z zakresu:

- kontroli dostępu i ewidencji czasu pracy (system bibi.net),
- kluczy USB do zabezpieczania oprogramowania i szyfrowania danych (HAK2),
- pomocy dydaktycznych (Dydaktyczny System Mikroprocesorowy DSM-51),
- czytników RFID.

Od samego początku działalności firma jest otwarta na wszelkie uwagi i spostrzeżenia docierające od użytkowników jej wyrobów. Pozwala to na dopracowanie produktów zgodnie z wymaganiami rynku.

Takie podejście jest jedną z podstaw rozwoju firmy MicroMade i zadowolenia jej klientów.



Bezpośr. inf. MicroMade



Firma NEXT! zaprasza na premierę platformy integracyjnej

Firma NEXT! przygotowała na targi Securex 2008 premierę najnowszej wersji programowej platformy integracyjnej dla agencji ochrony – **Kronos NET 2.0 „Revolution”**. Obok takich funkcji, jak monitoring budynków, pojazdów, środowiska, strażników, a także monitoring wizyjny oraz prawdopodobnie największego hitu tego sezonu – modułu służącego do monitoringu osób, program zapewnia też zarządzanie działem serwisu oraz wspiera automatyczne rozliczanie z klientami. Rewolucyjność produktu polega na połączeniu agencji ochrony użytkujących Kronos NET w ogólnopolską sieć zleciennodawców i podwykonawców usług ochrony. Dodatkowo program oferuje niespotykaną wśród produktów konkurencji wydajność, umożliwiającą obsługę nawet największych agencji ochrony. Szczegóły można znaleźć na stronie www.next.biz.pl.

Bezpośr. inf. NEXT!

Prezes Polalarmu zastępcą przewodniczącego Rady Normalizacyjnej drugiej kadencji



Informujemy, że prezes zarządu Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „Polalarm” **Bogdan Tatarowski** na pierwszym posiedzeniu Rady Normalizacyjnej II kadencji (2007–2011), w grupie przedstawicieli Ogólnopolskich Organizacji Zawodowych i Naukowo-Technicznych, został wybrany na zastępcę przewodniczącego Rady.

T. K.
Redakcja

Współpraca firm Bosch i G4Tec

poszerza gamę zastosowań w dziedzinie wizyjnych systemów dozorowych
Oprogramowanie do zarządzania obrazem Symmetry obsługuje produkty wizyjne firmy Bosch

Współpraca firm **Bosch Security Systems** i **G4Tec** zaowocowała możliwością bezproblemowej obsługi sieciowych produktów wizyjnych Bosch w systemie zarządzania obrazem Symmetry G4Tec. Firma Bosch wsparła rozwój poprzez swój zestaw SDK, ułatwiając uzyskanie wysokiej jakości obrazu o częstotliwości odświeżania maks. 25 obrazów/s przy rozdzielczości 4CIF w systemie zarządzania obrazem Symmetry.

Firma Bosch Security Systems jest światowym liderem w dziedzinie kamer i nadajników sieciowych. Kamery sieciowe Bosch bazują na uhonorowanych wieloma nagrodami kamerach Dinion, FlexiDome i modułowych kamerach AutoDome.

G4Tec, mieszcząca się w Wielkiej Brytanii, jest jedną z najbardziej liczących się firm zajmujących się projektowaniem, produkcją, instalacją oraz serwisowaniem w pełni zintegrowanych rozwiązań z zakresu zarządzania bezpieczeństwem. Produktem tej firmy jest system zarządzania obrazem Symmetry, zapewniający całkowitą integrację z wiodącymi sieciowymi oraz samodzielnymi cyfrowymi rejestratorami wizyjnymi, włącznie z cyfrowym rejestratorem wizyjnym Divar firmy Bosch.

Bezpośr. Inf. Bosch Security Systems

GANZ rozwija ofertę rejestratorów z serii DigiMaster



DR16NRT – rejestracja w czasie rzeczywistym

Nowy model DR16NRT oferuje jednoczesny podgląd obrazu na żywo oraz przeglądanie nagrań przy jednoczesnej rejestracji w czasie rzeczywistym 400 klatek/s. Rejestrator zapewnia możliwość rejestracji w rozdzielczościach CIF/2CIF/4CIF. Zastosowana wersja kompresji MPEG4 zapewnia oszczędne wykorzystanie pojemności dysków przy jednoczesnym zachowaniu wysokiej jakości obrazu. Nagrania można kopiować i archiwizować zarówno na wydzielonych dyskach wewnętrznych, jak i na dołączanych dyskach i nośnikach zewnętrznych. Maksymalna pojemność czterech wewnętrznych dysków wynosi aż 2 TB, co zapewnia długi czas rejestracji.

Zaawansowana funkcjonalność

Nowy model charakteryzuje się pełną funkcjonalnością, która sprawia, że stanowi on profesjonalne rozwiązanie przystosowane do pracy zarówno w średnich, jak i rozbudowanych systemach wymagających wysokiej wydajności i szybkości pracy zastosowanych rozwiązań.

Funkcją wartą wyróżnienia jest zaawansowane narzędzie wyszukiwania nagrań. Zastosowana funkcja *Smart Search* umożliwia przeszukiwanie nagrań według zmian w wybranej części obserwowanej sceny (np. drzwi). Rozwiązanie to zwiększa efektywność wyszukiwania zmian w istotnym dla systemu obszarze obrazu. Ponadto funkcja inteligentnego wyszukiwania charakteryzuje się odtwarzaniem w dwóch różnych trybach panoramy. Jeden z tych trybów umożliwia odtwarzanie wybranego kanału z jednoczesnym wyświetlaniem 36 kolejnych klatek zarejestrowanych na dysku. Daje to możliwość śledzenia zmian oraz szybkiego wyszukiwania ujęć interesujących operatora. Dodatkowo drugi tryb panoramy umożliwia znaczne skrócenie czasu wyszukiwania poprzez jednoczesne odtwarzanie nagrań z jednej kamery w ośmiu oknach z przesunięciem czasowym odtwarzanego materiału o dowolny interwał (np. 0,5 godz., 1 godz., 3 godz.). Jednocześnie w dziewiątym oknie wyświetlany jest obraz na żywo z tej samej kamery.

Rejestratory DR16NRT można łączyć w grupy, tworząc zintegrowany system sieciowy wykorzystujący sieć



Ethernet. Wszystkie modele obsługują większość dostępnych na rynku kamer szybkoobrotowych dzięki zintegrowanemu interfejsowi RS485 oraz zaimplementowanym w systemie protokołom PTZ większości producentów.

Funkcja znaku wodnego zabezpiecza nagrania w momencie eksportowania danych, co zapewnia możliwość wykorzystania ich jako dowodów w przypadku postępowania sądowego. Dodatkowo funkcja ta skutecznie zabezpiecza pliki kopii rezerwowej przed próbami sfalszowania, retuszowania itp.

Rejestratory są wyposażone w cztery kanały audio, umożliwiające rejestrowanie dźwięków z niezależnych źródeł.

Intuicyjna obsługa i zarządzanie

Tak jak cała gama DigiMaster, również model DR16NRT charakteryzuje się niezwykłą łatwością oraz intuicyjnością obsługi i zarządzania. Do każdego rejestratora dodawane jest oprogramowanie klienckie, umożliwiające pełne zarządzanie systemem. DigiMasterem można sterować za pomocą przeglądarki internetowej, myszy, klawiatury USB, panelu przedniego lub też zdalnie, za pomocą pilota IR.

Ekonomiczność przy uwzględnieniu inteligentnej funkcjonalności i wydajności modelu DR16NRT sprawia, że charakteryzuje się on niezwykłą użytecznością. Stanowi korzystne i bezpieczne rozwiązanie, które można zastosować w wielu systemach telewizji dozorowej, np. w obiektach publicznych, na stadionach, w obiektach, w których odbywają się imprezy masowe itp.

Więcej informacji znajduje się na www.cbcpoland.pl. Po dodatkowe informacje zapraszamy również na stoisko nr 89 w pawilonie 3A podczas targów Securex w Poznaniu (22–25.04.2008).

Bezpośr. inf. CBC Poland





RISCO Group w Polsce

26 lutego 2008 roku nastąpiło otwarcie
biura firmy RISCO Group w Warszawie

– integracja w branży security?



Jest to pierwsze biuro firmy w Polsce. Mimo to RISCO Group od wielu lat znana jest na polskim rynku w postaci sprzedawanych produktów, głównie marki Rokonet. Produkty firmy RISCO Group charakteryzują się niezawodną technologią i nowoczesnym designem. Firma koncentruje się na tworzeniu zintegrowanych rozwiązań z zakresu systemów bezpieczeństwa, nie zapominając o potrzebach klienta korporacyjnego i indywidualnego. Wszystkie te starania przyniosły w minionym roku firmie RISCO Group zyski ze sprzedaży w Polsce w wysokości 1,1 miliona euro.

RISCO Group, z siedzibą główną w Izraelu, jest obecna na całym świecie poprzez swoje liczne biura regionalne w Europie, obu Amerykach, a także w Chinach. Country Managerem RISCO Group w Polsce został mianowany **Kazimierz Kacprzyk**, postać zasłużona i znana w branży *security* (poprzednio w GE). Na spotkaniu przedstawił filozofię działania firmy, która zasadza się na:

- dostarczaniu pomocy technicznej i marketingowej dotychczasowym partnerom,
- przygotowywaniu i dostarczaniu szkoleń technicznych dystrybutorom, instalatorom i użytkownikom końcowym,
- prezentowaniu i wdrażaniu nowych rozwiązań,
- poszukiwaniu nowych dróg rozwoju firmy w Polsce.

RISCO Group odnosi spektakularne sukcesy na całym świecie. W zeszłym roku firma otrzymała w Londynie „Oskara *security*” – została uznana za producenta roku w tej branży w konkursie 2007 Security Excellence Awards. Także w zeszłym roku bezprzewodowy system bezpieczeństwa Wisdom produkowany przez RISCO Group został uznany w USA przez *Consumer's Digest Ma-*

gazine za „Best Buy”, czyli najlepszy zakup spośród tysięcy innych ocenianych produktów.

Firma kładzie duży nacisk również na opracowywanie skalowalnych i łatwych w rozbudowie central systemów bezpieczeństwa oraz ciągły rozwój technologii bezprzewodowych.

Wśród produktów oferowanych przez RISCO Group wyróżnia się SynopSYS. Jest to zintegrowany system bezpieczeństwa i automatyki budynku, służący do zarządzania rozległymi systemami – zarówno lokalnymi, jak i zdalnymi – poprzez sieci LAN/WAN. Dzięki swej otwartej architekturze umożliwia integrację nie tylko rozwiązań RISCO Group w zakresie systemów sygnalizacji włamania i napadu czy kontroli dostępu, znanych już w naszym kraju, ale i systemów innych producentów – także z zakresu telewizji dozorowej, systemów sygnalizacji pożaru, klimatyzacji, wentylacji i innych instalacji, spotykanych w nowoczesnych, inteligentnych budynkach. Mimo wykorzystywania otwartych standardów komunikacyjnych SynopSYS zapewnia najwyższy możliwy poziom bezpieczeństwa dzięki stosowaniu nowoczesnych technologii szyfrowania.

Wszystkie oferowane na rynku polskim produkty posiadają certyfikaty kwalifikacyjne wydawane przez Techom.

Osobistym marzeniem Kazimierza Kacprzyka jest zintegrowanie środowiska branży *security*. Wyrazem tych dążeń było uczestniczenie w spotkaniu instalatorów, dystrybutorów i reprezentantów ważnych klientów oraz organizacji działających w środowisku *security* w Polsce.

Bezpośr. inf. RISCO Group



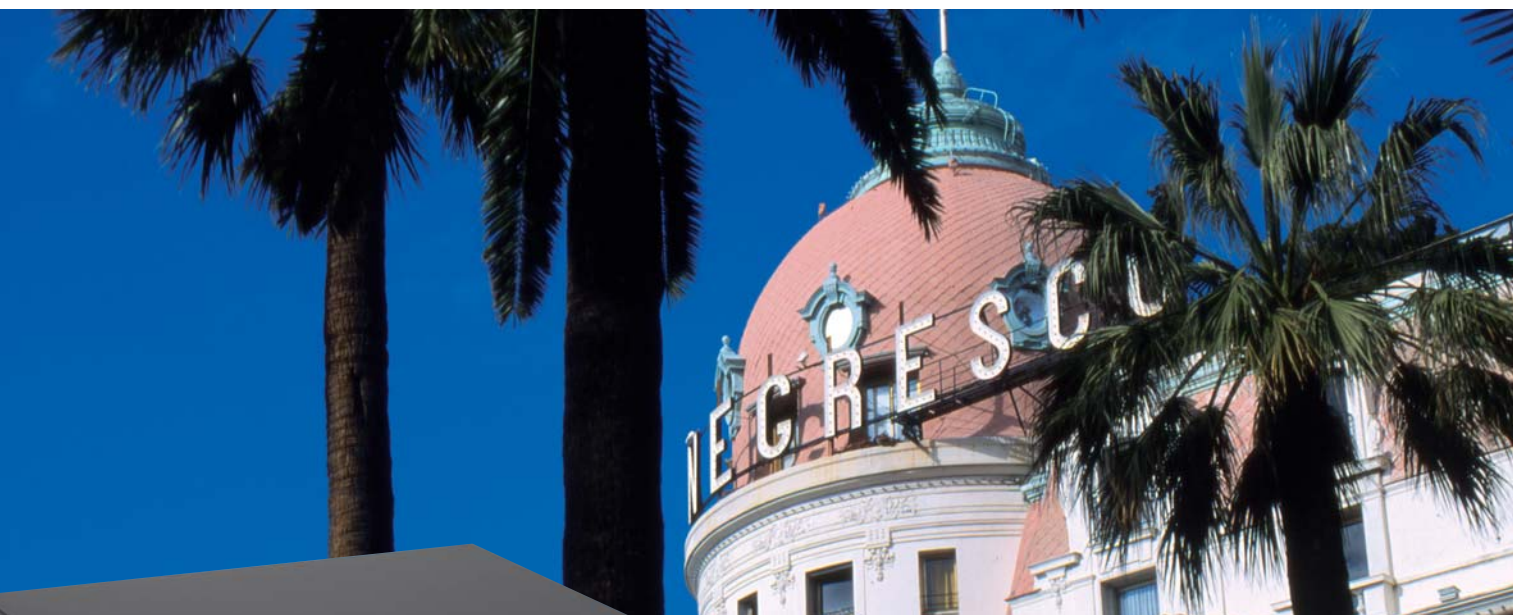
Cyfrowy rejestrator wizyjny Bosch nowej generacji

Dzięki nowemu cyfrowemu rejestratorowi wizyjnemu Divar firmy Bosch profesjonalna wydajność **cyfrowego zapisu DVR** jest już dostępna dla wszystkich. Łatwa obsługa w połączeniu z olbrzymią funkcjonalnością urządzenia powodują, że stanowi ono wygodne rozwiązanie do zarządzania materiałami wideo, które oprócz wysokiej jakości zapisu oferuje elastyczny system umożliwiający obsługę alarmów, sterowanie kamerą i sprawdzanie urządzeń.

Cyfrowy rejestrator wizyjny **Divar MR** oferuje zapis w czasie rzeczywistym i odtwarzanie w rozdzielczości CIF, jak również wysoką rozdzielczość transmisji oglądanych na żywo. Gdy potrzebna jest jeszcze większa dokładność, skorzystać można z rozdzielczości 4CIF. Doskonała jakość obrazu jest uzupełniona wysokowydajną kompresją obrazu MPEG4, dzięki czemu zmniejsza się zapotrzebowanie na pamięć, a więc również

Divar MR Control Center, które umożliwia pełne zdalne zarządzanie systemem, obejmujące oglądanie na żywo i sterowanie, odtwarzanie, konfigurację i zdalne powiadamianie o alarmach. Dzięki Divar MR Control Center wszystkie czynności związane z obsługą i sterowaniem można scentralizować, uzyskując rozwiązanie do zarządzania materiałami wideo o dużym współczynniku skalowalności. Dla jeszcze większej wygody do oglądania obrazów na żywo użytkownicy mogą używać przeglądarki Internet Explorer.

Do całej gamy przydatnych funkcji należą natychmiastowe odtwarzanie, zapis po naciśnięciu jednego przycisku, powiadomienie e-mailem po wystąpieniu zdarzenia, czy też ochrona przed skasowaniem, dzięki której ważne nagrania można zabezpieczyć. Wcześniejsze i aktualne zdarzenia można łatwo ze sobą porównywać, oglądając równocześnie zdjęcia na żywo



koszty przechowywania materiałów wideo. Materiały te można archiwizować m.in. na karcie pamięci USB czy opcjonalnej nagrywarce DVD. Odtwarzacz archiwum pozwala na odtwarzanie wyeksportowanych materiałów wideo na dowolnym komputerze klasy PC bez konieczności instalowania dodatkowego oprogramowania. Funkcja uwierzytelnienia obrazu oznacza, że zarchiwizowane materiały wideo mogą posłużyć jako dowód w postępowaniach sądowych.

Czy to jako część zintegrowanego systemu, czy też oddzielne urządzenie, Divar MR oferuje bezproblemową instalację, obsługę i zarządzanie. Wśród wielu metod sterowania i personalizacji wymienić tu można klawiaturę Bosch IntuiKey, mysz, pilota zdalnego sterowania na podczerwień oraz elementy regulacyjno-sterujące znajdujące się na przednim panelu urządzenia, w tym wygodne pokrętko. Oprócz tego w komplecie z urządzeniem dostarczane jest oprogramowanie

i z playbacku. Przeszukiwanie zapisanych materiałów wideo ułatwia natomiast funkcja *Smart Search*, która automatycznie szuka zmian w wybranej części sceny.

W porównaniu z tradycyjnymi urządzeniami zintegrowana budowa Divar MR oferuje wyższy poziom bezpieczeństwa w przypadku ataków z sieci i nie wymaga tylu czynności serwisowych. Divar MR zapewnia bezpieczeństwo nagrań, eliminując zamieszanie związane z instalowaniem łat programów i oprogramowania antywirusowego.

Zintegrowana architektura Divar MR jest prosta do skonfigurowania i obsługi. Zainstalowane interfejsy do podłączania różnych urządzeń zewnętrznych obsługują kamery PTZ zarówno firmy Bosch, jak i innych producentów.

Rodzina Bosch Divar MR obejmuje modele 8- i 16-kanalowe z możliwością podłączenia różnych dysków twardej, a gdy zajdzie taka potrzeba – wewnętrznej nagrywarki DVD. Niedrogie, a mimo to wyposażone w wygodne i bardzo przydatne funkcje urządzenie Divar MR stanowi wydajne rozwiązanie do zarządzania materiałami DVR w szkołach, hotelach, budynkach mieszkalnych, placówkach handlu detalicznego i w przypadku wielu innych zastosowań.

Bezpośr. inf. Bosch Security Systems

Nowy system Video Recording Manager firmy Bosch

Rozproszone systemy zapisu zwiększając niezawodność i wydajność sieci CCTV

System Video Recording Manager (VRM) firmy Bosch Security Systems zapewnia scentralizowane zarządzanie i monitorowanie serwerów wizyjnych, kamer i urządzeń zapisujących iSCSI połączonych w sieć CCTV.

System Bosch VRM 1.0 znacząco ulepsza zarządzanie przestrzenią zapisu, przypisując blokom zapisywanego materiału w systemie poziom logiczny lub wirtualny zamiast poziomu fizycznego. Wirtualizacja bloków zapisu zapewnia pełną elastyczność i skalowalność alokacji zapisu w obszarze sieci. Zapisywany obraz jest

jest np. przekierowanie zapisu z kamery i przydzielenie np. 10% przeznaczonej dla niej przestrzeni zapisu kamerze o większym zapotrzebowaniu na przestrzeń zapisu, która przesyła obraz z większą częstotliwością odświeżania.

Aby ułatwić szybkie wyszukiwanie, system VRM udostępnia bazę danych wyszukiwania nagrań i metadanych. Metadane (zdarzenia, dane z bankomatu, kasy fiskalnej lub inne dane tekstowe, dane wizyjnej detekcji ruchu) są zapisywane wraz z materiałem wizyjnym. Baza danych zawiera również informacje o lokalizacji bloków zapisu. Jeśli baza danych zostanie utracona, np. na skutek zniekształcenia danych, system VRM jest w stanie odtworzyć wszystkie informacje, odczytując jedynie zapisane metadane.

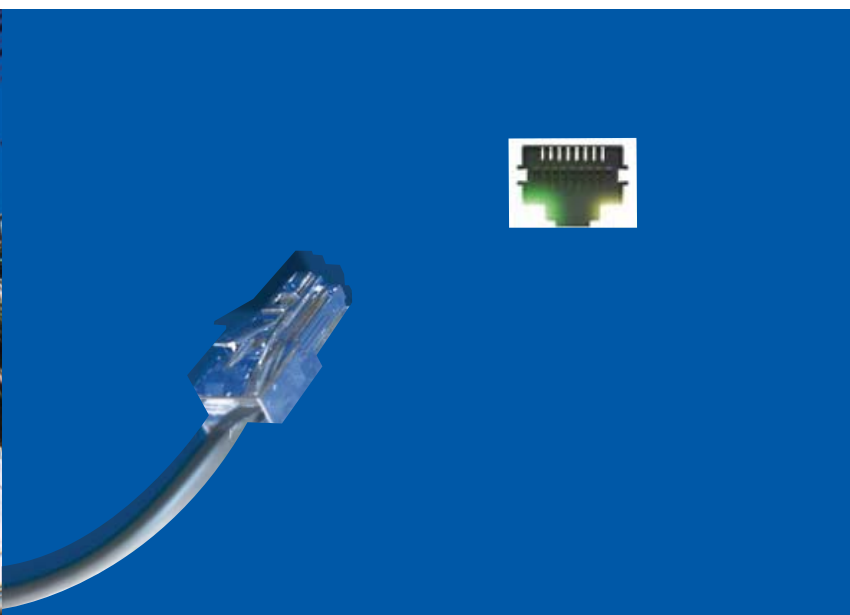
Pod kontrolą systemu VRM nadajniki mogą bezpośrednio zapisywać dane w urządzeniach iSCSI w blokach po 1 GB bez kierowania zapisu przez serwer oraz bez potrzeby istnienia systemu plików (oba te czynniki są potencjalnymi powodami awarii). Oprócz tego, dzięki wykorzystaniu bezpośredniego adresowania bloków, stare informacje są wprost nadpisywane nowymi i nie ma konieczności wcześniejszego kasowania niepotrzebnego już zapisu. Znakomicie poprawia to wydajność systemu w przypadku zapisu z bardzo wysoką częstotliwością odświeżania, umożliwiając macierzom dyskowym Bosch iSCSI osiągnięcie przepustowości 200 Mb/s, daleko przekraczającej granicę 70 Mb/s dostępną w dotychczasowych sieciowych rejestratorach wizyjnych (NVR).

Aby jeszcze bardziej rozszerzyć integralność systemu, oprogramowanie VRM 1.0 może być zsynchronizowane z drugim pracującym w tle oprogramowaniem VRM na innym serwerze w celu zapewnienia rezerwy na wypadek awarii pierwszego serwera. Jeśli nawet awarii ulegnie rezerwowy serwer VRM, każda macierz RAID iSCSI może kontynuować zapis w przestrzeni dyskowej 128 GB, co zapewnia rejestrację obrazów z jednej kamery przez 10 dni (przy założeniu przesyłania przez każdą kamerę strumienia 1 Mb/s).

System VRM 1.0 został wprowadzony do oferty w czwartym kwartale 2007 r., początkowo jako samodzielny produkt mający zastąpić system Bosch VIDOS-NVR. W pierwszym kwartale 2008 r. będzie dostępna wersja całkowicie zintegrowana z platformą programową Bosch VMS.

dystrybuowany pomiędzy wszystkie dostępne macierze RAID iSCSI w sieci, nie jest zaś zapisywany na pojedynczym urządzeniu zapisującym dołączonym do sieciowego rejestratora wizyjnego (NVR). System zapewnia również większą dostępność danych z możliwością automatycznego przekierowania zapisywanego obrazu na alternatywne urządzenia iSCSI w przypadku awarii macierzy dyskowej. Co więcej, urządzenia zapisujące RAID iSCSI mogą być umieszczone w dowolnym miejscu. Mogą być np. ustawione kaskadowo w zabezpieczonym, centralnym obiekcie mieszczącym systemy informatyczne, podobnie jak konwencjonalne sieciowe rejestratory wizyjne; jako rozproszone sieciowe urządzenia zapisujące mogą być umieszczone w zabezpieczonych szafach, gdzie są mniej narażone na pojedynczy akt sabotażu; mogą też być bezpośrednio dołączonym nośnikiem zapisu sprzężonym z nadajnikiem/odbiornikiem wizyjnym firmy Bosch.

System VRM 1.0 optymalizuje również wykorzystanie zasobów systemowych, monitorując użycie przestrzeni zapisu przez kamerę i dynamicznie przydzielając przestrzeń zapisu na podstawie zapotrzebowania. Możliwe



Bezpieczeństwo transakcji elektronicznych – relacja z konferencji

Druga już konferencja pt. „Bezpieczeństwo transakcji elektronicznych” o podtytule „**Biometria i przestępstwa przy użyciu kart płatniczych**” odbyła się w dniach 25 i 26 lutego w Centrum Konferencyjno-Szkoleniowym „BOSS” w Warszawie-Miedzeszynie. Ta prestiżowa impreza została zorganizowana przez Związek Banków Polskich – Forum Technologii Bankowych oraz firmę Software-Konferencje specjalnie dla przedstawicieli banków i firm zajmujących się technologią informacyjną. Sponsorami konferencji były firmy Hitachi, Wasko, Deep Blue Biometrics, Auto ID oraz INSI (Instytut Innowacji i Społeczeństwa Informacyjnego – centrum badawczo-rozwojowe Grupy ABG SPIN). Cztery pierwsze z wyżej wymienionych firm zaprezentowały swoje oferty na stoiskach zaaranżowanych obok sali konferencyjnej.

Otwarcia konferencji dokonał Krzysztof Pietraszkiewicz – prezes Związku Banków Polskich, po wprowadzeniu Remigiusza Kaszubskiego z tej samej organizacji, wielokrotnie jeszcze zabierającego głos podczas konferencji. Prelegentami byli polscy i zagraniczni eksperci w dziedzinie nowoczesnych technologii bankowych. Na zakończenie pierwszego dnia konferencji jej uczestnicy mieli możliwość wzięcia udziału w uroczystej kolacji, która stała się okazją do wymiany poglądów i doświadczeń oraz bliższego wzajemnego poznania się bankowców z kraju i z zagranicy. Pierwszy dzień konferencji był poświęcony biometrii (tej tematyce będzie poświęcona niniejsza relacja), a drugi – przestępstwom dokonywanym przy użyciu kart płatniczych, czyli skimmingowi.

David Byrch z brytyjskiej firmy konsultingowej Consult Hyperion omówił rolę rozwiązań biometrycznych i kart chipowych oraz zarządzania identyfikacją tożsamości w świetle wymogów obowiązujących w XXI wieku. Zwrócił uwagę m.in.

na problem wiarygodności tożsamości i korzyści z coraz powszechniejszego stosowania kart bezstykowych.

Praktyczne rozwiązania biometryczne w bankowości japońskiej omówił Peter Jones z Hitachi Europe. 81% banków w Japonii wybrało jako metodę uwierzytelniania swych klientów technologię rozpoznawania układu naczyń krwionośnych palca (ang. *Finger Vein Authentication*). Wprowadzaniu nowoczesnych rozwiązań w życie sprzyjają tam obowiązujące przepisy, które nakazują stosowanie biometrii w bankowości.

Anthony Franks z brytyjskiej firmy Optic Vision, będącej dostawcą rozwiązań elektronicznych systemów bezpieczeństwa, omówił międzynarodowe standardy związane z bezpieczeństwem w bankowości i zastosowanie biometrii oraz specjalistycznych narzędzi do monitorowania bezpieczeństwa w celu osiągnięcia zgodności z tymi standardami w praktyce.

Adrian Kapczyński z Auto ID przedstawił aktualne obszary zastosowań biometrii w Polsce. Zwrócił uwagę m.in. na to, że rozwiązania biometryczne stają się coraz tańsze i coraz lepsze, a także na problem żywotności wzorca biometrycznego.

Polski rynek biometryczny omówił Jakub Ożyński z Deep Blue Biometrics. Omówił m.in. tryby pracy systemów biometrycznych oraz zalety i wady poszczególnych technologii i podkreślił konieczność prawidłowej kalibracji urządzeń pracujących w tego typu systemach.

Trzy wystąpienia były poświęcone paszportom biometrycznym, które są już wprowadzane w naszym kraju. O doświadczeniach z wprowadzania tego typu rozwiązań biometrycznych w Polsce i na Litwie mówił Tomasz Goliński z Polskiej Wytwórni Papierów Wartościowych. Praktykę wdrażania Paszportowego Systemu Informacyjnego w MSWiA przedstawił Włodzimierz Sosnowski z WASKO, a aplikację do odczytu informacji z paszportu biometrycznego – Andrzej Białas z INSI.



Na zakończenie pierwszego dnia konferencji głos zabrał ponownie Remigiusz Kaszubski. Podkreślił, że banki są w Polsce liderami nowoczesnych rozwiązań technologicznych, niezbędnych do zapewnienia bezpieczeństwa transakcji i identyfikacji tożsamości. Zwrócił uwagę na konieczność wypracowania wspólnych rozwiązań w tym zakresie, gdyż tylko wtedy mają one szansę być zaakceptowane przez ogół obywateli i być stosowane w praktyce. Za rozwiązania, które będą się rozwijać równolegle w zakresie uwierzytelniania, uznał zarówno podpis elektroniczny, jak i rozwiązania biometryczne.

Adam Bułaciński
Redakcja



Wandaloodporna kamera Axis 212 PTZ-V

Firma **Axis Communications** przedstawia nową wersję popularnego modelu kamery 212 PTZ. Kamera **Axis 212 PTZ-V** to nie tylko gwarantowana wysoka jakość obrazu, ale przede wszystkim jeszcze lepsza ochrona przed zniszczeniem.

Metalowa obudowa i trwała, przezroczysta osłona soczewki kamery **AXIS 212 PTZ-V** zapewniają doskonałą ochronę przed ewentualnymi aktami wandalizmu. Dzięki temu kamera nadaje się między innymi do zastosowania w szkołach, sklepach, bankach i recepcjach, w których niezbędny jest podgląd całego obszaru. Funkcje natychmiastowego pozycjonowania w poziomie i pionie oraz zbliżenia pozwalają na szybkie i precyzyjne monitorowanie podejrzanego aktywności w polu widzenia kamery.

Kamera **AXIS 212 PTZ-V** jest wyposażona w 3-megapikselową matrycę i szerokokątny obiektyw. Kamera nie zawiera ruchomych części, więc błyskawicznie przełącza się między panoramicznym trybem pracy a uzyskiwanym natychmiastowo zbliżeniem, bez zużywania się mechanizmu i nieprzyjemnych dźwięków. Dzięki technologii PoE kamera sieciowa używa tego samego kabla zarówno do zasilania, jak i do transmisji wideo.



Kamera obsługuje zarówno adresy IPv4, jak i IPv6, a także oferuje szeroką gamę zabezpieczeń sieciowych i funkcji administracyjnych, m.in. wielopoziomowy dostęp, szyfrowanie HTTPS, IEEE 802.1X oraz filtrowanie adresów IP.

Autoryzowanym dystrybutorem Axis w Polsce jest firma **Softex Data**.

Bezpośr. inf. Softex Data

Relacja z konferencji DataCenter GigaCon



Airport Hotel Okęcie w Warszawie był 29 stycznia 2008 roku miejscem, w którym firma **Software-Konferencje**, specjalizująca się w propagowaniu wiedzy związanej z technologiami IT, zorganizowała konferencję poświęconą centrům przetwarzania danych (CPD). Wśród tematów poruszanych podczas konferencji znalazły się m.in. zagadnienia związane z bezpieczeństwem CPD i technologiami oraz narzędziami gwarantującymi niezawodny i bezpieczny dostęp do baz danych. W pierwszej części konferencji referaty wygłaszane były w sesji plenarnej, w drugiej – równolegle w dwóch salach, w różnych sesjach tematycznych. W kulkarach rozmieszczono stoiska firm uczestniczących aktywnie w konferencji, dzięki czemu istniała możliwość zapoznania się z ofertą tych firm oraz dyskusji na tematy interesujące uczestników konferencji.

W konferencji wzięło udział ok. 240 uczestników – głównie specjalistów branży IT z przedsiębiorstw państwowych oraz firm prywatnych, których codzienna praca jest związana z CPD. Referaty wygłosili przedstawiciele sponsorów konferencji (FAST Group, APC-MGE), sponsorów poszczególnych sesji (Ortronics, Infomex), innych firm uczestniczących (Polcom, Lanster), a także Instytutu Informatyki Politechniki Łódzkiej i Toyota Bank Polska. Partnerem medialnym konferencji była firma TechIT, a czasopismo *Zabezpieczenia* – jednym z jej patronów medialnych.

Naszych czytelników najbardziej zainteresowałyby wystąpienia sponsorów głównych konferencji. Trzy referaty firmy

FAST Group dotyczyły zasad budowy i architektury bezpiecznych CPD, w jednym z nich przedstawiono w szczególności przykład redundantnego systemu zasilania tego typu ośrodków. W referacie firmy APC-MGE zaprezentowano możliwości optymalizacji systemów infrastruktury serwerowni z wykorzystaniem oprogramowania InfraStruXure. Wspomniano też o systemie monitorowania NetBotz Surveillance, który, chociaż umożliwia rejestrację obrazu z kamer sieciowych rozmieszczonych w CPD, nie jest przeznaczony do ochrony obiektu, lecz służy do analiz związanych z eksploatacją CPD (np. ułatwia poznanie przyczyn ewentualnych awarii).

Tematyka konferencji obejmowała także następujące zagadnienia: macierze pamięci nowej generacji, wydajność i wirtualizacja serwerów, *data mining* (efektywna eksploracja dużych zasobów danych w celu pełnego wykorzystania informacji w nich ukrytej), transfer i tzw. hurtownie danych.

Podczas konferencji rozstrzygnięto także, głosami jej uczestników, konkurs pod nazwą Złoty Bit na najlepszy produkt informatyczny wspierający pracę polskich firm i instytucji. Do konkursu tego mogła zgłosić swoje rozwiązanie każda z firm prezentujących je podczas swoich wystąpień konferencyjnych. **Złoty Bit DataCenter GigaCon** zdobyła dużą większością głosów firma APC-MGE.

Adam Bułaciński
Redakcja

NASTĘPNA GENERACJA SYSTEMÓW ZABEZPIECZEŃ PRZYBYŁA



FIKCJA STAŁA SIĘ FAKTEM ... SYSTEMY ZABEZPIECZEŃ I-PRO PANASONIC.

Panasonic opanował najnowszą technologię IP, aby stworzyć naprawdę futurystyczny system zabezpieczeń i-pro, zawierający pełną gamę produktów. Pozwala on powstrzymać nie tylko inwazję intruzów, ale także znacząco redukuje koszty związane z użytkowaniem systemu, między innymi poprzez zmniejszenie ilości kabli oraz kosztów obsługi. Ponieważ posiadamy specjalistyczną wiedzę w tej dziedzinie, jesteśmy w stanie zaproponować najlepsze z możliwych rozwiązań.

Więcej informacji o produktach i-pro uzyskasz pod numerem telefonu (22) 33 81 177
lub odwiedzając stronę pss.panasonic.eu

i-pro

Panasonic
ideas for life

DOSKONAŁA FUNKCJONALNOŚĆ ZA NIESPOTYKANĄ CENĄ

24Mop.pl

wyłączny przedstawiciel producenta w Polsce

przetestuj
przez 10 dni
za darmo

**pokręć
jog
shuttle**



2399 PLN netto

**obsługa
przez
mysz**



1299 PLN netto

**pokręć
jog
shuttle**

**Rejestratory MPEG4, triplex, VGA
4 x audio, LAN, polskie menu**

- pełna konfiguracja zdalna przez soft
- obsługa wielu rejestratorów jednocześnie przez soft
- dostęp przez sieć wielu użytkowników równocześnie
- obsługa myszą
- polskie menu i soft
- obsługa 4 dysków [REJX8 i 16]
- trzy poziomy uprawnień
- maskowanie stref detekcji
- wyjście VGA i s-video
- 4 niezależne kanały audio

- rozdzielczość, ilość klatek, jakość ustalana niezależnie dla każdej kamery, godziny, zdarzenia
- LAN
- MPEG4 w zapisie i przez sieć
- triplex
- pilot
- programowalne wyjścia SPOT
- USB
- jog shuttle
- DVD opcjonalnie

REJX16

REJX4

Specyfikacja

Cecha	REJX16	REJX4
wejścia video	16 x BNC przelotowe	4 x BNC
wejścia audio	4 x chinch	4 x chinch
wyjścia video	1 x BNC, 1x spot-out, 1 x VGA, 1x s-video	1 x BNC, 1x spot-out, 1 x vga, 1x s-video
wyjścia audio	1 x chinch	1 x chinch
kompresja video	MPEG4	MPEG4
rozdzielczość	704 x 576, 704 x 288, 352 x 288	704 x 576, 704 x 288, 352 x 288
szybkość odtwarzania	400 klatek / s [16 x 25]	100 klatek / s [4 x 25]
tryb nagrywania	ciągły, detekcja, alarm, harmonogram, kryzysowy	ciągły, detekcja, alarm, harmonogram
konfiguracja przez sieć	tak	tak
nośnik	4 x HDD 3,5" ATA [bez limitu]	2 x HDD 3,5" ATA



automatyczne zaznaczenie
obszarów w których wykryto ruch

zobacz online:
www.24m.pl/rejx4



intuicyjne menu graficzne



menu w języku polskim



precyzyjny harmonogram pracy



filtr powiadomień mailowych



dostępne wersje z CD i DVD

24Mop.pl

tel. 071 333 87 22, 071 724 52 82, 0601 24 66 66, poczta@24m.pl, **www.24m.pl**

ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (0 58) 320 94 00, fax: (0 58) 320 94 01
e-mail: satel@satel.pl, www.satel.pl

Monitorowanie oprogramowania

Zagadnienie monitorowania oprogramowania wywołuje wiele kontrowersji. Osoby na co dzień zajmujące się realizacją zadań wynikających z konieczności stałego badania poziomu bezpieczeństwa sieci informatycznej wiedzą, iż działania te są prowadzone według przejrzystych zasad, w sposób opisany procedurami, zgodny z wytycznymi wspólnymi dla wszystkich użytkowników sieci, a wykonywane czynności są realizowane cyklicznie, według wcześniej opracowanego harmonogramu

Zasady, które zostały opisane powyżej, nie są tworem z utopijnego świata.

W największym uproszczeniu monitorowanie bezpieczeństwa oprogramowania w każdej sieci informatycznej powinno być:

- prowadzone jako proces ciągły,
- realizowane zgodnie ze zdefiniowanymi wcześniej zasadami
 - tożsamymi dla wszystkich użytkowników w sieci – zgodnymi z polityką bezpieczeństwa firmy, której zasoby podlegają monitorowaniu,
- prowadzone przez kompetentny, rzetelny personel,
- raportowane.

Każdy użytkownik systemu informatycznego objętego monitorowaniem powinien być w związku z tym zaznajomiony z panującymi w jego organizacji zasadami. Zasady te powinny jasno wyznaczać granice, których pracownik nie powinien przekraczać, realizując powierzone czynności służbowe i wykorzystując do ich realizacji sprzęt i oprogramowanie informatyczne udostępniane przez pracodawcę.

Do skutecznego prowadzenia monitorowania bezpieczeństwa oprogramowania może być wykorzystywanych wiele różnorodnych narzędzi informatycznych, od prostych programów antywirusowych instalowanych na pojedynczych urządzeniach począwszy, na zaawansowanych systemach kończąc. Dzięki takim systemom sprawny, doświadczony operator – potrafiący wykorzystać ich zaawansowane możliwości – może prowadzić szereg działań podnoszących bezpieczeństwo chronionych zasobów informatycznych, a sposób jego pracy uzależniony jest od rozwiązania technologicznego stosowanego w danym przedsiębiorstwie. W niewielkich instytucjach dbałość o bezpieczeństwo IT może ograniczać się do stosowania prostego oprogramowania antywirusowego i zapory ogniowej (firewalla programowego lub sprzętowego) minimalizujących prawdopodo-

bieństwo przeprowadzenia skutecznego ataku z zewnątrz na chronioną sieć wewnętrzną.

Im lepsze (niekoniecznie droższe) narzędzia, tym większe jest prawdopodobieństwo wykrycia i usunięcia złośliwego oprogramowania lub zablokowania zewnętrznego ataku na urządzenia wchodzące w skład chronionej sieci komputerowej. Głównym wyznacznikiem sukcesu w przypadku tego typu narzędzi jest czas pojawienia się na stronie producenta nowych definicji wirusów (szczepionek antywirusowych), czas ich instalacji na naszych komputerach, a także stała aktualizacja systemu operacyjnego i odpowiednia konfiguracja zapór ogniowych. Takie działania prowadzone są najczęściej w sposób automatyczny, a ingerencja człowieka ogranicza się jedynie do weryfikacji, czy aktualizacja przebiegła zgodnie ze zdefiniowanym wcześniej harmonogramem, czy konieczne jest jej „ręczne” przeprowadzenie.

By mówić o monitorowaniu, musimy się skupić na rozwiązaniach stosowanych w dużych przedsiębiorstwach, w których codzienne czynności wykonywane przez kadrę pracowniczą są realizowane przy wykorzystaniu dużej liczby komputerów (przeszło kilkuset). W takiej sieci prowadzenie monitorowania bezpieczeństwa IT jest konieczne, gdyż niekontrolowany rozwój złośliwego oprogramowania może doprowadzić do paraliżu działalności całej firmy.

Podstawowym działaniem prowadzonym przez służby monitorujące, odpowiedzialne za zapewnienie odpowiedniego poziomu chronionych zasobów informatycznych, jest dbanie o aktualność oprogramowania antywirusowego na każdym z komputerów funkcjonujących w sieci firmowej. Wystarczy tylko kilka urządzeń, na których zupełnie brak oprogramowania antywirusowego lub oprogramowanie jest zainstalowane, ale bazy sygnatur (definicji wirusów) są nieaktualne, aby doprowadzić do infekcji kolejnych komputerów. Komputery

z aktualnymi sygnaturami powinny w krótkim czasie poradzić sobie z wykryciem i usunięciem wirusa, jednakże lawinowo spada wydajność całej sieci komputerowej, ponieważ procesor każdej z zarażonych maszyn musi wykonać dodatkowe operacje związane z koniecznością odparcia ataku przez aplikacje antywirusowe.

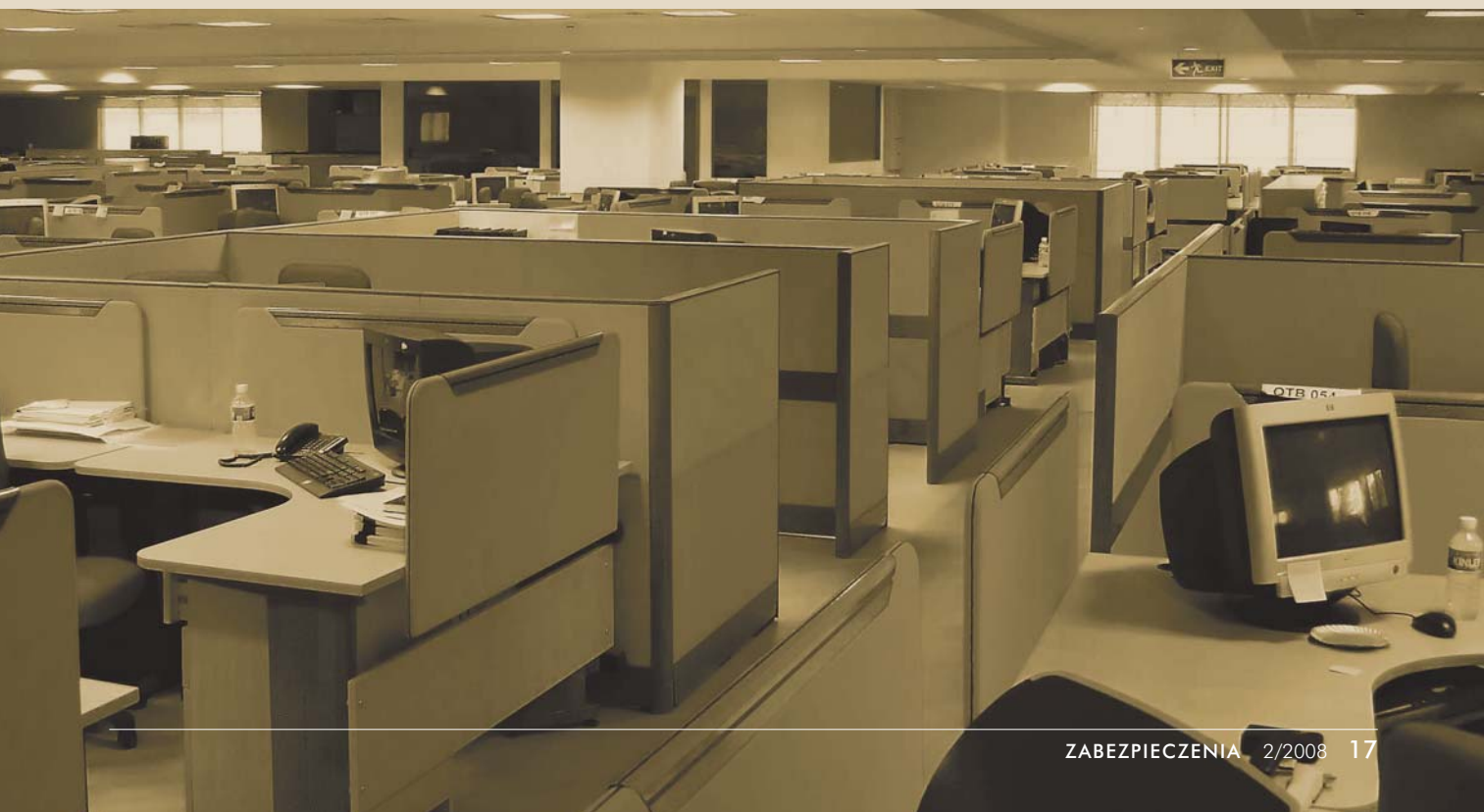
Powodów wystąpienia tego typu nieprawidłowości (brak oprogramowania antywirusowego lub nieaktualność sygnatur) może być kilka. Problemem może być brak jasnych reguł przy wdrażaniu nowo zakupionych urządzeń (brak zapisów w umowach z dostawcami dotyczących standardu oprogramowania w kupowanych urządzeniach, brak koordynacji pomiędzy zakupem a wdrożeniem) lub – co gorsza – świadome działanie użytkownika (celowe wyłączanie oprogramowania, odinstalowanie oprogramowania). W przypadku wystąpienia ostatniej z wymienionych ewentualności służby monitorujące powinny pouczyć użytkownika o prowadzeniu przez niego działań niezgodnych z zasadami bezpieczeństwa obowiązującymi w firmie (o ile przepisy takie funkcjonują w przedsiębiorstwie). Jeśli mimo pouczenia sytuacja powtarza się, zazwyczaj wyciągane są konsekwencje dyscyplinarne wobec niesubordynowanego pracownika. Bywa również i tak, iż niektóre starsze systemy operacyjne (np. Windows 95 czy Windows 98), dla których już nie jest realizowane wsparcie ze strony producenta, nie są w stanie w sposób automatyczny przeprowadzić aktualizacji definicji wirusów i w takiej sytuacji konieczne jest przeprowadzenie aktualizacji bezpośrednio przez personel informatyczny.

Prócz realizacji zadań wynikających z konieczności zapewnienia ochrony antywirusowej na odpowiednim poziomie, rozbudowane systemy monitorowania pozwalają dodatkowo na monitorowanie parametrów systemów operacyjnych (sprawdzanie, czy przeprowadzana jest ciągła aktualizacja systemu operacyjnego, które poprawki systemu są zainstalowane, jaki jest stan bezpieczeństwa systemu) oraz na weryfikację wykorzystywanego przez użytkowników oprogramowania. Jest to bardzo istotne z punktu widzenia bezpieczeństwa, gdyż wiele z wykorzystywanych przez użytkowników – samowolnie instalowanych – aplikacji (darmowych w szczególności) ma

dodatkowe, ukryte dla przeciętnego użytkownika funkcje. Umożliwiają one wykradanie zapisanych na twardych dyskach informacji lub nawet przechwytywanie loginów i haseł dostępu do systemów informatycznych i wysyłanie w ten sposób pozyskanych informacji na serwery zewnętrzne, zarządzane przez nieuprawnione – z punktu widzenia firmy – osoby. Brak kontroli w tym obszarze może także doprowadzić do zakłócenia stabilności pracy systemów biznesowych wykorzystywanych w firmie (zwiększenie obciążenia procesora, uruchamianie procesów powodujących konflikt z procesami pochodzącymi od aplikacji biznesowych). Systemami pomocniczymi do monitorowania tego typu nieprawidłowości są systemy weryfikujące aktywność użytkowników w zakresie przeglądania stron internetowych. Tego rodzaju monitorowanie budzi wśród pracowników wiele kontrowersji, natomiast, statystycznie rzecz biorąc, przeważająca większość niedopuszczonego do użytkowania w sieci wewnętrznej firmy oprogramowania pobierana jest przez użytkowników właśnie ze stron WWW. Dopiero korelacja zdarzeń wykrytych przez systemy antywirusowe oraz badanie aktywności danego użytkownika w sieci pozwala na jednoznaczne określenie źródła infekcji i rozpoznanie, czy działanie użytkownika jest celowym nadużyciem, czy działaniem nieświadomym, co z kolei warunkuje dalszy sposób postępowania. Najistotniejsze jest to, by infekcja w jak najkrótszym czasie została wykryta, a niebezpieczeństwo zarażenia kolejnych komputerów zminimalizowane. Z punktu widzenia bezpieczeństwa najistotniejsze jest jak najszybsze zdefiniowanie źródła niebezpieczeństwa, a następnie podjęcie odpowiednich kroków zmierzających do wyeliminowania go bądź zminimalizowania ryzyka wystąpienia danego zagrożenia w przyszłości.

Podsumowując, zabezpieczanie sieci można przyrównać do antykoncepcji – istnieje wiele metod, które zapewniają skuteczność bliską 100%, jednak żadna z nich nie gwarantuje nam pełnej skuteczności. Im więcej zabezpieczeń zastosujemy, tym większe są nasze szanse na uchronienie się przed atakiem.

KRZYSZTOF BIAŁEK





masz wybór...



www.ccx.pl

POLON-ALFA

**Największy polski
producent systemów
sygnalizacji pożarowej**

www.polon-alfa.pl



**Systemy
Kontroli Dostępu**



MaxiTalk

Obsługuje do 22000
użytkowników i 4000 drzwi



Maxi.Net

Zarządzanie Systemem Kontroli
poprzez internet



MaxiMate

Łatwy, szybki i przyjazny System
Kontroli Dostępu do 8700
użytkowników i 16 drzwi

**Systemy
Przeciw włamaniowe**



ProSYS™

Zintegrowane Systemy Bezpieczeństwa



Agility™

Elastyczne rozwiązanie bezprzewodowe
z komunikacją dwustronną



WisDom™

Bezprzewodowe Systemy Bezpieczeństwa



WatchOUT™
niezawodny Detektor
Zewnętrzny



WatchIN™
Przemysłowy
Detektor Grade 3

**Zintegrowany
System Zarządzania
Bezpieczeństwem**



SynopSYS™

System Zarządzania Bezpieczeństwem i
Automatyką budynków rozproszonych

- to oprogramowanie do zdalnego zarządzania automatyką budynków rozproszonych
- łączy bezpieczeństwo i automatykę budynków w jedno rozwiązanie
- elastyczny w implementacji indywidualnych projektów

RISCO
GROUP

Creating Security Solutions.
With Care

riscogroup.com

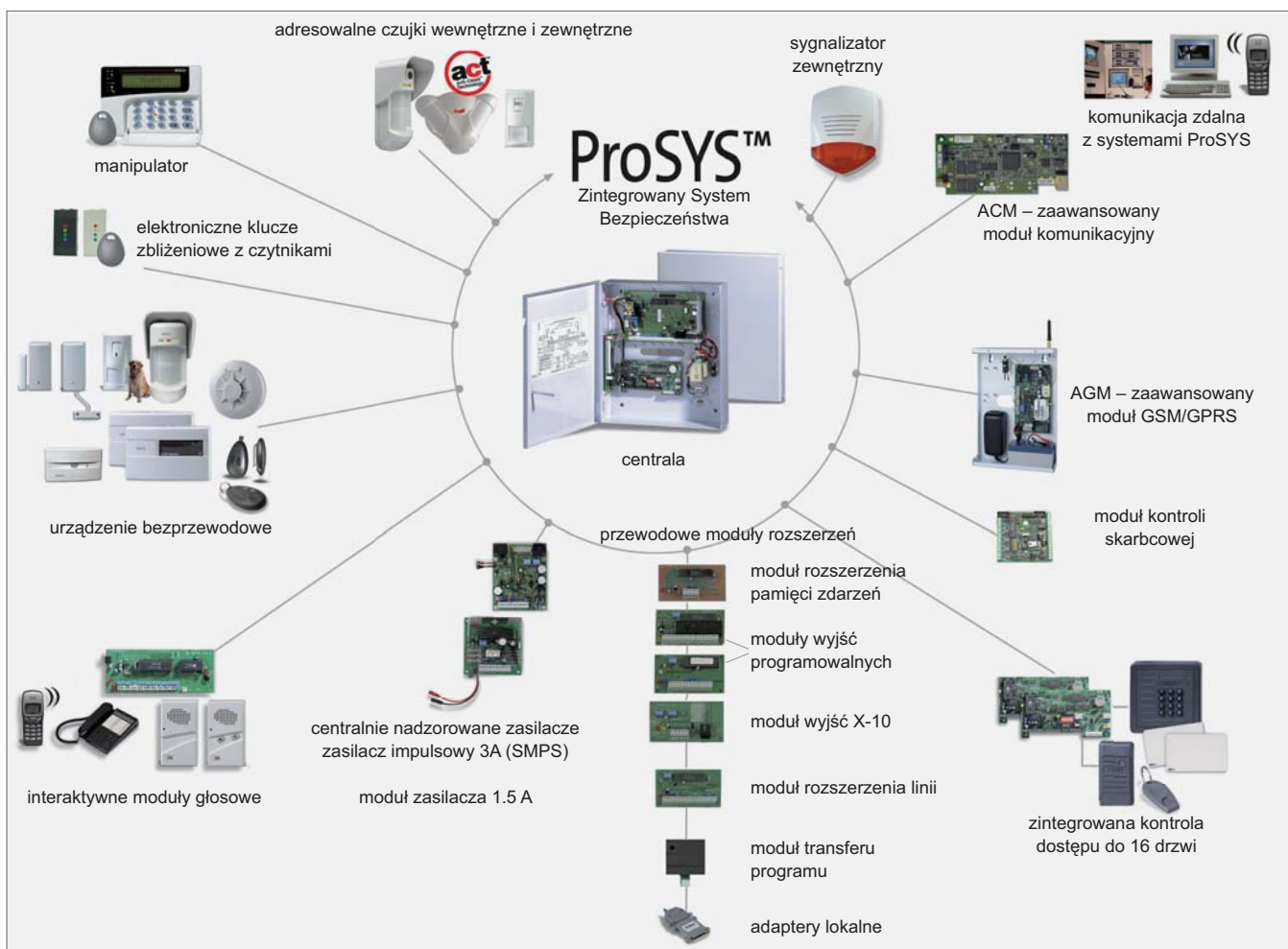
RISCO Group Poland Tel: +48 22 500 28 40, Fax +48 22 500 28 41, email: Poland@riscogroup.com

RISCO Group prezentuje zintegrowany system bezpieczeństwa ProSYS

RISCO Group, wiodący światowy lider systemów bezpieczeństwa, ma przyjemność zaprezentować system bezpieczeństwa ProSYS. Produkt ten, wyposażony w podwójną magistralę komunikacyjną i rozwiązania komunikacyjne IP/GPRS, jest punktem zwrotnym w technologii zintegrowanych systemów zabezpieczeń. Jeden producent proponuje kompleksowe rozwiązanie systemów bezpieczeństwa dla różnych grup odbiorców – od ochrony obiektu aż po stacje monitorujące

ProSYS jest łatwy w instalacji i rozbudowie. Można zainstalować podstawowy system przeciwwłamaniowy, a następnie płynnie i bez komplikacji dodawać moduły i funkcje, takie jak komunikatory IP lub GSM/GPRS, kontrola dostępu (*Access Control*), moduły dźwiękowe (*Voice Module*)

czy funkcje bezprzewodowe (*Wireless*). ProSYS umożliwia podłączenie bezpośrednio do magistrali, bez konieczności stosowania dodatkowych ekspanderów, do 32 detektorów. Są to detektory takie, jak WatchOUT (zewnętrzny detektor), WatchIN Industrial Detector (detektor do zastosowań



Rys. 1. Zintegrowany system bezpieczeństwa ProSYS



Fot. 1. Podstawowe elementy systemu ProSYS

przemysłowych w trudnym środowisku) oraz Industrial LuNAR, przeznaczony do instalacji na sufitach w wysokich pomieszczeniach.

Przyjazny w instalowaniu, programowaniu i obsłudze ProSYS zawiera w sobie zaawansowaną technologię *Auto-Install Technology*. Centrala samoczynnie wykrywa wszystkie urządzenia podłączone do magistrali, co pozwala uniknąć czasochłonnej ręcznej konfiguracji. Zapewnia również możliwość samotestowania oraz wygodnej diagnostyki przy użyciu klawiatury LCD lub zdalnie, poprzez oprogramowanie konfiguracyjne. Przy tak zaawansowanej technologii osiągamy efekt pracy na odległość; instalator lub operator może sprawdzać niezbędne parametry, takie jak napięcie na akumulatorze sygnalizatora zewnętrznego czy poziomy sygnałów obu kanałów podczerwieni w detektorach zewnętrznych WatchOUT, bez potrzeby pojawiania się w obiekcie.

ProSYS wykonany jest w trzech wersjach (do 16, do 40, do 128 stref) z szeroką gamą elementów do rozbudowy.

Zaawansowany moduł komunikacyjny ACM umożliwia programowanie centrali oraz zestawienie łącza transmisji alarmu poprzez sieć LAN/WAN.

Centrale ProSYS mogą być wyposażone w dedykowany moduł komunikacji GSM, umożliwiający transmisję poprzez kanał głosowy, SMS lub GPRS. Tego typu rozwiązanie umożliwia zdalne programowanie i diagnostykę centrali alarmowej w pełnym zakresie. Moduł ten może pracować także jako łącze zapasowe, symulując linię telefoniczną w przypadku uszkodzenia innego łącza. Transmisja do ACO (Alarmowego Centrum Odbiorczego) jest realizowana z wykorzystaniem pełnego formatu raportów SIA lub Contact ID.

O RISCO Group:

RISCO Group tworzy oparty na protokole IP zintegrowany system bezpieczeństwa dla rynku globalnego. Firma proponuje najwyższej jakości produkty, dopasowane do wymagań klientów i standardów przemysłowych, stosowane w rozwiązaniach przewodowych i bezprzewodowych z oprogramowaniem integrującym. Dzięki zastosowaniu wyrafinowanej technologii w produkcji detektorów i niezawodnym systemom kontroli dostępu RISCO Group dostarcza najlepsze rozwiązania do budowy i monitoringu systemów bezpieczeństwa. Nasze rozwiązania znalazły zastosowanie w handlu, przemyśle, instytucjach publicznych oraz prywatnych rezydencjach na całym świecie.

Aby być bliżej klientów, firma RISCO Group otworzyła biuro w Polsce. Więcej informacji można znaleźć na stronie www.riscogroup.com.

Biuro w Warszawie:
ul. 17 Stycznia 56
02-146 Warszawa
tel.: (22) 500 28 40, faks: (22) 500 28 41

W chwili obecnej detektory WachOUT to jedno z najbardziej niezawodnych detektorów zewnętrznych. Charakteryzują się podwyższoną odpornością na sygnały wywołane przez kołyszące się obiekty, takie jak krzaki czy drzewa. Wyposażone są w czujniki odporne na sygnały generowane przez zwierzęta o wzroście do 70 cm. Posiadają mechanizm wykrywający próby zamalowania lub zakrycia detektora oraz wiele innych cech niespotykanych w produktach konkurencyjnych.

Dualny detektor Industrial LuNAR umożliwia niezawodną i ekonomiczną ochronę wysokich pomieszczeń (do 8,6 m wysokości). Zastosowanie technologii *Anti-Cloak* pozwala na wykrycie zamaskowanego intruza, niewidocznego dla standardowych pasywnych czujek podczerwieni (PCP). Duże pole detekcji (o średnicy 22 m) czujki pozwala zabezpieczyć rozległe powierzchnie magazynowe przy niskich nakładach finansowych. Wystarczy cztery czujki połączone jednym kablem magistrali do zabezpieczenia hali o powierzchni ponad 1500 m².

Bardzo ciekawym przykładem zastosowania ProSYS jest uruchomienie systemu bezpieczeństwa poczty belgijskiej. W 800 oddziałach pocztowych zainstalowano centrale ProSYS z modułem komunikacyjnym IP, zintegrowaną kontrolą dostępu oraz modułami przeznaczonymi do nadzoru skarbców i bankomatów (*Vault Control Units* – VCU). Dzięki modułowi VCU operatorzy ACO mogą zdalnie nadzorować w czasie rzeczywistym pomieszczenia skarbcza oraz obszary ściśle związane z bankomatami we wszystkich oddziałach poczty jednocześnie. Do ochrony tych pomieszczeń zastosowano najnowsze czujki dualne z technologią *Anti-Cloak*.

ProSYS otwiera nowe możliwości biznesowe dla instalatorów systemów bezpieczeństwa. Dla nich „marzenie stało się rzeczywistością”.

RISCO GROUP

ALARMTECH

projektowanie ❖ produkcja ❖ dystrybucja

NOWA ARCHITEKTURA SYSTEMÓW ALARMOWYCH AGENTOWY SYSTEM ROJU NOVATOR

- ❖ architektura systemów sztucznej inteligencji
- ❖ łatwość budowy, autokonfiguracja
- ❖ wysoki poziom bezpieczeństwa
- ❖ elastyczność - brak ograniczeń
- ❖ wszechstronność zastosowań
- ❖ skalowalność systemu
- ❖ optymalizacja kosztów
- ❖ samonaprawialność
- ❖ odporność na ataki
- ❖ niezawodność

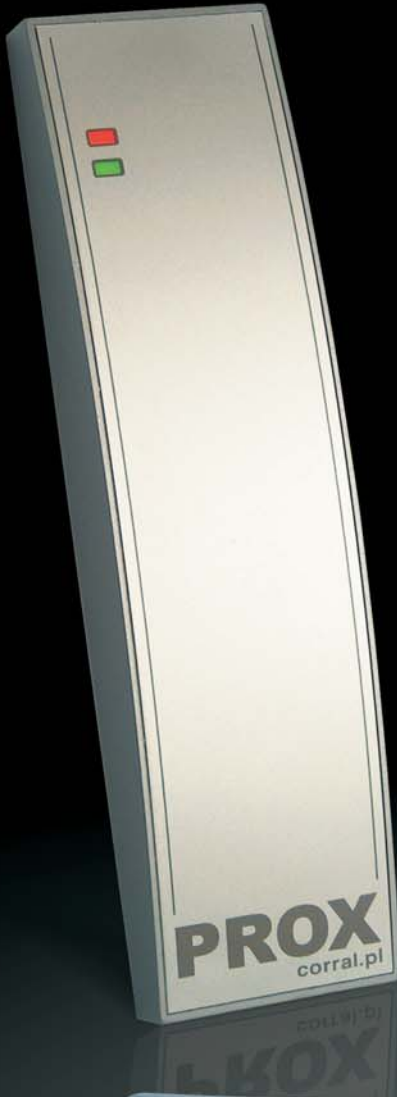
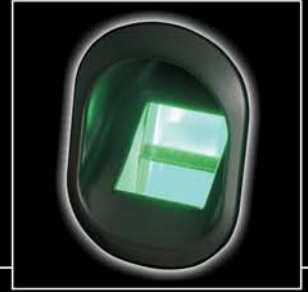


**Zgodny z europejskimi
standardami**

**Szczegółowe informacje na naszym stoisku
SECUREX 2008, Pawilon 3A, Box 71**

ZAPRASZAMY

Alarmtech Polska sp. z o.o., ul. Kielnieńska 115, 80-299 Gdańsk
tel. 058 340 24 40, fax 058 340 24 49, info@alarmtech.pl, www.alarmtech.pl



- kontroler oparty o TCP/IP obsługujący:
 - czytniki zbliżeniowe
 - odbiorniki radiowe
 - czytniki linii papilarnych
 - urządzenia Wiegand
- rejestracja zdarzeń i czasu pracy
- bezpłatne oprogramowanie klient-serwer
- karty i breloki zbliżeniowe:
 - UNIQUE 125 kHz
 - MIFARE 13.56 MHz
- akcesoria (zasilanie, rygle, zwory)
- profesjonalny nadruk na kartach:
 - ISO
 - Clamshell



iProtect

– sieciowy system zabezpieczenia obiektów (moduły SSWiN oraz RCP)



Na łamach czasopisma *Zabezpieczenia* ukazały się już dwa artykuły opisujące system *iProtect* firmy Keyprocessor:

- w numerze 6/2007 – traktujący o ogólnych właściwościach systemu,
- w numerze 1/2008 – opisujący moduły kontroli dostępu oraz telewizji dozorowej IP (Video IP).

W tym numerze chcemy przybliżyć Państwu moduły Systememu Sygnalizacji Włamania i Napadu (SSWiN) oraz Rejestracji Czasu Pracy (RCP).

SSWiN

Moduł SSWiN pozwala na zarządzanie w systemie *iProtect* wieloma centralami alarmowymi IBC128 firmy Keyprocessor. Może on być używany oddzielnie, jak również w połączeniu z innymi modułami wchodzącymi w skład systemu. Posiada pełną funkcjonalność zaawansowanej centrali alarmowej (zgodność z normą EN50131), a dzięki integracji w systemie *iProtect* funkcjonalność ta znacząco wzrasta. Centrala alarmowa IBC128 pozwala na podłączenie do 128 linii alarmowych. Wbudowana jednostka komunikacyjna umożliwia komunikację alarmową poprzez połączenie AL1 (ISDN/B) lub AL2 (ISDN/D). Nowoczesna klawiatura LCD z panelem dotykowym pozwala użytkownikowi na wybór koloru podświetlenia oraz sposobu montażu (nad- lub podtynkowy), co znacznie podnosi walory estetyczne przy zachowaniu pełnej funkcjonalności. Specjalnie wykonany panel dotykowy uniemożliwia intruzowi odgadnięcie cyfr wchodzących w skład kodu dostępu. Opcjonalnie klawiatura ta może być połączona z dedykowanym czytnikiem kart zbliżeniowych.

Integracja w iProtect

System alarmowy może być zarządzany poprzez łatwy w użyciu i przejrzysty interfejs użytkownika systemu *iProtect*. Technologia sieciowa pozwala na bezpieczne i bezproblemowe zarządzanie systemem z każdego miejsca na świecie z dostę-

pem do Internetu. Wszystkie zdarzenia mają swoje odzwierciedlenie w systemie *iProtect*. Interaktywne mapy natychmiast informują o miejscu wystąpienia zdarzenia i wskazują na czujnik, który wygenerował alarm. Dodatkowo zdarzenie to będzie odnotowane i przechowywane w pamięci systemu wraz z niezbędnymi informacjami odnoszącymi się do niego. Dzięki integracji możliwe jest także natychmiastowe zweryfikowanie alarmu za pomocą innych systemów.

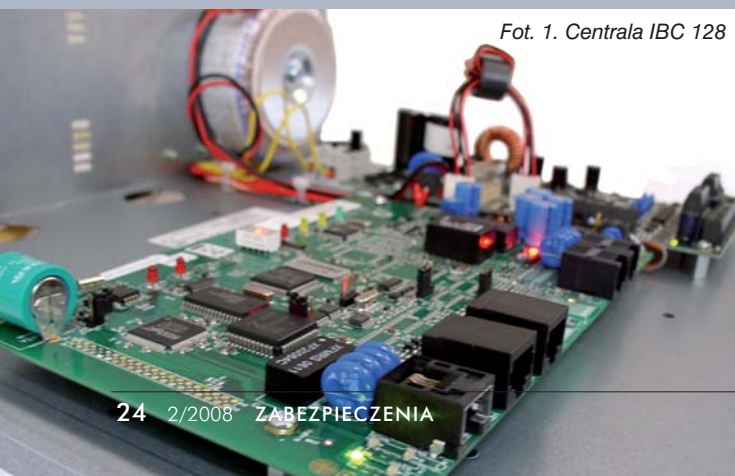
Integracja z innymi modułami

Poprzez dodawanie kolejnych modułów system *iProtect* może być rozbudowany do w pełni zintegrowanego systemu zarządzania bezpieczeństwem. Jedną z wielu zalet integracji różnych systemów bezpieczeństwa w *iProtect* jest to, że takie rozwiązanie umożliwia łączenie funkcjonalności tych systemów. Integracja wielu różnych modułów bezpieczeństwa stwarza możliwość optymalizacji całego systemu i znacznego wyeliminowania fałszywych alarmów poprzez ich zaawansowaną weryfikację. Dzięki *iProtect* możliwe jest uzyskiwanie obrazów na żywo z miejsc, w których wykryto alarm. Przy połączeniu SSWiN z Systemem Kontroli Dostępu (SKD) możliwe jest blokowanie dostępu do stref, które są uzbrojone, lub automatyczne rozbrajanie stref po autoryzacji karty dostępu w czytniku. Każdy czytnik SKD może po udzieleniu dostępu do określonej strefy automatycznie ją rozbroić i jednocześnie uzbroić inną strefę (np. tę, którą użytkownik opuszcza). Dodatkowo system może być skonfigurowany tak, aby nie można było uzbroić strefy, w której znajdują się ludzie.

Dzięki integracji kontroli dostępu z Video IP bardzo łatwa jest weryfikacja wizualna osób wchodzących do pomieszczeń. Także zdarzenie alarmowe może zostać zweryfikowane poprzez odpowiednią akcję systemu Video IP. Są to tylko niektóre przykłady integracji SSWiN z innymi systemami zabezpieczenia w obrębie *iProtect*. Rozbudowana i elastyczna architektura systemu oferuje znacznie więcej możliwości, których wykorzystanie zależy od wymagań inwestora i inwencji projektanta.

Szybki dostęp do obrazów wideo

Po wystąpieniu zdarzeń w systemie alarmowym często trudne jest znalezienie odpowiednio powiązanych sekwencji wideo. Dzięki integracji systemu telewizji dozorowej z innymi systemami w *iProtect* jest to bardzo łatwa operacja. Wystarczy kliknąć na wiersz z informacją o interesującym nas zdarzeniu, aby natychmiast otrzymać odpowiedni fragment obrazu wideo z właściwych kamer.



Fot. 1. Centrala IBC 128

Konstrukcja SSWiN

Pomimo tego, że moduł centrali alarmowej został zaprojektowany dla systemu *iProtect*, możliwa jest w pełni autonomiczna jego praca. Uzupełnieniem centrali alarmowej są moduły rozszerzeń wejść i wyjść oraz klawiatury LCD ze zintegrowanym czytnikiem zbliżeniowym. Dla zapewnienia maksymalnego bezpieczeństwa, aby zagwarantować bezawaryjną komunikację z serwerem, SSWiN powinien pracować w wydzielonej sieci lokalnej. Dlatego serwer dedykowany dla systemu *iProtect* ma co najmniej dwie karty sieciowe, a jego komunikacja w sieci TCP/IP jest zabezpieczona za pośrednictwem protokołu SSL.

System RCP

System *iProtect* zawiera przyjazne dla użytkownika i elastyczne oprogramowanie Rejestracji Czasu Pracy (RCP) z nieograniczonymi możliwościami raportowania. Jest ono odpowiednie dla zmiennych godzin pracy, rejestracji nieobecności i innych aspektów rozliczania czasu pracy. Rejestracja rozpoczęcia, zakończenia, przerw i innych zdarzeń związanych z czasem pracy może odbywać się z wykorzystaniem czytników SKD, specjalnych terminali RCP oraz terminali wirtualnych INFOBOX.

Dzięki zaawansowanym funkcjom importu i eksportu moduł RCP daje się z łatwością integrować z wieloma zewnętrznymi systemami kadrowo-płacowymi.

Mnogość opcji programowania, zaawansowane terminale, w pełni sieciowa praca, elastyczność i szerokie możliwości wymiany danych z systemami zewnętrznymi czynią moduł *iProtect* RCP idealnym rozwiązaniem dla wymagających użytkowników.

Rejestracja godzin...

Coraz większa liczba organizacji wdraża elektroniczne systemy Rejestracji Czasu Pracy. Niekiedy wystarczająca jest prosta forma rejestracji godzin pracy (każdego dnia zapisywane są godziny przyścia i wyjścia pracowników, a czas pomiędzy nimi traktowany jest jako godziny pracy). Jeżeli jest to konieczne, do wyników obliczeń wprowadzane są stałe czasy przerw w pracy.

...a Rejestracja Czasu Pracy

Obecnie klienci wymagają więcej. Chcą na przykład zaimplementować w systemie zbiorowe umowy pracy i regulacje własnej organizacji. Te umowy i regulacje mają bezpośredni wpływ na sposób rejestracji czasu pracy. Celem jest zawsze otrzymanie precyzyjnej informacji o sposobie spędzania czasu w pracy przez pracowników.

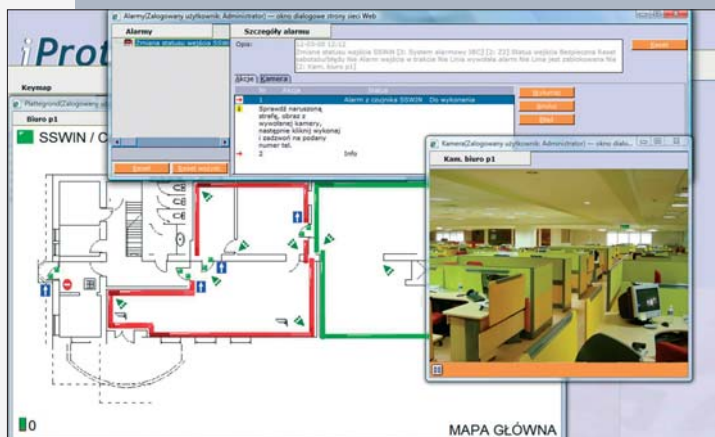
Ciągłe śledzenie godzin pracy

System Rejestracji Czasu Pracy jest szczególnie wymagany tam, gdzie stosowane są zmienne godziny pracy. Taki system przynosi korzyści nie tylko zarządowi firmy, ale również pracownikom.

Moduł RCP systemu *iProtect* pozwala pracownikom, poprzez terminal TC9320 lub wirtualny terminal INFOBOX, sprawdzać ich własne dane dotyczące godzin pracy, rozkładu dni, urlopów itp. – bez konieczności zwracania się do działu personalnego. W standardzie system zakłada obsługę 3000 pracowników.

Terminal TC9320

W systemie *iProtect* możliwe jest korzystanie z łatwego w obsłudze i jednocześnie zaawansowanego terminala TC9320. Jest



Fot. 2. Ekran przedstawiający komunikat o zdarzeniu alarmowym z mapą piętra na którym wystąpił alarm oraz obrazem z kamery

on podłączany bezpośrednio do sieci TCP/IP. Za jego pośrednictwem pracownicy mogą dokonywać różnego rodzaju czynności związanych z RCP. Zalogowanie się do terminala odbywa się za pomocą tej samej karty co dla kontroli dostępu czy parkingu. Wszelkie zmiany/odstępstwa od reguły (zapomniane meldowania, zwolnienia, zmiany rozkładów dni) są łatwe do zaimplementowania w terminalu. Co więcej, możliwe jest lokalne zarządzanie działem/departamentem – wtedy przełożony ma dostęp tylko do danych podległych mu pracowników.

Nadgodziny bez skomplikowanych obliczeń

W *iProtect* można wprowadzić bardzo szczegółowe schematy nadgodzin. Dopłaty, np. za soboty i niedziele, lub wzrost stawek wynagrodzenia w zależności od liczby nadgodzin (po odpowiednim wprowadzeniu schematów do systemu) są automatycznie obliczane i przedstawiane w postaci czytelnego raportu. Wszystkie obliczenia mogą być również eksportowane do systemów administracji plac. Elastyczny interfejs do systemów kadrowo-płacowych zakłada wymianę informacji przy pomocy automatycznie lub ręcznie generowanych plików raportów XML, CSV, jak również bezpośredniej komunikacji baz danych – JDBC, ODBC.

Podsumowanie

Omawiane w niniejszym, a także we wcześniejszych artykułach moduły SKD, SSWiN, Video IP, oraz RCP składają się na podstawową funkcjonalność zintegrowanego systemu *iProtect*. Nie należy zapominać, że pozostałe moduły – parkingu zaawansowanego oraz ochrony osób – jak również dodatkowe funkcje, takie jak rejestracja gości, zaawansowane zarządzanie I/O oraz nadruki na kartach (Key Badge Photo ID), znacząco wpływają na poprawę funkcjonalności całego systemu i czynią go perfekcyjnym rozwiązaniem do zarządzania bezpieczeństwem.

Niewątpliwą zaletą systemu *iProtect* jest to, że jest on oparty na technologiach sieciowych, a sama aplikacja jest uruchamiana z serwera. Dzięki temu nie jest



Fot. 3. Klawiatura LCD z panelem dotykowym

konieczne instalowanie dodatkowego oprogramowania na wszystkich komputerach.

Zarówno oprogramowanie, jak i zestaw urządzeń w systemie *iProtect* są całkowicie skalowalne. Użytkownik może zacząć od małego systemu (np. SKD + SSWiN), który następnie będzie rozbudowany, aby sprostać zwiększającym się wymaganiom, bez utraty dokonanych już inwestycji.

W celu uzyskania dodatkowych informacji dotyczących systemu *iProtect*, a także innych produktów z asortymen-

tu Miwi-Urmet, zachęcamy do kontaktu z naszą firmą. Organizujemy także prezentacje opisywanego systemu oraz zapewniamy profesjonalną pomoc przed- i posprzedażową.

Zapraszamy do odwiedzenia naszego stanowiska podczas targów **Securex 2008 (Pawilon 3A, stoisko nr. 104)**.

ŁUKASZ SZAFONI
MIWI-URMET

ES instal
sp. z o.o.

02-743 Warszawa
ul. Batuty 1/804
tel./faks 022 847 47 52
e-mail: andrzej@acn.pl
<http://www.esinstal.pl>

Jesteśmy firmą, która rozwiązuje problemy z zakresu bezpieczeństwa osób, mienia i ochrony informacji

Realizujemy projekty z każdego, najbardziej wymagającego zakresu zabezpieczenia techniczno-organizacyjnego i branż pokrewnych

Audyty bezpieczeństwa
Usługi projektowe
Kosztorysowanie
Kompleksowe opracowanie Polityki Bezpieczeństwa
Usługi prawno-organizacyjne

Jesteśmy ekspertami w zakresie projektowania systemów sygnalizacji zagrożeń, okablowania strukturalnego, organizacji ochrony fizycznej, systemów ochrony informacji niejawniej, zarówno w zakresie technicznym, jak i organizacyjnym



Panasonic EBL 512

Analogowy Adresowalny System Alarmu Pożaru

Zaprojektowany w celu wczesnej detekcji zagrożenia pożarowego i minimalizacji fałszywych alarmów. EBL 512 są to 4 pętle dozoru po 128 adresów i możliwość pracy w sieci do 30 central. System posiada aktualne świadectwa dopuszczenia wyrobu do stosowania w ochronie przeciwpożarowej w Polsce

www.raj-international.net

ul. Księcia Ziemowita 55/57
03-885 Warszawa
tel. 22 679 92 11
fax. 22 679 49 87

Panasonic
Panasonic Electric Works
Fire & Security Technology Europe AB
Dystrybutor systemu wykrywania Pożaru





druga odsłona systemu iP-pro



System **iP-pro** należy do rodziny systemów IP video i jest idealnym rozwiązaniem dla takich obiektów jak: szkoły, dworce, szpitale, hotele, obiekty przemysłowe i biurowe. Druga edycja **iP-pro** posiada rozszerzoną ofertę kamer IP oraz wysoką jakość obrazu.

Do systemu dedykowane są dwie platformy zarządzania, dające możliwość łatwego tworzenia systemów hybrydowych. Podnoszą również funkcjonalność oraz poziom bezpieczeństwa, są to:

- ✓ **NVR-PRO** – aplikacja rejestrująca obraz i dźwięk z maks. 64 kanałów, przeznaczona do zarządzania wszystkimi urządzeniami systemu **iP-pro** oraz rejestratorami cyfrowymi **MY-DVR**.
- ✓ **NETSTATION** – profesjonalna platforma, dla rozwiązań zaawansowanych.

Rejestratory wykorzystujące platformę Netstation, przeznaczone są do pracy z kamerami IP, transponderami 1-kanałowymi systemu **iP-pro** oraz dedykowanymi kamerami megapikselowymi.

NADAJNIKI • STACJE MONITORINGU RADIOWEGO • REPEATERY

150zł

NADAJNIKI

WIOSENNA PROMOCJA!*

Na nadajniki pracujące ze stacjami VISONIC, KP, NOKTON.

* promocja trwa do 15.05.2008r. i dotyczy tylko nowych klientów!

ZAPRASZAMY RÓWNIEŻ DO ODWIEDZENIA NASZEJ STRONY INTERNETOWEJ

www.messer.com.pl

C & C

TKH
GROUP

SHC-735



SAMSUNG

TECHWIN

... znakomite obrazy



- › Rozdzielczość 560/700 TVL (kolor/bw)
- › Czułość 0.0001 Lux (tryb sens-up)
- › WDR (128x)
- › Sterowanie OSD (RS-485)
- › Cyfrowa stabilizacja obrazu (DIS)

Autoryzowany dystrybutor Samsung Techwin w Polsce:
C&C Partners - Leszno

www.samsungcctv.ccpartners.pl

Inteligentne czujki serii Professional z wielopunktowym antymaskingiem

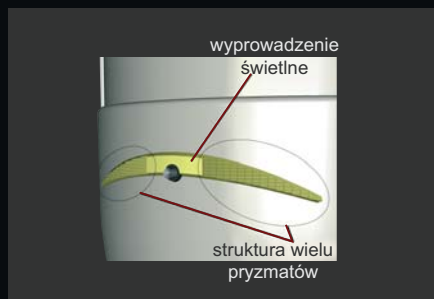
Na rynku systemów zabezpieczeń oferowane są wszelkiego rodzaju rozwiązania systemów alarmowych z całego świata. Trudno jest jednoznacznie stwierdzić, który system jest najlepszy, gdyż zależy to w dużej mierze od ich przeznaczenia. W przypadku czujek dostępnych na rynku często decydującym kryterium jest cena. Niestety wybór zazwyczaj odbywa się kosztem funkcjonalności. Czy czujki zbudowane na bazie najtańszych komponentów powinny wchodzić w skład systemu bezpieczeństwa? Naszym zdaniem w systemach bezpieczeństwa nie ma miejsca na tego typu kompromisy



Rys. 1. Technologia Bogunce-Beck. Emiter IR wytwarza wokół czujki „bańkę” (IR bubble)



Rys. 2. Przekrój czujki z dwoma fotodiodami



Rys. 3. Technologia Retro Reflektor. Struktura wielu pryzmatów (multi-prismatic structure) wbudowana w moduł świetlny czujki z zaznaczonym wyprowadzeniem świetlnym (light pipe)

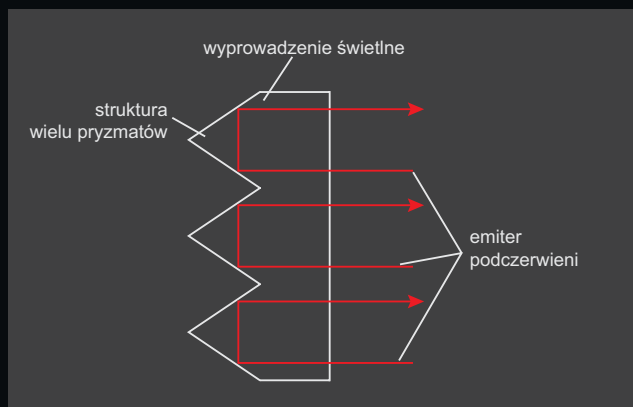
Firma Bosch Security Systems znana jest na rynku systemów zabezpieczeń przede wszystkim z niezawodnych produktów i rozwiązań o najwyższej jakości. Dzięki swojemu Centrum Badawczo-Rozwojowemu tworzy i wprowadza najnowsze technologie, często wyznaczając nowe standardy na rynku security.

Inteligentne czujki z serii Professional są jednym z efektów pracy Centrum Badawczo-Rozwojowego. Powiększają one rodzinę produktów SSWiN o kolejne dwa nowe modele czujek z wielopunktowym antymaskingiem. Poniżej spróbujemy wyjaśnić, na czym polega ich szczególna inteligencja.

Już od pewnego czasu dostępne w ofercie czujki profesjonalne zostały bardzo dobrze przyjęte zarówno na polskim rynku, jak i na całym świecie. Konsumenci docenili zaawansowane i opatentowane rozwiązania zastosowane w czujkach firmy

Bosch. Czujki te mają aż pięć czujników: detektor PIR dalekiego zasięgu, detektor PIR średniego i bliskiego zasięgu, czujnik mikrofalowy, czujnik światła białego oraz czujnik temperatury. Wszystkie czujniki zostały zintegrowane w jednej czujce. Dzięki opatentowanej technologii *Sensor Data Fusion* (SDF), która polega na inteligentnym przetwarzaniu sygnałów ze wszystkich detektorów przez zastosowany w czujce mikrokontroler, zaimplementowane w nim oprogramowanie przetwarza wszystkie sygnały z czujników na sygnały





Rys. 4. Zasada działania czujki w czasie jej normalnej pracy. Struktura wielu pryzmatów w pełni odbija promienie wytworzone przez emiter IR

stref wykrywania. 86 stref rozmieszczonych nad 11 stałymi kurtynami detekcyjnymi eliminuje występowanie stref martwych.

Wbudowany czujnik światła białego uniemożliwia zakłócenie pracy detektorów PIR bez względu na natężenie i charakterystykę czasową światła białego. Funkcja aktywnej redukcji światła białego eliminuje taki problem, jak przejeżdżające nocą pojazdy lub inne ruchome źródła światła.

Funkcja dynamicznej kompensacji temperatury, dzięki wbudowanemu czujnikowi temperatury, pozwala w obiekcie na zmianę czułości detektorów PIR w krytycznych zakresach temperaturowych, tj. zbliżonych do temperatury ciała człowieka.

Dzięki tak wielu informacjom pochodzącym z pięciu detektorów mikrokontroler eliminuje ryzyko występowania fałszywych alarmów. Wbudowana inteligencja wyznacza nowe standardy w systemach alarmowych.

Wielopunktowy antymasking

Najnowsze czujki z serii Professional poszerzyły ofertę produktową firmy Bosch o kolejne dwa modele z funkcją antymaskingu. Polega on na wykrywaniu prób maskowania lub blokowania czujki materiałami pochłaniającymi promieniowanie podczerwone.

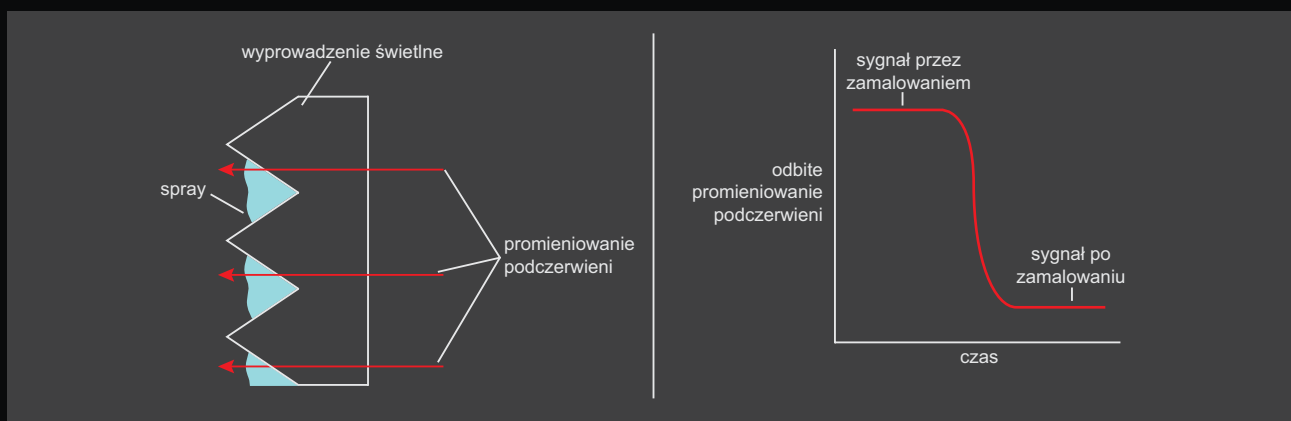
Jako pierwsza czujka na świecie spełnia wszystkie wytyczne najnowszej normy europejskiej EN50131. Aby czujka mogła spełniać wszystkie tak surowe wymagania, musi być odporna i rozpoznawać próby maskowania za pomocą takich materiałów, jak:

- czarny papier,
- blacha aluminiowa,
- warstwa akrylowa,
- biała pianka poliestrowa,
- przezroczysta taśma samoprzylepna,
- przezroczysty spray,
- lakier,
- rozpylona farba.

System wielopunktowego antymaskingu łączy w sobie trzy aktywne technologie wykrywania maskowania. To dzięki zastosowaniu w czujce czterech aktywnych emiterów podczerwieni i trzech fotodiod podczerwieni informacja o próbie maskowania czujki wysyłana jest do centrali alarmowej, która z kolei powiadamia o problemie właściwe osoby.

cyfrowe i przetwarza je według zaawansowanego algorytmu. Po takiej obróbce sygnałów podejmowana jest decyzja o alarmie.

Czujka wyposażona w optykę *TriFocus* posiada trzy ogniskowe o trzech różnych zasięgach: dalekiego zasięgu, średniego zasięgu i strefy podejścia. Przy montażu na wysokości od 2 do 3 m optyka gwarantuje pełne pokrycie strefy chronionej bez konieczności jakiegokolwiek regulacji. Takie rozwiązanie zapewnia bardzo dużą gęstość



Rys. 5. Zasada działania czujki, gdy zostanie ona zamalowana sprayem. Pokryte pryzmaty przepuszczają promieniowanie wytworzone przez emiter IR

Bogunce-Beck

Technologia Bogunce-Beck polega na wytworzeniu wokół czujki „bańki” podczerwieni (IR) rozciągającej się na ok. 30 cm. Bańkę promieniowania wytwarza wbudowany emiter, tak jak zostało to pokazane na Rys. 1.

Jeżeli czujka została zasłonięta, to odbite promieniowanie IR odbierane jest przez dwie fotodiody wewnątrz czujki. Fotodiody wykrywają zwiększony poziom energii IR i wysyłają informację o zasłonięciu czujnika do systemu (Rys. 2).

Retro Reflektor

Opatentowana technologia Retro Reflektor polega na odbijaniu promieniowania podczerwieni emitowanego przez emiter IR przez specjalną strukturę wielu pryzmatów. Struktura wielu pryzmatów została wbudowana w moduł świetlny czujki.

Podczas normalnej pracy struktura wielu pryzmatów w całości odbija promienie IR i nie przepuszcza ich (tak, jak widać to na Rys. 4).

Gdy czujka zostanie zamalowana, struktura pryzmatów straci swoje właściwości fizyczne i padające promienie nie będą odbijane. Przepuszczone promieniowanie będzie padać na fotodiode, która spowoduje wygenerowanie alarmu oznaczającego zamalowanie sprayem czujki.

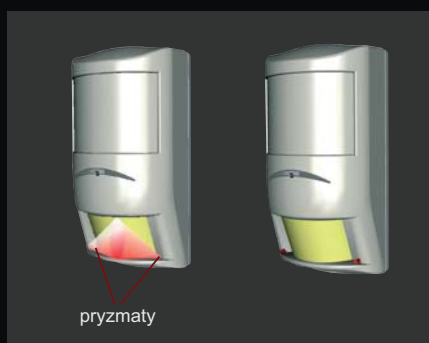
Through-the-Lens

Technologia *Through-the-Lens* wykrywa próby bezpośredniego zamaskowania soczewki, czyli sytuacje, gdy materiał typu taśma klejąca zostanie umieszczony na soczewce. Czujka emituje promieniowanie podczerwieni, które poprzez dwa pryzmaty znajdujące się u dołu czujki, odbija tę energię z powrotem na powierzchnię soczewki.

Jeżeli soczewka została zamaskowana (zaklejona), wtedy fotodioda wewnątrz czujki **rejestruje** spadek poziomu energii odbitej od pryzmatów. Wówczas czujka powiadamia centralę o próbie maskowania.



Rys. 6. Przekrój czujki z zaznaczonym emiterem podczerwieni, fotodiody podczerwieni, strukturą wielu pryzmatów i wyprowadzeniem świetlnym



Rys. 7. Dwa odbijające pryzmaty umieszczone na dole czujki



Rys. 8. Przekrój czujki z zaznaczoną fotodiody

Dzięki trzem różnym opatentowanym technologiom system wielopunktowego antymaskingu zastosowany w czujkach serii Professional zabezpiecza czujkę przed wszelkiego rodzaju próbami maskowania. Dzięki temu czujka potrafi sama nadzorować swoją pracę. Wbudowany mikrokontroler oraz oprogramowanie powodują, że czujka ma swoją wewnętrzną inteligencję, co pozwala na analizowanie warunków panujących w otoczeniu i na podejmowanie na tej podstawie decyzji o wygenerowaniu alarmu. Zbudowana na bazie najwyższej klasy komponentów czujka gwarantuje stabilną pracę. Dwumodułowa konstrukcja, wbudowane przełączniki DIP oraz poziomicą pęcherzykowa ułatwiają i przyspieszają instalację nawet o 25%.

Czujki serii Professional to najbardziej zaawansowane technologicznie detektory, zaprojektowane na podstawie najnowszych badań Centrum Badań i Rozwoju firmy Bosch. Zastosowane technologie powodują, że czujki gwarantują najwyższą w swojej klasie skuteczność wykrywania, a przy tym największą odporność na fałszywe alarmy. Ich konstrukcja i funkcjonalność wyznaczają nowe standardy w systemach alarmowych.

KRZYSZTOF KOSTECKI
BOSCH SECURITY SYSTEMS

SECUREX 2008

pawilon 3A parter
stoisko nr 50

firma

ATLine®

kompleksowe zabezpieczanie obiektów



15 LAT
DOŚWIADCZENIA

BEZPIECZEŃSTWO W KAŻDYCH WARUNKACH

PROJEKTOWANIE... KOMPLEKSOWYCH DOKUMENTACJI

- TECHNICZNYCH, ARCHITEKTONICZNO - BUDOWLANYCH
WRAZ Z NIEZBĘDNymi BRANŻAMI SPECJALISTYCZNYMI
OBIEKTÓW BIUROWYCH I PRZEMYSŁOWYCH
- INNOWACYJNYCH SYSTEMÓW OCHRONY
- TELETECHNICZNYCH, ELEKTRYCZNYCH
I AUTOMATYKI PRZEMYSŁOWEJ

WYKONYWANIE...

ZAAWANSOWANYCH TECHNOLOGICZNE
SYSTEMÓW OCHRONY I BEZPIECZEŃSTWA

SPRZEDAŻ...

NOWOCZESNYCH SYSTEMÓW OCHRONY



SERIA CZUJEK CYFROWYCH DSC



Precyzyjna cyfrowa technologia opracowana przez firmę DSC pozwala wykryć intruza, redukując tym samym ilość fałszywych alarmów do minimum.

Na terenie prywatnych posiadłości, jak i w budynkach biurowych, seria czujek LC usprawnia system alarmowy, zapewniając niezawodność działania również podczas najbardziej wymyślnych prób włamania.

Dodatkowo smukła linia obudowy, odporność na zwierzęta, prosta instalacja, różne sposoby montażu, odporność na światło białe oraz wiele innych właściwości powoduje, że nowa seria czujek jest niezwykle atrakcyjnym produktem.

Wyłączny dystrybutor w Polsce:



AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

**LC-100-PI Czujka PIR odporna na zwierzęta**

Wymiary	92 mm x 62,5 mm x 40 mm
Waga	61 g
Metoda detekcji	czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie	od 8,2 do 16 V=
Pobór prądu (czuwanie)	8 mA (± 5%)
Pobór prądu (działanie)	10 mA (± 5%)
Sabotaż: styk NC	0,1 A @ 28 V=
Odporność na zakłócenia:	
• radiowe	10 V/m 80-1000 MHz
• statyczne	8 kV kontakt, 15 kV powietrze
• przepięciowe	2,4 kV @ 1,2 J

**LC-101-CAM Czujka PIR z kamerą (czarno-biała/kolorowa), odporna na zwierzęta**

Wymiary	116 mm x 62,5 mm x 40 mm
Waga	112 g
Metoda detekcji	czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie	od 8,2 do 16 V=
Pobór prądu (czarno-biała)	115 mA
Pobór prądu (kolorowa)	150 mA
Sabotaż: styk NC	0,1 A @ 28 V=
Odporność na zakłócenia:	
• radiowe	10 V/m 80-1000 MHz
• statyczne	8 kV kontakt, 15 kV powietrze
• przepięciowe	2,4 kV @ 1,2 J

**LC-102-PIGBSS Czujka PIR oraz zbita szyby, odporna na zwierzęta**

Wymiary	118 mm x 62,5 mm x 41 mm
Waga	83 g
Metoda detekcji	czteroelementowy pasywny czujnik podczerwieni (Quad PIR)
Zasilanie	od 8,2 do 16 V=
Pobór prądu (czuwanie)	16,5 mA
Pobór prądu (działanie)	22 mA
Sabotaż: Styk NC	0,1 A @ 28 V=
Odporność na zakłócenia:	
• radiowe	10 V/m 80-1000 MHz
• statyczne	8 kV kontakt, 15 kV powietrze
• przepięciowe	2,4 kV @ 1,2 J

**LC-103-PIMSK Czujka PIR + mikrofala z antymaskingiem, odporna na zwierzęta**

Wymiary	118 mm x 62,5 mm x 41 mm
Waga	102 g
Metoda detekcji	czteroelementowy pasywny czujnik podczerwieni (Quad PIR) + mikrofala Doppler
Zasilanie	od 8,2 do 16 V=
Pobór prądu (czuwanie)	18 mA
Pobór prądu (działanie)	25,5 mA
Sabotaż: styk NC	0,1 A @ 28 V=
Odporność na zakłócenia:	
• radiowe	10 V/m 80-1000 MHz
• statyczne	8 kV kontakt, 15 kV powietrze
• przepięciowe	2,4 kV @ 1,2 J

**LC-104-PIMW Czujka PIR + mikrofala**

Wymiary	118 mm x 62,5 mm x 41 mm
Waga	102 g
Metoda detekcji	czteroelementowy pasywny czujnik podczerwieni (Quad PIR) + mikrofala Doppler
Zasilanie	od 8,2 do 16 V=
Pobór prądu (czuwanie)	18 mA
Pobór prądu (działanie)	25,5 mA
Sabotaż: styk NC	0,1 A @ 28 V=
Odporność na zakłócenia:	
• radiowe	10 V/m 80-1000 MHz
• statyczne	8 kV kontakt, 15 kV powietrze
• przepięciowe	2,4 kV @ 1,2 J

**LC-105-DGB Czujka zbita szyby**

Wymiary	79 mm x 48 mm x 21 mm
Waga	40 g
Zasięg	10 m max
Zasilanie	od 9 do 16 V=
Pobór prądu (czuwanie)	15 mA @ 12 V=
Pobór prądu (działanie)	40 mA @ 24 V=
Sabotaż: styk NC	50 mA @ 24 V=
Odporność na zakłócenia:	
• radiowe	10 V/m 80-1000 MHz
• statyczne	8 kV kontakt, 15 kV powietrze
• przepięciowe	2,4 kV @ 1,2 J

Wielowiązkowe

bariery podczerwieni REDNET



Obecne na naszym rynku 16-wiązkowe bariery Rednet stanowią wyjątkowo interesujące rozwiązanie dla ochrony obwodowej. O wyjątkowości tego rozwiązania stanowi duża liczba wiązek tworząca gęstą sieć o wysokości 175 cm, zoptymalizowaną do tego typu ochrony. Zastosowanie takiej koncepcji w systemie ułatwia projektowanie i wykonanie niezwykle skutecznej i bezpiecznej instalacji ochrony obwodowej

Firma Optex, znana ze swoich wysokiej jakości produktów z zakresu zabezpieczania chronionych obszarów, posiada w swojej ofercie urządzenia, które powstały dzięki nowatorskiemu podejściu do wielu zagadnień detekcji. Znane w branży zabezpieczeń bariery AX czy czujki zewnętrzne serii VX i BX cieszą się renomą wśród instalatorów i użytkowników. Czujka Rednet to produkt bardzo specyficzny, adresowany do klientów o bardzo wyszukanych wymaganiach dotyczących poziomu bezpieczeństwa systemu ochrony obwodowej.

Urządzenia zostały zaprojektowane do pracy w obudowach kolumnowych (typu wieża) o wysokości 175 cm. Jest to typowa wielkość dla zabezpieczeń obwodowych instalowanych w słupkach. Co prawda rekord świata w skoku wzwyż wynosi 2,45 m (Javier Sotomayor, Kuba), ale tak wysoko skacze jedynie kilku ludzi na świecie i jest mało prawdopodobne, aby chcieli oni przeskakiwać zabezpieczenia chronionych obiektów. Tym, co wyróżnia czujkę Rednet na tle rozwiązań konkurencyjnych, jest aż 16 wiązek pomiędzy nadajnikiem i odbiornikiem tworzących sieć, jak na Rys. 1. Dzięki temu niemal każdy obiekt przemieszczający się pomiędzy nadajnikiem i odbiornikiem zostanie wykryty. Algorytm aktywujący stan alarmowy analizuje zarejestrowane przecięcia wiązek. Wielokryteriowe przetwarzanie informacji – ważna jest zarówno liczba przeciętych wiązek, jak i ich rozmieszczenie oraz czas przecięcia – pozwala na stosunkowo dokładne oszacowanie wielkości obiektu oraz prędkości jego przemieszczania. Jeśli obserwowany obiekt spełnia kryteria związane z ruchem człowieka, urządzenie inicjuje stan alarmowy.

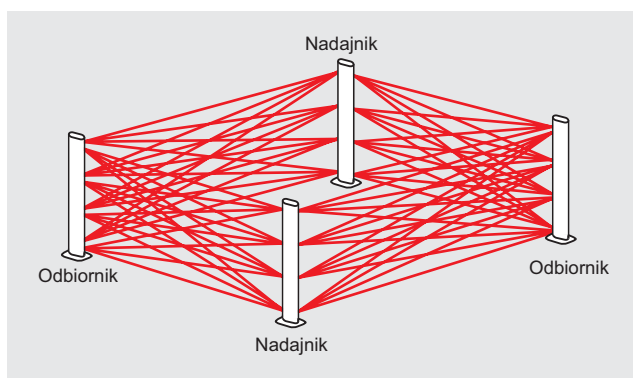
Kolejną wyjątkową cechą tego systemu detekcji, wyróżniającą go spośród innych dostępnych na rynku jest fakt, że analizie poddane są wszystkie wiązki pomiędzy częścią nadawczą i odbiorczą urządzenia. W przypadku innych systemów, zazwyczaj mamy do czynienia z zestawem dwóch albo, trzech urządzeń, które zabezpieczają pas o wysokości 30–40 cm, nie współpracując ze sobą. Można wyobrazić sobie sytuację (jak na Rys. 2), w której intruz spowoduje przecięcie dwóch wiązek, ale nie zostanie wykryty. Dzięki technologii detekcji zastosowanej w czujce Rednet taka sytuacja nie będzie miała miejsca.

Geometria układów optycznych powoduje, że czujka może funkcjonować poprawnie w określonym zakresie odległości pomiędzy nadajnikiem i odbiornikiem. Soczewkowo-zwierciadłany układ optyczny głowicy roboczej posiada swoją określoną strefę rozproszenia wiązki. Przeciwnie część czujki musi cała

znajdować się w tej strefie rozproszenia. Ulokowanie jej bliżej lub dalej powodować będzie zakłócenia w pracy detektora w postaci fałszywych alarmów, ponieważ w takiej sytuacji nie będzie możliwe obieranie wszystkich 16 wiązek. Dlatego urządzenia Rednet proponowane są dla dedykowanych zakresów odległości w trzech wariantach: 10–25 m, 25–75 m oraz 75–150 m.

Poza wyszukanyymi technologiami detekcji czujki Rednet mają szereg cech, które służą ułatwieniu pracy instalatora. Czujka jest dostarczana w pełni okablowana. Zestaw zawiera wszystkie elementy czujki oraz wszystkie akcesoria niezbędne do montażu w obudowie oraz do prawidłowego dostrojenia. W zestawie znajduje się między innymi zestaw płytek maskujących i tester dostrojenia. Dostrojenie czujki nie jest

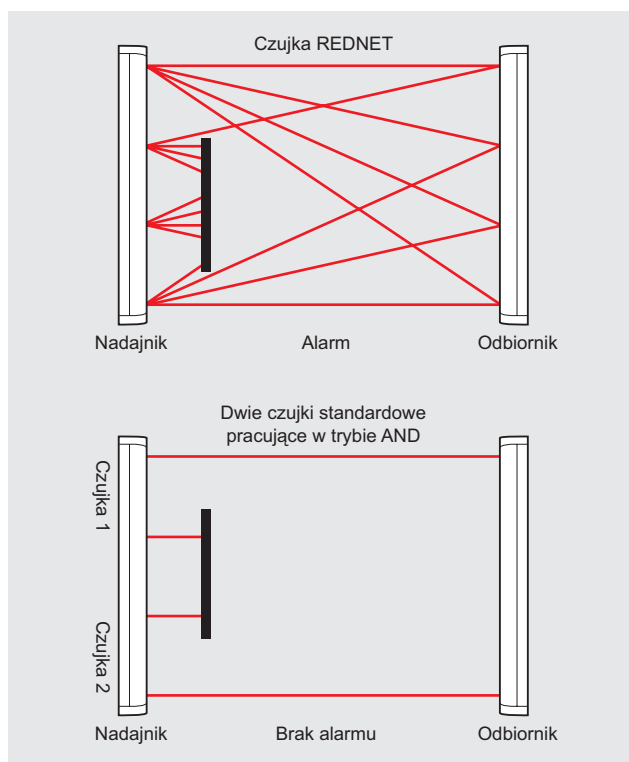




Rys. 1. Rozmieszczenie wiązek podczerwieni w czujce REDNET.

zadaniem prostym i wymaga od instalatora nieco wprawy i cierpliwości. Co prawda nadajnik i odbiornik posiadają tylko po cztery głowice robocze, a mechanizm regulujący ich położenie jest wyjątkowo prostej konstrukcji, lecz trudność polega głównie na konieczności uzyskania tej samej wysokiej jakości dostrojenia dla wszystkich 16 wiązek.

Kolejnym istotnym udogodnieniem są podgrzewacze zintegrowane w obudowie głowic roboczych. Instalator czy projektant nie musi pamiętać o tym, aby dodać te elementy do projektu. Poza tym czujkę wyposażono w wyjście sygnalizujące wyłączenie czujki na skutek działania czynników środowiskowych (np. szronu, mgły). Algorytmy analizujące natężenie promieniowania podczerwonego docierającego do odbiornika służą nie tylko do zmiany stopnia wzmocnienia odbieranych sygnałów – Automatyczna Regulacja Wzmocnienia (ang. AGC) – ale są również w stanie ocenić, czy spadek natężenia sygnału w odbiorniku związany jest ze zmianą warun-



Rys. 2. Przykład różnic w sposobie detekcji pomiędzy czujką REDNET a dwiema osobnymi czujkami pracującymi w trybie iloczynu logicznego dwu lub więcej wiązek.

ków środowiskowych. Jeśli poziom odbieranego sygnału nie zapewnia już prawidłowej pracy bariery, aktywowane jest wyjście sabotażu środowiskowego. Gwoli przypomnienia, Rednet, jak wszystkie inne bariery firmy Optex, zachowuje pełną stabilność przy 99-procentowym blokowaniu wiązki, co jest bardzo wysokim osiągnięciem wobec tego typu urządzeń i świadczy o wyjątkowych walorach użytkowych opisywanych rozwiązań.

Do zastosowania z czujkami Rednet są dostępne dedykowane obudowy typu „wieża”. Występują one w dwóch rodzajach: do montażu na ścianie (jednostronna) oraz wolnostojąca (dwustronna). Aby zmontować gotowe do pracy urządzenie, wystarczy zainstalować w wybranej obudowie okablowane już moduły czujki.

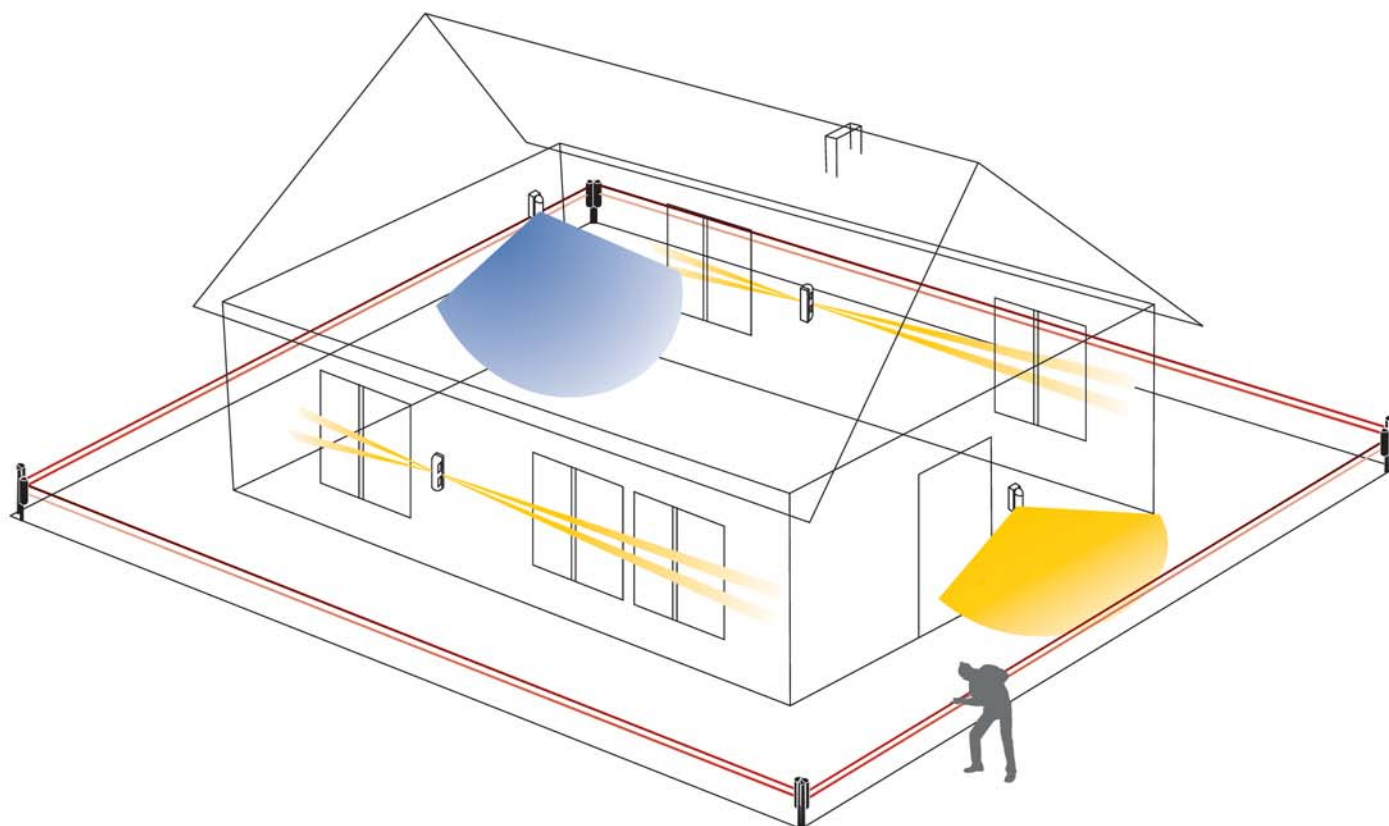
Podsumowując, czujki Rednet oferują niezwykle wysoki stopień ochrony dzięki wielu czynnikom, m.in. dużej liczbie wiązek o wyjątkowym ułożeniu oraz zaawansowanym funkcjom i algorytmom zapewniającym wysoką jakość detekcji i odporność na fałszywe alarmy. Uzupełnione o udogodnienia ułatwiające zastosowanie barier w aplikacjach wymagających ochrony obwodowej o dużej wysokości, stanowią interesującą alternatywę dla standardowych rozwiązań w tym zakresie. Instalator nie musi martwić się o dobór odpowiedniej liczby czujników i akcesoriów (podgrzewacze, termostaty itp.) oraz zmontowanie tych wszystkich elementów w jedną całość. Wybierając Rednet instalator otrzymuje produkt kompletny, który po zamontowaniu w jednej z dwóch dedykowanych obudów jest gotowy do użycia. Minimalizując ryzyko popełnienia błędu, użytkownik otrzymuje wysoki poziom ochrony dla swoich klientów oraz pewność stabilnej, długotrwałej pracy urządzenia.

Bariery Rednet oraz pozostałe produkty firmy Optex są do nabycia w sieci handlowej firmy AAT-T – dystrybutora firmy Optex.

JAROSŁAW GIBAS
OPTEX SECURITY



TRÓJSTREFOWA ochrona



Firma Optex stworzyła niezawodny, kompleksowy system urządzeń, wykrywających wtargnięcie intruza na teren obiektu chronionego, jak i na jego obrzeża. System składa się z trzech stref ochrony obiektu:

• STREFA OCHRONY WEWNĘTRZNEJ • STREFA OCHRONY ZEWNĘTRZNEJ • STREFA OCHRONY OBWODOWEJ

Chroni pomieszczenia obiektu.

W tej strefie zastosowanie znajdują pasywne czujki podczerwieni, czujki dualne (PIR + mikrofala) oraz bariery podczerwieni.

- RX-40QZ/40PT
- MX-40QZ/50QZ
- CX-502AM
- CX-702
- FX-360
- SX-360Z
- AX-100S/100SR

Chroni elewację budynku oraz obszar pomiędzy ogrodzeniem a obiektem.

W tej strefie zastosowanie znajdują pasywne czujki podczerwieni oraz bariery podczerwieni.

- LX-402
- LX-802N
- VX-402/402REC
- BX-80N
- BX-100PLUS

Chroni obwód terenu wokół budynku.

W tej strefie zastosowanie znajdują cyfrowe i analogowe bariery podczerwieni krótkiego i dalekiego zasięgu.

- AX-70TN/130TN/200TN
- AX-100TF/200TF
- AX-250PLUS/500PLUS
- AX-350TF/650TF
- AX-350/650DH MK III

Te trzy poziomy bezpieczeństwa zapewniają pewną ochronę obiektu i polepszają działania prewencyjne.

Specyfikacja techniczna

OCHRONA WEWNĘTRZNA

	RX-40QZ/40PT	MX-40QZ	MX-50QZ	CX-502AM	CX-702	FX-360	SX-360Z	AX-100S/100SR
								
W domach	✓	✓	✓	-	-	✓	-	✓
W małych biurach	✓	✓	✓	-	-	✓	✓	✓
W dużych biurach	-	-	✓	✓	✓	-	✓	-
W pomieszczeniach przemysłowych	-	-	-	✓	✓	-	-	-
Zasięg detekcji	12x12 m	12x12 m	15x15 m	15x15 m	21x21 m 45x2,4 m	Ø8 - 12 m, kąt 360°	Ø18 m, kąt 360°	30 m
Zasilanie	9,5 - 16 V=	9,5 - 16 V=	9,5 - 16 V=	9 - 18 V=	9,5 - 16 V=	9,5 - 18 V=	6 - 18 V=	8 - 18 V=
Pobór prądu	11 mA maks.	18 mA maks.	20 mA maks.	19 mA maks.	11 mA	18 mA maks.	18 mA maks.	52 mA maks. odbiornik+nadajnik
Temperatura pracy	-20°C - +50°C	-10°C - +55°C	-10°C - +55°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C

OCHRONA ZEWNĘTRZNA

	LX-402	LX-802N	VX-402	VX-402REC	BX-80N	BX-100PLUS
						
W domach	✓	✓	✓	✓	✓	✓
W małych biurach	✓	✓	✓	✓	✓	✓
W dużych biurach	-	✓	✓	✓	✓	-
W pomieszczeniach przemysłowych	-	-	✓	✓	✓	-
Współpraca z CCTV	✓	✓	✓	✓	✓	-
Zasięg detekcji	12 x 15 m	24 x 2 m	12 m, kąt 90°	12 m, kąt 90°	24 m (po 12 m na każdą stronę)	30 m
Zasilanie	10,8 - 13,2 V=	10,8 - 13,2 V=	9,5 - 18 V=	9,5 - 18 V=	10 - 28 V=	10,5 - 28 V=
Pobór prądu	25 mA maks.	25 mA maks.	NC : 28 mA maks. NO : 35 mA maks.	NC : 180 mA maks. NO : 200 mA maks.	38 mA maks.	75 mA maks. odbiornik+nadajnik
Stopień ochrony obudowy	IP54	IP54	IP54	IP54	IP55	IP54
Temperatura pracy	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-20°C - +50°C	-35°C - +55°C

OCHRONA OBWODOWA

	AX-70TN/AX-130TN	AX-200TN	AX-100TF/AX-200TF	AX-250PLUS/AX-500PLUS	AX-350TF/AX-650TF	AX-350DH MRIB/AX-650DH
						
W domach	✓	✓	-	-	-	-
W małych biurach	✓	✓	✓	-	-	-
W dużych biurach	✓	✓	✓	✓	✓	✓
W pomieszczeniach przemysłowych	-	-	✓	✓	✓	✓
Zasięg detekcji	20 m/40 m	60 m	30 m/60 m	75 m/150 m	100 m/200 m	100 m/200 m
Zasilanie	10,5 - 28 V=	10,5 - 28 V=	10,5 - 28 V=	10,5 - 30 V=	10,5 - 30 V=	10,5 - 30 V=
Pobór prądu (odbiornik + nadajnik)	38 mA maks./41 mA maks.	45 mA maks.	44 mA maks./48 mA maks.	50 mA maks.	60 mA maks./62 mA maks.	105 mA maks./110 mA maks.
Stopień ochrony obudowy	IP65	IP65	IP65	IP54	IP54	IP65
Temperatura pracy	-35°C - +60°C	-35°C - +60°C	-35°C - +60°C	-25°C - +55°C	-35°C - +60°C	-35°C - +60°C



Obiektywy

które widzą więcej



computar®

Computar - synonim japońskich obiektywów, najczęściej stosowanych w systemach CCTV na całym świecie.

Funkcjonalność oferowanych obiektywów Computar pozwala na dostosowanie wybranego modelu obiektywu w dowolnej aplikacji - np. różnorodne systemy dozoru, specjalistyczne maszyny przemysłowe.

Doskonała i sprawdzona jakość obiektywów znacząco wpływa na zwiększenie efektywności systemów, w których są stosowane.

Wszystkie obiektywy Computar objęte są 3-letnią gwarancją.



Obiektywy w systemach telewizji dozorowej

DOBÓR OBIEKTYWU – PODSTAWOWE POJĘCIA

computar®



Wybór prawidłowego typu obiektywu jest tak samo ważny, jak wybór kamery. Zła jakość obiektywu może znacznie obniżyć ogólną jakość funkcjonowania systemu

Dokonując wyboru odpowiedniego obiektywu, należy rozumieć znaczenie podstawowych terminów:

Ogniskowa – odległość, w jakiej od centrum optycznego obiektywu powstaje obraz obiektu położonego w nieskończoności. Jest ona mierzona w milimetrach. Dla danego rozmiaru przetwornika i danej ogniskowej można wyliczyć kąt widzenia kamery. Zależność między ogniskową a kątem widzenia kamery jest odwrotnie proporcjonalna.

Przysłona – mechanizm regulacji otworu względnego (apertury), zmieniający ilość światła przechodzącego przez obiektyw i padającego na przetwornik obrazu kamery telewizji dozorowej. Obiektywy o stałej przysłonie są oznaczane jako „no IRIS” (bez przysłony).

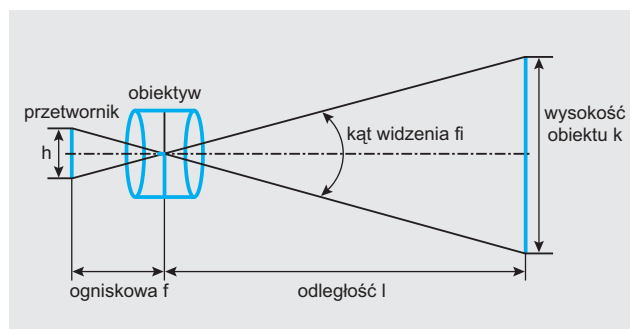
Apertura (jasność) obiektywu (F) – wskaźnik teoretycznej zdolności przepuszczania światła obiektywu. Jest określany skalą F. Szereg F to: 1; 1,4; 2; 2,8; 4; 5,6; 8; 11; 16; 22; 32; 45; 64 itd. Ze wzrostem liczby F maleje ilość światła przepuszczanego przez obiektyw. W tabeli podano ilości światła przepuszczanego przy różnych wartościach przysłony.

Jeśli przysłona obiektywu pozwala na całkowite zamknięcie, to liczba F jest równa nieskończoności (może być to oznaczane terminem *closed* – zamknięta). Najczęściej podawane są dwie wartości liczby F. Pierwsza z nich określa maksymalne otwarcie przysłony, a druga minimalne.

Liczba transmisyjna obiektywu (T) – wskaźnik rzeczywistej zdolności przepuszczania światła przez obiektyw. Skala ta pozwala na bezwzględną ocenę jakości obiektywu, gdyż uwzględnia wpływ np. gatunku szkła na przepuszczanie różnych częstotliwości światła.

Inne ważne parametry to: głębia ostrości, maksymalna rozdzielczość, ostrość i kontrastowość otrzymywanych obrazów, korekcja kolorów związana z aberracją chromatyczną.

Typy mocowań obiektywów – spotykane są dwa: CS oraz C. Odległość powierzchni przetwornika i płaszczyzny mocowania obiektywu wynosi 12,5 mm dla obiektywów CS i 17,526 mm dla obiektywów C. Gwint o mniejszej średnicy występuje w kamerach płytkowych.



Rys. 1. Wygląd układu optycznego obiekt-obiektyw-przetwornik obrazowy i związane z nim parametry

Liczba F	Ilość przepuszczanego światła
1,0	100%
1,4	50%
2,0	25%
2,8	12,5%
4,0	6,3%
5,6	3,13%
8,0	1,6%
16	0,8%

Tab. 1. Teoretyczna zależność ilości przepuszczanego światła od liczby F

Wielkości obiektywu, a wielkość przetwornika

Wielkość obrazu, jaki może być wytworzony przez obiektyw, podaje się w calach, podobnie jak wielkość przetwornika. Producenci podają największy format przetwornika, z jakim dany obiektyw może współpracować. Do wielkości przetwornika musi być dopasowany obiektyw, przy czym zawsze można stosować większy obiektyw do kamery z mniejszym przetwornikiem, co w niektórych sytuacjach może być korzystne, jako że pozwala na zmniejszenie zniekształceń obrazu (zniekształcenia obiektywu zwiększają się wraz z oddaleniem się od osi). Przy tym samym obiektywie mniejszy przetwornik spowoduje wyświetlenie mniejszego fragmentu obserwowanego obiektu.

Zasadnicza kwestia – odpowiedni dobór ogniskowej

Dla danego rozmiaru przetwornika i danej ogniskowej można wyliczyć kąt widzenia kamery. Zależność między ogniskową a kątem widzenia kamery jest odwrotnie proporcjonalna. Należy zauważyć, iż kąt widzenia w płaszczyźnie poziomej wynoszący 30 stopni jest podobny do kąta widzenia człowieka. Okazuje się, że taki kąt jest osiągnięty wtedy, gdy ogniskowa jest równa wymiarowi przetwornika.

Znając format przetwornika, odległość od obserwowanego przedmiotu oraz jego rozmiary, możemy wyliczyć, jaka będzie potrzebna ogniskowa, a także jaki będzie kąt widzenia kamery z obiektywem o takiej ogniskowej. Ze względu na prostokątny kształt przetwornika obliczenia należy wykonać zarówno w płaszczyźnie pionowej, jak i poziomej.

Doboru obiektywu można dokonać, używając wzorów, kalkulatorów, wykresów oraz specjalnej lunetki zwanej *view finder*. W razie możliwości należy także przeprowadzić próby terenowe, podczas których można dobrać spośród wielu obiektywów te, które najlepiej spełnią swe zadanie.

Dobór ogniskowej na podstawie wykresów sprowadza się do odczytania wartości ogniskowej w zależności od szerokości i odległości od obiektu oraz od formatu przetwornika. Ich wadą jest mała dokładność, spowodowana brakiem wykresów dla każdego możliwego przypadku.

W przypadku użycia lunetki ustawia się ją w miejscu, gdzie ma być zainstalowana kamera, po czym dokonuje się regulacji pierścieniami lunetki do momentu osiągnięcia pożądanego zakresu obserwacji. Wtedy należy dokonać odczytu wartości szukanej ogniskowej.

Z kolei kalkulatory mają postać dwóch współosiowych kół z naniesionymi liczbami. Ustawiając odległość i wielkość obiektu oraz wybierając format przetwornika, można z nich odczytać wartość wymaganej ogniskowej.

Ogniskową można wyliczyć samodzielnie, korzystając ze wzorów bazujących na podstawowych i dobrze znanych zależnościach trygonometrycznych. W obliczeniach wykorzystujemy następujące wzory do wyznaczania kątów:

$$\text{– kąt widzenia w płaszczyźnie pionowej } \Phi_h = 2 \arctan(h/2f) = 2 \arctan(k/2l)$$

$$\text{– kąt widzenia w płaszczyźnie pionowej } \Phi_v = 2 \arctan(v/2f) = 2 \arctan(m/2l)$$

(na przykład dla przetwornika 1/4" o wymiarach 2,7 x 3,6 mm, czyli o przekątnej 4 mm, i obiektywu o ogniskowej 3,6 mm kąt widzenia pionowy i poziomy wynoszą odpowiednio:

$$\text{– kąt widzenia pionowy } \Phi_h = 2 \cdot \arctan(2,7/7,2) = 2 \cdot \arctan(0,375) = 41 \text{ stopni}$$

$$\text{– kąt widzenia poziomy } \Phi_v = 2 \cdot \arctan(3,6/7,2) = 2 \cdot \arctan(0,5) = 52 \text{ stopnie}$$

oraz wzory do obliczania pola widzenia:

$$\text{– wysokość pola widzenia } k = h \cdot l / f$$

$$\text{– szerokość pola widzenia } m = v \cdot l / f$$

(na przykład dla przetwornika 1/4" i obiektywu 3,6 mm wysokość i szerokość pola widzenia kamery w odległości 10 m wynoszą:

$$\text{– wysokość pola widzenia } k = 2,7 \cdot 10\,000 / 3,6 = 7500 \text{ mm} = 7,5 \text{ m}$$

$$\text{– szerokość pola widzenia } m = 3,6 \cdot 10\,000 / 3,6 = 10000 \text{ mm} = 10 \text{ m})$$

Wszelkie obliczenia muszą być dokonywane z użyciem jednolitych jednostek, czyli wszędzie konsekwentnie stosujemy albo metry albo milimetry i stopnie albo radiany.

Fizycznie przekątna przetwornika różni się od przekątnej podawanej w katalogach, jest od niej mniejsza, a co za tym idzie, także inne wymiary są mniejsze:

ogniskowa [mm]	kąt	odległość [m]													
		2	4	6	8	10	12	14	16	18	20	30	50	80	100
2,1	98	4,6	9,1	13,7	18,3	22,8	27,4	32,0	36,5	41,1	45,7	68,5	114,2	182,7	228,4
2,5	88	3,8	7,7	11,5	15,3	19,2	23,0	26,9	30,7	34,5	38,4	57,6	95,9	153,5	191,9
3,6	67	2,7	5,3	8,0	10,7	13,3	16,0	18,7	21,3	24,0	26,6	40,0	66,6	106,6	133,2
4	62	2,4	4,8	7,2	9,6	12,0	14,4	16,8	19,2	21,6	24,0	36,0	60,0	95,9	119,9
6	44	1,6	3,2	4,8	6,4	8,0	9,6	11,2	12,8	14,4	16,0	24,0	40,0	64,0	80,0
8	33	1,2	2,4	3,6	4,8	6,0	7,2	8,4	9,6	10,8	12,0	18,0	30,0	48,0	60,0
12	23	0,8	1,6	2,4	3,2	4,0	4,8	5,6	6,4	7,2	8,0	12,0	20,0	32,0	40,0
15	18	0,6	1,3	1,9	2,6	3,2	3,8	4,5	5,1	5,8	6,4	9,6	16,0	25,6	32,0
25	11	0,4	0,8	1,2	1,5	1,9	2,3	2,7	3,1	3,5	3,8	5,8	9,6	15,4	19,2
33	8,3	0,3	0,6	0,9	1,2	1,5	1,7	2,0	2,3	2,6	2,9	4,4	7,3	11,6	14,5
50	5,5	0,2	0,4	0,6	0,8	1,0	1,2	1,3	1,5	1,7	1,9	2,9	4,8	7,7	9,6
100	2,7	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0	1,4	2,4	3,8	4,8

Tab. 2. Wysokość obiektu widzianego na monitorze przez kamerę z przetwornikiem 1/3"

- 1" – przetwornik o wymiarach 9,6 x 12,8 mm (przekątna 16 mm),
- 2/3" – przetwornik o wymiarach 6,6 x 8,8 mm (przekątna 11 mm),
- 1/2" – przetwornik o wymiarach 4,8 x 6,4 mm (przekątna 8 mm),
- 1/3" – przetwornik o wymiarach 3,6 x 4,8 mm (przekątna 6 mm),
- 1/4" – przetwornik o wymiarach 2,7 x 3,6 mm (przekątna 4 mm).

W tabelach 2 i 3 zawarto przykładowe wyniki obliczeń dla przetworników 1/3", uzyskane na bazie powyższych zależności. Należy znać odległość od obserwowanego obiektu, jego wymiary, czyli wysokość i szerokość, oraz wielkość przetwornika.

Analizując wzory i tabele, zauważamy, iż zmniejszając format przetwornika, zmniejszamy kąt widzenia. Wizualnie objawia się to zwiększaniem liczby rozróżnianych szczegółów obrazu.

Wybór typu przysłony

Należy pamiętać, iż czułość kamer jest podawana przy danej przysłonie, np. 0,05 lx przy przysłonie $F = 1.2$, a zatem, jeśli stosujemy obiektyw z przysłoną $F = 1.8$, to czułość kamery będzie mniejsza, gdyż mniej światła dociera do jej przetwornika. W typowych warunkach wystarczają obiektywy o jasności $F = 1.2-64$, jednakże jeśli stosujemy kamery o dużej czułości, np. 0,01 lx, w przypadku oświetlenia silnym światłem słonecznym zamknięcie przysłony będzie niewystarczające i może dojść do prześwietlenia obrazu. W takim przypadku należy zastosować obiektyw o dużej liczbie określającej minimalną przysłonę. Innym rozwiązaniem jest stosowanie filtrów szarych, lecz ograniczają one czułość przy słabym oświetleniu. Przy naprawdę dużym nasłonecznieniu można się spotkać z sytuacją, w której nawet zastosowanie obiektywu z automatyczną przysłoną nie da zadowalających efektów – na ekranie monitora obraz nie będzie mieć jednakowej jasności. W zależności od ustawień obiektywu może zdarzyć się, że np. w środkowej części będzie prześwietlony, a z kolei w bocznych częściach niedoświetlony. Z takimi problemami można walczyć, stosując obiektywy, które dodatkowo wyposażone są w specjalny filtr –

tw. plamkowy, naniesiony na środkową część powierzchni soczewki.

Przysłona regulowana ręcznie

Jest ona stosowana w warunkach stałego oświetlenia, przeważnie wewnątrz budynków. Regulacja polega na jednorazowym ustawieniu pierścienia lub dźwigni przysłony. Oprócz przysłony ręcznej występują dwa rodzaje przysłon automatycznych.

Automatyczna przysłona (AI – Auto Iris)

Tego typu przysłona utrzymuje stałą ilość światła padającego na przetwornik, bez względu na warunki oświetlenia. Migawka elektroniczna ustawia się na 1/50 s, natomiast obiektyw z AI jest przysmykany i otwierany stosownie do natężenia oświetlenia. Kamera i obiektyw z AI są w stanie pracować poprawnie w warunkach bardzo dużych zmian oświetlenia. Z reguły kamery do obserwacji zewnętrznej w dzień i w nocy wręcz wymagają takiego obiektywu. Kamera z AI jest wyposażona w specjalne wyjście sterujące obiektywem z AI. W zależności od sygnału na tym wyjściu obiektyw zamyka lub otwiera przysłonę, utrzymując ilość padającego na niego światła na stałym poziomie.

Ustawienie parametrów pracy automatycznej przysłony

Głównym celem dobierania parametrów ekspozycji jest osiągnięcie optymalnej jasności zarówno dla oświetlenia w dzień, jak i w nocy. Fabryczny obiektyw wyposażony w *Auto Iris* jest wyregulowany fabrycznie i zazwyczaj regulacja przez użytkownika jest zbędna. Zdarza się jednak, że taką regulację trzeba przeprowadzić. Polega ona na ustawieniu regulatorów *Level* i *AGC* w położeniu środkowym, a następnie ustawieniu za pomocą tego pierwszego pożądanego poziomu jasności obrazu. Kolejnym krokiem jest ustawienie regulatora *ALC*, w zależności od sposobu reakcji na oświetlenie, a potem założenie filtra szarego i wyregulowanie ostrości.

Sytuacje szczególne

Problem braku ostrości w kamerach

Ostrość obrazu to możliwość rozróżnienia szczegółów limitowana rozdzielczością przetwornika lub monitora.

ogniskowa [mm]	kąto- odległość [m]	odległość [m]													
		2	4	6	8	10	12	14	16	18	20	30	50	80	100
2,1	81	3,4	6,9	10,3	13,7	17,1	20,6	24,0	27,4	30,8	34,3	51,4	85,7	137,0	171,3
2,5	72	2,9	5,8	8,6	11,5	14,4	17,3	20,1	23,0	25,9	28,8	43,2	72,0	115,1	143,9
3,6	53	2,0	4,0	6,0	8,0	10,0	12,0	14,0	16,0	18,0	20,0	30,0	50,0	80,0	99,9
4	48	1,8	3,6	5,4	7,2	9,0	10,8	12,6	14,4	16,2	18,0	27,0	45,0	72,0	89,9
6	33	1,2	2,4	3,6	4,8	6,0	7,2	8,4	9,6	10,8	12,0	18,0	30,0	48,0	60,0
8	25	0,9	1,8	2,7	3,6	4,5	5,4	6,3	7,2	8,1	9,0	13,5	22,5	36,0	45,0
12	17	0,6	1,2	1,8	2,4	3,0	3,6	4,2	4,8	5,4	6,0	9,0	15,0	24,0	30,0
15	14	0,5	1,0	1,4	1,9	2,4	2,9	3,4	3,8	4,3	4,8	7,2	12,0	19,2	24,0
25	8,24	0,3	0,6	0,9	1,2	1,4	1,7	2,0	2,3	2,6	2,9	4,3	7,2	11,5	14,4
33	6,24	0,2	0,4	0,7	0,9	1,1	1,3	1,5	1,7	2,0	2,2	3,3	5,5	8,7	10,9
50	4,12	0,1	0,3	0,4	0,6	0,7	0,9	1,0	1,2	1,3	1,4	2,2	3,6	5,8	7,2
100	2,06	0,1	0,1	0,2	0,3	0,4	0,4	0,5	0,6	0,6	0,7	1,1	1,8	2,9	3,6

Tab. 3. Szerokość obiektu widzianego na monitorze przez kamerę z przetwornikiem 1/3"

Regulacja ostrości jest w rzeczywistości zmianą położenia centrum optycznego obiektywu w odniesieniu do przetwornika. Brak ostrości to jeden z najczęściej spotykanych problemów podczas instalacji i regulacji kamer i obiektywów. Dotyczy on zarówno obiektywów o stałej, jak i o zmiennej ogniskowej. Zdarza się, że dokonując regulacji ostrości w obiektywie, nie można uzyskać ostrego obrazu. Najczęściej występuje to w skrajnych położeniach regulacji ostrości obiektywu. W takim przypadku należy poluzować kluczem imbusowym (jest na wyposażeniu prawie każdej kamery) śrubę mocującą pierścień, w który wkręcamy obiektyw, a następnie ustawić możliwie najlepszą ostrość obrazu. Regulacja powinna być przeprowadzona przy najkrótszej ogniskowej i ostrości ustawionej na nieskończoność. Regulacji ostrości należy dokonywać przy maksymalnym otwarciu przysłony, stosując np. filtr szary. Należy zauważyć, iż tej regulacji dokonuje się jedynie w razie konieczności. Praktycznie rzadko się zdarza, by pierścień kamery wymagał regulacji.

Eliminacja odbłasków w zakresie światła widzialnego

Nawet właściwy dobór ogniskowej i przysłony nie zawsze pozwala osiągnąć dobry obraz. Zazwyczaj głównym problemem są różnego rodzaju odbłaski od ścian, podłóg, szyb, mebli, a także od szyb, przez które prowadzimy obserwację. W zasadzie jedynym sposobem wyeliminowania odbłasków jest stosowanie filtrów polaryzacyjnych montowanych przed obiektywem. Filtr polaryzacyjny przepuszcza fale świetlne tylko jednej polaryzacji.

Obracając filtr wokół jego osi, zmieniamy także polaryzację fali, która przez niego przechodzi. Można wtedy znaleźć takie położenie, w którym dominująca polaryzacja światła odbitego zostanie maksymalnie wytłumiona, a tym samym odbłask zostanie zminimalizowany.

Kompromis pomiędzy liczbą kamer a dokładnością obserwacji

Poszerzenie pola widzenia kamer oznacza, iż do obserwacji tego samego terenu potrzeba będzie mniej kamer. Trzeba jednakże pamiętać, że poszerzając pole widzenia kamery, czyli zmniejszając ogniskową, równocześnie zmniejszamy rozróżnialność szczegółów. Dlatego obiektywy o krótkiej ogniskowej należy stosować rozważnie, gdyż może się zdarzyć, iż w razie potrzeby nie będzie można na zapisanym obrazie dostrzec ważnych szczegółów.

Powyżej podano podstawowe informacje, umożliwiające wybór odpowiedniego obiektywu do danej aplikacji. Niniejszym rozpoczęliśmy cykl artykułów mających służyć jako pomoc i źródło wiedzy o obiektywach stosowanych w systemach telewizji dozorowej. Zachęcamy do kierowania pytań i propozycji kolejnych edycji poradnika na adres email: computar@cbcpoland.pl

CBC (POLAND)

Tylko dla wymagających



Wideodrukarka Mitsubishi CP 31 W
- natychmiastowe zdjęcie z cyfrowego rejestratora wideo

Rozdzielczość: 423 ppi
Czas wydruku: 16 sek
Frontowy system ładowania papieru z wewnętrzną kasetą na papier
Zintegrowany panel kontrolny
System PAL dla S-Video i Composite Video



Rejestrator cyfrowy Mitsubishi DX TL 4516

Kompresja JPEG 2000
Nowe rozwiązania technologiczne
Nagrywanie 100 pps/ 2CIF
Podgląd na żywo 800 pps
Własny system operacyjny
Dwa niezależne multipleksery



Monitor IP 32" TFT serii Public View VMC-32LCD-PVM

Zdalne wyświetlanie informacji tekstowej
Przesuwane banery
Obsługa nadawania komunikatów alarmowych
Komunikacja przez sieć LAN (oprogramowanie klienta)
Wbudowana kamera WDR
Wejścia 2 kamer zewnętrznych z zasilaniem 12 VDC
Wbudowana detekcja ruchu
Wbudowany twardy dysk i głośniki
Tryby wyświetlania z podziałem




Oficjalny przedstawiciel

NSyTech™

Nowe Systemy i Technologie

NSyTech Sp. z o.o.
00-367 Warszawa ul. Kopernika 3
Tel: (22) 8287907 8287908
Fax: (22) 8287909
<http://www.nsytech.pl>
e-mail: nsytech@nsytech.pl

Zapraszamy do odwiedzenia naszej ekspozycji
TARGI SECUREX 2008 POZNAŃ
22-25 kwietnia 2008
PAWILON 3A stoisko 107



CZY DOMYŚLASZ SIĘ CO ROBI NA NIEJ TAKIE WRAŻENIE?

Najlepsza oferta systemów domofonowych i wideodomofonowych

- różnorodna stylistyka oferowanych urządzeń • najwyższa jakość użytych materiałów
- bardzo bogata funkcjonalność • praktycznie nieograniczone możliwości rozbudowy
- możliwość pracy na każdym rodzaju okablowania • profesjonalna obsługa klienta



UTOPIA



FOLIO



K-STEEL



SINTHESE

Kompetentny partner
w dziedzinie zabezpieczeń



GUNNEBO
For a safer world®

Gunnebo Polska Sp. z o.o., ul. Piwonicka 4, 62-800 Kalisz, tel. +48 (0) 62 768 55 70, fax +48 (0) 62 768 55 71, e-mail: polska@gunnebo.com, www.gunnebo.pl

FIRE WATER EARTH AIR and CCTV

Life with cctv.



G70 WB36
Outdoor High Speed Dome

AU-G70 Series • Intelligent High-Speed Dome Camera with sunshield • Sony Inside

www.vido-europe.com

DISTRIBUTOR FOR POLAND

VIDO.AT
CCTV Manufacturer

VIDO Electronic Vertriebs GmbH

Favoritner Gewerbering 15
A-1100 Vienna, Austria

+43 1 95826 9820
sales@vido-europe.com

ALARMNET SP.J.

022 663 40 85
www.alarmnet.com.pl

MIWI-URMET SP. z o.o.

042 616 21 00
www.miwurmet.com.pl

DOSKONAŁA FUNKCJONALNOŚĆ ZA NIESPOTYKANĄ CENĘ

24MopI

wyłączny przedstawiciel producenta w Polsce



KARTY DVR

Karty DVR z polskim oprogramowaniem - kompresja do wyboru MPEG4 / H.264, stabilna praca, dostęp przez sieć, obsługa zdalna przez program lub sieć.



Specyfikacja

Model	DVR_4_50	DVR_4_100
wejścia video	4 x BNC	4 x BNC
szybkość	50 klatek na sekundę	100 klatek na sekundę
kompresja video	H.264 / MPEG4	H.264 / MPEG4
rozdzielczość	640x480, 352x288, 320x240	640x480, 352x288, 320x240
zabezpieczenie hasłem	tak	tak
możliwość łączenia kart	do 6 kart	do 6 kart
ilość wyświetlanych kamer	1, 4, 9, 16, 25, 36	1, 4, 9, 16, 25, 36
tryb nagrywania	ciągły, detekcja, harmonogram	ciągły, detekcja, harmonogram
praca w sieci	dołączone oprogramowanie lub przeglądarka	dołączone oprogramowanie lub przeglądarka
sterowanie kamerami	lokalne i zdalne	lokalne i zdalne
nagrywanie na wielu dyskach	tak	tak

Model	DVR_8_200	DVR_16_200
wejścia video	8 x BNC	16 x BNC
szybkość	200 klatek na sekundę	200 klatek na sekundę
kompresja video	H.264 / MPEG4	H.264 / MPEG4
rozdzielczość	640x480, 352x288, 320x240	640x480, 352x288, 320x240
zabezpieczenie hasłem	tak	tak
możliwość łączenia kart	do 4 kart	do 2 kart
ilość wyświetlanych kamer	1, 4, 9, 16, 25, 36	1, 4, 9, 16, 25, 36
tryb nagrywania	ciągły, detekcja, harmonogram	ciągły, detekcja, harmonogram
praca w sieci	dołączone oprogramowanie lub przeglądarka	dołączone oprogramowanie lub przeglądarka
sterowanie kamerami	lokalne i zdalne	lokalne i zdalne
nagrywanie na wielu dyskach	tak	tak

24MopI

tel. 071 333 87 22, 071 724 52 82, 0601 24 66 66, poczta@24m.pl, www.24m.pl



the Art of
PROTECTION

Najlepsze Systemy transmisji audio video



Nasze systemy transmisji spełniają wymagania Rozporządzenia MSWiA w sprawie sposobu utrwalania przebiegu imprez masowych oraz Rozporządzenia w sprawie monitorowania szkół.



Szczegóły oferty, lista dystrybutorów na stronie:

www.pag.com.pl

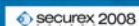


Nowoczesne Systemy Kontroli Dostępu



- ponad 1000 wdrożonych systemów KD
- ponad 800 wdrożonych systemów RCP
- ponad 80 mln wyemitowanych kart
- producent sprzętu i oprogramowania
- przedstawiciel wiodących firm
- 3 oddziały w Polsce

Uczestnik targów



POZNAŃ teren MTP

pawilon 3A stoisko 58

22-25 kwietnia 2008

Zapraszamy firmy instalatorskie do współpracy



UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. 012 39 89 900
e-mail: biuro@unicard.pl

ODDZIAŁ WARSZAWA
ul. Ratuszowa 11
03-450 Warszawa
tel. 022 24 47 200
e-mail: warszawa@unicard.pl

ODDZIAŁ POZNAŃ
Os. Polan 33
61-249 Poznań
tel. 061 62 32 750
e-mail: poznan@unicard.pl

PROTECTOR

SYSTEM DEPOZYTARIUSZY KLUCZY/SKRYTEK

PROXSAFE FLEXX, PROXSAFE 19" RACK SYSTEM, CABINET-32

- Obudowa wykonana ze stali (opcja: szklane lub stalowe przednie drzwi)
- Panele Flexx wyposażone w gniazda kluczy i uchwyty do kluczy
- Identyfikacja klucza w otworze
- Kontrola włożenia klucza do właściwego otworu
- Pełne zabezpieczenie sabotażowe
- Możliwość instalacji od 16 do 128 kluczy w jednej obudowie
- Możliwość łączenia depozytariuszy kaskadowo
- Pełne zabezpieczenie kluczy (cylinder z blokadą)
- Terminal sterujący z polskim oprogramowaniem, wyświetlaczem LCD oraz zaimplementowanym czytnikiem 125KHz w pełni kompatybilnym z kartami/brelokami systemu kontroli dostępu SOYAL
- Praca w magistrali RS-485 oraz w sieci LAN
- Interfejs USB/RS-485(RS-485/LAN)
- Przyrząd montażowy do zarabiania kluczy
- Oprogramowanie zarządzające w języku polskim umożliwia:
pełną kontrolę nad depozytariuszem, raportowanie pobieranych/zdawanych kluczy,
możliwość tworzenia użytkowników, grup kluczy i użytkowników, multiklient
- Możliwość zarządzania 64 panelami FLEXX (1024 kluczy) z poziomu jednego terminala sterującego
- Sterowanie - karta, karta + pin kod, pin kod



Obudowa o wysokości **24U**
max **128 kluczy**



Obudowa o wysokości **12U**
max **64 kluczy**

ProxSafe - 32
Cabinet



**Automatycznie
otwierana/zamykana
żaluzja**



Obudowa o wysokości **6U**
max **32 kluczy**

**Dowolna konfiguracja depozytariusza
PROXSAFE 19" RACK SYSTEM**



*Zapraszamy na nasze stoisko podczas
zblizających się targów*

**MTP SECUREX 2008
PAWILON 3A stoisko nr.83**

www.protector-polska.pl

tel: +48 (091) 431 83 10

fax: +48 (091) 431 83 11

biuro@protector-polska.pl



Międzynarodowe Targi Poznańskie



spotkaj przyszłość



securex 2008

P O L A N D

Największa Międzynarodowa Wystawa Zabezpieczeń

22 - 25 . 04 . 2008 Poznań

Targi
z rekomendacją
Polskiej Izby Przemysłu Targowego

SECUREX bo nie wszyscy są Fair...

- ▶ Ponad 200 wystawców
- ▶ Ponad 180 nowości
- ▶ I Mistrzostwa Polski Instalatorów Systemów Alarmowych
- ▶ Liczne konferencje, seminaria tematyczne i spotkania z przedstawicielami branży zabezpieczeń

PLATYNOWY WYSTAWCA

SPS trading **Aper**®

BEZPIECZEŃSTWO — OCHRONA — MONITORING

Zarejestruj się on-line **www.securex.pl**
a otrzymasz tańszy bilet oraz katalog za złotówkę
NOWOŚĆ! Bilety trzydniowe

Najnowsze systemy bezprzewodowe do monitoringu wizyjnego firmy P.W. Camsat



Bezprzewodowy monitoring wizyjny znajduje z każdym rokiem coraz szersze zastosowanie – począwszy od dozoru pojedynczych posesji, przez wielozakładowe korporacje, instytucje publiczne i monitoring miejski, po obiekty, w których odbywają się imprezy masowe. W wielu rozwiązaniach nie można zastosować przewodowych systemów monitoringu wizyjnego, które są dobrze znane projektantom i instalatorom. Czasem barierą są względy ekonomiczne, ale także w wielu miejscach wręcz nie ma możliwości wykonania okablowania. Alternatywą dla standardowych rozwiązań są urządzenia firmy P.W. Camsat działające w wysoce stabilnym i niewymagającym zezwoleń paśmie ISM 5,8 GHz.

Nie jest prawdą, iż koszt monitoringu bezprzewodowego przewyższa koszty standardowej sieci przewodowej. Jednym z istotniejszych kosztów związanych z instalacją elektronicznych systemów bezpieczeństwa są nakłady na robociznę, ponoszone podczas układania rozległych sieci kablowych, a także koszty koniecznych do uzyskania pozwoleń, położonego okablowania czy dzierżawy światłowodów.

Transmisja obrazu video za pośrednictwem zestawu **TCO 5808h**, pracującego na częstotliwości 5,8 GHz, pozwala na znaczne oszczędności w zakresie instalacji urządzeń. System ten został stworzony na potrzeby profesjonalnej telewizji przemysłowej oraz telewizji kablowej, spełnia więc w zupełności także wymagania instalatorów telewizji dozorowej. Ponadto czas niezbędny do realiza-

cji przedsięwzięcia jest krótszy niż w przypadku systemów przewodowych, znacznie mniejszy jest także wpływ instalacji na infrastrukturę obiektu.

Możliwość zastosowania aż do ośmiu niezależnych kanałów video w powiązaniu z bardzo wysoką jakością obrazu sprawia, że zestaw **TCO 5808h** nadaje się niemal do każdego systemu monitoringu wizyjnego o dużych wymaganiach. Dodatkowym atutem systemu radiowego jest łatwość montażu i mobilność sprzętu oraz możliwość zmiany lokalizacji kamer bez dokonywania żadnych nowych inwestycji. Zestaw **TCO 5808h** może być także uzupełnieniem już istniejącej przewodowej sieci monitoringu, bez konieczności ingerencji w zainstalowane wcześniej okablowanie.

Podstawowym zastrzeżeniem instalatorów i użytkowników w stosunku do urządzeń bezprzewodowych są występujące zakłócenia transmisji. Należy jednak podkreślić, iż zakłócenia przemysłowe to problem urządzeń systemów pracujących w paśmie 2,4 GHz, które jest udostępnione także sieciom komputerowym WLAN czy urządzeniom Bluetooth.

Zjawisko to zupełnie nie dotyczy systemów **TCO 5808h**, gdyż pracują one w paśmie wydzielonym tylko i wyłącznie dla transmisji video i audio.

Transmisja video 5,8 GHz w cenie jak dla systemów 2,4 GHz

Urządzenia działające na częstotliwości 2,4 GHz były obecne na rynku głównie z powodu bardziej przystępnej ceny. Firma P.W. Camsat wprowadziła nowe urządzenia **TCO 5807h** w cenie urządzeń 2,4 GHz. Dzięki temu systemy 5,8 GHz tej firmy mogą całkowicie zastąpić systemy poprzedniej generacji. Dla lepszej identyfikacji produktów P.W. Camsat firma zmieniła swój znak firmowy (logo). Pozwoli to inwestorom oraz instalatorom uniknąć zakupu urządzeń innych producentów, które także pojawiają się na rynku, a nie zawsze spełniają wysokie normy odnośnie jakości obrazu i wymaganego zasięgu.



Fot. 1. Zestaw **TCO 5808h** do transmisji video o zasięgu do 3 km

TCO 5807h to najnowszy hermetyczny zestaw do bezprzewodowej transmisji obrazu oraz dźwięku w paśmie 5,8 GHz. Charakteryzuje się również wysoką jakością obrazu jak poprzedni system TCO 5808h i jest porównywalny pod tym względem z urządzeniami do transmisji przewodowej. Wyróżnia się także niewielkimi rozmiarami oraz przystępną ceną. Zasięg standardowego zestawu hermetycznego to 2 km.

Rozwiązania bezprzewodowe dla kamer obrotowych

Każdy system bezprzewodowy wideo 5,8 GHz można dodatkowo wyposażać w moduł telemetryczny **CD-04** do bezprzewodowego sterowania kamerami obrotowymi. System monitoringu wizyjnego powinien umożliwiać śledzenie zmian na obserwowanym obszarze. Musi więc być zapewniona możliwość sterowania każdą kamerą zgodnie z dynamicznie zmieniającą się sytuacją i wykonania płynnego zbliżenia istotnych szczegółów bez widocznych opóźnień. Z tego względu sygnały sterowania kamerami nie mogą być blokowane przez przekaz dużych pakietów informacji, a jest to możliwe tylko wtedy, gdy system zapewnia przesyłanie sygnałów sterowania kamerami za pośrednictwem specjalnego kanału, niezależnego od kanału wideo – tak jak w przypadku CD-04.

Profesjonalny moduł telemetryczny CD-04 wykorzystuje wszystkie funkcje kamer, jak przy sterowaniu przewodowym. Współpracuje z dowolnym interfejsem RS485 lub RS232 (m.in. PELCO-D, PELCO-P, SAMSUNG, COP-2, Santachi, PANASONIC, Longcomity, HUNDA600, LILIN, VICON, MOLYNX, KALATEL, VCL, Reserved, COP-1, Ultrak).

Moduł CD-04 realizuje dwukierunkową transmisję (*half duplex*), która jest wymagana przez większość kamer obrotowych dla potwierdzenia transmisji czy odebrania alarmów z kamer (czujki ruchu w kamerach, wejścia sabotażowe itd.). Prędkość transmisji protokołu jest regulowana w zakresie 1200–9600 kb/s. Dziesięć kanałów pracy gwarantuje poprawną pracę modułu w każdym terenie.

Moduł CD-04 pracuje w wolnym paśmie radiowym ISM 869 MHz, niewymagającym zezwoleń. Większość dostępnych na rynku urządzeń nie posiada wystarczającej mocy dla stabilnej pracy kamer. Natomiast moduł CD-04, dzięki mocy 500 mW, dozwolonej dla tej częstotliwości, gwarantuje stabilną pracę bez opóźnień czy utraty kontroli oraz zasięg do 5 km (z miniaturowymi antenami dookólnymi) albo nawet do 30 km (z antenami kierunkowymi).

Brak opóźnień odróżnia moduł CD-04 także od rozwiązań cyfrowych, które generują znaczne opóźnienia.

Moduł CD-04 może być dowolnie łączony z systemami transmisji wizji 5,8 GHz oraz 2,4 GHz. Dzięki tym cechom



Fot. 2. Zastosowanie CD-04 w systemach telewizji dozorowej

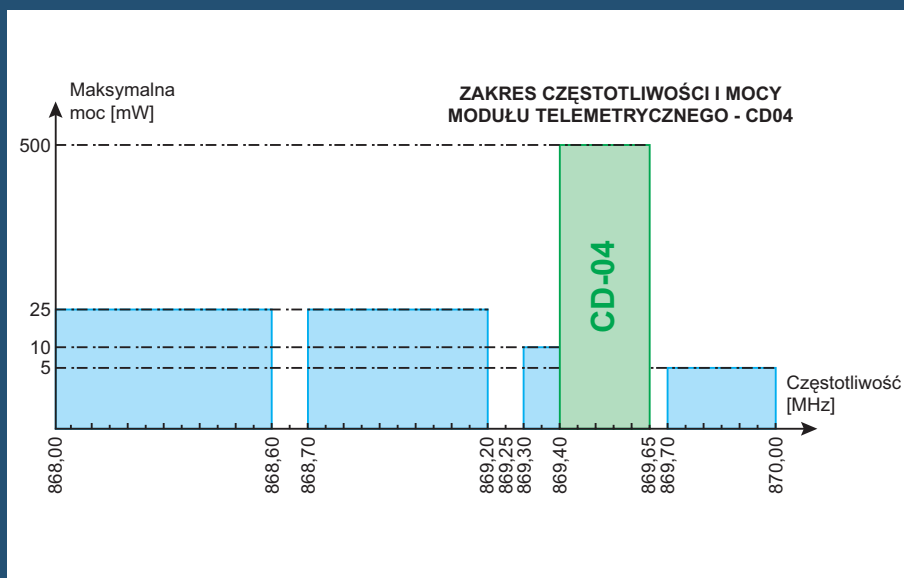
CD-04 w zupełności wystarcza do większości systemów zabezpieczeń. W zależności od zastosowań przesyłany sygnał wideo oraz sygnały sterowania (PTZ) mogą być zakodowane albo nie.

Podobnie jak w przypadku systemu TCO 5808 uruchomienie systemu wideo z transmisją PTZ ogranicza się wyłącznie do instalacji i podłączenia samych urządzeń transmisyjnych.

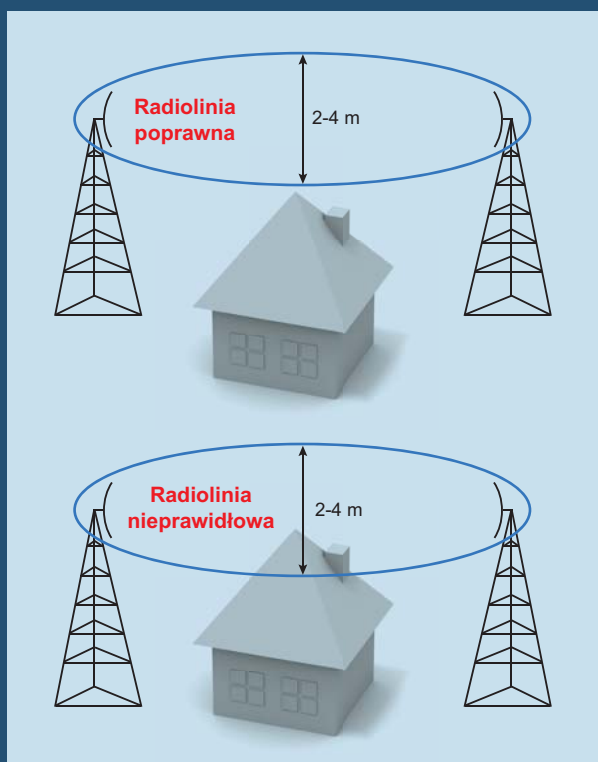
W każdej dziedzinie życia można zauważyć ciągłą ekspansję urządzeń bezprzewodowych, dlatego takie rozwiązania cieszą się coraz większym zainteresowaniem i uznaniem wielu klientów i dystrybutorów z branży telewizji dozorowej. Z roku na rok umacniają one swoją pozycję dzięki uzyskiwaniu świetnych efektów tam, gdzie inne rozwiązania nie zdały egzaminu. Systemy bezprzewodowego przesyłu wizji oraz telemetryczne nadają się do monitoringu miejskiego, monitoringu lasów, szpitali, szkół, parkingów, posesji prywatnych, zarówno do pracy wewnątrz, jak i na zewnątrz obiektów.

Zasady odpowiedniego dobierania systemów bezprzewodowych

W celu uzyskania prawidłowego działania systemów bezprzewodowych należy spełnić kilka podstawowych warunków.



Rys. 1. Zakres częstotliwości pracy CD-04



Rys. 2. Strefa Fresnela w przypadku właściwej oraz wadliwej instalacji radiolinii

Najważniejszą zasadą prawidłowej pracy wszystkich systemów mikrofalowych jest „widzialność optyczna” anten. Jest to warunek krytyczny dla radiolinii o zasięgu powyżej 50 m. W systemach 5,8 GHz należy zagwarantować fali radiowej „czysty korytarz” o średnicy około 2–4 m (jest to tzw. pierwsza strefa Fresnela). Najlepszą jakość transmisji uzyskuje się, montując anteny co najmniej 2 m nad przeszkodami. Powyżej przedstawiono właściwy oraz wadliwy sposób usytuowania urządzeń radiowych 5,8 GHz.

W przypadku braku „widzialności optycznej” anten możliwa jest retransmisja sygnału w celu ominięcia przeszkody, bez straty sygnału czy spadku jakości obrazu.

Dobór zestawów dla kamer szybkoobrotowych

Dobór systemów bezprzewodowych dla kamer szybkoobrotowych polega na zaopatrzeniu się w moduł telemetryczny, np. CD-04, dla klawiatury oraz dla każdej kamery.

Poniżej przykłady doboru urządzeń.

Dla:

- **jednej kamery szybkoobrotowej** – jeden zestaw wideo (np. TCO 5808h) + dwa moduły telemetryczne CD-04,
- **dwóch kamer szybkoobrotowych** – dwa zestawy wideo (np. TCO 5808h) + trzy moduły telemetryczne CD-04,
- **pięciu kamer szybkoobrotowych** – pięć zestawów wideo (np. TCO 5808h) + sześć modułów CD-04 itd.

Więcej informacji dostępnych jest na witrynie internetowej producenta www.camsat.com.pl (w tym karty katalogowe urządzeń). W przypadku wątpliwości polecamy kontakt z technikami firmy P.W. Camsat z Solca Kujawskiego.

AGNIESZKA GRALAK

P.W. CAMSAT



PROFESJONALNE SYSTEMY
BEZPRZEWODOWE VIDEO 5.8GHz

Wzbogaciliśmy ofertę naszej firmy o nowe zestawy do przesyłu obrazu „TCO5807h” oraz sterowania kamerami obrotowymi „CD04”. Stanowią one połączenie najwyższej jakości obrazu, łatwej instalacji oraz wszechstronności zastosowań.

5.8GHz w cenie 2.4GHz

TCO5807H

BEZPRZEWODOWY ZESTAW
TRANSMISJI OBRAZU 5.8GHz DO 2KM

- siedem kanałów pracy
- praca w czasie rzeczywistym
- IP65

CD04

BEZPRZEWODOWY MODUŁ TELEMETRYCZNY
DO STEROWANIA KAMERAMI OBROTOWYMI ORAZ
REJESTRATORAMI DVR

- zasięg 6 km
- praca w czasie rzeczywistym bez opóźnień
- porty RS232 oraz RS485
- prędkości od 1200 - 9600 bps
- współpracuje z każdym protokołem transmisyjnym

PRODUCENT:

P.W. CAMSAT
86-050 Solec Kujawski
ul. Prosta 32
tel. +48 52 387 3658
fax. +48 52 387 5466
email: biuro@camsat.com.pl

www.camsat.com.pl

Najnowsza
technologia ochrony
rozległych terenów zewnętrznych

RADARY

Idealne zabezpieczenie
dla lotnisk i baz wojskowych

Radar RDTS
na granicy USA



Wizualizacja PSRS
z kamerą THV



Radar PSRS
z kamerą THV



**ZAPRASZAMY NA TARGI
SECUREX 2008
PAW.12, ST.17**



Systemy radarowe wykrywają każde
wtargnięcie na chroniony obszar i stale
monitorując aktualną pozycję intruza
mogą sterować zintegrowanym
systemem nadzoru wizyjnego



www.adt.pl

Liderzy rynku zabezpieczeń **zapraszają** **na Dni Otwarte Wzorcowni!**

Zadzwoń dzisiaj, aby umówić się na wizytę w nowym salonie wystawienniczym firm ADT i Tyco Fire & Integrated Solutions. Jeśli jesteś klientem, projektantem, instalatorem lub specjalistą branży zabezpieczeń poszukującym solidnego partnera do współpracy czekamy na Ciebie.

Więcej informacji o Dniach Otwartych Wzorcowni znajdziesz na stronie internetowej www.adt.pl oraz pod numerem infolinii **0801 801 238**

NOWE SYSTEMY KAMEROWE PELCO (cz. 2)

Na początku roku firma Pelco, światowy lider w dziedzinie systemów CCTV, wprowadziła do swojej oferty nowe modele kamer kolorowych o wysokiej rozdzielczości: kamerę sieciową IP3701-2X i kamery serii C10CH. Celem artykułu jest dostarczenie podstawowych informacji o tych produktach

Kamera IP3701-2X

IP3701-2X jest kolorową kamerą o wysokiej rozdzielczości, przeznaczoną do pracy w sieciach IP. Wyposażona jest w interfejs sieciowy 100 Base-TX, przez który przesyła strumienie wideo do standardowej przeglądarki internetowej lub urządzenia rejestrującego. Nagrywanie materiału może być realizowane przy użyciu oprogramowania niezależnych producentów, takich jak Milestone Systems czy On-Net Surveillance Systems, Inc. (OnSSI). W sieciowym systemie Endura produkowanym przez Pelco strumienie wideo są nagrywane przez rejestratory sieciowe serii NVR5000. Pod koniec drugiego kwartału bieżącego roku przewidywane jest rozpoczęcie sprzedaży rejestratora Pelco DVR5100 w wersji 1.5, który będzie miał możliwość rejestracji strumieni wideo z kamer IP3701-2X i innych kamer IP produkowanych przez Pelco.

Wbudowany w kamerę IP3701-2X serwer wideo może wprowadzać do sieci trzy strumienie wideo. Dwa strumienie MPEG4 25 obrazów/s mogą być odbierane przez urządzenia rejestrujące i wyświetlające systemu Endura lub dowolne oprogramowanie z interfejsem zgodnym z protokołem IP Pelco. Trzeci skalowalny strumień MJPEG może być odbierany bezpośrednio przy użyciu przeglądarki internetowej Microsoft Internet Explorer lub Mozilla Firefox. Obsługiwane przez kamerę protokoły sieciowe to TCP, UDP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP i NTP. Dostępne rozdzielczości pracy dla strumieni MPEG4 to 4CIF (704 x 576), 2CIF (704 x 288), CIF (352 x 288) i CIF (176 x 144).

Kamera jest przeznaczona do pracy wewnątrz pomieszczeń w zakresie temperatur od -10°C do 50°C. Uchwyt montuje się do górnej lub dolnej części obudowy. Minimalne oświetlenie obserwowanej sceny to 0,5 lx mierzone przy f/1,2, 40IRE i włączonej funkcji AGC. Obiektyw nie należy do wyposażenia kamery.

Firmy oferujące oprogramowanie typu BMS mogą zintegrować kamery IP3701-2X ze swoimi produktami, ponieważ Pelco udostępnia producentom oprogramowania dokumentację API umożliwiającą stworzenie sterownika do odbioru strumieni wideo. Do komunikacji z innymi urządzeniami kamery IP Pelco używają języka XML.

Podstawowe cechy IP3701-2X:

- zasilanie w standardzie PoE (IEEE802.3af) lub 24 V~,
- otwarta architektura,



- trzy jednocześnie strumienie wideo:
 - dwa strumienie MPEG-4 (25 obr/s przy QCIF, CIF, 2CIF, 4CIF),
 - skalowalny strumień MJPEG do przeglądarki internetowej,
- protokoły TCP, UDP (Unicast, Multicast IGMP), UPnP, DNS, DHCP, RTP i NTP,
- wielopoziomowa hierarchia dostępu,
- rozszerzony zakres dynamiki (EDR),
- możliwość stosowania obiektywów C/CS,

- rozdzielczość 480 TVL,
- kompensacja oświetlenia tła,
- serwisowe analogowe wyjście wideo.

Rekomendowane obiektywy

Seria 13FA, 13FD – obiektywy o stałej ogniskowej, format 1/3 cala, FA (ręczna przesłona), FD (automatyczna przesłona, DD). Seria 13VA, 13VD – obiektywy o zmiennej ogniskowej, format 1/3 cala, VA (ręczna przesłona), VD (automatyczna przesłona, DD).

Kamery C10CH

Seria C10CH to w pełni wyposażone kamery kolorowe z przetwornikiem CCD 1/3 cala. Zostały tak zaprojektowane, aby zapewnić wyjątkową jakość obrazu nawet w bardzo trudnych warunkach oświetleniowych. Kamery cechuje kompaktowa obudowa, wysoka rozdzielczość 540 TVL i możliwość pracy przy oświetleniu minimum

trudnych warunków oświetleniowych, analogową funkcję „eclipser” i kompensację oświetlenia tła, która koryguje obraz tak, aby obiekty w polu widzenia kamery nie były widziane jako ciemne, jeśli ich tło jest silnie oświetlone. Ustawień związanych z funkcjami kamery dokonuje się przy użyciu menu ekranowego.

Kamera C10CH jest przystosowana do obiektywu z mocowaniem CS. Mogą być stosowane obiektywy ze stałą, ręcznie regulowaną lub automatyczną przesłoną (typu DC lub VD). Podłączenie sterowania przesłoną jest realizowane poprzez czterostykowy kwadratowy wtyk, który należy do standardowego wyposażenia obiektywów produkowanych przez Pelco. Menu ekranowe pozwala wybrać obszary maskowania, nazwy, korekcie pikseli i profile oświetlenia.

Instalacja kamer C10CH jest bardzo łatwa. Dla modelu C10CH-6X rekomendowane są obudowy DF5, DF8A, EH100, EH3508 i EH2508. Kamery te mogą być częścią zestawów Pelco DomePak i ImagePak. Opcjonalny uchwyt C10-UM może być stosowany wszędzie tam, gdzie kamera C10CH-6X lub C10CH-7X będzie montowana bez obudowy – na ścianie, suficie lub do profilu.

Rekomendowane obiektywy

Seria 13FA, 13FD – obiektywy o stałej ogniskowej, format 1/3 cala, FA (ręczna przesłona), FD (automatyczna przesłona, DD). Seria 13VA, 13VD – obiektywy o zmiennej ogniskowej, format 1/3 cala, VA (ręczna przesłona), VD (automatyczna przesłona, DD). Seria 13ZD – obiektywy motor-zoom, format 1/3 cala (automatyczna przesłona, DD). Obiektów nie należy do wyposażenia kamery.

Główne cechy serii C10CH:

- kompaktowa obudowa,
- przetwornik CCD 1/3 cala,
- cyfrowa obróbka sygnału wizyjnego (DSP),
- rozdzielczość 540 TVL,
- czułość 0,4 lx,
- mocowanie obiektywu typu CS,
- automatyczna detekcja rodzaju sterowania przesłoną (DC/wideo),
- menu kamery na ekranie,
- funkcja automatycznego i ręcznego balansu bieli,
- automatyczna regulacja wzmocnienia, elektroniczne sterowanie migawką,
- kompensacja oświetlenia tła, redukcja migotania,
- automatyczna detekcja zasilania 12V~/24V~.

Modele

0,3 lx. Na zastosowanie w większości aplikacji CCTV pozwalają wbudowane funkcje: automatyczna detekcja rodzaju zasilania 12V= lub 24V~, automatyczna regulacja wzmocnienia (AGC), elektroniczne sterowanie migawką (ESC), redukcja migotania. Dodatkowo C10CH ma wbudowaną funkcję automatycznego balansu bieli (AWB) dla

Więcej informacji na temat opisanych kamer kolorowych można znaleźć na stronie <http://www.pelco.com> oraz u dystrybutorów Pelco w Polsce.

Kamera	Zasilanie	Model
CCD 1/3", kolorowa, 540 TVL, PAL	24V~/12V=	C10CH-6X
CCD 1/3", kolorowa, 540 TVL, PAL	230V~	C10CH-7X

NORBERT GÓRA
PELCO EUROPE

SAMSUNG

TECHWIN



SAMSUNG DIGITAL SECURITY SOLUTIONS



ProfiCCTV
ul. Heleny Szafran 10
60-179 Poznań
tel: 0 61 842 29 62
email: samsung@samsungcctv.pl

- Wysoka rozdzielczość - **560 linii TV kolor 700 linii TV BW.**
- Funkcja dzień/noc z ruchomym filtrem podczerwieni.
- Czułość: **0,2 Lux (F1.2) Kolor, 0,0001 Lux (F1.2) (Sens-up) BW**
- Szeroki zakres balansu bieli (1800°K~10,500°K)
- Redukcja obciążenia dysku oraz „efektu ducha” za pomocą technologii **SSNR II** - druga generacja.
- Nowa generacja DSP Super Vision - **SV IV.**
- Szeroki zakres dynamiki **128x WDR**

www.samsungcctv.pl

**Zapraszamy firmy
z branży SECURITY
do odwiedzin nowego
serwisu internetowego**

www.infocam.com.pl

- * internetowa hurtownia elektronicznych systemów zabezpieczeń
- * codzienna aktualizacja cen i stanów magazynowych
- * pełna baza danych informacji o produktach
- * czytelny i prosty w obsłudze interfejs użytkownika
- * pełna kontrola realizacji zamówień i statusu przesyłek
- * aktualności z branży zabezpieczeń
- * informacje o nowościach i zapowiedziach
- * stały kontakt online z opiekunem
- * możliwość składania zamówień 24h na dobę
- * codziennie nowe promocje i okazje

PROMOCJE
NOWOŚCI
CENNIKI
FORMULARZE
LINKI

O FIRMIE
KAMERY CCTV

AKTUALNOŚCI

DOWNLOAD

KONTAKT

SYSTEMY MOBILNEJ REJESTRACJI

PEŁNA OFERTA

- Monitor
 - LCD VGA (5)
 - CRT VGA (1)
 - CRT Composite (1)
 - LCD Composite
- Urządzenia analogowe
 - Magnetowidy Time Lapse (1)
- Akcesoria dodatkowe
 - Transmisja sygnału
 - Dyski twarde
- Rejestratory
 - Stand Alone
 - KCS PC
 - Akcesoria
 - Karty PCI (6)
- Monitor
 - CRT VGA
 - CRT Composite
 - LCD VGA
 - LCD Composite
- Kamery
 - kolorowe
 - dzień/noc
 - czarno-białe
- Obiektywy
 - Stała ogniskowa
 - Zmienna ogniskowa

TWÓJ KOSZYK

Zalagowany: Gość

NAJNOWSZE PRODUKTY I OFERTY



AVERDIGLE1704HYBRID

Rejestратор hybrydowy 4ch Pracuje w sieci LAN
Możliwość podłączenia 4 kamer 2P lub composite BNC
Wbu

cenar: 3 965,00 pln

[Do koszyka](#)

[Zobacz pełny opis](#)



AVERDIGLE1704HDV-D

Rejestратор hybrydowy 4ch Pracuje w sieci LAN
Możliwość podłączenia 4 kamer 2P lub composite BNC
Wbu

cenar: 4 514,00 pln

[Do koszyka](#)

[Zobacz pełny opis](#)



AVERDIGLE1504NET-DVD

4 wejścia wideo BNC, 4 wejścia, 1 wyjście audio,
praca w sieci LAN, wbudowana nagrywalna DVD
Wbu

cenar: 3 233,00 pln

[Do koszyka](#)

[Zobacz pełny opis](#)

KONTO UŻYTKOWNIKA

[Edycja danych](#) [Zmiana hasła](#) [Historia zamówień](#) [Wiadomości \(1 nowe\)](#)

Zalogowany: Jan Kowalski

Twój opiekun: Paweł Ławniczak, tel 024 262 02 47

temat	otrzymano	usuń
Informacja o przesyłce	2008-03-04 16:14:27	usuń
Promocja miesiąca	2008-03-04 16:11:05	usuń

ID	wartość	dodano	status	szczegóły
45	1227.10	2008-03-04 16:16:32	nowe	zobacz
44	8419.30	2008-03-04 16:04:12	zrealizowane	zobacz

[zobacz wszystkie zamówienia](#)

Twoje dane:

Dane adresowe do wysyłki:

Jan Kowalski
Perspektywy 7
77-077 Kraków
22 878 25 65 / 501878266

Dane do wystawienia faktury:

Zakład Instalacyjny Jan Kowalski
Perspektywy 7
77-077 Kraków
NIP:788-94-85-78

[zmień dane](#)

**NIE ZWLEKAJ,
ZAREJESTRUJ SWOJE KONTO
JUŻ DZIŚ**

Zapraszamy na międzynarodową
wystawę zabezpieczeń



securex 2008
P O L A N D

w dniach 22-25 kwietnia 2008 r.,
pawilon **3a** (parter), stoisko nr **101**

Matryce w kamerach telewizji dozorowej

Często niedocenianym lecz niezwykle ważnym elementem kamery telewizji dozorowej jest jej matryca światłoczuła. To właśnie ona jest w dużej mierze odpowiedzialna za jakość obrazu otrzymywanego z kamery. Podstawy technologii stosowanych w dotychczasowych matrycach sięgają lat 70. XX wieku, nic zatem dziwnego, że to właśnie matryce są obecnie najmocniej rozwijającym elementem kamer. Warto przyjrzeć się, jakie poszczególne parametry matrycy wpływają na jakość otrzymywanych za ich pomocą obrazów

Czym jest matryca?

Na początek kilka słów o tym, czym jest i jak działa matryca światłoczuła. Matryca to najczęściej krzemowa płytka zbudowana z elementów światłoczułych, zwanych dla uproszczenia pikselami, wyłapująca światło w postaci padających na nią fotonów. Ogniskowane są one na matrycy za pomocą mikrosoczewki umieszczonej przed nią. Fotony w wyniku tzw. efektu fotoelektrycznego wewnętrzne powodują uwolnienie elektronów (nośników ładunku), które są magazynowane w kondensatorach. Im dłużej trwa ekspozycja, tym więcej elektronów zostanie przechwyconych. Zgromadzone w ten sposób ładunki

pada jedynie światło o spektrum odpowiadającym konkretnej barwie (najczęściej czerwonej, niebieskiej lub zielonej), co pozwala na określenie natężenia w danym miejscu konkretnej barwy i zbudowanie kolorowego obrazu. Jest to jednocześnie jedna z przyczyn, dla których kamery kolorowe mają zazwyczaj niższą rozdzielczość niż kamery czarno-białe. O tym jednak kilka słów poniżej.

Rodzaje matryc

Większość popularnych kamer wyposażona jest w matryce określane akronimami CCD (*Charge-Coupled Device*) lub CMOS (*Complementary Metal-Oxide-Semiconductor*)



w danym przedziale czasowym, po przeliczeniu informują o natężeniu światła padającego na poszczególne piksele, co pozwala na określenie jasności dla każdego piksela i na tej pod-

stawie zbudowanie przez przetwornik analogowo-cyfrowy kompletnego obrazu padającego na matrycę CCD. Warto zwrócić uwagę, że w ten sposób układ nie otrzymuje żadnych informacji o kolorze danego piksela, dlatego przed matrycą światłoczułą umieszcza się filtr barwny RGB. Problem uzyskania informacji o kolorze został rozwiązany właśnie za pomocą wspomnianego filtra, który powoduje, że na dany element światłoczuły (piksel)

mimo tego, że w rzeczywistości skróty te odnoszą się jedynie do zastosowanych technologii, a nie do samych matryc. Obie matryce wykorzystują to samo zjawisko fotoelektryczne i działają na podobnej zasadzie, różnią się jednak sposobem przetwarzania i dostępu do zarejestrowanego w danym pikselu natężenia. W matrycach CMOS każdy piksel jest wyposażony w swój własny wzmacniacz oraz rejestr odczytu i w każdej chwili elektronika może dowolną ilość razy odczytać stan dowolnego piksela. W przypadku matryc CCD, nie posiadających własnych wzmacniaczy i rejestrów, odczyt przeprowadzany jest wierszami bądź kolumnami, dodatkowo z wyzerowaniem zmierzonych wartości. Z tego względu matryce CMOS są szybsze od matryc CCD, charakteryzują się także znacznie mniejszym poborem prądu. Koszt wytworzenia matrycy CMOS dzięki zastosowaniu popularnych produktów półprzewodnikowych jest niższy niż koszt wytworzenia matrycy CCD. Dlaczego jednak to właśnie matryce CCD są

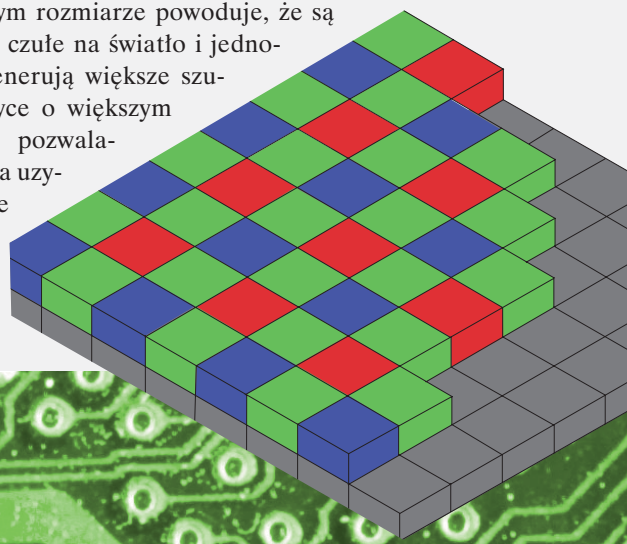
obecnie najczęściej stosowanymi elementami w kamerach telewizji dozorowej?

Charakterystyczne dla matrycy CMOS jest to, że gorzej radzą sobie w warunkach słabego oświetlenia. Dzieje się tak między innymi dlatego, iż część powierzchni matrycy jest zajęta przez elektronikę. Dodatkowo wspomniana mała powierzchnia czynna tej matrycy powoduje, że znacznie trudniej uzyskać w niej wysoką rozdzielczość niż ma to miejsce w matrycach CCD o tym samym rozmiarze. Zwiększenie rozdzielczości i tym samym liczby tranzystorów na matrycy CMOS przy zachowaniu jej rozmiaru powoduje, że rejestruje ona coraz słabszy prąd, co zmniejsza jej czułość i wpływa na zwiększenie szumów obrazu.

Ciekawym rozwiązaniem, które pojawiło się stosunkowo niedawno na rynku kamer telewizji dozorowej, są matryce Pixim określane akronimem DPS (*Digital Pixel System*). DPS jest urządzeniem cyfrowym, analizującym rejestrowany obraz w odmienny od dotychczasowego sposób. Światło padające na matrycę przy określonej ekspozycji zostaje poddane wielokrotnemu próbkowaniu. W ten sposób ustalany jest maksymalny czas ładowania pojedynczego piksela. System DPS magazynuje informację o czasie potrzebnym do naładowania pojedynczego piksela wraz z jego aktualną wartością i dalsze naświetlanie tego piksela, powodujące prześwietlenie w klasycznych przetwornikach, nie ma już znaczenia, gdyż został on już zmagazynowany. Dalsze „doświetlanie” ma znaczenie jedynie dla pikseli, które jeszcze nie

1/4" w kamerach, w których wykorzystano matrycę o rozmiarze 1/3". Można zastosować obiektyw przeznaczony dla kamer o większej matrycy w kamerach, w których zastosowano mniejszą matrycę, jednakże zaowocuje to wyświetleniem mniejszego fragmentu obrazu. Przykładowo, zastosowanie obiektywu o ogniskowej 2,8 mm w kamerze z przetwornikiem 1/3" pozwoli na obserwację szerszego pola widzenia niż w przypadku zastosowania tego samego obiektywu w kamerze z przetwornikiem 1/4".

Jaki wpływ ma jednak wielkość zastosowanej w kamerze matrycy na jakość generowanego przez nią obrazu? Jak już wcześniej zasygnalizowano, rozmiar matrycy ma bezpośredni wpływ na jakość otrzymywanego z niej obrazu szczególnie w sytuacji, kiedy na niewielkich rozmiarach matrycy chce się uzyskać jak największą rozdzielczość, czyli umieścić jak najwięcej pojedynczych elementów światłoczułych. Konieczność umieszczenia większej liczby elementów światłoczułych w matrycach o mniejszym rozmiarze powoduje, że są one mniej czułe na światło i jednocześnie generują większe szumy. Matryce o większym rozmiarze pozwalają zatem na uzyskanie nie



zostały dostatecznie naładowane. Można powiedzieć, że w systemach Pixim DPS każdy piksel matrycy traktowany jest jak niezależna kamera, która posiada własny czas ekspozycji. Sposób ten znacznie zwiększa zakres dynamiki kamery, co pozwala na jednoczesne zarejestrowanie większej ilości szczegółów obrazu w jasnych i ciemnych partiach obserwowanej sceny niż ma to miejsce w klasycznych przetwornikach CCD i CMOS.

Rozmiary matryc

W kamerach telewizji dozorowej najczęściej stosowane są obecnie matryce o wielkości 1/3" oraz 1/4". Dostępne są jednak także kamery z matrycami o rozmiarze jednego cala, 1/2" oraz 2/3". Podstawowym elementem, na który wpływa wielkość matrycy, jest rodzaj obiektywu zastosowanego w kamerze. Obiektyw musi być dostosowany do wielkości matrycy w kamerze, dlatego pozbawione sensu jest zastosowanie obiektywu przeznaczonego dla kamer

tylko większej rozdzielczości obrazu, lecz także obrazu o lepszej jakości.

Elementy optyczne przed matrycą

Nierozerwalnie związane z matrycami są elementy optyczne umieszczone przed matrycą, w skrócie zwane filtrami. Do najważniejszych zalicza się wspomniany na wstępie filtr barwny zwany siatką Bayera, pozwalający na zmierzenie natężenia kolorów w poszczególnych elementach światłoczułych i tym samym uzyskanie kolorowego obrazu. Zastosowanie tego filtra jest jedną z przyczyn, dla których kamery kolorowe często mają niższą rozdzielczość niż kamery czarno-białe. W wyniku użycia filtra dla uzyskania informacji o kolorze jednego piksela obrazu konieczne jest odczytanie natężenia w czterech elementach światłoczułych (RGBG), dlatego też w matrycach kolorowych o wysokiej rozdzielczości stosuje się znacznie więcej elementów światłoczułych niż w matrycach do kamer czarno-białych.

SKRYTKI DEPOZYTOWE

System monitorowanych skrytek z rozbudowanym oprogramowaniem zarządzającym i raportującym zgodnym z Systemem SAIK

SAIKBOX



MTP securex 2008
22 - 25 kwietnia
stoisko 67 pawilon 3A



bt electronics sp. z o.o.

tel. + 48 12 / 410-85-10
www.saik.pl

Kolejnymi filtrami umieszczanymi przed matrycą jest tzw. grupa filtrów dolnoprzepustowych, do których zalicza się m.in. filtr podczerwieni. Światło w paśmie podczerwieni niesie ze sobą w warunkach dziennych informacje powodujące powstawanie niepotrzebnych zakłóceń w obrazie. Filtr odcina pasmo podczerwieni, pozwalając na uzyskanie lepszej kolorystyki i jakości obrazu, powoduje jednak również zmniejszenie ilości docierającego do matrycy światła, co zmniejsza jej czułość. Dlatego też w przypadku kamer typu dzień/noc filtr ten może być automatycznie odsuwany sprzed matrycy, co pozwala kamerze na zwiększenie czułości kosztem jakości obrazu. Odsuwanie filtra umożliwia również zastosowanie doświetlaczy typu IR, które w przypadku kamery posiadającej stały filtr podczerwieni nie będą jednak działały. Najważniejszą rolą wszystkich filtrów dolnoprzepustowych jest poprawienie jakości rejestrowanego obrazu w warunkach dziennych.

Poprawianie jakości matrycy

Proces rozwoju matryc światłoczułych nie jest oczywiście zakończony. Wiele firm stosuje unikatowe rozwiązania w celu poprawy jakości obrazu generowanego przez przetworniki analogowo-cyfrowe. Pierwszym krokiem było stworzenie matryc typu SUPER CCD, w których elementy światłoczułe miały postać kwadratów obróconych o 45 stopni, co pozwoliło na uzyskanie większej rozdzielczości. Firma Sony w swoich przetwornikach stosuje technologię HAD (*Hole Accumulation Diode*) pozwalającą na



znaczną redukcję szumów w matrycach CCD i dokładniejsze odzwierciedlenie kolorystyki. Jednocześnie trwają badania mające na celu stworzenie nowych rodzajów matryc o wysokiej czułości na światło, a także najmniejszych zakłóceń. Powoli raczkuje także technologia Foveon X3, która pozwala na rejestrację kolorowego obrazu za pomocą pojedynczego elementu światłoczułego, co znacznie zwiększa rozdzielczość użytkową matryc. Matryce pozostają sercem kamer i to one będą w przyszłości wyznaczały kierunek rozwoju telewizji dozorowej.

MARCIN GIERSZNER

ALPOL




Nareszcie wszystko w porządku...

Zapraszamy do współpracy partnerskiej!

- KAMERY IP
- OPROGRAMOWANIE
- AKCESORIA

Poleczki 47, 02-822 Warszawa
tel. 0/22 33 11 990 fax 0/22 33 11 511
softex@softex.com.pl
www.kameryaxis.pl, www.softexdata.pl



MAGICARD

Promocja na Targi Securex!



Chcesz zapoznać się z nowościami i aktualnymi promocjami drukarek do kart plastikowych?

Odwiedź nas na Targach Securex 2008
pawilon 3A stoisko 44

Informacje o produktach i aktualnych promocjach dostępne są również na naszych stronach internetowych

MAGICARD MASTER DEALER

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C, 01-496 Warszawa
tel: +48 22 8324744, fax: +48 22 8324644
biuro@acss.com.pl
www.acss.com.pl, www.magicard.com.pl



NOWA generacja rejestratorów

16-kanalowy rejestrator cyfrowy serii 5800

- pentapleks: zapis, podgląd, odtwarzanie, archiwizacja/mirroring i praca w sieci
- nagrywanie: do 400 obr/s [720x288] - rejestrator „real-time recording”
- rozdzielczość nagrywania: 720x576, 720x288, 360x288
- kompresja: MPEG-4 ASP
- zapis 16 kanałów audio, zdalny odsłuch przez sieć
- funkcja przed-alarmu do 30 min dla każdej kamery
- przechwytywanie danych tekstowych: ATM, POS, AC itp.
- DVD-RW, USB
- program RASplus (podgląd, przeglądanie nagrań, zarządzanie, mapy)
- spełnia wymagania rozporządzenia w sprawie sposobu utrwalania przebiegu imprez masowych (Dz. U. z 2004 r., nr 243, poz. 2438)



Wyłączny dystrybutor produktów NOVUS® w Polsce:



AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

KAMERY OBROTOWE

Novus – II generacja

Wydanie magazynu *Zabezpieczenia*, które trzymacie Państwo w ręku, jest wydaniem targowym. Ten numer zamyka również okres mojej dwuletniej współpracy z redakcją i prezentowania oferty firmy Novus z zakresu systemów telewizji dozorowej. Za udostępnienie mi łamów magazynu *Zabezpieczenia* i ogrom życzliwości niniejszym chciałbym Pani redaktor naczelnej wraz z zespołem serdecznie podziękować. Chciałbym również, aby spotkanie targowe, do czego gorąco zachęcam, było okazją do osobistego spotkania z Czytelnikami oraz wymiany doświadczeń i uwag związanych z instalacją i eksploatacją proponowanych rozwiązań.

Niniejszym artykułem będę kontynuować rozpoczęte w numerze 4/2007 omówienie dotyczące kamer szybkoobrotowych CamaI oraz Cama-mini. Kontynuacja ta wynika, jak wiele poprzednich artykułów, z rozwoju technologicznego i wprowadzania kolejnych generacji urządzeń. Dotychczasowe modele zostaną zastąpione przez serię CamaII oraz Cama-miniII.

Nowa seria kamer składa się z czterech modeli o krotnościach zoomu x18, x26, x36 oraz x22. Różnice między modelami wynikają z zastosowanego typu modułu kamerowego i dotyczą jedynie ustawień podmenu „USTAWIENIA KAMERY”.

Ważnym usprawnieniem jest wprowadzenie dla ujęć programowalnych niezależnych ustawień automatyki ekspozycji oraz ostrości. Pozwala to w presecie lub podczas realizacji patrolu składającego się z presetów zoptymalizować ustawienia ekspozycji oraz ostrości i uzyskać wysokiej jakości obraz. Stosowanie funkcji ma szczególne uzasadnienie w przypadku dużych obszarów nadzoru o zmieniających warunkach oświetlenia. Podczas realizacji funkcji automatyzacji obserwacji ustawienia są automatyczne, natomiast w momencie wywołania presetu kamera przechodzi na zaprogramowane przez użytkownika i dopasowane do obserwowanej sceny ręczne ustawienia. Dodatkowo, w celu podniesienia komfortu pracy operatora, wprowadzono opcjonalnie zamrożenie obrazu przy przemieszczaniu się kamery do presetu, ponieważ obraz generowany przy przemieszczaniu może być zamazany i nieczytelny.

Liczba tras obserwacji została zwiększona do ośmiu, natomiast dostępna pamięć pozwala na rejestrację ręcznie zaprogramowanych schematów obserwacji o łącznym czasie do 500 s i, co ważne, może być w dowolnych proporcjach dzielona pomiędzy poszczególne trasy.

Zgodnie z życzeniami administratorów dostęp do ustawień menu został zabezpieczony poprzez wprowadzenie

przed wejściem do menu sześciocyfrowego hasła, tworzonego z wykorzystaniem 38 dostępnych znaków alfanumerycznych.

Od generacji kamer serii CamaII wprowadzono możliwość aktualizacji oprogramowania kamery przez użytkownika. Ma to szczególne znaczenie w kontekście coraz częściej wprowadzanych poprawek i nowych funkcji już w trakcie eksploatacji urządzeń.

W porównaniu z poprzednią generacją znacznie ulepszono sterowanie głowicą oraz wprowadzono dodatkowe menu „USTAWIENIA OBROTU”, w którym można zde-

finiować prędkość obrotu i uchyłu przy ręcznym sterowaniu (tryb wolny, normalny, turbo) oraz maksymalne wartości prędkości dla różnych trybów. Również sterowanie kamerą (zwłaszcza przyspieszanie i hamowanie) odbywa się płynnie dzięki rozszerzonej liczbie dostępnych prędkości pośrednich, zależnych od wychylenia joysticka.

Kamery NVC-SD236DN z 36-krotnym zoomem optycznym posiadają dodatkowo funkcję detekcji ruchu dla ujęć programowalnych. Dotychczas obraz z kamer obrotowych musiał być rejestrowany w trybie ciągłym ze względu na niemożność kompensacji ruchu kamery na tle obserwowanej sceny, co powodowało dużą zajętość pamięci rejestratora oraz brak możliwości filtrowania zapisanego materiału, np. według kryterium detekcji ruchu.

Implikowało to długi czas wyszukiwania potrzebnego materiału. Opisywany model kamery w przypadku pracy z ujęciami programowalnymi i uaktywnioną funkcją detekcji ruchu możeysterować jedno z czterech wyjść przekąźnikowych i wyzwoić alarmowy tryb nagrywania w rejestratorze (dodatkowo np. z funkcją przedalarmu).

Zakres zmian wprowadzonych w kamerze Cama-miniII jest znacznie szerszy, ponieważ obejmuje zmiany modułu kamerowego oraz mechaniki kamery. W kamerze zastosowano moduł kamerowy z NVC-SD222DN, co poprawiło ogniskowanie kamery oraz zwiększyło możliwość dokonywania zbliżeń. Tym samym ustawienia modułu zostały wzbogacone między innymi o funkcje szerokiego zakresu dynamiki, wydłużonej migawki, a przede wszystkim tryb pracy dzień/noc. Dostęp do menu urządzenia został zabezpieczony hasłem składającym się z czterech cyfr. W porównaniu z poprzednią wersją kamery dodano funkcję parkowania umożliwiającą rozpoczęcie realizacji zaprogramowanej funkcji po określonym czasie bezczynności. Najważniejsza zmiana budowy mechanicznej kamery



dotyczy dookólnego nieograniczonego obrotu oraz systemu silników do sterowania kamerą. Prędkość obrotu kamery w poziomie została tym samym zwiększona do 375 stopni/s.

Zmodernizowane i ulepszone zostały również obudowa zewnętrzna oraz uchwyty montażowe. W celu zapewnienia bezproblemowej modernizacji oraz rozbudowy istniejących już instalacji systemów telewizji z kamerami obrotowymi Camał wszystkie modele kamer i obudów są w pełni kompatybilne. Na szczególną uwagę zasługuje uchwyt ścienny NVB-SD40PWB/230 z wbudowanym transformatorem 230 V_{AC}/24 V_{AC} oraz zabezpieczeniem przeciwprzepięciowym w torze zasilania 24 V_{AC}. Uchwyt ten wyposażono dodatkowo w terminal złącz do podłączenia sygnałów alarmowych, sterowania i zasilania za pomocą dostarczanej wraz z obudową wiązki kablowej, znacznie ułatwiającej montaż kamery. Stosowany w uchwytych (ściennych oraz sufitowych) system łączenia z obudową za pomocą nakrętki mocującej oraz tulei uniemożliwia wewnętrzne skręcenie połączeń kablowych. W celu zabezpieczenia obudowy przed upadkiem w trakcie montażu została ona wyposażona w linkę zakończoną karabińczykiem do połączenia z uchwytem.

Jakość opisywanych urządzeń można rzeczywiście zweryfikować dopiero w realnych warunkach w obiekcie. Dotyczy to szczególnie kamer obrotowych, których rzeczywiste warunki pracy wiążą się ze stałym obciążeniem mechanicznym podczas realizacji funkcji automatyzacji obserwacji (presety, trasy, patrole) oraz obciążeniem układów optycznych związanym z ciągłymi zmianami ogniskowej oraz ustawieniami ostrości. I choć ten główny test dopiero przed kamerami, już podczas targów będzie możliwość zapoznania się z nimi i weryfikacji przedstawionych funkcji.

PATRYK GAŃKO

Novus



CONTROL SYSTEM FMN Sp. z o.o.

Al. KEN 96, 02-777 Warszawa
www.cs.pl, mail: biuro@cs.pl
tel./fax +48 22 855 00 17 do 19

Nowootwarta hurtownia

Specjalne warunki
dla pośredników i instalatorów

Kompleksowa oferta systemów zabezpieczeń i identyfikacji personalnej

- Autoryzowany importer systemów KD: Synel, HID, AdamsRite
- Wyłączny dystrybutor i autoryzowane centrum serwisowe drukarek do kart plastikowych Fargo
- Integracja systemów:
 - oprogramowanie KD,
 - RCP,
 - identyfikacja personalna
- Monitoring wizyjny



RACS ROGER ACCESS CONTROL SYSTEM

seria radius



Seria Radius

Seria Radius to całkowicie nowa linia wzornicza czytników i kontrolerów dostępu zaprojektowana w oparciu o wieloletnie doświadczenie firmy Roger w tej dziedzinie.

W skład rodziny wchodzi czytniki i kontrolery różniące się konstrukcją mechaniczną oraz funkcjonalnością, w zależności od modelu obsługują one karty standardu EM 125kHz lub 13.56MHz Mifare. Nową kategorię produktów stanowi wandaloodporny czytnik zbliżeniowy (PRT64VP) w którym zarówno przednia część obudowy jak i klawisze są wykonane w całości z metalu.

Na szczególną uwagę zasługuje również kontroler PR602LCD, który został specjalnie zaprojektowany dla systemów rejestracji czasu pracy (RCP) co nie wyklucza jednak możliwości stosowania go jako zwykłego kontrolera dostępu. Urządzenia rodziny Radius mogą być instalowane na zewnątrz budynków i są kompatybilne z wcześniej produkowanymi kontrolerami dostępu serii PR oraz czytnikami PRT, mogą one być dołączane do istniejących już systemów kontroli dostępu pracujących autonomicznie lub pod kontrolą programu PR Master (*).

(*) Informacja

Począwszy od 1 września 2007 program PR Master jest rozprowadzany z darmową licencją bez ograniczenia liczby kontrolerów w systemie.



CE

profesjonalna
kontrola
dostępu

System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001

Cz. 1. Wprowadzenie

Artkuł ten jest pierwszą częścią cyklu poświęconego zarządzaniu bezpieczeństwem informacji zgodnemu z normą ISO/IEC 27001. W następnych częściach zostaną omówione kolejno procesy zarządzania bezpieczeństwem informacji, elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz jeden z modeli zarządzania bezpieczeństwem systemów informatycznych (PDCA)

1. Wstęp

Ogólną definicję pojęcia bezpieczeństwa jako stanu spokoju, braku zagrożenia, niezakłóconego funkcjonowania możemy wprost odnieść do człowieka, obiektu lub procesów, w tym także biznesowych. Wraz z rozwojem technologii teleinformatycznych pojawił się problem zapewnienia bezpieczeństwa systemów teleinformatycznych oraz środowisk, w których są stosowane, w taki sposób, aby wytwarzane, przetwarzane, przekazywane i przechowywane w nich informacje i świadczone usługi można było uważać za bezpieczne.

Bezpieczeństwo procesów biznesowych sprowadza się do zarządzania bezpieczeństwem informacji w każdym aspekcie funkcjonowania organizacji.

Prawidłowo funkcjonujący biznes nie może już obyć się bez wsparcia rozwiązań informatycznych. Jednocześnie zaawansowane rozwiązania technologiczne stwarzają nowe formy zagrożeń. Statystyki obrazujące nowe formy przestępstw przeciwko informacji, w tym wykorzystujące zaawansowane techniki komputerowe, wykazują konieczność zarządzania bezpieczeństwem procesów biznesowych.

Technologia informatyczna rozwija się niezwykle dynamicznie, powodując powstanie nowych produktów i usług. Jednocześnie powoduje to dynamiczną ekspansję nowych zagrożeń. Sytuacja ta wymaga wprowadzenia zorganizowanego zapewnienia bezpieczeństwa informacji oraz stwarza potrzebę wypracowania jednolitego podejścia do zagadnień związanych z zarządzaniem i kontrolą nad technologiami informatycznymi.

Stosowane standardy zarządzania bezpieczeństwem informacji powinny umożliwiać szybką reakcję na zmiany zachodzące w procesach biznesowych mających wpływ na infrastrukturę systemów informatycznych oraz modyfikowanie zabezpieczeń zależnie od typu występujących w danym momencie zagrożeń.

Cykl artykułów w skróconej formie przybliży stosowane standardy zarządzania bezpieczeństwem systemów informatycznych, poczynwszy od dobrych praktyk i standardów umożliwiających certyfikację. Zostaną w nich przedstawione wybrane aspekty zarządzania bezpieczeństwem informacji w celu zapewnienia bezpieczeństwa procesów biznesowych zachodzących w szeroko pojętej organizacji. W artykule zaprezentowano dokładniej jeden z nowszych standardów zarządzania bezpieczeństwem informacji ISO/IEC 27001 (polski odpowiednik PN-ISO/IEC 27001: 2007), który umożliwia przeprowadzenie

certyfikacji wdrożonego SZBI¹. Ze względu na rozległość tematyką zagadnienia skupiono się na podstawowych wytycznych, które w ostatniej części cyklu zostaną zaprezentowane w postaci uproszczonego modelu PDCA².

Norma ISO/IEC 27001 umożliwia przeprowadzenie procesu certyfikacji w zakresie zarządzania bezpieczeństwem informacji. Standard ten staje się coraz bardziej popularny i stanowi podstawę organizacji procesu zarządzania bezpieczeństwem informacji w różnych organizacjach.

Drugim wiodącym elementem pracy jest zaprezentowanie interdyscyplinarnego charakteru zarządzania bezpieczeństwem informacji, który musi uwzględniać bardzo różne aspekty bezpieczeństwa, w tym: teleinformatycznego, fizycznego, osobowego, organizacyjnego, prawnego, społecznego, psychologicznego, a nawet kulturowego.

Omówione zostały podstawowe procesy zarządzania bezpieczeństwem informacji, tj. ustanowienie systemu, wdrożenie i eksploatacja, monitorowanie i przegląd, utrzymanie i doskonalenie.

Jednym z podstawowych zadań niniejszego opracowania jest wprowadzenie do zagadnień zarządzania bezpieczeństwem informacji w systemach informacyjnych.

2. Definicje i terminy

Dla zrozumienia tematu oraz jego skomplikowania niezbędne jest poznanie specyficznego języka, jakim posługują się specjaliści. Język ten jest często trudno przyswajalny dla specjalistów branży teleinformatycznej, dlatego wydaje się właściwe zaprezentowanie podstawowych definicji i terminów z zakresu zarządzania bezpieczeństwem informacji.

Zamieszczone poniżej definicje mają na celu przybliżenie i usystematyzowanie terminologii stosowanej w zakresie zarządzania bezpieczeństwem informacji oraz zdefiniowanie pojęć, których znajomość jest niezbędna do zrozumienia treści niniejszej pracy.

W podanym słowniku pojęć podano wyłącznie definicje zawarte w normach związanych z bezpieczeństwem i audytem systemów informatycznych (PN ISO/IEC 27001, PN-I-02000:2002, PN-I-07799-2:2005, PN-I-13335-1:1999). Zdarza się, że ujęte w słowniku terminy definiowane są odmiennie przez różne źródła. Samodzielna interpretacja nie

1) SZBI – System Zarządzania Bezpieczeństwem Informacji
2) PDCA – z ang. *Plan-Do-Check-Act* – Planuj-Wykonuj-Sprawdzaj-Działaj

powinna jednak wypaczyć podstawowego charakteru określenia. Słownik podzielony został na grupy tematyczne.

bezpieczeństwo (*security*) – stan lub ochrona przed niekontrolowanymi stratami lub skutkami, kombinacja usług zapewniających poufność, integralność i dostępność

bezpieczeństwo informacji (*information security*) – bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji

System Zarządzania Bezpieczeństwem Informacji (SZBI) – z ang. ISMS (*Information Security Management System*) – część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji

Uwaga: system zarządzania obejmuje strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby (aktywa)

polityka bezpieczeństwa (*security policy*) – zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu

bezpieczeństwo informacji (*information security*) – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność [ISO/IEC 17799:2005]

bezpieczeństwo systemu informatycznego (*IT security*) – wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu informatycznego

polityka bezpieczeństwa instytucji w zakresie systemów informatycznych (*IT security policy*) – zasady, zarządzenia i procedury, które określają, jakie zasoby – włącznie z informacjami wrażliwymi – są zarządzane, chronione i dystrybuowane w instytucji i jej systemach informatycznych

podstawowa ochrona (*baseline controls*) – minimalny zbiór zabezpieczeń ustalony dla systemu lub instytucji

deklaracja stosowania (*statement of applicability*) – dokument, w którym opisano cele stosowania zabezpieczeń oraz zabezpieczenia, które odnoszą się do SZBI danej organizacji i mają w nim zastosowanie.

aktywa (*assets*) – wszystko, co ma wartość dla organizacji [ISO/IEC 13335-1:2004]

zasoby – to samo, co aktywa

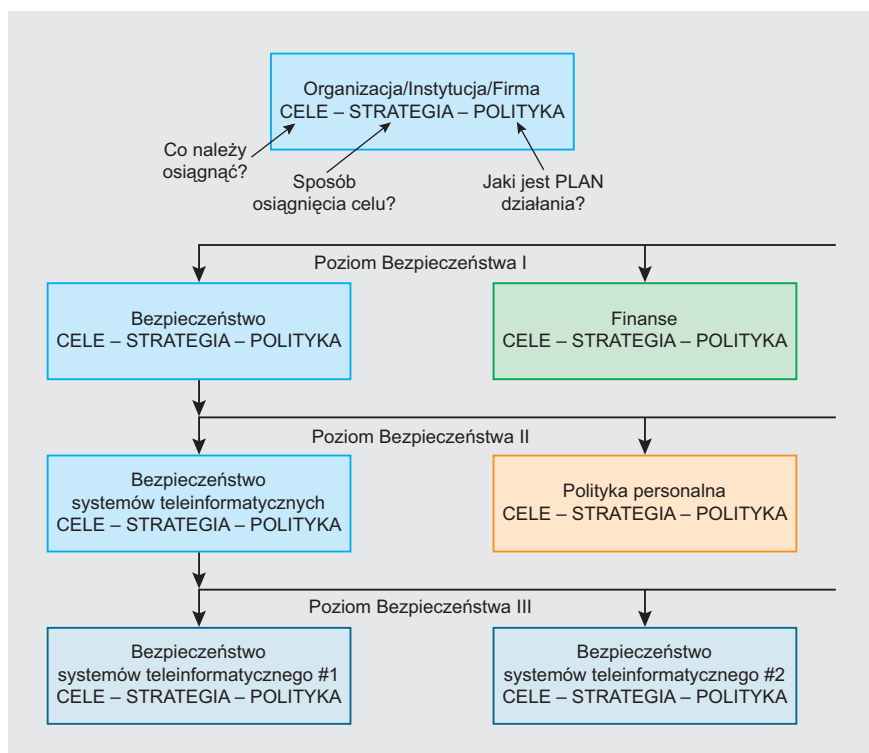
poufność (*confidentiality*) – właściwość, że informacja nie jest udostęp-

niana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom [ISO/IEC 13335-1:2004]

integralność (*integrity*) – właściwość zapewnienia dokładności i kompletności aktywów [ISO/IEC 13335-1:2004]

dostępność (*availability*), zwana też dyspozycyjnością – jest zdefiniowana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne [ISO/IEC 17799:2005] lub **dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu [ISO/IEC 13335-1:2004]

autentyczność (*authenticity*) – właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;



Rys. 1. Trójpłazmowy model bezpieczeństwa



Rys. 2. Zasada synergii systemu bezpieczeństwa informacji

autentyczność dotyczy takich podmiotów, jak użytkownicy, procesy, systemy i informacja [ISO/IEC 13335-1:2004]

niezawodność (*reliability*) – właściwość oznaczająca spójne, zamierzone zachowanie i skutki

rozliczalność (*accountability*) – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2:1989)

zagrożenie (*threat*) – potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji

analiza zagrożeń (*threat analysis*) – badanie działań i zdarzeń, które mogą szkodliwie wpływać na system przetwarzania danych

podatność (*vulnerability*) – słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie

zdarzenie związane z bezpieczeństwem informacji (*security information event*) – jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem [ISO/IEC TR 18044:2004]

incydent związany z bezpieczeństwem informacji (*security information incident*) – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [ISO/IEC TR 18044:2004]

następstwa (*impact*) – rezultat niepożądanego incydentu

ryzyko (*risk*) – prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów

zabezpieczenie (*safeguard*) – praktyka, procedura lub mechanizm redukujący ryzyko

analiza ryzyka (*risk analysis*) – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka [ISO/IEC Guide 73:2002]

szacowanie ryzyka (*risk assessment*) – szacowanie zagrożeń, ich wpływu, podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia.

ocena ryzyka (*risk evaluation*) – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka [ISO/IEC Guide 73:2002]

zarządzanie ryzykiem (*risk management*) – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dla bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów [ISO/IEC 17799:2005] lub **zarządzanie ryzykiem** – skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka [ISO/IEC Guide 73:2002]

ryzyko szczątkowe (*residual risk*) – ryzyko pozostające po procesie postępowania z ryzykiem [ISO/IEC Guide 73:2002]

akceptowanie ryzyka (*risk acceptance*) – decyzja, aby zaakceptować ryzyko [ISO/IEC Guide 73:2002]

postępowanie z ryzykiem (*risk treatment*) – proces wyboru i wdrażania środków modyfikujących ryzyko [ISO/IEC Guide 73:2002]

Uwaga: w normie ISO/IEC 27001 pojęcie „zabezpieczenie” jest używane jako synonim „środka bezpieczeństwa”

audyt bezpieczeństwa (*security audit*) – niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamania bezpieczeństwa oraz zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach

badanie zgodności (*validation*) – przeprowadzenie testów i dokonanie ocen bezpieczeństwa w celu ustalenia zgodności ze specyfikacją i z wymaganiami systemu bezpieczeństwa

dokumentacja (*documentation*) – pisemna lub zarejestrowana w innej formie informacja o przedmiocie oceny, wymagana do jego oceny

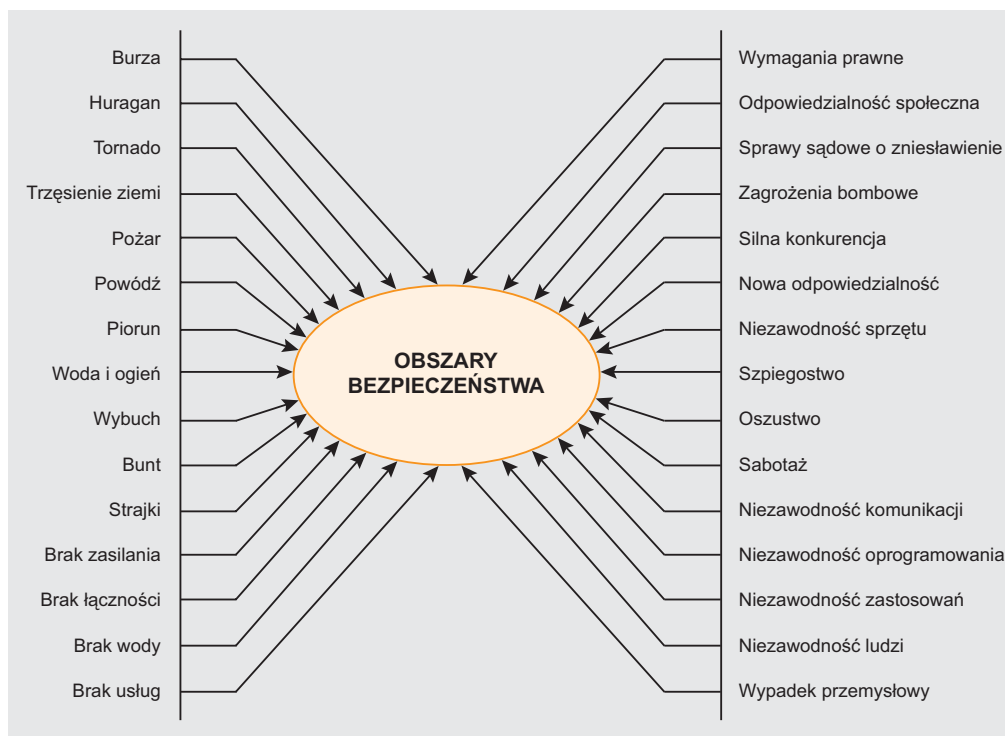
ciągłość działania (*continuity operations*) – utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii

w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak pożar lub trzęsienie ziemi, lub zdarzeniami wywołanymi umyślnie, np. sabotażem

3. Wprowadzenie do zarządzania bezpieczeństwem informacji

3.1. Polityka bezpieczeństwa

Ogólne bezpieczeństwo informacji ma szersze znaczenie niż bezpieczeństwo teleinformatyczne, gdyż obejmuje także informację znajdującą się poza systemami teleinformatycznymi, występującą na nośnikach tradycyjnych, np. w dokumentach papierowych, na mikrofilmach lub w środkach łączności i zapisu akustyczno-wizualnego. Jednak ze względu na podstawową rolę elektronicznego



Rys. 3. Oddziaływanie typowych zagrożeń na obszary bezpieczeństwa

przetwarzania informacji we współczesnych organizacjach bezpieczeństwo teleinformatyczne zajmuje dominującą rolę i jest często utożsamiane z bezpieczeństwem informacji.

Ponadto bezpieczeństwo teleinformatyczne, związane ze stosowaniem środków łączności, zostało wchłonięte, ze względów technologicznych, przez bezpieczeństwo teleinformatyczne.

Szczególne znaczenie dla kompleksowego przedstawienia zagadnień bezpieczeństwa informacji ma trójpłazmowy model odniesienia oparty o cele, strategię i politykę organizacji³:

- **cel** – identyfikuje to, co ma być osiągnięte,
- **strategia** – określa, jak osiągnąć wytyczony cel,
- **polityka** – podaje konkretne zasady realizacji.

Na pierwszym poziomie precyzowane są podstawowe zasady bezpieczeństwa i wytyczne dla całej organizacji. Jest to wyrażone w postaci **polityki bezpieczeństwa instytucji**⁴.

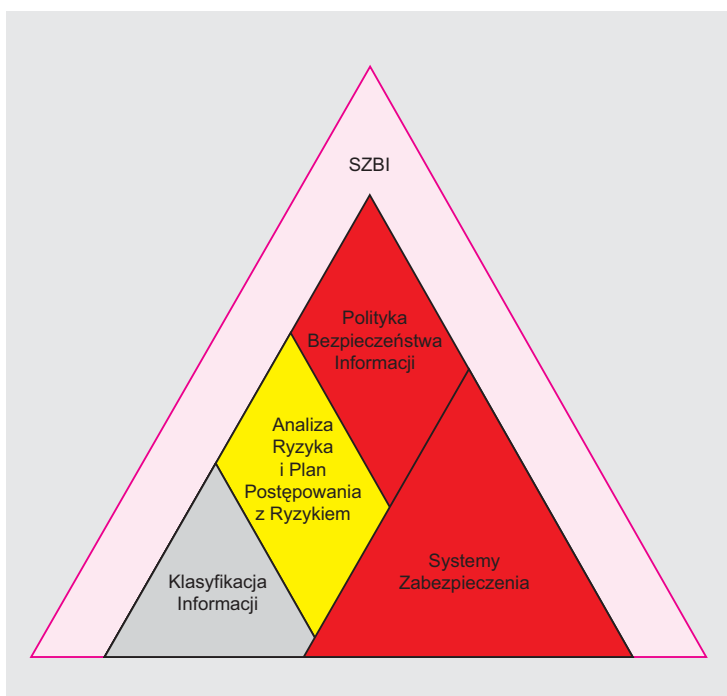
Na poziomie drugim modelu odniesienia rozpatrywane jest bezpieczeństwo konkretnych systemów teleinformatycznych, bezpieczeństwa fizycznego oraz osobowego. Określa się to mianem **polityki bezpieczeństwa teleinformatycznego instytucji**.

Trzeci poziom bezpieczeństwa organizacji dotyczy bezpieczeństwa systemów teleinformatycznych funkcjonujących w organizacji. Określane jest to jako zestaw praw, zasad i najlepszych praktyk, regulujących sposób ochrony informacji wrażliwej oraz usług krytycznych⁵ wewnątrz określonego systemu.

Na rysunku nr 1⁶ zaprezentowano trójpłazmowy model bezpieczeństwa.

Podsumowując, można stwierdzić, że cele⁷, strategię i politykę mogą być opracowane hierarchicznie, od poziomu instytucji do poziomu eksploatacyjnego. Zaleca się, aby odzwierciedlały one potrzeby instytucji i uwzględniały wszelkie występujące w instytucji ograniczenia; jednorodność powinna być zapewniona na każdym poziomie i pomiędzy poziomami. Bezpieczeństwo wchodzi w skład odpowiedzialności na każdym poziomie kierowniczym instytucji i w każdej fazie cyklu życia systemów. Cele, strategię i politykę powinny być utrzymywane i aktualizowane w oparciu o wyniki cyklicznych przeglądów bezpieczeństwa (na przykład analizy ryzyka, audytów bezpieczeństwa) oraz zmian w celach działania instytucji.

Trójpłazmowy model odniesienia przenosi się na strukturę zarządzania bezpieczeństwem oraz strukturę opracowanej dokumentacji zarządzania bezpieczeństwem informacji.



Rys. 4. Prezentacja hierarchicznej struktury bezpieczeństwa informacji

3.2. Elementy bezpieczeństwa

Kompleksowa polityka bezpieczeństwa każdego poziomu powinna uwzględniać wszystkie niezbędne elementy i tworzyć spójny synergetyczny system.

Zamieszczony rysunek nr 2⁸ prezentuje ideę kompleksowego bezpieczeństwa instytucji, wykorzystującą **zasadę synergii**.

Zasada synergii oznacza współpracę różnych czynników (w tym przypadku elementów – podsystemów bezpieczeństwa), której efekt jest większy niż suma ich oddzielnego działania. Inaczej formułując, synergiczność działań – wspólne działanie dające większe, lepsze efekty; działania uzupełniają się poprzez synchronizację.

W każdym ujęciu polityka bezpieczeństwa powinna uwzględniać⁹:

- podsystem ochrony teleinformatycznej,
- podsystem ochrony fizycznej i środowiska,
- podsystem zarządzania zasobami ludzkimi (bezpieczeństwo osobowe),
- zgodność z aktami prawnymi i normatywnymi, mającymi wpływ na przebieg funkcjonowania procesów biznesowych,
- podsystem zarządzania bezpieczeństwem.

W każdym modelu zarządzania bezpieczeństwem należy uwzględnić różne zagrożenia, na jakie potencjalnie narażone są zasoby (aktywa). Zbiór zagrożeń ulega stałym zmianom w czasie i jest znany tylko częściowo.

Na rysunku nr 3¹⁰ zilustrowano oddziaływanie typowych zagrożeń na obszary bezpieczeństwa.

3.3. Podstawowe funkcje modelu zarządzania systemem bezpieczeństwa

Istotą funkcjonowania każdego modelu jest zapewnienie bezpiecznego, skutecznego i efektywnego przebiegu procesu działania i eliminacja potencjalnych zagrożeń.

3) Patrz Andrzej Białas „Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie”

4) Terminy organizacja i instytucja są w niniejszej pracy używane przemienne i oznaczają wszystkie formy organizacyjne funkcjonujące w sferze politycznej, gospodarczej i prawnej państwa.

5) Informacje wrażliwe oraz usługi krytyczne wynikają z przeprowadzonej klasyfikacji informacji przetwarzanych w instytucji oraz analizy ryzyka.

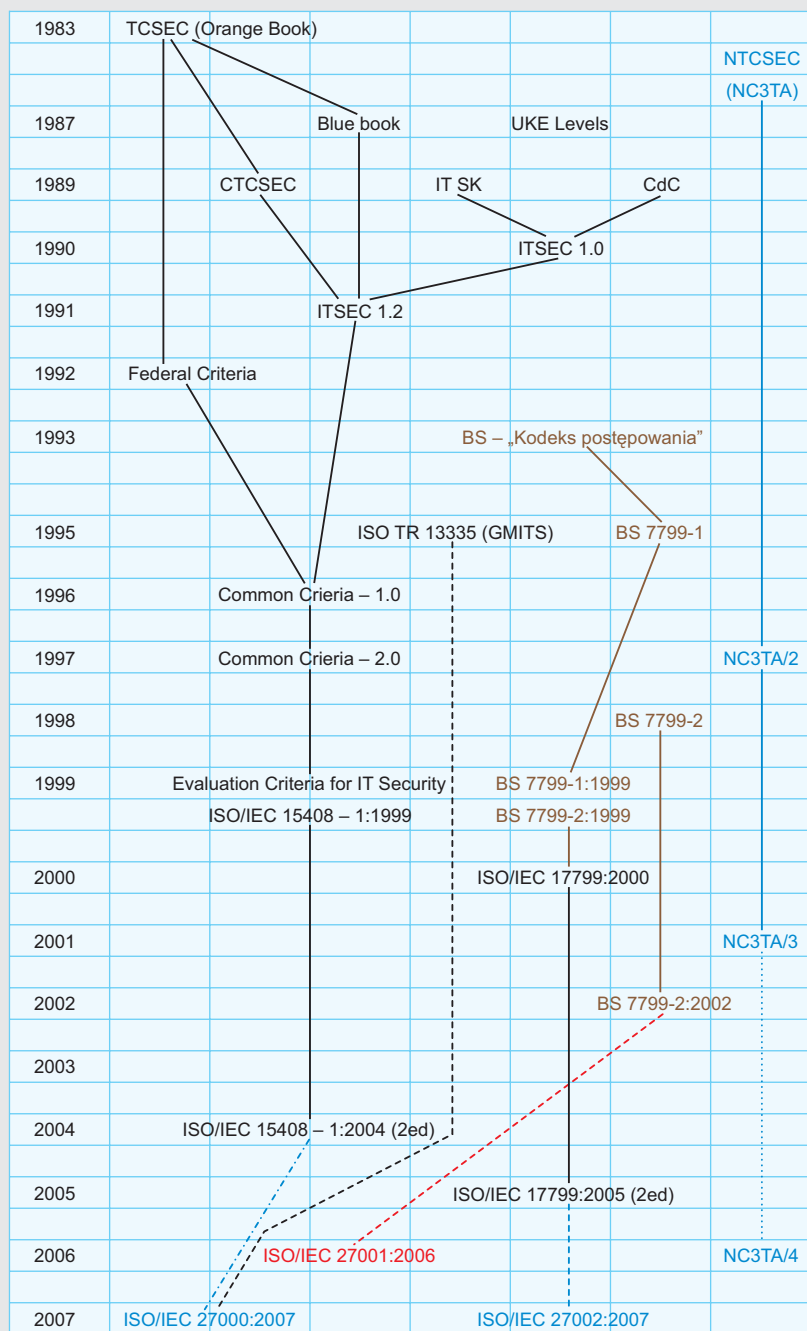
6) Na podstawie Andrzej Białas „Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie”

7) Na podstawie PN-1-13335-1:199 Wytyczne do zarządzania bezpieczeństwem systemów informacyjnych – Pojęcia i modele bezpieczeństwa systemów informatycznych

8) Opracowanie własne

9) Opracowanie własne

10) Na podstawie prezentacji – Marek Blim „Ochrona informacji”, 2006 r.



Rys. 5. Historyczny rozwój standardów bezpieczeństwa teleinformatycznego

Model zarządzania bezpieczeństwem powinien zawierać elementy:

- klasyfikacji informacji (chronionej ustawowo i prawnie, np. niejawną, wrażliwą, krytyczną itd.),
- analizy (zagrożeń i oceny) ryzyka,
- systemów zabezpieczeń (z ich technologiami),
- polityki bezpieczeństwa informacji (z jej składowymi),
- ISMS¹¹ (Systemu Zarządzania Bezpieczeństwem Informacji).

System bezpieczeństwa organizacji powinien być systemem kompleksowym, tzn. wszystkie metody ochrony fizycznej, organizacyjnej, kadrowej, teleinformatycznej muszą być stosowane łącznie, w spójny sposób, inaczej system taki będzie posiadał luki (ważna jest synergia działania).

11) Albo SZBI (nazwa zamienna)

- ochrona rozwiązań informatycznych w sytuacjach krytycznych (ochrona pro-aktywna rekomendowana przez FIRST, SESA Symantec);
- metodologie/narzędzia zarządzania zintegrowanego jakością i bezpieczeństwem informacji (TQM, TSM, TISM);
- narzędzia utrzymania bezpieczeństwa standardu normatywnego (ITIL – BS15000, COBRA-BS7799, Callio Secura 17799);
- metodologie zarządzania stanami hazardowymi jako formuły niezbędne dla potrzeb oceniania niebezpieczeństwa środowiskowego ze strony systemu (analiza SWOT – dla rozwoju polityki zabezpieczeń, metoda FTA – drzewa błędów, metoda FMEA/FMECA – metoda krytycznej oceny architektury i procesów realizacji systemu, metoda

12) Na podstawie prezentacji – Janusz Cendrowski, Krajowa Konferencja Zastosowań Kryptografii „Enigma”, 2005 r.

Zamieszczony rysunek nr 4¹² przedstawia ujednoliconą, hierarchiczną strukturę bezpieczeństwa informacji.

3.4. Standardy zarządzania bezpieczeństwem informacji

Szeroko rozumiana kwestia standaryzacji problematyki ogólnie pojętego bezpieczeństwa systemów teleinformatycznych i jego oceny sięga lat 80. i podlega ciągłej ewolucji. Zasadniczo kryteria różnych standardów bezpieczeństwa informacyjnego (informatycznego, teleinformatycznego) umocowane są w dwóch historycznie określonych momentach i miejscach, tj.:

- **kryteria techniczno-technologiczne** – skierowane na produkt – wywodzą się z USA i prac nad TCSEC (lata 1965–1983) dla potrzeb systemów teleinformatycznych wojska i rządu,
- **kryteria organizacyjno-zarządcze** – skierowane na system i zarządzanie systemem – wywodzą się z Wielkiej Brytanii i prac nad BS 7799 (lata 1993–1999) dla potrzeb środowiska biznesowego.

Ich historyczny rozwój, wzajemne odniesienia oraz integrację normatywną prezentuje rysunek nr 5. W wielu pracach dotyczących zagadnień bezpieczeństwa teleinformatycznego nie wspomina się o standardach wojskowych NTCSEC.

Do najczęściej wykorzystywanych grup standardów i dobrych praktyk stowarzyszeniowych należą następujące rozwiązania:

- 1) klasyfikacja bezpieczeństwa („Orange Book”, TSEC, ITSEC, CC);
- 2) klasyfikacja i zarządzanie bezpieczeństwem (metodologie i narzędzia audytorskie – COBIT, COBRA);
- 3) identyfikacja bezpiecznych rozwiązań (standardy: IEEE, CMM/ CMMI, ISACA, ISSC NATO);

HAZOP-I – jako rodzaj półformalnej procedury inspekcyjnej, wychwytyjącej odstępstwa od założonego działania w obszarze udokumentowanych reprezentatywnych ryzyk STI);

- 8) standardy zintegrowane (informacyjne + *soft-hard-ware chains*);
- 9) quasi-standardy, czyli doraźne konglomeraty rozwiązań cząstkowych, zapożyczonych ze sprawdzonych norm i standardów, które są użytkowane na bazie deklarowanych i utrzymywanych warunków bezpieczeństwa STI (System Teleinformatyczny) w danej organizacji/firmie/korporacji (np. w niektórych firmach ITIL jest stosowany do implementacji STI w organizacji zorientowanej usługowo, a Six Sigma do monitorowania jakości procesów operacyjnych; inne organizacje implementują COBIT, aby ustanowić wytyczne audytu i bezpieczeństwa, a CMM/CMMI aby zapewnić niezawodny rozwój aplikacji w STI – bardzo często spotykany w korporacjach z udziałem spółek USA).

Wybrane standardy zarządzania bezpieczeństwem:

- **ITIL (Information Technology Infrastructure Library)** to jeden z najbardziej powszechnie znanych standardów zarządzania IT na świecie; ITIL opisuje procesy potrzebne do zarządzania infrastrukturą IT tak, by były spełnione odpowiednie założenia dotyczące efektywnego świadczenia usług przez IT oraz zagwarantowana odpowiednia jakość ich świadczenia;
- **model referencyjny standardu COBIT** – opracowany przez związany z ISACA IT Governance Institute standard COBIT (ang. *Control Objectives for Information and Related Technology*) definiuje referencyjny model procesów organizacyjnych związanych z funkcjonowaniem systemu informatycznego w przedsiębiorstwie;
- **model zarządzania bezpieczeństwem informacji zgodny z PN ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji**
- **norma międzynarodowa ISO/IEC 17799:2005 (2ed)** odpowiadająca standardowi brytyjskiemu BS 7799 – **normie BS 7799-1:1999** przyjętej jako ISO 17799 w dniu 15 grudnia 2000 roku (norma PKN w języku polskim o sygn. **PN – ISO/IEC 17799:2003** z dnia 20 marca 2003 roku) a także **normie BS 7799-2:2002** przyjętej w dniu 5 września 2002 roku (norma PKN w języku polskim o sygn. **PN-I-07799-2:2005** z dnia 20 stycznia 2005 roku);
- **norma dotycząca obszaru zarządzania bezpieczeństwem samego systemu (ISO 13335)** oraz oprogramowania i sprzętu (**ISO 15408**) wsparta normami dotyczącymi projektowania systemu, jego oprogramowania i jakości (**ISO/IEC 9126, ISO 12207, ISO 9000-3:2004**);
- **normy dotyczące obszaru zarządzania bezpieczeństwem informacji i organizacji, która wykorzystuje dane STI (PN –ISO/IEC 17799:2003, PN-I-07799-2:2005, a w perspektywie rodzina norm ISO 27000)**, wykorzystujące oprócz weryfikowalnych mierników (certyfikacja) również szereg wskaźników – dobrych praktyk (deklaracja) odnoszących się do starań w celu zapewnienia założonego poziomu bezpieczeństwa systemu informacji.

Wszyscy zainteresowani zgłębieniem opisanych zagadnień mogą skorzystać ze specjalistycznej literatury i opisów zawartych w Internecie. Poniżej przedstawiono wybór pozycji i źródła informacji na ten temat.

DR INŻ. ANDRZEJ WÓJCİK

Literatura:

1. Marian Molski, Małgorzata Łacheta „Przewodnik audytora systemów informatycznych”, Helion 2007.
2. Andrzej Białas „Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie”, WNT 2006.
3. Ross Anderson „Inżynieria zabezpieczeń”, WNT 2005.
4. Kewin Lam i inni „Ocena bezpieczeństwa sieciowego”, Microsoft 2005.
5. Eric Cole i inni „Bezpieczeństwo sieci”, Helion 2005.
6. Krzysztof Czerwiński „Audyt wewnętrzny”, InfoAudit 2005.
7. Edward Yourdon „Wojny na bity”, WNT 2004.
8. Krzysztof Liderman „Podręcznik administratora bezpieczeństwa teleinformatycznego”, Mikom 2003.
9. Krzysztof Liderman „Bezpieczeństwo teleinformatyczne”, WSISiZ 2003.
10. Marian Molski, Sebastian Opala „Elementarz bezpieczeństwa systemów informatycznych”, Mikom 2002.
11. Donald L. Pipkin „Bezpieczeństwo informacji”, WNT 2002.
12. Dorothy E. Denning „Wojna informacyjna i bezpieczeństwo informacji”, WNT 2002.
13. Eric Maiwald „Bezpieczeństwo w sieci. Kurs podstawowy”, 2000, 2001.
14. Tadeusz Kifner „Polityka bezpieczeństwa i ochrony informacji”, Helion 1999.

Normy i standardy:

1. PN ISO/IEC 27001 Systemy zarządzania bezpieczeństwem informacji. Wymagania.
2. PN ISO/IEC 17799:2005 Praktyczne zasady zarządzania bezpieczeństwem informacji.
3. PN ISO/IEC 15408-1:2001 Kryteria oceny zabezpieczenia systemów. Model ogólny oceny zabezpieczenia systemów.
4. PN ISO/IEC 15408-3:2002 Kryteria oceny zabezpieczenia systemów. Wymagania uzasadnienia pewności.
5. PN ISO/IEC 17799:2003 Praktyczne zasady zarządzania bezpieczeństwem informacji.
6. PN-I-13335-1:1998 Wytyczne do zarządzania bezpieczeństwem systemów informacyjnych – Pojęcia i modele bezpieczeństwa systemów informatycznych.

Pisma branżowe:

1. „CSO Magazyn Zarządzających Bezpieczeństwem”, wydawca: International Data Group Poland
2. „Ochrona Mienia i Informacji”, wydawca: Euro-Media

Strony internetowe:

- <http://www.iso27000.pl/>
- <http://www.bsi-poland.pl/>
- <http://www.tuvnord.pl/>

Referaty:

1. Prezentacja – Janusz Cendrowski, Krajowa Konferencja Zastosowań Kryptografii „Enigma”, 2005 r.
2. Prezentacja – Marek Blim „Ochrona informacji”, 2006 r.
3. Prezentacja – Andrzej Wójcik „Polityka bezpieczeństwa. Wybrane zagadnienia”, 2006 r.
4. Wykłady – Andrzej Wójcik „Polityka bezpieczeństwa informacji 2005–2008”

CENTRUM KSZTAŁCENIA
I DOSKONALENIA KADR w Warszawie

TELCOMP - SERVICE



zaprasza na kursy zawodowe

więcej informacji: <http://www.centrum-ts.pl>

w zakresie:

- Projektant systemów zabezpieczenia technicznego w klasach SA 2 do SA 4 (od 1490 zł)
- Instalator elektronicznych urządzeń i systemów alarmowych (od 1290 zł)
- Ekspert - doradca w zakresie bezpieczeństwa
- Pracownik stacji monitorowania systemów alarmowych
- Seminarium uzupełniające
- Szkolenie techniki pamięci
- Kurs pracowników w zakresie obsługi monitorowania wizyjnego

Telcomp-Service Sp. z o.o.
ul. Annopol 4
03-236 Warszawa

tel. (022) 811-02-59, tel. kom. 0-662-008-600



TECHNIKA ZABEZPIECZEŃ, OCHRONA OSÓB, MIENIA I DANYCH
CENTRUM KSZTAŁCENIA I DOSKONALENIA KADR
PROFESJONALNE SPRZĄTANIE WNĘTRZ

TELCOMP - SERVICE

SZKOŁA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

TECHOM w WARSZAWIE

inż. Bogdana Tatarowskiego

Zezwolenie Kuratorium Oświaty
i Wychowania w Warszawie nr 663/K/95

zaprasza na

KURSY ZAWODOWE

w zakresie

► Instalowania, konserwacji i eksploatacji systemów alarmowych

Dla przyszłych wykonawców prac instalatorskich
i konserwacyjnych oraz dla użytkowników
systemów, inwestorów i administratorów
obiektów chronionych

► Projektowania systemów alarmowych w klasach od SA-1 do SA-4

Dla obiektów cywilnych i wojskowych
oraz obiektów z tzw. „listy wojewody”

► Zarządzania bezpieczeństwem obiektu

Bezpieczeństwo teleinformatyczne
Wymogi Prawne i normatywne

► Rzeczoznawstwa

- Systemy Technicznego Zabezpieczenia
Osób i Mienia
- Zarządzania Bezpieczeństwem Obiektu

Autoryzacja absolwentów kursów

Dla potrzeb inwestorów
i towarzystw ubezpieczeniowych

Informacja oraz przyjmowanie zgłoszeń:

TECHOM

ul. Marszałkowska 60/27
00-545 Warszawa
tel. 022 625 34 00, 022 625 32 96
tel./faks 022 625 26 75
e-mail: techom@techom.pl
www.techom.com

WANDALOODPORNĄ KONTROLĄ DOSTĘPU

ACIE Polska

02-822 Warszawa ul. Poleczki 21

tel (0-22) 894 61 63, 509 849 791

www.acie.pl info@acie.pl



Możesz
wybrać!

Uczyn swoją kontrolę dostępu
WODOSZCZELNĄ!



- CZYTNIKI
- SZYFRATORY
- BIOMETRIA
- KONTROLER
30 DRZWI

KLASA
SZCZELNOŚCI
DO IP67



- ZWORY
- PRZYCISKI
- ELEKTROZACZEPY
- OSŁONY PRZEWODÓW



Identyfikatory RFID 2,45GHz
dalekiego zasięgu
3-10m



ASD[®]

91-849 Łódź, ul. Zagajnikowa 39
tel. (0-42) 656 43 05, 656 43 10
e-mail: asd@asd.pl



PRZEDSIĘBIORSTWO
FAIR PLAY

• **SPRZEDAŻ URZĄDZEŃ:**
SATEL, EUROFOCUS, BOSCH, BIBI,
VISONIC, ELMES, ROGER, KOBÉ,
CROW, SAMSUNG TECHWIN, CSB.



• **ATRAKCYJNE CENY
I WYSOKIE RABATY
DLA INSTALATORÓW**



• **POMOC TECHNICZNA**



• **SKLEP INTERNETOWY**

• **SZKOLENIA I WARSZTATY**



SYSTEMY SYGNALIZACJI
WŁAMANIA I NAPADU



SYSTEMY TELEWIZJI
DOZOROWEJ



SYSTEMY SYGNALIZACJI
POŻAROWEJ I DSO



SYSTEMY NAGŁOŚNIENIOWE
I PRZYWOŁAWCZE



SYSTEMY KONTROLI
DOSTĘPU



OKABLOWANIE
STRUKTURALNE

www.asd.pl, www.eurofocus.pl

Comelit[®]

GROUP S.P.A.

www.comelit.com.pl

DIVA- ESTETYKA, KTÓRA POCIĄGA



SECUREX 2008
pawilon 3A stoisko 43

DIVA jest kolorowym wideodomofonem o oryginalnej
stylizacji, wyposażonym w 3,5" monitor oraz unikalny
system hands-free.

DYSTRYBUTOR w Polsce:

alarmnet[®]

ALARMNET Sp. J.
ul. Karola Miarki 20c, 01-496 Warszawa
tel. 022 663 40 85, fax 022 833 87 95
biuro@alarmnet.com.pl
www.alarmnet.com.pl

Z C Z A S O P I S M O ZABEZPIECZENIA

Zapraszamy na nasze
stoisko na targach

Securex 2008

Paw. 3A, St. 4

www.zabezpieczenia.com.pl



Cyfrowa KASA PANCERNA

Często chcemy rejestrować nasze poufne dane na nośnikach CD-ROM w taki sposób, aby nikt niepowołany nie mógł ich odczytać. Można je oczywiście zaszyfrować przed zapisem, wykorzystując specjalistyczne oprogramowanie, które służy do tego celu. Nic prostszego? Otóż jest znacznie prostsze i równie skuteczne rozwiązanie – samozapisujące się nośniki o nazwie CDSOft-R Cryptex z wbudowaną technologią szyfrowania zapisywanych danych

Dzięki temu rozwiązaniu w celu zaszyfrowania danych wystarczy je zapisać na nośniku (płyce) CD-ROM firmy TX typu CDSOft-R Cryptex, wykorzystując dowolną nagrywarke, a przy próbie jego odczytu na dowolnym czytniku CD/DVD pojawi się żądanie hasła dostępu do plików.

Płyty CDSOft-R Cryptex zawierają łatwy w obsłudze program nagrywający, który jednocześnie szyfruje zapisywane dane. W ten sposób, posługując się jedynie hasłem, można chronić wrażliwe dane i zabezpieczyć je na nośniku CD-ROM. Do zabezpieczenia wrażliwych plików na znanym ze swojej niezawodności nośniku wystarczy kilka kliknięć. CDSOft-R Cryptex to rozwiązanie służące do skutecznej ochrony, zabezpieczenia i szyfrowania danych. Technologia zaimplementowana na dysku uwalnia od konieczności instalacji jakiegokolwiek oprogramowania. Dla pełnej poufności wszystkie ślady plików przeniesionych na CD (np. pliki tymczasowe) mogą zostać bezpowrotnie usunięte.

Ochrona danych jest realizowana dzięki hasłu o maksymalnej pojemności pliku równej 64 bajty, w którym można użyć do 255 znaków (dopuszczalne, a wręcz zalecane dla lepszej ochrony są znaki specjalne). Zintegrowana klawiatura wirtualna, wyświetlająca się w oknie oprogramowania płyty CDSOft-R Cryptex, umożliwia wprowadzanie hasła przy użyciu myszy, bez pozostawiania śladów na klawiaturze komputera i bez niebezpieczeństwa podglądu klawiatury.

Zapisywanie nośnika jest wykonywane przy użyciu sprawdzonej w innych aplikacjach i niewymagającej uaktualnień technologii „fuzzy logic” Soft-R. Na nośniku udostępnione jest 680 MB miejsca na dane. Możliwa jest wielosesyjność – przestrzeń na CD może zostać zapisana w kilku sesjach, z których każda może zostać zamknięta niezależnie (dane zapisywane sprawdzane są bit po bicie). CDSOft-R Cryptex „chowa” zapisywane pliki do pliku-sejfu, niczym do kasy pancernej.

Plik-sejf jest tworzony dla każdej sesji nagrywania. Użytkownik może zachować wcześniejsze wersje nagrywanych plików. Na strukturę pliku-sejfu składają się dwie części: szyfrowanie (EC) i składowanie danych (DATA). Część DATA jest formatowana w strukturze FAT zgodnej z Windows. Dane są szyfrowane standardowym algorytmem szyfrującym: „AES-256 bit w modzie CBC (Cipher Block Chaining)”. Klucze szyfrujące tworzone są na podstawie hasła użytkownika, za pomocą funkcji rozrztu stochastycznego zgodnie z algorytmem SHA-256. W ten sposób tworzy się nieprzenikalny cyfrowy sejf na pliki. Wszystkie dane w pliku-sejfie są kodowane funkcją losową. Oznacza to, że powtarzalne bloki danych szyfrowane są innymi sekwencjami bitów.

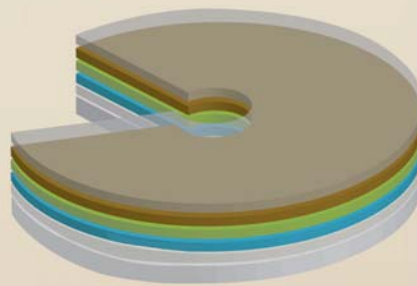
Usuwanie danych odbywa się z wykorzystaniem technologii „WIPE”. Plik przeznaczony do usunięcia zostaje zlokalizowany na dysku, zmienia nazwę w File System Descriptor, a jego zawartość zostaje zamieniona danymi stochastycznymi.

Następnie plik jest wymazywany. W ten sposób na dysku nie pozostają żadne ślady po wymazanym pliku, co uniemożliwia jego odtworzenie. CDSOft-R Cryptex ma podwójne zabezpieczenie przed zarysowaniami i promieniowaniem ultrafioletowym, dzięki czemu „żyje” dłużej niż standardowe nośniki CD-ROM.

CDSOft-R Cryptex to idealne rozwiązanie do ochrony poufnych danych, łączące szyfrowanie oprogramowe z podwyższonym poziomem niezawodności dysku.

Dokładniejsze informacje o rozwiązaniu CD Soft-R Cryptex TX Eastern Europe w Warszawie, przy ul. Wołoskiej 18 (tel. 0 22 842 88 19)

Redakcja opracowano na podstawie literatury firmy TX Eastern Europe



Lakier zabezpieczający
Silkscreen
Warstwa zabezpieczająca
Warstwa odbijająca
Barwnik
Poliwęglan

	CDSOft-R Cryptex
Kompatybilność z VISTA	TAK
Kompatybilność z XP/2000	TAK
Wolne miejsce	680 MB
Instalacja sterowników	NIE
Wielojęzyczność	TAK
Wirtualna klawiatura	16 języków
Długość hasła	do 255 znaków
Algorytm	AES-256 Bits CBS
Technologia „Wipe”	TAK
Wielosesyjność	TAK

Tab. 1. Zestawienie właściwości CDSOft-R Cryptex



CDSOft-R CRYPTEX

Wielkie możliwości dwóch przewodów

System domofonowy i wideodomofonowy BTicino

Opotrzebie stosowania systemów domofonowych i wideodomofonowych nie trzeba przekonywać nikogo. Oddawane do użytkowania budynki mieszkalne są praktycznie zawsze wyposażone w systemy kontroli dostępu, z których domofon jest rozwiązaniem najprostszym. Podstawowa funkcja, jaką realizuje taka instalacja, bez względu na jej zaawansowanie, to zapewnienie bezpieczeństwa mieszkańcom poprzez świadomą kontrolę tożsamości osób wpuszczanych za próg

Na polskim rynku oferowanych jest wiele systemów o zróżnicowanym stopniu zaawansowania, estetyce i wykorzystujących odmienne typologie okablowania, z przewodem koncentrycznym włącznie. W ostatnich latach bardzo wzrosła rola elastyczności stosowanego rozwiązania, konieczności dostosowania do przyszłych zmian, rozbudowy, czy też specyficznych wymagań klientów.

Bardziej niż kiedykolwiek wykonawcy potrzebują propozycji systemu prostego, a jednocześnie elastycznego i o szerokich możliwościach. Takie rozwiązanie zostało pod koniec 2007 roku wprowadzone na polski rynek przez firmę Legrand Polska, a jest nim dwuprzewodowy system domofonowy i wideodomofonowy marki BTicino.

Obecnie wiele budynków to budynki wielorodzinne, a coraz częściej także wydzielone osiedla. Dla tego rodzaju inwestycji został zaprojektowany system dwuprzewodowy BTicino. W gąszczu obecnych na polskim rynku rozwiązań stanowi on swego rodzaju wyjątek – oferuje maksimum możliwości przy ograniczeniu do minimum koniecznego okablowania – wymaga jedynie **dwóch przewodów**.

System dwuprzewodowy BTicino jest przeznaczony dla instalacji każdej wielkości, począwszy od domów jedno- i dwurodzinnych poprzez budownictwo wielorodzinne, a skończywszy na rozległych osiedlach. Jeden system może obsługiwać obiekty lub osiedla liczące nawet do 3900 lokatorów.

Podstawową zaletą systemu jest łatwość i szybkość jego projektowania, instalacji oraz ewentualnej rozbudowy w przyszłości. Wszystko dzięki temu, że system wykorzystuje **tylko dwa niespolaryzowane przewody** w każdym miejscu instalacji. Jest to system w pełni cyfrowy, w którym każde urządzenie ma swój indywidualny adres systemowy, nadany poprzez użycie odpowiednich konfiguratorów.

Istotnymi zaletami systemu są:

- poufność rozmów,
- możliwość realizacji połączeń interkomowych,
- możliwość sterowania funkcjami dodatkowymi,
- możliwość tworzenia podsystemu w mieszkaniu i niezależnych pionów,
- łatwa zmiana systemu domofonowego na system wideodomofonowy z wykorzystaniem tych samych dwóch przewodów,

– możliwość rozbudowy o dodatkowe kamery i tworzenie domowego systemu monitoringu.

Często bywa tak, że to użytkownik końcowy decyduje o ostatecznym wyposażeniu mieszkania lub apartamentu. Dlatego też deweloperzy coraz powszechniej wymagają od projektantów i wykonawców, aby zastosowany system umożliwiał w przyszłości wprowadzanie zmian, zgodnie z indywidualnymi wymaganiami lokatorów. Przykładem może być obiekt, w którym standardowym rozwiązaniem jest instalacja domofonowa, ale za dodatkową opłatą lokator ma mieć możliwość wymiany aparatu na wideodomofon.

W przypadku większości dostępnych na polskim rynku systemów taka potrzeba oznacza konieczność zmiany okablowania lub dokładania do systemu wielu dodatkowych produktów.

System dwuprzewodowy BTicino pozwala na bezproblemowe tworzenie instalacji mieszanych audio i wideo (Rys. 1), czyli takich, w których tylko wybrane lokale będą wyposażone w wideodomofony. Oczywiście wymaga to zastosowania koniecznych dla obsługi przekazu wideo elementów, jak choćby modułu kamery w panelu zewnętrznym. Niemniej jednak, wykorzystując te same dwa przewody, możemy szybko i łatwo zmienić instalację, po prostu wymieniając domofony na wideodomofony. Zastosowanie w panelu zewnętrznym kolorowej kamery jeszcze bardziej poszerza zakres dostępnych opcji – lokator może zdecydować nie tylko, czy chce mieć domofon czy wideodomofon, ale także, czy odbierany obraz ma być czarno-biały czy kolorowy.

Kolejnym przykładem może być sytuacja, w której dla pewnej grupy lokatorów zostają udostępnione dodatkowe funkcje. Oprócz zastosowania w systemie i odpowiedniego skonfigurowania koniecznego przekaźnika lub aparatu, taka operacja nie pociąga za sobą konieczności prowadzenia dodatkowych przewodów lub wykonywania innych skomplikowanych i często trudnych do przeprowadzenia prac.

To tylko dwa podstawowe przykłady rozbudowy funkcjonalności systemu bazowego bez konieczności zmian w istniejącym okablowaniu, które często wiążą się z uciążliwymi i kosztownymi pracami murarskimi. Takich przypadków może być więcej. Może pojawić się potrzeba rozbudowy systemu o dodatkowe panele (kilka bramek lub

wjazdów na osiedle lub dostęp dwuetapowy). Natomiast dodatkowe kamery zewnętrzne pozwoliłyby obserwować otoczenie (np. dzieci bawiące się na placu zabaw) na monitorze domofonu. Posiadacze apartamentów mogą oczekiwać dodatkowego, indywidualnego panelu zewnętrznego lub kamery przy wejściu do lokalu. System dwuprzewodowy BTicino pozwala na stworzenie w budynku wielorodzinnym podsystemu w pojedynczym mieszkaniu (Rys. 1). Taki system, oprócz funkcjonowania w obrębie całej instalacji, będzie realizował funkcje dodatkowe, dedykowane tylko dla wybranego lokalu, wykorzystując wybrane przez lokatora elementy dodatkowe. Mogą to być dodatkowe panele lub kamery, aparaty audio lub wideo wyposażone w funkcję interkomu (wewnętrznej komunikacji w apartamencie), sterowniki dodatkowych funkcji, nawet niezwiązanych z instalacją kontroli dostępu, ale sterowanych z domofonu lub wideodomofonu, z funkcjami automatyki włączanie (sterowanie roletami, oświetleniem etc.).

Wszystkie opisane powyżej przykłady zastosowań w budownictwie wielorodzinnym można zrealizować w systemie BTicino z wykorzystaniem tylko dwóch przewodów. Parametry techniczne pozwalają na realizację instalacji bardzo rozległych, o liczbie lokatorów do 3900 i maksymalnej odległości między panelem zewnętrznym a najdalszym aparatem wewnętrznym wideo aż 600 metrów (1200 metrów dla instalacji domofonowej).

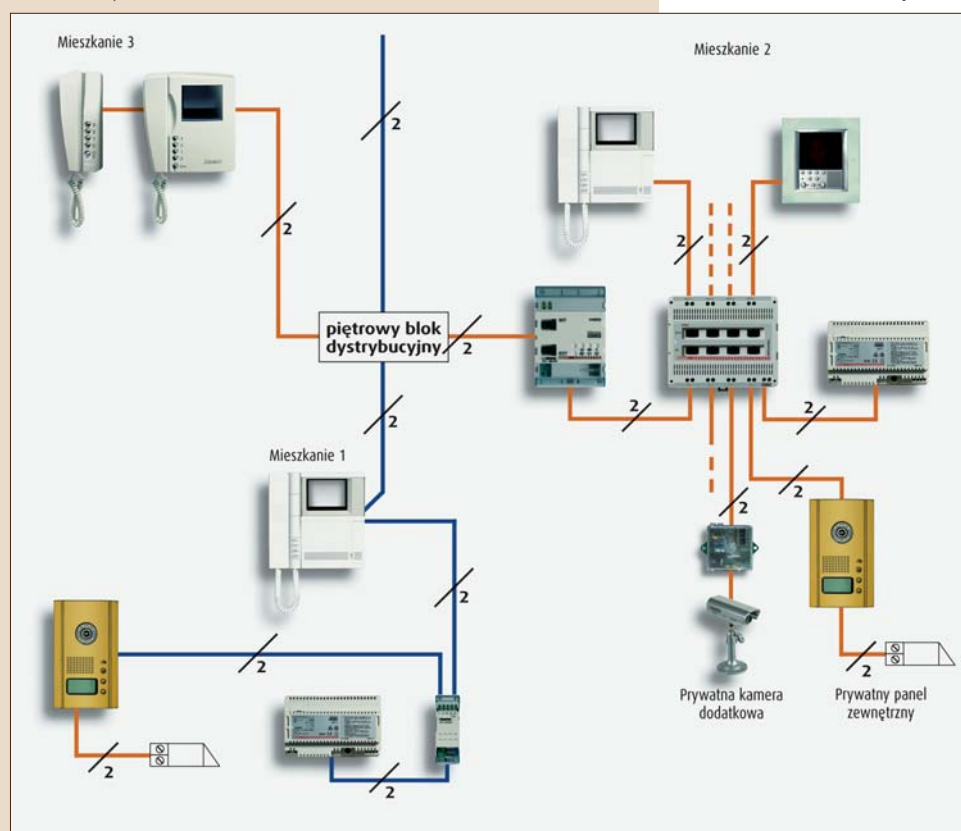
System dwuprzewodowy to doskonale rozwiązanie nie tylko w rozległych instalacjach wielorodzinnych. Również w budownictwie jednorodzinnym otwiera on przed użytkownikami szerokie możliwości. Tak więc oprócz podstawowych funkcji, typowych dla instalacji domofonowej czy wideodomofonowej (odebranie wywołania i otwarcie drzwi), dostępne są dodatkowe funkcje, w zależności od potrzeb inwestora.

W instalacji jednorodzinnej możemy mieć dodatkowe panele zewnętrzne, kamery zewnętrzne, funkcję interkomu, sterowanie dodatkowymi urządzeniami (zapalanie światła,

podlewanie ogrodu, automatyka), domowy system monitoringu, a nawet transmisję obrazu z panelu zewnętrznego na ekran telewizora.

Warto w tym miejscu dodać, że w ofercie BTicino znajdują się również gotowe zestawy domofonowe i wideodomofonowe, które z jednej strony są idealnym rozwiązaniem dla instalacji jednorodzinnych o podstawowych funkcjach, a z drugiej strony pozwalają na rozbudowę w przyszłości. Zestawy dwuprzewodowe, zarówno audio jak i wideo, są idealnym rozwiązaniem, jeżeli chcemy wymienić istniejącą instalację dzwinkową na domofonową lub wideodomofonową. W takiej sytuacji wystarczy zmienić urządzenia, podłączając je do już ułożonych przewodów.

Doskonale funkcjonalnie rozwiązanie to jednak nie wszystkie zalety oferty BTicino. Przy



Rys. 1. Budowa systemu dwuprzewodowego BTicino

Panel zewnętrzny

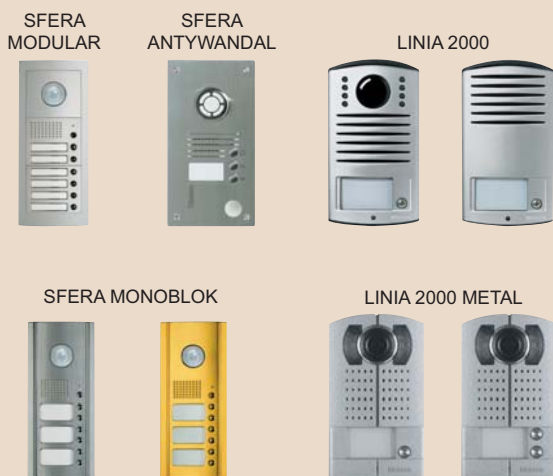
Najdalszy aparat wewnętrzny

← 600 metrów! →

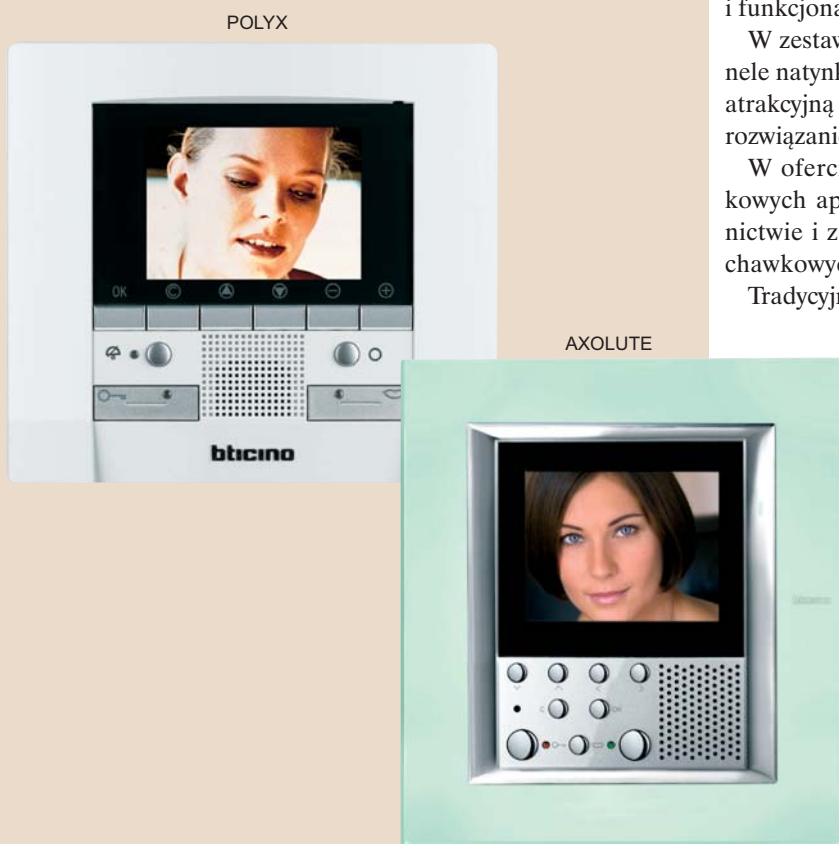
INSTALACJA MOŻE OBEJMOWAĆ:

- 3900** mieszkań
- 5** aparatów wewnętrznych w mieszkaniu
- 96** paneli zewnętrznych wideo
- 3900** prywatnych paneli zewnętrznych
- 39** niezależnych pionów/klatek schodowych

Rys. 2. Możliwości systemu dwuprzewodowego



Fot. 1. Wersje paneli zewnętrznych SFERA oraz LINIA



Fot. 2. Zaawansowane aparaty wewnętrzne



Fot. 3. Aparaty wewnętrzne (video)

projektowaniu oferowanych systemów postawiliśmy sobie wysokie wymagania, wychodząc naprzeciw potrzebom naszych klientów, zwłaszcza w zakresie stylistyki, estetyki i jakości. Oryginalne wzornictwo i bogactwo rozwiązań gwarantuje, że każdy użytkownik znajdzie coś odpowiedniego dla siebie i pasującego do każdego wnętrza, nawet najbardziej ekskluzywnego i nowoczesnego. Dotyczy to zarówno paneli zewnętrznych, jak i aparatów wewnętrznych.

Dla instalacji wielorodzinnych proponujemy panele zewnętrzne w trzech wersjach:

- SFERA MODULAR (kolor aluminium),
- SFERA MONOBLOK (kolor stalowy i mosiężny),
- SFERA ANTYWANDAL (stal).

Każda z wymienionych wersji wykorzystuje jednakowe, uniwersalne moduły funkcyjne, więc ewentualna zmiana w przyszłości ogranicza się wyłącznie do zmiany obudowy. Dodatkowo panele SFERA MODULAR mogą być montowane natynkowo. Taka oferta pozwala na wybranie wzoru najbardziej odpowiedniego pod względem estetycznym i funkcjonalnym.

W zestawach jedno- i dwurodzinnych dostępne są też panele natynkowe LINIA 2000 i LINIA 2000 METAL, łączące atrakcyjną i lekką formę z solidnym, ale łatwym w montażu rozwiązaniem.

W ofercie dostępne są trzy linie tradycyjnych słuchawkowych aparatów wewnętrznych o zróżnicowanym wzornictwie i zaawansowaniu oraz dwa typy aparatów bezsłuchawkowych.

Tradycyjne aparaty audio i wideo:

- SPRINT,
- SWING,
- PIVOT.

Zaawansowane bezsłuchawkowe aparaty wideo:

- AXOLUTE,
- POLYX.

Aparaty Axolute i Polyx posiadają konfigurowalne menu, pozwalające na dostosowanie go do indywidualnych potrzeb użytkownika. Aparaty te umożliwiają nie tylko obsługę funkcji systemu domofonowego i wideodomofonowego, ale także sterowanie funkcjami automatyki, scenariuszami itp.

Wydająca się z Włoch marka BTicino obecna jest w ponad 60 krajach na całym świecie. Jej ofertę, obok wysokiej jakości i funkcjonalności, charakteryzuje silny akcent przypadający na walory estetyczne i nowoczesne wzornictwo.

Dedykowany i wysoko wykwalifikowany zespół inżynierów sprzedaży firmy Legrand Polska służy inwestorom i wykonawcom doradztwem technicznym oraz pomocą przy projektowaniu systemów i wyborze najlepszych rozwiązań BTicino.

LEGRAND POLSKA
INFO.BTICINO@LEGRAND.COM.PL
WWW.BTICINO.PL
INFOLINIA: 0 801 133 084



bticino

BEZPIECZEŃSTWO
ELEGANCJA
KOMFORT

SWING



SFERA



Systemy domofonowe i wideodomofonowe **BTicino** łączą zaawansowaną technologię z wyjątkowo atrakcyjnym włoskim wzornictwem. A wszystko po to, aby zapewnić mieszkańcom bezpieczeństwo i przyjemność użytkowania.

BTicino jest marką znaną i cenioną w ponad 60 krajach świata. Teraz dbamy o wysokie standardy komfortu i bezpieczeństwa w domach naszych Klientów również w Polsce.

www.bticino.pl
0 801 133 084

Marka Grupy | **legrand**

Dystrybutor w Polsce:



AAT Trading Company Sp. z o.o.
02-801 Warszawa, ul. Puławska 431, tel. 022 546 0 546, fax 022 546 0 501
www.aat.pl

Zabezpieczenia kart elektronicznych – nadruk UV – **EDISecure**

Niniejszym artykułem rozpoczynamy serię publikacji o najnowszych zabezpieczeniach kart elektronicznych. Problem z niedozwolonym kopiowaniem spędza sen z oczu nie tylko producentom filmowym. Na długiej liście tych, którzy nie mogą z tego powodu zasnąć, są również użytkownicy i dostawcy kart elektronicznych. Na szczęście ci ostatni są w położeniu o tyle lepszym, że najnowsze technologie dostarczają coraz to bardziej skutecznych rozwiązań w dziedzinie zabezpieczeń przed nieuprawnionym kopiowaniem

W niniejszym krótkim opracowaniu przyjrzymy się technologii nadruku UV, a więc nadruku widzianego w obszarze promieniowania światła ultrafioletowego.

Zasada fizyczna jest prosta: do wykonywania nadruku UV, czy to na banknotach, czy właśnie na kartach elektronicznych, używa się specjalnego atramentu lub farby, która jest niewidzialna. Promieniowanie ultrafioletowe (długość fali 100–380 nm) może powodować świecenie, tj. fluorescencję wielu substancji chemicznych. W praktyce farbę UV ogląda się, oświetlając ją wiązką światła o kolorze fioletowym, które powoduje świecenie substancji chemicznych zawartych w niewidzialnej gołym okiem farbie.

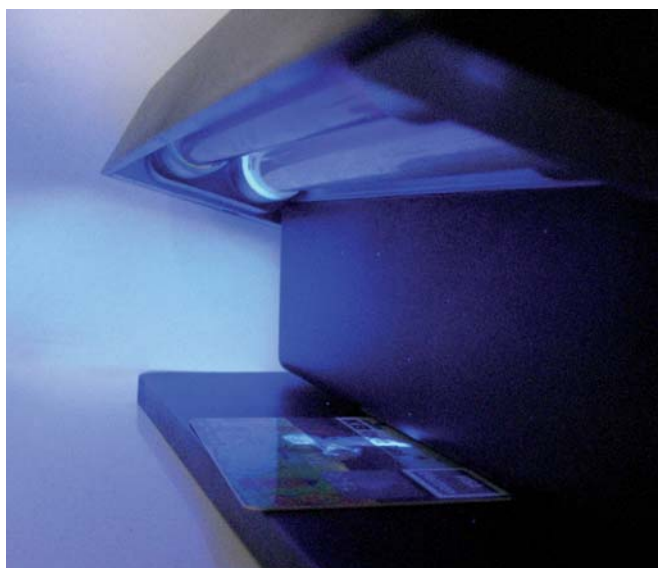
Na kartach elektronicznych stosowano dotychczas metodę pokrywania fragmentu powierzchni nadrukiem wykonanym barwnikiem UV, który można zobaczyć po oświetleniu go specjalnym światłem. Barwnik zakrywał przy tym inne informacje, tj. określony obszar karty musiał być wydzielony wyłącznie do zabezpieczenia nadrukiem UV. Nowość, którą proponuje firma Digital Identification Solutions, polega na zastosowaniu wnikania (*dye-sublimation*) barwnika UV w powierzchnię karty lub folii re-transferowej (PVC) razem z barwnikiem widzialnym gołym okiem.

Innowacje

– Barwnik UV znajduje się pod powierzchnią karty, dzięki czemu jest niewidoczny nawet przy silnym oświetleniu słonecznym. Normalne drukarki dokonują nadruku UV na

powierzchni, przez co nadruki mogą być nieznacznie widoczne przy ustawieniu karty pod odpowiednim kątem do promieniowania słonecznego, które przecież obejmuje spektrum ultrafioletu.

Taśma barwiąca UV używana do nadruków posiada filtr UV. Odczytanie nadruku możliwe jest tylko przy użyciu specjalnego oświetlenia



(w praktyce latarki lub lampki UV), które daje silniejszą wiązkę ultrafioletu niż światło słoneczne.

– Drukarka automatycznie drukuje w ultrafiolecie specjalny numer u góry karty, który jednoznacznie identyfikuje m.in. numer seryjny urządzenia drukującego, co może być nieocenioną pomocą w przypadku konieczności określenia, na którym egzemplarzu drukarki karta została wydrukowana. Drukowania numeru nie można zablokować. Nadruk projektowany jest przy pomocy najnowszej wersji oprogramowania EDISecure.

– Nadruk jest możliwy w 256 odcieniach – jakość fotografii twarzy nie powinna być kwestionowana nawet przez osoby przesadnie dbające o swój wygląd.

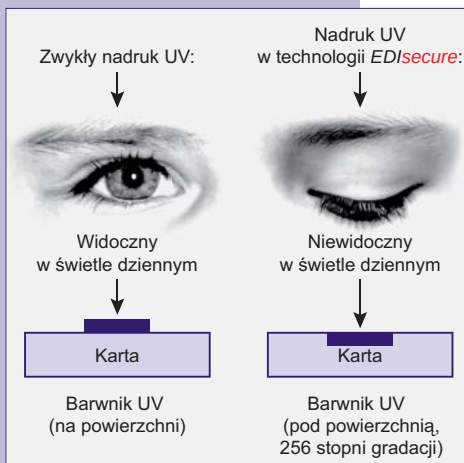
Technologia wyżej opisanego nadruku UV dostępna jest w firmie Digital Identification Solutions, której partnerem w Polsce jest EDP Support Polska (adres: ul. Chłapowskiego 33, 02-787 Warszawa, tel.: 022 644 51 53, faks: 022 644 31 04, www.edps.com.pl).

Securex 2008 – Pawilon 3A, stoisko nr 106



**JANUSZ SALACIŃSKI
EDP SUPPORT POLSKA**

EDPS



System inteligentnego domu HOASIS firmy BPT

Firma BPT znana jest na polskim rynku jako dostawca zaawansowanych technologii systemów wideofonowych zarówno dla domów jednorodzinnych, jak i złożonych systemów wieloblokowych. Od wielu lat BPT intensywnie rozwija również technologię automatyki inteligentnego domu (*Domotica/HomeSapiens*), a pierwsze gotowe rozwiązania zaprezentowała na 50-lecie swojego istnienia na targach w Mediolanie w 2003 roku. BPT oferuje dwie linie produktów: system Hoasis Plus, stanowiący podstawowe narzędzie realizacji większości funkcji automatyki domu, oraz system Nehos, przeznaczony do integracji różnych instalacji, w tym Hoasis, wideofonowej, teleinformatycznych (telefon, WWW, e-mail), bezpieczeństwa (system alarmowy, telewizja dozorowa) oraz audio-video. Niniejszy artykuł prezentuje najważniejsze cechy i typowe zastosowania systemu Hoasis Plus

System Hoasis Plus

Hoasis Plus przeznaczony jest przede wszystkim do zastosowań w obiektach mieszkalnych, takich jak domy, wille, apartamenty czy penthousy. Może być również zastosowany w niewielkich obiektach o charakterze komercyjnym, jak biura, sale konferencyjne, baseny itp. System Hoasis Plus obszarem zastosowań i ogólną ideą, polegającą na zastąpieniu tradycyjnej instalacji elektrycznej instalacją cyfrowego sterowania z rozproszoną logiką, odpowiada znanemu standardowi europejskiemu EIB, choć różni się od niego warstwą sieciową, protokołem komunikacji czy sposobem programowania. Hoasis oparty jest na rozwiązaniu sieciowym LonWorks i protokole komunikacji Lon Talk, który firma BPT wykorzystuje w systemie wideofonowym serii 300.

Niewątpliwą zaletą systemu Hoasis jest możliwość zintegrowania go z systemem wideofonowym X2 BPT za pomocą odbiornika Mitho (Fot. 1), który z jednej strony pełni tradycyjną funkcję aparatu wideofonowego, zaś z drugiej strony stanowi konsolę sterującą systemu Hoasis i systemu alarmowego Brahms BPT.

Hoasis Plus, realizując funkcje sterujące inteligentnego domu, umożliwia (Rys. 1):

- strefową regulację temperatury (grzanie i chłodzenie) według automatycznych harmonogramów i ręcznych ustawień,
- sterowanie oświetleniem w sposób dwustanowy i płynny, również przy pomocy scenariuszy i harmonogramów czasowych,
- otwieranie i zamykanie żaluzji, rolet, okien dachowych, bram, zaworów gazu i wody – ręcznie, automatycznie oraz pod wpływem czujników,
- automatyczne podlewanie ogrodu,
- optymalizację zużycia energii w porze dużego zapotrzebowania,
- obsługę zdarzeń alarmowych.



Fot. 1. Odbiornik Mitho. Wideofon, terminal Hoasis, konsola Brahms

Podstawowym interfejsem dla użytkownika w systemie Hoasis jest montowany natynkowo terminal OH/T (Fot. 2) z monochromatycznym, podświetlanym ekranem dotykowym o przekątnej 4 cale. W systemie można użyć do 3 terminali OH/T, a każdy z nich umożliwia pełny dostęp do funkcji sterujących Hoasis. W systemie Hoasis wymagane jest zastosowanie modułu OH/A, który dostarcza zasilanie do pozostałych urządzeń i jest odpowiedzialny za realizację niektórych funkcji, np. timera. Oprócz wielofunkcyjnych terminali OH/T do sterowania temperaturą w strefie można zastosować termostaty cyfrowe z nastawnikiem i wyświetlaczem LCD o symbolu OH/Z (Fot. 3).

Terminal OH/T dzięki prostocie i niewielkim rozmiarom pasuje do każdego wystroju wnętrza. Moduły OH/Z sterujące ogrzewaniem w strefie dostępne są w dwóch kolorach: czarnym i białym, a znajdujące się w zestawie adaptory pozwalają na zainstalowanie ramek o różnych stylizacjach i kolorach.

Wszystkie moduły w systemie Hoasis łączy się magistralą o swobodnej topologii, wykorzystującą dwużyłową, nieekranowaną

Moduł	Funkcja	Liczba i rodzaj wyjść	Liczba wejść
OH/R.01		4 (NC/NO)	4
OH/6I		0	6
OH/RI		1 (NO)	3
OH/RP		1 (NO o zwiększonej obciążalności)	
OH/2RP		2 (NO o zwiększonej obciążalności)	
OH/3RPI		3 (NO o zwiększonej obciążalności)	3
OH/MA	sterowanie żaluzjami	2 (UP, DOWN), 1 NC/NO	3 (UP, Stop, DOWN)
NH-DIM	ściemniacz	1 (analogowe 0-10V), 1 (NO)	1
OH/Z			1

Tab. 1. Zestawienie modułów Hoasis

skrętkę niepolaryzowaną, której łączna długość może wynosić do 500 m.

W podstawowej konfiguracji przy programowaniu ręcznym system pozwala na podłączenie 64 przełączników i 71 wejść służących do ichysterowania, zdefiniowanie 16 timerów i 3 scenariuszy. Przy programowaniu z użyciem komputera PC i specjalizowanego programatora elastyczność i możliwości systemu znacznie wzrastają osiągając pojemność do 255 wejść, 255 wyjść przełącznikowych, 20 niezależnych stref ogrzewania (sterowane modułami OH/Z lub terminalami OH/T), 40 timerów i 16 scenariuszy.

System Nehos

Nehos jest rozwiązaniem wyższego poziomu funkcjonalnego, integrującym w sobie sterowanie i obsługę większości elektrycznych i elektronicznych instalacji oraz mediów w domu. Nehos realizuje wszystkie funkcje systemu Hoasis, gdyż Hoasis staje się jednym z wielu zintegrowanych przez Nehos systemów. Różnica w obsłudze obu systemów polega na tym, że terminale OH/T zostają zastąpione wielofunkcyjnymi terminalami dotykowymi Nehos NH-T (Fot. 4).

Poza funkcjami sterowania realizowanymi w systemie Hoasis terminal Nehos NH-T pozwala wykorzystać kolorowy ekran dotykowy o przekątnej 8,4 cala do (Fot. 5):

- podglądu obrazu z kamer CCTV,
- obsługi centrali alarmowej Brahms BPT,
- przeglądania stron WWW,
- korzystania z poczty e-mail,
- oglądania telewizji,
- odtwarzania filmów wideo (np. z DVD),
- korzystania z telefonu (zarówno stacjonarnego, jak i opartego o technologię VOIP).

Dodatkowym atutem jest możliwość integracji systemu z siecią domofonową, wideofonową i interkomową w technologii X2/300 firmy BPT.

Nehos w najprostszej konfiguracji można traktować jako rozwinięcie systemu Hoasis, w którym terminale OH/T oraz jednostka zasilająca OH/A zostają zastąpione terminalami NH-T (maks. 7) łączonymi z jednostką centralną NH-BC przy użyciu sieci Ethernet. Dzięki standardowi Ethernet otrzymujemy dużą elastyczność wyboru miejsca podłączania terminali, a ponadto możliwość emulacji (wirtualizacji) terminala przy wykorzystaniu popularnych przeglądarek WWW (Microsoft Internet Explorer, Mozilla Firefox) na dowolnym komputerze PC do sterowania wszystkimi funkcjami systemu Nehos.

Istnieje również możliwość zdalnego podłączenia się do sieci Nehos spoza domu (np. z biura, hotelu) za pośrednictwem rutera lub kanału VPN i sterowania wszystkimi funkcjami wyłącznie z podglądem obrazu z kamer CCTV.

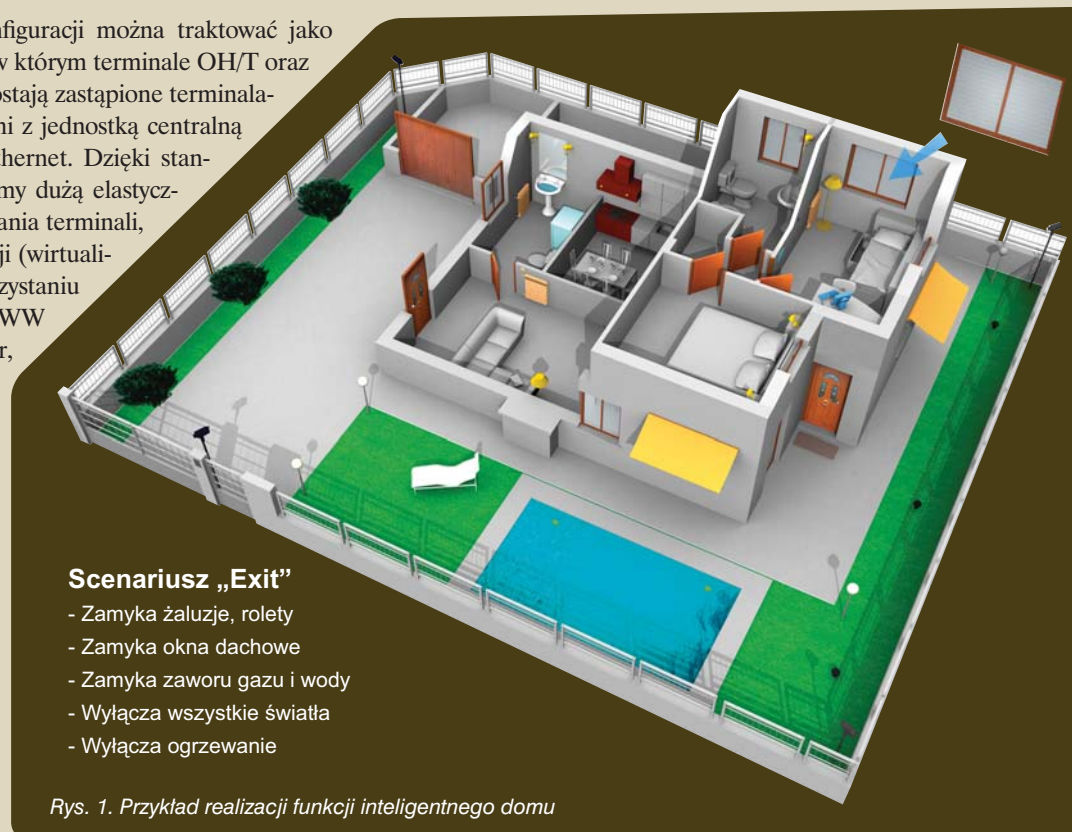
Poza połączeniem przewodowym terminala NH-T



z jednostką centralną NH-BC, Nehos oferuje również połączenie bezprzewodowe w technologii Wi-Fi, dzięki czemu uzyskuje się pełną swobodę korzystania z terminala w każdym miejscu w domu.

Urządzenia systemu Hoasis

W systemie Hoasis poza wymienionymi wcześniej podstawowymi elementami OH/T, OH/A i OH/Z stosuje się różne moduły wejściowo-wyjściowe. Przez wejście rozumiane jest



Scenariusz „Exit”

- Zamyka żaluzje, rolety
- Zamyka okna dachowe
- Zamyka zaworu gazu i wody
- Wylacza wszystkie światła
- Wylacza ogrzewanie

Rys. 1. Przykład realizacji funkcji inteligentnego domu

dowolne urządzenia stykowe, np. czujnik, przycisk, przełącznik. Wejścia sterują wyjściami przełącznikowymi. Oferowane przez BPT moduły wejściowo-wyjściowe (patrz tabela poniżej) są zaprojektowane tak, aby były dopasowane do typowych funkcji sterujących instalacji, zapewniając jednocześnie pełne wykorzystanie wszystkich portów. Moduły wejściowo-wyjściowe mogą zostać zainstalowane w skrzynkach elektrycznych na szynie DIN lub w puszkach elektrycznych pod wyłącznikami ze względu na niewielkie rozmiary.

Poza standardowymi przełącznikami BPT oferuje przełączniki o zwiększonej obciążalności styków, moduł NH-DIM do płynnego sterowania natężeniem oświetlenia oraz dedykowany moduł OH-MA przeznaczony do sterowania roletami, oknami czy bramami.

Zastosowanie systemu Hoasis

Wyobraźmy sobie, że po wejściu do domu jednym przyciskiem włączamy wszystkie potrzebne nam urządzenia, punkty świetlne, odsłaniamy rolety oraz nastawiamy odpowiednią temperaturę w pomieszczeniach. Podobnie, wychodząc z domu, jednym przyciskiem wyłączamy oświetlenie, wyłączamy ogrzewanie lub chłodzenie, w zależności od pory roku, utrzymując dyżurną temperaturę, zamykamy zawory wody i gazu, uzbrajamy system alarmowy. Podlewanie ogrodu uruchamiane jest w wybrane dni tygodnia o wyznaczonej przez nas godzinie, a rolety same zasuwały się na wypadek burzy lub silnego wiatru. Wszystko to możliwe jest właśnie dzięki systemowi automatyki Hoasis Plus.

Podstawowym mechanizmem funkcjonalnym obsługi systemu są scenariusze. Są to zdefiniowane sekwencje czynności,

które mogą aktywować/dezaktywować wybrane wyjścia, sterować roletami, zmieniać tryb pracy ogrzewania/klimatyzacji w danej strefie. Przykładem może być tu scenariusz „Wyjście”, wyłączający wszystkie światła w domu, zamykający rolety i wyłączający ogrzewanie wszystkich stref. Innym przykładem może być scenariusz „Noc”, który wyłącza niepotrzebne światła, zamyka żaluzje i bramy, zamyka zawory gazu i wody, uzbraja system alarmowy w trybie nocnym. Scenariusze mogą być uruchamiane z terminali OH/T, zwykłych przycisków montowanych w różnych miejscach domu oraz przy pomocy timerów.

Poza wyborem wejść sterujących poszczególnymi wyjściami Hoasis daje możliwość wyboru odpowiedniej funkcji, czyli sposobu realizacji tego wystrojenia („włącz”, „wyłącz”, „przełącz”, „bezpośrednio”, „impulsowo”, „zezwolenie”). Zestaw tych prostych



Fot. 5. Funkcje terminala Nehos NH-T

czynności, wykonanych kolejno dla wszystkich wejść i wyjść, pozwala na pełne skonfigurowanie systemu.

Zdalny nadzór nad domem

Moduł GSM dostępny w systemie Hoasis, obsługiwany przy pomocy standardowego telefonu komórkowego poprzez wysyłanie wiadomości SMS, pozwala na sprawdzenie stanu systemu automatyki na żądanie lub raportowanie jego stanu co 12 lub 24 godziny, a także zapewnia powiadomienie o wszystkich ważnych zdarzeniach w domu, takich jak alarmy czy awarie. Ponadto moduł daje możliwość zdalnego uruchomienia wybranego scenariusza, ustawienia trybu pracy termostatu, sprawdzenia temperatury i statusu regulacji temperatury we wszystkich strefach domu.

Podsumowanie

Zastosowanie systemu Hoasis to z jednej strony wygoda, elastyczność i przyspieszenie obsługi wielu instalacji w domu, a z drugiej strony optymalizacja kosztów zużycia energii i mediów. Automatyzacja czynności sterujących za pomocą scenariuszy to także zwiększenie bezpieczeństwa i ochrony domu przed różnymi zagrożeniami oraz wyeliminowanie polegania na często zawodnej pamięci ludzkiej. Możliwość programowania i zmiany funkcji oraz scenariuszy pozwala dopasować je do indywidualnych potrzeb lokatorów bez konieczności modyfikacji instalacji przewodowej, często niemożliwej w tradycyjnym rozwiązaniu.

Hoasis stanowi podstawowe a jednocześnie wystarczające narzędzie do zrealizowania większości funkcji sterujących inteligentnego domu, otwierając także drogę do realizacji bardziej wyrafinowanego systemu integrującego, jakim jest system Nehos.

Nowy odbiornik wideofonowy Mitho firmy BPT z kolorowym dotykowym wyświetlaczem LCD, stanowiącym jednocześnie interfejs do zarządzania automatyką domu Hoasis i systemem alarmowym Brahms, będzie naturalnym pomostem i ogniwem łączącym rozwiązania BPT w zakresie wideofonów ze światem automatyki inteligentnego domu.

ANDRZEJ GRODECKI
MACIEJ KRZYCZKOWSKI



Fot. 2. Terminal Hoasis OH/T



Fot. 3. Termostat strefowy z nastawnikiem Hoasis OH/Z



Fot. 4. Terminal Nehos NH-T

bpt

MITHO



Ekran dotykowy 16:9
Rozdzielczość 480x272

3 w 1

- System wideofonowy
- Inteligentny dom
- System alarmowy

BPT znów zaskakuje

www.bpt.pl

IQinvision
smart camera systems

logiware

VIVOTEK

milestone

Monitoring wideo IP

- kamery megapikselowe
- kamery ip
- systemy rejestrujące

NASZ

IP

212.85.105.79

SECUREX 2008
PAWILON 3A

Sumo

PPHU SUMA SP. Z O.O.
Ul. Rozdzińskiego 88A
40-203 Katowice
tel. +48(032) 258 05 97
www.suma.com.pl

Rejestratory cyfrowe 4-, 8-, 16-kanałowe marki **EuroFocus®**



Model	EF-DF400	EF-DF8010VGA	EF-DVR166VGA
Wejścia video przelotowe	4 x BNC	8 x BNC	16 x BNC
Wejścia audio	4 x RCA		
Wyjścia wideo	2 x monitor BNC		
Wyjścia audio	tak		
Wyjście VGA	opcja	tak	
Prędkość zapisu	maks. 100 kl./s		
Rozdzielczość zapisu	720 x 480		
Rozdzielczość wyświetlania	720 x 576		
Kompresja	MPEG-4		
Funkcja triplex	zapis / odtwarzanie / transmisja po sieci		
Tryby zapisu	ciągły / ręczny / kalendarzowy / alarmowy / detekcja ruchu		
Tryby odtwarzania	prędkość odtwarzania x1, x2, x4, x8, x16, obraz zatrzymany (STILL)		
Wyszukiwanie zapisu	czas, zdarzenie, plik		
Archiwizacja	USB, CD-RW, sieć		
Zasoby dyskowe	4 szt. do 500 GB	1 + 4 szt. do 500 GB	
Sterowanie	panel przedni / RS485 / pilot IR (w komplecie)		
Funkcje sieciowe	przeglądanie na żywo / odtwarzanie archiwum / archiwizacja		
Zabezpieczenia zapisu	znak wodny		
Zasilanie	12V / 5A DC, zasilacz w komplecie		
Wymiary	440 x 401,9 x 88 mm		
Masa	około 7 kg		

Kamery w obudowie wandaloodpornej



Model	EF-500 D	EF-500 DV
Przetwornik	1/3", kolor, SONY	
Ilość pikseli	795 (H) x 596 (V)	
Rozdzielczość	540 TVL	
Czułość DZIEN/NOC DSS	0,3/0,01 lx	0,3/0,003 lx
Funkcje specjalne	zaawansowana konfiguracja menu cyfrowa redukcja szumu	
Odstęp sygnał/szum	50 dB	
Migawka	1/50 - 1/100 000 s	
Obiektyw	3,7 mm	4 - 9 mm A.I.
Zasilanie/pobór prądu	12V DC / 180 mA	
Temperatura pracy	-25°C / +50°C	
Temperatura przechowywania	-10°C / +55°C	
Wymiary	61 x 55 x 104 mm	
Masa	400 g	

ASD®

ASD SYSTEMY ZABEZPIECZEŃ

ul. Zagajnikowa 39
91-849 Łódź
tel. (42) 656 43 05
fax (42) 656 47 90

www.asd.pl
www.eurofocus.pl
email: asd@asd.pl
email: sklep@eurofocus.pl

Kolorowe drukarki do kart identyfikacyjnych PVC


MAGICARD


HoloKote™ - znak wodny drukowany na całej powierzchni karty. Widoczny przy patrzeniu pod kątem.



Nadruk od krawędzi do krawędzi z jakością 300 dpi.



HoloPatch™ - okno w rogu karty, w którym znak wodny jest bezpośrednio widoczny (opcja karty).



Możliwość kodowania pasków magnetycznych (opcja).



Dwustronny nadruk – tylko drukarka Avalon Duo.



Taśmy kolorowe nadruk 250, 300 lub 350 kart.
Taśmy monochromatyczne nadruk 1000 kart.
Kolory taśm monochromatycznych: czarny, czerwony, niebieski, zielony, złoty, srebrny, biały oraz taśma typu scratch-off (zdrapka).

Specyfikacja techniczna

Prędkość nadruku

Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund

Monochromatyczny wydruk karty w 6 sekund

Cykl działania

Ciągły

Wbudowane zabezpieczenia

HoloKote™ anty-coping – znak wodny na całej powierzchni karty

Typ taśmy

AV1: YMCKO nadruk 250 kart

LC1: YMCKO nadruk 350 kart

LC3: Monochromatyczny nadruk 1000 kart

LC8: YMCKOK nadruk dwustronny 300 kart (tylko Avalon Duo)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR80 o grubości od 0,38 mm do 1,6 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych
Dostępne karty z HoloPatch™

Pojemność magazynków kart

Podajnik 100 kart

Zasobnik kart nadrukowanych 50 sztuk

Głowica

300 dpi (wymenna)

Interfejs do PC

USB rev. 1.1. (kompatybilny z USB 2.0)

Sterowniki

Windows 2000, XP, VISTA

Kompatybilność elektromagnetyczna i certyfikat

EN 50 081-1 i EN 50 082-1 (Europa)/CE

Zasilanie

90-265 V / 47-63 Hz

Wymiary

Avalon (445 x 200 x 220) mm

Avalon Duo (470 x 200 x 220) mm

Masa

Avalon około 7,2 kg

Avalon Duo około 8,3 kg

Kolor

Srebrny metalik (fioletowe ścianki boczne)

Temperatura pracy

10-30°C

Gwarancja

2 lata

Dystrybutor w Polsce:

ACSS ID Systems Sp. z o.o.

ul. Karola Miarki 20C
01-496 Warszawa

tel. (22) 832 47 44, fax (22) 832 46 44

biuro@acss.com.pl

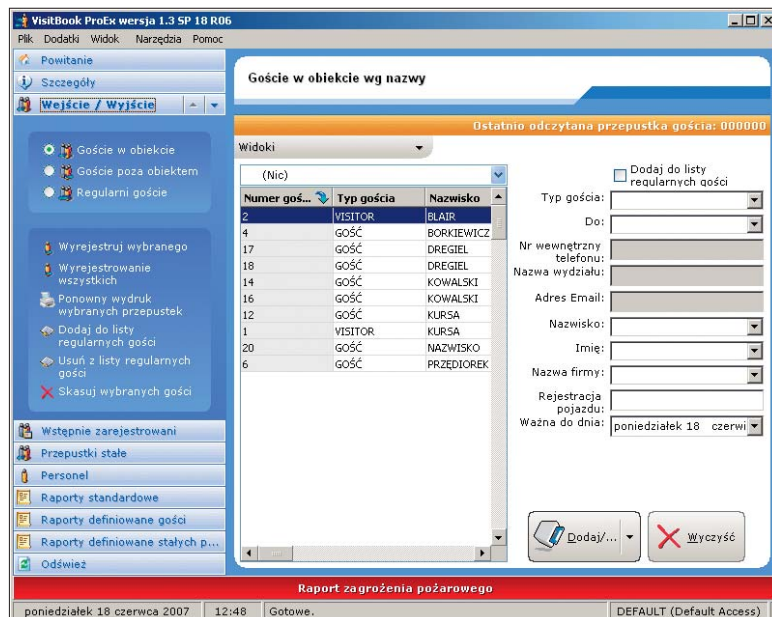
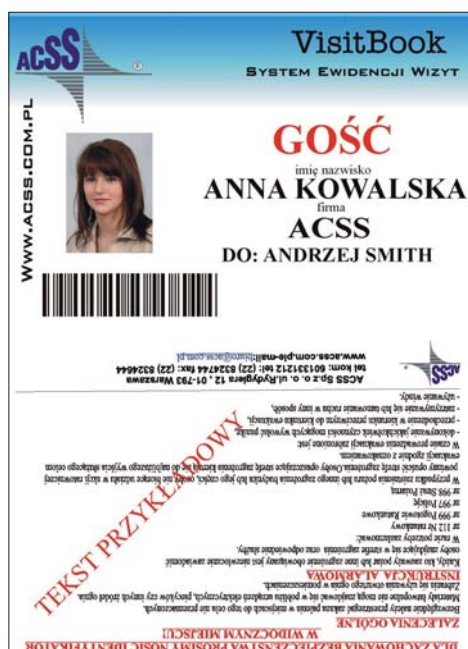
www.acss.com.pl

www.magicard.com.pl



System rejestracji gości VisitBook

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



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

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

Ostatnia z nich – wersja ProEx jest wersją najbardziej rozbudowaną. Umożliwia ona wydruk przepustki wraz ze zdjęciem oraz zawiera między innymi funkcję projektowania własnych wzorów przepustek. Wydruk przepustek możliwy jest na standardowych drukarkach biurowych oraz drukarkach termosublimacyjnych do kart PVC (tylko wersja ProEx).

Zasadniczą zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program dodatkowo zawiera kilka użytecznych funkcji takich jak: manager personelu, manager kontrahentów, obsługa konferencji.

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



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

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

GOLD-IBT

inteligentny tester akumulatorów

Producenci akumulatorów zalecają wymianę akumulatora, jeżeli jego współczynnik pojemności spada poniżej 65%. Typowym miernikiem można zmierzyć tylko napięcie akumulatora.

Jak zmierzyć jego pojemność?

Inteligentny Tester Akumulatorów GOLD-IBT w kilka sekund dokonuje symulacji pełnego rozładowania akumulatora. Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.



- Testuje w ciągu kilku sekund akumulatory wykonane w technologii AGM (elektrolit uwięziony w separatorach z włókna szklanego) – powszechnie używane w systemach alarmowych i UPS.
- Automatycznie wyświetla temperaturę otoczenia, napięcie akumulatora i aktualną pojemność.
- Cyfrowo zaprogramowany do pomiaru szczelnych akumulatorów (SLA) 12 V oraz akumulatorów samochodowych o pojemności od 1,2 Ah do 200 Ah.
- Testuje akumulatory szybko, dokładnie i jest łatwy w użyciu.

Dane techniczne:

Model: GOLD-IBT

Zasilanie: 12 V DC (10-15 V DC)

Typ akumulatora: szczelne akumulatory (SLA) 12 V oraz akumulatory samochodowe

Pojemność akumulatora: 1.2 Ah – 200 Ah

Symulowany test rozładowania akumulatora: C20 do 10,50 V DC @ 25°C

Wyświetlacz: podświetlany LCD

Pomiar temperatury: 0°–100°C

Ostrzeżenie o zbyt wysokim napięciu: >15 V DC

Ostrzeżenie o zbyt niskim napięciu: <10 V DC

Ostrzeżenie o zbyt niskiej pojemności: < 0.5 Ah

Tolerancja pomiaru Ah: 10% (zależy od konstrukcji i parametrów produkcyjnych akumulatora)

Zabezpieczenie temperaturowe odwrócenia polaryzacji: dioda blokująca

Zdolność wykonania kolejnych testów: do 15 następujących bezpośrednio po sobie

Ostrzeżenie przed przegrzaniem: >55°C ±10°

Wymiary: 111 mm x 55 mm x 35 mm

Długość przewodów przyłączeniowych: 40 cm

Masa w opakowaniu: 400 gramów

Zawarte akcesoria: futerał, certyfikat zgodności, etykiety na akumulatory

Gwarancja: 1 rok

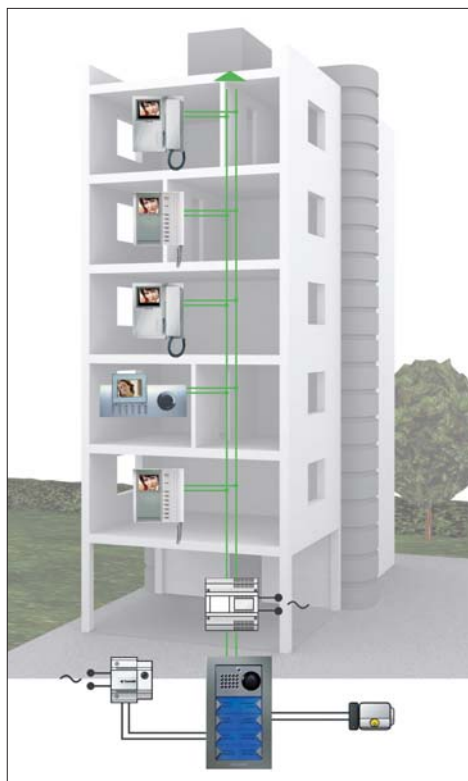
alarmnet®

ALARMNET Sp. j.
ul. Karola Miarki 20C
01-496 Warszawa

tel.: 022 663 40 85
faks 022 833 87 95
www.alarmnet.com.pl

2-przewodowy, kolorowy system wideodomofonowy

firmy COMELIT



Cechy systemu:

- kolorowe monitory z ekranami LCD;
- 2 przewody łącznie z zasilaniem monitora;
- 4 magistrale na zasilacz (np. 4 piony w budynku mieszkalnym);
- do 8 monitorów z funkcją interkomu na każdy apartament;
- do 240 użytkowników;
- do 600 m maksymalnej odległości pomiędzy panelem wejściowym, a ostatnim monitorem;
- nieograniczona liczba paneli głównych i dodatkowych;
- centralny moduł portiera;
- proste programowanie za pomocą przełączników;
- możliwość tworzenia systemów mieszanych audio i wideo.

Aparaty wewnętrzne dostępne w systemie Simplebus Color



GENIUS



BRAVO



DIVA



UNIFON STYLE

Panele wejściowe



W systemie Simplebus2 można zastosować panele wejściowe serii Powercom jak i wandaloodporne Vandalcom. Oba panele występują w wersji cyfrowej z elektronicznym spisem nazwisk oraz z indywidualnymi przyciskami wywołania. Ramki zewnętrzne paneli dostępne są w różnych kolorach.



Dystrybutor w Polsce:

alarmnet[®]

Alarmnet Sp.j.

ul. Karola Miarki 20c
01-496 Warszawa
tel. (22) 663 40 85, fax (22) 833 87 95

e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl
www.comelit.com.pl

DF6000 – nowoczesna adresowalna centrala sygnalizacji pożaru

Charakterystyka centrali DF6000:

- Wersje jedno, dwu oraz czteropętlowe
- Adresowanie programowe wraz z liniami bocznymi
- Szeroki wybór kompatybilnych urządzeń pomocniczych
- Jasnoszary lub grafitowy kolor obudowy
- Zintegrowana drukarka w opcji
- Opcjonalna, zamykana, przezroczysta pokrywa jako ochrona wyświetlacza
- Centrale mogą pracować samodzielnie lub połączone w sieć
- 127 adresów w pętli
- Przyjazne i proste oprogramowanie
- Niepowtarzalny i estetyczny wygląd



DF6000 jest wysoko wyspecjalizowanym nowoczesnym, adresowalnym systemem detekcji i sygnalizacji pożaru, który łatwo można dopasować do różnych obiektów. Łączy w sobie wysoką funkcjonalność z łatwą obsługą i estetycznym wyglądem.

OPIS SYSTEMU

- System składa się z centrali DF6000 oraz szerokiego zakresu kompatybilnych detektorów, ręcznych ostrzegaczy pożarowych, sygnalizatorów akustycznych, sygnalizatorów optycznych, paneli wyniesionych i interfejsów
- Każde z urządzeń zewnętrznych DF6000 zawiera integralny izolator zwarcia, aby zapewnić maksymalną ochronę przed zwarciami w obwodach zewnętrznych

Specyfikacja techniczna centrali DF6000

Normy	EN 54-2 1998 & EN 54-4 1998, EN 50130-4
Liczba pętli	1 - DF6000/1 2 - DF6000/2 4 - DF6000/4
Maksymalna liczba adresów w pętli	127
Liczba linii konwencjonalnych sygnalizatorów akustycznych	4 (możliwe do programowania w parach)
Pomocnicze wyjście do sterowania urządzeniami gaśniczymi	(monitorowane) 24 V, 30 mA
Pomocnicze wyjście do sterowania urządzeniami pomocniczymi	(monitorowane) 24 V, 30 mA
Pomocnicze wyjście alarmowe do stacji monitorowania	(monitorowane) 24 V, 30 mA
Napięcie znamionowe systemu	24 V
Wejście zasilania sieci	230 V AC +10% / -15%
Pomocniczy przekaźnik	1 styk przełączny, aktywowany w przypadku pożaru
Porty wyjścia	RS485, RS232
Czas podtrzymania w przypadku awarii zasilania 230 V	Zależy od obciążenia obwodu oraz konfiguracji baterii do 72 h
Bateria	2x12 Ah (wersje standardowe) 4x12 Ah (wersje EB)
Wejścia przewodów	35 z góry, 4 z dołu, 2 z boku (20mm)
Warunki pracy	IP30; od -50°C do +40°C; wilgotność maks. 5% (bez kondensacji)

INTERFEJS UŻYTKOWNIKA

- Głównym elementem interfejsu użytkownika w centrali DF6000 jest dużych rozmiarów (120mmx90mm obszar widzenia) dotykowy ekran LCD, który dostarcza użytkownikowi informacji, jak również odgrywa rolę wielofunkcyjnej klawiatury.
- Centrala DF6000 zawiera 96 diod LED, dostarczających jasnych informacji o stanie systemu i rozprzestrzenianiu się ognia

ZDOLNOŚĆ WYKRYWANIA

- Do centrali DF6000 możemy podłączyć maksymalnie cztery pętli, w każdej pętli 127 adresów, zgodnie z obowiązującymi przepisami.
- Do jednej centrali nie powinno być podłączonych więcej niż 512 adresów
- W sieć możemy podłączyć 63 centrale, co daje całkowitą pojemność systemu ponad 32 tys. urządzeń

ZDOLNOŚĆ ALARMOWANIA

- Do 60 zasilanych sygnalizatorów akustycznych i optycznych lub interfejsów wyjściowych w pętli
- 3 poziomy dostępu dla konserwacji, serwisu i programowania urządzeń wyjściowych
- 4 wyjścia konwencjonalnych sygnalizatorów na płycie centrali
- Dodatkowe, konwencjonalne sygnalizatory akustyczne mogą być podłączona do modułu MPU424

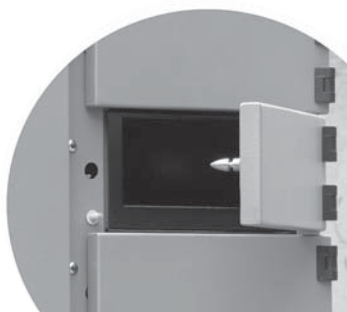


D+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław

tel. (71) 323 52 50, fax (71) 323 52 40
e-mail: biuro@dhpolska.pl
www.dhpolska.pl

Wewnętrznie monitorowane skrytki depozytowe

SAIK BOX jest najnowszym systemem, z produkowanej przez bt electronics rodziny systemów SAIK. Cechą wspólną każdego z tych produktów jest gromadzenie i przetwarzanie informacji związanych z użytkowaniem systemu. Imię i nazwisko osoby deponującej lub pobierającej przedmioty ze skrytek oraz dokładne parametry czasu i miejsca zdarzenia tworzą podstawowy zapis w historii działania systemu. Modułowa budowa SAIK BOX pozwala nie tylko na rozbudowę systemu o kolejne segmenty, ale również na wybór ilości oraz wielkości poszczególnych skrytek. Bogactwo opcji konfiguracyjnych dostępnych z poziomu oprogramowania umożliwia idealne dopasowanie działania systemu do indywidualnych potrzeb użytkownika. Dzięki kamerom zainstalowanym w każdej skrytce, administrator ma możliwość przeglądania zdjęć zrobionych podczas deponowania i pobierania każdego przedmiotu, co znacząco wpływa na podniesienie poziomu bezpieczeństwa chronionego mienia. Interesującym rozwiązaniem są także komputerowe stanowiska alarmowe, do których spływają na bieżąco komunikaty o zdarzeniach zachodzących w systemie. Dzięki podłączeniu systemu do sieci Ethernet/Internet, lokalizacja stanowisk alarmowych jest dowolna, dlatego mogą one znajdować się zarówno na stanowisku ochrony, jak i w siedzibie firmy oddalonej nawet bardzo od miejsca zainstalowania systemu.



Specyfikacja techniczna

Wymiary	wysokość x szerokość x głębokość
moduł wąski	850 x 260 x 360
moduł szeroki	850 x 520 x 360
Rozmiary skrytek w modułach	wysokość x szerokość x głębokość
moduł wąski	76 x 160 x 300, 176 x 160 x 300, 376 x 160 x 300
moduł szeroki	76 x 420 x 300, 176 x 420 x 300, 376 x 420 x 300
Zasilanie główne	230 V
Zasilanie awaryjne	min. 4 h
Kolor	RAL 9007*
Czytnik identyfikatorów	dowolny
Pin użytkownika	tak (do 32 znaków)
Identyfikacja przedmiotu znajdującego się w skrytce	tak* (czytnik zbliżeniowy)
System komunikatów głosowych	tak
Sposób połączenia elementów systemu	sieć Ethernet
Dotykowy ekran ciekłokrystaliczny	tak
Imienna identyfikacja użytkownika na wyświetlaczu LCD	tak
Rejestracja przedmiotów w momencie deponowania w skrytkach	tak (zdjęcia)
Kod skrytki	tak
Maks. liczba skrytek obsługiwanych przez jeden panel główny	120
Maks. liczba skrytek obsługiwanych przez system	bez ograniczeń
Maks. liczba pracowników obsługiwanych przez system	bez ograniczeń
Maks. liczba paneli modułów obsługiwanych przez system	bez ograniczeń
Indywidualne przydziały dostępu do skrytek	tak
Grupy pracowników	tak
Strefy czasowe	tak
Stanowiska alarmowe	tak
Minimalne wymagania stanowiska komputerowego administratora	Win 98
Liczba stanowisk komputerowych z zainstalowanym oprogramowaniem	bez ograniczeń
Format bazy danych	PostgreSQL

*wyposażenie lub zmiana – opcjonalnie na życzenie klienta



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

System wideodomofonowy serii 480



GDE POLSKA wprowadza do sprzedaży nowy system wideodomofonowy przeznaczony do instalacji w biurach, budynkach mieszkalnych i osiedlach zamkniętych. System może obsłużyć do 480 abonentów.

System charakteryzuje się bardzo prostą instalacją i programowaniem.

W skład systemu wchodzi:

- kamery DRC-480L
- monitory APV-480L
- unifony AP-480AL
- centrale portierskie CDS-480L

System umożliwia tworzenie zaawansowanych struktur łącząc maksymalnie 99 kamer DRC-480L i 480 monitorów

APV-480L. Zamiast monitora (lub równolegle z monitorem) może pracować unifon AP-480AL. Jeśli u jednego lokatora jest zainstalowanych kilka odbiorników (monitorów, unifonów) możliwe jest takie skonfigurowanie systemu aby z kamery wywołać jednocześnie wszystkie odbiorniki lub każdy osobno (kilka kodów użytkowników).

Wywołanie monitorów/unifonów jest możliwe z klawiatury numerycznej na panelu z kamerą. Klawiatura ta umożliwia także otwieranie drzwi wejściowych (system indywidualnych kodów). Opcjonalnie istnieje możliwość otwierania drzwi kartą (czytnik kart zamontowany w kamerze).

Po zainstalowaniu centrali portierskiej mamy możliwość kontroli dostępu osób wchodzących/wychodzących poprzez portiera. Osoba odwiedzająca może nawiązać komunikację bezpośrednio z danym lokatorem wybierając kod abonenta lub (jeśli np. nie znamy kodu abonenta) poprzez portiera, który nawiąże połączenie z danym lokatorem.

W systemie tym jest także możliwość nawiązania rozmowy pomiędzy lokatorami (funkcja interkomu). W tym celu lokator dzwoni do portiera, który nawiązuje połączenie z kolejnym lokatorem.



DRC-480L ▶



◀ Przykładowy schemat podłączenia

Kolorowy system wideodomofonowy COMMAX

Nowoczesne wzornictwo monitorów kolorowych zostało docenione przez niemiecką organizację iF. Rodzina monitorów „Smart View” dostała prestiżową nagrodę „Product design award”. Dzięki temu wiemy, że przełamywanie stereotypów ma sens.

Cechy monitora:

- monitor kolorowy
- wyświetlacz panoramiczny 7" Color TFT-LCD
- obsługa czterech wejść
- możliwość podłączenia dodatkowych monitorów
- funkcja interkomu
- wbudowany moduł pamięci 128 obrazów
- współpraca z kamerami analogowymi czteroprzewodowymi
- zasilanie 230 V



Specyfikacja

Okablowanie	Monitor - kamera: 4 przewody Monitor - unifon: 4 przewody
Zasilanie	AC 100-240 V 50/60 Hz
Pobór mocy	Stan czuwania: 6 W Praca: 19 W
Temperatura pracy	0 - 40 °C
Wymiary (szer. / wys. / gł.):	315 mm x 175 mm x 53 mm
Masa:	1,7 kg

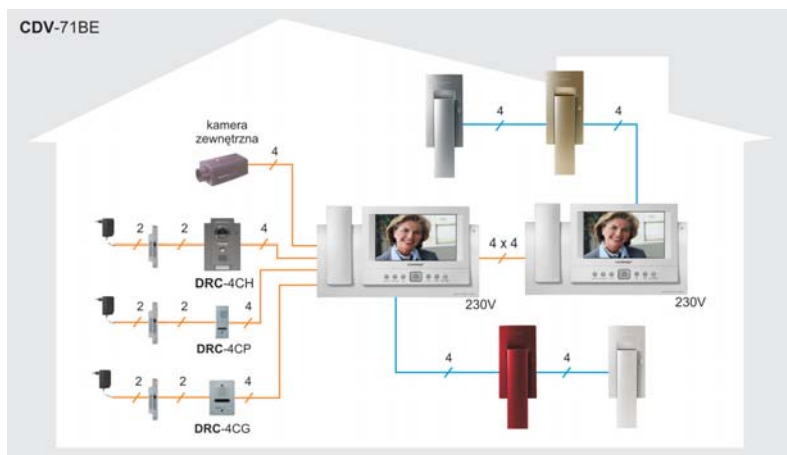
Monitor CDV-71BE



Unifon DP-4VH
– 5 wersji kolorystycznych



Kamera DRC-4CH



ZEWNĘTRZNA CZUJKA PIR MS-12FE firmy TAKEX

MS12FE to zewnętrzna czujka ruchu o jak dotąd niepowtarzalnych parametrach technicznych i użytkowych. Dwa niezależnie regulowane układy optyczne pozwalają na zabezpieczenie powierzchni o długości 24m (2x12m) i kącie detekcji 180° (2 x 90°). Jest to obszar o powierzchni 226m². To dwa razy więcej niż możliwości popularnych czujek oferowanych na naszym rynku. MS12FE to czujka wyposażona w 4 elementy PIR (dwa na każdy układ) oraz System Podwójnej Strefy (ang. *Dual Zone System*). Pole widzenia czujki zostało podzielone na obszar górny i dolny. Dopiero w przypadku wykrycia intruza w obu obszarach czujka wygeneruje alarm. Taki system zapewnia skuteczną eliminację fałszywych alarmów wywołanych przez ptaki lub małe zwierzęta.

Dowolna regulacja pola detekcji w zakresie długości oraz kąta detekcji pozwala na montaż czujki w każdym miejscu oraz w jakiegokolwiek konfiguracji. Dodatkowa możliwość zamaskowania wybranych wiązek pozwala na tworzenie charakterystyki kurtynowej, niezbędnej na niektórych obiektach (rys. 2).

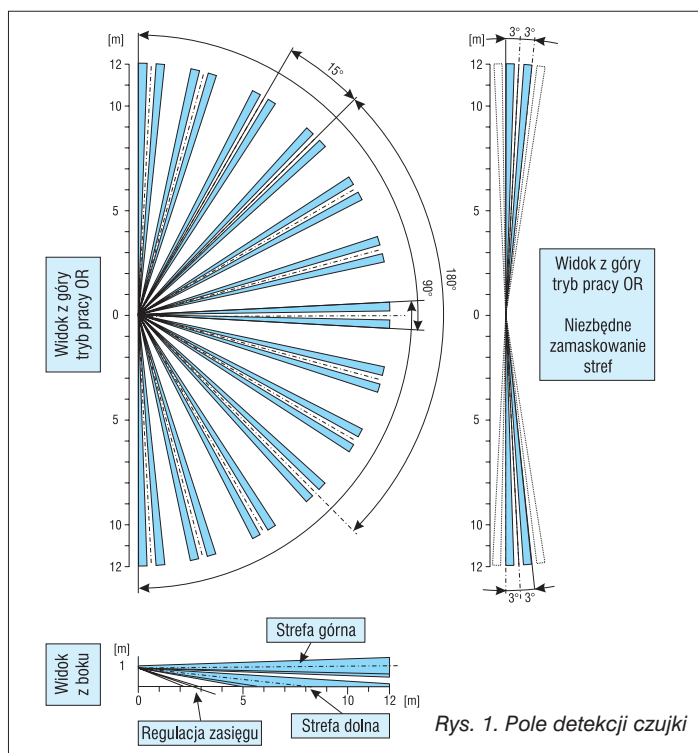
Czujka MS-12FE posiada świadectwo kwalifikacyjne Tecom oraz CE.

Jest to jedyna jak dotąd czujka zewnętrzna o takich parametrach.



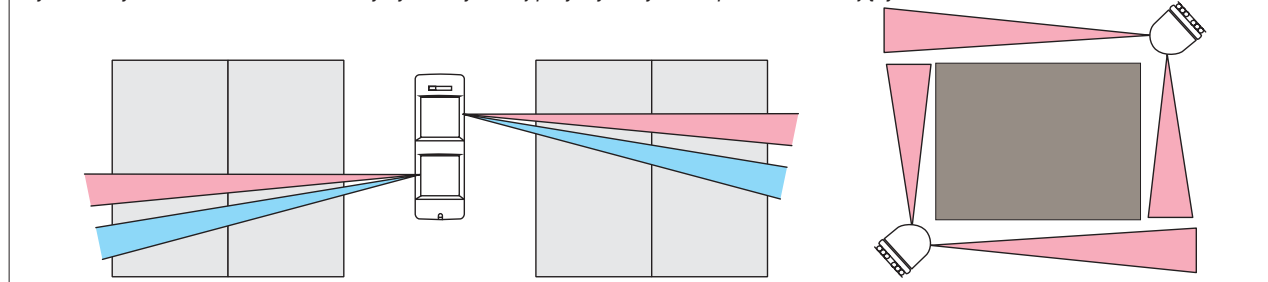
Podstawowe parametry czujki:

- Dwie tradycyjne czujki w jednej obudowie
- Japońska precyzja wykonania
- Brak reakcji na zwierzęta
- Pole detekcji: 2 x 12 m, 2 x 90°
- Cztery elementy PIR
- 2 układy optyczne, regulowane osobno: regulacja pola detekcji: od 3 do 12 m, od 15° do 180°
- System Podwójnej Strefy
- Tryb pracy AND/OR
- Tryb pracy dzień/noc
- Licznik impulsów: 1 lub 3
- Regulacja czasu aktywacji wyjścia alarmowego: od 2 s do 5 min.
- Wodoszczelna obudowa
- Płynna regulacja czułości od 30% do 170%
- Wysokość montażu: od 0,8 m do 1,2 m
- Montaż ścienny lub na słupku (opcjonalnie)
- Paski maskujące w komplecie
- Napięcie zasilania: 12 V_{DC}-30 V_{DC}
- Maksymalny pobór prądu: 40 mA
- Temperatura pracy: od -20°C do +50°C



Rys. 1. Pole detekcji czujki

Rys. 2. Przykład stworzenia charakterystyki kurtynowej przy wykorzystaniu pasków maskujących



CZTEROWIĄZKOWE BARIERY PODCZERWIENI SERII PB-IN-50/100/200HF (KLASA S)

Zasięgi:

PB-IN-50HF na zewnątrz 50 m, wewnątrz 100 m
PB-IN-100HF na zewnątrz 100 m, wewnątrz 200 m
PB-IN-200HF na zewnątrz 200 m, wewnątrz 400 m

TAKEX



WŁAŚCIWOŚCI:

- **Wybór częstotliwości:** cztery częstotliwości pracy, które umożliwiają instalacje większej ilości jednostek bez ryzyka interferencji fal;
- **Zabezpieczenie przed zewnętrznym światłem:** bezawaryjną pracę w warunkach luminacji do wartości 50000 lx zapewnia wbudowany filtr kompensacyjny światła zewnętrznego;
- **Odporność na fałszywe alarmy:** zastosowanie czterech zsynchronizowanych wiązek, ze względu na wymóg przerywania ich jednocześnie w celu inicjacji alarmu, skutecznie eliminuje najczęstsze przyczyny powstawania fałszywych alarmów;
- **Łatwa synchronizacja wiązek:** Specjalny wizjer pozwala na szybką i prawidłową synchronizację nadajnika z odbiornikiem. Dodatkowo bariery zostały wyposażone w wyjście kontrolno pomiarowe ułatwiające kontrole czułości, sygnalizację świetlną za pomocą diody LED wskazującej czy sygnał wiązki spełnia wymogi założonego poziomu (funkcja przydatna w celu weryfikacji zestrojenia po założeniu osłon na bariery). Wbudowano też sygnalizator dźwiękowy, obrazujący za pomocą poziomu sygnału dźwiękowego stopień zestrojenia;
- **Zabezpieczenie przeciwko złodowaceniu/rosie:** specjalna osłona na obudowie bariery zapewnia odpowiednią ochronę wiązek;
- **Dwa poziomy mocy transmisji wiązek:** umożliwiają dostosowanie mocy wiązek do dystansu pomiędzy nadajnikiem i odbiornikiem;
- **Sygnalizacja złych warunków pogodowych:** sygnał informujący o złych warunkach pogodowych zostaje wysłany w momencie, gdy poziom wiązki podczerwieni spadnie poniżej dopuszczalnego progu;
- **Pamięć alarmu:** dioda LED sygnalizuje wystąpienie zdarzenia, dzięki czemu w przypadku, kiedy na jednej linii pracuje kilka barier, łatwo zlokalizować, które urządzenie wygenerowało sygnał alarmowy.

Specyfikacja

Oznaczenie modelu	PB-IN-50HF	PB-IN-100HF	PB-IN-200HF
Sposób detekcji	Cztery zsynchronizowane wiązki (logika AND)		
Źródło podczerwieni	Pulsująca dioda LED, podwójna modulacja		
Zasięg	do 50 m	do 100 m	do 200 m
Maks. zasięg wiązki	do 500 m	do 1000 m	do 2000 m
Czas reakcji wiązki	od 50 ms do 700 ms		
Napięcie zasilania	12 V do 30 V DC (bez polaryzacji)		
Pobór prądu	60 mA	70 mA	85 mA
Wyjście alarmowe	30 V (AC/DC), prąd obciążenia do 1 A		
Wyj. kontrolne otoczenia	30 V (AC/DC), prąd obciążenia do 1 A		
Wyjście tamper	Aktywacja w momencie usunięcia obudowy bariery, 30 V (AC/DC), prąd obciążenia do 0.1 A		
Alarm LED	Czerwona dioda LED na odbiorniku sygnalizująca alarm		
Sygnalizacja poz. mocy wiązki	Czerwona dioda LED na odbiorniku sygnalizująca alarm		
Temperatura pracy	-25°C do 66°C		
Zastosowanie	zewnętrzne		

Moduły GSM/GPRS

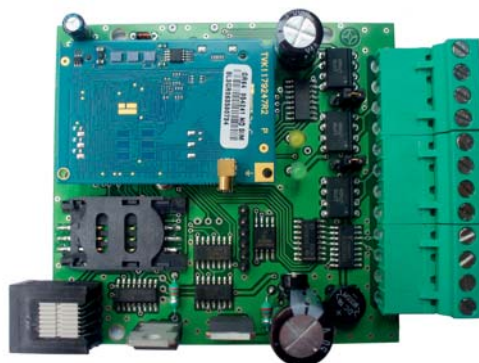
Urządzenia TX404, TX800, TX1000 przeznaczone są do monitoringu, komunikacji i powiadamiania o stanach alarmowych chronionych obiektów wykorzystując sieć telefonii komórkowej dowolnego operatora GSM. Monitoring stanów alarmowych możliwy jest za pomocą zwykłej wiadomości tekstowej SMS lub z wykorzystaniem funkcji Clip do stacji monitoringu.



Urządzenia służą również do zdalnego sterowania innymi urządzeniami wykonawczymi w dowolnych systemach. Każdy z modeli

serii TX jest zintegrowany z modułem komunikacyjnym GSM/GPRS i wymaga tylko włożenia aktywnej karty SIM. Poprzez dołączone w zestawie oprogramowanie konfiguracyjne należy urządzenie odpowiednio zaprogramować.

Urządzenia przeznaczone są do zastosowań profesjonalnych w systemach zabezpieczeń i automatyce przemysłowej.



Model urządzenia	TX406	TX800	TX1000
Wejścia binarne			
Liczba wejść	6	8	8
Optoizolacja wejść	Tak	Tak	Tak
Typ wejść	NO-NC / napięciowe	NO-NC / napięciowe	NO-NC / napięciowe
Możliwość blokowania wejść	Tak	Tak	Tak
Wyjścia			
Liczba wyjść	2	8	8
Czasowe przełączanie wyjść	Tak	Tak	Tak
Wiadomości SMS			
Liczba numerów telefonów	8	8	8
Dynamiczne formatowanie treści SMS	Tak	Tak	Tak
Programator czasowy			
Liczba programowalnych zdarzeń	4	8	8
Rodzaj zdarzeń czasowych	Odstępy czasowe Dokładna godzina	Odstępy czasowe Dokładna godzina	Odstępy czasowe Dokładna godzina
Polecenia SMS			
Polecenia standardowe ¹	Tak	Tak	Tak
Maks. liczba poleceń użytkownika ²	8	8	8
Wyjścia analogowe			
Liczba wejść	0	0	2 lub 4
Rozdzielczość wejść	-	-	10 lub 16 bit
Zakres pomiaru napięcia	-	-	0 do 10 V
Transmisja danych na serwer FTP	-	-	Tak

¹ Polecenia standardowe - wbudowane polecenia do zdalnej zmiany stanu wyjść, zapytania o stan urządzenia

² Polecenia użytkownika - polecenia o dowolnie konfigurowalnej treści i rodzaju czynności do wykonania przez urządzenie



inter-Kompas

inter-Kompas s.c.
33-300 Nowy Sącz
ul. Grottera 3

tel. (18) 547 40 11, fax (18) 547 40 09
www.interkompas.com.pl
interkompas@interkompas.com.pl

ROGER ACCESS CONTROL SYSTEM SERIA RADIUS

Seria Radius to całkowicie nowa linia wzornicza czytników i kontrolerów dostępu zaprojektowana w oparciu o wieloletnie doświadczenie firmy Roger w tej dziedzinie.

W skład rodziny wchodzi czytniki i kontrolery różniące się konstrukcją mechaniczną oraz funkcjonalnością, w zależności od modelu obsługują one karty standardu EM 125 kHz lub 13,56 MHz Mifare. Nową kategorię produktów stanowi wandaloodporny czytnik zbliżeniowy (PRT64VP), w którym zarówno przednia część obudowy jak i klawisze są wykonane w całości z metalu. Na szczególną uwagę zasługuje również kontroler PR602LCD, który został specjalnie zaprojektowany dla systemów rejestracji czasu pracy RCP, co nie wyklucza jednak możliwości stosowania go jako zwykłego kontrolera dostępu. Urządzenia rodziny Radius mogą być instalowane na zewnątrz budynków i są kompatybilne z wcześniej produkowanymi kontrolerami serii PR oraz czytnikami PRT, mogą one być dołączone do istniejących już systemów kontroli dostępu pracujących autonomicznie lub pod kontrolą programu PR Master.

Charakterystyka – kontrolery serii PRxx2

- Kontrola jednostronna lub dwustronna przejścia
- Praca autonomiczna lub w zintegrowanym systemie sieciowym
- Wbudowany czytnik zbliżeniowy kart EM 125 kHz oraz klawiatura

- Cztery programowalne klawisze funkcyjne
- Wyświetlacz LCD 4x20 znaków (PR602LCD)
- Trzy wejścia NO/NC
- Dwa wyjścia tranzystorowe oraz jedno przekaźnikowe
- Współpraca z ekspanderem XM-2
- Kontrola dostępu w windzie (wymaga modułu XM-8)
- Interfejs komunikacyjny RS485 (dowolna topologia magistrali)
- Współpraca z dodatkowym czytnikiem Wiegand, Magstripe lub serii PRT
- 4.000 użytkowników
- 250 grup dostępu
- 99 harmonogramów czasowych
- 128 przedziałów czasowych wewnątrz harmonogramu
- Ustawienia świąteczne
- Pamięć 32.000 zdarzeń
- Lokalny anti-passback (wymaga drugiego czytnika)
- Globalny anti-passback (wymaga centrali CPR32-SE)
- Rejestracja zdarzeń dla celów RCP
- Możliwość definicji własnych typów rejestracji RCP
- Aktualizacja oprogramowania przez port szeregowy
- Praca w warunkach zewnętrznych
- Programowanie wyłącznie z komputera PC*
- Program zarządzający Windows XP/Vista
- Znak CE

* niezbędny interfejs komunikacyjny UT-2, UT2USB lub UT-4



roger

Roger Sp. J.
Gościszewo 59
82-416 Gościszewo

tel. (55) 272 01 32
fax (55) 272 01 33
e-mail: biuro@roger.pl
www.roger.pl



2M ELEKTRONIK

ul. Majora 12a
31-422 Kraków
tel. (12) 412 35 94
faks (12) 411 27 74
e-mail: 2m@2m.pl
www.2m.pl



Producent Bezprzewodowych Systemów Transmisji A/V i Telenet
Pasmo 2.4 i 5.8 GHz

3D Wielobranżowe Przedsiębiorstwo Sp. z o.o.

ul. Kościuszki 27A
85-079 Bydgoszcz
tel. (52) 321 02 77
faks (52) 321 15 12
e-mail: biuro@3d.com.pl
www.3d.com.pl



4 COM Sp. z o.o.

ul. Adama 1
40-467 Katowice
tel. (32) 609 20 30
faks (32) 609 20 30 wew. 103
e-mail: biuro@4.com.pl
www.4.com.pl



AAT Trading Company Sp. z o.o.

ul. Puławska 431
02-801 Warszawa
tel. (22) 546 05 46
faks (22) 546 05 01
e-mail: aat_wawa@aat.pl
www.aat.pl

Oddziały:

ul. Raclawicka 82, 60-302 Poznań
tel. (61) 662 06 60
faks (61) 662 06 61

ul. Mieszczańska 18, 30-313 Kraków
tel. (12) 266 87 95
tel./faks (12) 266 87 97

Al. Niepodległości 659, 81-855 Sopot
tel. (58) 551 22 63
tel./faks (58) 551 67 52

ul. Zielona 42, 71-013 Szczecin
tel. (91) 483 38 59, 489 47 23
faks (91) 489 47 24

ul. Na Niskich Łakach 26, 50-422 Wrocław
tel./faks (71) 348 20 61
tel./faks (71) 348 42 36

ul. Ks. W. Siwka 17, 40-318 Katowice
tel. (32) 351 48 30
tel. (32) 256 69 34
tel./faks (32) 256 60 34

ul. Dowborczyków 25, 90-019 Łódź
tel./faks (42) 674 25 45
tel./faks (42) 674 25 48

ul. Łęczycka 37, 85-737 Bydgoszcz
tel./faks (52) 342 91 24, 342 98 82



ACIE Polska Sp. z o.o.

ul. Poleczki 21
02-822 Warszawa
tel./faks (22) 894 61 63
e-mail: info@acie.pl
www.acie.pl

ACSS ID Systems Sp. z o.o.

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



ADT POLAND Sp. z o.o.

ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 8 414
faks (22) 430 8 302
e-mail: adtpoland@tycoint.com
www.adt.pl



ALARM SYSTEM Marek Juszczyński

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



ALARMNET 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. Kielnińska 115
80-299 Gdańsk
tel. (58) 340 24 40
faks (58) 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl



ALDOM F.U.H.

ul. Łanowa 63
30-725 Kraków
tel. (12) 411 88 88
faks (12) 294 18 88
e-mail: handel@aldom.pl
www.aldom.pl

ALPOL Sp. z o.o.

ul. H. Krahelskiej 7
40-285 Katowice
tel. (32) 790 76 56
faks (32) 790 76 61
e-mail: alpol@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. Portowa 14, 44-100 Gliwice
tel. (32) 790 76 23
faks (32) 790 76 65
e-mail: gliwice@e-alpol.com.pl

ul. Pachonńskiego 2a, 31-223 Kraków
tel. (32) 790 76 51
faks (32) 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Ochotnicza 10, 20-012 Lublin
tel. (32) 790 76 50
faks (32) 790 76 74
e-mail: lublin@e-alpol.com.pl

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

ul. Os. Na Murawie 10/2, 61-655 Poznań
tel. (32) 790 76 37
faks (32) 790 76 70
e-mail: poznan@e-alpol.com.pl

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

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

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

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

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



ALKAM SYSTEM Sp. z o.o.

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



Ambient System Sp. z o.o.

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



ANB Sp. z o.o.

ul. Ostrobramska 91
04-118 Warszawa
tel. (22) 612 16 16
faks (22) 612 29 30
e-mail: anb@anb.com.pl
www.anb.com.pl



Zakład Produkcyjno-Usługowo-Handlowy

ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. (71) 363 38 93
faks (71) 363 17 53
e-mail: anma@anma-pl.eu
www.anma-pl.eu



ATLine Spółka Jawna

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

**AVISmedia**

ul. Żeromskiego 10
64-200 Wolsztyn
tel. (68) 347 09 25
faks (68) 347 09 26
e-mail: office@merlaud.com.pl
www.merlaud.com.pl

**Zakłady Kablowe BITNER**

ul. Friedleina 3/3
30-009 Kraków
tel. (12) 389 40 24
faks (12) 380 17 00
e-mail: bitner@bitner.com.pl
www.bitner.com.pl

**ROBERT BOSCH Sp. z o.o.**

ul. Poleczki 3
02-822 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.com.pl

**P.W.H. BRABORK Laboratorium Sp. z o.o.**

ul. Postępu 2
02-676 Warszawa
tel. (22) 257 68 12
faks (22) 257 68 95
e-mail: brabork@braborklab.pl
www.braborklab.pl

**bt electronics Sp. z o.o.**

ul. Dukatów 10 b
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.**

Al. Wyścigowa 8
02-681 Warszawa
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrand.pl

**C&C PARTNERS TELECOM Sp. z o.o.**

ul. 17 Stycznia 119,121
64-100 Leszno
tel. (65) 525 55 55
faks (65) 525 56 66
e-mail: info@ccpartners.pl
www.ccpartners.pl

**CAMSAT**

ul. Prosta 32
86-050 Solec Kujawski
tel. (52) 387 36 58
faks (52) 387 54 66
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

**CBC (Poland) Sp. z o.o.**

ul. Morcinka 5 paw. 6
01-496 Warszawa
tel. (22) 638 44 40
faks (22) 638 45 41
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

**CCX**

ul. Ligocka 103
Budynek 9.2
40-568 Katowice
tel. (32) 609 90 80
faks (32) 609 90 81
e-mail: biuro@ccx.pl
www.ccx.pl

**CENTRUM MONITOROWANIA****ALARMÓW Sp. z o.o.**

ul. Puławska 359
02-801 Warszawa
tel. (22) 546 08 88
faks (22) 546 06 19
e-mail: mail@cma.com.pl
www.cma.com.pl

Oddział:

ul. Świętochłowska 3, 41-909 Bytom
tel. (32) 388 09 50
faks (32) 388 09 60

**CEZIM Jolanta Podrażka**

ul. Partyzantów 1
96-500 Sochaczew
tel./faks (46) 863 56 50
e-mail: cezim@cezim.pl
sklep@cezim.pl
www.cezim.pl

**COM-LM**

ul. Ściegiennego 90
25-116 Kielce
tel. (41) 368 71 90
faks (41) 368 71 12
e-mail: biuro@com-lm.pl
www.com-lm.pl

**CONTROL SYSTEM FMN Sp. z o.o.**

Al. Komisji Edukacji Narodowej 96 Lok. U15
02-777 Warszawa
tel. (22) 855 00 17÷19
faks (22) 546 19 78
e-mail: cs@cs.pl
www.cs.pl, www.ckp.com.pl

**D+H Polska Sp. z o.o.**

ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
Dział SAP: tel. (71) 323 52 47
e-mail: biuro@dhpolska.pl
www.dhpolska.pl

Oddziały:

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

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

ul. Płochocińska 19 lok. 43
03-191 Warszawa
tel. (22) 614 39 52
faks (22) 614 39 64

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

**DANTOM s.c.**

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

**DAR-ALARM**

ul. Nieszawska 3C
03-382 Warszawa
tel. (22) 498 60 62
tel./faks (22) 814 10 30

ul. Polnej Róży 2/4
02-798 Warszawa
tel./faks (22) 649 27 97
e-mail: handlowy@darsystem.pl
www.darsystem.pl
www.tvtech.com.pl

**DELTA BUSINESS SERVICE**

ul. Ciepla 15/50
50-524 Wrocław
tel. (71) 367 06 16, 364 78 64
faks (71) 367 06 16
e-mail: biuro@delta-dbs.pl
www.delta-dbs.pl

**DG ELPRO Sp. J.**

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

**DOM Polska Sp. z o.o.**

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

**JABLOTRON Ltd.**

Generalny dystrybutor:

DPK System

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



Przedsiębiorstwo Usług Inżynieryjnych DRAVIS Sp. z o.o.
ul. Gliwicka 3
40-079 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
www.dravis.pl

Dyskret Sp. z o.o.
ul. Mazowiecka 131
30-023 Kraków
tel. (12) 423 31 00
tel. kom. (0) 501 510 175
faks (12) 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl



EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 812 05 05
faks (22) 812 62 12
e-mail: office@ebs.pl, j.haschka@ebs.pl
www.ebs.pl



EDP Support Polska Sp. z o.o.
ul. Chłapowskiego 33
02-787 Warszawa
tel. (22) 644 53 90
faks (22) 644 35 66
e-mail: jacek.urbanowicz@edps.com.pl
katarzyna.osiecka@edps.com.pl
www.edps.com.pl



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



EL-MONT A. Piotrowski
ul. Wyzwolenia 15
44-200 Rybnik
tel. (32) 42 23 889, 42 30 728
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
el-mont@internetdsl.pl
www.el-mont.com



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



ELTCRAC Centrum Zabezpieczeń
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60 do 61
faks (12) 292 48 62
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl



Elza Elektrosystemy
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 266 46 10
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl



EMU Sp. z o.o.
ul. Twarda 12
80-871 Gdańsk
tel. (58) 344 04 01 ÷ 03
faks (58) 344 88 77
e-mail: gdansk@emu.com.pl
www.emu.com.pl

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



EUREKA SOFT & HARDWARE
Rynek 13
62-300 Września
tel. (61) 437 90 15
faks (61) 436 27 14
e-mail: biuro@eureka.com.pl
www.eureka.com.pl



FES Sp. z o.o.
ul. Nałkowskiej 3
80-250 Gdańsk
tel. (58) 340 00 41 ÷ 44
faks (58) 340 00 45
e-mail: fes@fes.pl
www.fes.pl



GE Security Polska Sp. z o.o.
ul. Sadowa 8
80-771 Gdańsk
tel. (58) 301 38 31, 760 64 80
faks (58) 301 14 36
www.gesecurity.pl

Oddziały:
Al. Stanów Zjednoczonych 59
04-028 Warszawa
tel. (22) 810 00 03
faks (22) 810 10 55

Os. Na Murawie 11/2, 61-655 Poznań
tel. (61) 821 35 66
faks (61) 821 31 94



GUNNEBO POLSKA Sp. z o.o.
ul. Piwonińska 4
62-800 Kalisz
tel. (62) 768 55 70
faks (62) 768 55 71
e-mail: polska@gunnebo.com
www.rosengrens.pl
www.gunnebo.com



GV Polska Sp. z o.o.
ul. Kuropatwy 26B
02-892 Warszawa
tel. (22) 831 56 81, 636 13 73
faks (22) 831 28 52
tel. kom. 0 693 029 278
e-mail: warszawa@gv.com.pl

ul. Lwowska 74a
33-300 Nowy Sącz
tel. (18) 444 35 38, 444 35 39
faks (18) 444 35 84
tel. kom. 0 695 583 424
e-mail: biuro@gv.com.pl

ul. Racławicka 60a
53-146 Wrocław
tel. (71) 361 66 02
faks (71) 361 66 23
tel. kom. 0 695 583 292
e-mail: wroclaw@gv.com.pl
www.gvpolska.com.pl



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



ICS Polska
ul. Żuławskiego 4/6
02-641 Warszawa
tel. (22) 646 11 38
faks (22) 849 94 83
e-mail: biuro@ics.pl
www.ics.pl



ID ELECTRONICS Sp. z o.o.
ul. Przy Bażantarni 11
02-793 Warszawa
tel. (22) 649 60 95
faks (22) 649 61 00
e-mail: sales@ide.com.pl
www.ide.com.pl



INFO-CAM
Al. Kilińskiego 5
09-402 Płock
tel. (24) 266 97 12
tel./faks (24) 266 97 13
e-mail: handlowy@infocam.com.pl
www.infocam.com.pl

Oddział:
ul. Opolska 29, 61-433 Poznań
tel. (61) 832 48 94
tel./faks (61) 832 48 75
e-mail: biuro@infocam.com.pl



Przedsiębiorstwo Usług Technicznych INTEL Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. (12) 411 49 79
faks (12) 411 94 74
e-mail: intel@intel.net.pl
www.intel.net.pl

P.W. IRED
Kazimierzówka 9
21-040 Świdnik
tel. (81) 751 70 80
tel. kom. 0 605 362 043
faks (81) 751 71 80
e-mail: ired@exe.pl
www.ired.com.pl



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



KABE Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 32 48 900
faks (32) 32 48 901
e-mail: handel@kabe.pl
www.kabe.pl, www.kabe.eu



Systemy Alarmowe
KOLEKTOR Sp. z o.o.
ul. Gen. Hallera 2b/2
80-401 Gdańsk
tel. (58) 341 27 31
faks (58) 341 44 90
e-mail: info@kolektor.com.pl
www.kolektor.com.pl



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



KRAK-POŻ Sp. z o.o.
Centrum Ochrony Przeciwpowarowej
i Antywłamaniowej
ul. Ceglarska 15
30-362 Kraków
tel. (12) 266 99 85, 266 52 84, 266 95 08
faks (12) 269 25 79
e-mail: biuro@krakpoz.pl
www.krakpoz.pl



PPUH Laskomex
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: marketing@laskomex.com.pl
www.laskomex.com.pl



MAXBAT Sp. J.
ul. Nadbrzeźna 34A
58-500 Jelenia Góra
tel. (75) 764 83 53
faks (75) 764 81 53
e-mail: info@maxbat.pl
www.maxbat.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, 642 45 35
faks (75) 642 45 25
e-mail: info@micronix.pl
www.micronix.pl



MIWI-URMET Sp. z o.o.
ul. Pojezierska 90a
91-341 Łódź
tel. (42) 616 21 00
faks (42) 616 21 13
e-mail: miwi@miwiurmet.com.pl
www.miwiurmet.com.pl



NOMA 2
Zakład Projektowania i Montażu
Systemów Elektronicznych
ul. Plebiscytowa 36
40-041 Katowice
tel. (32) 359 01 11
faks (32) 359 01 00
e-mail: systemy@noma2.com.pl
www.systemy.noma2.pl

Oddziały:
ul. Ryżowa 42, 02-495 Warszawa
tel./faks (22) 863 33 40
e-mail: systemy-wa@noma2.com.pl

ul. Brzozowa 71, 61-429 Poznań
tel./faks (61) 830 40 46
e-mail: systemy-pz@noma2.com.pl



NORBAIN POLSKA Sp. z o.o.
ul. Szczecińska 1 FA
72-003 Dobra k. Szczecina
tel. (91) 311 33 49
faks (91) 421 18 05
e-mail: info@norbain.pl
www.norbain.pl

Biuro:
ul. Ostrobramska 101 lok. 202
04-041 Warszawa
tel. (22) 465 65 81
faks (22) 465 65 80
infolinia: 0 801 055 075



OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
fax, (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. Grunwaldzka 119, 60-313 Poznań
tel. (61) 657 93 60
poznan@omc.com.pl



PAG Sp. z o.o.
Bogdanka
21-013 Puchaczów
tel./faks (81) 462 51 36, 462 51 26
e-mail: pag@pag.com.pl
www.pag.com.pl

Oddział:
ul. Zemborzycka 112, 20-445 Lublin
tel. (81) 748 02 00 + 09
faks (81) 744 90 62



PANASONIC POLSKA Sp. z o.o.
Al. Krakowska 4/6
02-284 Warszawa
tel. (22) 338 11 77
faks (22) 338 12 00
e-mail: dariusz.labedzki@panasonic.com.pl
www.panasonic.pl



PETROSIN Sp. z o.o.
Rynek Dębnicki 2
30-319 Kraków
tel. (12) 266 87 92
faks (12) 266 99 26
e-mail: office@petrosin.pl
www.petrosin.pl

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

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



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



POL-ITAL
ul. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35, 831 18 97
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.pl



POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61, 363 92 60
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV
ul. Heleny Szafran 10
60-693 Poznań
tel./faks (61) 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl
www.dmaxcctv.pl
www.samsuncctv.pl





PROXIMA Sp. J.
ul. Filtrowa 23
87-100 Toruń
tel. (56) 660 20 00
faks (56) 660 20 03
e-mail: proxima@proxima.pl
www.proxima.pl

Filia: (alarmy do obiektów)
ul. Olbrachta 4/6
87-100 Toruń
tel. (56) 661 18 96
faks (56) 661 18 97
e-mail: alarmy@proxima.pl



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



P.P.H. PULSON
ul. Czerniakowska 18
00-718 Warszawa
tel. (22) 851 12 20
faks (22) 851 12 30
e-mail: biuro@pulsan.pl
www.pulsan.pl

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



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



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



Sagitta Sp. z o.o.
ul. Piekarnicza 18
80-126 Gdańsk
tel./faks (58) 322 38 45
e-mail: sagitta@sagitta.pl
www.sagitta.pl



SAMAX S.A.
ul. Mińska 25
03-808 Warszawa
tel./faks (22) 813 44 25, 870 43 80, 870 77 36
e-mail: samax@samax.pl
www.samax.pl

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



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



SCHRACK SECONET POLSKA Sp. z o.o.
ul. Wołoska 5
02-675 Warszawa
tel. (22) 60 60 614 + 617
faks (22) 60 60 618
e-mail: office.warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddział:
ul. M. Palacza 13
60-242 Poznań
tel. (61) 66 43 140 - 42
faks (61) 66 43 143
e-mail: office.poznan@schrack-seconet.pl



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



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

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



SOFTEX DATA S.A.
ul. Poleczki 47
02-822 Warszawa
tel. (22) 331 19 90
faks (22) 331 15 11
e-mail: softex@softex.com.pl
www.softex.com.pl

SOLAR ELEKTRO Sp. z o.o.
ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: communication@solar.pl,
security@solar.pl
www.solar.pl



Oddziały:
ul. Łużycka 3B
81-537 Gdynia
tel. (58) 662 00 00/04/05
tel. kom. 0 603 963 695
faks (58) 664 04 00

ul. Radzikowskiego 35
31-315 Kraków
tel. (12) 638 91 16
tel. kom. 0 605 366 396
faks (12) 638 91 22

ul. Witosa 3
20-330 Lublin
tel. (81) 745 59 00
faks (81) 745 59 05

ul. Smoluchowskiego 7
60-179 Poznań
tel. (61) 863 02 04
faks (61) 863 02 70

ul. Heyki 3
70-631 Szczecin
tel. (91) 485 44 00
tel. kom. 0 601 570 247
faks (91) 485 44 01

ul. Krakowska 141-155
50-428 Wrocław
tel. (71) 377 19 12
tel. kom. 0 607 038 023
faks (71) 377 19 19



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

Oddziały:
ul. Budowlanych 64E
80-298 Gdańsk
tel. (58) 340 77 00
faks (58) 340 77 01
e-mail: gdansk@sprint.pl

ul. Przemysłowa 15
85-758 Bydgoszcz
tel. (52) 365 01 01
faks (52) 365 01 11
e-mail: bydgoszcz@sprint.pl

ul. Heyki 27c
70-631 Szczecin
tel. (91) 431 00 04
faks (91) 462 48 95
e-mail: szczecin@sprint.pl

ul. Canaletta 4
00-099 Warszawa
tel. (22) 826 62 77
faks (22) 827 61 21
e-mail: warszawa@sprint.pl



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

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

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

ul. Inflancka 6, 91-857 Łódź
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.com.pl

ul. 1 Maja 11/2, 10-117 Olsztyn
tel. (89) 527 92 72
faks (89) 527 92 30
e-mail: olsztyn@spstrading.com.pl

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



SYSTEM 7 SECURITY
ul. Krakowska 33
43-300 Bielsko-Biala
tel. (33) 821 87 77
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.s7.pl, www.sevenguard.com,
www.system7.biz

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



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



TAC Sp. z o.o.

Oddziały:
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail: tac_pol@tac.com
www.tac.com.pl

ul. Stefana Batorego 28-32
81-366 Gdynia
tel. (58) 782 00 00
faks (58) 782 00 22

ul. Walońska 3-5
50-413 Wrocław
tel. (71) 340 58 00
faks (71) 340 58 02

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

TALCOMP



TALCOMP SYSTEMY BEZPIECZEŃSTWA
Konrad Talar
ul. Fałęcka 48
30-441 Kraków
tel. (12) 655 85 85, 425 63 67
faks (12) 425 63 68
e-mail: talcomp@talcomp.pl
www.talcomp.pl



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



**Zakład Rozwoju Technicznej Ochrony
Mienia TECHOM Sp. z o.o.**

– Centrum Kształcenia Zawodowego
Instalatorów i Projektantów
Systemów Alarmowych, Monitoringu
oraz Rzeczoznawstwa

– Laboratorium Badawcze Elektronicznych
Urządzeń Alarmowych

ul. Marszałkowska 60
00-545 Warszawa
tel. (22) 625 34 00
faks (22) 625 26 75
e-mail: techom@techom.com
www.techom.com



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



TELCOMP-SERVICE Sp. z o.o.
ul. Annopol 4
03-236 Warszawa
tel. (22) 811 02 59
tel. kom. (0) 662 008 600
e-mail: biuro@telcomp-service.pl
www.centrum-ts.pl

TP TELTECH

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60, 639 88 72
faks (42) 639 89 85
e-mail: teltechinfo@tpeltech.pl
www.tpeltech.pl

Oddziały:
ul. Długa 22/27
80-801 Gdańsk
tel. (58) 302 52 12
faks (58) 346 25 09
e-mail: michal.mikolajski@telekomunikacja.pl

ul. Nasypowa 12
40-551 Katowice
tel. (32) 202 30 50
faks (32) 201 13 17
e-mail: dariusz.gawor@telekomunikacja.pl

ul. Rakowiecka 51
31-510 Kraków
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Rzeczypospolitej 5
59-220 Legnica
tel./faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl

ul. Kosmonautów 82
20-358 Lublin
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbiegniew.chodkiewicz@telekomunikacja.pl



TRIKON
32-447 Siepraw 1123
tel. (12) 274 61 27
faks (12) 274 51 51
e-mail: biuro@trikon.com.pl
www.trikon.com.pl

**TYCO FIRE AND INTEGRATED
SOLUTIONS Sp. z o.o.**
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 8 301
faks (22) 430 8 302
e-mail: tycofis-pl@tycoint.com
www.tycofis.pl



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

Oddziały:
ul. Ratuszowa 11, 03-450 Warszawa
tel. (22) 619 22 04
faks (22) 818 64 67

Os. Polan 33, 61-249 Poznań
tel. (61) 872 92 08 ÷ 10
faks (61) 872 96 30



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



WIZJA Sp. z o.o.
ul. Zakładowa 6
62-052 Komorniki k. Poznania
tel. (61) 810 08 00
faks (61) 810 08 10
www.wizja.com.pl



Vision Polska

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



VISONIC Sp. z o.o.
ul. Smoleńskiego 2
01-698 Warszawa
tel. (22) 639 34 36, 37
faks (22) 833 48 60
e-mail: visonic@visonic.com.pl
www.visonic.com.pl

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	-	TAK	TAK	TAK	-
3D	TAK	TAK	-	-	TAK
4 COM	-	TAK	TAK	TAK	TAK
AAT Trading Company	-	TAK	TAK	-	TAK
ACIE	TAK	-	TAK	TAK	TAK
ACSS ID Systems	-	-	TAK	-	TAK
ADT Poland	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	-
Alarmnet Sp. J.	-	-	TAK	-	TAK
Alarmtech Polska	TAK	TAK	-	-	TAK
Aldom	-	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	-
Alpol Sp. z o.o.	-	-	TAK	-	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	-	TAK	TAK	TAK	TAK
Anma	-	TAK	-	TAK	TAK
Atline Sp. J.	-	TAK	TAK	-	TAK
AVISmedia	-	TAK	TAK	-	TAK
Bitner Zakłady Kablowe	TAK	-	-	-	-
BOSCH	TAK	-	TAK	-	-
P.W.H. Brabork - Laboratorium	-	TAK	TAK	TAK	-
bt electronics	TAK	-	TAK	TAK	-
C&C Partners	-	TAK	TAK	-	TAK
CAMSAT	TAK	TAK	TAK	-	-
CBC Poland	-	-	TAK	-	-
CCX	TAK	-	TAK	TAK	-
Cezim	TAK	TAK	TAK	-	TAK
CMA Sp. z o.o.	TAK	-	-	TAK	-
COM-LM	TAK	TAK	TAK	TAK	-
CONTROL SYSTEM FMN	-	TAK	TAK	TAK	TAK
D + H Polska	TAK	TAK	TAK	TAK	-
DANTOM	TAK	-	TAK	-	-
DAR-ALARM	-	TAK	TAK	TAK	TAK
Delta Business Service	-	TAK	-	TAK	TAK
DG Elpro	-	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	-	-
DPK System	-	-	TAK	-	TAK
Dravis	-	TAK	-	TAK	-
Dyskret	-	TAK	TAK	TAK	TAK
EBS	TAK	-	TAK	-	-
EDP Support Polska	TAK	TAK	TAK	TAK	TAK
ela-compile	TAK	TAK	TAK	-	TAK
EI-Mont	TAK	TAK	-	TAK	-
Elproma	-	TAK	-	TAK	-
Eltrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy-Instalacje	-	TAK	-	TAK	TAK
Emu	-	-	TAK	-	-
Eureka	-	TAK	-	TAK	-
FES	-	TAK	TAK	TAK	-
GE Security Polska	-	-	TAK	-	TAK
Gunnebo	TAK	TAK	TAK	TAK	TAK
GV Polska	-	-	TAK	-	TAK
HSA	-	-	TAK	-	-
ICS Polska	-	-	TAK	-	TAK
ID Electronics	-	TAK	TAK	TAK	-
Info-Cam	TAK	TAK	TAK	TAK	TAK
Intel	-	TAK	TAK	TAK	TAK

DZIAŁALNOŚĆ

firma	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Ired	TAK	TAK	TAK	TAK	-
Janex International	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	-	TAK	-	TAK	-
Kolektor MR	-	TAK	TAK	TAK	-
Krak-Poż	-	TAK	-	TAK	-
Laskomex	TAK	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	-	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	-	-	-	-
Micronix	-	TAK	TAK	-	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK
Noma 2	TAK	TAK	TAK	TAK	-
NORBAIN Polska	TAK	-	TAK	-	TAK
OBIS Sp. J.	-	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	-	-	TAK	-	-
PAG	TAK	TAK	TAK	TAK	-
Panasonic	-	-	TAK	-	TAK
Petrosin	-	TAK	-	TAK	-
Pointel	-	TAK	-	TAK	-
POL-ITAL	-	-	TAK	-	-
Polon-Alfa	TAK	-	-	-	-
ProfiCCTV	-	TAK	TAK	-	TAK
PROXIMA Sp. J.	TAK	-	TAK	-	-
Pulsar	TAK	-	TAK	-	-
PPH Pulson	TAK	TAK	TAK	-	-
Radioton	-	-	TAK	-	-
Ramar	TAK	-	TAK	TAK	TAK
ROPAM Elektronik	TAK	-	TAK	-	-
Sagitta Sp. z o.o.	TAK	-	-	-	-
Samax	TAK	TAK	-	TAK	TAK
Satel	TAK	TAK	-	-	TAK
Sawel	-	TAK	TAK	TAK	-
Schrack Seconet Polska	TAK	-	-	-	TAK
Secural	TAK	TAK	TAK	-	TAK
S.M.A.	-	TAK	-	TAK	-
SOFTEX Data	-	-	TAK	-	TAK
Solar	-	-	TAK	-	-
Sprint Sp. z o.o.	-	TAK	-	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK
STRATUS	-	TAK	TAK	-	TAK
SYSTEM 7 SECURITY	TAK	TAK	TAK	-	TAK
TAC	-	TAK	TAK	TAK	-
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	-	-	TAK	-	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	-	-	-	-	TAK
Technokabel	TAK	-	-	-	-
Telcomp-Service	-	-	-	-	TAK
TP TELTECH	-	TAK	TAK	TAK	-
Trikon	TAK	TAK	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	TAK
UNICARD S.A.	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	-	-
Wizja	-	-	TAK	TAK	-
Vision Polska	-	TAK	TAK	-	TAK
Visonic	-	-	TAK	-	-

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
2M Elektronik	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
3D	-	TAK	-	-	-	-	-	-	-
4 COM	TAK	TAK	TAK	TAK	-	TAK	TAK	TAK	-
AAT Trading Company	TAK	TAK	TAK	TAK	-	TAK	TAK	-	-
ACIE	-	-	TAK	-	-	-	-	-	-
ACSS ID Systems	systemy identyfikacji								
ADT Poland	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
Alarm System	TAK	TAK	TAK	-	-	-	-	-	-
Alarmnet Sp. J.	-	TAK	TAK	-	-	TAK	-	-	-
Alarmtech Polska	TAK	-	-	-	-	-	-	-	-
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Alkam System	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
Alpol Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Ambient System	TAK	TAK	TAK	TAK	-	-	-	-	TAK
ANB	TAK	TAK	-	TAK	-	TAK	TAK	-	TAK
Anma	TAK	TAK	TAK	TAK	-	TAK	-	-	-
ATLine Sp. j.	TAK	TAK	TAK	-	TAK	TAK	-	-	-
AVISmedia	-	-	-	TAK	-	-	-	-	TAK
Bitner Zakłady Kablowe	-	TAK	-	TAK	-	-	TAK	-	TAK
BOSCH	TAK	TAK	-	TAK	-	-	TAK	-	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
bt electronics	-	-	TAK	-	-	TAK	-	TAK	-
C&C Partners	-	TAK	-	-	-	-	TAK	-	-
CAMSAT	-	TAK	-	-	-	-	-	-	-
CBC Poland	-	TAK	-	-	-	-	-	-	-
CCX	-	-	TAK	-	-	-	-	TAK	-
Cezim	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
CMA Sp. z o.o.	-	-	-	-	-	-	TAK	-	-
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Control System FMN	TAK	TAK	TAK	-	-	TAK	-	TAK	-
D + H	-	-	-	TAK	-	TAK	-	-	TAK
DANTOM	TAK	TAK	TAK	TAK	-	-	-	TAK	-
DAR-ALARM	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Delta Business Service	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	-	-	TAK	-	-	-	-	TAK	-
DPK System	TAK	TAK	-	-	-	-	TAK	-	-
Dravis	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Dyskret	TAK	TAK	TAK	TAK	-	TAK	-	TAK	TAK
EBS	TAK	-	TAK	TAK	-	TAK	TAK	-	-
EDP Support Polska	-	TAK	TAK	-	TAK	TAK	-	TAK	-
ela-compil	-	-	-	-	-	TAK	-	-	-
EI-Mont	TAK	TAK	TAK	-	TAK	-	-	-	-
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Eltrac	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Elza Elektrosystemy-Instalacje	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	-	TAK	TAK	TAK	-	-
FES	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
GE Security Polska	TAK	TAK	TAK	TAK	TAK	TAK	-	-	-
Gunnebo	-	-	TAK	-	-	-	-	TAK	-
GV Polska	-	TAK	-	-	-	-	TAK	-	-
HSA	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
ICS Polska	TAK	TAK	TAK	-	-	-	-	-	-
ID Electronics	TAK	TAK	TAK	-	TAK	-	-	TAK	-
Info-Cam	TAK	TAK	TAK	-	-	TAK	TAK	-	TAK
Intel	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK

KATEGORIE

firma	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Ired	TAK	TAK	TAK	-	-	TAK	TAK	-	-
Janex International	TAK	TAK	TAK	TAK	-	-	TAK	-	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
Krak-Poż	-	-	-	TAK	-	-	TAK	-	TAK
Laskomex	-	TAK	TAK	-	-	-	TAK	TAK	-
Legrand Polska	-	-	TAK	-	-	-	-	-	-
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
MicroMade	-	-	TAK	-	Rejestracja czasu pracy			-	-
Micronix	TAK	TAK	TAK	TAK	-	-	-	TAK	-
Miwi-Urmet	TAK	TAK	TAK	-	TAK	TAK	-	-	-
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
NORBAIN Polska	-	TAK	-	-	-	TAK	-	-	-
OBIS Sp. J.	TAK	TAK	TAK	TAK	-	TAK	TAK	-	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	-	-	-	-	TAK	-
PAG	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Panasonic	-	TAK	TAK	-	-	-	-	-	-
Petrosin	TAK	TAK	TAK	-	-	-	-	-	-
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
POL-ITAL	-	-	TAK	-	-	-	-	TAK	-
Polon-Alfa	-	-	-	TAK	-	-	-	-	-
ProfiCCTV	TAK	TAK	TAK	TAK	-	-	-	-	-
Proxima Sp. J.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Pulsar	TAK	TAK	TAK	-	-	-	-	TAK	-
PPH Pulson	-	-	-	-	-	TAK	TAK	-	-
Radioton	-	TAK	-	-	-	-	-	-	-
Ramar	TAK	TAK	TAK	-	TAK	-	TAK	-	-
ROPAM Elektronik	TAK	-	TAK	TAK	-	-	TAK	-	-
Sagitta Sp. z o.o.	-	-	-	TAK	-	-	-	-	-
Samax	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	TAK
Satel	TAK	TAK	TAK	-	-	-	TAK	-	-
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	-
Schrack Seconet Polska	-	-	-	TAK	-	-	-	-	-
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Softex Data	-	TAK	-	-	-	TAK	TAK	-	-
Solar	TAK	TAK	TAK	TAK	-	-	-	-	TAK
Sprint Sp. z o.o.	TAK	TAK	TAK	TAK	TAK	TAK	-	-	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK	-
STRATUS	TAK	TAK	TAK	TAK	TAK	-	-	-	TAK
SYSTEM 7 SECURITY	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
TAC	TAK	TAK	TAK	-	TAK	TAK	TAK	-	-
Talcomp	TAK	TAK	TAK	-	TAK	-	-	-	-
Tap – Systemy Alarmowe	TAK	-	TAK	-	TAK	-	-	-	-
Tayama	TAK	TAK	TAK	-	-	TAK	-	-	TAK
Techom	TAK	-	-	-	-	-	-	-	-
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	-	TAK
Telcomp-Service	szkolenia								
TP TELTECH	TAK	TAK	TAK	TAK	-	-	TAK	-	-
Trikon	-	-	TAK	-	-	-	-	TAK	-
TYCO	TAK	TAK	TAK	TAK	-	TAK	-	-	TAK
UNICARD S.A.	-	-	TAK	-	-	TAK	-	TAK	-
W2	TAK	-	-	TAK	-	-	-	-	-
Wizja	-	-	-	-	-	-	-	-	TAK
Vision Polska	-	-	-	TAK	-	-	-	-	-
Visonic	TAK	-	TAK	-	-	-	TAK	-	-

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny

Teresa Karczmarzyk

teresa@zabezpieczenia.com.pl

Redaktor merytoryczny

Adam Bułaciński

adam@zabezpieczenia.com.pl

Dział marketingu i reklamy

Ela Końska

ela@zabezpieczenia.com.pl

Redaguje zespół:

Marek Blim

Patryk Gańko

Norbert Góra

Ireneusz Kryśowyty

Paweł Niedziejko

Edward Skiepmo

Ryszard Sobierski

Waldemar Szulc

Adam Wojcinowicz

Współpraca zagraniczna

Rafał Niedzielski

rafal@zabezpieczenia.com.pl

Współpraca

Jarosław Barszcz

Krzysztof Białek

Sławomir Wagner

Marcin Pyclik

Skład i łamanie

Robert Zadrożny

Korekta

Paweł Karczmarzyk

Adres redakcji

ul. Puławska 359, 02-801 Warszawa

tel. (22) 546 09 51, 53

faks (22) 546 09 59

www.zabezpieczenia.com.pl

Wydawca

AAT Trading Company Sp. z o.o.

ul. Puławska 431, 02-801 Warszawa

tel. (22) 546 05 97

faks (22) 546 05 29

Druk

Regis Sp. z o.o.

ul. Napoleona 4, 05-230 Kobyłka

Cennik reklam

cała strona, pełny kolor	– 3600 zł
cała strona, czarno-biała	– 2100 zł
1/2 strony, pełny kolor	– 2200 zł
1/2 strony, czarno-biała	– 1300 zł
1/3 strony, pełny kolor	– 1700 zł
1/3 strony, czarno-biała	– 1000 zł
1/4 strony, pełny kolor	– 1300 zł
1/4 strony, czarno-biała	– 800 zł
karta katalogowa, 1 strona	– 800 zł
artykuł sponsorowany – indywidualne negocjacje	

Reklama na okładkach

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

Spis teleadresowy

jednorazowy wpis	– 60 zł
------------------	---------

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji.

W przypadku zamówienia na 12 emisji – 10% rabat.

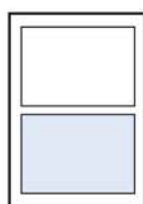
Podane ceny nie uwzględniają podatku VAT (22%).

Nr konta: AAT Trading Company Sp. z o.o.

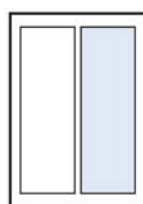
PKO SA VIII Oddział/Warszawa 3412401112111000001649659



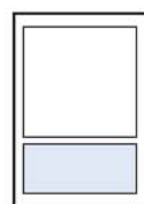
cała strona
200 x 282 mm
+ 3 mm spad



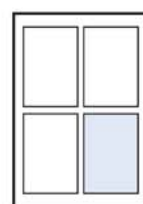
1/2 strony
170 x 125 mm



1/2 strony
81,5 x 257 mm



1/3 strony
170 x 80,5 mm



1/4 strony
81,5 x 125 mm

Materiały reklamowe przyjmowane są tylko w formie elektronicznej.

Redakcja przyjmuje pliki w CMYK-u w plikach:

- **tiff** – 1 warstwa, rozdzielczość 300 dpi,
- **eps, ai, pdf** – teksty zamienione na krzywe, rozdzielczość bitmap 300 dpi, PDF 1.3,
- **cdr** – do wersji 11, teksty zamienione na krzywe, rozdzielczość bitmap 300 dpi,
- **jpg** – możliwie najwyższa jakość (*maximum quality*), rozdzielczość 300 dpi.

Uwaga!

Reklamy całostronicowe muszą zawierać min. 3 mm spady z każdej strony.

Redakcja nie ponosi odpowiedzialności za zgodność kolorów w innej niż CMYK przestrzeni kolorystycznej.

Redakcja przyjmuje materiały reklamowe na płytach CD lub e-mailem (do 5 MB).

Materiały należy dostarczyć na 3 tygodnie przed planowanym zamknięciem numeru.

SPIS REKLAM

24M.pl	14, 47	Gunnebo	46
AAT-T	34, 38, 64, 81	HID	112
ACIE	86	Info-Cam	59
ACSS	63	Kabe	54
ADD	86	Messer	28
ADT	55	Miwi-Urmet	27, 45, 111
Alarmnet	48, 76	MTP	50
Alarmtech	22	PAG	48
Ambient System	2	Panasonic	13
ASD	76	Polon-Alfa	18
ATIline	23	ProfiCCTV	58
Bosch	1	Protector Polska	49
bt electronics	62	RAJ International	26
C&C Partners	29	RISCO Group	19
Camsat	53	Roger	67
CBC Poland	40	Satel	15
CCX	18	Softex	63
Control System	66	Suma	75
Corral	33	Techom	75
ES Instal	26	Telcomp-Service	74
Faxon Professional	44	Unicard	46

Redakcja nie zwraca materiałów nie zamówionych oraz zastrzega sobie prawo do skrótu i redakcyjnego opracowania tekstów przyjętych do druku. Za treść reklam, ogłoszeń i tekstów sponsorowanych redakcja nie odpowiada. Wszelkie prawa zastrzeżone. Przedruk tekstów, zdjęć i grafiki bez zgody redakcji zabroniony.

ZABEZPIECZENIA

CZASOPISMO BEZPŁATNE ISSN 1505-9415 DWUMIESIĘCZNIK NR 2(80)/2008

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

Czujka zewnętrzna OD850 technologia TriTech
Niezawodna ochrona obwodowa



W NUMERZE:

- Monitorowanie oprogramowania
- Matryce w kamerach telewizji dozorowej
- Obiektywy w systemach telewizji dozorowej. Dobór obiektywu – podstawowe pojęcia
- System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Cz. 1. Wprowadzenie

iProtect™

ZINTEGROWANY SYSTEM
ZARZĄDZANIA BEZPIECZEŃSTWEM
oparty na sieci TCP/IP



Myślisz, że nie możesz uzyskać wysokiej jakości wydruku?

Wzrost
szczęśliwej

hidglobal.com



FARGO®

**Niezawodna drukarka Fargo HDP5000
gwarantuje wysoką jakość wydruku
kosztowo porównywalnego do jakości
wydruku ze standardowych drukarek.**

Firma HID Global, światowy lider w dziedzinie zbliżeniowych systemów identyfikacji, przedstawia nowość pośród drukarek wysokiej wydajności - Fargo HDP5000. Wykorzystanie technologii retransferowej pozwala uzyskać niezwykłą ostrość obrazu i zabezpiecza przed uszkodzeniem przy przenoszeniu go na kartę. HDP5000 idealnie radzi sobie z kartami wyposażonymi w moduł chipowy, ponieważ drukarka nie ma bezpośredniego kontaktu z kartą. To chroni zarówno drukarkę jak i kartę przed ewentualnym uszkodzeniem i eliminuje ewentualne koszty wymiany.

Pomyśl o drukarce HDP5000, jeżeli chcesz uzyskać wysoką i trwałą jakość wydruku za bezprecedensową cenę.



ACCESS quality.

www.hidglobal.com/hdp

Więcej informacji uzyskasz pod numerem 1-800-459-5636 lub pisząc na adres sales@fargo.com