CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3(67)/2009

ZABEZPIECZENIA

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

W NUMERZE:

Przekaż swoją wiadomość dalej bez względu na miejsce, czas i treść

Praesideo - idealne połączenie dźwiękowego systemu ostrzegawczego i nagłośnieniowego. Praesideo jest czymś o wiele więcej niż prostym połączeniem dwóch systemów: ostrzegawczego i nagłośnieniowego. Jest mistrzem samym w sobie. Do niektórych z jego ponadprzeciętnych cech należą:

- Zgodność z najważniejszymi światowymi normami i wymaganiami CNBOP
- Pierwszy na skalę światową całkowicie cyfrowy dźwiękowy system ostrzegawczy
- Maksymalna wygoda instalacji dzięki zastosowaniu technologii sieciowej
- Nieograniczone możliwości konfiguracyjne oraz doskonała jakość dźwięku
- Możliwość rozproszenia wzmacniaczy, stacji mikrofonowych oraz mikrofonów strażaka
- Wysoka niezawodność i szybka diagnostyka błędów z dowolnego miejsca na świecie
- Nowe wersje wzmacniaczy znacząco obniżające koszty instalacji
- Automatyczna regulacja głośności muzyki uzależniona od hałasu otoczenia

BOSCH

Technologia bliżej nas

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

Spis treści

Wysoka ocena elektronicznych legitymacji studenckich firmy Gemalto

– wyniki badań

Szesnastego kwietnia 2009 roku znajdująca się w światowej czołówce w dziedzinie cyfrowych systemów bezpieczeństwa firma **Gemalto** przedstawiła wyniki ogólnopolskiego badania na temat funkcjonowania elektronicznych legitymacji studenckich na polskich uczelniach. Studenci z pięciu największych ośrodków akademickich w Polsce (Gdańska, Krakowa, Poznania, Warszawy i Wrocławia) pozytywnie ocenili dotychczas wdrożony nowy system identyfikacji tożsamości studenckiej oraz wskazali inne funkcje i obszary, w jakich chcieliby wykorzystywać w przyszłości elektroniczną kartę studencką.

Elektroniczne karty studenckie zaczęto wprowadzać w Polsce na szeroką skalę pod koniec 2007 r. W chwili obecnej korzysta z nich ponad 115 wyższych uczelni, a kolejne 300 przygotowuje się do ich wprowadzenia w najbliższym czasie. Z kart elektronicznych produkcji Gemalto korzysta na co dzień 1,1 miliona polskich studentów. Elektroniczna legitymacja to nie tylko dokument potwierdzający studencką tożsamość, ale również wielofunkcyjna karta otwierająca drzwi uczelnianych stołówek, akademików, pracowni i laboratoriów, a także bilet komunikacji miejskiej czy elektroniczna portmonetka. Studenckie karty elektroniczne o wiele trudniej jest podrobić niż ich papierowe odpowiedniki. Blankiet legitymacji wyposażony jest w szereg zaawansowanych i skutecznych rozwiązań ochronnych. Są to zabezpieczenia zarówno elektroniczne (dwa mikroprocesory: procesor stykowy oraz bezstykowy), jak i wizualne (mikrodruki), które są nanoszone na etapie produkcji.

Elektroniczna Legitymacja Studencka – wygoda i funkcjonalność

Wyniki badania pokazują, że studenci polubili elektroniczne legitymacje studenckie – 80% osób jest zadowolonych z ich użytkowania. W opinii studentów jest to wygodna, funkcjonalna i przy okazji wizualnie atrakcyjna forma identyfikacji tożsamości studenckiej. Największą zaletą elektronicznej legitymacji studenckiej jest wygoda jej użytkowania oraz małe rozmiary (50% spontanicznych odpowiedzi).

Karta elektroniczna doskonale wpisuje się w styl życia młodych ludzi, którzy są niezwykle mobilni oraz sprawnie poruszają się w świecie nowych technologii oraz w internecie. Studenci oczekują funkcjonalnych i bezpiecznych rozwiązań, które ułatwią im funkcjonowanie w środowisku akademickim. Gdyby studenci mieli możliwość samodzielnego wyboru rodzaju legitymacji studenckiej, wówczas aż 86% zdecydowałoby się na kartę elektroniczną.

– Wdrożenie nowego systemu elektronicznej karty studenckiej na polskich uczelniach jest największym tego typu projektem w Europie. Pozytywna reakcja studentów na elektroniczną legitymację studencką bardzo cieszy i jednoznacznie pokazuje kierunek rozwoju w zakresie systemów identyfikacji w najbliższej przyszłości. Dodatkowo w przyszłości karta może służyć do wymiany danych pomiędzy studentami uczelni zagranicznych – komentuje Marek Strzelecki, przedstawiciel ECCA (European Campus Card Association).

Elektroniczna Legitymacja Studencka – wiele możliwości

Legitymacja w formie karty elektronicznej umożliwia dodawanie kolejnych przydatnych aplikacji. Obecnie spośród dodatkowych dostępnych na karcie funkcji studenci korzystają głównie z karty wstępu do obiektów studenckich, takich jak akademiki, biblioteki, baseny (70%), oraz z biletu komunikacji miejskiej (43%).

Zwiększeniem zakresu funkcji dostępnych obecnie na karcie byłby zainteresowany co trzeci student. Spośród spontanicznie wymienianych funkcji studenci najbardziej są zainteresowani elektronicznym indeksem, kartą płatniczą, kartą kredytową oraz kartą rabatową do sklepów i kawiarni. Z listy wspomaganej najbardziej pożądane przez studentów aplikacje to: zdalny dostęp do wyników egzaminów i planów zajęć, bilet do kina/teatru i na imprezy masowe oraz bilet na samolot.

Studenci z entuzjazmem przyjęliby informatyczne usprawnienia w komunikacji nie tylko z podmiotami akademickimi, ale również z urzędami państwowymi. Bezpieczną wymianą danych z instytucjami państwowymi przy pomocy elektronicznej legitymacji studenckiej byłoby zainteresowanych 77% studentów. Biorąc pod uwagę rodzaj uczelni, najbardziej zainteresowani tą funkcją byłyby osoby studiujące na uczelniach ekonomicznych (96% ankietowanych).

Karty elektroniczne to naturalny kierunek, w jakim będą się rozwijały systemy identyfikacji tożsamości. Elektroniczna legitymacja studencka to proste, funkcjonalne i korzystne rozwiązanie zarówno dla studentów, jak i dla władz uczelni. Potwierdzeniem tej opinii są wyniki przedstawionego badania oraz liczba 6 milionów kart dostarczonych przez firmę Gemalto dla wyższych uczelni w Ameryce Łacińskiej, Maroku, Portugalii, Serbii, Hiszpanii, Wielkiej Brytanii, Stanach Zjednoczonych i na Węgrzech.

Bezpośr. inf. Monika Kaźmierczak
TBWA\PR

„Raport Gemalto: Elektroniczna legitymacja studencka na polskich uczelniach – jedna karta wiele możliwości z dnia 16.04.2009"

Szybka konfiguracja DSO

Program do projektowania dźwiękowego systemu ostrzegawczego Plena firmy Bosch

Obecnie konfiguracja dźwiękowego systemu ostrzegawczego **Plena** jest jeszcze łatwiejsza. **Bosch Security Systems** zachęca do korzystania z nowego narzędzia Plena dla projektantów. Aplikacja prezentuje możliwości dźwiękowego systemu ostrzegawczego bazującego na systemie Plena i głośnikach firmy Bosch. Program jest dostępny nieodpłatnie na stronie internetowej http://programplena.boschsecurity.pl/.

Program Plena umożliwia dobór i konfigurację sprzętu potrzebnego do wykonania systemu o zadanych parametrach. Oprócz listy urządzeń generuje on schemat blokowy danego systemu. Znacząco ułatwia to pracę projektantom dźwiękowych systemów ostrzegawczych (DSO).

Certyfikowany system nagłośnieniowo-ostrzegawczy Plena jest dedykowany dla małych i średnich obiektów, które wymagają stosowania instalacji DSO. Wszystkie podstawowe funkcje ewakuacyjne, w tym nadzorowanie poprawności działania systemu, przełączanie wzmacniaczy rezerwowych, nadzorowanie linii głośnikowych, zarządzanie komunikatami cyfrowymi, a także interfejs panelu strażaka, są połączone ze sprawdzoną technologią audio, która gwarantuje doskonałą zrozumiałość mowy i niezawodną dystrybucję informacji.

System Plena bazuje na kontrolerze systemu nagłośnieniowo-ostrzegawczego Plena, który obsługuje maksymalnie sześć stref. Zawiera wbudowany manager komunikatów cyfrowych, mikrofon do nadawania ostrzeżeń oraz 240-watowy wzmacniacz mocy. Kontroler Plena można rozbudować do obsługi aż 60 stref dzięki zastosowaniu 6-strefowych ruterów. Ponadto na potrzeby rutingu komunikatów istnieje możliwość podłączenia ośmiu stacji wywoławczych z 32 klawiaturami zawierającymi programowalne klawisze. Całość można łatwo zainstalować: składniki systemu są wyposażone w gniazda RJ45, które łączy się skrętką CAT 5. Aby uzyskać system dwukanałowy lub zwiększyć jego moc, można zastosować dodatkowe wzmacniacze Plena.

Bezpośr. inf. Bosch Security System

Samsung Techwin wprowadza linię kamer szybkoobrotowych **Speed Dome**

Osiem modeli popularnej serii kamer szybkoobrotowych SPD firmy **Samsung Techwin** zostało wprowadzone na rynek i jest obecnie dostępne w całej Europie.

– *W ofercie mamy modele kamer szybkoobrotowych odpowiednich do zastosowania przykładowo w małych sklepach, biurach, a także w większych obiektach, takich jak centra handlowe, parkingi i inne miejsca użyteczności publicznej* – mówi Peter Ainsworth, kierownik ds. produktów w dziale systemów zabezpieczeń firmy Samsung Techwin.

Siedem modeli ma ten sam wygląd i nadaje się do montażu wewnątrz budynku. Dostępny jest także duży wybór obudów zewnętrznych, umożliwiających montaż kamer na zewnątrz obiektu (do temperatury – 40°C). Uchwyty montażowe umożliwiają sprawne przenoszenie kamer z jednej podstawy do drugiej.

Modele powyższe są dostępne z 27-, 33- oraz 37-krotnym zoomem optycznym. Dwa modele tej linii (**SPD-3700T i SPD-3750T**) posiadają funkcję automatycznego śledzenia, która pozwala bez ingerencji operatora automatycznie śledzić obiekty i dokonywać zbliżenia w celu zebrania materiałów dowodowych. Funkcja ta może być szczególnie przydatna w przypadku takich zastosowań, jak nadzór wizyjny poza godzinami pracy oraz ochrona obwodowa. Wybrane modele mają udoskonaloną funkcję WDR (szeroki zakres dynamiczny), przydatną w trudnych warunkach oświetleniowych.

Standardowe modele wyposażono w funkcje ciągłego, dookolnego obrotu (360°) stref prywatności, DIS (cyfrowa stabilizacja obrazu), detekcji ruchu, a także pamięć ustawień oraz wielojęzyczne menu.

Model **SPD-1000** ma możliwość obrotu o 360 stopni w tempie 100 stopni na sekundę oraz większość cech wspólnych z pozostałymi kamerami serii. Model umożliwia realizację 10-krotnego zoomu optycznego. Dzięki temu kamera nadaje się praktycznie do wszystkich zastosowań zewnętrznych.

Wszystkie modele posiadają funkcję dzień/noc, wbudowany filtr podczerwieni, unikatową technologię redukcji szumów (SSNR) eliminującą szumy obrazu, odbicia i zamazania powstające w warunkach słabego oświetlenia. Dzięki temu można zaoszczędzić nawet 70% miejsca na twardym dysku oraz pasma transmisji sieciowej.

Dodatkowo dostępne są akcesoria do montażu kamer, w tym uchwyty do montażu naściennego, uchwyty zwieszane, uchwyty do montażu narożnikowego, wysięgnikowego, na słupie, do montażu podsufitowego, w suficie oraz montażu gzymsowego.

Bezpośr. inf. David Solomons
DRS Marketing

Dwudziesta rocznica wprowadzenia do sprzedaży systemu wizyjnego **Allegiant firmy Bosch**

Bosch Security Systems, producent pełnej gamy najwyższej jakości rozwiązań z zakresu bezpieczeństwa, obchodzi 20. rocznicę wprowadzenia na rynek systemów krosownic wizyjnych **Allegiant**. Firma świętuje również imponującą sprzedaż krosownic (niemal 30 000 sztuk).

Od roku 1989 firma Bosch wprowadziła na rynek osiem modeli systemu Allegiant. W celu spełnienia rosnących wymagań ze strony nabywców i użytkowników końcowych gama oferowanych produktów jest stale poszerzana. W roku 2009 firma wydała najnowszą aktualizację wszechstronnej serii LTC 900.

Krosownice serii Allegiant umożliwiają wyświetlenie obrazu z dowolnej kamery na dowolnym monitorze dołączonym do systemu. System taki doskonale sprawdza się w wielu zastosowaniach, od niewielkich instalacji począwszy, aż po instalacje obejmujące 6000 kamer, 500 monitorów i 120 klawiatur. Tego rodzaju systemy są instalowane w kasynach, więzieniach, domach poprawczych, na lotniskach, w obiektach rządowych oraz wielu innych obiektach komercyjnych i przemysłowych na całym świecie. Mają niezmiennie dobrą opinię jako urządzenia niezawodne i spójne pod względem obsługi.

Pełna oferta krosownic serii Allegiant znajduje się na stronie internetowej *www.boschsecurity.pl*.

Bezpośr. inf. Bosch Security Systems

HID na pulpicie

Wygoda i bezpieczeństwo spotykają się na pulpicie

Rozwiązanie „HID na pulpicie” (ang. *HID on the Desktop*) w wygodny sposób ułatwia zarządzanie ryzykiem w przedsiębiorstwie dzięki wykorzystaniu istniejących w organizacji kart do fizycznej kontroli dostępu w celu logowania się do infrastruktury IT.

Trzyelementowe rozwiązanie składa się z kart **Prox**, **iCLASS** lub **Crescendo**, czytników **OMNIKEY** i oprogramowania **NaviGO**. Zapewnia ono elastyczność w zakresie umożliwienia indywidualnych ustawień oraz spełnienia wymagań użytkowników w przypadku rozwiązań zarówno stykowych, jak i bezstykowych. *HID on the Desktop* umożliwia organizacji rozpoczęcie stosowania tego rozwiązania przy małej liczbie kart oraz zaplanowanie dalszego rozwoju zgodnie z jej potrzebami. Pozwala poza tym na implementację różnych poziomów bezpieczeństwa dla różnych typów użytkowników w ramach tej samej organizacji, przy wykorzystaniu w każdym z przypadków oprogramowania NaviGO. Użytkownicy nie muszą wybierać tego czy innego rozwiązania, a i zastosowany sprzęt wraz z oprogramowaniem są łatwe do instalacji i zarządzania oraz wymagają tylko minimalnego wsparcia ze strony działu IT.

HID Global dostarcza obecnie niezbędne elementy logicznej kontroli dostępu, które wspierają e-platformy fizycznej kontroli dostępu. Jest to konwergentne rozwiązanie

z pojedynczą kartą, która może służyć zarówno jako identyfikator, jak i „klucz” do otwierania drzwi. Może ona być użyta także w celu uwierzytelniania przy logowaniu się do komputera stacjonarnego albo laptopa.

HID on the Desktop służy do zapewniania: wygody – użytkownikowi, prostoty – kierownikowi i wyższego poziomu bezpieczeństwa dostępu logicznego – organizacji.

Bezpośr. inf. HID Global
Tłumaczenie: Redakcja

Siemens chroni bibliotekę Albertina w Lipsku

Siemens Building Technologies opracował i zainstalował kompletny system zabezpieczeń dla jednej z najstarszych i najważniejszych bibliotek na świecie.

Dla ochrony biblioteki Albertina, głównego budynku biblioteki uniwersyteckiej w Lipsku, jednej z najstarszych bibliotek uniwersyteckich w Niemczech, Siemens dostarczył w pełni działający system obejmujący detekcję włamań, nadzór telewizyjny, detekcję pożarów oraz system zarządzania bezpieczeństwem. Założona w roku 1543 biblioteka służy jako źródło literatury i informacji dla studentów i pracowników uniwersytetu oraz dla szerokiej publiczności. Jej ogromne zbiory historyczne i kolekcje specjalne znane są nie tylko w Niemczech, ale i na całym świecie.

Kompletny system zabezpieczeń zaprojektowano i zainstalowano w trzech etapach dla zapewnienia ochrony personelu i studentów uniwersytetu, wypożyczających oraz zasobów bibliotecznych (szczególnie cennych książek) przed ogniem, zniszczeniem i kradzieżą.

System sygnalizacji włamania obejmuje 1216 grup czujek i 26 obszarów zamków blokowych z 83 drzwiami oraz ochroną okien dla celów ochrony obwodowej. Różne obszary biblioteki zabezpiecza 125 czujek ruchu w technologii zwykłej i dualnej. Eksponaty specjalne są chronione przez 12 czujek w witrynach wystawienniczych i 23 czujki do ochrony obrazów (czujki firmy Siemens). W skarbcu, w którym zgromadzone są najwartościowsze książki z biblioteki, zainstalowano 32 czujki sejsmiczne Siemensa. System alarmowy jest połączony z systemem nadzoru wizyjnego Siemensa, który obejmuje zapis cyfrowy oraz przechowywanie obrazów z danymi zebranymi przez 17 kamer. W przypadku alarmów włamaniowych lub nadużycia wyjść awaryjnych umożliwiają one szybkie zbadanie zdarzenia.

System detekcji pożaru **AlgoRex** firmy Siemens zawiera 270 grup czujek z ponad 1000 detektorów, 21 systemów zasysających, system usuwania dymu i ciepła z 10 centralami i 60 napędami oraz ochronę drzwi ewakuacyjnych z 23 centralami.

System zarządzania bezpieczeństwem biblioteki (DMS – *danger management system*) łączy system sygnalizacji włamania z systemem detekcji pożaru, a także umożliwia sterowanie klimatyzacją budynku. DMS zapewnia indywidualny dostęp do każdego systemu. System biblioteczny jest używany jako zdalny system zarządzania, który poprzez Ethernet łączy się sieciowo z najważniejszymi obiektami biblioteki. Jest to ekonomiczny sposób zapewnienia zdalnego dostępu do działającego systemu, szczególnie wieczorami i w weekendy, kiedy to służba ochrony może zdalnie monitorować zdarzenia w bibliotece.

Poza budynkiem głównym Bibliotheca Albertina w skład biblioteki wchodzi czterdzieści innych obiektów, usytuowanych blisko instytucji akademickich. Aktualnie jej magazyn obejmuje pięć milionów woluminów i około 7700 periodyków. Są tam między innymi rękopisy średniowieczne i nowożytne, inkunabuły, papirusy, autografy, ostrakony i monety.

Sam Uniwersytet Lipski, znajdujący się w Wolnym Państwie Saksonia w Niemczech, jest jednym z najstarszych uniwersytetów w Europie. Uniwersytet ten to 600 lat nieprzerwanego nauczania i badań. W roku 2005 w centrum Lipska rozpoczęto budowę głównego budynku. Szacowany koszt projektu wyniesie 140 milionów euro. Zakończenie prac przewidywane jest na rok 2009, czyli na czas świętowania 600-lecia uniwersytetu.

Źródło: www.securityworldhotel.com
Tłumaczenie: Redakcja

Hybrydowe rejestratory wizyjne **Divar XF** firmy Bosch

Hybrydowa konstrukcja zapewnia obsługę kamer analogowych i sieciowych H.264 oraz zoptymalizowanej macierzy RAID-4

Nowy cyfrowy rejestrator wizyjny **Bosch Divar XF** to inwestycja przyszłościowa. Hybrydowa konstrukcja umożliwia obsługę ośmiu lub 16 kamer analogowych i maksymalnie ośmiu kamer sieciowych H.264. Firma Bosch wyposażyła urządzenie w zaawansowane funkcje zapewniające najwyższą możliwą jakość i maksymalną ochronę zapisywanego obrazu.

Rejestrator Divar XF umożliwia zapis i odtwarzanie w czasie rzeczywistym w pełnej rozdzielczości 4CIF dla wszystkich kanałów. Zapewnia przy tym wysoką jakość obrazu, zarówno przy podglądzie obrazu bieżącego, jak i odtwarzaniu zapisu. Dzięki zastosowaniu zaawansowanej technologii kompresji H.264 urządzenie dodatkowo minimalizuje zapotrzebowanie na pasmo przesyłania i przestrzeń zapisu. Koszty przestrzeni zapisu maleją nawet o 30% w porównaniu z systemami bazującymi na dotychczasowym kodowaniu MPEG-4.

Fakt, że obraz zapisywany jest na maksymalnie czterech wewnętrznych dyskach twardych, gwarantuje najwyższą ochronę zapisanego materiału wizyjnego. Dyski są dostępne z płyty czołowej urządzenia, co zapewnia łatwe serwisowanie i elastyczne możliwości dodawania kolejnych dysków twardych i (lub) dysków o większej pojemności (w razie potrzeby). Obecnie dzięki zestawowi rozbudowy przestrzeni zapisu możliwe jest powiększenie jej do maks. 4 TB. Rejestrator Divar XF obsługuje również wbudowaną zoptymalizowaną macierz RAID-4 (ang. *Redundant Array of Independent Disks*), czyli technologię zapewniającą całkowitą niezawodność systemu nawet w przypadku awarii dysku twardego.

Seria rejestratorów Divar XF posiada dodatkowo wbudowaną nagrywarkę DVD, dzięki której możliwy jest zapis sekwencji wizyjnych bezpośrednio na płycie (bez potrzeby dołączania komputera PC).

Funkcja połączenia przelotowego klawiatury umożliwia sterowanie maksymalnie 16 rejestratorami Divar XF za pomocą jednej klawiatury Bosch IntuiKey. Zapewnia to pełną kontrolę nad systemami złożonymi z wielu rejestratorów i maksymalnie 384 kamer PTZ przy pomocy tylko jednego joysticka.

Zainstalowane już rejestratory Divar XF można zaktualizować do wersji 2.0 oprogramowania układowego bez ponoszenia jakichkolwiek kosztów. Oprogramowanie układowe w wersji 2.0 i oprogramowanie na komputer PC do zdalnego dostępu są teraz dostępne na stronie internetowej firmy Bosch Security Systems. Niektóre nowe funkcje wymagają opcjonalnej licencji programowej.

Rejestrator Divar XF jest przeznaczony przede wszystkim do zastosowania w średnich, dużych lub rozwojowych systemach dozorowych instalowanych np. w centrach handlowych, bankach, instytucjach finansowych, centrach miast, kasynach i hotelach.

Bezpośr. inf. Bosch Security Systems

Niezwykły projekt głowicy **ULISSE COMPACT** firmy **Videotec**

VIDEOTEC zaprezentował na targach IFSEC nowy produkt z grupy zaawansowanych głowic obrotowych z rodziny ULISSE. Głowica **ULISSE COMPACT** ma oryginalny i bardzo ciekawy *design*. Charakteryzuje się ona wytrzymałą i zwartą konstrukcją oraz cechami, które czynią ją optymalnym rozwiązaniem dla instalacji telewizji dozorowej.

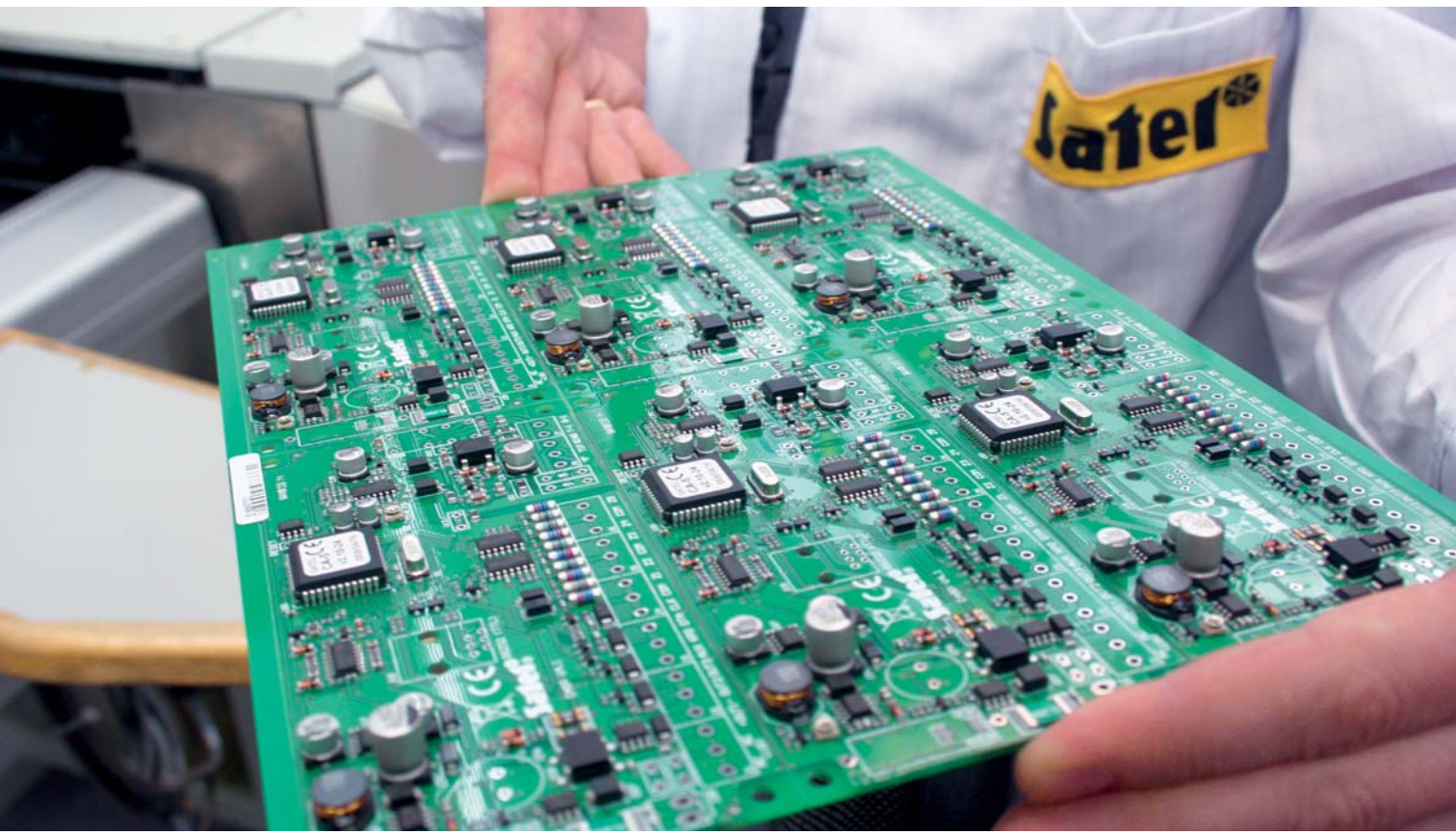
Głowica ULISSE COMPACT łączy ciągły obrót o dużej prędkości i płynności z dokładnym pozycjonowaniem i prostotą instalacji. Wbudowany moduł kamery **Sony** zapewnia najwyższą jakość obrazu i wyjątkową precyzję (nawet w środowisku o słabym oświetleniu).

Głowica ULISSE COMPACT doskonale sprawdza się w warunkach zewnętrznych. Może służyć do obserwacji ruchu ulicznego, autostrad, nabrzeży i portów, do obserwacji granic, stadionów, terenów przemysłowych, zakładów karnych oraz obiektów wojskowych. Jest także wykorzystywana w systemach ochrony obwodowej.

Bezpośr. inf. VIDEOTEC SpA
Tłumaczenie: Redakcja

Wywiad z Ireneuszem Kowalukiem współwłaścicielem firmy SATEL

rozmawia Teresa Karczmarzyk



Satel to firma z niewątpliwie bogatą i prawie dwudziestoletnią tradycją. Proszę powiedzieć, skąd wziął się pomysł na firmę o takim profilu?

Jako młodzi absolwenci Politechniki z wiedzą i ambicjami postanowiliśmy zrealizować swoje pasje. Profil był wyborem przypadkowym. Interesowało nas bardzo wiele obszarów z zakresu elektroniki, jednak ostatecznie wybraliśmy urządzenia do systemów alarmowych – i chyba postąpiliśmy właściwie.

Ilu pracowników zatrudnia firma i jak bardzo powiększyła się przez lata działalności?

Powiększyła się. W 1998 roku zatrudnialiśmy 29 osób. W 2000 roku (pamiętam, jak organizowaliśmy 10-lecie firmy) było 50 osób łącznie z kooperantami i wtedy wydawało nam się, że jest to bardzo duża firma. Dziś zatrudniamy blisko 250 osób (pracowników etatowych i osoby pracujące dla nas na zlecenie). Jest to już całkiem spora liczba, a co za tym idzie – duża odpowiedzialność.

W jaki sposób udało się firmie zaistnieć na rynku polskim? Przecież w Polsce jest obecnych wiele renomowanych firm zagranicznych i wydawałoby się, że mogą one stanowić silną konkurencję.

Naszym zdaniem dobry produkt to podstawa. Zwłaszcza taki, który w całości – od koncepcji poprzez konstrukcję, badania i testy aż do postaci finalnej – powstał w jednej firmie, w której jest także produkowany i serwisowany. Wiedza o takim produkcie umożliwia jego rozwój, zwłaszcza w kontekście wsłuchiwania się w oczekiwania klienta. Dobry produkt to również perfekcyjna technologia gwarantująca powtarzalną jakość produktu. No i... ludzie, ludzie, ludzie...

Na tle tej ogromnej konkurencji wyroby Satela wyróżniają się bardzo dobrą jakością. Jakie kroki przedsięwzięliście, aby tak było?

Główną receptą na sukces jest ciągłe udoskonalanie procesów ukierunkowanych na rozwój i na uzyskanie satysfakcji klientów.

Firma Satel ma już prawie 20 lat. Na jakim etapie znajduje się obecnie, co jest jeszcze do zrobienia w perspektywie najbliższych lat?
Wciąż mamy nowe pomysły, wciąż nam się jeszcze trochę chce, w związku z tym nie zamierzamy zrezygnować z rozwoju. Zawsze będzie coś ciekawego do zrobienia.

Co stanowi obecnie ofertę firmy Satel?
W ofercie mamy blisko 250 pozycji cennikowych. Główne grupy wyrobów to centrale alarmowe, czujki różnych typów, sygnalizatory oraz moduły komunikacyjne GSM i moduły ethernetowe. Ważnymi produktami są dwukierunkowy system bezprzewodowy ABAX i system kontroli dostępu ACCO. Interesującą pozycją w naszej ofercie są również stacje monitorowania. Pełną ofertę można znaleźć na naszej stronie internetowej.

Czy w najbliższej przyszłości planowane jest rozszerzenie gamy urządzeń systemu bezprzewodowego ABAX o klawiatury bezprzewodowe?
Tak. W ciągu najbliższych kilku miesięcy powinny pojawić się klawiatury bezprzewodowe do systemu ABAX oraz sterowniki typu pilot, umożliwiające dwukierunkową komunikację z systemem alarmowym.

Czy planowane jest stworzenie centrali alarmowej dla bardzo rozbudowanych aplikacji o liczbie linii dozorowych większej niż 128?
Prowadzimy takie prace.

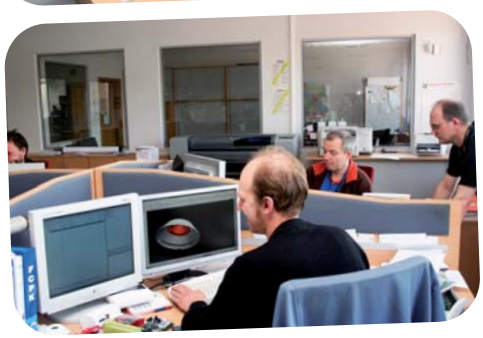
Czy seria aktywnych barier podczerwieni będzie rozszerzana o urządzenia o większych niż dotychczas zasięgach?
Nie planujemy tego w najbliższym czasie.

W ofercie firmy znajdują się dzielniki obrazu z serii SV. Czy firma planuje dalszą ekspansję na rynku telewizji dozorowej? Mam na myśli rozszerzenie oferty o kamery, cyfrowe rejestratory wizji etc.
W najbliższym czasie nie planujemy uruchomienia produkcji nowych wyrobów związanych z CCTV. W ciągu najbliższych trzech lat będziemy mieć tak dużo innych projektów do wykonania, że niezbyt poważnie byłoby deklarować jakieś prace związane z rozszerzeniem oferty telewizji dozorowej.

Ponieważ jedną z najbardziej widocznych części systemu alarmowego stanowi klawiatura, część klientów końcowych zadaje pytania dotyczące możliwości jej wyboru. Czy w najbliższej przyszłości planujecie stworzenie dodatkowej linii klawiatur o zupełnie odmiennym i nowatorskim wyglądzie?
Pracujemy nad tym.





Jakie nowoczesne technologie wdraża firma? Jakich ciekawych nowych produktów Satela możemy oczekiwać w najbliższej przyszłości?

Pracujemy nad wieloma nowymi rzeczami, ale jest za wcześnie na to, by mówić o konkretach. Z pewnością będziemy rozwijać systemy kontroli dostępu i systemy bezprzewodowe.

Gdzie macie swoje przedstawicielstwa za granicą i w jakich krajach firma odniosła największy sukces?

Nasze produkty są sprzedawane w około czterdziestu krajach na całym świecie. Obecnie kierujemy eksport przede wszystkim do Europy Środkowej i krajów skandynawskich.

Czy zamierzacie rozwijać sieć dealerów zewnętrznych, czy może planujecie własną?

Jako producent skupiamy się na produkowaniu dobrego produktu; na razie nie zamierzamy budować własnej sieci dystrybucji.

Czy ciągle szukacie nowych rynków zbytu?

To oczywiste, że każdy szanujący się producent szuka nowych rynków zbytu. Naturalne jest również budowanie i umacnianie marki oraz popularyzowanie produktów. Stąd nasz udział w wielu branżowych targach na terenie całej Europy, między innymi w Paryżu, Moskwie, Birmingham, Mediolanie. Jest to dobry sposób poszukiwania nowych rynków zbytu.

Jakie produkty są liderem eksportu w firmie?

Na pewno centrale. Systemy bezprzewodowe oraz kontrola dostępu – jako produkty relatywnie nowe – również bardzo dobrze rokują.

Czy działalność Satela jest odporna na konkurencję z Dalekiego Wschodu?

Sprzedajemy produkty o określonej funkcjonalności i jakości. Kierujemy je do świadomych klientów, dajemy wsparcie techniczne i serwis, organizujemy sympozja i szkolenia, słuchamy uwag klientów. Moim zdaniem, działając w ten sposób, oferujemy produkty zupełnie inne niż dalekowschodnie.

Czy z punktu widzenia prowadzenia biznesu i ze względu na specyfikę rynku security popyt jest uzależniony przede wszystkim od jakości asortymentu? Przecież nawet w naszej branży decydującą rolę odgrywa czynnik cenowy.

Cena powinna odzwierciedlać jakość produktu. W branży samochodowej prawie wszyscy to rozumieją i akceptują. W naszej branży niestety nie zawsze. Cena jest oczywiście ważna, ale warto czasami zastanowić się nad tym, co za nią otrzymujemy.

Czego się spodziewacie w 2009 r.? Jaki to będzie rok dla branży security w Polsce?

Dla nas będzie to kolejny rok wytężonej pracy. W naszej branży natomiast zmniejszy się prawdopodobnie liczba dużych inwestycji, może będzie mniej pieniędzy z budżetu na rozwój czy rozbudowę systemów w administracji. Uważam, że będzie to rok, w którym możemy zwrócić się w kierunku takich inwestorów jak umowny „Kowalski" – nasz klient docelowy. Tak jak standardem w nowobudowanych domach jedno- i wielorodzinnych stało się budowanie instalacji antenowej, tak obecnie wykonuje się również instalację telefoniczną, domofonową i alarmową. Rynek masowy to cel, który chcemy jak najszybciej osiągnąć.

Dlatego firma Satel jest pomysłodawcą/współautorem strony www.mieszkajbezpiecznie.pl?

Taki był nasz pomysł na dotarcie do tego olbrzymiego segmentu rynku. Chcemy w sposób prosty i zrozumiały przedstawić nasze systemy. Myślę, że wraz ze wzrostem świadomości klienta popularność naszych produktów będzie rosła.

Satel jest polską firmą. Czy odczuwacie skutki światowego kryzysu gospodarczego?

O kryzysie u nas raczej trudno mówić. Realizujemy zamówienia, wprowadzamy do sprzedaży nowości, planujemy nowe produkty, inwestujemy w udoskonalanie technologii, rozwijamy działy wsparcia sprzedaży. U nas kryzysu nie widać. Na razie...

Jak po okresie boomu w budownictwie, z jakim mieliśmy do czynienia chociażby jeszcze rok temu, obecnie kształtuje się sprzedaż wyrobów firmy?

Nie zauważamy szczególnej różnicy.

Jak podsumowalibyście rok 2008? Jakie są Państwa plany na rok 2009?

Rok 2008 był dobry dla naszej firmy. Zakończyliśmy budowę nowej hali produkcyjnej, debiutowaliśmy – z sukcesem – na targach we Włoszech i we Francji, pozyskaliśmy wielu nowych klientów. Chcielibyśmy, aby rok 2009 nie był gorszy.

Czy Satel ma jakąś strategię, misję, która przyświeca działalności firmy?

Jak już wcześniej mówiłem, staramy się robić wszystko jak najlepiej, z pasją i zaangażowaniem.

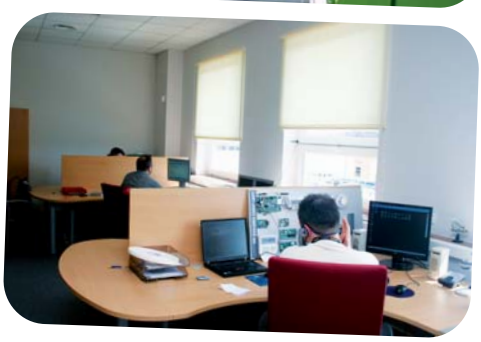
Co w tym momencie jest największą siłą firmy?

Myślę, że ludzie, ich doświadczenie i wiedza. Równie ważne są metody oraz organizacja pracy.

Czy trudno jest łączyć pełne pasji życie zawodowe z życiem prywatnym?

Trzeba umieć zachować odpowiedni dystans i unikać kolizji, tak aby rodzina na tym nie ucierpiała.

Dziękuję bardzo za rozmowę i życzę powodzenia w realizacji planów.



ZSJZ

AQAP 2110:2006

SYSTEM ZARZĄDZANIA PCBC

Certyfikowany na zgodność z: PN - EN ISO 9001 : 2001

firma **ATLine®**

kompleksowe zabezpieczanie obiektów

16 LAT DOŚWIADCZENIA

BEZPIECZEŃSTWO
W KAŻDYCH WARUNKACH

16 lat doświadczenia, profesjonalizm i wysoka jakość oferowanych przez nas usług, gwarantują Państwu pełną satysfakcję.
Oferujemy Państwu atrakcyjne ceny, bezpłatne szkolenia i wsparcie fachowców w ramach zakupu.
Zapraszamy na naszą stronę www.atline.pl
Wszelkie wyceny i propozycje zabezpieczeń przeprowadzamy bezpłatnie.

- wykonywanie kompleksowych dokumentacji technicznych i architektoniczno-budowlanych
- wykonywanie zaawansowanych systemów bezpieczeństwa
- sprzedaż (głównie zewnętrznych systemów ochrony obwodowej)

Firma ATLine sp.j. K. Cichulski S. Pruski, 91-845 Łódź, ul. Franciszkańska 125
tel. +48 042 657 30 80, fax +48 042 655 20 99, e-mail: info@atline.pl, handel@atline.pl

Versa
wszechstronne centrale alarmowe

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

Satel®

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

Wykorzystanie sterowników PLC

do budowy systemów realizujących funkcje SSWiN i SSP w budynku mieszkalnym

W budynkach mieszkalnych coraz częściej instaluje się systemy automatyki sterujące pracą poszczególnych urządzeń i grup urządzeń w celu uzyskania określonych w danym momencie parametrów i stanów. Dodatkowo użytkownik chce mieć również bieżącą informację dotyczącą stanu obiektu. W artykule zostanie przedstawiona koncepcja budowy układu realizującego funkcje systemu sygnalizacji włamania i napadu (SSWiN) oraz systemu sygnalizacji pożarowej (SSP) wykorzystującego sterownik programowalny PLC zamiast standardowej centrali alarmowej. W artykule zostaną przedstawione możliwości i ograniczenia takiego układu w porównaniu z klasycznym wykonaniem systemu SSWiN i SSP

Wstęp

Od nowoczesnych instalacji elektrycznych stosowanych w budynkach mieszkalnych coraz częściej wymaga się realizacji założeń idei inteligentnych budynków. Jako budynek inteligentny rozumiemy budynek, w którym zainstalowane urządzenia w celowy i właściwy sposób reagują samoistnie na występujące w jego otoczeniu zdarzenia oraz zmieniające się czynniki zewnętrzne [5]. Z punktu widzenia użytkownika budynku mieszkalnego oprócz niezawodności i skuteczności takiego systemu ważne jest jeszcze kilka innych czynników. Pierwszym czynnikiem, szczególnie ważnym na etapie procesu inwestycyjnego, jest ograniczenie kosztów instalacji. Następne cechy, szczególnie ważne już w okresie użytkowania obiektu, to programowalność systemu oraz jego ergonomiczność i energochłonność. Pogodzenie wszystkich przedstawionych cech wydaje się być zrealizowane tylko w przypadku zastosowania systemu zintegrowanego, w którym rolę centrali nadzorująco-sterującej będzie realizował jeden układ, np. sterownik PLC. Takie rozwiązanie upraszcza konfigurację systemu i eliminuje konieczność powielania elementów, które realizują tę samą funkcję, ale współpracują tylko z jednym układem autonomicznym (na przykład tylko z systemem SSWiN). Z drugiej strony uniemożliwia ono jednak wykorzystanie klasycznych układów spełniających wprawdzie tylko wąski, ale wyspecjalizowany zakres możliwości.

W dalszej części artykułu zostanie przedstawiona koncepcja budowy systemów SSWiN i SSP realizowana na bazie sterownika PLC. W opisywanym systemie jako elementy detekcyjne i wykonawcze będą zastosowane standardowe elementy wykorzystywane w klasycznych systemach SSWiN i SSP (detektory, czujki, manipulatory, sygnalizatory optyczno-akustyczne). Niniejszy artykuł odnosi się w szczególności do układów stosowanych w budownictwie (zastosowanie w pojedynczych mieszkaniach lub domach jednorodzinnych, gdzie nie występuje żaden wyspecjalizowany dozór zewnętrzny), dlatego zbudowany system realizujący funkcje SSWiN i SSP będzie musiał spełniać następujące wymagania dotyczące [1]:

- kategorii zagrożenia mienia i osób – Z1 (mienie o małej wartości),
- klasy systemu alarmowego – SA1 i SA2 (zastosowanie w obiektach o małym lub średnim ryzyku szkód),
- klasyfikacji środowiskowej elementów SSWiN – klasa I i II (wewnętrzna ograniczona i wewnętrzna).

Zaproponowane rozwiązanie ma na celu podniesienie bezpieczeństwa użytkowania całego budynku dzięki zastosowaniu indywidualnych systemów autonomicznych, które w mieszkaniach lub domach jednorodzinnych będą realizować zadania stawiane systemom SSWiN i SSP. Taki system umożliwi również użytkownikowi dostosowanie procedur do własnych potrzeb, szczególnie gdy system realizujący funkcje systemów SSWiN i SSP będzie częścią zintegrowanego systemu sterowania. Dodatkowo celem takiego rozwiązania jest ograniczenie kosztów obsługi tego systemu oraz zewnętrznej ingerencji w pracę systemu, jakie mogłyby zaistnieć w przypadku zastosowania scentralizowanego rozwiązania dla grupy użytkowników. Na stworzonym modelu systemu alarmowego (wykorzystanie modułu MFD firmy Moeller) zostaną przeprowadzone badania sprawdzające możliwości takiego układu w porównaniu z funkcjami i zadaniami realizowanymi przez fabryczne układy decyzyjne (centrale alarmowe) dla systemów SSP i SSWiN spełniające opisane wyżej wymagania.

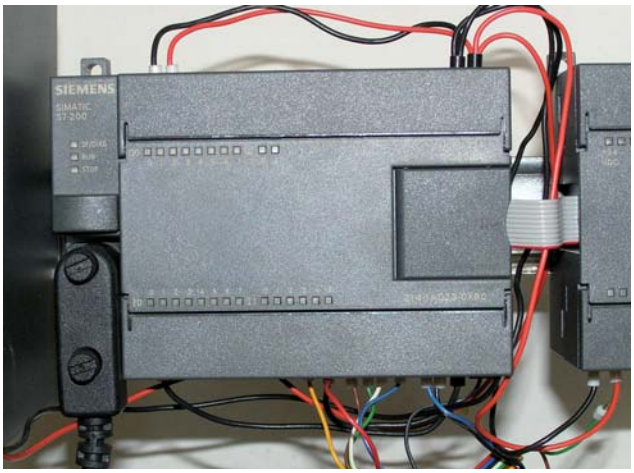
Sterowniki PLC

Norma IEC 61131-1 [2] definiuje programowalny sterownik cyfrowy (*ang. Programmable Logic Controller* – PLC) jako cyfrowy system elektroniczny do stosowania w środowisku przemysłowym. Posługuje się on programowalną pamięcią do przechowywania zorientowanych na użytkownika instrukcji w celu sterowania szeroką gamą maszyn i procesów za pomocą cyfrowych lub analogowych wejść i wyjść. Definicja zawarta w normie sugeruje, że sterowniki PLC wywodzą się z automatyki przemysłowej, gdzie były i nadal są wykorzystywane do sterowania grupami urządzeń w procesach produkcyjnych. Bardziej uogólniona definicja sterownika PLC określa go jako układ mikroprocesorowy przeznaczony do sterowania pracą urządzeń i procesów. Sterowniki te spełniają wszystkie funkcje stycznikowych i przekaźnikowych układów sterowania, układów logicznych, programatorów oraz układów przetwarzających sygnały dyskretne i ciągłe [3].

Od czasu pierwszych zastosowań w przemyśle sterowniki PLC przeszły długą drogę w procesie ciągłego dostosowywania się do potrzeb użytkownika. Szybko się okazało, że zalety przemysłowych sterowników PLC zostały zauważone również przez użytkowników ogólnych. Obecnie wyróżnia się dwie grupy sterowników:

– sterowniki przemysłowe (np. Siemens typ S7200; fot. 1a),
– sterowniki do zastosowań ogólnych (np. Siemens LOGO, Moeller Easy; fot. 1b).

Sterowniki przemysłowe z racji przewidzianego zastosowania są bardziej rozbudowane, mają większe możliwości konfiguracyjne, obsługują większą ilość układów wejścia/wyjścia

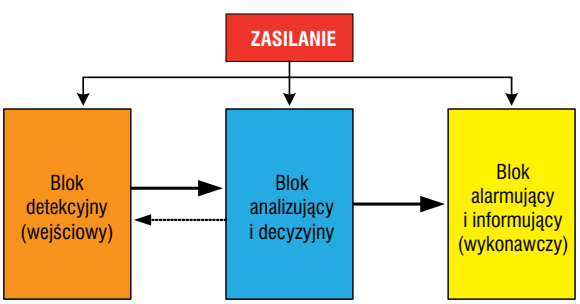


Fot. 1a. Przemysłowy sterownik programowalny PLC

Fot. 1b. Sterownik programowalny PLC ogólnego przeznaczenia

(wejście/wyjście to w skrócie I/O). Jednak są one dość drogie (koszt kilkanaście razy większy w porównaniu z ceną sterownika PLC ogólnego przeznaczenia). Zatem takie układy mogą być wykorzystywane tylko w rozbudowanych systemach automatyki i z racji swojej ceny nie są stosowane ani spotykane w budynkach mieszkalnych. Sterowniki do zastosowań ogólnych są układami mniej skomplikowanymi pod względem technologicznym, dzięki czemu ich cena jest dużo niższa (koszt pojedynczego sterownika kształtuje się już od kilkuset złotych). Ich możliwości programowe nie odbiegają od możliwości sterowników przemysłowych (ograniczona jest jedynie liczba poszczególnych modułów funkcyjnych i układów I/O). Obecnie pewnym standardem stało się wyposażanie sterowników PLC we wbudowane układy komunikacyjne, umożliwiające zarówno ich łączenie z jednostką programującą (port komunikacyjny sterownika-komputer), jak i ich wzajemną współpracę. Takie rozwiązanie umożliwia budowę rozproszonych systemów sterujących, które zwiększają możliwości konfiguracyjne systemu przy jednoczesnym ograniczeniu okablowania instalacyjnego.

Uruchomienie sterownika PLC rozpoczyna się od wpisania algorytmu programu do jego pamięci operacyjnej. W tym celu można wykorzystać wbudowane w sterownik przyciski funkcyjne. Najczęściej jednak wczytanie programu odbywa się z komputera PC z zainstalowanym programem konfiguracyjnym za pomocą przewodu komunikacyjnego.



Rys. 1. Schemat blokowy systemu alarmowego

Zgodnie z normą IEC 61131 [2] określone zostały następujące ujednolicone języki programowania:

– języki tekstowe:
  • IL (*Instruction List*) – listy instrukcji,
  • ST (*Structured Text*) – tekst strukturalny.
– języki graficzne:
  • LD (*Ladder Diagram*) – schemat drabinkowy,
  • FBD (*Function Blok Diagram*) – schemat bloków funkcyjnych,
  • grafy sekwencji SFC (*Sequential Function Chart*).

Ze względu na realizowane zadania w sterowniku PLC wyróżnia się trzy podstawowe elementy [4]:

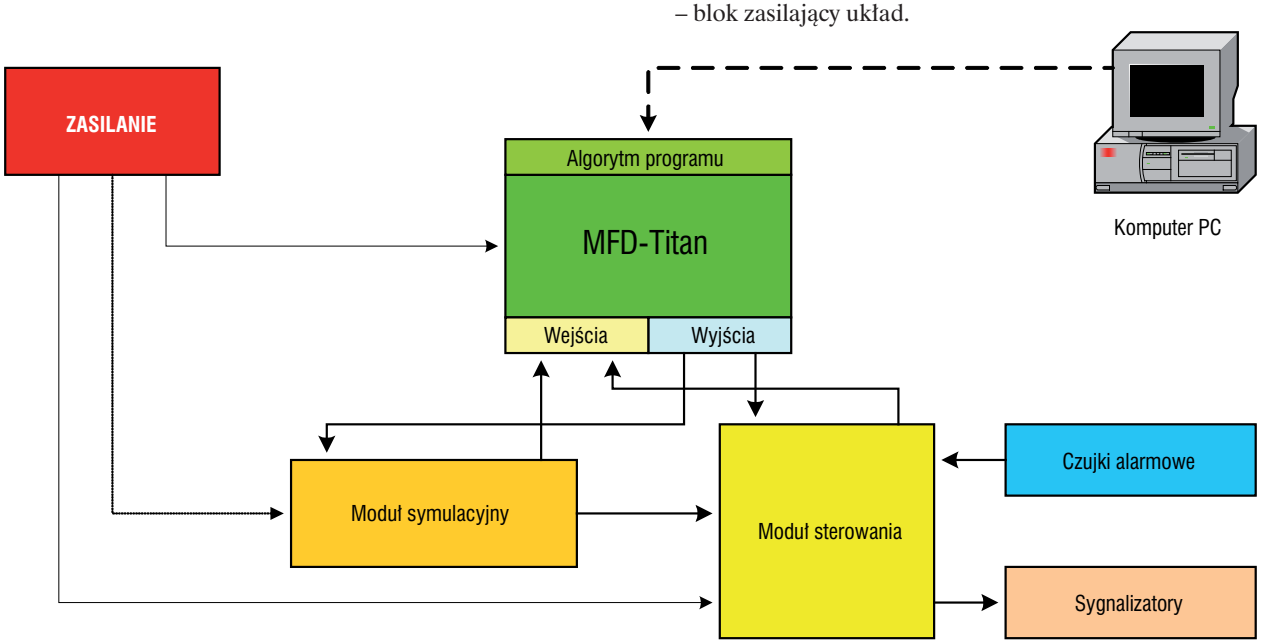
– moduły wejściowe, których zadaniem jest wprowadzanie do systemu sterownika analogowych i cyfrowych sygnałów wejściowych (np. z czujek, łączników);
– jednostkę centralną (CPU), która przetwarza sygnały wejściowe zgodnie z zadanym (zapisanym w pamięci sterownika) algorytmem oraz przekazuje wyniki na wyjścia;
– moduły wyjściowe, których zadaniem jest przekazywanie obliczonych wartości do elementów wykonawczych.

Zadaniem sterownika programowalnego jest sterowanie wyjściami na podstawie informacji otrzymywanych z wejść sterownika oraz procedur zawartych w blokach funkcyjnych.

System SSWiN i SSP oparty na sterowniku PLC jako jednostce zarządzającej

Zadanie stawiane systemom alarmowym to skuteczne powiadomienie użytkownika o zaistniałym zagrożeniu. Technicznie jest to zespół współpracujących urządzeń (również z instalacją przewodową), które mają na celu wykrywanie zagrożeń, wywołanie alarmu oraz inicjowanie przedsięwzięć zmierzających do likwidacji takiego zagrożenia. Ze względu na cele stawiane takiemu systemowi można w nim wyodrębnić kilka podstawowych powiązanych ze sobą bloków funkcyjnych (rys. 1):

– blok analizująco-decyzyjny,
– blok detekcyjny (wejściowy),
– blok alarmująco-informujący (wykonawczy),
– blok zasilający układ.



Rys. 2. Schemat blokowy modelu systemu alarmowego zbudowanego z wykorzystaniem sterownika PLC

W zależności od przyczyny wywołania alarmu (w przypadku systemu SSWiN jest to naruszenie strefy chronionej, a w przypadku systemu SSP – wykrycie ogniska pożaru) rola systemu nadzorującego wykorzystywanego w obiektach mieszkalnych (mieszkania lub domy jednorodzinne) sprowadza się zazwyczaj do powiadomienia użytkownika oraz otoczenia o zaistniałym zagrożeniu. Dodatkowo, jeśli spełnione są pewne konieczne wymagania techniczne (np. powiązanie systemu SSWiN lub SSP z innymi systemami automatyki budynku), może również nastąpić dalsze przekazanie informacji do innych układów, które spowodują na przykład blokadę wyjść (w przypadku wykrycia włamania) lub odbezpieczenie zamków wyjść (w przypadku wykrycia zagrożenia pożarowego).

Na rys. 2 przedstawiono schemat blokowy systemu realizującego funkcje systemów SSWiN i SSP oraz wykorzystującego sterownik PLC jako jednostkę sterującą pracą układu.

Na rys. 2 oprócz sterownika PLC, elementów detekcyjnych i sygnalizacyjnych, które wchodzą w skład tradycyjnego schematu blokowego systemu alarmowego, umieszczono także blok symulacyjny i blok sterowania (pośredniczący). Za pomocą tych bloków możliwe jest podłączenie poszczególnych manipulatorów, czujek alarmowych i sygnalizatorów oraz przeprowadzenie symulacji działania zaproponowanego algorytmu bez konieczności podłączania do wejść i wyjść rzeczywistych elementów.

Taka budowa stanowiska umożliwia przeprowadzenie pełnej symulacji oraz zaprezentowanie możliwości i funkcjonalności poszczególnych elementów systemu alarmowego. Za pomocą odpowiedniej konfiguracji modelu możliwe jest również badanie fabrycznych central alarmowych.

Do badań użyto sterownika MFD-Titan firmy Moeller (fot. 2) jako układu realizującego funkcję centrali alarmowej. W jego skład wchodzą następujące podzespoły:

– moduł CPU – MFD-CP8-NT,
– moduł wyświetlacza – MFD-80-B,
– moduł wejść/wyjść – MFD-R16.

Fot. 2. Moduły sterownika programowalnego MFD-Titan

Na fot. 3 został przedstawiony widok panelu czołowego modelu systemu alarmowego, który wykorzystuje sterownik PLC jako centrum decyzyjne.

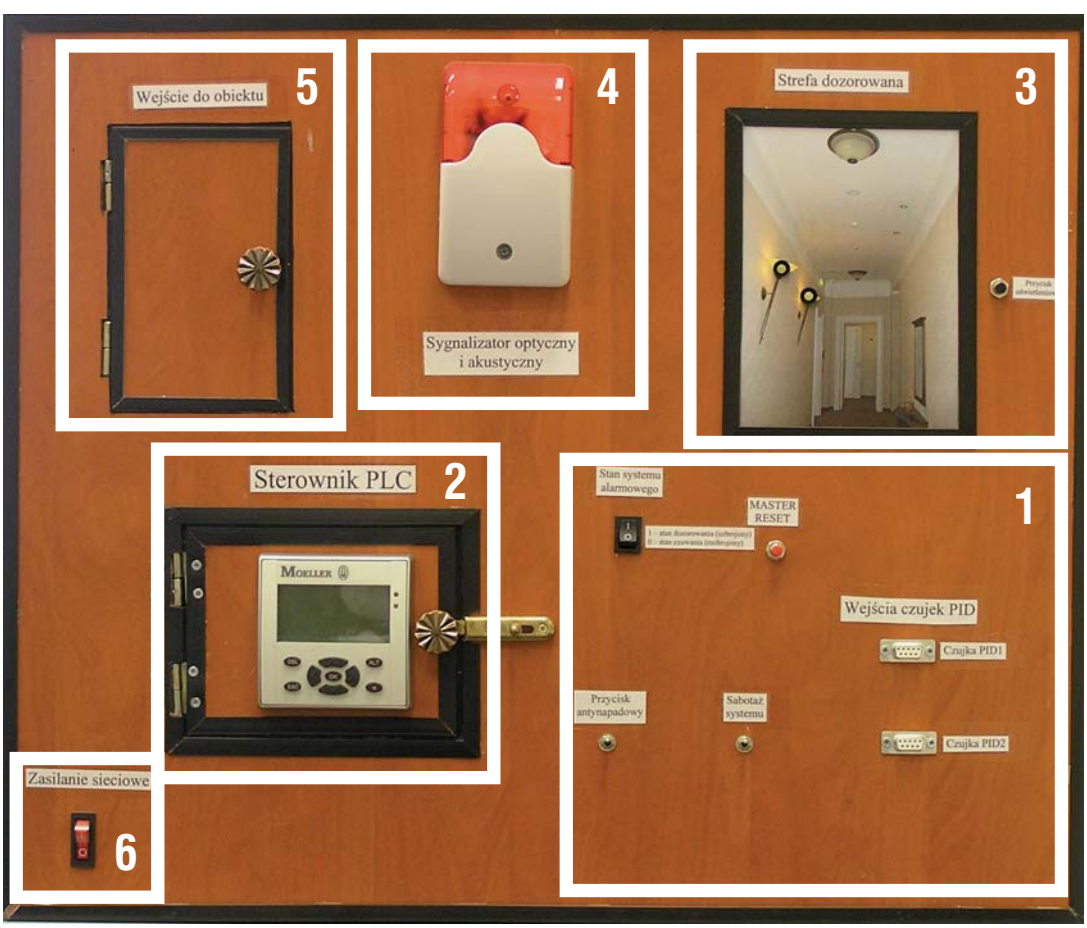
Umieszczony na płycie czołowej panel symulacyjny i wejściowy (obszar 1 na fot. 3) umożliwia zarówno zasymulowanie pewnych zdarzeń, jak i podłączenie rzeczywistych obiektów w celu sprawdzenia działania takiego systemu w rzeczywistości. W charakterze elementów wejściowych można podłączyć szeroką gamę czujek alarmowych stosowanych w systemach SSWiN (czujki PIR, mikrofalowe, mikrofonowe, kontaktronowe) oraz systemach SSP (optyczne lub jonizacyjne czujki dymu), manipulatorów i zamków szyfrowych. Na fot. 4 przedstawiono elementy współpracujące z klasycznymi (fabrycznymi) centralami alarmowymi, wykorzystanymi do współpracy ze sterownikiem PLC, które tworzą alternatywne do fabrycznych rozwiązanie budowy systemu SSWiN i SSP. Dodatkowo pod poszczególne wyjścia sterownika można podłączać inne urządzenia elektryczne niespełniające wprawdzie w systemie zadań związanych z realizacją funkcji systemów SSWiN i SSP, ale mogące z nimi współpracować. Przykładem takiej współpracy może być wykorzystanie jako czujki obecności czujek PIR do załączania w pomieszczeniach oświetlenia elektrycznego (wyjście Q1) w systemie wyłączonym ze stanu dozoru.

Wyniki badań testowych

Możliwości tak stworzonego układu zostały sprawdzone na kilku hipotetycznych, ale możliwych do wystąpienia w rzeczywistości projektach. Jednym z przykładów wykorzystania modelu jest układ sterowania systemem alarmowym wykorzystującym osiem wejść, cztery wyjścia cyfrowe oraz dwie diody wbudowane w panel sterownika.

Założenia do projektu są następujące:

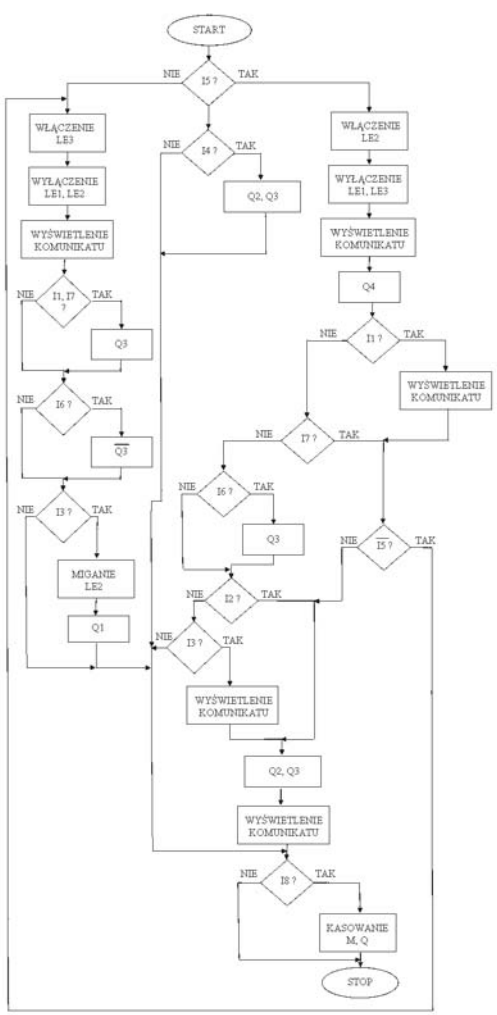
- Czujka PIR 1 (I1) zasilana jest na stałe ze źródła niezależnego od pracy sterownika PLC; wejście w obszar jej działania wtedy, gdy system nie jest włączony w dozór spowoduje zgaszenie/zapalenie oświetlenia na korytarzu, a w stanie dozorowania po czasie t = 8 s powoduje wywołanie optyczno-akustycznego sygnału alarmowego (Q2) oraz zapalenie oświetlenia na korytarzu (Q3).
- Czujka PIR 2 (I2) początkowo jest nieaktywna; jej zasilanie jest załączane po czasie t = 31 s od przejścia w stan dozorowania; jej aktywacja w tym stanie powoduje wywołanie optyczno-akustycznego sygnału alarmowego oraz zapalenie oświetlenia na korytarzu.
- Naruszenie linii sabotażowej czujek PIR 1 lub PIR 2 (I3) w stanie wyłączenia z dozoru powoduje wywołanie akustycznego sygnału alarmowego oraz miganie czerwonej diody na panelu sterownika (LE2), a w stanie dozorowania powoduje wywołanie optyczno-akustycznego sygnału alarmowego, zapalenie oświetlenia na korytarzu oraz wyświetlenie komunikatu „sabotaż!”.
- Załączanie w dozór/wyłączanie z dozoru odbywa się za pomocą przełącznika podłączonego do wejścia sterownika (I5).



Fot. 3. Widok płyty czołowej stanowiska dydaktycznego: 1 – panel symulacyjny i wejściowy, 2 – panel sterownika programowalnego MFD-Titan, 3 – panel oświetleniowy, 4 – sygnalizator optyczno-akustyczny, 5 – panel symulujący wejście do obiektu, 6 – włącznik/wyłącznik zasilający sterownik PLC oraz elementy i urządzenia z panelu przedniego z wykorzystaniem sterownika PLC

– Załączenie/wyłączenie oświetlenia na korytarzu odbywa się za pomocą przycisku podłączonego do wejścia sterownika (I6).
– Otwarcie drzwi powoduje rozwarcie styków kontaktronu, zamknięcie – zwarcie styków.
– Kasowanie zawartości komórek pamięci: markerów M, wyjść sterownika Q (przejście w stan niski – 0V).

Fot. 4. Elementy systemu alarmowego: 1 – pasywna czujka podczerwieni typu Satel Aqua, 2 – czujka kontaktronowa, 3 – optyczna czujka dymu typu ADR-20N, 4 – zamek typu Roger SL1000



Rys. 3. Algorytm pracy systemu alarmowego

Podanie napięcia na poszczególne wejścia sterownika (stan wysoki – 24 V) odpowiada za:
– **I1** – zadziałanie pasywnej czujki podczerwieni PIR 1,
– **I2** – zadziałanie pasywnej czujki podczerwieni PIR 2,
– **I3** – wysłanie sygnału sabotażowego z czujek PIR 1 lub PIR 2,
– **I4** – wywołanie alarmu napadowego,
– **I5** – uzbrojenie/rozbrojenie alarmu za pomocą manipulatora,
– **I6** – zapalenie/zgaszenie diod LED,
– **I9** – zadziałanie kontaktronu zamontowanego w drzwiach,
– **I10** – centralny reset sterownika PLC (kasowanie zawartości: M, Q).

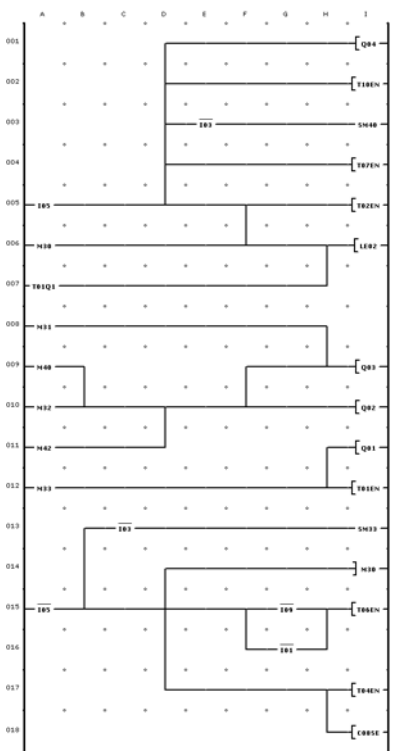
Wyjścia sterownika odpowiadają za załączenie:
– **Q1** – sygnału akustycznego,
– **Q2** – sygnału optyczno-akustycznego,
– **Q3** – zapalenia diod LED (oświetlenie korytarza),
– **Q4** – źródła zasilania czujki PIR 2,
– **LE1** – zapalenie/zgaszenie oświetlenia wyświetlacza sterownika,
– **LE2**, **LE3** – zapalenie/zgaszenie diod na panelu sterownika (odpowiednio: czerwona, zielona).

Na rys. 3 został zaprezentowany algorytm pracy systemu alarmowego działającego i realizującego założenia projektowe opisywanej konfiguracji. Natomiast na rys. 4 przedstawiony został fragment schematu drabinkowego algorytmu sterującego pracą systemu.

Podsumowanie

Po dokonaniu serii badań testowych na stworzonych algorytmach sterujących oraz później na systemach zbudowanych z rzeczywistych elementów należy stwierdzić, że tak zbudowane systemy spełniają swoją rolę i mogą być przeznaczone do ochrony obiektów o małym lub średnim ryzyku szkód (systemy klasy SA1 i SA2), a także do ochrony mienia o małej wartości (kategoria Z1).

Współpraca elementów klasycznego systemu alarmowego ze sterownikiem programowalnym jest na ogół bezproblemowa. Zwrócić należy jedynie uwagę na staranny dobór wartości napięć znamionowych elementów wejściowych i wyjściowych, dzięki czemu czujki i sygnalizatory zastosowane w systemie alarmowym (zbudowanym na przykład z wykorzystaniem centrali alarmowej CA6 firmy Satel) spełniają te same funkcje co w przypadku zastosowania sterownika programowalnego MFD-Titan firmy Moeller. W przypadku różnych wartości napięć znamionowych istnieje konieczność wyposażenia systemu w układy dopasowujące (np. układy przekaźnikowe lub dzielniki napięć).



Rys. 4. Fragment schematu drabinkowego algorytmu sterującego pracą systemu

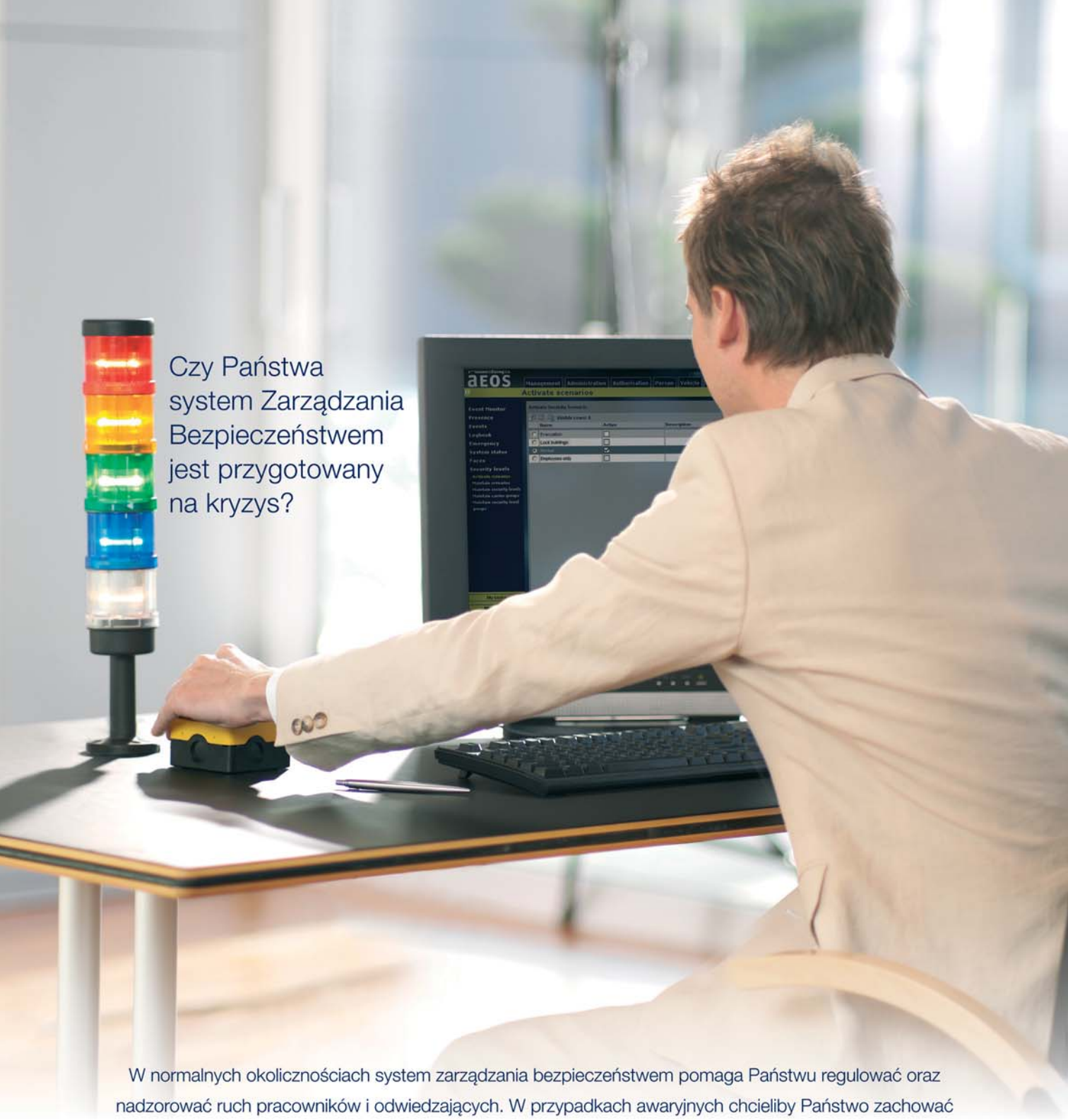
W odróżnieniu od rozwiązań fabrycznych system zbudowany na bazie sterownika PLC ma możliwość dowolnego kształtowania algorytmu sterującego. Szczególnie ważne jest to w przypadku wykorzystania takich układów w mieszkaniach lub budynkach mieszkalnych. Daje to użytkownikowi możliwość doboru indywidualnych parametrów i indywidualnej konfiguracji sprzętowej. Wadą tego rozwiązania jest natomiast konieczność poznania przez użytkownika co najmniej jednego języka programowania sterowników PLC.

Dzięki modułowej budowie tych układów istnieje możliwość szybkiej rozbudowy systemu, co jest ważną zaletą. A poprzez zastosowanie dodatkowych elementów (np. układów I/O) system może mieć charakter systemu rozproszonego.

dr inż. Marcin Buczaj
mgr inż. Piotr Kowalik
Politechnika Lubelska
Katedra Inżynierii Komputerowej i Elektrycznej

Literatura:

1. PN-EN 50131-1:2002 *Systemy alarmowe – Systemy sygnalizacji włamania – Część 1: Wymagania ogólne.*
2. Norma PN-EN 61131 – *Sterowniki Programowalne.*
3. Brock S., Muszyński R., Urbański K., Zawirski K.: *Sterowniki programowalne.* Wydawnictwo Politechniki Poznańskiej, Poznań 2000.
4. Kasprzyk J.: *Programowanie sterowników przemysłowych.* Wydawnictwo Naukowo-Techniczne, Warszawa 2006.
5. Petykiewicz P.: *Nowoczesna instalacja elektryczna w inteligentnym budynku.* COSiW SEP, Warszawa 2001.
6. *www.automatyka.siemens.pl*
7. *www.moeller.pl*



Czy Państwa system Zarządzania Bezpieczeństwem jest przygotowany na kryzys?

W normalnych okolicznościach system zarządzania bezpieczeństwem pomaga Państwu regulować oraz nadzorować ruch pracowników i odwiedzających. W przypadkach awaryjnych chcieliby Państwo zachować ten sam poziom kontroli. Dzięki AEOS Security Levels firmy Nedap mają Państwo pełną kontrolę nad dostępem do pomieszczeń, nawet w sytuacji kryzysowej. Upoważnienia mogą być zmieniane lub odwoływane za jednym naciśnięciem przycisku dzięki poziomom bezpieczeństwa, które można predefiniować w AEOS. AEOS Security Levels pozwala na szybką reakcję w okolicznościach, które mogłyby poważnie naruszyć Państwa bezpieczeństwo.

Nie ryzykuj. Nedap AEOS. AEOS.

nedap

aeos

W celu uzyskania bliższych informacji, proszę skontaktować się z działem Nedap Security Management (Zarządzanie Bezpieczeństwem) +48 607 852 699, info@nedap-aeos.com lub odwiedzić naszą stronę internetową www.nedap-securitymanagement.com

Zupełnie inny monitoring!

Nawet tam gdzie nie ma możliwości korzystania
z patrolu ochrony,
powiadomienie niezwłocznie dotrze do klienta:

- lokatora mieszkania w bloku
- mieszkańca domu w zamkniętym osiedlu
- właściciela działki
- właściciela garażu
- właściciela magazynu
- zarządcy nieruchomości

Bezpieczny Dom da informacje o:

- włamaniu
- alarmach technicznych
- zalaniu wodą
- ulatnianiu gazu
- spadku zasilania
- zagrożeniu pożarowym
- itp.

Bezpieczny Dom to:

- powiadomienie przez sms lub operatora
- usługa na terenie całego kraju
- nadzór ACO 24h/7dni
- zniżki w ubezpieczeniach
- niski abonament

Centrum Monitorowania Alarmów Sp. z o.o.
ul. Puławska 359, 02-801Warszawa,
tel.: (022) 546 0 888, fax: (022) 546 0 619
www.cma.com.pl

Pracownik

Potencjalne źródło wypływu informacji z firmy

W czasach kryzysu coraz łatwiej o utratę pracy, a trudniej o znalezienie nowej. By ją zdobyć, może już nie wystarczyć samo posiadanie umiejętności specjalistycznych i organizacyjnych. Aby podnieść swoją wartość na trudnym rynku pracy, niektóre osoby ubiegające się o pracę w nowym miejscu posuwają się do kradzieży wartości intelektualnej dotychczasowemu pracodawcy. Jak się przed tym chronić?

Globalny kryzys ekonomiczny. Któż z nas o nim nie słyszał. W jednych krajach bardziej dotkliwy dla społeczeństwa, w innych mniej. Środki masowego przekazu codziennie przekazują nam kolejną dawkę informacji na jego temat. A to za granicą zarządzający funduszem inwestycyjnym – w którym tysiące ludzi ulokowało oszczędności całego życia – przez lata oszukiwali swoich klientów, a to dobrze prosperujący polski koncern stracił wiele milionów złotych na opcjach walutowych. Jedne zakłady wprowadzają przymusowe przestoje, inne ogłaszają upadłość, jeszcze inne redukują zatrudnienie, aby jak najbardziej ograniczyć koszty prowadzenia działalności gospodarczej i aby dzięki temu przetrzymać trudny okres. Jedni mówią, że bardziej rozwinięte kraje zostały dotknięte przez kryzys silniej niż Polska, inni głoszą, że najgorsze jeszcze przed nami. Wszyscy jednak są zgodni co do tego, że kryzys ma już swoje odzwierciedlenie w statystykach dotyczących rosnącego bezrobocia. Jeszcze kilkanaście miesięcy temu zmiana miejsca pracy była w zasięgu ręki prawie każdego chętnego. Wystarczyło mieć trochę odwagi, przejrzeć ogłoszenia w prasie, internecie, złożyć dokumenty w terminie i udać się na kilka rozmów kwalifikacyjnych. Ci, którzy mieli więcej odwagi, szukali szczęścia poza granicami kraju, ale dziś mało kto decyduje się na taki ruch. Wiele osób wraca, gdyż w Irlandii czy Wielkiej Brytanii coraz trudniej o dobrą pracę. W Polsce również o pracę coraz trudniej. Sama chęć do pracy i zdolności interpersonalne już nie wystarczają. Aby zdobyć pracę, trzeba na tle innych wyróżniać się czymś wyjątkowym. Dla nielojalnych pracowników dodatkowym atutem w staraniach o dobrą posadę mogą być na przykład dane firmy, takie jak lista adresów potencjalnych klientów, plany, gotowe projekty czy też rozwiązania, które inni wypracowują przez całe lata. A w obecnym miejscu pracy te materiały są na wyciągnięcie ręki. Byle tylko udało się je niepostrzeżenie wynieść...

W wielu firmach pojęcie ochrony informacji albo w ogóle nie funkcjonuje, albo ogranicza się do stosowania zabezpieczenia pod postacią umów o zachowaniu poufności informacji ze współpracującymi podmiotami. Zazwyczaj klauzule dotyczące zakazu ujawniania informacji pozyskanych w trakcie współpracy obowiązują nawet wiele lat po zakończeniu współpracy. Każdy z pracowników podmiotu zewnętrznego – mający dostęp do informacji wrażliwych – zobowiązany jest do podpisania odpowiedniego oświadczenia. Za ujawnienie informacji będących przedmiotem kontraktu grożą surowe kary finansowe. Niewiele to jednak pomoże firmie, jeśli na skutek ujawnienia przez pracownika informacji poufnych firma straci reputację, a także zaufanie kontrahentów, co może w konsekwencji doprowadzić do jej upadku.

A w jaki sposób firmy zabezpieczają się przed niekontrolowanym wypływem informacji spowodowanym przez własnych pracowników? Standardem są takie umowy o pracę, w których niewiele jest napisane na temat zachowania poufności informacji. Pracownik jest zobowiązany do nieujawniania informacji stanowiących tajemnicę służbową w okresie, w którym jest związany z pracodawcą umową o pracę. W przypadku ujawnienia takich informacji przez byłego już pracownika po zakończeniu okresu zatrudnienia jego były pracodawca może wystąpić przeciw niemu na drogę sądową z powództwa cywilnego, ale jest to skomplikowany i długotrwały proces. Poszkodowany – w tym wypadku były pracodawca – musi udowodnić, że jego były pracownik dopuścił się kradzieży wartości intelektualnej. Będzie mógł tego dokonać jedynie wtedy, jeśli wcześniej przedsięwziął odpowiednie kroki, w przeciwnym razie taki proces może okazać się stratą czasu i pieniędzy.

Należy wcześniej podjąć działania zaradcze, aby być „mądrzejszym przed szkodą" i skutecznie zadbać o bezpieczeństwo informacji wewnątrz organizacji. Tak jak w przypadku wirusów komputerowych, tak i tutaj nie ma niestety recepty na stuprocentowe zabezpieczenie się przed nieuprawnionym wyniesieniem informacji przez pracowników. Konieczne jest jednak wdrożenie pewnych zabezpieczeń prowadzących do zminimalizowania niebezpieczeństwa wystąpienia tego typu zagrożeń, ponieważ najczęściej wynikają one z celowego działania pracownika, a nie z jego niewiedzy bądź przypadku.

Odpowiednia dbałość o bezpieczeństwo informacji powinna być zachowana w całym okresie życia informacji: od jej powstania aż do jej trwałego zniszczenia.

Warto więc pamiętać o kilku zasadach zabezpieczania informacji, w szczególności tej przetwarzanej elektronicznie.

1. **Uporządkowanie gospodarki sprzętowej.** Podstawowe czynności w tym zakresie to inwentaryzacja stacji roboczych i laptopów oraz jednoznaczne przypisanie ich do poszczególnych użytkowników. Aby chronić informację przechowywaną w postaci elektronicznej, najpierw musimy wiedzieć, gdzie jest ona zgromadzona i kto ma do niej dostęp. Laptop „widmo", czyli urządzenie nie przypisane do żadnego użytkownika, może stać się furtką do niekontrolowanego wypływu informacji. Za takie urządzenie żaden z pracowników nie czuje się odpowiedzialny, a co za tym idzie, nikt nie jest zobowiązany do odpowiedniej ochrony ani tego laptopa, ani zgromadzonych na nim danych.
2. **Ograniczenie możliwości niekontrolowanego wyjmowania dysków twardych z komputerów służbowych.** Prostym, a zarazem bardzo skutecznym sposobem na ograniczenie niekontrolowanego wypływu informacji jest umieszczenie plomb na obudowach urządzeń w taki sposób, aby wyjęcie dysków twardych było niemożliwe lub aby przeprowadzenie takiego działania nie pozostało bez śladu, tj. zniszczenia plomby.
3. **Zablokowanie możliwości kopiowania danych na nośniki zewnętrzne.** Nie chodzi tu wyłącznie o nagrywarki dysków CD/DVD, ale przede wszystkim o zablokowanie możliwości kopiowania danych na pamięci masowe podłączane do portów USB (z racji ich ogromnej dostępności). Samo zablokowanie portów jednak nie wystarczy. Przeprowadzenie takich działań wiąże się z koniecznością wdrożenia odpowiedniej polityki bezpieczeństwa, polegającej na oddzieleniu funkcji administratora i użytkownika stacji, tak aby ten ostatni nie miał uprawnień do samodzielnej zmiany konfiguracji systemowej swojego komputera. Zablokowanie portów USB może okazać się stosunkowo trudne do wykonania i to nie ze względu na problemy techniczne, ale z powodu ich wszechstronnego zastosowania, ponieważ ten interfejs komunikacyjny jest coraz częściej wykorzystywany przez drukarki, klawiatury, myszy i inne urządzenia peryferyjne.
4. **Uzupełnienie rozwiązań organizacyjno-sprzętowych specjalistycznymi narzędziami systemowymi.** Dzięki ich funkcjom (w zależności od zastosowanych rozwiązań) możliwe jest:
   – zarządzanie uprawnieniami dostępu do poszczególnych dokumentów (możliwość odczytu, modyfikacji, kopiowania, drukowania),
   – kontrolowanie przepływu dokumentacji elektronicznej wewnątrz firmy (ang. *workflow*),
   – gromadzenie informacji o działaniach użytkownika, w szczególności w zakresie kopiowania na nośniki zewnętrzne chronionych danych, przesyłania ich poza firmę po sieci Ethernet, Wi-Fi czy też za pośrednictwem Bluetooth,
   – blokowanie na komputerach służbowych możliwości korzystania z serwerów poczty prywatnej, w tym portali społecznościowych umożliwiających przesyłanie plików pomiędzy użytkownikami,
   – blokowanie komunikatorów internetowych,
   – blokowanie programów wykorzystujących połączenia P2P (*peer-to-peer*) umożliwiające przesyłanie danych pomiędzy użytkownikami.

Dla wielu użytkowników działania tego typu mogą wydawać się przesadne i zbyt drastyczne. Ze statystyk jednak wynika, że najczęściej do wypływu z wnętrza firmy informacji chronionych dochodzi właśnie z powodu niestosowania przedstawionych tu propozycji zabezpieczeń.

5. **Skuteczne niszczenie danych zgromadzonych w urządzeniach wycofywanych z użytku.** Wiele firm decyduje się na odsprzedaż lub bezkosztowe przekazanie wycofywanego sprzętu komputerowego własnym pracownikom. Warto jednak wcześniej zniszczyć w sposób nieodwracalny umieszczone na dyskach twardych dane, by wyeliminować możliwość późniejszego ich odtworzenia. Do tego celu można wykorzystać nawet darmowe oprogramowanie dostępne w sieci Internet.
6. **Prowadzenie skutecznego rozliczania z dokumentów i urządzeń pracownika, z którym rozwiązywana jest umowa o pracę.** W praktyce jest to jednak trudne do osiągnięcia, gdyż pracodawca zobowiązany jest do terminowego przekazania świadectwa pracy pracownikowi, z którym wygasa umowa o pracę, nawet w przypadku, gdy ten nie dopełnił wszystkich formalności związanych m.in. z wypełnieniem karty obiegowej.

Jedną z najważniejszych, najskuteczniejszych i zarazem najprzyjemniejszych metod, chroniących przed celowym wyniesieniem informacji przez pracownika, jest dbałość o dobrą atmosferę w miejscu pracy. Osoby żegnające się z firmą z powodu redukcji zatrudnienia czy też na własne życzenie i mające w pamięci tylko dobre wspomnienia z nią związane, będą nadal czuły się wobec niej lojalne i nie zdecydują się na „zrobienie jej krzywdy" poprzez kradzież informacji chronionych. Wszystko zatem w Waszych rękach, Pracodawcy!

Krzysztof Białek

Światłowody a przepięcia

Większość instalatorów systemów monitoringu wizyjnego zetknęła się z przypadkami zniszczenia urządzeń telewizyjnych na skutek przepięć wywoływanych przez czynniki naturalne, takie jak burzowe wyładowania atmosferyczne, czy przez czynniki sztuczne, takie jak przepięcia komutacyjne w sieciach energetycznych. Wymienione powyżej kategorie zjawisk nie różnią się jakościowo. W obu przypadkach podobne są zarówno kształty przebiegów elektrycznych, jak i ich charakterystyki widmowe

W pewnych sytuacjach zależności amplitudowe mogą wykazywać także znaczne podobieństwa. Fala udarowa indukująca się w przewodach elektrycznych na skutek odległego wyładowania burzowego może nieść podobną energię, co przepięcie powstałe na skutek iskry, przeskakującej w odłącznikach energetycznych w momencie odłączania obciążeń reaktancyjnych o znacznej mocy.

Dlaczego instalacje telewizyjne są tak podatne na uszkodzenia spowodowane przepięciami? Na czym polega niszcząca siła fali udarowej?

Chcąc odpowiedzieć na te pytania, należy zastanowić się nad dwoma zagadnieniami:

– Jaki jest kształt impulsów stanowiących falę udarową?

– Jaki jest rozkład energii w widmie takiej fali?

Odpowiedź na pierwsze z tych pytań jest zawarta w normach, dotyczących zabezpieczeń przeciwprzepięciowych. W wyniku wielu badań oraz pomiarów (przeprowadzonych zarówno w warunkach naturalnych, jak i w wytworzonych sztucznie warunkach laboratoryjnych) przyjęto, że powstająca w wyniku wyładowań iskrowych fala udarowa w zasadniczej swej części ma charakter impulsu stałoprądowego o czasie narastania T1 równym 8 μs, który jest liczony od 10% do 90% wartości maksymalnej, oraz o czasie trwania T2 równym 20 μs liczonym od momentu, gdy narastająca fala osiąga 10% wartości szczytowej do momentu, gdy spada ona do 50% wartości maksymalnej.

Trudno dyskutować nad tym, dlaczego przyjęto akurat taką definicję standardowej fali udarowej, dość powiedzieć, że jest ona powszechnie stosowana. Dla ułatwienia standardową falę udarową w wielu publikacjach określa się jako 8 μs/20 μs lub nawet tylko 8/20.

Tyle na temat zależności czasowych. W celu pełnego opisu typowej fali udarowej 8 μs / 20 μs, powstającej w wyniku bezpośredniego uderzenia pioruna, należy jeszcze określić jej parametry amplitudowe. Z badań statystycznych wynika, że połowa wszystkich występujących w przyrodzie wyładowań atmosferycznych osiąga amplitudę przekraczającą 18 kA, dziesięć procent tych wyładowań jest związana z przepływem prądu rzędu 100 kA, maksymalne odnotowane wartości dochodzą do 400 kA, przy czym ze statystycznego punktu widzenia stanowią one margines. W wyniku powyższych analiz jako znormalizowaną falę udarową, generowaną przez statystyczny piorun, przyjęto falę 8 μs / 20 μs o amplitudzie 18 kA.

W tym miejscu należy podkreślić losowy charakter wszelkich, nawet najdoskonalszych, zabezpieczeń przeciwprzepięciowych dostosowanych do „znormalizowanych" fal udarowych o relatywnie niskiej amplitudzie równej 18 kA. Nikt nie jest w stanie zagwarantować bezpieczeństwa instalacji elektrycznej potraktowanej falą udarową o amplitudzie wielu setek tysięcy amperów. Prawdopodobieństwo zaistnienia tego typu zjawiska jest niskie, lecz nie zerowe, niestety przed klasycznym pechem nie ma ucieczki.

W przypadku częstych w naszych szerokościach geograficznych udarów piorunowych fala 8 μs/20 μs powstaje w wyniku przeskoku pierwszej iskry i niesie większą część energii wyładowania. W wyniku wyładowań wtórnych w późniejszym okresie generowane są fale o mniejszej energii, ale o krótszych czasach narastania i opadania, które z niewielkim błędem można określić jako 1 μs/5 μs.

Wyładowania wtórne pomimo swojej mniejszej siły są równie niebezpieczne, gdyż mają inny rozkład widmowy niż wyładowania główne. Szczególnie istotny jest czas narastania przedniego zbocza fali udarowej, który w sprzyjających warunkach może osiągać wartości rzędu 250 ns.

Jak widać, tego typu fale udarowe mimo stałej polaryzacji mają charakter impulsu o krótkim czasie narastania. Neutralizacja skutków przepływu prądu opisanego takimi zależnościami czasowymi nie jest łatwa, gdyż wszelkie próby jego zwarcia bądź odprowadzenia w bezpiecznym kierunku wymagają zastosowania elementów o bardzo szybkim działaniu i o bardzo niskiej indukcyjności. Można nawet powiedzieć, że w pewnej klasie instalacji skutki wyładowań wtórnych, opisywanych jako fale 1 μs/5 μs i niosących relatywnie niższą energię, są groźniejsze od oddziaływania silniejszych, ale wolniejszych fal 8 μs/20 μs.

Innym problemem jest niezakłócanie przebiegów, które są transmitowane w danym torze, co stoi w jawnej sprzeczności z odfiltrowywaniem znacznie od nich silniejszych, ale podobnych w charakterze, bo także zmiennoprądowych fal udarowych. Jak widać, nie jest to proste zagadnienie i nie znajduje ono ostatecznego rozwiązania. Jedyne, co możemy zaproponować, to ograniczenie prawdopodobieństwa przeniknięcia do urządzeń elektronicznych fal udarowych o dużej energii, jednak całkowite wykluczenie tego zjawiska w technologii transmisji przewodowej jest niemożliwe.

Przyjmuje się, że większa część energii fali 8 μs/20 μs jest zawarta w paśmie do 1 MHz, zaś przysłowiowy „ogon" ciągnie się asymptotycznie aż do dalekich mikrofal. Jest to kolejny powód, dla którego fale indukowane w instalacjach słaboprądowych są takie groźne nawet w przypadku bardzo odległych wyładowań atmosferycznych.

Podczas burzy należy liczyć się z możliwością przepływu znacznych prądów o charakterystyce czasowej odpowiadającej fali 8 μs / 20 μs nawet w bardzo starannie wykonanej i dobrze zabezpieczonej instalacji przewodowej. Przyczyną tego stanu rzeczy są zjawiska rezonansowe, które występują w kablach o dużych długościach. Przyjmując, że gęstość widmowa fal elektromagnetycznych emitowanych przez wyładowania piorunowe zachowuje wysokie wartości w zakresie do 1 MHz, odpowiada to falom radiowym o długościach rzędu 300 m oraz większych. Jak wiadomo, jedną z doskonalszych anten odbiorczych skutecznie absorbujących energię fal radiowych z otaczającego nas umownego „eteru" jest dipol półfalowy. W naszym przypadku będzie to przewód o długości około 150 m. Równie dobrą anteną odbiorczą, tym razem wymagającą współpracy z uziemieniem, jest dipol ćwierćfalowy, czyli w naszym przypadku odcinek kabla o długości około 75 m. Kable o innych długościach także będą stanowiły anteny odbiorcze, tyle że mniej skuteczne, ale nie oznacza to, że generowane w nich fale udarowe nie okażą się niszczące dla urządzeń elektronicznych.

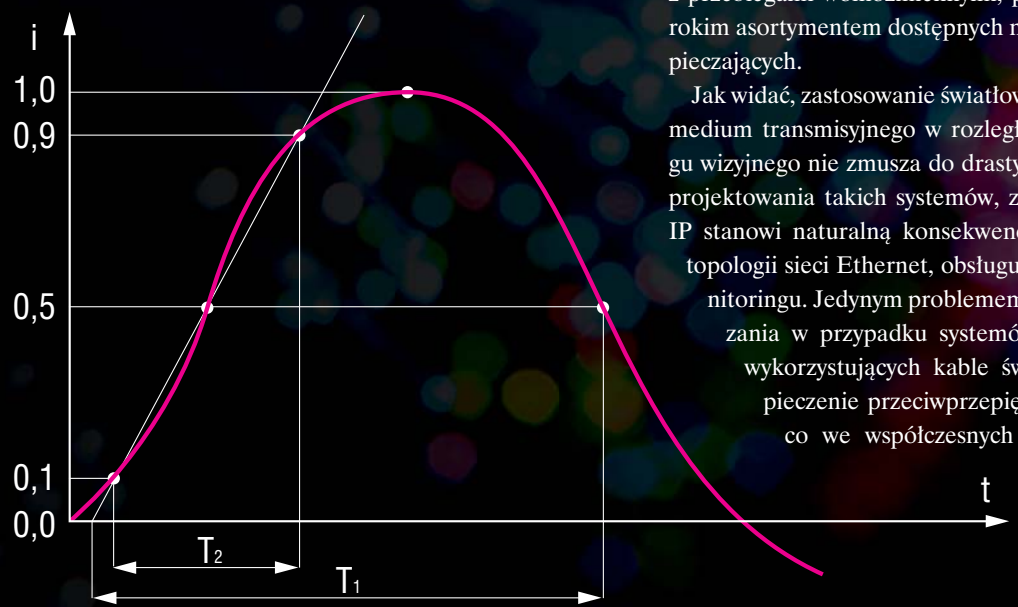
Z jakimi długościami kabli mamy do czynienia w realnym systemie monitoringu wizyjnego? Niestety właśnie z takimi, o jakich wspomniano powyżej. Jeśli do tego przewody składające się na instalację CCTV przebiegają w pewnej odległości od ziemi, co ma miejsce w przypadku monitoringu wszystkich wysokich budynków, wówczas tworzą się układy anten, które

wykazują mniej lub bardziej przypadkowe właściwości rezonansowe, a przez to bardzo skutecznie absorbują energię fal emitowanych w szerokim widmie przez wyładowania atmosferyczne.

Sposobem na eliminację zagrożeń, wynikających z indukowania silnych fal udarowych jest cięcie przewodów stanowiących instalację kamerową na krótsze odcinki i przepuszczanie sygnałów telewizyjnych przez tak zwane izolatory mas. Poprawnie zaprojektowana analogowa instalacja kamerowa wykorzystująca kable miedziane powinna zawierać zarówno izolatory mas, jak i elementy neutralizujące skutki przepięć na obu końcach torów kablowych. Wiąże się to jednak ze sporymi kosztami i z tego powodu bardzo często elementy te są pomijane, jeśli nie przez projektantów, to przynajmniej przez instalatorów.

Nie od rzeczy będzie dodać, że sytuacja ta dotyczy zarówno klasycznych analogowych systemów monitoringu wizyjnego, jak i nowoczesnych systemów IP, wykorzystujących w warstwie fizycznej sieć Ethernet 100Base-TX czy jakąkolwiek jej „miedzianą" odmianę. Sytuację poprawiają nieco urządzenia sieciowe, czyli koncentratory, przełączniki, rutery i inne urządzenia aktywne, które w większości przypadków posiadają co najmniej elementarne zabezpieczenia przeciwprzepięciowe. Ethernet z definicji jest siecią wykorzystującą odcinki kablowe krótsze niż 100 m, co w znacznym stopniu ogranicza niszczące skutki opisanych powyżej efektów antenowych, jednak wszelkie instalacje, w których podstawę stanowią przewody miedziane, są narażone na negatywne skutki przepięć elektrycznych.

Zadajmy sobie kolejne pytanie: czy rezygnacja ze stosowania kabli miedzianych na rzecz połączeń światłowodowych poprawia tę sytuację? Oczywiście tak, ale nie do końca. Światłowody w sensie elektrycznym są izolatorami i pozostają obojętne na skutki emisji fal radiowych, nawet o bardzo dużych energiach. Zakres widmowy, w jakim pracują światłowody, różni się o wiele rzędów wielkości od widma fal udarowych, generowanych przez wyładowania atmosferyczne, co także powoduje brak zakłóceń transmitowanych sygnałów.



Rys. 1. Definicja fali udarowej

W dobie analogowych systemów monitoringu wizyjnego niska popularność kabli światłowodowych związana była głównie z czynnikami ekonomicznymi. Chcąc stosować tego typu połączenia na krótkich odcinkach oraz dla znacznej liczby kamer, należało liczyć się z podwojeniem kosztów całej instalacji.

Inaczej przedstawia się sytuacja w sieciowych systemach monitoringu, wykorzystujących urządzenia IP. Jedną z wielu możliwych do zastosowania, aczkolwiek mało popularnych odmian sieci Ethernet, jest wersja 100Base-FX. Bazuje ona na światłowodowych kablach wielomodowych i używana jest głównie ze względu na wyższy maksymalny zasięg transmisji. Inną odmianą sieci Ethernet, tym razem bardzo popularną, jest Ethernet 1000Base-SX. Wykorzystuje się go do budowy sieci szkieletowych lub tak zwanych „ringów" światłowodowych. Jest to rozwiązanie typowe dla rozległych instalacji IP, układanych w dużych budynkach lub w obiektach otwartych, takich jak stadiony sportowe. Pomijając uwarunkowania wynikające z topologii sieci, zastosowanie światłowodów przyczynia się do znakomitej poprawy odporności całej instalacji na skutki przepięć, głównie tych najsilniejszych, generowanych przez wyładowania atmosferyczne.

Zastosowanie światłowodów nie zwalnia projektantów i instalatorów systemów monitoringu wizyjnego od obowiązku stosowania zabezpieczeń przeciwprzepięciowych w obwodach zasilających, w tym w sieci energetycznej. Zagadnienia te są precyzyjnie określane przez współczesne przepisy budowlane, dlatego można zakładać, że w większości obiektów odpowiednie zabezpieczenia istnieją i działają prawidłowo.

Osobnym zagadnieniem jest zabezpieczenie przeciwprzepięciowe oddalonych punktów kamerowych, np. zainstalowanych na wysokich masztach z dala od budynków. Zastosowanie transmisji obrazów za pomocą światłowodu pozwala zapomnieć o problemach związanych z warstwą słaboprądową, jednakże nie stanowi gwarancji powodzenia. Konieczne jest staranne zabezpieczenie obwodów zasilających. Zagadnienie to jest o tyle łatwiejsze do realizacji, że w obwodach zasilających mamy do czynienia albo z prądem stałym, albo z przebiegami wolnozmiennymi, ponadto dysponujemy szerokim asortymentem dostępnych na rynku elementów zabezpieczających.

Jak widać, zastosowanie światłowodów jako podstawowego medium transmisyjnego w rozległych systemach monitoringu wizyjnego nie zmusza do drastycznych zmian w koncepcji projektowania takich systemów, zaś w przypadku systemów IP stanowi naturalną konsekwencję wyboru pierścieniowej topologii sieci Ethernet, obsługującej rozległe obszary monitoringu. Jedynym problemem, jaki pozostaje do rozwiązania w przypadku systemów monitoringu wizyjnego wykorzystujących kable światłowodowe, jest zabezpieczenie przeciwprzepięciowe obwodów zasilania, co we współczesnych warunkach nie powinno stanowić problemu.

Andrzej Walczyk
ALTRAM

ALTRAM

Zwiększ swoje możliwości. Wyprzedź innych, pracuj z najlepszym oprogramowaniem na rynku.

Sony wprowadza na rynek telewizji przemysłowej rozwiązanie hybrydowe pozwalające na łatwą integrację nowych sieciowych i starych analogowych rozwiązań po to, aby powstała instalacja, która dziś i jutro będzie zapewniała bezpieczeństwo.

Najnowsza wersja oprogramowania Sony Real Shot Manager – RSM Advanced, przeniesie twoją telewizję przemysłową na wyższy poziom, gdzie będziesz mógł wykorzystywać analizę obrazu w czasie rzeczywistym połączoną z automatyczną detekcją zagrożeń w celu zapewnienia najwyższej ochrony. Dzięki innowacyjnej, Inteligentej Detekcji Przedmiotów oraz Inteligentej Detekcji Ruchu automatycznie włączają się alarmy, uruchamia się oświetlenie, a drzwi otwierają się lub zamykają. Zminimalizowana liczba fałszywych alarmów w połączeniu z aktywną inteligencją, wyszukującą podejrzane obiekty lub osoby, dają doskonały efekt w przypadku realnych zagrożeń – wykrywając je i pozwalając na ich szybkie usunięcie. Podobnie jak w podstawowej wersji doskonale znanego oprogramowania Real Shot Manager, interfejs użytkownika jest niezwykle prosty i intuicyjny, ułatwiający korzystanie ze wszystkich funkcji podglądu, nagrywania, odtwarzania oraz konfiguracji. Oto powody, dla których Real Shot Manager to najlepszy wybór. Aby dowiedzieć się więcej wejdź na: **www.sonybiz.pl**

Unikalna hybrydowa technologia zaprojektowana z myślą o bezpieczeństwie

SONY

MIGRACJA → ROZWÓJ → ZAPIS → PODGLĄD → OBRAZ

KAMERY ANALOGOWE
GO HYBRID
KAMERY IP

ALTRAM tel. +48 22 847 5505 altram@altram.com.pl www.altram.com.pl

Monitoring trzeciej generacji

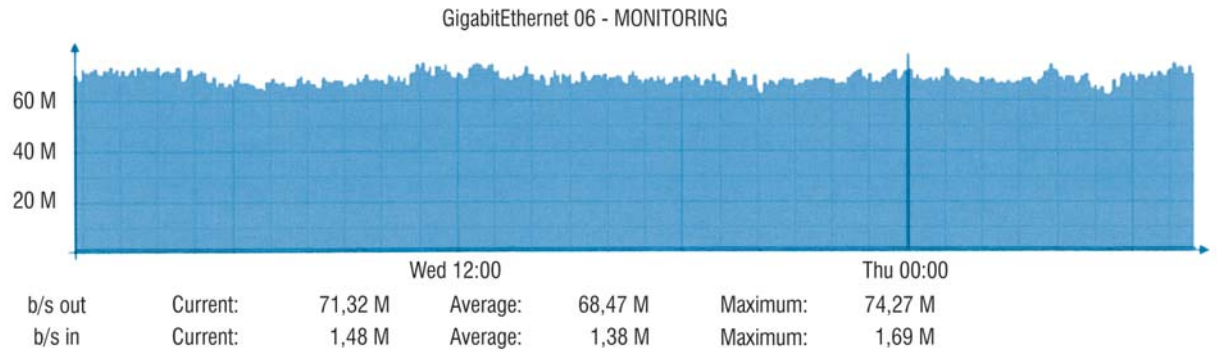
O tym, że analogowe systemy monitoringu wizyjnego powoli ustępują miejsca systemom monitoringu w technologii IP, wie już większość osób związanych z branżą CCTV. Ceny sprzętu do monitoringu wizyjnego spadają, a on sam jest coraz lepszy, o czym świadczy wzrost liczby kamer w monitoringu oraz poprawa jakości nadawanych obrazów. Właśnie jakość, stopień kompresji czy sam rodzaj zastosowanego kodowania nadawanych obrazów to jedne z najważniejszych parametrów w monitoringu IP, gdyż od nich w znacznym stopniu zależy przepustowość kanału dla danej kamery oraz ilość gigabajtów wymagana przez urządzenie NVR do archiwizacji wygenerowanych obrazów.

Obecnie kamery stosowane w monitoringu IP pozwalają na wybór rodzaju kodowania (najczęściej MJPEG, MPEG4 czy H.264), jakości obrazu, stopnia kompresji czy maksymalnego pasma, którego kamera nie może przekroczyć. Wszystkie te zabiegi prowadzą jednak do pogorszenia jakości przesyłanych przez kamerę obrazów. Co dzieje się w przypadku, gdy dany system monitoringu wymaga przesyłania obrazów jak najlepszej jakości i w jak największej możliwej rozdzielczości (gdy stosuje się na przykład kamery megapikselowe)? Wtedy zaczynają się problemy dotyczące głównie wymaganej przepustowości. Dla prostej instalacji złożonej z sześciu kamer megapikselowych oraz PTZ zapotrzebowanie na przepustowość może przekraczać 60 Mb/s (rys. 1).

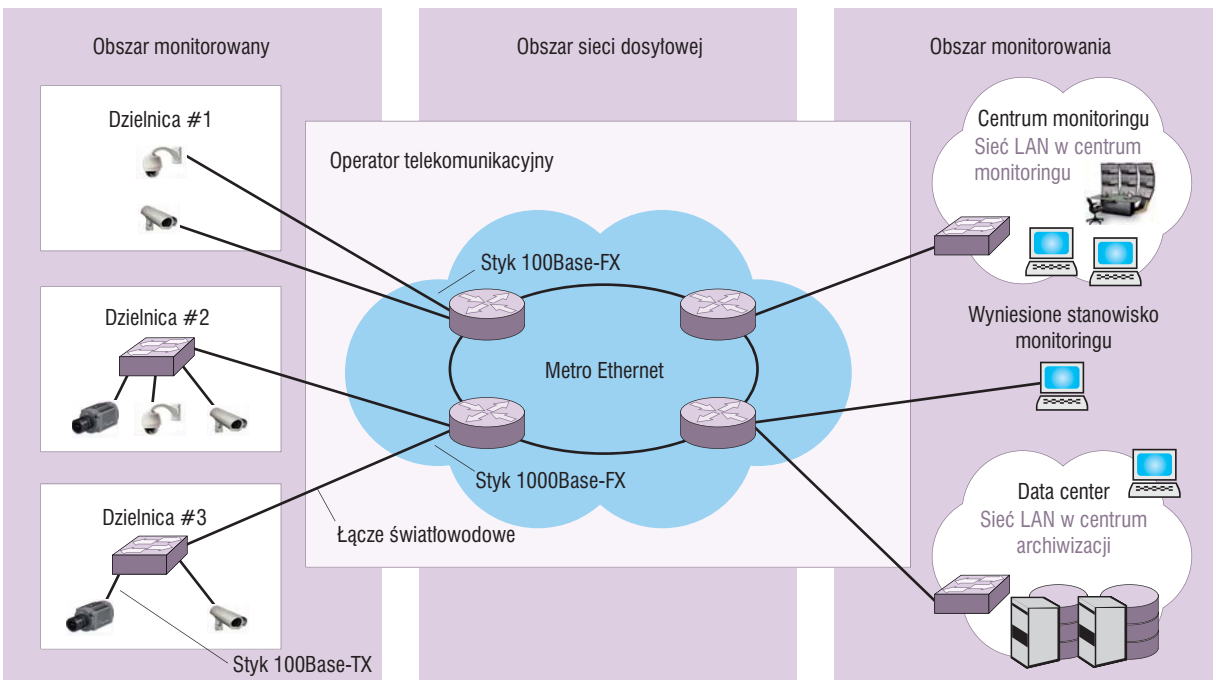
Dla instalacji składającej się przykładowo ze stu kamer i dwóch centrów monitoringu oddalonych od siebie o wiele kilometrów zapotrzebowanie na przepustowość łącza będzie znacznie większe. W takim przypadku najlepszym medium transmisyjnym, które jest w stanie przenieść setki megabitów ruchu na duże odległości, jest **światłowód jednomodowy**.

Jak to działa?

Wykonany w technologii IP system monitoringu wizyjnego daje użytkownikom możliwość zdalnego wykonywania takich czynności, jak: podgląd z kamer, sterowanie, archiwizowanie oraz przeglądanie nagrań przy wykorzystaniu lokalnych sieci komputerowych LAN lub Internetu. W takim systemie stosuje się kamery IP, kamery analogowe wraz z wideoserwerami, urządzenia sieciowe, np. routery i switche (czyli przełączniki), rejestratory sieciowe (NVR) oraz urządzenia stosowane w centrach monitoringu (komputery, monitory, urządzenia dekodujące, specjalistyczne oprogramowanie). Kamera generuje obraz za pośrednictwem obiektywu, krzemowego przetwornika CCD lub CMOS oraz szeregu działań związanych z cyfrowym przetwarzaniem sygnałów i kompresją. Sygnał skompresowany jest następnie wysyłany poprzez port ethernetowy (najczęściej za pomocą skrętki) do najbliższego przełącznika i dalej poprzez sieć światłowodową do centrów monitoringu lub konkretnych odbiorców sygnału. W tych miejscach znajdują się serwery z zainstalowanym oprogramowaniem specjalistycznym służącym do zarządzania kamerami i generowanymi przez nie obrazami. Oprogramowanie takie często dostarczane jest przez producenta kamery, jednak wtedy w większości przypadków obsługuje ono jedynie urządzenia danego producenta. Istnieją także systemy oprogramowania współpracujące z wieloma typami kamer różnych producentów (np. rodzina systemów XProtect firmy Milestone).



Rys. 1. Wymagana przepustowość łącza dla czterech kamer megapikselowych i dwóch PTZ



Rys. 2. Przykładowa architektura monitoringu w technologii IP

Usługa monitoringu

Zamawiający system monitoringu wizyjnego po raz pierwszy nie musi wydawać jednorazowo ogromnych pieniędzy na budowę infrastruktury, zakup urządzeń oraz uruchomienie systemu. Wszystkim zajmuje się usługodawca – od budowy infrastruktury światłowodowej (jeżeli jeszcze jej nie ma w miejscu wyznaczonym przez zamawiającego na zainstalowanie kamery), poprzez zakup wymaganych urządzeń, po opiekę nad sprawnym działaniem całego systemu.

Cechy usługi:

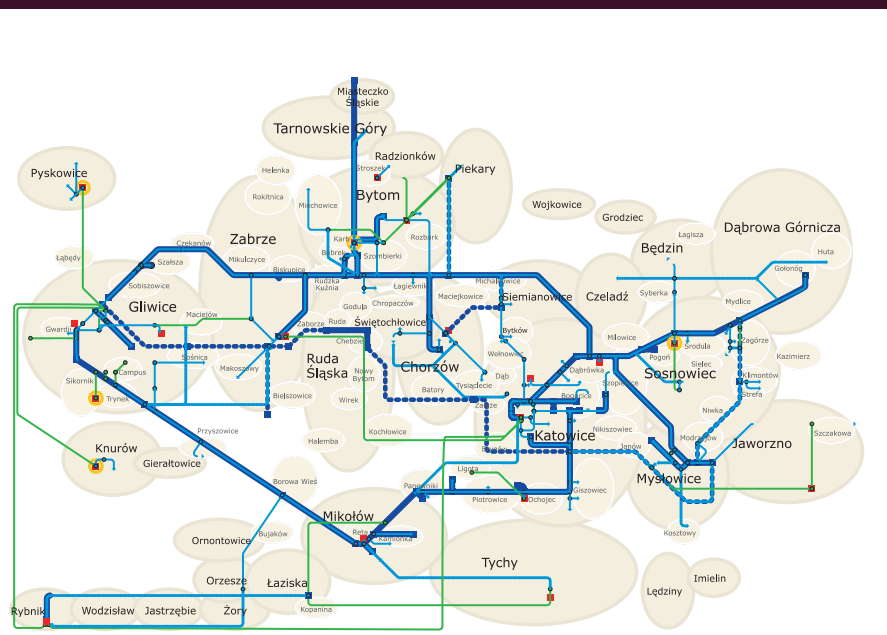
– brak kosztów inwestycyjnych;
– proces uruchomienia usługi trwa zwykle trzy miesiące;
– nie ma ograniczenia w liczbie instalowanych kamer oraz centrów monitoringu, które mogą się znajdować w dowolnym miejscu aglomeracji;
– utrzymanie kamer, dewastacje, awarie, kradzieże, postęp techniczny, prawo budowlane – to wszystko problem usługodawcy;
– usługa objęta jest przez tzw. SLA (*service level agreement*), tzn. klient nie płaci za czas niedziałania.

Przykład zastosowania usługi w Bytomiu i Katowicach

Pilotaż usługi monitoringu wizyjnego został wykonany w Katowicach i Bytomiu. W sumie jest to sześć kamer megapikselowych oraz typu PTZ, z których obraz przekazywany jest do centrum monitoringu mieszczącego się w Komendzie Miejskiej Policji w Bytomiu. Obrazy z systemu wykorzystuje na swoje potrzeby również Urząd Miasta Bytom oraz Miejski Zarząd Dróg i Mostów.

Za pośrednictwem łączy światłowodowych obraz z kamer jest przekazywany również do siedziby Szkoły Policji w Katowicach (w ramach programu „Razem bezpieczniej"). System służy słuchaczom tej szkoły jako narzędzie dydaktyczne, pozwalające na prowadzenie zajęć w warunkach zbliżonych do rzeczywistych. Obserwacja z wykorzystaniem kamer zainstalowanych w śródmieściu śląskich miast jest dostępna w sali odpraw Wielofunkcyjnego Centrum Symulacji Policyjnych. System uruchomiono w niespełna trzy miesiące.

Rys. 3. Przykład możliwości kamer monitoringu miejskiego



Rys. 4. Dostępność usługi monitoringu wizyjnego

Dlaczego światłowody?

Istotnym argumentem przemawiającym za stosowaniem światłowodów jest to, że zapewniają one najlepszą jakość transmisji przy jej dużym bezpieczeństwie. Dodatkowo za pomocą światłowodów możemy osiągnąć olbrzymie przepływności przy niskim tłumieniu, które wynosi 0,2-0,35 dB/km. Ważna jest również duża odporność światłowodów na zakłócenia i mała wrażliwość na środowisko.

Przedstawiona w artykule usługa monitoringu wizyjnego w technologii IP jest interesującym rozwiązaniem dla wielu podmiotów odpowiedzialnych za stan bezpieczeństwa oraz czystość i porządek w mieście. Usługa dostępna jest na terenie całej aglomeracji śląskiej.

Adam Hrynkiewicz
3S Śląskie Sieci Światłowodowe

3S ŚLĄSKIE SIECI ŚWIATŁOWODOWE

3S Śląskie Sieci Światłowodowe (marka TKP) to operator telekomunikacyjny działający na terenie Śląska i Zagłębia. Buduje on infrastrukturę światłowodową i udostępnia ją innym operatorom, dużym przedsiębiorstwom oraz instytucjom. 3S dysponuje siecią linii światłowodowych o długości ponad 600 kilometrów. Sieć ta pokrywa obszar 1500 km^2, na którym mieszka ponad trzy miliony mieszkańców aglomeracji śląskiej. Więcej informacji na *www.3s.pl*.

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

NOWE kamery IP

kamery IP kompaktowa i wandaloodporna

- matryca CCD, 1/3" SONY Super HAD
- mechaniczny filtr podczerwieni, możliwość pracy w podczerwieni
- wysoka rozdzielczość: do 600 TVL
- wbudowany webserwer
- kompresja i transmisja przez sieć wideo i audio w czasie rzeczywistym
- kompresja MPEG-4 lub M-JPEG
- możliwość definiowania stopnia kompresji, rozdzielczości i prędkości strumienia wideo
- sprzętowa detekcja ruchu
- dodatkowe wyjście analogowe BNC
- obudowa wandaloodporna o klasie szczelności IP 65 (NVIP-HDN4000VP)
- przesyłanie wideo i audio w standardzie RTP/RTSP

Wyłączny dystrybutor produktów NOVUS® w Polsce:

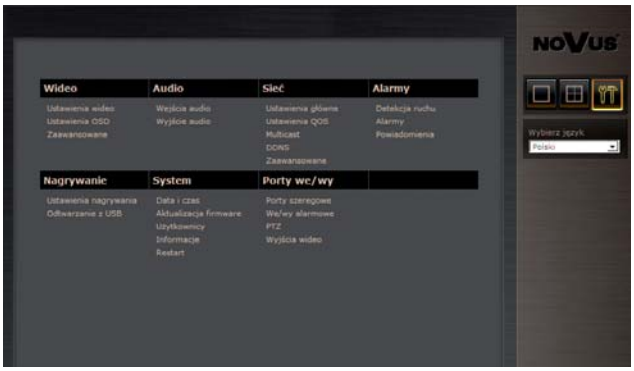
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 022 546 05 46, faks 022 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Monitoring wizyjny IP marki NOVUS

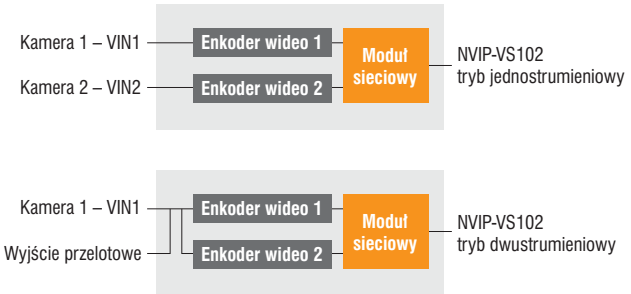
Trudno dziś sobie wyobrazić kompletną ofertę systemów telewizji dozorowej bez systemu monitoringu wizyjnego IP. Zdecydowana większość producentów oferuje i dynamicznie rozwija systemy IP. Posiadanie pojedynczych urządzeń, kamer czy wideoserwerów wizyjnych jest już dalece niewystarczające. O jakości systemu IP CCTV przy porównywalnej jakości urządzeń decyduje w głównej mierze aplikacja oraz jej interakcje z kamerami i wideoserwerami. W niniejszym artykule chciałbym zaprezentować system monitoringu wizyjnego IP marki NOVUS, możliwości sprzętu (kamer i wideoserwerów) oraz aplikacji NMS (Novus Management System)

W ofercie kamer IP znajdują się dwa modele: kamera kompaktowa NVIP-HDN5000 oraz wandaloodporna kamera NVIP-HDN4000VP. Są to klasyczne kamery typu dzień/noc z mechanicznymi filtrami podczerwieni i tym samym możliwością pracy w podczerwieni. Generują one obraz w wysokiej rozdzielczości (do 540 TVL w trybie kolorowym oraz 600 TVL w trybie czarno-białym). Wysoka czułość (0.05 lx/F=1.2) pozwala na otrzymanie klarownego obrazu nawet przy niskim natężeniu oświetlenia. O powyższych parametrach kamer warto wspomnieć z dwóch powodów: oprócz portu Ethernet do transmisji sieciowej obie te kamery posiadają również lokalne wyjście analogowe do wykorzystania dodatkowo w analogowym systemie nadzoru lub do celów serwisowych . Drugi powód to zastosowanie w kamerach matryc CCD, które w porównaniu z matrycami CMOS często wykorzystywanymi w kamerach IP wciąż cechują się dużo wyższą światłoczułością i tym samym pozwalają na pracę w trudnych warunkach oświetlenia, z którymi w praktyce instalacyjnej spotykamy się bardzo często. Dodatkowo kamery mogą współpracować z obiektywami, posiadającymi automatyczną przysłonę sterowaną prądowo (typu D), a nie tylko elektroniczną migawkę, która nie zapewnia odpowiedniej dynamiki ekspozycji. Kamera kopułowa wandaloodporna NVIP-HDN4000VP posiada wbudowany obiektyw z przysłoną typu D o zmiennej ogniskowej f=4~9 mm. Dodatkowo kamera ta posiada stopień IP65 zapewniający ochronę przed wnikaniem pyłów i strumieni wody. Wszelkie ustawienia dotyczące jakości sygnału wizji dokonuje się na panelu tylnym kamer za pomocą grupy potencjometrów. Ustawienia te obejmują funkcje automatycznej regulacji wzmocnienia, trybu pracy migawki (ALC/ELC), kompensacji jasnego oświetlenia tła BLC, redukcji migotania a także dodatkowo dla kamery kopułowej ustawienia korekcji Gamma oraz odwrócenia obrazu. Obie kamery posiadają wejście audio do podłączenia mikrofonu zewnętrznego i – poprzez oprogramowanie – możliwość odsłuchu i zapisu ścieżki dźwiękowej.

Wszelkie ustawienia dotyczące parametrów transmitowanego strumienia IP dokonuje się za pomocą przeglądarki internetowej lub za pomocą oprogramowania NMS. Najważniejszą zaletą tych urządzeń jest możliwość generacji strumienia wizji w rozdzielczości D1 (720 x 576) w czasie rzeczywistym (25 obrazów/s) w kompresji MPEG4 lub MJPEG. Oczywiście parametry strumienia można dostosowywać w zależności od przepustowości sieci w zakresie kompresji, rozdzielczości, prędkości i jakości. Do transmisji w sieci wykorzystywany jest



Fot. 1. Menu główne kamery



Rys. 1. Schemat pracy dwustanowiskowej

powszechny dla takich zastosowań protokół RTSP. W obrębie niniejszego artykułu nie sposób przedstawić szczegółowo wszelkich dostępnych ustawień interfejsu sieciowego. Dla ogólnej orientacji przedstawiam menu główne kamery (fot. 1).

W ofercie oprócz kamer znajdują się również wideoserwery IP. Warto w tym miejscu postawić pytanie o celowość stosowania wideoserwerów w przypadku, kiedy można zastosować bezpośrednio kamery IP. Istnieją dwa podstawowe powody ich stosowania. Pierwszy powód – to potrzeba przejścia z już istniejącego analogowego systemu nadzoru wizyjnego na system cyfrowy. Drugi wynika natomiast z ciągle jeszcze większej różnorodności oraz lepszej jakości kamer analogowych w porównaniu do kamer cyfrowych. Równie ważny w tym kontekście jest aspekt ekonomiczny: w tym przypadku analogowa kamera szybkoobrotowa w komplecie z wideoserwerem IP może być tańszym rozwiązaniem niż szybkoobrotowa kamera IP. Bardzo wiele urządzeń IP powstało zresztą poprzez zamknięcie w jednej obudowie dotychczas istniejących kamer analogowych z płytką serwera.

Wszystkie ustawienia dotyczące parametrów transmitowanego strumienia IP dokonuje się w identyczny sposób jak w przypadku opisywanych powyżej kamer IP. Ciekawą różnicą w przypadku wideoserwerów IP jest możliwość pracy dwustrumieniowej. W trybie tym wideoserwery wideo (tylko NVIP-VS102 i NVIP-VS104) pozwalają z jednego analogowego sygnału wejściowego uzyskać dwa strumienie cyfrowe różniące się parametrami wideo (kompresja, ilość klatek, rozdzielczość itd.). Powoduje to jednak utratę co drugiego kanału wideo. NVIP-VS102 pracuje jako dwustrumieniowy wideoserwer jednokanałowy, a NVIP-VS104 jako dwustrumieniowy wideoserwer dwukanałowy. Pracę dwustrumieniową wykorzystuje się przy transmisji sygnału wideo do obszarów sieci o różnej przepustowości lub w przypadku różnych ustawień jakości strumienia dla rejestracji i podglądu. Schemat pracy dwustrumieniowej przedstawiony jest na rys. 1.

W wideoserwerach IP wbudowano dodatkowo złącze RS485 do sterowania kamer obrotowych. Możliwość sterowania kamerą obrotową obejmująca pełne ustawienia menu istnieje z poziomu zarówno przeglądarki, jak i aplikacji NMS.

Zarówno kamery, jak i wideoserwery IP posiadają funkcję sprzętowej detekcji ruchu. Jest to pewne novum w porównaniu do tradycyjnych systemów, gdzie funkcja detekcji ruchu realizowana była po stronie rejestratora czy karty przechwytującej, nigdy zaś po stronie kamery.

NVIP-VS102

NVIP-VS101LITE

NVIP-VS104

NVIP-VS101

Fot. 2. Modele wideoserwerów: NVIP-VS101LITE, NVIP-VS101, NVIP-VS102, NVIP-VS104

Fot. 3. Kamery IP: NVIP-HDN4000VP oraz NVIP-HDN5000

Ustawienia detekcji można dokonywać na trzech warstwach, dla których czułość detekcji oraz próg detekcji możemy zdefiniować niezależnie. W przypadku detekcji ruchu informacja o tym jest wysyłana do oprogramowania NMS, które może wówczas podjąć nagrywanie w zależności od ustawień. Przenoszenie analizy obrazu do serwerów/kamer odciąża komputer i czyni system bardziej niezawodnym.

Dodatkowo trwają prace nad rozszerzeniem listy urządzeń kompatybilnych z oprogramowaniem NMS o kamery/wideoserwery innych producentów, wykorzystujących do transmisji sieciowej protokół RTSP. W tym przypadku funkcja ta ma dotyczyć tylko przechwytywania strumienia wideo.

Przed instalacją oprogramowania NMS warto zapoznać się z rozdziałem dotyczącym zalecanej konfiguracji komputera PC. Jest to szczególnie ważne w przypadku rejestracji i wyświetlania wielu strumieni wideo, ponieważ wraz ze zwiększaniem ilości tych strumieni wymagania te szybko rosną. Poniżej zawarte są wymagania dla komputera PC w przypadku obsługi 4 lub 16 kanałów wideo w rozdzielczości D1 i w czasie rzeczywistym. Wymagania te mogą być niższe w przypadku jednoczesnego wyświetlania mniejszej ilości kanałów wideo, obrazów o mniejszej rozdzielczości lub mniejszej ilości klatek. Warto tutaj dodać, że zasoby systemowe w głównej mierze pochłaniane są w procesie wyświetlania lub odtwarzania (dekodowania) strumienia. Natomiast bezpośredni zapis strumieni na twardy dysk w niewielkim zakresie obciąża komputer.

Równolegle z oprogramowaniem NMS instalowane jest narzędzie NOVUS IPtool pozwalające na wykrycie wszystkich urządzeń dostępnych w sieci (nawet w przypadku różnych podsieci komputera PC i urządzenia), zdalną zmianę ich adresów IP oraz ich diagnostykę, w tym aktualizację firmware-'u (oprogramowania wewnętrznego). Uproszczona wersja tego narzędzia do wyszukiwania i automatycznego dodawania urządzeń do programu NMS została zaimplementowana również w samym oprogramowaniu.

Interfejs programu NMS skomponowany jest z ruchomych paneli, których funkcja opisana jest poniżej. Charakterystyczną cechą programu jest możliwość dostosowania interfejsu poprzez przemieszczenie bądź ukrywanie poszczególnych paneli. Na fot. 5 zaprezentowano jedną z możliwych realizacji rozmieszczenia paneli programu. Daje to użytkownikowi praktycznie nieograniczone możliwości komponowania własnego interfejsu, dostosowanego do jego potrzeb i preferencji. Po wyłączeniu programu układ interfejsu zostaje zapamiętany i po ponownym uruchomieniu programu jest on wczytywany domyślnie. Dodatkowo własny układ paneli można zapisać i następnie odtworzyć. Jest to szczególnie wartościowa cecha w kontekście możliwości pracy wielomonitorowej oprogramowania, gdzie każdorazowe optymalne ustawienie aktywnych paneli niepotrzebnie zabierałoby czas operatorowi systemu.

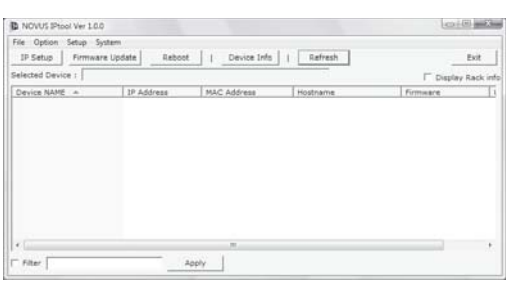
Oprogramowanie NMS pozwala na równoczesną obsługę do 64 strumieni wideo, choć liczba kanałów tylko rejestrowanych nie jest limitowana. Unikalną cechą systemu jest możliwość równoczesnego uruchomienia dwóch okien wideo (maksymalny podział każdego okna 4 x 4) oraz nadzoru 32 strumieni wideo równolegle w trybie *live* i odtwarzania.

W celu łatwego zarządzania systemem w oprogramowaniu dodano moduły edycji i podglądu graficznych podkładów użytkownika, tj. map. Pozwalają one na intuicyjne zarządzanie systemem monitoringu wizyjnego i w łatwy sposób mogą być tworzone na bazie plików graficznych w formacie JPG i bmp.

Program pozwala przede wszystkim na rejestrowanie przechwytywanych strumieni nawet z prędkością 25 obrazów dla pojedynczego kanału. Ustawienia harmonogramu nagrywania oraz definicji przestrzeni do nagrywania dla każdego kanału są realizowane indywidualnie. W takim przypadku każdy

Podzespoły	4 kamery	16 kamer
Procesor CPU (minimum)	Intel Pentium IV 3 GHz	Intel Core2Duo 3 GHz
Pamięć RAM PC (minimum)	1 GB	3 GB
Pamięć RAM karty graficznej	128 MB	min 512 MB

Tab. 1. Zalecane przykładowe konfiguracje komputera PC

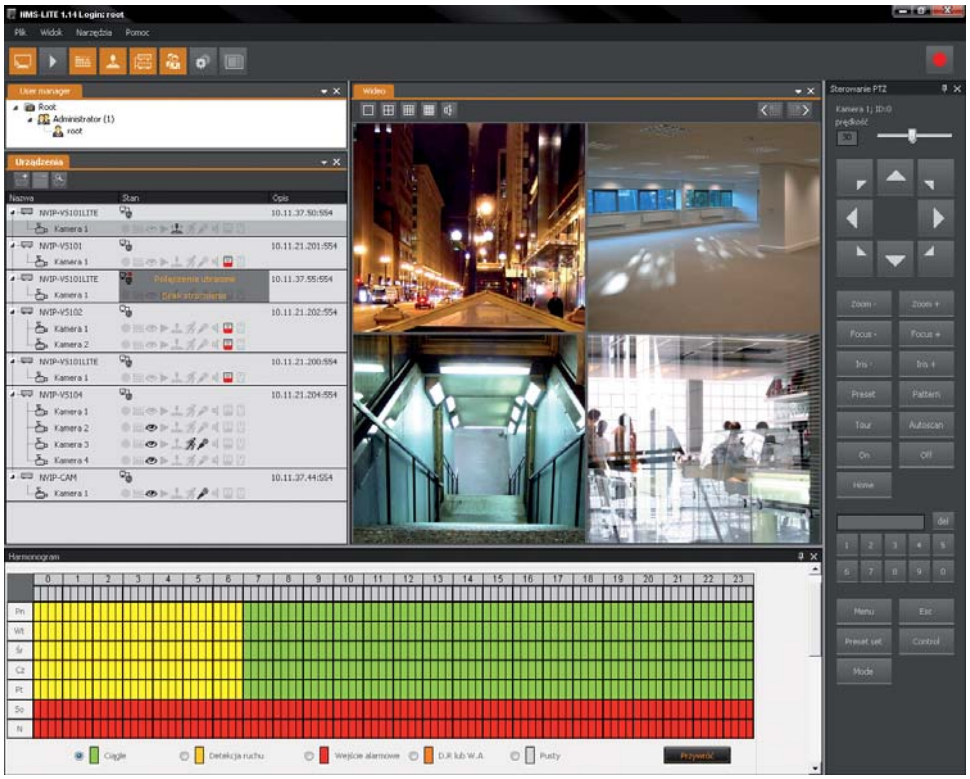


Fot. 4. Interfejs narzędzia NOVUS IPtool

strumień możemy traktować niczym pojedynczy rejestrator. W celu udostępnienia zarejestrowany materiał może być eksportowany do formatu AVI. Równolegle ze strumieniem wideo rejestrowany jest również strumień audio. Odtwarzanie strumieni wideo można realizować bezpośrednio, wybierając datę i czas za pomocą graficznej linii czasu lub wybierając dane zdarzenie z bardzo rozbudowanego rejestru zdarzeń aplikacji i urządzeń.

NMS pozwala również na bezpośredni dostęp do ustawień parametrów urządzeń w takim samym zakresie, w jakim można to zrealizować za pomocą przeglądarki.

Aplikacja posiada bardzo przydatną funkcję automatycznej aktualizacji. Przy każdorazowym uruchomieniu aplikacja łączy się z serwerem, sprawdzając aktualnie dostępną wersję oprogramowania, a po potwierdzeniu ściąga ją i instaluje. Ułatwia to zarządzanie kolejnymi wersjami oraz ich dystrybucję do użytkowników. Jest to szczególnie ważne w kontekście częstego udostępnania wersji oprogramowania wzbogaconych o nowe funkcje.



Fot. 5. Interfejs programu NMS

Fot. 6. Edytor map

Podsumowanie

Oprogramowanie NMS dodawane jest do każdego urządzenia (wideoserwera lub kamery IP) w ofercie marki NOVUS. Licencja aplikacji nie ogranicza liczby stanowisk, na których może być ona instalowana. Aplikacja cały czas jest rozwijana i w przyszłości traktowana ma być jako platforma integrująca różne systemy bezpieczeństwa, w tym m.in. system kontroli dostępu. Równolegle trwają prace nad wprowadzeniem tzw. kamer megapikselowych, generujących strumień wideo o wysokiej rozdzielczości.

Najlepszym sposobem na przetestowanie wszystkich funkcji oprogramowania jest samodzielna instalacja oraz testowanie oprogramowania. Na stronie internetowej *www.aat.pl* została udostępniona 30-dniowa wersja demonstracyjna oprogramowania NMS Lite. Po ściągnięciu i zainstalowaniu aplikacji można połączyć się z wybranymi kamerami i wideoserwerami. W zależności od sposobu połączenia (poprzez przeglądarkę internetową lub aplikację NMS) należy wybrać porty HTTP lub RTSP.

Dostępne porty do połączenia zdalnego:
Adres: *http://demo.novuscctv.com:xxxx*
HTTP: 6080, 6180, 6280, 6480
RTSP: 6081, 6181, 6281, 6282, 6481, 6482, 6483, 6484.

W celu efektywnej obsługi wielu użytkowników po dziesięciu minutach następuje rozłączenie dla podanej lokalizacji na okres jednej minuty dla danego adresu IP.

Patryk Gańko
NOVUS Security

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

NOWE wideoserwery IP

1/2/4 - kanałowe wideoserwery IP

- kompresja i transmisja przez sieć wideo i audio w czasie rzeczywistym
- kompresja MPEG-4 lub M-JPEG
- rozdzielczość przechwytywania/transmisji wideo do D1
- możliwość definiowania stopnia kompresji, rozdzielczości i prędkości strumienia wideo odrębnie dla każdego kanału
- przesyłanie wideo i audio w standardzie RTP/RTSP
- sprzętowy filtr przeplotu (deinterlacing filter)
- sprzętowa detekcja ruchu
- praca dwustrumieniowa (NVIP-VS102, NVIP-VS104)
- port RS-485 do podłączenia kamer PTZ (NVIP-VS101, NVIP-VS102, NVIP-VS104)
- transmisja audio - kodowanie w standardzie G.711 (NVIP-VS101, NVIP-VS102, NVIP-VS104)

Wyłączny dystrybutor produktów NOVUS® w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 022 546 05 46, faks 022 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Wpływ opóźnień w sieciach IP

na skuteczność monitoringu wizyjnego część 2

W pierwszej części artykułu omówiono problematykę monitoringu wizyjnego wykorzystującego sieci IP ze szczególnym uwzględnieniem analizy powstających w takim przypadku opóźnień transmisji. W drugiej części przedstawiona zostanie koncepcja stanowiska laboratoryjnego do badania opóźnień w sieciach IP, będą także zaprezentowane wyniki przeprowadzonych na tym stanowisku badań

1. Koncepcja stanowiska laboratoryjnego do badania opóźnień w przesyłanych poprzez sieć IP obrazach monitoringu wizyjnego

Wraz z coraz powszechniejszą technologią cyfrową, zastępującą rozwiązania analogowe, postępować będzie dalszy rozwój w takich dziedzinach jak wysoka rozdzielczość czy zaawansowana kompresja wideo. Ale sukces działania systemu monitorowania będzie ostatecznie zależał od tego, jak szybko informacja zostanie przekazana. W analogowych systemach dozorowych, które wykorzystywały magnetowidy, obraz nie był kompresowany, a do jego podglądu służył monitor analogowy. Cała informacja z kamery przesyłana była w sposób ciągły. W kolejnych rozwiązaniach do cyfrowego zapisu obrazu analogowe systemy telewizji dozorowej wykorzystywały rejestratory cyfrowe (DVR). Opóźnienie występujące w tym rozwiązaniu, wynikające z przekształcenia obrazu do postaci cyfrowej i skompresowania go w celu zapisania jak największej ilości danych, było niewielkie. Natomiast w sieciowych systemach dozoru wizyjnego, wykorzystujących kamery sieciowe, obraz jest przesyłany poprzez sieć IP za pośrednictwem przełączników sieciowych, a następnie zapisywany na standardowym komputerze z oprogramowaniem zarządzającym. W tym przypadku opóźnienie może osiągać znaczne wartości. Zależy ono między innymi od przepustowości samej sieci, a także od kamery – od tego, jaką rozdzielczość i jaką metodę kompresowania wykorzystujemy.

W związku z powyższym nie można skumulować badań tylko na pomiarach opóźnień pakietów TCP/IP. Stanowisko laboratoryjne musi umożliwiać dwa rodzaje pomiarów:

– badania opóźnień przy zmianie topologii sieci,
– badania kamer sieciowych.

Biorąc pod uwagę, że jest to system bezpieczeństwa, zestawione stanowisko pomiarowe powinno zapewnić pomiar opóźnienia z punktu widzenia operatora. Opóźnienie mierzone jest jako różnica czasu pomiędzy rzeczywistym zdarzeniem wywołanym przed kamerą sieciową a czasem, po którym to zdarzenie pojawi się na ekranie operatora.

1.1 Budowa stanowiska pomiarowego

W Laboratorium Systemów Bezpieczeństwa i Analizy Zagrożeń Instytutu Optoelektroniki Wojskowej Akademii Technicznej zostało zbudowane stanowisko do pomiaru opóźnień w przesyłanych przez sieć obrazach monitoringu wizyjnego. Fot. 1 przedstawia zestawione i gotowe do użycia stanowisko.

Na stanowisku pomiarowym zostały przeprowadzone następujące badania pod względem opóźnień przesyłanego obrazu wizyjnego:

– badania wybranych modeli kamer sieciowych,
– badania wybranych modeli połączeń sieciowych.

1.1.1 Schemat blokowy stanowiska pomiarowego

Schemat podstawowego układu pomiarowego został przedstawiony na rys. 1.

W skład stanowiska pomiarowego wchodzą:

– kamery sieciowe,
– urządzenia sieciowe (TCP/IP) umożliwiające połączenie z siecią i przełączanie pakietów,
– dwa detektory wykrywające zdarzenie czasu rzeczywistego (detektor 1) oraz to samo zdarzenie po przejściu przez sieć i wyświetleniu na monitorze (detektor 2),
– komputer z monitorem służące do wizualizacji i konfiguracji elementów sieciowych (kamer IP),
– generator służący do sterowania diodą elektroluminescencyjną,
– oscyloskop służący do pomiaru różnicy dwóch czasów.

1.1.2 Wykaz urządzeń znajdujących się w układzie laboratoryjnym

Urządzenia znajdujące się w układzie laboratoryjnym:

1. Kamery sieciowe różnych typów i różnych producentów (rok produkcji 2007/2008). Ze względu na specyfikę niniejszego artykułu nazwy przebadanych kamer pozostaną do wiadomości autora , a w artykule nazwane będą K1, K2 itd.;
2. Oscyloskop Hewlett Packard 54610B;
3. Generator cyfrowy sterujący diodą Hewlett Packard 33120A;
4. Detektor (fotodioda) x2 Thorlabs PDA 500
   Specyfikacja:
   – detektor: GaAsP (fosforoarsenek galu),
   – powierzchnia światłoczuła: 1,3 mm x 1,3 mm,
   – zakres czułości: 300 – 680 nm,
   – zakres temperatury pracy: od 10 do 60° C,
   – możliwość wzmocnienia: pięć poziomów,
   – impedancja detektora: 50 Ω;
5. Przełącznik 10/100 Fast Ethernet D – Link DES – 1008D.

Urządzenia nie umieszczone w podstawowym układzie laboratoryjnym, ale pozostające do zastosowania podczas badania modeli kamer przy zmianie topologii sieci:

1. Mediakonwerter 100BASE TX /100 FX, wielomodowy (x2) Transition Networks J/CFE-CF-02;
2. Ruter bezprzewodowy Linksys WRT54GC;
3. Hub Unex HD080;
4. Modem Alfa 1 + most Ethernet Beta 1 (x2) Goramo W6744.

1.2 Metodyka pomiaru opóźnienia

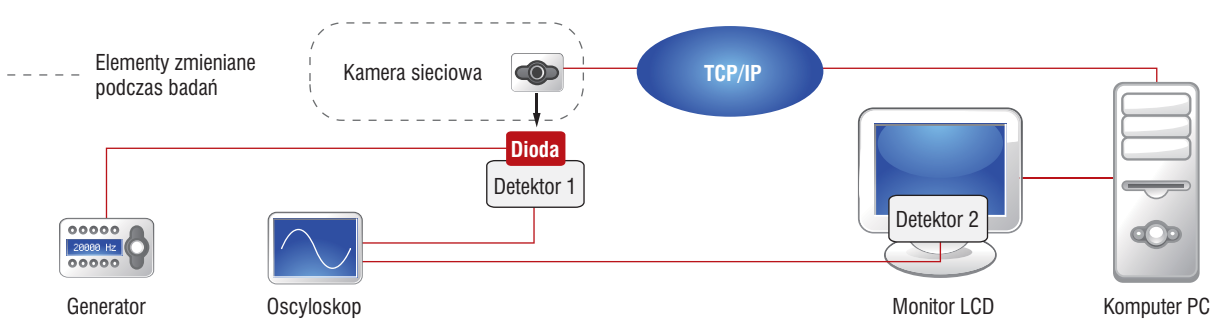
Pomiar opóźnienia dokonywany jest na podstawie wskazań oscyloskopu HP 54610B. Do kanałów oscyloskopu (K1, K2) podłączone są dwa detektory (fotodiody). Źródłem światła dla pierwszej fotodiody jest czerwona dioda sterowana generatorem HP 33120A. Pierwszy detektor umieszczony jest przed diodą i kamerą oraz podłączony do kanału K1 oscyloskopu. Sygnał z pierwszej fotodiody dochodzi w chwili zaświecenia diody (po wychwyceniu światła przez fotodiodę). Jednocześnie zaświecenie diody jest obserwowane przez kamerę podłączoną do sieci. Obraz z kamery po przejściu przez sieć pojawia się na monitorze komputera. Pojawiający się na monitorze obraz świecącej się diody jest źródłem światła dla drugiego detektora. Detektor ten podłączony jest do kanału K2 oscyloskopu. Sygnał z drugiej fotodiody jest sygnałem, który przechodzi przez kamerę, przełącznik i sieć i jest on odbierany w chwili pojawienia się obrazu zaświecenia diody na monitorze komputerowym. Wartość opóźnienia to różnica czasów pojawienia się dwóch wyżej opisanych sygnałów podanych na kanały K1 i K2 oscyloskopu.

Fot. 2 przedstawia dwa wyżej opisane detektory. W celu uzyskania jak najlepszej jakości sygnałów na oscyloskopie badania wykonano w zaciemnionym pomieszczeniu. Dodatkowo do ekranu monitora przyczepiona została czarna tektura z odpowiednim otworem obejmującym tylko obraz świecącej się diody. Pozwala to na wyeliminowanie odbierania przez fotodiody dodatkowych, niepotrzebnych sygnałów pochodzących od świetlówek i monitora.

Na wielkość opóźnienia, oprócz opóźnień w sieci, ma wpływ opóźnienie związane z czasem reakcji monitora. Czas reakcji ekranu jest miarą tego, jak szybko piksele potrafią ukończyć jeden pełny „cykl" wyświetlania, tak że mogą brać udział w kolejnej klatce odtwarzanych obrazów. Czas reakcji matrycy wykorzystanego monitora LCD to 8 ms.

2. Badania wybranych modeli kamer sieciowych pod względem opóźnień przesyłanego obrazu wizyjnego

Podczas projektowania i budowy systemu monitoringu wizyjnego niezbędny jest wybór odpowiedniej kamery. Dla systemu sieciowego jednym z kryteriów wyboru jest opóźnienie wnoszone przez samą kamerę podczas transmisji obrazu przez sieć. Konieczne jest ustawienie parametrów kamer w taki sposób, aby było ono jak najmniejsze. W związku z tym w badaniach



Rys. 1. Schemat blokowy podstawowego układu pomiarowego

Fot. 1. Stanowisko laboratoryjne do pomiaru opóźnień

laboratoryjnych zwrócono szczególną uwagę na podstawowe parametry kamer sieciowych, które są najczęściej modyfikowane i które mają największy wpływ na zmianę opóźnień. Podczas pomiarów konfigurowano następujące ustawienia poszczególnych kamer:

– rozdzielczość obrazu przy maksymalnej liczbie klatek na sekundę,
– standard kodowania,
– liczbę wyświetlanych klatek obrazu/sekundę dla kilku rozdzielczości.

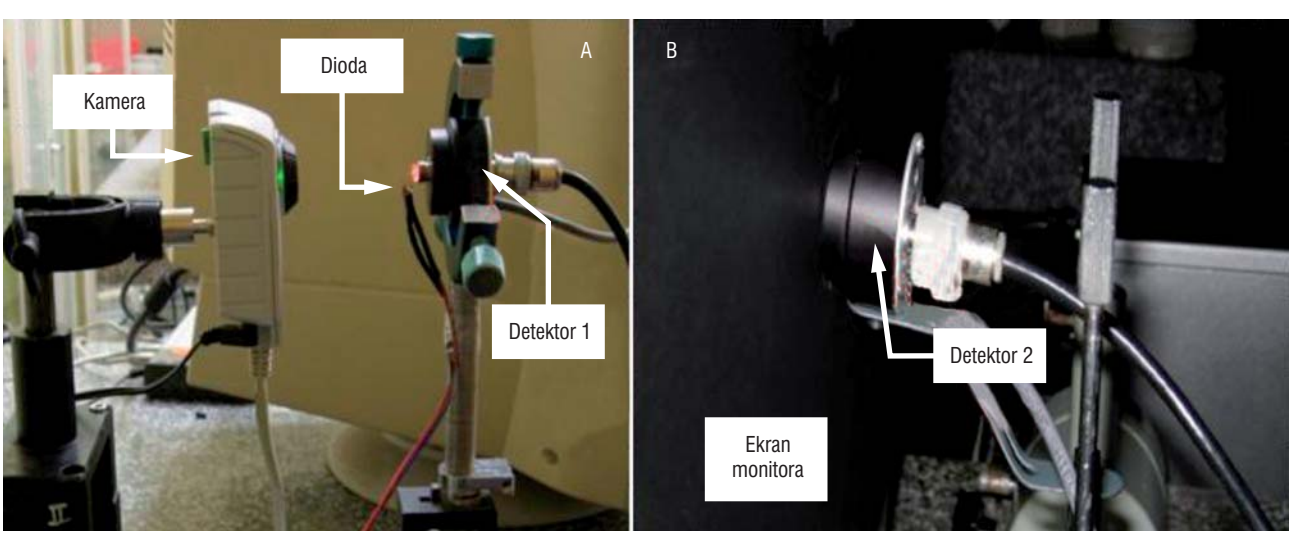
Pozostałe parametry dla wszystkich kamer sieciowych pozostawały niezmienione aby uniknąć dodatkowych błędów pomiarowych, wynikających z wzajemnego oddziaływania tych kamer. Dla każdej kamery sieciowej, przy każdej zmianie ustawienia parametrów, przeprowadzono 15 pomiarów niezbędnych do wykonania analizy statystycznej wyników pomiarów.

Ze względu na ograniczoną ilość miejsca w artykule zrezygnowano z przedstawiania poszczególnych wyników tabelarycznych. Wyniki te zawarte są w pracy dyplomowej Łukasza Stawickiego. Przedstawione w niej tabele pomiarowe odzwierciedlają rzeczywiste wartości opóźnień w zależności od zastosowanych kamer sieciowych podczas przesyłu obrazu wizyjnego w sieci. Badania przeprowadzono dla siedmiu kamer sieciowych przy ustalonym połączeniu sieciowym. W ten sposób możliwe było porównanie wartości opóźnień wprowadzanych wyłącznie przez zmianę kamery bądź jej parametrów. Wybór parametrów został przeprowadzony na podstawie najczęściej modyfikowanych przez instalatorów i użytkowników ustawień.

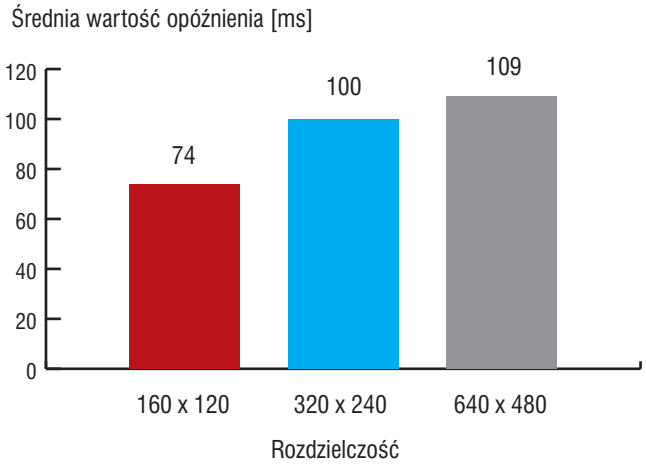
Analizując wyniki pomiarów, zaobserwowano, że na wartość opóźnienia znaczny wpływ ma rozdzielczość obrazu. Im większa jej wartość, tym większe opóźnienie. Wynika to z faktu, że zwiększając ustawienia rozdzielczości, zwiększamy też rozmiar obrazu, a zatem mamy większą ilość informacji do przesłania łączem sieciowym, co wymaga dłuższego czasu potrzebnego do jej przesłania. Związane jest to z zastosowaniem łącza o większej przepustowości. Przykładowo dla kamery K1 średnie wartości opóźnienia dla kolejnych rozdzielczości przedstawia rys. 2.

Dla wszystkich badanych kamer sieciowych wraz ze wzrostem rozdzielczości rośnie wartość opóźnienia. Największa wartość opóźnienia przesyłanego obrazu wizyjnego wynikająca ze zmiany rozdzielczości występuje w kamerach megapikselowych. Obraz w rozdzielczości megapikselowej zawiera dużo więcej szczegółów i jest bardzo dobrej jakości. Jest to niewątpliwie odpowiednie rozwiązanie dla monitoringu wizyjnego. Jednak przesył w sieci zajmuje więcej czasu niż przy standardowych rozdzielczościach. Na rys. 3 przedstawiono średnie wartości opóźnień dla kamer megapikselowych w zależności od zmiany rozdzielczości.

Rozdzielczość 1280x960 pikseli (4 x VGA, VGA – 640x480 pikseli) zapewnia rozdzielczość jednego megapiksela. Można zaobserwować, że dla rozdzielczości megapikselowych opóźnienie jest znacznie większe. Dla kamery K2 opóźnienie przy 640x480 pikseli wynosi 116 ms, natomiast przy 1280x1024 pikseli wynosi 273 ms. Zwiększa się zatem ponad dwukrotnie. Kamera K3 charakteryzuje się największym opóźnieniem



Fot. 2. Fotodiody wykorzystane w układzie pomiarowym, a) przed kamerą, b) przed monitorem



Rys. 2. Wykres średniej wartości opóźnienia w zależności od zmiany rozdzielczości obrazu dla kamery K1

zarówno dla małych, jak i dużych rozdzielczości. Natomiast model K5 wykazuje najmniejsze opóźnienie przy rozdzielczościach megapikselowych oraz niewielkie przy mniejszych.

Megapikselowe kamery sieciowe umożliwiają uzyskanie proporcji obrazu 16:9. Również ta zmiana jest związana z opóźnieniem, ponieważ przy zastosowaniu tej proporcji zmniejsza się rozdzielczość, a co za tym idzie – także opóźnienie. Najlepiej przedstawiają to wyniki pomiarów dla kamery K5. Porównanie tych wartości przedstawia rys. 4.

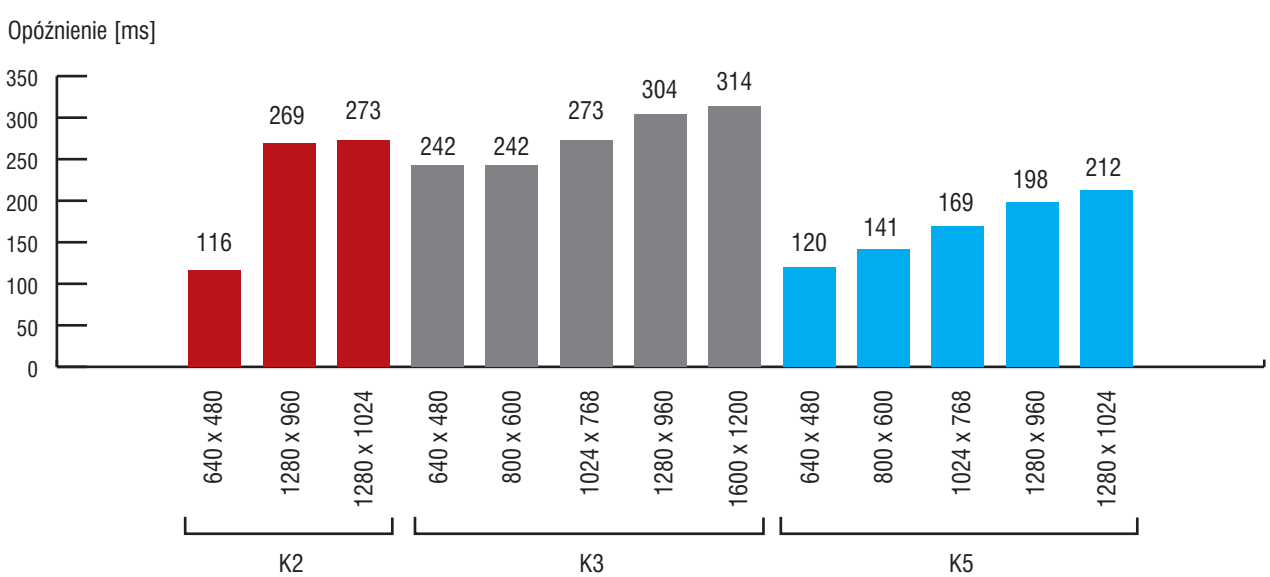
Dzięki zastosowaniu proporcji obrazu 16:9 można zyskać nie tylko na liczbie pikseli, ale także na zmniejszeniu zajętości pasma i miejsca podczas zapisu. Jednak w niektórych przypadkach część dolna i górna obrazu są na tyle istotne, że nie należy stosować tej proporcji (lepszym rozwiązaniem będzie proporcja 4:3).

Kolejnym parametrem wpływającym na wartość opóźnienia jest format kompresji. Konieczność digitalizacji jest oczywista: nieskompresowany plik wideo zajmuje dużo miejsca i pasma. Przykładowo obraz o rozmiarach 1024x768 pikseli, w którym każdy piksel jest zakodowany w 24 bitach (po osiem bitów na kolor czerwony, zielony i niebieski), bez kompresji będzie liczył ok. 2,5 MB. Przesłanie go przez łącze o szybkości 256 kb/s zajęłoby ponad minutę. Jeśli obraz zostanie skompresowany w stopniu 20:1, to czas jego transmisji skróci się również dwudziestokrotnie.

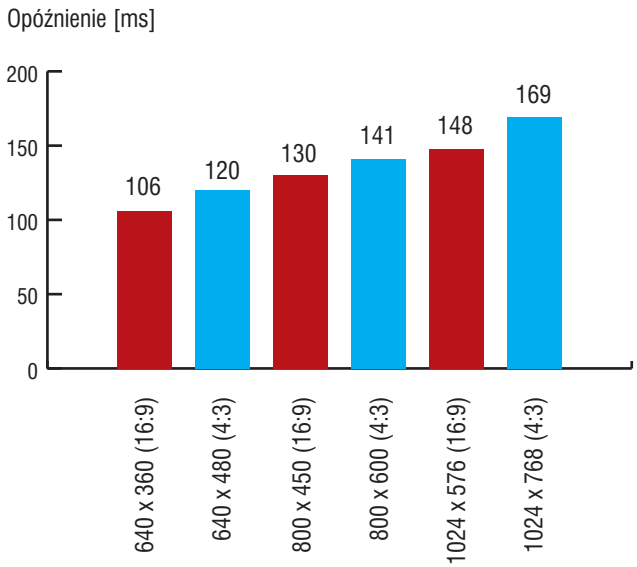
We współczesnych kamerach sieciowych stosowane są najpowszechniej dwa standardy kompresji: M-JPEG i MPEG-4. Najczęściej stosowanym standardem w sieciowych systemach telewizji dozorowej jest Motion JPEG (M-JPEG). Kamera sieciowa rejestruje i kompresuje określoną liczbę pojedynczych zdjęć na sekundę, a następnie udostępnia je jako ciągły strumień obrazów w sieci. Natomiast w technice kompresji MPEG następuje porównywanie skompresowanych zdjęć. W kolejnym obrazie przesyłane są tylko te fragmenty, które różnią się od poprzedniego obrazu. W związku z tym dzięki MPEG-4 następuje zmniejszenie ilości przesyłanych informacji w porównaniu z M-JPEG. Zmniejsza się więc zapotrzebowanie na przepustowość sieci. Jednak technika MPEG-4 ma również wady związane ze wzrostem opóźnienia przesyłanego obrazu wizyjnego, co można zaobserwować na podstawie wyników pomiarów. Przykładowo na rys. 5 przedstawiono różnicę wartości opóźnienia podczas przesyłania obrazu wizyjnego dla dwóch wyżej opisanych standardów kompresji.

W każdym przypadku widać, że wartość opóźnienia przy stosowaniu kompresji MPEG-4 jest większa niż przy M-JPEG. Najmniejsza wartość opóźnienia dla MPEG-4 oraz mała różnica między dwoma standardami występuje dla kamery K5. Większa wartość opóźnienia w technice MPEG-4 wynika z faktu, że proces kodowania i dekodowania wymaga dużej mocy obliczeniowej, a więc i więcej czasu. Mimo generacji mniejszej niż w M-JPEG ilości danych obrazów przesyłanych przez sieć, a więc mniejszym wykorzystaniu przepustowości, złożoność procesu kompresji przyczynia się do większych zwłok czasowych w porównaniu ze standardem Motion JPEG, powodując większe opóźnienie. W Motion JPEG występuje niewielkie opóźnienie związane z kompresją i złożeniem pojedynczych zdjęć.

Następnym parametrem, który przebadano dla kilku typów kamer sieciowych, jest szybkość transmisji, czyli liczba klatek na sekundę. Na podstawie wyników pomiarów dla kamery K3 (rys. 5) można wywnioskować, że wraz ze zmniejszaniem



Rys. 3. Wartość opóźnienia dla kamer megapikselowych w zależności od zmiany rozdzielczości



Rys. 4. Porównanie wartości opóźnień w zależności od proporcji obrazu dla kamery K5

ilości klatek/sekundę nieznacznie rośnie wartość opóźnienia. Dla ustalonej rozdzielczości 640x480 przy ustawieniu 25 kl/s opóźnienie wyniosło 129 ms. Gdy liczbę klatek zmniejszono do 10, wówczas opóźnienie wzrosło do wartości 187 ms. W pozostałych przypadkach zmiana szybkości transmisji powodowała niewielkie zmiany rzędu 10 ms. Najmniejsze zmiany zauważono przy porównaniu 25 kl/s oraz 30 kl/s. Także przy stosowaniu kompresji MPEG-4 zmiany liczby klatek/s były nieznaczne. Przykładem jest tu pomiar dla kamery K1, gdzie różnica między szybkością 25 kl/s a 15 kl/s przy rozdzielczości 640x480 pikseli jest niezauważalna.

Wzrost wartości opóźnienia pod wpływem zmniejszenia ilości przesyłanych klatek/s może tłumaczyć większe wartości opóźnień dla kamery K4, w której szybkość transmisji nie przekracza 12 klatek/s.

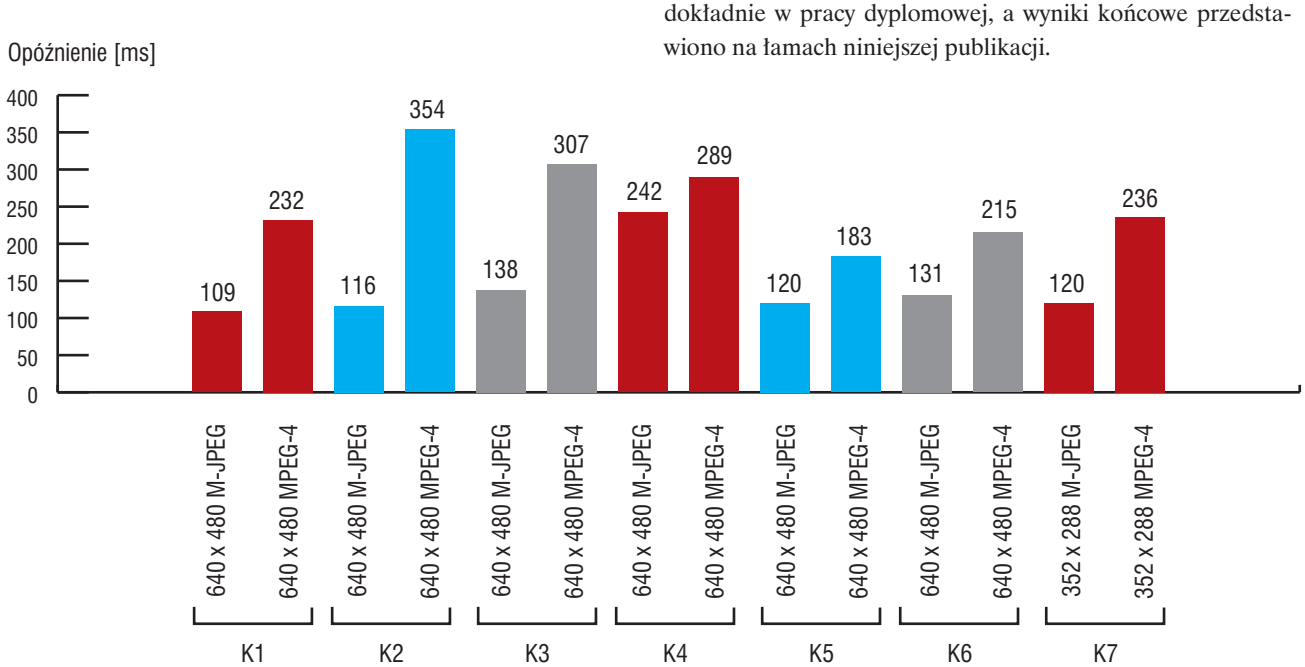
Na wartość opóźnienia ma również wpływ samo powiększenie obrazu. Dla dwóch kamer (K1, K7) można było zwiększyć obraz bez zmiany rozdzielczości bezpośrednio w przeglądarce internetowej. Pierwsza kamera charakteryzuje się małą różnicą średniego opóźnienia przy powiększeniu dwukrotnym (1 ms) oraz czterokrotnym (6 ms). Różnica dla drugiej kamery przy powiększeniu dwukrotnym wynosi 42 ms.

Badania opóźnienia przeprowadzono również dla trzech kamer sieciowych podłączonych jednocześnie. W danej chwili można było zrobić pomiary dla jednej kamery – tej, której obiektyw zwrócony był na migającą diodę. Obrazy z kamer były wyświetlane na jednym monitorze za pomocą przeglądarki internetowej. Spowodowało to zwiększenie ilości informacji do przesłania przez sieć oraz obciążenie systemu. Stosowane pasmo wystarczyło, aby przesłać obrazy bez znacznego wzrostu średniego opóźnienia. Jedynie przy przesyłaniu obrazu wysokiej rozdzielczości następuje wzrost opóźnienia o ok. 80 ms.

Podczas badania kamery sieciowej K1 zmieniono monitor z typu LCD na kineskopowy (CRT). Wyniki zamieszczone w pracy ukazują wzrost wartości opóźnienia w wyniku tej modyfikacji stanowiska. Wiąże się to z częstotliwością odświeżania ekranu monitora CRT i czasem reakcji matrycy w monitorach LCD.

Istotne zmiany wartości opóźnienia można zauważyć przy zmianie komputera PC. Podstawowe parametry nowego komputera: Windows 200 Professional, 256 MB RAM, procesor 731 MHz. Pomiary przy tej modyfikacji zostały przeprowadzone dla jednej kamery. Kluczowe elementy odpowiadające za wzrost opóźnienia to: system operacyjny, karta sieciowa, szybkość procesora, ilość wolnej pamięci RAM. Przykładowo dla rozdzielczości 320x240 pikseli różnica wartości opóźnienia dla dwóch komputerów wynosi 83 ms, a dla 640x480 pikseli przy standardzie kompresji MPEG-4 różnica ta wynosi 235 ms. Można więc wywnioskować, że istotnym elementem mającym wpływ na wartość opóźnienia jest zastosowanie odpowiedniego sprzętu komputerowego.

Badania kamer sieciowych pokazały, że wartość opóźnienia zależy od wielu czynników. Wszystkie te czynniki oraz ich wpływ na czas przesłania obrazu wizyjnego zostały opisane dokładnie w pracy dyplomowej, a wyniki końcowe przedstawiono na łamach niniejszej publikacji.



Rys. 5. Opóźnienie przesyłanego obrazu wizyjnego w zależności od przyjętego standardu kompresji

3. Badania wybranych modeli połączeń sieciowych pod względem opóźnień przesyłanego obrazu wizyjnego

Niewątpliwie bardzo duży wpływ na wielkość opóźnienia przesyłanego obrazu wizyjnego ma rodzaj medium transmisyjnego, po którym ten przekaz następuje. Najczęściej wykorzystywanym protokołem do transmisji danych jest TCP/IP omówiony w pierwszej części artykułu. Prędkość transmisji na poziomie 100 Mbit jest wystarczająca dla transmisji wideo z kamery sieciowej. We współczesnych sieciach komputerowych występują różnorodne odmiany Ethernetu, z których najczęściej stosowane są [1]:

– 10 Mbit/s Ethernet (10BASE–T) – ze względu na wąskie pasmo mniej stosowany. Wykorzystuje on cztery przewody (dwie skręcone pary). W tym układzie każdy element sieci podłączony jest do rozdzielacza (huba) lub przełącznika kablem dwuparowym.
– Fast Ethernet (100Mbit/s) – najbardziej rozpowszechniony standard w sieciach komputerowych. Podstawowy standard tego typu to 100BASE-T, który dzieli się na dwie kategorie: 100BASE-TX – transmisja kablem ośmiożyłowym ze skręconymi parami kategorii 5 oraz 100BASE-FX – transmisja kablem światłowodowym.
– Gigabit Ethernet (1000 Mbit/s) – Ten standard jest dzisiaj wykorzystywany w elementach struktury sieciowej do połączeń pomiędzy serwerami czy też sieciowymi przełącznikami.

Obecnie na szeroką skalę wprowadzane są bezprzewodowe sieci lokalne oparte na technologii IEEE 802.11. Podstawowe standardy tej technologii [1]:

– 802.11b – szybkość transmisji danych do11Mb/s, pasmo 2,4 GHz,
– 802.11g – szybkość transmisji danych do 54Mb/s, pasmo 2,4 GHz,
– 802.11a – szybkość transmisji danych do 54Mb/s, pasmo 5 GHz.

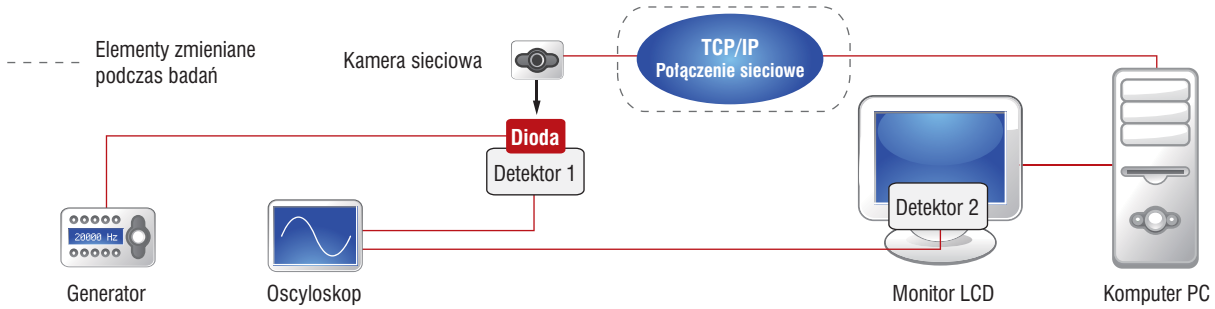
Szybkość transmisji obrazu wizyjnego zależy więc w znacznym stopniu od fizycznego nośnika, po jakim dany przesył następuje, czyli od połączenia sieciowego. Przykłady fizycznych nośników zostały przedstawione w pierwszej części artykułu. Stanowisko laboratoryjne umożliwia pomiar opóźnienia wynikającego z modelu połączenia sieciowego. Oczywiście badania, zgodnie z założeniem, prowadzone są z punktu widzenia operatora.

Ze sprzętu dostępnego w laboratorium zestawiono i zbadano pod względem opóźnienia pięć rodzajów połączeń sieciowych opisanych w tym rozdziale.

3.1 Stanowisko do badania wybranych modeli połączeń sieciowych

Na rys. 6 przedstawiono schemat układu laboratoryjnego do badania połączeń sieciowych.

Zestawione stanowisko pomiarowe umożliwia badania różnych modeli połączeń sieciowych. W celu wskazania różnicy do wszystkich typów połączeń zastosowano jedną kamerę – K1 o ustalonych parametrach. Do wizualizacji obrazu z kamery służy komputer z przeglądarką internetową.



Rys. 6. Schemat stanowiska pomiarowego do badania wybranych modeli połączeń sieciowych

Wszystkie pomiary wykonano przy częstotliwości ustawionej na generatorze f = 200 mHz oraz przy przebiegu prostokątnym. W celu zwiększenia dokładności pomiaru pokrętłem regulacji podstawy czasu na oscyloskopie wybrano taką pozycję, aby uzyskać stabilne i widoczne przebiegi.

Badania przeprowadzono dla następujących modeli połączeń sieciowych:

– połączenia wykorzystującego skrętkę miedzianą UTP zaopatrzonej w złącza RJ-45,
– połączenia światłowodowego,
– połączenia bezprzewodowego (1 przełącznik),
– połączenia bezprzewodowego + światłowodowego (2 przełączniki),
– połączenia kablem telefonicznym zaopatrzonym w złącza RJ-11.

Wykaz urządzeń wraz ze specyfikacją techniczną został przedstawiony w rozdziale 3.

Wyniki końcowe przedstawione w postaci wykresu (rys. 7) odzwierciedlają rzeczywiste wartości opóźnień w zależności od zmiany modelu połączenia sieciowego. Dla niektórych połączeń sieciowych wartości tego parametru dochodziły do kilku sekund.

W sieciach komputerowych najczęściej stosowanym przewodowym nośnikiem transmisyjnym jest skrętka miedziana nieekranowana UTP (Unshielded Twisted Pair) [1] zakończona obustronnie złączem RJ-45. Składa się ona z czterech par skręconych ze sobą żył miedzianych. Do transmisji danych są używane dwie oddzielne ścieżki: jedna para transmituje dane nadawcze Tx, a druga para odbiera dane Rx. Obecnie w przypadku sieci lokalnych używających skrętki szybkość transferu danych zawiera się w przedziale od 10 Mb/s do 1 Gb/s [1]. Większość urządzeń sieciowych (przełącznik, rozdzielacz itp.) jest zgodna z technologią 100Base-TX, pozwalającą na komunikowanie się z prędkością 100 Mb/s. Na rys. 9 można zaobserwować, że połączenie z zastosowaniem skrętki miedzianej charakteryzuje się małą wartością średniego opóźnienia (171 ms). Wynika to z faktu, że do przesyłu skompresowanego obrazu wizyjnego wystarczy pasmo mniejsze od 100 Mb/s. Opóźnienie jest tu głównie związane z oczekiwaniem i przejściem pakietów w przełącznikach sieciowych.

Podobna wartość średniego opóźnienia (166 ms) występuje dla połączenia z zastosowaniem światłowodu. Światłowód przenosi impulsy świetlne. Każdy impuls reprezentuje jeden bit. Światłowody są odporne na zakłócenia elektromagnetyczne i oferują niebywałe prędkości transmisji, nawet do setek Gb/s. Z tego powodu stały się preferowanym przewodowym nośnikiem transmisji. Dość wysoki koszt urządzeń optycznych (odbiorniki i przełączniki, transmitery) powoduje, że technologia światłowodowa jest wdrażana głównie w przypadku dużych odległości. Wykorzystane w stanowisku laboratoryjnym mediakonwertery światłowodowe zapewniają zmianę medium przewodzącego strumień informacji pomiędzy kablem skręcanym UTP (standard 100BASE-TX) a światłowodem wielomodowym – 1300 nm (standard 100BASE-FX). Wynika z tego, że zapewniona jest transmisja 100 Mb/s, co tłumaczy niskie opóźnienie w porównaniu z kolejnymi modelami połączeń.

Wartość opóźnienia w przypadku połączenia bezprzewodowego jest większa od wartości dla dwóch wcześniej omówionych modeli. Zależy to od wielu czynników, a przede wszystkim od środowiska propagacji oraz odległości, na jaką sygnał będzie przenoszony. Ze środowiskiem związane jest osłabienie sygnału spowodowane przez przeszkody znajdujące się na drodze transmisji, odbicia sygnałów od przeszkód oraz zakłócenia wywołane przez inne sygnały elektryczne. Kanały radiowe wykorzystywane lokalnie mają zasięg od 10 do kilkuset metrów. Podsumowując, można powiedzieć, że błędy bitowe występują dużo częściej w łączach bezprzewodowych niż w przewodowych, stąd też być może bierze się zwiększona wartość opóźnienia. Badania przeprowadzono przy wykorzystaniu rutera bezprzewodowego z wbudowanym punktem dostępowym sieci bezprzewodowej oraz adaptera USB podłączonego do komputera. Każda stacja bezprzewodowa musi związać się z punktem dostępowym, zanim będzie mogła wysłać lub odbierać dane. Wyniki pomiarów dla trzech różnych ustawień sieci bezprzewodowej przedstawione zostały w sposób graficzny na rys. 7. Zaobserwowano, że wartość opóźnienia rośnie wraz ze zmniejszeniem zasięgu działania sieci bezprzewodowej (z 86% na 58%) oraz przy obciążeniu sieci poprzez wyświetlanie na wielu komputerach tego samego obrazu z kamery. Szybkość transmisji dla tych ustawień wynosiła 36 Mb/s (wskazania oprogramowania). W rzeczywistości szybkość ta jest mniejsza (ok. 20 Mb/s) i zmienia się wraz ze zmianami wywołanymi przez wyżej wymienione czynniki.

Kolejny model połączenia sieciowego to łączność bezprzewodowa powiązana z siecią światłowodową. W przeciwieństwie do poprzedniego modelu w badaniach wykorzystano dwa przełączniki. Wiąże się to z dodatkowym opóźnieniem spowodowanym przejściem pakietów przez kolejny przełącznik. Jednak głównym czynnikiem znacznego (w porównaniu do wszystkich poprzednich modeli połączeń) wzrostu opóźnienia jest mały zasięg (42%) oraz korzystanie ze standardu 802.11b

Italians Do It Better

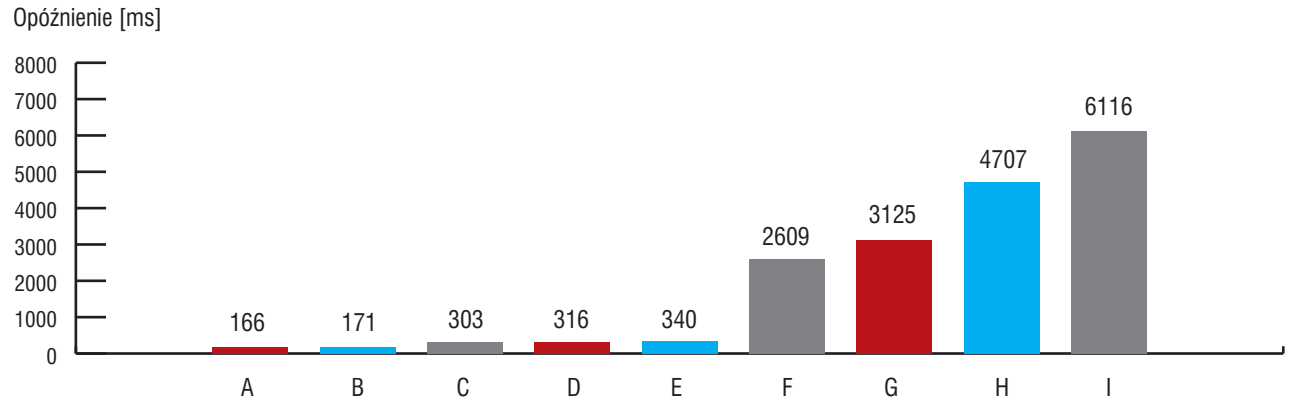
ULISSE COMPACT

Dzięki swojej zwartej i zdecydowanej sylwetce ULISSE COMPACT umożliwia ciągły obrót z dużą prędkością, bezwzględną dokładność ustawienia i większą jakość obrazu oraz ekstremalną wytrzymałość i uproszczoną konfigurację systemu.

ULISSE COMPACT jest idealnym rozwiązaniem w przypadku wymagających zastosowań zabezpieczających i monitorowania na zewnątrz budynków.

VIDEOTEC

VIDEOTEC S.p.A. CCTV PRODUCTS **WWW.VIDEOTEC.COM** | **HEADQUARTERS ITALY**: Tel. +39 0445 697411 - info@videotec.com | **FRANCE:** Tel. +33 2 32094900 - info@videotec-france.com
UK/IRELAND: Tel. +44 01353 775438 - uksales@videotec.com | **U.S.A./CANADA:** Tel. +1 973 5950788 - usasales@videotec.com | **ASIA PACIFIC:** Tel. +852 2333 0601 - info@videotec.com.hk



Rys. 7. Wykres średniego opóźnienia w zależności od modelu połączenia sieciowego. Połączenie: A – z zastosowaniem światłowodu, B – z zastosowaniem skrętki miedzianej, C – bezprzewodowe (86%, 36 Mb/s), D – bezprzewodowe (86%, 36 Mb/s, obciążenie), E – bezprzewodowe (58%, 36 Mb/s), F – bezprzewodowe (42%, 11 Mb/s, obciążenie) + światłowodowe, G – z zastosowaniem modemów (512 kb/s), H – z zastosowaniem modemów (256 kb/s), I – z zastosowaniem modemów (128 kb/s).

sieci bezprzewodowej, co wiąże się ze zmniejszeniem szybkości transmisji do ok. 5 Mb/s [1]. Teoretycznie pasmo tego rozwiązania wynosi 11 Mbps. Średnie opóźnienie w tym przypadku wynosi 2609 ms, a więc istnieje nawet możliwość niezauważenia zdarzenia wywołanego przed kamerą.

Modelem połączenia sieciowego, który na pewno nie powinien mieć zastosowania w systemach telewizji dozorowej, gdyż charakteryzuje się bardzo dużym opóźnieniem, jest model wykorzystujący modemy połączone zwykłym kablem telefonicznym obustronnie zakończonym złączem RJ-11. Do realizacji takiego połączenia w laboratorium wykorzystano modemy Alfa 1 firmy Goramo wraz z mostami Beta 1, dzięki którym możliwe jest ich podłączenie do przełączników sieciowych za pomocą skrętki UTP. Dwa modemy (master oraz slave) umożliwiają przesyłanie sygnałów z różnymi prędkościami. Badania przeprowadzono dla trzech prędkości: 512 kb/s, 256 kb/s oraz 128 kb/s. Naturalnie, wraz ze zmniejszaniem prędkości opóźnienie przesyłanego obrazu wizyjnego gwałtownie rośnie (rys. 7). Dla najniższej prędkości wyniosło ono ponad 6 s. Wysokie opóźnienie dla tego typu połączenia jest wynikiem przede wszystkim małej szybkości transmisji danych. Istnieje duże prawdopodobieństwo, że przejście osoby przed kamerą nie zostanie wyświetlone na monitorze operatora.

Z badania modeli połączeń sieciowych można wywnioskować, że dla systemów monitorowania najlepszym rozwiązaniem, jak podpowiada intuicja, są połączenia z zastosowaniem światłowodu oraz skrętki miedzianej. Gwarantują one niskie opóźnienie przesyłu obrazu wizyjnego, a więc szybszą reakcję na zaistniałe zdarzenie. Sieci bezprzewodowe sprawdzają się na niewielkich odległościach, gdy zasięg ich działania oraz szybkość transmisji są na tyle duże, aby można było bez zakłóceń przesłać obraz wizyjny. Jednak czasami instalatorzy nie mają wpływu na to, do jakiej sieci będzie podłączony system, w związku z tym najlepszym rozwiązaniem byłoby korzystanie z łączy dedykowanych, zapewniających niezawodną łączność i gwarantowane duże pasmo przepustowości.

Podsumowanie

Mając na uwadze, że sieciowy monitoring wizyjny jest systemem bezpieczeństwa, nie należy podczas analizy opóźnień skupiać się wyłącznie na opóźnieniach samego protokołu TCP/IP. Dlatego zaprojektowano i wykonano stanowisko laboratoryjne, które zapewnia pomiar z punktu widzenia operatora. Opóźnienie jest mierzone jako różnica czasu pomiędzy rzeczywistym zdarzeniem wywołanym przed kamerą sieciową a czasem, po którym to zdarzenie pojawi się na ekranie operatora.

Zaprojektowane stanowisko laboratoryjne pozwala na przeprowadzenie dwóch rodzajów badań pod względem opóźnienia przesyłanego obrazu wizyjnego:

– badania wybranych modeli kamer sieciowych,

– badania wybranych modeli połączeń sieciowych.

Analizując pierwszy rodzaj pomiarów, zaobserwowano, że istotny wpływ na wartość czasu potrzebnego na przesłanie danych mają parametry kamer, takie jak rozdzielczość obrazu i standard kompresji. Pomiary wykonano dla siedmiu kamer sieciowych. Sprawdzono również wartości opóźnień w przypadku zmiany monitora oraz komputera PC.

Badania modeli połączeń sieciowych wykazały, że są one głównym czynnikiem, mającym największy wpływ na wartość opóźnienia. Pomiary wykonane dla pięciu typów układu połączeń wskazują na to, że najlepszym sposobem dla systemu monitorowania jest zastosowanie skrętki miedzianej bądź światłowodu. Charakteryzują się one niewielkim opóźnieniem i najlepszą stabilnością w stosunku do innych badanych topologii sieci.

Na podstawie pomiarów zrealizowanych na wykonanym stanowisku laboratoryjnym oraz po podsumowaniu ich wyników można stwierdzić, że nadal celowe pozostaje zadanie pytania: czy kamera internetowa aby na pewno pokazuje to, co się aktualnie dzieje? Czytelnik, znając niedomagania sieci ethernetowej w naszym kraju, może zadać sobie pytanie: czy sensowne jest zastosowanie sprzętu, który w czasie transmisji obrazu zgubi informację o zaistniałym zdarzeniu i nawet nikt o tym nie zostanie poinformowany?

dr inż. Marek Życzkowski
mgr inż. Łukasz Stawicki

Bibliografia:

1. James F. Kurose, Keith W. Ross.: *„Sieci komputerowe. Od ogółu do szczegółu z Internetem w tle”*. Wydawnictwo Helion, Gliwice 2006.

Świat IP coraz bliżej.

SONY

Najnowsze oprogramowanie Real Shot Manager Advanced dostaniesz w prezencie przy zakupie dowolnych 4 kamer IP. Jest to autorskie oprogramowanie Sony stworzone do monitoringu. W połączeniu z kamerami IP Sony dostajecie Państwo gwarancje, serwis oraz Prime Support*. Ponadto łącząc inteligentną analizę wideo, alarmy na żądanie i wiele innych funkcjonalności, Real Shot Manager Advanced zapewnia bezpieczeństwo na najwyższym poziomie oraz daje możliwość wprowadzenia klienta w świat IP.

*Prime Support coś więcej niż gwarancja, zamiana uszkodzonego sprzętu na sprawny w ciągu trzech dni!!!

Chcesz wiedzieć więcej, skontaktuj się z nami:
www.sonybiz.pl

IPELA

GO Advance

RealShot Manager to oprogramowanie dobrze znane osobom pracującym z kamerami IP marki Sony. Doczekało się ono premiery wersji zaawansowanej, która uwzględnia uwagi użytkowników wersji standardowej poprzez dodanie szeregu udogodnień zwiększających efektywność pracy operatorów. RealShot Manager Advanced dostępny jest jako aplikacja dla systemu operacyjnego Windows lub jest wbudowany w nową serię rejestratorów sieciowych NSR (NSR-1050H, NSR-1100 i NSR-1200). Co ważne, rozwiązania te są ze sobą kompatybilne – na urządzeniach z serii NSR-1000 pracuje dokładnie ta sama aplikacja RSM Advanced, tyle że w wersji dla platformy Linux. W niniejszym artykule przybliżymy kilka kluczowych cech nowej platformy software'owej marki Sony

Prosty setup i łatwe użytkowanie

W porównaniu z poprzednią wersją aplikacja RealShot Manager Advanced (RSM Advanced) posiada wiele nowych udogodnień. Jedną z nich jest automatyczna rejestracja kamer w systemie. Rejestrację dowolnej liczby kamer wraz z ustawieniem dla nich harmonogramu nagrywania można w RSM Advanced wykonać w niecałą minutę! Siatka z podglądami obrazów z kamer jest automatycznie tworzona i dopasowywana do rozdzielczości monitora. Oczywiście wciąż można tworzyć swoje własne schematy podglądu obrazów.

Kolejną ciekawostką jest zupełnie nowa obsługa kamer za pomocą myszy. W RSM Advanced wystarczy kliknąć na dowolny obszar obrazu kamery, aby stał się on środkiem obserwowanego obrazu. Za pomocą myszy można też sterować funkcją *zoom*. Poprzez zaznaczenie na obrazie prostokątnego obszaru wymuszamy na kamerze automatyczny zoom i wyśrodkowanie kadru.

Rozbudowany został również moduł wyszukiwania nagrań, dzięki czemu oprogramowanie pozwala na wyszukiwanie według wielu kryteriów. Wyszukane nagrania (które często mogą być bardzo krótkie) można połączyć w jeden film i oglądać go w trybie przyśpieszonym. Nagrania można eksportować do powszechnie akceptowalnych formatów.

Aplikacja RSM Advanced wyręcza operatorów monitoringu w wielu czynnościach, dzięki czemu przeciwdziała ich szybkiemu znużeniu. Po pierwsze odróżnia ona alarm od zdarzenia. Nie każde wykryte przez kamerę zdarzenie musi być traktowane jako alarm przykuwający uwagę operatora. W pewnych warunkach wykryty ruch nie będzie powodował alarmowania, za to może być nagrany jak alarm. Jeśli przykładowo monitorujemy korytarze w centrum handlowym, to ruch wykryty w godzinach otwarcia centrum nie zostanie potraktowany jako zdarzenie alarmowe, będzie jednak nagrywany. Ruch wykryty po zamknięciu centrum też jest nagrywany, ale wtedy będzie już wywoływać alarm przykuwający uwagę operatora. Po drugie, obraz z kamery wykrywającej alarm można przekierować na oddzielnie zdefiniowany monitor (ang. *Hot Spot*).

Jedną z nowych funkcji w oprogramowaniu jest definiowanie akcji systemu monitoringu dla określonych zdarzeń. Możemy na przykład stworzyć schemat z podglądem kamery skierowanej na drzwi, a obok ikony kamery umieścić ikonę przycisku do otwierania drzwi. Jeśli na obrazie z kamery zobaczymy osobę uprawnioną do wejścia, możemy kliknąć na ikonę przycisku otwierania, co spowoduje wysłanie impulsu do systemu kontroli dostępu otwierającego drzwi.

W celu poznania innych nowych funkcji RSM Advanced prosimy o kontakt z producentem.

Rejestratory serii NSR-1000 – GO HYBRID

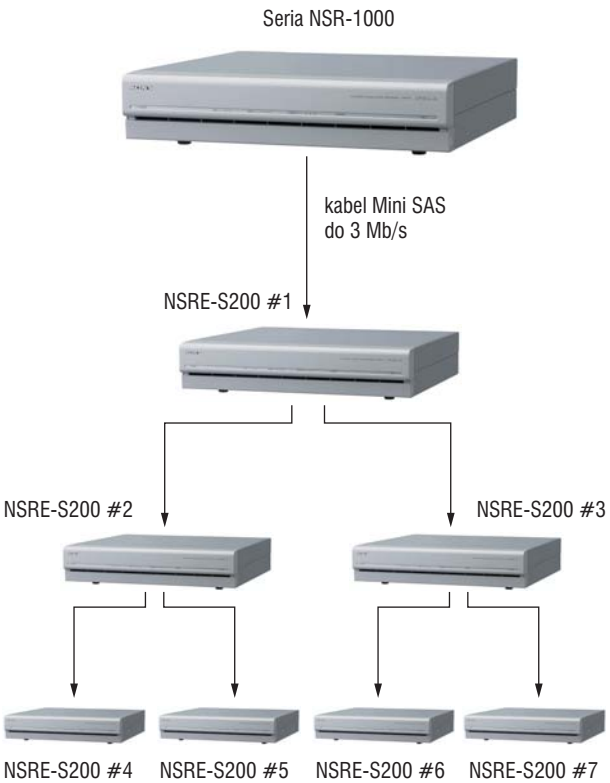
Nowe rejestratory sieciowe (wyposażone w RealShot Manager Advanced dla systemu Linux) są dostępne w trzech wersjach: NSR-1050H, NSR-1100 i NSR-1200. Pomagają one przejść w sieciach IP z rozwiązań analogowych na cyfrowe w sposób płynny i ekonomicznie efektywny, co jest głównym celem prowadzonej przez firmę Sony kampanii „GO HYBRID". Wszystkie modele NSR-1000 (oprócz pełnej obsługi kamer IP) pozwalają na podłączenie kamer analogowych bez wykorzystywania dodatkowych urządzeń (np. konwerterów). Główne różnice

pomiędzy poszczególnymi urządzeniami przedstawia poniższa tabela. Pierwszy wymieniony model pozwala standardowo na podłączenie maksymalnie 16 kamer analogowych. Za pomocą zaawansowanych filtrów wykrywających zdarzenia (np. przekroczenie linii, zniknięcie obiektu czy zgromadzenie się określonej grupy osób) obraz z kamer analogowych będzie podlegał analizie pozwalającej na detekcję ruchu oraz obróbkę. Kamery IP Sony podłączone do NSR-a mogą wysyłać do niego obraz w celu rejestracji czy też wtórnej analizy obrazu, ale w przypadku kamer cyfrowych bazowanie na ich własnej wbudowanej inteligencji jest dużo bardziej efektywne. W takim przypadku kamery odciążą rejestrator sieciowy od zaawansowanej analizy obrazu i stworzą z innymi urządzeniami system rozproszonej inteligencji (platforma DEPA).

Otwarta platforma

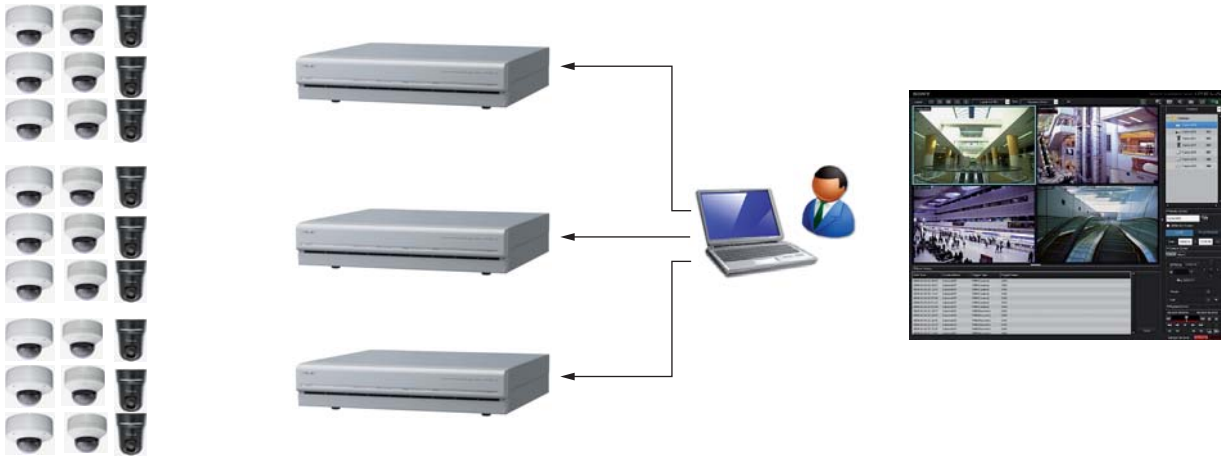
Aplikacja RSM Advanced dla platformy Windows pozwala na współpracę z urządzeniami NSR z serii 1000. Dzięki niej może mieć miejsce taka na przykład sytuacja, że w każdym sklepie należącym do sieci handlowej X zainstalowanych jest dziesięć kamer analogowych oraz dziesięć kamer sieciowych. Kamery połączone są z NSR-1050H znajdującym się w sklepie, na tym urządzeniu rejestrowane są też nagrania. Osoba odpowiadająca za bezpieczeństwo może połączyć się z NSR-em w dowolnym sklepie, może ponadto zarządzać kamerami, przeglądać nagrania czy też przekonfigurować ustawienia. Wszystko to może wykonać za pomocą bezpłatnej aplikacji klienckiej RSM Advanced. W przypadku większej liczby kamer można użyć kilku urządzeń NSR (lub komputerów z serwerową wersją RSM Advanced) i przechowywać centralną bazę użytkowników na jednym z nich. System uprawnień użytkowników pozwala na bardzo zaawansowane dostosowanie uprawnień do niemal każdego typu monitorowanych obiektów. Jeśli okaże się, że pojemności dysków w rejestratorach NSR nie są wystarczające, wówczas do każdego rejestratora można podłączyć kaskadowo siedem zewnętrznych macierzy dyskowych Sony (2 TB każda).

W przyszłości RealShot Manager będzie wspierał standard ONVIF, który umożliwi obsługę kamer czołowych producentów (w tym Sony) przez ten sam interfejs. Obecnie kamery niemal każdego producenta są obsługiwane inaczej i w każdym oprogramowaniu dedykowanym dla systemów monitoringu należy je osobno definiować. Mimo, że na zakończenie prac nad standardem ONVIF należy jeszcze poczekać, w najnowszej wersji RealShot Manager Advanced będzie obsługiwał wszystkie modele kamer Axis. Już w tej chwili RSM Advanced obsługuje pięć najpopularniejszych modeli kamer sieciowych tego producenta.

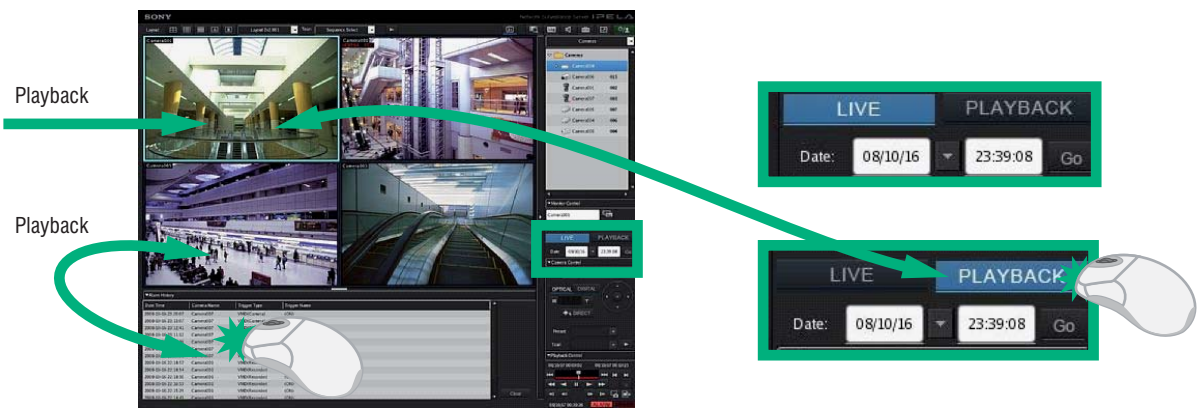


Rys. 1. Rozbudowa powierzchni dyskowej NSR serii 1000 o kolejne zewnętrze dyski

Cecha	NSR-1200	NSR-1100	NSR-1050H
Wewnętrzna pamięć	2 TB (500GB x 4)	1 TB (500GB x 2)	500 GB (500GB x 1)
RAID	RAID 5	RAID 0	-
Liczba kamer	64	32	20
Wejście analogowe	W standardzie nie, przy zastosowaniu karty NSBK -A16 - tak (16 wejść analogowych)		Tak (16 wejść analogowych)
	4CIF/2CIF/CIF x 16 wejść na jednej karcie, kodowanie w MPEG4, maksymalnie 4CIF, 100 fps (100 obrazów/s)		
Wyjście analogowe RGB	Tak (2 wyjścia)		
HDMI	Tak (2 wyjścia)		
SAS Interface	Tak		
Port GbE	x 4 (logiczne x3) (#3,#4 Channel Bond)		
Włącznik zasilania	x1		
AC inlet	x1		
USB	USB 2.0 x3		
Wyjście audio L/R	x1		
Wejście mikrofonowe	x1		
Wejście dla konektora kamer analogowych (opcjonalne)	DVI x1 (do przyłączenia 16 kanałów wideo (BNC) i 4 kanałów audio)		
Zewnętrzne macierze I/F	Mini SAS x1 / iSCSI x1(v1.1)		
Wejście/wyjście alarmowe	8 wejść / 8 wyjść		
Obsługiwane protokoły	RS232C x1(UPS)		
	RS232C/422/485 x1(PTZ)		



Rys. 2. Możliwy schemat działania rozproszonych instalacji wielokamerowych



Rys. 3. Łatwy dostęp do nagrań, odtwarzanie i podgląd na żywo równocześnie

Obsługa w języku polskim

Pod koniec maja 2009 r. bardzo popularne w Polsce oprogramowanie RealShot Manager będzie dostępne także w językach polskim i portugalskim. Dotychczas dostępne są wersje w językach: angielskim, japońskim, chińskim, niemieckim, francuskim, hiszpańskim, włoskim i rosyjskim.

Podsumowanie

Firma Sony rozpoczęła nową kampanię GO HYBRID, która przyczyniła się do wprowadzenia serii rejestratorów sieciowych NSR-1000, dedykowanych zarówno dla rozwiązań hybrydowych (analogowo-cyfrowych), jak i rozwiązań standardowych w sieciach IP. Rejestratory są wyposażone w zupełnie nowe oprogramowanie RealShot Manager Advanced, dostępne również jako samodzielna aplikacja dla platform Windows. Użytkownikom ceniącym efektywność i wygodę obsługi oprogramowanie to na pewno przypadnie do gustu. Systemy bazujące na tych rozwiązaniach można ze sobą łączyć w niemal dowolny sposób, a w przyszłości będą one współpracowały z rozwiązaniami innych wiodących producentów. Pod koniec maja RSM Advanced będzie dostępny w wersji polskiej. Do końca czerwca obowiązuje promocja – kupując dowolne cztery kamery sieciowe Sony, można bezpłatnie otrzymać 4-kamerową licencję na RealShot Manager Advanced.

Marta Małecka
Jacek Gawrych
Sony Poland

C & C

DYSTRYBUTOR ROKU 2008

TH GROUP

NOWA SERIA KAMER SZYBKOOBROTOWYCH
SAMSUNG TECHWIN

SAMSUNG TECHWIN

KAMERY SPD 3750T / 3750 / 3350 / 3700T / 3700 / 3310 / 2700 / 2510

- maks. zoom optyczny: 37x
- maks. zoom całkowity: 444x
- rozdzielczość: 550 TV Kolor / 680 B&W
- funkcja Auto Tracking (wersja T)
- 255 ustawień PRESET
- cyfrowy Auto Flip
- maks. szybkość obrotu: 500°/s
- wejścia/wyjścia alarmowe

Autoryzowany dystrybutor Samsung Techwin w Polsce: C&C Partners Telecom Sp. z o.o.
ul. 17 Stycznia 119, 121, 64-100 Leszno, tel. (0) 65 525 55 55, fax (0) 65 525 56 66, e-mail: cctv@ccpartners.pl

Biura Handlowe: Leszno, e-mail: leszno@ccpartners.pl / Gdańsk, e-mail: gdansk@ccpartners.pl
Katowice, e-mail: katowice@ccpartners.pl / Warszawa, e-mail: warszawa@ccpartners.pl

Zyskaj więcej

dzięki instalacji profesjonalnych rozwiązań systemów zabezpieczeń firmy

Samsung Techwin

Nigdy dotąd klienci nie mieli tak ogromnego wyboru wśród wielkiej liczby producentów z całego świata, którzy walczą o udział w rynku telewizji dozorowej. Jednocześnie spadły ceny, a to stanowi oczywiście wspaniałą wiadomość dla klientów, którzy w obecnej trudnej sytuacji gospodarczej poszukują możliwości maksymalnego wykorzystania posiadanych do dyspozycji środków kapitałowych na urządzenia zabezpieczające

Niestety obecnie na rynku dostępnych jest wiele tanich urządzeń, które „dziś są, a jutro ich już nie ma". Instalatorzy systemów zabezpieczeń często skarżą się, że po zakupieniu urządzeń telewizji dozorowej od małych i nieznanych producentów nie mogą zamówić dodatkowych urządzeń, ponieważ zaprzestano produkcji danej linii. Tanie produkty mogą też oznaczać zawodność, niewielką fachowość pomocy technicznej oraz niską jakość samego wyrobu. Urządzenia telewizji dozorowej mają w założeniu pracować nieprzerwanie przez siedem dni w tygodniu – nic więc dziwnego, że produkty o niższej jakości nie wytrzymują dłużej niż rok, a kiedy dojdzie do awarii, nie można uzyskać pomocy technicznej, co grozi powstaniem długich przerw w pracy instalacji zabezpieczającej.

Coraz liczniejsza grupa instalatorów przekonuje się natomiast do korzyści, jakie daje współpraca z firmą Samsung Techwin. Firma jest jedną z najszybciej rozwijających się w Europie w dziedzinie profesjonalnych urządzeń zabezpieczających, oferującą pełen zakres najwyższej jakości urządzeń elektronicznych po bardzo konkurencyjnych cenach (nawet w porównaniu do cen najmniej znanych producentów). Firma szybko zdobywa doskonałą reputację także ze względu na oferowane wsparcie techniczne, które chroni i wspiera instalatorów.

– *Skupiamy się całkowicie na dążeniu do zajęcia czołowej pozycji wśród markowych firm w dziedzinie profesjonalnych urządzeń zabezpieczających w Europie, co wiąże się z oferowaniem najwyższej klasy produktów po konkurencyjnych cenach* – mówi Zuzana Adamova, menedżer ds. telewizji dozorowej na Europę Wschodnią w firmie Samsung Techwin. – *Rozmowy z instalatorami świadczą o tym, że są oni zaskoczeni niskim kosztem przejścia od produktów nieznanej marki do naszych wyrobów. Po uwzględnieniu trwałości produktu i oferowanego przez nas wsparcia koszt ten zmienia się wręcz w oszczędność. Oznacza to*

również, że dbamy nadzwyczaj o zapewnienie dostępności naszych produktów zgodnie z potrzebami klientów. Posiadamy własny europejski magazyn zapasów, a nasze produkty można zakupić za pośrednictwem sieci czołowych dystrybutorów urządzeń bezpieczeństwa, co zapewnia doskonałą dostępność oraz szybką dostawę produktów.

Dodatkowy pakiet od firmy Samsung Techwin

Firma Samsung Techwin oferuje imponujący pakiet wsparcia, obejmujący bezpłatny projekt systemu, bezpłatną pomoc techniczną i pełną trzyletnią gwarancję na cały zakres produktów.

Gary Fletcher-Moore został powołany na stanowisko europejskiego menedżera ds. technicznych w kwietniu 2008 r. Nadzorował on znaczące inwestycje, zmierzające do wzmocnienia zespołów przed- i posprzedażowej pomocy technicznej oraz serwisu Samsung Techwin. – *Nasze produkty charakteryzują się wysokim stopniem niezawodności, dlatego nie boimy się oferować trzyletniej gwarancji, a dodatkowo zobowiązujemy się do naprawy usterek w terminie pięciu dni, aby jak najszybciej usunąć problem w przypadku jakiejkolwiek awarii. Obecnie średni czas naprawy wynosi cztery dni, a w przyszłości zamierzamy jeszcze usprawnić ten proces. Wszystko to jest częścią naszego dążenia, by być najlepszą firmą w branży* – wyjaśnia Gary. – *Inwestujemy także we wsparcie lokalne na terenie całej Europy, aby pomagać klientom bez względu na lokalizację.*

Za pośrednictwem sieci dystrybutorów w całej Europie firma Samsung Techwin zamierza pomóc firmom instalatorskim w zwiększeniu ich zysków poprzez zdobywanie nowych i zatrzymywanie dotychczasowych klientów. – *W ciągu ostatnich dwunastu miesięcy zatrudniliśmy profesjonalny i wykwalifikowany zespół ds. sprzedaży na Europę, który świadczy usługi przed- i posprzedażowe dla rosnącej rzeszy naszych klientów* – mówi Zuzana Adamova. – *Wszyscy członkowie zespołu to specjaliści z dziedziny telewizji dozorowej, których entuzjazm i wiedza są bardzo cenione i podkreślają nasze zaangażowanie na rzecz wysokiego poziomu wsparcia dla naszych klientów.*

Technologia superredukcji szumów Samsung (SSNR) stosowana jest wyłącznie we wszystkich kamerach i kamerach kopułkowych firmy Samsung Techwin. Technologia opracowana w celu eliminacji szumów obrazu w warunkach słabego oświetlenia umożliwia zaoszczędzenie niemal 70% miejsca na dysku twardym i maksymalizację szerokości pasma sieci, co pozwala na przekazywanie większej liczby klatek na sekundę i poprawę jakości obrazu.

Linia kamer SPD z głowicą zintegrowaną posiada podstawy montażowe z możliwością szybkiej wymiany. Są one wyposażone we wbudowaną pamięć, która pozwala na korzystanie z rozwiązań elastycznego nadzoru na terenie zakładu, tj. częstego przenoszenia kamer z jednej podstawy montażowej na drugą. Różne ustawienia kamer można także zapisać w pamięci, dzięki czemu ustawienia danej kamery zostaną automatycznie zmienione po przeniesieniu w inne miejsce, tak aby zoptymalizować jakość przekazywanego obrazu. Niektóre modele wyposażono też w unikatowe w branży moduły umożliwiające 37-krotne zbliżenia optyczne, które przyczyniają się do jeszcze większej elastyczności zastosowań.

„Niemądrze jest płacić zbyt dużo, ale płacenie zbyt mało też się nie opłaca. Płacąc za dużo, stracimy część pieniędzy. To wszystko. Płacąc zbyt mało, można czasem stracić wszystko, ponieważ kupiony produkt może nie nadawać się do celów, dla których został nabyty. Podstawowe prawo biznesu zabrania zatem płacenia niewiele za dobry produkt. Nie da się tego osiągnąć. Do współpracy z osobą, która oferuje najniższą cenę, dobrze jest wkalkulować ryzyko. A po uwzględnieniu ryzyka okazuje się, że stać nas na kogoś lepszego."

John Ruskin (ekonomista)

Technologia umożliwiająca realną oszczędność kosztów

Koncentracja firmy Samsung Techwin na opracowaniu technologii oferującej istotne korzyści dla ochrony jest dostrzegalna praktycznie w każdej linii produktów.

Na przykład wszystkie nagrywarki cyfrowe SVR są w pakiecie oferowane wraz z bezlicencyjną kopią oprogramowania Systemu Centralnego Zarządzania (CMS), która umożliwia tworzenie gotowej sieci o szerokich możliwościach – darmowej obserwacji z wielu miejsc i przez wielu obserwatorów, sterowania oraz instalacji połączonych urządzeń Samsung Techwin. Produkty SVR posiadają także łatwe do wymiany dyski twarde i maksymalnie 32 kanały wejścia, co umożliwia obniżenie kosztów ewentualnej rozbudowy systemu bazującego na posiadanych już urządzeniach.

Samsung Techwin – rozwiązania systemów zabezpieczeń, które przerosną Twoje wyobrażenia

Firma Samsung Techwin cieszy się doskonałą reputacją w zakresie technologii, niezawodności i jakości, o czym świadczą przyznane niedawno nagrody i wyróżnienia branżowe. Posiada również szeroki zakres produktów dla telewizji dozorowej w konkurencyjnych cenach przy jednoczesnym zachowaniu wysokiej jakości, wydajności i niezawodności. Więcej informacji można uzyskać, kontaktując się telefonicznie z zespołem Samsung Techwin pod numerem +44 (0)1932 455 300 lub pisząc na adres e-mail *STEsecurity@samsung.com*

Samsung Techwin

Odmieniony Praesideo

Czterokrotnie szybciej działająca jednostka centralna, elektroniczna matryca przełączająca MCI (ang. *Multichannel Interface*), ekonomiczne wzmacniacze BAM (ang. *Basic Amplifiers*) klasy D oraz dowolna topologia linii głośnikowych to tylko część zmian wprowadzonych w ostatnim czasie do systemu Praesideo.

Przypomnijmy, że system cyfrowy Praesideo, obecny od ponad pięciu lat na polskim rynku, jako jeden z pierwszych otrzymał certyfikat Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej oraz został dopuszczony do stosowania jako dźwiękowy system ostrzegawczy w ochronie przeciwpożarowej budynków. Jego ogromne możliwości zaowocowały znaczną liczbą zakończonych sukcesem instalacji. Obecnie system Praesideo czuwa nad bezpieczeństwem milionów ludzi zarówno w Polsce, jak i w innych krajach.

Firma Bosch szybko dostosowuje się do nowych wymagań użytkowników. Dzięki rozszerzeniu funkcjonalności systemu oraz technicznym możliwościom ich realizacji firma wprowadziła na rynek kolejną, lepszą wersję Praesideo. Nowy kontroler sieciowy NC (ang. *Network Controler*), zachowujący kompatybilność z dotychczasowymi modelami wzmacniaczy, jest teraz szybszy i potrafi zarządzać nowymi modułami. Jednym z nich jest cyfrowa matryca przełączająca MCI, która pełni zadanie komunikacji z innymi elementami sieci oraz służy do rozdziału sygnałów audio i kierowaniu ich do wybranych stref.

Dodatkowym zadaniem matrycy jest monitorowanie poprawności działania dołączonych do niej wzmacniaczy BAM oraz linii głośnikowych. Należy zauważyć, że budowa linii głośnikowych może mieć teraz dowolną topologię. Linia głośnikowa ze względu na adresowalność układu kontroli linii może przybierać kształt zbliżony do układu naczyń krwionośnych w ciele człowieka, docierając w każde miejsce w najbardziej optymalny sposób. Ogranicza to koszty instalacji oraz umożliwia budowanie rozwiązań bardziej dopasowanych do potrzeb klienta. Warto wspomnieć, że kontrola linii głośnikowych nadal polega na zastosowaniu sprawdzonego sygnału pilota 20 kHz. Zatem, w przeciwieństwie do alternatywnie stosowanej metody kontroli linii wykorzystującej pomiar impedancji, tutaj nie występuje wymóg ograniczania liczby głośników w linii głośnikowej. Maksymalna konfiguracja nowego systemu Praesideo to 440 stref nagłośnieniowych dostarczających w sumie 160 kW mocy.

Wzmacniacze typu BAM operujące w klasie D ściśle współpracują z matrycą MCI. W porównaniu z dotychczasowym typem wzmacniaczy PAM (ang. *Power Amplifiers*) wyróżniają się niższą ceną przy jednoczesnym spełnieniu wszystkich wymagań stawianych systemom DSO. Wzmacniacze BAM nie komunikują się bezpośrednio z kontrolerem sieciowym NC, dzięki czemu ich konstrukcja jest mniej złożona. Budowa systemu DSO ze wzmacniaczami BAM to obniżenie kosztu systemu nawet o dwadzieścia pięć procent w porównaniu z konfiguracją z PAM. W obliczu takich oszczędności nie sposób przejść obojętnie obok nowych możliwości.

Nowością jest również numeryczna stacja wywoławcza, która umożliwia selektywne adresowanie dowolnej strefy systemu. W sytuacji zapewnienia selektywnego dostępu do 440 stref stosowanie stacji wywoławczych z tradycyjnymi przyciskami nie jest możliwe. Budowa takiego pulpitu wiązałaby się z koniecznością skonstruowania urządzenia o wysokości 5 m. Dzięki numerycznej stacji wywoławczej pulpit nadający komunikat do dowolnej z 440 stref jest niewielki i prosty w obsłudze.

Fot. 1. Klawiatura numeryczna systemu Praesideo

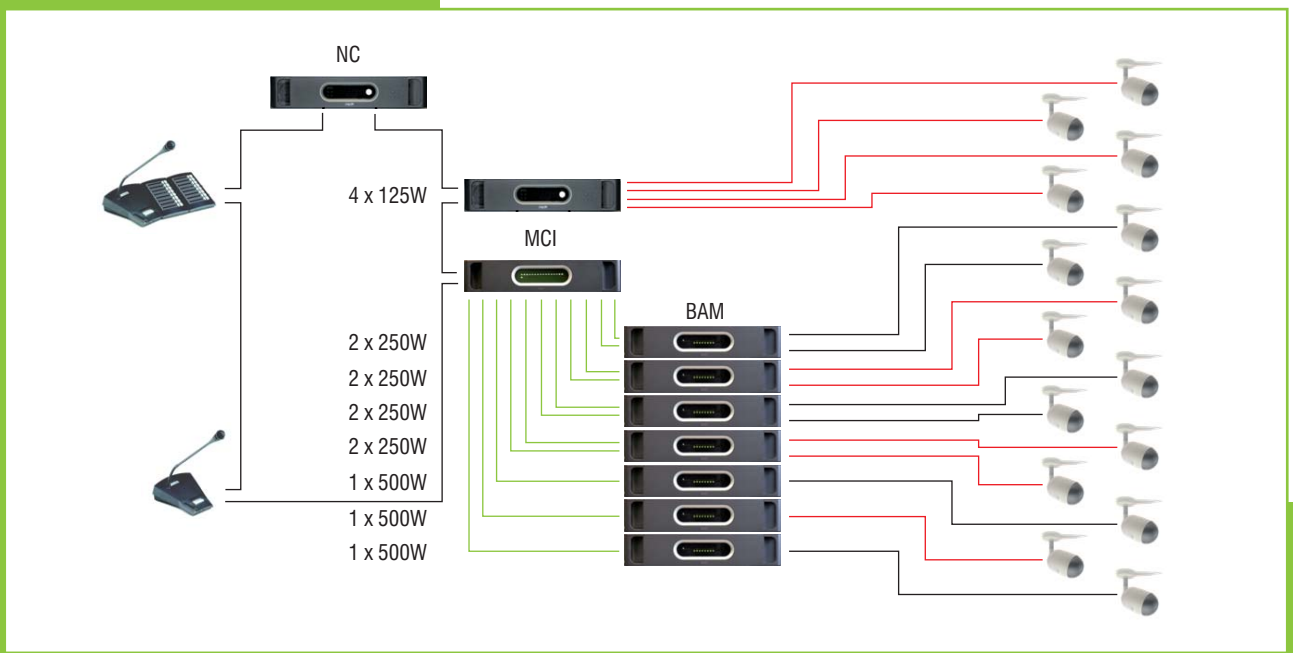
Fot. 2. Moduł pamięci wywołań „Call stacker"

Obsługa dużych systemów nagłośnienia przez wielu użytkowników jednocześnie zazwyczaj oznacza konflikt. Pojawia się on w przypadku żądania jednoczesnego dostępu do wybranej kombinacji stref przez np. dwóch operatorów. Aby wyeliminować tego typu niedogodności, firma Bosch proponuje zastosowanie w systemie zaledwie jednego pulpitu lub, co wygodniejsze, modułu pamięci wywołań, tzw. *call stacker*. Zadaniem *call stacker* jest buforowanie wszystkich wywołań odwołujących się do tej samej strefy. Nadanie ich z pamięci do wybranych przez operatorów stref następuje zgodnie z przyporządkowaną hierarchią ważności, czyli priorytetami. Wszystko dzieje się na tyle automatycznie i sprawnie, że użytkownik systemu nie zdaje sobie sprawy, iż jego komunikat napotkał problem dostępu do strefy. Wie natomiast, że komunikat został nadany zgodnie z przeznaczeniem i bez konieczności oczekiwania na zwolnienie zajętej strefy.

Dodatkową zaletą zastosowania modułu *call stacker* jest możliwość zapisania w jego pamięci treści komunikatu operatora. Po zakończeniu wypowiedzi operator może lokalnie odsłuchać nagrany komunikat i, w zależności od decyzji, wyemitować go lub poprawić. Niejednokrotnie jest to również jedyna możliwość uniknięcia sprzężenia zwrotnego w systemie DSO w przypadku trudnych warunków akustycznych w obszarze umiejscowienia pulpitu operatora. Dzięki innowacjom firmy Bosch wyeliminowany został problem spotykany w instalacjach DSO.

Znacznie więcej zmian i jeszcze więcej udogodnień odnajdziemy w oprogramowaniu systemu. Tworzenie interaktywnych paneli dotykowych operatora zawierających wizualizację nagłaśnianego obiektu czy też łączenie systemów przy użyciu sieci Internet to tylko fragment nowych możliwości. Dzięki wprowadzonym udoskonaleniom system ten jeszcze bardziej umocnił pozycję lidera wśród urządzeń DSO. Praesideo to symbol nowoczesnej technologii znacznie wyprzedzającej wymagania czasów, w których powstała.

Adrian Filip
Bosch Security Systems



Rys. 1. Nowe elementy systemu Praesideo – matryca MCI, wzmacniacze BAM

Szwajcarska jakość
systemów DSO

Rozwój cywilizacyjny oraz rosnące tempo życia generują wiele nowych zagrożeń, z którymi wcześniej się nie stykaliśmy. W natłoku codziennych spraw i zawrotnym tempie życia już nawet sobie nie uświadamiamy, jak często znajdujemy się w miejscach, gdzie narażone jest nasze życie lub zdrowie. Robiąc zakupy w supermarkecie, uczestnicząc w koncercie czy siedząc w kinie, nieświadomie wkraczamy w obszar, gdzie nasze życie może zależeć od prawidłowej organizacji procesu ewakuacji, a więc i od technicznych systemów, które ją wyzwalają. Chcemy jednak wierzyć, że jesteśmy bezpieczni i w sytuacji zagrożenia ktoś wyprowadzi nas poza zagrożony obszar. Aby tak się stało, konieczne jest wcześniejsze, właściwe zaprojektowanie wielu różnych technicznych systemów bezpieczeństwa, spośród których jednymi z istotniejszych są Dźwiękowe Systemy Ostrzegawcze (DSO). Zwiększając zagrożenia, współczesność wyposaża nas jednocześnie w technologie, które pomagają uchronić się przed nimi. Warunkiem powodzenia jest jednak stosowanie systemów niezawodnych i produkowanych ze „szwajcarską" precyzją…

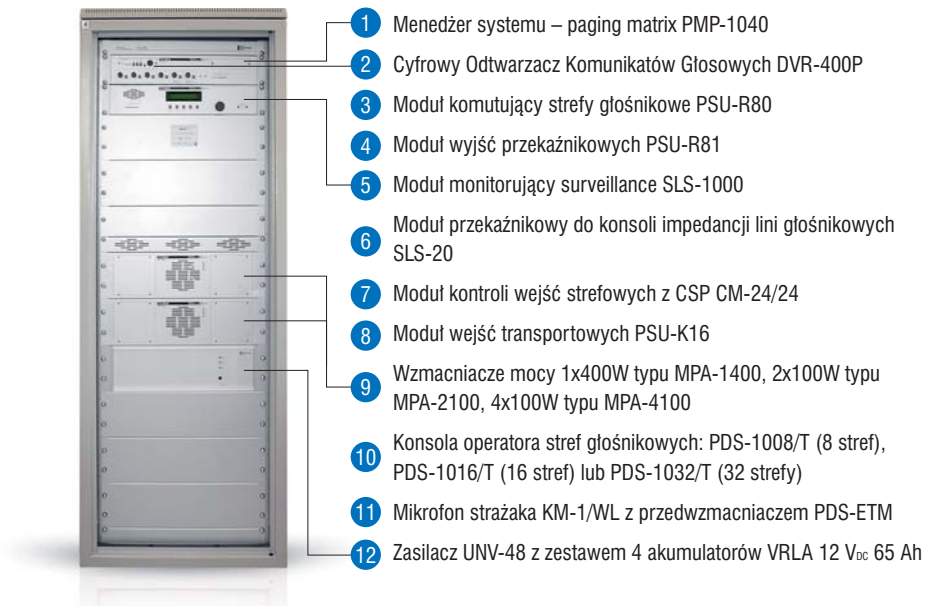
System PRODAS UNITON jest takim właśnie systemem. Produkowany przez szwajcarską firmę UNITON, która posiada wieloletnie doświadczenie i tradycję w zakresie elektroakustyki, daje gwarancję najwyższej „szwajcarskiej" jakości i niezawodności. Ciągły rozwój stosowanych technologii oraz szczególna szwajcarska dbałość o jakość oferowanych produktów owocują satysfakcją i zadowoleniem klientów w ponad 50 krajach na całym świecie. UNITON specjalizuje się szczególnie w budowie systemów nagłośnieniowych dużych obiektów – zarówno centrów handlowych, hoteli, jak i obiektów przemysłowych.

Dźwiękowy System Ostrzegawczy PRODAS UNITON (zgodny ze standardem PN-EN 60849) jest najnowszą ofertą firmy UNITON oraz jej polskiego partnera handlowego – firmy AAT Holding.

W przypadku pożaru lub innego zagrożenia PRODAS UNITON pozwala w sposób automatyczny (po otrzymaniu sygnału sterującego z Systemu Sygnalizacji Pożarowej – SSP) przekazywać komunikat do zagrożonych w obiekcie stref, co umożliwia sprawną ewakuację. Komunikaty nadawane z systemu mogą być odtwarzane z ich wcześniejszych nagrań lub podawane na żywo przez osobę kierującą akcją ratowniczą. PRODAS jako system ratujący ludzkie życie posiada wszystkie cechy wymagane przez PN EN 60849 – co znalazło potwierdzenie w Certyfikacie Zgodności 2651/2008 oraz Świadectwie Dopuszczenia 0346/2008, które zostały przyznane przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej (CNBOP).

Cechy tego systemu to:

– stałe nadzorowanie wszystkich elementów istotnych dla funkcjonowania DSO oraz automatyczne sygnalizowanie

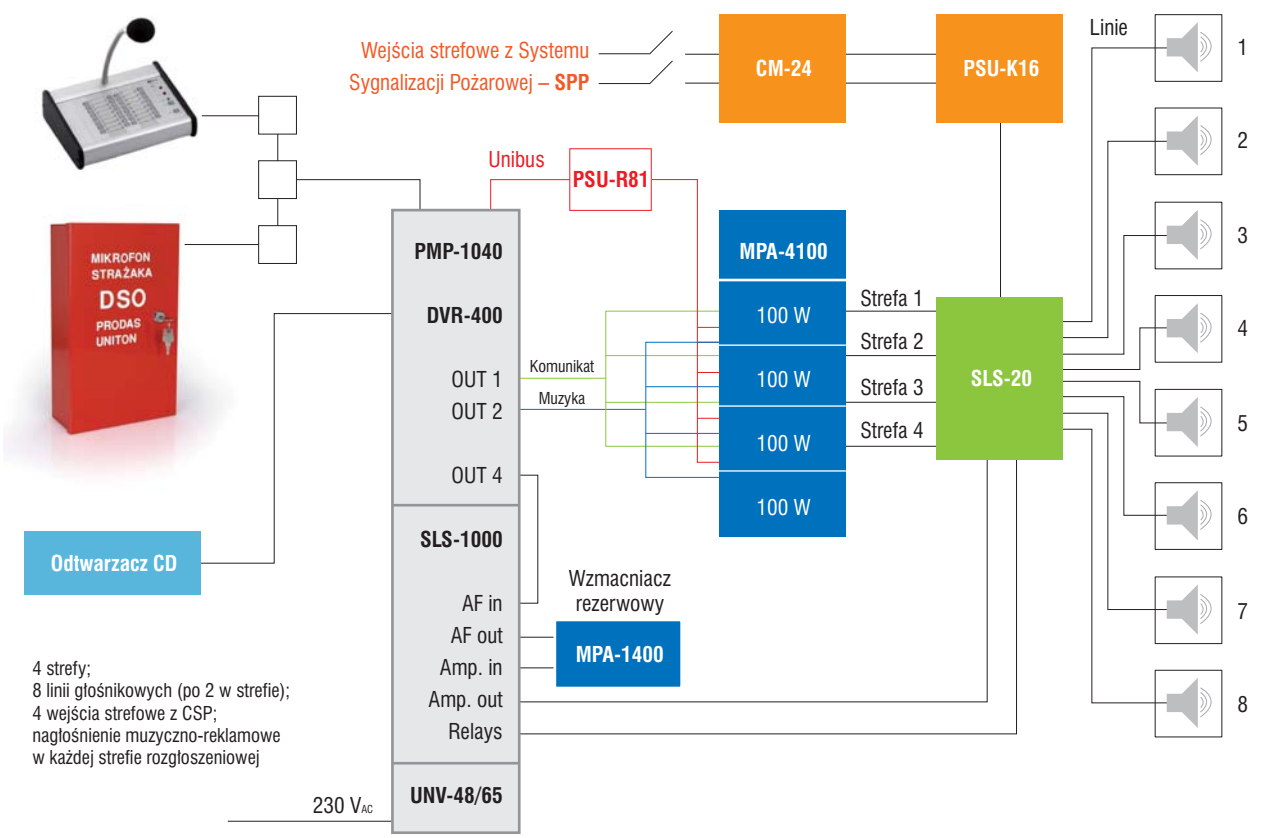


Rys. 1. Przykładowa konfiguracja systemu w szafie teleinformatycznej

ewentualnej usterki za pomocą sygnału dźwiękowego i świetlnego;
– wbudowany system zasilania awaryjnego, gwarantujący poprawną pracę systemu w przypadku awarii zasilania podstawowego;
– zbiór komunikatów ewakuacyjnych i ostrzegawczych zapisanych w pamięci nieulotnej systemu, które można automatycznie wyemitować w sytuacji zagrożenia;
– możliwość integracji z systemem wykrywania i sygnalizacji pożaru (do 32 niezależnych wejść strefowych).

Konfiguracja PRODAS UNITON jest tworzona indywidualnie dla każdego obiektu. Całość konfiguracji jest umieszczona w szafie teleinformatycznej (z wyłączeniem konsoli operatora oraz mikrofonu strażaka).

System PRODAS UNITON jest elastyczny i umożliwia ekonomiczny dobór liczby wzmacniaczy mocy w zależności od rozległości instalacji rozgłoszeniowej w obiekcie budowlanym. Na rys. 2 zaprezentowano przykładowo system dla czterech stref rozgłoszeniowych, zbudowany przy zastosowaniu jedynie dwóch wzmacniaczy mocy (w tym jednego rezerwowego). Zastosowany moduł wyjściowy PSU-R81 zapewnia selektywne załączanie dowolnej konfiguracji czterech składowych wzmacniaczy logicznych 100 W (po jednym dla każdej ze stref) tworzących wzmacniacz MPA-4100. Pozwala on również na przełączanie dwóch różnych wejść sygnałowych – komunikatów oraz nagłośnienia muzyczno-reklamowego.



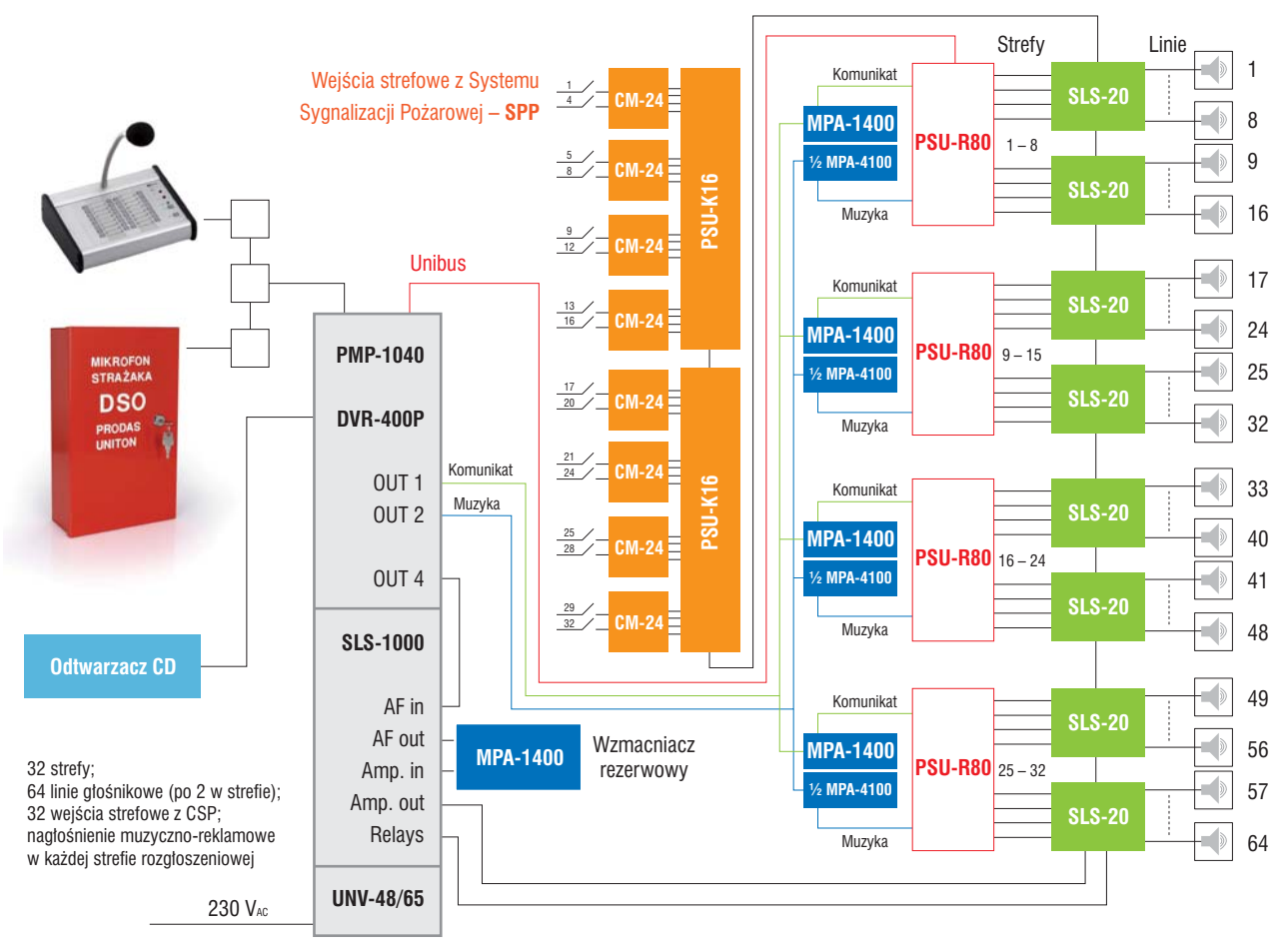
Rys. 2. Przykład konfiguracji dla obiektu 4-strefowego

Producent może pochwalić się systemami zrealizowanymi między innymi w następujących obiektach:
Obiekty handlowe
Migros (Szwajcaria), Coop (Szwajcaria, Szwecja, Niemcy); Woolworth (Niemcy); Globus (Szwajcaria); Jemoli (Szwajcaria); Einkaufszentrum (Szwajcaria)
Hotele
Maria Teresa (Kitzbuhl); Holiday Inn (Innsbruck); Sheraton (Lagos, Jeddah, Frankfurt); Radisson (Malmo); International (Wiedeń); Plaza (Kopenhaga); Holiday (Tunis); Adlon (Berlin)
Obiekty przemysłowe
UBS (Szwajcaria); ZKB Zuricher Kantonalbank (Zurich); Hoffmann La Roche AG (Bazylea); Nestle (Vevey); IBM Schweiz (Zurich); Nile City (Kair)

Rys. 3 przedstawia konfigurację systemu dla 32 stref rozgłoszeniowych. W tym przypadku zastosowanie znalazły cztery moduły komutujące strefy rozgłoszeniowe (każdy z nich posiada dowolną konfigurację – maksymalnie do ośmiu przypisanych mu stref). Rozwiązanie takie umożliwia znaczną redukcję liczby wzmacniaczy mocy (zastosowano ich łącznie tylko siedem, w tym jeden rezerwowy) poprzez odejście od zasady sztywnego przyporządkowania jednego wzmacniacza do jednej strefy bądź wręcz do jednej linii głośnikowej. Jeżeli efektywne zapotrzebowanie mocy w linii i strefie nie uzasadnia potrzeby wydzielenia dedykowanego wzmacniacza mocy, to moduł komutujący umożliwia załączanie do tego wzmacniacza więcej niż jednej strefy – bez utraty możliwości selektywnego rozgłaszania w strefach. Efekt ekonomiczny takiego rozwiązania jest oczywisty.

Dźwiękowy System Ostrzegawczy PRODAS UNITON ratuje ludzkie życie w przypadku pożaru lub innego zagrożenia (np. terrorystycznego). Do stref zagrożonych pożarem wysyłany jest automatycznie uprzednio nagrany i zapisany w pamięci nieulotnej komunikat głosowy, który ostrzega przed zagrożeniem lub wprost podaje właściwy sposób ewakuacji. Ponadto umożliwia przekazywanie „na żywo" adresowalnych komunikatów nadawanych z poziomu konsoli operatora – będących natychmiastową reakcją na dynamicznie zmieniającą się sytuację w trakcie ewakuacji ludzi z obiektu. Najwyższy priorytet ma komunikat rozgłaszany przez kierującego akcją ratowniczą przy wykorzystaniu mikrofonu strażaka. Oferowane przez system PRODAS UNITON rozwiązanie, umożliwiające komutowanie stref rozgłoszeniowych, redukuje liczbę niezbędnych wzmacniaczy mocy i przekłada się na ekonomiczne koszty centrali. Swój udział w wysokiej ocenie tego produktu ma również jego szwajcarska jakość oraz precyzja wykonania.

Krzysztof Kycia
Rafał Kowal
Dariusz Mieszkowski
AAT Holding

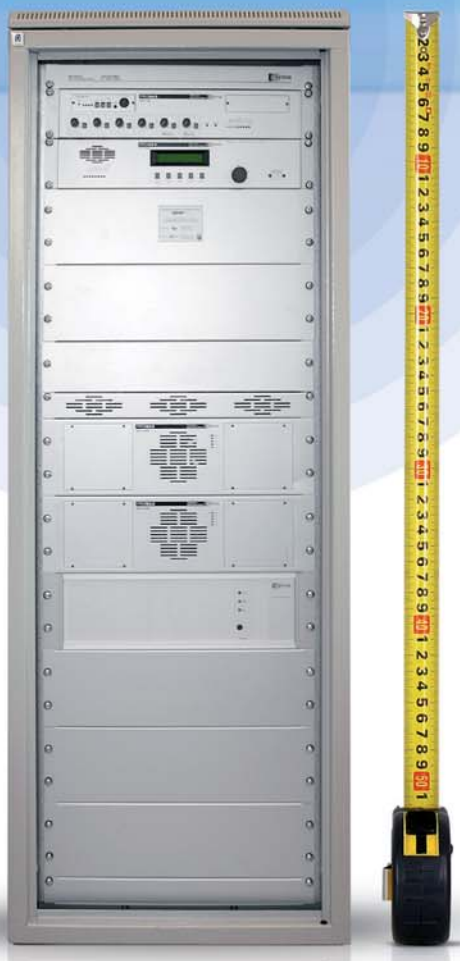


Rys. 3. Przykład konfiguracji dla obiektu 32-strefowego

DŹWIĘKOWY SYSTEM OSTRZEGAWCZY

PRODAS UNITON

szyty na miarę!



Oszczędny! Zastosowanie modułów komutujących strefy głośnikowe pozwala na ograniczenie liczby wzmacniaczy do niezbędnego minimum, co znacznie obniża koszty systemu

Sprawdzony! System spełnia wszystkie wymagania PN-EN 60849
(CNBOP: Certyfikat 2651/2008 i Świadectwo Dopuszczenia: 0346/2008)

Na miarę! Konfiguracje przygotowywane indywidualnie dla każdego obiektu

Wyłączny dystrybutor systemu PRODAS UNITON w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 022 546 05 46, faks 022 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

NEDAP to holenderski producent systemów kontroli dostępu. Firma powstała w Holandii w roku 1929, a obecnie zatrudnia na całym świecie ponad 660 pracowników. Główna siedziba firmy znajduje się w Groenlo we wschodniej Holandii. Firma posiada w różnych krajach rozbudowaną sieć spółek-córek; działa również poprzez tzw. sieć partnerską, w skład której wchodzą autoryzowani dystrybutorzy i instalatorzy. Idea opracowania systemu AEOS narodziła się w wyniku przeglądu zadań, które należało zrealizować podczas modernizacji i rozwoju systemów zabezpieczeń w poszczególnych organizacjach. Do sukcesu przyczyniła się również integracja tych organizacji w większe systemy, a w ich ramach zmodyfikowanie systemów zabezpieczeń oraz zwiększenie ich bezpieczeństwa

AEOS

nowe podejście do obsługi zabezpieczeń

Widok zestawu modułów systemu AEOS

Okazało się bowiem, że główną przeszkodą w integracji systemów zabezpieczeń obiektu w przypadkach reorganizacji, łączenia w większe organizmy itd. jest zazwyczaj konieczność wymiany całości lub znacznej części osprzętu i okablowania. Zwykle towarzyszy temu również konieczność przeorganizowania funkcji i procedur w systemie, co powoduje dodatkowe koszty i trudności. Jest to szczególnie ważne w przypadku łączenia organizacji, które dotychczas były wyposażone w oddzielne systemy, często pochodzące od różnych producentów lub dostawców. Dodatkowe trudności stwarza rozproszenie lokalizacji poszczególnych części organizacji, niejednokrotnie odległych od siebie o setki kilometrów.

Najprostszy przykład to rozwijająca się organizacja, w której znajduje się system zarządzania bezpieczeństwem obsługujący 64 przejścia i 999 kart. Po przekroczeniu tej granicy organizacja może napotkać poważny problem, ponieważ konieczne będzie wtedy zainstalowanie dodatkowego systemu, a przecież w wyniku ciągłego postępu system ten może posiadać już inne, niekoniecznie kompatybilne z obecnym, oprogramowanie. Jeżeli na dodatek w wyniku różnych działań rynkowych organizacja nasza zostanie włączona do struktur innej organizacji lub sama wchłonie inną organizację, wówczas prawie na pewno wymiana tradycyjnego systemu zarządzania bezpieczeństwem obiektu będzie nieunikniona. Pociąga to za sobą oczywiście znaczne koszty, a i czas poświęcony na zintegrowanie systemów będzie długi, nie wspominając już o najbardziej prawdopodobnej wymianie identyfikatorów w systemie.

System AEOS zaprojektowano jako odpowiedź na te wszystkie problemy. Przy jego opracowaniu zastosowano najnowsze osiągnięcia techniki komputerowej z wykorzystaniem internetu, otwarte (tzn. dostępne dla wszystkich) standardy przemysłowe oraz inteligencję rozproszoną. Przede wszystkim skoncentrowano się na tym, aby przenieść maksimum funkcji i operacji zarządzania systemem na jak najniższy, podstawowy poziom. Chodzi tu o uprawnienia dostępowe oraz zaprogramowane reakcje i działania systemu. Dzięki temu zarówno funkcjonowanie systemu, jak i poziom bezpieczeństwa uniezależniają się od dostępności sieci czy serwera. Wszystkie funkcje, takie jak *anti-passback* (zakaz ponownego użycia identyfikatora na wejściu bez uprzedniego opuszczenia obszaru), zliczanie gości czy zarządzanie garażem, są realizowane na podstawowym poziomie systemu i nie zależą od dostępu do serwera.

System AEOS, podobnie jak wszystkie inne systemy kontroli dostępu, również bazuje na sieci kontrolerów kontroli dostępu, kontrolerów drzwiowych, elementów wejściowych (takich, jak: czytniki kart, identyfikatory, przywieszki, pastylki, czytniki biometryczne itp.) oraz elementów wyjściowych (takich, jak: zamki do drzwi i bram, sygnalizatory, sterowniki trójnogów i in.).

Zasadnicze różnice w funkcjonowaniu tego systemu w porównaniu z wieloma innymi systemami polegają na tym, że:

a) to kontroler na najniższym poziomie za pośrednictwem dowolnej stacji roboczej PC systemu jest bezpośrednim odbiorcą informacji od operatora systemu;
b) kontrolery łączą się między sobą bezpośrednio (*peer-to-peer*) poprzez sieć TCP/IP, a nie poprzez serwer. Dzięki temu łączność między nimi nie zależy od dostępności serwera i przepustowości jego łącza;
c) dzięki wykorzystaniu łączy TCP/IP odpowiednio uprawniony pracownik (operator) może na bieżąco (w ramach swoich upoważnień) modyfikować zarówno uprawnienia dostępowe gości i pracowników, jak i reakcje systemu; modyfikacja ta może być wykonana z dowolnej nawet bardzo odległej stacji roboczej w sieci, a uprawnienia nie muszą być ograniczone tylko do pracowników działu ochrony lub HR.

System AEOS to nie tylko rozwiązania sprzętowe. To również (a może przede wszystkim) rozwiązania programowe. Oprogramowanie systemu AEOS (pakiet AEMon) jest zainstalowane na serwerze w pełni zgodnym ze standardem serwera aplikacji JBoss. Pakiet nie jest zatem zależny od systemu operacyjnego i może pracować w takich środowiskach, jak Windows 2003, Unix, Linux, serwer SQL, Oracle, MySQL. Posiada on interfejsy do najpowszechniej stosowanych pakietów HR, takie jak HR SAP czy PeopleSoft; posiada również interfejsy dla języka XML.

Dzięki łączom TCP/IP serwer z zainstalowanym pakietem AEMon nie musi być zlokalizowany w nadzorowanym obiekcie. Ma to istotne znaczenie w sytuacji, gdy wielkość obiektu (tj. liczba przejść i liczba użytkowników) nie przekracza pojemności jednego kontrolera AEpu (AP8001). Pakiet AEMon może być zainstalowany na serwerze dostępnym poprzez sieć WWW, dzięki czemu podczas aktualizacji oprogramowania nie istnieje konieczność wgrywania go do wszystkich stacji roboczych, gdyż najbardziej aktualna wersja jest zawsze dostępna w sieci.

Język oraz uprawnienia użytkownika można konfigurować dla poszczególnych osób, tak aby każdy dział (wydział, sekcja) organizacji mógł mieć przypisane automatycznie właściwe dla niego zadania. Każdy z użytkowników widzi tylko te funkcje i menu, do których ma prawo dostępu, i tylko do nich ma dostęp. Uprawnienia te są w pełni konfigurowalne dla poszczególnych osób; nie są one w żaden sposób powiązane z konkretnymi stacjami roboczymi lub komputerami PC. I tak na przykład:

– Pracownicy określonego budynku mogą widzieć tylko drzwi wewnątrz swojego budynku i kontrolować wszystkie wydarzenia związane z tymi konkretnymi drzwiami, z tym konkretnym miejscem.
– Kadra zarządzająca może widzieć wszystkie miejsca (lokalizacje) i drzwi oraz może je wszystkie kontrolować. Zarząd może mieć pełen ogląd i w dowolnej chwili podejmować decyzje.
– Pracownicy działu HR mogą widzieć kartoteki wszystkich pracowników, natomiast pracownikom czy strażnikom dane te nie są udostępniane.

Dzięki internetowemu charakterowi tego oprogramowania zmiana uprawnień poszczególnych użytkowników może odbywać się bezproblemowo, bez konieczności przeinstalowywania programu klienta na jego stacji roboczej.

Ciekawostką jest fakt, że każdy użytkownik tego oprogramowania może wybrać pewne funkcje, które wykonuje najczęściej, i zdefiniować je jako „Moje zadania". Po zalogowaniu się do systemu ekran „Moje zadania" pojawia się automatycznie, ułatwiając użytkownikowi wyszukanie najczęściej wykorzystywanych przezeń opcji.

Filtry wejścia

Zastosowanie filtrów wejścia spowoduje, że użytkownicy końcowi będą widzieć tylko grupę drzwi (przejść) związanych z określonym budynkiem, wydziałem, przejściem itp. Zarządzający może ponadto zdecydować, czy dana osoba posiada uprawnienia do przeglądania całości działań systemu, czy tylko do oglądania zdarzeń pochodzących z określonych miejsc lub przejść.

Jednostki

Jednostka to grupa pracowników, związanych z określonym budynkiem czy zakładem. Można ją swobodnie definiować, jeśli zajdzie taka potrzeba.

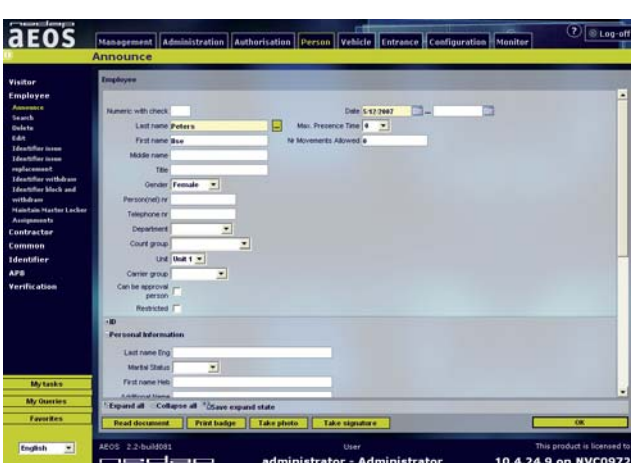
Przykład:

Jeśli system obejmuje różne lokalizacje, ale działa na jednym serwerze centralnym, to każdy z użytkowników systemu może kontrolować jedynie własną lokalizację (czyli przeglądać zdarzenia, personel, drzwi i uprawnienia tylko w ramach tego oddziału). Nadzór centralny natomiast może w każdej chwili przejąć zabezpieczenie tego zakładu.

Zarządzanie ruchami gości

Śledzenie ruchów gości zawsze może być procesem czasochłonnym. AEOS zapewnia wszechstronny system zarządzania gośćmi. Ponieważ działa on poprzez sieć internetową, każdy może mieć do niego dostęp i zgłosić wstępnie osobę odwiedzającą. Po zgłoszeniu się przy bramie goście muszą podać tylko swoje nazwisko, a identyfikator zostanie automatycznie wydrukowany przez strażnika z podaniem poprawnych danych dotyczących osoby odwiedzającej oraz jej pojazdu. Można wprowadzić tańsze identyfikatory specjalne, zawierające na przykład tylko kod kreskowy albo pasek magnetyczny, zamiast znacznie droższych identyfikatorów RFID, używanych przez personel stały.

Fot. 1. Przykład ekranu „Moje zadania”



Fot. 2. Wprowadzanie danych

Zarządzanie podwykonawcami

Zarządzanie podwykonawcami obejmuje wszystkie osoby wykonujące prace w obiekcie, ale niezatrudnione w nim w jednym systemie. W AEOS osoba określona jako Podwykonawca jest definiowana tak samo jak Pracownik i Gość, ale podlega innym procedurom zgłaszania, a także innym sposobom określania historii zdarzeń. Dostęp Podwykonawców jest automatycznie blokowany w razie wygaśnięcia zezwolenia dla związanego z nimi dostawcy lub w razie dokonania naruszeń przepisów, mogących spowodować umieszczenie ich na czarnej liście. W razie zakończenia umowy z dostawcą lub podwykonawcą blokowane są wszelkie związane z nimi identyfikatory, a także przepustki dla pojazdów.

Przykład:

Pewna firma sprzątająca zatrudnia dziesięciu pracowników, którym potrzebne są karty wstępu do zakładu. Gdy umowa z tą firmą wygasa, chcesz mieć pewność, że wszystkie wydane identyfikatory zostały zablokowane. W normalnych warunkach byłoby to bardzo czasochłonne, ponieważ poszczególne osoby sprzątające przekazują sobie nawzajem karty wstępu. AEOS zapobiega temu problemowi i gwarantuje, że wszystkie identyfikatory związane z tą konkretną firmą zostaną zablokowane bez względu na to, kto je posiada.

Zarządzanie zliczaniem na parkingu

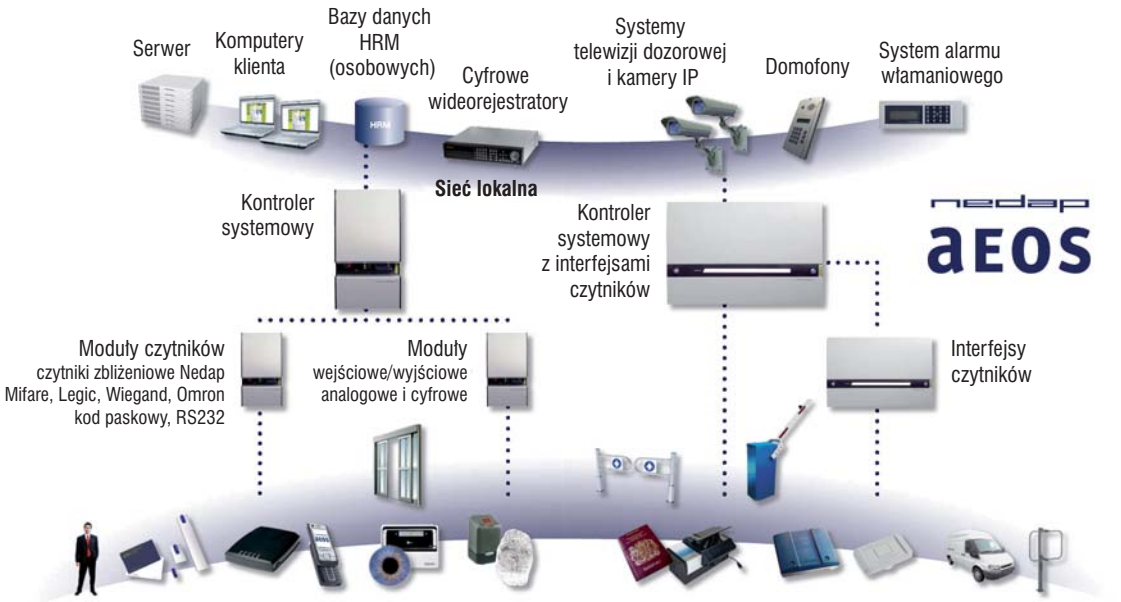
Zawarta w AEOS funkcja zarządzania zliczaniem na parkingu obejmuje następujące opcje:

- Dostęp do parkingu dla wszystkich (wszędzie na terenie parkingu).
- Dostęp do parkingu dla określonych grup ludzi, nawet gdy parking oznaczony jest dla innych jako „pełen”.
- Budynki z wieloma najemcami: firma wynajmująca część budynku biurowego ma prawo do posiadania na parkingu określonej liczby miejsc parkingowych.
- Strefy parkowania (strefy naliczania): strefy te określają obszar parkingu, na którym wolno parkować pojazdy.

Funkcje i właściwości opisane powyżej to tylko niektóre przykłady wykorzystania pakietu AEMon.

Silnik reguł (*Rule Engine*)

Nadawanie uprawnień poszczególnym osobom, a następnie upewnianie się, czy wszystkie osoby wewnątrz Twojego budynku są rzeczywiście uprawnione do przebywania w nim w danej chwili, to w przypadku dużych firm lub organizacji bardzo czaso- i pracochłonne operacje. Zastosowany w pakiecie silnik reguł NEDAP AEOS pozwala na efektywne, proste i szybkie zarządzanie uprawnieniami. Upoważnienie do wejścia dla pracownika, pojazdu, gościa czy wykonawcy może on łatwo i szybko połączyć z takimi atrybutami, jak wiek, wydział czy budynek. Aby te uprawnienia lokalnie lub w skali całej



Rys. 1. Podstawowa architektura

organizacji zastosować w stosunku do poszczególnych osób lub grup, wystarczy jedno naciśnięcie przycisku. Baza danych upoważnień może być aktualizowana tak często, jak to potrzebne, na przykład co godzinę lub co noc (przy większych bazach danych). Prawa dostępu dla pracowników opuszczających firmę są unieważniane automatycznie, natomiast uprawnienia pracowników, którzy zmieniają lokalizację lub wydział, są natychmiast przełączane na inne, właściwe dla ich nowego miejsca pracy.

Architektura systemu AEOS

Podstawowe założenia architektury systemu AEOS pokazuje rys. 1. Podstawową jednostką systemu AEOS jest kontroler systemowy AEpu. Kontroler tego rodzaju może zarówno funkcjonować jako jednostka samodzielna, jak i łączyć się z innymi kontrolerami AEpu poprzez sieć IP dla zrealizowania zadań systemu kontroli dostępu w większym budynku. Do kontrolera przyłączane są moduły czytników systemu NEDAP lub moduły interfejsów czytników innych technologii (Mifare, Legic, Omron, HID, czytniki kodów paskowych itp.).

Podstawowym kontrolerem systemowym AEpu jest kontroler typu AP8001 wyposażony w dwa interfejsy RS232 oraz łącze Ethernet do sieci LAN/WAN.

Kontrolery AEpu, jak np. AP4801, mogą mieć wbudowane interfejsy czytników. We wspólnej obudowie znajdują się tam takie urządzenia, jak: kontroler, cztery interfejsy czytników systemu NEDAP, osiem programowalnych wejść cyfrowych (dwustanowych) oraz cztery programowalne wyjścia typu przekaźnikowego.

Inne wersje tych kontrolerów to:

– wersja AP4803, która może współdziałać z czytnikami kart praktycznie wszystkich stosowanych standardów, takich jak karty magnetyczne, kody paskowe, Mifare, Legic, HID i inne. AP4803 posiada ponadto interfejsy Omron, Wiegand i RS232. Podobnie jak AP4801, kontroler wyposażony jest w osiem wejść dwustanowych i cztery programowalne wyjścia typu przekaźnikowego. W tej konfiguracji kontroler może nadzorować cztery przejścia. Do kontrolera można dołączyć dodatkowe sterowniki czytników, np. AP4003 4-in-1, co pozwala na objęcie nadzorem łącznie do szesnastu przejść;
– wersja AP4807 przystosowana do współdziałania z identyfikatorami Mifare (cztery czytniki na cztery przejścia). Po dołączeniu dodatkowych sterowników czytników Mifare typu AP4007 4-in-1 nadzorem można objąć do szesnastu przejść. W porównaniu z tradycyjną technologią Mifare dodatkową zaletą tego rozwiązania jest fakt, że dzięki zwiększeniu czułości systemu można sterownik (odpowiedzialny za odczyt i zdekodowanie informacji z identyfikatora) umieścić po zabezpieczonej stronie systemu nieco dalej od elementu bezpośrednio czytającego (anteny).

Modułami systemowymi bezpośrednio działającymi na przejściach są sterowniki czytników. NEDAP oferuje różne wykonania – na pojedyncze drzwi, z możliwością nadzorowania do czterech przejść. Sterowniki są dostosowane do odczytu danych zarówno ze specjalistycznych identyfikatorów NEDAP, jak i identyfikatorów innych powszechnie stosowanych technologii i protokołów, np. Mifare, Wiegand, Legic, HID, kodów paskowych czy kart z paskiem magnetycznym. Większość czytników umożliwia bezdotykowy odczyt danych z identyfikatora nawet z odległości ok. 40 cm, dzięki czemu możliwe staje się przejście bez konieczności zbliżania identyfikatora do anteny czytnika. Specjalne wykonanie anten przewidziano dla identyfikacji pojazdów wjeżdżających na teren garaży lub parkingów.

Sterowniki czytników łączą się z kontrolerami systemowymi za pośrednictwem magistrali AEbus, natomiast z czytnikami przy poszczególnych przejściach – za pośrednictwem okablowania wymaganego przez czytnik.

Nowym produktem w tej rodzinie jest sterownik czytników AP6003X 4-in-1, który z kontrolerami systemowymi komunikuje się wyłącznie poprzez sieć IP. Sterownik AP6003X posiada interfejsy do przyłączenia do dwóch czytników. Interesującym

Fot. 3. Kontroler systemowy AEpu – model AP8001

rozwiązaniem jest możliwość zasilenia modułu poprzez sieć Ethernet (przy większych odległościach od modułów zasilających istnieje również możliwość zasilenia go z oddzielnego modułu zasilającego).

Inne moduły systemowe

Dla uzupełnienia systemu i zapewnienia bezproblemowego dopasowania go do innych systemów bezpieczeństwa oraz połączenia z nimi przewidziano kilka modułów. Są to na przykład:

a) zasilacze systemowe AP2001 i AP2003;
b) moduły wejść analogowych AP3003 do odbioru takich informacji, jak temperatura, wilgotność itp. (do wykorzystania w zintegrowanym systemie zabezpieczeń);
c) moduły wejść cyfrowych dwustanowych AP3001 i AP3002, pozwalające wykorzystywać sygnały np. z systemu sygnalizacji alarmu włamaniowego czy z przycisków napadowych;
d) moduły AP3004 wyjść przekaźnikowych do sterowania (np. drzwiami, windami, sygnalizatorami itp.).

Fot. 5. Kontroler systemowy i kontroler czytników AP4801

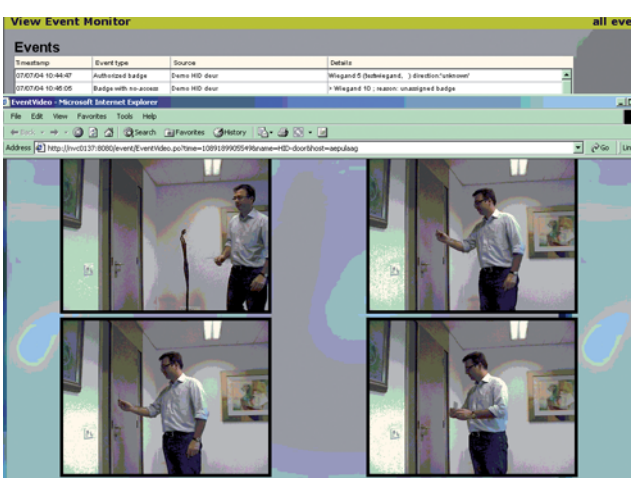
Dla wszystkich modułów systemowych, kontrolerów i sterowników zaprojektowano jednolitą szatę wzorniczą. Wszystkie one wyglądają podobnie jak kontroler AP8001 (wyjątkiem są kontrolery AP8401 i AP4803). Dla ułatwienia instalacji zaprojektowano obudowę AEbox, w której można zabudować i połączyć między sobą różne moduły systemu. W razie konieczności zapewnienia zasilania rezerwowego można zastosować zespół AX2004 do zainstalowania baterii zasilania rezerwowego. Obudowy AEbox uzyskały wiele międzynarodowych nagród za wyjątkowe i zgodne z nowoczesnymi tendencjami wzornictwo.

Opcje dodatkowe

Poprzez sieć IP dostawca lub administrator systemu może skomunikować z daną stacją roboczą różne urządzenia dodatkowe, z którymi może współpracować system AEOS. Przy użyciu poleceń systemu AEOS kamera cyfrowa skomunikowana ze stacją roboczą może na przykład pozwolić na wyświetlanie obrazów na ekranie. W systemie AEOS można również zapamiętywać podpisy, o ile system wyposażono w odpowiedni pulpit. Inne możliwości to drukowanie kart wejściowych (np. dla gości), skanowanie danych osobowych z paszportów czy kart wejściowych oraz realizowanie bardzo wielu innych zadań związanych z systemami bezpieczeństwa.

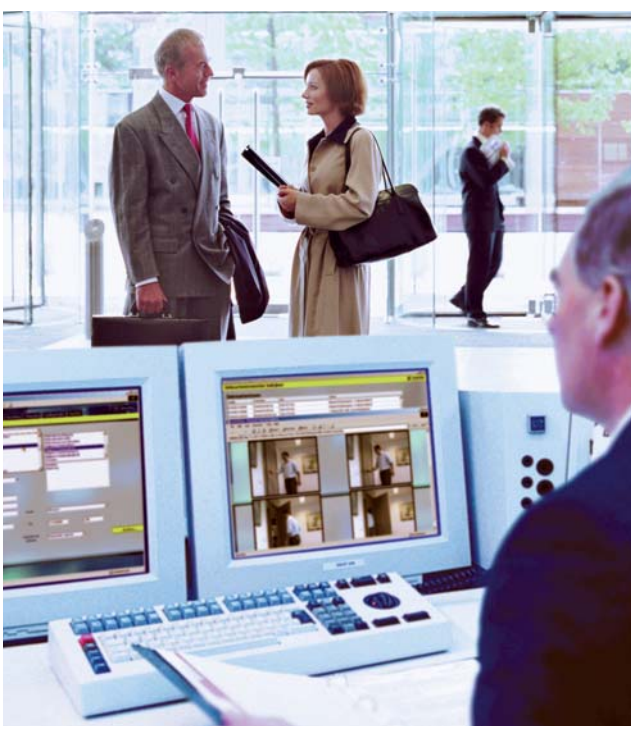
Poniższy ekran pokazuje serię zdjęć uzyskanych z kamery połączonej z systemem AEOS:

Fot. 4. Czytniki zbliżeniowe różnych formatów kart

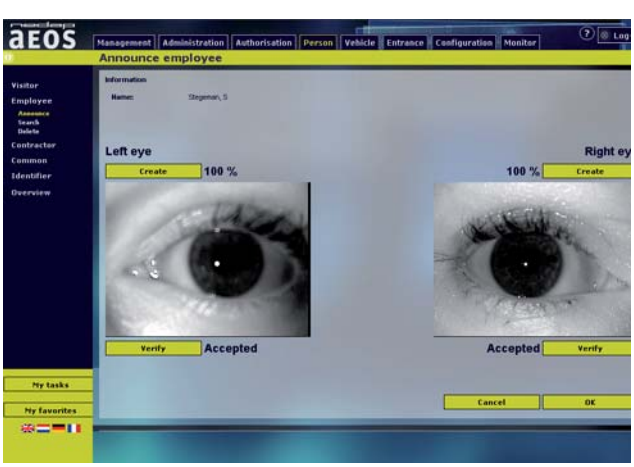


Fot. 6. Seria zdjęć zdarzenia

Fot. 7. Klawiatury z czytnikami



Fot. 8. Widząc obraz, operator może skonfrontować go z danymi w bazie



Fot. 9. Weryfikacja obrazu tęczówki w systemie AEOS

Integracja systemowa

Otwarta architektura AEOS ułatwia integrację z innymi systemami. Kontrola dostępu i działanie monitoringu tworzą podstawę zintegrowanego systemu zarządzania bezpieczeństwem, obejmującego system sygnalizacji włamań oraz nadzór wizyjny (CCTV). Umożliwia to natychmiastowe reagowanie na alarm za pomocą wielu sposobów.

Monitor alarmów może na przykład zasygnalizować alarm, podając dokładną lokalizację zdarzenia i stosowne instrukcje. Konfiguracja AEOS zapewnia w czasie rzeczywistym możliwość wymiany danych z innymi systemami, np. kartotekami pracowniczymi. Informacje pochodzące z baz danych stron trzecich, np. bazy danych zasobów ludzkich (HR), mogą być importowane do bazy danych AEOS. Można to robić automatycznie w zadanych przedziałach czasowych (np. co noc) lub ręcznie – poprzez wykonanie eksportu danych z HR i zaimportowanie ich do systemu Kontroli Dostępu.

Podsumowanie funkcji AEOS

– Kontrola dostępu pracowników, gości, podwykonawców i pojazdów.
– Dowolnie definiowane harmonogramy o wielu interwałach i elastycznej konfiguracji cyklu czasowego (np. pięć dni zamiast tygodnia).
– Elastyczne grupowanie wejść (niezależnie od konfiguracji sprzętu). Drzwi można łączyć z wieloma grupami.
– Prawa dostępu określane na podstawie zdefiniowanych profili. Indywidualnie modyfikowane prawa dostępu mogą być zmieniane bez konieczności zmiany pierwotnego profilu.
– Możliwość definiowania rozpoczęcia i zakończenia okresów ważności.
– Tymczasowe uprawnienia pojedynczych osób.
– Rejestracja wejść/wyjść z wielopoziomową opcją „*anti-pass back*”, z dopuszczeniem „twardych” i „miękkich” (np. czasowo znoszonych) trybów pracy APB.
– Autoryzacja danych (zarządzanie sektorowe): przyporządkowanie zastrzeżonych praw użytkownika do realizacji określonych zadań związanych z drzwiami, zdarzeniami i osobami.
– Zaawansowane ustawienia upoważnień, jak np. „cztery oczy”, „kierownik pierwszy” lub „kierowca” czy też „kierowca i pojazd”.
– Zintegrowana weryfikacja kodu PIN z możliwością wyboru własnego kodu.
– Zintegrowana identyfikacja biometryczna.
– Swobodnie konfigurowalne otwieranie drzwi dla poszczególnych wejść.
– Nieograniczona liczba dowolnie definiowanych ról i praw użytkowników.
– Zadania definiowane wg roli użytkownika, które każdy z użytkowników może widzieć i wybierać, korzystając z funkcji „Moje zadania”.
– Nieograniczona liczba definiowalnych wolnych pól dla zarządzania informacjami dodatkowymi.
– Funkcja dziennika z filtrami wyszukiwania dla zapisywania, kto, co i kiedy zrobił w AEOS.

Fot. 10. (na górze) Otwarty czytnik zbliżeniowy
Fot. 11. (na dole) Obudowa montażowa AEbox

– Niezależne od serwera powiązanie „*peer-to-peer*" (twarzą-w-twarz) wejść oraz wyjść analogowych i cyfrowych z elementami działań oraz odpowiedzi systemu.
– Nieustanne monitorowanie miejsc wchodzenia i wychodzenia osób.
– Dowolnie definiowane ostrzeżenia.
– Dowolnie konfigurowana funkcja obrazowania zdarzeń.
– Graficzny interfejs użytkownika (ang. *Graphic User Interface*) wraz z dowolnie konfigurowanymi priorytetami alarmów oraz zestawami instrukcji do poszczególnych alarmów (SMA).
– Konfigurowana funkcja wtargnięcia do stref kontrolowanych, włącznie z aktywacją/dezaktywacją połączonych lub zewnętrznych systemów sygnalizacji alarmów.
– Możliwość bezproblemowego zintegrowania systemu powiadamiania o wtargnięciu z systemem kontroli dostępu.
– Zarządzanie ruchem gości – łącznie z wcześniejszym powiadamianiem przez pracowników oraz zdalnym wydrukiem kart itp.
– „Moje ulubione": osobiste skróty z aplikacji do innych aplikacji sieciowych.
– Kontrola dostępu dla wykonawców i podwykonawców, z uprawnieniami powiązanymi z ich zleceniami i zezwoleniami.
– Kontrola zagęszczenia w danej przestrzeni lub strefie w celu podania na przykład liczby dostępnych miejsc parkingowych.
– Czarna lista oraz zarządzanie naruszeniami mającymi bezpośredni wpływ na prawo dostępu.
– Wysyłanie informacji o zdarzeniach, np. e-mail, SMS itp.
– Zadania inteligentne, włączanie kamer lub wykonywanie innych zadań systemowych.
– Wielojęzyczny interfejs użytkownika powiązany z jego nazwą (loginem).

Zakończenie

Polskim przedstawicielstwem kieruje Robert Mazur. Wszelkie pytania prosimy kierować pod adres: *robert.mazur@nedap.com*

Robert Mazur
NEDAP

RACS ROGER ACCESS CONTROL SYSTEM

seria radius

CE

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 wchodzą czytniki i kontrolery różniące się konstrukcją mechaniczną oraz funkcjonalnością, w zależności od modelu obsługują one karty standardu EM 125 kHz lub 13,56MHz Mifare. Nową kategorię produktu stanowi wandalo-odporny czytnik (PRT64EM-VP), w którym przednia część obudowy i klawisze są wykonane w całości z metalu.
Na szczególną uwagę zasługuje kontroler PR602LCD specjalnie zaprojektowany dla systemów rejestracji czasu pracy RCP, do których oferowane jest nowoczesne oprogramowanie RCP Master.

RCP Master *PR602LCD*

RCP Master

Kompleksowe rozwiązanie RCP firmy ROGER ułatwia zarządzanie czasem pracy oraz wpływa na redukcję kosztów oraz precyzję rozliczania, przyczyniając się pośrednio do wzrostu produktywności w przedsiębiorstwie. RCP Master posiada łatwy w obsłudze, przyjazny interfejs. Program może być użytkowany bezpłatnie w celach ewaluacyjnych przez pierwsze 60 dni. RCP Master oferowany jest z licencją do obsługi 50, 250 lub powyżej 250 pracowników a także w wersji jedno lub wielostanowiskowej, co umożliwia dopasowanie rozwiązania do struktury i wielkości przedsiębiorstwa. Program RCP Master został opracowany w środowisku Microsoft .NET i jest przeznaczony dla systemów operacyjnych Windows XP i Vista.

profesjonalna kontrola dostępu

roger®

www.roger.pl

Wielokanałowość połączeń
w systemie wideofonowym **300 Bpt**

Od kilku lat w Polsce powstaje coraz więcej zamkniętych osiedli mieszkaniowych o dużej liczbie lokali, sięgającej nawet do tysiąca mieszkań. W osiedlach tych stosowane są systemy wideofonowe z wieloma wejściami głównymi na teren oraz wieloma stanowiskami portierskimi. W tak dużych kompleksach mieszkaniowych pojawia się często problem zajętości linii łączącej główne panele wejściowe oraz centrale portierskie z układami klatkowymi, obsługującymi odbiorniki lokatorskie. Rozwiązanie tego problemu umożliwia cyfrowy system wideofonowy serii 300 Bpt dzięki zastosowaniu zwielokrotnionej liczby kanałów komunikacji pomiędzy układem głównych paneli wejściowych oraz central portierskich a układami blokowymi (klatkowymi), zawierającymi odbiorniki lokatorskie. Artykuł ten w głównej mierze adresowany jest do projektantów systemów wideofonowych, którzy chcieliby wykorzystać zaawansowane funkcje systemu 300 Bpt.

Wielokanałowość komunikacji

Rozważmy na początek najprostszy schemat (rys. 1). W układzie głównym zawiera on dwa panele wejściowe oraz dwie centrale portierskie połączone magistralą główną z układami blokowymi, które posiadają własne panele blokowe (klatkowe) i odbiorniki lokatorskie.

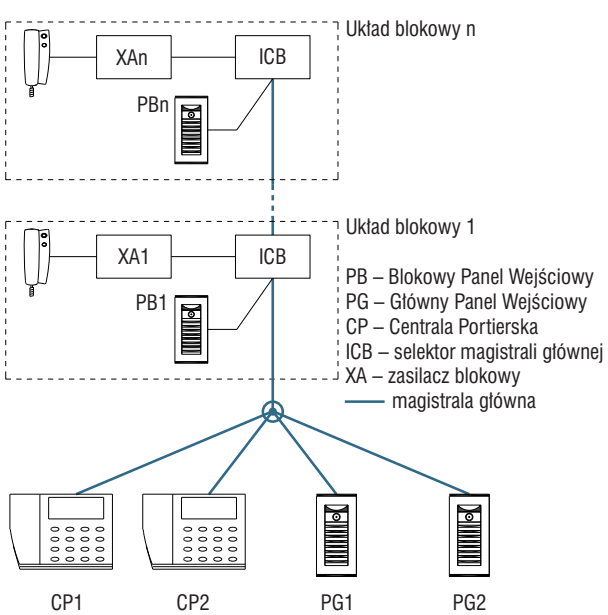
W przypadku, gdy portier dzwoni do dowolnego lokatora, blokuje wtedy automatycznie możliwość połączenia z innym lokatorem z głównych paneli wejściowych i drugiej centrali portierskiej. Oznacza to, że gdy ustanowione jest połączenie z dowolnego urządzenia układu głównego, pozostałe urządzenia muszą poczekać na zakończenie tej rozmowy. Prawdopodobieństwo wystąpienia stanu zajętości jest tym większe, im więcej głównych paneli wejściowych, central portierskich oraz odbiorników lokatorskich jest w całym układzie.

W systemie wideofonowym serii 300 Bpt możemy w znacznym stopniu wyeliminować ten problem, zwiększając przepustowość komunikacji pomiędzy układem głównym a układami blokowymi dzięki zastosowaniu dodatkowych magistral głównych. Na rys. 2 przedstawiono ten sam układ realizowany na czterech magistralach głównych. Ogólnie w systemie 300 można zastosować od jednej do czterech magistral głównych. Oznacza to, że w tej samej chwili mogą być zestawione cztery połączenia z układu głównego do różnych układów blokowych. Zakładając równomierny rozkład częstotliwości połączeń ze wszystkich urządzeń układu głównego (dwie centrale i dwa panele wejściowe), można w rozważanym układzie prawie 4-krotnie zmniejszyć prawdopodobieństwo zajętości przy założeniu dużej liczby układów blokowych. Przy ocenie prawdopodobieństwa zmniejszenia zajętości należy wziąć pod uwagę również liczbę układów blokowych, gdyż w pojedynczym układzie blokowym (z reguły klatce) mamy zawsze tylko jeden kanał komunikacji, niezależnie od liczby zastosowanych głównych magistral. Oznacza to, że w tym samym czasie można uzyskać połączenie z pojedynczym blokiem tylko z jednego urządzenia w układzie głównym (nawet w przypadku zastosowania kilku magistral).

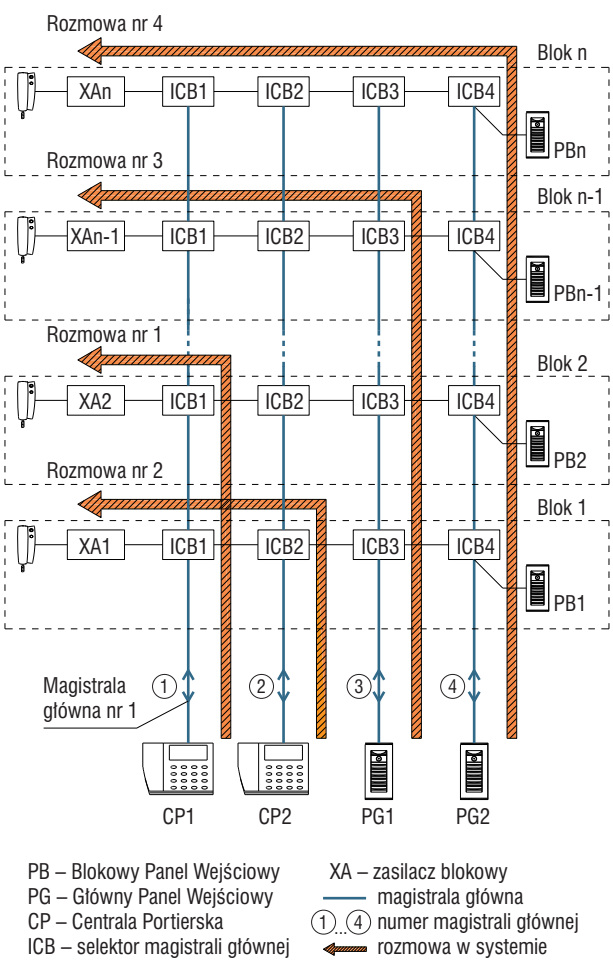
W systemie wielokanałowym do każdego układu blokowego z systemowym zasilaczem blokowym XA/301LR dodano jeden selektor magistrali głównej ICB/300 na każdą magistralę główną. Jest to główna różnica w doborze urządzeń w porównaniu z rozwiązaniem jednokanałowym. Zmianie ulega również miejsce podłączenia blokowych paneli wejściowych – dołączane są one zawsze do ostatniego selektora blokowego. Pomiędzy układem głównym a układami klatkowymi należy ułożyć tyle przewodów UTP Kat. 5, ile zastosowano kanałów komunikacji.

Sygnały audio i wideo z paneli blokowych do układu głównego można transmitować dowolną magistralą główną. Na rys. 2 założono, że wszystkie układy blokowe dołączone są do czterech magistral głównych. W celu ograniczenia komunikacji pomiędzy niektórymi urządzeniami układu głównego i układami blokowymi możliwe są jednak dowolne kombinacje podłączeń poszczególnych bloków do odpowiednich magistral głównych, jak pokazano na rys. 3. Praktyczne zastosowanie takiego rozwiązania to np. ograniczenie dostępu do części osiedla z danego panelu głównego lub obsługa przez danego portiera tylko wybranych budynków (lub grupy klatek) na osiedlu.

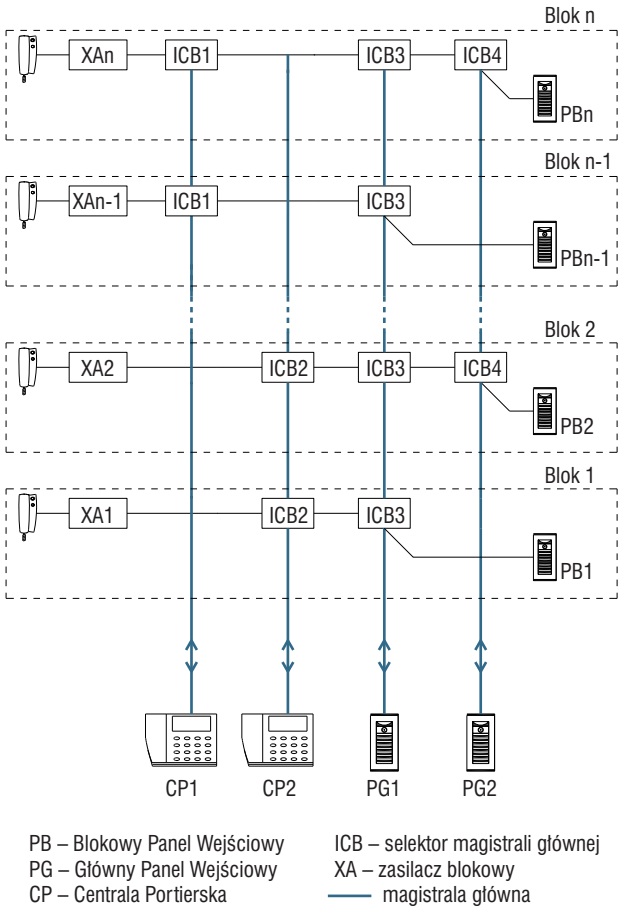
W porównaniu z rozwiązaniem przedstawionym na rys. 1 układ wielokanałowy z rys. 2 ma jednak poważną wadę funkcjonalną. Żadne z urządzeń układu głównego nie może komunikować się z pozostałymi urządzeniami tego układu, co np. oznacza, że nie ma łączności z portierami z dwóch głównych paneli wejściowych. Mimo iż istnieją przewodowe połączenia między urządzeniami głównymi za pośrednictwem selektorów ICB we wszystkich blokach, to jednak ten rodzaj komutacji nie jest możliwy.



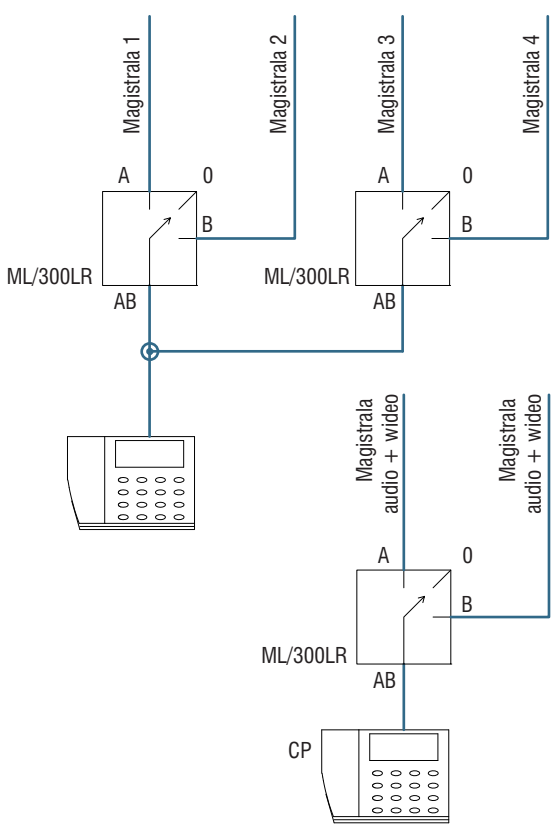
Rys. 1. Układ wieloblokowy z jedną magistralą główną



Rys. 2. Układ wieloblokowy z czterema magistralami głównymi



Rys. 3. Układ z ograniczonym dostępem do magistral głównych z układów blokowych



Rys. 4. Schemat działania selektora / rozdzielacza magistrali głównej ML/300LR

Selektor/rozdzielacz magistrali głównej ML/300LR

Rozważany powyżej problem może być rozwiązany dzięki zastosowaniu specjalnego urządzenia, zwanego selektorem/rozdzielaczem magistrali głównej o symbolu ML/300LR. Selektor ML/300LR można sobie wyobrazić jako trzypozycyjny przełącznik (rys. 4), który w przypadku braku połączenia znajduje się w pozycji neutralnej „0", zaś w celu ustanowienia połączenia wybiera on magistralę A lub B, odłączając nieużywaną magistralę. Selektor ML/300LR jest zarówno logicznie, jak i elektrycznie przyporządkowany do pojedynczego urządzenia w układzie głównym, pozwalając temu urządzeniu (dołączonemu do portu AB) podłączać się dynamicznie razem z sygnałami audio i wideo do jednej z dwóch magistral (A lub B), jeśli wystąpiło żądanie połączenia poprzez tę magistralę. Selektor ML/300LR nie jest zatem urządzeniem, które na czas komunikacji ma tworzyć dynamicznie „pomost" między magistralami.

Do każdego urządzenia w układzie głównym (panelu lub centrali portierskiej) można dołączyć maksymalnie dwa moduły ML/300LR, co umożliwia przełączanie się urządzenia pomiędzy czterema magistralami głównymi.

Po dodaniu selektorów do central portierskich z rys. 2 otrzymamy układ jak na rys. 5, w którym możliwe będą już połączenia z głównych paneli wejściowych do central portierskich oraz połączenia pomiędzy centralami portierskimi. W celu zapewnienia podobnej funkcjonalności w zakresie połączeń w układzie głównym można by zaproponować inne konfiguracje połączeń urządzeń głównych za pomocą modułów ML/300LR. Korzystną cechą tego systemu jest niewątpliwie elastyczność doboru rozwiązania, ale wymaga ona pewnego doświadczenia w przypadku projektowania bardziej złożonych układów.

W systemie 300 na etapie programowania układu tworzone są automatycznie listy wszystkich możliwych połączeń w systemie. Pojedyncza lista reprezentuje jedną magistralę i zawiera wszystkie możliwe urządzenia, które mogą komunikować się ze sobą po tej magistrali głównej. Dla magistrali głównej nr 3 z rys. 5 lista ta będzie zawierała panel PG1, centrale portierskie CP1 i CP2, układy blokowe od 1 do N oraz blokowe panele wejściowe PB. Należy zauważyć, że centrala portierska CP1 może połączyć się z dowolnym układem blokowym (blokowym panelem wejściowym lub odbiornikami w bloku) za pośrednictwem magistrali nr 1, 3 lub 4 w zależności od tego, która z magistral o najniższym numerze logicznym będzie wolna. Jeśli magistrali nr 4 przydzieliliśmy najniższy numer logiczny (tutaj 2), to centrala CP1 w pierwszej kolejności będzie próbowała połączyć się z odbiornikami lokatorskimi poprzez magistralę główną nr 4, a nie nr 1. Jest to oczywiście rozwiązanie niekorzystne, gdyż centrala będzie blokowała połączenia do odbiorników z panelu wejściowego PG2. W rozważanym schemacie dobrze jest przyjąć numery logiczne magistral zgodne z ich numeracją fizyczną.

Zwróćmy uwagę na jeszcze jedną zaskakującą cechę systemu komutacji połączeń. Mimo że obie centrale portiera nie są połączone przez żaden kanał selektorów ML (można by np. wykorzystać wolny kanał B na drugim selektorze ML

każdej centrali), to mogą one komunikować się ze sobą poprzez magistralę 3 lub 4 (wg priorytetu określonego przez numery logiczne magistral), podłączając się na czas rozmowy do jednej z tych magistral.

Podział na gałęzie

System 300 posiada jeszcze inną ciekawą cechę. Otóż poszczególne główne magistrale komunikacji można „pociąć" na mniejsze części, zwane gałęziami. Na rys. 6 przedstawiono schemat przykładowego układu, w którym osiedle zostało podzielone na dwie części – każda z własną centralą portierską CP1 (i odpowiednio CP2) oraz własnym głównym panelem wejściowym PG1 (i odpowiednio PG2). Dodatkowo w systemie istnieje wspólny panel wejściowy PG3 oraz wspólna centrala portiera CP3 dla całego osiedla. Układ główny wykorzystuje zatem trzy magistrale główne, ale podzielony jest na cztery gałęzie. Zgodnie z wcześniej opisanymi regułami do każdego z urządzeń w układzie głównym z rys. 6 można dołączyć maksymalnie dwa moduły ML/300LR w celu realizacji połączeń między tymi urządzeniami oraz zwiększenia dla nich liczby kanałów komunikacji. Dobierane na etapie programowania instalacji numery logiczne gałęzi mogą przyjmować wartości od 1 do 255. Przy programowaniu systemu centrale portiera CP1 i CP2 mogą być zdefiniowane jako centrale blokowe, pod warunkiem że obsługują tylko jeden blok (XA). Muszą być one wówczas podłączone do pierwszego selektora ICB.

Podsumowanie

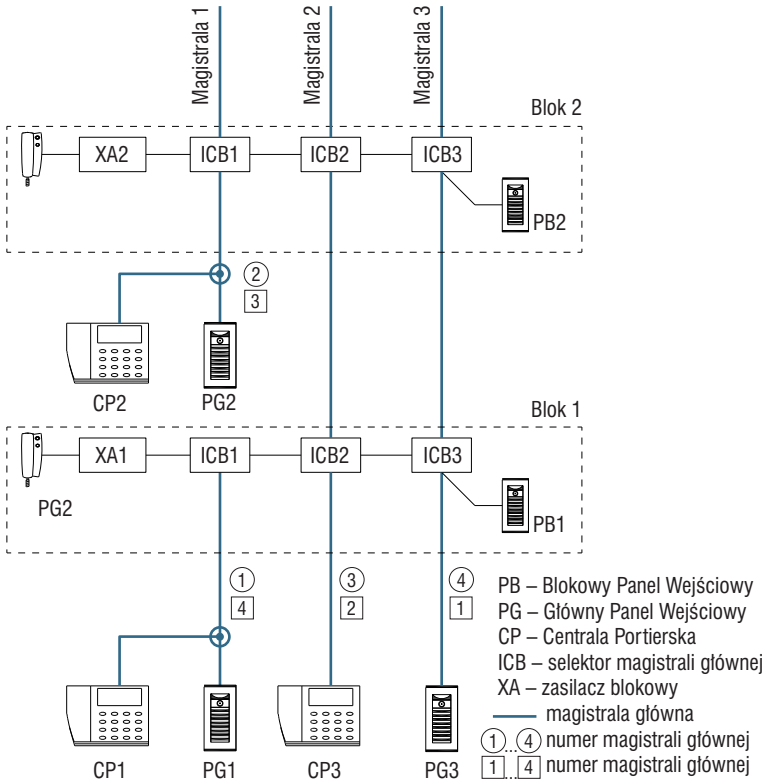
Dobierając liczbę głównych linii komunikacyjnych i projektując podział na gałęzie, trzeba wziąć pod uwagę następujące zagadnienia i zalecenia:

1. Liczbę urządzeń w układzie głównym. Jeśli np. w układzie głównym jest tylko jedno urządzenie, wówczas nie ma sensu stosować kilku magistral. Jeśli w układzie głównym są tylko dwa urządzenia, to można zastosować co najwyżej dwie magistrale.
2. Przyporządkowanie urządzeń układu głównego (panele i centrale) do poszczególnych gałęzi, tak aby równoważyć rozkład połączeń pomiędzy wszystkie główne magistrale. Należy przeanalizować, które urządzenia będą najczęściej wykorzystywane do komunikacji, i starać się je umieścić na różnych magistralach.
3. Wzajemne połączenia pomiędzy urządzeniami układu głównego (komunikacja z paneli głównych do central i pomiędzy centralami) oraz wymagane połączenia od urządzeń układu głównego do układów blokowych.
4. Minimalizację liczby selektorów ML/300LR. Połączenia między urządzeniami system często pozwala zrealizować na wiele sposobów, a zatem należy wybierać wariant najprostszy, który minimalizuje liczbę połączeń przewodowych i urządzeń rozdzielczych.
5. Przyporządkowanie selektorów ML/300LR zwykle do central portierskich, a nie paneli wejściowych. Z reguły w systemie zawsze jest mniej central portierskich niż paneli wejściowych, dlatego też przyporządkowanie selektorów ML/300LR do central portierskich upraszcza schemat połączeń.

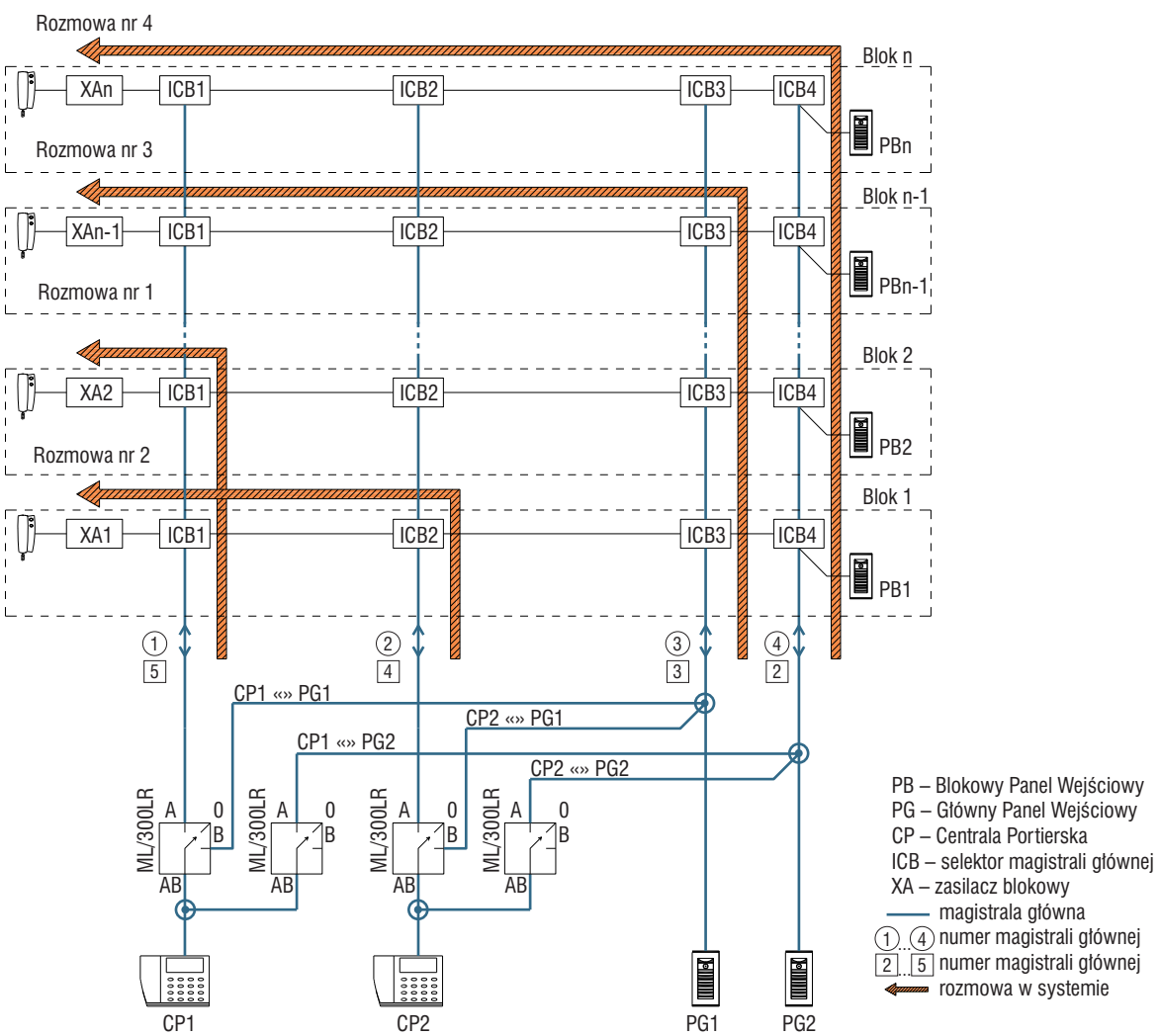
6. Odpowiednią numerację gałęzi, tak aby urządzenia układu głównego w pierwszej kolejności realizowały połączenia poprzez dedykowaną dla siebie gałąź.

Wielokanałowość i elastyczność konfiguracji połączeń w układzie głównym daje możliwość budowy różnych ciekawych i praktycznych układów, ale jednocześnie wymaga pewnego doświadczenia przy projektowaniu, potrzebnego do optymalizacji przepustowości połączeń w systemie. Dzięki wielokanałowości i zastosowaniu selektorów ML/300LR można nie tylko zwiększyć liczbę równolegle realizowanych połączeń, ale w przypadku zajętości podstawowej gałęzi komunikacji również umożliwić wykonywanie połączeń alternatywnymi kanałami. Na bazie wielokanałowych układów połączeń w systemie wideofonowym zrealizowano do tej pory wiele ciekawych inwestycji mieszkaniowych, o których będzie jeszcze mowa w kolejnych artykułach.

Andrzej Grodecki
ADD



Rys. 6. Podział magistrali głównej na gałęzie



Rys. 5. Schemat komunikacji między urządzeniami w układzie głównym

WYZNACZAMY NOWE GRANICE OCHRONY

SYSTEMY ALARMOWE

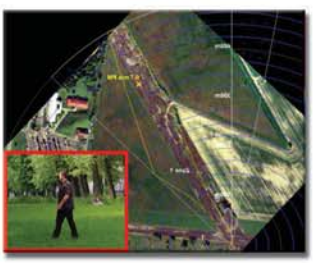
KABE

RADARY NADZORUJĄCE

OCHRONA ŚWIATŁOWODOWA

Poznaj możliwości zaawansowanych systemów nadzorujących.

Nie daj się zaskoczyć. Przejmij kontrolę nad sytuacją.



Namierz intruza zanim dostanie się na Twój teren.

Śledź każdy jego krok i podejmij skuteczną interwencję.

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63, 43-190 Mikołów
tel. 032 32 48 900, fax 032 32 48 901
systemy@kabe.pl / www.kabe.pl

Systemy sygnalizacji włamania

Część 2 – Linie dozorowe

Jak już opisano w części pierwszej niniejszego cyklu artykułów, systemy alarmowe sygnalizacji włamania zawierają najczęściej następujące części składowe: centralę alarmową, jedną lub więcej czujek, jeden lub więcej sygnalizatorów i (lub) systemów transmisji alarmu, jeden lub więcej zasilaczy. W tym artykule będą opisane zagadnienia związane z liniami dozorowymi i sposobami ich konfiguracji w systemach sygnalizacji włamania.

Norma europejska EN 50131-1:2006 „Alarm systems – Intrusion and hold-up systems – Part 1: System requirements", która ma jednocześnie status Polskiej Normy PN-EN 0131-1:2007 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe", zawiera wykaz definicji i skrótów, które stosowane są następnie w kolejnych rozdziałach tej normy. Wśród nich jest m.in. definicja:

– **łączność** (ang. *communication*) – transmisja komunikatów i (lub) sygnałów między elementami składowymi systemu sygnalizacji włamania i napadu.

W zależności od założeń przyjętych podczas projektowania systemu sygnalizacji włamania i rozwiązań konstrukcyjnych producenta w stosowanych urządzeniach istnieją różne możliwości połączenia czujek z płytą główną (lub modułami) centrali alarmowej.

1. Linie dozorowe central alarmowych

W klasycznych centralach telekomunikacyjnych typu abonenckiego bardzo istotną rolę odgrywają linie abonenckie, które łączą aparat telefoniczny z centralą telefoniczną. Muszą się one charakteryzować określonymi parametrami (m.in. impedancją „widzianą" od strony centrali oraz długością, która nie może przekraczać pewnej wartości maksymalnej). Nieco inną rolę pełnią linie dozorowe przewodowe lub radiowe łączące centralę alarmową z czujką lub innym urządzeniem, które jest w stanie przekazać informacje alarmowe o stanie dozorowanego pomieszczenia lub obiektu. Ponieważ współczesne centrale alarmowe to urządzenia mikroprocesorowe, a z nimi współpracują określone urządzenia dozorowe, można więc wyróżnić trzy podstawowe systemy linii dozorowych, a mianowicie:

– konwencjonalny,
– radiokomunikacyjny,
– adresowalny.

Podział linii dozorowych współpracujących z centralami alarmowymi przedstawiono na rys. 1.

Linie dozorowe w systemie konwencjonalnym można podzielić na:

a) zwykłe:
– typu otwartego (NO, ang. *normally open*),
– typu zamkniętego (NC, ang. *normally closed*),
b) parametryczne:
– typu pojedynczego,
– typu podwójnego.

1.1. Linie dozorowe zwykłe

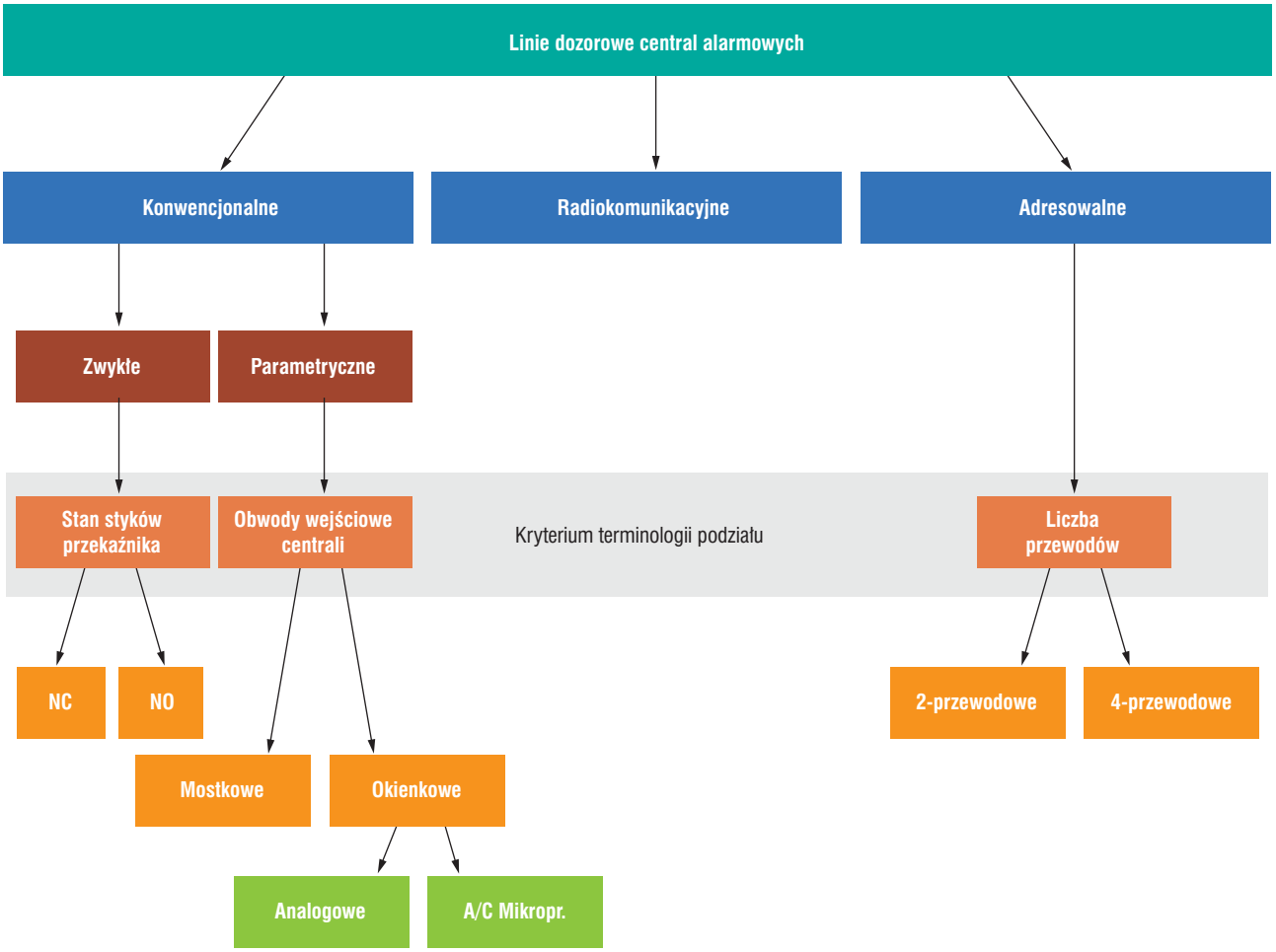
Linie zwykłe można podzielić na: linie dozorowe typu otwartego, które współpracują z czujką wyposażoną w zestyki, tzw. normalnie otwarte (NO) i linie typu zamkniętego, które współpracują z czujką wyposażoną w zestyki, tzw. normalnie zamknięte (NC). Kryterium alarmu to zwarcie lub rozwarcie linii. Linie typu otwartego są rzadko stosowane ze względu na niemożność odróżnienia przerw w linii od stanu czuwania. Znacznie częściej stosowane są linie typu zamkniętego (NC). Podstawową wadą tych linii jest brak sygnalizacji zwarcia linii, istotny zwłaszcza w przypadku, gdy do danej linii jest podłączonych kilka czujek i zwarcie w linii może wyeliminować pewną liczbę czujek z systemu. Wadę tę można wyeliminować, stosując linie parametryczne z grupy linii konwencjonalnych.

1.2. Linie dozorowe parametryczne

Na rys. 2 przedstawiono sposób podłączenia do centrali alarmowej czujki z wyjściem normalnie zamkniętym (NC) bez rezystora parametrycznego (rys. 2a) oraz czujek z wyjściem normalnie zamkniętym (NC) i czujek z wyjściem normalnie otwartym (NO) z zastosowaniem rezystora parametrycznego (rys. 2b).

Na rys. 3 przedstawiono podłączenie czujek standardowych posiadających zestyk antysabotażowy (SAB, oznaczany czasem angielskim słowem tamper). Na rys. 3a przedstawiono podłączenie czujki z wyjściem normalnie zamkniętym (NC) z pojedynczym rezystorem parametrycznym (często zwany rezystorem charakterystycznym – R_{CH}), zaś na rys. 3b przedstawiono czujkę z wyjściem normalnie zamkniętym (NC) i z wyjściem sabotażowym (SAB), gdzie zastosowano dzielony rezystor parametryczny.

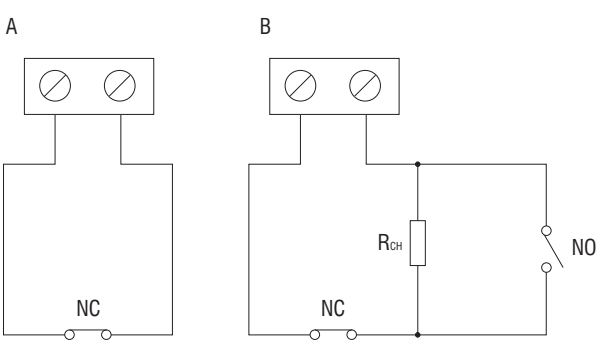
Linia dozorowa parametryczna jest linią, która jest zakończona rezystorem charakterystycznym. Zadaniem rezystora R_{CH} jest ustalenie wartości prądu płynącego w linii dozorowej w stanie dozorowania. Zmiana tego prądu może być spowodowana przejściem czujki w stan alarmu, np. na skutek



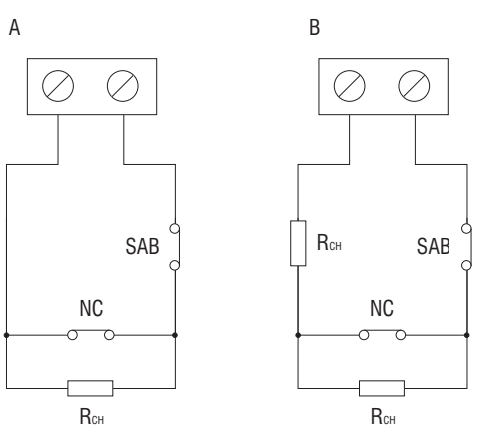
Rys. 1. Podział linii dozorowych współpracujących z centralami alarmowymi

pojawienia się intruza w chronionym obiekcie, co powoduje zmianę wartości napięcia na wejściu centrali alarmowej. Zmianę tę wykrywają obwody wejściowe centrali i odpowiednio ją interpretują. Rezystancja charakterystyczna linii dozorowej R_{CH} (a więc wartość tego rezystora) dla danego typu central jest indywidualnie określana przez producenta. Może być ona złożona z kilku rezystorów instalowanych w czujkach dołączonych do linii dozorowej.

Poważnym błędem jest podłączanie rezystora charakterystycznego R_{CH} bezpośrednio do zacisków wejściowych linii dozorowych centrali alarmowej. Rezystor charakterystyczny R_{CH} musi być zawsze montowany w czujce na końcu linii dozorowej. W przypadku większej liczby czujek NC, dołączonych do tej samej linii dozorowej parametrycznej, rezystor charakterystyczny R_{CH} powinien być montowany w czujce najbardziej oddalonej od centrali alarmowej.



Rys. 2. Podłączenie czujek do centrali alarmowej:
A – czujka NC bez rezystora parametrycznego,
B – czujki NC i NO z rezystorem parametrycznym.



Rys. 3. Podłączenie czujek z zestykiem antysabotażowym do centrali alarmowej:
A – czujka z wyjściem normalnie zamkniętym (NC) z rezystorem parametrycznym i zestykiem SAB,
B – czujka z wyjściem normalnie zamkniętym (NC) z dzielonym rezystorem parametrycznym i zestykiem SAB.

Linia dozorowa parametryczna może być definiowana jako linia pracująca w trybie dwustanowym lub trójstanowym.

Linia dozorowa parametryczna pracująca w trybie dwustanowym to taka linia, która rozróżnia dwa stany linii:

– stan alarmu,

– stan dozoru.

Można więc w trybie dwustanowym zdefiniować trzy przedziały charakteryzujące napięcie linii dozorowej występujące na wejściu dozorowym centrali alarmowej. W tabeli 1 przedstawiono uzyskane laboratoryjnie przykładowe rozkłady napięć wejściowych linii dozorowych centrali alarmowej charakteryzujące trzy stany.

Podane wartości napięć pojawiające się na wejściu linii dozorowych w centrali alarmowej są wartościami przykładowymi uzyskanymi w laboratorium, zależnymi od długości linii dozorowej, której rezystancję można obliczyć na podstawie równania (1). Na rys. 4 przedstawiono linię dozorową z uwzględnieniem rezystancji przewodów.

Równanie (1) pozwala w prosty sposób obliczyć rezystancję pętli (zamkniętej) linii dozorowej

$$R_{linii} = \rho \cdot \frac{l}{S} \quad (1)$$

gdzie:

ρ – rezystywność miedzi Cu wynosząca $1{,}75 \times 10^{-8}$ Ωm,

l – długość [m] linii dozorowej (całkowita),

S – przekrój [m^2] przewodu linii dozorowej (jeśli średnica kabla wynosi 0,5 mm, to $S = 0{,}196$ mm^2).

Napięcie na końcach przewodu jednorodnego o jednolitym na całej długości l i przekroju S można zgodnie z prawem Ohma obliczyć z równania (2)

$$U_L = I \cdot \rho \cdot \frac{l}{S} \quad (2)$$

gdzie:

I – prąd płynący w pętli linii dozorowej w [A]

U_L – spadek napięcia na całkowitej długości pętli linii dozorowej w [V]

Lp.	Przedział napięć	Jednostka	Stan linii dozorowej
1	(0 ; 4,3)	V	ALARM (zwarcie)
2	<4,3 ; 8,3>	V	stan dozoru
3	(8,3 ; 13,8)	V	ALARM (rozwarcie)

Tab. 1.

Lp.	Przedział napięć	Jednostka	Stan linii dozorowej
1	(0 ; 3,2)	V	sabotaż (zwarcie)
2	<3,2 ; 6,2>	V	ALARM
3	(6,2 ; 8,2)	V	stan dozoru
4	<8,2 ; 10,2>	V	ALARM
5	(10,2 ; 13,8)	V	sabotaż (rozwarcie)

Tab. 2.

Maksymalna długość linii dozorowej jest także określana przez konstruktorów i producentów central alarmowych.

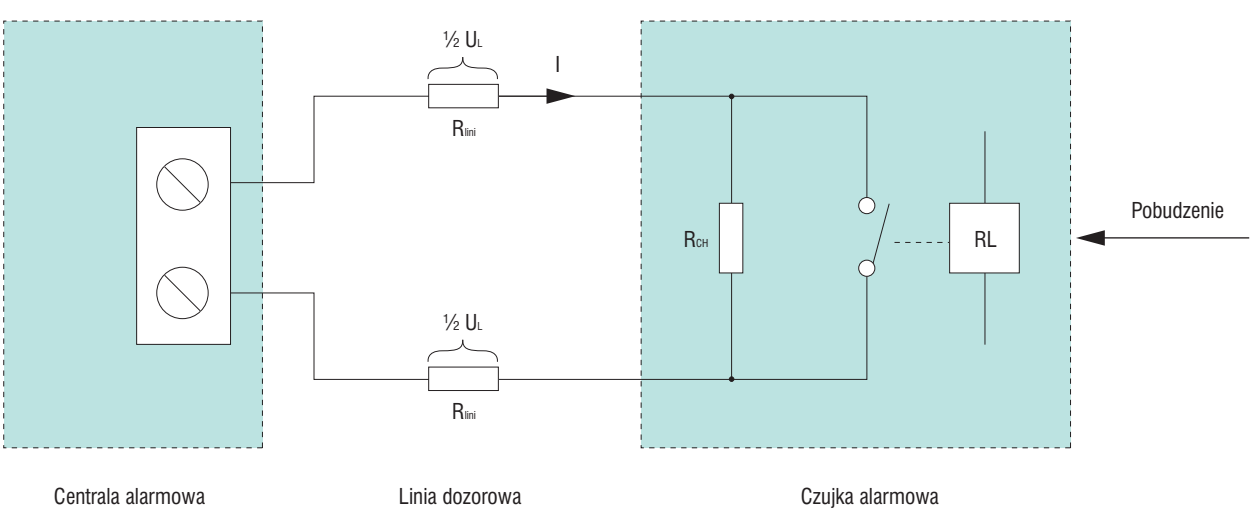
W liniach dozorowych parametrycznych pracujących w trybie trójstanowym można wyróżnić trzy stany linii, ale w pięciu przedziałach (jeśli chodzi o napięcie pojawiające się na wejściu linii dozorowych w centralach alarmowych). Stany linii dozorowych w trybie trójstanowym można podzielić na:

– stan sabotażu,

– stan alarmu,

– stan dozoru.

W tabeli 2 przedstawiono przykładowe przedziały napięć odpowiadające określonym stanom, które odczytuje centrala alarmowa.

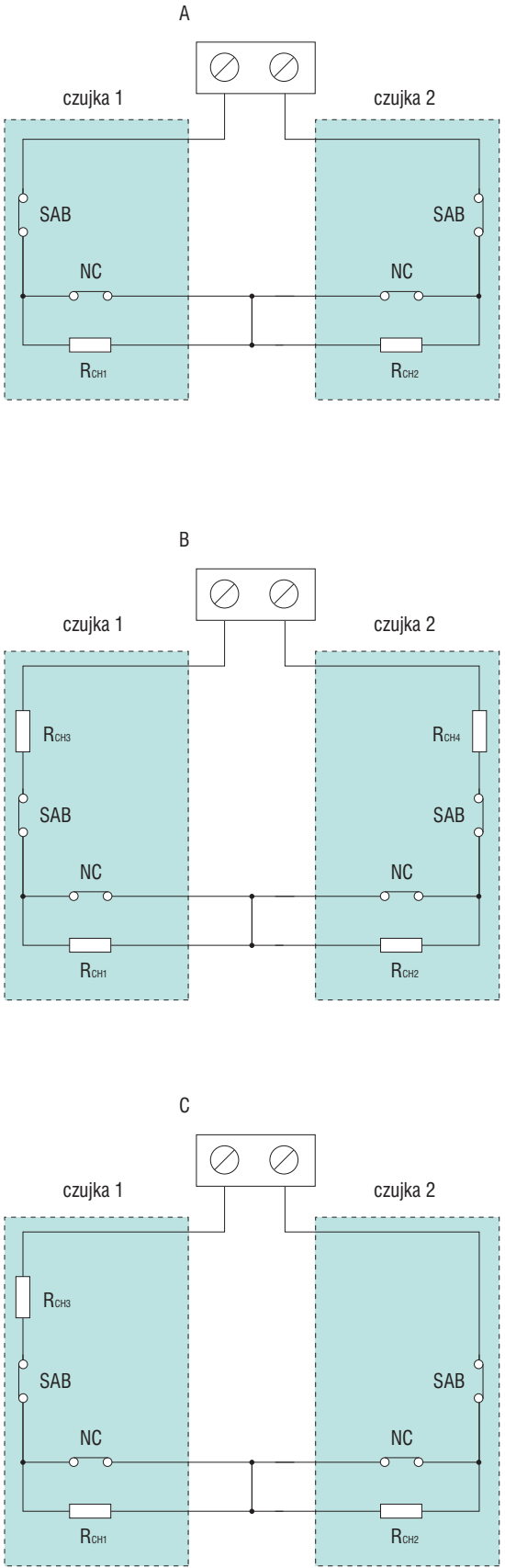


Rys. 4. Linia dozorowa z uwzględnieniem rezystancji przewodów

Podane w tabeli 2 wartości napięć są przykładowe i naturalnie zależne zarówno od wartości rezystorów charakterystycznych R_{CH}, jak i od długości linii dozorowej, a dokładniej jej rezystancji obliczonej z równania (2). Wartości tych napięć są także zależne od typu zastosowanej centrali alarmowej. Badania laboratoryjne dotyczyły polskiej centrali alarmowej.

Dawne centrale mikroprocesorowe posiadały wejścia linii dozorowych parametrycznych w układach mostkowych, gdzie rezystor charakterystyczny R_{CH} był składową mostka znajdującego się w równowadze. Zakłócenie tej równowagi oznaczało alarm. Układy mostkowe parametryczne linii dozorowych były wstępnie równoważone fabrycznie. Dokładne równoważenie tego mostka należało do instalatora i było czynnością pracochłonną i uciążliwą. Poza rezystorem charakterystycznym R_{CH} należało brać pod uwagę również rezystancję linii $R_{linii} = f(r, l, S)$. Kolejnym krokiem w budowie central alarmowych było wprowadzenie tzw. dyskryminatorów okienkowych realizowanych za pomocą układów komparacyjnych. Tego typu wejście do centrali alarmowej było zdefiniowane jako parametryczne dwu- lub trójstanowe. Mogło ono wprawdzie współpracować z linią dozorową o wielu podłączonych czujkach, ale niestety bez możliwości identyfikacji czujki znajdującej się w stanie alarmu. Dynamiczny rozwój technologii mikroprocesorowej stosowanej w budowie central alarmowych umożliwił wprowadzenie nowej jakości, która pozwala na pełne definiowanie właściwości linii na etapie jej konfigurowania przez projektanta i instalatora. Współczesne centrale alarmowe obsługiwane przez układy mikroprocesorowe zawierają 8- lub 10-bitowy przetwornik A/C (analogowo-cyfrowy). Stosowane układy mikroprocesorowe często zawierają multipleksery analogowe, które umożliwiają podłączenie do procesora ośmiu linii analogowych. W przypadku braku takiego multipleksera mikroprocesor centrali współpracuje z zewnętrznymi multiplekserami (umieszczonymi na płycie głównej). Każdy multiplekser obsługuje osiem wejść analogowych. Zwykle całkowita liczba wejść dozorowych centrali alarmowej jest wielokrotnością cyfry 8 (a więc: 8, 16, 32, 64, 128, 256, 512, 1024). Linie dozorowe podłączone są do wejść analogowych mikroprocesora poprzez układy dopasowania i układy zabezpieczające. Z powyższych rozważań wynika, że w typowym obwodzie centrali alarmowej mikroprocesorowej można wyróżnić następujące bloki:

– **układ zabezpieczający** mający za zadanie zabezpieczyć obwody wejściowe przed niebezpiecznymi przepięciami dodatnimi bądź ujemnymi (niestety układ taki nie chroni przed wyładowaniami atmosferycznymi); zwykle jest to układ typu RC lub wykorzystujący warystory, diody typu „Transil" albo kombinacje tych układów;
– **układy dopasowania** służące do dopasowanie poziomu napięcia w linii dozorowej do poziomu napięcia wejściowego przetwornika (zwykle wykorzystują dzielnik rezystancyjny obniżający maksymalne napięcie linii 13,8 V do maksymalnego napięcia przetwornika A/C, a więc do 5 V);
– **multiplekser analogowy** mający za zadanie cyklicznie podłączać kolejne linie dozorowe do przetwornika A/C;



Rys. 5. Sposób podłączenia dwóch czujek z antysabotażem („tamperem") do linii dozorowej podwójnej:
A – sposób konwencjonalny,
B – dzielone rezystory parametryczne,
C – dzielony jeden rezystor parametryczny.

– **przetwornik A/C (analogowo-cyfrowy)** zamieniający wielkość analogową, jaką jest wartość napięcia linii dozorowej (zależnie od stanu czujki), na wielkość cyfrową 8- lub 10-bitową.

Gdy zostanie zastosowany np. 8-bitowy przetwornik, mikroprocesor centrali alarmowej jest w stanie odczytać napięcie w linii dozorowej z dokładnością około 53 mV. Gdy zaś zostanie zastosowany przetwornik 10-bitowy, dokładność teoretyczna odczytu wynosi około 14 mV. Można więc zdefiniować wiele przedziałów w linii dozorowej i przypisać im określony stan systemu alarmowego. Tak zdefiniowana linia dozorowa doprowadzona do wejścia centrali alarmowej może pracować z wieloma czujkami podłączonymi do tej samej linii dozorowej. Istnieje więc możliwość zidentyfikowania miejsca, w którym dana czujka jest w stanie alarmu. Wykorzystując tę cechę, wielu konstruktorów central alarmowych wprowadziło możliwość zdefiniowania linii parametrycznej jako pojedynczej lub jako podwójnej. Nie stosuje się linii o większej krotności ze względu na:

– dostępną tolerancję rezystorów parametrycznych,
– zmienną rezystancję linii dozorowych wynikającą ze zmian rezystancji izolacji, np. na skutek zmian wilgotności,
– zmiany rezystancji przejścia zestyków przekaźnika w czujkach (zależne np. od czasu i jakości samych zestyków),
– potrzebę zachowanie niezbędnego marginesu w celu zapewnienia odporności na zakłócenia.

Istnieją różne warianty podłączenia czujek standardowych do linii podwójnej. Sposób podłączenia czujek został przedstawiony na rys. 5 (a, b, c). Warto zauważyć, że dla rozróżnienia która z dwóch czujek podłączonych do jednej linii dozorowej jest w stanie alarmu rezystory parametryczne podłączone równolegle do zestyków alarmowych NC powinny mieć różne wartości (R_{CH1}, R_{CH2}). Podobnie, w przypadku dzielonych rezystorów parametrycznych (rys. 5b), zróżnicowanie wartości rezystorów R_{CH3} i R_{CH4} pozwala na dokładniejsze zdiagnozowanie rodzaju zwarcia w linii dozorowej, jeśli takie się pojawi.

1.3. Linie adresowalne

W systemach alarmowych z liniami konwencjonalnymi (zwykłymi i parametrycznymi) centrala alarmowa jest w stanie zlokalizować miejsce alarmu z dokładnością do grupy czujek podłączonych do jednej linii. Zupełnie inaczej centrala alarmowa lokalizuje konkretną czujkę w systemie adresowalnym. Nasuwają się więc pytania:

– gdzie stosuje się systemy konwencjonalne?
– gdzie stosuje się systemy adresowalne?

Odpowiedź jest prosta i następująca:

– systemy z liniami konwencjonalnymi stosuje się w małych obiektach – gdy liczba zainstalowanych czujek nie przekracza kilkudziesięciu sztuk;
– systemy z liniami adresowalnymi stosuje się wówczas, gdy obiekt ma wiele pomieszczeń oraz gdy istotny jest czas samej instalacji oraz uruchamiania systemu alarmowego; należy je stosować również tam, gdzie istnieje duża liczba czujek w systemie, a nie jest możliwe

Lp.	Numer końcówki I_D	Kolor przewodu	Funkcja
1	1	żółty	L +
2	2	niebieski	L –
3	3	biały	przewód sterujący

Tab. 3.

Lp.	Odległość czujki od centrali alarmowej	Liczba czujek z modułami I_D
1	100 m	30
2	200 m	15
3	400 m	7
4	800 m	3

Tab. 4.

prowadzenie dużej liczby przewodów przy długości pojedynczej linii nie większej niż 100 m (maks. około 30 czujek).

Każda z czujek podłączonych do linii dozorowej adresowalnej jest wyposażona w moduł, który ma swój indywidualny numer identyfikacyjny ustalony przez projektanta i instalatora (lub ustalony fabrycznie). Tak więc informacja o numerach czujek zainstalowanych w systemie alarmowym wprowadzana jest do centrali przez instalatora na etapie jego konfigurowania. W praktyce spotyka się także wiele rozwiązań układowych współpracujących z liniami adresowalnymi. W pewnych rozwiązaniach moduły podłączone są za pomocą linii czteroprzewodowej, której przewody mają najczęściej następujące przeznaczenie:

– dwa przewody zasilania (napięcie znamionowe U_Z=12 V),
– jeden przewód synchronizacji (przy wspólnej masie),
– jeden przewód niosący właściwą informację (przy wspólnej masie).

Przy takim rozwiązaniu centrala alarmowa wysyła cyklicznie do linii adresowalnej impuls synchronizacji, po czym oczekuje na odbiór informacji o stanach wszystkich podłączonych czujek. Następuje więc cykliczne „przepatrywanie", przy którym każdy moduł w czujce ma swój moment czasowy pomiędzy impulsami synchronizującymi, w którym powinien on przesłać informację o swoim stanie. Istnieje jednak rozwiązanie zwane I_D (ang. *Intelligent Device* – inteligentne rozwiązanie), w którym w ściśle określonych interwałach czasowych każdy moduł (lub większa ich liczba) podłączony do adresowalnej linii dwuprzewodowej wysyła cyklicznie dwa sygnały impulsowe, a mianowicie:

– sygnał informacyjny o stanie czujki, z którą jest połączony,
– sygnał, tzw. diagnostyczny, o poprawności pracy.

System alarmowy wykonywany w technologii I_D jest typowy dla systemów adresowalnych. Technologia I_D jest więc bardzo wygodna, jeśli chodzi o minimalizację liczby przewodów, czasu instalacji systemu i jego uruchamiania. W technologii I_D są stosowane wyspecjalizowane układy scalone, które umożliwiają nadawanie czujkom indywidualnych adresów. Wszystkie moduły podłączone są do dwuprzewodowej linii dozorowej, która jest jednocześnie linią zasilającą i sygnałową. Musi być jednak zapewniona osobna linia do zasilania czujek. Zwykle do jednej linii można podłączyć do 30 modułów typu I_D w zupełnie dowolnej kolejności. Każdy moduł podłączony do pojedynczej linii musi mieć inny numer (adres). Moduły typu I_D mają możliwość reagowania na pole magnetyczne, a więc mogą zastąpić typową rurkę kontaktronową. Zwykle moduły typu I_D są produkowane jako:

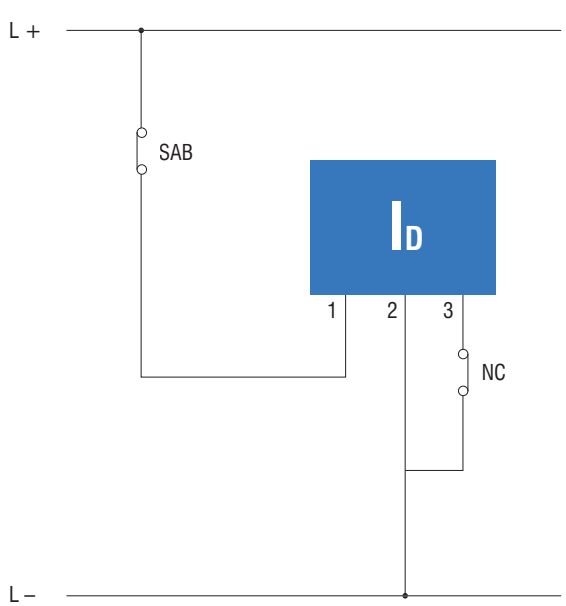
– moduły I_D wkładane do podstawki w czujkach wykonanych w technologii I_D. Moduł pakowany jest w kapsułę (z tworzywa sztucznego), zwaną „biscuitem", o kształcie umożliwiającym włożenie go do gniazda tylko w jeden określony sposób;
– moduły I_D z wyprowadzonymi przewodami mogą być przeznaczone do współpracy ze standardowymi czujkami;
– zestyki kontaktronowe typu I_D mają średnicę standardową, np. Ø =10 i 20 mm.

Moduł typu I_D wyposażony jest w trzy przewody. Oznaczenia przewodów zestawiono w tabeli 3.

Na rys. 6 przedstawiono podłączenie modułu I_D do standardowej czujki, tak aby mogła ona współpracować z linią adresowalną.

Czujka połączona jest z centralą alarmową kablem czterożyłowym, w którym można wyróżnić: dwie żyły do zasilania czujki i dwie żyły linii I_D. Przy wykorzystaniu modułu I_D jako kontaktronu przewód sterujący będzie niewykorzystany. Jak już wspomniano, każdy moduł I_D ma własny adres. Moduły I_D produkowane są z adresami od 1 do 30.

Przy przekroju pojedynczej żyły klasycznego przewodu instalacyjnego S = 0,2 mm^2 (czyli o średnicy d = 0,5 mm) można podłączyć (wg danych fabrycznych, zależnie od odległości od centrali) liczbę czujek zgodną z tabelą 4.



Rys. 6. Układ podłączenia modułu I_D do zestyków NC przekaźnika w czujce standardowej

Spostrzeżenia i wnioski

Niniejszy artykuł dotyczy głównie linii dozorowych stosowanych w systemach sygnalizacji włamania. Następna część (3) cyklu artykułów będzie dotyczyła głównie problemów transmisji pomiędzy poszczególnymi elementami systemu. Wracając jednak do części 2 niniejszego artykułu, można sformułować następujące spostrzeżenia i wnioski dotyczące sposobów konfigurowania wejść (linii dozorowych) współczesnych central alarmowych:

a) Opcja NC (ang. *Normally Closed* – normalnie zwarte) to wejście zaprogramowane w ten sposób, że jest kontrolowane tylko zwarcie lub rozwarcie linii dozorowej. W momencie wystąpienia alarmu przekaźnik lub jego zestyk w detektorze (czujce) rozwiera się i przez centralę alarmową generowany jest sygnał alarmu.

b) Opcja NO (ang. *Normally Open* – normalnie otwarte) to lustrzane odbicie poprzedniego stanu podłączenia. Różnica polega na tym, że podczas alarmu wejście jest zwierane do masy. Podczas normalnego stanu centrali alarmowej wejście pozostaje rozwarte. Należy się jednak liczyć również z tym, że każde zwarcie przewodu będzie wywoływało alarm.

c) Opcja EOL NC (EOL *Normally Closed* – normalnie zwarte sparametryzowane) oznacza zwieranie wejścia ograniczonego rezystorem końca linii (EOL – ang. *End of Line*), np. 2,2 kΩ. Różnica między połączeniem NC, a EOL NC polega na tym, że w pierwszym przypadku potencjalny intruz ma możliwość zwarcia przewodów linii dozorowej masy i linii przed czujką, przy braku możliwości wykrycia alarmu w momencie, np. otwarcia drzwi, w których był zainstalowany kontaktron (czujka magnetyczna). Sparametryzowanie linii dozorowej rezystorem wymusza na intruzie konieczność zwarcia linii z użyciem rezystora. Jest to jednak opcja o wiele trudniejsza, a błąd kończy się najczęściej sygnałem alarmowym.

d) Opcja EOL NO (EOL *Normally Open* – normalnie otwarte i sparametryzowane). W takim przypadku również mamy lustrzane odbicie w stosunku do EOL NC i sytuacja jest dokładnie odwrotna. W momencie czuwania linia dozorowa jest otwarta oraz sparametryzowana jednym rezystorem.

e) Opcja 2EOL NC (2EOL *Normally Closed* – normalnie zwarte i podwójnie sparametryzowane). Linia dozorowa podwójnie sparametryzowana dwoma rezystorami umożliwia odróżnienie przez jedną linię dozorową stanów: sabotażu, alarmu i przecięcia linii dozorowej. Zastosowanie dwóch rezystorów (np. po 8 kΩ) pozwala centrali alarmowej rozróżnić, czy wystąpił alarm (gdy rezystancja na wejściu wynosi 8 kΩ), czy sabotaż (gdy centrala alarmowa „widzi" 2 × 8 kΩ, a więc 16 kΩ). Można więc stwierdzić, że potencjalnemu intruzowi w znaczący sposób utrudniono wywołanie sabotażu. Znacznie również ograniczono liczbę przewodów niezbędną do podłączenia, np. czujki PIR – do czterech lub (gdy istnieje wyższa konieczność) do trzech przewodów łącznie z zasilaniem 12 V.

f) Opcja 2EOL NO (2EOL *Normally Open* – normalnie otwarte i podwójnie sparametryzowane). Zasadnicza różnica w stosunku do opcji 2EOL NC dotyczy stanu linii dozorowej podczas czuwania i stanu alarmu. Faktycznie polega ona na zmianie polaryzacji w przekaźniku czujki przy przejściu z jednego z tych stanów do drugiego z nich.

g) Opcja linii dozorowych, gdzie zastosowano łącza radiowe typu on-line (a więc z potwierdzeniem), stanowi odrębny problem, o którym wspominano już wcześniej. W grę wchodzą zasięgi wynikające z konstrukcji obiektu. Zupełnie inaczej wygląda problem alarmu sabotażowego, który powstaje na przykład w wyniku przerwania łączności między czujką a modułem radiowym lub z powodu uszkodzonej baterii zasilającej czujkę.

doc. dr inż. Waldemar Szulc
Wyższa Szkoła Menedżerska w Warszawie,
Wydział Informatyki Stosowanej,
Zakład Bezpieczeństwa Obiektów i Informacji,
współpracownik: Wojskowa Akademia Techniczna,
Wydział Elektroniki.

dr inż. Adam Rosiński
Wyższa Szkoła Menedżerska w Warszawie,
Wydział Informatyki Stosowanej,
Zakład Bezpieczeństwa Obiektów i Informacji.

Bibliografia:

1. Haykin S.: *Systemy telekomunikacyjne*. Tom I i II. WKiŁ, Warszawa 2004.
2. Horowitz P., Hill W.: *Sztuka elektroniki*. Tom I i II. WKiŁ, Warszawa 2006.
3. Instrukcje serwisowe firm AAT i SATEL oraz dotyczące central GALAXY i RANKOR.
4. Kula S.: *Systemy teletransmisyjne*. WKiŁ, Warszawa 2004.
5. Kurdziel R.: *Podstawy elektrotechniki*. WNT, Warszawa 1972.
6. Maksymowicz R.: *Linie dozorowe central alarmowych*. *Systemy alarmowe*. Nr 5/98, Warszawa 1998.
7. Nawrocki W.: *Komputerowe systemy pomiarowe*. WKiŁ, Warszawa 2006.
8. Norma: PN-EN 50131-1.
9. Szulc W., Rosiński A.: *Analiza niezawodnościowa złożonego systemu bezpieczeństwa dla obiektu o specjalnym przeznaczeniu*. *Zabezpieczenia* Nr 4 (56)/2007, wyd. AAT, Warszawa 2007.
10. Szulc W., Rosiński A.: *Problemy eksploatacyjno-niezawodnościowe rozproszonego systemu bezpieczeństwa. Zabezpieczenia* Nr 1 (47)/2006, wyd. AAT, Warszawa 2006.
11. Szulc W., Rosiński A.: *Prace własne*. WSM, Warszawa 2006–2008.
12. Szulc W., Rosiński A.: *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków* (część I – analogowa). Oficyna Wydawnicza WSM, Warszawa 2008.

Wysterować, ale jak?
UCS 4000 bez tajemnic

W numerze 2/2007 czasopisma *Zabezpieczenia* ukazał się artykuł opisujący nowy produkt firmy POLON-ALFA, który uzupełnia rodzinę central systemu POLON 4000. Uniwersalna centrala sterująca UCS 4000, bo o niej mowa, została w tym artykule dość szeroko opisana pod kątem jej funkcjonalności. Niniejszy artykuł przedstawia konkretne sposoby wykorzystania tej centrali

Uniwersalna centrala sterująca UCS 4000 stanowi znakomite uzupełnienie gamy urządzeń adresowalnego systemu sygnalizacji pożarowej POLON 4000.

Przypomnijmy, że centrala UCS 4000 posiada:
- przekaźnik główny potencjałowy P1,
- przekaźniki dodatkowe P2 i P3 (przy wykorzystaniu pakietu PSD-4000),
- linie kontrolne dla stanu dozorowania i alarmu,
- konwencjonalną linię dozorową,
- linię dla przycisków oddymiania,
- linię przeznaczoną do uruchomienia oddymiania przez zewnętrzny system sygnalizacji pożarowej.

Ze względu na wyposażenie oraz funkcjonalność centrali możliwa jest jej współpraca z kilkoma rodzajami urządzeń. W niniejszym artykule zostaną omówione przykłady połączeń, które w projektach z zastosowaniem systemów oddymiania występują najczęściej.

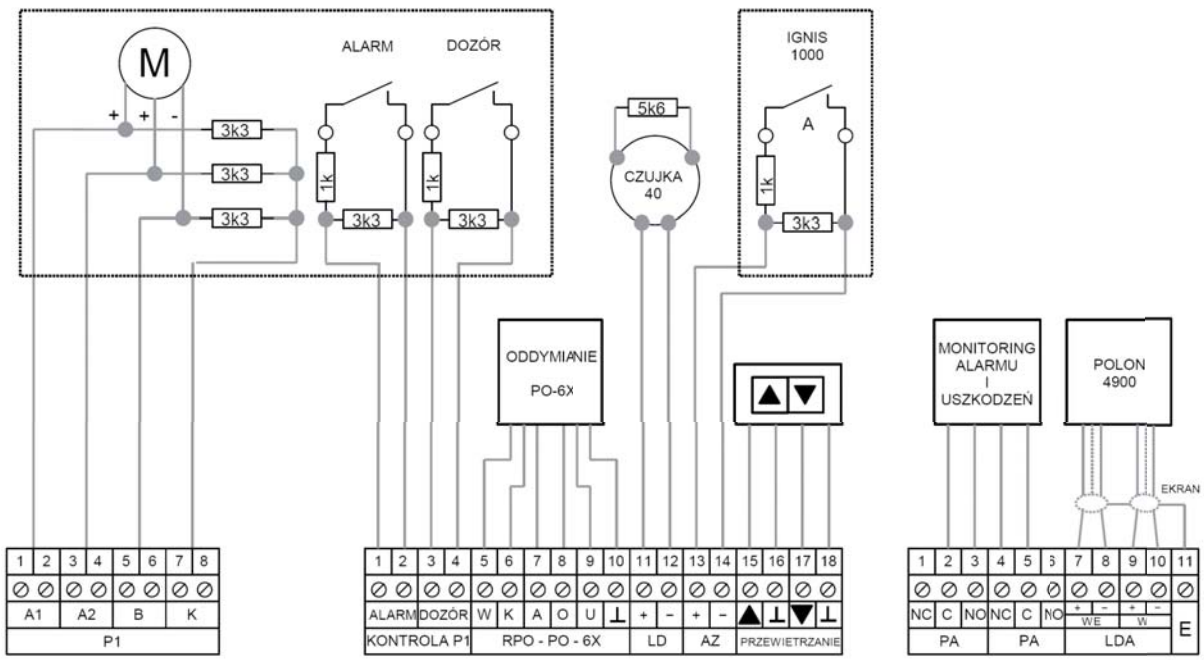
Podłączenie popularnych siłowników

Najczęściej występujące na rynku siłowniki to urządzenia sterowane 2-przewodowo. Ich uruchomienie realizowane jest poprzez podanie napięcia znamionowego na dwa zaciski zasilania, w celu zamknięcia siłownika natomiast polaryzacja tego napięcia jest odwracana.

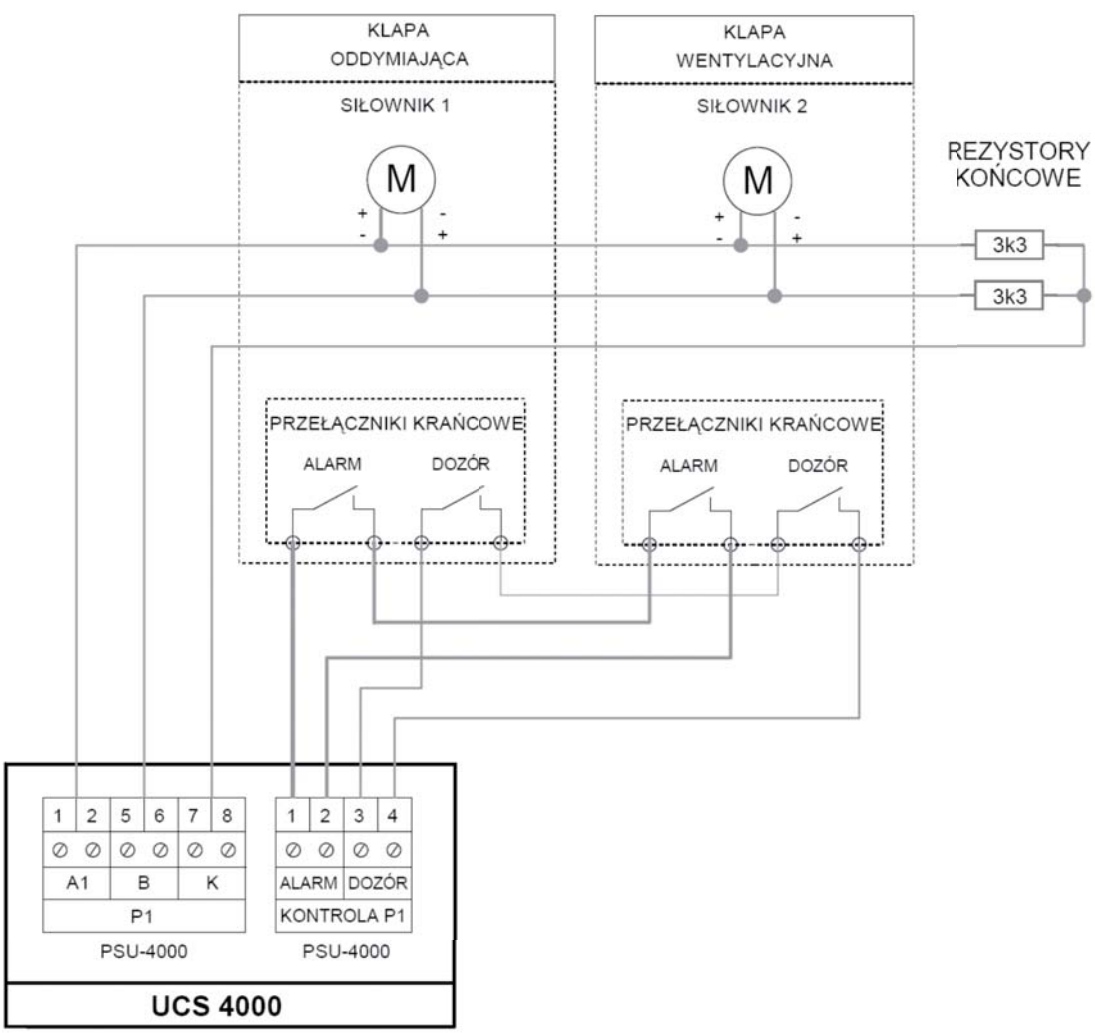
Centrala UCS 4000 realizuje tę funkcję za pomocą przekaźnika P1 ustawionego w trybie 1.

Ustawienia te są niezależne od pracy indywidualnej centrali lub pracy w systemie POLON 4000. Praca z urządzeniami zasilanymi 2-przewodowo realizowana jest poprzez połączenie wyjść przekaźnika głównego P1 z zaciskami A1, B i K. Zaciski A1 oraz B przeznaczone są do zasilania urządzenia, zacisk K służy do podłączenia wspólnej żyły w celu kontroli sprawności linii zasilającej.

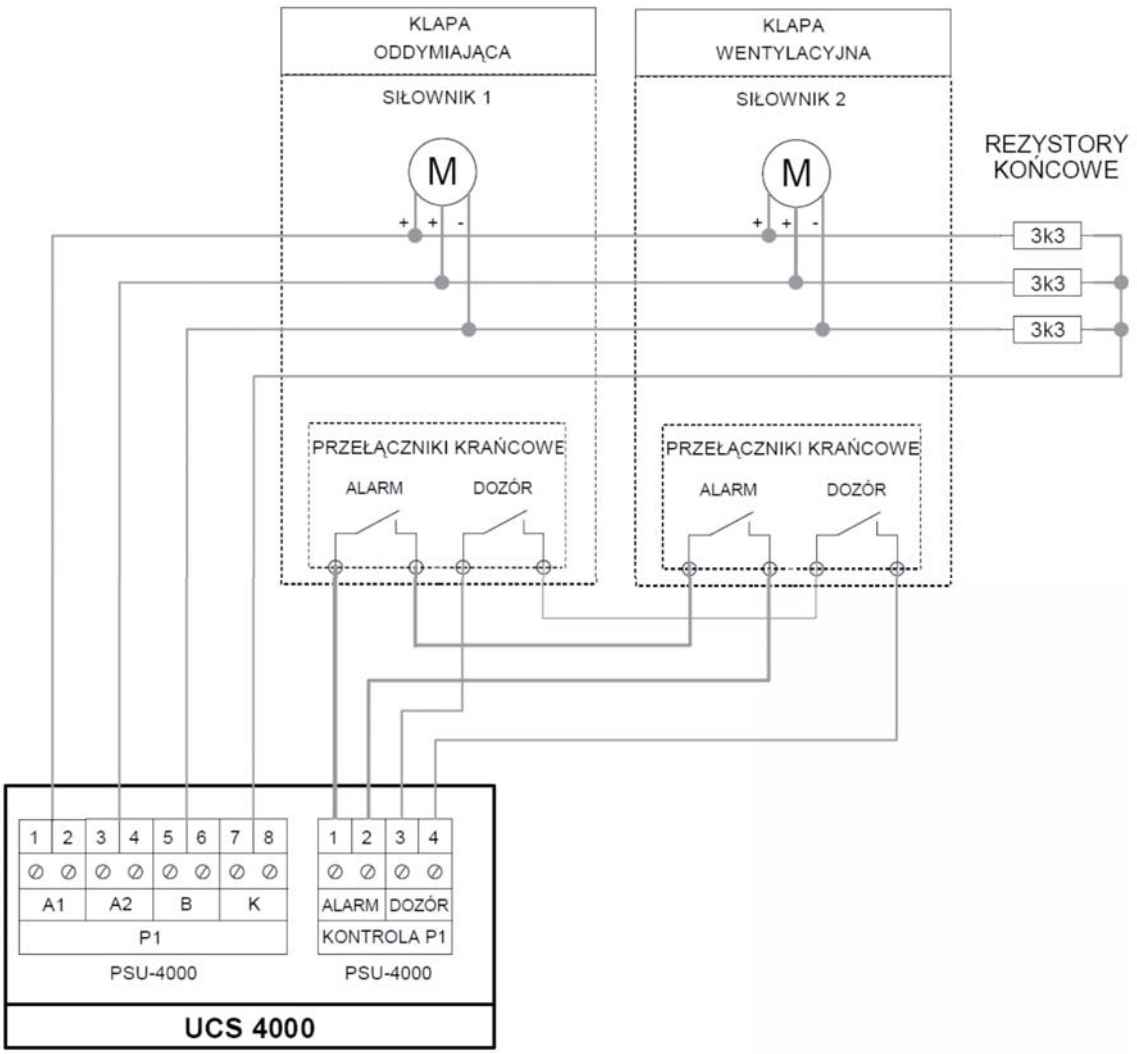
Przygotowanie centrali do pracy wymaga zadeklarowania typu pracy przekaźnika P1 oraz sposobu realizacji zasilania. Ze względu na różne typy urządzeń istnieje możliwość wyboru pracy za pomocą: impulsu zasilania, przerwy zasilania, zasilania ciągłego lub odcinania zasilania. Urządzenia klap oddymiających wyposażone są zazwyczaj w siłowniki wrzecionowe lub łańcuchowe i wymagają zasilania przez cały okres realizacji napędu.



Rys. 1. Schemat przykładowego połączenia centrali UCS z różnymi urządzeniami



Rys. 2. Połączenie centrali UCS z urządzeniami sterowanymi 2-przewodowo wraz z realizacją kontroli stanu urządzeń

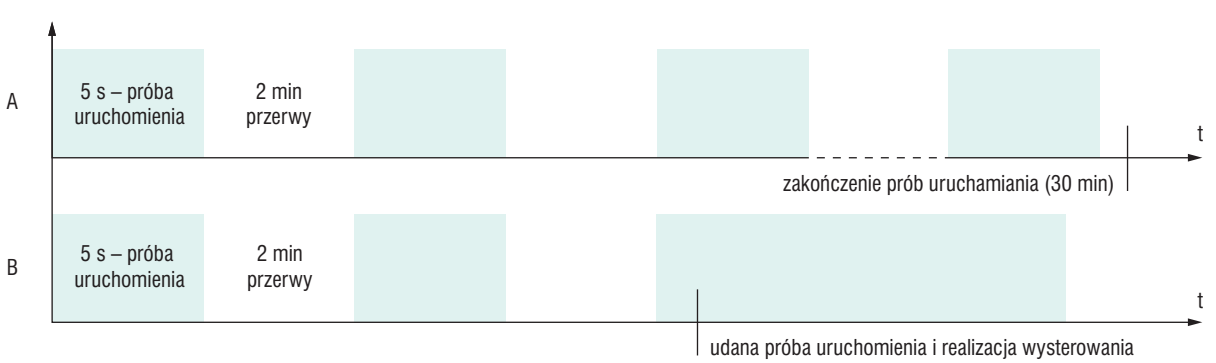


Rys. 3. Realizacja sterowania urządzeniami wymagającymi 3-przewodowego zasilania

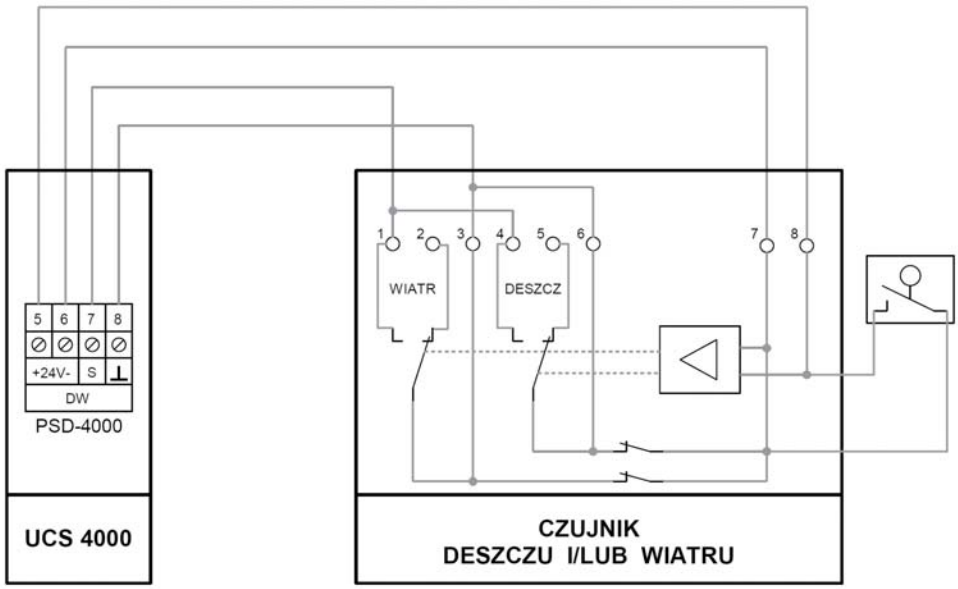
Podłączenie siłowników 3-przewodowych

W ofercie napędów urządzeń automatyki pożarowej siłowniki 3-przewodowe stanowią mniejszość. Z napędami tego typu centrala UCS 4000 łączy się, korzystając z łączówek A1, A2, B i K wyjść przekaźnika głównego P1. Ten sposób zasilania odbywa się w chwili zmiany kierunku pracy napędu poprzez przełączenie bieguna dodatniego pomiędzy łączówkami A1 i A2 przy zachowaniu na łączówce B stałego bieguna zasilania ujemnego i kontroli ciągłości zasilania poprzez łączówkę K.

Tryb pracy impulsowej ustawia się identycznie jak w przypadku opisanego wcześniej trybu pracy 2-przewodowej.



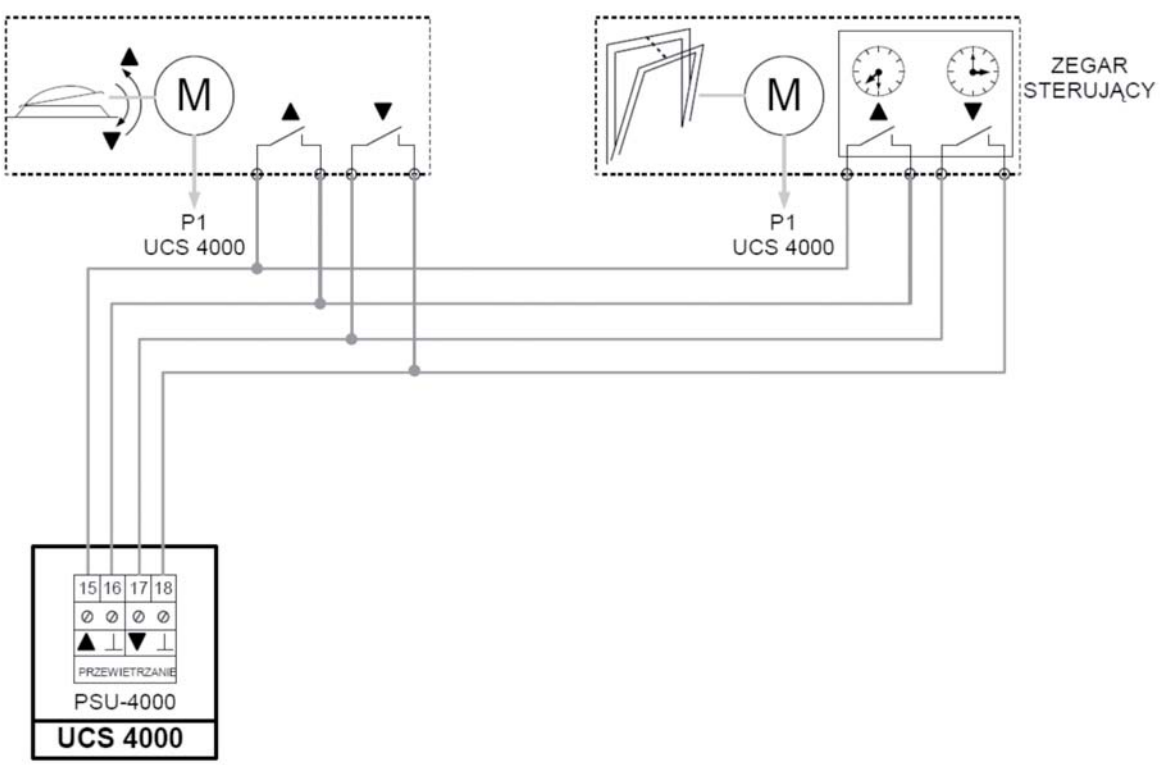
Rys. 4. Realizacja funkcji „Dead-Lock": A – nieudane wysterowanie B – wysterowanie zakończone sukcesem



Rys. 5. Schemat współpracy centrali z automatyką pogodową

Lód na klapach i oporne siłowniki

Rzeczywiste warunki pracy pożarowych klap dymowych oraz innych urządzeń automatyki mają również swoje ciemne strony. Pierwsza z nich – to zmienne zjawiska pogodowe i możliwość wystąpienia oblodzenia klap. Druga natomiast wynika m.in. z faktu starzenia się środków smarujących napęd we wnętrzu siłownika. Wystąpienie takich zjawisk może spowodować utrudnienie startu napędu siłownika, a w skrajnych przypadkach nawet unieruchomienie klap. Centrala UCS 4000 jest przygotowana na możliwość pojawienia się podobnych trudności i w takich sytuacjach uruchamia tzw. działanie przeciwko zablokowaniu klap („Dead-Lock"). Przy ustawieniu pracy w trybie 1 i uaktywnieniu tej opcji centrala przez 30 minut będzie forsowała uruchomienie siłownika za pomocą pięciosekundowych impulsów powtarzanych co 2 minuty.



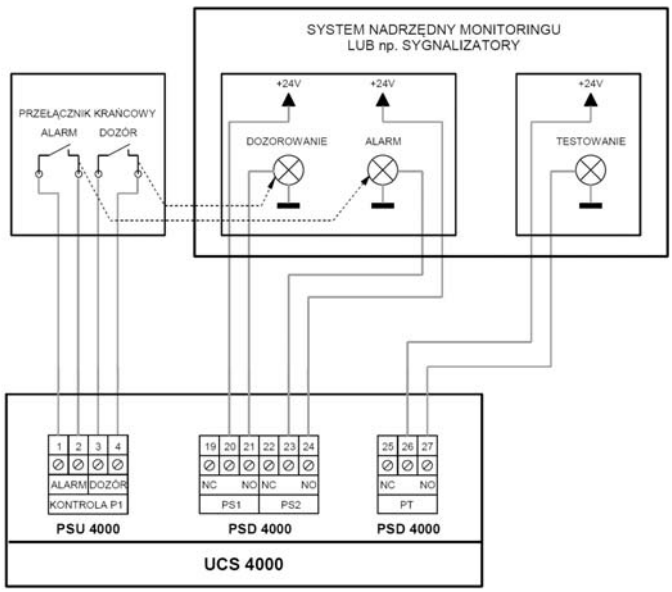
Rys. 6. Realizacja sterowania przewietrzaniem za pomocą zegarów oraz przycisków sterujących

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

SYGNAŁ BEZPIECZEŃSTWA

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

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



Rys. 7. Wizualizacja stanu sterowanego urządzenia przy użyciu przekaźników P2 i P3 pakietu PSD-4000

Dzięki monitorowaniu stanu zestyków krańcowych położenia dozorowania i alarmu centrala może stwierdzić, czy udało się ostatecznie uruchomić napęd i czy rozpoczęło się otwieranie klapy. Potwierdzenie skutecznej próby uruchomienia urządzenia sprawia, że centrala przechodzi do realizacji funkcji przypisanej do przekaźnika zgodnie z ustaleniami, czyli albo do chwili otwarcia potwierdzonego zmianą stanów krańcowych styków, albo do zakończenia zaprogramowanego czasu otwierania.

Przewietrzanie

Centrala UCS 4000 została wyposażona w funkcję przewietrzania i możliwość podłączenia centralki pogodowej.

Przyciski sterujące przewietrzaniem włączamy do zestyków 15-18 pakietu PSU-4000 w zależności od sposobu zasilania siłowników elektrycznych dwukierunkowych (praca przekaźnika P1 w trybie 1). Sposób pierwszy to otwieranie lub zamykanie tylko w tym czasie, gdy naciśnięty jest odpowiedni przycisk. Sposób drugi to pełne otwarcie lub zamknięcie po jednorazowym naciśnięciu przycisku.

Przy korzystaniu z funkcji przewietrzania należy pamiętać o ograniczeniach, które wynikają z normy EN12101. Gdy zasilanie centrali UCS 4000 realizowane jest z akumulatorów zasilania rezerwowego, przewietrzanie przestaje działać. Podobnie dzieje się wówczas , gdy automatyka centralki pogodowej stwierdzi przekroczenie ustalonych parametrów prędkości wiatru lub wystąpienie opadów deszczu.

Z punktu widzenia sterowania urządzeniami podłączonymi do centrali UCS 4000 najwyższym priorytetem jest stan alarmu pożarowego bądź uruchomienie oddymiania poprzez przyciski PO-63. Przejście w stan alarmu powoduje w centrali ignorowanie zarówno przycisków przewietrzania odpowiedzialnych za zamykanie, jak i ignorowanie informacji z centrali pogodowej.

Dla centrali UCS 4000 nie stanowią problemu również duże obiekty, gdzie przewija się znaczna liczba osób bądź występują takie warunki, które powodują konieczność automatycznego przewietrzania. Połączenie funkcji przewietrzania z zegarami sterującymi da możliwość automatycznej wymiany powietrza w określonym czasie. W tym przypadku istnieje również możliwość połączenia funkcji przewietrzania z systemem zarządzania budynkiem. System ten zrealizuje wówczas przewietrzanie o odpowiednich porach, przykładowo w okresie letnim w razie wystąpienia wyższych temperatur w ciągu dnia.

Praca samodzielna i konieczność sygnalizacji stanu centrali

Uniwersalna centrala sterująca UCS 4000 ma możliwość pracy samodzielnej. W takim przypadku może zaistnieć konieczność wizualizacji stanu pracy sterowanego urządzenia. Dzięki programowalnym przekaźnikom pakietu PSD-4000 istnieje możliwość przedstawienia stanu styków urządzenia podłączonych do centrali UCS 4000.

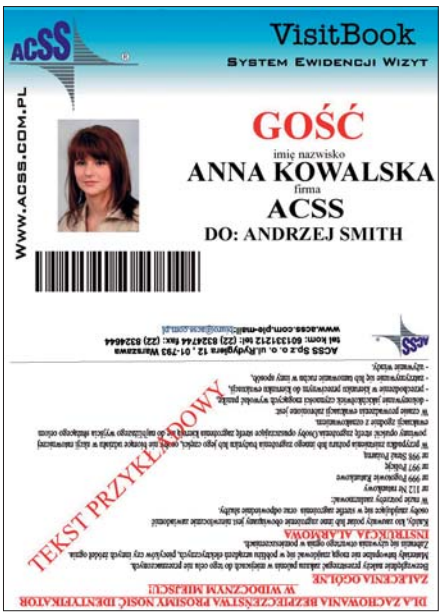
Takie rozwiązanie sprawi, że w ramach zintegrowanego systemu sterowania oddymianiem zostanie na przykład zobrazowane położenie przeciwpożarowych klap dymowych w odległych pomieszczeniach.

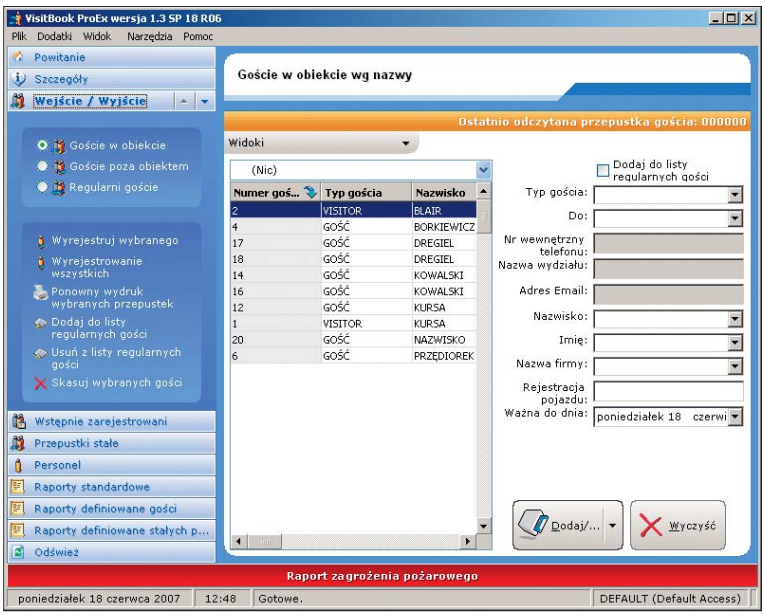
Przedstawione sposoby połączenia centrali UCS 4000 z urządzeniami automatyki pożarowej stanowią jedynie fragment oferowanych przez nią możliwości. Realizacja innych funkcji tej centrali i konkretne sposoby jej podłączenia zależne są zarówno od urządzeń przeznaczonych do sterowania oraz ich wymagań elektrycznych, jak i od scenariusza pożarowego określającego całą hierarchię działań.

Mariusz Sowiński
Krzysztof Marchlewski
„POLON-ALFA" Zakład Urządzeń Dozymetrycznych

ZABEZPIECZENIA 3/2009 88

System rejestracji gości VisitBook





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

System rejestracji gości VisitBook jest narzędziem służącym do wspomagania pracy recepcji. Zastępuje papierową księgę gości – jest jej elektronicznym odpowiednikiem. System umożliwia rejestrację danych osób 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 stosując czytnik kodów kreskowych. Program VisitBook jest dostępny w czterech wersjach: Lite, Pro, ProEx i xFR.

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.

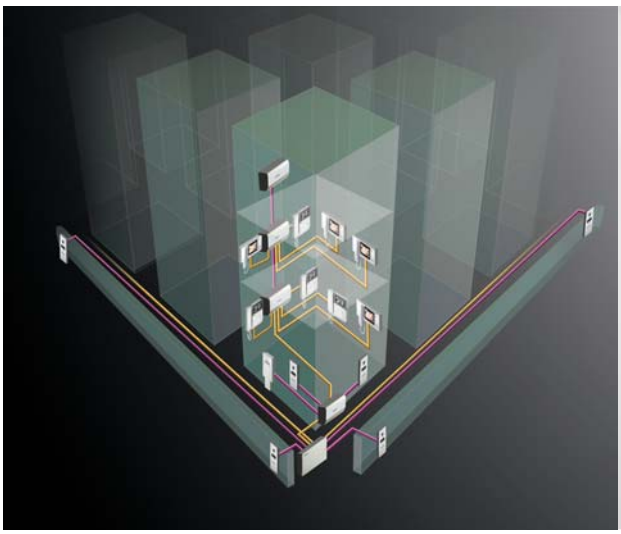
ProEx jest wersją bardziej rozbudowaną w porównaniu do wcześniejszych. Umożliwia wydruk przepustki wraz ze zdjęciem i zawiera m.in. funkcję projektowania własnych wzorów przepustek.

Podstawową zaletą różniącą czwartą wersję xFR od pozostałych jest zastosowana w niej platforma SQL zapewniająca szybkość i niezawodność obsługi dużych, ruchliwych obiektów.

Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera kilka użytecznych funkcji, takich jak: manager personelu, manager kontrahentów, obsługa konferencji.

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

System wieloabonentowy serii 2400



Elementy systemu:

Monitory / Unifony

CAV-51M

APV-4PM

CAV-51AM

AP-5HM

1 przewód . . . . . wiele możliwości

Stacje bramowe

DRC-MSC/MSB
DRC-OSC/OSB

DRC-nSC/nSB

DR-nSB

DR-nMS

Dystrybutory

CCU-OS

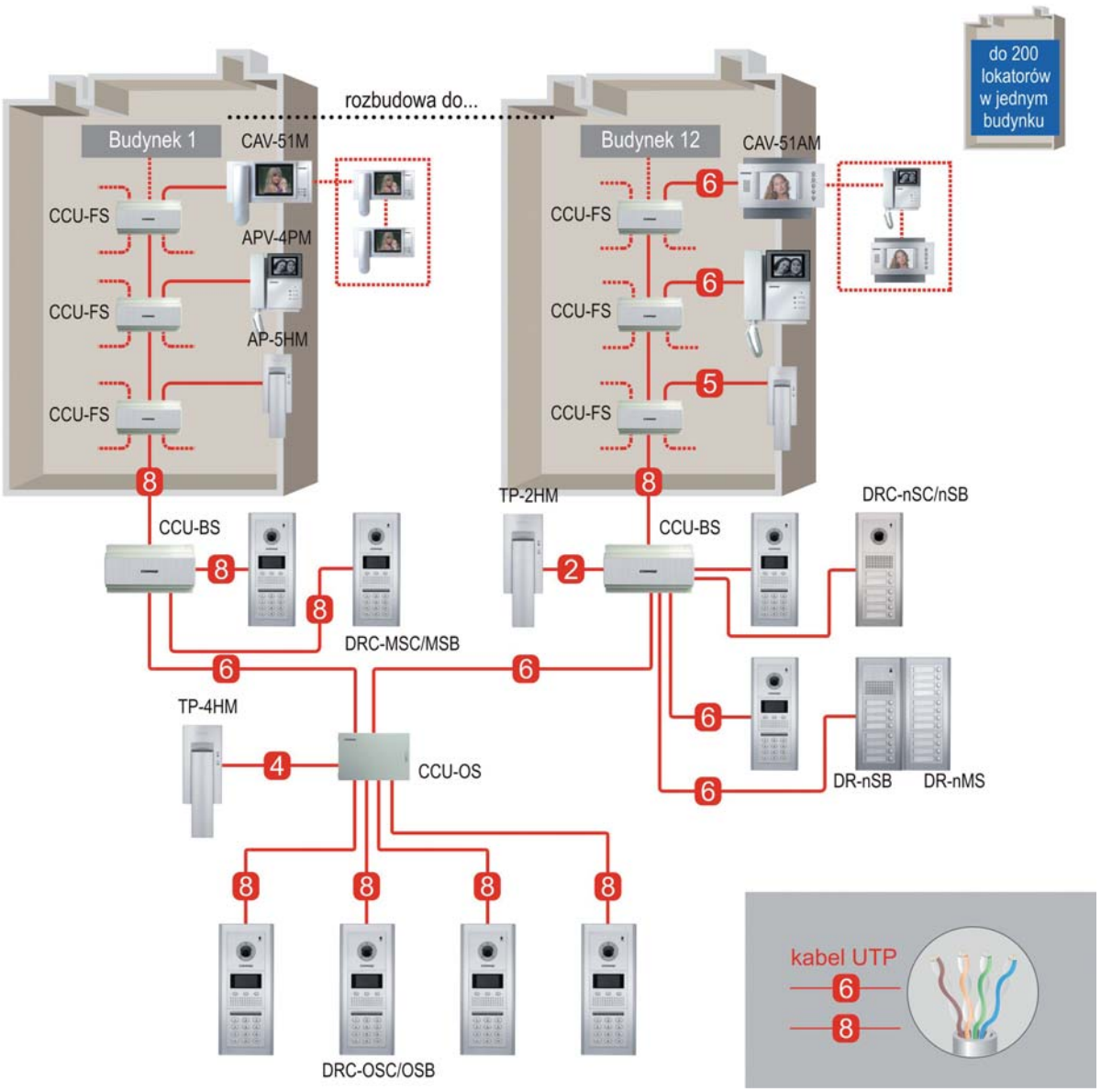
CCU-BS
CCU-FS

GDE POLSKA
Global Distributor of Electronics

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

System wieloabonentowy serii 2400



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

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

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak wideo - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów).

System może być wyposażony w unifon instalowany w portierni, przez co lokatorzy mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków, jak i całych osiedli zamkniętych, gdzie ogrodzonych może być kilkanaście budynków, a całość nadzorowana przez kilku portierów.

GDE POLSKA
GLOBAL DISTRIBUTOR OF ELECTRONICS

GDE Polska
ul. Koniecznego 46
32-040 Świątniki Górne

tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

Kamera termowizyjna serii TI2500

stała kamera ze zintegrowaną optyką

Cechy produktu

– Podczerwień długofalowa (LWIR), niechłodzony mikrobolometr z tlenkiem wanadu
– Rozdzielczość 320 x 240, rozmiar piksela - 38 mikronów
– Czułość poniżej 85mK przy f/1.4
– Programowalne ustawienia kamery
– Moduł łącznikowy dla zasilania wejściowego 24 V_{AC} / 24 V_{DC}
– Analogowe wyjście wideo NTSC/PAL
– 2x zoom cyfrowy
– 3 opcje obiektywu (35 mm, 50 mm oraz 100 mm)
– Sterowanie ostrością i funkcją zoom za pomocą protokołu Pelco D (jedynie model TI25100)
– Zaprojektowane dla maksymalnej ochrony przed deszczem
– Kompaktowa i lekka konstrukcja z aluminium
– Spełnia normy NEMA Type 4X oraz IP66
– W komplecie z osłoną przeciwsłoneczną oraz urządzeniem nagrzewającym

Seria **TI2500** to kompletne, zintegrowane i zaawansowane urządzenia termowizyjne w obudowie Pelco przeznaczone do stosowania na zewnątrz lub wewnątrz. Sercem urządzenia jest niechłodzona kamera LWIR, zbudowana na bazie mikrobolometru (38 mikronów) z tlenkiem wanadu. Kamera termowizyjna dostarcza obrazy wideo o rozdzielczości 320 x 240 i posiada dwukrotny zoom cyfrowy.

Seria **TI2500** charakteryzuje się również wysoką czułością, na poziomie poniżej 85mK przy f/1.4. Umożliwia wyświetlanie w wielu formatach, np. białe-gorące, czarne-gorące oraz schematy kolorowe. Seria **TI2500** jest dostępna z trzema różnymi obiektywami (długość ogniskowej 35, 50 i 100 mm) dla efektywnego wykorzystania, zależnie od wymogów.

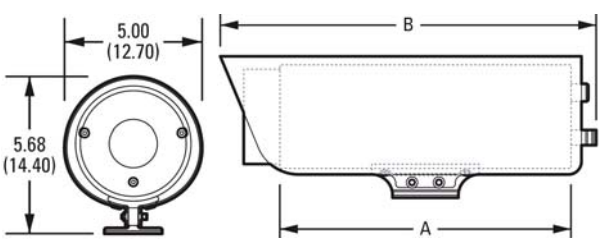
Dzięki aluminiowej, malowanej proszkowo konstrukcji obudowy seria **TI2500** jest idealna do stosowania wewnątrz i na zewnątrz pomieszczeń. Dzięki szerokiemu zakresowi temperatur roboczych – od -25° do 131°F (od -32° do 55°C) – urządzenia mogą być stosowane w wielu różnych miejscach.

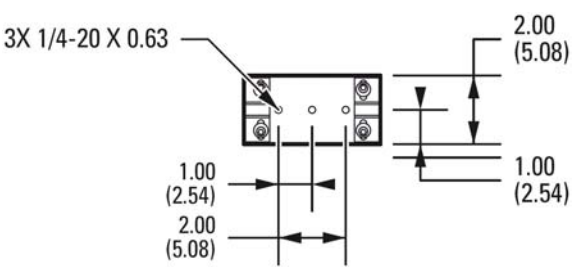
Osłona przeciwsłoneczna oraz sterowane termostatycznie urządzenie nagrzewające stanowią standardowe wyposażenie serii **TI2500**.

Kamera serii **TI2500** rozpoczyna przesyłanie obrazu już po 5 sekundach od czasu uruchomienia pod warunkiem, że temperatura otoczenia mieści się w zakresie temperatur pracy.

Serię **TI2500** zasila napięcie wejściowe 24 V_{AC} lub 24 V_{DC}.

Kamery **TI2535** oraz **TI2550** są fabrycznie wyregulowane (ostrość ustawiona na nieskończoność), jednakże istnieje możliwość ich regulacji przez uprawnionego konserwatora. Kamera TI2500 jest wyposażona w funkcję zdalnego ustawiania ostrości w zakresie odległości od 9,8 stóp (3m) aż do nieskończoności.





	A	B
2535	8.00 (20.32)	10.50 (26.60)
2550		
25100	12.00 (30.48)	14.50 (36.83)

t.a.c by Schneider Electric
TAC Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10, faks (22) 313 24 11
e-mail: tac_pol@tac.com
http://www.tac.com/pl

Kamera termowizyjna serii TI2500

stała kamera ze zintegrowaną optyką

Modele		
Numer modelu	**Format**	**Odległość ogniskowa**
TI2535	NTSC	35 mm
TI2535-X	PAL	35 mm
TI2550	NTSC	50 mm
TI2550-X	PAL	50 mm
TI25100	NTSC	100 mm
TI25100-X	PAL	100 mm
TI2535-1	NTSC, 9 Hz	35 mm
TI2535-X-1	PAL, 9 Hz	35 mm
TI2550-1	NTSC, 9 Hz	50 mm
TI2550-X-1	PAL, 9 Hz	50 mm
TI25100-1	NTSC, 9 Hz	100 mm
TI25100-X-1	PAL, 9 Hz	100 mm

Informacje mechaniczne	
Blokowanie	2 sześciokątne śruby blokujące
Płyta przednia	2 śruby sześciokątne
Wejścia dla przewodów	2 regulowane, 0,5-calowe (NPT) zaciskane wodoszczelne

Informacje elektryczne	
Połączenia	Listwa z zaciskami śrubowymi (16 – 24 Gauge) na płycie przyłączeniowej (zaciski polaryzowane)
Moc pobierana	4 W, 6.2 VA nominalnie
Napięcie wejściowe	
24 V_{AC} 24 V_{DC}	18 – 27 V_{AC} 14 – 32 V_{DC}
Pobór mocy, 24 V_{AC}	
TI2535 oraz TI2550 TI25100	260 / 350 mA 1.5 A
Pobór mocy, 24 V_{DC}	
TI2535 oraz TI2550 TI25100	170 / 290 mA 1.0 A
Urz. Nagrzewające	Sterowane termostatycznie

Informacje ogólne	
Konstrukcja	Aluminium
Wykończenie	Proszkowa szara farba poliestrowa
Środowisko pracy	Wewnętrzne/zewnętrzne
Temperatura robocza	od -25° do 131°F (-32° do 55°C)
Temperatura magazynowania	od -58° do 185°F (-50° do 85°C)
Masa	**Jednostka / z opakowaniem**
TI2535 oraz TI2550	4.7 funta (2.1 kg) / 11 funtów (5 kg)
TI25100	7.5 funta (3.4 kg) / 15 funtów (7 kg)

Certyfikaty / Wartości znamionowe
CE, Klasa A
FCC, Klasa A
Certyfikat UL/cUL
C-Tick
Urządzenie spełnia normy NEMA Type 4X oraz IP66

Kamera termalna / optyka	
Detektor	Mikrobolometr niechłodzony, tlenek wanadu
Układ	320 x 240
Rozmiar piksela	38 mikronów
Odpowiedź widmowa	7.5–13.5μm LWIR
Wyjście wideo	1 Vp-p, 75 Ohm
Źródło normalizacji	Migawka wewnętrzna (jedynie offset), 0,7 sekundy zamrożenia obrazu w czasie zamknięcia migawki
Czas do wyśw. obrazu	Poniżej 2 sekund, bez chłodzenia termoelektrycznego
Sterowanie obrazem	Dwukrotny zoom cyfrowy
Interfejs szeregowy	Kompatybilny z RS232 / RS422
Czasowe NEdT	85mK przy f/1.4
Formaty wyświetlania	biały-gorący, czarny-gorący, formaty kolorowe
Zorientowanie	Odwracanie / przywracanie, sterowane oprogramowaniem
Pole widzenia	
TI2535	20° (poz.) x 15° (pion.)
TI2550	14° (poz.) x 10° (pion.)
TI25100	7° (poz.) x 5.2° (pion.)
Ostrość	
TI2535	3 stopy (1 m) do nieskończoności
TI2550	13 stóp (4 m) do nieskończoności
TI25100	9.8 stóp (3 m) do nieskończoności
Odległość hiperfokalna	
TI2535	85 stóp (26 m)
TI2550	114 stóp (35 m)
TI25100	Nie dotyczy

Zalecane mocowania	
Sufit/piedestał	
EM1009U, EM1015U	Uchwyt dla średniego obciążenia do mocowania na suficie / piedestale
Ściana	
EM1450	Uchwyt ścienny dla średniego obciążenia
Słupy/rury	
EM1109	Uchwyt dla średniego obciążenia do mocowania na słupie / rurze poziomej lub pionowej
EM2000	Uchwyt dla średniego obciążenia do mocowania na słupie / rurze pionowej
EM2200	Uchwyt dla średniego obciążenia do mocowania na słupie / rurze poziomej

Zalecane źródła zasilania	
WCS1-4	Zewnętrzny zasilacz dla kamery; napięcie wejściowe 100 / 120 / 240 V_{AC}; jedno wyjście 24 / 26 / 28 V_{AC}; całkowita obciążalność 4 A (100 VA)
WCS4-20	Zewnętrzny zasilacz dla wielu kamer; napięcie wejściowe 120 / 240 V_{AC}; cztery wyjścia 24 / 28 V_{AC} z bezpiecznikami; całkowita obciążalność 20 A (480 VA)

t.a.c by Schneider Electric
TAC Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10, faks (22) 313 24 11
e-mail: tac_pol@tac.com
http://www.tac.com/pl

Kompleksowe rozwiązanie RCP firmy ROGER

Kompleksowe rozwiązanie RCP firmy ROGER ułatwia zarządzanie czasem pracy, precyzyjne jego rozliczanie oraz wpływa na redukcję kosztów, przyczyniając się do wzrostu efektywności przedsiębiorstwa.

Program RCP Master został opracowany w środowisku Microsoft .NET i jest przeznaczony dla systemów operacyjnych Windows XP i Vista. RCP Master posiada przyjazny interfejs, jest bezpieczny i łatwy w obsłudze. Program może być użytkowany bezpłatnie w celach ewaluacyjnych przez pierwsze 60 dni po instalacji.

Dla celów rejestracji czasu pracy firma Roger zaleca wykorzystanie kontrolera PR602LCD. Kontroler ten posiada wyświetlacz LCD oraz zestaw czterech programowalnych klawiszy funkcyjnych, które mogą być wykorzystane jako przyciski wyboru rodzaju rejestracji (wejście, wyjście, wyjście służbowe itp.). Kontroler PR602LCD posiada wbudowany bufor zdarzeń i może pracować samodzielnie lub w sieciowym systemie kontroli dostępu typu RACS (Roger).

Charakterystyka RCP Master

Import/eksport danych

- Import zdarzeń z systemu kontroli dostępu RACS v4.2.5.38 i wyższe
- Import zdarzeń z pliku tekstowego w formacie CSV oraz XML
- Eksport raportów w formacie Adobe Acrobat (.pdf), Microsoft Excel (.xls), Microsoft Word (.doc), Rich Text Format (.rtf) i Crystal Reports (.rpt)
- Eksport raportów czasu pracy w formacie XML

Definicje

- Dni kalendarza: dzień roboczy, dzień roboczy dodatkowy, święto, dzień wolny itp.
- Typów obecności i absencji: urlop wypoczynkowy, nieobecność nieusprawiedliwiona, przerwa obiadowa itp.
- Maksymalnych i minimalnych czasów przebywania (np. maks. dzienna norma przerw na papierosa, minimalny czas pracy itp.)
- Dodatkowe opcje związane ze spóźnieniami, wcześniejszymi wyjściami, zaliczaniem czasu przed i po godzinach pracy itp.
- Typów przejść: wejście, wyjście, wyjście służbowe itd.
- Wymiarów urlopów i raport stanu ich wykorzystania

Raporty

- Raporty: grupy pracowników, pracownicy, kalendarze, punkty kontrolne, rejestr zdarzeń RCP, raporty czasu pracy, wymiary urlopów, indywidualne kalendarze itp.
- Możliwość tworzenia dowolnego zestawienia raportów przy pomocy kreatora raportów zarówno zbiorczych dla całej grupy, jak i indywidualnych dla poszczególnych pracowników
- Możliwość automatycznego rozsyłania indywidualnych raportów pocztą e-mail na adres pracownika

Plik Danych

- Relacyjna, plikowa baza danych typu MS Access
- Praca z lokalną bazą danych lub udostępnioną w sieci komputerowej
- Możliwość ustawiania hasła dostępu do pliku bazy danych
- Możliwość szyfrowania pliku bazy danych
- Kompaktowanie i naprawa pliku bazy danych
- Możliwość operacji na bazie z dowolnego innego programu (np. własna implementacja dopisywania zdarzeń RCP przez system zewnętrzny)

Pozostałe

- Możliwość korekty i wstawiania brakujących zdarzeń RCP oraz edycja absencji
- Indywidualne kalendarze pracy z możliwością korekty kalendarza dla poszczególnych pracowników np. odpracowywanie, zamiany itp.
- Obsługa zaokrąglania czasu rozpoczęcia i zakończenia pracy
- Obsługa przerw płatnych i niepłatnych
- Obsługa nadgodzin (5 predefiniowanych typów)
- Definiowanie operatorów programu i ich uprawnień
- Rejestracja działań operatorów
- Systemy operacyjne: Windows XP i Vista
- Darmowa aktualizacja w ramach tej samej wersji programu

Wersje licencji

- Maksymalna obsługiwana liczba pracowników:
  - do 50
  - do 250
  - bez ograniczeń
- Rodzaje licencji:
  - Jednostanowiskowa (pojedyncza instalacja)
  - Wielostanowiskowa (obsługa określonej liczby stanowisk z programem, wymagana instalacja serwera licencji)

roger®

Roger Sp.j.
Gościszewo 59
82-416 Gościszewo, woj. Pomorskie

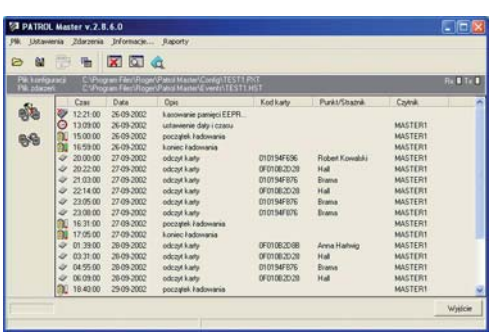
tel. (55) 272 0132, faks (55) 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

PATROL II LCD – rejestracja pracy wartowników

PATROL II LCD jest przenośnym czytnikiem transponderów zbliżeniowych UNIQUE, przeznaczonym do rejestracji obecności wartownika w wyznaczonych miejscach i o określonych porach . Urządzenie przeznaczone jest do weryfikacji rzetelności pracy wartowników, niemniej może znaleźć zastosowanie wszędzie tam gdzie zachodzi potrzeba kontroli przemieszczania się ludzi pod względem miejsca i czasu. Instalacja systemu polega na rozmieszczeniu w wybranych miejscach obiektu punktów kontrolnych oraz skonfigurowaniu czytnika. Każdemu punktowi kontrolnemu oraz identyfikatorowi użytkownika przypisuje się etykiety co umożliwia później łatwą interpretację historii zarejestrowanych zdarzeń.

Charakterystyka

- Nieulotna pamięć ostatnich 3500 odczytów
- Sygnalizacja niskiego stanu baterii oraz zapełnienia pamięci
- Zegar czasu rzeczywistego
- Wyświetlacz LCD z podświetleniem
- Złącze USB do transmisji danych
- Ładowanie baterii bezpośrednio z gniazdka USB
- Program PATROL Master II (Windows)



Patrol II LCD

- Czytnik
- Kabel USB
- Dwa akumulatorki AA 1.5V
- Futerał
- Ładowarka baterii

roger®
Roger Sp.j.
Gościszewo 59
82-416 Gościszewo, woj. Pomorskie
tel. (55) 272 0132, faks (55) 272 0133
e-mail: roger@roger.pl
http://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

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

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

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

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

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

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

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

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

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

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

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

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

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

ADT Fire and Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 83 01
faks (22) 430 83 02
e-mail: 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. Kielnieńska 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
Infolinia 0 801 77 77 90
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. Uszczyka 11, 44-100 **Gliwice**
tel. (32) 790 76 23
faks (32) 790 76 65
e-mail: gliwice@e-alpol.com.pl

Al. Solidarności 15b, 25-211 **Kielce**
tel. (32) 720 39 81
faks (32) 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Pachońskiego 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: sekretariat@anb.com.pl
www.anb.com.pl

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

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

ATLine Sp. J.
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
handel@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.
Tulipan House
ul. Domaniewska 50
02-672 Warszawa
tel. (22) 549 23 30
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. Krasińskiego 41A
01-755 Warszawa
tel. (22) 633 90 90
faks (22) 633 90 60
e-mail: handlowy@cbcpoland.pl
www.cbcpoland.pl

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

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

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

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

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. (12) 260 1 395
faks (12) 260 1 396

ul. Racławicka 82, 60-302 **Poznań**
tel./faks (61) 861 40 51
tel. kom. (0) 601 203 664
e-mail: poznan@cma.com.pl

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

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. KEN 96/U15
02-777 Warszawa
tel./faks (22) 855 00 17
e-mail: pk@cs.pl
www.cs.pl

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

D+H POLSKA Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
Biuro SAP: (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. Płochocińska 19 lok. 44-45, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

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

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

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

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

DELTA BUSINESS SERVICE
Andrzej Bryl
ul. Ciepła 15/50
50-524 Wrocław
tel./faks (71) 367 06 16
e-mail: bok@delta-security.com.pl
www.delta-security.com.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. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
tel./faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
info@dravis.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: katarzyna.osiecka@edps.com.pl
www.edps.com.pl

ela-compil Sp. z o.o.
ul. Słoneczna 15 A
60-286 Poznań
tel. (61) 869 38 50
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
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
www.el-mont.com

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

ELTCRAC
Centrum Zabezpieczeń
Systemy Domofonowe
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60/61, 292 48 70
faks (12) 292 48 62, 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

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

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

Oddział:
ul. Jana Kazimierza 61, 01-267 **Warszawa**
tel./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

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

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

ul. Grabiszyńska 66e, 53-504 **Wrocław**
tel. (71) 78 74 741
faks (71) 78 74 742
e-mail: factor.wr@factor.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

GDE POLSKA
ul. Koniecznego 46
32-040 Świątniki Górne
tel. (12) 256 50 25/35
faks (12) 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

GUNNEBO POLSKA Sp. z o.o.
ul. Piwonicka 4
62-800 Kalisz
tel. (62) 768 55 70
faks (62) 768 55 71
e-mail: polska@gunnebo.com
www.rosengrens.pl
www.gunnebo.pl

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. 693 029 278
e-mail: warszawa@gv.com.pl
www.gv.com.pl

ul. Lwowska 74a
33-300 **Nowy Sącz**
tel. (18) 444 35 38, 444 35 39, 444 35 83
faks (18) 444 35 84
tel. kom. 695 583 424
e-mail: nowysacz@gv.com.pl

ul. Racławicka 60a
53-146 **Wrocław**
tel. (71) 361 66 02
faks (71) 361 66 23
tel. kom. 695 583 292
e-mail: wroclaw@gv.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

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

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

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

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, 341 47 18
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

P.P.U.H. LASKOMEX
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: handel@laskomex.com.pl
www.laskomex.com.pl

MAXBAT Sp. J.
ul. Nadbrzeżna 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

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 341 98 54
faks (71) 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

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

Przedstawicielstwo:
ul. 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@pointel.pl
www.pointel.pl

POL-ITAL Sp. z o.o.
ul. Dzielna 1
00-162 Warszawa
tel. (22) 831 15 35
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.com.pl

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

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

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

P.P.H. PULSON
ul. Czerniakowska 18
00-718 Warszawa
tel. (22) 851 12 20
faks (22) 851 12 30
e-mail: biuro@pulson.com.pl
www.pulson.eu

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 Elektronik s.c.
Os. 1000-lecia 6A/1
32-400 Myślenice
tel. (12) 379 34 47
tel./faks (12) 272 39 71
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

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 314 69 50
e-mail: info@satie.pl
www.satie.pl

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

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

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

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

P.T.H. SECURAL Jacek Giersz
ul. 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. Różyckiego 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 POLSKA Sp. z o.o.
ul. Rokicińska 162
92-412 Łódź
tel. (42) 677 58 00
faks (42) 677 58 01
e-mail: centrala@solar.pl
www.solar.pl www.weblink.solar.pl
www.solar.pl/blueenergy

Oddziały:
ul. Radzikowskiego 35, 31-315 **Kraków**
tel. (12) 638 91 00
faks (12) 638 91 22
e-mail: krakow@solar.pl

ul. Witosa 3, 20-330 **Lublin**
tel. (81) 745 59 00
faks (81) 745 59 05
e-mail: lublin@solar.pl

ul. Smoluchowskiego 7, 60-179 **Poznań**
tel. (61) 863 02 04
faks (61) 863 02 70
e-mail: poznan@solar.pl

ul. Heyki 3, 70-631 **Szczecin**
tel. (91) 485 44 00
faks (91) 485 44 01
e-mail: szczecin@solar.pl

ul. Krakowska 141-155, 50-428 **Wrocław**
tel. (71) 377 19 00
faks (71) 377 19 16
e-mail: wroclaw@solar.pl

ul. Łużycka 3B, 81-537 **Gdynia**
tel. (58) 662 00 00
faks (58) 664 04 00
e-mail: gdynia@solar.pl

ul. Armii Krajowej 1, 58-302 **Wałbrzych**
tel. (74) 880 01 14/17
faks (74) 847 00 69
e-mail: walbrzych@solar.pl

ul. Przemysłowa 4F, 33-100 **Tarnów**
tel. /faks (14) 629 80 20
e-mail: tarnow@solar.pl

ul. Glinki 144 bud. A, 85-861 **Bydgoszcz**
tel. (52) 320 50 88/89
faks (52) 362 01 52
e-mail: bydgoszcz@solar.pl

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 24 51
tel. kom. (0) 692 403 272, 600 206 117
faks (22) 520 25 77
e-mail: diana.jesionek@eu.sony.com
marta.malecka@eu.sony.com
www.sonybiz.net/nvm

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) 485 50 00
faks (91) 485 50 12
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.pl
www.aper.com.pl

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

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

ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.pl

ul. Dąbrowszczaków 2 A, 10-541 **Olsztyn**
tel. (89) 527 92 72
faks (89) 527 92 30
e-mail: olsztyn@spstrading.pl

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

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

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

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

SYSTEM 7
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
infolinia 0 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.sevenguard.com,
www.system7.pl

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

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

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

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

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

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, 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o.
ul. Marszałkowska 60/27
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 77
Sprzedaż: (22) 516 97 97
faks (22) 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
al. Wyzwolenia 70, 71-510 **Szczecin**
tel./faks: (91) 423 70 55
e-mail: witold.brzozowski@telekomunikacja.pl

ul. Rzeczypospolitej 5, 59-220 **Legnica**
tel. (76) 856 60 71
faks (76) 856 60 71
e-mail: marian.sitko@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. Rakowicka 51, 31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Kosmonautów 82, 20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.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
tel./faks (52) 584 01 92
e-mail: lukasz.cellari@w2.com.pl
www.w2.com.pl

V4S Sp. z o.o.
ul. Szczecińska 1FA
72-003 Dobra
tel. (91) 421 16 52, 311 33 49
Infolinia 0 801 055 075
faks (91) 421 18 05
e-mail: info@v4s.pl
www.v4s.pl

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
2M Elektronik	–	TAK	TAK	TAK	–
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	–	TAK	TAK	TAK	TAK
Alarm System	TAK	–	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Aldom	–	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
ANB	–	TAK	TAK	TAK	–
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	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	TAK	TAK
C&C Partners	–	TAK	TAK	–	TAK
CAMSAT	TAK	TAK	TAK	–	–
CBC Poland	TAK	–	TAK	–	TAK
CCX	–	TAK	TAK	TAK	TAK
Cezim	TAK	TAK	TAK	–	TAK
CMA	TAK	TAK	TAK	TAK	–
COM-LM	TAK	TAK	TAK	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DANTOM	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-compil	TAK	–	TAK	–	TAK
El-Mont	–	TAK	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	–
GDE Polska	–	–	TAK	–	TAK
Gunnebo	TAK	TAK	TAK	TAK	–
GV Polska	–	–	TAK	–	TAK
HSA	–	–	TAK	–	–
ICS Polska	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Info-Cam	TAK	TAK	TAK	TAK	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	–	TAK	–	–
KABE	TAK	TAK	TAK	TAK	TAK
Kolektor	–	TAK	–	TAK	–
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	–	–	–	TAK
Micronix	–	TAK	TAK	–	–
Miwi-Urmet	TAK	–	TAK	–	TAK
Noma 2	TAK	TAK	TAK	TAK	–
OBIS	–	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	–	–	TAK	–	–
PAG	TAK	TAK	TAK	TAK	–
Panasonic	–	–	TAK	–	TAK
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	TAK	–	–
PPH Pulson	TAK	TAK	TAK	–	–
Radioton	–	–	TAK	–	–
Ramar	TAK	–	TAK	TAK	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Sagitta	TAK	–	–	–	–
Satel	TAK	–	–	–	–
SATIE	TAK	–	TAK	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	–	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
SOFTEX Data	–	–	TAK	–	TAK
Solar	–	–	TAK	–	–
Sony	TAK	–	–	–	–
Sprint	–	TAK	–	TAK	TAK
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	TAK	TAK	–	TAK
TAC	TAK	TAK	TAK	TAK	TAK
Talcomp	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	TAK	TAK	TAK	TAK	TAK
Techom	–	–	–	–	TAK
Technokabel	TAK	–	–	–	–
TP TELTECH	–	TAK	TAK	TAK	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
V4S	TAK	–	TAK	–	TAK
Vision Polska	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
2M Elektronik	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	TAK	TAK	TAK	–	–	TAK	–	TAK	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	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	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–
AVISmedia	–	–	–	TAK	–	–	–	–	TAK
Bitner Zakłady Kablowe	kable i przewody do SSWiN, systemów telewizji dozorowej, kontroli dostępu i in.								
BOSCH	TAK	TAK	–	TAK	–	–	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
bt electronics	–	–	TAK	–	–	–	–	TAK	–
C&C Partners	TAK	TAK	TAK	–	TAK	TAK	TAK	–	–
CAMSAT	–	TAK	–	–	–	–	–	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CCX	–	–	TAK	–	–	–	–	TAK	–
Cezim	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
CMA	TAK	–	–	–	–	–	TAK	–	–
COM-LM	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Control System FMN	TAK	TAK	TAK	TAK	–	TAK	–	TAK	–
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H	–	–	–	TAK	–	TAK	–	–	TAK
DANTOM	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	–	TAK	–
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	–	–
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	TAK	TAK	TAK	–	–	–	–	TAK	–
Gunnebo	–	–	TAK	–	TAK	–	–	TAK	–
GV Polska	–	TAK	TAK	–	–	–	TAK	–	–
HSA	TAK	TAK	TAK	–	–	–	–	–	–
ICS Polska	TAK	TAK	TAK	–	–	–	–	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Info-Cam	TAK	TAK	TAK	–	–	TAK	TAK	–	TAK
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	TAK	TAK	–	–	TAK	TAK	–	–
Janex International	TAK	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
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Miwi-Urmet	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK	–
Noma 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
OBIS	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	–	–	TAK	–	–	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	–	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
PPH Pulson	TAK	–	–	–	–	TAK	TAK	–	–
Radioton	–	TAK	–	–	–	–	–	–	–
Ramar	TAK	TAK	TAK	–	TAK	–	TAK	–	–
ROPAM Elektronik	TAK	–	TAK	TAK	–	–	TAK	–	–
Sagitta	–	–	–	TAK	–	–	–	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	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	–	TAK	–	TAK
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	–	–	–	TAK
SYSTEM 7	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	–	–	–	–	–	–
Tayama	TAK	TAK	TAK	–	–	TAK	–	–	TAK
Techom					szkolenia				
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
TP TELTECH	TAK	TAK	TAK	TAK	TAK	–	TAK	–	–
UNICARD	–	–	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
V4S	–	TAK	–	–	–	TAK	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktor merytoryczny
Stanisław Banaszewski

Dział marketingu i reklamy
Ela Końka

Redaguje zespół:
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Ireneusz Krysowaty
Paweł Niedziejko
Edward Skiepko
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz
Marek Życzkowski

Współpraca zagraniczna
Rafał Niedzielski

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

Skład i łamanie
Marek Bladoszewski

Korekta
Elżbieta Kaluga

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

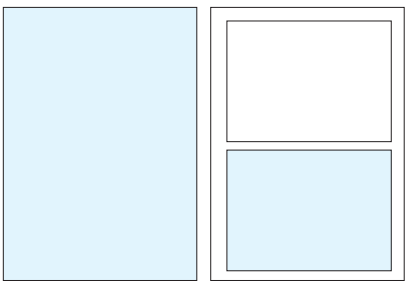
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 0 546
faks (22) 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

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



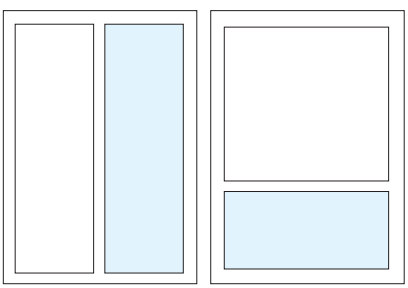
cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

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

Reklama na okładkach:

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

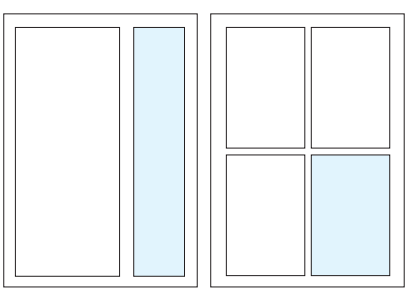


1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Spis teleadresowy:

jednorazowy wpis	70 zł



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na minimum 6 kolejnych emisji

W przypadku zamówienia na 12 emisji 10% rabat

Podane ceny nie uwzględniają podatku VAT (22%)

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

Spis reklam

Spadek kursu decybela.
Złoty się umacnia.

Dzięki interwencji Ambient System na rynku głośników pożarowych złoty zaczął się umacniać. Jeszcze nigdy decybel nie był taki tani.

Ambient System sięgnął po najskuteczniejszą broń.

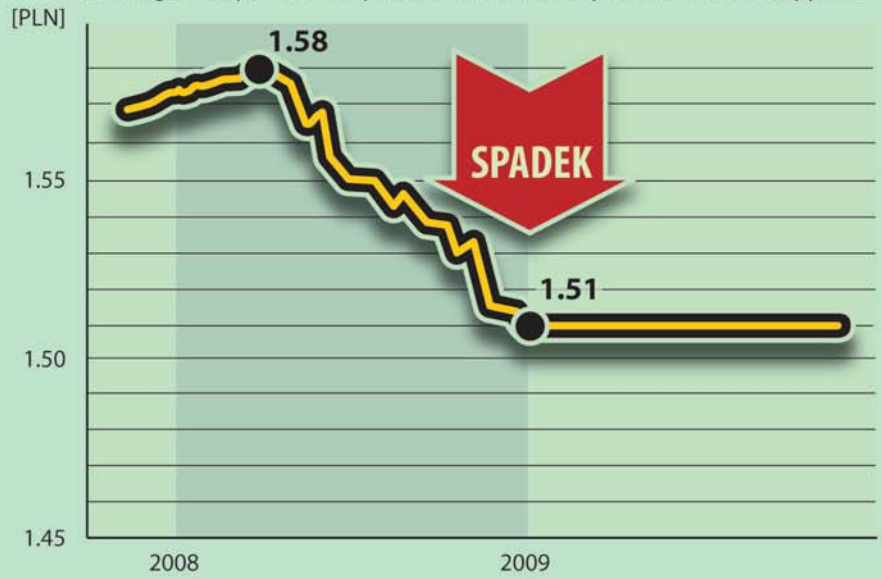
„Aprecjacja złotego w stosunku do decybela to najlepszy krok w kierunku obniżenia kosztów DSO." - z przekonaniem twierdzi szefowa marketingu w Ambient System. Korzyść jest podwójna. Po pierwsze, w systemie DSO ABT-Venas mamy unikatowy system modularnego zasilania, którego wielkość jest ściśle związana z efektywnością głośników.

98dB/1W

Im efektywność głośników jest większa, tym mniejsze zapotrzebowanie na moc, a co za tym idzie, niższy koszt zakupu systemu zasilania podstawowego i rezerwowego. Podobnie ze wzmacniaczami. Zwiększenie efektywności głośników o 3 dB tnie potrzebną moc wzmacniaczy o 50%. Zatem kupując ABT-Venas, inwestor płaci tylko za to, co niezbędne. Po drugie, następuje odczuwalna redukcja kosztów związanych z drożejącą energią elektryczną. Tanieje eksploatacja DSO.

Stąd, gwarantowane w ten sposób długoterminowe oszczędności są wystarczająco silnym bodźcem dla inwestorów myślących poważnie o podniesieniu rentowności swych inwestycji.

Według analityków branży, nadszedł doskonały moment na zakupy DSO



OPINIE | Długo oczekiwany spadek decybela znacznie poprawi nastroje inwestorów

Dlatego zrozumiałe jest, że coraz częściej wybór pada na nowe głośniki pożarowe, wprowadzone w ostatnim czasie przez Ambient System. Głośnik pożarowy sufitowy z rzeczywistym poziomem SPL 98dB/1W wywindował poprzeczkę naprawdę wysoko.

więcej na **www.ambientsystem.pl**

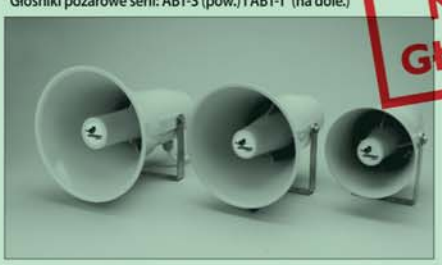
Silni powiększają ofertę

NOWOŚĆ | Kategoria klimatyczna C

Umacnianie pozycji na rynku DSO to stała strategia Ambient System.

Świadczy o tym poszerzenie oferty o głośniki pożarowe pracujące we wszystkich kategoriach klimatycznych A, B i C. Głośniki w łazienkach mogą się wydawać zwykłą zachcianką. Jednak gdy weźmiemy pod uwagę ich minimalne gabaryty (średnica ABT-S106 wynosi ledwie 10cm), oraz rozsądną, zaskakująco niską cenę, wszystko staje się jasne. Ambient konsekwentnie dąży do celu. Żadnych kompromisów. Wszystkie pomieszczenia gdzie przebywają ludzie muszą być objęte przez DSO. Odważna decyzja o zastosowaniu tańszego od stali ABS-u do produkcji tub pożarowych, to dowód na to, że firmie Ambient System zależy również na ostrożnych inwestorach. Zastosowane nowatorskie rozwiązanie konstrukcyjne wytrzymało testy w temperaturze 820°C. Żadnego kapania roztopionego plastiku. Po spaleniu wszystko pozostało na swoim miejscu. Wszystko, za wyjątkiem zainteresowania nową ofertą Ambientu. To poszybowało w górę.

Głośniki pożarowe serii: ABT-S (pow.) i ABT-T (na dole.)



Pod kontrolą

PRAWO | Certyfikaty i świadectwa

Nowe głośniki pożarowe to: **sufitowe ABT-S106, 136 2010, 2710** oraz tubowe **ABT-T1510, 2215, 2430.** Wszystkie posiadają wymaganą dokumentację.

ambient SYSTEM

HID Global, światowy lider technologii kart i czytników kontroli dostępu, przedstawia nowe spektrum bezpiecznej identyfikacji.

Firma HID rozsławiła się dobrą reputacją opartą o najwyższą jakość, pewność technologii i ciągłą innowacyjność w dziedzinie kart i czytników kontroli dostępu. Teraz postanowiliśmy wzbogacić naszą ofertę produkcji kart o nowe możliwości, poczynając od kontroli dostępu poprzez protokoły Ethernet, aż do rozwiązań wykorzystywanych w transporcie publicznym. Wierzymy, iż przyszłość bezpiecznej identyfikacji należy upatrywać w otwartości na nowości, elastycznych produktach i zbieżności technologii. To jest naszym celem, więc jeżeli szukasz nowych rozwiązań identyfikacji zgłoś się do HID. Twoje oczekiwania mogą już być wykorzystane w naszych kartach.

HID

ACCESS choices.