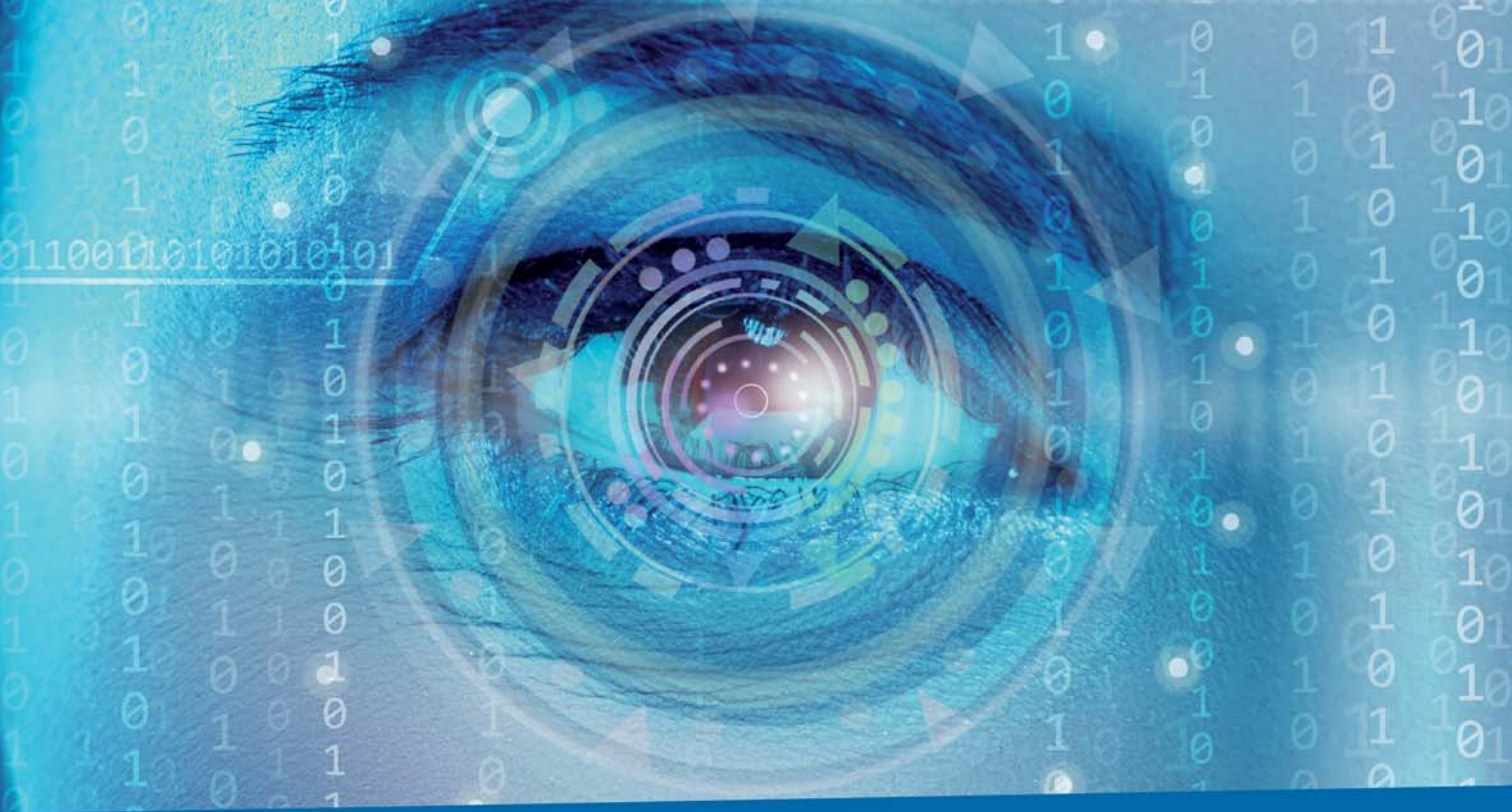
CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(101)/2015

ZABEZPIECZENIA

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

W NUMERZE:



Oferując dedykowane rozwiązania w zakresie bezpieczeństwa trwale wspieramy rozwój naszych Klientów

Instalacje Gaśnicze Wodne
- Instalacje mgły wodnej
- Instalacje tryskaczowe i zraszaczowe
- Systemy pianowe
- Systemy gaszenia iskier
- Instalacje hydrantowe

Instalacje Gaśnicze Gazowe
- Mieszaniny gazów obojętnych
- Gazy chemiczne
- CO_2

Instalacje Elektryczne
- Zewnętrzne i wewnętrzne
- Średniego napięcia
- Rozdział energii
- Oświetlenie

Instalacje Teleinformatyczne (LAN i IT)

Instalacje Teletechniczne
- Elektroniczne Systemy Przeciwkradzieżowe (EAS)
- Systemy Kontroli Dostępu (ACC)
- Systemy Sygnalizacji Pożaru (SSP)
- Dźwiękowe Systemy Ostrzegawcze (DSO)
- Systemy Nadzoru Wizyjnego (CCTV)
- Systemy Sygnalizacji Włamania i Napadu (SSWiN)

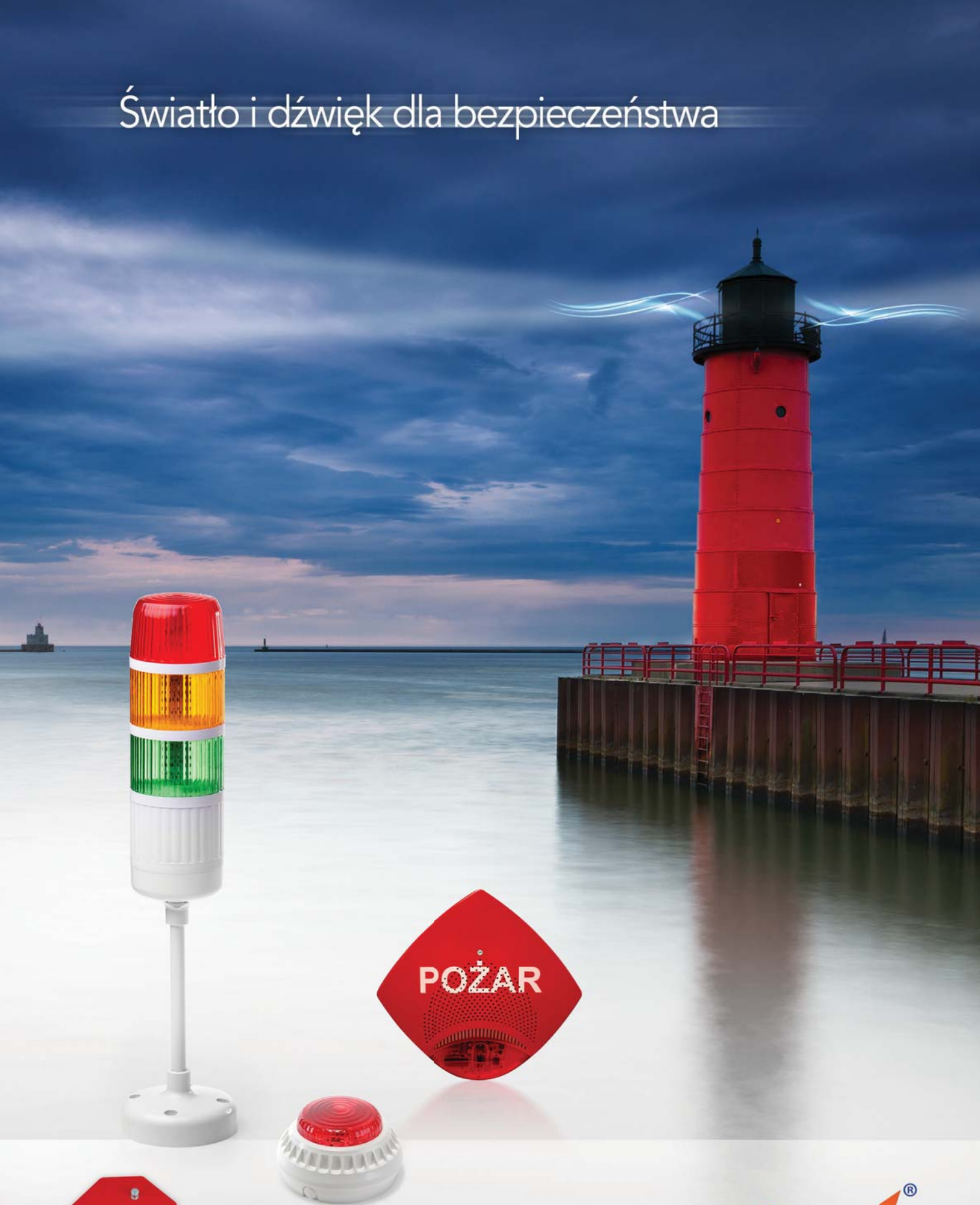
Instalacje Automatyki Budynkowej i BMS
- Sterowanie wentylacją i klimatyzacją
- Monitoring zużycia mediów (woda, prąd, ciepło)
- Integracja systemów
- Oszczędność zużycia energii

Instalacje dedykowane dla sektora handlu detalicznego

AGIS Fire & Security Sp. z o.o. ul. Palisadowa 20/22, 01-940 Warszawa,
tel.: (0-22) 430 83 01, faks: (0-22) 430 83 02,
Infolinia ogólna: 801 801 238, e-mail: agisfs.pl@agisfs.com
Infolinia serwisowa: 800 800 238, e-mail: serwis@agisfs.com
www.agisfs.pl

AGIS
Fire & Security

Światło i dźwięk dla bezpieczeństwa



POLSKI PRODUCENT sygnalizatorów pożarowych,
włamaniowych, automatyki i osprzętu instalacyjnego

ul. Czajcza 6 • 86-005 Białe Błota • biuro@w2.com.pl • www.w2.com.pl

w2®

SPIS TREŚCI 01 2015

OCHRONA PRZECIWPOŻAROWA

SSWIN

TELEWIZJA DOZOROWA

MOBOTIX i25 – nowa kompaktowa kamera hemisferyczna

i25 to nowa dyskretna kamera hemisferyczna niemieckiej marki **MOBOTIX**, która generuje wysokiej rozdzielczości obraz panoramiczny bez martwego pola. Zainstalowana na ścianie, ma pole widzenia 180° i monitoruje całe pomieszczenie od ściany do ściany i od podłogi do sufitu. To kamera do zastosowań wewnętrznych, która bazuje na wydajnej platformie sprzętowej umożliwiającej uzyskanie obrazu o rozdzielczości 5 megapikseli. Cechą charakterystyczną kamery i25 są niewielkie rozmiary ułatwiające instalację. Tak jak zawsze w produktach firmy MOBOTIX, cała inteligencja jest zawarta w kamerze. i25 oferuje między innymi wirtualną funkcję PTZ, dostępną podczas oglądania obrazu zarówno na żywo, jak i zarchiwizowanego. Nie ma potrzeby zakupu dodatkowego oprogramowania czy użycia komputera. Bez względu na liczbę kamer i liczbę użytkowników oprogramowanie MOBOTIX jest zawsze bezpłatne. Archiwizacja może odbywać się w pamięci umieszczonej wewnątrz kamery. Rejestrator jest zbędny, a zdalny dostęp do kamery można uzyskać w każdym miejscu na świecie, wykorzystując Internet.

Kamera występuje w dwóch wersjach – z przetwornikiem kolorowym lub monochromatycznym. Dzięki temu możliwości jej zastosowania jest bardzo wiele. W wielu przypadkach do obserwacji całego pomieszczenia wystarczy jedna kamera i25 umieszczona np. nad drzwiami wejściowymi.

i25 to połączenie znakomitej funkcjonalności z bardzo dobrą ceną.

Bezpośr. inf. Linc Polska

MxDisplay firmy MOBOTIX – „smartfon" na ścianę

MxDisplay to stacja odbiorcza umożliwiająca zarówno obsługę połączeń z wideodomofonu T25M, jak i oglądanie obrazu z kamer marki MOBOTIX. Główną cechą wyróżniającą MxDisplay jest czytelny graficzny interfejs użytkownika gwarantujący dostęp do wszystkich kluczowych funkcji wideodomofonu oraz kamer firmy MOBOTIX. Użytkownik może uzyskać podgląd obrazu z kamer zainstalowanych w budynku, wykonawszy kilka ruchów palcem. Ekran pozwala także na przeglądanie najnowszych wiadomości wizyjnych z wideodomofonu, pozostawionych przez gości. Ponadto umożliwia skonfigurowanie kamer i samego wideodomofonu. Przykładowo – na ekranie MxDisplay administrator systemu może wygenerować nowe kody dostępu dla gości. Można także w łatwy i intuicyjny sposób zarządzać kartami RFID, które umożliwiają na przykład otwieranie drzwi lub furtki bez użycia kluczy. Bez względu na to, co aktualnie jest wyświetlane na ekranie MxDisplay, zawsze dostępne są klawisze szybkiego dostępu. Przykładowo – wciśnięcie przycisku klucza spowoduje natychmiastowe wyświetlenie obrazu na żywo z wideodomofonu, a dłuższe przytrzymanie tego przycisku spowoduje otwarcie drzwi. W razie potrzeby funkcję tę można dodatkowo zabezpieczyć za pomocą kodu PIN lub przez transponder. Ponadto na ekranie jest widoczny przycisk z symbolem koperty umożliwiający szybki dostęp do wiadomości.

Ekran MxDisplay może być montowany zarówno w puszkach natynkowych, jak i podtynkowych. Jest dostępny w dwóch kolorach – czarnym i białym. Kolejną zaletą MxDisplay jest możliwość jego obsługi przez sieć bezprzewodową. Dzięki temu może on być stosowany również jako stacja bazowa dla innych wyświetlaczy umieszczonych w budynku. Dzięki funkcji Wi-Fi Access Point MxDisplay zapewnia dostęp do Internetu dla smartfonów i komputerów, co sprawia, że nie ma potrzeby konfigurowania osobnego systemu Wi-Fi w budynku. Jeśli w obiekcie istnieje sieć Wi-Fi, wówczas MxDisplay może pracować w trybie klienta. Dzięki temu nie ma konieczności doprowadzenia przewodu ethernetowego do ekranu. Wymagane jest jedynie podłączenie zasilacza. Ta cecha znacznie upraszcza instalację.

Ze względu na funkcjonalność oraz prostotę obsługi polecamy stosowanie MxDisplay w połączeniu z wideodomofonem oraz kamerami marki MOBOTIX.

Bezpośr. inf. Linc Polska

Produkty niemieckiej firmy IPS Intelligent Video Analytics już na polskim rynku

Dynamiczny rozwój rynku wizyjnych systemów dozorowych dotyczy nie tylko nowoczesnego sprzętu, ale także rozwiązań software'owych. Do wiodących producentów oprogramowania realizującego inteligentną analizą treści obrazu z kamer i zarządzającego nowej generacji systemami wizyjnymi IP należy niemiecka firma **IPS Intelligent Video Analytics**. Firma istnieje od 1965 roku i specjalizuje się w tworzeniu inteligentnych systemów analizy treści obrazu z kamer dla branży *security* (VideoAnalytics) oraz oprogramowania zarządzającego (VideoManager). Od niedawna jej autoryzowanym partnerem w Polsce jest firma **Innovative Security Systems** – dostawca innowacyjnych rozwiązań do systemów zabezpieczeń. Doświadczenie firmy IPS wywodzi się z rynku niemieckiego i długoletniej współpracy z firmami z branży wizyjnych systemów dozorowych i techniki zabezpieczeń. Produkty firmy IPS są przeznaczone do ochrony obiektów należących do infrastruktury krytycznej, budynków i obszarów rządowych, zakładów karnych, placówek bankowych, muzeów oraz centrów logistycznych.

Innovative Security Systems
Innowacyjne Systemy Zabezpieczeń

Zastosowanie systemów inteligentnej analizy treści obrazów IPS Intelligent Video Analytics radykalnie poprawia warunki pracy operatora wizyjnego systemu dozorowego, uwalniając go od konieczności koncentrowania się wyłącznie na wypatrywaniu szczegółów obrazu. Dzięki odpowiedniej konfiguracji w każdej strefie objętej analizą treści obrazu będą wykrywane charakterystyczne dla niej zagrożenia. Operator jest informowany o specyficznych zagrożeniach. Chaotyczny zbiór obrazów staje się uporządkowanym katalogiem, który można odpowiednio przetwarzać. Systemy analizujące treść obrazów z kamer są bardzo skuteczne i zdecydowanie redukują liczbę fałszywych alarmów.

Do najpopularniejszych systemów wizyjnych służących do ochrony peryferyjnej należy Outdoor Detection, który ma nadany przez urząd UK certyfikat iLIDS dla systemów analizujących treść obrazów z kamer, oraz oprogramowanie Critical Infrastructure Protection, Outdoor Detection, 3D Artwork Protection, Public Transport Protection, Privacy Protection, Dome Tracker i Parking Violation Detection. Wymienione pakiety oprogramowania są kompatybilne z oprogramowaniem służącym do zarządzania sieciowymi systemami wizyjnymi, między innymi Seetec, Milestone, Schille, Axis AVHS oraz IPS VideoManager.

IPS Intelligent Video Analytics

Więcej informacji można znaleźć na stronach *www.is-systems.pl* i *www.ips-analytics.com*.

Bezpośr. inf. Magdalena Dziemidek
Innovative Security Systems

Kontrola dostępu i automatyka hotelowa

Firma **ROGER** poszerzyła swoją ofertę o urządzenia do kontroli dostępu i automatyki przeznaczone do zastosowań hotelowych.

W skład tej nowej grupy urządzeń wchodzą:

– PR821-CH – kontroler dostępu z funkcjami automatyki hotelowej,
– HRT82MF – czytnik kart Mifare z sygnalizacją funkcji hotelowych,
– HRT82FK – panel programowalnych dotykowych klawiszy funkcyjnych,
– HRT82PB – panel przycisków z izolowanym stykiem NO/NC.

Kontroler PR821-CH jest wyposażony w kieszeń na kartę i przeznaczony do montażu w pokoju hotelowym jako urządzenie zarządzające dostępem do pokoju oraz realizujące funkcje automatyki pokojowej. Z kontrolerem może współpracować czytnik zbliżeniowy umieszczony przy wejściu do pokoju (HRT82MF) oraz panel dotykowych przycisków funkcyjnych (HRT82FK). Czytnik HRT82MF pełni rolę czytnika korytarzowego. Jego podstawową funkcją jest sterowanie dostępem do pokoju. Ponadto jest wyposażony w przycisk dzwonka oraz wskaźniki świetlne przypisane do typowych usług hotelowych, takich jak wezwanie obsługi, wezwanie pomocy, zamówienie sprzątania, a także komunikatu „nie przeszkadzać". Prośby o poszczególne usługi są sygnalizowane na osobnych wskaźnikach świetlnych, które mogą być uruchamiane za pomocą panelu z klawiszami dotykowymi (HRT82FK) lub przyciskiem dołączanym do linii wejściowej kontrolera. Kontroler umożliwia blokowanie zasilania elektrycznego w pokoju, sterowanie klimatyzacją, a także we współpracy z czujnikami otwarcia drzwi i okien, realizuje proste funkcje antywłamaniowe. Umieszczenie karty w kieszeni kontrolera może załączać zasilanie elektryczne w pokoju i (lub) klimatyzację. Wszystkie opisane tutaj urządzenia są wyposażone w obudowy linii wzorniczej QUADRUS.

Więcej informacji na stronach 72 i 73.

Bezpośr. inf. ROGER

HDcctv Alliance i Dahua standaryzuje HDCVI 2.0

HDcctv Alliance ogłasza ustanowienie nowego globalnego standardu analogowej telewizji o wysokiej rozdzielczości – **HDCVI 2.0**. Standard ten bazuje na technologii HDCVI firmy Dahua. Standaryzacja umożliwia wprowadzenie rygorystycznej certyfikacji, dzięki której wszystkie odpowiednio oznakowane produkty HDCVI będą ze sobą całkowicie kompatybilne. Dzięki temu użytkownicy będą mogli swobodnie dobierać sprzęt zabezpieczający różnych marek. Jako twórca technologii HDCVI firma Dahua, właściciel patentu, wprowadziła rozwiązania, które są kamieniami milowymi w rozwoju HDCVI. Teraz jej własna, opatentowana technologia stała się globalnym standardem. Dahua udostępnia ją osobom trzecim, w tym także konkurującym między sobą producentom. Współudział w pracach HDcctv Alliance ułatwi im dalszą współpracę podczas konstruowania i produkcji urządzeń zgodnych ze standardem HDCVI 2.0, co przyczyni się do szybszej akceptacji tego standardu na rynku.

Jako członek stowarzyszenia HDcctv Alliance firma **Dahua** docenia, że jej technologia stała się światowym standardem przemysłowym. – *Od momentu, w którym zastosowaliśmy HDCVI po raz pierwszy, w 2012 r., technologia ta zdążyła wzbudzić wielkie zainteresowanie nie tylko w Chinach, ale na całym świecie* – powiedział **Henry Zhang**, wiceprezes Dahua Technology. – *Teraz HDCVI jest światowym standardem, a nie tylko jednym z analogowych rozwiązań HD w przemyśle*.

Na konferencji prasowej, która odbyła się podczas Security China Exhibition w Pekinie, firma **Shany Electronics** – członek HDcctv Alliance – zaprezentowała swoją najnowszą kamerę o szerokim zakresie dynamiki, zasilaną przez kabel koncentryczny (czyli z funkcją PoC) i bazującą na technologii HDCVI. – *Shany oferuje produkty i rozwiązania w branży zabezpieczeń technicznych od ponad 20 lat* – powiedział **Danny Tang**, Deputy General Manager w Shany Electronics. – *Dzięki naszemu doświadczeniu w produkcji kamer analogowych mamy możliwość opracowania kamer HDCVI zaspokajających różnorodne wymagania naszych klientów. Przykładowo – takie funkcje jak True WDR, Auto Defog, LSC, 2D/3D DNR i PoC powodują, że rozwiązania zgodne z HDCVI sprawdzają się zarówno pod względem jakości obrazu, jak i stabilności urządzeń. Dzięki temu nasze produkty odróżniają się od produktów konkurencyjnych na coraz bardziej zatłoczonym rynku. Poza wysoką rozdzielczością obrazu nasze urządzenia mają również inne, unikalne właściwości* – dodał Tang.

HDCVI 2.0 zyskał ostatnio akceptację członków stowarzyszenia. – *Skoro już mowa o certyfikacji, HDcctv Alliance nadal będzie odgrywać ważną rolę w testowaniu produktów i przyznawaniu znaków świadczących o ich zgodności ze standardem* – powiedział **Todd Rockoff**, przewodniczący HDcctv Alliance.

Rockoff podkreśla, że stowarzyszenie HDcctv Alliance zarządza wydawaniem oznaczeń zgodności ze standardami HDCVI 1.0, HDCVI 2.0, a także z mającym ukazać się w ciągu 12 miesięcy standardem HDCVI 3.0. – *Tylko produkty członków stowarzyszenia HDcctv Alliance, które zostaną pozytywnie ocenione podczas certyfikacji, mogą być odpowiednio oznakowane, zarówno na obudowach urządzeń, jak i na opakowaniach. Dzięki tym oznakowaniom odbiorcy będą mogli łatwo rozpoznać produkty kompatybilne ze standardem i zyskać pewność, że wybrane urządzenia będą poprawnie pracować w dowolnym fragmencie systemu wizyjnego.*

Bezpośr. inf. JoJo Li
Dahua Technology
Tłumaczenie: Redakcja

Kamery 4K firmy Dahua

Dahua Technology, przodujący producent i dostawca urządzeń do nadzoru wizyjnego z siedzibą główną w Hangzhou (Chiny), wprowadza swoją pierwszą sieciową kamerę 4K – **IPC-HF81200E**, wkraczając w ten sposób w erę rozwiązań UHD (Ultra HD).

Właściwie 4K nie jest określeniem nowym, szczególnie dla użytkownika sprzętu elektronicznego, ale teraz staje się terminem stosowanym w branży przemysłu związanego z nadzorem wizyjnym. Kamera zgodna ze standardem 4K, zdefiniowanym i zaaprobowanym przez Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union – ITU), powinna wytwarzać, obraz o proporcjach 16:9 i o rozdzielczości 3840×2160, ze skanowaniem progresywnym z prędkością 25 lub 30 klatek na sekundę, z bardzo wiernym odwzorowaniem kolorów.

Innymi słowy – kamera 4K ma rozdzielczość czterokrotnie wyższą niż kamera zgodna ze standardem 1080p oraz znakomicie odwzorowuje szczegóły i kolory obrazu, co jest bardzo pomocne w systemach służących do obserwacji dużych obszarów, takich jak parkingi, dworce kolejowe, rozległe obszary miejskie etc.

Kamera IPC-HF81200E firmy Dahua jest w pełni zgodna ze standardem 4K. Jest wyposażona w 12-megapikselowy przetwornik obrazowy i wydajny procesor sygnałowy, dzięki czemu wytwarza doskonałej jakości obraz o rozmiarach 4000×3000 pikseli z prędkością 15 klatek na sekundę lub o rozdzielczości 4K z prędkością 30 klatek na sekundę, nie przekraczając sugerowanej przepustowości łącza wynoszącej 8 Mb/s. Dzięki temu obraz obiektów ruchomych jest płynnie transmitowany z wykorzystaniem dostępnego pasma sieciowego. Kamera może wytwarzać trzy zróżnicowane strumienie wizyjne o parametrach dostosowanych do wymagań wynikających z konkretnych aplikacji.

Kamera IPC-HF81200E realizuje złożone funkcje umożliwiające jej wykorzystanie w różnych warunkach. Może wytwarzać poprawny obraz podczas mgły, dokładniej odwzorowywać wybrane obszary obserwowanej sceny (funkcja ROI), a także generować sygnały ostrzegawcze po wykryciu twarzy w obserwowanej scenie, wykrywać intruzów przekraczających wirtualne linie czy sygnalizować incydenty polegające na jej obróceniu i gwałtownej zmianie pola widzenia.

Przykładowo, utworzenie wirtualnej strefy chronionej na wjeździe do stacji benzynowej może przynieść podwójne korzyści. W momencie wykrycia ruchu pracownicy stacji słyszą dźwiękowy sygnał ostrzegawczy. Jeden z nich może natychmiast podejść do dystrybutora i szybko obsłużyć klienta, co przekłada się na realne zyski finansowe. Z drugiej strony możliwe jest wykrywanie niebezpiecznych sytuacji, takich jak palenie tytoniu czy prowadzenie rozmów przez telefon komórkowy na terenie stacji, co przyczynia się do podniesienia poziomu bezpieczeństwa.

– *Dahua jest jednym z pierwszych producentów, którzy wprowadzają na rynek kamery 4K, przez co wykorzystanie standardu UHD w wizyjnych systemach dozorowych staje się czymś realnym* – powiedział **Peter Pan**, Product Manager w Dahua Technology. – *W przyszłym* (2015 – przyp. red.) *roku zamierzamy wprowadzić więcej modeli, aby klienci mieli więcej możliwości i mogli znaleźć kamerę 4K, która najlepiej odpowiada ich potrzebom. W listopadzie* (2014 – przyp. red.) *wprowadzimy na rynek kamery odznaczające się wysokim stosunkiem jakości do ceny (C/P).*

Bezpośr. inf. JoJo Li
Dahua Technology
Tłumaczenie: Redakcja

Kamery 3 Mpx pracujące w czasie rzeczywistym

Wśród dostępnych na rynku kamer pracujących w czasie rzeczywistym, tzn. generujących 30 kl./s, dominowały kamery o maksymalnej rozdzielczości HD 1920×1080. Dla kamer o wyższych rozdzielczościach prędkość odświeżania była odpowiednio niższa. Niektóre z tych kamer generowały zaledwie kilka klatek na sekundę. W związku z tym urządzenia o wyższych rozdzielczościach bardziej przypominały szybkie aparaty cyfrowe niż kamery.

Nowe kamery marki **NOVUS** generują 30 klatek o rozdzielczości 2048×1536 (3 Mpx) na sekundę i tym samym umożliwiają obserwację dynamicznych procesów na obrazie o wysokiej jakości.

Wśród nowych produktów są trzy modele wandaloodpornych kamer kopułowych – **NVIP-3DN3050V/IR-1P**, **NVIP-3DN3051V/IR-1P**, **NVIP-3DN3052V/IR-1P**. Dwa ostatnie modele mają certyfikat wandaloodporności IK10. Ostatni z ww. modeli jest wyposażony w obiektyw z ogniskową regulowaną w zakresie f=7 ~ 22 mm/F=1.6 oraz 25 diod LED o zasięgu 50 m i kącie świecenia 60°.

Każda kamera może generować równocześnie trzy strumienie wizyjne skompresowane metodą H.264. Dla wszystkich wymienionych kamer wyspecyfikowano również parametr łącznej przepływności na poziomie 40 Mbps. Ta wartość pozwala na równoczesną pracę kamer w wielu systemach (dostęp w aplikacji NMS, przez przeglądarkę i klienta RTSP etc.).

Bezpośr. inf. Patryk Gańko
NOVUS

NMS kompatybilny z rejestratorami IP serii 5000

Do chwili obecnej rejestratory **NOVUS IP z serii 5000** mogły być obsługiwane lokalnie – z użyciem podłączonej do nich myszy USB – lub zdalnie – za pomocą przeglądarki Internet Explorer. Równolegle trwały prace nad zintegrowaniem powyższej serii rejestratorów IP z aplikacją **NMS** (Novus Management System). Aplikacja może obsłużyć wiele rejestratorów sieciowych serii 5000 (jedyne ograniczenia wynikają z wydajności sprzętowych elementów systemu) i realizować połączenia typu *multi-site* (z wieloma rejestratorami równocześnie). Aplikacja umożliwia podgląd „na żywo" i odtwarzanie zarejestrowanych obrazów, a operator ma dostęp do dzienników (logów) urządzenia. Możliwe jest zdublowanie procesu nagrywania i jego realizowanie zarówno zdalnie – w urządzeniu – jak i w aplikacji NMS – na wyznaczonych obszarach pamięci. Zapewnia to lepsze zabezpieczenie danych. Dodatkowo rejestratory IP serii 5000 można konfigurować z poziomu aplikacji, za pomocą przeglądarki Internet Explorer, bez konieczności wpisywania adresu rejestratora. Rejestratory sieciowe serii 5000 są kompatybilne z aplikacją NMS od wersji 1.31.10.

Bezpośr. inf. Patryk Gańko
NOVUS

1 stycznia 2015 r. zmarł nagle **Jerzy Karczewski** – prezes zarządu firmy POLON-ALFA z Bydgoszczy, największego polskiego producenta systemów sygnalizacji pożarowej i aparatury do pomiaru promieniowania jonizującego. Miał 56 lat.

Pracę w firmie rozpoczął w 1988 roku na stanowisku konstruktora, by już po dwóch latach, jako główny konstruktor, stanąć na czele całego zespołu. W latach 1993–1995, będąc przewodniczącym rady pracowniczej, czynnie uczestniczył w przeprowadzeniu trudnego procesu prywatyzacji POLON-ALFA. Kolejny rok przyniósł awans na stanowisko wiceprezesa zarządu, a w 2001 roku rada nadzorcza powierzyła mu funkcję prezesa zarządu.

Był wielokrotnie odznaczany, m.in. Srebrnym Krzyżem Zasługi, Srebrnym Medalem za Zasługi dla Obronności Kraju, Medalem za Zasługi dla Pożarnictwa, Medalem Prezydenta Miasta Bydgoszczy, Medalem Starosty Bydgoskiego, a także nagradzany tytułami „Pracodawca Roku" i „Biznesmen 20-lecia".

Będąc prezesem POLON-ALFA, ale również członkiem Zarządu Pracodawców Kujaw i Pomorza, Izby Przemysłowo-Handlowej, Pomorsko-Kujawskiej Izby Budownictwa, Ogólnopolskiego Stowarzyszenia Producentów Zabezpieczeń Przeciwpożarowych i Sprzętu Ratowniczego oraz Business Centre Club, potrafił, jak niewielu, łączyć skuteczne zarządzanie prężnie rozwijającą się spółką z działalnością będącą wzorem społecznej odpowiedzialności.

Trudno wymienić wszystkie Jego zasługi dla firmy, branży i regionalnego biznesu. Wszystkie sukcesy zawodowe z wrodzoną sobie skromnością przedstawiał najczęściej jako wynik pracy zespołu, którym kierował. Niezwykle cenił sobie rzetelność, lojalność i przyjaźń.

Zaledwie dwa lata temu na łamach jednego z branżowych czasopism mówił o zawodowych marzeniach: „Chciałbym, aby logotyp POLON-ALFA był utożsamiany zawsze z wysoką jakością, nowoczesnością i niezawodnością. Aby ta marka, dziś doskonale rozpoznawalna i ceniona na rynku polskim, miała takie samo znaczenie na rynkach zagranicznych".

Dziś wracamy do tych słów z ogromnym żalem, – bo tych planów nie uda Mu się już zrealizować osobiście, ale i z wiarą, bo wiemy, że pozostawił po sobie doskonały zespół, który tworzył przez lata.

Był prawdziwym miłośnikiem swojej pracy, której efekty służyły i służą zabezpieczaniu najwyższych wartości: ludzkiego życia, zdrowia i mienia. Był człowiekiem pełnym energii, życzliwości i pogody ducha. Był…

Koniec roku był jak zwykle pracowity. Parę dni przed świętami Bożego Narodzenia przyszedł się pożegnać i złożyć świąteczno-noworoczne życzenia. Wybierał się na odpoczynek i planował wrócić dopiero 7 stycznia. Mógł sobie pozwolić na taki długi urlop, bo wiedział, że mijający właśnie rok skończy się sukcesem. Nie wrócił...

Redakcja

Forum Monitoringu Polskiego 2014

podsumowanie

W dniach 16–17 października 2014 r. w hotelu Zamek w Pułtusku odbyło się XVI Seminarium Forum Monitoringu Polskiego zorganizowane przez stowarzyszenie **POLALARM**.

Tematyka tegorocznego seminarium obejmowała aktualne aspekty prawno-normatywne oraz kierunki rozwoju systemów monitorowania. Uczestniczyli w nim przybyli z całej Polski przedstawiciele ponad czterdziestu firm związanych z branżą bezpieczeństwa publicznego. Swoje propozycje rynkowe prezentowało sześciu dystrybutorów sprzętu i oprogramowania. W części seminaryjnej dwudniowego spotkania wygłoszono ponad dwadzieścia referatów. Dominowała tematyka prawna i normatywna. W szczególności uwzględniono obowiązujące w naszym kraju nowe normy międzynarodowe i europejskie. Omawiane były także zagadnienia związane z bezpieczeństwem granic i obronnością Polski. Nie zabrakło prelekcji o charakterze technicznym. Dużym zainteresowaniem cieszyły się prezentacje dotyczące budowy i eksploatacji miejskich systemów monitoringu wizyjnego. Równie interesujące były referaty, których autorzy porównywali różne techniki zabezpieczeń i technologie związane z produkcją sprzętu oraz oprogramowania.

Uczesticy Forum mogli lepiej się poznać i przedyskutować interesujące ich zagadnienia w trakcie kilku przerw kawowych oraz uroczystej kolacji zorganizowanej w zamkowej restauracji. Imprezę zamknął prezes stowarzyszenia POLALARM, Mirosław Prokocki, który wręczył uczestnikom dyplomy potwierdzające ich udział w spotkaniu.

Zapraszamy do obejrzenia fotorelacji na stronie *www.zabezpieczenia.com.pl.*

Redakcja

RACS 5

System kontroli dostępu

- Wieloprzejściowe kontrolery dostępu serii MC
- Skalowalne oprogramowanie zarządzające VISO w architekturze klient – serwer
- Plikowa lub serwerowa baza danych w technologii MSSQL
- Bezpieczna komunikacja szyfrowana AES 128 CBC
- Funkcje automatyki budynkowej
- Integracja sprzętowa z systemem alarmowym
- Monitorowanie w trybie tekstowym i graficznym
- Integracje CCTV: Hikvision, Dahua
- Możliwość podziału systemu na zarządzane indywidualnie części

Rozszerzono ofertę o produkty do automatyki hotelowej

Wysoka niezawodność i funkcjonalność potwierdzona w tysiącach wdrożonych z sukcesem instalacji w Polsce i za granicą.

roger®

Piąta edycja spotkania partnerów Axis Communications za nami

16 października 2014 r. w Hotelu Regent w Warszawie już po raz piąty odbyło się spotkanie partnerów firmy **Axis Communications**, światowego lidera rynku sieciowych systemów wizyjnych. Na spotkaniu, na którym jak zwykle obecni byli partnerzy, klienci, prasa i sympatycy, zaprezentowane zostały najnowsze produkty oraz strategia firmy. Gościem specjalnym był **Andres Vigren**, Product Manager zajmujący się sieciowymi kamerami stałopozycyjnymi.

– *Z dużą satysfakcją gościmy po raz kolejny naszych partnerów biznesowych, jak również przedstawicieli mediów branżowych. Spotkania te gromadzą z roku na rok coraz więcej naszych sympatyków i pokazują, że trud włożony w popularyzację marki Axis na rynku polskim przynosi efekty* – powiedziała **Agata Majkucińska**, Key Account Manager w Axis Communications. – *Spotkanie partnerów to dla nas nie tylko okazja do wymiany doświadczeń czy zaprezentowania planów na najbliższe miesiące, lecz także spotkanie z ludźmi, którzy są dla nas jak członkowie zespołu. To wyjątkowe wydarzenie, podczas którego możemy podzielić się swoimi spostrzeżeniami, oczekiwaniami czy nawet udzielić odpowiedzi na pytania dotyczące wprowadzania i rozbudowywania sieciowych systemów wizyjnych na terenie całego kraju* – dodała.

Podczas tegorocznego spotkania wszystkim zgromadzonym przedstawiono nowych pracowników polskiego oddziału Axis Communications – **Justynę Puławską**, nowego koordynatora ds. marketingu i komunikacji, odpowiedzialną za Polskę i kraje bałtyckie, oraz **Jakuba Kozaka**, Sales Managera, również odpowiedzialnego za region Polski i krajów bałtyckich.

Najważniejsza część prezentacji dotyczyła najnowszych produktów i rozwiązań technologicznych. Poprowadził ją gość specjalny – Andres Vigren, Product Manager, ekspert w zakresie sieciowych kamer stałopozycyjnych. Poruszył on zagadnienia związane z techniką WDR – Forensic Capture, elektroniczną stabilizacją obrazu oraz najnowszym osiągnięciem, jakim są produkty o rozdzielczości 4K Ultra HD. Zaprezentował również urządzenia, które w najbliższym czasie zostaną wprowadzone na polski rynek, w tym kamery z serii F zawierającej najmniejsze dostępne w ofercie Axisa modułowe kamery o szerokim zakresie dynamiki, najnowszy model kamery termowizyjnej AXIS Q1941-E oraz serię obrotowych kamer telekonferencyjnych przeznaczonych do przeprowadzania transmisji broadcastowych – AXIS V59. Najwięcej emocji wśród zgromadzonych wzbudziła jednak panoramiczna kamera AXIS Q6000-E ze względu na swoją nowatorską konstrukcję i niespotykane do tej pory połączenie z wcześniejszym modelem AXIS Q60-E.

Kolejnym punktem programu spotkania partnerów była prezentacja rozwiązań firmy Top-Key. **Marcin Guziński**, dyrektor operacyjny Top-Key, przedstawił aplikacje dla sektora sprzedaży detalicznej oraz oprogramowanie wspierające kamery Axis.

O techniczną stronę wszystkich prezentacji wizualnych zadbała firma **AB Micro**, która dostarczyła ekran marki **Barco**.

Spotkanie było również okazją do wyróżnienia szczególnie zasłużonych partnerów Axis Communications. W tym roku statuetki trafiły do firmy mvb – „Najlepszego Partnera", tytuł „Eksperta w branży" otrzymała firma Top-Key, natomiast firma Honeywell została wyróżniona w kategorii „Ciekawy projekt".

– *Dla naszych partnerów i uczestniczących w spotkaniu dziennikarzy przygotowaliśmy w tym roku niespodziankę. Konferencji towarzyszyły bowiem specjalnie przygotowane stoiska, na których kilka firm partnerskich – **Netrex, Metel, IPS** i **Optex** – prezentowało nowe zastosowania naszych produktów w połączeniu ze swoimi rozwiązaniami* – powiedział **Jan Grusznic**, Sales Engineer w Axis Communications. – *W ten sposób pokazaliśmy, że Axis to nie tylko same produkty, lecz również szereg ciekawych aplikacji i programów tworzonych przez naszych partnerów, które rozszerzają i uzupełniają funkcjonalność kamer Axis. Pokazujemy w ten sposób, że cały czas staramy się sprostać oczekiwaniom wciąż powiększającego się rynku sieciowych systemów wizyjnych i dostarczać naszym klientom kompleksowe rozwiązania dostosowane do ich potrzeb* – dodał.

Bezpośr. inf. Axis Communications

Zapraszamy do obejrzenia fotorelacji (www.zabezpieczenia.com.pl).


AXIS
COMMUNICATIONS


ATM


Innovative

Konferencja Kronos Polska – podsumowanie

Firma **Kronos Polska** wraz z partnerami zorganizowała po raz trzeci konferencję dla przedstawicieli agencji ochrony i monitoringu z całej Polski. Spotkanie odbyło się w dniach 23–24 października ub.r. w Hotel & SPA w Kocierzu. To jeden z ośrodków hotelowo-konferencyjnych, który jest znany z malowniczego położenia oraz wielu atrakcji dla tych, którzy lubią aktywny wypoczynek.

Firma Kronos Polska jest wyłącznym dystrybutorem produktów firmy Next! (jednego z partnerów konferencji), producenta oprogramowania **Kronos NET** służącego do zarządzania stacjami monitorowania.

Podczas konferencji gospodarze przedstawili nowe funkcje oprogramowania **Kronos NET 2.2**. i elektroniczny system prowadzenia dokumentacji w agencjach ochrony – **Koios**.

System Koios jest zgodny z *Rozporządzeniem Ministra Spraw Wewnętrznych z dnia 16 grudnia 2013 r. w sprawie dokumentowania działalności gospodarczej w zakresie usług ochrony osób i mienia i Rozporządzeniem Ministra Spraw Wewnętrznych z dnia 26 sierpnia 2014 r. w sprawie przechowywania, noszenia oraz ewidencjonowania broni i amunicji.*

Koios umożliwia tworzenie m.in. rejestru umów, wykazu pracowników ochrony, książki transportu wartości pieniężnych, książki stanu uzbrojenia i wydania oraz pobrania broni. Ułatwia również prowadzenie ewidencji broni w magazynie. Ponadto może przetwarzać dane zawarte w Kronos NET, takie jak lista klientów, dane obiektów lub umowy.

Firma Kronos Polska ma w swojej ofercie również produkty używane w systemach monitorowania zagrożeń i środowiska, stosowane m.in. przez koncerny paliwowe i energetyczne, wojsko, policję, straż pożarną.

Partnerami konferencji były firmy Infis, Orange Polska, Konsmetal Alians, Next! i Risco Group. O tym, w jakim zakresie partnerzy konferencji współpracują z firmą Kronos Polska oraz co zaprezentowali podczas spotkania, można dowiedzieć się z poniższych wypowiedzi.

Konrad Zając (Infis): „Firma Infis, jako lider branży AVL, zaprezentowała szereg unikatowych rozwiązań wykorzystujących nowoczesne technologie GSM/GPS, które uzupełniają ofertę dla agencji ochrony. Połączenie systemu INFIS z mobilnymi tabletami zmienia całkowicie jakość komunikacji z grupami interwencyjnymi. W wyniku integracji platformy INFIS z systemem Kronos agencje otrzymują gotowy produkt do monitorowania sygnałów z terminali telematycznych, dzięki czemu skracamy do minimum czas wdrożenia. Oferowane przez Infis rozwiązanie pozwala na odczyt wszelkich dostępnych sygnałów z komputerów pokładowych pojazdów. Uzyskane w ten sposób dane są poddawane analizie za pomocą rozbudowanego modułu raportowego. Unikatowe rozwiązanie w postaci modułu ewidencji floty, kart paliwowych, dostępu do bieżącej informacji z pojazdu, systemu powiadomień, czy też możliwości komunikacji z kierowcą, pozwalają na stworzenie pożądanych przez rynek narzędzi. Architektura systemu umożliwia integrację z istniejącym systemami ERP/SAP".

Bartłomiej Kowalewski (Konsmetal Alians): „Konsmetal Alians podjął współpracę w zakresie integracji naszych produktów, w szczególności Systemu Zarządzania Walorami (wspomagającego obrót gotówki w przedsiębiorstwie) oraz Systemu Ochrony i Ewidencji (pozwalającego na elektroniczny nadzór nad bronią i dokumentacją niejawną umieszczoną w szafach i magazynach) z oprogramowaniem firmy Kronos. W trakcie konferencji pokazaliśmy, jak znacząco nasze rozwiązania wpływają na przyśpieszenie procesu rozliczania kasjerów i kierowników przy zachowaniu wysokiego poziomu bezpieczeństwa przechowywanych wartości pieniężnych. Innowacyjnym rozwiązaniem, zgodnym z nowym *Rozporządzeniem Ministra Spraw Wewnętrznych z dnia 26 sierpnia 2014 r. w sprawie przechowywania, noszenia oraz ewidencjonowania broni i amunicji*, była zaprezentowana elektroniczna ewidencja broni połączona z systemem identyfikacji broni w naszych urządzeniach, jak również w projektowanych i wykonywanych przez naszą firmę magazynach broni, kancelariach tajnych oraz innych pomieszczeniach specjalnych".

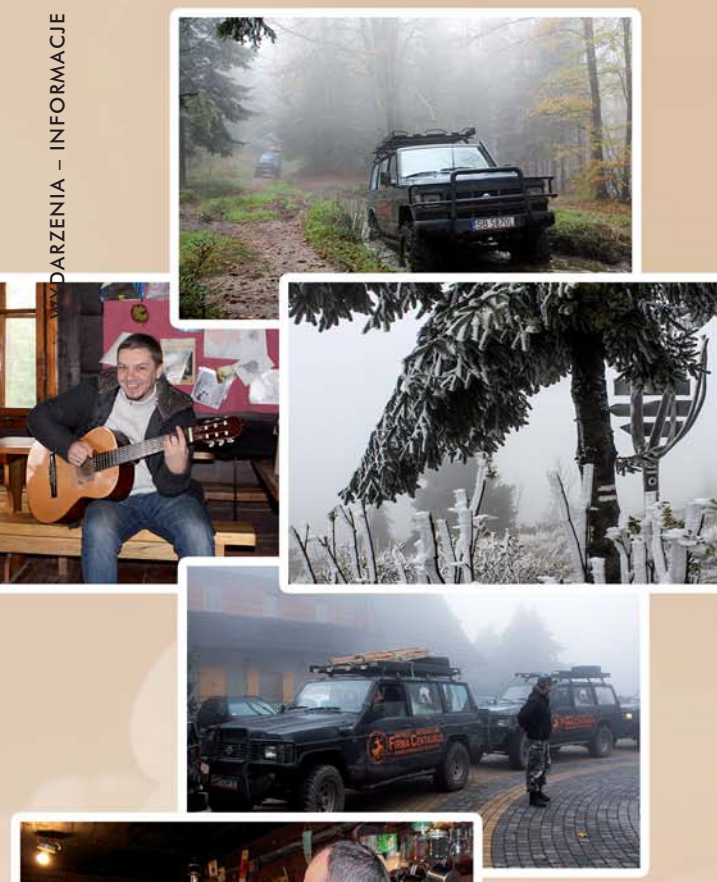
Szymon Woliński (Next!): „Firma Next! z Bielska-Białej to przede wszystkim producent oprogramowania i sprzętu, przeznaczonego głównie dla branży *security*. Flagowym produktem bielskiej spółki jest oprogramowanie służące do zarządzania stacją monitorowania – Kronos NET. Ciągła praca nad systemem pozwoliła nie tylko ugruntować pozycję firmy na rynkach polskim i międzynarodowym, lecz również zdobyć doświadczenie niezbędne przy projektowaniu nowych rozwiązań, m.in. dla banków oraz firm zajmujących się kontrolą strażników pracujących w terenie. Podczas spotkania w Kocierzu odbyły się dwie prezentacje, przygotowane przez przedstawicieli Next! W trakcie pierwszej z nich przedstawiona została najnowsza wersja oprogramowania Kronos NET, a mianowicie wersja 2.2. Szczególny nacisk położono na rozszerzenie profilu usług świadczonych przez agencje ochrony o technologie mobilne. Pojawiła się zatem nowa aplikacja na telefony komórkowe oraz strona WWW, która umożliwia wgląd w bieżące i archiwalne dane dotyczące chronionych obiektów, a także ich edycję. Możemy zatem sprawdzić bieżącą pozycję monitorowanego pojazdu, obejrzeć obraz z kamer CCTV zainstalowanych w domu, a także zobaczyć, czy dziecko wróciło już ze szkoły. Inną grupę mobilnych aplikacji stanowią moduły dla grup interwencyjnych oraz serwisantów, przeznaczone do instalacji na smartfonach i umożliwiające lepszą kontrolę pracowników. Należy zwrócić uwagę na zdecydowaną poprawę wydajności całego systemu, którą udało się uzyskać dzięki współpracy z największymi agencjami ochrony. Druga prezentacja dotyczyła nowości w asortymencie oferowanych urządzeń. Zaprojektowano je w całości w firmie, Next! we współpracy z inżynierami od wielu lat projektującymi urządzenia służące do ochrony. Przedstawiono trzy niezależne rozwiązania:

1) **Arrow** – komunikator do central alarmowych transmitujący sygnały kanałami LAN i WAN, w pełni zintegrowany ze środowiskiem Kronos NET i umożliwiający kontrolę kosztów transmisji.
2) **4Time** – urządzenie do kontrolowania poprzez sieć GSM strażników pracujących w terenie, wyposażone w wyświetlacz, odbiornik GPS oraz czytnik RFiD i zapewniające komunikację głosową.


Oprogramowanie serwerowe
Oprogramowanie w chmurze
Klient WWW - WebKit


INFIS


kronos
www.next.biz.pl



3) **Xamelo** – pierwszy przemysłowy komputer przeznaczony na rynek security, wykorzystywany w sektorze bankowym; potężne narzędzie do integracji wielu systemów bezpieczeństwa.

Mikołaj Ratyński (Orange Polska): „Orange Polska jest częścią światowej grupy telekomunikacyjnej France Telecom. Oferuje kompleksowe rozwiązania i usługi telekomunikacyjne w Polsce – jako przodujący dostawca. Z firmą Kronos Polska współpracujemy od 2012 roku, przede wszystkim w zakresie technologii M2M (*Machine to Machine*). Podczas ostatniej konferencji zaprezentowaliśmy m.in. strategiczne kierunki rozwoju M2M w ramach struktur Orange, zarówno w wymiarze globalnym, jak i na rynku polskim. Podczas spotkania klienci mogli zapoznać się z oferowanymi przez Orange usługami z dziedziny *security*, a w szczególności z zarządzaniem bezpieczeństwem urządzeń, z systemami MDM (Mobile Device Management) do zarządzania urządzeniami oraz ochrony przed atakami DDoS. Na polskim rynku Orange jest liderem w zakresie wdrażania technologii M2M. Swoje usługi realizuje we współpracy ze spółką powstałą w ramach Orange, Integrated Solutions, która dostarcza rozwiązania ICT, takie jak m.in. zabezpieczenia IT, sieci LAN, WAN, usługi *Data Center* oraz szereg usług chmurowych".

Włodzimierz Garwacki (RISCO Group): „Prezentowane na konferencji praktyczne aspekty wykorzystania chmury RISCO w systemach alarmowych są naturalną konsekwencją ciągłego rozwoju RISCO Group. Od 35 lat nasza firma dostarcza kompleksowe rozwiązania z dziedziny elektronicznej ochrony mienia i osób. Tworzymy innowacje, o czym świadczą wyróżnienia naszych produktów przez doceniające nas organizacje branżowe. Nowatorskie rozwiązania można znaleźć zarówno w detektorach (WatchOUT, BWare itd.), jak i w centralach alarmowych (LightSYS, Agility). Warto zwrócić uwagę także na parametry naszych modułów typu GSM/GPRS oraz IP służących do transmisji danych. Nasza współpraca z firmą Kronos Polska ma związek właśnie z nimi. Integracja polega na implementacji unikalnych protokołów transmisji, używanych przez nasze urządzenia, bezpośrednio do obsługi stacji monitorowania z oprogramowaniem Kronos Net. W efekcie administratorzy stacji mają możliwość bezproblemowego, bezpośredniego odbioru sygnałów z chronionych obiektów, ale także mogą zdalnie diagnozować system alarmowy".

Po części merytorycznej konferencji odbyła się uroczysta kolacja, a po niej – degustacja whisky. Następnego dnia odbył się rajd terenowy po drogach górskich. Każdy z gości miał okazję spróbować własnych sił i umiejętności jako kierowca terenowego samochodu Nissan Patrol. Jazda była bardzo emocjonująca i dostarczyła uczestnikom wielu wrażeń.

Podczas konferencji zaprezentowano wiele produktów i rozwiązań, które ułatwiają pracę pracownikom agencji ochrony. Zapewniają niezawodne działanie systemu monitorowania, jednego z najważniejszych elementów wpływających na poziom bezpieczeństwa.

Bardzo dziękujemy firmie Kronos Polska za zaproszenie i życzymy kolejnych udanych konferencji.

Zapraszamy do obejrzenia fotogalerii ze spotkania na naszej stronie internetowej (*www.zabezpieczenia.com.pl*).

Ela Końka

NOVUS®

Bezpłatna aplikacja NMS MOBILE
do zdalnego monitoringu IP

NOVUS MANAGEMENT SYSTEM

- Wyświetlanie „na żywo" obrazu z jednej lub wielu kamer
- Odtwarzanie nagrań
- Sterowanie kamerami PTZ
- Obsługa zdarzeń alarmowych
- Intuicyjny, przyjazny dla użytkownika interfejs

Android Compatible

Zobacz nagrania na swoim smartfonie lub tablecie

NMS Mobile to profesjonalne oprogramowanie klienckie do efektywnego monitoringu 24/7 przez Internet. Aplikacja została zaprojektowana na telefony komórkowe i tablety pracujące na systemie Android (wersja 4.1 lub wyższa)

[http://192.168.0.0]

Prosta instalacja

NMS Mobile można łatwo zainstalować i skonfigurować. Wystarczy tylko wprowadzić w aplikacji adres IP serwera NMS, aby otrzymać zdalny dostęp do materiałów wideo z systemu monitoringu NOVUS IP

Więcej informacji o oprogramowaniu NMS znajdziesz na www.novuscctv.pl

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

Scenariusz rozwoju zdarzeń w czasie pożaru
(Część 1)

Ryszard Małolepszy

W europejskim systemie prawnym zakres ochrony przeciwpożarowej w budownictwie został określony w Rozporządzeniu Parlamentu Europejskiego i Rady Europy Nr 305/2011 z dnia 9 marca 2011 r., ustanawiającym zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych i uchylającym dyrektywę 89/106/EWG

W załączniku nr 1 do tego rozporządzenia (*Podstawowe wymagania dla obiektów budowlanych*) określono, iż obiekty budowlane jako całość oraz ich poszczególne części muszą nadawać się do użycia zgodnie z ich zamierzonym zastosowaniem, przy czym należy w szczególności wziąć pod uwagę zdrowie i bezpieczeństwo osób mających z nimi kontakt przez cały cykl życia tych obiektów. Przy normalnej konserwacji obiekty budowlane muszą spełniać podstawowe wymagania przez gospodarczo uzasadniony okres użytkowania. W punkcie 2 załącznika do rozporządzenia, po wymaganiach dotyczących nośności i stateczności budynków, określone zostały poniższe wymagania dotyczące bezpieczeństwa pożarowego.

Obiekty budowlane muszą być zaprojektowane i wykonane w taki sposób, aby w przypadku wybuchu pożaru:

a) nośność konstrukcji została zachowana przez określony czas,
b) powstawanie i rozprzestrzenianie się ognia i dymu w obiektach budowlanych było ograniczone,
c) rozprzestrzenianie się ognia na sąsiednie obiekty budowlane było ograniczone,
d) osoby znajdujące się wewnątrz mogły opuścić obiekt budowlany lub być uratowane w inny sposób,
e) uwzględnione było bezpieczeństwo ekip ratowniczych.

Powyższe wymagania mają odzwierciedlenie w przepisach techniczno-budowlanych[1] wydanych na podstawie ustawy *Prawo budowlane*, z tym że w tych przepisach nie uwzględniono jeszcze możliwości uratowania ludzi w inny sposób. Uznając jednak, iż przepis europejski ma rangę wyższą niż jakikolwiek krajowy przepis techniczny, należy stosować go bezpośrednio.

Zadaniem projektanta obiektu budowlanego jest dostosowanie się do ww. podstawowych wymagań z zakresu bezpieczeństwa pożarowego. Zadanie to można zrealizować poprzez całkowite spełnienie wymagań techniczno-budowlanych i dotyczących ochrony przeciwpożarowej, które są zawarte w przepisach. Należy spełnić wszystkie wymagania, gdyż nie określono, w jakich przypadkach konkretne przepisy mają zastosowanie. Można też zapewnić spełnienie wymagań podstawowych, w różnym stopniu, kierując się podejściem inżynieryjnym, zorientowanym na osiągnięcie celów funkcjonalnych (ang. *performance based approach*). Takie podejście jest popularniejsze choćby w Australii, Nowej Zelandii, Wielkiej Brytanii czy krajach skandynawskich. W Polsce również podjęto próbę wprowadzenia podejścia inżynieryjnego do przepisów, czego dowodem może być §2, ust. 2 i 3a przepisu techniczno-budowlanego, w którym pojawia się następujące sformułowanie: „przy nadbudowie, rozbudowie, przebudowie i zmianie sposobu użytkowania budynków istniejących wymagania tego przepisu, z wyłączeniem wymagań charakterystyki energetycznej, mogą być spełnione w sposób inny niż określony w tym przepisie, stosownie do wskazań ekspertyzy technicznej właściwej jednostki badawczo-rozwojowej albo rzeczoznawcy budowlanego oraz do spraw zabezpieczeń przeciwpożarowych, uzgodnionych z właściwym komendantem wojewódzkim Państwowej Straży Pożarnej lub państwowym wojewódzkim inspektorem sanitarnym, odpowiednio do przedmiotu tej ekspertyzy. Dla budynków i terenów wpisanych do rejestru zabytków lub obszarów objętych ochroną konserwatorską na podstawie ustaleń miejscowego planu zagospodarowania przestrzennego ekspertyza, o której mowa wyżej, podlega również uzgodnieniu z wojewódzkim konserwatorem zabytków".

Również zgodnie z art. 9, ust. 1 ustawy *Prawo budowlane* z dnia 7 lipca 1994 r.[2] można zastosować rozwiązania równoważne lub związane z funkcjonalnością, na podstawie indywidualnego odstępstwa od przepisów techniczno budowlanych. Możliwość zastosowania rozwiązań alternatywnych lub równoważnych istnieje także w przypadku ochrony przeciwpożarowej. W każdym z przypadków nieodłącznym elementem procedury dopuszczającej rozwiązania alternatywne lub równoważne jest dokładne ustalenie zagrożeń, określenie kryteriów funkcjonalnych, zapewniających spełnienie wymagań podstawowych, i dobór akceptowalnych systemów zabezpieczeń na tej podstawie.

Podejście inżynieryjne, zgodnie z którym najważniejsza jest funkcjonalność, jest przydatne w sytuacjach, w których przepisy techniczno-budowlane czy przeciwpożarowe nie mogą mieć zastosowania, a także wówczas, gdy pożądany jest wyższy poziom bezpieczeństwa pożarowego niż ten określony przepisami.

Trudno oprzeć się wrażeniu, iż określenie „scenariusz rozwoju zdarzeń w czasie pożaru", wprowadzone do przepisu o ochronie przeciwpożarowej dotyczącego uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej, jest również zaleceniem przeprowadzenia inżynieryjnej analizy pożaru, jego rozwoju i wpływu na zdarzenia w danym obiekcie budowlanym celem określenia i zastosowania

1) Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 2002 r. Nr 75, poz. 690 z późn. zm.).

2) Ustawa z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. z 1994 r. Nr 89, poz. 414 z późn. zm.).

w obiekcie odpowiednich, akceptowalnych i spełniających wymagania podstawowe systemów zabezpieczeń przeciwpożarowych.

Krajowe podstawy prawne dla scenariusza rozwoju zdarzeń w czasie pożaru

Formalnie określenie „scenariusz rozwoju zdarzeń w czasie pożaru" zostało wprowadzone do przepisu o ochronie przeciwpożarowej dotyczącego uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej[3] w kontekście doboru urządzeń przeciwpożarowych. Jeden z 14 warunków poprawnego zaprojektowania ochrony przeciwpożarowej w obiekcie budowlanym sformułowano następująco: „11) dobór urządzeń przeciwpożarowych w obiekcie budowlanym, dostosowany do wymagań wynikających z przepisów dotyczących ochrony przeciwpożarowej i przyjętego scenariusza rozwoju zdarzeń w czasie pożaru, a w szczególności: stałych urządzeń gaśniczych, systemu sygnalizacji pożarowej, dźwiękowego systemu ostrzegawczego, instalacji wodociągowej przeciwpożarowej, urządzeń oddymiających, dźwigów przystosowanych do potrzeb ekip ratowniczych". Nie zdefiniowano jednak pojęcia scenariusza. Czy w takim razie warunek jest sformułowany jasno i zrozumiale dla wszystkich uczestników procesu projektowania?

Jeśli odczytuje się użyte sformułowanie dosłownie, bez możliwych interpretacji, to chodzi o samo zjawisko powstania i rozwój pożaru, jego wpływ na strukturę i wyposażenie budynku, na zachowanie i bezpieczeństwo użytkowników budynku, a także o funkcje systemów i ich zadania, które będą wykonywane w czasie pożaru, oraz procedury bezpieczeństwa.

Sposób opracowania scenariusza rozwoju zdarzeń w czasie pożaru

Aby zgodnie z intencjami autorów opracować „scenariusz rozwoju zdarzeń w czasie pożaru", trzeba posłużyć się zasadami inżynierii bezpieczeństwa pożarowego i przyjąć funkcjonalność jako kryterium. Kierując się podejściem inżynieryjnym i stosując sprawdzone procedury, można osiągnąć akceptowalne dla zainteresowanych stron rozwiązanie w postaci scenariusza rozwoju zdarzeń w czasie pożaru. W niniejszym artykule zostanie zaproponowana metodyka przedstawiona w poradniku dla inżynierów *SFPE Engineering Guide to Performance-Based Fire Protection*. Poradnik ten zawiera propozycję uniwersalnej struktury proceduralnej, zgodnie z którą inżynierowie mogą tworzyć rozwiązania z zakresu ochrony przeciwpożarowej zapewniające poziom bezpieczeństwa, który może być uznany za akceptowalny. Zawiera również zalecenia jako metodologię ustalania i dokumentowania tego, że dany, określony cel funkcjonalny ochrony przeciwpożarowej został osiągnięty w konkretnym przypadku zagrożenia pożarowego, a także określa parametry, jakie powinny być uwzględnione w procesie projektowym lub ustalaniu celów funkcjonalnych. Podczas pracy nad niniejszym artykułem wykorzystano również inne dostępne materiały z dziedziny inżynierii bezpieczeństwa pożarowego.

Ze względu na interdyscyplinarność zagadnienia scenariusz rozwoju zdarzeń w czasie pożaru powinien być uzgodniony zarówno z projektantem obiektu, jak i z projektantami branżowymi, a także z inwestorem, który dysponuje określonym budżetem. Ale kto powinien scenariusz przygotować? Wydaje się, że najwłaściwszą osobą jest inżynier zajmujący się bezpieczeństwem pożarowym, odpowiednio przygotowany, kompetentny, posiadający wiedzę dotyczącą charakterystyki pożarów, rozumiejący specyfikę zagrożeń pożarowych, znający skutki pożaru w budynku, jego wpływ na zachowanie ludzi, a także sposoby działania ekip ratowniczych. W polskim systemie prawnym nie zostały określone wymagania dla projektanta, dlatego często przyjmuje się, że scenariusz powinien opracować rzeczoznawca do spraw zabezpieczeń przeciwpożarowych, który rzeczywiście w odpowiednim stopniu jest przygotowany do tego zadania. Należy jednak pamiętać o jednej z głównych zasad dotyczących procesu projektowania, a mianowicie o jak najpełniejszym wyeliminowaniu konfliktów. Zgodnie z polskim prawem projektant powinien przygotować scenariusz, który następnie powinien zostać uzgodniony z rzeczoznawcą.

Proces przygotowywania scenariusza rozwoju zdarzeń w czasie pożaru

Proces przygotowania scenariusza powinien być jednym z etapów projektowania budynku i rozpocząć się w fazie projektu koncepcyjnego, gdy podejmowane są kluczowe decyzje. Ważne jest podejście zespołowe, w tym również udział inwestora lub jego upoważnionego przedstawiciela. Koordynacja pomiędzy dyscyplinami jest niezbędna w celu zapewnienia prawidłowego współdziałania systemów.

Poszczególne etapy procesu przygotowania scenariusza powinny obejmować:

- określenie zakresu scenariusza,
- określenie celów ogólnych,
- określenie celów szczegółowych,
- określenie kryteriów funkcjonalnych,
- opracowanie scenariuszy pożaru i projektowych scenariuszy pożaru,
- dobór biernych i czynnych zabezpieczeń przeciwpożarowych,
- zaplanowanie działań urządzeń przeciwpożarowych i zadań ludzi w przypadku pożaru,
- opracowanie matrycy sterowania.

Określenie zakresu scenariusza

Określenie zakresu scenariusza polega na identyfikowaniu i dokumentowaniu:

- ograniczeń projektu i harmonogramu jego realizacji,
- uczestników procesu realizacji projektu – zainteresowanych stron,
- cech proponowanej konstrukcji budynku i cech pożądanych przez właściciela lub najemcę,
- charakterystyki budynku i jego użytkowników,
- przeznaczenia i funkcji budynku,

3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 czerwca 2003 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz. U. Nr 121, poz. 1137 z późn. zm.).

– zastosowania przepisów i norm,
– zarządzania projektem i jego realizacją (co może pokazać stopień zaangażowania autora scenariusza).

Określenie celów ogólnych

Ochrona przeciwpożarowa ma cztery powiązane ze sobą podstawowe cele:

1) Ochrona życia i zdrowia. Należy zapewnić ochronę mieszkańcom i użytkownikom budynków, a także służbom ratowniczym.
2) Ochrona mienia. Należy zminimalizować zniszczenia dóbr materialnych powstałe wskutek pożaru.
3) Należy umożliwić zachowanie ciągłości działalności (np. umożliwić zachowanie zdolności operacyjnej, kontynuowanie produkcji), minimalizując zniszczenia.
4) Ochrona środowiska. Należy ograniczyć wpływ pożaru na środowisko związany z uwalnianiem się produktów spalania i możliwością skażenia środowiska szkodliwymi substancjami, które mogą powstać lub uwolnić się w wyniku pożaru.

Określenie celów szczegółowych

Cele szczegółowe są zasadniczo celami ogólnymi scenariusza, które są następnie sprowadzone do konkretnych wielkości i uściślone w kategoriach inżynierskich. Cele szczegółowe to wyeliminowanie lub ograniczenie konsekwencji pożaru sprowadzonych do utraty życia, utraty zdrowia, konkretnych, policzalnych strat materialnych i konkretnych, dających się dokładnie określić ograniczeń w funkcjonowaniu obiektu. Określa się wielkość obszaru objętego pożarem, wielkość obszaru, na którym obecne są produkty spalania, maksymalne dopuszczalne obrażenia osób, uszkodzenia budynku lub jego wewnętrznego wyposażenia, uszkodzenia najważniejszych urządzeń, zakłócenia najważniejszych procesów przebiegających w budynku, długość przestoju lub zakłócenia działalności.

Określenie kryteriów funkcjonalnych

Kryteria funkcjonalne są dalszym uściśleniem celów projektowych w postaci wartości liczbowych. Kryteria funkcjonalne mogą dotyczyć między innymi wartości progowych temperatury materiałów, temperatury gazów, poziomów karboksyhemoglobiny (COHb), utraty widoczności w związku z zadymieniem, poziomów strumienia promieniowania cieplnego itp.

Przy określaniu kryteriów funkcjonalnych trzeba pamiętać, że nie ma środowiska całkowicie wolnego od zagrożenia lub ryzyka. Pamiętajmy, że zmniejszając dopuszczalne zagrożenie lub ryzyko, ponosimy zazwyczaj wyższe koszty.

Następna część zostanie zamieszczona w kolejnym numerze.

Ryszard Małolepszy
Absolwent Szkoły Głównej Służby Pożarniczej
rzeczoznawca ds. zabezpieczeń przeciwpożarowych
rzeczoznawca SITP
dyrektor Izby Rzeczoznawców Stowarzyszenia Inżynierów i Techników Pożarnictwa

Dobre praktyki w zarządzaniu bezpieczeństwem monitorowania systemów pożarowych

Janusz Sawicki

Urządzenia wchodzące w skład systemów transmisji pożarowych sygnałów alarmowych i sygnałów uszkodzeniowych (UTAPS) są wyrobami budowlanymi. Jako wyroby budowlane podlegają regulacjom prawnym i technicznym dotyczących tej grupy wyrobów. Wymagania prawne dotyczące wytwarzania, procesu certyfikacji, obrotu i stosowania UTAPS są takie same jak dla innych wyrobów budowlanych

Ogólne wymagania techniczne dotyczące systemów transmisji pożarowych sygnałów alarmowych i sygnałów uszkodzeniowych są ujęte w mandacie nr M109 na opracowanie norm zharmonizowanych dotyczących grupy wyrobów przeznaczonych do wykrywania i sygnalizacji pożaru, określonych jako podzespoły. Do tej grupy zostały zaklasyfikowane między innymi następujące urządzenia:

– czujki dymu, czujki ciepła i czujki płomienia,
– urządzenia sterujące i sygnalizacyjne,
– urządzenia do transmisji sygnałów alarmowych,
– izolatory zwarć,
– urządzenia alarmowe,
– zasilacze,
– urządzenia wejścia/wyjścia,
– ręczne ostrzegacze pożarowe.

Wynika z tego, że urządzenia do transmisji alarmu pożarowego są potraktowane jako urządzenia mające działać w początkowej fazie pożaru. Analiza rozwoju zdarzeń w czasie pożaru, dokonywana ze względu na potrzebę tworzenia scenariuszy pożarowych, zakłada, że najbardziej pożądane jest przesłanie komunikatu za pomocą UTAPS-u i odbiór potwierdzenia jego przyjęcia przez jednostkę ratowniczo-gaśniczą Państwowej Straży Pożarnej w czasie nie przekraczającym dziesięciu minut od momentu wejścia centrali sygnalizacji pożarowej (CSP) w stan pracy alarmowej. Pozwoli to na przyjazd i rozwinięcie jednostek ratowniczo-gaśniczych (JRG) w takiej fazie rozwoju pożaru (chodzi przede wszystkim o temperaturę), w której będzie możliwe skuteczne i w miarę bezpieczne działanie ekip ratowniczo-gaśniczych. Jednocześnie umożliwi to bezpieczną ewakuację ludzi z zagrożonej strefy pożarowej – taką, której przebieg nie będzie zakłócał działań gaśniczych.

Zastosowanie urządzeń do transmisji alarmów pożarowych

Urządzenia do transmisji alarmów pożarowych i uszkodzeniowych umożliwiają odpowiednie wczesne działanie JRG, a tym samym ograniczenie strat w ludziach i strat materialnych. Pomimo ich ogromnego znaczenia dla bezpieczeństwa pożarowego obiektów budowlanych sytuacja prawna dotycząca procesu certyfikacji i zastosowania tych wyrobów jest dosyć skomplikowana.

Należy sobie przypomnieć, że norma PN-EN 54-21:2009 dotyczy tylko urządzeń nadawczych. Oznacza to, że proces uznawania, badań kwalifikacyjnych i cały proces certyfikacji i nadzoru na certyfikatem zgodności dotyczy tylko części systemu przesyłania sygnałów alarmu pożarowego. Urządzenia odbiorcze i pośredniczące nie podlegają powyższym wymaganiom, a więc ich status nie jest do końca zdefiniowany.

Aby nieco uregulować sprawy związane z odbiorem sygnałów alarmowych i uszkodzeniowych, a także zapewnić wysłanie sygnału potwierdzenia do urządzenia nadawczego, w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji w sprawie wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. Nr 85 z 27 kwietnia 2010 r., poz. 553) zawarto wymagania dla urządzeń odbiorczych. Oznacza to, że urządzenia nadawcze UTAPSU powinny być stosowane w ochronie przeciwpożarowej na podstawie dwóch dokumentów, a mianowicie certyfikatu dopuszczenia (CE) wydanego przez europejską jednostkę akredytowaną i świadectwa dopuszczenia wydanego przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej PIB im. J. Tuliszkowskiego w Józefowie. Dla urządzeń odbiorczych (pośredniczących) wymagane jest tylko świadectwo dopuszczenia.

Bardzo ważne jest określenie zadań UTAPS-u w związku z podstawowymi wymaganiami dotyczącymi bezpieczeństwa pożarowego w obiektach budowlanych. Stosowanie systemów

transmisji sygnałów alarmów pożarowych i sygnałów uszkodzeniowych ma na celu spełnienie podstawowych wymagań dotyczących bezpieczeństwa pożarowego w obiektach budowlanych, które można ująć następująco:

- ograniczenie powstawania i rozprzestrzeniania się ognia i dymu – zapewniają je systemy sygnalizacji pożarowej, oddymiania i zapobiegania zadymieniu, systemy gaszenia gazem, oddzielenia pożarowe, systemy transmisji sygnałów alarmu pożarowego i sygnału o uszkodzeniu UTAPS;
- umożliwienie opuszczenia obiektu przez mieszkańców lub ratowania ich w inny sposób – zapewniają to systemy ewakuacji (oświetlenia ewakuacyjnego, kontroli dostępu, dźwigi osobowe dla straży pożarnej i inne systemy techniczne obiektu nie będące instalacjami przeciwpożarowymi), dźwiękowe systemy ostrzegawcze, systemy UTAPS, urządzenia alarmujące, systemy oddymiania i oddzieleń pożarowych;
- zadbanie o bezpieczeństwo ekip ratowniczych – zapewniają je systemy UTAPS, dźwigi dla straży pożarnych, dźwiękowe systemy ostrzegawcze, systemy oddymiania, telewizja dozorowa, instalacje i systemy nadzoru technicznego obiektu zintegrowane w taki sposób, aby umożliwić działanie odpowiednich instalacji na życzenie ekip ratowniczo-gaśniczych.

Z tego wynika, że systemy transmisji, umożliwiając współpracę instalacji przeciwpożarowych w obiekcie z jednostkami ratowniczo-gaśniczymi, pełnią kluczową rolę w całym systemie bezpieczeństwa pożarowego obiektów budowlanych.

Regulacje dotyczące bezpieczeństwa pożarowego w rozporządzeniu nr 305/2011 Parlamentu Europejskiego i Rady Europy z 9 marca 2011 r.

Nowe rozporządzenie nr 305/2011 wprowadza nowe regulacje prawne dotyczące wprowadzania do obrotu i stosowania wyrobów budowlanych, a więc także UTAPS-u. Rozporządzenie stawia przed producentami wyrobów budowlanych nowe wymagania dotyczące określania cech zasadniczych wyrobów i ich weryfikacji w jednostkach akredytowanych. Przede wszystkim wprowadza nowy sposób deklarowania właściwości użytkowych wyrobu oraz jednolite oznakowanie „CE" dla wyrobów budowlanych. Rozporządzenie jest nazywane w skrócie rozporządzeniem CPR (*Construction Products Regulation*).

Wszystkie przepisy rozporządzenia obowiązują od dnia 13 lipca 2013 r. Rozporządzenie nr 305/2011 dotyczy wszystkich państw członkowskich UE i powinno być przez nie traktowane jako akt prawny, który jest nadrzędny wobec przepisów krajowych. Państwa członkowskie, w tym Polska, musiały dostosować do niego przepisy krajowe, usuwając sprzeczności. Rozporządzenie CPR zastąpiło w całości regulacje wynikające z dyrektywy budowlanej 89/106 EWG.

A co u nas w kraju?

Niestety Polska nie zdążyła wprowadzić zapisów rozporządzenia 305/2011 do 13 lipca 2013 r. W związku z tym zmodernizowano i dostosowano do okresu przejściowego ustawę o wyrobach budowlanych z 2004 r.

Zgodnie z art. 4 zmienionej ustawy o wyrobach budowlanych z dnia 8 sierpnia 2013 r. akty wykonawcze do rozporządzenia 305/2011 mają być opracowane do 8 sierpnia 2015 r. Należą do nich:

- Rozporządzenie Ministra Infrastruktury i Rozwoju w sprawie deklarowania zgodności wyrobów budowlanych oraz sposobu znakowania ich znakiem budowlanym,
- Rozporządzenie Ministra Infrastruktury i Rozwoju w sprawie krajowych ocen technicznych,
- Rozporządzenie Ministra Infrastruktury i Rozwoju w sprawie zakresu informacji o wynikach zleconych do badań próbek, przeprowadzonych kontrolach wyrobów budowlanych wprowadzonych do obrotu lub udostępnionych na rynku krajowym i wydanych postanowieniach, decyzjach i opiniach, a także o sposobie i terminie przekazywania tych informacji,
- projekt ekspercki: Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej zmieniające rozporządzenie w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie.

A co w UE?

UE wydała następujące przepisy wykonawcze do rozporządzenia nr 305/2011:

- Rozporządzenie delegowane nr 574/2014 Komisji Europejskiej z dnia 21 lutego 2014 r. zmieniające załącznik III do rozporządzenia nr 305/2011 Parlamentu Europejskiego i Rady Europy w odniesieniu do wzoru, który należy stosować przy sporządzaniu deklaracji właściwości użytkowych wyrobów budowlanych – Dz. U. UE Nr L 159/41 (PL) z 28.05.2014 r. (do przestrzegania całości rozporządzenia zobowiązane są wszystkie państwa UE).
- Rozporządzenie delegowane nr 157/2014 z dnia 30 października 2013 r. w sprawie udostępniania deklaracji właściwości użytkowych wyrobów budowlanych na stronie internetowej – Dz. U. UE nr L 52 z 21 lutego 2014 r., s. 1 (do przestrzegania całości rozporządzenia zobowiązane są wszystkie państwa UE).

Z tego wynika, że czeka nas prawdziwa rewolucja i gigantyczna praca legislacyjna.

Sugestie ludzi z branży

Przed przystąpieniem do pracy nad niniejszym artykułem pozwoliłem sobie poprosić kilka kompetentnych osób o sugestie, wskazanie problemów i dobrych praktyk. Oto wskazówki:

1) Należy uporządkować regulacje dotyczące systemu transmisji sygnałów alarmu pożarowego od momentu jego wysłania do odbioru przez Państwową Straż Pożarną. Obecnie wytyczne dla komendantów rejonowych PSP nie stanowią prawa dla projektantów, inwestorów i operatorów.

Komentarz: „Oczywiście takie regulacje powinny być opracowane z udziałem podmiotów zainteresowanych bezpieczeństwem pożarowym, a więc przedstawicieli branży urządzeń do transmisji alarmów, PSP, firm ubezpieczeniowych oraz przedstawicieli środowisk naukowych i normalizacyjnych zajmujących się tą problematyką".

2) Obecne przepisy – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2006 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. Nr 80 z 11 maja 2006 r., poz. 563, nowelizacja z 6 maja 2010 r.) – enumeratywnie wymieniają obiekty, które należy wyposażyć w SSP i urządzenia do monitorowania alarmu pożarowego. Lista obiektów budowlanych nie odpowiada rzeczywistości i powinna być poszerzona.

Komentarz: „Uważam, że wszystkie obiekty o dużym znaczeniu dla gospodarki, a więc przede wszystkim obiekty kategorii PM, powinny być wyposażone w systemy transmisji sygnałów alarmu pożarowego. Duże znaczenie mają w tym przypadku decyzje towarzystw ubezpieczeniowych".

3) Na etapie projektowania powinny być określone i wprowadzone czasy opóźnień uruchomienia UTAPS-u, i podziału na strefy pożarowe. Czasy powinny wynikać z opracowanych scenariuszy pożarowych dla obiektu budowalnego lub matryc sterowań.

Komentarz: „Tak – wszystkie dane ilościowe, w tym dane dotyczące opóźnień, blokad i sposobu ich realizacji, powinny być czerpane ze scenariusza zdarzeń w czasie pożaru. Dokument ten powinien być opracowany wraz z projektem budowlanym obiektu i być podstawą doboru urządzeń przeciwpożarowych, sposobu ich działania i przeprowadzania testów odbiorowych. Na podstawie scenariusza pożarowego powinien być oceniany poziom bezpieczeństwa danego obiektu. Scenariusz powinien zostać utworzony przez ekspertów z dziedziny inżynierii bezpieczeństwa pożarowego".

4) Należy prawnie zastrzec konieczność tworzenia systemów bezpieczeństwa, w tym systemów pożarowych, przez osoby lub firmy posiadające kompetencje potwierdzone uprawnieniami i certyfikatami.

Komentarz: „Sprawa jest bardzo nagląca i wszystkie środowiska związane z bezpieczeństwem pożarowym obiektów budowlanych powinny dążyć do tego, by prawo budowlane narzucało taką konieczność. Zmiany próbowało wprowadzić Stowarzyszenie Inżynierów i Techników Pożarnictwa w 2011 r. Niestety nie udało się. Sytuacja, w której o nasze bezpieczeństwo dbają osoby przypadkowe i niekompetentne, jest nie do przyjęcia".

Podsumowanie

Systemy transmisji sygnałów alarmu pożarowego są jednymi z wielu systemów przeciwpożarowych w obiektach, od których działania zależy bezpieczeństwo użytkowników, mieszkańców, a także ekip ratowniczo-gaśniczych. Sprawy opisane w niniejszym artykule dotyczą wszystkich urządzeń przeciwpożarowych. Techniczne środki zabezpieczeń powinny charakteryzować się wysoką niezawodnością działania zarówno w momencie ich zainstalowania, jak i w całym okresie eksploatacji. Potrzebna jest także praca ośrodków eksperckich i szkoleniowych – ludzie odpowiedzialni za bezpieczeństwo pożarowe obiektów budowlanych powinni mieć odpowiednią wiedzę potrzebną do pracy z urządzeniami w czasie pożaru, a więc w sytuacji kryzysowej.

mgr. inż. Janusz Sawicki
IBP Nodex

Protec 6400
innowacja w ochronie przeciwpożarowej

Konrad Kowal

Firma D+H Polska powiększyła ofertę o nowy system sygnalizacji pożarowej Protec 6400. Jest to interaktywna, cyfrowa i adresowalna centrala sygnalizacji pożarowej przeznaczona dla obiektów o średniej i dużej kubaturze, takich jak obiekty przemysłowe, hotele, biurowce, lotniska, szpitale. System charakteryzuje się wysoką odpornością na fałszywe alarmy, precyzyjnym lokalizowaniem zdarzeń pożarowych (aż 120 znaków opisu na wyświetlaczu) i można do niego przyłączyć wiele elementów pętlowych. System Protec jest znany i ceniony za wysoką jakość i niezawodność. Od lat jest stosowany w krajach Europy Zachodniej. Dzięki firmie D+H jest dostępny również w Polsce. Centrala Protec 6400 przeszła pozytywnie proces certyfikacji i posiada świadectwo dopuszczenia CNBOP

Fot. 1. Centrala Protec 6400

Protec umożliwia transmisję dużej ilości informacji, bardziej szczegółowych niż w systemach analogowych. Centrala może pracować w różnych trybach, zgodnie z funkcją obiektu i panującymi w nim specyficznymi warunkami środowiskowymi. Czujki Protec potrafią rozpoznawać czynniki kwalifikujące zdarzenie jako pożarowe i odróżnić je od czynników wywołujących fałszywe alarmy. Z tego powodu system doskonale sprawdza się w trudnych warunkach środowiskowych.

Bezpieczna sieć

Sieć systemu tworzą rozproszone po obiekcie panele kontroli i wyświetlania (6400/DCN), panele obsługi pętli (6400/LPN) oraz ich różne konfiguracje (np. 6400/DCN/LPN) w jednej obudowie. Połączenie paneli w pętle i użycie protokołu komunikacyjnego RS485 daje pewność, że żadne pojedyncze uszkodzenie nie spowoduje wstrzymania pracy systemu. Sprawność działania sieci paneli zapewnia również przesyłanie pomiędzy nimi bieżących informacji systemowych. Można zobaczyć je w każdym panelu (6400/DCN). W celu zwiększenia bezpieczeństwa panele (6400/DCN i 6400/LPN) przechowują zaprogramowaną konfigurację systemu. Każdy z nich (6400/DCN) umożliwia także sterowanie i konfigurację całej sieci, bez potrzeby wyznaczenia jednego panelu głównego. Połączenia sieciowe mogą być realizowane za pomocą przewodów miedzianych lub światłowodów.

Integralność systemu i zwiększona sprawność

Panele rozmieszcza się, uwzględniając strukturę obiektu oraz łatwość ułożenia okablowania. Dzięki temu pętle oraz linie sygnalizatorów są krótsze, bo przyłączone do najbliższego panelu (6400/LPN). Takie rozwiązanie pozwala nam na uniknięcie prowadzenia wszystkich przewodów systemu do jednego centralnie położonego miejsca. Tym samym zwiększa się integralność i sprawność działania całego układu, ponieważ pojedyncze zdarzenie na pętli spowoduje problemy w niewielkiej części systemu.

Fot. 2. 6000 MCP WP – adresowalny ręczny ostrzegacz pożarowy (ROP)

Fot. 3. 6000 SSR2 – adresowalny sygnalizator akustyczny

Fot. 4. 6000PLUS/HT – interaktywna, adresowalna czujka ciepła

Duża elastyczność

Centrala Protec umożliwia dołączanie różnych dodatkowych elementów pętlowych. Na pętli dozorowej mogą być montowane ręczne ostrzegacze pożarowe, adresowalne sygnalizatory akustyczne zasilane z pętli, różnego rodzaju detektory, w tym adresowalne czujki liniowe i (lub) czujki zasysające, oraz moduły. Istnieje również możliwość bezpośredniego włączenia do pętli dozorowej adresowalnego, pętlowego wyświetlacza LCD. Wszystkie elementy systemu Protec są włączone do centrali za pomocą przewodu pętlowego, dzięki czemu można znacznie obniżyć koszty okablowania.

System 6400 jest systemem rozproszonym, dlatego można go łatwo rozbudować przez dodanie paneli obsługi pętli (6400/LPN). Każda z czterech pętli umożliwia przyłączenie do 127 interaktywnych, adresowalnych urządzeń Protec Algo-Tec 6400, co daje łącznie 508 adresowalnych urządzeń na jeden panel (6400/LPN). Przy maksymalnym wykorzystaniu 99 paneli pojemność sieci to ponad 50000 urządzeń. Jeżeli ta liczba okaże się za mała, można stworzyć drugą sieć i połączyć je ze sobą.

Konfiguracja

System jest programowany na miejscu, z wykorzystaniem specjalnego oprogramowania komputerowego. Dane konfiguracyjne można pobrać z dowolnego panelu 6400/DCN za pośrednictwem wbudowanego portu RS232 i rozesłać siecią systemu Protec 6400. Taka metoda programowania nie tylko skraca czas konfiguracji w obiekcie, ale także pozwala tworzyć kopie bezpieczeństwa systemu.

Szeroka gama urządzeń peryferyjnych

System Protec 6400 może współpracować z wieloma typami czujek – czujkami ciepła, czujkami optyczno-termicznymi, czujkami z dodatkowym sensorem CO, czujkami zasysającymi Cirrus Pro i samokalibrującymi się czujkami liniowymi. Poniżej wymienione są niektóre z nich.

6000PLUS/HT – interaktywna, adresowalna czujka ciepła
Czujka ta jest wyposażona w półprzewodnik charakteryzujący się niską barierą reakcji na energię termiczną, reagujący

Rys. 1. Programowanie różnych trybów pracy z uwzględnieniem funkcji obiektu oraz panujących w nim specyficznych warunków środowiskowych

Fot. 5. 6000PLUS/OP – interaktywna, adresowalna optyczna czujka dymu

szybko na wszelkie zmiany temperatury. Inne czujki ciepła, które można zastosować, to 6000PLUS/HT/S, 6000PLUS/HT/SL oraz 6000PLUS/HT/TSL.

6000PLUS/OP – interaktywna, adresowalna optyczna czujka dymu
Czujka ta gwarantuje wysoką wydajność i szybkie wykrywanie pożaru z wykorzystaniem rozproszonej wiązki światła. Można zastosować także inną optyczną czujkę dymu – 6000PLUS/OPT/S.

6000PLUS/OPHT – interaktywna, adresowalna czujka optyczno-termiczna
Jest to wysokowydajna czujka, która jest połączeniem dwóch współpracujących ze sobą detektorów. Inne możliwe do zastosowania wersje tej czujki to 6000PLUS/OPHT/S, 6000PLUS/OPHT/L, 6000PLUS/OPHT/SL, 6000PLUS/OPHT/TS, 6000PLUS/OPHT/TSL.

6000PLUS/OPHTCO – interaktywna, adresowalna czujka optyczno-termiczna z detektorem CO
Czujka ta jest bardzo wydajna i jest wyposażona w dodatkowy detektor tlenku węgla. Inne możliwe do zastosowania wersje tej czujki to 6000PLUS/OPHTCO/S, 6000PLUS/OPHTCO/L, 6000PLUS/OPHTCO/SL, 6000PLUS/OPHTCO/TSL.

6000PLUS/BASE – niskoprofilowe gniazdo czujek adresowalnych
Jest to gniazdo odpowiednie dla detektorów Algo-Tec 6000PLUS.

6000/MCP – adresowalny ręczny ostrzegacz pożarowy (ROP)
Ostrzegacz ten ma wbudowany izolator zwarć. Umożliwia łatwy test z użyciem kluczyka serwisowego.

6000/SSR2 – adresowalny sygnalizator akustyczny
Sygnalizator ten jest zasilany z pętli i charakteryzuje się niskim poborem prądu. Można go dowolnie konfigurować.

6000/MICCO – moduł wejścia/wyjścia (zasilany z pętli)
Moduł ten jest wyposażony w monitorowane wejście oraz wyjście przekaźnikowe o maksymalnej obciążalności 240 V. Służy do podłączenia urządzeń zewnętrznych.

6000/2IO – ma dwa monitorowane wejścia oraz dwa wyjścia przekaźnikowe. Służy do podłączenia urządzeń zewnętrznych.

6000/APZA – moduł konwencjonalnej linii bocznej i sygnalizatorów (zasilany zewnętrznie).

Cirrus Pro – czujka konwencjonalna, przeznaczona do bardzo wczesnego wykrywania zagrożenia pożarowego. Charakteryzuje się dużą odpornością na fałszywe alarmy powodowane przez kurz, opary, skroplenia, wilgoć, przepływ powietrza czy zmiany temperatury. Można ją wykorzystać jako urządzenie pętlowe po zastosowaniu dodatkowej karty adresowej.

Konrad Kowal
Senior Product Manager
D+H Polska

Fot. 6. Czujka Cirrus Pro 200

Zasilacze buforowe serii EN54 do systemów przeciwpożarowych

Część 2 – funkcje

Pulsar

Zasilacze buforowe do systemów przeciwpożarowych serii EN54 firmy PULSAR to nowoczesne urządzenia zaprojektowane zgodnie z wymaganiami przedstawionymi w normach PN-EN 54-4:2001/A2:2007, PN-EN 12101-10:2007 oraz punkcie 12.2 rozporządzenia MSWiA z 20.06.2007 (Dz. U. nr 143, poz. 1002) ze zmianami z 27.04.2010. Zasilacze nie tylko spełniają powyższe wymagania, ale także mają szereg nowatorskich właściwości i funkcji

Firma Pulsar oferuje zasilacze z wyświetlaczem LED i zasilacze z wyświetlaczem LCD. Różnica pomiędzy nimi polega na sposobie prezentacji parametrów na panelu czołowym. Jedne i drugie występują w odmianach o wydajności prądowej 2A, 3A, 5A, i 7A. Urządzenia te mają wszystkie potrzebne funkcje i spełniają wszystkie wymagania, jakim muszą sprostać zasilacze do systemów sygnalizacji pożarowej. Oprócz tego na wyświetlaczu LED można odczytać następujące parametry:

– aktualne napięcie na wyjściu,
– aktualny prąd pobierany przez urządzenia dołączone do zasilacza,
– rezystancję obwodu akumulatorów zmierzoną podczas ostatniego testu,
– aktualną temperaturę akumulatorów,
– napięcie zasilające (sieciowe).

Za pomocą wyświetlacza można łatwo i zgodnie z wymaganiami użytkownika skonfigurować parametry

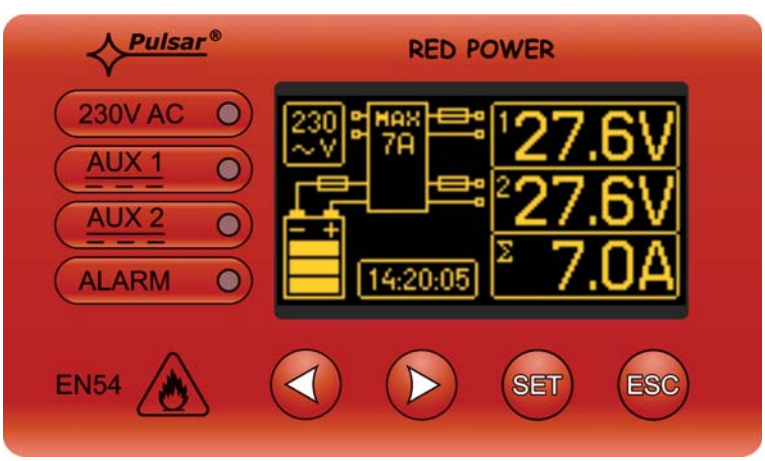
zasilacza, takie jak: czas opóźnienia sygnalizacji braku napięcia sieciowego, wyłączenie i załączenie sygnalizatora akustycznego, wyłączenie lub załączenie wyświetlacza, załączenie wyjścia technicznego EXTo oraz parametry komunikacji. Można również w każdej chwili wykonać test akumulatora.

Dzięki wyświetlaczowi możemy odczytać powiadomienia o bieżących awariach zasilacza, jak również historię awarii. Kody awarii są przedstawione w trzycyfrowej formie. Tabela kodów, dzięki której możemy ustalić rodzaj awarii, jest dołączana do każdego zasilacza.

Diody LED na panelu pozwalają na szybką ocenę pracy zasilacza bez korzystania z menu. Z kolei zasilacze wyposażone w wyświetlacz LCD umożliwiają jeszcze pełniejszą i bardziej komfortową kontrolę nad parametrami i konfiguracją urządzenia. Po pierwszym załączeniu zasilacza z wyświetlaczem LCD można wybrać język, w którym będzie odbywać się komunikacja z użytkownikiem. Dostępnych jest kilkanaście języków. Oczywiście język można później zmienić.

Oprócz ekranu głównego, na którym wyświetlane są podstawowe parametry pracy zasilacza, dostępne są cztery ekrany dodatkowe:

1) Ekran parametrów bieżących (napięcie zasilające, napięcie baterii, temperatura baterii, napięcia na wyjściach AUX1, AUX2).
2) Ekran bieżących awarii. Wyświetla informacje o awariach, które występują w danej chwili.



Fot. 1. Wyświetlacz graficzny LCD

Fot. 2. Wyświetlacz LED

Certyfikat zgodności i świadectwo dopuszczenia CNBOP dla zasilaczy serii EN54 (RED POWER)

3) Ekran historii parametrów. Na nim w formie wykresu podawane są parametry zasilacza – napięcia wyjściowe, napięcie baterii, napięcie zasilające, prąd, temperatura. Można sprawdzać, jakie były parametry w danym okresie.
4) Ekran historii zdarzeń. Pozwala zapoznać się z informacjami o zdarzeniach (np. start zasilacza, wyłączenie) oraz awariach zapisanych w historii. W informacjach podana jest data, opis i kod zdarzenia.

Do ustawień konfiguracyjnych służy menu nastawy zasilacza. Jest ono podzielone na trzy części:

1) Menu zasilacz. Umożliwia ustawienie takich parametrów jak sygnalizacja dźwiękowa, opóźnienie sygnalizacji zaniku napięcia sieciowego, załączenie/wyłączenie dodatkowego wyjścia technicznego EXTo, a także zmianę parametrów komunikacji zasilacza. W tym menu można w każdej chwili uruchomić test akumulatora.
2) Menu pulpit. Umożliwia ustawienie daty, czasu, języka, podświetlenia zasilacza, jasności, kontrastu i wygaszenia wyświetlacza.
3) Menu hasło. Umożliwia ustawienie trzech poziomów dostępu do zasilacza zabezpieczonych osobnymi hasłami:
– blokada klawiatury – dostępny jest tylko ekran główny zasilacza, bez podania hasła nie można skorzystać z menu;
– użytkownik – pozwala na sprawdzenie parametrów zasilacza i zmianę podstawowych spośród nich, takich jak język, data, czas, podświetlenie;
– instalator – pozwala na pełną kontrolę i konfigurację parametrów zasilacza.

Więcej informacji można znaleźć na stronie producenta (*www.pulsar.pl*).

Pulsar
Siedlec 150
32-744 Łapczyca
e-mail: biuro@pulsar.pl
www.pulsar.pl

NOWOŚĆ!

Nowoczesne zasilacze do systemów ochrony przeciwpożarowej

Pulsar®

www.pulsar.pl

Certyfikat zgodności i świadectwo dopuszczenia

CNBOP-PIB

Zasilacze buforowe

zgodne z normą EN 54-4

z możliwością monitoringu przez sieć Ethernet, Wi-Fi, RS485, USB

5 LAT GWARANCJI

CNBOP-PIB CE 1438 Pulsar

Certyfikat zgodności CNBOP Nr 1438-CPR-0385
Świadectwo dopuszczenia CNBOP Nr 2174/2014

RED POWER

Dostępne modele

		Prąd wyjściowy (praca chwilowa $I_{max\ b}$)			
		2A*	3A*	5A*	7A*
Miejsce na akumulator	2×17Ah	EN54-2A17	EN54-3A17	EN54-5A17	EN54-7A17
	2×28Ah	-	EN54-3A28	EN54-5A28	EN54-7A28
	2×40Ah	-	-	EN54-5A40	EN54-7A40

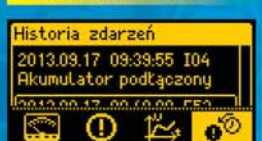
wyświetlacz LED

wyświetlacz graficzny LCD

bieżące parametry zasilacza

bieżące awarie zasilacza

historia parametrów zasilacza



historia zdarzeń

Systemy na miarę nowoczesnych budynków

Karolina Olechowicz

Zgodnie z analizami Cushman & Wakefield ożywienie gospodarcze jest widoczne we wszystkich sektorach, co pozytywnie wpływa na rynek nieruchomości komercyjnych. W Warszawie na etapie planowania i realizacji jest rekordowa liczba biurowych projektów deweloperskich[1]. Inwestorzy, deweloperzy i generalni wykonawcy dbają o optymalny czas realizacji, atrakcyjność i nowoczesność projektu, efektywność podziału powierzchni użytkowej i przystosowanie jej do różnych potrzeb najemców. Na etapie realizacji inwestycji uwzględniane są potrzeby przyszłych użytkowników i komfort ich pracy, a zarazem efektywność zarządzania obiektem i wdrożonymi w nim systemami. Nowoczesne rozwiązania mają wspierać zarządców budynku w optymalizacji kosztów, ale przede wszystkim – dzięki dopasowaniu ich do potrzeb i przyzwyczajeń użytkowników – zapewniać komfort i kształtować przyjazną atmosferę w danej przestrzeni biurowej

1) Raport „Marketbeat Polska – Jesień 2014", Cushman & Wakefield

Komfort użytkowników i optymalizacja kosztów utrzymania budynku

Nowoczesne technologie wykorzystywane w budynkach mogą zwiększyć koszty inwestycji, ale obniżają koszty eksploatacji. W tym celu wykorzystuje się np. sterowanie systemami wentylacji i klimatyzacji, sterowanie oświetleniem, monitorowanie zużycia wody, prądu i ciepła. Dobranie systemu odpowiadającego specyfice obiektu, odpowiedni sposób instalacji, integracja z innymi systemami z uwzględnieniem funkcjonalności i założeń eksploatacyjnych to kluczowe czynniki wpływające na wykorzystanie potencjału wdrożonych rozwiązań.

Systemy automatyki budynkowej i zarządzania budynkami (ang. *Building Automation Systems* – BAS, *Building Management Systems* – BMS) to zaawansowane rozwiązania techniczne, których celem jest efektywne sterowanie instalacjami znajdującymi się w obiekcie. Dzięki centralizacji systemów BAS i BMS istnieje możliwość połączenia wielu wyposażonych w nie obiektów w grupy i sterowania nimi centralnie, z dowolnego miejsca na świecie, za pośrednictwem Internetu (np. można zdalnie wyłączać oświetlenie i wentylację po godzinach pracy biura lub załączać alarm w dozór). Daje to możliwość monitorowania pracy wszystkich instalacji w obiekcie i szybkiego reagowania na ewentualne nieprawidłowości. Osoby odpowiedzialne za obsługę techniczną budynku mają informacje na temat zużycia energii, zdarzeń alarmowych i awarii określonych urządzeń. Możliwe jest centralne raportowanie i sterowanie wszystkimi systemami funkcjonującymi w danym obiekcie. Ma to istotny wpływ na komfort obsługi systemów oraz szybkość podejmowanych działań w sytuacjach wymagających interwencji.

Zaawansowane technologicznie systemy gaszenia

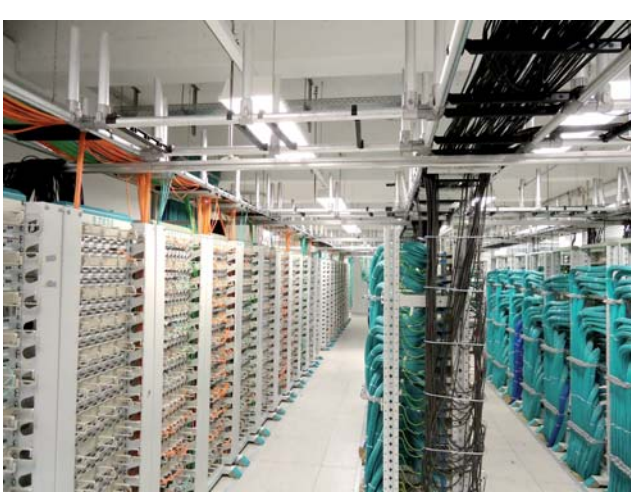
Bezpieczeństwo osób przebywających w obiekcie jest priorytetem. Zarządcy i właściciele budynków poszukują zatem skutecznych technologii, efektywnych rozwiązań, zwracając uwagę na ich cenę. Ze względu na

Fot. 1. Gaszenie mgłą wodną

korzyści z zastosowania wielu zwolenników zyskują systemy gaszenia mgłą wodną. Znajdują one zastosowanie m.in. w budynkach biurowych, przemysłowych, w centrach przetwarzania danych, muzeach, archiwach, hotelach. Dzięki zautomatyzowanemu mechanizmowi wyzwalania środka gaśniczego reakcja na pożar jest natychmiastowa i ogranicza straty wynikające z rozprzestrzeniania się ognia. Komponenty są małe, dlatego można zainstalować taki system w miejscu o ograniczonej powierzchni sufitowej. Mgła wodna działa skutecznie. Wypiera tlen z ogniska pożaru. Większość produktów spalania zostaje zaabsorbowana przez mikroskopijne krople wody. W następstwie pożar wraz z zarzewiem ognia zostaje zagaszony.

Skuteczne gaszenie dzięki wysokiemu współczynnikowi ciśnienia

Bardzo skuteczne systemy gaszenia mgłą wodną AQUASYS, których wyłącznym dystrybutorem w Polsce jest firma AGIS Fire & Security, wykorzystują wysokie ciśnienie, które skierowuje wodę poprzez rury ze stali nierdzewnej do specjalnie zaprojektowanych dysz produkujących mgłę. Uzyskane z dysz niezwykle małe krople wody odparowują w ogniu, zwiększając tym samym swoją objętość. Mgła wodna nie przewodzi prądu, a zatem z powodzeniem może być stosowana do ochrony urządzeń pod napięciem czy w centrach przetwarzania danych. Dzięki zastosowaniu wysokiego ciśnienia



Fot. 2. Serwerownia chroniona mgłą wodną

Fot. 3. Mgła wodna

wody proces tłumienia ognia może przebiegać skutecznie nawet przy włączonych urządzeniach wentylacyjnych (np. chłodzących sprzęt IT).

Wielofunkcyjne działanie mgły

Rezultatem zwiększenia objętości kropel wody jest pochłanianie energii z ognia w procesie parowania, dzięki czemu następuje chłodzenie, wypieranie tlenu z ogniska pożaru, a tym samym hamowanie procesu spalania. Ponadto wielowarstwowa osłona z drobnych kropel wody stanowi ochronę przed promieniowaniem cieplnym i ogranicza rozprzestrzenianie się ognia. Osłona ta jest tworzona z kropel wody o niezwykle małej masie oraz trójwymiarowej dyspersji mgły wodnej i jest wspierana przez ciepło wytwarzane przez ogień.

Korzyści z zastosowania mgły wodnej

Mgła wodna H2O3 jest niezwykle efektywna w walce z ogniem, a także nieszkodliwa dla ludzi i środowiska, a system AQUASYS może być aktywowany natychmiast w przypadku zagrożenia pożarem. Mgłą wodną można gasić nawet szczególnie trudne do ugaszenia pożary, np. płonące zbiorniki z olejem.

Firma AGIS Fire & Security oferuje swoim klientom kompleksowy pakiet usług – zaprojektowanie, zainstalowanie, uruchomienie, serwis i konserwację systemu. Oferta rozwiązań wdrażanych przez AGIS obejmuje m.in. instalacje teletechniczne, instalacje teleinformatyczne (LAN, IT), wodne i gazowe instalacje gaśnicze, instalacje automatyki budynkowej i BMS, instalacje elektryczne (zewnętrzne i wewnętrzne, średniego napięcia, rozdział energii, oświetlenie). Dzięki specjalistycznej wiedzy i doświadczeniu spółka realizuje duże i niełatwe projekty, także takie o kategorii podwyższonego ryzyka dla klientów z branży przemysłowej.

AGIS Fire & Security nie poprzestaje na gotowych rozwiązaniach – oferowane systemy są tworzone wspólnie z klientami, aby całkowicie spełniać ich oczekiwania. Naszymi klientami są firmy z różnych branż – m.in. budowniczej, przemysłowej, handlowej, logistycznej, telekomunikacyjnej, IT. Więcej informacji znajduje się na stronie *www.agisfs.pl.*

Karolina Olechowicz
AGIS Fire & Security

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

SYSTEM SYGNALIZACJI POŻAROWEJ
POLON 6000

NOWOŚĆ

Do ochrony **dużych i rozległych** obiektów
Centrala o **architekturze rozproszonej**

Nowy szereg elementów **liniowych 6000**
Współpraca z elementami **szeregu 4000**

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.
85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

System sygnalizacji włamania i napadu zaprojektowany z wykorzystaniem mikrokontrolerów
(Część 2)

Maciej Wieczorek
Adam Rosiński

W części drugiej artykułu przedstawiono zastosowanie mikrokontrolera ATmega 328 i układu bazowego ARDUINO UNO w celu zaprojektowania i wykonania stanowiska dydaktyczno-badawczego systemu sygnalizacji włamania i napadu (SSWiN). Opracowane stanowisko będzie wykorzystywane przez studentów zdobywających wiedzę z zakresu inżynierii systemów bezpieczeństwa (mających oczywiście podstawową wiedzę z zakresu elektroniki [1,2]). Umożliwi zapoznanie się z urządzeniami alarmowymi w praktyce i z zasadami ich współpracy z centralą alarmową

1. Zastosowane urządzenia peryferyjne

Platforma Arduino jest wyposażona w wiele modułów peryferyjnych umożliwiających projektowanie i konstruowanie urządzeń zgodnych z wymaganiami użytkownika. Dla potrzeb stanowiska dydaktyczno-badawczego SSWiN wybrano następujące moduły [3]:

– moduł wyświetlacza LCD 16x2 (fot. 1; umożliwia wyświetlanie danych w formacie alfanumerycznym),
– cyfrowy czujnik temperatury i wilgotności (fot. 2; dokonuje pomiaru temperatury i wilgotności otoczenia),
– pasywna czujka podczerwieni PIR ME003 (fot. 3),
– serwomechanizm SG90 (fot. 4),
– moduł zegara czasu rzeczywistego,
– czytnik kart RFID wraz z kartami (fot. 5).

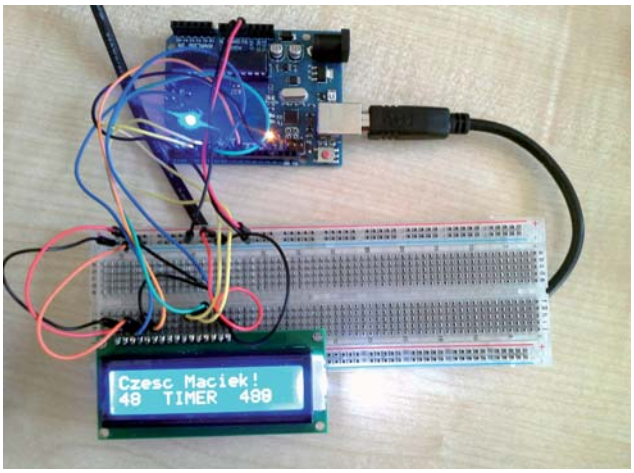
2. Oprogramowanie Arduino IDE

Do prawidłowej pracy mikrokontrolera wymagane jest oprogramowanie, które steruje jego działaniem. Głównym językiem, w jakim pisze się programy dla mikrokontrolerów, jest Asembler. Układ w swojej wewnętrznej pamięci ROM ma zakodowaną listę rozkazów, które wywoływane są poprzez kolejne komendy napisane w języku Asembler. Znajomość Asemblera jako języka niskiego poziomu nie jest zbyt rozpowszechniona w środowiskach programistycznych. Obecnie edukacja informatyczna ukierunkowana jest na naukę języków wysokiego poziomu, takich jak JAVA, C, C++, C#. Większość studentów lepiej radzi sobie w środowisku JAVA niż z Asemblerem.

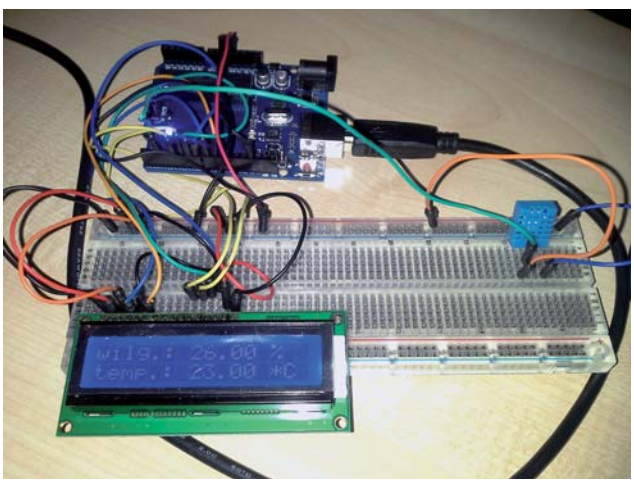
Twórcy platformy Arduino, dążąc do maksymalnej elastyczności systemu, stworzyli własne środowisko programistyczne z własnym językiem programowania oraz dużą liczbą bibliotek zawierających dane umożliwiające dopasowanie różnych urządzeń peryferyjnych do mikrokontrolera. Biblioteki te mogą być w prosty sposób edytowane przez użytkownika, co rozszerza możliwości – umożliwia podłączanie kolejnych, nowych urządzeń.

Do pisania oprogramowania stworzony został język WIRING. Język ten jest oparty na strukturach języków C i C++. Podobnie jak to miało miejsce w języku C program składa się ze zmiennych, funkcji oraz struktur. Konstrukcja programu dla mikrokontrolera ATmega jest przejrzysta i prosta.

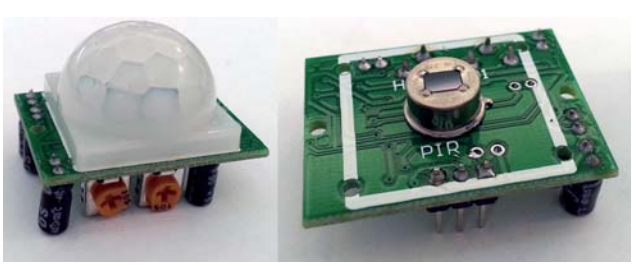
Oprogramowanie Arduino IDE zostało stworzone przez twórców platformy Arduino w celu łatwego pisania programów w języku



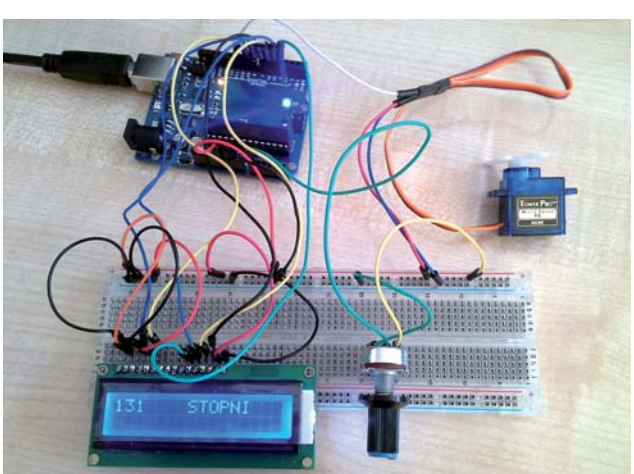
Fot. 1. Moduł wyświetlacza wraz z ARDUINO UNO



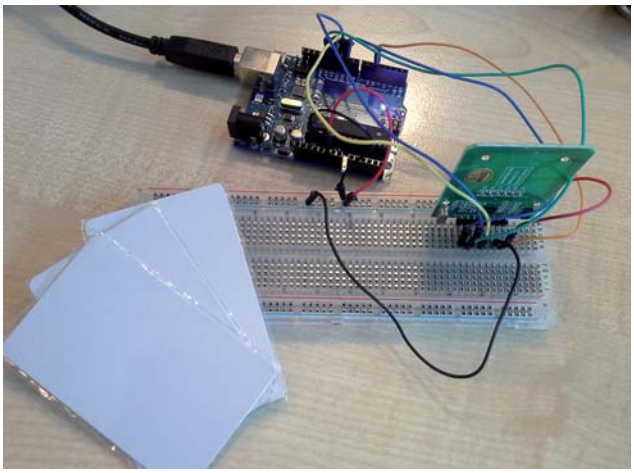
Fot. 2. Czujnik DHT11 wraz z ARDUINO UNO



Fot. 3. Czujka PIR ME003 i zastosowany w niej element piroelektryczny



Fot. 4. Widok serwomechanizmu SG90 wraz z ARDUINO UNO i innymi modułami



Fot. 5. Czytnik kart MIFARE MF522 oraz widok czytnika kart wraz z ARDUINO UNO

WIRING oraz wgrywania stworzonego kodu wynikowego do mikrokontrolera. Arduino IDE ma w swojej strukturze kompilator z edytorem, co oznacza, że przed wgraniem do układu program jest sprawdzany pod względem poprawności. Ewentualne błędy są wyświetlane w oknie edycyjnym Arduino IDE.

3. Ćwiczenia dydaktyczno-badawcze z zakresu SSWiN

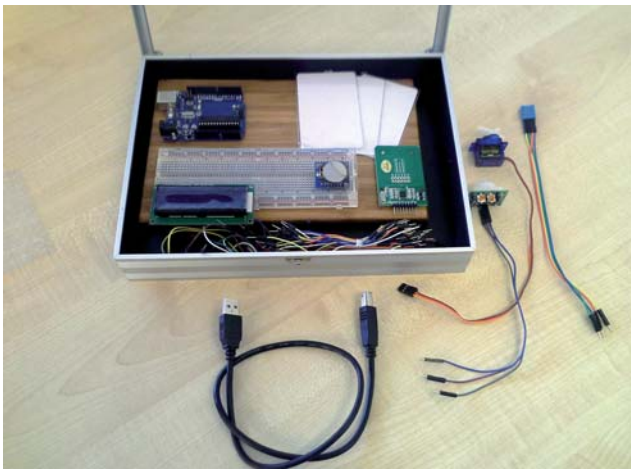
Ćwiczenia praktyczne z wykorzystaniem platformy Arduino są bardzo dobrym edukacyjnym rozwiązaniem dla studentów kierunków technicznych (związanych nie tylko z inżynierią systemów bezpieczeństwa). W ramach tych ćwiczeń student wykorzystuje walizkę (fot. 6), w której znajdują się modułowe elementy systemu, do których należą:

- moduł ARDUINO UNO,
- pośrednia płytka połączeniowa,
- komplet kabli połączeniowych,
- moduły peryferyjne: wyświetlacz LCD 16x2, czujka PIR ME003, czytnik kart RFID z trzema kartami chipowymi, moduł zegara czasu rzeczywistego TinyRTC, sensor temperatury i wilgotności DHT11, serwomechanizm SG90, kabel USB do podłączenia modułu ARDUINO UNO do komputera PC,
- elementy dyskretne: potencjometr, rezystory, diody LED,
- płyta CD zawierająca instrukcje do ćwiczeń, programy i schematy.

Integralną częścią platformy są instrukcje prowadzące krok po kroku przez ćwiczenia – od najprostszych do skomplikowanych. Instrukcje zostały napisane tak, że można uruchomić układy bez dostępu do Internetu. Na końcu każdego ćwiczenia znajduje się lista zagadnień i zadań do samodzielnego wykonania (np. połączenie ćwiczenia dotyczącego wyświetlacza z ćwiczeniem opisującym czytnik RFID lub dodanie diod LED, czerwonej i zielonej, wskazujących stan dostępu w tym czytniku).

4. Podsumowanie

W artykule zaprezentowano stanowisko wykorzystywane w celach dydaktyczno-badawczych, służące do ćwiczeń



Fot. 6. Zestaw dydaktyczno-badawczy z widocznymi modułami i akcesoriami

z zakresu SSWiN. Do jego zaprojektowania i wykonania wykorzystano moduł bazowy ARDUINO UNO z mikrokontrolerem ATmega 328 oraz urządzenia peryferyjne, m.in.: wyświetlacz LCD, czujkę PIR, czytnik kart RFID, sensor temperatury i wilgotności, serwomechanizm. Umożliwia to studentom studiującym inżynierię systemów bezpieczeństwa praktyczne zapoznanie się z funkcjonowaniem poszczególnych urządzeń wchodzących w skład SSWiN. Jednocześnie można też dokładnie poznać zasady współpracy urządzeń zewnętrznych z płytą główną centrali alarmowej z uwzględnieniem różnego rodzaju formatów transmisji danych.

Możliwa jest dalsza rozbudowa opisanego stanowiska – dodanie do niego kolejnych urządzeń zewnętrznych (np. czujek ultradźwiękowych, czujek magnetycznych, czujek magistralowych). Stanowisko to jest tak skonstruowane, że umożliwia dowolną rozbudowę użytkownikom zainteresowanym programowaniem i konstruowaniem urządzeń wykorzystujących mikrokontrolery AVR firmy ATMEL.

Bibliografia

1. W. Szulc, A. Rosiński *Wybrane zagadnienia z elektroniki cyfrowej dla informatyków* (*część II – cyfrowa*), Warszawa 2012.
2. W. Szulc, A. Rosiński *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków* (*część I – analogowa*), Warszawa 2012.
3. M. Wieczorek, *Projekt stanowiska dydaktyczno-badawczego z wykorzystaniem Arduino – platformy edukacyjnej opartej na mikrokontrolerach firmy Atmel*, dyplomowa praca inżynierska, Wyższa Szkoła Menedżerska w Warszawie, Wydział Menedżerski i Nauk Technicznych, Warszawa 2014.

inż. Maciej Wieczorek
dr inż. Adam Rosiński
Politechnika Warszawska
Wydział Transportu
Zakład Telekomunikacji w Transporcie

Wpływ nowych trendów i technologii na rozwój rynku wizyjnych systemów dozorowych w roku 2015 i w latach późniejszych

Johan Paulsson

Podobnie jak w latach poprzednich, w roku 2014 Internet Rzeczy (IoT – *Internet of Things*) nadal wywoływał wiele dyskusji przedstawicieli wielu dziedzin przemysłu. Rozmawiano zarówno o urządzeniach o złożonej konstrukcji, takich jak inteligentne samochody, jak i prostych urządzeniach stosowanych w gospodarstwie domowym, takich jak lodówki podłączane do Internetu. W wyniku tych dyskusji wielu konsumentów, a także biznesmenów zyskało nową wiedzę na temat korzyści wynikających z coraz szerszego wykorzystania Internetu w życiu codziennym. Dotyczyło to także przedstawicieli branży zabezpieczeń elektronicznych oraz właścicieli obiektów użytkowych dążących do podniesienia poziomu bezpieczeństwa w swoich przedsiębiorstwach

Według profesjonalistów działających w branży zabezpieczeń elektronicznych naturalnym kierunkiem dalszego udoskonalania wizyjnych systemów dozorowych będzie upowszechnienie standardu 4K zapewniającego czterokrotnie wyższą niż w popularnym obecnie standardzie HD rozdzielczość obrazu. Umożliwi to znaczne rozszerzenie pola widzenia kamer z zachowaniem tego samego poziomu rozróżnialności szczegółów obrazu. Przewiduje się, że tendencja ta da się zauważyć w wizyjnych systemach dozorowych już w roku 2015 i pogłębi się w latach późniejszych.

Podczas dyskusji na temat przydatności standardu 4K do celów dozorowych mówi się zazwyczaj o wysokiej rozdzielczości obrazu, a zapomina o warunkach, w jakich ten obraz powstaje. Prawdziwym wyzwaniem dla konstruktorów sprzętu jest optymalizacja jakości obrazu w każdych, nawet najgorszych warunkach oświetleniowych i środowiskowych. Motorem dalszego postępu będzie dążenie do stworzenia innowacyjnych rozwiązań umożliwiających skuteczniejsze wykorzystanie wizyjnych systemów dozorowych w najtrudniejszych warunkach eksploatacyjnych.

Wizyjne usługi sieciowe i przetwarzanie danych w chmurze

Poprawa jakości obrazu powoduje wzrost wymagań dotyczących sposobów zarządzania zgromadzonym materiałem wizyjnym. Nie chodzi tu tylko o zwiększenie obciążenia sieci oraz pamięci masowej, czemu można zaradzić, stosując skuteczniejsze metody kompresji obrazu. Problem polega na konieczności zwiększenia skuteczności działania aplikacji służących do analizy treści obrazu i zarządzania informacjami uzyskanymi z wizyjnych systemów dozorowych. Z tego względu przewiduje się wzrost popularności wizyjnych usług sieciowych (*VSaaS – Video Surveillance as a Service*) realizowanych w chmurze internetowej. Dzięki temu z tych samych strumieni wizyjnych będą mogły korzystać różne podmioty, zaś wizyjne systemy dozorowe staną się użytecznym narzędziem do wykrywania przestępstw kryminalnych i zapobiegania przestępczości na terenie rozległych obiektów publicznych, takich jak centra handlowe, parki, dworce kolejowe, lotniska.

Szybki wzrost wartości rynku wizyjnych systemów dozorowych wynika z obawy o poziom bezpieczeństwa publicznego na całym świecie. Zgodnie z wynikami badań przeprowadzonych przez organizację Transparency Market Research w roku 2019 rynek wizyjnych systemów dozorowych oraz usług VSaaS osiągnie wartość 43 miliardów dolarów, co oznacza, że w latach 2013–2019 będziemy mieli do czynienia z rocznym wzrostem na poziomie 19%. Przewiduje się również szybki rozwój rynku sieciowych wizyjnych systemów dozorowych, którego szacowany roczny wzrost wartości w latach 2013–2019 to 24%. Ponadto przewiduje się, że rynek urządzeń wizyjnych, którego wartość w roku 2012 wyniosła 9,5 miliarda dolarów, w latach 2013–2019 wykaże roczny wzrost na poziomie 17%. Chodzi tu o wszystkie rodzaje urządzeń, w tym kamery analogowe i sieciowe, rejestratory, pamięci masowe, kodery i monitory. W tym momencie warto podkreślić, że ze względu na wzrost popularności usług VSaaS realizowanych w chmurze internetowej udział rejestratorów i pamięci masowych w rynku urządzeń wizyjnych, który w roku 2012 wynosił 37%, będzie wykazywał tendencję spadkową. Tymczasem udział kamer w rynku urządzeń wizyjnych, który w roku 2012 wynosił 32%, wykazuje tendencję wzrostową i przewiduje się, że w roku 2019 będzie wynosić około 46%. Ma to związek ze wzrostem popularności kamer sieciowych, oferujących obraz o coraz wyższej jakości i stwarzających możliwość zapisu materiału wizyjnego na wewnętrznych kartach pamięci.

W ostatnich latach w kręgach osób zajmujących się sieciowymi systemami dozorowymi zapis i obróbka materiału wizyjnego w chmurze internetowej stanowiły swoistą modę, jednakże prawdziwe zmiany w tej dziedzinie mamy dopiero przed sobą. Zarówno w systemach otwartych, w których dzierżawienie serwerów i ich wykorzystywanie wspólnie z innymi użytkownikami stało się powszechnie akceptowaną praktyką, jak i w systemach prywatnych, w których dane i aplikacje nie są z nikim współdzielone, gromadzenie i obróbka materiału wizyjnego w chmurze przynosi wymierne korzyści. Są to: nadmiarowość, skalowalność i przeniesienie kosztów z wydatków inwestycyjnych na wydatki operacyjne. Niezależnie od tego, czy chmura jest hostowana w Internecie czy utworzona wewnątrz jakiejś wydzielonej sieci, zyskujemy wygodę w związku z przekazaniem obowiązku wykonywania wszystkich czynności konserwacyjnych, takich jak modernizacje, aktualizacje i poprawki, osobom trzecim. Skalowalność ma znaczenie nie

Johan Paulsson z Axis Communications

tylko w przypadku próby zwiększenia liczby kamer pracujących w danym systemie. Dzięki niej można wpływać na intensywność wykorzystania serwerów i innych zasobów sieciowych, na przykład w sytuacji, w której zachodzi konieczność zwiększenia rozdzielczości obrazów i prędkości ich transmisji przy zachowaniu niezmienionej liczby kamer. Przykładowo, jeśli dla poprawy wiarygodności oceny ruchu klientów na terenie obiektu handlowego konieczne jest uruchomienie skuteczniejszych niż dotychczas aplikacji analizujących treść zgromadzonego materiału wizyjnego, jedynym elementem, za który trzeba dodatkowo zapłacić, jest dodatkowa moc obliczeniowa. Takie aplikacje lepiej funkcjonują w strukturze rozproszonej i znajdują zastosowanie w systemach o znaczeniu krytycznym. Dodatkowa moc obliczeniowa może być wykorzystana na przykład do analizy treści obrazów pięciuset tysięcy tablic rejestracyjnych samochodów przejeżdżających codziennie z prędkością 40 kilometrów na godzinę przez punkt kontrolny na ruchliwej autostradzie. Innym interesującym aspektem VSaaS jest możliwość stworzenia kompleksowych usług, na przykład natychmiastowego zaangażowania dodatkowych służb wartowniczych lub zewnętrznych firm zajmujących się ochroną obiektów, jeśli zajdzie taka potrzeba.

Analiza danych i wnioski natury biznesowej

W roku 2015 i w latach późniejszych aplikacje analizujące treść obrazów z kamer będą podlegać dużym zmianom. To samo dotyczy całego przemysłu związanego z wizyjnymi systemami dozorowymi. Kamery pracujące w wizyjnych systemach dozorowych wytwarzają nieprzerwany strumień danych, niezbędny do pracy służb bezpieczeństwa, jednak na tym nie kończy się ich rola. Dzięki analizie ogromnych ilości uporządkowanych i nieuporządkowanych danych, zgromadzonych w postaci zarejestrowanego materiału wizyjnego, możliwe jest wyciągnięcie daleko idących wniosków natury biznesowej. Inteligentne aplikacje umożliwiają uporządkowanie i interpretację tych danych oraz przekształcenie ich w materiał nadający się do dalszego wykorzystania. W takim kontekście pojawia się określenie 3V – od angielskich słów *volume* (mnogość), *variety* (różnorodność), *velocity* (zmienność). Umiejętna obróbka ogromnej ilości różnorodnych, szybko zmieniających się danych prowadzi do pozyskiwania cennych informacji, które mogą być przydatne w warunkach kryzysowych i mogą pojawiać się we właściwym, najbardziej oczekiwanym momencie. Dane faktograficzne pochodzące z systemów sygnalizacji włamania i napadu, systemów kontroli dostępu i innych systemów sieciowych mogą być ze sobą powiązane, dzięki czemu można uzyskać na przykład użyteczne informacje przyczyniające się do zmniejszenia kosztów eksploatacji jakiegoś obiektu. Na tym właśnie polegają zmiany wynikające z rewolucji teleinformatycznej, z jaką mamy obecnie do czynienia. Kamery, które służyły zazwyczaj do wykrywania i identyfikacji przestępców i były narzędziem ułatwiającym rozwiązywanie problemów związanych z bezprawnymi incydentami, weszły w skład skomplikowanych, interaktywnych systemów zarządzania obiektami. Na przykład obrazy z kamer zainstalowanych w centrach handlowych mogą być poddane analizie z udziałem komputerów o dużej mocy obliczeniowej, w wyniku czego uzyskane zostaną informacje usprawniające proces sprzedaży. Informacje te mogą dotyczyć tras, którymi klienci przemieszczają się najczęściej, problemów klientów z dostępem do najliczniej odwiedzanych stoisk, a także wąskich gardeł przyczyniających się do powstawania kolejek. Sprzedawcy będą mogli uzyskać przewagę nad konkurentami dzięki wykorzystaniu tych danych i powiązaniu ich z informacjami uzyskiwanymi z innych źródeł, jakimi mogą być harmonogramy dostaw towarów, listy promocyjne, cenniki z innych placówek handlowych, portale społecznościowe. Wykwalifikowani specjaliści od przetwarzania danych mogą dostrzec powiązania i zależności, z których nikt przedtem nie zdawał sobie sprawy.

Kompresja obrazu i efektywne wykorzystanie pasma sieciowego

Kompresja obrazu telewizyjnego ma na celu zmniejszenie ilości nadmiarowych danych, transmitowanych wraz ze strumieniem wizyjnym i niepotrzebnie zapisywanych na dyskach komputerowych. Efektywne techniki kompresji umożliwiają znaczne zmniejszenie objętości zapisywanych plików bez zauważalnego pogorszenia jakości obrazów. Znanych jest kilka standardowych metod kompresji, w tym M-JPEG, MPEG-4 i H.264. Ostatnia z nich ma największą skuteczność i jest powszechnie stosowana zarówno w wizyjnych systemach dozorowych, jak i w telewizji profesjonalnej. Wzrost rozdzielczości obrazów wytwarzanych przez współczesne kamery powoduje wzrost wymagań dotyczących skuteczności kompresji. Zmusza to do usprawnienia algorytmów kompresji obrazów w celu utrzymania kosztów związanych z transmisją i zapisem strumieni wizyjnych na możliwie niskim poziomie. Równie istotne są prace zmierzające do zmniejszenia poziomu szumów w obrazie i uzyskania skutecznej kompresji podczas transmisji i rejestracji obrazów o niskiej poklatkowości.

W wyniku kolejnych usprawnień standardu H.264 opracowana została nowa jego odmiana, a mianowicie H.265, z którą wiązane są duże nadzieje na przyszłość. We właściwych warunkach umożliwia ona dalszą redukcję objętości strumieni wizyjnych o około 50%. Początkowo kompresja H.265 ma być wykorzystywana głównie w telewizji profesjonalnej i w przemyśle rozrywkowym. Prawdopodobnie w najbliższym czasie taki rodzaj kompresji będzie wykorzystywany jedynie w najlepszych kamerach profesjonalnych, o bardzo wysokiej rozdzielczości, jednak metoda ta wkrótce na dobre zadomowi się także w wizyjnych systemach dozorowych, zaś oba omawiane standardy kompresji, czyli H.264 i H.265, będą koegzystować na rynku telewizyjnym.

Konkluzja

Upowszechnienie standardów telewizji o wysokiej rozdzielczości, takich jak 4K, musi iść w parze z doskonaleniem innych technologii, umożliwiających szersze wykorzystanie obrazów z kamer, nie tylko w celu poprawy stanu bezpieczeństwa chronionych obiektów, lecz także w celu uzyskania korzyści biznesowych, zwiększenia rentowności przedsiębiorstw i uzyskania przewagi nad konkurencją. Te aspekty powinny być brane pod uwagę przez wszystkie osoby poszukujące nowych rozwiązań technologicznych w branży wizyjnych systemów dozorowych.

Axis Communications

Opracowanie: Redakcja

Tekst został opracowany na podstawie wypowiedzi Johana Paulssona z Axis Communications

Ucz się.
Zwyciężaj.

Sukces w biznesie jest nierozerwalnie związany z wiedzą. Axis Communications' Academy daje Ci możliwość dostarczania lepszych i mądrzejszych rozwiązań w zakresie systemów bezpieczeństwa.

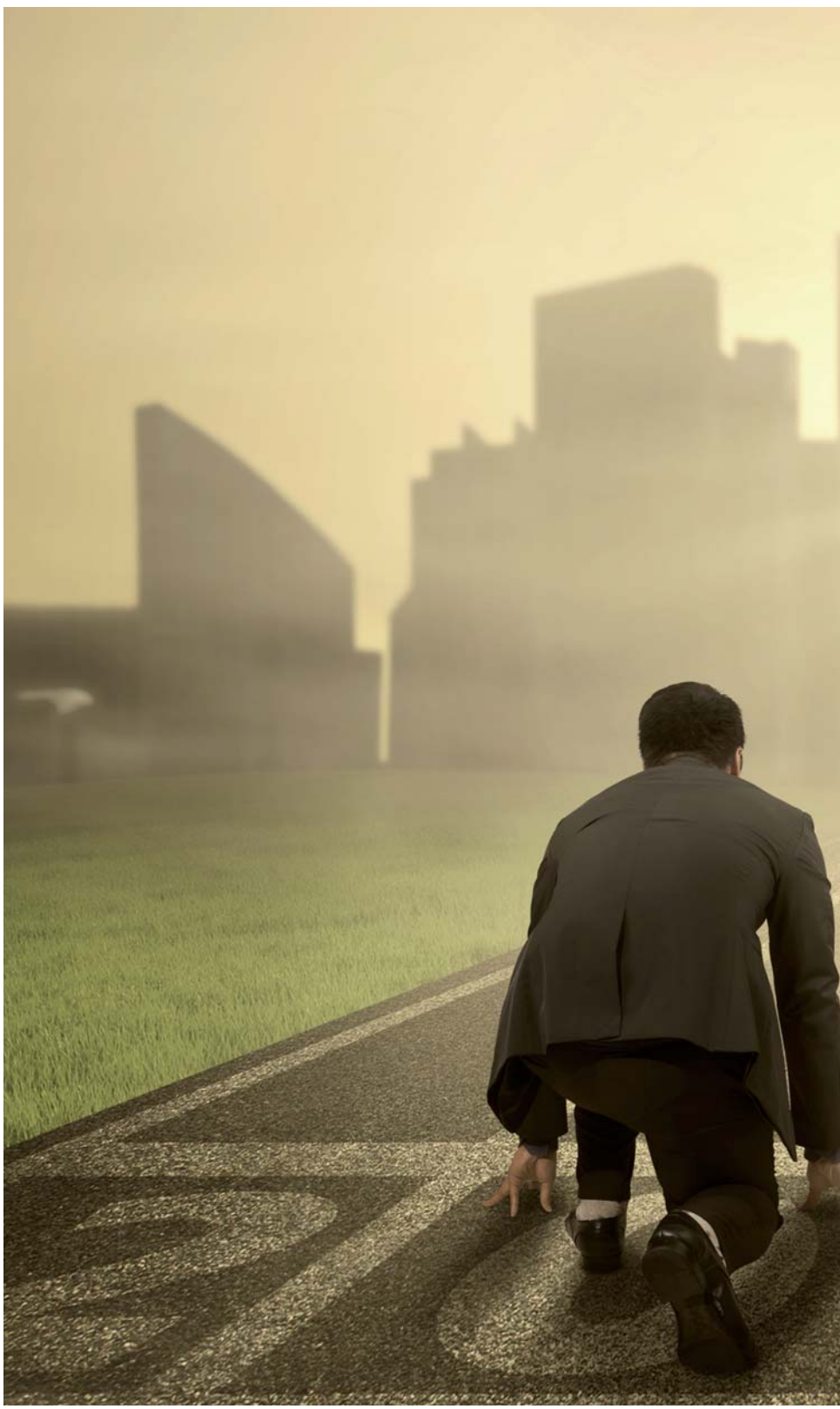
Axis Communications' Academy – Budowanie wiedzy.
Odwiedź: www.axis.com/academy

AXIS COMMUNICATIONS

Dokąd zmierza CCTV?

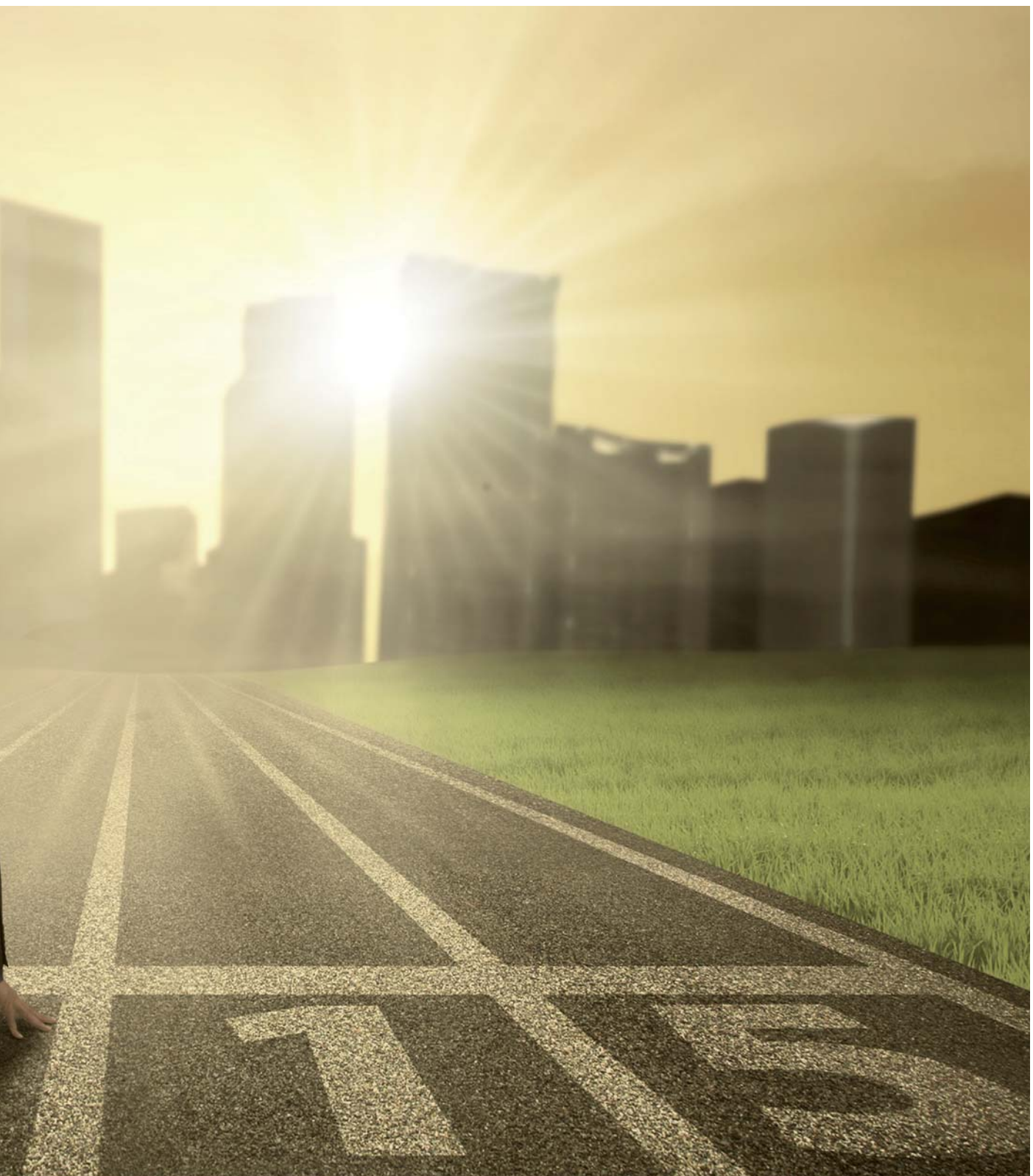
Andrzej Walczyk

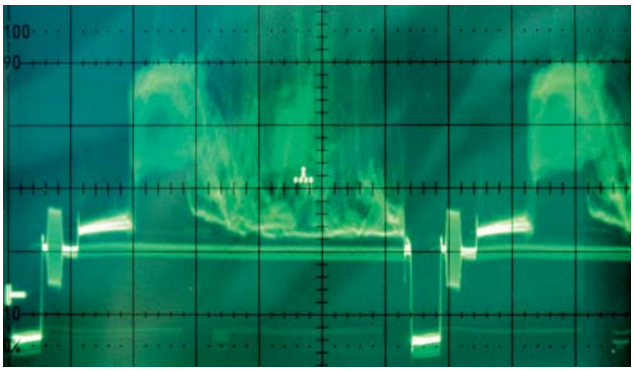
Postęp technologiczny w dziedzinie wizyjnych systemów dozorowych jest na tyle szybki, że jesteśmy nieustannie zalewani potokiem informacji dotyczących nowych urządzeń i coraz doskonalszych rozwiązań systemowych. Podaż rynkowa jest bardzo duża, zaś specjaliści od marketingu prześcigają się w działaniach mających na celu wypromowanie konkretnych produktów



Historycznie rzecz biorąc, jeszcze w latach 60. XX wieku w sprzedaży pojawiły się kamery przemysłowe, a wraz z nimi powstały pierwsze systemy CCTV. W Polsce były to urządzenia monochromatyczne, zgodne ze standardem CCIR-B, produkowane przez Warszawskie Zakłady Telewizyjne. Sprzęt importowany nie był dostępny ze względu na barierę cenową, zaś ograniczona produkcja krajowa powodowała, że popularność wizyjnych systemów dozorowych była niewielka. Sytuacja uległa zmianie pod koniec lat 80., kiedy to w wyniku rozwoju technologicznego lampa widikonowa została zastąpiona półprzewodnikowym elementem światłoczułym o nazwie CCD. Dzięki temu zdecydowanie ograniczono wielkość i ciężar kamer telewizyjnych oraz znacznie poprawiono ich parametry. W tym okresie na polskim rynku pojawiły się liczne modele kamer monochromatycznych oraz pierwsze kamery kolorowe zgodne ze standardem PAL. Nastała era analogowych wizyjnych systemów dozorowych, określanych jako systemy CCTV.

W standardzie PAL kształt sygnału wizyjnego jest ściśle określony, jego widmo rozciąga się od prądu stałego do częstotliwości równej około 5 MHz.





Fot. 1. Zespolony sygnał wizyjny w standardzie PAL

W rozpowszechnionej w Polsce wersji standardu PAL raster telewizyjny składa się z 625 poziomych linii, zaś kolejne obrazy są wyświetlane z częstotliwością 25 Hz. Tak niska częstotliwość odświeżania jest przyczyną przykrego dla widza migotania obrazu, które zostało wyeliminowane przez wprowadzenie tak zwanego wyświetlania z przeplotem. Każdy z obrazów został podzielony na dwa półobrazy, które są wyświetlane jeden po drugim, z częstotliwością 50 Hz. Ten sposób poprawy jakości obrazu stanowił duże udogodnienie w początkowym okresie rozwoju systemów CCTV, jednakże w okresie późniejszym przyczynił się do wielu problemów związanych z zapisem i obserwacją obrazów obiektów ruchomych.

Urządzenia zgodne ze standardem PAL umożliwiały wytwarzanie i rejestrację obrazów o stosunkowo wysokiej jakości. Taki stan techniki utrzymywał się przez kilkanaście lat, zaś jakiekolwiek próby zmian były z góry skazane na niepowodzenie, gdyż ograniczenie tkwiło w samym standardzie. Nie można było zwiększyć liczby linii tworzących raster telewizyjny, zaś szerokość pasma toru wizyjnego była ograniczona do około 5 MHz, co z kolei powodowało ograniczenie maksymalnej rozdzielczości obrazu.

W pierwszych, analogowych systemach CCTV sygnały wizyjne z kamer były transmitowane za pośrednictwem kabli koncentrycznych. Na tym etapie rozwoju technologicznego stanowiło to normę i przyczyniło się do ugruntowania pewnych przyzwyczajeń projektantów i instalatorów.

Uwolnienie od ograniczeń standardu PAL nastąpiło dopiero w momencie upowszechnienia się cyfrowej telewizji IP. Początkowo w tej dziedzinie nie było sprecyzowanych standardów. Wymagania narzucali producenci sprzętu. Odejście od standardu PAL umożliwiło zwiększenie rozdzielczości obrazu oraz szybkości jego odświeżania. Miało to związek z całkowicie odmienną techniką transmisji i rejestracji sygnału wizyjnego. W zasadzie w cyfrowej telewizji IP trudno mówić o sygnale wizyjnym, gdyż zastąpił go strumień danych cyfrowych.

Pojawienie się telewizji IP stworzyło nową sytuację na rynku. W cyfrowych systemach wizyjnych można było uzyskać obrazy o wysokiej rozdzielczości, ale projektanci i instalatorzy musieli uzupełnić wiedzę i poznać niezrozumiałą dla nich technikę cyfrową. Kabel koncentryczny, który był masowo stosowany w analogowych systemach CCTV, został zastąpiony kablem sieciowym, co także stanowiło pewną barierę, gdyż modernizacja starych systemów wiązała się z koniecznością wymiany całego okablowania.

W tym momencie dochodzimy do sedna sprawy. Cyfrowe systemy wizyjne kusiły doskonałą jakością obrazu i możliwością realizacji zupełnie nowych funkcji użytkowych, ale odstraszały wysoką ceną urządzeń i koniecznością zdobywania nowej wiedzy. Tę sytuację wykorzystali producenci sprzętu analogowego i co sprytniejsi specjaliści od marketingu. W reklamach zaczęła pojawiać się przewrotna maksyma: „Nie musisz nic wiedzieć o IP, my damy Ci analogową telewizję HD". Zastanówmy się, jakie skutki rynkowe przyniosła taka polityka.

W latach 2008–2009 w branży wizyjnych systemów dozorowych najszybciej rozwijała się technologia IP, jednak już wtedy pojawiały się pierwsze analogowe systemy wizyjne o wysokiej rozdzielczości. Towarzyszył temu agresywny marketing rokujący rychły upadek telewizji IP. Koronnymi argumentami były niska cena kamer i możliwość modernizacji istniejących systemów analogowych bez konieczności wymiany okablowania.

Na pierwszy ogień poszedł interfejs SDI i systemy HD-SDI. Interfejs SDI jest zgodny ze standardem SMPTE (*The Society of Motion Picture and Television Engineers*), który został opracowany jeszcze w 1989 roku. Trudno tu mówić o innowacyjności, gdyż w chwili pojawienia się pierwszych systemów HD-SDI interfejs SDI był od kilkudziesięciu lat wykorzystywany w telewizyjnym sprzęcie studyjnym. Obecnie pomału wychodzi z użycia na rzecz połączeń sieciowych o przepustowości 1 Gb/s.

W profesjonalnych systemach studyjnych transmisja sygnału wizyjnego poprzez interfejs SDI odbywa się z użyciem specjalnych, kosztownych kabli koncentrycznych. Mimo iż transmitowany jest sygnał analogowy, jest to transmisja cyfrowa z przepływnością równą około 1,5 Gb/s. Uzyskiwane dystanse nie przekraczają 300 m.

Standard SMPTE ma wiele odmian, w tym wersję SMPTE 292M przystosowaną do cyfrowej transmisji obrazu o rozdzielczości 720p i 1080p z przepływnością 1485 Mb/s. Właśnie ta wersja została wykorzystana w systemach HD-SDI. Widmo sygnału transmitowanego przez kabel koncentryczny sięga kilkuset megaherców, co w praktyce oznacza, że należy stosować specjalne kable o niskiej tłumienności w paśmie dochodzącym do gigaherca.

Transmisja sygnału wizyjnego przez interfejs SDI z użyciem tanich kabli koncentrycznych (np. RG59) stosowanych

HD 720p – 1280×720 | 960H – 960×540 | D1 PAL – 720×576

Fot. 2. Porównanie wielkości obrazów w trzech omawianych standardach

w tradycyjnych instalacjach analogowych jest możliwa na odległość nie przekraczającą kilkunastu metrów. Jeszcze gorzej jest w przypadku korzystania z wyeksploatowanych kabli koncentrycznych, które utraciły swoje właściwości na skutek starzenia się materiałów dielektrycznych oraz utleniania się powierzchni przewodów miedzianych, z których są zbudowane. Zasięgi uzyskiwane w takich przypadkach są jeszcze mniejsze, o czym nie wspominają żadne materiały reklamowe. W ten sposób znika koronna zaleta systemów HD-SDI, jaką jest możliwość modernizacji wizyjnych systemów dozorowych z wykorzystaniem istniejących kabli koncentrycznych.

Jak już wyjaśniono, w systemach HD-SDI transmitowany jest niekompresowany i niekodowany analogowy sygnał wizyjny, co skutkuje brakiem opóźnień podczas wyświetlania obrazu, jednak jest okupione przepływnością na poziomie 1,5 Gb/s. Zapis tak gigantycznego strumienia danych jest bardzo kosztowny, a monstrualna objętość materiałów archiwalnych uniemożliwia ich długotrwałe przechowywanie. Z tych przyczyn dane są kompresowane przed zapisem. Kompresja strumieni danych o przepływności 1,5 Gb/s zmusza do stosowania bardzo szybkich procesorów DSP, dlatego rejestratory stosowane w systemach HD-SDI są bardzo drogie i przeważnie mają niewiele wejść wizyjnych.

W ten sposób znika kolejna, szeroko reklamowana zaleta systemów HD-SDI, jaką jest niska cena kamer. Owszem, kamery HD-SDI są tańsze od kamer IP, ale to nie decyduje o kosztach całego systemu. Chcąc oszacować koszty kompletnych instalacji, należy brać pod uwagę wszystkie ich składniki. W systemie HD-SDI średni koszt kabli i rejestratorów przeliczony na jedną kamerę kilkakrotnie przewyższa wartość samej kamery.

Te i inne przyczyny spowodowały, że systemy HD-SDI, które w zamyśle miały wyeliminować z rynku sieciowe systemy dozorowe, nie doczekały się wielu wdrożeń, zaś w świadomości projektantów i instalatorów stanowią jedynie przebrzmiałą ciekawostkę.

Inną techniką, która w odróżnieniu od HD-SDI zdobywa zasłużoną popularność, jest 960H. W zasadzie nie jest to standard, więc brakuje odpowiedniego określenia. Z drugiej strony można mówić o powtarzalności pewnych parametrów i ujednoliceniu konstrukcji urządzeń, więc technika 960H ma jednak pewne cechy standardu. Jej nazwa zawiera informację o rozmiarach obrazu. Kamery analogowe wykorzystywane w systemach 960H mają przetworniki o rozmiarach 976×582 pikseli, zaś rozmiary użytecznego rastra telewizyjnego wynoszą 960×540 pikseli.

W materiałach reklamowych mówi się o zwiększeniu rozmiarów kadru o 30%. W efekcie, jeśli uwzględni się proporcje obrazu (16:9), faktyczna poprawa jakości nie jest aż tak duża.

By w pełni wykorzystać zalety techniki 960H, trzeba stosować specjalne rejestratory. Kompatybilność z jakimkolwiek znanym standardem nie jest zachowana. Obraz jest nieco lepszy niż w standardzie PAL, a nieco gorszy niż w standardzie HD 720p. Niewątpliwą zaletą są jego proporcje, równe 16:9, gdyż cztery takie obrazy można łatwo wyświetlić na monitorze o rozdzielczości Full HD.

Z powyższych względów nie należy lekceważyć techniki 960H. Stanowi ona użyteczne rozszerzenie tradycyjnych rozwiązań analogowych i faktycznie umożliwia tanią modyfikację istniejących systemów dozorowych, bez konieczności wymiany okablowania. Z reguły rejestratory 960H są wyposażone w interfejsy IP, dzięki czemu można je łatwo łączyć w większe grupy. Możliwe jest także udostępnianie obrazów 960H w sieci, czyli jest to użyteczna namiastka systemów IP.

Kolejnym standardem analogowym, który ostatnio pojawił się na rynku, jest AHD. Jest on przeznaczony dla wszystkich entuzjastów technik innych niż sieciowe i w odróżnieniu od HD-SDI stanowi faktyczną alternatywę dla rozwiązań IP.

Porównując AHD z HD-SDI, należy stwierdzić, że nowa technika nie stanowi adaptacji jakiegoś istniejącego standardu, lecz została opracowana od zera i jest dobrze dostosowana do specyfiki wizyjnych systemów dozorowych. Jakość uzyskiwanego dzięki niej obrazu jest na tyle wysoka, że zastosowanie AHD można na serio brać pod uwagę podczas projektowania małych i średnich wizyjnych systemów dozorowych.

Trudno w ramach krótkiej prezentacji omówić technikę AHD, jednak należy podkreślić jej następujące właściwości:

- Do transmisji specyficznego sygnału wizyjnego stosowana jest częstotliwość podnośna i kwadraturowa modulacja amplitudy.
- Jednym kablem koncentrycznym transmitowane są trzy sygnały: wizyjny, dźwiękowy i sterujący.
- Stosując popularne kable koncentryczne, można uzyskać zasięg dochodzący do kilkuset metrów, który jest znacznie większy niż w przypadku kabli miedzianych stosowanych w sieciach Ethernet.
- Podczas transmisji sygnałów wizyjnych i sygnałów sterujących nie występują zauważalne opóźnienia, co przekłada się na wysoki komfort pracy operatorów systemów AHD.
- Stosowana jest technika zapewniająca kompensację zniekształceń sygnału podczas transmisji na duże odległości.
- Do budowy urządzeń AHD wykorzystywany jest specjalnie w tym celu opracowany zestaw układów scalonych (chipset).
- W wyniku kodowania jakość obrazu nie ulega pogorszeniu.
- W systemach AHD można wykorzystać kamery 960H, co stwarza dalsze ułatwienia podczas modernizacji systemów analogowych.

System AHD ma topologię gwiazdy. Możliwe jest tworzenie dużych systemów przez łączenie wielu podsystemów. Punktami węzłowymi są rejestratory, które jednocześnie pełnią funkcję urządzeń sterujących. Transmisja obrazów odbywa się w trybie P2P, czyli do każdego urządzenia peryferyjnego prowadzi osobny kabel koncentryczny.

Obecnie w systemach AHD wykorzystuje się jedynie dwa formaty obrazów, to znaczy 720p (1280×720 pikseli) i 1080p (1920×1080 pikseli), jednak producenci przewidują dalszy rozwój tej techniki i jej przystosowanie do wytwarzania i transmisji obrazów o rozdzielczości 4K.

Systemy AHD stanowią realną alternatywę dla rozwiązań sieciowych i oferują wiele funkcji niedostępnych w tradycyjnych systemach analogowych. Ich podstawowymi zaletami są wysoka jakość obrazu i brak opóźnień podczas transmisji sygnałów wizyjnych i sterujących. Trudno przewidzieć, czy systemy AHD staną się popularniejsze niż systemy IP, aczkolwiek obecnie ich popularność ciągle wzrasta. O ich dalszym losie zadecydują wysiłki producentów, reakcje potencjalnych klientów oraz upływ czasu.

Andrzej Walczyk

NOVUS®

Szybkoobrotowa KAMERA IP 2 MPX

do obserwacji rozległych terenów

Doskonale nadaje się do monitoringu dużych parkingów i centrów logistycznych, ponieważ umożliwia odczytywanie tablic rejestracyjnych samochodów.

POSTAW NA MEGAPIKSELOWĄ JAKOŚĆ OBRAZU!

NOVUS IP | NMS Compatible | ONVIF | 5000 SERIA IP | NOVUS 3 lata gwarancji

Kamera sieciowa NVIP-2DN5022SD/IRH-2

z oświetlaczem IR
z automatyczną regulacją mocy świecenia diod

Wyłączny dystrybutor produktów NOVUS® w Polsce:

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

Pozwala dostrzec nawet najdrobniejsze szczegóły

[zoom 22x]

Kamera wyposażona jest w obiektyw motor-zoom z automatycznym sterowaniem przysłony i ostrości, umożliwiający 22-krotną zmianę ogniskowej w zakresie od 4,7 mm do 103 mm. Może generować dwa strumienie wizyjne z prędkością do 30 kl/s i kompresją H.264 o maksymalnej rozdzielczości Full HD (strumień główny). Obraz z kamery jest wyraźny, ostry i charakteryzuje się dobrym odwzorowaniem detali obserwowanej sceny.

Widzi w ciemności

[IR LED 100 m]

Kamera ma wbudowany oświetlacz podczerwieni, czyli 12 diod LED o dużej mocy, które oświetlają obszar oddalony maksymalnie o 100 metrów od kamery. Ich moc jest regulowana automatycznie, w zależności od aktualnej wartości zoomu optycznego, ale można ją również ustawiać ręcznie, dopasowując do wymagań konkretnej instalacji. Kamera nie wymaga montowania dodatkowych źródeł światła, więc pozwala obniżyć sumaryczny koszt wdrożenia systemu.

NOVUS MANAGEMENT SYSTEM

oprogramowanie do monitoringu IP w komplecie z kamerą!

Niezawodna w każdych warunkach

[F-DNR]

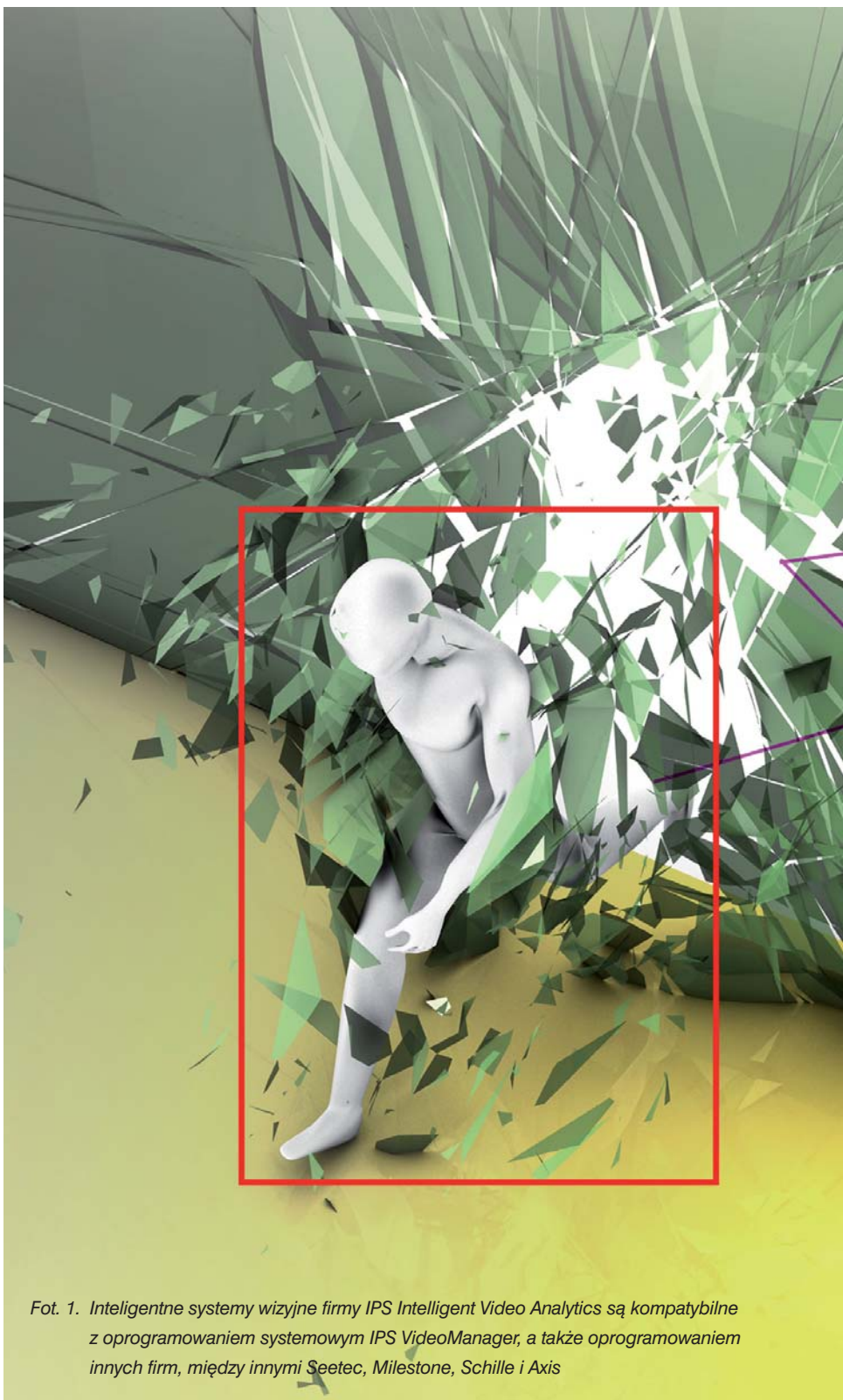
Zintegrowana grzałka oraz wentylator umożliwiają działanie kamery w temperaturze od -40°C do 60°C. Obudowa o klasie szczelności IP 66 chroni korpus przed kurzem i wilgocią. Innowacyjnym rozwiązaniem jest zastosowanie w kamerze funkcji defog (F-DNR), która poprawia widoczność podczas mgły lub mżawki.

Więcej informacji o produktach NOVUS® znajdziesz na:
www.novuscctv.pl

Nowa era – inteligentny nadzór wizyjny

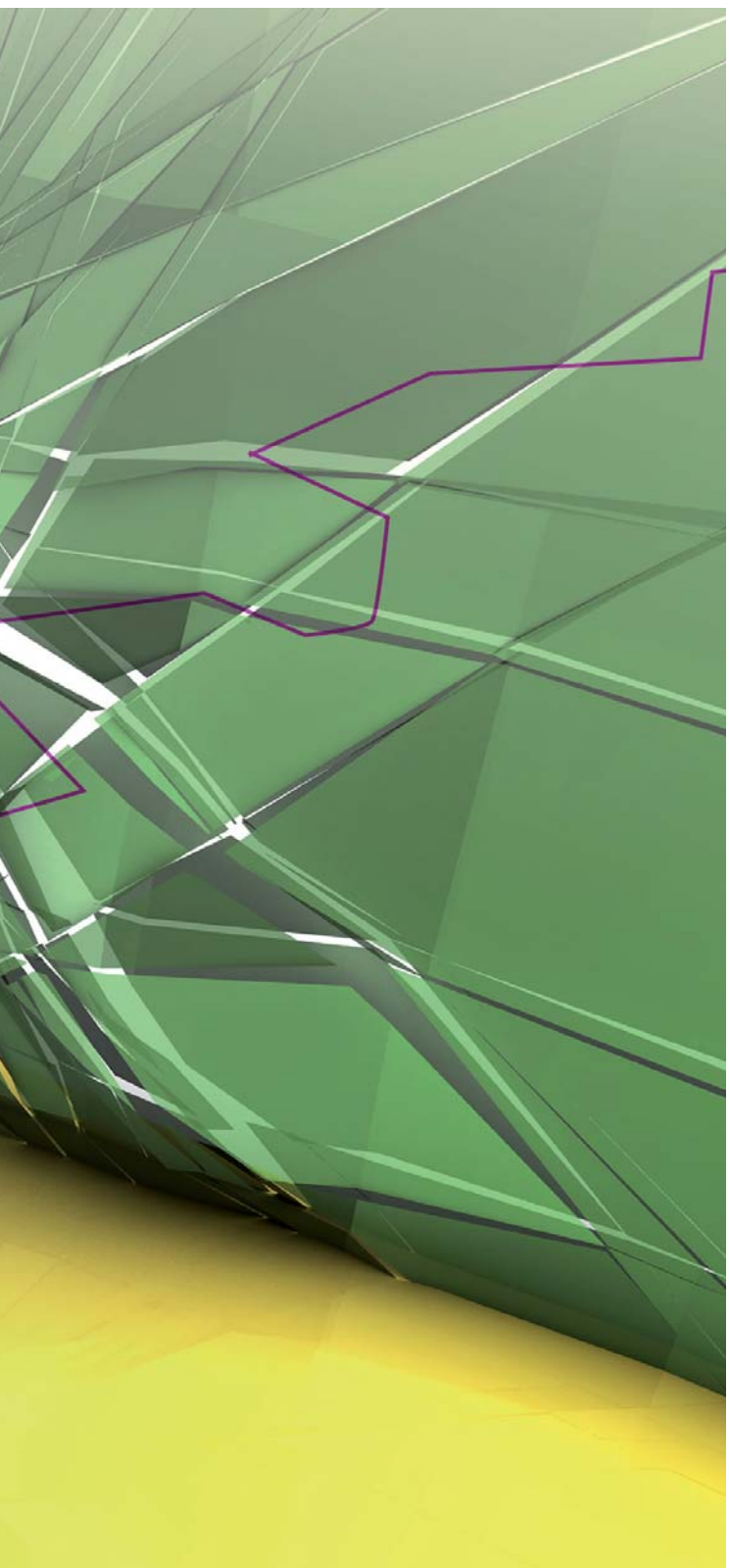
Magdalena Dziemidek

W inteligentnych wizyjnych systemach dozorowych wykorzystywane są zaawansowane algorytmy służące do automatycznej analizy treści cyfrowego obrazu przesyłanego z kamer monitoringu wizyjnego. Dzięki wykorzystaniu różnych procesów umożliwiają one rozpoznanie wcześniej zdefiniowanych wzorców obiektów i zachowań. W Polsce nadal pokutuje przekonanie, że jeśli analiza treści obrazu w pełni nie zastąpi obecności operatora systemu dozorowego, to jej zastosowanie nie ma racji bytu. Innego zdania są operatorzy systemów dozorowych w takich firmach jak Raiffeisen Bank, Allianz, Statoil, Deutsche Bahn Schenker, Franke, Media Markt czy Ikea



Fot. 1. Inteligentne systemy wizyjne firmy IPS Intelligent Video Analytics są kompatybilne z oprogramowaniem systemowym IPS VideoManager, a także oprogramowaniem innych firm, między innymi Seetec, Milestone, Schille i Axis

Rozbudowa wizyjnych systemów dozorowych jako trend wynika z potrzeby poprawy bezpieczeństwa publicznego i prywatnego. Jeżeli system jest rozbudowywany, trzeba nabyć odpowiedni sprzęt, w tym rejestratory i serwery wizyjne, a także zatrudnić więcej pracowników do obsługi systemu i sprawdzania rejestrowanego materiału wizyjnego. Kontroli i weryfikacji rejestrowanych zdarzeń dokonują pracownicy ochrony, zaś zarejestrowany materiał można wykorzystać podczas ewentualnego śledztwa. Obserwacja obrazów przez człowieka wymaga dużego wysiłku, jest kosztowna i nieefektywna z powodu zmęczenia operatora lub zaburzeń percepcji. Przeprowadzono wiele badań nad skutecznością pracy operatorów wizyjnych systemów dozorowych. Wynika z nich, że koncentracja operatora ulega pogorszeniu o 90 procent już po 22 minutach pracy. Z tego powodu wykorzystuje się funkcję automatycznej detekcji ruchu.



Warunkiem efektywności zastosowanych algorytmów jest wiedza na ich temat oraz właściwe dopasowanie kryteriów analizy do konkretnego przypadku. Zaoferowanie jednego, uniwersalnego rozwiązania dla każdego obiektu czy automatyczna detekcja różnych zagrożeń może nie przynieść oczekiwanych rezultatów. Każdy obiekt wymaga indywidualnego podejścia i właściwego zoptymalizowania algorytmów wykorzystywanych podczas analizy obrazów. Wymaga to specjalistycznej wiedzy, umiejętności i doświadczenia. Dla przykładu – funkcja wykrywania ruchu jest wykorzystywana przede wszystkim w celu redukcji ilości rejestrowanego materiału wizyjnego, a nie detekcji obiektów czy wydarzeń mających wpływ na bezpieczeństwo.

Do wiodących producentów inteligentnych systemów analizujących treść obrazu i zarządzających pracą kamer IP nowej generacji należy niemiecka firma IPS Intelligent Video Analytics. Firma istnieje od 1965 roku i specjalizuje się wyłącznie w tworzeniu inteligentnych systemów analizy treści obrazu dla branży zabezpieczeń – VideoAnalytics – oraz oprogramowania zarządzającego – VideoManager. Od 2006 roku firma jest związana z czołowym niemieckim producentem i integratorem systemów alarmowych i zabezpieczeń elektronicznych – firmą Securiton. Rozwiązania firmy IPS nie były do tej pory dostępne w Polsce, gdyż jej model biznesowy zakłada współpracę z ograniczoną liczbą partnerów w danym kraju. IPS stawia na profesjonalizm, dlatego oferowane systemy mogą być dystrybuowane wyłącznie przez przeszkolonych i doświadczonych pracowników. W Polsce autoryzowanym partnerem IPS jest od niedawna firma Innovative Security Systems – dostawca innowacyjnych systemów zabezpieczeń. Firma wywodzi swoje doświadczenie z rynku niemieckiego i długoletniej współpracy z firmami z branży systemów wizyjnych i zabezpieczeń elektronicznych. Prezes zarządu firmy ISS, Enrique Lafuente Romero, od ponad sześciu lat jest zatrudniony w firmie Securiton i jest odpowiedzialny za wdrażanie oprogramowania VideoManager oraz systemu VideoAnalytics w wielu obiektach na terenie Niemiec. Do grona klientów IPS Intelligent Video Analytics należy między innymi ponad 50 zakładów karnych, ponad 40 banków w Szwecji, w tym sieć banków Raiffeisen, ponad 70 rafinerii w Hiszpanii, placówki muzealne oraz centra logistyczne.

Systemy firmy IPS Intelligent Video Analytics informują o zagrożeniu w czasie rzeczywistym oraz umożliwiają wydobycie informacji z zarejestrowanego materiału wizyjnego. Istotą ich działania jest tworzenie strumienia metadanych, które są transmitowane równolegle ze strumieniem wizyjnym. W połączeniu z właściwym systemem zarządzania VMS umożliwia to konkretne działania, takie jak aktywacja alarmu, współpraca z systemem kontroli dostępu, zarządzanie zapisem materiału wizyjnego oraz szybkie przeszukiwanie zarchiwizowanych danych w celu znalezienia konkretnego obiektu lub wydarzenia.

Fot. 2. Przyszłość w zasięgu ręki – maska prywatności nałożona na wybrane strefy lub obszary ruchome. Maskę mogą zdjąć upoważnione osoby

Warto wymienić typowe algorytmy, które służą do analizy treści obrazów i umożliwiają ich automatyczną klasyfikację. Oto przykłady:

1) **Rozpoznanie obiektu**. Jest to algorytm wychwytujący zmiany w rejestrowanym obrazie. Analizie podlegają dane z pojedynczych obrazów i zmiany w obserwowanej scenie. Ten proces jest wykorzystywany przede wszystkim w celu redukcji ilości rejestrowanego materiału wizyjnego, a nie w celu detekcji obiektów czy wydarzeń mających wpływ na bezpieczeństwo.
2) **Śledzenie obiektu.** Jest to algorytm służący do rejestracji poruszających się obiektów. W tym przypadku następuje detekcja obiektów i ich śledzenie w następujących po sobie sekwencjach obrazów.
3) **Klasyfikacja obiektu.** Jest to algorytm umożliwiający rozróżnienie wcześniej zdefiniowanych rodzajów obiektów, na przykład osób, zwierząt, pojazdów. Obiekty pojawiające się w polu widzenia kamer podlegają analizie i są klasyfikowane na podstawie wcześniej zdefiniowanych znaków szczególnych.
4) **Identyfikacja obiektu.** Jest to algorytm umożliwiający wychwycenie specyficznych właściwości obiektów, takich jak twarze i sylwetki osób, tablice rejestracyjne pojazdów.
5) **Interpretacja wyglądu obiektu.** Jest to algorytm umożliwiający rozróżnienie specyficznych stanów obiektów, takich jak zachowanie, liczba elementów składowych.
6) **Interpretacja wyglądu scen.** Jest to algorytm umożliwiający rozróżnienie widocznych obiektów, na przykład ogrodzenia, budynku, torów kolejowych, oraz dokonanie analizy treści obrazu zgodnie z wybranymi priorytetami.

Bezpieczniej i efektywniej

Najczęstsze zastosowania inteligentnych systemów wizyjnych to:

– obserwacja wybranych obszarów,
– ochrona kamer przed aktywnym sabotażem,
– ochrona pomieszczeń, ochrona peryferyjna, ochrona terenów otwartych,
– detekcja włóczęgostwa i podejrzanych zachowań,
– ochrona prywatności w publicznych i prywatnych obszarach objętych nadzorem wizyjnym,
– prewencyjna detekcja podejrzanych przedmiotów,
– ochrona infrastruktury krytycznej,
– ochrona dzieł sztuki przed uszkodzeniem i kradzieżą,
– wykrywanie zdarzeń w ruchu drogowym.

Niemiecka niezawodność

W przypadku inteligentnych systemów analizy treści obrazu wykorzystywanych w branży zabezpieczeń najważniejszym zagadnieniem jest skuteczność działania algorytmów. Oprogramowanie musi identyfikować każde wtargnięcie, gdyż wszystko, co nie zostanie wykryte, może potencjalnie narazić chroniony obiekt na niebezpieczeństwo. Skuteczność to także niski poziom fałszywych alarmów lub alarmów wywołanych przez zwierzęta, spadające liście czy śnieg. Zastosowanie systemów IPS Intelligent Video Analytics gwarantuje zwiększenie skuteczności i efektywności nadzoru wizyjnego. Obecnie firma oferuje 16 różnych systemów przeznaczonych do stosowania w ściśle określonych środowiskach. Systemy alarmują w czasie rzeczywistym w przypadku włamania na teren monitorowanego obiektu oraz wykrywają i analizują podejrzane zachowania. Do najpopularniejszych systemów służących do

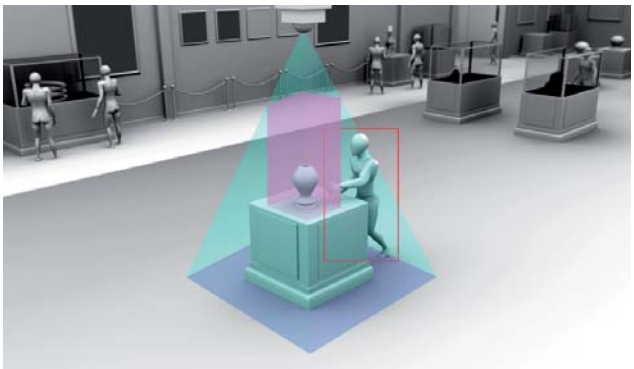
Fot. 3. Najpopularniejszy system wizyjny firmy IPS z certyfikatem iLIDS, wykorzystywany do profesjonalnej ochrony peryferyjnej

Fot. 4. Skuteczność inteligentnych systemów wizyjnych zależy od właściwego ustawienia kamer, indywidualnej konfiguracji stref i właściwego doboru algorytmów analizy

ochrony peryferyjnej należy Outdoor Detection, który ma certyfikat iLIDS nadawany w Wielkiej Brytanii systemom analizującym treść obrazów z kamer.

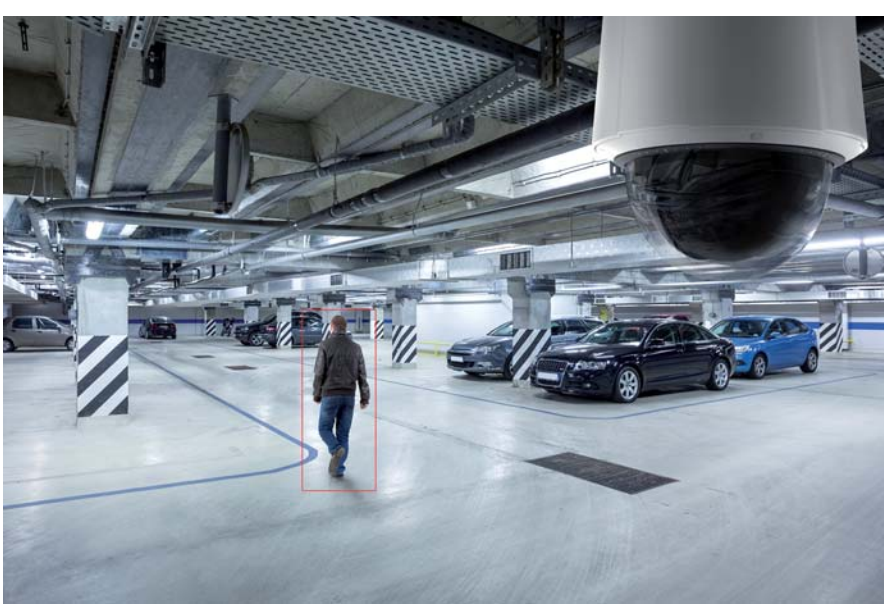
Przykłady inteligentnych systemów wizyjnych firmy IPS Intelligent Video Analytics

1) **Critical Infrastructure Protection** to inteligentny system przeznaczony do ochrony infrastruktury krytycznej. Do grona klientów należą elektrownie atomowe i rafinerie.
2) **Outdoor Detection** to inteligentny system zgodny z normą iLIDS, służący do ochrony peryferyjnej. System informuje w czasie rzeczywistym o wtargnięciu intruzów na chroniony obszar. Dzięki opatentowanej koncepcji trzech stref detekcji umożliwia dokładną analizę i odróżnienie osób uprawnionych do wstępu od intruzów. Dodatkowo może być optymalnie dostosowany do otoczenia. Ułatwia to detekcję wtargnięć nawet w trudnych warunkach atmosferycznych. System jest wykorzystywany do ochrony placówek więziennych, ochrony peryferyjnej, ochrony budynków i obszarów rządowych i wojskowych oraz zakładów produkcyjnych.
3) **3D Artwork Protection** to inteligentny system alarmujący w przypadku nieuprawnionego zbliżenia się do dzieła sztuki, którego miejsce przechowywania lub ekspozycji jest stałe. System tworzy dokładną, trójwymiarową kopię przestrzeni oraz wirtualną strefę ochronną wokół rzeźby lub obrazu, wykorzystując najnowszą technikę *Time-of-Flight*.
4) **Public Transport Protection** to system alarmujący w przypadku wystąpienia sytuacji kryzysowej w podziemnym lub naziemnym obiekcie kolejowym. Rozpoznaje ludzi i pociągi, stwierdza obecność ludzi na peronach i analizuje ich zachowanie, a także rozpoznaje zagrożenia i nietypowe sytuacje. Ułatwia to wykrywanie niebezpieczeństw nawet w trudnych warunkach atmosferycznych.



Fot. 6. System 3D Artwork Protection jest stosowany w wielu galeriach sztuki i placówkach muzealnych jako alternatywa dla tradycyjnych form ochrony ekspozycji dzieł sztuki

5) **Privacy Protection** to system służący do ochrony prywatności obszarów obserwowanych w czasie rzeczywistym. Ma on funkcję umożliwiającą nałożenie maski prywatności na wybrane strefy, obiekty ruchome oraz twarze osób przebywających w polu obserwacji. W odróżnieniu od masek prywatności nakładanych bezpośrednio w kamerach funkcja ta umożliwia zdjęcie maski podczas odtwarzania nagranego materiału przez upoważnione do tego osoby.
6) **Dome Tracker** to system służący do kontroli chronionego obszaru w czasie rzeczywistym z wykorzystaniem kamer PTZ. Automatycznie wykrywa i śledzi poruszające się obiekty znajdujące się w obrębie chronionego obszaru. Korzystanie z danych 3D umożliwia intuicyjne sterowanie funkcjami PTZ poprzez kliknięcie przycisku myszki po wskazaniu kursorem wybranego miejsca na obrazie pochodzącym z innej kamery lub na planie sytuacyjnym. System pozwala na automatyczne śledzenie obiektów przemieszczających się pomiędzy polami widzenia różnych kamer, przez co upraszcza obsługę kamer PTZ, nawet w obrębie złożonych obszarów nadzoru.
7) **Parking Violation Detection** jest systemem działającym w czasie rzeczywistym, informującym o zatrzymaniu się pojazdu w niedozwolonym sektorze monitorowanego obszaru. System odróżnia strefy przejazdu od stref parkowania, rozpoznaje zatrzymujące się pojazdy i kontroluje czas ich postoju. Dzięki tym funkcjom umożliwia bezbłędne wykrywanie pojazdów zaparkowanych w niedozwolonych miejscach.



Fot. 5. Współpraca kamer stałopozycyjnych z obrotowymi – sygnał alarmowy, wywołany na skutek wykrycia obiektu przez kamerę stacjonarną, jest przekazywany do kamery obrotowej, która przejmuje śledzenie obiektu

Magdalena Dziemidek
Innovative Security Systems
www.is-systems.pl
www.ips-analytics.com

INFIS: lokalizacja z wykorzystaniem GPS, telematyka, komunikacja, integracja

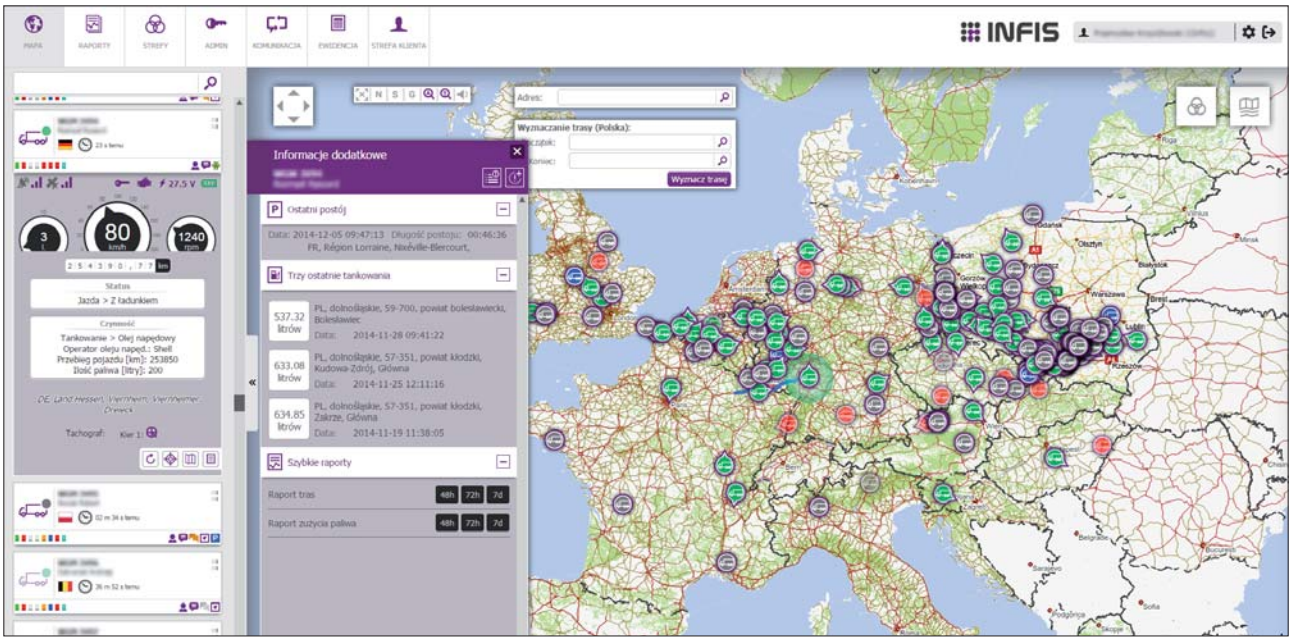
Przemysław Kropidłowski

W ciągu dziesięciu minionych lat nastąpił dynamiczny rozwój w dziedzinie telekomunikacji oraz pojawiły się nowe technologie. W tym czasie można było zaobserwować równie szybki rozwój firm wykorzystujących nowe możliwości. Na polskim rynku debiutowały coraz nowsze systemy informatyczne, w tym systemy wykorzystywane do zdalnego śledzenia flot pojazdów z użyciem GPS. Obecnie oferta w tej branży jest bogata. W gruncie rzeczy przedsiębiorstwa oferują rozwiązania zbliżone do tych, których oczekują potencjalni nabywcy. Dopiero szczegółowa weryfikacja poszczególnych ofert jest w stanie uwidocznić ich różnorodność i prawdziwy potencjał. Oprócz produktów z segmentów VTS (*Vehicle Tracking Services* – usługi śledzenia pojazdu) i AVLS (*Automatic Vehicle Location Services* – usługi automatycznej lokalizacji pojazdu) producenci sprzętu i oprogramowania proponują rozwiązania dla branży ochrony osób i mienia

Jedną z takich firm jest Infis – młoda, powstała w 2009 roku, wrocławska firma zatrudniająca doświadczonych specjalistów – począwszy od kadry zarządzającej, mającej ponad piętnastoletnie doświadczenie w pracy w branży, po pracowników utrzymujących bezpośredni kontakt z klientami. Specyficzna strategia rozwoju przedsiębiorstwa i budowy relacji z klientami to podstawa działania firmy Infis.

Tworząc nasze rozwiązania, stawiamy na jakość i możliwość łatwej personalizacji naszego głównego produktu oraz produktów pobocznych. Strukturę naszego systemu od początku opracowywaliśmy tak, aby mógł on tworzyć sieć powiązań z innymi, zintegrowanymi z nim systemami. Chcemy, aby nasi klienci mogli go wykorzystać na różne sposoby, do różnych celów. Dostarczamy narzędzi przeznaczonych do optymalizacji procesów logistycznych związanych z wykorzystaniem flot pojazdów oraz maszyn, rozliczeń i zarządzania personelem – powiedział Konrad Zając, członek zarządu.

System INFIS przyspiesza wymianę i przetwarzanie danych, umożliwia ich łatwą analizę oraz pomaga optymalizować koszty eksploatacji wszelkich zasobów. W swojej działalności firma

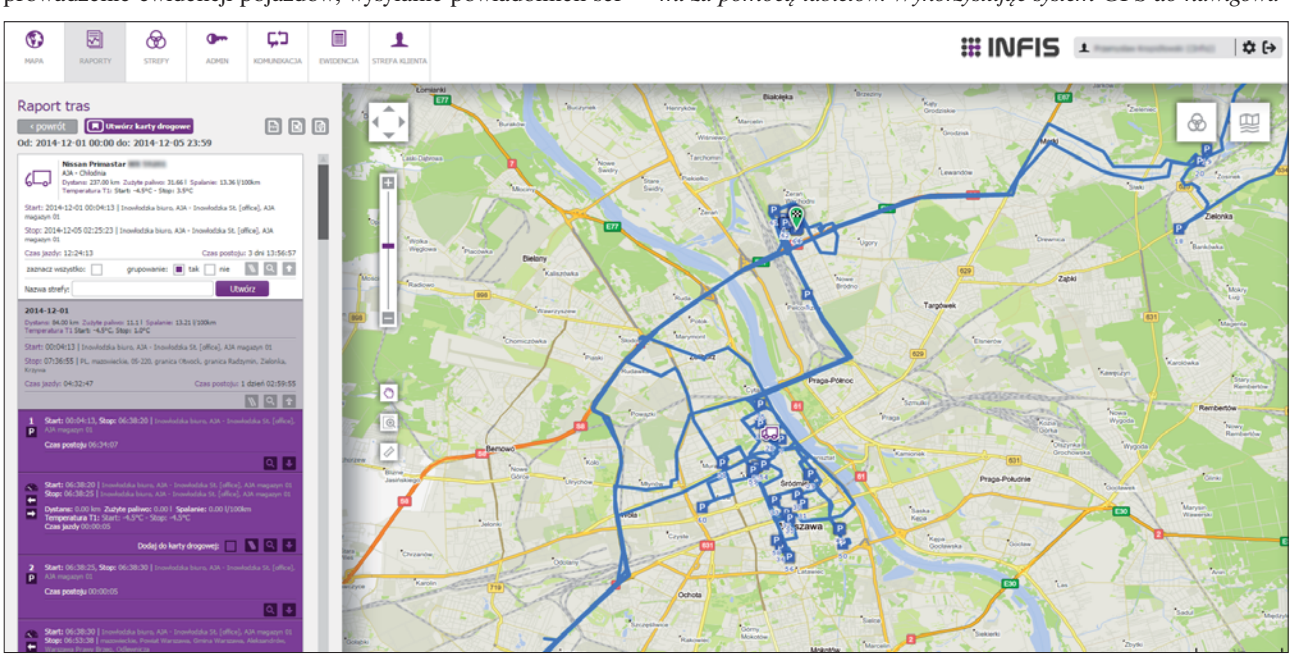


Fot. 1. Moduł mapowy systemu INFIS, do monitorowania obiektów w czasie rzeczywistym

Infis nie ogranicza się wyłącznie do tworzenia rozwiązań informatycznych. Jest również producentem zaawansowanych rejestratorów GPS. Wykorzystuje je we własnych wdrożeniach oraz umożliwia ich wykorzystanie swoim integratorom z Polski i zagranicy, m.in. firmom z branży ochrony osób i mienia (w tym największym agencjom ochrony w Polsce).

Aby zobrazować zakres możliwości wykorzystania rozwiązań oferowanych przez firmę Infis, należy wymienić chociaż niektóre jej produkty. Najważniejszy z nich to system ułatwiający zarządzanie flotą pojazdów. Umożliwia on rejestrację zarówno podstawowych danych pochodzących z komputerów pokładowych pojazdów, np. dotyczących zużycia paliwa, jak i bardziej złożonych danych informujących o technice prowadzenia pojazdu (tzw. *eco-driving*). Pozwala także na odczytywanie parametrów roboczych z maszyn i pobieranie sygnałów z różnego rodzaju czujników zewnętrznych. Poza tym system umożliwia prowadzenie ewidencji pojazdów, wysyłanie powiadomień serwisowych (pocztą elektroniczną i za pośrednictwem SMS) oraz rozliczanie faktur i automatyczne zestawianie danych z systemów operatorów paliwowych: AS24, BP, DKV, iDS, Lotos, Lukoil, Orlen, Petromiralles, Shell, Routex, UTA czy PetroConsulting. Częścią systemu INFIS jest moduł harmonogramów do nadzorowania pracy działów handlowych, a także system zleceń dla transportu ciężkiego, z możliwością nawigowania, nadawania statusów pracy przez kierowców i komunikacji tekstowej z dyspozytorami. Wszystko to jest realizowane za pomocą przeprogramowanych tabletów z systemem operacyjnym Android. Część klientów spółki wykorzystuje system w szerszym zakresie. W firmach transportowych INFIS pozwala na wymianę danych z takim oprogramowaniem jak Pascom Flota II, zaś w agencjach ochrony – z oprogramowaniem KRONOS i AdInfo.

Aktualnie pracujemy nad rozwiązaniem dla agencji ochrony, które umożliwi kontaktowanie się grup interwencyjnych z dyspozytorami za pomocą tabletów. Wykorzystując system GPS do nawigowa-



Fot. 2. Moduł raportowy systemu INFIS – raport tras

Fot. 3. Moduł raportowy systemu INFIS – raport zużycia paliwa uwzględniający dane z dwóch sond z transmisją analogową danych

nia, komunikację tekstową, nadawanie informacji statusowych czy zdalne wydawanie poleceń jesteśmy w stanie znacznie przyspieszyć akcje grup interwencyjnych. Właściwie od razu, zaraz po otrzymaniu zgłoszenia patrol może zostać wysłany na miejsce określone z dokładnością do trzech metrów – powiedział Konrad Zając.

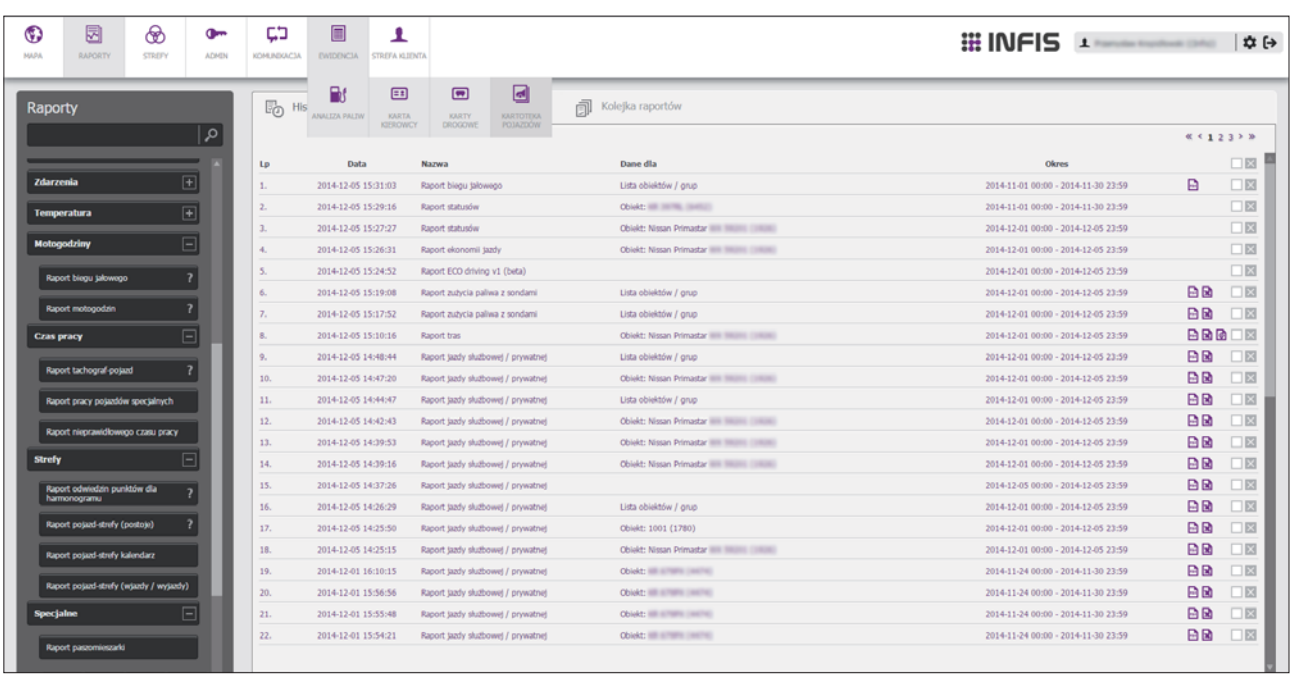
INFIS współpracuje również z giełdami transportowymi TimoCom oraz TransEU. Aby klienci mogli uzyskiwać najwyższej jakości dane topograficzne, system wykorzystuje mapy TARGEO.

Wykorzystując szybki rozwój rynku aplikacji mobilnych i masowy dostęp do nowoczesnych urządzeń, firma Infis bezpłatnie udostępnia swoim klientom system z ograniczonymi funkcjami, w wersji na smartfony i tablety.

Jednym z ostatnich przedsięwzięć firmy było stworzenie systemu do ewidencji odbioru nieczystości, przeznaczonego dla gmin i przedsiębiorstw oczyszczania. System nazywa się ODPADER i ułatwia dostosowanie się do przepisów, które od 1 lipca 2013 r. nałożyły na samorządy obowiązek odbioru nieczystości, dodatkowo zobowiązując je do monitorowania i tworzenia sprawozdań z przebiegu realizacji zadań. ODPADER wykorzystuje urządzenia mobilne i metodę NFC do skanowania kodów umieszczonych na pojemnikach. Na potrzeby jednego z małopolskich samorządów ODPADER został zintegrowany z systemem Arisco GOMIG służącym do gospodarowania odpadami.

Zakres działalności firmy Infis jest szeroki, jednak firma zajmuje się przede wszystkim tworzeniem rozwiązań wykorzystujących GPS, GPRS i GSM do lokalizacji obiektów i przesyłania danych. Warto nadmienić, że Infis to polska spółka bez udziału obcego kapitału.

Przemysław Kropidłowski



Fot. 4. Moduł wyboru raportu do wygenerowania, z chronologicznym wykazem raportów wygenerowanych

Praga chroniona przez system monitoringu wizyjnego firmy Geutebrück

Arpol

Praga to największe miasto i zarazem stolica Czech. Jest najważniejszym ośrodkiem administracyjnym, handlowo-usługowym oraz przemysłowym w kraju. Za sprawą licznych atrakcji oraz zabytkowej starówki, wpisanej na listę światowego dziedzictwa UNESCO, należy do najchętniej odwiedzanych miast w Europie. Zarówno mieszkańcy, jak i liczni turyści mają prawo czuć się tu bezpiecznie. Ochrona przed przestępczością i aktami wandalizmu, zapewnienie płynności ruchu w mieście i zminimalizowanie ryzyka wypadków to najważniejsze zadania miejskiego systemu nadzoru wizyjnego. Powinien on działać z poszanowaniem prywatności obywateli. Rada miejska w Pradze postawiła na sprawdzone i niezawodne rozwiązanie firmy Geutebrück

Obecnie w systemie pracuje około 3000 kamer, które monitorują kluczowe miejsca w mieście, takie jak stacje metra, przedszkola i szkoły, drogi i ulice, zabytkowe budynki, place i pomniki. Obraz jest rejestrowany z wykorzystaniem platformy GeViScope i ponad 200 rejestratorów należących do różnych serii urządzeń: GeViStore, GeViScope, re_porter. Ze względu na rozległość instalacji i potrzebę wykorzystania już wcześniej istniejących zasobów oprócz nowoczesnych kamer HD nadal używane są kamery poprzednich generacji. Całodobowy nadzór jest prowadzony w 15 centrach monitorowania. Dostęp do obrazów z kamer mają również służby porządkowe i ratownicze, policja oraz straż pożarna. Możliwych jest aż 60 jednoczesnych połączeń ze stacjami operatorów, obsługiwanych przez każdy z serwerów. Oznacza to, że w sytuacji kryzysowej aż 60 użytkowników może jednocześnie obserwować obrazy ze wszystkich kamer obsługiwanych przez każdy z serwerów. Obrazy pozostają w archiwum przez miesiąc, a prędkość ich odświeżania wynosi 12,5 kl./s. Najważniejsze użytkowe cechy systemu to łatwość obsługi, skuteczność, niezawodność działania oraz możliwość realizacji wielu różnych scenariuszy pracy awaryjnej. Dzięki modułowej architekturze system może być nieustannie modernizowany i rozbudowywany, co jest szczególnie ważne w przypadku dużej i dynamicznej metropolii. Każda kolejna generacja urządzeń i oprogramowania jest kompatybilna z poprzednimi, a władze miejskie mają pewność, że sprzęt firmy Geutebrück to efektywna inwestycja na długie lata.

Funkcja zaawansowanej detekcji ruchu przeznaczona do zastosowań zewnętrznych (VMD) w połączeniu ze wstępnie przygotowanymi widokami alarmowymi zwiększa efektywność pracy operatorów systemu i i umożliwia im skoncentrowanie się na istotnych w danym momencie elementach przestrzeni miejskiej. Możliwe jest natychmiastowe, automatyczne powiadomienie odpowiednich służb. Doskonałym przykładem takiego wykorzystania systemu jest słynny Most Karola. Ten charakterystyczny punkt Pragi, łączący brzegi Wełtawy, cieszy się dużym zainteresowaniem turystów. Niestety wielu z nich ignoruje zakazy oraz zasady bezpieczeństwa i przekracza balustradę, aby sfotografować się na tle ustawionych na moście posągów. Jest to niebezpieczne dla ludzi i szkodliwe dla zabytków. Dzięki funkcji VMD każde takie działanie skutkuje alarmem i powiadomieniem najbliższej jednostki policji. Zgromadzone nagrania mogą być wykorzystane jako materiał dowodowy w postępowaniu sądowym. Algorytm analizy treści obrazu działa niezawodnie w każdych warunkach pogodowych i umożliwia odróżnianie ludzi od innych obiektów, np. ptaków. Dzięki temu liczba fałszywych alarmów generowanych przez system jest ograniczona, a operatorzy nie rozpraszają się. Analizy treści obrazu dokonuje także ponad 300 kamer monitorujących ponad sześciokilometrowy tunel Blanka. Operatorzy są w stanie dostrzec sytuacje awaryjne, mające związek m.in. z zatorami czy zatrzymywaniem się pojazdów na pasie awaryjnym. W trosce o bezpieczeństwo najmłodszych kilkaset kamer przeznaczono do nadzoru miejskich przedszkoli. Również wszystkie stacje metra (obecnie 57) przez całą dobę są monitorowane przez odpowiednie służby.

Zarządzanie tak dużym systemem stanowi nie lada wyzwanie. Wykorzystując możliwość pełnej integracji i otwarty,

Fot. 1. Kamery do nadzoru ruchu drogowego na placu I.P. Pawłowa w Pradze (źródło: Aktron/Wikimedia Commons)

dobrze udokumentowany pakiet SDK, stworzono nakładkę graficzną, która ułatwia pracę operatorom systemu. Na planach miasta naniesione są wszystkie elementy aktywne i zwizualizowany jest ich stan. Do sterowania kamerami obrotowymi, których w systemie jest ponad 1000, służy interfejs typu „wskaż i obserwuj". Użytkownik wybiera kamerę, zaznacza na mapie lokalizację, którą chce obserwować, a kamera pokazuje wybrane przez niego miejsce. Dalsze, precyzyjne sterowanie kamerami obrotowymi jest możliwe za pomocą manipulatorów drążkowych.

System nadzoru wizyjnego firmy Geutebrück umożliwia władzom oraz służbom porządkowym Pragi utrzymanie bezpieczeństwa w mieście oraz ochronę dziedzictwa architektonicznego i kulturowego. Dzięki niemu policja może interweniować szybciej niż kiedykolwiek, gdziekolwiek jest to konieczne. Modułowa architektura systemu, pozwalająca na bezproblemową rozbudowę, w połączeniu z jego skutecznością oraz niezawodnością umożliwia nieustanne rozszerzanie zasięgu jego działania.

Arpol

Systemy kontroli dostępu i elektroniczne zamki – aktualne trendy

Pavel Doležal

Elektroniczna kontrola dostępu daje lepszą ochronę i możliwość łączenia różnych systemów niż tradycyjny system zamków i kluczy mechanicznych. Zwiększeniu zapotrzebowania na takie zabezpieczenie towarzyszy wzrost zainteresowania elektronicznymi zamkami. Taka tendencja utrzyma się pod warunkiem, że na rynku będą szybciej pojawiać się nowe sieciowe systemy kontroli dostępu i przyjmą się nowe urządzenia bezprzewodowe. Do tych urządzeń należą elektroniczne zamki, które łączą się bezprzewodowo z sieciowym systemem kontroli dostępu i można je otworzyć za pomocą smartfonów, które działają jako urządzenia potwierdzające uprawnienia użytkownika

Fot. Smartfon jako karta zbliżeniowa do czytnika kontroli dostępu

Według firmy IHS w 2017 r. dochody ze sprzedaży elektrozaczepów i zwór elektromagnetycznych znacznie przewyższą dochody ze sprzedaży zamków mechanicznych. W raporcie zatytułowanym *Market Insight* ze stycznia 2014 r. IHS stwierdza, że dochody uzyskane ze sprzedaży tych produktów mają wzrosnąć – skumulowany roczny wskaźnik wzrostu (ang. *Compound Annual Growth Rate*) ma wynosić odpowiednio 6,9 i 7,8 procent. Dla porównania wskaźnik CAGR dla zamków mechanicznych w tych samych ramach czasowych wynosi 4,5 procent. Adi Pavlovic, analityk z firmy IHS, łączy zwiększenie zapotrzebowania na te produkty ze wzrostem popularności elektronicznych systemów kontroli dostępu. Według firmy zwory elektromagnetyczne i elektrozaczepy są najbardziej popularnymi elektrycznymi urządzeniami zamykającymi używanymi razem z systemami kontroli dostępu.

Migracja systemów kontroli dostępu w kierunku rozwiązań wykorzystujących IP

Elektroniczne systemy kontroli dostępu mogą być jeszcze bardziej atrakcyjne w przypadku wykorzystania do komunikacji rozwiązań IP. Do zalet tego rodzaju komunikacji należy m.in. możliwość jej rozszerzenia i dostosowania do indywidualnych potrzeb, uproszczenie systemu operacyjnego, a także możliwość połączenia systemu fizycznej kontroli dostępu z wieloma innymi rozwiązaniami w obrębie tej samej sieci.

Obecnie większość firm i instytucji dysponuje różnymi niepołączonymi i odizolowanymi systemami zabezpieczeń: kontroli dostępu, monitoringu, reagowania na zdarzenia, ochrony obwodowej i monitorowania alarmów. Systemy te zazwyczaj nie wymieniają bezpośrednio informacji pomiędzy sobą. Rozwiązania, w których wykorzystuje się IP, ułatwiają ich zintegrowanie i sprawiają, że powstały w ten sposób system może być znacznie lepszy niż suma jego odseparowanych, działających osobno, niepołączonych części. Możliwość zarządzania wszystkimi systemami w jednej sieci pozwala również na lepsze zarządzanie obiektem. Pojedynczy system może mieć różne funkcje i zarazem jeden interfejs, za pośrednictwem którego dostępne są wszystkie aplikacje. Firmy, które wcześniej korzystały z kilku systemów bezpieczeństwa działających w osobnych sieciach, mogą w zamian zainwestować w jedną sieć IP, a urządzenia, które wcześniej koegzystowały tylko fizycznie, mogą być zarządzane i kontrolowane logicznie.

Kontrola dostępu wykorzystująca IP podwyższa poziom zabezpieczenia. Jednym z powodów jest to, że możliwe jest połączenie jej z monitoringiem. Możliwość zarządzania całym materiałem wizyjnym i podsystemami analitycznymi, urządzeniami do wykrywania intruzów i powiązanymi urządzeniami ochrony peryferyjnej wykorzystującymi IP za pośrednictwem jednego interfejsu użytkownika umożliwia lepszy nadzór, gdyż wszystkie informacje mogą być natychmiast połączone i powiązane. Wykorzystaniu IP w kontroli dostępu będzie towarzyszyć również stosowanie podłączanych bezprzewodowo zamków, które umożliwiają ich kontrolowanie i otwieranie praktycznie w czasie rzeczywistym. To zredukuje koszty okablowania i ograniczy problemy z mechanicznymi kluczami, które łatwo ukraść lub zgubić, trudno kontrolować, którymi trudno zarządzać i które utrudniają analizę zdarzeń. Zanim zastosuje się elektroniczne zamki w sieciowej kontroli dostępu, należy wziąć pod uwagę pewne związane z tym zagadnienia.

Modernizacja systemów kontroli dostępu

Wdrażanie nowych rozwiązań wykorzystujących zamki elektroniczne pracujące w sieciowych systemach kontroli dostępu powinno zapewnić ciągłość funkcjonowania i rozwoju pomiędzy tradycyjnymi zamkami mechanicznymi bez wbudowanej „inteligencji" a „inteligentnymi" i w pełni funkcjonalnymi rozwiązaniami, jakie oferują sieciowe systemy kontroli przejść. Takie systemy muszą być przystosowane do przyszłego rozwoju danej lokalizacji w zakresie zapewnienia wymaganego poziomu bezpieczeństwa. Oznacza to, że taki system powinien gwarantować możliwość kontroli kilku drzwi oraz od kilkudziesięciu do kilkuset posiadaczy kart dziś, a także zarządzanie setkami drzwi w wielu obiektach i kontrolowanie nawet 100 tysięcy lub więcej posiadaczy kart jutro.

W przeciwieństwie do rozwiązań dedykowanych, które opierają się na wykorzystaniu paneli z dedykowanym oprogramowaniem OEM, rozwiązanie bazujące na protokole IP zapewnia dostęp do setek opcji oprogramowania systemu kontroli dostępu. To gwarantuje, że użytkownik końcowy, który kupuje kontroler z prostym, aktualnie oferowanym oprogramowaniem, będzie mógł w przyszłości wymienić oprogramowanie na spełniające wyższe wymagania bez konieczności wymiany sprzętu. Aby uzyskać optymalną skalowalność systemu, rozwiązania przeznaczone do kontroli dostępu z wykorzystaniem protokołu IP powinny oferować również kompletne deweloperskie zestawy zawierające standardowe interfejsy programistyczne (API) umożliwiające dostęp do funkcji wbudowanych w oprogramowanie systemu kontroli dostępu. To umożliwi klientom dostosowanie systemu do zmieniających się wymagań i rozbudowanie go w przyszłości, a ich inwestycja nie straci na wartości. Użytkownik powinien mieć również wiele możliwości dołączania do systemu kontroli dostępu modułów systemu sygnalizacji pożarowej, czujek systemu alarmowego dołączanych do kodowanej magistrali komunikacyjnej Hi-O oraz możliwość sterowania zamkami elektrycznymi 12/24 V_{DC} i modułami *plug and play* typu we/wy (IO) po obu stronach kontrolowanego przejścia.

Bezprzewodowe zamki elektroniczne

Zastosowanie inteligentnych bezprzewodowych zamków elektronicznych jest pierwszym krokiem ku umożliwieniu swobodnych połączeń w sieciowych systemach kontroli dostępu. Te urządzenia upowszechnią się, gdy na rynku pojawią się bardziej energooszczędne i tańsze modele. Będą one opłacalną alternatywą dla urządzeń przewodowych stosowanych obecnie w systemach kontroli dostępu, ponieważ nie będzie konieczności prowadzenia okablowania do kontrolowanych drzwi.

Wraz z wprowadzeniem do użytku bezprzewodowych zamków elektronicznych obserwujemy także wzrost popularności mobilnej kontroli dostępu, w której do uwierzytelniania używa się smartfonów i innych tego typu urządzeń, zastępujących tradycyjne karty zbliżeniowe. Tradycyjne karty zbliżeniowe będą zatem w użyciu równolegle z kartami „cyfrowymi" zaimplementowanymi w smartfonach, używanymi również do obsługi innych aplikacji w sieciach IP. Instalując inteligentne kontrolery IP z otwartą architekturą, użytkownik będzie miał do wyboru wiele przewodowych i bezprzewodowych zamków elektronicznych wykorzystujących różne metody uwierzytelniania.

Wykorzystanie możliwości smartfonów

Następnym krokiem po prostej emulacji karty zbliżeniowej będzie wykorzystanie zaimplementowanych w smartfonach inteligentnych rozwiązań i możliwości w zakresie połączeń sieciowych do realizacji większości zadań wykonywanych obecnie przez tradycyjne czytniki, kontrolery i serwery kontroli dostępu. Urządzenie mobilne wykorzysta swoje możliwości w zakresie łączności bezprzewodowej oraz zaimplementowane klucze, procesy i zasady do podejmowania decyzji dotyczących kontroli dostępu. Może to zainicjować odwrócenie ról i dotychczasowego sposobu widzenia, zwanego czasami dualizmem, zgodnie z którym urządzenie mobilne zawierające dane uwierzytelniające staje się jednostką decyzyjną, zastępując sterownik kontroli dostępu, a kontrolowane przejście, a nie karta, staje się identyfikatorem. Ta koncepcja wyeliminuje potrzebę instalowania inteligentnych czytników (i zamków) i połączeń kablowych z urządzeniami końcowymi. Wszystko, co będzie wymagane, to autonomiczne elektroniczne zamki, które potrafią rozpoznawać polecenie „zezwól na dostęp" wysłane z mobilnego urządzenia i działać zgodnie ze zdefiniowanym wcześniej zbiorem reguł dotyczących dostępu.

Redukcja kosztów rozbudowy systemów

Wykorzystanie urządzeń mobilnych do uwierzytelniania radykalnie zredukuje koszty związane z zastosowaniem systemów kontroli dostępu, dzięki czemu producenci będą mogli zabezpieczyć tym systemem więcej wewnętrznych drzwi, szafy na dokumenty, szafki do przechowywania różnych przedmiotów i inne miejsca, w których instalowanie tradycyjnej infrastruktury przewodowej jest zbyt kosztowne.

Dostępna będzie mieszana struktura z przewodowymi, bezprzewodowymi i autonomicznymi zamkami, a także nowe sposoby bardziej ekonomicznego rozmieszczenia urządzeń do kontroli dostępu w procentowo większej części dotychczas ogólnie dostępnych przestrzeni w obiektach.

Kontrola dostępu z wykorzystaniem połączeń IP będzie coraz powszechniej stosowana i spodziewane jest dalsze zwiększenie ilości elektronicznych urządzeń zamykających. Do wypływających z jej zastosowania korzyści należy uproszczenie działania systemu, możliwość jego rozbudowy i dostosowania do indywidualnych potrzeb, a także możliwość połączenia systemu fizycznej kontroli dostępu z innymi rozwiązaniami w jednej sieci. Ponadto dzięki przesunięciu inteligentnych rozwiązań do kontrolowanego przejścia łatwiejsze będzie monitorowanie systemu kontroli dostępu, zarządzanie nim i generowanie raportów.

Wkrótce także podejmowanie decyzji dotyczącej zezwolenia na dostęp będzie należeć do smartfonów. To będzie zmiana podejścia i dotychczasowych reguł, dzięki której będzie można elektronicznie zabezpieczyć więcej drzwi niż kiedykolwiek wcześniej, stosując kombinację przewodowych, bezprzewodowych i autonomicznych zamków, przewodowe i bezprzewodowe inteligentne czytniki, a także różne metody uwierzytelniania.

Pavel Doležal
Area Sales Manager
HID Global
Tłumaczenie: Redakcja

Systemy alarmowe **Satel**

Centrala alarmowa **VERSA Plus**

Manipulatory
VERSA-LCDM-WRL oraz **INT-TSG**

Komunikacja **doskonała**

Elastyczność i skalowalność to cechy charakterystyczne produktów SATEL - nie inaczej jest w przypadku najnowszej centrali alarmowej **VERSA Plus**.

To wyjątkowe urządzenie umożliwia stworzenie systemu zarówno hybrydowego, jak i w pełni bezprzewodowego, który może działać w jednym lub w dwóch kierunkach.

Pewność komunikacji w systemie opartym na centrali **VERSA Plus** gwarantują aż trzy kanały komunikacji (Ethernet, PSTN, GSM/GPRS), a jego wygodną obsługę zapewnia dedykowany manipulator bezprzewodowy VERSA-LCDM-WRL oraz manipulator dotykowy INT-TSG.

Więcej informacji na **www.satel.pl**

Satel Sp. z o.o.
ul. Budowlanych 66, 80-298 Gdańsk, tel.: (58) 522 66 00, fax: (58) 522 66 94 01,
e-mail: satel@satel.pl, **www.satel.pl**

Skuteczna detekcja w każdych warunkach

ADPRO by Xtralis – zewnętrzne czujki PIR dalekiego zasięgu

Jakub Sobek

Szybka detekcja intruza to najważniejsza właściwość skutecznie działającego systemu ochrony perymetrycznej. Oczywiście równie istotne jest eliminowanie fałszywych alarmów. To wszystko można uzyskać, stosując inteligentne, pasywne czujki podczerwieni przystosowane do pracy na zewnątrz, które ograniczają do minimum ewentualność wystąpienia fałszywych alarmów. Ich pracę można dodatkowo usprawnić, używając kamer umożliwiających weryfikację przyczyn alarmów. W wielu przypadkach takim uzupełnieniem mogą być kamery termowizyjne. Tak samo jak pasywne czujki podczerwieni, te kamery „widzą" w zupełnej ciemności oraz przez mgłę, deszcz czy śnieg. Pasywne czujki podczerwieni mogą pracować w każdych warunkach pogodowych, zarówno w dzień, jak i w nocy. Nie można ich oślepić silnym światłem widzialnym lub promieniem laserowym. Także tradycyjne metody kamuflażu nie pozwalają ukryć się przed taką czujką

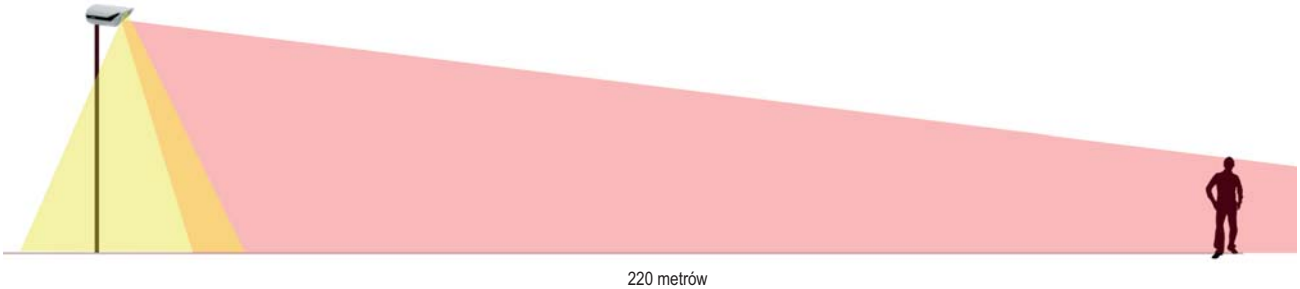
Połączenie w jednym systemie wielu różnych technik wykrywania intruza umożliwia tworzenie efektywnych rozwiązań.

Wykorzystanie podczerwieni w systemach zabezpieczeń

Ludzkie oko reaguje na światło białe i na wszystkie jego kolory składowe. Jest to jednak tylko niewielki wycinek całego widma promieniowania elektromagnetycznego, które nas otacza. Część tego widma, którą można wykorzystać w systemach zabezpieczeń, to promieniowanie podczerwone. Promieniowanie podczerwone jest znane każdemu z nas. Przykładowo, przechodząc obok gorącego kaloryfera, odczuwamy jego ciepło. Wszystko, co ma temperaturę powyżej -273 stopni Celsjusza, emituje promieniowanie podczerwone. Właśnie ta cecha została wykorzystana w czujkach PIR, których głównym zadaniem jest detekcja obiektu, czyli wykrycie zmian temperatury.

Nowa seria PRO E czujek ADPRO by Xtralis

W najnowszej serii zewnętrznych czujek PIR marki ADPRO wykorzystano zaawansowane funkcje i złożoną analizę zmian



Rys. 1. Funkcja 360 Protect umożliwia ochronę czujki przed sabotażem

sygnałów z detektorów podczerwieni, eliminując wpływ całego szeregu fałszywych pobudzeń. Seria PRO E obejmuje dwie główne grupy czujek: czujki kurtynowe i czujki wolumetryczne.

Czujki kurtynowe pozwalają na detekcję intruzów z odległości do 220 metrów. Co istotne, kurtynowa charakterystyka czujek marki ADPRO jest tak ukształtowana, że obszar wykrywania intruzów przy bardzo długich zasięgach zachowuje małą szerokość (2–3 metry). Dzięki temu nie jest konieczne wytyczenie bardzo szerokiej strefy dla systemu ochrony perymetrycznej. Tak dalekie zasięgi detekcji w przypadku czujek kurtynowych umożliwiają także redukcję kosztów – do stworzenia systemu ochrony obwodowej potrzeba mniej czujek, a także mniej słupów i okablowania. Oszczędzamy też czas potrzebny na instalację takiego systemu.

Czujki wolumetryczne umożliwiają zabezpieczenie dużych obszarów. Działają na krótszych dystansach, ale szerokość obszaru detekcji jest w ich przypadku dużo większa. Czujki te są stosowane przede wszystkim do zabezpieczania dużych obszarów, takich jak place, parkingi itp. Mają funkcję zliczania impulsów – dopiero wówczas, gdy czujka zliczy zadaną ilość przekroczeń progu alarmowego, wygenerowany zostaje sygnał alarmowy.

Bardzo istotne są dodatkowe zabezpieczenia wszystkich czujek z serii PRO E marki ADPRO, które chronią przed próbami sabotażu. Najnowsze produkty mają funkcję *360 Protect*. Do jej realizacji wykorzystywany jest dodatkowy czujnik umożliwiający wykrycie osoby stojącej w martwej strefie. Wykryta może być osoba stojąca maksymalnie osiem metrów przed czujką albo metr za nią. Wszystkie czujki mają zabezpieczenie przed zmianą ich ustawienia. Powolna zmiana położenia czujki sprawi, że zostanie wygenerowany alarm sabotażowy. Jest to możliwe dzięki elektronicznemu kompasowi, który jest zintegrowany w układzie scalonym. Dodatkowo czujki mają czujnik światła padającego od zewnątrz. Jego przeznaczeniem jest wykrywanie wszelkich prób zakrycia, zamaskowania czy zamalowania. Czujki są więc w pełni chronione przed sabotażem. Są odporne także na wszelkie próby dostania się do ich wnętrza przez nawiercanie, przepiłowywanie czy uszkodzenie obudowy w inny sposób. Wewnątrz czujki znajduje się czujnik światła, który wykrywa każdą tego typu próbę sabotażu.

Wszystkie modele czujek marki ADPRO mogą pracować w systemach bezprzewodowych – mogą być zasilane bateriami umieszczonymi w ich wnętrzu. Zasilana w ten sposób czujka może pracować nieprzerwanie przez trzy lata. W takim przypadku sygnały alarmowe z czujki są przesyłane drogą radiową. W tym celu wykorzystywany jest standard Inovonics. Duża skuteczność i redukcja kosztów to bardzo silne argumenty przemawiające za stosowaniem opisanych rozwiązań.

Bardzo istotną cechą wszystkich czujek marki ADPRO jest możliwość ich zdalnej konfiguracji przez port RS485. Bezpłatne oprogramowanie, które jest dostarczane przez producenta, umożliwia zaprogramowanie wszystkich parametrów urządzenia i sprawdzenie przebiegu wszystkich sygnałów w czujce w graficznym interfejsie użytkownika. Dzięki temu można bardzo dokładnie sprawdzić sposób działania czujki oraz poprawność jej montażu. Przez port RS485 można także transmitować sygnały alarmowe wytwarzane przez czujkę. Interfejs ten może zostać wykorzystany także w celu podłączenia innych urządzeń, np. FastTrace. Czujki PIR mają pięć wyjść alarmowych, przy czym każde z nich może informować o innym zdarzeniu alarmowym. Dzięki temu czujki można podłączyć do klasycznych central alarmowych. W efekcie otrzymywana jest dokładna informacja o wykrytym zdarzeniu, nawet gdy nie jest wykorzystywany port RS485.

Czujki ADPRO by Xtralis to profesjonalne urządzenia przeznaczone do pracy w systemach ochrony perymetrycznej. Ich wyjątkowe możliwości i ponadprzeciętny zasięg sprawiają, że wyraźnie wyróżniają się na rynku zabezpieczeń.

Fot. 1. Pasywna czujka podczerwieni ADPRO by Xtralis z serii PRO E

Jakub Sobek

Więcej na stronie: www.xtralis.linc.pl

System komunikacji wewnętrznej VoIP

Inteligentny terminal dotykowy

Zdalne aplikacje

Kontroler i czytnik IP

emerald™

Świat możliwości na wyciągnięcie ręki

emerald™ to wielofunkcyjny inteligentny terminal dostępowy rewolucjonizujący przemysł zabezpieczeń.

Dzięki eleganckiej konstrukcji i specjalnie zaprojektowanemu nowoczesnemu ekranowi dotykowemu urządzenie emerald stanowi wydajny czytnik kart i kontroler w jednym, oferujący w pełni zintegrowany system komunikacji wewnętrznej Voice over IP (VoIP) oraz asortyment zdalnych aplikacji, zapewniających różnorodne możliwości kontroli dostępu. System emerald otwiera świat niezliczonych możliwości umieszczając system kontroli dostępu CEM w awangardzie przyszłości.

emerald™ — najbardziej wielofunkcyjny inteligentny terminal dostępowy w branży.

Jeśli potrzebujesz więcej informacji, prosimy o kontakt:
T: +44 (0)28 9045 6767
E: cem.info@tycoint.com
lub odwiedź nas na stronie www.cemsys.com/emerald

CEM SYSTEMS
From Tyco Security Products

HRT82MF

Czytnik kart zbliżeniowych MIFARE do zastosowań hotelowych

HRT82MF jest czytnikiem kart zbliżeniowych MIFARE zaprojektowanym do zastosowań hotelowych jako tzw. czytnik korytarzowy. Czytnik jest wyposażony w przycisk dzwonka oraz wskaźniki świetlne przypisane do typowych usług hotelowych, takich jak wezwanie obsługi, wezwanie pomocy, zamówienie sprzątania, a także komunikatu „nie przeszkadzać". Prośby o poszczególne usługi są sygnalizowane na osobnych wskaźnikach świetlnych, które mogą być uruchamiane za pomocą panelu z klawiszami dotykowymi (HRT82FK) lub przyciskiem dołączanym do linii wejściowej kontrolera.
Komunikacja z kontrolerem jest realizowana za pomocą linii interfejsu RACS CLK/DTA (ROGER). Podobnie jak kontroler PR821-CH oraz panel dotykowy HRT82FK czytnik HRT82MF jest umieszczony w obudowie serii QUADRUS tworząc w ten sposób jednorodną linię wzorniczą produktów przeznaczonych do zastosowań hotelowych.

Charakterystyka

- Odczyt kart zbliżeniowych MIFARE
- Cztery wskaźniki LED
- Przycisk dzwonka
- Interfejs komunikacyjny RACS CLK/DTA
- Dwa wejścia NO/NC
- Zasilanie 12 V_{DC}

Producent: roger®

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

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

PR821-CH

Kontroler dostępu i automatyki hotelowej z kieszenią na kartę

Kontroler **PR821-CH** jest przeznaczony do montażu w pokoju hotelowym jako urządzenie zarządzające dostępem do pokoju oraz realizujące funkcje automatyki pokojowej. Z kontrolerem może współpracować czytnik zbliżeniowy umieszczony przy wejściu do pokoju oraz panel dotykowych klawiszy funkcyjnych (HRT82FK). Do kontrolera można podłączyć dowolny czytnik zbliżeniowy pracujący w standardzie RACS CLK/DTA (ROGER). Najbardziej do tego celu predestynowany jest czytnik HRT82MF, który posiada wskaźniki LED przeznaczone do sygnalizacji typowych sytuacji spotykanych w hotelach (zamówienie sprzątania i sygnalizacja „nie przeszkadzać"). Kontroler umożliwia sterowanie zasilaniem elektrycznym w pokoju, sterowanie klimatyzacją jak również we współpracy z czujnikami otwarcia drzwi i okien, realizację prostych funkcji antywłamaniowych. Funkcje te umożliwiają z jednej strony bardziej ekonomiczne zarządzanie systemami dostępnymi w pokoju, a z drugiej zwiększenie komfortu jego użytkowania.

Charakterystyka

- Kieszeń na kartę z obsługą kart EM 125 kHz i MIFARE
- Współpraca z zewnętrznym czytnikiem umieszczonym przy wejściu do pokoju
- Współpraca z panelem dotykowych klawiszy funkcyjnych (HRT82FK)
- Obsługa z poziomu programu PR Master
- Możliwość sterowania zasilaniem elektrycznym w pokoju poprzez umieszczenie karty w kieszeni kontrolera
- Komunikacja RS485
- Trzy wejścia NO/NC
- Dwa wyjścia tranzystorowe 15 V_{DC}/1 A
- Wyjście przekaźnikowe 30 V/1.5 A
- Zasilanie 12 V_{DC}

Producent: roger®

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

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

Kamera sieciowa Ultra HD, 12 Mpx – DH-IPC-HF81200E

Dane techniczne

- Przetwornik CMOS, 1/2,3" ze skanowaniem progresywnym
- Rozdzielczość 12 Mpx (4000×3000)
- Dwa kodeki: H.264/MJPEG
- Trzy strumienie wizyjne
- 15 kl./s przy rozdzielczości 12 Mpx
- Dostępne funkcje: Ultra Defog, ROI, EIS
- Detekcja twarzy
- Detekcja przekroczenia umownej linii, wtargnięcia na chroniony obszar
- Detekcja zmiany ustawienia kamery
- Automatyczna regulacja ostrości
- Wbudowany mikrofon
- Interfejs Ethernet 100/1000M Base-T

Model	DH-IPC-HF81200EP	DH-IPC-HF81200EN
Cechy przetwornika		
Rodzaj i wielkość	CMOS 1/2.3", 12 Mpx	
Liczba pikseli	4000(H)×3000(V)	
Min. poziom oświetlenia	kolor: 0,01 lx przy F1.2, cz./b.: 0,001 lx przy F1.2	
Cechy kamery		
Oświetlacz IR	brak	
Funkcja dzień/noc	automatyczne przełączanie trybu pracy	
Balans bieli	automatyczny/ręczny	
Regulacja wzmocnienia	automatyczna/ręczna	
Redukcja szumów	3D	
Maskowanie	maks. 4 obszary prywatności	
Stabilizacja obrazu	tak, elektroniczna	
Funkcja Ultra Defog	tak	
Regulacja ostrości	tak	

Model		DH-IPC-HF81200EP	DH-IPC-HF81200EN
Obiektyw			
Rodzaj zamocowania		C/CS	
Parametry obrazu			
Kompresja		H.264/MJPEG	
Rozdzielczość		12M (4000×3000)/8M (3840×2160)/ 1080P (1920×1080)/720P (1280×720)/ D1 (704×576)/CIF (352×288)	
Liczba kl./s	główny strumień	12M (1~15fps)/ 8M/1080P (1~25/30fps)	
	drugi strumień	D1/CIF (1 ~ 25/30fps)	
	trzeci strumień	1080P/720P/D1 (1 ~ 50/60fps)	
Przepływność		dla H.264 od 32 kb/s do 96 Mb/s	
Funkcja ROI		maks. 4 obszary	
Parametry dźwięku			
Kompresja		G.711a/G.711u	
Interfejs		1 kanał wejściowy, 1 kanał wyjściowy, wbudowany mikrofon	
Inne zaawansowane funkcje			
Detekcja		przekroczenia umownej linii wtargnięcia na chroniony obszar zmiany ustawienia kamery porzuconych / znikających przedmiotów głośnych dźwięków twarzy	
Parametry sieciowe			
Interfejs Ethernet		RJ-45 (10/100/1000Base-T)	
Kompatybilność		ONVIF, PSIA, CGI	
Dodatkowe interfejsy			
Gniazdo pamięci		Mikro SD, maks. 128 GB	
RS485		1 port	
Wejścia/wyjścia alarmowe		2 wejścia, 1 wyjście	
Warunki pracy			
Zasilanie		12 V_{DC}/24 V_{AC}, PoE (802.3af)	
Pobór mocy		maks. 12 W (z włączonym ABF i ICR)	
Warunki środowiskowe		temperatura od -30°C do +60°C, wilgotność względna poniżej 95 %	

Producent:

Dahua Technology Co., Ltd.
1199' BinAn Road, Binjiang District
Hangzhou, China

tel.: +86-571-87688883, faks +86-571-87688815
e-mail: overseas@dahuatech.com
www.dahuasecurity.com

Kontroler ośmiu przejść bibi-K25

Charakterystyka urządzenia

Kontroler **bibi-K25** jest podstawowym elementem systemu kontroli dostępu i rejestracji czasu pracy bibinet-2.5.

Posiada zegar czasu rzeczywistego synchronizowany do internetowych serwerów czasu. Wbudowana pamięć pozwala na zapamiętanie 10000 kart, ich uprawnień i przechowywanie ostatnich 50000 zdarzeń. Dzięki temu kontroler bibi-K25 może pracować zarówno on-line jak i off-line.

Jego elastyczność pozwala na spełnienie dowolnych wymagań stawianych przed systemem kontroli dostępu. Posiada tylko dwa wyjścia przekaźnikowe, ale w rzeczywistości potrafi obsłużyć nawet 8 przejść. Jest to możliwe dzięki różnorodnym elementom dołączanym do jego wewnętrznej magistrali bibi-BUS zbudowanej w standardzie RS485. Magistrala ta pozwala na przesłanie w czasie rzeczywistym informacji z czytników do kontrolera, oraz przesyłanie do oddalonych modułów rozkazów sterowania przejściami.

Zarówno transmisja z komputerem poprzez sieć Ethernet, jak i cała transmisja po szynie bibi-BUS jest szyfrowana. Dla każdego połączenia, na podstawie indywidualnych kluczy danej instalacji generowane są klucze szyfrujące sesji.

Do magistrali bibi-BUS można dołączać:

– czytniki kart zbliżeniowych bibi-R40 i bibi-R50 – odporne na warunki atmosferyczne,
– czytniki kart z ekranem dotykowym LCD bibi-R42 i bibi-R52 dedykowane do ewidencji czasu pracy,
– terminale bibi-T40 i bibi-T50 - czytniki z wejściami kontrolnymi oraz z wyjściem do sterowania ryglem,
– moduły dodatkowych wejść/wyjść bibi-D51,
– moduły przeznaczone do obsługi czytników innych producentów,
– wyświetlacze czasu systemowego bibi-W50.

Cztery konfigurowalne wejścia kontrolne służą do podłączenia czujników otwarcia drzwi, przycisków wyjścia (lub kurtyny), czujek sabotażowych, alarmowych itp.

Kontroler bibi-K25 jest funkcjonalnym urządzeniem pozwalającym zaspokoić wymagania wielu projektantów, instalatorów i użytkowników systemów kontroli dostępu i ewidencji czasu pracy.

Dane techniczne

- Pamięć kart: 10 000
  - Podział kart: 256 grup i 256 pionów
  - Kalendarze: 16
  - Schematy czasowe: 256
  - Upoważnienia: stałe i przepustki
  - Pin kody: 4-6 cyfr
- Pamięć zdarzeń: 50 000
- Połączenie z komputerem: Ethernet
  - Protokół: TCP/IP
  - Prędkość transmisji: 10/100 Mbps
- Podłączenie czytników: bibiBUS (standard RS485)
- Wyjścia przekaźnikowe: 2 – NO 24 V/1 A (NC 24 V/0,6 A)
- Impuls otwarcia rygla: do 60 s
- Wejścia: 4 konfigurowalne
- Napięcie zasilania: 12 V
- Pobór prądu: 100 mA
- Wymiary: 90×71×58 mm
- Obudowa: DIN - 4M
- Środowisko pracy: -10°C…+40°C, IP 40

Produkcja:
MicroMade Gałka i Drożdż sp.j.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
http://www.micromade.pl

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

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

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

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

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

ul. Biskupińska 14, 30-732 **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 606/610, 81-855 **Sopot**
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

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

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

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

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

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

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

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

ALPOL Sp. z o.o.
ul. Ścigały 10
40-208 Katowice
tel. 32 790 76 56
faks 32 790 76 61
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

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

ul. Łęczycka 55, 85-737 **Bydgoszcz**
tel. 32 720 39 67
faks 32 790 76 85
e-mail: bydgoszcz@e-alpol.com.pl

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

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

ul. Opolska 18 klatka C parter, 31-323 **Kraków**
tel. 32 790 76 46
faks 32 790 76 73
e-mail: krakow@e-alpol.com.pl

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

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

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

ul. Oleska 99, 45-222 **Opole**
tel. 32 750 30 36
faks 32 750 30 38
e-mail: opole@e-alpol.com.pl

ul. Odolanowska 49a, 63-400 **Ostrów Wlkp.**
tel. 32 750 30 25
e-mail: ostrow@e-alpol.com.pl

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

ul. Zbrowskiego 100, 26-600 **Radom**
tel. 32 750 30 33
faks 32 750 30 35
e-mail: radom@e-alpol.com.pl

ul. 3 Maja 59, 81-850 **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. Rzymowskiego 34, 02-697 **Warszawa-Mokotów**
tel. 32 790 76 34
faks 32 790 76 69
e-mail: warszawa@e-alpol.com.pl

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

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

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

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

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

bt electronics sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 429 36 16
faks 12 410 85 11
e-mail: saik@saik.pl
www.saik.pl

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

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58
faks 52 387 54 66
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
faks 22 633 90 60
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

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

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

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 342 03 78
faks 71 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. 12 260 13 96
faks 12 260 13 95
e-mail: info@cma.com.pl

ul. Nowy rynek 2, 62-002 **Suchy Las k/Poznania**
tel. 61 861 40 51
faks 61 861 40 51
e-mail: poznan@cma.com.pl

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

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17
faks 22 546 19 78
e-mail: biuro@cs.pl
www.cs.pl

D-MAX Polska Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 822 60 52
e-mail: dmax@dmaxpolska.pl
www.dmaxpolska.pl

DAHUA TECHNOLOGY Co., Ltd.
No. 1199, Bin an Road, Bin jiang District
Hangzhou
P.R. China
P.C. 310053
e-mail: overseas@dahuatech.com
www.dahuasecurity.com

DG ELPRO
Z. Durlak, K. Durlak, J. Golonka Sp. J.
ul. Wadowicka 6
30-415 Kraków
tel./faks 12 263 93 85
e-mail: biuro@dgelpro.pl
www.dgelpro.pl

DMSI Software
ul. Kłobucka 23c/119
02-699 Warszawa
tel. 22 112 17 91
e-mail: biuro@dmsi.pl
www.dmsi.pl
www.safestar.pl

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

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00
faks 22 518 84 99
e-mail: sales@ebs.pl
www.ebs.pl

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

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. 22 398 96 53
faks 22 398 96 54
e-mail: elproma@elproma.pl
www.elproma.pl

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

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
Al. Jerozolimskie 133 lok. 13
02-304 Warszawa
tel./faks 22 115 71 50
e-mail: kontakt@estpolska.pl
www.estpolska.pl

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

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

GORKE ELECTRONIC Sp. z o.o.
ul. Staromiejska 31 B
43-200 Pszczyna
tel. 32 326 30 70
faks 32 447 73 30
e-mail: biuro@gorke.com.pl
www.gorke.com.pl

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

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

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

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

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

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

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

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

NUUXE RADIOTON Sp. z o.o.
Siedziba w Krakowie:
ul. Olszańska 5H
31-513 Kraków
tel. 12 393 58 00, 417 36 77
faks 12 393 58 02
e-mail: nuuxe@nuuxe.com
www.nuuxe.com

Biuro:
ul. Polska 43
81-337 Gdynia
tel. 58 621 55 21
faks 58 621 55 21
e-mail: gaszenie@nuuxe.com

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

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

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

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

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

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

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

RISCO Group
14 Hachoma Street
75655 Rishon LeZion
Izrael
tel. +972 396 37 777
faks +972 396 16 584
e-mail: info@riscogroup.com
www.riscogroup.com

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

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

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

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl
www.dmaxcctv.pl
www.samsungcctv.pl

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

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16
faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

SAMSUNG TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Marynarska 15
02-674 Warszawa
tel. 22 205 07 77
faks 22 205 07 63
www.samsung-security.pl

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
tel. 58 320 94 00
faks 58 320 94 01
e-mail: satel@satel.pl
www.satel.pl

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

SCHNEIDER ELECTRIC POLSKA Sp. z o.o.
ul. Konstruktorska 12
02-673 Warszawa
tel. 22 511 82 00
faks 22 511 82 02
e-mail: poland.helpdesk@schneider-electric.com
www.schneider-electric.pl

Oddziały:
ul. Galaktyczna 36A
80-299 **Gdańsk**

ul. Muchoborska 18
54-424 **Wrocław**

Budynek KBP100
ul. Krakowska 280
32-080 **Zabierzów**

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44A
02-672 Warszawa
tel./faks 22 33 00 620, 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

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

ul. Jasnogórska 23 lok. 17 (wejście od ul. Stawowej)
31-358 **Kraków**
tel. 12 637 11 74
krakow@schrack-seconet.pl

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

ul. Mydlana 1, 51-502 **Wrocław**
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

PRZEDSIĘBIORSTWO TECHNICZNO- HANDLOWE
SECURAL Jacek Giersz
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. 32 291 86 17
faks 32 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl

SEVITEL Sp. z o.o.
ul. Leopolda 29
40-189 Katowice
tel. 32 705 73 00
faks 32 705 73 99
e-mail: sevitel@sevitel.pl, handel@sevitel.pl
www.sevitel.pl

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

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

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

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

SPS Electronics Sp. z o.o.
ul. Krakowiaków 80/98
02-255 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spselectronics.pl
www.spselectronics.pl

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

al. Roździeńskiego 188a, 40-203 **Katowice**
tel. 32 255 64 27
faks 32 255 64 52
e-mail: katowice@spselectronics.pl

ul. Kamiennogórska 22, 60-179 **Poznań**
tel. 61 852 19 02
faks 61 825 09 03
e-mail: poznan@spselectronics.pl

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

Biuro Partnerskie SPS Partner
ul. Przybyszewskiego 199/205, 93-120 **Łódź**
tel. 42 617 00 32
e-mail: lodz@spspartner.pl

ul. Szosa Chełmińska 217A, 87-100 **Toruń**
tel. 56 653 99 43
faks 56 653 90 81
e-mail: torun@spspartner.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

UNICARD S.A.
ul. Łagiewnicka 54
30-417 Kraków
tel. 12 398 99 00
faks 12 398 99 01
e-mail: zapytania@unicard.pl
www.unicard.pl

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

Kontrolery autonomiczne przeznaczone do pracy w małych systemach kontroli dostępu

KaDe

- Zintegrowane z czytnikami kart UNIQUE, HID Prox (125 kHz) lub Mifare (13,56 MHz)
- Kontrola 1 przejścia jedno- lub dwustronnie
- Instalacja wewnątrz i na zewnątrz, dostępne modele wandaloodporne
- Łatwe programowanie za pomocą kart administratora, pilota na podczerwień lub wbudowanej klawiatury

KZC-300-U/H-white | KZC-300-U/H-black | KZ-400-U/H | KZ-500-U/H | KZ-600-U | KZ-700-U/H | KZC-800-U/H KZC-800-M | KZC-900-U/H

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS FIRE & SECURITY	–	TAK	TAK	TAK	TAK
Alarmnet	–	–	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	TAK	TAK	–	TAK
ASSA ABLOY	–	–	TAK	–	–
BOSCH	TAK	–	–	–	–
P.W.H. Brabork - Laboratorium	–	TAK	–	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	–	TAK	–	–
CBC (Poland)	–	–	TAK	–	TAK
CMA	TAK	TAK	–	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	–
D-MAX	–	–	TAK	–	–
DAHUA TECHNOLOGY	TAK	TAK	TAK	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	–
DMSI Software	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
EST POLSKA	TAK	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	–	TAK	–	TAK
GORKE ELECTRONIC	TAK	–	–	–	–
ICS POLSKA	–	TAK	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Janex International	–	–	TAK	–	–
KATON	–	–	TAK	–	TAK
Kolektor	–	TAK	TAK	TAK	–
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
Novatel	–	TAK	TAK	TAK	TAK
NUUXE RADIOTON	–	TAK	TAK	TAK	TAK
OMC INDUSTRIAL	–	–	TAK	–	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	–	TAK	TAK	–
RISCO Group	TAK	–	–	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	TAK
Samsung Techwin Europe	TAK	–	TAK	–	–
Satel	TAK	–	–	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schneider Electric Polska	–	–	TAK	–	–
Schrack Seconet Polska	TAK	TAK	TAK	–	TAK
Secural	TAK	TAK	TAK	–	TAK
Sevitel	–	–	TAK	TAK	–
SMA	–	TAK	–	TAK	–
SPS Electronics	–	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	TAK	TAK	–	TAK
UNICARD	TAK	TAK	–	TAK	TAK
W2	TAK	TAK	TAK	–	–

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, karty magnetyczne i zbliżeniowe								
AGIS FIRE & SECURITY	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarmnet	–	TAK	TAK	–	–	TAK	–	–	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	–	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	TAK	TAK	TAK	–	–	–	TAK	–	–
CBC (Poland)	–	TAK	–	–	–	–	–	–	–
CMA	TAK	TAK	TAK	–	–	TAK	TAK	–	–
CONTROL SYSTEM FMN	–	–	TAK	–	–	–	–	TAK	–
D-MAX	–	TAK	–	–	–	–	TAK	–	–
DAHUA TECHNOLOGY	–	TAK	TAK	–	–	–	–	–	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DMSI Software	–	–	–	–	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
EBS	transmitery GSM/GPRS/IP, systemy RFID i GPS, produkcja OEM/ODM, rozwiązania M2M								
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
EST POLSKA	–	TAK	TAK	–	–	TAK	TAK	–	–
FES	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	–	TAK	–
GORKE ELECTRONIC	TAK	–	–	–	–	–	TAK	–	–
ICS POLSKA	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
Janex International	TAK	TAK	TAK	TAK	–	–	–	–	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
Novatel	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
NUUXE RADIOTON	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	–	TAK	TAK	–	–	TAK
RETT-POL	TAK	–	TAK	TAK	–	–	TAK	–	–
RISCO Group	TAK	–	–	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung Techwin Europe	–	TAK	TAK	–	–	–	–	–	–
Satel	TAK	–	TAK	TAK	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Schneider Electric Polska	–	TAK	TAK	–	–	TAK	TAK	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Sevitel	–	–	TAK	TAK	–	TAK	–	TAK	–
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Tap – Systemy Alarmowe	TAK	TAK	TAK	–	TAK	TAK	–	–	–
UNICARD	–	–	TAK	TAK	–	TAK	–	–	–
W2	TAK	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

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

Skład i łamanie
Tomasz Kaczmarczyk

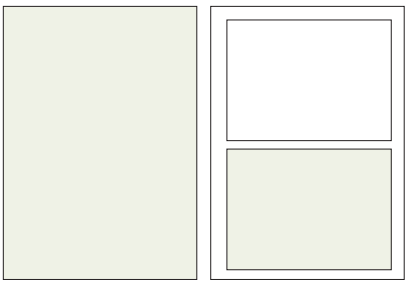
Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. 22 546 0 951, 953
faks 22 546 0 959
www.zabezpieczenia.com.pl

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

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

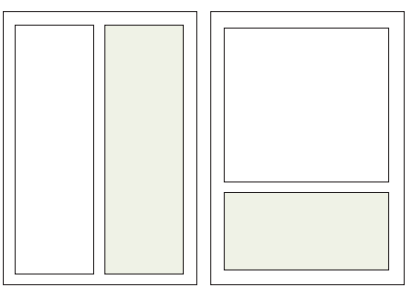
Dostępne formy reklamy

Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona


cała strona (200 x 282 mm + 3mm spad)
1/2 strony (170 x 125 mm)

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

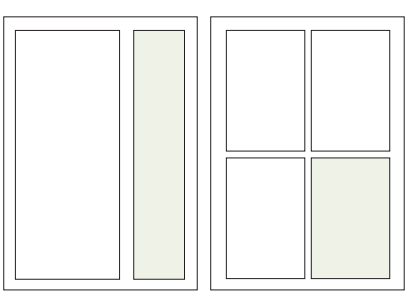
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)


1/2 strony (83 x 260 mm)
1/3 strony (170 x 80 mm)

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

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


1/3 strony (54 x 260 mm)
1/4 strony (83 x 125 mm)

Udostępniamy również powierzchnię reklamową na naszej sronie internetowej http://www.zabezpieczenia.com.pl

Spis reklam

4K

jakość i różnorodność w przystępnej cenie

Doskonała jakość obrazu, duże możliwości dekodowania

4K w przystępnej cenie

Wysoka jakość obrazu przy zachowaniu rozsądnej ceny

Różnorodność zastosowań 4K

Oferujemy różnorodne produkty, od najprostszych do najbardziej wyrafinowanych

Rekomendowane modele:

Kamera sieciowa 4K Ultra HD
IPC-HF81200E

Wandaloodporna kamera sieciowa 4K Ultra HD z obiektywem typu rybie oko i oświetlaczem pracującym w podczerwieni
IPC-EB(W)81200

Rejestrator sieciowy Super 4K, 128 kanałów, wysokość 2U
NVR608-128/608R-128-4K

Kamera sieciowa 4K Ultra HD w małej obudowie tubowej, z oświetlaczem pracującym w podczerwieni
IPC-HFW4800E

Kamera sieciowa 4K Ultra HD w małej obudowie kopułkowej, z oświetlaczem pracującym w podczerwieni
IPC-HDBW4800E

Rejestrator sieciowy 4K, 8/16/32 kanałów, wysokość 1U, 8 portów PoE
NVR4208/4216/4232-8P-4K

CE FC UL RoHS ISO 9001:2000

IFSEC 2015
16–18 Jun 2015 ExCel London, UK
Booth: E1300

DAHUA TECHNOLOGY CO., LTD.
No.1199 Bin an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

www.dahuasecurity.com


OUR PASSIONS BY
SCHRACK
SECONET
2015
Nasze pasje już znasz.
Jakie są Twoje ...?
www.schrack-seconet.pl