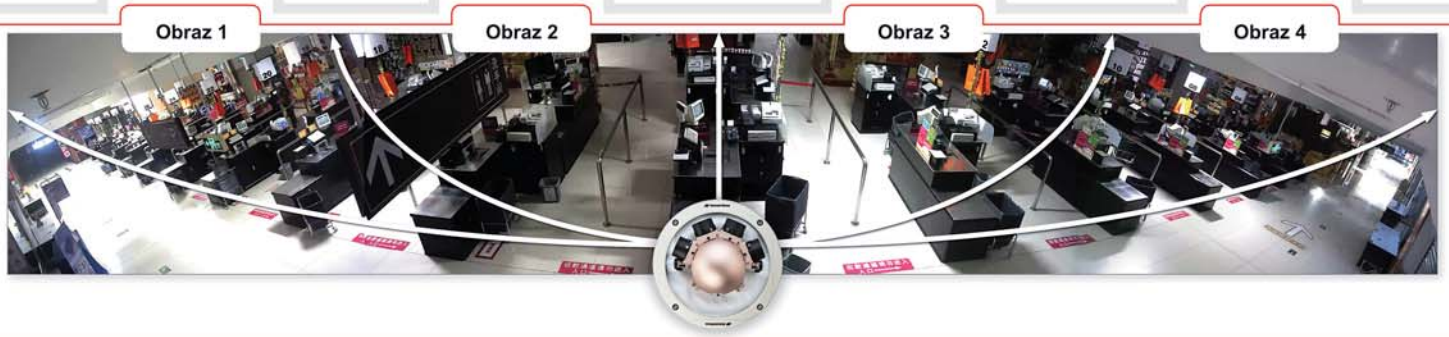
CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(102)/2015

ZABEZPIECZENIA

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



W NUMERZE:

FUJIFILM
Value from Innovation

Bezpieczeństwo w nowym wymiarze:

4K

Pierwszy obiektyw Fujinon typu Vari Focal

kremer kommunikation

Day Night

Nowy DV2.2x4.1SR4A-SA2L firmy Fujifilm
Doskonała rozróżnialności szczegółów dzięki rozdzielczości obrazu 4K.
Nadający się do użytku 24 godziny na dobę dzięki technologii dzień/noc.
Więcej informacji na stronie www.fujifilm.eu/fujinon lub per scan.
Fujinon. Widzisz więcej. Wiesz więcej.

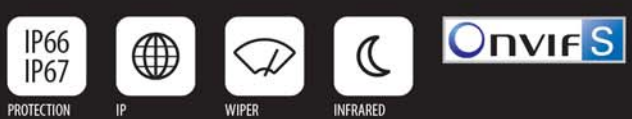
FUJINON

ULISSE COMPACT **HD**

RENOMOWANE I NIEZAWODNE URZĄDZENIE PTZ PRZEZNACZONE DO ZASTOSOWAŃ ZEWNĘTRZNYCH, AKTUALNIE DOSTĘPNE W WERSJI FULL HD 1080P!

ULISSE COMPACT HD jest kamerą sieciową PTZ Full HD 1080p, umożliwiającą uzyskanie obrazu wideo doskonałej jakości o wysokiej rozdzielczości. To zintegrowane urządzenie PTZ jest odporne na środowiska ekstremalne, gwarantuje dużą prędkość i dokładność detekcji obiektu w każdych warunkach.

ULISSE COMPACT HD jest idealnym rozwiązaniem przeznaczonym dla skomplikowanych zastosowań nadzoru, takich jak: kontrola ruchu drogowego i autostrad, nadzór graniczny, stadionów i budynków przemysłowych, więzień, instalacji wojskowych oraz nadzór granic obszarów.



PRODUCTS FOR CCTV | WWW.VIDEOTEC.COM | E-mail: info@videotec.com

VIDEOTEC

SPIS TREŚCI 02 2015

OCHRONA PRZECIWPOŻAROWA

KONTROLA DOSTĘPU

SSWiN

TELEWIZJA DOZOROWA

Wielofunkcyjne urządzenia firmy Videotec do zadań specjalnych

Włoski producent **Videotec**, przodujący w sprzedaży urządzeń zabezpieczających do zastosowań przemysłowych, może pochwalić się kompletnym asortymentem oferowanych urządzeń CCTV przeznaczonych do wszelakich zastosowań związanych z obserwacją miejsc znajdujących się na zewnątrz budynków. Urządzenia te są zarazem innowacyjne i atrakcyjne wizualnie. Działają w sposób niedościgniony.

Od kilku lat firma Videotec oferuje rozwiązania umożliwiające podniesienie poziomu bezpieczeństwa, które są całkowicie odmienne od tych dostępnych na rynku zabezpieczeń. Mają one zastosowania w transporcie lądowym i morskim oraz w branży naftowej. Stworzyła specjalistyczne urządzenia, których właściwości umożliwiają działanie w specyficznych warunkach i które pomyślnie przeszły przez złożone procedury certyfikacyjne.

Videotec oferuje usługi z zakresu wsparcia technicznego i rzeczoznawstwa, dotyczące zarówno doboru urządzeń, jak i zagadnień jakościowych. Proponuje rozwiązania, dzięki którym można uzyskać najbardziej opłacalny w danych warunkach poziom solidności i jakości działania wizyjnego systemu dozorowego.

Branża naftowa

Kilka przodujących przedsiębiorstw z branży naftowej, a także głównych międzynarodowych przedsiębiorstw farmaceutycznych, powierzyło ochronę swoich obiektów urządzeniom firmy Videotec.

Certyfikowane, iskrobezpieczne kamery PTZ i kamery stałopozycyjne firmy Videotec zapewniają najwyższy stopień zabezpieczenia i umożliwiają natychmiastowe sprawdzenie, co dzieje się w danym miejscu. Sprawdzają się w ważnych zadaniach, w miejscach narażonych na eksplozję i silną korozję. Mają solidną konstrukcję ze stali nierdzewnej, która zapewnia ciągłe działanie w najbardziej surowych i zmiennych warunkach pogodowych, i nie wymagają żadnej konserwacji.

Infrastruktury i transport

Dzięki dużemu asortymentowi oferowanych obudów do kamer i głowic PTZ Videotec jest w stanie sprostać najwyższym wymaganiom dotyczącym bezpieczeństwa publicznego, monitorowania infrastruktury i ruchu na drogach i autostradach, monitorowania centrów miast i nadzoru wizyjnego w zróżnicowanych wewnętrznie środowiskach.

Urządzenia ULISSE PTZ należą do najbardziej uznanych produktów firmy Videotec. Generują wyraźne obrazy z dużą liczbą widocznych detali w dzień i w nocy (także wówczas, gdy odległość od obserwowanych obiektów jest duża), mogą działać nieprzerwanie, umożliwiają precyzyjne pozycjonowanie kamer, reagują natychmiast na polecenia wydawane przez operatora, pozwalają na uproszczone zarządzanie dzięki możliwości zdalnej aktualizacji oprogramowania, łatwą instalację typu *plug and play* i mają otwartą architekturę umożliwiającą pracę w sieciach IP. Z powyższych właściwości urządzeń ULISSE PTZ wynikają konkretne korzyści w zastosowaniach związanych z transportem i kontrolą ruchu drogowego.

Tysiące urządzeń ULISSE PTZ firmy Videotec pracuje efektywnie w instalacjach CCTV na całym świecie. Urządzenia te mają właściwości umożliwiające eliminację ograniczeń typowych dla tradycyjnych szybkoobrotowych kamer kopułowych. Dzięki ich zastosowaniu można stworzyć znakomity system dozorowy, który sprosta ciężkim warunkom środowiskowym panującym w terenach otwartych i nie będzie wymagał żadnej konserwacji. Zapewniają bardzo dobrą jakość obrazu i perfekcyjnie śledzą obiekty bez względu na szybkość ich przemieszczania się i odległość. Dostępnych jest wiele modeli, dzięki czemu można dostosować system do różnych wymagań.

Na morzu i na lądzie

Oferując wiele specjalistycznych urządzeń służących do budowy wizyjnych systemów dozorowych, firma Videotec może pomóc w rozwiązaniu skomplikowanych problemów występujących w zastosowaniach morskich.

Wiele spośród urządzeń firmy Videotec zaprojektowano tak, aby były one odporne na korozję. Kamer PTZ i obudów ze stali nierdzewnej można używać w każdym środowisku morskim, na wszystkich rodzajach statków, np. na tankowcach, kontenerowcach, statkach przewożących skroplony gaz ziemny. Można też wykorzystać je w zastosowaniach przemysłowych oraz w tunelach drogowych.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

Zdalny pomiar temperatury
innowacyjna funkcja kamer Axis

Fot. 1. Kamery AXIS Q29 z funkcją zdalnego pomiaru temperatury pomagają wyeliminować ryzyko przegrzania

Seria **Axis Q29** to pierwsze kamery firmy Axis przeznaczone do zdalnego pomiaru temperatury urządzeń i obiektów, takich jak podstacje energetyczne czy serwerownie, a także newralgicznych miejsc, takich jak składy węgla.

Axis Communications, światowy lider w dziedzinie sieciowych rozwiązań wizyjnych, wprowadza na rynek nową serię kamer sieciowych umożliwiających zdalny nadzór nad zmianami temperatury. Są to kamery AXIS Q29 Temperature Alarm, które są dostarczane wraz z dwoma obiektywami przeznaczonymi do różnych zastosowań. Kamery mają rozdzielczość 336x256 i umożliwiają nadzór nad najważniejszymi obiektami i zdalny pomiar ich temperatury, zarówno na krótkich, jak i na długich dystansach.

– *Od momentu wprowadzenia na rynek pierwszej kamery termowizyjnej mieliśmy wiele zapytań dotyczących urządzeń, które pozwolą na detekcję zmian temperatury. Głównym przeznaczeniem tego typu kamer jest wykrywanie intruzów, ale służą one również do zdalnego nadzoru wizyjnego nad urządzeniami i najważniejszymi miejscami, takimi jak serwerownie lub magazyny* – powiedział **Jan Grusznic**, Sales Engineer w firmie Axis Communications. – *Kamera Q2901-E Temperature Alarm może być używana do całodobowego pomiaru temperatury urządzeń w celu wyeliminowania ryzyka przegrzania.*

Zastosowanie kamer Q2901-E i Q2901-E PT Mount umożliwia utworzenie wielu stref alarmowych wysyłających powiadomienia, gdy temperatura obserwowanych obiektów osiągnie poziom wyższy lub niższy od określonych wcześniej progów. Kamery mają również dodatkowe funkcje, które ułatwiają pracę operatorom systemów dozorowych, takie jak palety izotermiczne i punktowe pomiary temperatury. Pozwalają one uniknąć awarii poprzez wcześniejsze wskazanie obszarów zagrożonych przegrzaniem, zanim obszary te zostaną zauważone w inny sposób lub przegrzanie doprowadzi do zatrzymania pracy maszyn.

Dzięki instalacji z wykorzystaniem jednego kabla oraz zasilaniu metodą PoE (IEEE 802.3af) kamery z serii Q29 są łatwe w montażu i mogą być bezproblemowo zintegrowane z istniejącymi systemami bezpieczeństwa.

Kamera Q2901-E PT Mount jest wyposażona w port szeregowy umożliwiający komunikację w standardzie RS422/RS485 z głowicami uchylno-obrotowymi, które zapewniają nadzór nad dużym obszarem.

Kamera Q2901-E ma wspornik ścienny przystosowany do montażu na ścianie lub suficie, natomiast kamera Q2901-E PT Mount ma funkcję Corridor Format pozwalającą na uzyskanie obrazu o orientacji pionowej, odpowiedniego np. do nadzoru korytarzy, serwerowni czy też powierzchni magazynowych.

Kamery z serii AXIS Q29 są odporne na trudne warunki pogodowe, a ich obudowy zapewniają ochronę przed aktami wandalizmu i uderzeniami.

Kamery AXIS Q2901-E i AXIS Q2901-E PT Mount mogą współpracować z aplikacjami należącymi do największego w tej branży zbioru programów służących do zarządzania materiałem wizyjnym, który został utworzony w ramach Axis Application Development Partner Program, oraz z autorskim oprogramowaniem AXIS Camera Station. Współpracują również z platformami Axis Camera Companion, Axis Camera Application Platform oraz Axis Video Hosting System (AVHS) i są zgodne ze standardem ONVIF, dzięki czemu ułatwiają integrację z urządzeniami i oprogramowaniem innych producentów.

Kamery AXIS Q2901-E i AXIS Q2901-E PT Mount będą dostępne w pierwszym kwartale 2015 r. za pośrednictwem kanałów dystrybucyjnych firmy Axis.

Bezpośr. inf. Axis Communications

Otwarty system zarządzania bezpieczeństwem

Platforma SMS iProtect jest przykładem systemu zarządzania bezpieczeństwem, który zawiera interfejsy umożliwiające integrację z systemami zewnętrznymi. Zakres integracji zależy w głównej mierze od potrzeb inwestora i wymogów konkretnego projektu.

Najczęściej integracja dotyczy wizualizacji oraz odbioru informacji alarmowych z innych systemów bezpośrednio w platformie SMS iProtect. Dzięki niej operator może kontrolować stan wszystkich systemów za pomocą jednego oprogramowania zarządzającego. Często dokonywana jest również synchronizacja baz użytkowników i uprawnień, która usprawnia procesy zarządzania systemem. Dzięki otwartym interfejsom integracja może być realizowana zarówno przez firmę **C&C Partners**, jak i samodzielnie – przez klienta.

Ostatnio udostępnione zostały cztery interesujące interfejsy, dzięki którym możliwa jest integracja z następującymi systemami zewnętrznymi:

– systemem sterowania windami KONE,
– systemem sygnalizacji pożarowej Schrack-Seconet,
– systemem zarządzania kluczami Hartmann-Tresore,
– systemem zarządzania kluczami Protector.

Platforma iProtect jest zintegrowana także z wieloma systemami innych producentów. Jej rozszerzenie o dodatkowe funkcje integracyjne zwiększa efektywność działań operatorów i skraca czas podejmowania decyzji w momencie zajścia zdarzenia alarmowego.

Bezpośr. inf. C&C Partners

Dahua wprowadza kamery HDCVI drugiej generacji

Firma **Dahua Technology**, przodujący producent i dostawca urządzeń do wizyjnych systemów dozorowych z siedzibą w Hangzhou w Chinach, wprowadziła na rynek kamery HDCVI drugiej generacji, czyniąc tym samym krok w kierunku upowszechnienia standardu HD over Coax 2.0.

– Wprowadzenie na rynek urządzeń zgodnych ze standardem HD over Coax 2.0 świadczy o pierwszoplanowej roli firmy Dahua w dziedzinie innowacyjnych, analogowych wizyjnych systemów dozorowych o wysokiej rozdzielczości – powiedział **Tim Shen**, dyrektor handlowy firmy Dahua Technology. – *Coraz szersza akceptacja naszych produktów oraz pozytywne informacje zwrotne docierające do nas z rynku stanowią siłę napędową pozwalającą nam na wprowadzanie kolejnych innowacji przynoszących wymierne korzyści użytkownikom systemów dozorowych.*

Kamery HDCVI drugiej generacji są wyposażone w przetwornik obrazowy o bardzo dobrych parametrach oraz w chipset DH5000 zawierający zarówno procesor sygnałowy ISP, który służy do obróbki obrazu, jak i koder TX służący do transmisji sygnału wizyjnego, dzięki czemu uzyskano znaczną poprawę jakości obrazu w stosunku do wcześniejszych modeli. Nowe kamery wytwarzają obraz w formacie 720p lub 1080p i mogą być wykorzystane zarówno w dziennych, jak i w nocnych warunkach oświetleniowych.

Rozszerzony zakres dynamiki tych kamer pozwala na uzyskanie obrazu o znakomitej jakości podczas obserwacji scen odznaczających się wysokim kontrastem. W kamerach HDCVI drugiej generacji zostały zachowane funkcje wprowadzone we wcześniejszych modelach, takie jak przełączanie trybów pracy (HD/SD) czy menu ekranowe.

W celu jeszcze lepszego spełnienia oczekiwań poza kamerami wyposażonymi w obiektywy o stałej ogniskowej oferowane są kamery z obiektywami typu vari-focal oraz długo oczekiwane kamery z obiektywami o zmiennej ogniskowej, regulowanej w zakresie

od 2,7 mm do 12 mm za pomocą silnika. W ostatnim z wymienionych przypadków firma Dahua wykorzystuje zoptymalizowane algorytmy umożliwiające poprawę dokładności i przyspieszenie pracy układu automatycznej regulacji ostrości obrazu.

W sumie wprowadzonych zostało siedem nowych modeli kamer różniących się wyglądem i konstrukcją mechaniczną, w tym kamery w obudowach kulistych, tulejowych oraz kopułkowych, o stopniu szczelności IP66 oraz klasie odporności na udary IK10. Są one w stanie pracować w trudnych warunkach środowiskowych i są zabezpieczone przed skutkami sabotażu.

Kamery zgodne z zatwierdzonym przez stowarzyszenie HDcctv Alliance standardem HDCVI 2.0 wykorzystują technologię HDCVI opracowaną przez firmę Dahua i mogą współpracować na zasadzie *plug and play* z dowolnymi rejestratorami wizyjnymi zgodnymi z tym standardem, niezależnie od tego, kto jest ich producentem. – *Dahua jest firmą promującą ideę interoperacyjności urządzeń i popierającą kooperację między firmami zrzeszonymi w stowarzyszeniu HDcctv Alliance, co pozwala na przyspieszenie prac związanych z opracowywaniem nowych urządzeń oraz przyczynia się do wzrostu zadowolenia klientów czerpiących wymierne korzyści z zainstalowanych systemów dozorowych o wysokiej rozdzielczości* – dodał Shen.

Bezpośr. inf. Dahua Technology
Tłumaczenie: Redakcja

G-Scope/8000 – Expert Server firmy Geutebrück

Nie ma rzeczy niemożliwych – **G-Scope/8000**, Expert Server z rodziny urządzeń G-Scope służących do rejestracji obrazów i zarządzania materiałem wizyjnym, oferuje maksymalną redundancję oraz niemal nieograniczoną wszechstronność i skalowalność. Stanowi idealny komponent specjalistycznych wizyjnych systemów dozorowych, które spełniają najwyższe wymagania użytkowe i są stosowane w obiektach o wysokim poziomie ryzyka, takich jak zakłady karne czy kasyna.

64-bitowe oprogramowanie G-Core zapewnia urządzeniom G-Scope najwyższą efektywność. Akceleracja z wykorzystaniem procesora graficznego umożliwia 3-krotne przyspieszenie przetwarzania obrazu, a dualna struktura bazy danych gwarantuje błyskawiczny dostęp do zapisanych danych oraz zabezpiecza przed próbami manipulacji. Uzupełnieniem całości jest zintegrowany system analizy obrazu – detekcja aktywności (powodująca uruchomienie rejestracji na skutek wykrycia jakiegoś zdefiniowanego zdarzenia) oraz weryfikacja wyglądu sceny (umożliwiająca wykrywanie prób sabotażu przez zmianę ustawienia kamer) należą do standardowego zestawu funkcji. Funkcje analizy treści obrazu w trudnych warunkach środowiskowych (algorytmy VMD i VMX) oraz automatycznego odczytu numerów rejestracyjnych pojazdów mogą być dostosowane do indywidualnych wymagań.

G-Scope/8000 wyróżnia się wysokim poziomem niezawodności. Ustanawia nowe standardy, gdyż w skład podstawowego wyposażenia wchodzą redundantne dyski SSD z systemem operacyjnym, redundantne zasilacze i wentylatory, a także zintegrowana macierz RAID. Konstrukcja mechaniczna zapewnia skalowalność systemu, w którym zastosowano te serwery – każde z urządzeń ma wysokość od 1 do 3 jednostek U i jest wyposażone w 4, 8 lub 16 kieszeni na twarde dyski. Istnieje także możliwość podłączenia dodatkowych, zewnętrznych macierzy RAID i JBOD.

Ze względu na możliwość jednoczesnej rejestracji obrazów ze 128 kamer IP urządzenie G-Scope/8000 może stanowić samodzielnie funkcjonujący składnik wizyjnych systemów dozorowych lub wchodzić w skład dużych, zintegrowanych systemów sieciowych.

Bezpośr. inf. Arpol

Ekonomiczna linia kamer 3 Mpx serii 3000 marki NOVUS

W poprzednim numerze *Zabezpieczeń* zaprezentowano **kamery IP serii 3000** marki **NOVUS** o rozdzielczości 3 Mpx, które generują obraz z prędkością 30 kl./s. Dla systemów spełniających jedynie podstawowe wymagania, gdzie monitorowane procesy nie mają dynamicznego charakteru, proponujemy nowe kamery z przetwornikiem CMOS o rozdzielczości 2048×1536 pikseli i prędkości odświeżania 15 kl./s. Dla standardowych, typowych zastosowań (biura, hale logistyczne, hotele etc.) te parametry są wystarczające. Przy odświeżaniu obrazów z prędkością 15 kl./s obserwator ma wrażenie zlewania się ze sobą kolejnych obrazów i tym samym płynnego ruchu.

Wszystkie opisywane kamery mają funkcję rozszerzania zakresu dynamiki, dzięki czemu doskonale sprawdzą się w przeszklonych budynkach, gdzie często występuje kontrastowe oświetlenie monitorowanych obiektów. Można ustalić wiele reakcji kamer na zdarzenia alarmowe: wysłanie e-maila z załącznikiem, zapis plików na serwerze FTP oraz zapis plików na kartach micro SD/SDHC (NVIP-3DN3014V/IR-1P). Kamery współpracują z aplikacją NMS (Novus Management System) przeznaczoną do rejestracji materiału wizyjnego, podglądu na żywo, odtwarzania zarejestrowanych obrazów oraz zdalnej konfiguracji sieciowych urządzeń wizyjnych. Kamery generują równocześnie maksymalnie trzy strumienie wizyjne, w tym strumień z kompresją MJPEG. Można je zintegrować z innymi systemami bezpieczeństwa poprzez komendy CGI.

Wśród dostępnych modeli są kamery w obudowach określanych mianem *bullet* oraz wandaloodporne kamery kopułowe. Kamera kopułowa NVIP-3DN3012V/IR-1P ma płaską szybę, dzięki czemu wyeliminowane są zniekształcenia występujące w przypadku zastosowania standardowych kloszy sferycznych. Kamery występują w wersjach z obiektywami ze stałą ogniskową równą 4 mm i liczbą przysłony równą F:1,6 lub z obiektywami ze zmienną ogniskową regulowaną w zakresie od 2,8 mm do 12 mm i liczbą przysłony równą F:1,4. Wszystkie kamery zostały wyposażone w promienniki o zasięgu 25 m zbudowane z diod LED (maks. 42 sztuki). Co bardzo ważne, w menu kamery oświetlacz podczerwieni można wyłączyć. Ta funkcja jest szczególnie przydatna w przypadku instalacji kamer w obiektach o dobrym oświetleniu oraz w przypadku występowania odbić światła od elementów obserwowanej sceny. Przy instalacji kamer w trudnych warunkach oświetleniowych można ręcznie sterować migawką, aby uzyskać prawidłowe ustawienia ekspozycji.

Szczegółowe informacje o modelach NVIP-3DN3011H/IR-1P, NVIP-3DN3012H/IR-1P, NVIP-3DN3012V/IR-1P, NVIP-3DN3013V/IR-1P i NVIP-3DN3014V/IR-1P są dostępne na stronie *www.novuscctv.pl*.

Bezpośr. inf. Patryk Gańko

NOVUS®
Profesjonalne rozwiązanie dla systemów zabezpieczeń

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

AGIS wykonawcą instalacji niskoprądowych w biurowcu Q22

Firma **AGIS Fire & Security** podpisała umowę z przodującym polskim deweloperem Echo Investment i wkrótce wykona wszystkie systemy niskoprądowe w 155-metrowym biurowcu Q22 zlokalizowanym w biznesowym centrum Warszawy.

W obiekcie oferującym około 50000 m^2 powierzchni biurowej AGIS Fire & Security wdroży m.in. systemy kontroli dostępu, systemy sygnalizacji pożarowej, dźwiękowe systemy ostrzegawcze, systemy dozoru wizyjnego, systemy sygnalizacji włamania i napadu. Firma zainstaluje także interkomy i wideomofony oraz wykona okablowanie strukturalne. Rozpoczęcie prac planowane jest na połowę lutego.

Fot. Biurowiec Q22 (źródło: Echo Investment)

Biurowiec Q22 powstaje w miejscu dawnego hotelu Mercure, przy skrzyżowaniu al. Jana Pawła II i ul. Grzybowskiej. Projekt budynku powstał w renomowanej pracowni architektonicznej Kuryłowicz & Associates we współpracy z Buro Happold Polska. Lokalizacja, wysmakowana architektura oraz wysoki standard budynku sprawiają, że będzie to jeden z najbardziej prestiżowych biurowców w Warszawie.

Bezpośr. inf. Karolina Olechowicz
AGIS Fire & Security

Dahua i Exar podpisują pierwszą umowę licencyjną dotyczącą HDCVI

Firma **Dahua Technology** z siedzibą w Hangzhou (Chiny) – przodujący producent i dostawca urządzeń do nadzoru wizyjnego – ogłasza podpisanie strategicznej umowy z firmą **Exar**, która w efekcie będzie uprawniona do wykorzystania HDCVI (High Definition Composite Video Interface). Zgodnie z warunkami tej umowy Exar otrzymuje licencję na projektowanie, produkowanie i sprzedawanie swoich produktów wykorzystujących HDCVI.

Jako twórca i właściciel patentu firma Dahua uczyniła HDCVI światowym otwartym standardem, umożliwiając pełny dostęp do niego osobom trzecim, w tym konkurencyjnym przedsiębiorstwom. Współpraca z HDcctv Alliance umożliwi producentom przyczynienie się do wprowadzenia i rozpowszechnienia HDCVI 2.0.

Zhu Jiangming, wiceprezes wykonawczy w Dahua Technology, zwraca uwagę na to, że od kiedy HDCVI jest światowym standardem, a nie tylko jednym z analogowych rozwiązań HD, firma Dahua jest jeszcze bardziej pewna, że telewizja analogowa ma przed sobą przyszłość. Współpraca z Exarem to jeszcze jeden dobry przykład naszej otwartości i silnej determinacji.

– Dzięki zastosowaniu interfejsu HDCVI w analogowych kamerach i rejestratorach wizyjnych można czerpać korzyści z obrazu o wysokiej rozdzielczości niewielkim kosztem. HDCVI umożliwia transmisję sygnału wizyjnego o wysokiej rozdzielczości na odległość przekraczającą 500 metrów standardowym kablem koncentrycznym – skomentował **Louis DiNardo**, prezes i dyrektor generalny w firmie Exar.

Exar dołącza do Dahuy, aby opowiedzieć się po stronie HDCVI podczas ustanawiania przemysłowego standardu, z którym mają być zgodne analogowe urządzenia do nadzoru wizyjnego umożliwiające uzyskanie wysokiej rozdzielczości obrazu. Obydwie firmy są członkami HDcctv Alliance, który promuje wykorzystywanie i dostosowywanie się producentów do standardu HDCVI. Urządzenia Exara wykorzystujące HDCVI są w pełni zgodne ze standardem HDCVI 2.0, co przekłada się na ich działanie i współpracę z innymi urządzeniami zgodnymi z tym samym standardem. Pierwszy produkt firmy Exar wykorzystujący HDCVI – moduł kamerowy generujący obraz w trybie 1080p – będzie wkrótce zademonstrowany.

– Analogowe wizyjne systemy dozorowe, które zapewniają rozdzielczość HD, mogą być niezawodne i niekłopotliwe w eksploatacji, a ich ceny mogą być równie przystępne jak ceny systemów oferujących niższą rozdzielczość. Umowa firm Dahua i Exar zapoczątkowuje nowy etap w wykorzystywaniu analogowych metod transmisji sygnału wizyjnego. Wkrótce producenci sprzętu będą mieli możliwość wyboru dostawców komponentów przeznaczonych do produkcji urządzeń zgodnych ze standardem HDCVI 2.0. Obustronne zobowiązanie firm Dahua i Exar przyniesie korzyść producentom i użytkownikom końcowym – powiedział **Todd Rockoff**, dyrektor wykonawczy w **HDcctv Alliance**.

Bezpośr. inf. Dahua Technology
Tłumaczenie: Redakcja

Geutebrück oraz RISCO Group łączą siły w celu opracowania kompleksowego systemu sterowania i kontroli

Geutebrück ogłasza rozpoczęcie współpracy z **RISCO Group**, przodującym dostawcą zintegrowanych rozwiązań z zakresu bezpieczeństwa.

Dzięki współpracy obie firmy mogą zaoferować najwyższej klasy zintegrowany system sterowania i kontroli, stanowiący połączenie najnowszego rozwiązania CCTV firmy Geutebrück z platformą zintegrowanego bezpieczeństwa i zarządzania budynkiem SynopSYS dostarczaną przez RISCO Group. Partnerzy i użytkownicy końcowi odniosą korzyści dzięki zaawansowanym funkcjom sterowania, lepszym możliwościom przeglądu sytuacji i większej zdolności reagowania na naruszenia zabezpieczeń, która umożliwia szybką i adekwatną reakcję na wszelkie zagrożenia. Kolejną zaletą jest zmniejszenie sumarycznych kosztów wdrożenia i eksploatacji systemu dzięki jego wysokiej wydajności, która wynika z tego, że wszystkie informacje są przekazywane za pośrednictwem jednego interfejsu.

Owocna wspólna praca nad znaczącym europejskim projektem umożliwiła integratorom systemów z obu firm wdrożenie zintegrowanego systemu zarządzania bezpieczeństwem. Jest to reakcja na popyt, a synergia firm pozwoliła osiągnąć jeszcze lepsze wyniki. Kompleksowy system sterowania i kontroli, stanowiący połączenie najnowszego rozwiązania CCTV firmy Geutebrück GmbH z platformą zintegrowanego bezpieczeństwa i zarządzania budynkiem SynopSYS dostarczaną przez RISCO Group, jest już dostępny dla integratorów.

Więcej informacji na stronie *www.geutebrueck.com.*

Bezpośr. inf. Arpol

Seminarium projektowe „Integracja 2015” podsumowanie

W dniach 5–6 lutego 2015 roku w hotelu Turówka w Wieliczce odbyło się seminarium projektowe **„Integracja 2015”** zorganizowane przez firmy **AxxonSoft Polska, Honeywell Life Safety** oraz **TAP-Systemy Alarmowe**. Było to drugie tego typu spotkanie.

Celem seminarium było omówienie kluczowych zagadnień związanych z projektowaniem zintegrowanych systemów bezpieczeństwa wykorzystujących centrale Galaxy Dimension, oprogramowanie Axxon Intellect oraz urządzenia SSP Esser. Uczestnicy mieli okazję poznać najnowsze funkcje systemów Galaxy Dimension, SSP Esser oraz PSIM Axxon Intellect, gdyż część seminaryjna była połączona z prezentacją sprzętu. W godzinach wieczornych odbyło się spotkanie integracyjne połączone z uroczystą kolacją.

Redakcja

Wybrane zagadnienia dotyczące projektowania systemów wykrywania dymu z czujkami zasysającymi

Beata Idziak
Mariusz Konik
Andrzej Obłój

Niniejszy artykuł jest rozwinięciem publikacji *Projektowanie instalacji z zasysającymi czujkami dymu* z numeru 6/2013 *Zabezpieczeń*, w której omówione zostały parametry i zagadnienia podstawowe, takie jak priorytetowe traktowanie otworów, odróżnianie czułości otworu od nastawy czujki, efekt kumulacyjny, zrównoważenie orurowania, zwracanie uwagi na tło. Tym razem chcemy się zająć zagadnieniami praktycznymi, istotnymi dla projektanta i instalatora, których znajomość pozwoli lepiej wykorzystać zalety czujek zasysających. Naszym celem nie jest szkolenie Czytelników. Chodzi raczej o pokazanie za pomocą przykładów, jak wiedza oraz informacje uzyskane od przyszłego użytkownika systemu pozwalają uniknąć problemów oraz obniżyć koszty instalacji i serwisu

Optymalizacja systemów zasysających

Specyfiką technologii zasysania jest to, że opiera się na mechanice płynów. Nie jest to dziedzina wiedzy popularna wśród projektantów systemów elektrycznych. Systemy zasysające są charakteryzowane przez wiele parametrów. Zmiana każdego z nich pociąga za sobą zmianę wszystkich innych. Optymalizacji systemów zasysających dokonuje się metodą kolejnych przybliżeń. Jest to żmudne i czasochłonne. Niedoświadczony projektant zaczyna od rozwiązania, które jest dalekie od optymalnego. W praktyce oznacza to, że do ochrony danego obiektu użyje większej liczby czujek. Jeśli nie ma czasu na optymalizację systemu, to inwestor kupi więcej sprzętu niż potrzeba. Przykład z życia wzięty: w projekcie, w którym zaproponowano 21 czujek, po optymalizacji dokonanej z udziałem doświadczonego projektanta zostało tylko 7.

Wykonywanie rurociągów

Rury w systemach zasysających, wykonane z ABS-u lub PCW, łączy się przez klejenie płynnym klejem do twardych

tworzyw sztucznych. Najłatwiej to zrobić źle – nakładając klej do środka mufy łączącej. Przy takim klejeniu klej utworzy w każdym połączeniu kryzę albo błonę utrudniającą bądź zupełnie blokującą przepływ powietrza. Pół biedy, gdy rura zostanie zaklejona, bo będziemy o tym wiedzieć. Jeśli jednak przy każdej mufie, łuku, trójniku są tylko nieznaczne kryzy, to możemy tego nie wykryć. Przepływ powietrza w rurze będzie jednak znacznie mniejszy niż projektowany, bo kryz będzie dużo. W systemach zasysających przepływ w bardzo istotny sposób wpływa na parametry wykrywcze instalacji. W omawianym przypadku wykrycie nastąpiłoby później. Instalację trzeba będzie naprawić, wycinając wszystkie połączenia. W miejscu trójnika musimy wstawić nowy trójnik i trzy mufki.…

Największy wpływ na koszt i parametry wykrywcze instalacji ma projekt i wykonanie orurowania. Stworzenia projektu i wykonania orurowania nie powinno się zlecać podwykonawcom w celu lokalnej optymalizacji kosztów, bo całkowity koszt instalacji może się zwiększyć. Może też być inaczej – koszty instalacji będą niskie, ale zagrożenie będzie wykrywane zbyt późno.

Podstawowe zasady projektowania zasysających czujek dymu

Na rozprzestrzenianie się dymu w obiekcie ma wpływ wiele czynników, ale na pewno nie użyta technika wykrywania zagrożenia. Dlatego w wielu instalacjach można rozmieszczać otwory zasysające, korzystając z wytycznych dla czujek punktowych.

Otwory zasysające to, w przybliżeniu, konwencjonalne czujki punktowe bez wskaźników zadziałania (o adresowalnych czujkach zasysających można przeczytać w numerze 6/2014 *Zabezpieczeń*). Stąd wynikają ograniczenia przestrzeni, która może być chroniona jednym detektorem zasysającym.

Pod wieloma względami otwory ssące są dogodniejsze niż czujki punktowe – mogą być umieszczane w miejscach, w których są silne przepływy powietrza, albo tam, gdzie nie ma miejsca na czujki punktowe. Mogą one być skierowane poziomo, można je dowolnie umiejscowić oraz łatwo i tanio zmienić ich lokalizację.

Specyfikacja parametrów technicznych czujek zasysających

Czujki zasysające mają wiele istotnych parametrów, które wzajemnie na siebie wpływają. Czytając ulotkę, można przecenić możliwości czujki, ponieważ parametry podawane są ndywidualnie, bez związku z innymi cechami. Niestety, mieszanka techniki i marketingu nie tworzy właściwego źródła informacji dla projektanta. Trzeba uwzględniać publikacje producenta dotyczące konkretnego zastosowania oraz ograniczenia wprowadzone w programach narzędziowych. Często okazuje się, że parametry czujek są skromniejsze niż te, które zostały przedstawione w ulotkach.

Dla przykładu: długości rur mogą być różne dla różnych klas detekcji, odległość najdalej położonego otworu może okazać się znacznie mniejsza niż dopuszczalna długość rury, a klasę A (patrz *Klasy detekcji*) uzyskuje się przy nastawie czułości detektora na granicy tła.

Parametry czujki a jej zastosowanie

Dobór zasysających czujek dymu powinien opierać się głównie na analizie warunków środowiskowych, w których będą one pracować. Nie istnieje czujka, która jest najlepsza dla każdego obiektu. Trzeba dobrać czujkę do konkretnego zastosowania. Na przykład w miejscach, w których są silne przepływy powietrza, (serwerownia, szyb windowy) czujka powinna mieć silny wentylator. W serwerowni ważnym parametrem jest maksymalna liczba otworów zasysających w klasie A, a dopuszczalna długość rur jest w praktyce nieistotna.

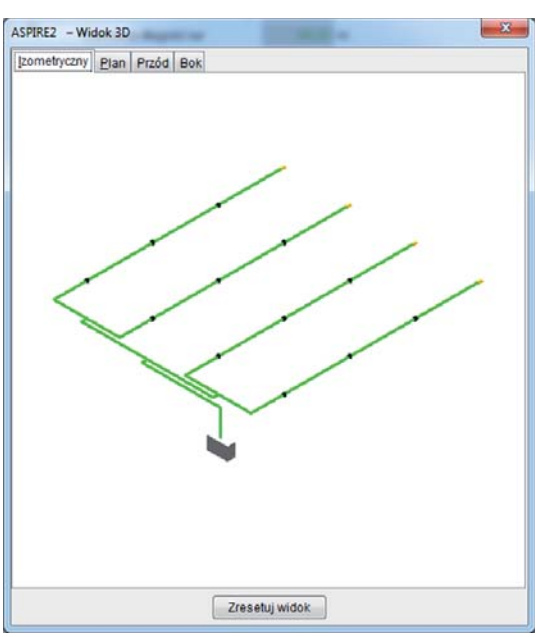
W magazynie wysokiego składowania bardzo wygodne są długie kapilary. Jeśli system umożliwia stosowanie wielometrowych kapilar, to należy tę cechę wykorzystać.

Wyobraźmy sobie magazyn bardzo wysokiego składowania chroniony zgodnie z wymaganiami VdS, według których co 6 m w pionie musi być warstwa otworów zasysających. Czy oznacza to albo kolumnadę rur pionowych z otworami co 6 m, albo warstwy rur poziomych co 6 m? Niekoniecznie. Projektuje się rurę z otworami na wysokości 12 m, a kapilary rozprowadza się w dół na 6 m oraz w górę na 18 m. Następna warstwa rur jest dopiero na wysokości 30 m, kapilary rozprowadza się w dół na 24 m, w górę na 36 m itd.

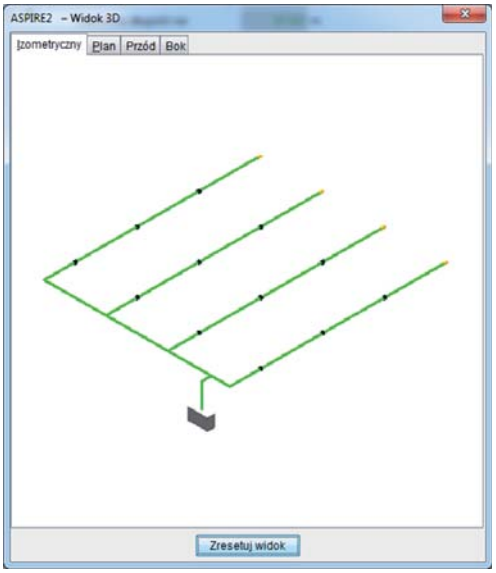
Projektowanie przebiegu orurowania

Chyba najbardziej czasochłonnym etapem projektowania jest wprowadzanie orurowania do programu służącego do obliczania przepływów w systemie zasysającym. Może dlatego w wielu projektach spotyka się konfiguracje, które są łatwiejsze do wpisania do programu, ale mniej korzystne z punktu widzenia przepływów.

Jak podzielić jedną rurę na cztery? Bardzo często jest to kaskada widełek (rys. 1). Takie rozwiązanie jest łatwe do zaprojektowania, ale wydłuża rury. Są tu odcinki, które zawracają. Zamiast tego zróbmy gałęzie odchodzące od głównej rury, jak na rysunku 2. W obu rozwiązaniach parametry wykrywcze są porównywalne, ale w tym, które przedstawiono



Rys. 1. Typowe dzielenie rury na widełki (powielanie konfiguracji U)



Rys. 2. Rozwiązanie, dzięki któremu można lepiej wykorzystać możliwości czujki – gałęzie odchodzące od głównej rury

na rys. 2, orurowanie jest krótsze. Czasem taka różnica decyduje o liczbie czujek, których trzeba użyć.

W celu właściwego zaprojektowania rurociągu, w szczególności wówczas, gdy mamy do czynienia ze skomplikowanym, niestandardowym układem rur, niezbędne jest korzystanie z profesjonalnego narzędzia programowego, uwzględniającego wszystkie kluczowe parametry techniczne oraz ograniczenia wynikające z obowiązujących norm (w Europie – EN54-20).

Z przebiegiem orurowania związany jest problem przenoszenia wyników obliczeń z jednego detektora na inny, innego producenta. Jeśli projekt był wykonany zgodnie z regułami sztuki, czyli najpierw rozmieściliśmy otwory zasysające w miejscach, gdzie spodziewamy się skutecznego wykrywania dymu, to oczywiście można „przenieść" rozmieszczenie otworów. Czy można „przenieść" przebieg orurowania? Tego nie można jednoznacznie powiedzieć. Nieskomplikowane układy orurowania często dadzą się „przenieść". Jeśli jednak projektant wykorzystał unikalne cechy jakiegoś systemu, na przykład długie kapilary, to układ rur trzeba zaprojektować od nowa.

Koniecznie trzeba ponownie obliczyć średnice otworów i parametry wykrywcze narzędziem dostawcy użytego systemu. Czujki zasysające mają tak różne parametry i pracują z tak różnymi przepływami i nastawami, że założenie, że parametry te są uniwersalne, jest błędne.

Zastosowanie czujek zasysających w trudnych warunkach środowiskowych

Czujki zasysające są coraz częściej stosowane w trudnych warunkach środowiskowych. Projektant podejmujący się opracowania projektu systemu zasysającego dla zakładu przemysłu ciężkiego, włókienniczego, spożywczego itp. powinien mieć wiedzę na temat technologii stosowanej w danym zakładzie i umieć przewidzieć najgorsze warunki pracy czujki.

Użytkownicy obiektów brudnych wiedzą, jakiego rodzaju i wielkości są cząstki zanieczyszczeń występujących w ich zakładzie. Projektant powinien uzyskać informacje na ten temat i wziąć je pod uwagę przy projektowaniu systemu wykrywania pożaru.

Jeśli przewidzimy, że możemy mieć wodę w rurach zasysających, to możemy się przed nią łatwo zabezpieczyć. Rury muszą dochodzić do czujki od dołu. Trzeba zainstalować pułapki na wodę. Czy to już wszystko? Tak łatwo? A jeśli rury będą ułożone nierówno? Każde lokalne obniżenie rury utworzy syfon... Zbierająca się w nim woda będzie zmniejszać przepływ powietrza. Trzeba więc układać rury ze spadkiem, bez lokalnych obniżeń w celu omijania podciągów itd. Nie ma w tym niczego trudnego, tylko trzeba to wszystko przewidzieć...

Znacznie więcej problemów sprawiają zanieczyszczenia powietrza. Trzeba wybierać czujkę pod kątem filtracji określonych zanieczyszczeń, na przykład wziąć pod uwagę to, czy ma filtr cząstek włóknistych i filtr cząstek ciężkich. Zwykły filtr piankowy nie zatrzyma cząstek ciężkich, a zanieczyszczenia włókniste zatkają go bardzo szybko. Kolejne pytania: czy stan filtru jest monitorowany przez czujkę? Jak duży jest filtr? Ile zanieczyszczeń pomieści? Jeśli wybierzemy czujkę przeznaczoną do zastosowań przemysłowych, to uciążliwość serwisu znacznie się zmniejszy.

W miejscach brudnych musimy przewidzieć przedmuchiwanie rur. Ochrona czujki to jedno zagadnienie, a ochrona rur to drugie. Automatyczne systemy przedmuchiwania są bardzo drogie, ale czasem są być albo nie być instalacji. Czujki zasysające pozwalają chronić obiekty bardzo brudne, a serwis jest stosunkowo prosty, pod warunkiem, że projektant przewidzi niezbędne czynności instalatora, a instalator wykonuje je regularnie.

Czujki zasysające są urządzeniami elektromechanicznymi. Wymagają bardziej starannego serwisu niż czujki punktowe lub liniowe. Źle zaprojektowana i wykonana instalacja w trudnych warunkach przemysłowych spowoduje częstsze, wymuszane przez awarie wyjazdy serwisowe generujące dodatkowe koszty.

Producenci czujek zasysających publikują mnóstwo opracowań dotyczących poszczególnych zastosowań. Trzeba je odszukać i przestudiować w celu wykonania systemu dostosowanego do warunków jego pracy.

Czujki zasysające w chłodni

Czujki zasysające są często stosowane w chłodniach. W tym przypadku brak doświadczenia projektanta lub instalatora będzie szczególnie dotkliwy. Wyobraźmy sobie, że system zasysający został wykonany prawidłowo, ale w czasie uruchamiania chłodni (obniżania temperatury) wentylator czujki – umieszczonej w innym pomieszczeniu – nie został włączony…

Obniżanie temperatury w chłodni prowadzi do zmniejszania się w niej ciśnienia i zasysania powietrza z zewnątrz poprzez czujkę i rury wchodzące do chłodni. Powietrze to ochładza się gwałtownie po przejściu przez ścianę chłodni, a zawarta w nim wilgoć skrapla się, zamarza i blokuje rury.

Jedną z dostrzegalnych tendencji jest wyniesienie instalacji poza chłodnię i wprowadzenie do niej grubych kapilar

Rys. 3. Klosz chroniący otwór zasysający przed zalodzeniem

zakończonych tak, aby otworów zasysających nie blokował szron. Jedno z takich rozwiązań pokazano na rysunku 3. Końcówka rury jest zakończona „kloszem". Jeśli dochodzi do zalodzenia, to jest ono najsilniejsze na jego krawędziach, a najsłabsze w środku. Kryza kalibrująca przepływ została wyniesiona poza chłodnię i nie jest narażona za zablokowanie.

Ciśnienie atmosferyczne otaczające instalację

Czujka zasysająca ma w środku wentylator. Można zgadnąć, że w próżni działać nie będzie. W polskich warunkach zmiany wysokości nad poziomem morza niewiele wpływają na parametry wykrywcze systemu.

Inaczej jest, gdy wlot i wylot czujki znajdą się w pomieszczeniach o różnym ciśnieniu. Dotyczy to przypadków ochrony pomieszczeń czystych, niektórych medycznych, szybów windowych. Jeśli rura z otworami zasysającymi znajduje się w pomieszczeniu o wyższym ciśnieniu niż detektor, przepływ powietrza przez komorę pomiarową czujki będzie większy niż obliczony i parametry wykrywcze będą inne. W niektórych programach narzędziowych możliwe jest ustawienie wartości nadciśnienia, a tym samym uzyskanie wyników uwzględniających „współpracę" wentylatora z nadciśnieniem. Właśnie takie czujki powinny być wybierane do tego typu zastosowań.

Wyzwaniem dla instalatora będą zmiany nadciśnienia, gdyż mogą one powodować sygnalizację błędu przepływu. Rozwiązaniem jest wprowadzenie rury wylotowej do pomieszczenia, z którego zasysamy powietrze. W przypadku szybu windowego jest to rozwiązanie rutynowe.

Wykrywanie dymu w silnym strumieniu powietrza

W kanale wentylacyjnych lub na wlocie klimatyzatora przepływ powietrza jest bardzo szybki. Dym, który jest transportowany w takim strumieniu, niemal nie dyfunduje na boki. Jak gęsto trzeba rozmieścić otwory zasysające, żeby dym ich nie minął? Według wytycznych NFPA 72 maksymalna powierzchnia nadzorowana w takich warunkach przez jeden otwór to 0,4 m^2.

Wykrywanie dymu czujką zasysającą w kanale wentylacyjnym wygląda na pierwszy rzut oka jak zastosowanie czujki punktowej w osłonie kanałowej (przeciwwietrznej). Podstawowe różnice to kierunek otworów wylotowych oraz to, że czujka zasysająca będzie wykrywać dym również przy wyłączonym wentylatorze kanału, a czujka punktowa w osłonie kanałowej – nie.

Prędkość powietrza w kanale wentylacyjnym może się bardzo zmieniać, co powoduje częstą sygnalizację błędów przepływu w czujce. Przepływ powietrza przez czujkę zasysającą może być niemal stały przy dużych zmianach szybkości powietrza w kanale, ale wymaga to znalezienia i przestudiowania odpowiedniego opracowania. Zachęcamy…

Fałszywe alarmy

Trzeba przyznać, że w wielu zastosowaniach czujki zasysające mają ustawioną zbyt dużą czułość. Zdarzają się takie wymagania klienta jak klasa A w dużej i brudnej hali fabrycznej… Bardzo często projektant nie ma żadnych danych na temat poziomu tła, bo zakład jeszcze nie pracuje… Z kolei instalator nie czuje się uprawniony do zmiany nastaw obliczonych przez projektanta. Efektem końcowym są fałszywe alarmy i przeświadczenie, że czujki zasysające są zbyt czułe.

Wyobraźmy sobie typowy przykład – centrum przetwarzania danych z tłem w okolicy 0,01% zaciemnienia/m. Co może zrobić projektant, gdy z obliczeń wynika, że dla klasy A wymaganej przez klienta trzeba ustawić czułość detektora na 0,025%? Wartość ta jest zdecydowanie zbyt blisko tła i fałszywe alarmy są niemal gwarantowane, szczególnie zimą, gdy włączamy ogrzewanie, a w okolicy zaczynają dymić kominy pieców opalanych węglem. Projektant może i powinien zmniejszyć liczbę otworów zasysających na orurowaniu danej czujki. To pozwoli podnieść próg ustawiany w czujce. Do „obsługi" pozostałych otworów potrzebna będzie jednak kolejna czujka. Instalacja będzie droższa. Innym rozwiązaniem jest zmiana klasy wykrywania – godzimy się na późniejsze wykrycie odpowiadające klasie B. Użytkownik powinien mieć świadomość możliwych wyborów i ich konsekwencji w czasie ewentualnego pożaru. Pozostawienie nastawy 0,025% stwarza niepotrzebne ryzyko.

Wiele czujek zasysających umożliwia swobodne programowanie nastaw w szerokim zakresie, więc łatwo je dostosować do miejsca aplikacji. Rutynowym etapem uruchamiania systemu zasysającego powinno być dopasowanie nastaw systemu do chronionego obiektu i oczekiwań użytkownika po pewnym czasie pracy systemu i funkcjonowania obiektu.

Pamięć zdarzeń czujki zasysającej

Jeśli już są fałszywe alarmy albo powtarzające się awarie, to skąd instalator ma wiedzieć, co zrobić, żeby było ich mniej? Z pamięci czujki. Czujki zasysające muszą mieć pamięć zdarzeń o dużej pojemności. Tylko wtedy można obejrzeć zapisy dotyczące zmian tła lub przepływu powietrza i zdecydować, co robić. Świadomie, bez zgadywania.

Obsługa systemów sygnalizacji pożarowej z czujkami zasysającymi

Systemy zasysające kojarzą się z wczesnym wykrywaniem zagrożenia pożarem przy małej gęstości dymu. Chociaż nie zawsze są tak zaprogramowane, to jednak to klasyczne zastosowanie jest częste i przysparza obsłudze systemu sygnalizacji pożarowej sporo kłopotów.

Nieprzeszkolona obsługa nie potrafi zlokalizować źródła dymu o małym stężeniu. Alarm sygnalizowany przez system

pracujący w klasie A prawdopodobnie potraktuje jako fałszywy. Co zrobić, aby nie zaprzepaścić szansy na zlikwidowanie zagrożenia we wczesnej fazie rozwoju?

Czujki zasysające mają na ogół kilka progów detekcji. Wykorzystujmy je. Używajmy kilku progów i przypiszmy do nich różne scenariusze. Na przykład wczesne wykrycie odpowiadające detekcji w klasie A może być traktowane jako informacja stawiająca obsługę na nogi. Liczymy się z fałszywym alarmem albo z zagrożeniem łatwym do opanowania, więc centrala SAP nie odlicza czasów T1 i T2. Przekroczenie następnego progu skutkuje prealarmem, który powinien utwierdzić obsługę w przekonaniu, że alarm nie jest fałszywy, i dać jej szansę na znalezienie źródła zagrożenia. Przekroczenie trzeciego progu skutkuje alarmem pierwszego stopnia. Jeśli obiekt jest gaszony, to przekroczenie czwartego progu może – w koincydencji z sygnałem alarmowym z innej czujki – wyzwalać gaszenie.

Podsumowanie

Czujki zasysające są urządzeniami umożliwiającymi wczesne wykrycie zagrożenia i kilkustopniowe potwierdzenie tego wykrycia. Są często stosowane w miejscach, dla których nie opracowano jeszcze wytycznych. Wiedza i doświadczenie projektanta i instalatora oraz informacje uzyskane od użytkownika obiektu są w takich zastosowaniach bardzo istotne. Użytkownicy systemów zasysających powinni mieć świadomość, że całkowity koszt inwestycji i eksploatacji systemu bardzo zależy od jakości projektu. Czujki zasysające nie są urządzeniami tanimi. Warto poświęcić nieco więcej czasu na projekt, żeby lepiej wykorzystać ich zalety i uniknąć pułapek wynikających z trudnych warunków, w których mogą pracować.

Beata Idziak
Mariusz Konik
Andrzej Obłój

Klasy detekcji

Norma EN54-20 wprowadziła trzy klasy detekcji (szybkości wykrywania zagrożenia) czujek zasysających:

1) Klasa A – bardzo wczesne wykrywanie niewielkiego stężenia dymu, niedostępne dla innych technologii. Typowe zastosowania: ważne serwerownie i centra przetwarzania danych, cenne archiwa.
2) Klasa C – wykrywanie zagrożenia na podobnym etapie rozwoju pożaru jak alarmowanie przez punktowe czujki dymu. Typowe zastosowania: szyby windowe, komory transformatorowe, zamknięte przestrzenie sufitowe.
3) Klasa B – wykrywanie znacznie wcześniejsze niż w przypadku klasy C, ale znacznie późniejsze niż w przypadku klasy A. Wbrew pozorom klasa ta jest (albo powinna być) bardzo często wybierana, na przykład dla pomieszczeń, w których unoszący się dym jest rozrzedzany przez wentylację lub rozrzedza się z powodu wielkości pomieszczenia – na przykład w atriach i magazynach wysokiego składowania.

Scenariusz rozwoju zdarzeń w czasie pożaru (Część 2)

Ryszard Małolepszy

Opracowanie scenariuszy pożaru i projektowych scenariuszy pożaru

Scenariusze pożaru są opisem sekwencji możliwych zdarzeń pożarowych i składają się z charakterystyki pożaru, charakterystyki budynku i charakterystyki użytkowników budynku. Scenariusze pożaru opisują funkcje ochrony przeciwpożarowej, źródła zapłonu, rodzaje i konfiguracje materiałów palnych, charakterystyki pożaru i wentylacji, cechy i lokalizacje osób oraz warunki stabilności konstrukcji nośnej i innego wyposażenia.

Według Charlesa Fleischmanna[1] scenariusz pożarowy to jakościowy opis przebiegu pożaru w czasie, przedstawiający najważniejsze zdarzenia pokazujące, w jaki sposób dany pożar różni się od innych pożarów[2]. Zakładany scenariusz pożarowy to reprezentatywny scenariusz pożarowy, który zostanie poddany analizie deterministycznej bazującej na inżynierii bezpieczeństwa pożarowego. Pożar projektowy to ilościowy opis możliwego pożaru w ramach reprezentatywnego scenariusza pożarowego (moc pożaru, wytwarzane substancje i gazy itd.).

Według tego samego autora należy rozpatrzyć reprezentatywne scenariusze pożarowe, a mianowicie:

1) Scenariusz 1 (zakładany scenariusz pożarowy dotyczący przeznaczenia budynku określonego rodzaju):
   – najgroźniejszy pożar przy najwyższej możliwej gęstości obciążenia ogniowego podczas normalnego użytkowania budynku,
   – należy wykazać, że osoby przebywające w budynku oraz strażacy nie będą narażeni na nieakceptowalne ryzyko uszkodzenia ciała.
2) Scenariusz 2 (pożar jest zlokalizowany w obrębie podstawowych dróg ewakuacyjnych):
   – należy założyć, że pożar w obrębie podstawowych dróg ewakuacyjnych powstał na skutek umyślnego podpalenia,
   – należy wykazać, że osoby przebywające w budynku oraz strażacy nie będą narażeni na nieakceptowalne ryzyko uszkodzenia ciała.
3) Scenariusz 3 (pożar w pomieszczeniu, w którym zazwyczaj nie przebywają ludzie):
   – pożar wybucha w pomieszczeniu, w którym zazwyczaj nie przebywają ludzie, i dociera tam, gdzie potencjalnie może przebywać największa liczba osób,
   – należy wykazać, że osoby przebywające w budynku oraz strażacy nie będą narażeni na nieakceptowalne ryzyko uszkodzenia ciała.
4) Scenariusz 4 (pożar w przestrzeni niedostępnej):
   – pożar wybucha w niedostępnej przestrzeni międzyściennej lub międzystropowej, przyległej do dużego pomieszczenia, w którym przebywają ludzie,
   – niewykryty pożar dociera do pomieszczeń w budynku, w których potencjalnie może przebywać duża liczba osób,
   – należy wykazać, że osoby przebywające w budynku oraz strażacy nie będą narażeni na nieakceptowalne ryzyko uszkodzenia ciała,
   – nie wymaga się analizy w przypadku konwencjonalnych rozwiązań – przegród przeciwpożarowych oraz systemów wykrywania/gaszenia pożaru.
5) Scenariusz 5 (pożar tlący w bliskiej odległości od pomieszczenia sypialnego):
   – wolno rozwijający się pożar tlący stanowi zagrożenie dla śpiących osób,

1) Charles Fleischmann (University of Canterbury), Projektowanie ochrony przeciwpożarowej w Nowej Zelandii w oparciu o inżynierię pożarową.

2) ibidem

– należy wykazać, że osoby przebywające w budynku oraz strażacy nie będą narażeni na nieakceptowalne ryzyko uszkodzenia ciała,
– trzeba wyposażyć pomieszczenia sypialne w system wykrywania dymu,
– nie wymaga się analizy dotyczącej pomieszczeń, w których nie śpią ludzie, lub pomieszczeń wyposażonych w system wykrywania dymu.

6) Scenariusz 6 (pożar zagrażający sąsiadującym obiektom):
– w budynku w pełni rozwinął się pożar,
– pożar rozprzestrzenia się na sąsiedni budynek,
– należy ograniczyć rozwój pożaru na inne obiekty do czasu przybycia jednostek straży pożarnej i podjęcia działań gaśniczych.

7) Scenariusz 7 (pożar zagrażający fasadzie zewnętrznej):
– ogień przedostaje się przez otwór okienny w fasadzie wykonanej z materiałów palnych lub źródło pożaru znajduje się blisko fasady,
– pożar może objąć również wyższe kondygnacje budynku,
– należy nie dopuścić do przeniesienia się pożaru na wyższe kondygnacje budynku oraz utrzymać na drogach ewakuacyjnych warunki nie zagrażające zdrowiu i życiu aż do momentu zakończenia ewakuacji.

8) Scenariusz 8 (pożar obejmujący wykończenie wnętrza):
– w narożniku pomieszczenia wybuchł niewielki pożar, który bezpośrednio zagraża wykończeniu ściany,
– może rozwinąć się nagły pożar obejmujący palne materiały, z których wykonane jest wykończenie wnętrz.

9) Scenariusz 9 (typowy pożar w budynku, w trakcie którego nie zadziała żaden bierny ani czynny środek zabezpieczenia):
– rozwiązania powinny być kompleksowe – awaria jednego z elementów systemu zabezpieczeń nie powinna powodować nieproporcjonalnie dużych zmian w funkcjonowaniu całego systemu,
– analiza typu „co, jeśli…”,
– nie wolno przyjmować, że systemy ochrony przeciwpożarowej są w 100% wiarygodne i skuteczne,
– należy założyć, że osiągnięcie akceptowalnego poziomu niezawodności wymaga wykonywania konserwacji zgodnej ze standardami.

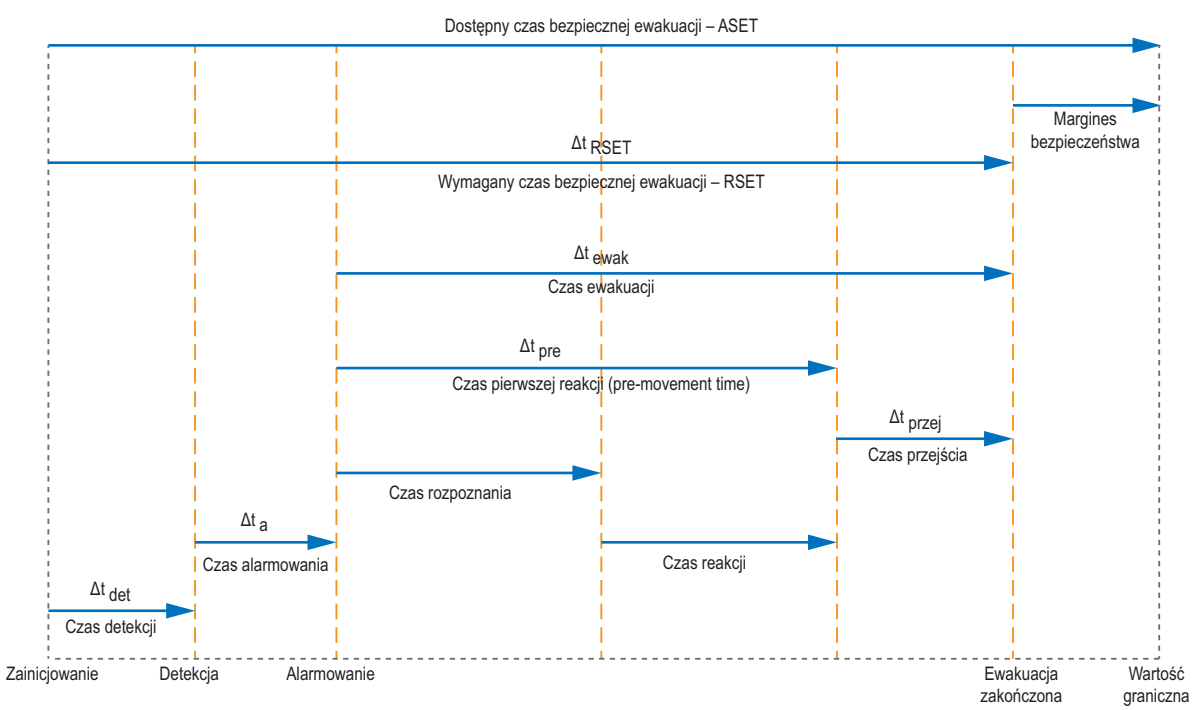
Nie wszystkie scenariusze pasują do wszystkich budynków. Na przykład w przypadku zastosowania systemów sygnalizacji pożarowej lub systemów gaśniczych niektóre scenariusze nie będą musiały być brane pod uwagę.

Zgodnie z PN-EN 1991-1- 2:2006 EUROKOD 1 typowy scenariusz pożaru opisuje proces powstania i rozwoju pożaru, fazę pełnego rozwoju i fazę zaniku oraz charakteryzuje środowisko budowlane i systemy, które wpływają na przebieg pożaru. Norma ta definiuje scenariusze pożarowe jako krzywe zmian temperatury w czasie (krzywe nagrzewania, krzywe nominalne) lub model rozwoju pożaru w pomieszczeniu.

Podsumowując – scenariusz pożarowy to opracowanie dotyczące dynamiki pożaru oraz jego oddziaływań na konstrukcję i warunki ewakuacji, zawierające wyniki przeprowadzonych symulacji komputerowych pokazujących prawdopodobny rozwój pożaru w danych warunkach.

Dobór biernych i czynnych zabezpieczeń przeciwpożarowych

Projekt doboru zabezpieczeń przeciwpożarowych charakteryzuje budynek, pożar oraz rozwiązania i systemy związane z bezpieczeństwem. Projekt ten powinien być oceniony obliczeniowo, z użyciem projektowych scenariuszy pożaru i na podstawie różnych metod obliczeniowych w celu określenia, czy zostały spełnione funkcjonalne kryteria dotyczące zabezpieczeń. Projekt może być opracowany z intencją porównania sposobu funkcjonowania dobranych zabezpieczeń ze sposobem funkcjonowania rozwiązań bazujących na przepisach nakazowych. Ma to szczególne znaczenie w przypadku projektów budynków



Rys. 1. Uproszczony schemat składowych czasu ewakuacji

wykonywanych bez jakichkolwiek odstępstw lub w przypadku stosowania rozwiązań równoważnych czy alternatywnych.

Na to, jak budynek jest chroniony przed pożarem, duży wpływ mają interakcje systemów bezpieczeństwa, zachowania użytkowników budynku oraz to, czy chroniona jest jakaś jego zawartość.

Ze względu na bezpieczeństwo pożarowe należy brać pod uwagę:

– inicjację pożaru i jego rozwój,
– rozprzestrzenianie się pożaru, utrzymywanie kontroli i zarządzanie zadymieniem,
– wykrywanie pożaru i alarmowanie,
– gaszenie lub lokalizowanie pożaru,
– warunki ewakuacji (w tym zachowanie ludzi),
– bierną ochronę przeciwpożarową.

Sposób podejścia do projektowania i wyboru metod zabezpieczeń przeciwpożarowych określa dokument *NFPA 550 Guide to the Fire Safety Concepts Tree.*

Tworząc system zabezpieczeń przeciwpożarowych, korzysta się ze z osiągnięć inżynierii pożarowej i dokonuje analizy ryzyka bazującej na metodach deterministycznych. Umożliwia ona zbadanie ogólnej skuteczności zaproponowanych systemów bezpieczeństwa pożarowego oraz określenie poziomu ryzyka, na które narażeni są użytkownicy budynku. Analiza powinna obejmować ocenę ryzyka, skuteczności, niezawodności oraz skutków uszkodzenia kluczowych środków ochrony przeciwpożarowej. Zakres niniejszego artykułu, ze względu na ograniczenia objętościowe, nie obejmuje podstaw oceny ryzyka.

W dalszej części omówione zostanie jedynie wykrywanie pożaru, alarmowanie i powiadamianie, a także, w skrócie, warunki ewakuacji i zachowanie ludzi w czasie pożaru.

Wykrywanie pożaru i alarmowanie

O pożarze muszą zostać poinformowani użytkownicy budynku i służby ratunkowe. Ponadto muszą zostać uruchomione aktywne system ochrony przeciwpożarowej, takie jak system zarządzania dymem, dźwiękowy system ostrzegawczy, system automatycznego uszczelnienia stref pożarowych, systemy gaśnicze i zabezpieczające. Pożar może być wykryty przez ludzi lub automatycznie. Ludzie mogą wykryć pożar pod warunkiem, że będą w pobliżu, zachowają czujność i zdolność do wykrycia różnych oznak pożaru oraz odpowiednio na nie zareagują. Budynek może być wyposażony w automatyczne detektory pożaru, które monitorują przestrzeń i są w stanie wykryć różne oznaki pożaru (np. ciepło, dym, promieniowanie cieplne, błysk płomienia i inne). Mogą one być przyłączone do systemu alarmowego, aby ostrzec użytkowników budynku oraz straż pożarną.

Problemem dotyczącym systemów wykrywania pożaru są nieodłączne opóźnienia. Mogą one być zmienne lub stałe. Zmienne opóźnienia to na przykład czas transportu produktów spalania docierających do detektora lub opóźnienia wynikające z reakcji detektora. Opóźnienia związane z transportem produktów spalania zależą od szybkości wydzielania ciepła, szybkości wytwarzania dymu, wysokości sufitu, odległości detektora od podstawy pożaru i przeszkód.

Kategoria scenariuszy i modyfikacje	**Pierwsi użytkownicy** $\Delta t_{pre(1\%)}$	**Rozkład użytkowników** $\Delta_{tpre(99\%)}$ **a**
A: czuwający i zaznajomieni		
M1 B1 - B2 A1 - A2	0,5	1,0
M2 B1 - B2 A1 - A2	1,0	2
M3 B1 - B2 A1 - A3	>15	>15
Dla B3 dodać 0,5 w celu odszukania drogi wyjścia		
M1 – wymagany jest dźwiękowy system ostrzegawczy, jeśli możliwa jest obecność niezaznajomionych z obiektem gości		
B: czuwający i niezaznajomieni		
M1 B1 A1 – A2	0,5	2
M2 B1 A1 – A2	1,0	3
M3 B1 A1 – A3	>15	>15
Dla B2 dodać 0,5 w celu odszukania drogi wyjścia		
Dla B3 dodać 1,0 w celu odszukania drogi wyjścia		
M1 – wymagany dźwiękowy system ostrzegawczy		
C_I: śpiący i zaznajomieni (np. mieszkania)		
M2 B1 A1	5	5
M3 B1 A3	10	>20
Dla pozostałych w bloku uznać 1 godzinę		
C_{II}: użytkownicy z systemem zarządzania (np. obsługiwane apartamenty, halle rezydencji)		
M1 B2 A1 – A2	10	20
M2 B2 A1 – A2	15	25
M3 B2 A1 – A3	>20	>20
C_{III}: śpiący i niezaznajomieni (np. hotel, pensjonat)		
M1 B2 A1 – A2	15	15
M2 B2 A1 – A3	20	20
Dla B3 dodać 1,0 w celu odszukania drogi wyjścia	>20	>20
M1 – wymagany dźwiękowy system ostrzegawczy		

Tab. 1. Sugerowane czasy (w minutach) pierwszych reakcji dla różnych projektowych scenariuszy zachowań

Uwaga!

- *Całkowity czas pierwszych reakcji = $\Delta_{tpre(1\%)} + \Delta_{tpre(99\%)}$*
- *Pozostałe sugerowane czasy dla innych typów użytkowania określono w PD 7974-6:2004*

Opóźnienia związane z reakcją detektora ciepła można obliczyć, jeżeli znany jest współczynnik RTI (*Rate Time Index*) detektora. Na przykład – model komputerowy DETACT wylicza opóźnienie reakcji detektora, wymagając RTI jako parametru wejściowego. Stałe opóźnienia są związane z cechami systemów, takimi jak opóźnienia central wynikające z odpytywania czujek, czasu weryfikacji alarmu lub występowania alarmu wstępnego w systemie. Opóźnienia systemowe mogą być ustalone na podstawie danych producenta.

Celem alarmowania jest powiadomienie mieszkańców budynku lub straży pożarnej, że powstał pożar, i ewentualnie dostarczenie informacji dotyczącej miejsca pożaru. Systemy powiadamiania mogą być automatyczne lub wykorzystywać działanie ludzi. Dźwiękowe i wizualne alarmowanie może być zainicjowane przez system wykrywania pożaru. Komunikaty głosowe nadawane przez dźwiękowy system ostrzegawczy powinny być nie tylko wystarczająco głośne, ale i zrozumiałe. Sygnał alarmowy, a także uszkodzeniowy, może być przekazany straży pożarnej. Powiadomienie straży może być zarazem poinformowaniem o umiejscowieniu pożaru.

W celu poprawnego i skutecznego wykonania projektu systemu wykrywania pożaru można posłużyć się dostępnymi w naszym kraju wytycznymi lub standardami. Można wymienić chociażby *Poradnik projektanta. Wytyczne projektowania. Urządzenia sygnalizacji pożarowej w projektach instalacji* wydany przez Polon Alfa lub *Wytyczne projektowania instalacji sygnalizacji pożarowej* wydane przez Stowarzyszenie Inżynierów i Techników Pożarnictwa.

Zachowanie ludzi i ewakuacja

Osoby przebywające w miejscu objętym pożarem muszą mieć możliwość dotarcia do bezpiecznego miejsca. Użytkownicy budynku powinni mieć możliwość dostępu do chronionej drogi ewakuacyjnej. W niektórych budynkach drogi ewakuacyjne powinny być obudowane i mieć odpowiednią odporność ogniową w celu ograniczenia napływu dymu i ciepła do czasu, gdy ostatni użytkownik budynku dotrze do bezpiecznego miejsca. Można zapewnić ludziom ochronę wewnątrz budynku. Użytkownikom budynku powinno się zapewnić dostęp do wystarczającej liczby wyjść o odpowiedniej przepustowości, oświetlenie awaryjne, ewakuacyjne znaki kierunkowe, a także chronioną drogę ewakuacyjną do bezpiecznego miejsca.

Podstawowe zasady inżynierii bezpieczeństwa pożarowego w zakresie ewakuacji ludzi określono w *Human Factors: Life Safety Strategies-Occupant Evacuation, Behaviour And Condition*[3] Dostępny czas na bezpieczną ewakuację (*Available Safe Escape Time*) powinien być dłuższy niż czas potrzebny na bezpieczną ewakuację (*Required Safe Escape Time*) – powinno się uwzględnić margines bezpieczeństwa W przypadku typowych, nowo projektowanych budynków, w których odpowiedni poziom bezpieczeństwa pożarowego jest osiągany poprzez spełnienie wymagań przepisów techniczno-budowlanych i przepisów dotyczących ochrony przeciwpożarowej, nie wymaga się dodatkowych sprawdzeń poziomu bezpieczeństwa. Z kolei w wielu złożonych, innowacyjnych obiektach, projektowanych z odstępstwami od obowiązujących przepisów techniczno-budowlanych, a także w budynkach już istniejących, w przypadku których przy nadbudowie, przebudowie lub zmianie sposobu użytkowania istnieje możliwość spełnienia wymagań dotyczących bezpieczeństwa w sposób inny niż określony w przepisach techniczno-budowlanych, wykorzystanie metod inżynierii bezpieczeństwa pożarowego jest niezbędne. W takich przypadkach należy wykazać, że w oszacowanym czasie przebywania ludzi w budynku i w czasie potrzebnym na ewakuację ludzi w trakcie pożaru na wydzielonych drogach ewakuacyjnych będą panowały warunki umożliwiające bezpieczną ewakuację.

Czas potrzebny na bezpieczną ewakuację RSET

Całkowity czas ewakuacji zależy od detekcji pożaru, ostrzeżenia o niebezpieczeństwie oraz zachowania i poruszania się ludzi w czasie ewakuacji. W uproszczeniu ewakuację można podzielić na dwie fazy. Pierwsza z nich obejmuje pierwsze reakcje, tzn. zachowania użytkowników budynku, które poprzedzają rozpoczęcie przemieszczania się po drogach ewakuacyjnych (*pre-movement behaviours*). Ta poprzedzająca właściwą ewakuację faza trwa najdłużej. Kolejną fazą jest przemieszczanie się ludzi po drogach ewakuacyjnych. W trakcie tego przemieszczania się na zachowanie ludzi (*travel behaviour*) wpływa widok ognia lub dymu, a także możliwość doznania urazów.

Rozkład czasów alarmowania i czasów pierwszych reakcji są zależne od trzech ważnych zmiennych:

– jakości systemu sygnalizacji pożarowej (poziomy od A1 do A3),
– złożoności budynku (poziomy od B1 do B3),
– jakości systemu zarządzania bezpieczeństwem (poziomy od M1 do M3).

– *Poziom A1 systemu alarmowego:* System sygnalizacji pożarowej obejmuje cały budynek. Natychmiast ogłaszany jest alarm dla wszystkich użytkowników znajdujących się w zagrożonych pożarem miejscach.

– *Poziom A2 dwuetapowy system alarmowy:* Automatyczny system wykrywania pożaru w całym budynku alarmuje osoby zarządzające budynkiem lub ochronę. Alarm dla wszystkich użytkowników budynku, którzy znajdują się w zagrożonych miejscach, jest uruchamiany przez obsługę lub samoczynnie, po upływie ustalonego czasu opóźnienia, jeśli wstępny alarm nie zostanie skasowany.

– *Poziom A3 systemu alarmowego:* Lokalny system wykrywania pożaru alarmuje tylko w niewielkim obrębie pożaru. Może brakować automatycznego systemu wykrywania pożaru – alarm dla wszystkich zagrożonych pożarem miejsc jest uruchamiany ręcznie przez obsługę.

Część 3 w kolejnym numerze.

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

3) British Standards. PD 7974-6:2004. The application of fire safety engineering principles to fire safety design of buildings. Part 6: Human factors: Life safety strategies-Occupant evacuation, behaviour and condition (Sub-system 6).

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

RED POWER

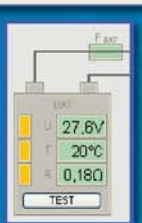
Zaawansowana kontrola zasilania

Układ UVP
(Under Voltage Protection)
$U_{AKU} \leq 20V +/- 0,2V$

Cykliczny test akumulatora
(5min - ustawienia fabryczne)
$R_{AKU} > 300m\Omega$
$U_{AKU} < 24V$

Kompensacja temperaturowa napięcia ładowania akumulatora

Oprogramowanie „Power Security"



24VDC

Wykrycie awarii w obwodzie akumulatora
wyjścia techniczne:
- APS FLT
- ALARM

Możliwość załączenia testu akumulatora na żądanie użytkownika

Zasilacze buforowe serii EN54 do systemów przeciwpożarowych

Część 3 – obwód zasilania rezerwowego

Pulsar

Jednym z podstawowych wymagań stawianych współczesnym systemom przeciwpożarowym jest zapewnienie ciągłości zasilania odbiorników przy braku głównego napięcia zasilającego z sieci energetycznej. Funkcję tę realizuje obwód zasilania rezerwowego, który jest jednym z ważniejszych elementów zasilacza i od którego poprawnego działania w dużej mierze zależy niezawodność całego systemu. Przeznaczone do zastosowania w systemach przeciwpożarowych zasilacze buforowe serii EN54 firmy PULSAR mają rozbudowany obwód zasilania rezerwowego, który zostanie opisany w niniejszym artykule

Zasilacze serii EN54 zostały wyposażone w inteligentne obwody ładowania akumulatorów z funkcją przyspieszonego ładowania oraz kontroli akumulatorów, których głównym zadaniem jest monitorowanie stanu akumulatorów i połączeń w ich obwodzie. Jeżeli sterownik zasilacza wykryje awarię w obwodzie akumulatorów, użytkownik zostanie poinformowany o tym zdarzeniu poprzez zmianę stanu wyjść technicznych zasilacza *APS FLT* oraz *ALARM*. Awaria może być wywołana różnymi czynnikami, takimi jak brak akumulatorów, zwarcie zacisków, odwrotne przyłączenie itp. Zasilacz został wyposażony w szereg funkcji pozwalających wykryć różne typy awarii obwodu zasilania rezerwowego.

Jedną z ważniejszych funkcji obwodu zasilania rezerwowego jest cykliczne sprawdzanie, czy rezerwowe źródło zasilania jest sprawne. Do tego celu służy funkcja testu akumulatorów. Co pięć minut zasilacz przeprowadza test, podczas którego dokonuje pomiarów parametrów elektrycznych zgodnie z zaimplementowaną procedurą pomiarową. Test może również zostać załączony ręcznie, na żądanie użytkownika, z poziomu menu zasilacza, np. w celu przetestowania akumulatorów po ich wymianie.

Wynik testu będzie negatywny, jeżeli ciągłość obwodu akumulatorów zostanie przerwana, rezystancja w obwodzie wzrośnie powyżej 300 mΩ lub napięcie na zaciskach akumulatorowych spadnie poniżej 24 V. Pomiar rezystancji obwodu akumulatorów jest wymagany przez normę PN-EN 54-4. Zasilacz ma zabezpieczenie programowe przed zbyt częstym wykonywaniem testu akumulatorów, które mogłoby spowodować ich niedoładowywanie. Zabezpieczenie polega na zablokowaniu możliwości wykonania testu przez 60 s od jego ostatniego załączenia.

W celu przedłużenia żywotności akumulatorów zastosowano zabezpieczenie przed nadmiernym rozładowaniem – UVP (Under Voltage Protection) oraz wprowadzono kompensację temperaturową napięcia ładowania. Zabezpieczenie UVP odłącza akumulatory od zasilacza w chwili, gdy napięcie na nich spadnie

Fot. 1. Załączenie testu akumulatora – zasilacz z wyświetlaczem LED

Fot. 2. Załączenie testu akumulatora – zasilacz z wyświetlaczem LCD

poniżej 20 V±0,2 V podczas pracy akumulatorowej. Ponowne załączenie akumulatorów do zasilacza następuje automatycznie w chwili pojawienia się napięcia sieciowego 230 V_{AC}. Kompensacja temperaturowa napięcia ładowania jest zrealizowana na podstawie pomiaru temperatury akumulatorów. Do tego celu służy czujnik temperatury znajdujący się w ich pobliżu. Na podstawie odczytów sygnałów z czujnika sterownik zasilacza dokonuje korekcji napięcia ładowania. Czujnik znajduje się w przedziale akumulatorów, dlatego też nie należy mylić jego wskazań z temperaturą otoczenia. Zasilacze zostały zabezpieczone również przed zwarciem zacisków akumulatora oraz przed odwrotnym przyłączeniem biegunów. W przypadku zwarcia obwód kontroli natychmiast odłącza akumulatory od pozostałych obwodów zasilacza w taki sposób, że na wyjściach zasilacza nie obserwuje się zaniku napięcia wyjściowego. Ponowne automatyczne załączenie akumulatorów do obwodów zasilacza jest możliwe dopiero po usunięciu zwarcia i poprawnym ich przyłączeniu. W przypadku nieprawidłowego przyłączenia następuje przepalenie bezpiecznika FBAT. Powrót do normalnej pracy jest możliwy dopiero po wymianie bezpiecznika i poprawnym przyłączeniu akumulatorów.

Więcej informacji o przedstawionej serii zasilaczy, a także o innych seriach, można znaleźć na stronie producenta (*www.pulsar.pl*).

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

Oryginalny, niezawodny produkt

Przeciwpożarowe puszki instalacyjne PIP-AN

W2

Firma W2 istnieje na polskim rynku już szesnasty rok, działamy prężnie i ciągle się rozwijamy. Jako pierwsi na rynku zaprezentowaliśmy przeciwpożarowe puszki instalacyjne. Oferując oryginalny, niezawodny produkt, przyczyniliśmy się do zwiększenia pewności działania systemów przeciwpożarowych

Prawidłowy montaż sygnalizatorów z użyciem puszek instalacyjnych zapewnia ciągłość linii sygnałowej w przypadku spalenia się sygnalizatora na skutek pożaru. Dzięki temu pozostałe sygnalizatory, które znajdują się poza strefą pożaru, działają nadal.

Jako polski producent mamy stały kontakt z klientami. Uwzględniamy ich uwagi i wdrażamy zmiany mające na celu stworzenie jak najlepszych produktów. Dlatego wprowadziliśmy nową serię przeciwpożarowych puszek instalacyjnych PIP-AN. Puszki PIP-AN były prezentowane na targach SECUREX 2014 i Kongresie Pożarnictwa w Warszawie w 2014 r. Do sprzedaży zostały wprowadzone w tym roku. Puszki PIP-AN posiadają Aprobatę Techniczną oraz Certyfikat Zgodności, wydane przez CNBOP-PIB.

Funkcjonalnie seria PIP-AN niczym nie różni się od serii PIP-A. Zyskuje za to na jakości, ponieważ montaż puszek PIP-AN jest dużo prostszy. Klient nadal otrzymuje produkt z blachy w kolorze czerwonym. Zmiana, na którą warto zwrócić uwagę, to zamiana przepustów z wkładanych (PIP-A) na wsuwane (PIP-AN). Obecnie, dzięki nowej budowie, wystarczy przyciąć przepust w celu dopasowania go do średnicy przewodu. Teraz nie ma już problemu z „przepychaniem" przewodu przez przepust na wysokościach. Przy montażu puszek PIP-AN nie trzeba stosować trzymaczy kabla – bo ich fizycznie nie ma. Prace instalacyjne stają się łatwiejsze.

W nowej serii puszek kolejną zmianą jest ułożenie kostek ceramicznych. Nowe ułożenie pozwala na bezpośrednie wyprowadzenie przewodu na zewnątrz w linii prostej. Również w tym przypadku mała zmiana daje duży efekt. Nie ma już tak zwanego „wychodzenia zza rogu" kostki ceramicznej z przewodem, a przestrzeń wewnątrz puszki jest większa. Wyrównano także wysokość „wejścia przewodu" z zaciskiem kostki ceramicznej. Jest to wynikiem zmienionego kształtu blachy – przetłoczenie podstawy puszki spowodowało lepsze jej przyleganie do podłoża oraz zwiększyło odporność termiczną produktu. Tak jak wcześniej, puszka jest przytwierdzana bezpośrednio do podłoża. Do montażu należy użyć kołków M6 o wymaganej odporności ogniowej.

Kolejnym atutem puszek PIP-AN jest możliwość zastosowania przewodów o większej średnicy – maksymalnie 19 mm lub 25 mm (puszka PIP-2AN 6 mm^2). Umożliwia to uzyskanie nowych typoszeregów.

Przy okazji tworzenia nowej serii przeciwpożarowych puszek instalacyjnych powstała puszka PIP-7A. Jest to zupełnie nowy produkt, który umożliwia łączenie przewodów, w których może być maksymalnie 20 żył.

Puszki PIP-AN mają odporność ogniową E 90. Ich montaż jest szybszy, dzięki czemu koszt prac instalatorskich jest niższy.

Więcej informacji znajduje się na naszej stronie internetowej (*www.w2.com.pl*).

W2

Wielopasmowa czujka płomienia PPW-40REx
Nowość w ofercie Polon-Alfa

Marcin Barnat

Wielopasmowa czujka płomienia PPW-40REx należy do grupy czujek wysoce wyspecjalizowanych, charakteryzujących się wysokim poziomem niezawodności w działaniu oraz budową przewidzianą do pracy w bardzo trudnych warunkach. Zadaniem tego typu czujek jest jak najszybsze wykrycie pożaru płomieniowego, podczas którego emitowane jest promieniowanie elektromagnetyczne widzialne tylko w zakresie podczerwieni

Fot. 1. Czujka PPW-40REx

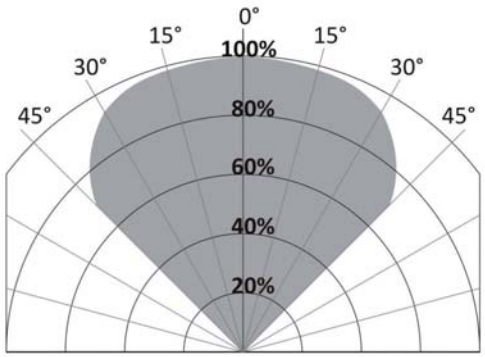
Jak działa?

Czujka jest wyposażona w mikrokontroler nadzorujący pracę trzech pasmowych detektorów reagujących na promieniowanie elektromagnetyczne w zakresie podczerwieni. Detektory te sprawiają, że czujka jest bardzo odporna na różnego rodzaju fałszywe alarmy mogące zakłócić pracę urządzenia i tym samym całego systemu sygnalizacji pożarowej, z którym współpracuje. Jest odporna na światło słoneczne padające bezpośrednio na jej układ detekcyjny lub odbijające się od składowanych w pobliżu materiałów, co jest główną przyczyną występowania fałszywych alarmów. Jej pracy nie są w stanie zakłócić również różnego rodzaju grzałki, promienniki oraz lampy, służące do ogrzewania lub po prostu oświetlania pomieszczeń.

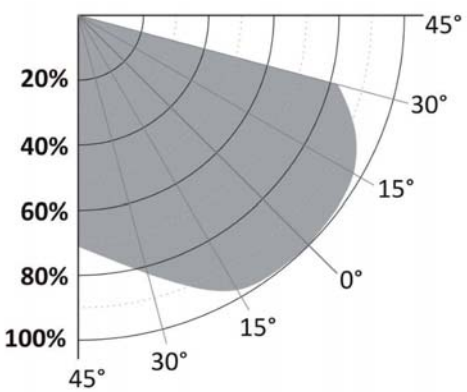
PPW-40REx charakteryzuje się między innymi bardzo szerokim polem detekcji obejmującym kąt do 80° w poziomie oraz 75° w pionie. W przypadku zastosowania odpowiednich wsporników, niezbędnych do kątowego ustawienia czujki, możliwe jest bardzo dokładne określenie obszaru, który czujka ma nadzorować.

Czujka ma pierwszą klasę czułości pożarowej (jej zasięg dochodzi do 25 m). Jest przeznaczona do pracy w trudnych warunkach atmosferycznych, zarówno wewnątrz, jak i na zewnątrz obiektów (stopień ochrony – IP66). Posiada certyfikat KDB 13ATEX0058X wydany przez Główny Instytut Górnictwa. Zaletą czujki PPW-40REx jest także wbudowany układ testujący zabrudzenie optyki oraz funkcja sprawdzająca co jedną minutę zabrudzenie czujki. Czujka jest wyposażona w grzałkę, która utrzymuje przeźroczystość optyki na odpowiednim poziomie.

Czujka PPW-40REx jest urządzeniem o najbardziej uniwersalnym charakterze. Jest przeznaczona do współpracy z centralami, które umożliwiają przyjęcie sygnału alarmowego z bezpotencjałowych styków przekaźnika o obciążalności 5 A/30 V_{DC}, lub z innymi systemami wykorzystującymi pętlę prądową 4–20 mA. Może pracować bezpośrednio na liniach dozorowych systemu IGNIS 1000/2000. Z systemem sygnalizacji pożarowej POLON 4000/6000 może być połączona za pośrednictwem adaptera linii bocznej ADC-4001M.



Rys. 1. Kąt widzenia czujki w poziomie



Rys. 2. Kąt widzenia czujki w pionie

Natężenie prądu (±0,3 mA)	Stan czujki
0 mA	uszkodzenie zasilania
1 mA	uszkodzenie ogólne
2 mA	uszkodzenie układu optyki
3 mA	podwyższone tło podczerwieni
4 mA	dozorowanie
20 mA	alarmowanie

Tab. 1. Natężenie prądu dla wyjścia 4÷20 mA w zależności od stanu czujki

Wyposażona jest także w wewnętrzną pamięć zdarzeń, zawartość której można odczytać poprzez interfejs RS485 współpracujący z oprogramowaniem serwisowym.

Gdzie je stosować?

Czujki PPW-40REx są przeznaczone do stosowania w miejscach, w których jako środek łatwopalny występują wszelkiego rodzaju paliwa zawierające węglowodory. Miejsca te zaliczamy do stref zagrożonych wybuchem mieszanin gazów i oparów cieczy palnych z powietrzem podgrup IIA, IIB, IIC oraz stref zagrożonych wybuchem mieszanin pyłów palnych z powietrzem podgrup IIIA, IIIB, IIIC (m.in. rafinerie, lakiernie, stacje paliw, hangary samolotowe oraz szyby kopalniane).

Osoby zainteresowane szerszą charakterystyką czujki PPW-40REx zapraszamy do odwiedzenia naszej strony internetowej *www.polon-alfa.pl.*

Marcin Barnat
Polon-Alfa

Cztery tegoroczne trendy dotyczące systemów kontroli dostępu

John Fenske

Trend pierwszy: w przemyśle odchodzi się od niedostosowanych do zmian struktur systemów kontroli dostępu na rzecz bezpieczniejszych, otwartych, adaptowalnych, przyszłościowych rozwiązań

Branża zabezpieczeń jest rozwijana na wiele sposobów. Progresywne przedsiębiorstwa dostosowują się do zmian. Dzięki temu dzisiejsze rozwiązania z dziedziny kontroli dostępu będzie można dostosować do przyszłych zastosowań. Te zastosowania mogą być bardzo różne, takie jak np. handel bezgotówkowy, kontrola obecności i rejestracja czasu pracy, bezpieczne zarządzanie drukowaniem czy bezpieczne logowanie w sieci jako funkcja wieloelementowego systemu bezpieczeństwa w firmie. Dzięki wykorzystaniu zarówno rozwiązań standardowych, takich jak OSDP, jak i tych adaptowalnych bezpieczeństwo przestaje zależeć od zastosowanego sprzętu i mediów.

Trend drugi: mobilna kontrola dostępu będzie nadal stopniowo rozwijać się

W 2014 roku wdrażano mobilną kontrolę dostępu z wykorzystaniem smartfonów zamiast kart – z ograniczeniami wynikającymi z dostępnej technologii. W następnej fazie moc obliczeniowa smartfonów i możliwości mediów

przezwyciężą ograniczenia, czego efektem będzie lepsza funkcjonalność i większy komfort użytkowania. W przyszłości możliwości komunikacyjne smartfonów będą wykorzystywane do większej liczby zadań niż dzisiejsze czytniki kart, serwery i panele w tradycyjnych systemach kontroli dostępu. Do zadań tych będzie należeć weryfikowanie tożsamości poprzez sprawdzenie, czy żądanie dostępu pojawia się w dozwolonym czasie (sprawdzenie jest możliwe dzięki modułowi GPS, który znajduje się w smartfonie) i czy osoba faktycznie jest w danym momencie w pobliżu drzwi. Uprawnienia użytkownika mogą zostać zweryfikowane dzięki aplikacji w chmurze, a zezwolenie na dostęp może być wysłane do kontrolera drzwi w formie poufnej wiadomości bezpiecznym kanałem komunikacyjnym.

Trend trzeci: fizyczne zabezpieczanie i kontrolowanie dostępu zmierza w stronę wykorzystania rozwiązań IP, które łatwiej zastosować i serwisować

Standardowy system wykorzystujący IP ułatwia integrację systemu fizycznej kontroli dostępu z innymi systemami, które mogą wykorzystywać tę samą sieć. Główna korzyść to „przeniesienie inteligencji na kontrolowane drzwi", które usprawnia ich monitorowanie, zarządzanie i raportowanie za pośrednictwem standardowych przeglądarek internetowych. Dzięki zastosowaniu inteligentnych kontrolerów IP o otwartej architekturze i zainwestowaniu w sprzęt, którego funkcjonowanie nie jest zależne od zastosowania zastrzeżonych protokołów i oprogramowania, można uprościć przyszłe usprawnienia i modyfikacje infrastruktury.

Trend czwarty: elektroniczne systemy kontroli gości będą coraz częściej wykorzystywane nie tylko przez przedsiębiorstwa prowadzące typową działalność biznesową, ale również w szkołach, szpitalach i w innych miejscach, gdzie miały miejsce znane incydenty, które dowiodły, że ochrona nie powinna ograniczać się do odnotowywania wizyt w papierowych rejestrach

Elektroniczne systemy kontroli gości są wykorzystywane coraz częściej. Przykładowo – w szpitalu papierowe rejestry są zastępowane systemami rejestracji, dzięki którym można wydawać gościom identyfikatory i sprawdzać, gdzie się znajdują, z wykorzystaniem filtrowanych list zdarzeń lub przynajmniej kontrolować najważniejsze obszary, takie jak oddział pediatryczny, czy też sprawdzać, co dzieje się w danych miejscach po godzinach pracy, gdy liczba obecnych pracowników jest mniejsza. Zaletą elektronicznego systemu kontroli gości jest też możliwość uzyskania przez osobę przybyłą do szpitala, by odwiedzić pacjenta, aktualnych informacji dotyczących jego statusu i miejsca pobytu, a zatem odwiedzający zawsze trafi do właściwego pokoju. Zastosowanie elektronicznych systemów kontroli gości w różnego rodzaju obiektach użyteczności publicznej umożliwia znacznie szybsze niż w przypadku korzystania z systemu papierowego przetwarzanie informacji i zbadanie zgodności procedur dostępu z lokalnymi przepisami.

John Fenske
Vice President of Product Marketing, Identity and Access Management w firmie HID Global
Tłumaczenie: Redakcja

Winkhaus blueSmart
Nowa generacja elektronicznej kontroli dostępu

Miron Łukaszczyk

Koncepcja systemu blueSmart narodziła się kilkanaście lat temu. Projekt, który wtedy stworzyła grupa specjalistów z firmy Winkhaus, był odpowiedzią na rosnące zapotrzebowanie na prosty w obsłudze, łatwy w montażu, a przede wszystkim niezawodny i tani w eksploatacji system kontroli dostępu

Oczywiście 150-letnie doświadczenie w produkcji mechanicznych systemów zabezpieczeń miało duży wpływ na koncepcję systemu – działanie poprzednika dzisiejszego blueSmarta, urządzenia o nazwie blueChip, bazowało na wykorzystaniu wkładek i kluczy. Od początku założenie twórców z Winkhausa było jasne: elektroniczny system kontroli dostępu ma w przyszłości bezboleśnie zastąpić mechaniczne systemy *master key*, eliminując ich najpoważniejsze wady i oferując dodatkowe właściwości, których nie mogą mieć urządzenia mechaniczne.

Fot. 1. blueSmart firmy Winkhaus to elektroniczny system wkładek otwieranych kluczem

Podstawowym elementem systemu blueSmart są wkładki, oczywiście w pełni zgodne wymiarowo z ich mechanicznymi odpowiednikami. Wkładki mają własne zasilanie, które zapewnia ich bezawaryjną pracę przez kilka lat. W zależności od wersji wkładki oraz częstotliwości użyć baterie umożliwiają zasilanie nawet przez dziesięć lat. W zależności od tego, czy instalujemy system blueSmart w drzwiach zewnętrznych czy wewnętrznych, należy zastosować odpowiednią wkładkę. Wkładki obu typów są oferowane przez firmę Winkhause. To zróżnicowanie bierze się z faktu, że w przypadku drzwi zewnętrznych wpływ niskich temperatur znacznie obniża sprawność baterii – wkładki do nich wyposaża się w bardziej wydajne baterie o większej pojemności.

Wyposażenie wkładek w baterie umożliwiło opracowanie klucza pasywnego, czyli pozbawionego własnego zasilania. Klucz blueSmart zawiera w swej strukturze transponder RFID, za pomocą którego jest identyfikowany przez wkładkę. Bezprzewodowa transmisja danych między wkładką a kluczem umożliwia nie tylko rozpoznawanie identyfikatora, ale również przenoszenie na klucz danych z wkładki. Wkładka zawiera bowiem w swej strukturze pamięć 2000 ostatnich zdarzeń. Przechowywane są informacje nie tylko o użytych we wkładce kluczach, ale również o prawach dostępu tych kluczy oraz dacie i godzinie wystąpienia zdarzenia, ponieważ każda wkładka blueSmart ma wbudowany zegar czasu rzeczywistego. Oprócz informacji o zdarzeniach wkładki zapisują na kluczu również informacje o stanie baterii oraz o sumarycznej liczbie otwarć w trakcie korzystania z danej baterii.

Klucz jako identyfikator w systemie blueSmart umożliwia zróżnicowany w czasie dostęp do wkładek. Zależnie od wersji oprogramowania, na kluczu można zapisać kilka profili czasowych z kilkudziesięciu dostępnych. W ten sposób z dokładnością do 15 minut można ograniczyć prawa dostępu dla poszczególnych użytkowników do określonych godzin w konkretne dni tygodnia. Możliwe jest umieszczenie na kluczu uprawnień do dostępu, które będą ważne dopiero od konkretnego dnia, do konkretnego dnia lub w jakimś ustalonym okresie – kiedy indziej klucz nie będzie aktywny. Oczywiście zmiany w prawach dostępu czy zmiany czasu ważności klucza są możliwe do przeprowadzenia w dowolnej chwili, bez ograniczeń. Także wszystkie profile czasowe mogą być dowolnie konfigurowane i wielokrotnie modyfikowane.

Jednym z najważniejszych elementów systemu blueSmart firmy Winkhaus jest czytnik online. To urządzenie jest punktem

Fot. 2. Poprzez czytnik online klucze użytkowników komunikują się z oprogramowaniem

dostępowym na stałe podłączonym do serwera w firmie. Jego zadaniem jest umożliwienie komunikowania się kluczy użytkowników z oprogramowaniem, za pomocą którego nadawane są prawa dostępu. Klucze użytkowników pośredniczą w wymianie informacji pomiędzy czytnikiem on-line a wkładkami. Takie bezprzewodowe połączenie oprogramowania z wkładkami za pomocą kluczy jest nazywane siecią wirtualną. Taką sieć współtworzą komponenty systemu, czyli wkładki i klucze, które *de facto* pracują offline, ale dzięki użyciu transponderów RFID nabywają cech urządzeń online.

Praca systemu blueSmart w praktyce wygląda następująco. Administrator wprowadza do oprogramowania wszystkie komponenty systemu. Lista wkładek z przypisanymi do nich drzwiami oraz lista kluczy z przydzielonymi do nich nazwiskami użytkowników tworzy w programie matrycę praw dostępu. Ustalanie uprawnień klucza sprowadza się do zaznaczenia pola na skrzyżowaniu kolumny (użytkownik) z wierszem (drzwi) i uwzględnienia ewentualnych profili czasowych. Tak przygotowany plan praw dostępu jest wysyłany do czytnika online, umieszczonego z reguły przy wejściu do budynku. Po zbliżeniu swojego klucza do czytnika użytkownik uzyskuje prawa dostępu na określony czas, na przykład na jeden dzień. Po tym czasie klucz przestaje działać i należy go ponownie aktywować w czytniku. Zorganizowana w ten sposób komunikacja z kluczem pozwala efektywnie zarządzać prawami dostępu. Każdy kontakt klucza z czytnikiem skutkuje również transmisją danych z klucza do czytnika. Dane te to informacje o zdarzeniach z wkładek używanych wcześniej oraz o stanie baterii znajdujących się w tych wkładkach. Wszystkie informacje są zapisywane w bazie danych na serwerze. Administrator może w dowolnej chwili przeglądać informacje o zdarzeniach z całej historii oraz segregować je, przyjmując jako kryteria czas wystąpienia zdarzenia i to, jakiego użytkownika i drzwi ono dotyczy.

W przypadku zgubienia klucza administrator blokuje go w oprogramowaniu zarządzającym systemu blueSmart, a informacja o tym natychmiast pojawia się w czytniku. Od tego momentu każdy klucz zbliżony do czytnika oprócz własnych praw dostępu pobiera również polecenie blokowania zgubionego klucza. Informacja jest przenoszona do każdej wkładki, która jest otwierana „poinformowanym" o blokadzie kluczem. Wkładki, które odebrały informacje o zablokowanym kluczu, przekazują je do innych kluczy. W ten sposób informacja o blokadzie klucza błyskawicznie roznosi się w systemie.

Fot. 3. Wkładki blueSmart mają identyczne wymiary jak powszechnie stosowane wkładki mechaniczne

Fot. 4. Zaletą systemu blueSmart jest brak okablowania, co czyni go doskonałym rozwiązaniem dla obiektów modernizowanych

Czasowa ważność klucza, która wymusza cykliczne aktywowanie go w czytniku, może być w niektórych przypadkach niepożądana. Oprogramowanie sterujące systemem blueSmart pozwala na ustawienie parametrów uprawnień klucza tak, by jego ważność nie wygasała. Podobnie jest w przypadku wkładek – jeśli użytkownik musi otworzyć drzwi bądź furtkę, która znajduje się przed punktem dostępowym, w którym aktywowany jest klucz, taką wkładkę określa się w programie jako „ignorującą" czasową utratę ważności klucza.

Uzupełnieniem systemu blueSmart są czytniki offline. Urządzenia te, konfigurowane podobnie jak wkładki, służą do sterowania innymi urządzeniami elektrycznymi. Po zbliżeniu uprawnionego klucza czytnik może załączyć elektrorygiel w drzwiach wejściowych, podnieść szlaban na parkingu bądź aktywować lub dezaktywować alarm. Identyfikatorem użytkownika może być w tym przypadku nie tylko klucz, ale również karta bądź brelok blueSmart.

Klucze systemu blueSmart są całkowicie bezobsługowe i bardzo trwałe. Winkhaus przewidział możliwość instalacji w kluczu dodatkowego transpondera. Dzięki niemu klucz może obsługiwać również inne systemy kontroli dostępu, w których wykorzystuje się identyfikatory RFID. Programiści z firmy Winkhaus zadbali również o zintegrowanie oprogramowania systemu blueSmart z popularnymi systemami hotelowymi.

Wkładki systemu blueSmart świetnie nadają się do obiektów zabytkowych i modernizowanych ze względu na ich dyskretny, prosty styl, brak konieczności instalacji dodatkowego okablowania i łatwość instalacji. System blueSmart firmy Winkhaus pozwala więc stworzyć wydajny, łatwy w zarządzaniu i tani w eksploatacji nowoczesny system kontroli dostępu, odpowiedni zarówno dla małych jak i bardzo dużych obiektów. W porównaniu do mechanicznych systemów dostępowych korzyści wynikające z użytkowania elektronicznego systemu blueSmart to przede wszystkim poprawa bezpieczeństwa i niskie koszty funkcjonowania.

Miron Łukaszczyk
Winkhaus Polska

25 1990 2015 | Satel®

INTELIGENTNE SYSTEMY ALARMOWE

2015 rokiem wyjątkowych **nowości SATEL**

Kontrolery **ACU-120** oraz **ACU-270**

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

Doskonałe zasięgi systemu bezprzewodowego i w pełni **bezprzewodowa obsługa**

- **w pełni bezprzewodowy** manipulator VERSA-LCDM-WRL
- nowe kontrolery ACU-120 i ACU-270 - **zasięg nawet do 500 m!**
- **obsługa central z serii VERSA** poprzez manipulator dotykowy **INT-TSG**

Więcej informacji na **www.satel.pl**

Satel Sp. z o.o.
ul. Budowlanych 66, 80-298 Gdańsk, tel.: (58) 320-94-00, fax: (58) 320-94-01,
e-mail: satel@satel.pl, **www.satel.pl**

Satel®

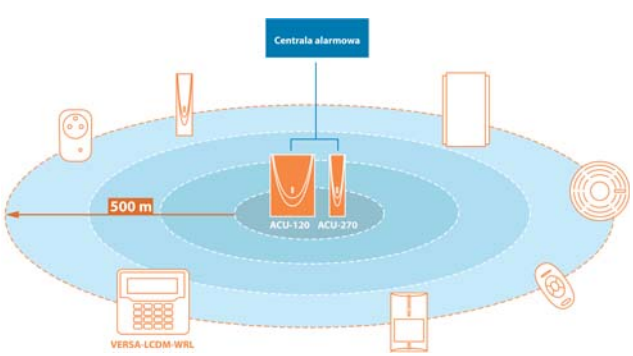
2015 rokiem nowości SATEL

SATEL

Przez wiele lat instalatorzy wykorzystywali powszechnie dostępne systemy przewodowe. Aktualnie coraz większą liczbę zwolenników zdobywają jednak systemy bezprzewodowe. Dlaczego tak się dzieje?

Technika łączności za pośrednictwem sygnału radiowego rozwija się bardzo dynamicznie, oferując coraz wyższą jakość. Dzięki temu systemy zabezpieczeń wykorzystujące urządzenia bezprzewodowe zapewniają jeszcze lepszą funkcjonalność, jeszcze więcej możliwości zastosowania oraz jeszcze wyższy poziom bezpieczeństwa. Wzrastająca popularność instalacji bezprzewodowych wynika także z ich atrakcyjnej ceny, prostego, szybkiego i czystego montażu, a także zachowania wszystkich funkcji i standardów charakterystycznych dla systemów przewodowych.

Wszystkie te cechy doceniane są zarówno przez profesjonalistów, którzy na co dzień projektują i instalują systemy zabezpieczeń, jak i właścicieli obiektów, którym zależy przede wszystkim na funkcjonalności, różnorodności zastosowań i wygodzie sterowania.



Rys. 1. Nowe kontrolery ACU-120 i ACU-270 zostały wyposażone w nowoczesny układ radiowy. Dzięki temu oferują doskonałe zasięgi – do 500 m w terenie otwartym

W związku z zapotrzebowaniem na początku roku do oferty firmy SATEL wprowadzone zostały nowe komponenty do budowy i obsługi bezprzewodowych systemów alarmowych: kontrolery ACU-120 i ACU-270, bezprzewodowy manipulator VERSA-LCDM-WRL, czytnik kart CZ-USB-1 oraz nowe wersje oprogramowania do manipulatora INT-TSG oraz do central z serii VERSA.

Doskonałe zasięgi urządzeń bezprzewodowych

Dwa nowe kontrolery – uniwersalny ACU-120 oraz miniaturowy ACU-270 – są elementami systemu ABAX. Współpracują

Fot. 1. Oprócz doskonałych zasięgów kontrolery ACU-120 i ACU-270 oferują także nowe możliwości obsługi systemu alarmowego wykorzystującego centrale z rodziny VERSA. Umożliwiają bowiem sterowanie nim za pomocą nowego, w pełni bezprzewodowego manipulatora VERSA-LCDM-WRL

z centralami z rodzin INTEGRA i VERSA, umożliwiając powiększenie stworzonego na ich podstawie systemu alarmowego o urządzenia bezprzewodowe. Oba kontrolery zostały wyposażone w nowoczesny układ radiowy, dzięki któremu zapewniają doskonały zasięg działania – w terenie otwartym jest to nawet 500 m. ACU-120 ma dodatkowo system dywersyfikacji anten, który wpływa na poprawę jakości sygnału.

Fot. 2. W pełni bezprzewodowy manipulator do sterowania systemem bazującym na centralach z serii VERSA

W pełni bezprzewodowa obsługa systemu alarmowego

VERSA-LCDM-WRL to pierwszy w ofercie firmy SATEL w pełni bezprzewodowy manipulator umożliwiający zdalną obsługę i programowanie central z serii VERSA. Dzięki współpracy z opisanymi wyżej kontrolerami ACU-120 i ACU-270 zasięg pracy VERSA-LCDM-WRL wynosi nawet 500 m! Co więcej, ten bezprzewodowy manipulator realizuje wszystkie funkcje swojego przewodowego odpowiednika. Został także wyposażony w czytnik, który umożliwia wygodną obsługę systemu za pomocą kart zbliżeniowych i breloków, dzięki którym możliwe jest pełne załączenie i wyłączenie czuwania, a także skasowanie alarmu.

VERSA-LCDM-WRL to urządzenie ekonomiczne – ma wbudowaną osobną baterię w celu podświetlenia wyświetlacza i klawiatury. Dzięki takiemu rozwiązaniu czas pracy tego manipulatora może wynieść nawet trzy lata. W celu jeszcze większego ograniczenia zużycia baterii możliwe jest wyłączenie czytnika kart zbliżeniowych (jeżeli nie przewiduje się obsługi systemu alarmowego za jego pomocą). Obudowa manipulatora umożliwia szybki i prosty montaż w dogodnym miejscu.

Fot. 4. Czytnik umożliwia wygodne i szybkie przydzielanie użytkownikom nowych kart i breloków

Wygodne wczytywanie kart

Kolejną nowością jest CZ-USB-1, czyli czytnik przyłączany bezpośrednio do portu USB komputera. To zupełna nowość w ofercie firmy SATEL, umożliwiająca szybkie i wygodne przydzielanie użytkownikom nowych kart, breloków itp. bezpośrednio w programie DLOADX. To proste i przydatne rozwiązanie oszczędza czas i usprawnia pracę każdego, kto zajmuje się administracją systemu alarmowego!

Nowe funkcje znanych urządzeń

Jak już wspomniano, nowości wprowadzane przez SATEL na początku roku obejmują także oprogramowanie do urządzeń znajdujących się już w ofercie firmy. Pierwsza zmiana dotyczy oprogramowania INT-TSG (firmware), które zostało zaktualizowane do wersji 1.03. Dzięki niej manipulator dotykowy INT-TSG umożliwia obsługę systemu alarmowego stworzonego na bazie centrali z rodziny VERSA. Aby skorzystać z takiej opcji, należy zaktualizować firmware centrali VERSA 5, 10 lub 15 do wersji 1.04. Co więcej, to samo oprogramowanie dla central VERSA umożliwia ich obsługę za pomocą opisanego wyżej w pełni bezprzewodowego manipulatora VERSA-LCDM-WRL.

Wersja 1.03 oprogramowania do manipulatora INT-TSG, oprócz sterowania systemem alarmowym zbudowanym na bazie centrali z rodziny VERSA, umożliwia także regulację głośności bezpośrednio za pomocą manipulatora, włączenie opcji wybudzania oraz zastosowanie manipulatora w charakterze ramki fotograficznej.

Aktualne wersje oprogramowania do obu urządzeń można pobrać ze strony *www.satel.pl.* Na tej stronie ukazały się także informacje o kolejnych nowościach, jakie firma SATEL proponuje wszystkim swoim klientom w roku 2015.

SATEL

Fot. 3. Dzięki firmware'owi w wersji 1.04 centrale alarmowe z rodziny VERSA umożliwiają obsługę systemu za pomocą manipulatorów bezprzewodowych VERSA-LCDM-WRL i manipulatorów z ekranem dotykowym INT-TSG

Wirtualizacja układów sterowania obrotnicami kamer PTZ w wizyjnych systemach dozorowych

Marcin Buczaj

Praca na stanowisku operatora wizyjnego systemu dozorowego polega na obserwowaniu obrazu wytwarzanego przez kamery oraz zarządzaniu pracą urządzeń dostępnych w systemie, w szczególności kamer PTZ. Kamery PTZ mają możliwość zmiany kierunku i kąta widzenia, dzięki czemu umożliwiają dopasowanie wielkości obserwowanej strefy dozorowej do aktualnych wymagań użytkownika. Do zarządzania pracą kamer PTZ służą najczęściej specjalne manipulatory. Po odpowiednim skonfigurowaniu manipulatora i przystosowaniu go do pracy z danym urządzeniem możliwa jest zmiana ustawień kamer PTZ. Ograniczeniem wynikającym z takiego rozwiązania jest konieczność ciągłego realizowania procedur umożliwiających realizację poszczególnych funkcji oraz możliwość wysterowania w danym momencie tylko jednej kamery. Można wykorzystać narzędzia wirtualne jako dodatkowe elementy wizyjnego systemu dozorowego, usprawniające sterowanie kamerami PTZ i ułatwiające pracę operatora przez uwolnienie go od konieczności żmudnego konfigurowania systemu. Koncepcja wirtualizacji systemów sterowania i nadzoru, przedstawiona na przykładzie sterowania pracą kamer PTZ w systemach CCTV, umożliwia zapoznanie się z nowymi możliwościami i wykorzystanie dostępnych narzędzi programistycznych przy tworzeniu zindywidualizowanych, dopasowanych do potrzeb użytkownika systemów zarządzania pracą urządzeń

1. Wstęp

Projektowanie wizyjnego systemu dozorowego od strony technicznej to określenie warunków użytkowych, w tym sprecyzowanie rodzaju zagrożeń, wyznaczenie obszarów, stref oraz celu stosowania systemu, określenie stopnia jego automatyzacji oraz sposobu sterowania i nadzorowania. Obsługa wizyjnego systemu dozorowego to nadzorowanie jego pracy, sterowanie i zarządzanie ustawieniami kamer, analiza rejestrowanego materiału wizyjnego oraz bieżącą kontrola prawidłowości pracy systemu. Administrowanie systemem to dopasowywanie sterowania do konkretnych wymagań w związku ze specyfiką obiektu, sprzętu i oprogramowania. Wszystkie przedstawione działania mają na celu opracowanie koncepcji, stworzenie i wdrożenie skutecznego systemu nadzoru umożliwiającego realizację założonych celów ochrony.

Jeśli system jest funkcjonalny i ergonomiczny, a operator doświadczony, można dostosowywać parametry rejestrowanego obrazu do aktualnie realizowanych zadań związanych z obserwacją danego obszaru. Dopasowanie

układów sterowania pracą urządzeń zastosowanych w wizyjnym systemie dozorowym do indywidualnych potrzeb użytkownika umożliwia lepsze i skuteczniejsze wykorzystanie posiadanych środków oraz zasobów sprzętowych i ludzkich.

Istnieje możliwość stworzenia wirtualnego systemu nadzoru. Fizyczne urządzenia sterujące i obrazujące (manipulatory, centrale alarmowe) zastępuje się ich software'owymi odpowiednikami. System bazuje na sprzęcie mikrokomputerowym z odpowiednim oprogramowaniem. Do tworzenia takich wirtualnych narzędzi umożliwiających sterowanie ustawieniami kamer PTZ i nadzorowanie pracy systemu wykorzystano środowisko programistyczne LabView. Wybranie go nie było przypadkowe. LabView jest wiodącym środowiskiem programistycznym umożliwiającym tworzenie aplikacji mających związek z różnymi dziedzinami techniki i jest obecnie powszechnie stosowane przy tworzeniu aplikacji sterujących, nadzorujących i diagnostycznych w różnych dziedzinach nauki i techniki.

2. Wizyjny system dozorowy

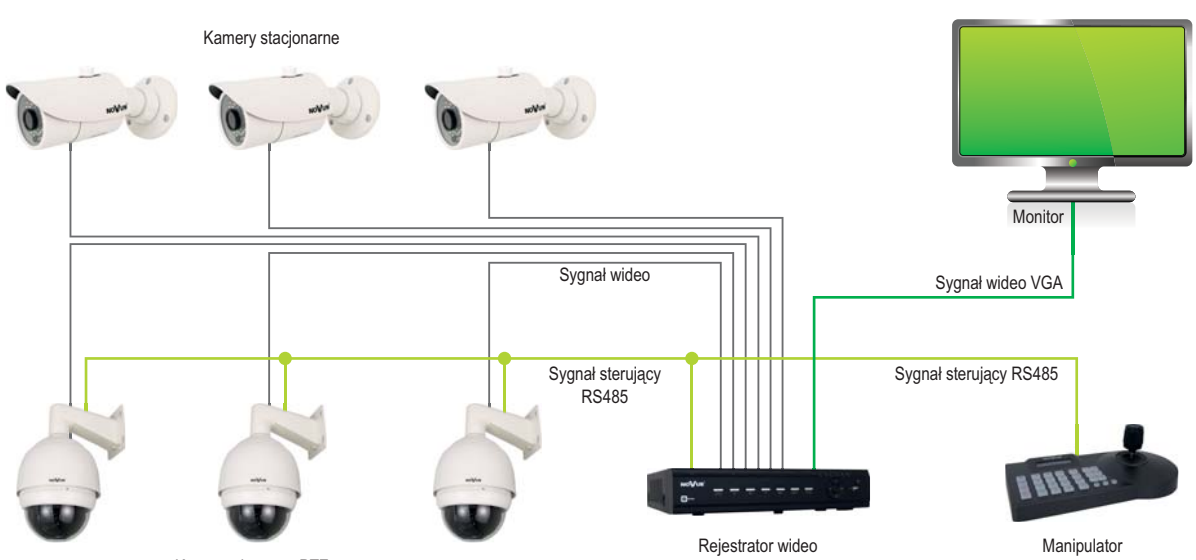
Wizyjny system dozorowy służy do obserwowania określonej strefy dozorowanej za pomocą odpowiedniego sprzętu. Dzięki obserwacji wiadomo, jaka jest sytuacja w danym miejscu – jaki jest stan tego miejsca. Obraz jest więc nośnikiem informacji. W skład wizyjnego systemu dozorowego (rys. 1) wchodzą elementy podstawowe służące do rejestracji obrazu (podsystem obserwacji), elementy służące do przesyłania sygnału wizyjnego (podsystem transmisji) oraz do jego wyświetlania (podsystem odbioru), a także układy (podsystemy) uzupełniające, które służą do archiwizacji rejestrowanego obrazu i do sterowania ustawieniami poszczególnych elementów systemu (kamer, obrotnic itp.) [1, 2, 3, 5].

Podstawowym elementem każdego wizyjnego systemu dozorowego jest kamera. Ze względu na funkcje, rolę w systemie oraz cenę można wyróżnić dwa typy kamer: kamery stacjonarne i kamery obrotowe. Zazwyczaj kamery stacjonarne są wykorzystywane do obserwacji stref dozoru ogólnego, natomiast kamery obrotowe – ze względu na więcej możliwości ustawień – do dozoru stref szczególnie istotnych (newralgicznych) w chronionym obiekcie. Poprzez zmianę parametrów układu optycznego kamery oraz jej ustawienia możliwe jest dopasowanie wielkości obserwowanej strefy dozorowej do aktualnych wymagań użytkownika. Zmiana parametrów PTZ (P – *panorama* – obrót, T – *tilt* – nachylenie, Z – *zoom* – zbliżenie) jest możliwa poprzez wykorzystanie układu sterowania.

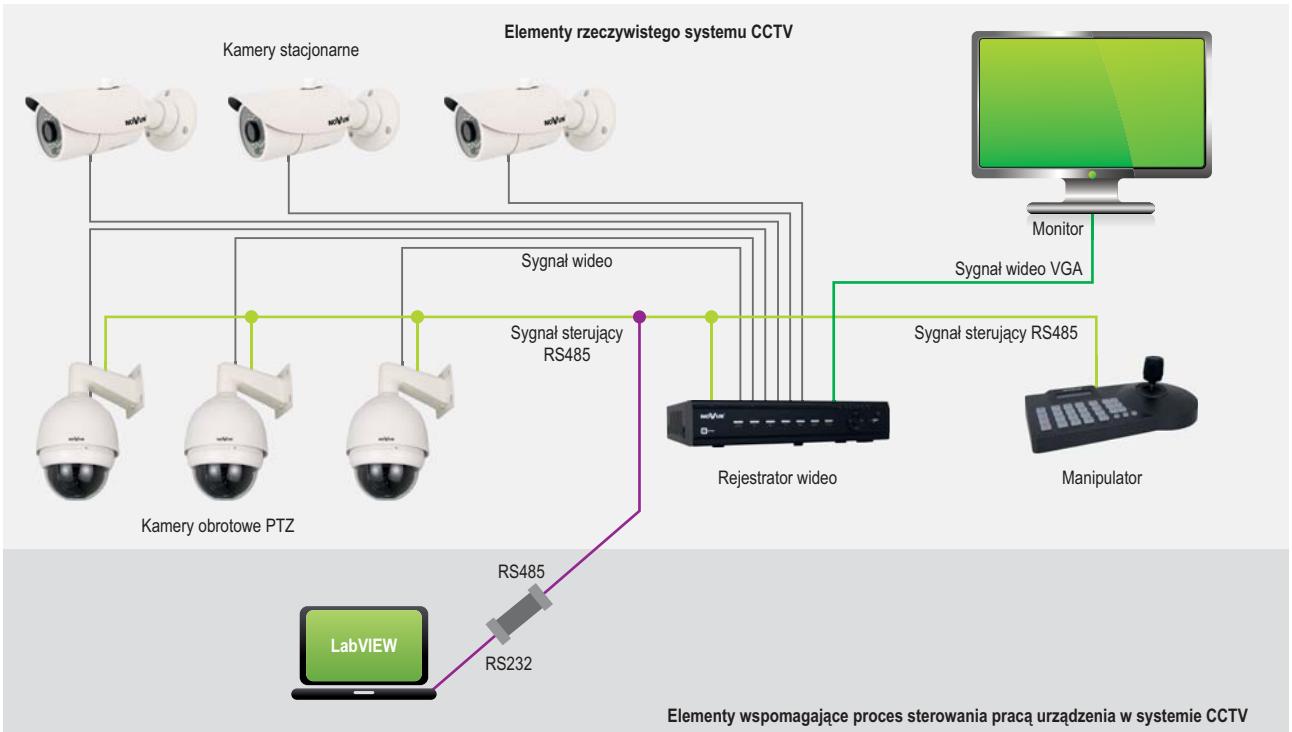
Układ sterowania pracą kamer PTZ bazuje zarówno na sprzęcie, jak i na oprogramowaniu. Warstwa sprzętowa to infrastruktura techniczna umożliwiająca fizyczne przesyłanie sygnału sterującego. Najbardziej rozpowszechnionym systemem przesyłu sygnału sterującego jest system przewodowy dostosowany do pracy w standardzie RS485. Standard RS485 został wprowadzony jako rozwinięcie standardu RS422A. Składa się z różnicowego (symetrycznego) nadajnika, dwuprzewodowego toru transmisyjnego i różnicowego odbiornika. Standard RS485 dopuszcza łączenie wielu nadajników i odbiorników na jednej linii [5]. Warstwa programowa układu sterowania pracą kamer PTZ to wybrany system transmisji sygnału wykorzystujący identyczny standard protokołu sterującego, taki sam dla elementu sterującego (manipulator) i sterowanego (kamera). Wybrany standard przesyłu nie musi być jednakowy dla wszystkich elementów systemu. Ważne jest, aby w danym momencie istniała korelacja (zgodność protokołu) między urządzeniem sterującym a sterowanym. W praktyce wykorzystywanych jest wiele standardów przesyłu, jednak największą popularność zyskały otwarte protokoły PTZ: Pelco-D i Pelco-P [7, 8]. Zarządzanie pracą wizyjnych systemów dozorowych zależy od wyboru elementów umożliwiających sterowanie ustawieniami kamer obrotowych PTZ. Kamerami PTZ można sterować sprzętowo, za pomocą manipulatorów, lub programowo, za pomocą aplikacji sterujących.

3. Idea platformy programowej zarządzającej pracą kamer PTZ

Przedstawiony na rys. 1 klasyczny wizyjny system dozorowy jest systemem autonomicznym, zbudowanym z elementów



Rys. 1. Schemat instalacji systemu monitoringu wizyjnego CCTV



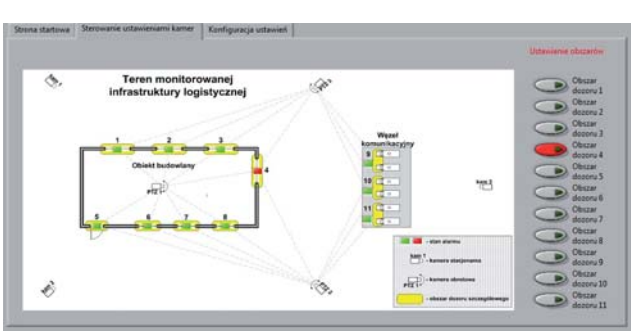
Rys. 2. Schemat ideowy wizyjnego systemu dozorowego z wirtualnym układem umożliwiającym sterowanie pracą kamer PTZ za pomocą aplikacji komputerowej

przeznaczonych do pracy w wizyjnych systemach dozorowych. Wadą takich rozwiązań jest hermetyczność, zarówno pod względem sprzętowym, jak i funkcjonalnym. Zaproponowana modernizacja klasycznego wizyjnego systemu dozorowego (rys. 1) polega na zastosowaniu wirtualnego systemu zarządzania pracą kamer PTZ (rys. 2). Taki układ ma za zadanie zwiększenie funkcjonalności systemu oraz zintegrowanie w większym stopniu poszczególnych systemów sterowania i nadzoru zainstalowanych w chronionym obiekcie. Dodatkowo umożliwia dopasowanie procedur sterujących do indywidualnych potrzeb użytkownika.

Podstawą działania wirtualnych systemów zarządzania pracą kamer PTZ jest aplikacja umożliwiająca sterowanie i kontrolowanie pracy wizyjnego systemu dozorowego przez mikrokomputerowy system nadzorujący stan chronionego obiektu. Aplikacja ta może zostać stworzona z wykorzystaniem dowolnego środowiska programistycznego. Ze względu na możliwości programowe, sprzętowe oraz uniwersalność zastosowań, a także dużą rozpoznawalność marki, tworzone aplikacje i wirtualne systemy sterujące mogą bazować na graficznym środowisku programistycznym LabView. LabView umożliwia realizację złożonych funkcji w procesach akwizycji i archiwizacji oraz podczas przetwarzania i analizy danych pomiarowych. Dodatkową zaletą aplikacji stworzonych w programie LabView jest ich indywidualność. Możliwe jest nie tylko wykorzystanie pewnych schematów, ale także wyposażenie programów w unikatowe rozwiązania proceduralne. Umożliwia to dopasowanie aplikacji do zmian zachodzących w zabezpieczanym obiekcie (np. do zmian architektonicznych, zmiany przeznaczenia poszczególnych pomieszczeń). LabView umożliwia swobodne kreowanie struktur programowych systemów pomiarowych i symulacyjnych, a walory środowiska LabView są często doceniane przez projektantów aplikacji wykorzystywanych w systemach sterowania nadzorujących przemysłowe procesy technologiczne, diagnostyczne oraz kontrolno-pomiarowe [4, 6].

4. Wirtualny system sterowania pracą kamer PTZ ułatwiający pracę operatora systemu

Dla realizacji zadań związanych z nadzorowaniem chronionego obiektu przez wirtualny wizyjny system dozorowy, stworzony z wykorzystaniem oprogramowania LabView, utworzono platformę programową w postaci aplikacji umożliwiającej jednoczesne sterowanie wieloma kamerami PTZ. Głównym zadaniem aplikacji jest generowanie sygnału przesyłanego do układu sterującego w postaci komunikatu (łańcucha kodów instrukcji), który umożliwia skierowanie kamer obrotowych ku wybranej strefie dozoru. Sterowanie kamerami PTZ polega na tym, że wybiera się jedno z wcześniej określonych ustawień. Z powodu braku interfejsu RS485 w standardowym komputerze PC konieczne jest wyposażenie układu w konwerter RS232/RS485 lub USB/RS485.



Rys. 3. Schemat terenowy obiektu z zaznaczonymi strefami dozoru szczegółowego

Obszar dozoru	1	2	3	4	5	6	7	8	9	10	11
Kamera PTZ 1	1	2	3	4	5	6	7	8	-	-	-
Kamera PTZ 2	-	-	-	1	2	3	4	5	6	7	8
Kamera PTZ 3	1	2	3	4	-	-	-	-	5	6	7

Tab. 1. Zdefiniowane ustawienia kamer obrotowych PTZ – tabela powiązań

Istotnym elementem etapu projektowania wirtualnego narzędzia wspomagającego proces sterowania ustawieniami kamer PTZ w wizyjnym systemie dozorowym jest określenie stref dozoru w obszarze chronionej infrastruktury, zarówno dozoru ogólnego (rys. 4), jak i szczegółowego (rys. 3). Obszary newralgiczne powinny być wskazane na podstawie oceny możliwości wystąpienia w nich zagrożenia lub możliwości kontrolowania przemieszczania się obiektów.

Ważnym elementem analizy indywidualnych możliwości systemu oraz tworzenia procedur sterowania (generowania instrukcji sterujących) jest określenie technicznych możliwości obserwowania danego obszaru przez poszczególne kamery. W tym celu konieczne jest wykonanie tabeli powiązań, indywidualnej dla każdego obiektu. Przykładową tabelę powiązań zdefiniowanych ustawień kamer PTZ, umożliwiających realizację celów obserwacji stref szczególnego dozoru (rys. 3), przedstawiono poniżej. Tabela taka przedstawia zależności między zdefiniowanymi ustawieniami poszczególnych kamer PTZ a obszarami szczególnego dozoru.

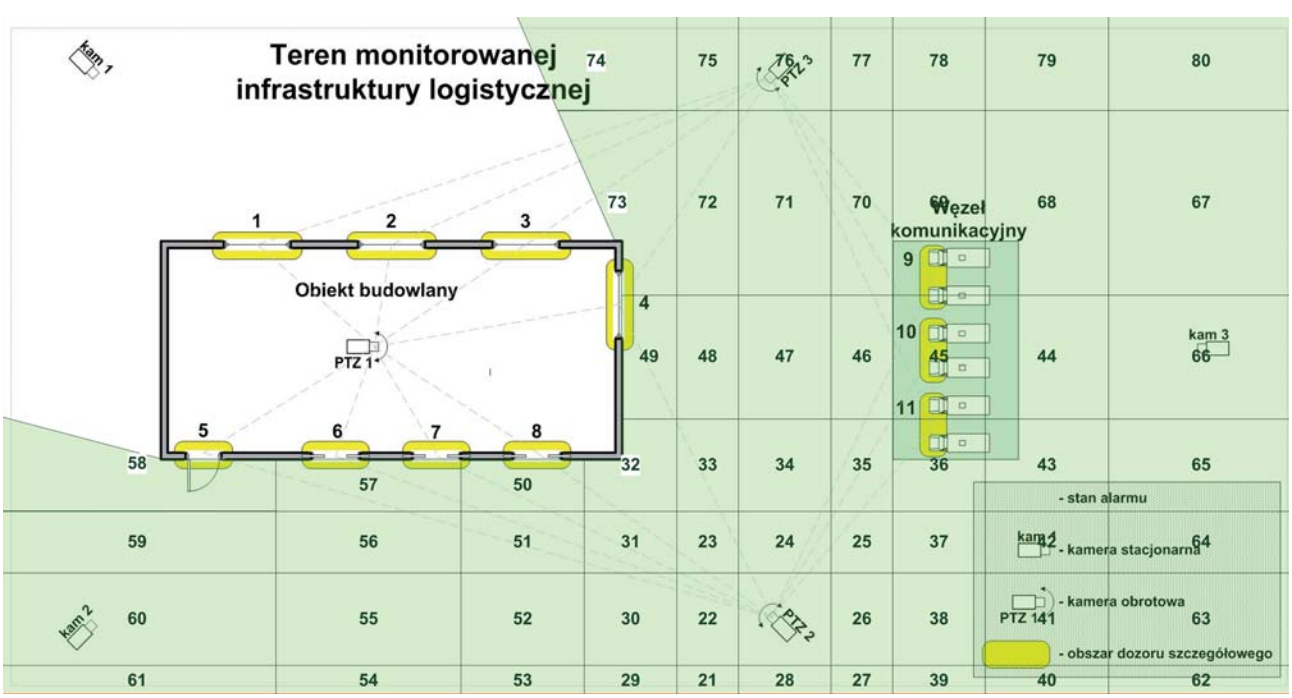
Przykładowy komunikat (łańcuch komend) zgodny ze standardem Pelco-P (kod heksadecymalny), generowany i przesyłany do układu sterującego (RS485) przez aplikację wspomagającą zarządzanie zdefiniowanymi ustawieniami kamer, umożliwiający ustawienie wszystkich dostępnych kamer tak, by obserwowały obszar szczególnego dozoru nr 4, ma postać:

A0 01 00 07 00 04 AF 0D;
A0 02 00 07 00 01 AF 0B;
A0 03 00 07 00 04 AF 0F.

W sposób analogiczny do przedstawionego na rys. 4 tworzone są obszary powiązane ze zdefiniowanymi ustawieniami dla wszystkich kamer PTZ wchodzących w skład wizyjnego systemu dozorowego. Poszczególne obszary są obszarami polowymi i odpowiadają pewnym obszarom okna dialogowego programu wyświetlanego na ekranie monitora. Zatem każdemu przypisanemu pikselowi na mapie synoptycznej (schemacie terenowym) chronionego obiektu przypisane są zależności odwołujące się do procedur wykonawczych służących do wywołania ściśle określonych, zdefiniowanych ustawień wszystkich kamer wchodzących w skład wizyjnego systemu dozorowego.

Operator systemu nie musi zajmować się każdą z kamer z osobna, lecz może dokonać zmian w ustawieniach tych kamer przez wywołanie odpowiednich procedur. Jeżeli stanowisko operatora jest wyposażone w monitor dotykowy, przewaga wirtualnego systemu sterowania nad systemem tradycyjnym, „sprzętowym", jest jeszcze bardziej widoczna.

Dodatkową opcją jest integracja wirtualnego systemu sterowania pracą kamer PTZ z innymi systemami zabezpieczeń. W takim przypadku zmiana ustawień kamer może nastąpić automatycznie, bez udziału operatora, po otrzymaniu i zinterpretowaniu sygnału informacyjnego pochodzącego z elementu detekcyjnego.



Rys. 4. Schemat terenowy obiektu z zaznaczonymi strefami dozoru ogólnego dla kamery PTZ2 i ze zdefiniowanymi ustawieniami tej kamery

Operator dysponuje mapą synoptyczną chronionego obiektu wyświetlaną na ekranie monitora. Miejsca na mapie odpowiadają rzeczywistym fragmentom terenu.

5. Podsumowanie

Skuteczne działanie wizyjnego systemu dozorowego zależy od właściwego współdziałania operatora z systemem i prawidłowego wykorzystania dostępnego sprzętu. Warto zainwestować nie tylko w najlepszy sprzęt umożliwiający rejestrację i archiwizację materiału wizyjnego, ale także w wyposażenie dodatkowe, dzięki któremu operator nie będzie musiał wykonywać zbędnych, skomplikowanych lub czasochłonnych czynności.

Wyposażenie klasycznego wizyjnego systemu dozorowego w opisany w artykule układ usprawniający proces zarządzania i sterowania ustawieniami kamer PTZ umożliwia szybki podgląd wybranej newralgicznej strefy w chronionym obiekcie za pośrednictwem wszystkich dostępnych w systemie kamer. Zadaniem operatora jest wybór interesującego go obszaru na mapie synoptycznej obiektu. Zmiana aktualnych ustawień kamer na zdefiniowane ustawienia związane z podglądem wskazanego obszaru przebiega płynnie i bezobsługowo. Znacznie skraca to czas potrzebny na zmianę ustawień kamer w porównaniu z ręczną obsługą urządzeń sterujących oraz umożliwia jednoczesne skierowanie wielu kamer ku wybranemu obszarowi.

Dalsza integracja systemu sterowania ustawieniami kamer PTZ z innymi systemami zabezpieczającymi (systemami sygnalizacji włamania i napadu, systemami kontroli dostępu oraz systemami sygnalizacji pożarowej) umożliwia automatyczną zmianę ustawień kamer w celu podglądu danej strefy w momencie wystąpienia zagrożenia lub w czasie przebiegu założonej procedury.

dr inż. Marcin Buczaj
Politechnika Lubelska
Wydział Elektrotechniki i Informatyki

Literatura

1. PN-EN 50132-7:2003 *Systemy alarmowe. Systemy dozorowe CCTV stosowane w zabezpieczeniach. Część 7: Wytyczne stosowania*, Wydawnictwo PKN, Warszawa 2003.
2. M. Buczaj, *System jednoczesnego sterowania ustawieniami kamer obrotowych systemu CCTV do zastosowania w nadzorze infrastruktury logistycznej*, Logistyka nr 3/2011, s. 215-222.
3. M. Buczaj, *Systemy sterowania i nadzoru szyte na miarę, Zabezpieczenia* nr 6(88)/2012, s. 20–24.
4. M. Chruściel, *LabVIEW w praktyce*, Wydawnictwo BTC, Legionowo 2008.
5. P. Kałużny, *Telewizyjne systemy dozorowe*, Wydawnictwo WKiŁ, Warszawa 2008.
6. W. Tłaczała, Środowisko LabVIEW w eksperymencie wspomaganym komputerowo, WNT, Warszawa 2002.
7. *http://sklep.delta.poznan.pl/pdf/pelcop_sot.pdf – specyfikacja standardu Pelco-P*
8. *http://videon.spb.ru/pelco-p.doc – specyfikacja standardu Pelco-P*

Znaczenie pamięci masowej w systemach zabezpieczeń

Leo Waldock

Coraz większa ilość rejestrowanego materiału wizyjnego, rosnąca liczba i możliwości kamer oraz nowe techniki analizy treści obrazu umożliwiające śledzenie osób lub pojazdów wymagają szybkiego dostępu do zarchiwizowanych danych. W odpowiedzi na te wymagania firma WD stworzyła serię dysków twardych przeznaczonych na rynek zabezpieczeń technicznych. Według producenta sprawdzą się one o wiele lepiej niż zwykłe dyski komputerowe, a nawet dyski AV

W większości systemów zabezpieczeń niezawodność działania dysku twardego ma kluczowe znaczenie – jeżeli ten element ulegnie awarii, cały system nie będzie funkcjonował poprawnie. Oczywiście uszkodzony dysk można wymienić w ramach gwarancji, ale to nie przywróci utraconych danych.

W handlu detalicznym komputerowe dyski twarde o pojemności 1 TB kosztują 220 zł, a dyski o pojemności 2 TB około 320 zł. Za nowe wyspecjalizowane napędy trzeba zapłacić o około 60 zł więcej od standardowych modeli przeznaczonych do pracy w komputerach, ale za to poziom bezpieczeństwa zarejestrowanych danych jest nieporównywalnie wyższy. To szczególnie interesująca propozycja dla osób tworzących niedrogie systemy dozoru wizyjnego, w których koszt instalacji rozbudowanej nagrywarki z kilkoma dyskami w układzie RAID jest wyższy od zakupu pojedynczego wyspecjalizowanego dysku o wysokiej niezawodności. Jeśli weźmiemy pod uwagę fakt, że jedna czwarta rejestratorów dostępnych na rynku ma jeden lub dwa miejsca na dyski twarde, a kolejna ćwiartka ma zaledwie cztery miejsca, koszt wymiany dysków na specjalistyczne stanowi zaledwie niewielką część kosztów całego systemu. Ogromna ilość danych generowanych przez kamery HD to kolejny, nie mniej ważny powód do wymiany starszych dysków na nowe, lepiej przystosowane modele.

Każda kamera z matrycą o rozdzielczości 1,3 megapikseli (720p) wytwarza obraz o czterokrotnie większej liczbie pikseli w porównaniu z kamerą o rozdzielczości VGA. Zdawałoby się, że możliwość rejestracji danych na lokalnej karcie SD rozwiązuje problem przesyłania danych przez sieć, ale należy również wziąć pod uwagę korzyści, jakie zapewnia możliwość scentralizowanej rejestracji obrazu na dysku twardym umieszczonym w bezpiecznym miejscu.

Jedynie około 30–40% stosowanych obecnie w Europie rejestratorów wizyjnych zapisuje obrazy o rozdzielczości HD. Nawet jeśli różnica w cenie urządzeń rejestrujących obrazy w formacie 720p i urządzeń rejestrujących obrazy w formacie 1080p maleje, te pierwsze wciąż cieszą się większą popularnością, głównie ze względu na fakt, że materiały wizyjne o wyższej rozdzielczości zajmują więcej przestrzeni dyskowej, a ich przesłanie wymaga wykorzystania sieci o większej przepustowości. W odczuciu większości projektantów i instalatorów wizyjnych systemów dozorowych właśnie ta przepustowość jest największym kłopotem, mimo rosnącej popularności sieci lokalnych.

Wkrótce we wszystkich systemach dozorowych obrazy będą rejestrowane w trybie 720p. Popularyzacja kamer z matrycami o rozdzielczościach 3 i 5 megapikseli, które wytwarzają obrazy w trybie 1080p, podwoi objętość danych przesyłanych przez sieć i zapisywanych na bezlitośnie eksploatowanym dysku twardym.

Napęd stworzony z myślą o systemach monitoringu

W ostatnich latach poczyniono znaczące postępy w dziedzinie gęstości zapisu danych na dyskach twardych. Producenci usprawnili powłokę magnetyczną, dopracowali konstrukcję głowic, a także zwiększyli dokładność serwomechanizmów kontrolujących ustawienie głowic. Wprowadzono także usprawnienia w układach pamięci podręcznej, kontrolerach dysków twardych oraz interfejsach dyskowych.

Kilka lat temu dyski WD Caviar miały pojemność 400 GB rozproszoną na czterech talerzach i kosztowały 780 zł. Dzisiaj dyski WD Purple o pojemności 4 TB kosztują 700 zł, czyli w ciągu 8 lat pojemność dysków wzrosła dziesięciokrotnie.

Zwiększenie gęstości zapisu danych zapewnia same korzyści, ponieważ większa gęstość upakowania informacji oznacza mniejsze opóźnienia i większą wydajność w procesie zapisu i odczytu danych. Zmniejszenie liczby talerzy zmniejsza również koszty produkcji. To dlatego napęd o pojemności 1 TB z pojedynczym talerzem jest tak tani.

Warto zauważyć, że od końca 2011 roku gęstość zapisu danych nie uległa zwiększeniu i do tej pory nie przekroczyła 1 TB na talerz. Zamiast tego zaczęto kłaść nacisk na optymalizację dysków przeznaczonych do konkretnych zastosowań. Firma WD zapoczątkowała ten trend od wprowadzenia serii dysków, które były oznakowane za pomocą kolorów. Seria czarna (Black) to modele o wysokiej wydajności, cechujące się wysoką prędkością obrotową talerzy, dużą objętością pamięci podręcznej, zastosowaniem dwóch kontrolerów. Seria zielona (Green) jest przyjazna środowisku (talerze obracają się wolniej, mechanizm pracuje ciszej). Jest też seria niebieska (Blue), która stanowi rozwiązanie pośrednie między modelami Black i Green.

Wprowadzenie w 2013 roku dysków WD Red przeznaczonych do pracy w systemach NAS było intrygującym posunięciem. Dyski Red działają podobnie do modeli Green, ale zmodyfikowano zastosowane w nich oprogramowanie układowe. Dysk twardy z serii Red potrafi sprawdzać, czy nie występują na nim błędy, i w razie potrzeby realizuje proces odzyskiwania informacji. Jeśli będzie to konieczne, napęd oznaczy dany sektor jako uszkodzony i przeniesie dane na inny. Funkcja ta nosi nazwę TLER (Time Limited Error Recovery) i zapewnia wymierne korzyści w systemach operacyjnych Linux stosowanych w urządzeniach NAS różnych producentów, na przykład firm QNAP czy Synology. Innymi słowy – dzięki zmodyfikowanemu oprogramowaniu układowemu dyski Red lepiej funkcjonują w systemach NAS.

W 2014 roku firma WD wprowadziła na rynek dyski Purple przeznaczone do pracy w wizyjnych systemach dozorowych

Mówiąc ogólnie, dyski twarde przeznaczone do przechowywania materiału wizyjnego są zwykłymi dyskami, z których usunięto funkcję korekcji błędów. Mogą one funkcjonować w każdym rejestratorze. W niektórych przypadkach producenci rejestratorów poświęcają zbyt mało czasu na zaprojektowanie systemów, które

Fot. 1. Dysk twardy do systemów monitoringu – WD Purple

współpracują z każdym dyskiem twardym, więc awarie nie zawsze są winą producentów dysków twardych. To skomplikowana sprawa i użytkownicy nie zawsze posiadają wszystkie potrzebne im informacje. Nic więc dziwnego, że czasami rejestratory zostają wyposażone w nieprawidłowe dyski, a tańsze urządzenia nie mogą obsłużyć dużych przestrzeni pamięci.

Napędy AV pracujące w domowych rejestratorach są silnie obciążone, gdyż nagrywają dwa strumienie wizyjne w trybie 720p, jednocześnie odtwarzając trzeci strumień. Prawdopodobnie w tle realizowane jest także indeksowanie, a wypadkowe obciążenie dysku jest przewidywalne. Najważniejsze wymagania dotyczące dysków AV to duża pojemność, niska cena i bardzo niski poziom hałasu, aby domowy rejestrator mógł pracować bezgłośnie. Z kolei napęd przeznaczony do pracy w wizyjnym systemie dozorowym może jednocześnie obsłużyć strumienie wizyjne generowane przez trzydzieści dwie kamery o rozdzielczości HD. Większe obciążenia wymagają zastosowania dysków serwerowych i modeli przeznaczonych dla przedsiębiorstw.

Dyski rejestrują wiele strumieni danych, a stosunek operacji zapisu do operacji odczytu wynosi mniej więcej 9:1.

Do wizyjnego systemu dozorowego mogą być podłączone zarówno kamery obserwujące puste place czy parkingi (w połączeniu z funkcją wykrywania ruchu), jak i kamery obserwujące wnętrza kasyn bądź stacji kolejowych, gdzie nieustannie przewijają się setki ludzi.

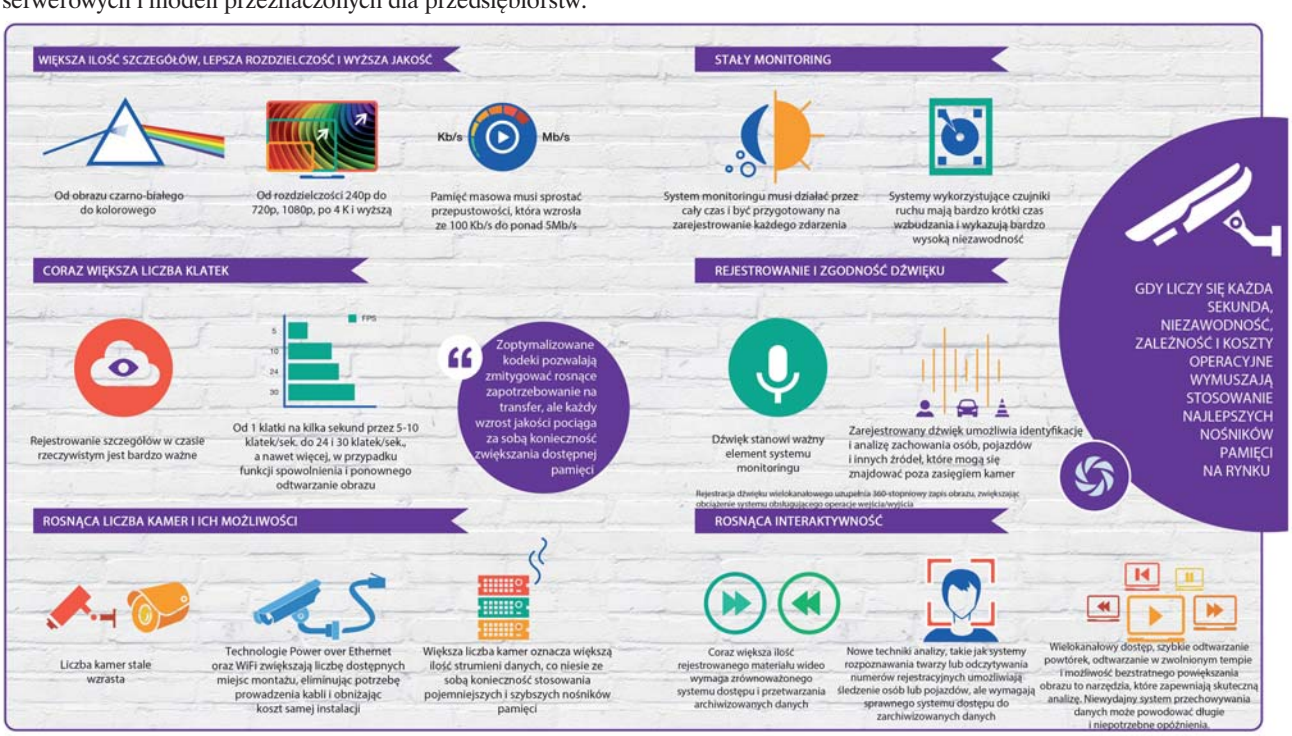
Niższe zużycie prądu skutkuje mniejszą emisją ciepła, co z kolei wydłuża żywotność dysku. Dysk WD Purple pobiera 5,1 W mocy, podczas gdy dysk Seagate Surveillance o 47% więcej, czyli 7,5 W.

Rozwiązanie problemu obciążenia jest zawarte w oprogramowaniu układowym. Oprogramowanie układowe dla dysków WD Purple nosi nazwę AllFrame i współpracuje z pamięcią podręczną o pojemności 64 MB, dzięki czemu dysk może obsłużyć wiele strumieni danych jednocześnie. AllFrame monitoruje obciążenie dysku i kontroluje liczbę rejestrowanych strumieni. Sprawdza też, jaką przepływność ma każdy z tych strumieni, po czym zapisuje dane na powierzchni dysku. W takiej sytuacji podczas zapisu bloków 1, 2, 3 i 4, a następnie bloków 5, 6, 7 i 8 położenie głowic ulega skokowym zmianom. Po kolejnym skoku głowice zapisują bloki 9, 10, 11 i 12.

Dysk jest dość hałaśliwy ze względu na konieczność częstego przemieszczania się głowic, ale nie ma to wpływu na żywotność mechanizmu. Żywotność napędu jest mierzona wyłącznie w ilości wykonywanych operacji odczytu i zapisu. Innymi słowy – nowe napędy przeznaczone do pracy w wizyjnych systemach dozorowych to konstrukcje, które zostały poddane modyfikacjom, dzięki czemu są idealnie przystosowane do konkretnego zadania wyjątkowo niewielkim kosztem.

Leo Waldock

Przedstawiciel firmy:
Norbert Koziar
e-mail: norbert.koziar@wdc.com
www.wdc.com



Rys 1. Rosnące wymagania systemów monitoringu dotyczące pamięci masowej (badania IDC na zlecenie WD)

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:

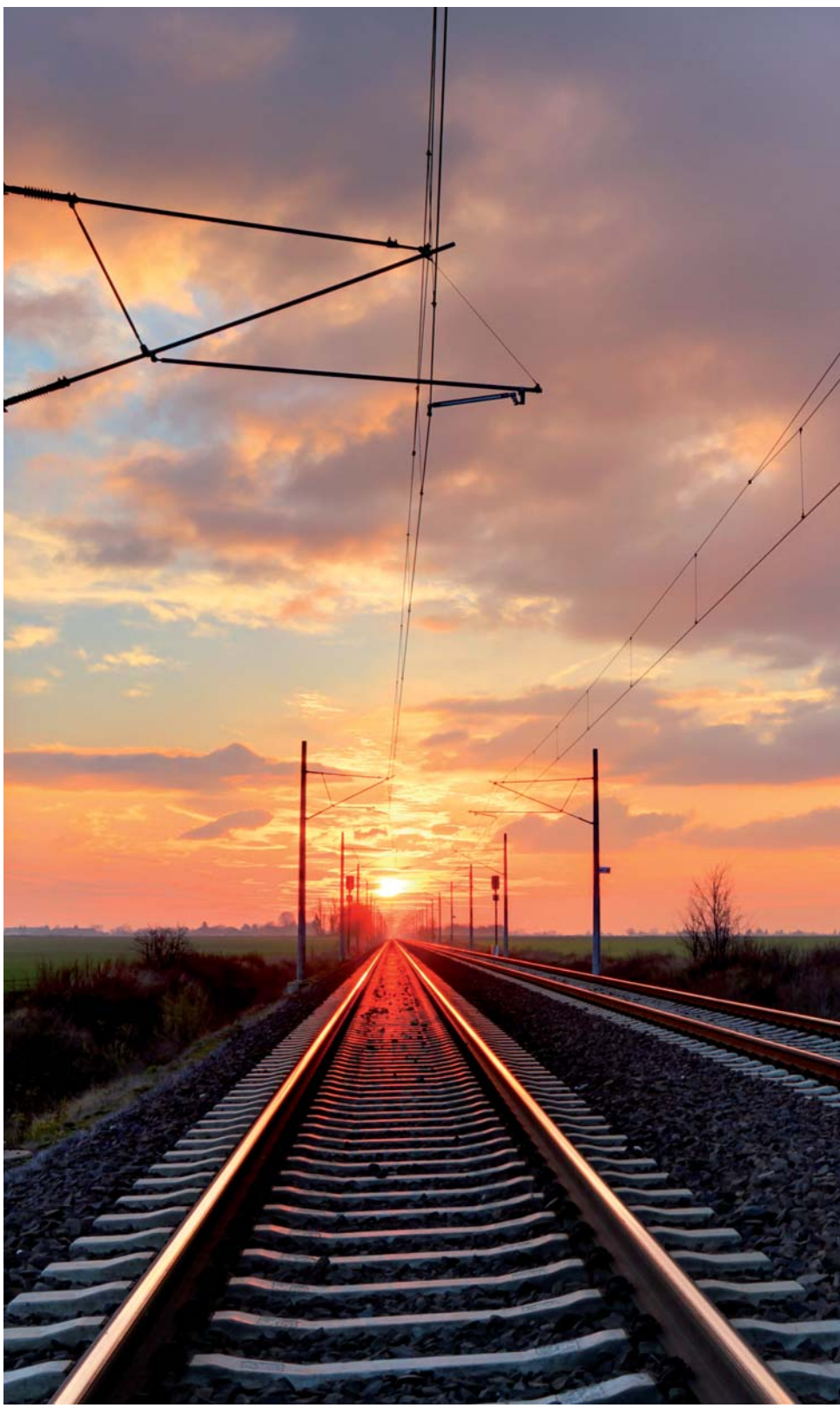
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Następna stacja – bezpieczeństwo

Scentralizowany dozór wizyjny w czasie rzeczywistym

Axis Communications

Trwa rewolucja w branży *security* polegająca na przejściu z technologii analogowej na cyfrową. Wnosi ona nowe, znaczące możliwości faktycznego i dostrzegalnego wzrostu poziomu bezpieczeństwa w dziedzinie transportu publicznego. Już dziś zarządcy wielu stacji i organy odpowiedzialne za transport doceniają korzyści płynące z wykorzystania obrazu o wysokiej rozdzielczości, automatycznie generowanych alarmów czy scentralizowanych systemów bezpieczeństwa



Jednym z przywódców tej rewolucji jest szwedzka firma Axis Communications. W 1996 roku firma wprowadziła na rynek pierwszą cyfrową kamerę dozorową, nazywaną częściej kamerą sieciową lub kamerą IP. Obecnie Axis całkowicie koncentruje swoją uwagę na sieciowych systemach wizyjnych i zatrudnia ponad 1800 pracowników. Jednym z nich jest Patrik Anderson odpowiedzialny za ofertę firmy Axis dla branży transportowej.

– Już kilkadziesiąt lat temu, w branży transportowej, jako jednej z pierwszych, zaczęto stosować systemy CCTV ze względu na to, że bezpieczeństwo odgrywa kluczową rolę w wyborze transportu publicznego jako środka komunikacji – powiedział Patrik Anderson, dyrektor ds. sprzedaży w dziale transportu firmy Axis Communications. *– Najważniejszym zadaniem organów odpowiedzialnych za transport jest utrzymanie ciągłości pracy taboru i służb zajmujących się jego obsługą oraz zminimalizowanie przestojów. Aby to osiągnąć, konieczne jest prowadzenie nieustannego dozoru, zarówno na stacjach, w pociągach, jak i w ramach całej infrastruktury transportowej. To tutaj sieciowy system wizyjny przydaje się najbardziej.*

Od materiału dowodowego do bezpieczeństwa w czasie rzeczywistym

Każdego dnia stacje i cała infrastruktura transportowa narażone są na wiele zagrożeń, począwszy od wandalizmu i nielegalnego malowania graffiti po kradzieże i akty przemocy. W stosowanych dotychczas analogowych systemach dozorowych nagrane obrazy z kamer służyły głównie jako materiał dowodowy dokumentujący zaistniałe zdarzenia. W sieciowych systemach wizyjnych obraz odgrywa znacznie ważniejszą rolę – daje nowe możliwości skutecznego dozoru i reagowania na zdarzenia w czasie rzeczywistym.

– Jedną z głównych zalet systemów sieciowych jest możliwość podglądu bieżących obrazów z kamer dozorowych przez sieć komputerową, w tym również bezprzewodową. Umożliwia to organom odpowiedzialnym za transport skuteczny nadzór wizyjny wszystkich stacji, taboru i infrastruktury z jednego lub kilku centrów nadzoru – wyjaśnił Anderson. *– Nawet jeżeli w tym samym czasie wydarzy się kilka incydentów, system sieciowy w czasie rzeczywistym dostarczy obraz niezbędny do całościowej oceny sytuacji.*

Skuteczna reakcja na incydenty

Aby w pełni zrozumieć znaczenie dostępu do bieżących obrazów z kamer, należy wziąć pod uwagę to, co dzieje się w centrum nadzoru w momencie zaistnienia zdarzenia. *– Każde zdarzenie, poważne czy błahe, musi być ocenione, a następnie podejmuje się decyzję dotyczącą działań, o ile są one potrzebne* – powiedział Anderson. *– Podjęcie odpowiednich działań jedynie na podstawie telefonu od zszokowanego pasażera czy zestresowanego pracownika ochrony jest z reguły bardzo trudne.*

Organy decydujące o wdrożeniu sieciowych wizyjnych systemów dozorowych otrzymują korzyści w postaci:

– skuteczniejszej oceny i hierarchizacji incydentów,
– szybszych i trafniejszych decyzji o podjęciu interwencji,
– zmniejszenia liczby opóźnień i przerw w komunikacji.

– Dzięki sieciowym systemom wizyjnym podgląd jest ułatwiony – można korzystać z różnych urządzeń, m.in. komputerów przenośnych, terminali mobilnych czy smartfonów – dodał Anderson. *– Dzięki temu możliwa jest lepsza ocena sytuacji po przybyciu na miejsce i sprawniejsze podjęcie właściwych działań.*

Jakość obrazu HDTV

Kolejną istotną zaletą sieciowych systemów wizyjnych jest doskonała jakość obrazu. *– W naszych domach mamy już możliwość oglądania ostrego i klarownego obrazu w telewizji o wysokiej*

Fot. 1. Na dużych stacjach każdego dnia zdarzają się różnego rodzaju incydenty. Sieciowy system dozorowy zapewnia ich skuteczną hierarchizację i umożliwia szybką reakcję

rozdzielczości (HDTV). Taką samą jakość obrazu zapewnia wiele kamer sieciowych – przekonywał ekspert.

Dzięki wykorzystaniu kamer HDTV obserwator może dostrzec więcej szczegółów obrazu, a pole widzenia może być szersze niż w przypadku kamer analogowych. – *Obraz z kamer sieciowych HDTV jest zapisywany z rozdzielczością megapikselową. Jest to dużym ułatwieniem podczas prowadzenia śledztwa – osoby i przedmioty znajdujące się na obrazie są lepiej widoczne, więc łatwiej je rozpoznać* – wyjaśniał Patrik Anderson. – *Gdy potrzebna jest obserwacja większego obszaru, kamery HDTV stanowią ekonomiczne rozwiązanie, ponieważ jedną taką kamerą można objąć obszar większy niż czterema kamerami analogowymi.*

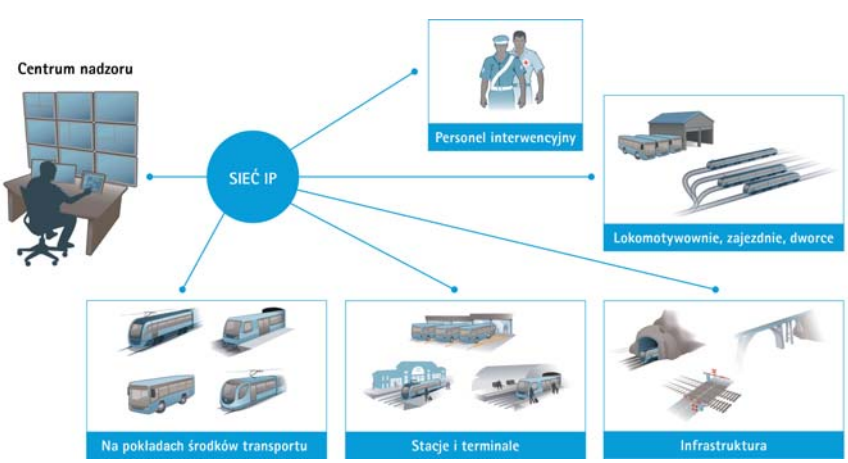
Inteligentne aplikacje wizyjne

W ostatnich latach wiele dyskutowano o możliwościach wykorzystania inteligentnych systemów wizyjnych do automatycznej sygnalizacji w sytuacjach alarmowych do sygnalizacji zagrożeń. Patrik Anderson wypowiada się na ten temat ostrożnie. – *Oczekiwania dotyczące nowych możliwości, które jeszcze kilka lat temu były nie do pomyślenia, mogą być przesadne, jednakże dostępnych jest kilka niezawodnych, „inteligentnych" funkcji, które przynoszą rzeczywiste korzyści personelowi ochrony. Przykłady to detekcja ruchu, rozpoznawanie tablic rejestracyjnych oraz wykrywanie prób sabotażu* – skomentował.

Kamera z funkcją sygnalizacji sabotażu automatycznie ostrzega operatora w przypadku jej zasłonięcia, zmiany ustawienia czy innych prób manipulacji. Dzięki temu centrum nadzoru może łatwo ocenić, czy kamery działają prawidłowo. Funkcja detekcji ruchu umożliwia automatyczne wykrywanie i ostrzeganie o aktywności w miejscach, w których takiej aktywności być nie powinno. Ułatwia to na przykład wykrycie grafficiarzy w lokomotywowniach, zajezdniach czy na dworcach, intruzów w tunelach bądź podejrzanie zachowujących się osób w infrastrukturze kolejowej.

Wdrożenia

Madryt, Moskwa, Oslo, Praga, Sztokholm i Sydney to niektóre z miast, w których infrastrukturze transportowej wdrożono sieciowe systemy wizyjne. Zagadnienia z tym związane omawiane są na konferencjach dotyczących bezpieczeństwa transportu, dlatego władze i operatorzy coraz bardziej interesują się nowymi możliwościami. – *W autobusach, pociągach, na stacjach, w terminalach, lokomotywowniach, zajezdniach i na dworcach w różnych częściach świata zainstalowaliśmy już ponad 50000 naszych kamer* – poinformował ekspert. – *Nasza oferta obejmuje sieciowe kamery termowizyjne oraz kamery z funkcją Lightfinder, które umożliwiają wykrywanie aktywności w kompletnej ciemności oraz reprodukcję kolorów nawet przy bardzo słabym oświetleniu. Zainteresowanie tymi produktami jest tak duże, że – jak mniemam – rewolucja w sieciowych systemach wizyjnych dopiero się rozpoczęła* – podsumował Anderson.



Rys. 1. Kilka firm i instytucji zajmujących się transportem wdrożyło już systemy dozorowe, które umożliwiają centralną obserwację zdarzeń zachodzących w podległej infrastrukturze transportowej. Dzięki możliwości podglądu bieżących obrazów z wielu kamer dozorowych rozmieszczonych w różnych miejscach podejmowanie decyzji, hierarchizacja i reagowanie na zdarzenia przebiegają bardzo sprawnie

Axis Communications

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

Inteligentne wizyjne systemy dozorowe

Samsung Techwin Poland

Wystarczy spojrzeć na karty katalogowe przedstawiające kamery produkowane przez wiodące firmy, takie jak Samsung Techwin, by się przekonać, jak wysokie są parametry obrazu i jak złożone są oferowane obecnie funkcje. Zaledwie kilka lat temu takich parametrów i funkcji nie można było sobie nawet wyobrazić

Do właściwości kamer, które przynoszą realne korzyści użytkownikom wizyjnych systemów dozorowych, należy szeroki zakres dynamiki, przekładający się na ostry i czytelny obraz w przypadku bardzo kontrastowych scen, i odporność na prześwietlenie najjaśniejszych fragmentów obrazu, dzięki której możliwe jest rozróżnienie szczegółów we wszystkich jego partiach i dostrzeżenie rzeczy, które uprzednio kryły się w jaskrawych światłach. Nie należy zapominać o funkcji *defog* umożliwiającej uzyskanie klarownych obrazów w złych warunkach pogodowych, podczas opadów deszczu czy śniegu, a także podczas obserwacji obszarów zasnutych mgłą lub dymem. Warto wspomnieć o technice progresywnego skanowania matrycy światłoczułej, dzięki której uzyskuje się ostry obraz szybko poruszających się przedmiotów. Równie istotna jest funkcja cyfrowej stabilizacji obrazu eliminująca wpływ drgań powodowanych przez silny wiatr lub wibracji przenoszonych z konstrukcji wsporczych, na których zamocowane są kamery.

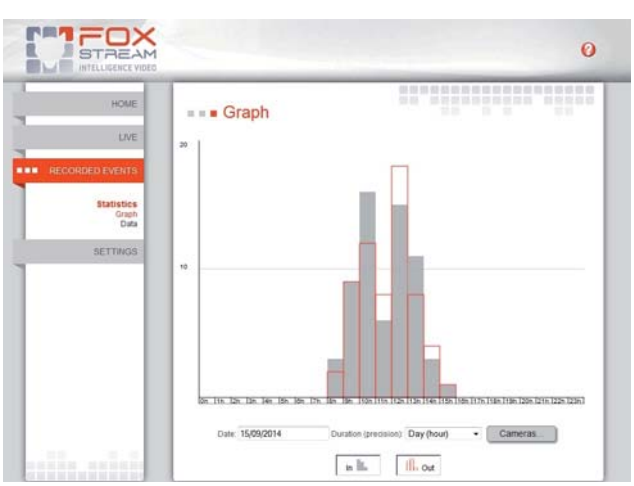
Fot. 1. Duże możliwości otwartej platformy programowej

Co niesie przyszłość?

Powyżej wymienione zostały tylko niektóre funkcje kamer, możliwe do uzyskania dzięki ogromnemu postępowi technologicznemu, które w sieciach publicznych mogą zwiększyć skuteczność zwalczania przestępczości, zaś w sieciach korporacyjnych mogą przyczynić się do podniesienia poziomu bezpieczeństwa pracowników i poprawy warunków ich pracy. Ponadto wzrastająca moc obliczeniowa procesorów DSP, stosowanych w najnowszych kamerach IP, zwiększa możliwości implementacji oprogramowania ułatwiającego pracę kadry kierowniczej, a tym samym usprawniającego procesy produkcyjne w przedsiębiorstwach. Tak więc z inwestycji związanych z instalacją wizyjnych systemów dozorowych mogą wynikać wymierne korzyści finansowe.

Co przyniesie przyszłość? W bieżącym roku usłyszymy więcej na temat otwartej platformy programowej, dzięki której możliwe będzie skuteczne wykorzystanie nadwyżek mocy obliczeniowej procesorów DSP typu WiseNetIII firmy Samsung Techwin. Podobnie jak w przypadku smartfonów czy tabletów, w kamerach można instalować dodatkowe aplikacje. Większość współczesnych kamer pozwala na uruchomienie pojedynczej aplikacji, jednakże duża nadwyżka mocy obliczeniowej procesorów DSP typu WiseNetIII firmy Samsung Techwin umożliwia jednoczesne uruchomienie kilku aplikacji.

Różne działy przedsiębiorstwa, zainteresowane gromadzeniem i przetwarzaniem specyficznych danych uzyskiwanych w procesie analizy treści obrazów, będą mogły wykorzystywać te same kamery do różnych zadań dzięki możliwości uruchomienia dodatkowych aplikacji. Daje to kadrze kierowniczej skuteczne narzędzia usprawniające działania przedsiębiorstwa, podnoszące poziom bezpieczeństwa i poprawiające warunki pracy. Obrazy mogą być wykorzystywane przez dział ochrony fizycznej przedsiębiorstwa, którego pracownicy będą mogli szybko reagować na incydenty wykrywane przez wizyjny system dozorowy.



Fot. 2. Statystyki tworzone przez aplikację FoxCounter

Analiza treści obrazów w urządzeniach peryferyjnych

Większość aplikacji uruchamianych na procesorach znajdujących się wewnątrz kamer dokonuje analizy treści obrazu wytwarzanego przez te kamery. Różnorodność dostępnych rozwiązań jest wręcz zadziwiająca. Przykładowo, osoby odpowiedzialne za przebieg operacji o znaczeniu krytycznym chętnie skorzystają z oprogramowania Foxstream, doskonale nadającego się do ochrony perymetrycznej obiektów, w których potrzebne są skuteczne narzędzia do wykrywania i śledzenia potencjalnych wandali lub włamywaczy.

Firma Arteco, przodujący producent oprogramowania służącego do analizy treści obrazu, oferuje aplikację służącą do automatycznego odczytu tablic rejestracyjnych

samochodów, która może być uruchomiona wewnątrz kamery, na procesorze WiseNetIII firmy Samsung Techwin. Aplikacja została stworzona z myślą o systemach kontroli dostępu i można z niej korzystać w takich obiektach jak lotniska, porty przeładunkowe czy centra dystrybucyjne, gdzie konieczne jest precyzyjne śledzenie ruchu pojazdów. Aplikacja pozwala na odczyt tablic rejestracyjnych pojazdów poruszających się z prędkością nie przekraczającą 50 km/godz. System bazujący na tym oprogramowaniu może być skonfigurowany w taki sposób, by generował sygnały ostrzegawcze w przypadku wykrycia pewnych ściśle określonych incydentów lub pojawienia się określonych tablic rejestracyjnych w polu widzenia kamer.

Automatyczne śledzenie obiektów

Obecnie dostępne są kamery PTZ o wysokiej rozdzielczości, z funkcją automatycznego śledzenia obiektów, wyposażone w obiektywy zmiennoogniskowe o krotności ×43. Dzięki takim kamerom operatorzy systemów dozorowych mogą kontrolować przebieg interesujących ich wydarzeń. Zastosowanie szczelnych obudów z grzałkami zasilanymi metodą PoE+ uodparnia kamery na wpływy środowiskowe i umożliwia poprawną pracę w skrajnie niskich temperaturach. Inne, wspomniane wcześniej funkcje, takie jak cyfrowa stabilizacja obrazu czy *defog*, pozwalają na uzyskanie obrazów o wysokiej jakości niemal w każdych warunkach pogodowych. Funkcja automatycznego śledzenia obiektów umożliwia ciągłą obserwację wybranych osób lub pojazdów. W trakcie tego procesu operator systemu ma wolne obie ręce, którymi może obsługiwać inne urządzenia.

Wielostrumieniowa transmisja obrazów o zróżnicowanych parametrach jakościowych umożliwia wykorzystanie ich na wielu stanowiskach wyposażonych w komputery PC lub inne urządzenia połączone z lokalną siecią, takie jak smartfony czy tablety. Wykorzystanie algorytmu kompresji obrazów H.264 w jego najnowszej wersji zmniejsza opóźnienia w transmisji obrazów, przez co wyeliminowane są problemy występujące dotychczas w systemach IP podczas ręcznego sterowania kamerami śledzącymi poruszające się obiekty.

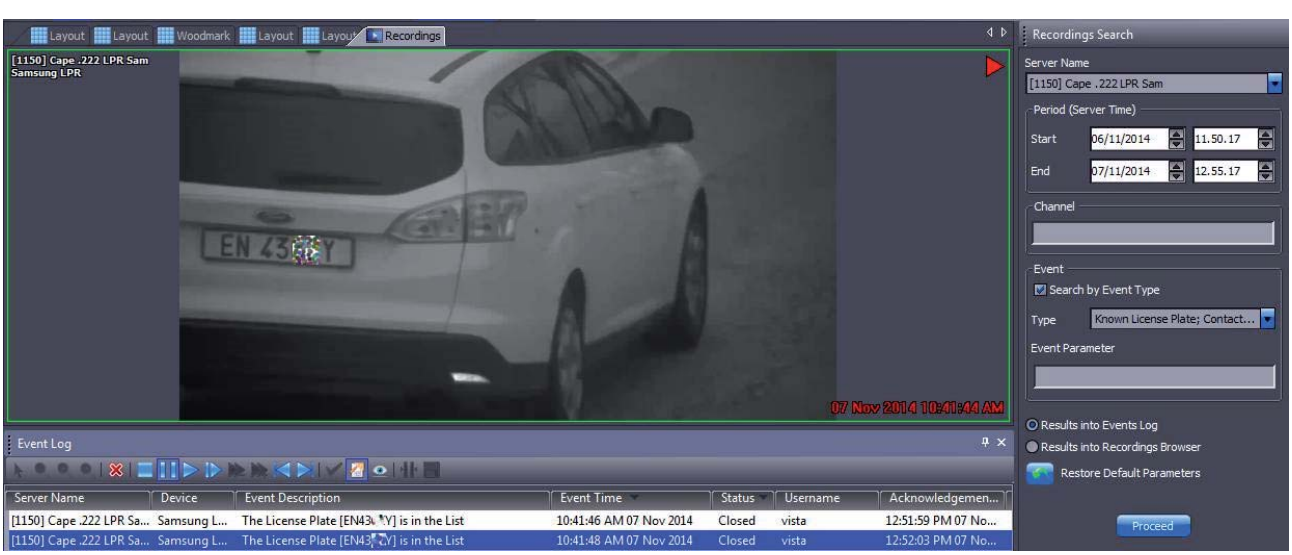
Fot. 4. Kamera SND-7084RP z procesorem WiseNet III

Obserwacja w polu widzenia odpowiadającym kątowi 360 stopni

Kamery o polu widzenia odpowiadającym kątowi 360 stopni są coraz częściej wykorzystywane w systemach zabezpieczających, w których wymagana jest ciągła obserwacja chronionego obiektu – przez dwadzieścia cztery godziny na dobę i siedem dni w tygodniu. Często zdarza się, że pojedyncza kamera o polu widzenia odpowiadającym kątowi 360 stopni jest jedynym elementem niezbędnym do skutecznego nadzorowania całego chronionego obszaru. Aby uzyskać taki sam efekt za pomocą standardowych kamer stacjonarnych, należałoby zastosować wiele takich kamer.

W realnych sytuacjach kamera o polu widzenia odpowiadającym kątowi 360 stopni umożliwia operatorowi systemu ciągłą obserwację całego chronionego obszaru, zaś dodatkowe kamery stacjonarne i obrotowe mogą być wykorzystane do likwidacji martwych pól i wychwytywania szczegółów w najważniejszych miejscach, takich jak na przykład drzwi wejściowe.

Obecnie na rynku dostępne są liczne modele kamer o polu widzenia odpowiadającym kątowi 360 stopni i rozdzielczości dochodzącej do 5 megapikseli. Wytwarzają one



Fot. 3. System rozpoznawania tablic Arteco wykorzystujący otwartą platformę programową Samsung Techwin

Fot. 5. Kamera hemisferyczna 5 Mpx SNF-8010P

obraz o bardzo wysokiej jakości i doskonałej rozróżnialności szczegółów. Wiele z nich ma funkcję PTZ realizowaną na drodze elektronicznej, dzięki czemu możliwe jest powiększanie dowolnie wybranych fragmentów obrazu bez konieczności przerywania obserwacji całego chronionego obszaru. Tej klasy kamery mają funkcję korekty zniekształceń geometrycznych wynikających z szerokiego kąta widzenia. Dzięki temu możliwe jest utworzenie jednego lub dwóch zobrazowań panoramicznych, przedstawiających cały obserwowany obszar w polu widzenia odpowiadającym kątowi 360 stopni.

Pełna integracja z innymi systemami

Kamery IP i inne sieciowe urządzenia zabezpieczające są obecnie najistotniejszymi składnikami wizyjnych systemów dozorowych, decydującymi o rozwoju rynku zabezpieczeń technicznych. Dzieje się tak dlatego, że użytkownicy chcą maksymalnie wykorzystać zalety swoich systemów i czerpać realne zyski z integracji różnorodnych urządzeń pracujących we wspólnej sieci.

W związku z tym należy wyjaśnić, co tak naprawdę oznacza słowo „integracja", i zasygnalizować potencjalne problemy, jakie mogą pojawić się podczas prób integracji wcześniej zainstalowanych systemów, które do tej pory pracowały niezależnie od siebie.

Od wielu lat pojawiają się liczne publikacje i wypowiedzi na temat integracji systemów zabezpieczających, jednak śmiało można stwierdzić, że często są to jedynie puste słowa. Początkowo przez integrację rozumiano przekazywanie sygnałów sterujących i alarmowych pomiędzy różnymi systemami, dzięki czemu incydenty wykrywane w jednym z nich powodowały określone reakcje w pozostałych systemach. Sygnalizacja wykrytych zdarzeń ograniczała się do zapalenia świateł ostrzegawczych czy uruchomienia sygnalizatorów dźwiękowych w pomieszczeniu kontrolnym. W późniejszym okresie informacje alarmowe pochodzące z różnych systemów były wyświetlane na ekranie monitora komputerowego.

W ostatnich latach w dziedzinie integracji systemów zabezpieczających nastąpił znaczny postęp. Jeśli weźmie się pod uwagę ogromne nakłady inwestycyjne, jakie czołowi producenci przeznaczyli na rozwój i opracowanie nowych technologii, nie powinno to nikogo dziwić. Motorem postępu była chęć czerpania maksymalnych zysków z najnowszych osiągnięć technologicznych w dziedzinie wizyjnych systemów dozorowych, systemów sygnalizacji włamania i napadu, sygnalizacji pożarowej, kontroli dostępu i ochrony obwodowej.

Kompatybilność zastosowanych rozwiązań

Zanim zapadną decyzje dotyczące zakupu urządzeń zabezpieczających, należy zastanowić się, na jakim poziomie można je zintegrować. Jeśli możliwa jest prawdziwa integracja, to urządzenia są kompatybilne zarówno z istniejącymi, jak i z przyszłymi systemami, które powstaną w wyniku kolejnych modyfikacji. Jeśli ten warunek nie jest spełniony, to systemy mogą zostać zintegrowane i współdziałać jedynie dzisiaj, zaś w przyszłości mogą narazić użytkowników na poważne kłopoty, na przykład wówczas, gdy któryś z producentów zmieni konstrukcję swoich urządzeń lub zaktualizuje ich oprogramowanie.

Z tych względów zalecana jest współpraca tylko z tymi producentami, których urządzenia są zgodne ze specyfikacją ONVIF, jednak nawet w takim przypadku prosta integracja będzie dotyczyła tylko wybranych funkcji. Konieczne jest więc zasięgnięcie porady u integratorów systemów czy przedstawicieli producentów, którzy pomogą zaprojektować system zabezpieczeń i wyjaśnią, jakich zmian można się spodziewać w przyszłości. W przypadku zintegrowanych systemów strzegących obiekty należące do infrastruktury krytycznej niepoprawne funkcjonowanie jednego z systemów składowych może uniemożliwić skuteczne działanie całej instalacji.

W przypadku standardowych systemów zabezpieczeń wykorzystywanych przez firmy transportowe czy produkcyjne istotna jest minimalizacja kosztów utrzymania i eksploatacji tych systemów. Należy więc wybierać rozwiązania, które mogą być łatwo modyfikowane i dostosowywane do przyszłych wymagań.

Wartość dodana dziś ma nie tracić znaczenia w przyszłości

W wielu firmach koszty wdrożenia i eksploatacji zintegrowanych systemów zabezpieczających są pokrywane przez działy HR, TI oraz służby ochrony, a także działy zajmujące się zarządzaniem, gdyż wszystkie one korzystają z informacji dostarczanych przez kamery. Kamery współdziałają z wieloma innymi urządzeniami i systemami, zaś poszczególne działy korzystają z przetworzonych informacji uzyskanych w wyniku analizy i obróbki materiału wizyjnego.

Na szczęście rozwój technologiczny w dziedzinie wizyjnych systemów dozorowych jest w stanie nadążyć za rosnącymi oczekiwaniami użytkowników końcowych. Te oczekiwania są podsycane przez dostępność kamer wytwarzających obrazy o wysokiej rozdzielczości, umożliwiające weryfikację wykrywanych wydarzeń i stanowiące źródło innych, dużo cenniejszych informacji.

Samsung Techwin Poland
Tłumaczenie: Redakcja

SAMSUNG TECHWIN

Odległość – żaden problem dla nowej kamery IP PTZ

Oferująca zaskakujący, 43-krotny zoom optyczy, funkcję automatycznego śledzenie obiektu oraz cyfrową stabilizację obrazu, nowa kamera IP Samsung ukazuje odległe obiekty z krystaliczną ostrością i w każdych warunkach oświetleniowych.

Zaprojketowany do wymagających warunków model SNP-5430 wyposażony jest w funkcję Defog (eliminacja mgły) oraz zasilanie w technologii PoE+ wraz z grzałkami.

Pójdź dalej, zobacz różnicę z nowymi kamerami IP Samsung Techwin.

WiseNet III

SNP-5430 SNP-5430H

www.samsung-cctv.pl

Autoryzowani Partnerzy firmy Schrack Seconet w Polsce

Marta Nowak

Co roku Schrack Seconet Polska organizuje spotkanie swoich partnerów biznesowych reprezentujących firmę na terenie kraju. Tegoroczna edycja odbyła się w Kazimierzu Dolnym w dniach 5-6 marca. W spotkaniu wzięli udział przedstawiciele kilkudziesięciu firm z całego kraju, które ściśle współpracują z producentem

Spotkania Autoryzowanych Partnerów Schrack Seconet Polska mają już swoją długoletnią tradycję. Ich celem jest wspólne opracowywanie strategii działania na rynku systemów zabezpieczeń w Polsce. W ostatnich latach skład grupy firm posiadających autoryzację firmy Schrack Seconet Polska uległ znacznej przebudowie. Celem było zapewnianie klientom najwyższego poziomu bezpieczeństwa.

Najważniejszym punktem tegorocznego spotkania była dyskusja dotycząca wspólnej działalności na rynku systemów bezpieczeństwa w Polsce, a także kształtu i przyszłości branży. Ponadto odbyły się prezentacje przygotowane przez zespół pracowników firmy Schrack Seconet, dotyczące między innymi działalności tej firmy w Polsce, nowych produktów, działań marketingowych, a także sytuacji na rynku. Po podsumowaniu wyników i działań ubiegłorocznych przyznano tytuł Partnera Roku firmie RS-System z siedzibą w Warszawie za najlepsze wyniki w sprzedaży systemów sygnalizacji pożarowej Schrack Seconet w roku 2014 oraz za wysoką jakość usług.

W roku 2013 znacznej modyfikacji uległa struktura grupy Partnerów Schrack Seconet w Polsce. Wyróżniono wtedy trzy

grupy kompetencyjne: Autoryzowanych Partnerów Wiodących, Autoryzowanych Partnerów oraz Partnerów Handlowych. W dalszym ciągu podstawowym statusem pozostał Autoryzowany Partner, jednak z tego grona zostały wyróżnione firmy spełniające najbardziej restrykcyjne warunki autoryzacji. Przedsiębiorstwa te tworzą dziś grupę Autoryzowanych Partnerów Wiodących. Statusy autoryzacji są przyznawane przez producenta na dwa lata, dlatego rok 2014 zakończono weryfikacją wszystkich firm z grona partnerów oraz aktualizacją uprawnień dla inżynierów zatrudnionych w tych przedsiębiorstwach. Na początku tego roku lista firm partnerskich uległa modyfikacji. Dzięki wysokiej jakości współpracy, bardzo dobrej kondycji finansowej, pozytywnym wynikom regularnych audytów producenta, wysoce wykwalifikowanej kadrze specjalistów i bogatej liście referencyjnej zrealizowanych wspólnie obiektów kilka firm zmieniło swój dotychczasowy status na wyższy.

Do grona Autoryzowanych Partnerów Wiodących dołączyły dwie firmy: ALKAM System z siedzibą w Legnicy oraz DEKK Fire Solution z siedzibą w Piasecznie. Obecnie w tym elitarnym gronie znajduje się 15 firm partnerskich.

Do grona Autoryzowanych Partnerów Schrack Seconet w Polsce w roku 2015 dołączyło dziesięć firm, mających dotychczas status Partnera Handlowego. Należą do nich: CERBEX z Krosna, Connect Marek Szczygielski z Torunia, Electro Croon Polska z Warszawy, ENTEC Solutions z Wrocławia, GMT z Mysłowic, LUMEN Polska z Wrocławia, Microsystem z Sopotu, PHTSPiO SUPON ze Szczecina, RAJ International W. Wójcik, B. Wójcik z Wrocławia, UNIMA 2000 z Krakowa oraz URKOM Adam Nocoń z Zabrza. Firmy z grona Autoryzowanych Partnerów również mają stabilną sytuację finansową, dbają o przestrzeganie zasad współpracy i zatrudniają wykwalifikowanych specjalistów. Podobnie jak Autoryzowani Partnerzy Wiodący przedsiębiorstwa te mają dostęp do wszelkich szkoleń technicznych i handlowych, pełne uprawnienia instalacyjne oraz możliwość bezpośrednich zakupów u producenta.

W latach 2013–2014 kilku przedsiębiorstwom z grona Autoryzowanych Partnerów nie udało się utrzymać statusu – na początku tego roku firmy te kontynuują współpracę z producentem na zasadach obowiązujących Partnera Handlowego. Obecnie na liście Autoryzowanych Partnerów Schrack Seconet jest 27 firm z całego kraju. Łącznie z Autoryzowanymi Partnerami Wiodącymi cała grupa liczy 42 przedsiębiorstwa.

Firmy, które działają na polskim rynku w dziedzinie profesjonalnych systemów zabezpieczeń, wykazują zainteresowanie współpracą i znalezieniem się w przyszłości w gronie Partnerów Handlowych czy Autoryzowanych Partnerów firmy Schrack Seconet w Polsce. Rozpoczynają one współpracę na warunkach określonych przez producenta (m.in. nie posiadają uprawnień do prowadzenia serwisu gwarancyjnego instalacji wykonanych przez Autoryzowanych Partnerów Wiodących i Autoryzowanych Partnerów).

Szczegółowe informacje dotyczące nowej polityki sprzedaży oraz zakresu uprawnień każdej z trzech grup partnerów biznesowych firmy Schrack Seconet w Polsce są zamieszczone na stronie *www.schrack-seconet.pl.*

Marta Nowak
Schrack Seconet Polska

SCHRACK SECONET

SZCZECIN
- PHTSPiO SUPON S.A.

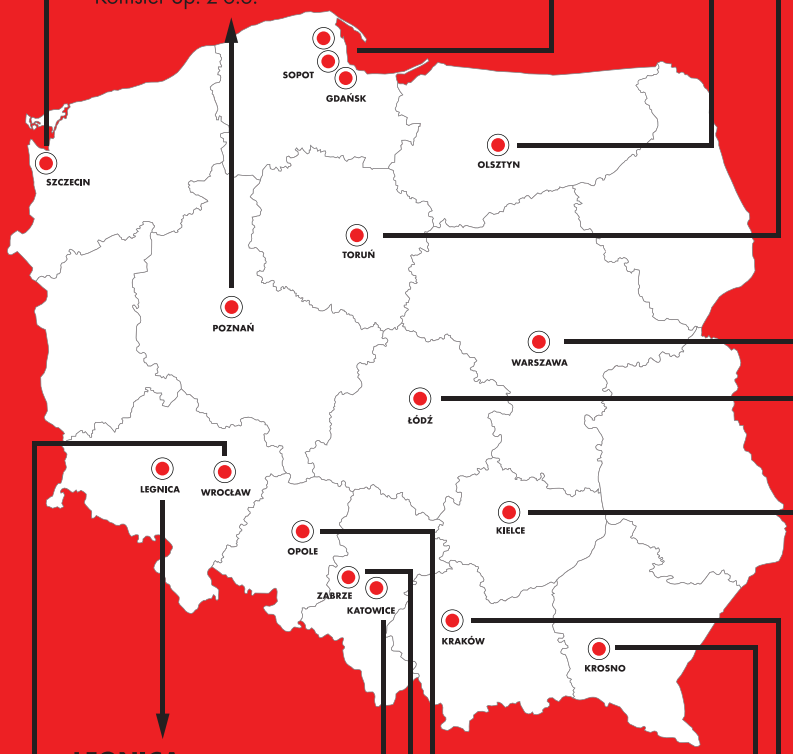
TRÓJMIASTO
- **Izotop Service Sp. z o.o.**
- Microsystem Sp. z o.o.

OLSZTYN
- Appelt Artur Appelt

TORUŃ
- Connect Marek Szczygielski

POZNAŃ
- **PPHU Tel-Poż-System ISKRA Sp. z o.o.**
- Komster Sp. z o.o.

REGION WARSZAWSKI
- Agis Fire&Security Sp. z o.o.
- **DEKK Fire Solutions Sp. z o.o.**
- **Elektro A-z Sp. z o.o.**
- Electro Croon Polska Sp. z o.o.
- InGas Sp. z o.o.
- **Johnson Controls International Sp. z o.o.**
- JUTOM Tomasz Ciok
- Konsalnet Secure Solutions Sp. z o.o.
- Luxmat-Telecom Sp. z o.o.
- **Panorama-SAP Sp. z o.o.**
- Qumak S.A.
- **RS System Sp. z o.o.**



ŁÓDŹ
- **01 Partner Sp. z o.o.**
- Futura Sp. z o.o.
- LVS-Tech Sp. z o.o.
- ZBAR PHU Mariusz Popenda

KIELCE
- Forestel Sp. z o.o.
- **PHT Supon Sp. z o.o.**

KRAKÓW
- "Dyskret Polska Sp. z o.o. " Sp. k.
- **Insap Sp. z o.o.**
- **PUI Megasystem Sp. z o.o.**
- Supo Cerber Sp. z o.o.
- Unima 2000 Systemy Teleinformatyczne S.A.

LEGNICA
- **Alkam System Sp. z o.o.**

OPOLE
- Initel Sp. z o.o.

WROCŁAW
- Hofman A.D. Grzegorz Banach Sp. j.
- Lumen Polska Sp. z o.o.
- **OBIS Cichocki Ślązak Sp. j.**
- **OBIS 2 Andrzej Ślązak**
- RAJ International W. Wójcik, B. Wójcik s.c.
- ENTEC Solutions Sp. z o.o. Sp. k.

ZABRZE
- URKOM Systemy Teleinformatyczne

KATOWICE
- **Noma 2 Sp. z o.o.**
- GMT Sp. z o.o.

KROSNO
- Cerbex Sp. z o.o.

AUTORYZOWANI PARTNERZY SCHRACK SECONET POLSKA POSIADAJĄ:

• rzetelną wiedzę techniczną o instalowanych produktach • licencjonowany pakiet najnowszego oprogramowania źródłowego do uruchamiania i serwisowania systemów • oryginalny sprzęt serwisowy • magazyn części zamiennych • Certyfikaty Autoryzacji dla firmy i imienne - dla specjalistów

Mapa Autoryzowanych Przedstawicieli Schrack Seconet Polska Sp. z o.o. według ich siedzib. Wszystkie firmy prowadzą działalność handlową i serwisową na terenie całego kraju; wiele z nich posiada oddziały także w innych miastach!

Prezentacja firmy Xtralis

Beata Idziak
Andrzej Obłój

Firma Xtralis powstała w Australii w latach 1982/83. Od ponad 30 lat jest czołowym producentem innowacyjnych urządzeń służących do wykrywania dymu w bardzo wczesnej fazie rozwoju pożaru oraz do wykrywania zagrożenia bezpieczeństwa

Fot. Nowa rodzina czujek zasysających VESDA E

Od początku działalności strategia firmy Xtralis była zorientowana na wczesne wykrywanie zagrożeń pożarowych oraz zdarzeń zagrażających bezpieczeństwu obiektu. Słowo „wczesne" jest bardzo istotne. Koncentrujemy się na technologiach, których zastosowanie powoduje niedopuszczenie do katastroficznego rozwoju zdarzeń. W systemach bezpieczeństwa wczesne wykrywanie jest możliwe dzięki ochronie obwodowej z weryfikacją wizyjną. W systemach sygnalizacji pożarowej – głównie dzięki zasysającym czujkom dymu.

Drugą cechą szczególną firmy jest innowacyjność i to pojęta rygorystycznie. Xtralis niemal nie produkuje urządzeń, których nie opracował i nie wprowadził na światowy rynek jako pierwszy. Oczywiście mamy takie wyroby w swoim katalogu, ale wynika to z przejmowania firm o komplementarnej ofercie.

Najważniejszym produktem firmy Xtralis jest VESDA (Very Early Smoke Detection Apparatus), której pierwsza generacja została wprowadzona na rynek w latach 80. XX wieku jako pierwsza i przez kilka lat jedyna zasysająca czujka dymu. Nierzadko zdarza się, że nazwa *vesda* jest używana jako określenie technologii wykrywania dymu lub urządzenia innego producenta.

VESDA jest naszym najbardziej znanym produktem służącym do wykrywania zagrożenia pożarem. Inne to: OSID – pierwsza liniowa czujka dymu o dwóch promieniach (IR i UV) i pierwsza czujka wieloliniowa, ECO – pierwsza wielopunktowa czujka gazu, VESDA E – pierwsza czujka zasysająca, która wykrywa dym poniżej poziomu zanieczyszczeń powietrza, oraz ICAM – druga linia czujek zasysających, która zapoczątkowała rozwój zasysających czujek adresowalnych wykorzystujących długie kapilary zamiast rur.

Xtralis jest firmą zorganizowaną i zarządzaną w bardzo nowoczesny i elastyczny sposób. Na każdym z kontynentów znajdują się centra kompetencji: projektowe, handlowe, wsparcia technicznego, logistyczne – w sumie ponad 30. Firma zatrudnia ponad 550 pracowników, a jej wyroby są sprzedawane przez firmy partnerskie w ponad 100 krajach. Ma przeszło 10000 stałych klientów. Nasze produkty przeszły badania i certyfikację w ponad 35 instytucjach regulacyjnych na całym świecie. Ze względu na nasze doświadczenie ściśle współpracujemy z tymi organizacjami, przyczyniając się do tworzenia nowych standardów międzynarodowych.

Wartość sprzedaży naszych detektorów do wykrywania dymu plasuje nas na czwartym miejscu na świecie, zaraz po trzech globalnych producentach systemów pożarowych, z ponad sześcioprocentowym udziałem w rynku. W dziedzinie zasysających czujek dymu udział Xtralisa w światowym rynku wynosi ponad 61%.

Beata Idziak
Regional Sales Manager, Fire, Central Europe
Andrzej Obłój
Technical Manager, Fire, Central Europe
Xtralis

autoryzowany dystrybutor produktów firmy Xtralis
www.visionpolska.pl

Nie czyń drugiemu on-line, co tobie niemiłe

Monika Brzozowska

Obrażanie, znieważanie czy pomawianie w sieci jest częste i bywa brutalne. Wiele osób doświadcza tzw. „hejtu” w sieci, ale równie wielu – korzystając z anonimowości – tworzy posty pełne nienawiści lub zawiści. Ustawodawca gwarantuje wolność słowa, ale istnieją oczywiście jej granice

Należy zacząć od tego, które prawo jest właściwe. Nie ma dziś jednolitego aktu prawnego dotyczącego Internetu. Z jednej strony szkoda, bo w wielu przypadkach sprawy nie są jednolite. Z drugiej strony odpowiedzialność karna czy cywilna ustanowiona w odpowiednich kodeksach obowiązuje zarówno w tzw. „realu", jak i w wirtualnej rzeczywistości.

Do naruszenia dóbr osobistych odnosi się kodeks cywilny (art. 23, 24, 448 kc), kodeks karny (art. 212 § 2 i 216 § 2 kk), ale również ustawa o świadczeniu usług drogę elektroniczną (głównie art. 14 związany z problematyką odpowiedzialności administratorów i podmiotów hostujących) i ustawa *Prawo prasowe* (która dotyczy m.in. forum internetowego).

W orzecznictwie wskazano, że „nienawiść" to uczucie silnej niechęci, wrogości do kogoś, zaś pojęcia „mowy nienawiści" (*hate speech*) używa się do określenia wypowiedzi, które „rozpowszechniają, podżegają, promują lub usprawiedliwiają nienawiść rasową, ksenofobię, antysemityzm albo inne formy nienawiści oparte na nietolerancji" (wyrok Sądu Apelacyjnego w Katowicach z dnia 5 marca 2010 r., I ACa 790/09, LEX nr 1236397).

Czym są dobra osobiste i które spośród nich są najczęściej naruszane w sieci?

Katalog dóbr osobistych jest otwarty. W art. 23 kc wymieniono zdrowie, wolność, cześć, swobodę sumienia, nazwisko, pseudonim, wizerunek, tajemnicę korespondencji, nietykalność mieszkania, twórczość naukową, artystyczną, wynalazczą i racjonalizatorską. Pozostają więc one pod ochroną prawa cywilnego, niezależnie od ochrony przewidzianej w innych przepisach. W sieci często narusza się godność, wizerunek, prywatność, uczucia religijne i prawo do tożsamości narodowej. Te dwa ostatnie dobra osobiste są niezwykle interesujące z punktu widzenia prawa.

Do najważniejszych dóbr naruszanych w Internecie należy godność. Ochrona godności przysługuje każdemu człowiekowi, niezależnie od jego pozycji społecznej, statusu czy rozwoju umysłowego – ochrona przysługuje także osobom z ograniczoną poczytalnością, osobom niedorozwiniętym umysłowo, dzieciom czy osobom skazanym.

W Internecie nagminnie narusza się także wizerunek. Wizerunek można zdefiniować jako cechy człowieka dostrzegalne dla otoczenia i pozwalające zidentyfikować daną postać. Nie znaczy to, że naruszeniem wizerunku jest publikacja zdjęcia, natomiast może nim być publikacja rysunku, karykatury lub kolażu.

Wizerunek jako dobro osobiste jest chroniony nie tylko przez kodeks cywilny, ale także prawo autorskie.

Zgodnie z art. 81 ust. 1 prawa autorskiego rozpowszechnianie wizerunku wymaga zgody osoby na nim

przedstawionej. Prawo autorskie określa trzy wyjątki. Zgoda nie jest wymagana, gdy:

1) dana osoba (np. model, modelka) otrzymała zapłatę za wykonanie wizerunku,
2) rozpowszechniany jest wizerunek osoby powszechnie znanej (z zastrzeżeniem przewidzianym przez prawo autorskie – o czym będzie mowa w dalszej części publikacji),
3) wizerunek danej osoby został uwidoczniony jako element większej całości (np. zdjęcia krajobrazu, zgromadzenia, zdjęcia z imprezy masowej).

Znaczy to, iż poza ww. sytuacjami, wskazanymi w ustawie, zawsze powinno się uzyskać zgodę na rozpowszechnienie wizerunku danej osoby.

W ostatnim czasie do dóbr osobistych często naruszanych w sieci dołączyły uczucia religijne. Naruszenie uczuć religijnych może nastąpić poprzez wyśmiewanie, ośmieszanie, prezentowanie przedmiotów kultu religijnego w określonym (np. seksualnym) kontekście, parodiowanie z intencją poniżenia itp. Warto pamiętać, że również przepisy prawa karnego zabraniają obrażania uczuć religijnych oraz publicznego znieważania miejsc lub przedmiotów kultu (art. 196 kk).

Dobrem osobistym, które wskutek rozwoju Internetu (w tym portali plotkarskich i forów internetowych) jest bardzo często naruszane, jest prywatność. Prywatność ma związek między innymi z tajemnicą korespondencji, prawem do wizerunku czy też nietykalnością mieszkania.

Prawo do prywatności jest zagwarantowane przez konstytucję i jest o nim mowa w dwóch artykułach. Każdy ma prawo do poszanowania jego życia prywatnego i rodzinnego (art. 47 Konstytucji RP), zaś jakiekolwiek ujawnienie informacji prywatnych może być wymagane tylko zgodnie z ustawą (art. 51 Konstytucji RP).

W wielu orzeczeniach pojawia się odniesienie do prywatności i zakazu publikowania informacji. Nie można na przykład publikować informacji dotyczących:

– zadłużenia danej osoby,
– stosunków małżeńskich (partnerskich),
– relacji pozamałżeńskich,
– nałogów, chorób,
– preferencji seksualnych,
– stanu majątku (zarobków).

Takie informacje nie powinny być dostępne publicznie. Wyjątkiem jest sytuacja, w której dotyczą one osoby publicznej i są podawane w związku z pełnieniem przez nią funkcji publicznych.

Sposoby naruszania dóbr osobistych w sieci. Specyfika forum internetowego

Sposobów może być bardzo wiele – od publikacji czyjegoś wizerunku (często w intymnym kontekście), przez obrażenie (np. przypisanie opisywanemu człowiekowi takich cech, które mogą go poniżać w opinii publicznej), aż do przypisywania czynów karalnych czy sugerowania działań amoralnych.

Dobra osobiste można naruszyć, używając wulgarnego języka, określeń pejoratywnych lub obelg. Często dochodzi do tego na forach internetowych, na których ludzie przedstawiają swoje poglądy. Oto niektóre opinie sądów na ten temat:

– język internautów na forum internetowym jest dosadny, skrótowy, często odbiega od standardów „normalnej" (niewirtualnej) komunikacji,
– często wulgaryzmy, które służą podkreśleniu ekspresji wypowiedzi, są tolerowane, a nawet powszechnie używane na forum,
– wulgaryzmy czy obelgi, jeśli nikomu nie uwłaczają, nie naruszają dóbr osobistych,
– należy uwzględnić specyfikę forum, gdzie sądy bywają wypowiadane spontanicznie, czasem bez namysłu, niekiedy w czasie żarliwej dyskusji – język może być w związku z tym dosadny.

Na pewno dosadny język na forum internetowym może być dopuszczalny, gdyż jest ono miejscem rozmowy, a w trakcie każdej rozmowy mogą być wypowiadane różne opinie. Nie znaczy to jednak, że można posunąć się do naruszenia dóbr osobistych. Warto podkreślić, że takie naruszenie może być dokonane w różnych formach – audialnej, wizualnej, pisemnej itp. Anonimowość (która zresztą może okazać się pozorna) wcale nie gwarantuje bezkarności.

Adwokat Monika Brzozowska

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

PR821-CH Kontroler dostępu do zastosowań hotelowych

- Realizacja kontroli dostępu do pokoju hotelowego
- Funkcje automatyki umożliwiające sterowanie:
  - zasilaniem elektrycznym pokoju
  - klimatyzacją
  - sygnalizacjami: Nie przeszkadzać, Posprzątać, Pomoc
- Współpraca z panelem dotykowych przycisków funkcyjnych HRT82FK oraz czytnikiem korytarzowym HRT82M

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

roger®

NOVUS®

KAMERY IP 3 MPX 15 kl/s

ciągłość obserwacji dla standardowych zastosowań

Kamery IP 3 MPX 15 kl/s generują obraz pełen detali, dzięki temu w sytuacji zagrożenia łatwo zidentyfikować ewentualnych sprawców zdarzeń.

BO W MONITORINGU LICZY SIĘ PEWNOŚĆ

NOVUS IP | NMS Compatible | ONVIF | 3000 SERIA IP | NOVUS 3 lata gwarancji

Kamery 3 MPX serii 3000 15 kl/s

wandaloodporne: NVIP-3DN3012V/IR-1P, NVIP-3DN3013V/IR-1P, NVIP-3DN3014V/IR-1P

w obudowie: NVIP-3DN3011H/IR-1P, NVIP-3DN3012H/IR-1P

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

Niska cena, wysoka jakość

[15 kl/s dla 3 MPX]

Kamery dostarczają obraz z prędkością 15 kl/s w rozdzielczości 3 MPX oraz 30 kl/s w rozdzielczości 2 MPX (i niższych), więc uzyskujemy wysokiej jakości materiał wideo, pełen szczegółów. Równocześnie kamery mogą generować do 3 strumieni o różnych parametrach. Dzięki wyjątkowo atrakcyjnej cenie, są doskonałym rozwiązaniem dla inwestorów z ograniczonym budżetem lub do instalacji z dużą liczbą punktów kamerowych

Uniwersalne, do różnych zastosowań

[IP 66]

Kamery zostały przystosowane do całodobowej obserwacji pomieszczeń wewnątrz budynków, jak również ich otoczenia zewnętrznego - drzwi wejściowych, bram, placów zabaw, boisk, parków. Dostępne modele wyposażone są w obiektywy o stałej lub zmiennej ogniskowej (f=4 mm lub f=2.8 ~ 12 mm), mogą pracować w temperaturze od -40°C do 50°C i są odporne na niekorzystne warunki pogodowe (klasa szczelności IP 66). Kamery NVIP-3DN301xV/IR-1P mają wandaloodporne obudowy z klasą ochrony IK 10, które chronią je przed uszkodzeniem mechanicznym

Kompatybilne z oprogramowaniem

NOVUS MANAGEMENT SYSTEM

Wydajne w trudnych warunkach oświetleniowych

[WDR]

Każda kamera jest wyposażona w oświetlacz IR, który umożliwia pracę w ciemności oraz funkcję szerokiego zakresu dynamiki WDR, pozwalającą na efektywną pracę kamer w nowoczesnych budynkach, z pomieszczeniami o przeszklonych ścianach lub z intensywnym sztucznym oświetleniem

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

DH-NVR608-64-4K

Wizyjny rejestrator sieciowy, 64 kanały o rozdzielczości 4K

Właściwości

- Obsługa 64 kamer IP
- Maksymalne pasmo wejściowe 384 Mb/s
- Rejestracja i odtwarzanie obrazów o rozdzielczości do 12 Mpx
- Jedno wyjście VGA i dwa wyjścia HDMI
- Obsługa macierzy RAID
- Obsługa N+M hot standby
- Obsługa jednostek pamięci iSCSI
- Kompatybilności z Dahua SDK pozwala na integrację z innymi platformami
- Obsługa kamer sieciowych różnych producentów: Dahua, Arecont Vision, AXIS, Bosch, Brickcom, Canon, CP Plus, Dynacolor, Honeywell, Panasonic,Pelco, Samsung, Sanyo, Sony, Videotec, Vivotek itd.
- Zgodność z ONVIF w wersji 2.4
- Możliwość użycia modułu zasilania rezerwowego (DH-NVR608R-64-4K)

Model	DH-NVR608-64-4K
System	
Główny procesor	Intel
System operacyjny	LINUX
Obraz i dźwięk	
Wejście dla kamer	64 kanałów IP
Dwukierunkowa komunikacja głosowa	jeden kanał wejściowy, jeden kanał wyjściowy, złącza RCA
Wyświetlane obrazy	
Interfejsy	dwa interfejsy HDMI (maks. rozdzielczość 3840×2160), jeden interfejs VGA
Rozdzielczość	3840×2160, 1920×1080, 1280×1024, 1280×720, 1024×768
Rejestracja obrazów	
Kompresja	H.265/H.264/MJPEG
Rozdzielczość	12, 8, 6, 5, 3, 1,3 Mpx, formaty 1080p i 720p
Prędkość zapisu	256 Mb/s
Przepływność	strumienie wizyjne 1 Mb/s ~ 20 Mb/s
Detekcja ruchu i funkcje alarmowe	
Wejścia alarmowe	16 kanałów, aktywny stan niski
Wyjścia przekaźnikowe	8 programowalnych kanałów NO/NC, obciążalność styków 1 A przy 24 V_{DC}
Sieć	
Interfejsy sieciowe	dwa porty RJ-45 10/100/1000 Mb/s
Ethernet	dwa niezależne porty Ethernet 1000 Mb/s
Liczba użytkowników	maks. 128
Obsługa przez smartfony	iPhone, iPad, Android, Windows Phone
Pamięć	
Wbudowane dyski HDD	osiem portów SATA III, maks. 48 TB
Tryb pracy dysków HDD	indywidualnie lub w macierzy Raid
Dodatkowe interfejsy	
USB	cztery porty USB, w tym trzy porty USB 2.0 i jeden port USB 3.0
eSATA	jeden port eSATA
RS232	jeden port do komunikacji z PC i klawiaturą
RS485	jeden port do sterowania kamer PTZ
Inne dane	
Zasilanie	110 V_{AC}~240 V_{AC}, 50~60 Hz
Pobór mocy	poniżej 40 W (bez uwzględnienia dysków HDD)
Warunki środowiskowe	temperatura -10°C~+55°C, wilgotność 10%~90%, ciśnienie atm. 86 kPa~106 kPa
Wymiary	486 mm (z uchwytami)×454,9 mm×91 mm
Masa	9 kg (bez dysków HDD)

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 65000 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-D50.

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: 65 000
- 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
- Klasa środowiskowa: II

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

PR312EM & PR312MF
Kontrolery dostępu z wbudowanymi czytnikami kart

Kontrolery **PR312EM** oraz **PR312MF** należą do rodziny zaawansowanych kontrolerów dostępu serii PRxx2 z wbudowanymi czytnikami dostępu oraz zestawem wbudowanych wejść i wyjść. Kontroler PR312EM współpracuje z kartami zbliżeniowymi standardu EM 125 kHz natomiast kontroler PR312MF z kartami standardu ISO14443A i MIFARE. Dostępne są urządzenia w wersji z klawiaturą oraz bez niej. Kontrolery typu PR312 mogą być stosowane jako autonomiczne punkty kontroli dostępu lub tworzyć sieć w ramach systemu kontroli dostępu RACS 4 obejmującego wiele kontrolerów dostępu i zarządzaną z poziomu aplikacji PR Master.

Charakterystyka

- Wbudowany czytnik standardu EM 125 KHz (PR312EM)
- Wbudowany czytnik standardu ISO 14443A i MIFARE (PR312MF)
- Dwustronna kontrola drzwi po dołączeniu czytnika serii PRT (ROGER)
- 4 000 użytkowników
- Bufor 32 000 zdarzeń
- Zasilanie 12 V_{DC}
- Wyjście przekaźnikowe 1,5 A/30 V
- Dwa wyjścia tranzystorowe
- Trzy wejścia NO/NC
- Klawiatura silikonowa z podświetleniem
- Dwa klawisze funkcyjne
- Wbudowany głośnik
- Praca w warunkach zewnętrznych
- Ochrona antysabotażowa (tamper)
- Komunikacja przez RS485 (dowolna topologia)
- Funkcje specjalne: wejście komisyjne, wejście warunkowe, losowa kontrola użytkowników
- Możliwa integracja z systemem alarmowym metodą sprzętową lub programową(*)
- Rejestrowanie zdarzeń dla celów rozliczania czasu pracy
- Tryby drzwi: normalny, zablokowane, odblokowane i warunkowo odblokowane
- Tryby identyfikacji: karta lub PIN, karta i PIN, tylko karta, tylko PIN
- Kontrola dostępu w windach (wymagany moduł XM-8)

* system RACS 4 umożliwia integrację programową z centralami INTEGRA firmy SATEL za pośrednictwem modułu INT-RS

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 przycisków 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

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

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 Sp. J.
ul. Bonarka 21
30-415 Kraków
tel./faks 12 263 93 85
email: 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
www.activetrack.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

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
02-672 Warszawa
tel. 801 133 084
e-mail: info@legrand.com.pl
www.legrand.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./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

ROPAM Elektronik s.c.
ul. Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07
faks 12 379 34 10
e-mail: biuro@ropam.com.pl
www.ropam.com.pl
www.ropam.eu

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

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

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

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

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. Rozdzieńskiego 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

NOVUS®

Rejestratory IP serii 5000

kompatybilne z oprogramowaniem NMS (Novus Management System)

5000 SERIA IP

NMS obsługuje rejestratory IP serii 5000

Pozwala na jednoczesne połączenie z wieloma rejestratorami IP 5000 w trybie podglądu „na żywo" i odtwarzania nagrań

NMS Compatible

Niższe koszty budowy systemu

W przypadku rozbudowanych, wielokamerowych systemów IP, rejestratory standalone serii 5000 można wykorzystać do archiwizacji nagrań, jako tańszą alternatywę dla rejestratorów typu PC-based. W zależności od potrzeb, w ramach jednego systemu, można dowolnie zestawiać rejestratory IP 5000 oraz PC-based

NMS działa jak stacja kliencka dla rejestratorów IP serii 5000

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

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	–
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	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	–
ROPAM Elektronik	TAK	–	TAK	–	TAK
Samsung Techwin Europe	TAK	–	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	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 kart, akcesoria do identyfikatorów, karty 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 GPS, produkcja OEM/ODM, 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
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	–	–
ROPAM Elektronik	TAK	TAK	TAK	–	–	TAK	TAK	–	–
Samsung Techwin Europe	–	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	–	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

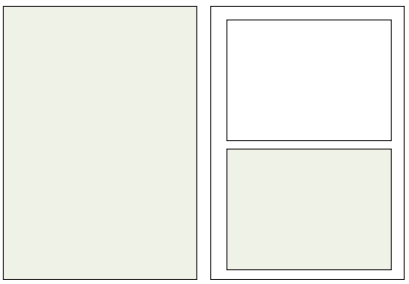
Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. 22 546 0 951, 953
faks 22 546 0 959
www.zabezpieczenia.com.pl

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

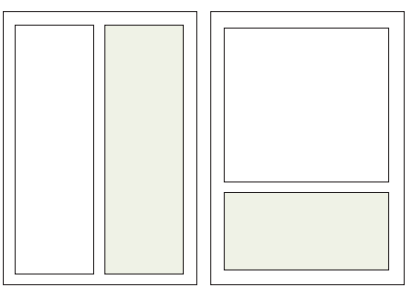
Dostępne formy reklamy

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

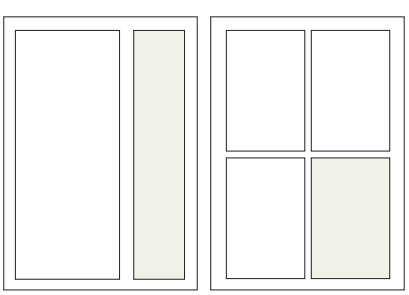
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)


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

dahua TECHNOLOGY

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

OGÓŁ i szczegóły.

Kamera sieciowa AXIS Q6000-E

AXIS Q6000-E zawiera cztery niezależne 2-megapikselowe przetworniki obrazu zapewniające pole widzenia 360° na dużych obszarach. Przy współpracy z kamerami PTZ serii AXIS Q60-E do zastosowań zewnętrznych umożliwia powiększenie optyczne dowolnego obszaru.

Aby zobaczyć działanie kamery AXIS Q6000–E i uzyskać informacje o wszystkich jej funkcjach, odwiedź naszą stronę www.axis.com

AXIS COMMUNICATIONS

Dystrybutorzy w Polsce: ABCDATA ADI GLOBAL DISTRIBUTION ANIXTER ARPOL ELEKTRONIKA DLA BEZPIECZEŃSTWA