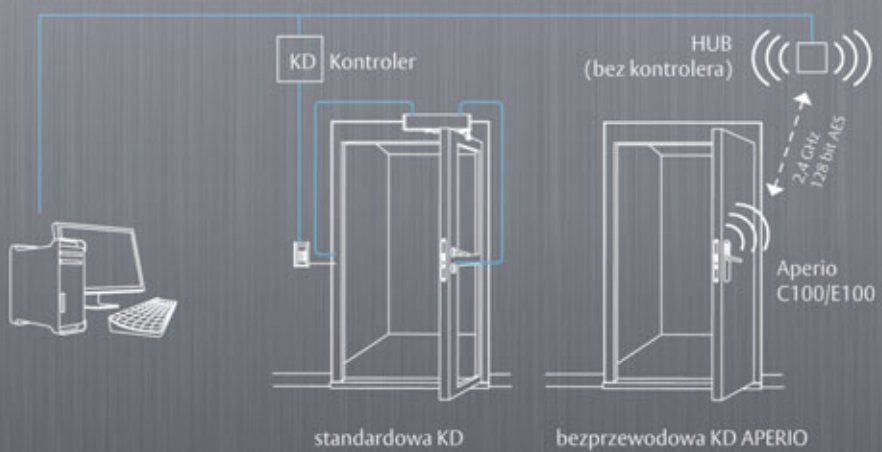
CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 4(80)/2011

ZABEZPIECZENIA

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

W NUMERZE:



aperio™

APERIO
bezprzewodowa technologia systemów kontroli dostępu

ASSA ABLOY

The global leader in
door opening solutions

Spis treści

CZASOPISMO ZABEZPIECZENIA 4/2011

Aspekty prawne a prawa dziecka w świetle zastosowania systemów monitoringu wizyjnego **18**

Dzięki systemowi Nedap AEOS nareszcie można skutecznie zarządzać kontrolą lotniskowych gate'ów **44**

Historia z przyszłością. Opowiadanie nie-*science-fiction* (część III) **52**

Prognoza dla systemów nagłośnieniowych. Nadciąga szerokopasmowy front układu wysokiego ciśnienia **64**

POLALARM zaprasza na XIII Forum Monitoringu Polskiego

Stowarzyszenie „POLALARM" serdecznie zaprasza do udziału w **XIII Forum Monitoringu Polskiego**, które odbędzie się w dniach **29 – 30 września 2011 r.** w Centrum Szkoleń i Konferencji GEOVITA w Jadwisinie.

Program, w trzech blokach tematycznych, obejmie m.in. następujące zagadnienia:

I blok: merytoryczny
- Monitorowanie sygnałów alarmowych w świetle nowych norm europejskich
- Nowe wymagania dotyczące rejestracji obrazu i dźwięku podczas trwania imprez masowych
- Wymagania dotyczące budowy nowoczesnych alarmowych centrów odbiorczych zgodnie z normą europejską EN 50518
- Oceny skuteczności działania centrum monitoringu
- Problematyka monitorowania obiektów ruchomych z wykorzystaniem informacji o położeniu GPS, przegląd obecnych trendów w największych agencjach ochrony

II blok: Monitoring sygnałów alarmowych i technicznych oraz obiektów ruchomych
- Zamiana transmisji alarmów metodą tonową, przez łącza PSTN, na postać sieciową TCP/IP
- Weryfikacja wizyjna, możliwości teoretyczne a praktyczne wdrożenia, ograniczenia techniczne oraz kosztowe

III blok: Monitoring wizyjny
- Monitoring wizyjny osiedli mieszkaniowych
- Analiza możliwości zastosowania nowoczesnych metod kompresji obrazów, w tym H.264 w zaawansowanych systemach monitoringu
- Upowszechnienie standardu Full HD w systemach monitoringu
- Zastosowanie łączy radiowych o dużym zasięgu na przykładzie sieciowych punktów retransmisyjnych

Program przewiduje także dyskusję po każdym bloku oraz dyskusję podsumowującą forum.

Zaproszenie i karta zgłoszenia będą wkrótce opublikowane na stronie *www.polalarm.org*. Osoby zainteresowane prosimy o kontakt z biurem zarządu stowarzyszenia „POLALARM" – tel. 22 626 90 31, 22 625 57 43, e-mail: *polalarm@polalarm.com.pl.*

Bezpośr. inf. POLALARM

„Pracownik zabezpieczenia technicznego w zakresie instalacji i konserwacji systemów alarmowych" zapraszamy na kursy

Dla osób zainteresowanych rozwojem zawodowym w branży ochrony osób i mienia firma **TARGET TRAINING** przygotowała profesjonalny kurs „Pracownik zabezpieczenia technicznego w zakresie instalacji i konserwacji systemów alarmowych". Prowadzimy go na terenie województwa zachodniopomorskiego, a od września br. będziemy prowadzić dla grup zorganizowanych także poza nim, w trybie dziennym, wieczorowym, weekendowym, a także w formie kształcenia na odległość.

Kurs trwa 120 godzin i skoncentrowany jest głównie na wykształceniu w uczestnikach umiejętności praktycznych, popartych rzetelną wiedzą merytoryczną. Naszymi wykładowcami są praktycy w dziedzinie zabezpieczeń technicznych, którzy chętnie dzielą się wiedzą zawodową i doświadczeniem. Przy kształceniu na odległość wiedzę teoretyczną w formie multimedialnego materiału szkoleniowego przekazujemy za pośrednictwem platformy e-learningowej, natomiast zajęcia praktyczne prowadzimy stacjonarnie w ramach zjazdów w trybie weekendowym. Taką formą kształcenia zainteresowane są głównie osoby zamieszkałe w miejscach oddalonych powyżej 150 kilometrów od miejsca realizacji zajęć.

Kurs kończy się egzaminem teoretycznym i praktycznym z zakresu umiejętności projektowania, wykonywania i uruchamiania systemu alarmowego, przeprowadzania analizy bezpieczeństwa obiektu oraz określania dokładnych kosztów materiałów i robót. Nasi absolwenci otrzymują zaświadczenia o ukończeniu kursu na druku MEN. Z tymi zaświadczeniami mogą wystąpić do właściwej dla swojego miejsca zamieszkania komendy wojewódzkiej policji i bez dodatkowych egzaminów uzyskać licencję pracownika zabezpieczenia technicznego pierwszego stopnia.

Najbliższą edycję szkolenia zaplanowaliśmy na okres **10.09.2011 r. – 29.10.2011 r.** (tryb weekendowy). Więcej informacji i formularz zgłoszenia do udziału w szkoleniu znajdą Państwo na stronie *www.target-training.pl*.

Bezpośr. inf. Tadeusz Taniewski, Maja Kornel
TARGET TRAINING

Nowa linia specjalistycznych, samodzielnych rejestratorów obrazu

Firma Rett-Pol Telewizja Przemysłowa i Telekomunikacja ma przyjemność poinformować o wprowadzeniu do oferty nowej linii specjalistycznych, samodzielnych rejestratorów obrazu, przeznaczonych do pracy w trudnych warunkach atmosferycznych, na otwartej przestrzeni. Poniżej prezentujemy główny model serii, dostępny już w ofercie firmy – RP-EKO-5210A.

RP-EKO-5210A to specjalistyczny aparat cyfrowy, działający bezobsługowo dzięki wbudowanym czujnikom ruchu. Został opracowany w celu obserwacji terenów otwartych, gdzie nie ma możliwości wykonania skomplikowanej instalacji kablowej, a zachodzi konieczność ciągłej ochrony. Możliwość doboru jednego z wielu dostępnych trybów pracy rozszerza zakres zastosowań aparatu i czyni go idealną „fotopułapką". Urządzenie może być wykorzystywane do obserwacji przyrody, zarówno przez jej strażników, jak i wielbicieli. Dzięki połączeniu zwartej konstrukcji z wysoką funkcjonalnością „Leśny Wielki Brat" stanowi idealne rozwiązanie dla wszystkich osób pragnących dyskretnie obserwować przyrodę.

Najważniejsze cechy aparatu to:
- automatyczne wykonywanie zdjęć dzięki zastosowaniu trzech czujników ruchu (mają one zasięg 20 metrów),
- wbudowany oświetlacz pracujący w podczerwieni (o zasięgu 10 metrów), przydatny podczas wykonywania zdjęć nocnych,
- wodoszczelna obudowa chroniąca aparat przed wpływem warunków atmosferycznych,
- matryca o rozmiarach 12 megapikseli,
- możliwość podłączenia do telewizora.

Bezpośr. inf. Rett-Pol
Telewizja Przemysłowa i Telekomunikacja

Samsung mianuje IP Product Managera na Europę

John Fisk pracuje w branży zabezpieczeń elektronicznych od ponad piętnastu lat. Bezpośrednio przed przejściem do **Samsunga** pracował w firmie Norbain na różnych stanowiskach, w tym jako Branded CCTV Product Manager.

Na nowym stanowisku będzie on odpowiedzialny za specjalistyczne doradztwo przed- i posprzedażowe w dziedzinie produktów sieciowych, jak również za pomoc projektową i techniczną przy realizacji dużych projektów.

– *Samsung jest w trakcie intensywnego rozwoju gamy produktów iPOLiS opartych na technologii sieciowej , dlatego moje zadanie jest bardzo ważne i niezwykle cieszę się z danej mi szansy* – powiedział John Fisk. – *Skoncentruję się na zapewnieniu klientom firmy Samsung w Europie wszelkich informacji niezbędnych do świadomego rekomendowania rozwiązań marki Samsung z zakresu bezpieczeństwa opartych na technologii IP.*

Nominacja ta odzwierciedla przekonanie firmy Samsung, dotyczące wzrastającego znaczenia sieciowych systemów zabezpieczających, które wkrótce będą stanowiły większość wśród nowo powstających średnich i dużych systemów w Europie. Konsultanci, instalatorzy i integratorzy systemów coraz częściej polecają rozwiązania sieciowe.

Bezpośr. inf. David Solomons
DRS Marketing

Avanguard+ Kontroler systemu kontroli dostępu

Firma **chomtech.pl** wprowadziła do sprzedaży kontroler **Avanguard+**. Jest to specjalistyczne urządzenie mikroprocesorowe stosowane w systemach zabezpieczeń technicznych i automatycznej identyfikacji ze szczególnym uwzględnieniem m.in. kontroli dostępu, obsługi szafek basenowych, śluz i kamer IP. Nowością w kontrolerze Avaguard+ jest umożliwienie połączenia z nadrzędnym kontrolerem Avanguard Professional, co pozwala na wykorzystanie wszystkich zaawansowanych możliwości kontrolera nadrzędnego. Jeżeli na miejscu istniejącego kontrolera Avanguard+ zainstalujemy kontroler Avanguard Professional, to Avanguard+ stanie się sterownikiem lokalnym, a Avanguard Professional przejmie globalne zarządzanie systemem kontroli dostępu.

Kontroler Avanguard+ steruje pracą czytników identyfikatorów, zapewniając pełną identyfikację i rejestrację zdarzeń. Monitoruje oraz rejestruje sygnały z różnych urządzeń dodatkowych, takich jak czujnik otwarcia drzwi, przycisk otwarcia awaryjnego, łącznik sabotażowy czytnika kontroli dostępu itp.

Dla każdego z urządzeń kontroler pozwala zdefiniować wiele typów reakcji, zapisywanych w pamięci wewnętrznej.

Avanguard+ może sterować czytnikami identyfikatorów i ustalać ich tryby pracy bazujące na harmonogramach. Kontroler może pracować zarówno pod nadzorem komputera nadrzędnego, jak i samodzielnie w trybie stand-alone. Rozwiązanie takie daje dużą elastyczność, szczególnie w systemach, gdzie stała komunikacja z komputerem nadrzędnym nie jest możliwa.

Bezpośr. inf. chomtech.pl
Opracowanie: redakcja

Nowa kamera kopułkowa
w ofercie firmy Rett-Pol

Firma **Rett-Pol Telewizja Przemysłowa i Telekomunikacja** informuje o wprowadzeniu do oferty nowej kopułkowej kamery, oznaczonej indeksem **RP-DVS-600IR-V**. Kluczowymi cechami tego produktu są innowacyjny przetwornik Sony Super HAD oraz obiektyw o ogniskowej regulowanej w zakresie 2,8 mm – 12 mm.

To idealne rozwiązanie dla najbardziej wymagających użytkowników, a w szczególności odpowiednie dla dużych pomieszczeń, które implikują zastosowanie najdoskonalszej technologii z możliwością wykonywania dużych powiększeń obrazu – mówi **Dariusz Godlewski**, prezes zarządu firmy Rett-Pol.

RP-DVS-600IR-V to nowy model kamery bazujący na przetworniku obrazu CCD SONY Super HAD. Przetwornik Super HAD to rozwiązanie pozwalające na budowę kamer o wysokiej czułości i znakomitej jakości obrazu. Kamera RP-DVS-600IR-V jest wyposażona w wysokiej jakości obiektyw o ogniskowej regulowanej w zakresie 2,8 – 12 mm, a dodatkowo posiada wbudowany promiennik IR zapewniający doświetlenie obserwowanej sceny, zarówno w ciemności, jak i w trudnych warunkach oświetleniowych. Rozbudowane, intuicyjne menu OSD oraz przełącznik na przewodzie pozwalają na łatwe sterowanie wszystkimi funkcjami kamery.

Kluczowe cechy kamery to:

– **regulacja migawki** – funkcja pozwalająca między innymi na precyzyjne uchwycenie szybko poruszającego się obiektu;
– **funkcja BLC** (kompensacja światła tylnego) – zmieniająca sposób pomiaru światła i doboru ekspozycji w celu poprawnego odwzorowania obiektów znajdujących się w cieniu lub na silnie rozświetlonym tle;

– **D-WDR (Digital Wide Dynamic Removable)** – funkcja wyrównująca jasność obrazu na całej jego powierzchni, tak aby zwiększyć jego czytelność;
– **SUNSE UP system** – funkcja pozwalająca na wydłużenie czasu otwarcia migawki matrycy CCD ze standardowej wartości 1/50 s nawet do 2 s.
– **szczelna obudowa** (o stopniu szczelności IP66) – umożliwiająca montaż kamery wewnątrz i na zewnątrz obiektu, w różnych pozycjach roboczych, zarówno na suficie, jak i na ścianie. Moduł kamery jest umieszczony w obudowie kulowej, co umożliwia jego obrót w dowolnej osi. Warto nadmienić, że wandaloodporna obudowa jest zbudowana z trwałych materiałów, które skutecznie chronią moduł kamery przed uszkodzeniami mechanicznymi oraz przed oddziaływaniem warunków atmosferycznych.

Bezpośr. inf. Rett-Pol
Telewizja Przemysłowa i Telekomunikacja

Seria kamer
z wbudowaną obsługą IVA

Kamery sieciowe z popularnych serii firmy **Bosch** są teraz dostarczane z fabrycznie uaktywnioną opcją inteligentnej analizy obrazu (IVA). Dotyczy to serii Dinion, FlexiDome, AutoDome, AutoDome Junior oraz termicznych kamer IP firmy Bosch. Oznacza to, że kupowanie oddzielnej licencji i rejestracja przez internet każdej kamery nie są już konieczne. Nadal dostępne są poprzednie modele kamer, zarówno z opcją IVA (ale wymagające oddzielnego zakupu licencji i aktywacji), jak i bez niej.

Rozwiązania z uaktywnioną obsługą technologii IVA są bardzo ekonomiczne i znacznie łatwiejsze do realizacji. Korzyści te są szczególnie odczuwalne w przypadku dużych instalacji. – *Wyobraźmy sobie system składający się z pięciuset kamer wykorzystujących technologię IVA oraz ich rejestrację przez internet i aktywowanie każdej z osobna* – powiedział Gerard Otterspeer, product marketing manager EMEA w firmie Bosch Security Systems. – *Obecnie, dzięki wstępnej aktywacji IVA, procesu tego można uniknąć, co pozwala zaoszczędzić czas. Zalety technologii IVA są teraz dostępne dla szerszego grona odbiorców telewizji dozorowej.*

Kamery firmy Bosch wyposażone w technologię IVA stanowią istotny element infrastruktury systemów nadzoru wizyjnego, udostępniają bowiem pracownikom ochrony wydajne i skuteczne narzędzie służące do wykrywania zdarzeń i generowania alarmów. Zoptymalizowana technologia IVA jest dostosowana do pracy w każdej serii kamer. Jej wyspecjalizowane wersje są instalowane również w kamerach HD i kamerach termicznych firmy Bosch.

Działając niezależnie w każdej kamerze, technologia IVA oferuje szeroką gamę zaawansowanych funkcji – od wykrywania ruchu po śledzenie jego trajektorii. Zdarzenia są wyświetlane natychmiast, a dane mogą być także archiwizowane w celu późniejszego odtworzenia za pomocą funkcji *Forensic Search* firmy Bosch.

IVA to kompleksowy system, który wychwytuje nawet drobne szczegóły rejestrowanych scen. Umożliwia to wyszukanie każdego zdarzenia – nawet jeśli początkowo nie było ono zdefiniowane jako sytuacja alarmowa.

Bezpośr. inf. Bosch Security Systems

Nowa wersja popularnego kontrolera dostępu PR402 w ofercie firmy ROGER

Firma **ROGER**, krajowy lider w dziedzinie profesjonalnych systemów kontroli dostępu oraz rozliczania czasu pracy, rozszerzyła swoją ofertę o nowy kontroler pojedynczego przejścia o symbolu **PR402DR**, który stanowi ulepszoną wersję popularnego kontrolera PR402. Nowe urządzenie ma wszystkie funkcje swojego poprzednika, a dodatkowo kilka nowych:

– cztery dodatkowe programowalne linie wejściowe NO/NC,
– możliwość zasilania z napięcia stałego 12 V_{DC} lub 24 V_{DC},
– możliwość sterowania obciążeniem 5 A/230 V_{AC},
– możliwość ustawienia adresu kontrolera za pomocą zworek,
– panel wskaźników LED zabudowany w obudowie kontrolera,
– możliwość montażu na szynie DIN lub jako moduł elektroniczny.

Kontroler dostępu PR402DR, tak jak jego poprzednik, może funkcjonować jako autonomiczny punkt kontroli dostępu lub jako element systemu sieciowego RACS4. Urządzenie jest przystosowane do pracy z jednym lub dwoma zewnętrznymi czytnikami dostępu, przy czym mogą to być czytniki popularnej serii PRT produkowanej przez firmę ROGER, jak również dowolne inne czytniki z interfejsem Wiegand lub Magstripe. Możliwość współpracy z czytnikami Wieganda jest szczególnie wskazana w sytuacji, gdy w danym obiekcie są już zainstalowane tego typu czytniki lub gdy zachodzi potrzeba dołączenia do kontrolera czytników specjalnych, takich jak czytniki dalekiego zasięgu, czytniki biometryczne itp. Kontroler PR402DR, podobnie jak jego poprzednik, ma m.in. wbudowany zegar czasu rzeczywistego, bufor pamięci zdarzeń (o pojemności 32 000 zdarzeń) oraz monitorowany zasilacz buforowy.

Cechą charakterystyczną kontrolera PR402DR jest dostępność w dwóch opcjach: jako moduł w obudowie z tworzywa sztucznego do montażu na standardowej szynie DIN 35 mm oraz jako moduł PCB. Pierwsza z podanych możliwości zdecydowanie upraszcza instalację dużych systemów poprzez efektywne wykorzystanie przestrzeni dostępnej wewnątrz standardowych obudów dla sprzętu elektrycznego. Daje to także możliwość instalacji kontrolera w istniejącej już obudowie zawierającej urządzenia elektryczne, co pozwala zredukować przestrzeń zajmowaną przez instalację KD.

Bezpośr. inf. ROGER

Bosch gwarancją najwyższej jakości
Etykieta z hologramem na CCS 900 Ultro

System kongresowy CCS 900 Ultro, zaprojektowany i wyprodukowany przez specjalistów Bosch w Europie, jest wynikiem wieloletnich doświadczeń w tworzeniu takich systemów. System ten cechuje się ergonomią i estetyką, elastycznością działania oraz znakomitą jakością dźwięku zoptymalizowaną pod kątem mowy. Obecnie na dolnej części obudowy tego urządzenia umieszczana jest etykieta z hologramem, który potwierdza oryginalność i wysoką jakość produktu marki Bosch. **Bosch Security Systems** wprowadził uniwersalny system kongresowy CCS 900 Ultro przede wszystkim z myślą o niedużych i średniej wielkości salach (np. w ratuszu miejskim), lokalnych centrach biznesowych i salach sądowych. System oferuje wiele funkcji ułatwiających prowadzenie spotkań, w tym zaawansowaną, zgłoszoną do opatentowania, funkcję *possible-to-speak*, sygnalizującą wizualnie za pomocą wskaźnika, kiedy uczestnik dyskusji może zabrać głos. Użytkownicy mogą słuchać obrad i w łatwy sposób bezpośrednio w nich uczestniczyć.

System oferuje również znakomitą zrozumiałość mowy dzięki opracowanej przez firmę Bosch technologii DAFS (ang. *Digital Acoustic Feedback Suppressor* – eliminator sprzężeń akustycznych). Od wielu lat technologia ta sprawdza się w systemach kongresowych i nagłośnieniowych produkowanych przez Bosch Security Systems.

Uniwersalny system CCS 900 Ultro działa w technologii *plug and play*. Z tego względu nie wymaga specjalnego przeszkolenia ani operatora obsługującego system. Dzięki intuicyjnej obsłudze każdy użytkownik może od razu rozpocząć pracę z systemem.

Bezpośr. inf. Bosch Security Systems

Samsung mianuje Business Development Managera na Polskę i kraje bałtyckie

Marcin Kucharski będzie odpowiedzialny za rozwój relacji z kluczowymi klientami z tego obszaru i użytkownikami końcowymi. Do jego zadań będzie należeć znajdowanie nowych możliwości sprzedaży produktów firmy Samsung: urządzeń sieciowych, systemów dozorowych CCTV, kontroli dostępu oraz wykrywania zagrożeń. Będzie także zapewniał wsparcie dla partnerów realizujących duże projekty.

Marcin Kucharski jest absolwentem Wydziału Elektrotechniki i Elektroniki Politechniki Łódzkiej. Rozpoczynał karierę zawodową jako specjalista IT/Telecom w Telekomunikacji Polskiej. Od dziesięciu lat jest związany z branżą zabezpieczeń elektronicznych (pracował między innymi w Risco Group na stanowisku Market Development and Sales Managera).

– *Z wielką niecierpliwością czekam na rozpoczęcie pracy z dotychczasowymi klientami firmy Samsung w Polsce i krajach bałtyckich* – powiedział Marcin Kucharski. – *Jestem bardzo podekscytowany perspektywą budowania relacji z nowymi klientami, którzy bez wątpienia będą pod wrażeniem tempa poszerzania zakresu oferty naszych produktów sieciowych, w skład której wchodzą już obecnie kamery Full HD oraz wyjątkowa linia urządzeń rejestrujących NVR. Nasza zdolność dostarczania zintegrowanych rozwiązań z zakresu bezpieczeństwa – zarówno dla pojedynczych obiektów, jak i rozbudowanych, miejskich systemów nadzoru – z pewnością zainteresuje integratorów poszukujących nowych możliwości biznesowych w tym ważnym obszarze.*

Marcin Kucharski będzie pracował razem z Piotrem Rogalewskim, menedżerem ds. technicznych i przedsprzedażowych.

Kontakt z Marcinem Kucharskim:

– telefoniczny: +48 607 60 30 09,

– lub za pośrednictwem poczty elektronicznej: *marcin.kucharski@samsung.com*.

Bezpośr. inf. David Solomons
DRS Marketing

Czujki ruchu firmy Bosch

Firmy z grupy **Bosch** konsekwentnie dążą do tego, aby ich wyroby odpowiadały na zmieniające się potrzeby rynku i były najnowocześniejsze technicznie, nowatorskie, wydajne, atrakcyjne i ergonomiczne.

W tym celu firma Bosch inwestuje średnio 11% wartości swojej sprzedaży w prace badawczo-rozwojowe. Firma zatrudnia na całym świecie ponad 25 tys. specjalistów pracujących nad ulepszaniem istniejących już rozwiązań i rozwojem nowych. Wynikiem tych prac są często produkty wyznaczające nowe standardy w branży.

Firma Bosch Security Systems ma wieloletnie tradycje związane z innowacyjnością w zakresie technologii alarmowej – uzyskała ponad trzydzieści patentów w tej dziedzinie. Wiele produktów będących pochodną tych patentów, np. czujnik ruchu *Pet Immunity* oraz układ *Microwave Noise Override*, stało się na rynku standardami.

Wiele spośród najnowszych innowacji w technologii czujek ruchu jest wynikiem współpracy między doświadczonymi projektantami czujek z firmy Bosch Security Systems oraz z centralnych ośrodków badawczych, które obsługują wszystkie jednostki biznesowe firmy Bosch, udostępniając im wyniki prowadzonych badań i najnowsze technologie.

W 1999 roku firma Bosch powołała w Ameryce Północnej Centrum Badawczo-Technologiczne (*Research and Technology Center* – RTC). Jest to jej pierwszy położony poza terenem Niemiec ośrodek zajmujący się wyłącznie pracami badawczo-rozwojowymi. Centrum to miało dotychczas dwa oddziały – w Palo Alto (Kalifornia) oraz w Pittsburgu (Pensylwania). Ostatnio powstał trzeci oddział w Cambridge (Massachusetts). Strategiczne położenie tych oddziałów umożliwia ścisłą współpracę nad rozwojem najnowocześniejszych technologii między pracownikami badawczymi z centrum Bosch RTC i znanymi uniwersytetami amerykańskimi, takimi jak Stanford, Berkeley, MIT i Carnegie Mellon.

Centrum Bosch RTC zatrudnia obecnie 63 pracowników badawczych zajmujących się wieloma kwestiami z zakresu zaawansowanych technologii oraz opracowywaniem produktów przeznaczonych do wykorzystania w branży motoryzacyjnej, budowlanej, towarów konsumpcyjnych oraz zastosowań przemysłowych. Oferta produktów obejmuje technologie czujek i komunikacji, protokoły bezprzewodowe, układy scalone, mikrosystemy elektromechaniczne (MEMS – *Micro Electro-Mechanical System*), aplikacje RF oraz oprogramowanie inżynierskie.

Połączone wysiłki zespołu badawczego oraz doświadczonych projektantów czujek ruchu z firmy Bosch Security Systems doprowadziły do opracowania najnowszej czujki ruchu z serii Professional. Centrum RTC przyczyniło się do tego poprzez udostępnienie wyników szeregu swoich badań, np. najlepszej w branży technologii antymaskingu oraz technologii Sensor Data Fusion, wykorzystującej zaawansowane algorytmy oprogramowania wbudowanego. Prace badawcze nad tymi rozwiązaniami nadal trwają.

W wyniku połączonych działań powstała seria wyjątkowych czujek ruchu, wyznaczająca nowe standardy bezpieczeństwa, niezawodności, trwałości i łatwości instalacji. Klienci zawsze kojarzą markę Bosch z wysoką jakością i innowacyjnością produktów. Wprowadzając na rynek nowe produkty, firma Bosch zawsze stara się o zachowanie i wzmocnienie tego wizerunku oraz zwiększenie zadowolenia klientów. W dziedzinie czujek ruchu oznacza to eliminację kosztownych fałszywych alarmów przy jednoczesnym zapewnieniu najwyższej skuteczności wykrywania włamania.

Czujki ruchu z serii Blue Line i Professional dowiodły swojej wysokiej jakości i niezawodności w wielu tysiącach instalacji alarmowych na całym świecie. Wiele firm instalujących systemy alarmowe kupuje czujki ruchu wyłącznie firmy Bosch.

Bezpośr. inf. Bosch Security Systems

Systemy przeciwpożarowe już dostępne w ofercie firmy Vidicon

Z przyjemnością informujemy, że firma **Vidicon** rozpoczęła sprzedaż zapowiadanych wcześniej central sygnalizacji alarmów pożarowych firmy **INIM Electronics**. W ofercie znajdują się centrale konwencjonalne – serii SmartLine, oraz adresowalne – serii SmartLight i SmartLoop.

Centrale konwencjonalne to modele różnej wielkości: od małych – dwuliniowych, do dużych – nawet 36-liniowych. Do każdej linii można włączyć do 30 czujek automatycznych lub do 10 ręcznych ostrzegaczy pożarowych.

Centrale adresowalne firmy Vidicon różnią się stopniem zaawansowania. Do prostszej serii SmartLight należą dwa modele wyposażone w jedną pętlę i, w zależności od modelu, mogące obsłużyć 64 lub 240 elementów adresowalnych (czujek i ROP-ów). Bardziej zaawansowane technicznie są centrale serii SmartLoop – jedno- lub dwupętlowe, z możliwością rozbudowy do ośmiu pętli. Mogą one pracować w sieci, zbudowanej z maksymalnie 30 central. W każdej z pętli można umieścić do 240 elementów adresowalnych, co przy maksymalnej konfiguracji sieciowej daje łącznie 57 600 elementów adresowalnych.

Wszystkie centrale wykorzystują unikatowe rozwiązania techniczne, które maksymalnie upraszczają instalację, serwis i konserwację takich systemów.

Więcej na temat central w numerze 4/2011 *Zabezpieczeń*.

Bezpośr. inf. Vidicon

Nowości w Sony Ipela

W ofercie handlowej firmy **Sony** są już dostępne sieciowe, szybkoobrotowe kamery o rozdzielczości HD i Full HD, zaprezentowane na tegorocznej wystawie IFSEC w Birmingham.

Są to dwa nowe modele z grupy Sony Ipela:

– **SNC-ER550** o rozdzielczości HD (1280×720 pikseli), z przetwornikiem CMOS Exmor 1/4" i obiektywem zmiennoogniskowym o krotności ×28 (maks. ogniskowa 98 mm);
– **SNC-ER580** o rozdzielczości Full HD (1920×1080 pikseli), z przetwornikiem CMOS Exmor 1/2,8" i obiektywem zmiennoogniskowym o krotności ×20 (maks. ogniskowa 94 mm).

Obie kamery mogą być zasilane metodą HPoE; ponadto dysponują opcją **e-flip**, czyli mają możliwość programowego odwracania obrazu o 180 stopni, co pozwala na ich montaż zarówno na wysięgniku – z modułem kamerowym zwróconym w dół, jak i na szczycie masztu – z modułem kamerowym zwróconym w górę. Maksymalny kąt obrotu modułu kamerowego w płaszczyźnie pionowej wynosi 210 stopni, co oznacza, że kamera zamocowana na wysięgniku jest w stanie obserwować obiekty znajdujące się 15 stopni powyżej linii horyzontu.

Bezpośr. inf. Altram

AN306 Ogrodzeniowa czujka wibracyjna nowej generacji

Na początku maja firma **ATLine** wprowadziła do swojej oferty nową ogrodzeniową czujkę wibracyjną **AN306** firmy **ANIKOM**, technologicznie bardzo zbliżoną do dobrze już znanej czujki AN307.

AN306 służy do ochrony jednej strefy metalowego ogrodzenia o maksymalnej długości trzystu metrów. Przewód czujki jest bardzo wrażliwy na wibracje mechaniczne, które występują na ogrodzeniu podczas próby przejścia przez nie. Kabel jest zakończony terminatorem i podłączony do sterownika systemu, który analizuje sygnały i wykrywa stany alarmowe. Dzięki wykorzystaniu najnowszej technologii DSIGPR czujka potrafi rozróżnić drgania mechaniczne ogrodzenia spowodowane naturalnymi zjawiskami pogodowymi, takimi jak na przykład wiatr, od drgań, których źródło jest inne niż naturalne wibracje. Drgania o źródle innym niż zwykłe zjawiska pogodowe są rejestrowane jako alarm. Zakłócenia spowodowane wpływem zewnętrznym, np. zakłócenia elektromagnetyczne, są skutecznie eliminowane. Czujka AN306 jest wyposażona w dwa wyjścia przekaźnikowe obsługujące dwie różne funkcje: sabotaż (przecięcie kabla detekcyjnego, jego zwarcie, odłączenie lub otwarcie obudowy) i alarm włamaniowy (sygnalizujący próbę wspinania się na ogrodzenie, odginania ogrodzenia w celu przejścia pod nim lub jego cięcia). Sterownik nie jest aktywowany podmuchami wiatru, chyba że ogrodzenie jest uszkodzone albo wiatr powoduje uderzanie jakimś przedmiotem o ogrodzenie. Powstawania alarmów nie powodują opady deszczu i śniegu ani ptaki siedzące na ogrodzeniu. Alarm powstaje również w wyniku odłączenia zasilania (wszystkie przekaźniki stają się rozwarte).

Bezpośr. inf. ATLine

Samsung wprowadza na rynek kamerę sieciową HD w pełni odporną na warunki pogodowe

Nowy produkt **Samsunga** to kamera sieciowa **SNO-5080R** – 1,3-megapikselowa, typu bullet.

Kamera ta, o stopniu szczelności IP66, odporna na trudne warunki pogodowe, została wyposażona we wszelkie komponenty kamery zewnętrznej w tym w obiektyw zmiennoogniskowy, osłonę przeciwsłoneczną i uchwyt. Może więc być zainstalowana natychmiast, bez konieczności montażu dodatkowych elementów.

Dzięki zastosowaniu wbudowanych diod LED pracujących w podczerwieni może generować obrazy o wysokiej rozdzielczości (720p) zarówno w świetle dziennym, jak i w całkowitej ciemności. Dzięki temu doskonale nadaje się do wielu zastosowań wymagających 24-godzinnego nadzoru, między innymi do monitorowania parkingów, obiektów przemysłowych, stacji benzynowych, szkół, szpitali, centrów handlowych, lotnisk i portów.

Model ten wyposażono w chipset Samsung WiseNet1 DSP, pozwalający na korzystanie z wielu zaawansowanych funkcji, takich jak:

– inteligentna analiza obrazu (IVA) z wirtualną barierą (*tripwire*) i możliwością detekcji kierunku wejścia w chroniony obszar lub wyjścia z niego,
– funkcja *Appear/Disappear* (pojawienie się/zniknięcie) do wykrywania zmian położenia obiektów.

Inteligentna analiza obrazu realizuje również funkcję monitorowania zmian pola widzenia kamery, włączającą alarm, gdy na przykład obiektyw kamery zostanie umyślnie zabrudzony farbą lub kąt obserwacji zostanie zmieniony bez autoryzacji.

Stosowane w modelu SNO-5080R metody kompresji – H.264, MPEG4, MJPEG i JPEG – dają użytkownikom możliwość równoczesnej transmisji obrazów do wielu odbiorców przy zróżnicowanej prędkości transmisji oraz w różnej rozdzielczości. Pozwala to uprawnionym użytkownikom na jednoczesne monitorowanie obrazów „na żywo" w jednym miejscu oraz ich rejestrowanie w innym miejscu. Równocześnie zastosowanie systemu PoE (*Power over Ethernet* – zasilanie przez Ethernet) redukuje koszty instalacji, zapewniając

zarówno zasilanie, jak transmisję wizji i dźwięku przez jeden kabel sieci Ethernet.

SNO-5080R korzysta z technologii *Samsung Super Dynamic Range* (SSDR), która automatycznie rozjaśnia niedoświetlone obszaru kadru, pozostawiając obszary jaśniejsze na niezmienionym poziomie jasności, dzięki czemu operatorzy mogą obserwować obiekty zwykle ukryte w cieniu. Kamera ta realizuje również funkcję Samsung Super Noise Reduction (SSNR) trzeciej generacji, eliminującą szumy spowodowane niedostatecznym oświetleniem, co pozwala na uzyskanie oszczędności w wykorzystaniu pasma transmisji oraz przestrzeni dyskowej urządzenia rejestrującego.

– Model SNO-5080R można określić jako kamerę sieciową dostosowaną do różnorodnych zastosowań zewnętrznych, wymagających obrazu megapikselowego lub o wysokiej rozdzielczości – powiedział **Peter Ainsworth**, senior product manager Europe w Samsung Techwin. *– Można ją szybko i łatwo zainstalować, jak również bez problemu podłączyć do istniejącej sieci. Co więcej, jako niezwykle atrakcyjna cenowo w porównaniu z innymi tego typu kamerami dostępnymi obecnie na rynku, sieciowa kamera SNO-5080R oferuje wielkie korzyści instalatorom rywalizującym o zlecenia na projekty wymagające dużej liczby kamer, ponieważ mogą oni uzyskać znaczne oszczędności dzięki eliminacji części kosztów przygotowawczych oraz instalacyjnych.*

Kamera sieciowa SNO-5080R jest dostępna u wszystkich autoryzowanych dystrybutorów produktów Samsung i oferowana z pełną obsługą serwisową Samsung Techwin (w tym również w zakresie projektowania systemu i bezpłatnej pomocy technicznej), a także z pełną trzyletnią gwarancją.

Bezpośr. inf. David Solomons
DRS Marketing

Systemy kontroli dostępu firmy Bosch na drogach ewakuacyjnych

Centrala kontroli dostępu z kontrolerami AMC2 firmy **Bosch** jako pierwsza na polskim rynku uzyskała potwierdzenie zgodności urządzenia z wymaganiami dotyczącymi sprzętu stosowanego w ochronie przeciwpożarowej; uzyskała także świadectwo dopuszczenia CNBOP.

Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 27 kwietnia 2010 r. – zmieniającym rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania – system kontroli dostępu może być stosowany na drogach ewakuacyjnych, jeżeli w razie pożaru lub awarii systemu zapewni automatyczne i ręczne, samoczynne otwarcie przejść kontrolowanych, bez możliwości ich blokowania, i pozostanie ich w stanie otwartym (Dz.U. nr 85 poz. 553). Spełnienie tych wymagań powinno być potwierdzone odpowiednim certyfikatem. System kontroli dostępu firmy Bosch bazujący na rodzinie urządzeń

AMC2 jest zgodny z tym wymogiem, co potwierdza świadectwo dopuszczenia CNBOP nr 0902/2011 i 0903/2011.

System ten jest skalowalny, dzięki czemu może kontrolować ruch osobowy w obiekcie dowolnej wielkości. Kontrolery AMC2 są podłączane do systemu przez interfejs RS-485 lub Ethernet, zależnie od specyfiki obiektu. Wykorzystanie karty pamięci o pojemności 2 GB umożliwia pracę w trybie offline. Kontrolery AMC2 są w pełni kompatybilne z oprogramowaniem zarządzającym Access Professional Edition oraz systemem integrującym Building Integration System.

Bezpośr. inf. Bosch Security Systems

Sieciowy punkt kamerowy **Compactcam HD** już w sprzedaży

Firma **Altram** informuje, że anonsowany wcześniej sieciowy punkt kamerowy, Compactcam HD, jest już w sprzedaży. Został on zbudowany na bazie modułu kamerowego Sony Full HD z przetwornikiem CMOS Exmor.

Unikatowe właściwości tego urządzenia to między innymi:

– pełna obsługa wszystkich funkcji przez sieć IP,
– odporność na wpływ warunków pogodowych (stopień szczelności IP66),
– możliwość montażu w pozycji prostej lub odwróconej, np. na suficie lub na maszcie,
– możliwość bezpośredniej obserwacji obiektów znajdujących się poniżej miejsca instalacji punktu kamerowego i ponad nim,
– maksymalna ogniskowa obiektywu równa 94 mm, zasięg w kat. 1 równy 38,7 m,
– automatyczna regulacja ostrości obrazu,
– wysoka dynamika toru wizyjnego,
– płaska przednia szyba obudowy modułu kamerowego, a dzięki niej brak aberracji optycznych wynikających ze stosowania czaszy kulistej,
– wycieraczka usuwająca zanieczyszczenia z przedniej szyby,
– oświetlacz diodowy pracujący w podczerwieni, obracający się wraz z modułem kamerowym.

Obecnie jest to jedyny dostępny na rynku sieciowy punkt kamerowy pozwalający w pełni sprostać skomplikowanym wymaganiom wynikającym z ustawy o ochronie imprez masowych.

Bezpośr inf. Altram

Kamery Sony Ipela w systemie monitoringu miejskiego m. st. Warszawy

W czerwcu br. najnowsze modele szybkoobrotowych kamer **Sony Ipela** zostały przetestowane w systemie monitoringu wizyjnego m. st. Warszawy. Kamery umieszczone w obudowach firmy Videotec zostały zainstalowane w rejonie ulicy Brackiej i podłączone do systemu dozorowego eksploatowanego przez Zakład Obsługi Systemu Monitoringu m. st. Warszawy.

Kamery Sony Ipela z serii **SNC-ER5xx** charakteryzują się wysoką dynamiką i znakomitymi parametrami optycznymi, uzyskiwanymi dzięki obiektywom o bardzo dużym zakresie zmian ogniskowej. Przeprowadzone próby potwierdziły ich wysoką przydatność do pracy operacyjnej w warunkach miejskich.

Bezpośr. inf. Altram

Nowe oprogramowanie **Video Client** firmy Bosch

Oprogramowanie *Bosch Video Client* (BVC) jest dostarczane bezpłatnie wraz ze wszystkimi kamerami sieciowymi firmy **Bosch**. Proste w instalacji i konfiguracji oraz intuicyjne w obsłudze znakomicie sprawdza się w mniej rozbudowanych instalacjach (do 64 kanałów sieciowych). Do takich obiektów należą niewielkie obiekty handlowe czy stacje benzynowe. Oprogramowanie można zainstalować w każdym komputerze PC z najnowszą wersją systemu Windows. BVC bezpłatnie obsługuje do 16 kamer sieciowych lub koderów; do obsługi większej liczby urządzeń (maksymalnie 64) należy wykupić licencję.

Oprogramowanie BVC umożliwia operatorowi podgląd obrazów z wielu kamer na pojedynczym monitorze PC oraz sprawną archiwizację nagrań. Oprogramowanie komunikuje się z innymi składnikami systemu za pośrednictwem sieci Ethernet, dzięki czemu w jednej lokalizacji możliwy jest podgląd obrazów z wielu kamer sieciowych.

Kreator w oprogramowaniu *Configuration Manager* przeprowadza użytkownika krok po kroku przez proces konfiguracji. Kamery można bardzo sprawnie przystosować do pracy zarówno w najbardziej typowych warunkach oświetleniowych, jak i do niestandardowych zastosowań specjalnych.

Oprogramowanie BVC pozwala wyświetlić jednocześnie nawet 20 bieżących obrazów pochodzących z kamer SD (w rozdzielczości standardowej) i HD (w rozdzielczości wysokiej). Każdy użytkownik ma także możliwość wskazania preferowanych grup kamer oraz łatwo dostępnych widoków. Jedno kliknięcie myszą spowoduje wyświetlenie obrazu z danego widoku. W trybie odtwarzania oprogramowanie BVC umożliwia jednoczesny podgląd obrazów aż z czterech kamer, wyszukiwanie zdarzeń alarmowych oraz związanych z detekcją ruchu, jak również eksportowanie potrzebnych nagrań.

Kamerami PTZ można sterować za pomocą myszy lub pulpitu. Zapis obrazu może być dokonywany lokalnie – na karcie pamięci kamery, lub centralnie – za pomocą oprogramowania Video Recording Manager firmy Bosch. Kreator konfiguracji oprogramowania BVC jest również pomocny przy instalacji systemu VRM.

W zapisanych obrazach oprogramowanie BVC umożliwia wyszukiwanie ruchu, zdarzeń alarmowych oraz wyszukiwanie na potrzeby dowodowe, włącznie z funkcją *forensic search*, która jest w standardzie. Funkcja powiększenia cyfrowego pozwala dokładnie przeanalizować krytyczne obszary w bieżących obrazach lub w obrazach zarejestrowanych wcześniej. Wygodnym rozwiązaniem jest również możliwość 10-minutowej rejestracji obrazu z dwóch źródeł. Obrazy można przesyłać w jednym z dwóch formatów: Windows ASF lub – w przypadku gdy wymagana jest autoryzacja nagrań – formacie natywnym Bosch. Eksport nagrań odbywa się w tle, nie ma zatem wpływu na pracę oprogramowania. Możliwy jest również lokalny eksport pojedynczych ujęć z materiału zarejestrowanego przez kamerę.

Bezpośr. inf. Bosch Security Systems

Kamery serii MIC firmy Bosch podglądają naturę

Od blisko dziesięciu lat kamery z serii **MIC**, stanowiące produkt firmy **Bosch Security Systems**, umożliwiają odwiedzającym Szkockie Centrum Ptactwa Morskiego wgląd w naturalny ekosystem tamtejszego wybrzeża, normalnie niedostępny dla człowieka. Pozwala na to wzmocniona konstrukcja kamer z funkcją obrotu/pochylenia/zoomu, która skutecznie znosi trudne warunki klimatyczne.

Organizacja Outersight (UK) z Plymouth specjalizuje się w projektowaniu systemów do obserwacji dzikiej przyrody w odległych i niebezpiecznych lokalizacjach. **Peter Barlow**, dyrektor generalny organizacji, od ponad dziesięciu lat współpracuje ze szkockim centrum, dla którego zaprojektował w tym czasie infrastrukturę do obserwacji przyrody.

Szkockie Centrum Ptactwa Morskiego to jedna z głównych atrakcji turystycznych tej części Wysp Brytyjskich. Wielokrotnie nagradzane za wykorzystanie kamer służących do obserwacji zwierząt, jest liderem w skali świata. Podgląda m.in. bieliki, głuptaki, maskonury czy foki szare.

Goście odwiedzający centrum oglądają materiały filmowe na dużych ekranach; za pomocą dżojstika mogą także sami sterować dziesięcioma kamerami, regulować ustawienie w osi poziomej i pionowej, przybliżać bądź oddalać obraz. Przypatrują się zatem temu, co ich interesuje. Kamery serii MIC dokonują automatycznie regulacji ostrości i przysłony, co doskonale optymalizuje obraz. Przez całą dobę dostępny jest również podgląd na stronie internetowej centrum.

Kamery serii MIC swoją wysoką renomę zawdzięczają wytrzymałej konstrukcji i trwałości, cechom niezbędnym w przypadku urządzeń pracujących w odległych lokalizacjach. – *Wiele interesujących miejsc jest niedostępnych w okresie lęgowym, inne znajdują się np. na klifach. Żeby do nich dotrzeć w razie awarii kamery, potrzebny byłby specjalistyczny sprzęt* – tłumaczy Peter Barlow. – *Ponieważ Szkockie Centrum Ptactwa Morskiego jest organizacją charytatywną, wydatki na działalność muszą pochodzić od darczyńców bądź ze sprzedaży biletów, zatem redukcja kosztów utrzymania jest dla nas sprawą kluczową.*

Sprzęt narażony jest na podmuchy porywistego wiatru (wiejącego z prędkością ponad 160 km/h), uderzenia fal morskich i piasku oraz korozję będącą wynikiem osadzania się pyłu wodnego. Według Petera Barlowa *z podobnymi niedogodnościami kamery serii MIC radzą sobie niezawodnie.*

W całym tym przedsięwzięciu jest ogromnie istotne, by obecność kamer nie zakłócała ptakom spokoju. – *Bezszczotkowa konstrukcja silników sprawia, że kamera porusza się prawie bezszelestnie, ptaki budują w jej pobliżu gniazda, a zwiedzający mają jedyną w swoim rodzaju możliwość podglądania zwierząt z bliska.*

Pierwszą kamerę serii MIC zainstalowano na wyspie May w 2001 roku. Sygnały wizyjne docierały wtedy do centrum przez kabel światłowodowy i analogowe łącze mikrofalowe. Rok po udanej próbie unowocześniono kamery zainstalowane na wyspie Bass Rock, a w 2003 roku kolejną kamerę umieszczono na tarasie widokowym Szkockiego Centrum Ptactwa Morskiego. Od tego czasu w różnych lokalizacjach zainstalowano jeszcze sześć kamer serii MIC.

Zwarta konstrukcja kamer serii MIC ogranicza napór wiatru, co z kolei zmniejsza wibracje przy dużym zbliżeniu. – *Dzięki opływowemu kształtowi kamery nie przeszkadzają ptakom, a przy odpowiednim kamuflażu farbą właściwego koloru wtapiają się w tę urokliwą scenerię, będąc z daleka ledwie zauważalne* – mówi Peter Barlow. – *Zależy nam, by ptaki nie odczuwały obecności kamer.*

Kamery serii MIC pozwalają na sterowanie obrotem w zakresie pełnych 360° oraz pochyleniem w zakresie 320°, co pozwala odwiedzającym szkockie centrum podziwiać widoki w całej okazałości. Wzmocnione, płaskie okno oraz wbudowana wycieraczka zapewniają niemal idealny obraz bez względu na warunki pogodowe, a jeden z najlepszych w branży stopień ochrony IP68 jest gwarantem tego, że kamery serii MIC są w stanie oprzeć się największym wyzwaniom pogodowym szkockiego wybrzeża.

Bezpośr. inf. Bosch Security Systems

Samsung wprowadza na rynek kamerę **SCV2081R**

Nowość **Samsunga** to wysokiej jakości kompaktowa, wandaloodporna kamera kopułkowa **SCV-2081R** z wbudowanymi diodami LED pracującymi w podczerwieni, które pozwalają na wytwarzanie obrazu w rozdzielczości 600 linii TV w warunkach nocnych. Dzięki temu użytkownik nie musi ponosić kosztów związanych z instalacją dodatkowego oświetlenia.

Kamera SCV-2081R nadaje się do zastosowania wewnątrz i na zewnątrz takich obiektów jak biura, lokale handlowe, szkoły i szpitale. Jest zgodna z klasą szczelności IP66, zatem doskonale sprawdzi się w miejscach narażonych na oddziaływanie surowych warunków pogodowych oraz na próby sabotażu lub uszkodzenia fizyczne.

Wbudowane w kamerę diody LED pracujące w podczerwieni umożliwiają wytwarzanie wyraźnego obrazu obiektów nawet w całkowitej ciemności. Intensywność ich promieniowania jest regulowana automatycznie, odpowiednio do odległości, w jakiej znajduje się obserwowany obiekt. Pozwala to wyeliminować prześwietlenie pierwszego planu obrazu oraz gwarantuje doskonałą równowagę między pierwszym planem i tłem obrazu.

Kamera SCV-2081R ma wbudowany obiektyw zmiennoogniskowy 3.6X (2.8 ~ 10 mm) oraz wykorzystuje wysoko oceniany chipset Samsung Techwin W-V DSP. Dzięki temu dysponuje wieloma zaawansowanymi funkcjami, w tym ośmioma strefami detekcji ruchu, dwunastoma strefami prywatności, technologią Samsung Super Noise Reduction trzeciej generacji (SSNRIII – cyfrowa redukcja szumu) oraz możliwością sterowania z użyciem kabla koncentrycznego. Pozwala to na wyświetlanie menu ekranowego w piętnastu językach, dostępnego z poziomu centrum monitoringu poprzez kompatybilne rejestratory DVR – takie jak wybrane rejestratory serii SRD firmy Samsung – bez konieczności instalowania dodatkowego okablowania.

Dodatkowe funkcje obejmują technologię Highlight Compensation (HLC), służącą do rozpoznawania i neutralizacji prześwietlonych obszarów obrazu, takich jak światła samochodu. Umożliwia to operatorowi podgląd szczegółów, które normalnie nie byłyby widoczne z powodu zbyt dużego kontrastu. Kamera SCV-2081R korzysta także z funkcji Samsung Super Dynamic Range (SSDR), czyli udoskonalonej technologii BLC, która automatycznie uwypukla szczegóły zaciemnionego obszaru kadru i uwidacznia obiekty ukryte w cieniu.

Bezpośr. inf. David Solomons
DRS Marketing

Samsung wprowadza na rynek dwa cyfrowe rejestratory wizji H.264 serii SRD

Seria **SRD** (niezwykle udana) to grupa sieciowych rejestratorów wizji wykorzystująca wysoce wydajną metodę kompresji H.264. Kompresja ta gwarantuje doskonałą jakość obrazu przy równoczesnym zminimalizowaniu wykorzystania pasma sieciowego oraz obniżeniu wymagań dotyczących przechowywania plików z zapisem wizyjnym. Do serii tej właśnie dołączają konkurencyjne cenowo cyfrowe rejestratory wizji **SRD-852D** (ośmiokanałowy) i **SRD-1652D** (szesnastokanałowy).

– *Modele te zostały wprowadzone, aby stworzyć rozwiązania w zakresie rejestracji dla zastosowań, w których istotna jest jakość zapewniana przez markę Samsung, ale które nie wymagają bardziej zaawansowanych funkcji, w jakie wyposażono pozostałe urządzenia z tej serii* – powiedział **Peter Ainsworth**, Senior Product Manager w **Samsung Techwin Europe**. – *W rezultacie możemy teraz zaoferować możliwość wyboru użytkownikom liczącym się z kosztami i jednocześnie oczekującym najlepszego, profesjonalnego działania ich systemu bezpieczeństwa.*

Ośmiokanałowy SRD-852D oraz szesnastokanałowy SRD-1652D są stosowane m.in. do monitorowania sklepów, lokali usługowych oraz osiedli mieszkaniowych. Mogą jednocześnie rejestrować obrazy w czasie rzeczywistym we wszystkich kanałach w jakości CIF albo w czasie rzeczywistym w wybranych kanałach w rozdzielczości 2-CIF lub 4-CIF, z możliwością rejestracji dźwięku z czterech kanałów.

Obydwa modele, oferujące sterowanie telemetryczne RS485, umożliwiają użytkownikowi zdalny podgląd obrazu w czasie rzeczywistym lub podgląd nagranego wcześniej obrazu przez Internet (w przeglądarce sieciowej) oraz za pomocą iPhone'ów lub smartphone'ów z systemem operacyjnym Android. Obraz może być zapisywany maksymalnie na czterech dyskach twardych, a do tworzenia kopii zapasowych można wykorzystać wbudowaną nagrywarkę DVD lub dwa gniazda USB.

Dodatkowe ułatwienia dla instalatorom i operatorom to m.in. zdejmowany tylny panel (umożliwiający wymianę dysków twardych bez konieczności odłączania kabli), a także wyjścia VGA i BNC oraz wielojęzyczny interfejs użytkownika.

SRD-852D i SRD-1652D są dostarczane z bezlicencyjnym oprogramowaniem Net-i-Viewer firmy Samsung. Mają taką samą strukturę intuicyjnego, graficznego interfejsu użytkownika (GUI) jak wszelkie pozostałe rejestratory cyfrowe z serii SRD, co znacznie ułatwia pracę operatorom na przykład podczas ustawiania na poszczególnych kanałach rejestracji w różnej prędkości zapisu i z różną rozdzielczością.

Cyfrowe rejestratory wizji SRD-852D oraz SRD-1652D są dostępne u wszystkich autoryzowanych dystrybutorów produktów Samsung i oferowane z pełną obsługą serwisową Samsung Techwin Europe (w tym również w zakresie projektowania systemów i doradztwa technicznego), a także z pełną trzyletnią gwarancją.

Bezpośr. inf. David Solomons
DRS Marketing

Certyfikat EN 54 dla dźwiękowych systemów ostrzegawczych firmy Bosch

Dźwiękowe systemy ostrzegawcze firmy **Bosch**, tj. bardziej ekonomiczny system Plena oraz najwyższej klasy, całkowicie cyfrowy system Praesideo, otrzymały certyfikat EN 54 przyznawany przez uprawnione instytucje. Oprócz sprzętu podstawowego certyfikat obejmuje urządzenia peryferyjne, w tym m.in. głośniki.

Od wielu lat firma Bosch Security Systems pozostaje pionierem i promotorem najwyższych standardów urządzeń w branży systemów zabezpieczeń; jako jedna z pierwszych na świecie otrzymała certyfikat zgodności z normą EN 54 dla dźwiękowych systemów ostrzegawczych. Pierwotnie certyfikat EN 54 odnosił się jedynie do systemów sygnalizacji pożarowej. Jednak w odpowiedzi na tendencje rynkowe, które zmierzają ku integracji systemów sygnalizacji pożarowej z dźwiękowymi systemami ostrzegawczymi, od niedawna obejmuje również ten drugi rodzaj systemów. Trzy główne obszary zastosowań, do których odnosi się norma EN 54, to centralne sterowanie dźwiękowym systemem ostrzegawczym i urządzeniami sygnalizacji (norma EN 54-16), głośniki (EN 54-24) oraz źródła zasilania (EN 54-4).

Z początkiem 2009 roku firma Bosch wprowadziła na rynek dźwiękowy system ostrzegawczy zgodny z normą EN 54-16. Od tego czasu Bosch współpracował z wieloma akredytowanymi organizacjami certyfikującymi w celu uzyskania certyfikatów dla wszystkich produkowanych przez siebie dźwiękowych systemów ostrzegawczych, zgodnie z wymogiem obowiązującym od kwietnia 2011 roku.

Dzięki podjętemu wysiłkowi firma może obecnie poszczycić się posiadaniem certyfikatu EN 54 dla wszystkich składników swoich dźwiękowych systemów ostrzegawczych, przyznanego przez współpracujące laboratoria akredytowane. Centralne urządzenia Praesideo 3.5 oraz Plena VAS 2.16 otrzymały certyfikat EN 54-16. Oprócz tego firma Bosch dostarcza ładowarki opatrzone certyfikatem EN 54-4; posiada też certyfikat producencki różnego rodzaju głośników przeznaczonych do współpracy z dźwiękowym systemem ostrzegawczym. W odróżnieniu od innych producentów, którzy oferują głośniki do najwyżej kilku zastosowań, firma Bosch dostarcza produkty opatrzone certyfikatem EN 54-24 do całej gamy zastosowań audio, w tym dźwiękowych systemów ostrzegawczych, nagłośnienia mowy i tła muzycznego, muzyki pierwszoplanowej oraz profesjonalnej techniki audio. Oferta obejmuje głośniki do zastosowań wewnętrznych i zewnętrznych, a także głośniki montowane na ścianach lub sufitach.

Przyznaniefirmie Bosch certyfikatu EN 54 dla dźwiękowych systemów ostrzegawczych i ich składników umożliwia rozszerzenie, po uzyskaniu certyfikatu dla central sygnalizacji pożaru serii 1200 i 5000, jej oferty certyfikowanych systemów sygnalizacji pożarowej i dźwiękowych systemów ostrzegawczych. Produkty firmy spełniają wymogi wszystkich zastosowań służących ochronie personelu i szeroko rozumianej strefy publicznej.

Bezpośr. inf. Bosch Security Systems

Ogólnopolskie spotkanie użytkowników programu **KRONOS** podsumowanie

W dniach 16 – 17 czerwca 2011 r. w Ustroniu, we wspaniale usytuowanym na beskidzkim stoku hotelu Belweder, odbyło się ogólnopolskie spotkanie użytkowników programu KRONOS, wspierającego pracę stacji monitorowania. Inicjatorami były firmy **Kronos Polska** i **Next!** z Bielska Białej.

Spotkanie było doskonałą okazją do wymiany uwag pomiędzy twórcami oraz użytkownikami programu, a także do wymiany doświadczeń samych użytkowników. Uczestniczyło w nim ponad 60 osób reprezentujących 40 firm z branży monitoringu i ochrony.

W części merytorycznej uczestnikom spotkania zostały przedstawione plany rozwoju oprogramowania KRONOS na lata 2011 i 2012. Wszyscy mieli możliwość zapoznania się z najnowszymi rozwiązaniami technicznymi przewodowych systemów sygnalizacji włamania i napadu, prezentowanymi przez Krzysztofa Parzyszka z Alarmtech Polska z Gdańska oraz uznanych w Polsce producentów systemów bezprzewodowych, m.in. firmę Jablotron z Czech, reprezentowaną przez Alana Fabika (dyrektora handlowego na Europę) oraz Piotra Panka (przedstawiciela w Polsce). W spotkaniu wziął udział także Eduard Bardinet z Francji, reprezentujący firmę Intervox – dystrybutora urządzeń do monitoringu medycznego.

W części nieoficjalnej, w trakcie „wieczoru szkockiego" można było zapoznać się z historią regionów Szkocji: Lowland, Speyside i Islay, oraz ich produktem eksportowym– whisky single malt. Wieczór połączony z degustacją wyśmienitych trunków poprowadził Jarosław Buss, ambasador marki Ballantines.

Na zakończenie organizatorzy wyrazili nadzieję, że takie spotkania staną się tradycją i będą miejscem wymiany doświadczeń oraz pogłębiania nawiązanych znajomości.

Bezpośr. inf. Andrzej Głogowski
KRONOS s.j. S.Piela.B.Dryja

Nowa generacja rozwiązań z zakresu zabezpieczeń i nadzoru wizyjnego firmy Samsung na targach IFSEC

Od 16 do 19 maja w kompleksie NEC w Birmingham trwała międzynarodowa wystawa rozwiązań w dziedzinie zabezpieczeń – **IFSEC 2011**. Największe w historii stoisko firmy Samsung było miejscem prezentacji najszybciej rozwijającej się w Europie marki z branży bezpieczeństwa – najnowszych produktów i technologii nadzoru wizyjnego. Jak można się było spodziewać, szczególnym zainteresowaniem ogromnej liczby ekspertów i użytkowników końcowych cieszyły się kamery Samsung z funkcją inteligentnej analizy obrazu (IVA).

– *Wszystkie kamery wyposażone w nasze chipsety WiseNet1 i SV-5 posiadają funkcję IVA, która jest potężnym narzędziem gwarantującym użytkownikom maksimum korzyści podczas obserwacji takich obiektów jak parkingi, zakłady przemysłowe, stacje paliw, szkoły, szpitale, centra handlowe, lotniska i porty* – powiedział **James Smith**, European Marketing Manager firmy Samsung Techwin Europe.

Bezlicencyjna inteligentna analiza obrazu (IVA) marki Samsung zawiera wirtualną barierę optyczną oraz funkcję detekcji wejścia w chroniony obszar lub wyjścia z tego obszaru, jak również funkcję detekcji pojawiania się/zniknięcia obiektu. IVA posiada także funkcję monitorowania zmian działania kamery, włączającą alarm, gdy na przykład obiektyw zostanie umyślnie zabrudzony farbą lub gdy pole widzenia kamery zostanie zmienione bez autoryzacji.

– *Jedną z kamer przyciągających znaczną uwagę był model SNP-5200 – 1,3-megapikselowa kamera sieciowa wysokiej rozdzielczości z głowicą PTZ, łącząca zalety kamery dzienno-nocnej z filtrem IR oraz 20-krotnym zoomem optycznym* – powiedział James Smith. *– Pomimo konkurencyjnej ceny kamera ta posiada wszystkie standardowe funkcje oraz jest „przyjazna dla pasma sieciowego", dzięki czemu nadaje się doskonale dla szerokiego zakresu zastosowań – wszędzie tam, gdzie głowica PTZ o wysokiej rozdzielczości jest wymagana jako część systemu nadzoru wizyjnego opartego na technologii IP.*

SNP-5200 wykorzystuje chipset WiseNet1 DSP marki Samsung, co zapewnia użytkownikom maksimum korzyści z najnowszej technologii kamer megapikselowych. Najważniejsze z nich to bezlicencyjna inteligentna analiza obrazu oraz dwustrumieniowa kompresja H.264/MJPEG, umożliwiająca równoczesną transmisję obrazów do wielu odbiorców przy zróżnicowanej prędkości transmisji oraz w różnej rozdzielczości.

Do alarmowych wiadomości e-mail mogą być dołączane zdjęcia w formacie JPEG stanowiące dokumentację zachodzących zdarzeń. Istnieje również możliwość przechowywania pre- i postalarmowych obrazów na karcie pamięci SD (gniazdo czytnika kart jest wbudowane w kamerę). Co więcej, złącza Ethernet i BNC oraz dodatkowy port telemetrii pozwalają na łatwe tworzenie hybrydowych systemów monitoringu. Złącze BNC zapewnia także łatwą konfigurację za pomocą standardowych monitorów instalatorskich.

Procesory DSP firmy Samsung

Istnieje wiele powodów, dla których używa się kamer dozorowych, oraz równie wiele środowisk, gdzie kamery te mogą być fizycznie instalowane. Mając na uwadze fakt, że wyposażenie pojedynczego chipsetu DSP we wszystkie możliwe funkcje jest nieekonomiczne i niepraktyczne, projektanci firmy Samsung opracowali serię chipsetów, z których każdy wyposażono w zestaw funkcji zapewniający optymalne rozwiązanie dla specyficznych typów zastosowań i projektów.

SV-5 DSP

Jedną z głównych zalet chipsetu SV-5 jest możliwość generowania obrazu o rozdzielczości dochodzącej nawet do 650 linii TV w kolorze, co umożliwiają nowe, wydajne przetworniki Super HAD (960H) CCD. Technologia Wide Dynamic Range (WDR), wbudowana w chipset SV-5, kompensuje problemy wynikające z oświetlenia tylnego 160 razy efektywniej niż standardowa funkcja BLC. Jest to możliwe dzięki scaleniu obrazów uzyskanych przy zastosowaniu szybkiej migawki w obszarach jasnych z obrazami uzyskanymi przy zastosowaniu wolnej migawki w obszarach zaciemnionych. Dokonuje ona precyzyjnej analizy obrazu w celu zebrania szczegółowych informacji z ciemnych obszarów bez efektu nasycenia obszarów jasnych.

Kamery z chipsetem SV-5 korzystają także z technologii *Samsung Super Noise Reduction* (SSNRIII), eliminującej szumy obrazu spowodowane niedostatecznym oświetleniem, bez występowania „efektu ducha" bądź rozmycia. SSNRIII realizuje funkcję doboru wzorca („Pattern Matching"), pozwalającą na równoczesną redukcję szumów i zachowanie ostrości krawędzi obiektów zarówno w obrazach statycznych, jak i ruchomych. Po usunięciu szumu zostaje uruchomiony system podziału matrycy na bardzo małe elementy (3×3 piksele) stanowiące wzorzec dopasowujący, co zapewnia identyczność obrazu generowanego przez kamerę z oryginałem, ale już bez widocznego szumu.

Dodatkową korzyścią wynikającą z zastosowania tej niezwykłej technologii jest możliwość zaoszczędzenia do 70% (sic!) przestrzeni dyskowej w cyfrowym rejestratorze obrazu, przy zmaksymalizowaniu wykorzystania pasma podczas przeglądania obrazu w sieci.

Inne ważne funkcje kamer wyposażonych w chipset SV-5 to:

– *Super Dynamic Range* (SDR) – automatycznie rozjaśnia zaciemnione obszary kadru, pozostawiając obszary jaśniejsze na tym samym poziomie szarości. Dzięki temu zaciemnione obszary stają się lepiej widoczne, co pozwala operatorowi zobaczyć obiekty ukryte w cieniu.
– Technologia kompensacji prześwietlenia (HLC) – rozpoznaje na obrazie obszary całkowicie wypełnione bielą (tj. obszary znacznie prześwietlone) i neutralizuje je poprzez przetworzenie ich na odpowiednie odcienie szarości. Umożliwia to kamerze efektywny podgląd tych obszarów, co z kolei pozwala operatorowi dojrzeć ukryte wcześniej detale (np. tablicę rejestracyjną pojazdu między jasnymi światłami przednich reflektorów).
– Technologia cyfrowej stabilizacji obrazu (DIS) – może zniwelować skutki drgań kamery wskutek silnego wiatru lub wibracji konstrukcji, na której zainstalowano kamerę.

Kamery wyposażone w chipset W-5 posiadają również funkcję stref prywatności oraz interfejs użytkownika w czternastu językach.

Bezpośr. inf. David Solomons
DRS Marketing

Ogólnopolskie Szkolenie Projektowe **Schrack Seconet 2011** podsumowanie

15 czerwca 2011 r. w Szkole Głównej Służby Pożarniczej w Warszawie odbyło się kolejne **Ogólnopolskie Szkolenie Projektowe** firmy **Schrack Seconet Polska** – polskiego oddziału jednego z największych i najbardziej znanych producentów systemów ochrony przeciwpożarowej na świecie.

W szkoleniu wzięło udział około 260 osób, głównie projektantów SSP oraz specjalistów z branży zabezpieczeń. Oprócz przedstawicieli firmy Schrack Seconet Polska w gronie autorów referatów znaleźli się zaproszeni goście: Jerzy Ciszewski i Janusz Sawicki z Instytutu Techniki Budowlanej. Organizatorzy spotkania umożliwili również firmie TOA Electronics Europe prezentację dźwiękowych systemów ostrzegawczych.

Pierwszą część spotkania rozpoczął Grzegorz Ćwiek – prezes zarządu Schrack Seconet Polska, który powitał uczestników i wprowadził w tematykę szkolenia, omawiając kilka najciekawszych obiektów referencyjnych firmy. Następnie Krzysztof Kunecki – dyrektor techniczny Schrack Seconet Polska, zaprezentował najnowsze funkcje i możliwości systemu sygnalizacji pożarowej i sterowania gaszeniem Integral IP, z naciskiem na nowe elementy peryferyjne techniki pętlowej X-LINE oraz analizę możliwych konfiguracji sieciowych przy zastosowaniu sieci Integral LAN i SecoNET. Omówił również zastosowanie czujek i rozwiązań specjalnych znajdujących się obecnie w ofercie Schrack Seconet, z uwzględnieniem nowej liniowej czujki dymu ILIA oraz nowych możliwości systemu wczesnej detekcji AirSCREEN ASD 535.

Jako pierwszy z gości wygłosił swój referat Janusz Sawicki. Tematem jego wystąpienia były obwody zasilania w systemach sygnalizacji pożarowej i automatyki pożarowej. W zagadnienia dźwiękowych systemów ostrzegawczych wprowadził słuchaczy Piotr Szaliński – dyrektor oddziału firmy TOA Electronics Europe w Polsce. Referat dotyczył przede wszystkim zmian w wymogach formalnych po 1 kwietnia 2011 r.

Już po pierwszej części szkolenia wywiązały się dyskusje dotyczące aktualnych regulacji prawnych i kwestii związanych z rzetelnym przygotowaniem projektu zaawansowanych systemów zabezpieczeń budynku.

W drugiej części spotkania swoje referaty wygłosił Jerzy Ciszewski. Dotyczyły one m.in. szczegółowej analizy rozwoju pożaru z uwzględnieniem zjawisk fizycznych oraz analizy systemu

wykrywania pożaru pod kątem doboru elementów, wraz z praktycznymi wskazówkami na temat właściwego doboru czujek. Ekspert poruszył również zagadnienia związane z projektowaniem systemów sygnalizacji pożarowej w oparciu o najnowsze wytyczne SITP, analizując je pod kątem najważniejszych różnic w stosunku do innych wytycznych dotyczących projektowania: PKN-CEN/TS 54-14 i VdS/CNBOP. W tej części spotkania zabrał głos również Paweł Tomaszewski – kierownik ds. produktu Schrack Seconet Polska, omawiając krótko najnowsze rozwiązania w dziedzinie komunikacji w obiektach służby zdrowia: system przyzywowy i komunikacji Visocall IP. Słuchacze zostali zaproszeni na oddzielne szkolenie z tego zakresu.

Uczestnicy spotkania mieli okazję zapoznać się nie tylko z aktualnymi zasadami dotyczącymi projektowania, przedstawionymi przez gości Schrack Seconet Polska, ale również z nowościami w ofercie firmy. Podczas spotkania zostało zaprezentowane jej najnowsze narzędzie projektowe – system INTEGRAL IP. Na przygotowanych schematach przedstawiono szczegółową topologię systemu i możliwości konfiguracyjne, z uwzględnieniem najważniejszych urządzeń dostępnych w ofercie Schrack Seconet. Narzędzie projektowe, podzielone tematycznie na dwie części, przedstawia m.in.: strukturę sieci central INTEGRAL IP; możliwości konfiguracyjne sieci; sieci kratowe; sieci SecoNET; możliwości połączeń LAN z systemem wizualizacji zdarzeń pożarowych SecoLOG i systemami automatyki budynkowej BMS/SMS; a także dostępne urządzenia peryferyjne (w tym elementy specjalne) w możliwych wariantach podłączeń.

W trakcie wystąpień słuchacze mieli również możliwość uzyskania odpowiedzi na pytania związane z najnowszymi wytycznymi i regulacjami prawnymi dotyczącymi projektowania. Szkolenie zakończył prezes firmy, dziękując uczestnikom za wzięcie w nim udziału i zapraszając do dalszej współpracy.

Ogólnopolskie szkolenia Schrack Seconet, które niezmiennie odbywają się o tej porze roku już od ponad piętnastu lat, są największymi tego typu szkoleniami w branży.

Bezpośr. inf. Schrack Seconet Polska

6 czerwca zginął w wypadku lotniczym kol. **Janusz Zieniewicz**, współwłaściciel firmy IDE Sp. z o.o.

Samolot Cessna 182T Skylane (SP-CFM), którym leciał, z niewyjaśnionych przyczyn spadł w czasie mgły na lotnisko Asturias (LEAS) w Hiszpanii.

Cześć Jego pamięci!

Zarząd i pracownicy
AAT Holding sp. z o.o.

Aspekty prawne a prawa dziecka w świetle zastosowania systemów monitoringu wizyjnego

Tomasz Malinowski

„Czy czuję się bezpiecznie?” Problematyka aspektów prawnych w dziedzinie używania monitoringu jest bardzo szeroka. Często pojawia się szereg wątpliwości związanych z projektem i montażem systemu. Równie często dostaję pytania: „Czy dyrektor może zainstalować system monitorowania bez zgody rodziców? Czy może sam wyznaczyć miejsca monitorowane? Dlaczego naruszana jest prywatność osób?”. Nie znając do końca specyfiki i okoliczności podjęcia decyzji o inwestycji, na takie pytania odpowiadam pytaniem: „A jak chcesz podnieść poziom bezpieczeństwa w szkole Twojego dziecka? Prześlij mi, proszę, parę pomysłów. Czy Twoje dziecko jest dla Ciebie najwyższą wartością? Zrób bilans zysków. Ciebie nie ma przecież w szkole na co dzień”. Najczęstszą odpowiedzią jest słowo: „Dziękuję”.

Kamery czy atrapy?

Na każdym etapie budowy obiektu (zamysł, koncepcja, projekt, realizacja projektu) należy kierować się dobrem człowieka i jego prawami – między innymi prawem do prywatności. Z całą pewnością każda osoba poruszająca się po terenie monitorowanym musi mieć świadomość, że jej zachowania są obserwowane i rejestrowane. Musi mieć również świadomość i pewność, że jej zachowanie nie jest ani nie będzie przedmiotem szyderstwa. Wchodząc w obszar monitorowany, człowiek podświadomie czuje się bezpieczniejszy. To poczucie bezpieczeństwa jest wzmacniane widokiem kamery, tabliczkami z napisami informującymi o monitorowaniu terenu. Tym samym poziom czujności (co do ewentualnego ataku przestępczego) osoby poruszającej się po tym terenie zostaje obniżony.

Naturalny jest również odruch ucieczki człowieka (podczas zagrożenia) w miejsce bezpieczne. Znając rozmieszczenie kamer w obiekcie szkolnym, uczniowie w momencie zagrożenia będą podążać w ich kierunku. Jeżeli jednak okaże się, że w miejscu kamer są atrapy, to uczeń przekonany, że będzie mu udzielona pomoc, trafia w pułapkę. Zainstalowanie atrap może być skrzętnie wykorzystane przez sprawców, którzy wiedząc, że ofiara liczy na szybką pomoc, stawiają śmiałe żądania i kontrolują sytuację. Kolejnym negatywnym aspektem stosowania atrap jest brak możliwości ustalenia przez policję (w toku prowadzonych postępowań) drogi pokonywanej przez sprawców do miejsca zdarzenia oraz drogi ucieczki.

Gdy weźmie się pod uwagę konwencje praw człowieka, konieczne wydaje się rzetelne określenie miejsc monitorowanych. Wynika z tego obowiązek stosowania kamer, a nie atrap, czyli prymitywnego środka zastępczego. Stosowanie atrap w systemach dozorowych CCTV jest naruszeniem praw człowieka, gdyż podwyższone poczucie bezpieczeństwa w obszarze rzekomo chronionym przez podmiot realizujący monitoring nie wynika z faktycznego nadzorowania tego obszaru, tylko ze stworzenia pozorów bezpieczeństwa. W razie wystąpienia zdarzenia instytucja (państwo) powinna ponosić pełną odpowiedzialność za szkody dotyczące zdrowia, życia lub mienia.

Jeśli jesteś potencjalnym wykonawcą systemu dozorowego i inwestor prosi Cię o montaż atrap, nie przyjmuj takiego zlecenia! Gdy projektujesz lub montujesz system z atrapami, ewentualnie zlecasz jego wykonanie – stań wewnątrz obiektu i spójrz w stronę atrapy. Odpowiedz sobie na pytanie: „Jak się czuję? Czy teraz jest bezpieczniej?”.

Należy zdać sobie sprawę, że działania na rzecz bezpieczeństwa ludzi poruszających się po terenach monitorowanych w szkole to nie ochrona sklepu, budynku czy samochodu przed złodziejem – bezpieczeństwo ucznia to sprawa znacznie ważniejsza, a na terenach szkolnych o naruszenie praw człowieka jest bardzo łatwo.

Należy dodać, że opisywane problemy dotyczą również szkół prywatnych – obowiązują je takie same zasady jak szkoły publiczne.

Skuteczny monitoring

Zasady stosowania monitoringu są następujące:

- Monitoring musi zostać wykonany na podstawie szczegółowych, profesjonalnie przygotowanych założeń i bez naruszenia praw człowieka.
- Projektant systemu musi posiadać doświadczenie, zarówno praktyczne, jak i teoretyczne (to warunek, aby zbudowany system spełniał pokładane w nim nadzieje).
- Monitoring musi być wykonany zgodnie z wymaganiami obowiązujących przepisów prawa i konwencji.
- Monitoring musi być wykonany w sposób profesjonalny, zgodnie z wymaganiami obowiązujących norm.
- Inwestorzy, projektanci i wykonawcy muszą realizować system monitoringu, wykorzystując sprzęt o wysokiej jakości, niezawodności i trwałości, a odrzucać sprzęt awaryjny o niskiej jakości.
- Sprzęt musi posiadać stosowne atesty i certyfikaty.
- Monitoring musi być obsługiwany przez osoby profesjonalnie przeszkolone – również w zakresie praw człowieka.
- Osoby znajdujące się w obszarze monitorowanym muszą mieć świadomość przebywania w takim obszarze.
- Osoby znajdujące się w obszarze monitorowanym muszą mieć poczucie bezpieczeństwa.
- Działanie monitoringu musi podlegać analizom, mającym na celu określenie, czy zamierzony cel został osiągnięty.

Prawo dziecka do ochrony

Podstawowym aktem prawnym gwarantującym dzieciom respektowanie ich praw jest Konwencja o Prawach Dziecka (przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych 20 listopada 1989 r. – Dz. U. z dnia 23 grudnia 1991 r.).

W rozumieniu tej konwencji (art. 1) „dziecko” oznacza każdą istotę ludzką w wieku poniżej osiemnastu lat, chyba że zgodnie z prawem odnoszącym się do dziecka uzyska ono

wcześniej pełnoletniość. Dziecko jest najwyższą wartością, a poprzez działania dorosłych następuje jego kształtowanie. Działania te muszą być oparte na kompetencjach i dbałości o bezpieczeństwo dziecka.

Przytoczmy więc niektóre podstawowe postanowienia odnoszące się do działań ukierunkowanych na zapewnienie bezpieczeństwa oraz określmy instytucje, których zadaniem jest zapewnienie bezpieczeństwa i poszanowania godności:

Art. 2.

1. Państwa-Strony w granicach swojej jurysdykcji będą respektowały i gwarantowały prawa zawarte w niniejszej konwencji wobec każdego dziecka, bez jakiejkolwiek dyskryminacji, niezależnie od rasy, koloru skóry, płci, języka, religii, poglądów politycznych, statusu majątkowego, niepełnosprawności, cenzusu urodzenia lub jakiegokolwiek innego tego dziecka albo jego rodziców bądź opiekuna prawnego.
2. Państwa-Strony będą podejmowały właściwe kroki dla zapewnienia ochrony dziecka przed wszelkimi formami dyskryminacji lub karania ze względu na status prawny, działalność, wyrażane poglądy lub przekonania religijne rodziców dziecka, opiekunów prawnych lub członków rodziny.

Art. 3.

1. We wszystkich działaniach dotyczących dzieci, podejmowanych przez publiczne lub prywatne instytucje opieki społecznej, sądy, władze administracyjne lub ciała ustawodawcze, sprawą nadrzędną będzie najlepsze zabezpieczenie interesów dziecka.
2. Państwa-Strony działają na rzecz zapewnienia dziecku ochrony i opieki w takim stopniu, w jakim jest to niezbędne dla jego dobra, biorąc pod uwagę prawa i obowiązki jego rodziców, opiekunów prawnych lub innych osób prawnie za nie odpowiedzialnych, i w tym celu będą podejmowały wszelkie właściwe kroki ustawodawcze oraz administracyjne.
3. Państwa-Strony czuwają, aby instytucje, służby oraz inne jednostki odpowiedzialne za opiekę lub ochronę dzieci dostosowały się do norm ustanowionych przez kompetentne władze, w szczególności w dziedzinach bezpieczeństwa, zdrowia, jak również dotyczących właściwego doboru kadr tych instytucji oraz odpowiedniego nadzoru.

Art. 19.

1. Państwa-Strony będą podejmowały wszelkie właściwe kroki w dziedzinie ustawodawczej, administracyjnej, społecznej oraz wychowawczej dla ochrony dziecka przed wszelkimi formami przemocy fizycznej bądź psychicznej, krzywdy lub zaniedbania bądź złego traktowania lub wyzysku, w tym wykorzystywania w celach seksualnych, dzieci pozostających pod opieką rodzica(ów), opiekuna(ów) prawnego(ych) lub innej osoby sprawującej opiekę nad dzieckiem.
2. Tego rodzaju środki ochronne powinny obejmować, tam gdzie jest to właściwe, skuteczne przedsięwzięcia w celu stworzenia programów socjalnych dla realizacji pomocy dziecku oraz osobom sprawującym opiekę nad dzieckiem, jak również innych form działań prewencyjnych dla ustalania, informowania, wszczynania i prowadzenia śledztwa, postępowania, notowania wymienionych wyżej przypadków niewłaściwego traktowania dzieci oraz tam, gdzie jest to właściwe – ingerencję sądu.

Art. 33.

Państwa-Strony będą podejmowały wszelkie odpowiednie kroki, w tym środki ustawodawcze, administracyjne, socjalne oraz środki w dziedzinie oświaty, w celu zapewnienia ochrony dzieci przed nielegalnym używaniem środków narkotycznych i substancji psychotropowych, zgodnie z ich zdefiniowaniem w odpowiednich umowach międzynarodowych, oraz w celu zapobiegania wykorzystywaniu dzieci do nielegalnej produkcji tego typu substancji i handlu nimi.

Konwencja Praw Dziecka dobitnie stawia dziecko na piedestale, podkreślając jego niewiarygodnie ważną pozycję w społeczeństwie. Wręcz narzuca konieczność zapewnienia mu bezpieczeństwa w szerokim tego słowa znaczeniu. Konieczne jest podejmowanie różnych przedsięwzięć i działań, a w naszym przypadku – stosowanie środków ochrony fizycznej i technicznej osób i mienia.

Zapewnienie bezpieczeństwa w szkołach

W związku z koniecznością zapewnienia przestrzegania praw dziecka dorośli mają wiele obowiązków. Jednym z nich jest zorganizowanie ochrony oraz zapewnienie poczucia bezpieczeństwa w sposób niezagrażający bezpieczeństwu. Dziwne to i może dla niektórych śmieszne sformułowanie. Wyjaśnienie jest jednak proste i wymowne: działania niewłaściwe lub pozorne (jak opisana wyżej instalacja atrap kamer) przynoszą więcej szkody niż pożytku. Czy na przykład możliwe jest prowadzenie ochrony przez osoby nieprzygotowane do realizacji takiego zadania lub przygotowane do niego nieprofesjonalnie?

Do ochrony terenów szkół powinny być kierowane osoby nie tylko wyszkolone technicznie, ale również posiadające przygotowanie do rozmów z uczniami i nauczycielami. Pracownik ochrony nie zna wystarczająco psychiki dziecka w określonym wieku, nie będzie w stanie zrozumieć poszkodowanego dziecka i jego wypowiedzi, a zatem również uzyskać od niego niezbędnych informacji o zdarzeniu w sposób skuteczny, a zarazem delikatny. W fazie postępowania przygotowawczego, służącego ustaleniu przebiegu zdarzeń relacjonowanego przez dziecko, konieczny jest udział psychologa. Trzeba mieć również świadomość, że poszkodowany, w momencie gdy stał się ofiarą przestępstwa, nie zarejestrował wszystkich jego okoliczności w sposób obiektywny i w swoich wypowiedziach przedstawia własną wersję wydarzeń. Psycholog oceni również wiarygodność wypowiedzi.

Należy pamiętać, że przestępstwa w szkołach bardzo często są dokonywane „po cichu" i polegają na tym, że sprawcy zastraszają pokrzywdzonego. Ogólnie przestępstwa popełniane w szkołach można podzielić na dwie grupy, które teraz krótko scharakteryzujemy.

Zdarzenia bez użycia przemocy fizycznej i psychicznej to na przykład kradzież, popełniona przez jednego lub kilku sprawców. Popełnienie tego czynu jest często związane z chęcią

osiągnięcia korzyści majątkowej lub chęcią wejścia do grupy bądź utrzymania przynależności do niej. Przedmioty kradzieży są sprzedawane lub pozostają w posiadaniu sprawców. Poszkodowany nie ponosi uszczerbku na zdrowiu fizycznym, natomiast naruszona zostaje jego psychika. Zdarzenie pozostaje w niej jako uraz, powodujący brak zaufania do otoczenia.

Zdarzenia z użyciem przemocy psychicznej i fizycznej to zwykle czyny dokonywane przez nieformalne grupy przestępcze istniejące w szkołach. Grupy te wzbudzają strach. Uczniowie doskonale wiedzą o ich istnieniu, ale panuje zmowa milczenia, której skutkiem jest nieujawnianie i bezkarność tych grup. Obawa przed wywarciem presji psychicznej lub innego rodzaju zagrożeniami ze strony grupy powoduje utrzymywanie informacji o niej i jej czynach w ścisłej tajemnicy. Grupy działają na terenach szkolnych, w najbliższej okolicy i poza terenem szkoły. Bardzo często członkowie grup charakteryzują się bezwzględnością, popełniając czyny zabronione w stosunku do osób i mienia.

Odpowiedzialność i wewnętrzne procedury bezpieczeństwa

Ochrona to złożony proces obejmujący między innymi obserwację, analizę, wnioskowanie i działania. Brak profesjonalizmu i doświadczenia w tych działaniach może doprowadzić do skutku odwrotnego niż zapewnienie bezpieczeństwa, a mianowicie do sprowadzenia zagrożenia na osoby i obiekty chronione. Zasada ta jest uniwersalna, obejmuje bardzo szeroki obszar zagadnień i odnosi się do całokształtu procesu ochrony – wszystkich jej kolejnych procesów i procedur.

Przeanalizujmy proces ustalania wewnętrznych procedur bezpieczeństwa. Aby procedury zostały prawidłowo zdefiniowane, muszą być poprzedzone obserwacjami, analizą, wnioskowaniem i podjęciem działań. Podobnie jest z procesem projektowania systemów bezpieczeństwa. Zaniechanie bądź wadliwe opracowanie i wdrożenie procesu spowoduje tzw. nieszczelności systemu, a w najbardziej niekorzystnym przypadku sprowadzi zagrożenie. Procedury i projekt można zmienić, a nawet całkowicie wycofać i zastąpić czymś nowym. Nie można natomiast cofnąć zdarzenia, które nastąpiło, ponieważ ochrona fizyczna okazała się nieskuteczna lub niewystarczająca. Bardzo ważne stają się więc wymienione wyżej obserwacje, analiza, wnioskowanie i podjęcie działań. Procesy te muszą stanowić spójną całość. Wykonanie jednego z elementów w sposób nieprawidłowy wywołuje zawsze skutek trudny do przewidzenia.

Powróćmy na krótką chwilę do procesu projektowania i powiążmy go z zagadnieniem ochrony fizycznej przy założeniu, że popełniono uchybienie polegające na wydaniu przez projektanta zgody na montaż atrapy kamery. Zadajmy sobie pytanie: czy osoba profesjonalnie przygotowana do prowadzenia obserwacji zareaguje na zdarzenie pod atrapą? Jaka jest odpowiedzialność projektanta, ale przede wszystkim decydenta (zarządca lub właściciel obiektu) za takie postępowanie?

Aby ochrona w takim przypadku zareagowała, musi otrzymać informację o zdarzeniu od świadka. Profesjonalizm osoby zajmującej się ochroną zostanie określony na podstawie sposobu przeprowadzenia interwencji. A sposób przeprowadzenia interwencji będzie zależny od wiarygodności świadka i użytych środków. Odpowiedzialność prawna w tym zakresie jest bardzo złożona, gdyż możemy mieć do czynienia z różnymi przypadkami, np. podjęcia działania w sposób prawidłowy albo w sposób nieprawidłowy, albo też zaniechanie działania. Działanie lub zaniechanie można jeszcze ocenić w aspekcie działania świadomego lub nieświadomego, w dobrej lub złej wierze.

Nie chodzi tu jednak o zawiłość logiczną, lecz jednoznaczne określenie problemu.

Odpowiedzialność za bezpieczeństwo osób i obiektu zaczyna się w momencie podjęcia decyzji o wdrożeniu pierwszych procedur związanych z zapewnieniem bezpieczeństwa (niekoniecznie zastosowaniem monitoringu), co w najprostszym przypadku oznacza zmiany w organizacji ruchu w obiekcie, wydzielanie stref, zamykanie obiektu itd. Wprowadzenie systemów ochrony technicznej (systemów CCTV, systemów alarmowych, systemów kontroli dostępu do poszczególnych stref i obiektów) to również wprowadzenie procedur – kolejnych. Do opracowania i wprowadzenia procedur bezpieczeństwa zobowiązane jest kierownictwo placówki, np. dyrektor szkoły.

Wdrażanie procedur

Wdrażanie procedur w organizacji nie tylko nie jest proste, jest również czasochłonne. W tym procesie muszą brać udział wszystkie osoby wskazane w procedurach bezpieczeństwa. Wdrażanie obejmuje zapoznanie z treścią stosownych dokumentów całego personelu organizacji, a następnie egzekwowanie tych zapisów. Należy też sukcesywnie przypominać uczestnikom wdrożone już procedury. Gdy chodzi o zagadnienia organizacyjne i techniczne, np. rozmieszczenie kamer lub urządzeń przyzywowych, uczestnicy muszą znać miejsca instalacji takich urządzeń, ponieważ może pojawić się potrzeba ucieczki przed napastnikami i szukania schronienia w polu widzenia kamer lub dotarcia do przycisku przyzywowego. Uczestnicy nie muszą natomiast znać miejsc obserwacji obrazów z kamer. Procedury reakcji na poszczególne zdarzenia powinny być trzymane w tajemnicy. Członkowie organizacji powinni otrzymać zapewnienie, że procedury zapewniają właściwą reakcję na zdarzenia krytyczne.

Odrobina techniki

Inwestorzy często stają przed koniecznością wyboru systemu, zadają pytania, czy lepszy będzie tradycyjny, czy IP; jakie kamery należy zastosować. Nie ma jednoznacznej odpowiedzi na te pytania. Idąc z duchem postępu technicznego, należałoby przyjąć technologię IP. Mając na uwadze oszczędności, należałoby przyjąć technologię tradycyjną.

Każdy obiekt jest inny. Każda organizacja ma własne procedury, które sugerują wybór rozwiązania. Istotne jest, aby spośród wielu możliwych urządzeń wybrać skuteczne, czyli te, które zapewnią podwyższenie bezpieczeństwa.

Kiedyś spotkałem się z wypowiedzią pracowników ochrony: „Nie jest ważne, co widzimy – ważne, jak zareagujemy”. Z mojej strony padło wówczas pytanie: „A jak dobierzesz siły i środki do interwencji?”. Przy tej okazji można zadać pytanie: „A jak wygląda twój materiał dowodowy ze zdarzenia?”. Ale najważniejsze pytanie, jakie należy sobie w tym kontekście zadać, to: „Czy czujemy się bezpiecznie?”.

Tomasz Malinowski

Naruszanie dóbr osobistych na forach internetowych

Monika Brzozowska

Już pobieżna analiza wpisów na forach internetowych świadczy o tym, że treść niektórych wpisów może być niezgodna z prawem, zwłaszcza z przepisami dotyczącymi ochrony dóbr osobistych. Internet umożliwia dokonywanie wpisów naruszających prawo, w dodatku anonimowych, przynajmniej z pozoru. Istniejące przepisy pozwalają jednak na podjęcie przez pokrzywdzonego działań umożliwiających ustalenie tożsamości autora wpisu i dochodzenie sprawiedliwości. Dobrym przykładem może być przypadek ministra spraw zagranicznych Radosława Sikorskiego i jego prawnej batalii z autorami wpisów na forach. Obraźliwe wpisy na forach mogą stanowić naruszenie dóbr osobistych, a także przestępstwo – znieważenie lub pomówienie. Sprawiedliwości można dochodzić na drodze karnej bądź cywilnej

Dochodzenie sprawiedliwości na drodze karnej

Generalnie, zgodnie z przepisami prawa karnego, wpis w Internecie może naruszyć dobro osobiste pokrzywdzonego w dwojaki sposób. Osoba korzystająca z forum może zniesławić pokrzywdzonego (art. 212 § 2 k.k.), to znaczy podać nieprawdziwą informację narażającą na poniżenie w opinii publicznej bądź narazić na utratę zaufania potrzebnego do obejmowania danego stanowiska lub wykonywania zawodu. Ten typ twierdzenia może być oceniany jako prawda albo fałsz, czyli pokrzywdzony może stwierdzić, iż zdanie zamieszczone na forum nie jest prawdziwe. Należy zauważyć, że jest to przestępstwo bezskutkowe, tzn. zaistnienie skutku – np. w postaci utraty zaufania wobec pokrzywdzonego – nie jest potrzebne. Wystarczy, że istnieje tylko możliwość utraty dobrego imienia lub zaufania.

Drugim rodzajem przestępstwa, często występującego w omawianym kontekście, jest znieważenie, czyli zamieszczenie wypowiedzi obraźliwej, ale nie dającej się zweryfikować. Jest to przestępstwo określone w art. 216 § 2 kodeksu karnego.

Obydwa typy przestępstw są najczęstszym sposobem naruszenia dóbr osobistych na forach internetowych i są ścigane na drodze karnej. Jedna wypowiedź może stanowić zarówno zniesławienie, jak i znieważenie. W orzecznictwie sądowym podkreśla się także, że wypowiedź może być w określonych warunkach zniesławiająca, a w innych znieważająca. W przypadku wspomnianej na wstępie sprawy ministra Sikorskiego na forum internetowym jednej z gazet pojawiły się wpisy obraźliwe. Oto jedna z wypowiedzi:

„Radosław Sikorski – mąż ortodoksyjnej z dziada pradziada amerykańskiej żydówki, wróg Polskości, biegle władający językiem polskim amerykański agent i mason, zdalnie sterowany przez teścia, naczelnego czosnka nowego Yorku, przejął pałeczkę destrukcji i destabilizacji kraju od niejakiego michnika – jednak bardziej niebezpieczny z racji zajmowanego wysokiego stanowiska – pod maską dobrotliwego gogusia ukryty bezwzględny sprzedawczyk, wyzbyty wszelkich zasad wykonawca rozkazów międzynarodowej kliki" (*www.gazetaprawna.pl*).

Należy odróżnić zniesławienie od znieważenia. Znieważenie sprowadza się do użycia określenia obraźliwego. Przy okazji przytoczonego fragmentu widać jednak doskonale, iż niektóre wypowiedzi będą w konkretnym przypadku nie zniesławieniem, lecz obraźliwym znieważeniem. Moim zdaniem określenie „wróg polskości" – choć teoretycznie nieweryfikowalne pod względem prawdziwości – jest znieważeniem. Wykazanie, iż jest się wrogiem bądź przyjacielem polskości, jest w praktyce niezwykle trudne. Wydaje się oczywiste, iż autor wypowiedzi chciał ministra obrazić, a nie racjonalnie skrytykować.

Przy tej okazji warto również nadmienić, iż zarówno zniesławienie, jak i znieważenie dokonane na forum internetowym jest tzw. typem kwalifikowanym. Jest dokonane przy użyciu środków masowego komunikowania, przez co kara grożąca sprawcy jest nieco wyższa.

Narzuca się pytanie, kto jest odpowiedzialny za wpis w świetle obowiązującego prawa – autor wpisu, administrator strony czy hostingujący ową stronę? Kogo można oskarżyć?

W przypadku większości czynów karalnych to prokurator popiera sprawę przed sądem oraz sporządza akt oskarżenia.

W przypadku znieważenia i zniesławienia w Internecie pokrzywdzony zobligowany jest do samodzielnego sporządzenia i popierania aktu oskarżenia. Może także wynająć w tym celu adwokata lub radcę prawnego. Istnieje jednak przepis, który znacznie ułatwia dochodzenie sprawiedliwości na drodze karnej w przypadku obraźliwych wpisów na forach internetowych. Zgodnie z art. 488 k.p.k. „Policja na żądanie pokrzywdzonego przyjmuje ustną lub pisemną skargę i w razie potrzeby zabezpiecza dowody, po czym przesyła skargę do sądu".

Z treści przepisu wynika, iż:

– osoba pokrzywdzona (lub adwokat w jej zastępstwie) może sporządzić tzw. prywatny akt oskarżenia i skierować go bezpośrednio do sądu albo zgłosić skargę na policję, skąd zostanie ona przesłana do właściwego sądu,
– w przypadku złożenia skargi na policję policja ma obowiązek zabezpieczyć dowody przestępstwa.

W przypadku przestępstw popełnionych za pośrednictwem Internetu ten ostatni obowiązek ma szczególnie doniosłe znaczenie. Na mocy tego przepisu policja powinna ustalić adres IP komputera, na którym dokonano obraźliwego wpisu. Oczywiście nie przesądza to jeszcze o winie właściciela komputera, ale znacznie ułatwia ustalenie tożsamości naruszającego prawo. Administrator strony może ewentualnie odpowiedzieć za pomocnictwo, jednak pod wieloma warunkami określonymi przez kodeks karny. Za znieważenie i (lub) pomówienie nie będzie natomiast ponosić odpowiedzialności podmiot hostingujący – ze względu na wyłączenie odpowiedzialności zgodnie z art. 14 ustawy o świadczeniu usług drogą elektroniczną. Oczywiście przy założeniu, że wpisy nie zostały dokonane bezprawnie. Jeśli natomiast miały taki bezprawny charakter, powinien on usunąć je oraz udzielić informacji o danych osobowych naruszyciela.

O tym, że ustalenie danych osobowych naruszyciela nie jest takie proste, dość boleśnie przekonałam się podczas prowadzenia sprawy o znieważenie jednego z polityków. Policja, którą poprosiliśmy o pomoc, zasłoniła się ustawą o ochronie danych osobowych, podobnie administrator oraz hostingujący. Sąd natomiast – do którego wniesiono prywatny akt oskarżenia – po prostu oddalił wniosek dowodowy o udostępnienie IP.

Coraz częściej jednak judykatura dostrzega konieczność podania numeru IP oskarżycielowi prywatnemu.

W jednym z najczęściej cytowanych orzeczeń Sądu Administracyjnego w Warszawie, w sprawie dotyczącej zniesławienia, zaakcentowano konieczność udostępnienia numerów IP komputerów oraz danych osobowych na potrzeby procesu karnego o zniesławienie. Zdaniem Sądu Administracyjnego w Warszawie „adres IP, pozwalający zidentyfikować autora wpisu na forum internetowym, należy do zbioru danych osobowych i administratorzy forum powinni go wydawać osobom, których dobra zostały naruszone" (Wyrok Sądu Administracyjnego w Warszawie, II SA/Wa 1598/09).

Jak już wspomniałam, akt oskarżenia sporządzany jest na ogół przez samego pokrzywdzonego (lub jego pełnomocnika), a w trakcie postępowania jest przez niego także popierany.

W wyjątkowych przypadkach, gdy wymaga tego interes społeczny, prokurator może wszcząć postępowanie w sprawie prywatnoskargowej lub przyłączyć się do toczącego się już postępowania. Prokurator ma duży margines swobody przy podejmowaniu decyzji dotyczącej wszczęcia bądź zaniechania postępowania w sprawie o zniesławienie bądź znieważenie. Według obowiązującego prawa powinien to uczynić za każdym razem, gdy naruszenie czci pokrzywdzonego może mieć implikacje ogólnospołeczne. Trzeba jednak podkreślić, że prokuratura bardzo rzadko przystępuje do takich spraw. Z informacji prasowych wynika, że w przypadku ministra R. Sikorskiego prokuratura wszczęła takie postępowanie. W przypadku wielu moich klientów (wśród których są również politycy) prokuratura umarzała tego typu postępowania, uznawszy, że pokrzywdzony może sam dochodzić swoich praw przed sądem.

Jak się bronić, jeśli jesteśmy oskarżeni?

W swojej praktyce adwokackiej stoję często po stronie oskarżyciela prywatnego (najczęściej). Zdarza mi się również bronić oskarżonych w tego typu procesach. Strategia obrony to skorzystanie z tzw. kontratypu (tj. wyłączenia odpowiedzialności) opisanego w art. 213 § 2 kodeksu karnego.

Zgodnie z tym artykułem nie popełnia przestępstwa określonego w art. 212 § 1 lub 2 ten, kto publicznie podnosi lub rozgłasza prawdziwy zarzut dotyczący postępowania osoby pełniącej funkcję publiczną lub służący obronie społecznie uzasadnionego interesu, przy czym – jeżeli zarzut dotyczy życia prywatnego lub rodzinnego – postępowanie dowodowe może być przeprowadzone tylko wtedy, gdy ma zapobiec zagrożeniu życia lub zdrowia człowieka albo demoralizacji małoletniego.

Zakres odpowiedzialności administratora będzie nieco inny w przypadku sprawy cywilnej, o czym niżej.

Droga postępowania cywilnego

Naruszenie dóbr osobistych może być ścigane także na drodze cywilnej. W nomenklaturze tej dziedziny prawa naruszenia, o których mowa w niniejszym artykule, są naruszeniami czci i dobrego imienia. Jedną z podstawowych różnic pomiędzy postępowaniem cywilnym a postępowaniem karnym jest to, że w przypadku postępowania cywilnego można pozwać także inne osoby, – nie tylko samego naruszającego.

Kluczem do zrozumienia tematu wydaje się być art. 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną:

„Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych".

Sens tego nieco enigmatycznego przepisu sprowadza się – w omawianym przypadku – do tego, że administrator forum internetowego nie może być pozwany na drodze cywilnej za naruszenie dóbr osobistych innych osób dopóki nie ma wiarygodnej informacji o bezprawności wpisów.

Wydaje się, iż podobna myśl przyświecała lubelskiemu Sądowi Apelacyjnemu, który w jednym z orzeczeń stwierdził: „jeśli właściciel strony internetowej jest świadomy bezprawności wpisów, to ma obowiązek natychmiast je usunąć; jeśli tego nie zrobi – ponosi odpowiedzialność".

Zatem moment uzyskania wiarygodnej informacji o bezprawności wpisu decyduje o odpowiedzialności gospodarza forum. Pozwanym może być więc podmiot hostingujący. O tym, co jest wiarygodną informacją, nie sposób orzec *in abstracto*. W ostateczności to sąd ustali, czy taka wiarygodna informacja została otrzymana.

W przypadku prawa prasowego ustawodawca idzie jeszcze dalej, stwierdzając, że podmiotami pozwanymi mogą być zarówno autor materiału prasowego, redaktor naczelny, jak również wydawca, przy czym – co niezwykle istotne – za materiał prasowy uznawany jest każdy opublikowany lub przekazany do opublikowania w prasie tekst albo obraz o charakterze informacyjnym, publicystycznym, dokumentalnym lub innym, niezależnie od środków przekazu, rodzaju, formy, przeznaczenia czy autorstwa (art. 7 ust. 1 pkt 4 prawa prasowego).

Przy okazji warto również zwrócić uwagę na specyficzny rozkład dowodu w sprawach o naruszenie dóbr osobistych. W postępowaniu cywilnym obowiązuje generalna zasada, którą można streścić i wyrazić następująco: jeżeli coś twierdzisz, to udowodnij to. W postępowaniu karnym zaś króluje zasada domniemania niewinności oskarżonego, która obowiązek przedstawienia wiarygodnych dowodów nakłada na oskarżyciela (najczęściej prokuratora).

W sprawach dotyczących takich naruszeń jak te omawiane w niniejszym artykule obowiązek przedstawienia dowodów spoczywa na potencjalnym naruszycielu, czyli oskarżonym (w postępowaniu karnym) albo pozwanym (w postępowaniu cywilnym). To te osoby są zobowiązane do wykazania prawdziwości stawianych tez. Możliwości wykazania prawdziwości tezy nie ma oczywiście w przypadku wyrażeń znieważających, jednoznacznie obraźliwych, nieweryfikowalnych pod względem prawdziwości.

Zakończenie

Istniejące przepisy prawa umożliwiają podjęcie walki z autorami obraźliwych tekstów na forach internetowych. Z pewnością nie jest to proste, ale autorzy ci coraz częściej goszczą na wokandach sądowych. Niektórym internautom wydaje się, że sieć jest w stanie zapewnić im całkowitą anonimowość, a przez to bezkarność. Przeświadczenie to jest złudne.

mec. Monika Brzozowska
adwokat, partner w kancelarii PD&B
specjalista z zakresu tzw. cyfrowego prawa

profesjonalne rozwiązania
do cyfrowej rejestracji obrazu

ponad 60 000 instalacji
pracujących na całym świecie

www.alnetsystems.com

ALNET SYSTEMS

sieciowe oprogramowanie do cyfrowej rejestracji obrazu — NS NETSTATION

hybrydowy system do cyfrowej rejestracji obrazu — NET HYBRID

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

profesjonalne oprogramowanie klienckie — CMS PROFESSIONAL

oprogramowanie klienckie dla urządzeń mobilnych — CMS MOBILE

blisko 1000 kamer zintegrowanych
z oprogramowaniem Alnet Systems

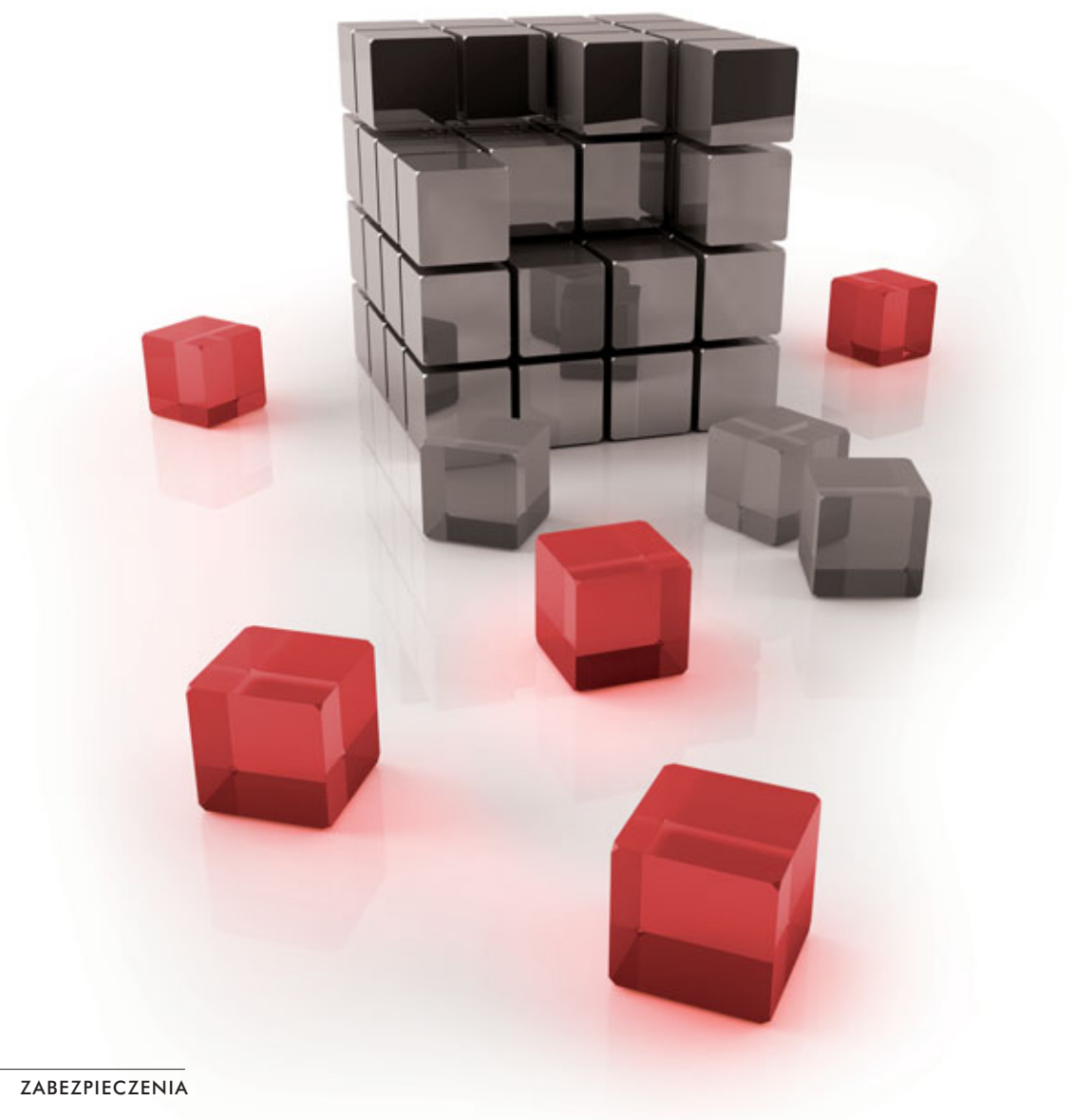
wybór należy do Ciebie!

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

Telewizja IP
Zalety rozwiązania hybrydowego

Tomasz Żuk

Planując instalację systemu telewizji dozorowej potencjalny inwestor musi wiedzieć, jakiego rodzaju system chce posiadać i czy ma być to rozwiązanie klasyczne (zwane analogowym) czy rozwiązanie IP. Oba rozwiązania mają zarówno wady, jak i zalety. Wadą rozwiązania klasycznego jest ograniczona odległość kamer od rejestratora i brak możliwości ich zdalnego konfigurowania. Z kolei w przypadku technologii IP problemem jest konieczność przystosowania infrastruktury sieciowej do wzmożonego ruchu związanego z przesyłaniem strumieni wizyjnych, które niejako z definicji alokują spore pasmo, co dodatkowo podwyższa cenę i tak droższego w porównaniu z klasycznym rozwiązania. A co zainstalować w przypadku, w którym inwestor chce jedynie „odmłodzić" istniejący system klasyczny i jednocześnie dodać do niego dodatkowe kamery IP? Odpowiedź jest tylko jedna – rejestrator hybrydowy



Rejestrator hybrydowy TVR60

Rejestrator TVR60 należący do linii urządzeń TruVision jest wydajnym, skalowanym cyfrowym rejestratorem hybrydowym, który umożliwia bieżący podgląd i wyszukiwanie obrazów oraz zapis i przesyłanie sygnału wizyjnego z maksymalnie dwudziestu czterech kamer analogowych lub sieciowych w pełnej rozdzielczości 4CIF i z szybkością 25 kl./s. Urządzenie to sprawdzi się zarówno tam, gdzie oczekuje się wydajnego rejestratora klasycznego (analogowego), potrafiącego zarejestrować do 16 kanałów w czasie rzeczywistym i rozdzielczości 4CIF, jak i tam, gdzie potrzebny jest niezawodny rejestrator sieciowy, który może zarejestrować do 16 strumieni IP zarówno w rozdzielczościach tradycyjnych (CIF, QCIF, 4CIF), jak i megapikselowych (SXGA, XGA). Jeżeli dodamy do tego dyski o sumarycznej pojemności sięgającej 12 TB, otrzymujemy urządzenie, które jest w stanie spełnić nawet najbardziej wygórowane wymagania.

Cechy rejestratora TVR60:

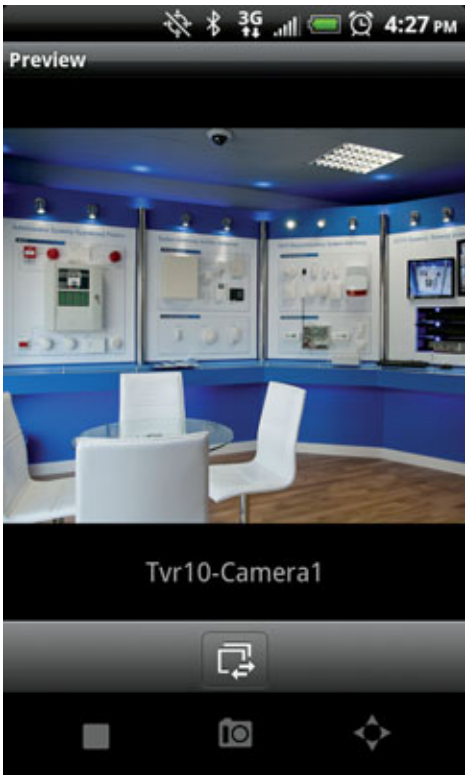
– możliwość rejestracji obrazów z 24 kanałów (elastyczny podział pomiędzy wejścia analogowe i sieciowe),
– pojemność dysków do 12 TB,
– kodowanie do 600 fps (4CIF),
– obrazy ze wszystkich kanałów są rejestrowane w czasie rzeczywistym w przypadku rozdzielczości 720p,
– obsługa funkcji *dual streaming*,
– trzy niezależnie konfigurowalne wyjścia monitorowe.

Rejestrator TVR60 współpracuje z oprogramowaniem TVRmobile przeznaczonym do urządzeń z systemem operacyjnym iOS, Android lub Windows Mobile. Aplikacja ta umożliwia wyświetlanie czterech strumieni wizyjnych jednocześnie oraz sterowanie kamerami PTZ za pomocą intuicyjnego menu.

Najnowszy format – H.264-SVC

Obecnie przeważająca większość producentów oferuje rejestratory wykorzystujące technologię H.264 jako standard kompresji zapisywanych obrazów. Wynika to przede wszystkim z faktu, że technologia ta daje najlepszy współczynnik kompresji w odniesieniu do subiektywnej jakości uzyskiwanego obrazu wizyjnego. Efektywniejsza kompresja przy zachowaniu tego samego poziomu jakości umożliwia zaoszczędzenie miejsca na dyskach rejestratorów i ogranicza w pewnym stopniu zapotrzebowanie na pasmo sieciowe wymagane do przesyłania obrazów. Oba te czynniki w sposób oczywisty przekładają się na zmniejszenie kosztu wykonania systemu. Mimo powszechności rozwiązanie to ma pewne istotne ograniczenie, mianowicie w celu uzyskania kilku strumieni wizyjnych o różnych parametrach, pochodzących z jednego źródła (kamery), należy zastosować kilka koderów. Każdy taki strumień jest następnie przesyłany do odbiornika, a zajętość sieci jest sumą przepływności wszystkich strumieni.

Fot. 1. Rejestrator TVR60



Fot. 2. Oprogramowanie TVRMobile

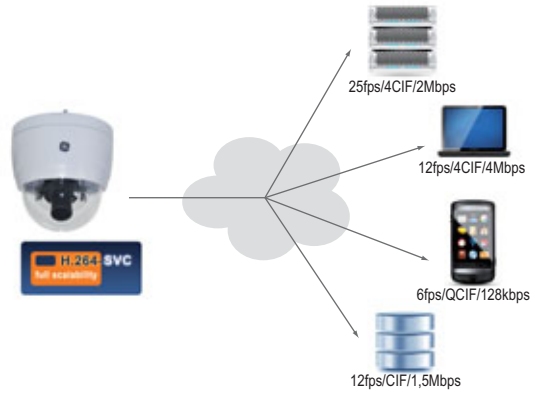
Innymi słowy – w przypadku technologii H.264 nie da się wyodrębnić kilku strumieni o różnych parametrach z jednego strumienia głównego.

Inaczej jest w przypadku opracowanego przez firmę GE Security (obecnie UTC Fire & Security) kodeka H.264-SVC (*Scalable Video Coding*). Największą zaletą tego rozwiązania jest jego skalowalność. Cecha ta oznacza, że w pojedynczym strumieniu wizyjnym zawarta jest informacja potrzebna do wydzielenia strumieni o różnych parametrach bez konieczności stosowania dodatkowych operacji dekodowania/kodowania, które wymagają urządzeń o podwyższonej mocy obliczeniowej oraz – co jest nawet ważniejsze – wprowadzają do sygnału spore opóźnienia. Dzięki możliwości stosowania pojedynczego strumienia wizyjnego zamiast kilku niezależnych strumieni obniżone zostaje zapotrzebowanie na pasmo sieciowe.

TruVision Navigator

Chyba nikt spośród osób profesjonalnie zajmujących się systemami telewizji dozorowej nie ma wątpliwości, że nawet najlepsze rejestratory i kamery bez oprogramowania komputerowego do zarządzania nimi nie są w pełni funkcjonalne. Czasy, w których do prowadzenia obserwacji używano monitorów podłączonych bezpośrednio do rejestratorów lub krosownicy wizyjnej, minęły. Widać to szczególnie wyraźnie w przypadku systemów sieciowych – nierzadko spotyka się modele rejestratorów pozbawione wyjść monitorowych, w przypadku których konfigurowanie

Fot. 3. Najnowszy kodek H.264-SVC (Scalable Video Coding)



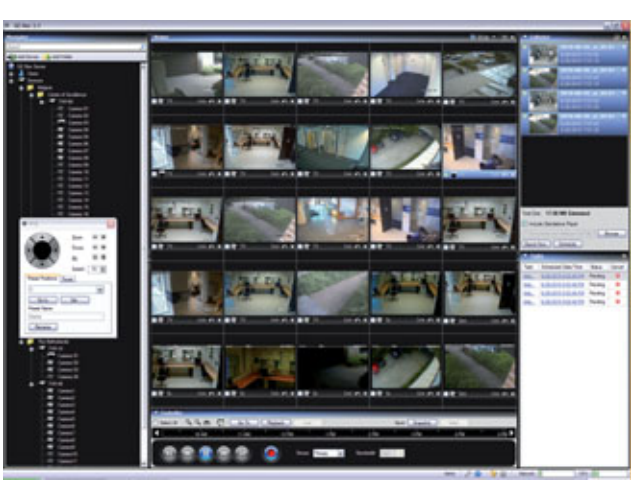
Rys. 1. Skalowalny kodek H.264 SVC – zasada działania

oraz oglądanie zgromadzonych obrazów jest możliwe tylko za pośrednictwem sieci i dedykowanego oprogramowania. Tego rodzaju oprogramowaniem jest GE Nav – nowoczesna platformą do zarządzania i monitoringu wizyjnego w systemie wykorzystującym rejestratory produkcji UTC F & S. Najnowsza wersja tej aplikacji nosi nazywę *TruVision Navigator*, co ma dodatkowo podkreślić powiązanie z linią produktów TruVision. TruVision Navigator jest wielostanowiskową aplikacją umożliwiającą zdalne zarządzanie kompletnym systemem telewizji dozorowej bazującym na rozwiązaniach UTC F&S.

Podstawowe zalety aplikacji TruVision Navigator:

– obsługa niemal wszystkich serii i typów rejestratorów produkcji UTC F&S zapewniająca kompatybilność ze starszymi produktami,
– możliwość sterowania kamerami PTZ za pomocą myszy,
– możliwość pełnej zdalnej konfiguracji urządzeń (rejestratorów i kamer),
– możliwość bardzo precyzyjnego doboru uprawnień nadawanych operatorom,
– możliwość obserwacji w trybie na żywo i jednoczesnego odtwarzania nagrań z wielu rejestratorów,
– zapis lokalnej kopii wybranego materiału wizyjnego w oparciu o harmonogram (możliwość określenia czasu przesyłania w celu optymalizacji wykorzystania sieci).

Warto wspomnieć, że oprogramowanie TruVision Navigator jest dostępne nieodpłatnie.



Fot. 4. TruVision Navigator

Obsługiwane kamery produkcji UTC F&S oraz wsparcie dla otwartego formatu PSIA

Często okazuje się, że nie można stworzyć kompletnego systemu dozorowego z wykorzystaniem sprzętu pochodzenia wyłącznie od jednego producenta. Powodem jest zbyt skromna, mało urozmaicona oferta.

W przypadku opisywanego systemu możliwe jest zastosowanie wielu typów i serii kamer, co pozwala na znalezienie odpowiedniej kamery dla niemal każdej aplikacji.

Rejestrator TruVision TVR60 jest kompatybilny z:

– serią kamer UltraView IP (kamery o niskiej rozdzielczości, dostępne w wersji standardowej (EVR) i w wersji o podwyższonej dynamice WDR (XP3), w obudowach standardowych i kopułowych);
– serią kamer TruVision IP (kamery megapikselowe o rozdzielczościach 1.3 i 2 Mpx, dostępne w wersji standardowej i kopułowej – w obudowie plastikowej i wzmacnianej);
– koderem IP UVE-101 (koder ten umożliwia podłączenie dowolnej kamery z wyjściem analogowym, zapewniając kodowanie w najnowocześniejszym formacie H.264-SVC).

Częstą słabością rozwiązań sieciowych jest konieczność stosowania kamer i rejestratorów pochodzących od jednego producenta, co jest konsekwencją konieczności zaimplementowania w obu urządzeniach tego samego protokołu komunikacyjnego wyższej warstwy, umożliwiającego komunikację pomiędzy obydwoma urządzeniami. Rozwiązaniem tego problemu byłoby opracowanie wspólnego protokołu lub zestawu protokołów, który ujednoliciłby sposób przesyłania strumieni wizyjnych z kamer do rejestratorów, a także zestandaryzowanie formatów i sposobów ich transmisji. Zadania tego podjęły się dwie wiodące obecnie organizacje standaryzacyjne: Physical Security Interoperability Alliance (PSIA) oraz Open Network Video Interface Forum (ONVIF). W wyniku ich prac zostały stworzone otwarte standardy, a jeden z nich – PSIA – został zaimplementowany w rejestratorze TVR60, dzięki czemu zyskuje się możliwość sprzęgnięcia tego rejestratora z kamerami innych producentów.

Widać wyraźnie, że kierunek rozwoju systemów telewizji dozorowej został wyznaczony przez systemy IP. Technologia IP ma swoje niepodważalne zalety, które powodują, że w wielu aplikacjach jest to właściwie jedyne rozwiązanie możliwe do wykorzystania. Z technologią IP mamy do czynienia zawsze, gdy zachodzi potrzeba zastosowania kamer megapikselowych. Technologia ta ma jednak również ograniczenia, które uwidaczniają się zwłaszcza wtedy, gdy użytkownik chce dołączyć pojedyncze urządzenia sieciowe do istniejącego systemu analogowego, stopniowo modyfikować system bez dużych jednorazowych wydatków związanych z wymianą już istniejącej infrastruktury. Takie podejście jest niemożliwe. W takim przypadku rozwiązanie hybrydowe sprawdza się najlepiej. Opisane powyżej urządzenia można połączyć, aby utworzyć komplementarne rozwiązanie składające się z wysokiej klasy rejestratora TVR60, kamer wykorzystujących najnowocześniejsze kodeki H.264-SVC oraz zaawansowanego oprogramowania służącego do zarządzania całością – TruVision Navigator.

Tomasz Żuk
UTC Fire & Security Polska

UTC Fire & Security

A United Technologies Company

Zintegrowane systemy bezpieczeństwa dla sektora bankowego

www.utcfssecurityproducts.pl

Centrala UTC Fire & Security Polska Sp. z o.o.
ul. Sadowa 8
80-771 GDAŃSK
tel.: (58) 301 38 31, (58) 760 64 80
fax: (58) 301 14 36

Oddział w Warszawie
Al. Stanów Zjednoczonych 59
04-028 WARSZAWA
tel.: (22) 810 00 03
fax: (22) 810 10 55

Oddział w Poznaniu
Oś. Na Murawie 11/2
61-655 POZNAŃ
tel.: (61) 821 35 66
tel./fax: (61) 821 31 94

Technologia Lightfinder firmy Axis Communications

doskonały nadzór w warunkach słabego oświetlenia

Agata Majkucińska

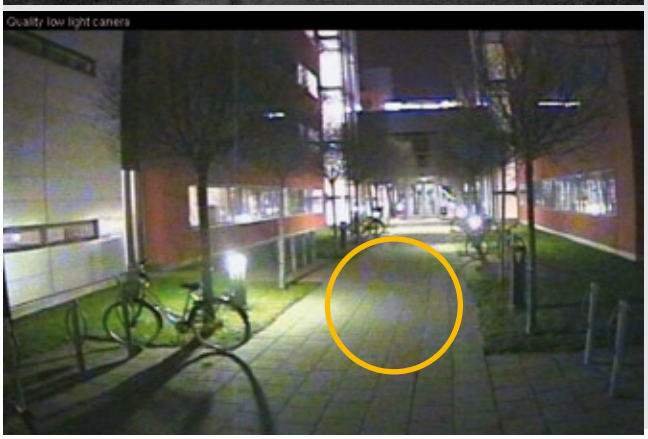
Kamera działająca w trybie dzień/noc jest przeznaczona do pracy w systemach nadzoru zewnętrznego lub wewnątrz budynków w warunkach słabego oświetlenia. Kolorowa sieciowa kamera dzienno-nocna dostarcza kolorowych obrazów podczas pracy dziennej. Gdy zmniejsza się poziom oświetlenia, kamera automatycznie przechodzi w tryb pracy nocnej i zaczyna wykorzystywać światło, którego widmo mieści się w zakresie bliskiej podczerwieni (IR), tworząc czarno-białe obrazy. Utrzymanie ostrości obrazu i niskich szumów okazuje się trudne, zwłaszcza w zróżnicowanym środowisku zewnętrznym

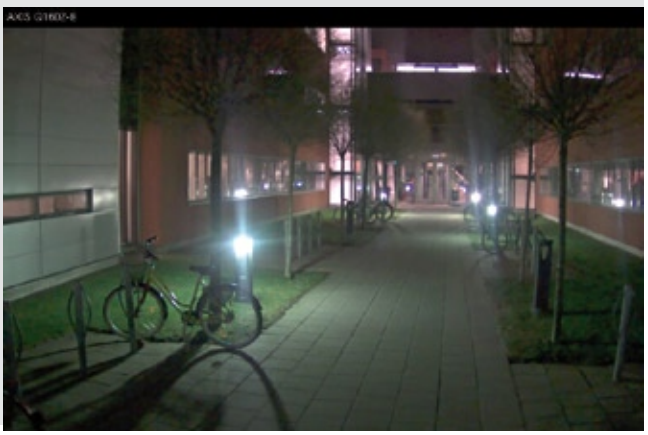
Dział badań i rozwoju firmy Axis Communications opracował nową technologię – Lightfinder. Jest to rezultat skrupulatnego doboru właściwego przetwornika obrazu i obiektywu oraz odpowiedniej obróbki obrazu. Fuzja tych czynników – przetwornik, obiektyw, własny procesor obrazu Axis (ARTPEC), a także sposób przetwarzania obrazu – sprawia, że kamery wykorzystujące tę technologię są niezwykle wydajne.

Technologia Lightfinder pozwala na zwiększenie czułości przetwornika obrazu CMOS, jednakże nie wynika to wyłącznie ze zmian w konstrukcji samego przetwornika. Jak wykazało bogate doświadczenie firmy Axis, którego efektem jest wiedza dotycząca przetwarzania obrazu, wykorzystana podczas projektowania wszystkich produktów służących do pracy w systemach nadzoru wizyjnego, odpowiednio opracowane oprogramowanie pozwala uzyskać obraz o najwyższej jakości. Kamery AXIS Q1602 i AXIS Q1602-E doskonale sprawdzają się w warunkach słabego oświetlenia dzięki właściwemu doborowi przetwornika obrazu i obiektywu oraz starannej obróbce obrazu.

W porównaniu z dowolną kamerą analogową kamery AXIS Q1602 i AXIS Q1602-E zapewniają lepszą rozdzielczość i bardziej realistyczne kolory, szczególnie w warunkach słabego oświetlenia. Wykorzystujący tę technologię system redukcji szumów jest znacznie lepszy od podobnych systemów stosowanych w dostępnych na rynku kamerach analogowych, co w połączeniu z wysoką czułością przetwornika daje efekt w postaci obrazu o doskonałej jakości. Gdy technologia Lightfinder jest zastosowana w urządzeniach cyfrowych, możliwe jest wykorzystanie przetworników z funkcją skanowania progresywnego oraz wszystkich innych rozwiązań typowych dla kamer IP. Korzyści wynikające z zastosowania technologii Lightfinder to wysoka czułość, doskonała jakość obrazu, niski poziom szumów, bogactwo detali, lepsze odwzorowanie barw w warunkach słabego oświetlenia. Kamery AXIS Q1602 i AXIS Q1602-E, które bazują na technologii Lightfinder, mają również wszystkie zalety kamer sieciowych i można łatwo zintegrować je z największą na rynku bazą aplikacji dzięki programowi partnerskiemu dla twórców oprogramowania – Axis Application Development Partner Program.

Fot. 1. Kamery AXIS Q1602 i AXIS Q1602-E z zaimplementowaną technologią Lightfinder





Fot. 2. Ochrona perymetryczna obszaru nieoświetlonego nocą, o 22:40. Niżej, po lewej stronie – dobrej jakości kamera analogowa przeznaczona do pracy w warunkach słabego oświetlenia. Niżej, po prawej stronie – AXIS Q1602-E z Lightfinder. W przypadku braku oświetlenia AXIS Q1602-E jest w stanie dostarczyć kolorowego obrazu, podczas gdy kamera analogowa daje obraz czarno-biały

Fot. 3. Nadzór wejścia do budynku nocą (23:50) i oświetlenie rzędu 4 i 6 luksów. Po lewej stronie – AXIS 221. Na środku – dobrej jakości kamera analogowa. Po prawej stronie – AXIS Q1602-E z Lightfinder. Obraz z kamery AXIS Q1602-E jest mniej zaszumiony w porównaniu z obrazem z dobrej jakości kamery analogowej przeznaczonej do pracy w trudnych warunkach oświetleniowych

Zastosowanie

Kamery sieciowe korzystające z zalet technologii Lightfinder są doskonałym rozwiązaniem w przypadku systemów nadzoru wizyjnego, zarówno wewnętrznego jak i zewnętrznego, w których kamery muszą pracować w warunkach słabego oświetlenia, zwłaszcza wtedy, gdy z przyczyn użytkowych konieczne jest posługiwanie się kolorowym obrazem dostarczającym informacji niezbędnych do rozpoznawania i identyfikacji obiektów. W przeciwieństwie do konwencjonalnych kamer pracujących w trybie dzień/noc, które przy słabym oświetleniu rejestrują obraz czarno-biały, urządzenia stworzone z wykorzystaniem Lightfinder zapewniają reprodukcję barw nawet w bardzo słabo oświetlonym środowisku. W wielu sytuacjach kolorowy obraz znacznie ułatwia identyfikację ludzi, pojazdów lub wykrycie incydentów.

Zastosowanie kamer z Lightfinder będzie szczególnie korzystne w przypadku systemów, które muszą spełniać wysokie wymagania użytkowe. Mogą one sprawdzić się w dozorze wizyjnym obszarów słabo oświetlonych, takich jak parkingi, szkoły, kampusy, place budów, a także w systemach monitoringu miejskiego.

Technologia Lightfinder może być przydatna także w ochronie perymetrycznej, np. elektrowni, wodociągów, więzień, infrastruktury kolejowej. W szczególnie trudnych warunkach, np. na placach budów, które nocą mogą być oświetlane przez tylko jedno źródło światła, kamery te mogą być uzupełnione oświetlaczem pracującym w podczerwieni, ale nie zawsze jest to konieczne, gdyż odznaczają się wysokim poziomem czułości.

Testy porównawcze w warunkach nocnych i przy słabym świetle dziennym

Porównaliśmy trzy różne kamery Axis przeznaczone do pracy w systemach nadzoru wizyjnego – AXIS 221 oraz AXIS Q1602 i Q1602-E z Lightfinder – z dobrą kamerą analogową jednego z konkurentów, przeznaczoną do pracy w warunkach słabego oświetlenia. Test miał miejsce w nocy, w różnych sceneriach. Porównanie wykazało, że kamera sieciowa z Lightfinder daje obraz o lepszej jakości, z mniejszymi szumami i pełną poklatkowością, natomiast kamera analogowa w pewnych warunkach oświetleniowych nie jest w stanie dostarczyć obrazu kolorowego.

Przyszłość

W przyszłości zamierzamy inwestować w rozwój kamer sieciowych o tak wysokim poziomie czułości, na jaki pozwala technologia Lightfinder, ale z jeszcze lepszą rozdzielczością. W przyszłości zwiększona czułość i redukcja szumów będą szczególnie uwzględnianymi właściwościami kamer. Axis zawsze wykorzystuje najnowsze pod względem technologicznym przetworniki obrazu i wciąż rozwija inteligentne oprogramowanie. Będziemy nadal rozwijać produkty przeznaczone do wykorzystania w trudnych warunkach oświetleniowych.

Agata Majkucińska
Key Account Manager
Axis Communications

Fot. 4. Nadzór magazynu w warunkach słabego oświetlenia. Z lewej strony – AXIS 221. Na środku – dobrej jakości kamera analogowa przeznaczona do pracy w warunkach słabego oświetlenia. Z prawej strony – AXIS Q1602-E z Lightfinder. Identyfikacja kolorów w materiale dostarczonym przez AXIS Q1602 jest łatwiejsza, a obraz jest mniej zaszumiony i ostrzejszy niż obraz z kamery analogowej

GODZINA 13:15
Jakieś zdarzenia?

Efektywny system zewnętrznego nadzoru wizyjnego chroni to co cenimy najbardziej, ostrzega o niespodziewanych zdarzeniach a nawet uaktywnia konkretne działania. Kamery te muszą wytrzymać intensywne nasłonecznienie , duże opady deszczu i silny wiatr – i zapewnić dobrą jakość materiału wizyjnego.

Kamery do zastosowań zewnętrznych Axis są wyjątkowo proste do zainstalowania, co oszczędza cenny czas i minimalizuje koszty utrzymania. Wytrzymują one ekstremalne warunki pogodowe i zapewniają wyjątkową jakość obrazu. Ponieważ system nadzoru wizyjnego musi dostarczać niepodważalne dowody w formie przejrzystego, wyraźnego materiału wizyjnego- nawet w najcięższych warunkach.

Przyjmij punkt widzenia Axis. Bądź zawsze o krok do przodu. Odwiedź stronę: www.axis.com/outdoor

Sieciowa kamera kopułkowa AXIS Q6034-E : obudowa klasy IP66 i NEMA 4X, 18x zoom optyczny, HDTV 720p w formacie 16:9, tryb dzień/noc, H.264, zasilanie przez Ethernet, Arctic Temperatur Control i wiele więcej.

AXIS COMMUNICATIONS

System Total Security Manager

James Smith

Technologia IP oraz produkty przeznaczone do pracy w sieci istotnie przyczyniają się do rozwoju rynku zabezpieczeń fizycznych, gdyż nowe instalacje w pełni wykorzystują zalety wynikające z obsługi urządzeń poprzez sieć. Sieciowe systemy zabezpieczeń są w stanie zaoferować poziom integracji, który jeszcze kilka lat temu był nieosiągalny. Niniejszy artykuł przedstawia zasady nowego, kompkeksowego podejścia do zagadnienia integracji systemów, możliwości czerpania zysków z tej integracji, a w szczególności sposoby optymalnego wykorzystania narzędzi programowych, takich jak analiza treści obrazu

Przez wiele lat integracja w obrębie środowiska związanego z zabezpieczeniami technicznymi była traktowana po macoszemu i wiele osób nie było jej przychylnych. W pewnym okresie przez integrację rozumiano instalację kilku osobnych systemów, które w przypadku incydentu powodują zapalenie kolorowych lampek w pomieszczeniu ochrony i uruchomienie sygnalizacji dźwiękowej. Do tego celu rzadko wykorzystywany był komputer.

W ostatnich latach można było odnotować pewien postęp w tej dziedzinie, lecz nadal nie wszyscy inwestorzy zdają sobie sprawę z tego, że pieniądze zainwestowane w badania i rozwój przez wiodących producentów sprzętu pozwalają użytkownikom końcowym na czerpanie korzyści z najnowszych technologii zastosowanych w systemach sygnalizacji włamania, pożaru, systemach kontroli dostępu, ochrony obwodowej, a także w jawnych lub ukrytych systemach dozorowych.

System Total Security Manager (TSM) jest odzwierciedleniem nowego podejścia do integracji systemów zabezpieczających i maksymalne wykorzystuje rozwiązania mające wiele zastosowań, takie jak ochrona infrastruktury, monitoring miejski i ochrona cywilna. Jego przeznaczeniem jest zwiększenie ogólnego poziomu bezpieczeństwa. System może być dostosowany do dowolnego środowiska, na przykład do obiektów związanych z handlem detalicznym, w których największy nacisk kładzie się na ochronę magazynów, jednak spełnia także inne, bardziej wyrafinowane wymagania pracowników ochrony odpowiedzialnych za stworzenie warunków do spokojnego życia i wydajnej pracy w chronionych środowiskach.

System Total Security Manager (TSM) umożliwia zarządzanie wieloma źródłami sygnału wizyjnego za pośrednictwem pojedynczej platformy, a także zarządzanie wieloma innymi systemami, przez co może ułatwić obsługę lokalnych stacji kontrolnych. Wyniki oceny ryzyka oraz incydenty wykryte dzięki inteligentnej analizie treści obrazów są prezentowane w postaci trójwymiarowych zobrazowań wygenerowanych dzięki technologii 3D Graphics Information System (GIS), tak by operatorzy mieli zapewniony natychmiastowy, czytelny wgląd w sytuację i mogli podejmować odpowiednie działania. Do systemu można wprowadzić wstępnie przygotowane scenariusze, co pozwoli operatorom na wykonywanie poleceń przygotowywanych na bieżąco, w miarę rozwoju wydarzeń, i przyczyni się do poprawy komunikacji i przyspieszenia reakcji służb ochrony.

Poniżej podaję kilka przykładów wykorzystania wyjątkowych właściwości systemu TSM, wykraczających poza oczekiwania związane z działaniem standardowego systemu zabezpieczającego.

Ochrona obszarów miejskich

Zarówno centralne części miast, jak i ich obrzeża mogą być bezpieczne dzięki przechwytywaniu i analizie obrazów telewizyjnych z takich obszarów, jak główne drogi, dzielnice mieszkaniowe, parki, obiekty powszechnie dostępne oraz środki transportu. Dzięki zdolności do jednoczesnego,

Fot. 1. Sieciowy rejestrator wizyjny z kompresją H.264

Fot. 2. Kamera sieciowa o rozdzielczości 1,3 megapiksela przystosowana do pracy w każdych warunkach pogodowych

automatycznego wykrywania wielu incydentów technologia Intelligent Video Analysis (IVA) pozwala na powiadamianie operatorów i funkcjonariuszy o takich wydarzeniach, jak gromadzenie się agresywnie nastawionego tłumu, nieprawidłowe parkowanie pojazdów itp. W celu poprawy wykrywalności incydentów i rozpoznawalności obiektów w każdych warunkach pogodowych i oświetleniowych możliwe jest jednoczesne wykorzystanie kamer sieciowych o wysokiej rozdzielczości (HD) oraz kamer termowizyjnych.

System wykrywający wypadki w tunelach

Technologia IVA może być wykorzystana do wykrywania nieprawidłowości podczas prowadzenia pojazdów, a także do wykrywania dymu i ognia w celu powiadamiania pracowników ochrony i służb ratowniczych o zaistniałych wypadkach. Pozwala to na automatyczne zatrzymanie ruchu lub wycofanie pojazdów z zagrożonego obszaru z wykorzystaniem znaków informacyjnych i ostrzegawczych, a także umożliwia natychmiastowe podjęcie akcji przez służby ratownicze. Wszystko to jest możliwe dzięki jasnym informacjom pochodzącym z kamer pracujących w systemie dozorowym, określającym rodzaj zaistniałego incydentu zanim służby ratownicze dotrą na miejsce wypadku. Dzięki zastosowaniu specyficznych algorytmów technologia IVA zapewnia skuteczne wykrywanie dymu i ognia, ciągłą analizę ruchu i wykrywanie wszelkich jego nieprawidłowości z uwzględnieniem takich czynników, jak prędkość ruchu, tworzenie się korków, nieprzestrzeganie kierunku ruchu, zachowanie pieszych na przejściach przez jezdnię, obecność obiektów, które spadły na jezdnię, itp.

Systemy ochrony obwodowej

W zaawansowanych bezobsługowych systemach zabezpieczeń, rozmieszczanych wzdłuż czegoś, co można nazwać bardzo długą granicą jakichś obszarów, mogą być wykorzystane kamery dzień/noc o bardzo dużym zasięgu oraz kamery termowizyjne połączone z robotami zabezpieczającymi oraz radarami naziemnymi celem pokrycia całego terenu. Skuteczny dozór w warunkach nocnych jest możliwy dzięki automatycznemu systemowi śledzenia obiektów na podstawie analizy obrazu z kamer termowizyjnych oraz kamer pracujących w widmie optycznym, zapewniających możliwość obserwacji na dystansie dochodzącym do dwóch kilometrów i zintegrowanych z systemem radarów naziemnych celem dokładnego określania lokalizacji obiektów.

Dysponujące sztuczną inteligencją roboty, które pracują w sieci teleinformatycznej, mogą wykrywać intruzów, działając synchronicznie z wieloma innymi urządzeniami detekcyjnymi, inteligentnymi kamerami i radarami, a następnie podejmować

Fot. 3. Kamera kopułowa PTZ o rozdzielczości 1,3 megapiksela

Fot. 4. Oprogramowanie sieciowe Samsung NET-i Ware

próbę fizycznego zatrzymania ich z użyciem broni nie stwarzającej śmiertelnego zagrożenia, na przykład za pomocą urządzeń akustycznych. Robot może pracować przez dwadzieścia cztery godziny na dobę w ekstremalnych warunkach pogodowych, a także w kompletnej ciemności.

Skalowalność rozwiązań

Jak już wspomniałem, Total Security Manager pracujący w sieci IP jest skalowalny. Umożliwia stworzenie systemu spełniającego aktualne wymagania użytkowników, a gdy wymagania te ulegną zmianie, może zostać rozbudowany. Na przykład, wykorzystując pojedynczy serwer, w standardowym systemie można zarządzać obrazami z 72 kanałów wizyjnych, przeglądać je i zapisywać. Taki system jest bardzo skuteczny w działaniu i tani w eksploatacji dzięki prostocie konstrukcji. Pozwala także na integrację analogowych kamer CCTV z urządzeniami sieciowymi w ramach tego samego serwera.

System TSM Professional umożliwia stworzenie platformy przydatnej do zarządzania średniej wielkości systemami zabezpieczającymi obsługiwanymi przez 16 użytkowników. Maksymalna liczba kanałów wejściowych utworzonych w ramach kilku serwerów nie może przekraczać 144. System TSM Professional pozwala operatorom na zarządzanie systemami o różnorodnym przeznaczeniu, zarówno najprostszymi, jak i zintegrowaną platformą wykorzystującą ścianę monitorów, opcję automatycznego rozpoznawania treści tablic rejestracyjnych (ANPR) czy identyfikacji pojazdów (VDS).

System TSM Enterprise daje możliwość nieograniczonej rozbudowy, co jest ważne na przykład w przypadku aplikacji obejmujących swoim zasięgiem tereny miejskie, a także umożliwia obsługę i integrację wydzielonych jednostek, co zwiększa bezpieczeństwo gromadzonych danych.

James Smith
Samsung Techwin Europe
Tłumaczenie: Redakcja

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.

RCP Master *PR602LCD*

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

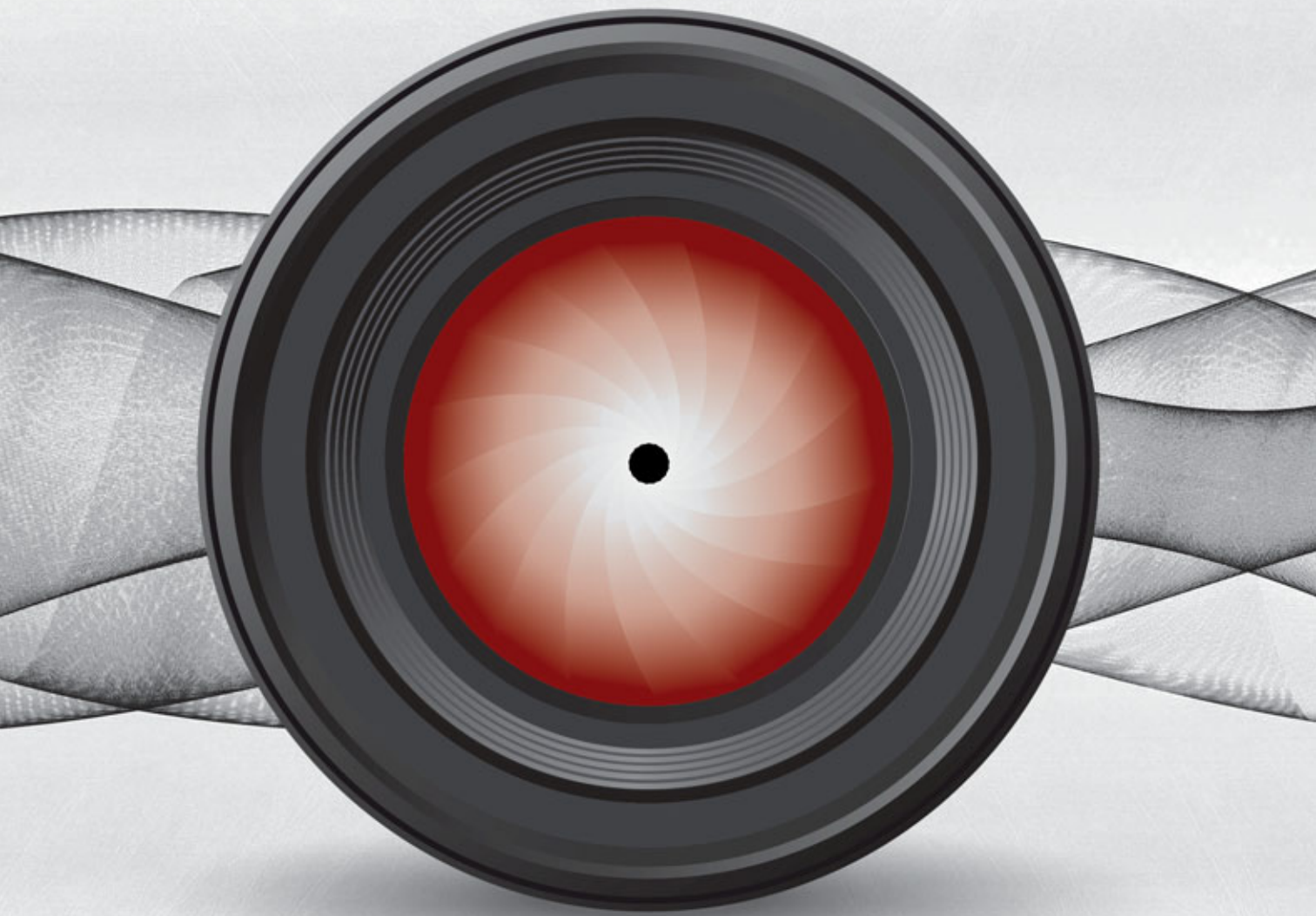
roger®

www.roger.pl

20 YEARS 1991-2011

Rozszerzono ofertę czytników EM 125 kHz serii PRTxxEM o modele **PRT32EM** i **PRT42EM**

Zagadnienia związane z regulacją przysłony



Andrzej Walczyk

Przysłona jako element przyrządów optycznych jest znana od ponad czterystu lat, od czasów Galileusza. Już pierwsi konstruktorzy lunet zauważyli, że użycie przysłony powoduje zmniejszenie jasności obrazu, jednak pozwala na poprawę jego ostrości i w efekcie może przynosić korzyści. Wprowadzanie stałych diafragm w prymitywnych obiektywach fotograficznych produkowanych na przełomie dziewiętnastego i dwudziestego wieku miało na celu zmniejszenie aberracji sferycznej i likwidację wewnętrznych odbić w układach optycznych. W efekcie następowała poprawa ostrości i kontrastu obrazu kosztem jego jasności. Tyle tytułem wstępu. Zastanówmy się nad wpływem przysłony na jakość obrazu uzyskiwanego we współczesnych kamerach telewizyjnych

Jak widać, przysłona jest elementem, który nie tylko reguluje ilość światła przepuszczanego przez obiektyw, lecz także ma wpływ na jakość uzyskiwanego obrazu. W przypadku współczesnych obiektywów, w których wykorzystywane są elementy asferyczne i niskodyspersyjne, sprawa nie jest tak prosta jak w przypadku archaicznych przyrządów optycznych z minionych epok, obarczonych silną aberracją sferyczną, w których zmniejszenie średnicy źrenicy wejściowej obiektywu zawsze powodowało poprawę jakości obrazu. Na rysunku 1 przedstawiony jest szkic układu optycznego obiektywu typu *Dagor*, używanego w aparatach wielkoformatowych, w którym na stałe wprowadzona jest przysłona zmniejszająca aberracje i w pewnym stopniu likwidująca wewnętrzne odbicia światła.

Obecnie stosowanie tak prostych środków nie wystarcza. Każdy ze współczesnych obiektywów ma określony optymalny zakres zmian przysłony, w którym jakość uzyskiwanego obrazu jest najlepsza, jednakże w większości przypadków użytkownik nie ma wpływu na ustawienie przysłony, gdyż robi to za niego układ automatycznej regulacji ekspozycji.

Chodzi przede wszystkim o regulację ekspozycji

Dla uściślenia pojęć zdefiniujmy parametr zwany ekspozycją, umownie rozumiany jako ilość światła padającego na przetwornik. Prawidłową wartość ekspozycji można ustalić po uwzględnieniu wszystkich czynników wpływających na pracę przetwornika obrazowego, z których najważniejszymi są:

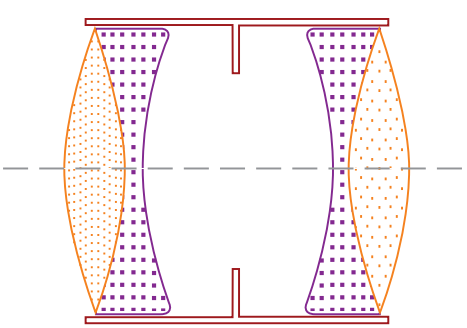
– poziom oświetlenia obserwowanej sceny,
– czułość kamery (w tym charakterystyka spektralna),
– aktualna, chwilowa wartość siły światła obiektywu, zależna od ustawienia przysłony,
– aktualna, chwilowa wartość czasu otwarcia migawki elektronicznej, nazywana także czasem ekspozycji.

Umowną jednostką ekspozycji jest EV, przy czym przyjmuje się, że dla danej kamery EV=0 oznacza prawidłową ekspozycję, pozwalającą na wytworzenie czytelnego obrazu o dobrej jakości.

Ekspozycja może być zbyt mała (wtedy przyjmuje wartości ujemne, a obraz jest niedoświetlony, czyli zbyt ciemny) lub zbyt duża (wtedy przyjmuje wartości dodatnie, a obraz jest prześwietlony, czyli zbyt jasny).

Przyjmuje się, że w warunkach stałego oświetlenia zmiana ekspozycji o jedną jednostkę EV jest równoznaczna z dwukrotną zmianą czasu naświetlania lub z przestawieniem przysłony o jedną umowną pozycję. Wyjaśniają to dane liczbowe umieszczone w tabelach 1, 2 i 3.

Jak łatwo zauważyć, wartości umieszczone w tabelach tylko w przybliżeniu tworzą ciągi geometryczne, jednakże w praktyce takie niewielkie odchyłki nie mają większego znaczenia,



Rys. 1. Szkic układu optycznego obiektywu typu Dagor

Wartość EV	Przysłona	Migawka
EV=3	F:2	T=1/60 s
EV=2	F:2,8	T=1/60 s
EV=1	F:4	T=1/60 s
EV=0	F:5,6	T=1/60 s
EV=-1	F:8	T=1/60 s
EV=-2	F:11	T=1/60 s
EV=-3	F:16	T=1/60 s

Tab. 1. Zmiany ekspozycji na skutek zmian przysłony

Wartość EV	Przysłona	Migawka
EV=3	F:5,6	T=1/8 s
EV=2	F:5,6	T=1/15 s
EV=1	F:5,6	T=1/30 s
EV=0	F:5,6	T=1/60 s
EV=-1	F:5,6	T=1/125 s
EV=-2	F:5,6	T=1/250 s
EV=-3	F:5,6	T=1/500 s

Tab. 2. Zmiany ekspozycji na skutek zmian czasu naświetlania

a ze względu na wygodę przyjęło się używanie przysłon i czasów otwarcia migawki o określonych wartościach.

Do poprawnej pracy kamery niezbędne jest utrzymanie ekspozycji w optymalnym zakresie, który jest relatywnie wąski. Cel ten realizują układy automatycznej regulacji przysłony i automatycznej regulacji czasu otwarcia migawki elektronicznej. Należy podkreślić, że taką samą ekspozycję można uzyskać przez zastosowanie nieskończonej liczby kombinacji różnych ustawień przysłony i migawki.

Przykładowo, przy założeniu, że poziom oświetlenia obserwowanej sceny jest stały, a kamera ma określoną czułość, tę samą wartość ekspozycji możemy uzyskać, stosując następujące ustawienia przysłony i migawki elektronicznej:

Wartość EV	Przysłona	Migawka
EV=0	F:16	T=1/8 s
EV=0	F:11	T=1/15 s
EV=0	F:8	T=1/30 s
EV=0	F:5,6	T=1/60 s
EV=0	F:4	T=1/125 s
EV=0	F:2,8	T=1/250 s
EV=0	F:2	T=1/500 s

Tab. 2. Stała ekspozycja pomimo zmian ustawienia przysłony i czasu naświetlania

Jak już wspomniałem, liczba możliwych kombinacji jest nieskończenie wielka. Dane zamieszczone w tabeli są jedynie poglądowe. Z punktu widzenia średniego poziomu jasności obrazu te ustawienia są równoważne. Czym będą różnić się naświetlone w ten sposób zdjęcia?

Fot. 1. Przysłona optymalna

Fot. 2. Przysłona niekorzystna

Podstawową, łatwo zauważalną różnicą będzie różnica w głębi ostrości. Obrazy powstałe przy całkowicie otwartym obiektywie będą odznaczać się małą głębią ostrości. Można będzie z łatwością zaobserwować, na który z planów nastawiona jest ostrość obiektywu. Obrazy powstałe przy mocno przysłoniętym obiektywie będą odznaczać się dużą głębią ostrości. Wszystkie plany będą robiły wrażenie jednakowo ostrych. Nie koncentrujmy się jednak zbytnio na zagadnieniu głębi ostrości, gdyż nie stanowi ono głównego tematu tego artykułu. Zastanówmy się nad rozdzielczością obrazu.

Należy pamiętać, że wszystkie te opisy mają charakter poglądowy i ich jedynym celem jest wyjaśnienie pewnych tendencji. W praktyce obiektywy o różnych konstrukcjach zachowają się nieco odmiennie, jednakże opisywane zjawiska fizyczne będą podobne.

Nie ma przy tym różnicy, czy mamy do czynienia z obiektywami fotograficznymi czy z obiektywami przeznaczonymi do współpracy z kamerami przemysłowymi, może za wyjątkiem problemów z dostępnością do szczegółowych danych technicznych. W przemyśle fotograficznym dokładna wartość rozdzielczości obiektywów jest jednym z istotniejszych elementów marketingowych i jest podawana w kartach katalogowych, zaś w przypadku telewizji dozorowej tego typu dane są trudno dostępne i przeważnie w ogóle nie są publikowane przez producentów.

Dokładna analiza rozdzielczości obrazów optycznych wytwarzanych przez obiektywy wykazuje, że zarówno w przypadku pełnego otwarcia przysłony, jak i w przypadku silnego przysłonięcia rozdzielczość obrazu jest gorsza niż wtedy, gdy zastosuje się pośrednie ustawienia przysłony. Czy jednak różnice są aż tak duże? Dane zaczerpnięte z kart katalogowych opisujących obiektyw fotograficzny firmy Olympus, którym zostały wykonane zaprezentowane zdjęcia testowe, są następujące:

Liczby zamieszczone w tabeli reprezentują umowny parametr oznaczany w literaturze mianem *lph*, określający rozdzielczość obiektywu wyrażoną liczbą poziomych linii, które można rozróżnić wzdłuż całej wysokości obrazu. Jak widać, w rogach obrazu rozdzielczość jest gorsza niż na jego środku i wykazuje niewielkie zmiany, zaś w centralnej części obrazu rozdzielczość jest lepsza, a różnice są wyraźniejsze, lecz nadal nie przekraczają one kilkunastu procent. Za optymalną należy uznać przysłonę F:8, przy której rozdzielczość utrzymuje się na najwyższym poziomie.

O wpływie tych parametrów na jakość obrazu można się przekonać, analizując załączone fotografie. Jedna z nich została wykonana z optymalną przysłoną F:8, druga – z niekorzystną przysłoną F:22.

Czy różnice między tymi obrazami są zauważalne? Czy gdyby nie podpisy pod zdjęciami w ogóle można byłoby zorientować się, który z nich jest który? Oczywiście w tym przypadku ocena jest bardzo subiektywna i nie może stanowić rzetelnego kryterium porównawczego, jednak daje pojęcie o skali zjawiska. Ocena przydatności obrazu dokonywana przez operatora obsługującego system monitoringu wizyjnego będzie równie subiektywna. Jedynym nasuwającym się wnioskiem jest to, że nie ma istotnych różnic w jakości tych obrazów.

Potraktujmy powyższe rozważania jako wstęp do właściwej części artykułu i przejdźmy do omówienia pewnych aspektów konstrukcji kamer przemysłowych i do sposobów regulacji ekspozycji obrazów. W przypadku starszych modeli kamer, pochodzących z lat osiemdziesiątych zeszłego stulecia, dominowała metoda regulacji przysłony o nazwie *Video-Iris.*

Przysłona	Środek obrazu, ogniskowa 14 mm	Brzeg obrazu, ogniskowa 14 mm	Środek obrazu, ogniskowa 25 mm	Brzeg obrazu, ogniskowa 25 mm	Środek obrazu, ogniskowa 54 mm	Brzeg obrazu, ogniskowa 54 mm
F:2,8	1600	1500	1600	1500	1600	1500
F:4	1700	1500	1700	1500	1700	1500
F:5,6	1700	1500	1700	1500	1700	1500
F:8	1800	1600	1700	1600	1700	1600
F:11	1700	1500	1700	1500	1600	1500
F:16	1600	1400	1600	1400	1500	1400
F:22	1600	1400	1600	1400	1500	1400

Obecnie metoda ta jest rzadko stosowana. Polega ona na tym, że do obiektywu doprowadzany jest odpowiednio spreparowany sygnał wizyjny (jest to klasyczny, zespolony sygnał wizyjny, z którego usunięto impulsy synchronizujące), zaś układy elektroniczne mierzą jego amplitudę i na tej podstawie dokonują modyfikacji ustawienia przysłony. Tak zbudowany układ automatycznej regulacji przysłony działa w pętli sprzężenia zwrotnego, przez co przysłona przyjmuje zawsze optymalne ustawienie i nadąża za zmianami jaskrawości obserwowanej sceny. Chwilowa wartość liczby przysłony nie jest znana, zresztą nikomu taka wiedza nie jest potrzebna, jedynym optymalizowanym parametrem jest wartość ekspozycji. Istotne jest to, że amplituda sygnału wizyjnego na wyjściu kamery zachowuje stałą wartość w szerokim zakresie zmian poziomu oświetlenia sceny obserwowanej przez kamerę, i to jest celem nadrzędnym wynikającym z regulacji przysłony.

Typowe kamery z przetwornikami CCD produkowane w latach osiemdziesiątych zeszłego stulecia nie dysponowały elektroniczną migawką i czas ekspozycji poszczególnych obrazów telewizyjnych był stały, przeważnie równy 1/50 sekundy. Ponadto z nie do końca zrozumiałych przyczyn kamery z tamtych lat miały bardzo wysoką czułość, przez co zakres regulacji przysłony musiał być bardzo szeroki, tak by kamery mogły pracować zarówno w warunkach nocnych, jak i w pełnym świetle słonecznym. Cała odpowiedzialność za zapewnienie prawidłowej ekspozycji obrazu spadała na obiektywy. Typowe wartości liczby przysłony mieściły się w granicach od F:1,2 do F:630. Konieczność silnego przysłaniania obiektywów stwarzała problemy konstrukcyjne, gdyż fizyczne rozmiary źrenicy wejściowej były bardzo małe. Konieczność precyzyjnej regulacji średnicy tak małych otworów zmuszała do stosowania równie precyzyjnych mechanizmów, a to wiązało się z wysokimi kosztami produkcji. Jakość obrazów uzyskiwanych w przypadku użycia obiektywów o takiej konstrukcji była niska, gdyż obiektywy te nie pracowały przy optymalnych wartościach liczby przysłony, zaś przysłowiowym gwoździem do trumny w sytuacji, w której średnica otworu w przysłonie była najmniejsza, były pierścienie dyfrakcyjne powstające w warunkach silnego oświetlenia.

Przełomem w konstrukcji kamer przemysłowych było wprowadzenie elektronicznej migawki, która stała się drugim (poza przysłoną) czynnikiem mającym wpływ na wartość ekspozycji. Powstały więc dwie pętle regulacyjne, których działanie nakładało się na siebie. W pewnych warunkach powodowało to niestabilność pracy kamer objawiającą się cyklicznym migotaniem obrazu. Zjawisko to zostało wyeliminowane przez wprowadzenie regulacji przysłony prądem stałym, określanej mianem *DC-Iris*. W tym przypadku decyzja co do optymalnego ustawienia przysłony zapada w kamerze, a nie w obiektywie, jak w przypadku metody Video-Iris. Ten sposób regulacji nie wykorzystuje zwykłej, prostej pętli sprzężenia zwrotnego, lecz stanowi rodzaj złożonego algorytmu regulującego jednocześnie dwa parametry.

Należy zwrócić uwagę na istotną cechę układu automatycznej regulacji ekspozycji metodą DC-Iris. W przypadku metody DC-Iris układy elektroniczne umieszczone w obiektywie pełnią rolę jedynie wykonawczą, a nie decyzyjną, dlatego za-

chodzi jednoznaczna zależność między chwilową wartością liczby przysłony a napięciem sterującym wytwarzanym w kamerze i doprowadzanym do obiektywu. Tak więc w systemie istnieje informacja na temat aktualnego ustawienia przysłony obiektywu. W tym sensie metoda DC-Iris niczym nie różni się od najnowszej, cyfrowej metody regulacji przysłony – P-Iris. Obie te metody różnią się jedynie sposobem, w jaki informacje z kamery są przekazywane do obiektywu, zaś pod względem funkcjonalnym są równoważne. Zaletą metody P-Iris jest jednoznaczność ustawienia przysłony, typowa dla wszystkich systemów sterowania cyfrowego. Wadą jest konieczność przystosowania kamer do praktycznej realizacji metody P-Iris, czyli obsługi obiektywów wykorzystujących taką metodę regulacji. Jak dotychczas żaden z wiodących producentów kamer nie podjął starań z tym związanych, tymczasem metoda P-Iris jest znana od 2009 roku i nic nie wskazuje na wzrost jej popularności. Za to wszystkie dostępne na współczesnym rynku kamery przemysłowe, zarówno analogowe jak i sieciowe, są przystosowane do regulacji przysłony obiektywów metodą DC-Iris.

Wśród argumentów mających świadczyć o dużej przydatności metody P-Iris wymieniana jest możliwość poprawy jakości obrazu przez wykorzystanie optymalnego zakresu przysłon obiektywu, jednakże metoda DC-Iris również umożliwia zrealizowanie takiej funkcji. Nie zależy to od sposobu transmisji danych sterujących z kamery do obiektywu, lecz od modyfikacji algorytmów dokonujących automatycznej regulacji ekspozycji obrazu. To, że uzyskiwany efekt jest niemal niezauważalny, sprawia jednak, że żaden z liczących się producentów kamer nawet nie wspomina o takiej możliwości. Tymczasem z materiałów marketingowych dotyczących metody P-Iris wynika, że jest to przełom na skalę światową, rewolucja w całej branży, dominujący trend i coś tam jeszcze.

Należy zwrócić uwagę na zmiany w konstrukcji kamer przemysłowych przeczące takiej argumentacji. Stosowanie elektronicznej migawki stało się zjawiskiem powszechnym, zaś dynamika tej regulacji na tyle wzrosła, że w prostszych modelach kamer w ogóle nie stosuje się regulacji przysłony. Pozwala to na bardzo znaczne zmniejszenie kosztów produkcji obiektywów. Zauważmy, że w większości współczesnych kamer możliwe jest skrócenie czasu ekspozycji do 1/100000 sekundy, czyli dynamika tej regulacji jest bardzo duża.

Tam, gdzie regulacja przysłony jest jednak konieczna, stosowane są obiektywy, których zakres regulacji jest znacznie zawężony w stosunku do rozwiązań sprzed kilkunastu lat. Chodzi o maksymalną wartość liczby przysłony, która we współczesnych konstrukcjach rzadko przekracza F:100. Tak więc niektóre aberracje wynikające z bardzo silnego przysłonięcia obiektywu w ogóle nie występują, zaś pogorszenie jakości obrazu wynikające z wpływu przysłony też jest nieznaczne.

Innym argumentem wymienianym przez entuzjastów metody P-Iris jest możliwość świadomej regulacji głębi ostrości obrazu przez operatora systemu, dzięki której można uzyskać obraz o wyższej rozróżnialności szczegółów. Taka argumentacja budzi bardzo poważne wątpliwości. Po pierwsze, większość współczesnych kamer jest zbudowana w oparciu o przetworniki CMOS o rozmiarach 1/3", 1/4" lub nawet mniejsze, w związku z czym standardowe obiektywy stanowiące wyposażenie takich kamer mają relatywnie krótkie ogniskowe, dzięki czemu zakres głębi ostrości jest bardzo duży i nie wymaga modyfikacji. W kamerach szybkoobrotowych, wykorzystujących obiektywy zmiennoogniskowe o relatywnie długiej ogniskowej powszechnie stosuje się automatyczną regulację ostrości zwaną *autofocusem*. Wąski zakres głębi ostrości może występować tylko przy najdłuższych ogniskowych, jednak wtedy operator systemu koncentruje swoją uwagę na powiększonym fragmencie sceny, która nie ma dużej rozpiętości – przeważnie widać jedną osobę lub jakiś przedmiot. We wszystkich tych przypadkach z pomocą przychodzi funkcja autofocus i nie występują żadne problemy z rozróżnialnością szczegółów.

Po drugie, czy istnieją takie platformy programowe obsługujące systemy monitoringu wizyjnego, które dysponują funkcją regulacji głębi ostrości? W zasadzie do czego ma służyć taka regulacja? Do zwiększania czy do zmniejszania zakresu głębi ostrości? Jaki jest cel takiego działania?

No i po trzecie, czy operator systemu dysponuje wiedzą i umiejętnościami pozwalającymi czerpać korzyści ze świadomego doboru zakresu głębi ostrości? Z pewnością nie. To jest umiejętność wykorzystywana w fotografii portretowej w celu stworzenia pewnego klimatu zdjęcia, a także w kinematografii, jako element narracji w sztuce filmowej (tak zwane prowadzenie ostrości mające koncentrować uwagę widza na określonych szczegółach), jednak jest to przysłowiowa wyższa szkoła jazdy dostępna wyłącznie dla osób biegłych sztuce, my tymczasem nie jesteśmy ani w studiu fotograficznym, ani na planie filmowym, tylko w pomieszczeniu ochrony i odpowiadamy za bezpieczeństwo obiektu. System monitoringu wizyjnego ma służyć za narzędzie pozwalające ocenić poziom zagrożenia w niebezpiecznych sytuacjach. W takich warunkach nikt nie będzie zastanawiał się nad głębią ostrości obrazów z kamer.

Zakładając, że taka świadoma regulacja głębi ostrości ma jednak jakiś sens, zastanówmy się nad możliwością praktycznej realizacji takiej funkcji. Jak już wyjaśniłem w pierwszej części artykułu, ekspozycja obrazu w danych warunkach obserwacyjnych musi być stała, tak więc aby zwiększyć lub zmniejszyć głębię ostrości, należy zmienić jednocześnie dwa parametry – średnicę przysłony i czas otwarcia migawki elektronicznej. Nie zawsze taka możliwość istnieje. Na przykład, w warunkach bardzo słabego oświetlenia, gdy przysłona obiektywu jest już całkowicie otwarta, a czas otwarcia migawki elektronicznej już dawno został wydłużony do 1/15 sekundy, zwiększenie zakresu głębi ostrości zmusi do dalszego przedłużenia czasu ekspozycji, co negatywnie odbije się na rozpoznawalności obiektów ruchomych. W przypadku pracy kamer w dobrych warunkach oświetleniowych zakres głębi ostrości jest szeroki z natury rzeczy, więc taka regulacja nie ma żadnego sensu.

Kończąc, należy podkreślić, że kamery i obiektywy umożliwiające praktyczną implementację metody P-Iris są dostępne jedynie u dwóch producentów sprzętu i nic nie wskazuje na to, że ta sytuacja ulegnie zmianie, tymczasem w przetargach pojawia się wymóg stosowania tej a nie innej metody regulacji przysłony, co eliminuje 95% konkurencji. Czy do tego ma służyć ta modyfikacja?

Andrzej Walczyk

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Megapikselowe kamery IP dzień/noc

Doskonała jakość obrazu, duża funkcjonalność!

Kamera standardowa

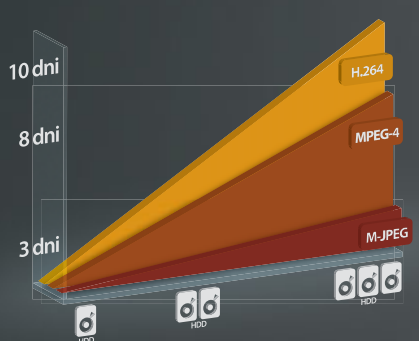
Megapikselowe kamery IP marki NOVUS

Rozdzielczość megapikselowa 2.0 Mpx

Pozwala na zapis nagrania w bardzo dobrej jakości, co umożliwia przybliżanie fragmentów obrazu i odczytanie najmniejszych szczegółów. Kamery o rozdzielczości 2.0 Mpx mogą obserwować obszar do 4.6x większy niż kamery o standardowej rozdzielczości 720x576. Można zatem przyjąć, że w niektórych sytuacjach, jedna kamera z przetwornikiem 2.0 Mpx odpowiada pięciu kamerom standardowym.

Praca w trybie trójstrumieniowym

Pozwala dopasować jakość i objętość transmitowanych danych do indywidualnych potrzeb użytkownika. Przykładowa konfiguracja strumieni wideo: ▪ pierwszy strumień wysokiej jakości i rozdzielczości do lokalnego monitoringu i rejestracji ▪ drugi strumień do podglądu obrazu przez internet ▪ trzeci strumień do transmisji przez sieć telefonii komórkowej (podgląd obrazu na telefonach i innych urządzeniach przenośnych).



Kompresja H.264

Zastosowanie najnowszej wydajniejszej kompresji H.264 pozwala, bez utraty jakości, zmniejszyć wielkość zapisywanego obrazu nawet o 80% w stosunku do kompresji M-JPEG i o ok. 20% w stosunku do MPEG-4. Dzięki temu, na dyskach o tej samej pojemności, można archiwizować znacznie większą ilość materiału.

T SERIA

NMS Compatible

ALNET Compatible

Oprogramowanie NMS do monitoringu wizyjnego IP w komplecie!

NVIP-TDN4401V/IR/MPX2.0

NVIP-TDN5401C/MPX2.0

- Mechaniczny filtr podczerwieni
- Maks. rozdzielczość przetwarzania wideo 1600 x 1200 (UXGA)
- 3 strefy prywatności
- Detekcja ruchu
- 1 wejście i 1 wyjście alarmowe
- Kontrola połączenia sieciowego oraz funkcja sprawdzania adresu IP
- Wparcie dla urządzeń mobilnych - strumień 3GPP
- Możliwość nagrywania na karty SD i serwery FTP
- Zasilanie: PoE (Power over Ethernet) lub 12 VDC (zasilacz sieciowy w zestawie)

NVIP-TDN5401C/MPX2.0

- Czułość: 0.5 lx/F=1.4
- Montaż obiektywu: CS

NVIP-TDN4401V/IR/MPX2.0

- Oświetlacz IR - 18 diod LED
- Wbudowany obiektyw f=2.7 ~ 9 mm
- Obudowa wandaloodporna, IP 66

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

Dzięki systemowi Nedap AEOS nareszcie można skutecznie zarządzać kontrolą lotniskowych gate'ów

Jakub Kozak

Na prośbę autora zastosowano oryginalne słownictwo związane z organizacją portu lotniczego.

Kontrola gate'ów odgrywa istotną rolę na każdym lotnisku. Dotychczas zarządzanie kontrolą gate'ów było zazwyczaj realizowane lokalnie, przy gate'cie. Nowy system pozwala zrobić to prościej i skuteczniej. Aplikacja kontroli gate'ów działa dzięki kontrolerowi bezpieczeństwa Nedap, który łączy wszystkie funkcje bezpieczeństwa, poprzednio wykonywane przez oddzielne systemy dedykowane. Tak zwany kontroler gate'ów łączy gate'y w sieć, która centralnie nadzoruje nastawy drzwi, z jednostką centralną, gdzie zainstalowano bazę danych, zawierającą dane osobowe i charakterystyki biometryczne personelu lotniska. Równocześnie kontroler realizuje zadanie lokalnego sterowania gate'em. Jest to rozwiązanie, które znakomicie usprawnia zarówno wydajność (przepustowość) gate'u, jak i bezpieczeństwo w jego obrębie

Na lotniskach europejskich kontrola gate'ów ma istotne znaczenie dla nadzorowania różnych uprawnień pasażerów pochodzących z krajów należących do układu Schengen oraz pozostałych pasażerów. Na większości lotnisk osoba odpowiedzialna za gate musi osobiście sprawdzić wszystkie wejścia za każdym razem, gdy samolot przybywa lub odlatuje. Ta osoba musi ręcznie skontrolować drzwi do każdego dokującego samolotu. Gate'y spełniają wiele funkcji i są używane do lotów zarówno do krajów układu Schengen, jak i do pozostałych. Z tego powodu dostęp przez gate musi być skonfigurowany tak, aby podróżni przylatujący byli odpowiednio oddzieleni od odlatujących. Najważniejszą kwestią jest absolutne zapewnienie, aby różne strumienie pasażerów przebiegały innymi trasami. Drzwi gate'ów są zwykle kontrolowane przy użyciu przepustek lub systemów klucza, niekiedy łącznie z urządzeniem technicznym, które zamyka lub otwiera drzwi. Wymaga to ręcznej interwencji wykonywanej pod nadzorem obecnego przy tym upoważnionego pracownika.

Kontroler gate'u

Wiele portów lotniczych przy współpracy z NEDAP sporządziło wykaz wymagań, mających na celu ułatwienie sprawdzania i jednoczesne zwiększenie bezpieczeństwa kontroli gate'ów. Z uwagi na zainwestowane już środki głównym celem było ponowne (w miarę możliwości) wykorzystanie istniejącego na lotnisku sprzętu. Zasadniczą zmianą wprowadzoną przez NEDAP było połączenie systemu sterującego z infrastrukturą sieciową. Wszystkie drzwi gate'ów można teraz monitorować online przez sieć. W tym rozwiązaniu podstawową rolę odgrywa kontroler gate'u, sprzęt obsługujący gate oraz drzwi podłączone do kontrolera. Programy sterujące drzwiami są zainstalowane w kontrolerach, jednak są też widoczne online na centralnym monitorze. Co więcej, system może odwoływać się do danych personalnych dotyczących podwykonawców, którzy mogą działać w porcie lotniczym zarówno lokalnie, jak i centralnie. Dane te obejmują przepustki wydane wymienionym wyżej osobom oraz ich parametry biometryczne. Kontroler gate'u łączy dane osobowe z przepustki, dane biometryczne osoby oraz kod (numer lotu) ze zdefiniowaną konfiguracją drzwi. Po wprowadzeniu prawidłowych danych ustawiana jest ustalona procedura dla gate'u.

Większe bezpieczeństwo

Weryfikacja tożsamości pracownika z wykorzystaniem danych biometrycznych minimalizuje ryzyko obsługi gate'u przez osoby nieuprawnione. Użycie kodów lub numerów lotów do automatycznego nastawiania prawidłowej konfiguracji drzwi zwiększa bezpieczeństwo oraz efektywność obsługi. Wprowadzenie kodu lub numerów lotu przez pracownika odbywa się lokalnie, ponieważ regularnie się zdarza, że samoloty muszą dokować przy innym gate'cie, co powoduje konieczność zmiany parametrów nastawy drzwi. Przekonfigurowane drzwi wysyłają sygnał zwrotny dla potwierdzenia przyjęcia nastawionej konfiguracji. Tylko wtedy może się rozpocząć ostatni etap boardingu pasażerów samolotu. Drzwi przy gate'cie są otwierane na zaprogramowany czas, a detektory ruchu sygnalizują ruch osób w gate'cie. Jeśli przez ustalony czas w gate'cie nie jest wykrywany ruch, drzwi gate'u automatycznie się zamykają. Oczywiście drzwi można zamknąć wcześniej (centralnie lub lokalnie).

Większa skuteczność

Wykorzystanie infrastruktury sieciowej oszczędza czas i umożliwia obsługę gate'ów przez mniejszą liczbę osób. Zmniejsza się także ryzyko popełnienia błędów, a możliwe błędy lub naruszenia są natychmiast sygnalizowane. Sieć pozwala na przejrzenie programów sterowania na każdym gate'cie i zapewnia zwartą kontrolę. Awaria sieci nie uniemożliwia wykonania programów, ponieważ działają one lokalnie. Jednak wprowadzenie zmian do programów sterujących odbywa się centralnie, jest ono bowiem szybsze i mniej skomplikowane niż zmiana wszystkich gate'ów na poziomie lokalnym. Łącze do systemu zarządzania personelem pozwala na bezpośredni dostęp kontrolera gate'u do danych osobowych personelu. Informacja przy gate'cie jest zawsze aktualna, ponieważ gdy personel odchodzi z firmy lub gdy upoważnienie danej osoby zostanie zawieszone, system jest natychmiast aktualizowany. Wszystkie zdarzenia odnoszące się do osób, obsługi gate'u i pozycji drzwi są zbierane i otrzymują wyraźne oznaczenie daty i czasu. System też może być tak ustawiony, że kombinacje zdarzeń powodują automatycznie podwyższenie stanu ostrzegania lub wygenerowanie alarmu. Dane zapisane w bazie danych mogą być łatwo przywołane dzięki funkcji wyszukiwania.

Identyfikacja wizualna

Niektóre porty lotnicze zwróciły uwagę na konieczność identyfikacji wizualnej podczas konfigurowania i obsługi gate'ów. Obrazy można skojarzyć z istniejącymi upoważnieniami poprzez przyłączenie kamery IP do kontrolera gate'u. Oznacza to na przykład, że gate może zostać dopuszczony do obsługi po zweryfikowaniu zdjęcia osoby z informacją zawartą w bazie danych. Dodatkową funkcją jest zapamiętanie zapisu wizyjnego razem z zarejestrowanymi zdarzeniami. Może być to szczególnie przydatne, gdy zdarzenia zostaną poddane późniejszej analizie. Wówczas zamiast szukać numerów identyfikatorów, można na odpowiednim zapisie wizyjnym natychmiast zobaczyć twarze osób biorących udział w zdarzeniu.

Zarządzanie Bezpieczeństwem w Porcie Lotniczym w Genewie, Szwajcaria (port lotniczy zabezpieczony systemami AEOS firmy Nedap)

Aéroport International de Genéve (w skrócie AIG) jest jednym z najdynamiczniejszych lotnisk w Europie.

Tylko w 2006 roku AIG obsłużył prawie 10 milionów pasażerów i 170 000 lotów – organizowanych przez 150 różnych linii lotniczych – do 100 portów. Oczywiście przy takich liczbach zapewnienie bezpieczeństwa jest nie lada wyzwaniem.

Zaimplementowany na terenie AIG system AEOS kontroluje dostęp dla 13 500 pracowników, zarządza 37 500 identyfikatorami, 60 sklepami i 150 organizacjami operującymi w obiektach lotniskowych. Zabezpieczenie i kontrolowanie takiego dynamicznego otoczenia wymaga elastycznego systemu kontroli dostępu, opartego na najnowszej technologii, która może spełnić współczesne oraz przyszłe wymagania polityki bezpieczeństwa.

AEOS

Dla AIG jedną z głównych przyczyn wyboru systemu AEOS firmy Nedap jako systemu zarządzania bezpieczeństwem była jego odmienna strukturalnie architektura oparta na modułach funkcjonalnych. Moduły funkcjonalne AEOS pozwalają systemowi wzmocnić politykę i procedury bezpieczeństwa lotniska, a dodatkowo zmiana wymagań lub procedur może być wdrożona znacznie łatwiej niż w systemach tradycyjnych

Rozmaite techniki kart i czytników w jednym systemie

W systemie kontroli dostępu AEOS w porcie lotniczym w Genewie stosowane są jednocześnie cztery różne techniki identyfikacji: Nedap, Mifare, Legic oraz karty magnetyczne, przy czym każda z technik służy innemu celowi. Na terenie portu wykorzystywana jest karta Nedap Combi, łącząca wszystkie stosowane rodzaje identyfikacji. Dzięki temu użytkownik nie musi nosić czterech różnych rodzajów kart.

Technologia Nedap jest stosowana do wygodnego dostępu typu *hands-free* – oferuje zasięg jednego metra w przypadku kontroli dostępu osób, a także kontroli wjazdu pojazdów przy użyciu czytnika Nedap TRANSIT identyfikującego pojazdy z odległości do dziesięciu metrów. W celu przesyłania danych stosuje się m.in. technikę Mifare, która pozwala na przykład na bezpieczne zapamiętywanie wzorców biometrycznych. Aby wykorzystać dotychczasowe inwestycje w obszarze kontroli dostępu, pozostawiono technologię Legic. Z kolei dla celów handlowych do karty Combi dodano pasek magnetyczny.

Zarządzanie wykonawcami, dostawcami i zezwoleniami

Większość pracowników AIG jest zatrudniona przez 150 przedsiębiorstw działających na terenie lotniska. Zarządzanie przepływem i prawami dostępu osób (wykonawców) pracujących dla tak dużej liczby firm zajmuje wiele czasu. Istotne jest również, aby przepływ wykonawców był oddzielony od przepływu pracowników AIG. Dla bezpieczeństwa lotniska ważne jest rozróżnienie praw dostępu oraz zdarzeń i alarmów generowanych w systemie kontroli dostępu dla każdej kategorii osób. Ponadto prawa dostępu dla wykonawców powinny być automatycznie blokowane po zakończeniu robót albo po wygaśnięciu zezwolenia na działalność.

Fakty i liczby dotyczące Międzynarodowego Portu Lotniczego w Genewie:
- 10 milionów pasażerów rocznie
- 170 000 lotów
- 150 organizacji i 60 sklepów
- 13 500 zatrudnionych (łącznie z podwykonawcami)
- 37 500 identyfikatorów
- 200 czytników Nedap (w najbliższej przyszłości rozbudowanych do 400)

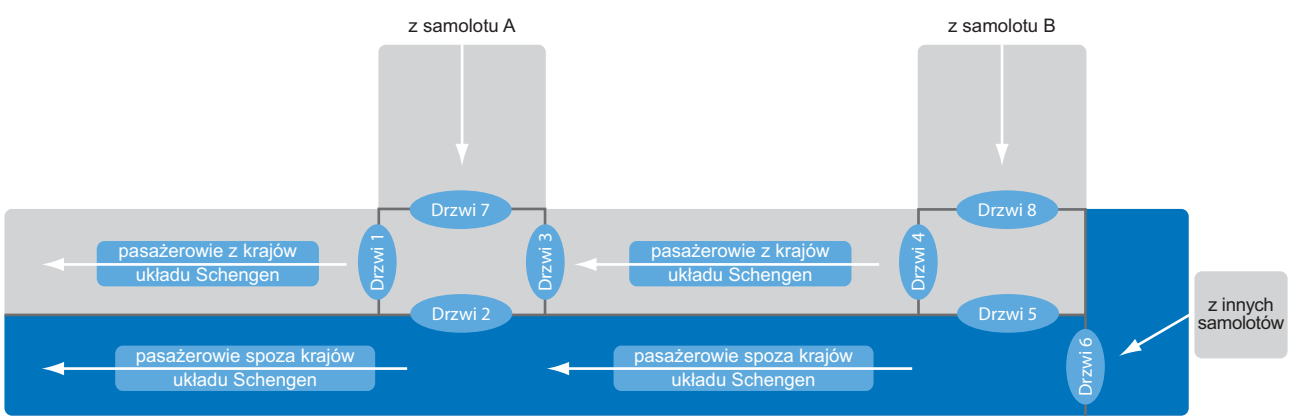
Problem ten rozwiązują właściwości oprogramowania AEOS dotyczące zarządzania wykonawcami, dostawcami i zezwoleniami. Zarządzanie wykonawcami odróżnia wykonawców od pracowników oraz od gości. Dane personalne podwykonawców są łączone z odpowiednimi informacjami o dostawcy i osobie kontaktowej, zazwyczaj pracowniku dostawcy. Zarządzanie dostawcami rejestruje stosowne dane dostawcy i łączy dostawcę z zezwoleniem. Zezwolenie określa, którzy dostawcy (i ilu) mogą pracować na jego podstawie, dla jakiego typu prac zostało wydane oraz jaki jest jego okres ważności. Po wygaśnięciu ważności zezwolenia wszystkie prawa dostępu podwykonawców są automatycznie blokowane.

Goście w Porcie Lotniczym w Genewie

W odniesieniu do gości prowadzona jest surowa polityka bezpieczeństwa. Nie mogą oni poruszać się swobodnie po całym obiekcie. Przez cały czas musi im towarzyszyć upoważniony pracownik, a dostęp przyznaje im się tylko do określonych obszarów, i to jedynie w obecności pracownika. Gościom towarzyszyć może tylko wybrana grupa pracowników. Ta polityka bezpieczeństwa jest wymuszana przez zasadę czworga oczu, która oznacza, że identyfikator gościa zostanie zaakceptowany tylko wtedy, gdy na tym samym czytniku w zadanym przedziale czasowym zostanie odczytany identyfikator pracownika. Dzięki modułom funkcjonalnym AEOS ta polityka bezpieczeństwa mogła zostać łatwo wdrożona. AEOS weryfikuje upoważnienie udzielone gościowi i sprawdza, czy pracownik jest upoważniony do prowadzenia gościa. Po spełnieniu obu tych warunków pracownik i gość uzyskują dostęp.

Rozległy monitoring

W zależności od rodzaju obszaru lub strefy zaplecza na AIG stosuje się różne poziomy zabezpieczeń. Niektóre ze



Rys. 1. Oddzielenie strumienia pasażerów z krajów układu Schengen od strumienia pozostałych pasażerów przy wykorzystaniu kontrolera gate'ów NEDAP

stref mają wysoki poziom zabezpieczeń i służbę operującą w trybie 24/7. Jeśli ktokolwiek życzy sobie wstępu do takiej strefy, musi przedstawić swój identyfikator w odpowiednim czytniku na stanowisku ochrony. Gdy AEOS zweryfikuje ważność upoważnienia, wyświetlacz nad stanowiskiem wskazuje, czy danej osobie udzielono czy też odmówiono wstępu. Równocześnie pracownik ochrony monitoruje przez AEOS dane tej osoby, jej zdjęcie i ważność upoważnienia, sprawdzając, czy dana osoba jest rzeczywiście prawnym posiadaczem tego identyfikatora. Funkcja oceny zdarzeń fotograficznych AEOS natychmiast dostarcza pracownikowi ochrony pozostałych informacji związanych z daną osobą, takich jak nazwisko, wydział, numer identyfikacyjny, przyczyny nieupoważnienia itp.

Jako element polityki bezpieczeństwa pracownicy, podwykonawcy i goście muszą przez cały czas nosić swoje identyfikatory w widocznym miejscu. Dla celów identyfikacji wzrokowej i określenia uprawnień identyfikatory są w różnych kolorach – w ten sposób informują pracowników ochrony o obszarach, do których te osoby mają dostęp. Za pomocą ręcznych skanerów Nedap GPRS patrolujący pracownicy ochrony mogą odczytać identyfikator danej osoby, zweryfikować jego ważność i odczytać ostatnie ruchy tej osoby.

Międzynarodowe Lotnisko Weeze w Niemczech

W ramach systemu AEOS międzynarodowe lotnisko Weeze zainstalowało specjalny mechanizm monitorowania wyjść oraz wdrożyło nową funkcję systemu kontroli dostępu AEOS, która osobom nieupoważnionym uniemożliwia wejście do chronionej części lotniska.

Zarząd lotniska Weeze wspólnie z Nedap znalazł również rozwiązanie problemu, z którym muszą sobie radzić niemal wszystkie lotniska, a mianowicie: w jaki sposób osobom nieupoważnionym uniemożliwić dostęp do chronionej części lotniska. Tak samo jak na każdym innym lotnisku, pasażerowie na lotnisku Weeze opuszczają tę część przez ruchome drzwi, umieszczone za salą, w której zgłaszają przewożone towary do oclenia. Takie przesuwne drzwi bez przerwy się otwierają i zamykają, co osobom znajdującym się w niechronionej części lotniska umożliwia swobodne wejście do jego chronionej części. Stwarza to potencjalne zagrożenie dla bezpieczeństwa obiektu.

Problem ten został rozwiązany przez niemieckiego partnera spółki Nedap – GST, która nad drzwiami przesuwnymi zamontowała czujkę radarową kontrolującą kierunek ruchu w tym obszarze. Ta czujka wykrywa, gdy ktoś wchodzi do nadzorowanego obszaru z przeciwnego kierunku. Wtedy w sterowni automatycznie uruchamia się interfejs AEOS, przekazujący nagrania wizyjne na żywo za pośrednictwem serwera FTP. Czujka ruchu działa także w sytuacji, kiedy kilka osób jednocześnie przechodzi we właściwym kierunku, a jedna osoba próbuje w tym samym czasie przejść z niechronionej do chronionej części lotniska.

Jakub Kozak
Country Manager Poland
Nedap Security Management, biuro w Polsce

KaDe Premium
czyli wersja zaawansowana

Ryszard Sobierski

W jednym z poprzednich numerów *Zabezpieczeń* opisany został system KaDe V1. Jest to wersja podstawowa, bazująca na zintegrowanych kontrolerach typu KZ-1000. Pora przedstawić wersję zaawansowaną, czyli KaDe Premium

Bardzo popularna, zwłaszcza w systemach telewizji dozorowej, technologia IP wkracza również do innych systemów zabezpieczeń elektronicznych. W przypadku systemów kontroli dostępu to rozwiązanie jest znane i stosowane od wielu lat, jednak dotychczas komunikacja za pośrednictwem sieci LAN/WAN pomiędzy serwerem z programem nadzorczym systemu kontroli dostępu a sterownikami drzwi (kontrolerami) była zarezerwowana dla systemów bardzo zaawansowanych i rozległych. Kontrolery KD z portami IP były stosunkowo drogie. Wraz ze spadkiem cen komponentów, popularyzacją tego typu rozwiązań oraz wzrostem podaży możliwe stało się zastosowanie technologii IP również w sterownikach KD przeznaczonych do mniejszych systemów. Wykorzystanie tej technologii w systemach kontroli dostępu polega na użyciu kontrolerów z wbudowanymi portami IP. Oczywiście możliwe jest również rozwiązanie polegające na wykorzystaniu niezależnych konwerterów IP/RS485, do których podłączamy „tradycyjne" kontrolery z portami RS485. Wówczas cała magistrala jest„widziana" przez program nadzorczy pod jednym adresem IP należącym do konwertera. Opisany w niniejszym

artykule system KaDe Premium oferuje wszystkie dostępne warianty komunikacji kontrolerów z serwerem KD.

Elementy systemu – program nadzorczy KaDe Premium

Program nadzorczy KaDe Premium jest przeznaczony do współpracy ze standardowymi kontrolerami typu KS-1012-RS, KS-1012-IP, KS-1024-RS, KS-1024-IP. KaDe Premium spełnia wszystkie funkcje programu KaDe-Soft-V1 oraz kilka nowych, które zostaną opisane w dalszej części artykułu.

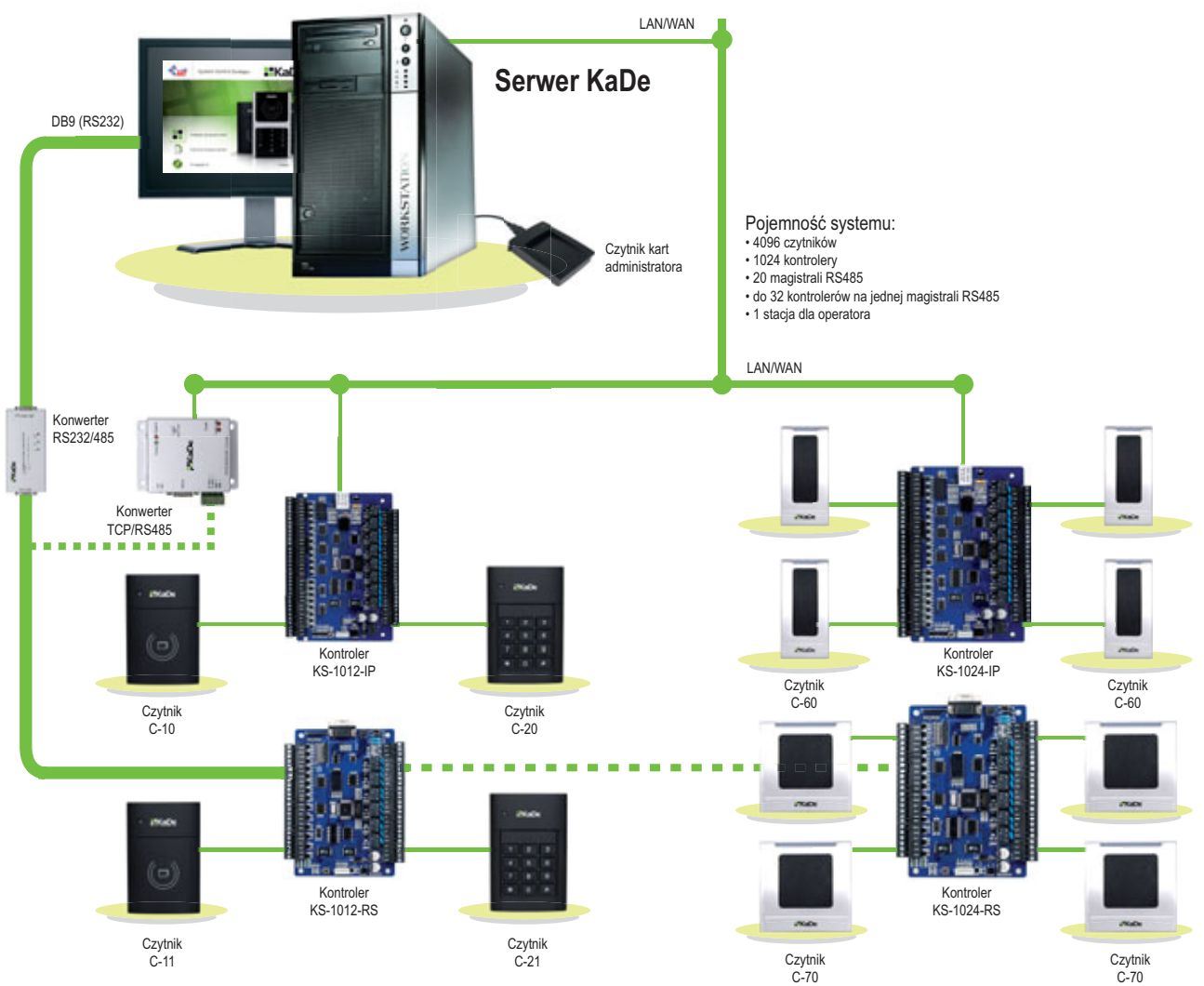
Program jest bardzo prosty w instalacji i ma wygodny dla operatora interfejs graficzny. Na uwagę zasługują zwłaszcza wyświetlane okna „Dynamicznej pomocy", czyli podręcznej instrukcji. Po kliknięciu na dowolne pole w oknie pulpitu wyświetlany jest opis wybranej pozycji i metoda definiowania lub konfiguracji danego elementu systemu.

Program nadzorczy KaDe Premium jest przeznaczony do stosowania w małych i średnich systemach kontroli dostępu. Interfejs operatora, podobnie jak w przypadku programu KaDe-Soft-V1, umożliwia również:

– konfigurację parametrów fizycznych elementów systemu,
– definiowanie elementów logicznych,
– monitorowanie stanu systemu „na żywo" dzięki graficznym mapom obiektów, zdjęciom, obrazom z kamer i komunikatom,
– wyświetlanie zdjęć przygotowanych przez użytkownika w przypadku użycia karty w czytniku,
– integrację z systemem CCTV poprzez użycie wizyjnej karty przechwytującej (wbudowanej w PC) lub rejestratora DVR i kamer logicznie przypisanych do kontrolowanych przejść,
– generowanie filtrowanych raportów zdarzeń i zapis w formacie *.xls.

W przypadku integracji z rejestratorem DVR podczas przeglądania raportów zdarzeń lub alarmów z trybu online w okienku wizyjnym wyświetlane jest jednominutowe nagranie z kamery przypisanej do elementu systemu. Plik wizyjny jest pobierany z archiwum rejestratora. W przypadku integracji z wizyjną kartą przechwytującą w archiwum znajdującym się w komputerze zapisywane jest pojedyncze zdjęcie z przypisanej kamery wykonane w chwili zaistnienia zdarzenia.

Program KaDe Premium oferuje szereg funkcji, opisanych szczegółowo w instrukcji dla operatora, które umożliwiają spełnienie różnych nietypowych wymagań administratora systemu, np. dostęp po użyciu dwóch, trzech lub czterech kart, pierwsze otwarcie kontrolowanego przejścia przez tzw. pierwszą kartę ze specjalnymi uprawnieniami czy dostęp po potwierdzeniu przez operatora. Omawiane oprogramowanie oferuje więcej trybów identyfikacji



Rys. 1. Schemat blokowy systemu KaDe Premium

użytkownika niż wersja KaDe V1, mianowicie tryby, w których potrzebne są:
– karta,
– kod PIN,
– karta lub kod PIN,
– karta i kod PIN.

Struktura systemu jest pokazana na załączonym schemacie blokowym.

Elementy systemu – standardowe kontrolery KS-1012-RS, KS-1012-IP, KS-1024-RS, KS-1024-IP

W standardowych kontrolerach (w odróżnieniu od kontrolerów zintegrowanych) moduł elektroniki sterownika jest oddzielnym elementem przystosowanym do zamontowania wewnątrz dedykowanej metalowej obudowy zasilacza buforowego. Do tak zamontowanego urządzenia podłączamy pozostałe akcesoria związane z kontrolowanym przejściem, czyli czytniki, zamki elektryczne, czujniki stanu drzwi oraz przyciski wyjścia. Standardowy kontroler powinien zostać umieszczony wewnątrz zabezpieczanej strefy. Dzięki temu można uzyskać większe bezpieczeństwo systemu niż w przypadku zastosowania kontrolerów zintegrowanych. Standardowe kontrolery są znacznie bardziej elastyczne niż kontrolery zintegrowane, chociażby ze względu na rodzaje czytników, jakie można do nich podłączyć. Czytniki mogą wykorzystywać dowolną technologię (również biometryczną) pod warunkiem, że posiadają interfejs Wieganda o długości kodu mieszczącej się w granicach 26–40 bitów.

Standardowe kontrolery typu KS-1012-RS, KS-1012-IP, KS-1024-RS i KS-1024-IP (4 modele) są przeznaczone do budowy systemów kontroli dostępu współpracujących z programem nadzorczym KaDe Premium.

W zależności od wybranego modelu kontroler może obsługiwać:
– jedne drzwi dwustronnie lub dwoje drzwi jednostronnie (KS-1012-RS, KS-1012-IP),
– dwoje drzwi dwustronnie lub czworo drzwi jednostronnie (KS-1024-RS, KS-1024-IP).

Modele KS-1012-RS i KS-1024-RS maja wbudowane przełączalne porty RS232/RS485. Modele KS-1012-IP i KS-1024-IP mają wbudowane porty IP.

Magistrale kontrolerów wykorzystujące protokół RS485 mogą pracować pod kontrolą programu nadzorczego na komputerze, jeśli zostaną połączone z tym komputerem poprzez konwerter na RS232 lub TCP. Program może obsłużyć do 20 magistral, a do każdej z nich mogą być podłączone 32 kontrolery. Modele kontrolerów z portem IP mogą komunikować się bezpośrednio poprzez sieć Ethernet. System może zawierać maksymalnie 1024 kontrolery, czyli w przypadku kontrolerów czterodrzwiowych może jednostronnie kontrolować 4096 przejść.

Fot. 1. Kontroler w obudowie zasilacza buforowego

Z ważniejszych funkcji, które pojawiły się w wersji KaDe Premium, należy wymienić:
– możliwość konfiguracji własnego formatu Wieganda z długością kodu mieszczącą się w przedziale 26–40 bitów (np. dla czytników HID),
– włączanie sekwencyjnego trybu pracy wybranego czytnika (po włączeniu tego trybu odczyt ważnej karty powoduje trwałe odryglowanie lub zaryglowanie drzwi),
– zdefiniowanie jednej lub dwóch grup czytników w ramach każdego kontrolera, które stworzą śluzę.

Oprócz wejść linii dozorowych, które są przeznaczone do podłączenia czujników stanu drzwi i przycisków wyjścia, kontrolery standardowe mają również po cztery linie dozorowe do ogólnego zastosowania. Można do nich podłączyć np. czujki ruchu i monitorować ich stan na mapie. Podobnie jest z wyjściami sterującymi kontrolera. Do każdego przejścia przypisane są domyślnie dwa przekaźniki – jeden do sterowania zamkiem elektrycznym, a drugi do sygnalizacji alarmowej. Oprócz tego każdy model kontrolera jest wyposażony w gniazdo do podłączenia modułu z czterema przekaźnikami (AL-1004). Przekaźniki te mogą być przełączane w chwili wystąpienia stanu alarmowego na jednej z linii dozorowych lub w chwili wystąpienia określonych zdarzeń.

Elementy systemu – czytniki

Serię czytników zbliżeniowych KaDe-C-XX współpracujących z kartami Unique uzupełniają analogiczne modele współpracujące z kartami Mifare. Są to następujące modele:
– C-11,
– C-21 (z klawiaturą).

Parametry elektryczne i środowiskowe są podobne do tych w czytnikach C-10 i C-20. Różnice sprowadzają się do rodzaju odczytywanych kart.

Na uwagę zasługuje model C-21, który ma możliwość przełączania formatu wyjściowego Wieganda dla kart i kodów PIN. Możliwe jest niezależne ustawienie jednego z dwóch formatów dla kart (26 lub 34 bitów Wiegand) oraz jednego z dwóch formatów dla klawiatury (4 lub 8 bitów). Dzięki temu można podłączyć ten czytnik do kontrolerów różnych producentów (np. Kantech, RBH).

Grupę czytników kart Mifare uzupełnia czytnik administratora C-ADM-M, który umożliwia szybkie wczytywanie 32-bitowych numerów kart.

Podsumowując powyższy opis, polecam ten system firmom instalacyjnym i klientom, którzy szukają prostego i taniego systemu kontroli dostępu. Zachęcam również do odwiedzenia naszej strony *www.aat.pl*, gdzie w sekcji KD dostępne są bezpłatne, pełne wersje instalacyjne obu programów KaDe oraz ich dokumentacja.

W kolejnym artykule opiszę integrację systemu KaDe z systemem RCP. Będzie w nim mowa o terminalach RCP (również biometrycznych) oraz profesjonalnym programie do rozliczania czasu pracy.

Ryszard Sobierski
Dział Kontroli Dostępu
AAT Holding

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Szybkoobrotowe kamery IP dzień/noc

Perfekcyjna jakość obrazu, szeroki zakres zastosowań!

Kompatybilne z oprogramowaniem NMS

Wraz z kamerą dostarczane jest w pełni funkcjonalne oprogramowanie NMS do zbudowania systemu monitoringu wizyjnego IP. W odróżnieniu od innych programów, bezpłatna licencja umożliwia podłączenie dowolnej liczby kamer IP oraz nie ma limitu przestrzeni do nagrywania. Nowoczesne i funkcjonalne oprogramowanie NMS o architekturze serwer - klient umożliwia m.in. rejestrację strumieni, odtwarzanie zarejestrowanego materiału, tworzenie map obiektów, sterowanie kamerami obrotowymi za pomocą myszki lub klawiatury z dżojstikiem.

Standardowa rozdzielczość HD 1080p

Obraz w wysokiej rozdzielczości

Kamery NVIP-1SD6118SD i NVIP-2DN6010SD posiadają megapikselowe przetworniki obrazu. Dzięki temu mogą generować strumień wideo H.264 w jakości HD (odpowiednio 1080p i 720p w zależności od modelu). Panoramiczny obraz uzyskiwany z tych kamer ma w przybliżeniu 2 lub nawet 5 razy więcej pikseli niż kamera standardowej rozdzielczości, a co za tym idzie, umożliwia odwzorowanie znacznie większej liczby detali obserwowanej sceny.

Kompaktowa konstrukcja

Kamery zintegrowane są z metalową obudową z kloszem akrylowym. Uchwyt ścienny i osłona przeciwsłoneczna dostarczane są w komplecie. Wszystkie elementy potrzebne do zainstalowania punktu kamerowego znajdują się w zestawie. Opcjonalnie dostępne są adaptery umożliwiające instalację kamery na suficie, na rogu budynku lub na słupie.

NMS Compatible

ALNET Compatible

Oprogramowanie NMS do monitoringu wizyjnego IP w komplecie!

NVIP-DN6137SD
- Rozdzielczość przetwornika: 680 TVL
- Czułość: 0.06 lx/F=1.6
- Zoom: 37 x optyczny
- Rozdzielczość przetwarzania wideo: 720 x 576
- 127 presetów
- Szeroki zakres dynamiki (WDR)

NVIP-1DN6118SD
- Rozdzielczość przetwornika: 1.3 Mpx
- Czułość: 0.02 lx/F=1.6
- Zoom: 18 x optyczny
- Rozdzielczość przetwarzania wideo: 1280 x 960
- 98 presetów
- Szeroki zakres dynamiki (WDR)

NVIP-2DN6010SD
- Rozdzielczość przetwornika: 2.0 Mpx
- Czułość: 1 lx/F=1.8
- Zoom: 10 x optyczny
- Rozdzielczość przetwarzania wideo: 1920 x 1080
- 128 presetów

■ Mechaniczny filtr podczerwieni ■ Typ obiektywu: motor-zoom z automatyczną przysłoną i ostrością ■ 8 patroli (20 akcji na patrol), 8 tras automatycznego skanowania, 4 trasy obserwacji (do 1200 poleceń) ■ Praca w trybie dwustrumieniowym - możliwość definiowania kompresji, rozdzielczości, prędkości i jakości dla każdego strumienia ■ Sprzętowa detekcja ruchu ■ Możliwość sterowania i konfiguracji bezpośrednio przez stronę www oraz z programu NMS ■ Klasa szczelności: IP 67 ■ Zasilanie: 12 VDC

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

Historia z przyszłością

Opowiadanie nie-*science-fiction*

(część 3)

Grzegorz Ćwiek

Rok 2211. Zebranie sił prewencyjnych międzygalaktycznej straży pożarnej. Po krótkim raporcie w sali zebrań uczestnicy spotkania udali się na przerwę. Sytuacja jest poważna. Od pięciu lunarmiesięcy w gwiazdozbiorze S-1 można zaobserwować niezwykłe anomalie magnetyczne mające istotny wpływ na komunikację nie tylko pomiędzy odległymi planetami, ale także między stacjami kosmicznymi rozlokowanymi w niedalekiej odległości. Służby międzyplanetarnej straży pożarnej odnotowały przybierające na sile, poważne zaburzenia ciągłości komunikacji. Powstało duże zagrożenie dla wszystkich ludzi i humanodroidów, których los już od wielu miesięcy spoczywa w rękach grupy ekspertów zajmujących się tym problemem

Po kilku lunarmiesiącach głębokich analiz, dzięki wnikliwemu studiowaniu historii ludzkiej cywilizacji, rozwoju i ewolucji technologii, młody kapitan międzygalaktycznej straży pożarnej odnalazł klucz do rozwiązania problemu bezpieczeństwa międzygwiezdnego. W starych notatkach swojego pradziadka odnalazł fragmenty opisu niezwykle zaawansowanego jak na owe czasy systemu bezpieczeństwa pożarowego Integral IP, który – poprzez analogię – wskazał młodemu kapitanowi najlepszą drogę do rozwiązania aktualnych problemów. Pozostało już tylko przekonać wyższe dowództwo oraz radę mędrców. Młody kapitan, pełen optymizmu i zapału, obawiał się jednej przeszkody, bez pokonania której cała operacja nie mogła się udać. Chodziło o pieniądze. Mimo upływu równo dwustu lat od czasu, gdy system Integral IP był instalowany na Ziemi, ani ludzie, ani humanodroidy nie znaleźli innego sposobu na finansowanie swoich przedsięwzięć. Co więcej, rasa ludzka, która przeżyła już okres świetności i powszechnego użycia drogocennych kamieni i kruszców jako środków płatniczych, a potem walut (takich jak amerykański dolar czy unijne euro), chciała dokonać wielkiej zmiany, ale inne, nowoodkryte rasy w międzyczasie uznały pieniądz za wynalazek przełomowy i konieczny do wspólnego wykorzystania we wszystkich galaktykach. Po rozpadzie Unii Europejskiej w roku 2015 i kolejnym wielkim kryzysie paliwowym w roku 2032, który na zawsze zakończył erę pojazdów napędzanych paliwami ropopochodnymi, ludzkość wybrała nowy środek płatniczy. Miało to związek z wynalezieniem rok wcześniej przez zdolnego, młodego naukowca z Polski nowego rodzaju paliwa i napędu hybrytronowo-antygrawitymowego, umożliwiającego podróżowanie poza Układ Słoneczny i szerokie wykorzystywanie przestrzeni międzymaterii do transmisji teleportacyjnych.

Ów nowy środek płatniczy tylko przez chwilę dawał nadzieję na to, że chciwość, nieuczciwość i oszustwa finansowe odejdą w zapomnienie, ale niestety ludzka natura, a jak okazało się później nie tylko ludzka, nie dały szans nowemu rozwiązaniu.

Kiedy w roku 2011, na Ziemi, przodkowie młodego kapitana cieszyli się zbliżającymi się mistrzostwami Europy w piłce nożnej Euro 2012, mającymi po raz pierwszy odbyć się w Polsce, nie przypuszczali, że wydarzenia bieżących i najbliższych miesięcy tak bardzo zmienią oblicze ich planety.

Młody kapitan międzygalaktycznej straży pożarnej dobrze wiedział o tamtych wydarzeniach. Przeczytawszy zapiski historyczne i notatki swoich przodków, doskonale przeanalizował wszystkie zdarzenia, jakie wpłynęły na późniejszy rozwój wypadków. Pierwszym sygnałem, który zignorowali jego przodkowie, były problemy z budową autostrady A2, która miała łączyć stolicę Polski z zachodnimi sąsiadami. Nieodpowiednie prawo, ignorancja urzędników i stosowana powszechnie w przetargach zasada „100% cena" spowodowały dramatyczne obniżenie jakości wszelkich usług na rynku. Wielka impreza sportowa, której oczekiwano z taką nadzieją, omal nie została przeniesiona do innych krajów z powodu błędów podczas tworzenia najważniejszych obiektów infrastruktury sportowej i drogowej, chciwości i nieuczciwości niektórych wykonawców, którzy za wszelką cenę chcieli zarobić jak najwięcej, nie bacząc na kiepską jakość swojej pracy i nierzetelność.

W przerwie posiedzenia młody kapitan dużo rozmyślał nad pracą, jaką wykonał do tej pory, wertując tysiące stron dokumentacji i zapisków z przeszłości. Teraz przedstawił swoją koncepcję dowództwu, wskazał możliwe rozwiązania, ale martwił się, czy nie okaże się znowu, że ze zdrowym rozsądkiem, profesjonalizmem i rzetelnością, na jaką wskazywało rozwiązanie zaczerpnięte z topologii Integrala IP i filozofii Schrack Seconet, wygra chęć ograniczenia wydatków na bezpieczeństwo i „łatania dziur" rozwiązaniami, których wykorzystanie jest po prostu czystą stratą czasu i pieniędzy.

Ileż przykładów z tamtego okresu wskazywało na zmarnowane szanse i porażki wykonawców obiektów, dróg czy wreszcie systemów bezpieczeństwa.

Tysiące uczciwych projektantów, specjalistów branżowych, pracowało nad dobrymi koncepcjami, rzetelnymi rozwiązaniami, projektami, a wykonywane na końcu prace nawet w kilku procentach nie odzwierciedlały ich kunsztu. Cena, cena, cena… Taniej, taniej, taniej… Zamienić, zamienić, zamienić!... Niech to szlag… Oby teraz było inaczej.

– *Panie kapitanie?*

– *Tak generale?*

– *Przepraszam, że przeszkadzam w przerwie. Wiem, że zostało nam jeszcze ponad pół lunargodziny na odpoczynek, ale trapi mnie kilka przemyśleń i chyba nie chciałbym o tym rozmawiać na forum. Czy mogę być z panem szczery?*

– Oczywiście. Ja także nie mogę oderwać myśli od tego Integrala…

– Ta firma… Schrack Seconet. Pan wie, że to właśnie ona wchłonęła wszystkie inne korporacje z branży bezpieczeństwa i po powstaniu Unii Międzygalaktycznej to jej następczynię mianowano jedynym dostawcą i producentem wszelkich droidów ratunkowych, robotów gaśniczych i całego sprzętu ratunkowego, jakim dziś dysponujemy.

– Tak. Oni pierwsi wpadli na to, jak ze zwykłych czujek dymu przejść do ultranowoczesnych multisensorów, takich jak CUBUS MTD 533. W pewnym momencie Integrale zamienili na...

– Tak, tak. Ta wiedza nie jest powszechnie znana, tym bardziej, że niektórym to przeszkadzało i Unia wolała nie drażnić innych swoich członków. Dlatego zabroniła używania powszechnie nazwy firmy. Nie dziwię się. W tamtych czasach jej konkurenci dysponowali dużo większymi organizacjami, bogatszymi i transnarodowymi kapitałami zaangażowanymi w działalność, a mimo to nie umieli stworzyć produktów przełomowych.

– Do czego pan zmierza generale?

– Jeżeli rada mędrców Unii dowie się o naszym planie i koncepcji wyjścia z trudnej sytuacji, zarówno marka Schrack Seconet, jak i system Integral IP staną się znowu głośne, jak dwieście lat temu w Europie. W obliczu dzisiejszego zakazu używania nazw własnych, międzygalaktycznych sporów z tym związanych… Hmm, przecież rasa tych dziwolągów z gwiazdozbioru Brobischa od dawna zabiegała o zmiany w tym zakresie… Czy nie uważa pan tego za zbyt ryzykowne? Znowu zaleją nas tym tanim świństwem ze wschodu i trzeba będzie kolejnych dwustu lat, żeby pozbyć się tego z rynku…

– Hmm… może warto wrócić wreszcie do dobrych tradycji, rzetelności, uczciwości i po prostu dobrych wzorców. Może w końcu należałoby przestać udawać, tak jak w przetargach publicznych sprzed dwustu lat, że cena jest najważniejsza, i skupić się na jakości, na uczciwości, na referencjach. Mamy wielki problem i tylko ta filozofia może pomóc nam go rozwiązać. Żadna inna. Widział pan prognozę pogody? Jeżeli nie zadziałamy szybko, najbliższa burza międzygwiezdna spowoduje dalsze zakłócenia w transmisji teleportacyjnej. Musimy działać szybko. Wróćmy na salę. Opowiem wszystkim więcej o Integralu IP. Jestem pewien, że wszyscy poprą naszą propozycję.

– Niech pan opowie o rozwiązaniach specjalnych Schracka. Ich odporność na zakłócenia elektromagnetyczne i zakres zastosowań był niebywały. Pamiętam, że były także w dobrej cenie. Może to ich przekona.

– Dobrze. Wracajmy na salę.

Dalsze odcinki *Historii z przyszłością*, opowiadania o losach międzygalaktycznej straży pożarnej, znajdą Państwo w następnych numerach *Zabezpieczeń*.

Grzegorz Ćwiek
Schrack Seconet Polska

firma ATLine®

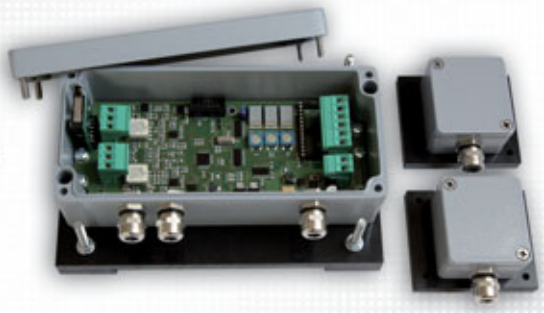
ZSJZ

www.atline.pl

AQAP 2110:2009
ISO 9001:2008

AN 307

- 2 strefy detekcji - każda strefa po 300m,
- 2 terminatory do zakończenia stref detekcji,
- możliwość posłuchu



AN 306

NOWOŚĆ

- 1 strefa detekcji - strefa o długości 300m,
- 1 terminator do zakończenia strefy detekcji,
- możliwość posłuchu

OGRODZENIA POD CZUJNĄ KONTROLĄ

ANIKOM ochrona obwodowa ogrodzeń

Rewolucyjne zmiany w systemach przeciwpożarowych

Wojciech Pawlica

Nadciągają rewolucyjne zmiany. Nie! Już są! No bo kto to słyszał, żeby zwykły, konwencjonalny system zachowywał się jak adresowalny. A jednak jest to możliwe, jeśli wybierzemy nowatorskie rozwiązanie włoskiej firmy INIM Electronics, której produkty na polskim rynku oferuje firma Vidicon

INIM Electronics to doświadczony producent systemów sygnalizacji alarmów włamaniowych i pożarowych. Wieloletnie doświadczenie firmy wywodzi się z czasów, gdy cały pion techniczny pracował jeszcze w Bentel Security.

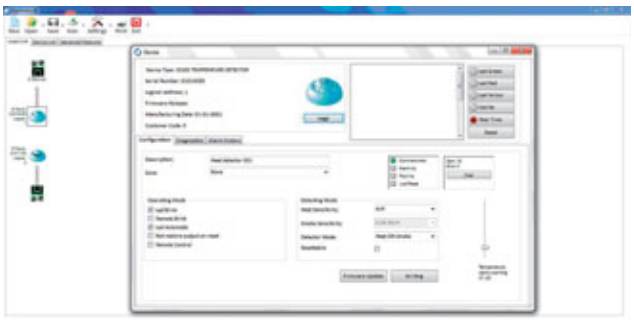
Wprowadzone w 2009 roku na polski rynek centrale systemów sygnalizacji alarmów włamaniowych również wykorzystują nowatorskie, nietypowe dla tej dziedziny rozwiązania. Obecnie jednak interesują nas systemy sygnalizacji pożarowej.

INIM postawił na własne, opatentowane pomysły i technologie, które w znakomity sposób rozwiązują problemy instalatorów.

Wszystko zdarzyło się za sprawą urządzenia testowego o nazwie EITK 1000 oraz serii czujek konwencjonalnych z rodziny IRIS, w których zastosowano najnowszą (innowacyjną) technologię Versa ++. W świecie detekcji konwencjonalnej INIM zastosował całkiem nową koncepcję – elastyczność. Każdą z tych czujek można skonfigurować indywidualnie, dopasowując jej parametry do środowiska, w którym pracuje. Dla celów konfiguracyjnych jest możliwość regulacji ustawienia jednego z czterech różnych poziomów czułości detektora czujek dymowych i dymowo-temperaturowych. Do tego dochodzi wybór jednego z czterech dostępnych trybów pracy czujki temperaturowej lub dymowo-temperaturowej.

Włączenie linii z czujkami do urządzenia EITK1000 pozwala na pełne zdiagnozowanie każdej z czujek oddzielnie i przetestowanie jej działania: sprawdzenie aktualnych parametrów, poziomu zanieczyszczenia w komorze detekcyjnej czujki dymu, zmianę czułości czujki i jej trybu pracy. Tester EITK1000 jest w stanie rozróżnić każdą z czujek, wykorzystując zaszyty, unikatowy numer każdej z nich. Czujka ma wbudowaną nieulotną pamięć pozwalającą na zapamiętanie zmierzonych wartości (dymu i/lub temperatury w zależności od modelu) w ciągu pięciu minut przed ostatnią sygnalizacją alarmu. Jest więc możliwość sprawdzenia, w jaki sposób czujka zachowywała się przed zasygnalizowaniem pożaru. To rozwiązanie nie jest dotychczas często stosowane w innych systemach.

Instalator korzystający z systemu INIM i Vidicon nie musi podczas prac serwisowych podchodzić do każdej czujki osobiście, wyjmować jej z gniazda i sprawdzać, czy jest sprawna i czy nie jest zabrudzona. Wystarczy przyłączyć linię dozorową do



Fot. 1. Zrzut ekranu Fire Genius

modułu EITK1000, uruchomić oprogramowanie Fire Genius, a na wyświetlaczu od razu pojawi się informacja, która z czujek uległa zabrudzeniu lub jest niesprawna. Więcej: jeśli w konwencjonalnej linii dozorowej wystąpiło zwarcie lub przerwa, to można wykryć, w którym miejscu pojawiła się dana usterka.

Dopiero po wykonaniu pełnej diagnostyki linii technik serwisu musi podejść do konkretnej czujki i wymienić ją lub oczyścić. Takie postępowanie znakomicie upraszcza i skraca konserwację systemu.

INIM oferuje też systemy adresowalne z rodziną czujek o nazwie ENEA. Czujki tej rodziny wykorzystują podobne rozwiązania jak czujki konwencjonalne.

W systemach wykorzystujących czujki adresowalne zastosowano kolejny patent firmy INIM, czyli technologię LoopMap, dzięki której centrala sama rozpoznaje konfigurację i topologię pętli, i to nawet wtedy, gdy zastosowano w niej odejścia i węzły typu T. System sam rozpoznaje konfigurację przyłączonej pętli na zasadzie *plug & play*. Jeśli pętla jest przyłączona do centrali lub modułu EITK, na komputerze można od razu rozpocząć proces programowania pętli zawierającej wszystkie szczegóły tak, jak zostało wykonane okablowanie. Technologia LoopMap pozwala na rozpoznanie sposobu wykonania pętli dozorowej, jeśli nawet w pętli występują tzw. linie boczne. LoopMap pozwala na zrekonstruowanie dokładnej topologii instalacji oraz uzyskanie łatwej do użycia interaktywnej mapy pętli, która zdecydowanie upraszcza i przyspiesza prace konfiguracyjne i serwisowe.

W takim przypadku można wykorzystać albo moduł testowy EITK1000, albo oprogramowanie SmartLeague, służące do programowania wszystkich typów central. Platforma oprogramowania SmartLeague jest wspólna dla systemów alarmowych i pożarowych. Wystarczy przyłączyć do centrali komputer klasy PC czy notebooka z programem SmartLeague. Otrzymujemy wówczas pełną diagnostykę linii: regulacje czułości, ustawianie trybu pracy czujek, sprawdzanie poziomu zabrudzeń, odczyt z pięciominutowej pamięci czujki, sprawdzanie aktualnego stanu systemu, diagnostykę zwarć i przerwań pętli.

Kolejną nowatorską technologią zastosowaną w systemach firmy INIM jest OpenLoop. Powstała ona w wyniku wspólnych wysiłków specjalistów z INIM Electronics w dziedzinie badań i rozwoju. Ta przełomowa technologia pozwala centralom przeciwpożarowym INIM przyłączyć urządzenia peryferyjne różnych marek. Jest to nadal najbardziej zaawansowana technologia zarządzania urządzeniami ochrony przeciwpożarowej dostępnymi na rynku. Pętla dozorowa jest w rzeczywistości elastyczna i gotowa do obsługi urządzeń peryferyjnych pracujących w trzech różnych protokołach (Argus, Apollo, INIM). Obsługiwane są również wszystkie typy urządzeń stosowanych w systemach sygnalizacji pożarowej (czujki, moduły wejść, moduły wyjść, ręczne ostrzegacze pożarowe, syreny itp.). Każda pętla może być wykonana w konfiguracji dwu- lub czteroprzewodowej (maksymalna długość linii lub pętli dozorowej wynosi dwa tysiące metrów). Zastosowanie technologii *open loop* pozwala również na funkcję samodiagnozowania i wykrywania anomalii pojawiających się w pętli. Udoskonalone właściwości systemu zarządzania elementami pozwalają podłączyć w każdej pętli imponującą liczbę do 240 urządzeń na pętlę.

Rozwiązania produktowe

Centrale konwencjonalne – seria SmartLine

Czujki, nawet najlepsze, nie mogą stworzyć pełnego systemu sygnalizacji pożarowej. Konieczne jest zastosowanie odpowiednich central. INIM proponuje kilka różnych central, dostosowanych do wielkości instalacji. Wszystkie z przedstawionych poniżej central posiadają Świadectwo Dopuszczenia wydane przez CNBOP.

INIM oferuje centrale konwencjonalne serii SmartLine. Do tej rodziny należą trzy centrale: SmartLine 020-2 (dwie linie dozorowe bez możliwości rozbudowy), SmartLine 020-4 (cztery linie dozorowe z możliwością rozbudowy do dwudziestu) oraz SmartLine 036-4 (cztery linie dozorowe z możliwością rozbudowy do trzydziestu sześciu). Nowatorskim rozwiązaniem każdej z tych central jest dodatkowy terminal I/O, oznaczający wejście/wyjście dla każdej linii. Może on służyć jako wyjście typu otwarty kolektor, wyjście nadzorowane, wejście nadzorowane, wejście czujnika gazu z interfejsem 4-20 mA, wejście czujnika gazowego z interfejsem wyjścia typu otwarty kolektor. Ta elastyczność znacząco zwiększa zakres stosowania rodziny central SmartLine. W ten sposób można uzyskać podwojenie linii (dla największej centrali możemy obsłużyć do siedemdziesięciu dwóch linii) lub nawet trzydzieści sześć wyjść dodatkowych. Informacje o stanie systemu zapewniają wyświetlacz graficzny oraz diody LED w centrali. SmartLine020 zarządza magistralą RS485, do której można przyłączyć maksymalnie cztery terminale wyniesione (model SmartLetUSee/LCD-Lite). Terminale wyniesione powtarzają wszystkie dane z centrali pożarowej i pozwalają użytkownikowi na dostęp do systemu i sterowanie nim zgodnie z przyznanym mu poziomem dostępu. Programowanie systemu z centrali jest proste i bezproblemowe dzięki wyświetlaniu instrukcji do wykonania na wyświetlaczu graficznym. System może również być zaprogramowany przy użyciu oprogramowania SmartLeague (pracującego w środowisku Windows). Metoda ta pozwala instalatorowi na zaprogramowanie całego systemu w domu lub w biurze, a następnie przesłanie przygotowanych danych przez port RS232 z komputera PC do centrali. Moduł SmartLAN/485 pozwala na połączenie płyty głównej centrali z dowolną siecią Ethernet za pomocą magistrali RS485 w celu uzyskania zdalnego dostępu (przez internet) do systemu wykrywania pożaru. Moduł ten pozwala na zdalne pobieranie lub wysyłanie danych i monitorowanie systemu dzięki oprogramowaniu SmartLook firmy INIM. Dodatkowy moduł gaszenia SmartLetLoose/ONE, opracowany dla wszystkich central serii SmartLine, zapewnia możliwość sterowania systemem gaszenia gazowego zgodnie z normą EN12094-1. Sterowanie kartą SmartLetLoose/ONE z centrali zapewnia wszelkie funkcje wymagane przez aktualne normy i pozwala na zarządzanie wszystkimi urządzeniami wymaganymi dla systemu przeciwpożarowego.

Centrale adresowalne

W rodzinie central pożarowych adresowalnych mamy do dyspozycji łącznie sześć typów central:

– SmartLight/S (centrala jednopętlowa, obsługująca maksimum sześćdziesiąt cztery elementy w szesnastu strefach),
– SmartLight/G (centrala jednopętlowa, obsługująca maksimum dwieście czterdzieści elementów w trzydziestu strefach),
– SmartLoop 1010G (jednopętlowa z możliwością pracy w sieci),
– SmartLoop 1010P (jednopętlowa z możliwością pracy w sieci oraz z opcjonalną drukarką i dodatkowym panelem synoptycznym, obsługująca maksimum dwieście czterdzieści elementów w dwustu czterdziestu strefach),
– SmartLoop 2080G (dwupętlowa z możliwością rozbudowy do ośmiu pętli oraz pracy w sieci, obsługująca maksimum tysiąc dziewięćset dwadzieścia elementów w dwustu czterdziestu strefach),
– SmartLoop 2080P (dwupętlowa z możliwością rozbudowy do ośmiu pętli, pracy w sieci i opcjonalną drukarką oraz dodatkowym panelem synoptycznym, obsługująca maksimum tysiąc dziewięćset dwadzieścia elementów w dwustu czterdziestu strefach).

Centrale adresowalne – seria SmartLight

W centralach SmartLight wykorzystano technologię OpenLoop. Centrale wyposażono w nadzorowane wyjście alarmowe oraz nadzorowane wyjście sygnalizacji usterki (sprawność obu jest stale monitorowana). Centrale sygnalizacji pożarowej SmartLight mogą wykryć i zdiagnozować usterki i błędy w pętli, a także zapewniają szerokie spektrum wizualizacji sygnałów: alarm, prealarm, usterka, wczesne ostrzeganie, wyłączenie, test, monitorowanie. Cały stan systemu pokazywany jest zarówno na diodach LED, jak i na wyświetlaczu graficznym.

Do centrali SmartLight można przyłączyć do czterech terminali wyniesionych, komunikujących się z nią przez magistralę RS485 (Model: SmartLetUSee/LCD-Lite). Moduły wyniesione powielają wszystkie dane systemu sygnalizacji pożarowej i pozwalają użytkownikom na dostęp do systemu oraz jego kontrolę zgodnie z ich poziomem dostępu. Możliwe jest także dołączenie do centrali modułu sterowania gaszeniem SmartLetLoose/ONE (dodatkowa opcja). Moduł ten spełnia normy EN12094-1 i oferuje pełny zakres funkcjonalności, jeśli chodzi o zarządzanie systemem gaszenia. Programowanie systemu z centrali jest proste dzięki instrukcjom pokazywanym na wyświetlaczu graficznym. Samoadresowanie czujek skraca czas programowania urządzeń w pętli i upraszcza całą procedurę. Centralę można także zaprogramować, używając przyjaznego dla użytkownika oprogramowania SmartLeague firmy INIM (działającego pod nadzorem systemu operacyjnego Windows). Metoda ta pozwala instalatorowi zaprogramować cały system w domu lub biurze, a następnie przesłać te dane przez łącze RS232 z komputera do centrali.

Centrale adresowalne – seria SmartLoop

Seria adresowalnych urządzeń SmartLoop wprowadza wyraźne zmiany w systemach wykrywania pożaru. Centrale te spełniają wymagania każdego z segmentów rynku: od małych domowych aplikacji, wymagających jedynie jednej pętli, po duże aplikacje, wymagające do ośmiu pętli. W maksymalnej konfiguracji możliwe jest połączenie do trzydziestu central w sieć pierścieniową; jeśli weźmie się pod uwagę, że każda z central będzie miała osiem pętli, a na każdej z pętli będzie znajdowało się po dwieście czterdzieści urządzeń, to wyraźnie widać, iż najnowsze rozwiązania z serii SmartLoop są nie do przecenienia, jeśli chodzi o elastyczność zastosowania. Seria central SmartLoop została specjalnie zaprojektowana w celach ulepszenia dostępnych wcześniej funkcji: najlepszej wydajności w swojej klasie, prostej obsługi przez użytkownika końcowego i bezproblemowej instalacji. Wszystkie te funkcje stały się możliwe do realizacji dzięki zastosowaniu architektury wieloprocesorowej nadzorowanej przez procesor 32-bitowy. Urządzenia zapewniają najwyższy poziom niezawodności, szybkość reakcji, łatwość użytkowania, prostotę połączenia, możliwość dodania dodatkowych modułów i elastyczność. W centralach z serii SmartLoop zostały wykorzystane opatentowane przez INIM technologie: technologia OpenLoop, technologia sieciowa HorNet, technologia Emergency54 oraz technologia Janus (ta sama, która jest wykorzystana w centralach alarmowych firmy INIM). Centrale SmartLoop mają pięć nadzorowanych wyjść do sygnalizacji alarmów i usterek (sprawność tych wyjść jest stale monitorowana). Centrala może wykryć i zdiagnozować błędy i usterki pętli. Zapewnia także szerokie spektrum wizualizacji sygnałów: alarm, prealarm, usterka, wczesne ostrzeganie, wyłączenie, test, monitorowanie. Cały stan systemu pokazywany jest zarówno na diodach LED, jak i na wyświetlaczu graficznym. Oprócz nadzorowanych wyjść centrala posiada dwa przekaźniki do sygnalizacji alarmu i usterki, a także wyjście sygnalizacji wyłączenia akumulatora.

W pracy sieciowej central można korzystać z technologii Hor-Net (kolejnego patentu INIM-a), która pozwala łączyć centrale w sieć. Maksymalnie w sieci może pracować do trzydziestu central, a odległość pomiędzy węzłami sieci może wynosić nawet do dwóch tysięcy metrów. Podczas pracy sieciowej z dowolnej centrali można sterować stanem każdej z podłączonych central i kontrolować go na zasadach równorzędności.

Podsumowanie

Jak widać, poza najmniejszą centralą SmartLight/S, w pozostałych każda pętla może przyjąć do dwustu czterdziestu adresowalnych elementów (czujników, ROP-ów, syren). Jest to możliwe (i zgodne z normą 54-2) dzięki zastosowaniu w każdej pętli niezależnego mikroprocesora zarządzającego.

Seria central SmartLoop została specjalnie zaprojektowana w celu ulepszenia dostępnych wcześniej funkcji: najlepszej wydajności w swojej klasie, prostej obsługi przez użytkownika końcowego i bezproblemowej instalacji. Ten nowoczesny sprzęt zapewnia najwyższy poziom niezawodności, szybkość reakcji, łatwość użytkowania, prostotę połączenia, możliwość dodawania dodatkowych modułów oraz elastyczność ich stosowania.

Więcej informacji o przedstawionych produktach znajduje się na naszej stronie *www.vidicon.pl*. Zainteresowanym zapewniamy możliwość bliższego zapoznania się z centralami na bezpłatnych szkoleniach i warsztatach sprzętowych organizowanych zarówno w biurze warszawskim, jak i wrocławskim.

Wojciech Pawlica
Vidicon

VIDICON POLECA

SYSTEMY PRZECIWPOŻAROWE

inim® ELECTRONICS
A PASSION for SECURITY

SYSTEMY KONWENCJONALNE

SmartLine

SYSTEMY ADRESOWALNE

SmartLight

SmartLoop

NAJLEPSZE CENY - INNOWACYJNE ROZWIĄZANIA

WWW.VIDICON.PL

Radiometr uniwersalny RK-100

Mariusz Radoszewski

Promieniowanie jonizujące będące „w służbie” człowieka czasami wymyka się spod kontroli, powodując zagrożenie zdrowia lub życia organizmów narażonych na jego działanie. W świetle ostatnich wydarzeń, związanych z katastrofą w elektrowni jądrowej Fukushima, tematyka promieniowania jonizującego jest bardzo intensywnie poruszana. Stwierdzenie obecności promieniowania w przestrzeni nie należy do zadań łatwych. Wykorzystuje się do tego celu różnego rodzaju urządzenia, w tym te bardzo popularne – uniwersalne radiometry. Polon-Alfa jest największym polskim producentem takich urządzeń, a jednym z podstawowych produktów jest radiometr RK-100 (fot. 1)

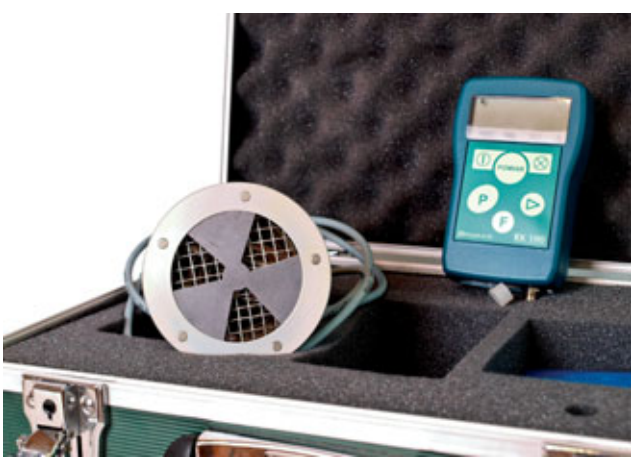
Fot. 1. Radiometr uniwersalny RK-100 w zestawie

RK-100 – przeznaczenie

Radiometr RK-100 (fot. 2) jest przeznaczony do:
- pomiaru skażeń powierzchni substancjami alfa-promieniotwórczymi,
- pomiaru skażeń powierzchni substancjami beta-promieniotwórczymi,
- pomiaru mocy przestrzennego równoważnika dawki promieniowania X i gamma,
- pomiaru mocy dawki promieniowania X i gamma,
- pomiaru dawki i przestrzennego równoważnika dawki promieniowania X i gamma.

RK-100 może służyć jako przyrząd pomiarowy wszędzie tam, gdzie wykorzystuje się źródła promieniowania. Można stosować go do wykrywania źródeł promieniowania i oceny poziomu skażeń. Ma prostą, trwałą obudowę i małą masę. Jest łatwy w obsłudze.

Radiometr RK-100 jest szczególnie przydatny w następujących zastosowaniach:
- w kontroli granicznej i celnej oraz w ratownictwie technicznym,
- w inspektoratach sanitarno-epidemiologicznych,
- do kontroli skażeń i mocy przestrzennego równoważnika dawki promieniowania w transporcie kolejowym i drogowym,
- do kontroli skażeń rąk, odzieży roboczej, powierzchni stołów roboczych w pracowniach radiobiologicznych oraz pracowniach medycyny nuklearnej,
- do kontroli szczelności źródeł jonizacyjnych w pożarowych czujkach dymu,



Fot. 2. Radiometr RK-100 z sondą zewnętrzną

Fot. 3. Radiometr RK-100 z sondą zewnętrzną

- do wszelkich pomiarów kontrolnych wykonywanych przez inspektorów ochrony radiologicznej.

RK-100 – budowa

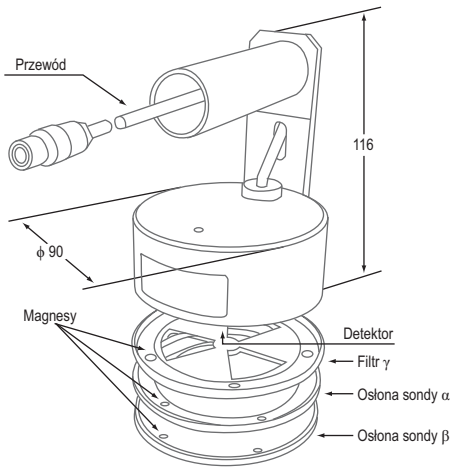
Radiometr RK-100 jest produkowany w następujących wersjach:
- z sondą wewnętrzną do pomiaru mocy równoważnika dawki, mocy dawki pochłoniętej, równoważnika dawki i dawki pochłoniętej promieniowania gamma oraz, po podłączeniu sondy zewnętrznej, do pomiaru skażeń powierzchni substancjami alfa-, beta- i gamma-promieniotwórczymi (fot. 3);
- z sondą wewnętrzną oraz z sondą zewnętrzną do pomiaru mocy równoważnika dawki oraz skażeń powierzchni substancjami alfa-, beta- i gamma-promieniotwórczymi (fot. 4).

Na przedniej ściance radiometru znajduje się wskaźnik ciekłokrystaliczny oraz klawiatura membranowa. Pojemnik baterii jest umieszczony na ściance tylnej. Na dolnej ściance znajduje się złącze do przyłączenia sondy zewnętrznej oraz, pod osłoną, nadajnik i odbiornik do komunikacji IR (w podczerwieni). Detektory sondy wewnętrznej są umieszczone przy górnej i tylnej ściance, pod wskaźnikiem. Wewnątrz obudowy zamontowany jest sygnalizator akustyczny.

RK-100 – sonda zewnętrzna (rys. 1)

Sonda zewnętrzna jest przystosowana do pomiaru:
- mocy równoważnika dawki po założeniu filtru γ (gamma); filtr ten koryguje charakterystykę

Fot. 4. Radiometr RK-100 z dołączoną sondą zewnętrzną



Rys. 1. Sonda zewnętrzna

energetyczną **γ** detektora w zakresie promieniowania, dostosowując ją do charakterystyki zgodnej z jednostkami mocy równoważnika dawki (Sv/h). Filtr γ nie osłania detektora przed promieniowaniem **β** (beta) i **α** (alfa). Jeżeli istnieje taka konieczność, filtr można założyć z osłoną **β** lub **α**. Należy jednak mieć na uwadze to, że wówczas charakterystyka energetyczna w zakresie niskich energii (<80 keV) zostanie znacznie obniżona;

– skażenia powierzchni **α**+**β**+**γ** w przypadku niezałożenia osłon **α** lub **β**;
– skażenia powierzchni **β**+**γ** przy założonej osłonie **α** (osłona ta odcina promieniowanie **α**);
– skażenia powierzchni **γ** przy założonej osłonie **β** (osłona ta odcina promieniowanie **β** i **α**).

Radiometr umożliwia trzy tryby pomiaru skażeń:
– pomiar względny wskazywany w jednostkach [s^{-1}],
– pomiar bezwzględny wskazywany w jednostkach [Bq/cm^2],
– pomiar bezwzględny różnicowy wskazywany w jednostkach [Bq/cm^2].

Pomiary dokonywane za pomocą radiometru mogą być zapisywane w jego wewnętrznej, nieulotnej pamięci. Zawartość pamięci może być przesłana do komputera PC za pośrednictwem wbudowanego w radiometr interfejsu komunikacyjnego IrDA (łącze podczerwieni). Dane z radiometru mogą być danymi w postaci tabel pomiarów, wykresów mocy dawki lub są zapisywane w formie „drzewa". Oprogramowanie RK-100 umożliwia również pełną konfigurację urządzenia, tak aby w maksymalnym stopniu dopasować jego charakterystykę pracy do wymagań użytkowników (ustawianie progów alarmowych itp.).

Coraz więcej zastosowań źródeł promieniowania jonizującego powoduje, że radiometry stają się bardzo popularnymi urządzeniami pomiarowymi. W sytuacjach zagrożenia oddziaływaniem promieniowania jonizującego stają się wręcz przedmiotami pierwszej potrzeby i nabierają szczególnego znaczenia dla ludzi, których to zagrożenie dotyczy.

mgr inż. Mariusz Radoszewski
POLON-ALFA

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

BEZPIECZNY ZAKUP

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k. (dawniej „POLON-ALFA" Zakład Urządzeń Dozymetrycznych sp. z o.o.)

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

Prognoza

dla systemów nagłośnieniowych

Nadciąga szerokopasmowy front układu wysokiego ciśnienia

Fabian Ukleja

Projektowanie systemu nagłośnieniowego sal widowiskowych i sportowych, w których wymagany jest system DSO, jest zawsze związane z kompromisem, który jest potrzebny, gdy trzeba zapewnić odpowiednią jakość dźwięku i zarazem odpowiednie ciśnienie akustyczne w związku z wysokim poziomem tła. Wybór właściwych głośników oraz przeprowadzenie symulacji akustycznej jest w tym przypadku kluczem do sukcesu

Dostępne na rynku rozwiązania najczęściej ograniczają się do głośników tubowych, które dzięki wysokiemu poziomowi SPL są w stanie wyemitować dźwięk o odpowiednim ciśnieniu w obiektach o wysokim poziomie tła akustycznego. Wadą takich rozwiązań jest wąskie pasmo przenoszenia, najczęściej w zakresie 400 Hz–5 kHz. Wyjątkiem są tuby muzyczne, w których pasmo przenoszenia zawiera się w zakresie od 100 Hz do 18 kHz, co oczywiście ma wpływ na obniżenie maksymalnego poziomu SPL (spadek o ok. 10 dB w porównaniu do standardowych głośników tubowych).

Wąskie pasmo przenoszenia głośników tubowych wyklucza zastosowania typowo muzyczne, w których wymagane jest szerokie pasmo przenoszenia zapewniające odpowiednią dynamikę utworów muzycznych.

Proponowanym przez firmę Bosch Security Systems rozwiązaniem przeznaczonym do nagłaśniania sal widowiskowych i sportowych jest najnowsza seria głośników LB3.

Seria LB3 to głośniki segmentu Premium przystosowane do pracy w systemach 100 V, w których jakość dźwięku ma szczególne znaczenie. Dzięki zastosowaniu przetworników używanych w profesjonalnych zestawach głośnikowych osiągnięto wysoką jakość dźwięku przy dużym poziomie SPL.

Rodzinę LB3 stanowią dwa modele – LB3-PC250 oraz LB3-PC350.

LB3-PC250 to zestaw głośnikowy o mocy 250 W z przetwornikiem nisko-/średniotonowym o średnicy 12" oraz głośnikiem kompresyjnym z wyjściem o średnicy 1" zamontowanym w tubie.

LB3-PC350 jest zestawem głośnikowym o mocy 350 W, w którym zainstalowano przetwornik nisko-/średniotonowy o średnicy 15" oraz głośnik kompresyjny z wyjściem o średnicy 1" zamontowanym w tubie.

Wszystkie głośniki Bosch są skonstruowane w taki sposób, aby zapewnić nieprzerwaną emisję dźwięku o mocy znamionowej przez sto godzin, co jest zgodne z wymaganiami normy IEC 268-5 (PHC). Firma Bosch opracowała specjalny test symulujący wystąpienie dodatniego sprzężenia akustycznego (SAFE – *Simulated Acoustical Feedback Exposure*), aby wykazać, że jej głośniki są w stanie emitować przez krótki czas moc dwa razy większą od mocy znamionowej bez ich uszkodzenia.

Zgodność głośników LB3-PC250 oraz LB3-PC350 z normą EN-54-24 umożliwia stosowanie ich w systemach DSO. Zgodność z normą EN54-24 jest potwierdzona certyfikatem zgodności wydanym przez CNBOP. Proces wydawania świadectwa dopuszczenia powinien zakończyć się wkrótce, w momencie publikacji niniejszego artykułu.

Specjalnie na potrzeby systemu DSO w obudowach głośników przygotowano miejsca na montaż płytek końca linii z oferty Bosch. W głośnikach zainstalowano również filtr (z możliwością obejścia), który odfiltrowywuje sygnał pilotujący 20 kHz.

Obudowa z tworzywa ABS zapewnia wysoki stopień tłumienia drgań i odporność na uderzenia. Przednia osłona głośnika została wykonana ze stali. Dzięki odpowiednim punktom montażowym możliwa jest instalacja podwieszana oraz na statywie.

Wysoki poziom SPL oraz szerokie pasmo przenoszenia są nieocenione w przypadku instalacji w salach widowiskowych i sportowych. Dynamiczny i krystaliczny dźwięk zdecydowanie poprawia atmosferę podczas wydarzeń sportowych i dostarcza niezapomnianych wrażeń z odbioru muzyki.

Dzięki wprowadzeniu serii LB3 do oferty firmy Bosch systemy DSO mogą pełnić również funkcję nagłaśniania obiektu bez utraty dynamiki i detali muzycznych, co bezpośrednio przekłada się na koszty budowy lub późniejszej przebudowy obiektu.

Fabian Ukleja
Bosch Security Systems

	LB3-PC250	LB3-PC350
Moc znamionowa	250 W	350 W
Efektywne pasmo przenoszenia (-10dB)	55 Hz–18 kHz	48 Hz–18 kHz
SPL przy mocy znamionowej/1W (1 m, 1 kHz)	117/94 dB	122/97 dB
Stopień szczelności	IP44	IP44
Wymiary (szer. x głęb. x wys.)	410 mm x 367 mm x 595 mm	470 mm x 420 mm x 720 mm
Materiał obudowy	ABS VO	ABS VO
Temperatura pracy	od -10°C do +40°C	od -10°C do +40°C
Masa	19 kg	34 kg

Tab. 1. Parametry zestawów głośnikowych z serii LB3

Plastikowy pieniądz

Krzysztof Białek

Obecnie niewiele osób otrzymuje pensję w gotówce. Pamiętam, jak ogromne wrażenie zrobiła na mnie w dzieciństwie pensja przyniesiona do domu przez tatę, wypłacona w czerwonych stuzłotówkach z Ludwikiem Waryńskim – sto tysięcy złotych, dziesięć paczek po sto banknotów (akurat tego dnia kasjerka miała tylko takie nominały w kasie). Ilu z nas może dziś pochwalić się pokazaniem swojej pensji w gotówce dziecku czy wnukowi?

W dzisiejszych czasach sięgamy po gotówkę zdecydowanie rzadziej. Coraz częściej dokonujemy przelewów i korzystamy z różnego rodzaju kart płatniczych. Wszystko to sprawia, że pokolenie najmłodszych zupełnie inaczej pojmuje wartość pieniądza i sam pieniądz – dla nich już niekoniecznie musi być on materialny. Obecnie trudno wytłumaczyć dziecku, że nie możemy mu kupić wszystkiego, na co ma ochotę, bo nie mamy pieniędzy. „Jak to nie?" – zapyta – „Przecież możesz pójść po pieniądze do bankomatu albo zapłacić kartą!". I jak tu wytłumaczyć kilkuletniemu brzdącowi, że to nie jest takie proste, skoro on przecież wie, że wystarczy włożyć kartę do bankomatu lub podać ją sprzedawcy w sklepie. Niby to tylko kawałek plastiku (coraz częściej wyposażony w dodatkowy chip), a jakiej nabrał wartości! W przypadku utraty karty lub przejęcia nadrukowanych na niej danych przez nieuprawnione osoby możemy mieć nie lada kłopoty.

Jak uchronić się przed niekontrolowanym wypływem pieniędzy z naszego konta lub niechcianym obciążeniem kredytowym? Po pierwsze zachować zdrowy rozsądek. Jednym z podstawowych warunków jest nieudostępnianie swojej karty ani jej numeru PIN nikomu, nawet – a może przede wszystkim – członkom rodziny. Może to wydawać się zaskakujące, ale właśnie nieuprawnione działania domowników są najczęstszą przyczyną zgłoszeń dotyczących nieautoryzowanych operacji. Czasami klienci, którzy nie uwierzyli w to, że pieniądze zniknęły za sprawą ich bliskich, chcą zobaczyć nagranie z kamery bankomatowej. Z reguły banki nie udostępniają zapisu bezpośrednio klientowi, tylko proponują przekazanie sprawy policji. W takich przypadkach skruszony sprawca zazwyczaj przyznaje się do winy, gdy właściciel karty tylko wspomni po powrocie do domu, że będzie musiał złożyć zawiadomienie. Niekiedy jednak przyznaje się dopiero w obecności funkcjonariusza policji.

Inaczej jest w sytuacji, w której karta została zgubiona lub ukradziona. Co powinien w takim przypadku zrobić właściciel? Najskuteczniejszym sposobem jest jak najwcześniejsze zastrzeżenie karty za pośrednictwem serwisu telefonicznego jej wystawcy – numer telefonu kontaktowego zawsze znajduje się na odwrocie karty płatniczej. Łatwo powiedzieć, ale co nam po numerze telefonu umieszczonym na karcie w przypadku jej utracenia? Aby uniknąć kłopotu, powinniśmy zapisać sobie ten numer w innym miejscu. Jeśli tego nie zrobiliśmy, nie powinniśmy wpadać w panikę – można zastrzec kartę w oddziale banku, który ją wystawił, lub poszukać numeru telefonu na jego stronie internetowej. Jest jeszcze jeden, bardzo prosty i zarazem przewrotny sposób na zabezpieczenie karty – napisanie niepoprawnego numeru PIN na „gęsiej skórce" i przyklejenie jej do karty. Przestępca raczej nie zaryzykuje dokonania płatności w sklepie, w którym byłby narażony na bezpośredni kontakt ze sprzedawcą. O ile nie spróbuje kupić czegoś w sklepie internetowym, najpierw postara się wypłacić pieniądze z bankomatu – tutaj nikt nie poprosi go o podpis. Przy bankomacie czeka go niemiła niespodzianka, bo numer PIN okaże się nieprawidłowy. W takich przypadkach przestępcy zazwyczaj próbują wpisać ponownie ten sam kod w obawie, że poprzednio popełnili błąd, a w następnej kolejności próbują innych kombinacji zapisanych cyfr (najczęściej wpisują je w odwrotnej kolejności). Po kilku błędnych próbach karta jest automatycznie zatrzymywana przez bankomat. Sposób „na gęsią skórkę" jest dosyć skuteczny, ponieważ usypia czujność przestępców. Może niektórym trudno w to uwierzyć, ale użytkownicy, w szczególności osoby starsze, nierzadko mają zapisany poprawny numer PIN w bliskim sąsiedztwie karty, np. w tym samym etui, portfelu lub w notesie przechowywanym w torebce. Jeśli torebka zostanie skradziona, przestępca wejdzie w posiadanie kompletu – karty oraz poprawnego numeru PIN.

Innym rodzajem przestępstwa z wykorzystaniem karty jest tzw. skimming, czyli nieautoryzowane skopiowanie danych umieszczonych na pasku magnetycznym karty. Aby pozyskać dane, przestępcy na ogół dokonują modyfikacji czytnika kart w bankomacie, dokładając do niego odpowiednio przygotowaną nakładkę sczytującą dane z karty po włożeniu jej do czytnika bankomatu. Ponadto podawany przez użytkownika w trakcie autoryzacji operacji numer PIN jest rejestrowany przez zakamuflowaną bezprzewodową kamerę umieszczoną na obudowie bankomatu. Posiadając komplet informacji – dane z paska magnetycznego oraz numer PIN zarejestrowany przez kamerę – przestępcy przygotowują kopię karty i realizują operacje bez konieczności wejścia w posiadanie oryginału. Takim procederem zajmują się najczęściej zorganizowane grupy przestępcze. Skimmerzy sami nie wykonują kopii kart. Zazwyczaj wysyłają pozyskane informacje do innych osób za pośrednictwem sieci Internet. W efekcie już tego samego dnia operacja bankomatowa z wykorzystaniem kopii karty może zostać dokonana w innym kraju, nawet na innym kontynencie. Ze względu na coraz lepsze zabezpieczenia czytników w bankomatach i stopniową zmianę standardu (karty chipowe zamiast magnetycznych) ten rodzaj przestępczości traci na sile. Mimo to powinniśmy zachować czujność podczas dokonywania operacji bankomatowych i zwracać uwagę na to, czy bankomat nie posiada dodatkowego, niewłaściwego wyposażenia. W przypadku wątpliwości najlepiej wybrać inny bankomat i poinformować o swoich podejrzeniach bank.

W dzisiejszych czasach technologia umożliwia zakupy bez wychodzenia z domu. Możemy zamówić prezent, kupić sprzęt RTV lub nawet artykuły spożywcze w sklepach internetowych. Sposobów płatności jest zazwyczaj kilka, lecz najszybsze dostarczenie towaru jest gwarantowane najczęściej po dokonaniu przelewu lub zapłaceniu kartą. Korzystanie z karty jest bardzo wygodne, aczkolwiek trzeba pamiętać o ochronie umieszczonych na niej danych.

Dokonując płatności, powinniśmy mieć pewność, iż korzystamy z bezpiecznego serwisu płatniczego. Zabezpieczenia systemu operacyjnego komputera, który wykorzystujemy do dokonywania płatności, powinny być na bieżąco aktualizowane. Powinniśmy korzystać także ze zaktualizowanego programu antywirusowego. Operacji płatniczych nie powinno dokonywać się za pośrednictwem komputerów publicznych (np. w kafejkach internetowych) lub użyczonych przez nieznajomych. W przypadku korzystania z danego serwisu płatniczego po raz pierwszy warto poznać wcześniej opinie na jego temat. W trakcie operacji płatniczych połączenie powinno być zabezpieczone – powinien pojawić się symbol kłódki, najczęściej w prawym dolnym rogu ekranu, choć może on znajdować się w innym miejscu, w zależności od wykorzystywanej przeglądarki. Dwukrotne kliknięcie na ten symbol powinno otworzyć okno z informacją, dla kogo został wydany certyfikat – powinien on być zbieżny z nazwą serwisu. Jedną z najskuteczniejszych metod ograniczenia strat w przypadku kradzieży jest korzystanie ze specjalnej karty płatniczej, która działa podobnie jak karta pre-paid w telefonach komórkowych. Konto takiej karty możemy uzupełnić kwotą potrzebną do wykonania zamierzonej operacji płatniczej w portalu internetowym. Dokonujemy tego, wykonując przelew bankowy. W efekcie podanie w sieci danych dotyczących karty płatniczej jest związane z ryzykiem utraty jedynie takiej sumy, jaka w danej chwili znajduje się na koncie takiej karty. W Polsce karty płatnicze typu pre-paid nie są jeszcze powszechne, lecz kilka banków posiada je w swojej ofercie. Jeśli pojawi się popyt na tego typu karty, zapewne zaproponuje je większość banków.

Krzysztof Białek

System Kontroli Dostępu

KaDe

Kontrolery zintegrowane z czytnikami kart zbliżeniowych

Wizualizacja systemu poprzez elektroniczne mapy z aktywnymi ikonami, zdjęciami użytkowników i obrazami wideo „na żywo"

Intuicyjne oprogramowanie nadzorcze

Komunikacja TCP/IP i RS-485

Integracja z systemem CCTV

C-70 C-60 C-10 C-20 KZ-1000

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

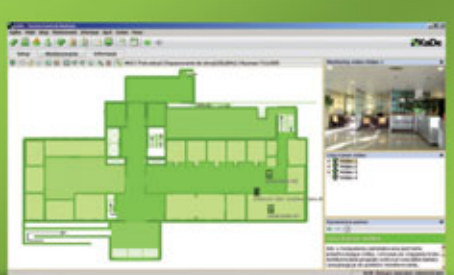
Kontroler KZ-1000	Kontroler przejścia integrujący: moduł kontrolera 1 przejścia, czytnik kart zbliżeniowych 125 kHz UNIQUE, klawiaturę do wprowadzania kodu PIN i przycisk dzwonkowy, sygnalizator optyczny i akustyczny, czujnik antysabotażowy

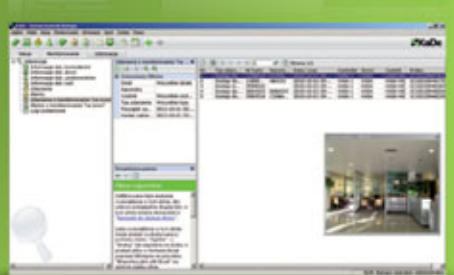
Czytniki kart zbliżeniowych typu UNIQUE (125 kHz):

C-10 C-60 C-70	Czytniki do instalacji wewnątrz i na zewnątrz pomieszczeń, różniące się między sobą jedynie obudową i kolorystyką, co umożliwia optymalne dopasowanie urządzenia i sposobu montażu do każdego wnętrza
C-20	Czytnik identyczny z powyższymi pod względem parametrów, dodatkowo wyposażony w klawiaturę kodową
C-ADM-U	Czytnik administratora przeznaczony do wprowadzania dużej liczby kart do bazy danych programu nadzorczego KaDe. Istnieje możliwość wykorzystania urządzenia do innych zastosowań, np. do współpracy z dowolnym edytorem lub polami edytowalnymi w różnych aplikacjach

Akcesoria

Konwerter RS232/485	Konwerter służy do połączenia magistrali kontrolerów z programem nadzorczym w komputerze poprzez port COM. Urządzenie umożliwia konwersję protokołu RS-232 na RS-422/RS-485
Konwerter TCP/RS485	Konwerter służy do połączenia magistrali kontrolerów z programem nadzorczym w komputerze poprzez sieć Ethernet. Urządzenie umożliwia konwersję protokołu RS-422/RS-485 na protokół sieciowy TCP/IP
Konwerter USB/RS485	Konwerter służy do połączenia magistrali kontrolerów z programem nadzorczym w komputerze poprzez port USB
Karty AST	System współpracuje z kartami zbliżeniowymi AST: AST-U-1001, AST-U-1002, AST-U-1003, AST-U-1004





INTERFEJS OPERATORA

- konfiguracja parametrów elementów fizycznych systemu
- definiowanie elementów logicznych
- monitorowanie stanu systemu „on-line" poprzez system graficznych map obiektów i komunikatów
- wyświetlanie zdjęć użytkownika
- integracja z systemem CCTV poprzez wbudowaną w PC kartę przechwytującą wideo lub zewnętrzny DVR/IP, kamery przypisane do kontrolowanych przejść lub czujek
- generowanie filtrowanych raportów zdarzeń i zapis w formacie *.xls

Funkcje specjalne realizowane przez system KaDe

- dostęp po użyciu 2, 3 lub 4 kart
- pierwsze otwarcie kontrolowanego przejścia przez tzw. pierwszą kartę ze specjalnymi uprawnieniami
- dostęp po potwierdzeniu przez operatora

Eksploatacja układów zasilających elektroniczne systemy bezpieczeństwa

Praktyczne badania wybranych układów zasilających (część 2)

Waldemar Szulc, Adam Rosiński

Poprzednia część (*Zabezpieczenia* nr 3/2011) niniejszego artykułu dotyczyła podstaw układów zasilających elektroniczne systemy bezpieczeństwa, głównie ich eksploatacji. Autorzy przedstawili trzy główne typy układów zasilania (A, B, C) stosowane w elektronicznych systemach bezpieczeństwa wraz z syntetycznym opisem pracy tych urządzeń. Przedstawione typy układów zasilających zawierają również zasilacze rezerwowe w postaci akumulatorów o ściśle dobranych pojemnościach zależnych od stopnia zabezpieczenia

1. Wprowadzenie

Szczegółowe dane zawarte są w normie PN-EN 50131-1:2009. Warto również wspomnieć, że układy zasilające są stosowane w następujących elektronicznych systemach bezpieczeństwa:

– systemach sygnalizacji włamania i napadu (przewodowych i bezprzewodowych),
– systemach kontroli dostępu,
– systemach monitoringu wizyjnego,
– systemach sygnalizacji pożarowej wraz z dźwiękowymi systemami ostrzegawczymi,
– zintegrowanych systemach bezpieczeństwa,
– inteligentnych budynkach,
– innych urządzeniach współpracujących z elektronicznymi systemami bezpieczeństwa,
– systemach monitorujących,
– elektronicznych systemach bezpieczeństwa w ruchomych środkach transportowych,
– elektronicznych systemach przywoławczych (dla szpitali) zgodnych z VDE-0834.

Właściwy dobór układów zasilających do powyżej przedstawionych elektronicznych systemów bezpieczeństwa nie jest łatwe ze względu na często stochastyczny charakter ich pracy. Na łamach *Zabezpieczeń* autorzy wielokrotnie omawiali problematykę niezawodnościowo-eksploatacyjną systemów alarmowych różnych typów ze szczególnym uwzględnieniem obiektów o charakterze specjalnym (kancelarie tajne, obiekty szczególnego znaczenia, banki, obiekty dziedzictwa narodowego itp.). Wspomniano również o normach PN-EN 50131-6 oraz PN-EN 54-4:2001, według których muszą być budowane i eksploatowane elektroniczne systemy bezpieczeństwa [6].

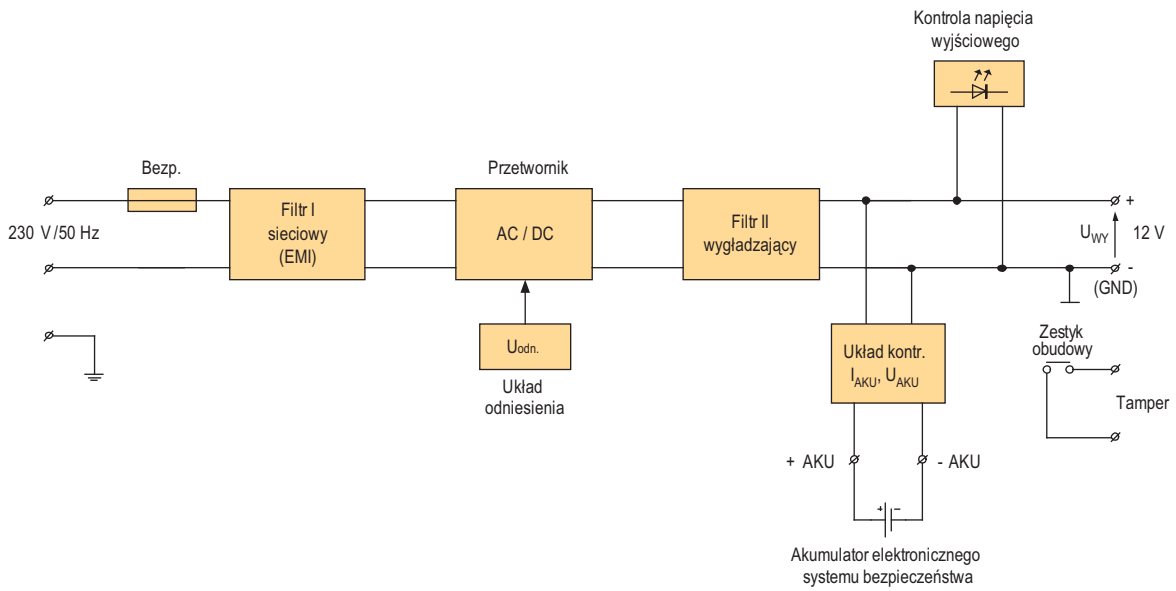
W części drugiej niniejszego artykułu zostaną przedstawione schematy blokowe (jedne z wielu) spotykanych układów zasilających elektroniczne systemy bezpieczeństwa wraz z charakterystycznymi danymi [5]. Będą to zewnętrzne urządzenia zasilające, które wspomagają prądowo elektroniczne systemy bezpieczeństwa z uwzględnieniem źródeł rezerwowych (akumulatorów). Podsumowując, urządzenia zasilające elektroniczne systemy bezpieczeństwa można podzielić na:

– zasilacze zintegrowane z płytą główną centrali alarmowej, które są kontrolowane systemowo (zasilacz zasadniczy i źródło rezerwowe);
– zasilacze zewnętrzne, w przypadku których kontrolowana jest głównie obudowa, w której zlokalizowano zasilacz, zaś sygnalizacja nieprawidłowego stanu pracy takiego zasilacza może mieć postać wskaźników lub sygnalizatorów na obudowie; zasilacze mogą być wyposażone w wyjście do urządzeń zewnętrznych, aktywowane w razie nieprawidłowej pracy zasilacza;
– UPS-y – to zewnętrzne urządzenia zasilające elektroniczne systemy bezpieczeństwa (wyposażone w akumulatory żelowe), które podtrzymują zasilanie systemu przez okres zależny od pojemności akumulatora (jak również od jego stanu technicznego).

Autorzy przedstawią również wyniki badań technicznych i eksploatacyjno-niezawodnościowych określonego typu zasilacza zasilającego elektroniczny system bezpieczeństwa. Badania wykonano na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa w Wyższej Szkole Menedżerskiej w Warszawie. Uczelnia posiada Laboratoria Systemów Alarmowych w ramach Zespołu Laboratoriów Systemów Bezpieczeństwa.

2. Przykładowe układy zasilające systemy bezpieczeństwa

Na rys. 1 przestawiono przykładowy zasilacz krajowego producenta przeznaczony do elektronicznych systemów bezpieczeństwa. Producent ten opracował ponad 150 typów rozwiązań. Wybrano trzy typy zasilaczy do zasilania elektronicznych systemów bezpieczeństwa, które szczególnie nadawały się do badań. Zasilacze poddano testom eksploatacyjnym i badaniom niezawodnościowo-eksploatacyjnym. Wyniki potwierdziły przydatność tych urządzeń do zasilania elektronicznych systemów bezpieczeństwa (można je stosować na przykład w transporcie). Badano m.in. wpływ zakłóceń radioelektrycznych pochodzących z trakcji oraz innych urządzeń emitujących



Rys. 1. Układ blokowy prostego zasilacza impulsowego wyposażony w rezerwowe źródło zasilania

zakłócenia w procesach eksploatacyjnych. Na rys. 1 przedstawiono prosty zasilacz impulsowy z przetwornikiem AC/DC, wyposażony w wejściowy filtr sieciowy (EMI), który ma eliminować zakłócenia wejściowe.

Zasilacz buforowy jest przeznaczony do „nieprzerwanego" zasilania elektronicznych systemów bezpieczeństwa, które wymagają stabilizowanego napięcia: U = 12 V$^{(+/- 15\%)}$. Badania laboratoryjne wykazały, że zasilacz dostarcza napięcia w zakresie od 13,4 V do 13,8 V, a w przypadku pracy z buforowym źródłem zasilania (akumulator bezobsługowy) – napięcia od 10,8 V do 13,8 V i wydajności prądowej I = 7 A.

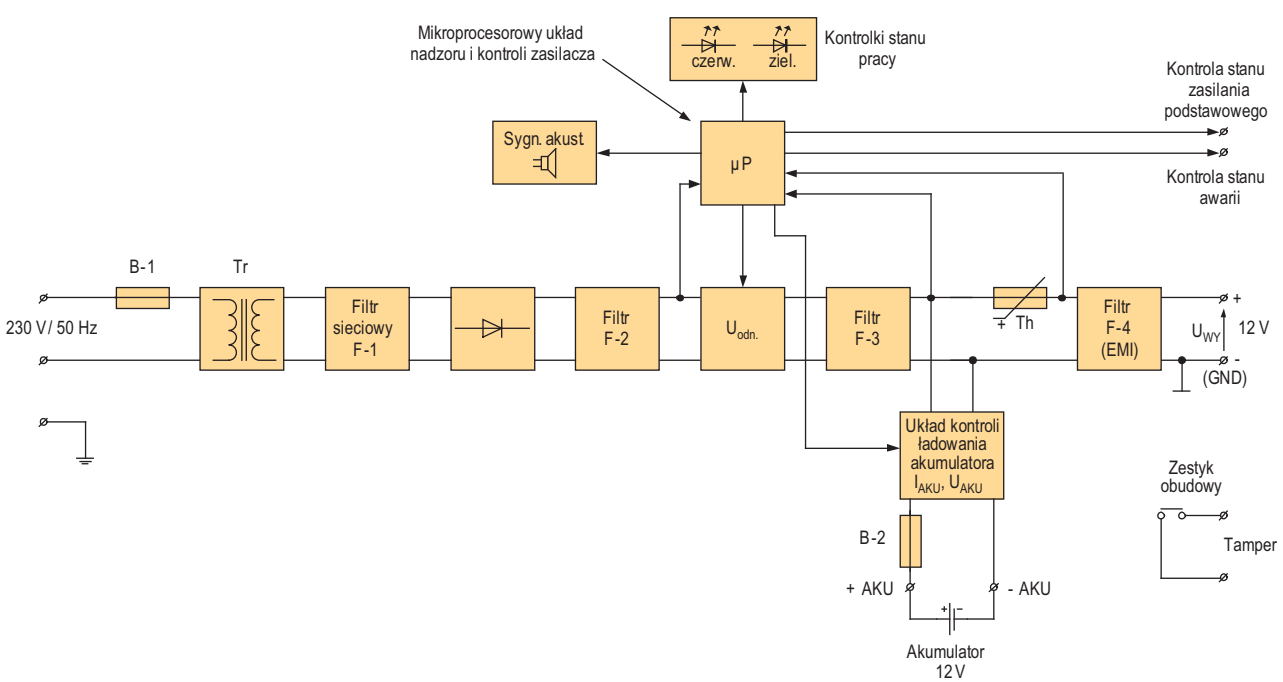
W przypadku zaniku napięcia zasadniczego (sieciowego) następuje natychmiastowe przełączenie na zasilanie rezerwowe (akumulatorowe). Konstrukcja zasilacza wykorzystuje moduł zasilacza impulsowego o wysokiej sprawności energetycznej η = 94% z uwzględnieniem korekty współczynnika mocy (PFC). Zasilacz został wyposażony w zabezpieczenia przeciwzwarciowe, przeciążeniowe, termiczne i nadnapięciowe. Układ zasilacza, choć prosty, umożliwia kontrolę automatycznego procesu ładowania i konserwacji źródła rezerwowego. Wyposażono go w ochronę źródła rezerwowego przed nadmiernym rozładowaniem oraz odwrotną polaryzacją przyłączenia, a także w optyczną sygnalizację pracy (diody LED) informującą o aktualnym stanie pracy (kontrola napięcia wyjściowego). Wszystkie elektroniczne systemy bezpieczeństwa, także zasilacze, muszą być wyposażone w układ antysabotażowy (Tamper).

Kolejnym bardzo ciekawym rozwiązaniem jest zasilacz analogowy z nadzorem mikroprocesorowym. Schemat blokowy tego urządzenia przedstawiono na rys. 2. Jest to stabilizowany zasilacz transformatorowy, a więc o galwanicznej izolacji sieci zasilającej (między innymi ze względów bezpieczeństwa). Jego konstrukcja umożliwiła uzyskanie bardzo wysokiego współczynnika stabilizacji (1).

$$S = \frac{\Delta U_{WE}}{\Delta U_{WY}} = 120 \qquad (1)$$

Napięcie sieci $U_{zasil.}$ = ~230 V (zmieniane zgodnie z obowiązującymi przepisami wynikającymi z rozporządzenia Ministra Gospodarki – Dz.U. Nr 80 poz. 911 – od ~207 V do ~241,5 V, a docelowo do ~253 V) jest obniżane za pomocą transformatora, a następnie filtrowane filtrem sieciowym (EMI) w celu eliminacji zakłóceń radioelektrycznych (filtr F1). Po filtracji napięcie wyjściowe jest prostowane i odfiltrowywane filtrem dolnoprzepustowym (F2). Kolejny etap to stabilizacja napięcia. Napięcie wyjściowe stałe (DC) jest korygowane w zależności od trybu pracy zasilacza z uwzględnieniem fazy ładowania akumulatora i jego konserwacji. Jest ono również filtrowane i wygładzane filtrem F-3. Termistor Th zapewnia termiczną kontrolę zasilacza. Informacja o niebezpiecznych fluktuacjach temperaturowych jest odczytywana przez mikroprocesor, który (po analizie) reguluje pracę zasilacza. Ze względu na możliwość pojawienia się zakłóceń radioelektrycznych układ zasilacza został wyposażony w kolejny filtr – F-4 (EMI). Nad całością poprawnej pracy zasilacza czuwa układ mikroprocesorowy (μP). Kontroluje on stan zasilania podstawowego, a także wykrywa stan awarii.

Zasilacz buforowy przedstawiony na rys. 2 jest przeznaczony do nieprzerwanego zasilania elektronicznych urządzeń bezpieczeństwa, które wymagają stabilizowanego napięcia U = 12 V$^{(+/- 15\%)}$. Dostarcza napięcia wyjściowego w zakresie od 11,00 V do 13,8 V_{DC} o maksymalnej wydajności prądowej I_{MAX} = 1,5 A. Układ zasilacza umożliwia kontrolę automatycznego procesu ładowania i konserwacji źródła rezerwowego. Został wyposażony w ochronę źródła rezerwowego przed nadmiernym rozładowaniem oraz odwrotną polaryzacją przyłączenia. W przypadku zaniku zasilania głównego (zasadniczego) następuje bezprzerwowe przełączenie układu na zasilanie rezerwowe (akumulator bezobsługowy).



Rys. 2. Układ blokowy zasilacza wyposażony w rezerwowe źródło U = 12V$^{(+/- 15\%)}$ z mikroprocesorowym nadzorem pracy

Gdy zasilacz korzysta ze źródła rezerwowego (akumulatora), system kontroluje napięcie akumulatora (U = 12 V), sprawdza, czy nie nastąpiło rozładowanie do dopuszczalnej wartości minimalnej 10,0 V, i wyłącza zasilacz. W ten sposób akumulator jest chroniony przed trwałym uszkodzeniem. Po przywróceniu głównego napięcia zasilania (~230 V) zasilacz powraca do pracy bezprzerwowej z funkcją doładowania i konserwacji akumulatora. Zasilacz został dodatkowo wyposażony w sygnalizatory optyczne (diody LED), które sygnalizują stan awarii i stan zasilania (AC/DC). Stan awarii jest sygnalizowany także akustycznie.

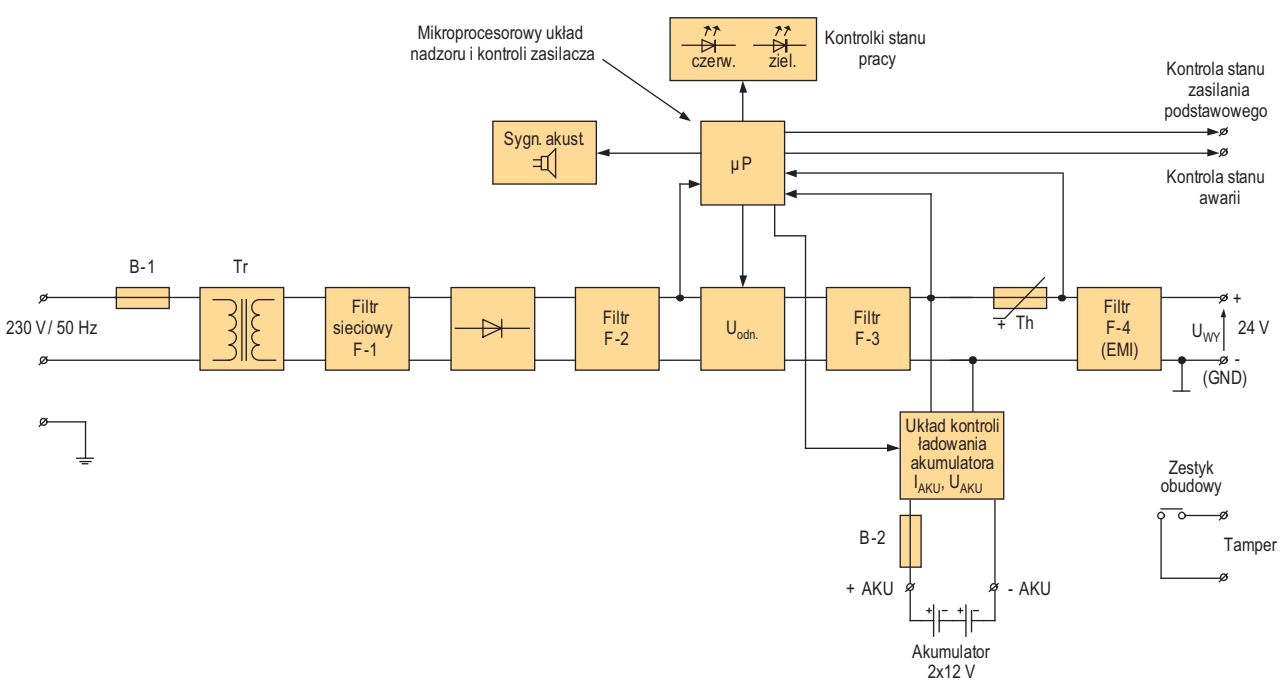
Wszystkie elektroniczne systemy bezpieczeństwa, również zasilacze, muszą być wyposażone w układ antysabotażowy (Tamper). Zasilacz jest wyposażony także w wyjście techniczne do systemów zewnętrznych kontrolujących stan pracy. Ze względu na dużą niezawodność i bezprzerwową pracę zasilacze tego rodzaju idealnie nadają się do zasilania elektronicznych systemów bezpieczeństwa.

Do elektronicznych systemów bezpieczeństwa, które stosowane są w stacjonarnych lub ruchomych środkach transportowych, zaliczane są systemy sygnalizacji pożarowej oraz niektóre elementy wykonawcze systemu kontroli dostępu. Te systemy bezpieczeństwa są zasilane napięciem stałym U = 24 V. Na rys. 3 przedstawiony został układ zasilacza o napięciu wyjściowym U_{WY} = 24 V $^{(+/- 15\%)}$. Taki układ jest przeznaczony do systemów sygnalizacji pożarowej, systemów dozorowych CCTV i kontroli dostępu. Zasada jego pracy jest identyczna jak w przypadku zasilacza przedstawionego na rys. 2. Na bezawaryjną pracę zasilacza oraz elektronicznych urządzeń bezpieczeństwa w transporcie istotny wpływ mają wszystkie cztery filtry. Dlatego też badania wykonywano między innymi w okolicach dworców kolejowych z trakcją elektryczną.

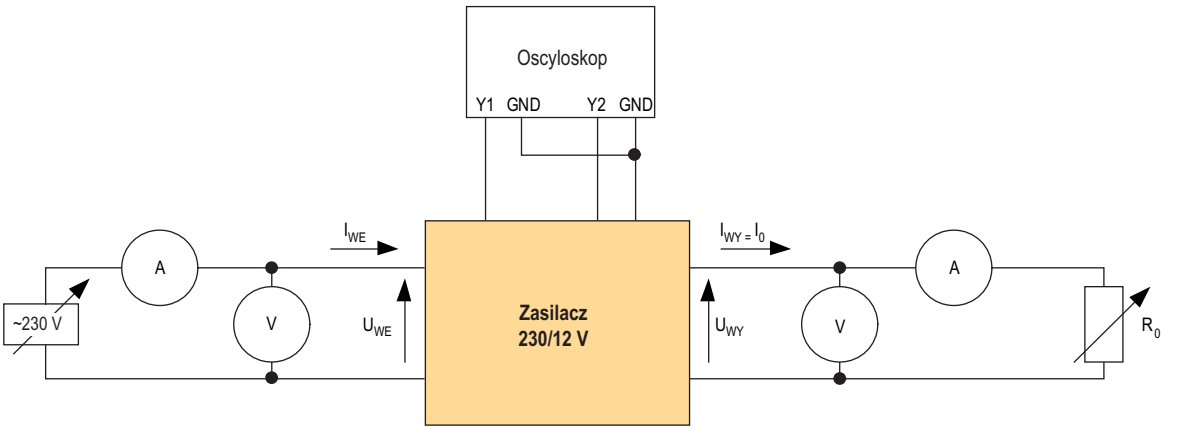
Zastosowany w zasilaczu liniowy układ stabilizacyjny dostarcza napięcia o mniejszym poziomie szumów i znacznie krótszym czasie odpowiedzi na zakłócenia niż w przypadku układu impulsowego. Zasilacz wytwarza napięcie wyjściowe w zakresie od 22,00 V do 27,6 V (w przypadku pracy z akumulatorami – od 20,00 V do 27,6 V), o maksymalnej wydajności prądowej I_{MAX} = 2,0 A. W przypadku zaniku zasilania głównego (zasadniczego) następuje bezprzerwowe przełączenie układu na zasilanie rezerwowe (akumulator bezobsługowy). Zasilacz został wyposażony w zabezpieczenia przeciwzwarciowe, przeciążeniowe, termiczne i nadnapięciowe. Urządzenie przedstawione na rys. 3 automatycznie kontroluje procesy ładowania i konserwacji akumulatorów (2×12 V). Jest również wyposażone w dynamiczny test źródła rezerwowego i układ ochrony przed nadmiernym rozładowaniem (poniżej 10 V/jednostkę). Zasilacz ten (podobnie jak jego poprzednik) został wyposażony w sygnalizację optyczną i akustyczną, która informuje o stanie pracy (zasilaniu i ewentualnych awariach). Ma też wyjścia techniczne, które służą do zdalnej kontroli pracy, oraz system ochrony antysabotażowej (Tamper). W trakcie badań uwzględniono dopuszczalną fluktuację napięcia wejściowego, które zgodnie z przepisami może zmieniać się w zakresie od ~207 V do ~241,5 V. Badania wykonywano również w warunkach laboratoryjnych, zmieniając napięcie wejściowe (od ~146,3 V do ~292,6 V). Ruchome urządzenia transportowe, np. wagony pasażerskie wyposażone w system sygnalizacji pożarowej, wymagają nieco innej konstrukcji zasilacza ze względu na brak napięcia przemiennego ~230 V. Stosuje się w nich przetwornicę DC/DC. Napięcie pokładowe w wagonach to =24 V, a w jednostkach trakcyjnych wynosi 110 V (od 70 V do 140 V). Zasilacze muszą być dostosowane do zasilania napięciami podanymi powyżej. W wagonach pasażerskich stosuje się systemy sygnalizacji pożarowej o zasilaniu =24 V (opisywane już przez autorów na łamach *Zabezpieczeń*).

3. Wyniki badań technicznych i eksploatacyjno-niezawodnościowych układu zasilającego

Na rys. 4 przedstawiono układ laboratoryjny do przeprowadzenia badań technicznych wybranego zasilacza współpracującego



Rys. 3. Układ blokowy zasilacza wyposażony w rezerwowe źródło U = 24 V $^{(+/- 15\%)}$ z mikroprocesorowym nadzorem pracy



Rys. 4. Układ do badania podstawowych charakterystyk układu zasilającego elektroniczny system bezpieczeństwa (~230V/=12V). Uwaga - może być również stosowany dla zasilaczy 230V/24V

z elektronicznym systemem bezpieczeństwa [1,2,3,4,7,8]. Badany układ to zasilacz zewnętrzny o znamionowym napięciu wejściowym U_{WE} = ~ 230 V, stabilizowanym napięciu wyjściowym U_{WY} = 12 V oraz U_{WY} = 24 V i maksymalnym prądzie obciążenia wynoszącym $I_{WY} = I_0$ = 5 A. Badania przeprowadzono, stosując obciążenie R_0 = const, jak również przy zmiennym prądzie wyjściowym I_0 (zmienne obciążenie).

Układ do badania podstawowych charakterystyk zasilaczy do elektronicznych systemów bezpieczeństwa umożliwia pomiar wielu różnych parametrów. Na kolejnych rysunkach przedstawiono kilka z nich.

Na rys. 5 – $U_{WY} = f(U_{WE})$, gdy $I_{WY} = I_0$ = const. Pomiarów dokonano dla 11 wartości prądów obciążenia. Przy U_{WE}= 230 V i prądzie obciążenia $I_{WY} = I_0$ napięcie wyjściowe waha się w granicach 23,9 V ≤ U_{WY} ≤ 24,10 V.

Na rys. 6 – $U_{WY} = f(I_{WY})$, gdy U_{WE} = const dla ośmiu wartości U_{WE} jako parametru.

Na rys. 7 – $I_{WE} = f(I_{WY})$, gdy U_{WE} = const dla ośmiu wartości U_{WE} jako parametru.

Na rys. 8 – sprawność η = $f(I_{WY})$, gdy U_{WE} = const dla ośmiu wartości UWE jako parametru. Badany układ zasilacza to układ transformatorowy. Sprawność tego zasilacza można uznać za dobrą i wahającą się w przedziale 72% ≤ η ≤ 84%.

Niezmiernie ważnym wskaźnikiem określającym jakość zasilacza jest współczynnik stabilizacji S (2). W przypadku badanego zasilacza z opisu znajdującego się na rys. 5 można odczytać, że ΔU_{WE} = 34,5 V ($U_{WE\,min}$ = 207 V, $U_{WE\,max}$ = 241,5 V, docelowo $U_{WE\,max}$ = 253 V), a odpowiadający tej zmianie przyrost napięcia wyjściowego to ΔU_{WY} = 0,18 V.

$$S = \frac{\Delta U_{WE}}{\Delta U_{WY}} = 191 \qquad (2)$$

Dokonano również pomiaru tętnień w zakresie obciążenia 0 A ≤ I_{WY} ≤ 5 A przy U_{WE} = 230 V i otrzymano 0,2 mV ≤ U_T ≤ 4 mV

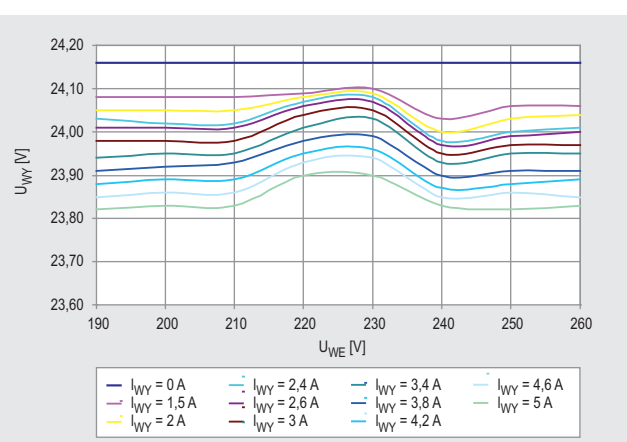
Wynik można uznać za bardzo dobry.

Sprawność η starannie zaprojektowanych zasilaczy impulsowych z nadzorem mikroprocesorowym znacznie wzrasta i może zawierać się w granicach 84% ≤ η ≤ 94%.

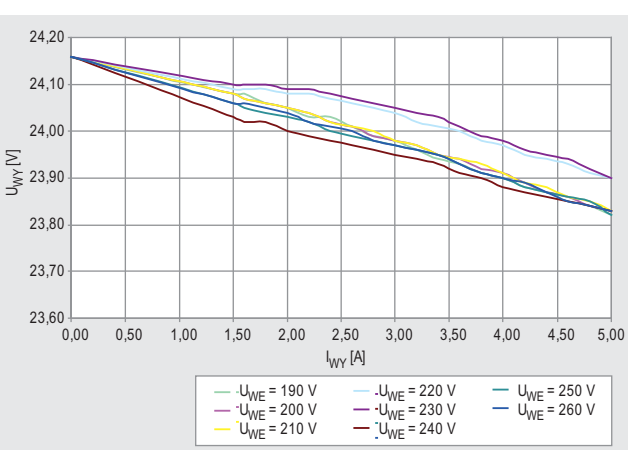
Badano również tzw. wskaźnik gotowości K_G zasilacza. Określenie wskaźnika gotowości (wynikające z teorii eksploatacji i niezawodności) to:

$$K_G = \frac{T_m}{T_m + T_n} \qquad (3)$$

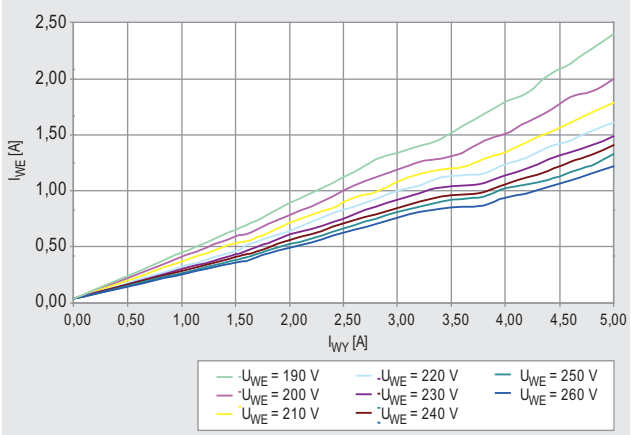
gdzie: K_G – stosunek wartości oczekiwanej czasu pracy układu zasilającego T_m do sumy wartości oczekiwanej czasu poprawnej pracy układu zasilającego T_m i czasu naprawy układu zasilającego T_n (także jego wymiany). Innymi słowy, współczynnik gotowości K_G to prawdopodobieństwo tego, że w określonej chwili t obiekt będzie znajdował się w stanie gotowości. Wskaźnik gotowości K_G przedstawia równanie 3.



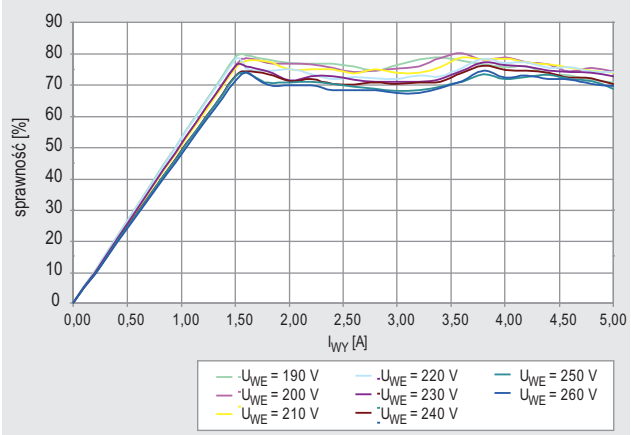
Rys. 5. Charakterystyki: $U_{WY} = f(U_{WE})$, gdy $I_{WY} = I_0$ = const



Rys. 6. Charakterystyki: $U_{WY} = f(I_{WY})$, gdy U_{WE} = const



Rys. 7. Charakterystyki: $I_{WE} = f(I_{WY})$, gdy $U_{WE} = const$



Rys. 8. Charakterystyki: sprawność $\eta = f(I_{WY})$, gdy $U_{WE} = const$

W takcie badań niezawodnościowo-eksploatacyjnych, które trwały 12 miesięcy (8760 godzin), stwierdzono, że czas naprawy pojedynczego uszkodzenia Tn wynosi 0,5 h, co daje wartość wskaźnika gotowości K_G = 0,99994. Należy wyraźnie podkreślić, że badany zasilacz był wykonany bardzo starannie przez renomowaną polską firmę specjalizującą się w budowie tego typu urządzeń. Nie wygląda to tak dobrze w przypadku bezmarkowych zasilaczy niewiadomego pochodzenia – wskaźnik K_G waha się w granicach od 0,4 do 0,5. Autorzy, którzy przeprowadzili badania, przestrzegają przed tego typu urządzeniami. Stwarzają one bardzo poważne zagrożenie poprawnej pracy elektronicznych systemów bezpieczeństwa.

Zakończenie

Zasilanie elektronicznych systemów bezpieczeństwa jest bardzo istotne ze względu na warunki pracy tych urządzeń (m.in. warunki klimatyczne i środowiskowe, zakłócenia elektromagnetyczne oraz wpływ na urządzenia nadzorujące bezpieczeństwo obiektu). W części pierwszej oraz wstępnej niniejszego artykułu zawarto ogólne informacje dotyczące budowy i zasad działania zasilaczy ze szczególnym uwzględnieniem zastosowania w transporcie (bardzo duże zakłócenia elektromagnetyczne pochodzące z trakcji i impulsowych przetwornic wagonowych). Podano także przykłady układów zasilających spotykanych w praktyce. Aby nie komplikować opisu, autorzy nie opisali zasilaczy, które uwzględniają własne źródła rezerwowe. Naturalnie chodzi tu o tzw. buforowy system pracy źródeł zasilających (przedstawiony na rys. 1, 2, 3). Niezmiernie istotna jest ciągła kontrola źródeł rezerwowych, która jest potrzebna po to, by w wyniku wadliwej eksploatacji nie doszło do ich trwałego uszkodzenia. Elektroniczne systemy bezpieczeństwa wykorzystywane w obiektach specjalnego przeznaczenia (także w obiektach związanych z transportem) powinny charakteryzować się bezawaryjną pracą podczas ich eksploatacji. Nie mogą oddziaływać w sposób niekontrolowany na inne układy elektroniczne zlokalizowane w danym obiekcie.

Techniczne badania, wśród nich pomiary parametrów (z konieczności tylko wybrane) przedstawione na rys. 5, 6, 7, 8, pokazują, jak ważne są wyniki pomiarów i jaki jest ich wpływ na prawidłową eksploatację elektronicznych systemów bezpieczeństwa. Autorzy zdają sobie sprawę, że w warunkach warsztatowych wykonanie takich badań stanowi bardzo poważne wyzwanie. Konieczna jest wyspecjalizowana aparatura i wiedza. Nawet najdoskonalszy elektroniczny system bezpieczeństwa przestanie funkcjonować, gdy zawiedzie zasilanie. Wskaźnik jakościowy K_G (tzw. wskaźniki gotowości) to bardzo ważny parametr eksploatacyjno-niezawodnościowy. Powinien on być bliski jedności. Na polskim rynku spotyka się wiele zasilaczy impulsowych pochodzących z niewiadomych źródeł, które ze względu na swoją awaryjność mogą uniemożliwić poprawną pracę elektronicznych systemów bezpieczeństwa.

doc. dr inż. Waldemar Szulc
Wyższa Szkoła Menedżerska w Warszawie
Wydział Informatyki Stosowanej i Technik Bezpieczeństwa

dr inż. Adam Rosiński
Wyższa Szkoła Menedżerska w Warszawie
Wydział Informatyki Stosowanej i Technik Bezpieczeństwa
Politechnika Warszawska
Wydział Transportu

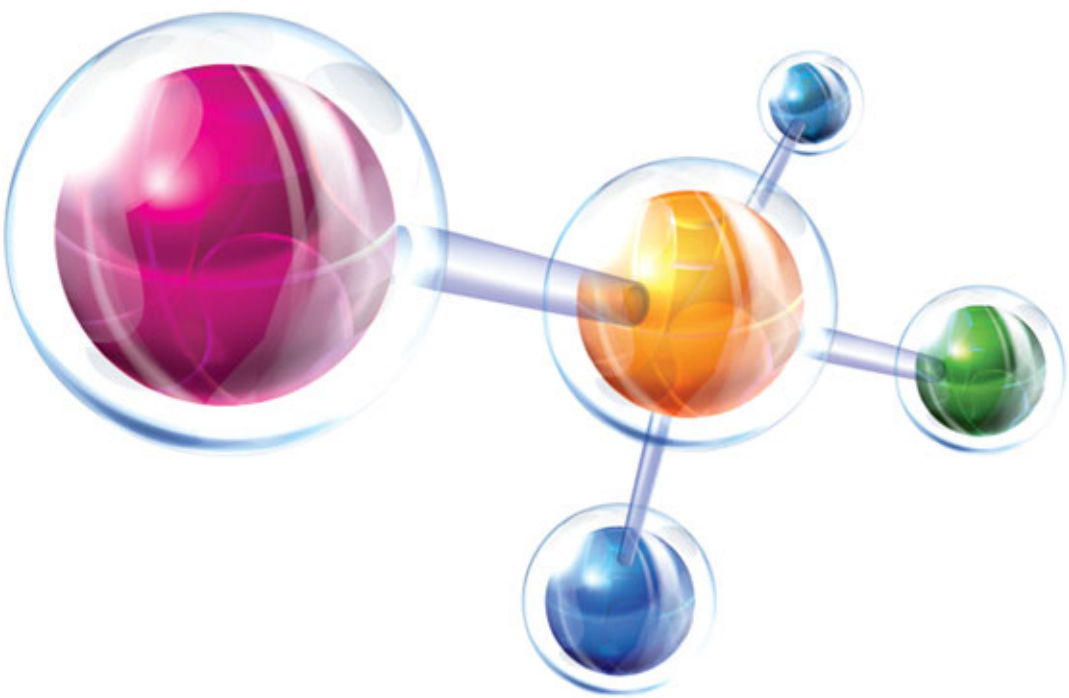
Bibliografia:

1. Dusza J., Gortat G., Leśniewski A., *Podstawy Miernictwa*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2009.
2. Haase L., *Zakłócenia w aparaturze elektronicznej*, Wyd. Radioelektronik, Warszawa 1995.
3. Horowitz P., Hill W., *Sztuka Elektroniki*, tom 1., WKiŁ, Warszawa 2006.
4. Kaźmierowski P, Matysik J., *Wprowadzenie do elektroniki i energoelektroniki*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2005.
5. Materiały informacyjne firmy PULSAR (instrukcje obsługi i montażu).
6. Normy: PN-EN 50131-1, PN-EN 50131-6, PN-EN 50132-7.
7. Szulc W., Rosiński A., *Wybrane zagadnienia z elektroniki cyfrowej dla informatyków*, Oficyna Wydawnicza WSM, Warszawa 2010.
8. Szulc W., Rosiński A., *Wybrane zagadnienia z miernictwa i elektroniki dla informatyków*, Oficyna Wydawnicza WSM, Warszawa 2008.

Monitorowanie systemów sygnalizacji włamania i napadu

z wykorzystaniem sieci Ethernet (część 1)

Adam Rosiński, Maciej Maszewski



W artykule przedstawiono zagadnienia związane z wykorzystaniem sieci Ethernet w systemach sygnalizacji włamania i napadu (SSWiN). Jest to obecnie jeden z bardziej rozwijanych i wykorzystywanych w praktyce sposobów łączności z SSWiN, już nie tylko do programowania, ale także do zarządzania. Artykuł został podzielony na trzy części. W pierwszej z nich zawarto wstęp oraz omówiono zagadnienia związane z łącznością w SSWiN. W części drugiej przedstawiono możliwości połączenia systemu do zarządzania i monitoringu z centralą alarmową poprzez sieć Ethernet. Część trzecia przedstawia koncepcje systemu bezpieczeństwa wykorzystującego Ethernet i odpowiednią, opracowaną z myślą o tym aplikację integrującą, która umożliwia zarządzanie wieloma systemami alarmowymi

1. Wstęp

Na rynku znajduje się obecnie wiele systemów do zabezpieczania obiektów. Są wśród nich zarówno systemy bardzo proste, które mają możliwości ograniczone do podstawowych funkcji, jak i inne, bardziej złożone, wymagające od użytkowników wiedzy na temat budowy całego systemu. Część z nich wykorzystuje zaawansowane technologie i można je rozbudować, dołączając urządzenia dodatkowe, poszerzające zakres funkcji systemu. Wszystkie te systemy można podzielić ze względu na ich funkcjonalność na: systemy sygnalizacji włamania i napadu (SSWiN), systemy monitoringu wizyjnego (CCTV), systemy kontroli dostępu (KD), systemy sygnalizacji pożarowej (SSP), systemy zarządzania budynkami (BMS), systemy zarządzania wentylacją i klimatyzacją (HVAC), systemy alarmowego centrum odbiorczego (ARC). Należy wspomnieć o grupie aplikacji, które nie są ściśle związane z systemami bezpieczeństwa, ale są bardzo istotne ze względu na zarządzanie nimi, zwłaszcza w przypadku rozbudowanych firmowych projektów, jakimi są systemy klasy ERP[1] służące między innymi do zarządzania zasobami ludzkimi i przechowujące dane o strukturze firmy. Umiejętne dobranie urządzeń i protokołów komunikacji między nimi oraz zaprojektowanie systemu scalającego urządzenia nowe i już istniejące stanowi poważne wyzwanie dla projektanta.

Rozwój połączeń sieciowych i Internetu ma coraz większy wpływ na technikę i organizację systemów bezpieczeństwa. Możliwości tkwiące w infrastrukturze internetowej zaczęto wykorzystywać w organizacji systemów zabezpieczeń technicznych, zapewniając globalne zarządzanie oraz optymalizację zasobów niezbędnych do ich właściwej obsługi. Poszczególne urządzenia pracujące w sieci mają przypisany adres IP, który umożliwia im wzajemną komunikację, jak również wymianę informacji z siecią znajdującą się poza chronionym obiektem, dzięki czemu można zdalnie nadzorować urządzenia. Konieczną do skutecznego i prawidłowego nadzorowania systemu dużą przepustowość łączy i szybkość transmisji sygnału na znaczne odległości zapewniają połączenia światłowodowe.

2. Systemy sygnalizacji włamania i napadu

Podstawowe funkcje systemu sygnalizacji włamania i napadu to:

– wczesne próby wykrywania włamania lub napadu,
– odstraszanie potencjalnego intruza,
– zapobieganie stratom w wyniku włamania, sabotażu itp.,
– ograniczenie do minimum wandalizmu,
– wczesne podjęcie środków i rozpoczęcie procedury interwencji.

Dodatkowe funkcje, jakie może posiadać taki system, to na przykład dostarczanie informacji o braku dopływu prądu do chronionego obiektu oraz o spadkach napięcia, informowanie o nieuruchomieniu systemu alarmowego, identyfikacja użytkownika. Wiele funkcji można w łatwy sposób dodać, korzystając z uniwersalnych wejść i wyjść centrali alarmowej i zewnętrznych komponentów, np. sygnalizujących warunki atmosferyczne panujące w chronionym obiekcie.

Priorytetowym zadaniem SSWiN jest zawsze jak najszybsze wykrycie zagrożenia i przekazanie informacji o nim służbom odpowiedzialnych za bezpieczeństwo chronionego obiektu.

Podstawowe elementy SSWiN [9]:

– centrala alarmowa,
– czujki,
– klawiatury,
– sygnalizatory (zewnętrzne i wewnętrzne, akustyczne i optyczne),
– zasilacze,
– akumulatory.

Dodatkowe elementy, w które może być wyposażony SSWiN:

– przyciski napadowe,
– urządzenia antysabotażowe sygnalizujące zagrożenia,
– urządzenia wykonawcze,
– moduły rozszerzeń,
– moduły powiadamiania telefonicznego, za pośrednictwem sieci GSM lub Internetu,
– moduły rozszerzeń dla elementów bezprzewodowych,
– piloty, karty magnetyczne,
– stacje PC monitorujące i (lub) zarządzające systemem,
– moduły światłowodowe umożliwiające podłączenie elementów znacznie oddalonych od siebie,
– drukarki,
– tablice synoptyczne.

Na rys. 1 przedstawiono jednostkę centralną SSWiN Integra firmy SATEL wraz możliwymi do podłączenia elementami. Można tu wyróżnić siedem kategorii urządzeń ze względu na rodzaj ich przyłączenia:

– urządzenia przyłączone przez magistralę manipulatorów,
– urządzenia przyłączone przez magistralę ekspanderów,
– urządzenia przyłączone do wejść,
– urządzenia przyłączone do wyjść,
– urządzenia przyłączone przez port RS232,
– urządzenia przyłączone przez łącze telefoniczne,
– urządzenia przyłączone przez gniazdo syntezatorów mowy.

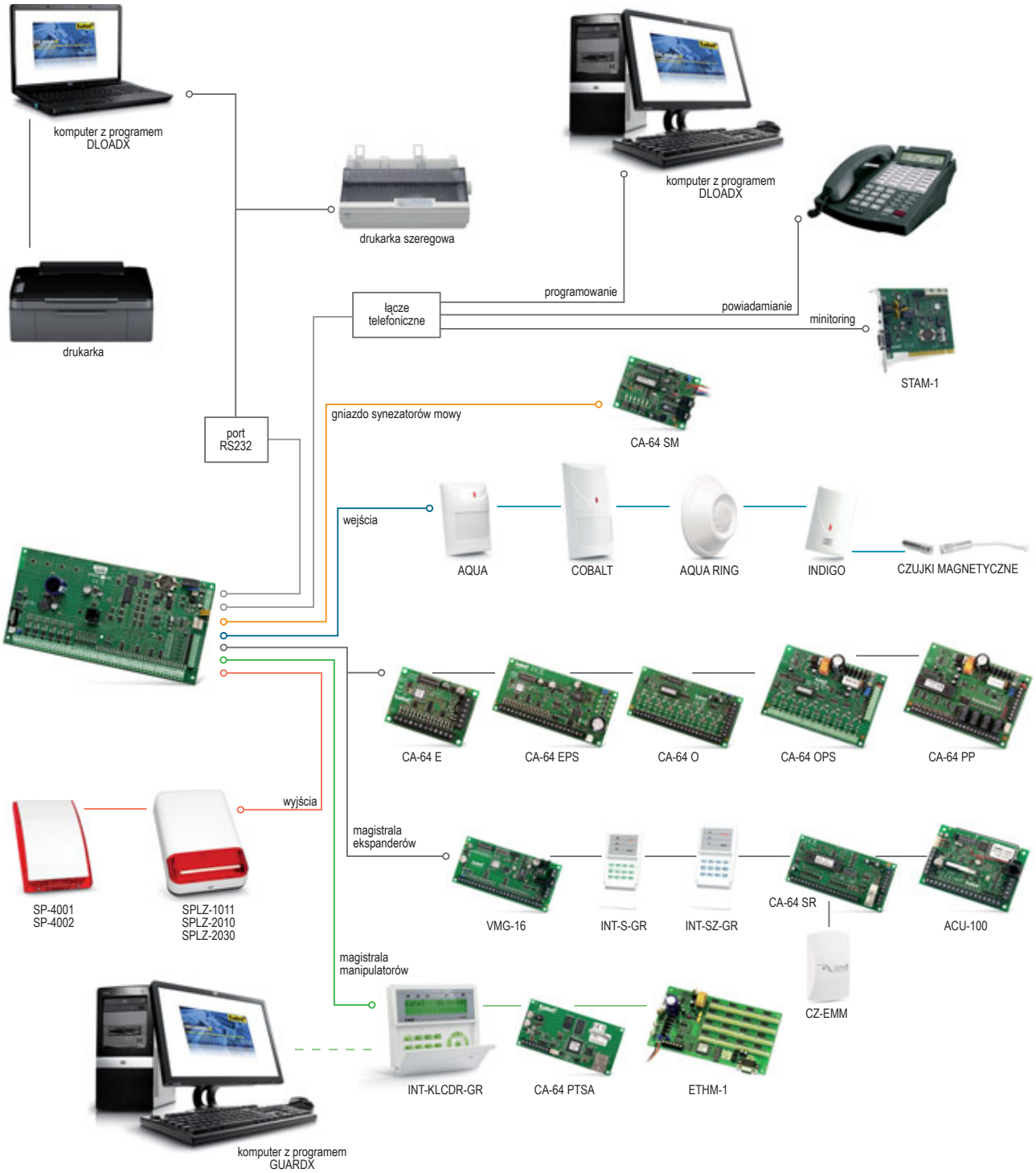
Struktury SSWiN zostały szczegółowo scharakteryzowane w artykule W. Szulca i A. Rosińskiego *Systemy sygnalizacji włamania*. Część 1 – *Konfiguracje central alarmowych* (*Zabezpieczenia* Nr 2(66)/2009) [11], dlatego też nie będą one obecnie powtórnie omawiane. Ich znajomość jest jednak niezbędna, by poprawnie zrozumieć omawiane w dalszej części niniejszego artykułu zagadnienia.

3. Łączność w SSWiN

Polska norma PN-EN 50131-1:2009 „Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 1: Wymagania systemowe" definiuje pojęcie łączności w systemie alarmowym, jako transmisję komunikatów i(lub) sygnałów między elementami składowymi systemu sygnalizacji włamania i napadu.

Łączność pomiędzy poszczególnymi elementami SSWiN może być realizowana na różne sposoby. Jest to uzależnione

1) ERP – ang. „Enterprise Resource Planning", czyli zaawansowane zarządzanie zasobami.



Rys. 1. Składniki SSWiN [1]

od producenta, potrzeby uwzględniającej warunki lokalizacyjne, odległości oraz konkretnego rozwiązania.

3.1 Łączność lokalna pomiędzy składnikami systemu

Elementy systemu wymagające jednostronnej komunikacji z centralą, takie jak przyciski napadowe, czujki magnetyczne, proste czujki PIR itp., mogą być podłączane do systemu alarmowego przy użyciu trzech podstawowych rodzajów linii dozorowych:

– konwencjonalnych,
– radiokomunikacyjnych,
– adresowalnych.

Linie dozorowe w systemie konwencjonalnym są najprostszym sposobem podłączenia elementów. Można wyróżnić następujące typy linii:

– zwykłe typu otwartego (NO[2]),
– zwykłe typu zamkniętego (NC[3]),
– parametryczne typu pojedynczego w trybie otwartym (EOL[4] NO),
– parametryczne typu pojedynczego w trybie zamkniętym (EOL NC),

2) NO – ang. normally open

3) NC – ang. normally closed

4) EOL – ang. End of Line

– parametryczne typu podwójnego w trybie otwartym (2×EOL NO),
– parametryczne typu podwójnego w trybie zamkniętym (2×EOL NC).

Linie adresowalne charakteryzują się tym, że każda z czujek podłączona do takiej linii jest wyposażona w moduł, który wysyła swój indywidualny numer identyfikacyjny. Informacja o numerach czujek zainstalowanych w systemie alarmowym znajduje się w centrali. Zaletą takiego rozwiązania jest niewielka liczba przewodów w instalacji składającej się z wielu czujek (informacje z różnych elementów wymieniane są tymi samymi przewodami), a także łatwość lokalizacji źródła alarmu (w porównaniu do czujek podłączonych do jednej linii dozorowej w wersji konwencjonalnej). Wadą – możliwość obezwładnienia większej liczby czujek w wyniku uszkodzenia linii.

Linie radiokomunikacyjne wykorzystują do wymiany informacji fale radiowe, stosując zazwyczaj protokoły transmisji opracowane przez producentów sprzętu. Do zalet takiego rozwiązania należy niewątpliwie uproszczenie instalacji ze względu na brak konieczności doprowadzenia linii przewodowych. Wadą jest większa podatność na zakłócenia oraz uzależnienie działania od transmisji fal radiowych.

Sygnalizatory, urządzenia wykonawcze są dołączane do centrali poprzez wyjścia, na których pojawia się sygnał analogowy lub cyfrowy (stan wysoki oraz stan niski) powodujący uruchomienie elementu podłączonego do danego wyjścia.

Elementy systemu wymagające dwustronnej komunikacji z centralą, takie jak manipulatory, moduły rozszerzeń, tablice synoptyczne, moduły komunikacyjne, czujki, podłączane są do magistrali systemowej.

W przypadku konieczności podłączenia elementu znacznie oddalonego od systemu można zastosować rozwiązanie pozwalające na przetransmitowanie sygnałów za pomocą takiego medium jak światłowód.

Urządzenia zewnętrzne, takie jak drukarka czy stacja PC, mogą wykorzystywać do łączności z systemem alarmowym formaty transmisji RS232, RS485 oraz RS422/423. Ze względu na to, że w stacjach PC dostępny jest tylko port RS232, do pozostałych dwóch formatów należy użyć konwerterów.

3.2 Zdalna łączność z systemem

Do zdalnego monitoringu i zarządzania systemem sygnalizacji włamania i napadu można wykorzystać następujące metody komunikacji [10]:
– sieć Ethernet,
– sieć GSM z wykorzystaniem transmisji pakietowej UMTS[5], EDGE[6] GPRS[7],
– sieć GSM z wykorzystaniem transmisji głosowej (np. DTMF[8]),
– sieć GSM z wykorzystaniem krótkich wiadomości tekstowych SMS[9],
– sieć telefoniczną PSTN[10],
– sieć telefoniczną ISDN[11].

4. Podsumowanie

W niniejszym artykule – pierwszej części cyklu artykułów dotyczących wykorzystania sieci Ethernet w monitorowaniu SSWiN – przedstawiono ogólnie zagadnienia związane z tymi systemami. Zwrócono przy tym szczególną uwagę na łączność w SSWiN (zarówno lokalną, jak i zdalną).

W części drugiej zostaną opisane możliwości łączności systemu zarządzania i monitorowania z centralą alarmową poprzez sieć Ethernet.

dr inż. Adam Rosiński
inż. Maciej Maszewski

Bibliografia

1) Centrala alarmowa INTEGRA – instrukcja instalatora, Satel.
2) Centrala alarmowa INTEGRA – instrukcja użytkownika, Satel.
3) Centrala alarmowa INTEGRA – instrukcja programowania, Satel.
4) Instrukcja modułu ETHM-1, Satel.
5) Instrukcja modułu INT-RS, Satel.
6) Instrukcja ogólna programu STAM-2, Satel.
7) Maszewski M., *Koncepcja wykorzystania sieci Ethernet w systemach bezpieczeństwa na bazie urządzeń firmy SATEL*, dyplomowa praca inżynierska, Wyższa Szkoła Menedżerska w Warszawie, Wydział Informatyki Stosowanej i Technik Bezpieczeństwa, Warszawa 2010.
8) Materiały dydaktyczne z Zespołu Laboratoriów Systemów Bezpieczeństwa Wydziału Informatyki Stosowanej i Technik Bezpieczeństwa Wyższej Szkoły Menedżerskiej w Warszawie.
9) Norma PN-EN 50131-1:2009: Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe.
10) Rosiński A., *Programowanie systemów sygnalizacji włamania i napadu*, 13th International Conference „Computer Systems Aided Science, Industry and Transport" TRANSCOMP 2009, Zakopane 2009.
11) Szulc W., Rosiński A., *Systemy sygnalizacji włamania. Część 1 – konfiguracje central alarmowych, Zabezpieczenia* Nr 2(66)/2009

5) UMTS – ang. Universal Mobile Telecommunications System

6) EDGE – ang. Enhanced Data Rates for GSM Evolution

7) GPRS – ang. General Packet Radio Service

8) DTMF – ang. Dual Tone Multi Frequency

9) SMS – ang. Short Message Service

10) PSTN – ang. Public Switched Telephone Network, czyli publiczna komutowana sieć telefoniczna

11) ISDN – ang. Integrated Services Digital Network, czyli sieć cyfrowa z integracją usług

Kolumny sygnalizacyjne serii KS-Ad

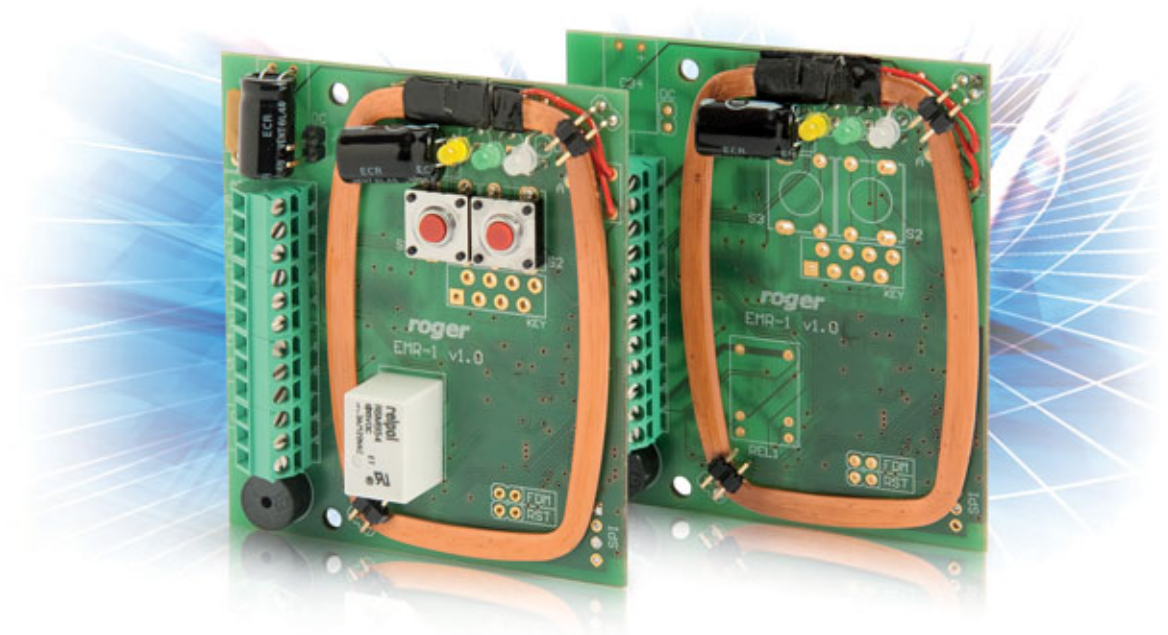
Seria kolumn sygnalizacyjnych przeznaczonych do pracy w układach automatyki przemysłowej, jak również w szeroko pojętych systemach sygnalizacji.
Kolumna serii KS-Ad jest odpowiednikiem klasycznych wież sygnalizacyjnych. Wykonana jest z tworzywa sztucznego ABS. W odróżnieniu od klasycznych rozwiązań, KS-Ad posiada wbudowane mechanizmy sterowania sygnałami akustyczno-optycznymi. Konstrukcja została oparta na diodach LED oraz przetworniku piezoceramicznym, dzięki czemu rozwiązanie jest energooszczędne.
Wbudowany mikroprocesorowy układ sterowania umożliwia sterowanie pracą kolumny za pomocą sygnału napięciowego 0-10 V_{DC} (sterowanie analogowe napięciowe), poprzez dołączanie do wejść kolumny rezystancji (sterowanie analogowe rezystancyjne) oraz poprzez stykowe zwieranie wejść kolumny do masy zasilania.
Kolumna umożliwia generowanie sygnałów optycznych: ciągłych; impulsowych; o nieregularnej częstotliwości; z modulowaną jasnością; stroboskopowych; obrotowych. Sygnały optyczne mogą być uzupełnione sygnałem tonowym. Wewnętrzne układy sterowania umożliwiają również wykonanie testu obwodów wejściowych i wykonawczych kolumny (test odbywa się poprzez zwarcie wejścia „TEST" do masy zasilania). W przypadku wersji wyrobu z modułem dźwiękowym, użytkownik ma możliwość wyłączenia sygnału tonowego w dowolnej chwili poprzez podanie masy zasilania na wejście blokady dźwięku. Dzięki zastosowaniu bloków rozłącznych, istnieje możliwość demontażu kolumny z maszyny bez konieczności demontażu okablowania (np. na czas transportu maszyny).
Wyrób dostępny jest w wersjach od 2 do 5 kolorów (standardowo czerwony, żółty, zielony, niebieski, biały), w kolorze obudowy białym lub czarnym, z mocowaniem prostym lub kątowym, z modułem dźwiękowym lub bez. Istnieje również możliwość wykonania kolumny z niestandardowym ułożeniem kolorów. Energooszczędna konstrukcja oparta na diodach LED.

Zalety:

- Uniwersalne sterowanie (napięciowe, rezystancyjne, stykowe)
- Sygnalizacja zdarzeń sygnałem optycznym lub akustyczno-optycznym
- Funkcja automatycznego testowania wewnętrznych obwodów sterowania
- Funkcja blokady sygnału dźwiękowego
- Łatwy montaż oraz demontaż dzięki zastosowaniu bloków rozłącznych

Producent:
W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. /faks 52 584 01 92
www.w2.com.pl
biuro@w2.com.pl

EMR-1
Uniwersalny moduł czytnika kart EM 125 kHz



EMR-1 jest uniwersalnym modułem czytnika zbliżeniowego kart standardu EM 125 kHz przeznaczonym do zabudowy w urządzeniach innych producentów lub w dowolnej obudowie. W wersji EMR-1-LT urządzenie działa jak standardowy czytnik zbliżeniowy serii PRTxxLT, natomiast w wersji EMR-1-SDC realizuje funkcję autonomicznego zamka na kartę zbliżeniową SDC66.

Charakterystyka:

EMR-1-SDC:

- Identyfikacja za pośrednictwem zbliżeniowych kart-kluczy
- Możliwość zaprogramowania do 120 kart-kluczy
- Opcja pracy z dowolną ilością kart-kluczy (każda karta-klucz otwiera drzwi)
- Selektywne dodawanie i usuwanie kart-kluczy
- Możliwość podłączenia czujnika otwarcia drzwi i przycisku wyjścia
- Wyjście przekaźnikowe 1.5 A/30 V i tranzystorowe 1 A/15 V
- Sygnalizacja stanów alarmowych
- Zasilanie z transformatora 12 V_{AC} lub zasilacza 12 V_{DC}
- Znak CE

Uwaga: *Moduł EMR-1-SDC współpracuje wyłącznie z następującymi transponderami zbliżeniowymi: EMKF-4, EMC-10, EMC-7*

EMR-1-LT:

- Odczyt kart EM 125 kHz
- Konfigurowalny format transmisji danych wyjściowych
- Formaty wyjściowe: Wiegand 26..66 bit, Magstripe (Clock & Data), RACS (Roger) i inne
- Rożne warianty transmisji kodów PIN oraz kodów klawiatury
- Osobne wejścia do kontroli wskaźnika LED oraz głośnika
- Zasilanie z zasilacza 12 V_{DC}
- Znak CE

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

Czytnik kart zbliżeniowych Mifare AV-G25 Helios

Doskonała jakość, bardzo wytrzymała konstrukcja, praca w każdych warunkach klimatycznych. Najwyższy poziom niezawodności w technologii zbliżeniowej.

Czytnik kart zbliżeniowych Mifare AV-G25 jest czytnikiem inteligentnych kart zbliżeniowych, pracującym w częstotliwości 13,56 MHz. Przeznaczony jest do stosowania w systemach kontroli dostępu, rejestracji czasu pracy, stołówkach i wszędzie tam, gdzie zachodzi potrzeba wykorzystania kart zbliżeniowych.

Czytnik Mifare AV-G25 charakteryzuje się ciekawym wzornictwem i kolorystyką (9 wersji kolorystycznych). Czytniki odczytują każdy rodzaj kart i tagów Mifare (standard, ultralight). Dzięki temu mogą stanowić alternatywę dla obecnie występujących produktów Mifare na naszym rynku.

Czytniki dostępne są w wykonaniu wewnętrznym lub zewnętrznym. Posiadają klawiaturę mechaniczną lub dotykową. Dostępna jest również opcja bez klawiatury. Dodatkowo każdy czytnik posiada wbudowany antysabotaż. Opcjonalnie urządzenia mogą być również wyposażone w kontroler, dzięki czemu mogą pracować jako pełny autonomiczny punkt dostępowy. Sygnalizacja stanów alarmowych odbywa się akustycznie i za pomocą kolorowych piktogramów.

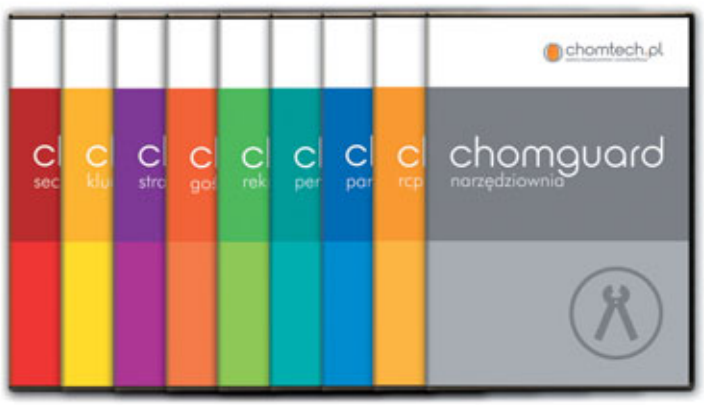
Podstawowe cechy drukarki	
Napięcie zasilania	od 9 do 16 V_{DC}
Zasięg odczytu	do 10 cm
Częstotliwość pracy	13,56 MHz
Temperatura pracy	od –35°C do 75°C
Format wyjściowy	Wiegand 26/34, ABATRACK2, ASYNC 9600, N, 8,1
Obudowa (materiał)	poliwęglan UL94
Wymiary	12,50×8,9×3,0 cm
Kolor	czarny, szary, srebrny, niebieski, czerwony, pomarańczowy, biały, zielony, żółty
Instalacja	na każdym podłożu
Sygnalizacja	dioda trójkolorowa i brzęczyk
Transmisja	szyfrowana, klucz 64 bity
Kontrolery	Avanguard, SD-108, IKR, IKR108, SD-660, SD-560
Masa	249,5 g
Wilgotność	5% – 95% bez kondensacji
Pobór prądu	50 / 75 mA przy zasilaniu 12 V_{DC}
Wodoodporny	IP 54

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

chomtech.pl sp. z o.o.
ul. Mieszczańska 5
30-313 Kraków

tel. 12 421 43 83, 428 12 00
faks 12 350 40 69
http://www.chomtech.pl

Chomguard – rodzina aplikacji przeznaczonych do wspomagania systemów bezpieczeństwa



chomguard®

Programy Chomguard są specjalistycznymi aplikacjami dedykowanymi do wspomagania zarządzania systemami bezpieczeństwa w obiektach dowolnego typu.

Aplikacje współpracują z kontrolerami, czytnikami kontroli dostępu, drukarkami do kart plastikowych, kamerami IP, wideorejestratorami, tripodami, furtami stadionowymi, centralami alarmowymi, rejestratorami czasu pracy, urządzeniami biometrycznymi, drukarkami fiskalnymi oraz innymi aplikacjami typu: MRP, CRM, HR stosowanymi do wspomagania zarządzania przedsiębiorstwem.

Programy Chomguard są podzielone na osobne tematycznie moduły które można łączyć w zależności od potrzeb użytkownika (rozwoju firmy) w bardzo zaawansowane systemy wykorzystujące sieci LAN, WAN, przeglądarki internetowe (praca rozproszona). Pracują na jednej bazie danych co oznacza, że wprowadzenie osoby do systemu w jednym module będzie równoznaczne z aktualizacją w pozostałych modułach Chomguard (dostępne silniki baz: Oracle, MSSQL, MySQL, PostgreSQL, Firebird).

- **Chomguard Security:** aplikacja przeznaczona do sterowania i wizualizacji systemów kontroli dostępu, telewizji dozorowej, alarmu, włamania i napadu – w zależności od wersji
- **Chomguard Klucze:** aplikacja przeznaczona do procesu zarządzania kluczami na terenie obiektu w którym występuje duża liczba pomieszczeń
- **Chomguard Strażnik:** aplikacja przeznaczona do weryfikacji osób wchodzących na teren zakładu pracy lub innych miejsc, gdzie występuje konieczność potwierdzenia tożsamości
- **Chomguard Goście:** aplikacja przeznaczona do kontroli obecności osób (gości) przebywających czasowo na terenie przedsiębiorstwa
- **Chomguard Rekreacja:** aplikacja przeznaczona do obsługi klientów obiektów rekreacyjnych z pełnym rozliczaniem usług np. basen, sauna, siłownia, catering itp.
- **Chomguard Personalizacja:** aplikacja przeznaczona do tworzenia projektów kart identyfikacyjnych oraz wydruków
- **Chomguard Parking:** aplikacja przeznaczona do zarządzania parkingiem komercyjnym lub zamkniętym, współpraca z biletерką, czytnikami, szlabanami itp.
- **Chomguard RCP:** aplikacja służąca do rejestrowania i automatycznego rozliczania czasu pracy
- **Chomguard Narzędziownia:** aplikacja służąca do ewidencji i nadzoru nad cennymi zasobami przedsiębiorstwa

chomtech.pl®
systemy bezpieczeństwa i autoidentyfikacji

chomtech.pl sp. z o.o.
ul. Mieszczańska 5
30-313 Kraków

tel. 12 421 43 83, 428 12 00
faks 12 350 40 69
http://www.chomtech.pl

Kamera XGB-21CS

XGB-21CS to kamera o bardzo wysokiej czułości i rozdzielczości (580 TVL w trybie kolorowym, 650 TVL w trybie B/W), wyróżniająca się bardzo dobrym i wiernym odwzorowaniem kolorów oraz przemyślanym systemem mocowania poprzez zastosowanie uchwytu pośredniczącego. Ten lekki i niewielkich rozmiarów uchwyt przykręcamy do ściany i dopiero do niego mocujemy kamerę. Niebanalny i estetyczny wygląd kamery pozwala lepiej wkomponować się w elewacje nowo budowanych obiektów.
W kamerze zastosowano procesor obróbki sygnału Blue-I.
W XGB-21CS, podobnie jak w CCM-21VF czy CBM-25VD, zastosowano diody SR LED (Single Reflective LED). Mimo mniejszej liczby diod niż w rozwiązaniach z konwencjonalnymi diodami osiągnięto równomierne oświetlenie obserwowanej sceny, a dodatkową zaletą jest mniejsza emisja ciepła.

Zalety:

- wbudowany jasny obiektyw F1,2 o zmiennej ogniskowej 7,5÷50 mm z automatyczną przysłoną DC,
- dodatkowe serwisowe wyjście wideo,
- mechaniczny filtr podczerwieni IR - TDN(ICR),
- funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 128 ramek zwiększająca czułość kamery,
- promiennik podczerwieni o zasięgu do 80 m,
- grzałka i wentylator,
- XWDR – poszerzony zakres dynamiki kamery,
- cyfrowa stabilizacja obrazu DIS,
- redukcja szumów 3D DNR, w porównaniu ze standardową redukcją DNR zapewnia zmniejszenie smużeń przemieszczających się obiektów,
- ukryty kabel w uchwycie.

Właściwości:

- bardzo wysoka rozdzielczość 580 TVL w trybie kolorowym oraz 650 TVL w trybie czarno-białym,
- 6,13-krotny cyfrowy zoom,
- menu ekranowe OSD,
- AGC, WDR, Eclipsa, BLC, AWB, 3D DNR, DIS, Flickerless, D/N, DZ – regulacja przez OSD,
- zasilanie 12 V_{DC}.

Model	XGB-21CS
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD II CCD
Rozdzielczość efektywna	752(H)×582(V) 440K
Rozdzielczość	580 TVL kolor, 650 TVL B/W
Wyjście wideo	1,0V_{p-p}, 75 Ohm
Odstęp sygnał/szum	>52 dB (wył. AGC)
WDR	on (3 poziomy, maks. 60 dB) /off
Obiektyw	f=7,5~50 mm, F1,2
Tryb dzień/noc	auto
Czułość	0,05 lx (kolor) / 0,0002 (DSS on, BW) / 0,00 lx (IR LED włączone)
Menu OSD	angielski, chiński, koreański, rosyjski, hiszpański, francuski
Podczerwień	SR IR LED 12EA (850 nm), czujnik 1EA
Zasięg promiennika IR	maks. 80 m
Cyfrowa redukcja szumu	3D DNR, 63 poziomy / wył.
Funkcja DSS	do 128 ramek obrazu
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	wł./3 poziomy
Eclipsa	16 stref
Kompensacja światła tylnego	BLC/3 poziomy
Redukcja migotania	wł./wył.
Cyfrowa stabilizacja obrazu	wł./wył.
Cyfrowy zoom	6,13x
Strefy prywatności	8 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Elektroniczna migawka	1/50~1/90 000 s
Stopień ochrony IP	IP67
Zasilanie	12 V_{DC}
Pobór prądu	maks. 1,7 A / 20 W
Wymiary (szer. x wys. x gł.)	125,7 x 222,3 x 372,4 mm
Temperatura pracy / Wilgotność	-30°C~50°C / 30%~80% RH
Masa	3,8 kg

Dystrybucja: GDE POLSKA
GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel./faks 12 256 50 35, 256 50 25
faks 12 270 56 96
e-mail: biuro@gde.pl

Kamera XCM-25VF

CNB TECHNOLOGY Inc.
ORYGINAL DESIGN

Wyróżniająca się estetyczną obudową kompaktowa kamera XCM-25VF charakteryzuje się bardzo wysoką czułością i rozdzielczością 600 TVL w trybie kolorowym oraz 650 TVL w trybie B/W.
Kamera przeznaczona jest do zastosowań zewnętrznych. Wyróżnia się zastosowanym procesorem obróbki sygnału Monalisa oraz technologią Intelligent IR. Intelligent IR to nowy rodzaj pracy promiennika IR opracowany przez dział badawczy firmy CNB. Eliminuje on efekt przejaskrawienia i rozmycia obrazu dla zbliżającego się obiektu. W standardowym rodzaju pracy jasność świecenia jest stała, dlatego bliskie obiekty są oświetlone tak samo jak dalekie, co w praktyce może spowodować prześwietlenie obrazu. Technologia Intelligent IR steruje jasnością podświetlenia w zależności od odległości od obserwowanego obiektu.

Zalety:

- wbudowany obiektyw o zmiennej ogniskowej 3,8-9,5 mm,
- mechaniczny filtr podczerwieni – TDN(ICR),
- zasięg promiennika podczerwieni do 35 m,
- Intelligent IR – adaptacyjna praca promiennika IR,
- SBLC – ulepszona odmiana BLC, czyli kompensacji tylnego oświetlenia,
- zasilanie dualne 12 V_{DC} / 24 V_{AC} – łatwiejsza instalacja w przypadku znacznego oddalenia kamer od źródeł zasilania.

Powyższe funkcje posiadają również kamery: B2310PVF (odsuwany filtr IR, obiektyw 3,8÷9,5 mm DC), B2810PVF (odsuwany filtr IR, funkcja DSS, obiektyw 3,8÷9,5 mm DC) oraz WCL-21S/WCL-11S z obiektywami o stałej ogniskowej 6 mm.

Właściwości:

- kamera dzień/noc
- przetwornik 1/3" Sony Super HAD II
- wysoka rozdzielczość 600 TVL (kolor), 650 TVL B/W)
- czułość 0,05 lx (kolor), 0,005 lx (BW), 0,00 lx (IR LED włączone)
- obiektyw 3,8-9,5 mm
- obudowa przystosowana do montażu ściennego lub sufitowego
- regulacje jasności oraz koloru
- AGC, SBLC, AWB, DNR, Flickerless, D/N – regulacja z poziomu menu ekranowego
- detekcja ruchu, strefy prywatności oraz funkcja mirror
- zasilanie dualne 12 V_{DC}/24 V_{AC}

Model	XCM-25VF
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD II CCD
Rozdzielczość efektywna	752(H)×582(V) 440K
Rozdzielczość	600 TVL kolor, 650 TVL B/W
Wyjście wideo	1,0V_{p-p}, 75 Ohm
Odstęp sygnał/szum	>50 dB (wył. AGC)
Obiektyw	f=3,8~9,5 mm, F1,2
Tryb dzień/noc	auto
Czułość	0,05 lx (kolor) / 0,005 lx (B/W) / / 0,00 lx (IR LED włączone)
Menu OSD	angielski, chiński
Podczerwień	Intelligent IR LED 42EA (850 nm, 30°)
Zasięg promiennika IR	maks. 35 m
Cyfrowa redukcja szumu	SDNR, 3 poziomy / wył.
Funkcja DSS	-
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	wł./wył.
Kompensacja światła tylnego	SBLC /3 poziomy
Redukcja migotania	wł./wył.
Strefy prywatności	4 programowalne strefy
Detekcja ruchu	4 programowalne strefy
Elektroniczna migawka	1/50~1/120 000 s
Stopień ochrony IP	IP66
Zasilanie	12 V_{DC} / 24 V_{AC}
Pobór prądu	maks. 0,5 A / 6,6 W
Wymiary (szer. x wys. x gł.)	92,2 x 218 mm
Temperatura pracy / Wilgotność	-10°C~50°C / 30%~80% RH
Masa	900 g

Dystrybucja: GDE POLSKA

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany

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

Monitor wideodomofonowy CDV-40Q

Monitor COMMAX CDV-40Q to nowy model w grupie analogowych systemów wideodomofonowych. Przeznaczony jest do użytku w domach jedno- lub wielorodzinnych. Zastosowanie 4-calowego wyświetlacza LCD zapewnia wysoką jakość wyświetlanego obrazu. Monitor obsługuje dwa panele wejściowe umożliwiając kontakt audiowizualny np. z dwoma furtkami (wraz z funkcją otwarcia obu wejść) Zestaw wideodomofonowy może być rozbudowany o dodatkowe monitory z serii CDV-xxx oraz unifony DP-4VH (dostępne w pięciu wersjach kolorystycznych) z funkcją interkomu wewnątrz budynku. Monitor wyposażony jest w podświetlane, sensoryczne przyciski obsługi. Współpracuje z panelem wejściowym w systemie 4-żyłowym umożliwiając konfigurację odpowiedniego zestawu według własnych potrzeb. Ponad 40-letnie doświadczenie firmy COMMAX w projektowaniu elementów systemów wideodomofonowych gwarantuje użytkownikowi doskonałą jakość i bezawaryjną pracę przez długi czas.

Właściwości:

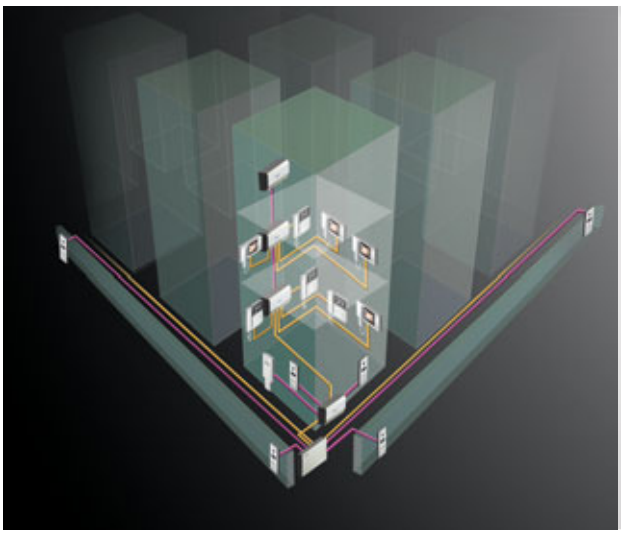
- monitor kolorowy,
- wyświetlacz 4" Color TFT-LCD 16:9,
- standard sygnału wideo PAL/NTSC,
- obsługa dwóch wejść (dwa panele wejściowe),
- sensoryczne przyciski,
- możliwość podłączenia dodatkowego monitora,
- współpraca z unifonami DP-4VR, DP-4VH,
- paging pomiędzy stacjami,
- instalacja czteroprzewodowa + obwód elektrozamka,
- współpracuje z kamerami analogowymi czteroprzewodowymi,
- zasilanie 230 V,
- wymiary: 235x140x36 mm.

Dystrybucja: GDE POLSKA

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany

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

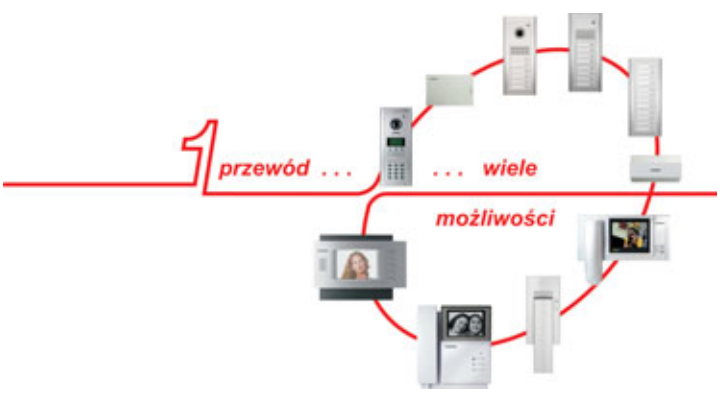
System wieloabonentowy serii 2400

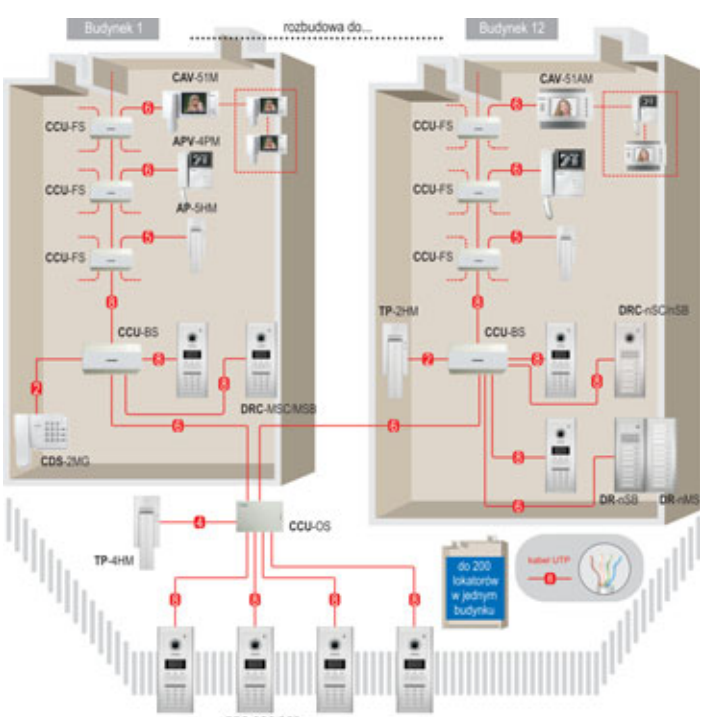


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna ilość obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu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

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

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak wideo - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów). System może być wyposażony w unifon lub stację portierską instalowaną w portierni, przez co lokatorzy oraz osoby ich odwiedzające mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków, jak i całych osiedli zamkniętych, gdzie ogrodzonych może być klikanaście budynków, a całość nadzorowana przez kilku portierów.





Dystrybucja:

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany

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

RioPro – Profesjonalna drukarka do kart identyfikacyjnych

Profesjonalna drukarka zaprojektowana do seryjnego wydruku identyfikatorów. Rio Pro to niezawodna, szybka i łatwa w obsłudze drukarka umożliwiająca w każdym momencie użytkowania szybką zmianę trybu pracy na drukowanie dwustronne. Wbudowane opatentowane funkcje HoloKote i HoloKoteFlex zabezpieczają karty przed nieautoryzowanym kopiowaniem. Funkcje te dają również możliwość personalizacji znaku wodnego zawierającego tekst lub logo firmy. Standardowo, podczas procesu wydruku karta pokrywana jest cienką folią (overlay) zabezpieczającą nadruk przed uszkodzeniem mechanicznym i promieniami UV. Rio Pro i Rio Pro Duo wyposażone są w wyświetlacz LCD z menu w języku polskim informujący o statusie drukarki. Drukarki posiadają 3-letnią gwarancję łącznie z mechanicznymi uszkodzeniami głowicy. Drukarki posiadają certyfikat CE i RoHS.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 23 sekundy
- Monochromatyczny wydruk karty w 6 sekund
- Interfejs do PC: USB i Ethernet
- Menu wyświetlacza w języku polskim
- Sterowniki 32 i 64 bit w języku polskim: Windows 2000, XP, Vista, Windows 7
- Rozdzielczość wydruku: 300 dpi
- Podajnik na 100 kart
- Odbiornik na 70 kart
- Możliwość ręcznego podawania kart
- Zasilanie: 100-240 V / 50-60 Hz
- Wymiary / Masa: 470 mm x 220 mm x 250 mm / 4,9 kg
- Temperatura pracy: od 10°C do 30°C
- 5 wzorów znaków wodnych do wyboru
- Wydruk na kartach wielkości CR-80 oraz CR-79
- Automatyczna regulacja grubości karty
- 3 lata gwarancji z możliwością przedłużenia do 4 lat, łącznie z mechanicznymi uszkodzeniami głowicy

Opcje dodatkowe:

Możliwość aktualizacji do wersji dwustronnej

Możliwość drukowania dwustronnego (Rio Pro Duo)

Możliwość kodowania kart magnetycznych, chipowych i zbliżeniowych

Taśmy

- Kolorowa 5 paneli nadruk 300 kart (MA300YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Kolorowa + czarna nadruk dwustronny 250 kart (MA250YMCKOK)
- Kolorowa 5 paneli nadruk 100 kart (MA100YMCKO)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 x 54) oraz CR-79 (84,1 x 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch

Zestaw czyszczący

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

Dystrybucja:

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

Pronto – Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

Mała, kompaktowa drukarka o nowoczesnym wyglądzie do zastosowania w każdej firmie i w każdym miejscu. Do szybkiego drukowania identyfikatorów oraz różnego rodzaju kart plastikowych. Drukarka Pronto jest łatwa w konfiguracji i użytkowaniu, posiada instrukcję i sterowniki w języku polskim do Windows 2000, XP, Vista, 7 i zapewnia niezawodne drukowanie kart przez wiele lat. Drukarka Magicard Pronto umożliwia wykorzystanie HoloKote i HoloPatch – opatentowanych zabezpieczeń przed nieautoryzowanym kopiowaniem kart.

Dzięki drukarce Pronto możesz samodzielnie wykonać kolorowe i monochromatyczne nadruki wysokiej jakości.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
- Monochromatyczny wydruk karty w 7 sekund
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1. (kompatybilny z USB 2.0)
- Sterowniki w języku polskim: Windows 2000, XP, Vista, 7
- Rozdzielczość wydruku: 300 dpi
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 270 mm × 215 mm × 233 mm / 4,4 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

Taśmy

- YMCKO 5 paneli nadruk 300 kart (MA300YMCKO)
- YMCKO 5 paneli nadruk 100 kart (MA100YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna zielona nadruk 1000 kart (MA1000K-GREEN)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 × 54) oraz CR-79 (84,1 × 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch i kartach do wielokrotnego zadruku TRW.

Zestaw czyszczący

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

Dystrybucja:

ACSS

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

tel. 22 832 47 44, faks 22 832 46 44
e-mail: biuro@acss.com.pl
http://www.acss.com.pl

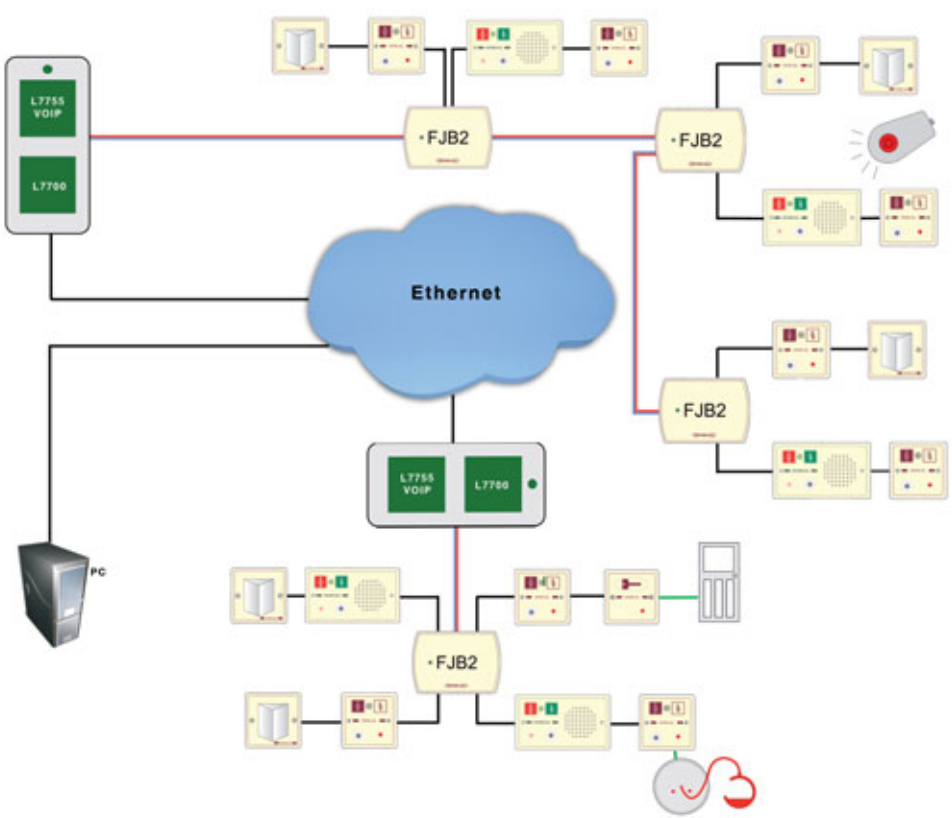
Intercall – szpitalny system przywoławczy

Prosty w instalacji – pomocny dla obsługi – zapewniający bezpieczeństwo pacjenta

Intercall jest najwyższej jakości systemem przywoławczym przeznaczonym dla specjalistycznych placówek opieki zdrowotnej (szpitale, domy opieki, hospicja itp.). Prosty w obsłudze i łatwy w rozbudowie, oferuje wyjątkowe funkcje: komunikację głosową (Intercall 700), rejestrację przywołań, przywołania o różnych priorytetach, czytelną i dokładną informację o rodzaju alarmu oraz miejscu wywołania.

Intercall zapewnia również maksymalnie uproszczony proces instalacji systemu, a dzięki 2-żyłowej magistrali (Intercall 600) pozwala na zastąpienie systemów starszej generacji, bez konieczności wymiany okablowania.

- Nieograniczone możliwości rozbudowy zarówno w zakresie punktów przywoławczych, jak i urządzeń sygnalizacyjnych
- Buforowanie oraz bieżący podgląd zdarzeń
- Dwukierunkowa komunikacja w trybie głośnomówiącym bez użycia słuchawek (Intercall 700)
- Definicja priorytetów zdarzeń alarmowych
- Możliwość bezpośrednich wydruków oraz powiadomienia na pager
- Szeroka gama punktów przywoławczych, w tym maty ciśnieniowe, czujniki moczenia, czujki ruchu, ręczne aktywatory ściskowe, ustne podmuchowe, łazienkowe oraz zdalne nadajniki podczerwieni
- Instalacja czterożyłowa (dwużyłowa przy systemie bez komunikacji głosowej)
- Bezpośrednie i zdalne konfigurowanie urządzeń za pomocą komputea PC



Dystrybucja: alarmnet®

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. 22 663 40 85, faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

Inteligentny Tester Akumulatorów GOLD-PLUS został zaprojektowany do testowania akumulatorów 6-voltowych o pojemności od 1,2 h do 12 Ah oraz 12-voltowych o pojemności od 1,2 Ah do 100 Ah. Zastosowana technologia symulacji pełnego rozładowania skraca normalny test rozładowania z 20 godzin do 20 sekund. Automatycznie wyświetla napięcie akumulatora i aktualną pojemność. Dzięki funkcji kalibracji testera możliwe jest testowanie szczelnych akumulatorów (SLA) wykonanych w technologii AGM, żelowych do pracy cyklicznej oraz akumulatorów samochodowych. Akumulatory można testować wielokrotnie bez przerw pomiędzy pomiarami. Wbudowana dioda LED ostrzega przed odwróceniem polaryzacji.

Wymiana akumulatora jest zalecana, jeżeli jego współczynnik pojemności spada poniżej 65%. Na obudowie umieszczona jest tabela referencyjna wskazująca, kiedy akumulator powinien zostać doładowany lub wymieniony.

Cechy charakterystyczne

- Testuje w ciągu 20 sekund 6- i 12-voltowe szczelne akumulatory (SLA) - AGM i żelowe oraz akumulatory samochodowe,
- automatycznie wyświetla napięcie akumulatora i aktualną pojemność,
- może być skalibrowany do testowania akumulatorów szczelnych, żelowych i samochodowych o pojemności od 1,2 Ah do 100 Ah,
- zabezpieczony przed odwróceniem polaryzacji,
- testuje akumulatory szybko, dokładnie i jest łatwy w użyciu,
- zastosowanie – akumulatory w systemach alarmowych, zasilaczach UPS, samochodach elektrycznych i spalinowych.

Parametry techniczne	
Model	GOLD- PLUS
Typy akumulatorów	szczelne (SLA) – AGM i żelowe samochodowe akumulatory obsługowe
Pojemność akumulatorów	6 V 1,2 Ah – 12 Ah oraz 12 V 1,2 Ah – 100 Ah
Impulsowe obciążenie akumulatora podczas pomiaru	6 A dla akumulatorów 1,2 Ah – 9,9 Ah, 18 A dla akumulatorów 10 Ah – 100 Ah
Kalibracja Ah	Kalibrowany w pozycji 0 dla nowego, w pełni naładowanego akumulatora SLA o temperaturze 20-25 °C. Regulacja kalibracji w zakresie 00-99 dla akumulatorów żelowych i samochodowych
Wyświetlacz	podświetlany LCD
Ostrzeżenie o odwróconej polaryzacji	czerwona dioda LED
Ostrzeżenie o zbyt niskim napięciu akumulatora	dla 6 V < 5,25 V_{DC}, dla 12 V < 12,0 V_{DC}
Tolerancja pomiaru Ah	+/- 10 % (zależy od konstrukcji i parametrów produkcyjnych)
Tolerancja pomiaru VDC	+/- 2 %
Zabezpieczenie odwrócenia polaryzacji	tak
Zdolność wykonania kolejnych testów	natychmiastowa
Obudowa	ABS
Szczelność	IP54
Wymiary	210 mm × 110 mm × 41 mm
Masa	600 g (w opakowaniu)
Wyposażenie	Przewody testowe, futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

Dystrybucja: alarmnet®

Alarmnet Sp. j.
ul. Karola Miarki 20c
01-496 Warszawa

tel. 22 663 40 85, faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
http://www.alarmnet.com.pl

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ALARMNET 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:
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

AMBIENT SYSTEM Sp. z o.o.
ul. Sucha 25
80-531 Gdańsk
tel./faks 58 345 51 95
e-mail: ambient@ambientsystem.pl
www.ambientsystem.pl

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

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

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

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

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

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

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

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

ul. Kutrzeby 16G, 61-714 **Poznań**
tel. 32 790 76 37
faks 32 790 76 70
e-mail: poznan@e-alpol.com.pl

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

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

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

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

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

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. 71 363 17 53, faks wew. 7
e-mail: anma@anma-pl.eu
www.anma-pl.eu

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

ATLine Sp. J.
Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. 42 657 30 80
faks 42 655 20 99
e-mail: info@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
Security Systems
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. 12 410 85 10
faks 12 410 85 11
e-mail: saik@saik.pl
www.saik.pl

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

CAMSAT
ul. Ogrodowa 2a
86-050 Solec Kujawski /k. Bydgoszczy
tel. 52 387 36 58, 387 54 66, faks wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

CBC (Poland) Sp. z o.o.
ul. Krasińskiego 41A
01-755 Warszawa
tel. 22 633 90 90
faks 22 633 90 60
e-mail: handlowy@cbcpoland.pl
www.cbcpoland.pl

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

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

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

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

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

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

CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U15
02-777 Warszawa
tel. 22 855 00 17
faks 22 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

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

D+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. 71 323 52 50
faks 71 323 52 40
e-mail: dh-polska@dh-partner.com
www.dhpolska.pl

Oddziały:
ul. Hagera 41, 41-800 **Zabrze**
tel. 32 375 05 70
faks 32 375 05 71

ul. Płochocińska 19 lok. 44-45, 03-191 **Warszawa**
tel. 22 614 39 52
faks 22 614 39 64

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

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

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

ul. Wołczyńska 18, 60-003 **Poznań**
tel. 61 863 82 08
faks 61 866 64 16

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

DOM Polska Sp. z o.o.
ul. Krótka 7/9
42-200 Częstochowa
tel. 34 360 53 64
faks 34 360 53 67
e-mail: dom@dom-polska.pl
www.dom-polska.pl

DPK System
ul. Piłsudskiego 41
32-020 Wieliczka
tel. 12 288 14 26 , 288 23 75
faks 12 278 48 91
e-mail: jablotron@jablotron.pl; biuro@dpksystem.pl
www.jablotron.pl

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

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

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

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

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

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

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

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

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

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

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

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

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. 91 489 41 81, 434 67 38
faks 91 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

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

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

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

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

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

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

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

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

NAPCO POLSKA
ul. Pszona 2
31-462 Kraków
tel. 12 410 05 10, 410 05 11
faks 12 412 13 12
e-mail: napco@napco.pl
www.napco.pl

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

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

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

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

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

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

P.P.H. PETROSIN Sp. z o.o.
ul. Rysi Stok 8/2
30-237 Kraków
tel. 12 266 87 92
faks 12 266 99 26
e-mail: office@petrosin.pl
www.petrosin.pl

Oddziały:
ul. Fabryczna 22, 32-540 **Trzebinia**
tel./faks 32 618 02 00, 618 02 02

ul. Chemików 1, 32-600 **Oświęcim**
tel. 33 847 30 83
faks 33 847 29 52

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

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

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

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

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

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

RETT-POL Telewizja Przemysłowa i Telekomunikacja
ul. Podmiejska 21
01-498 Warszawa
tel. 22 664 84 63
faks 22 833 09 07
e-mail: michal.dziwniel@rettpol.com.pl
www.rettpol.com.pl

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

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

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

SATIE
ul. Łączyny 3
02-820 Warszawa
tel. 22 462 30 86
faks 22 462 30 87
e-mail: info@satie.pl
www.satie.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.pl

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

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

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

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

P.T.H. SECURAL
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

S.M.A.
System Monitorowania Alarmów Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. 22 651 88 61
faks 22 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

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

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

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

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

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

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

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

SONY EUROPE LIMITED, Sp. z o.o. Oddział w Polsce
ul. Ogrodowa 58
00-876 Warszawa
tel. 22 520 25 73
tel. kom. 600 206 173
faks 22 520 25 77
e-mail: marcin.witkowski@eu.sony.com
www.sonybiz.net

SPRINT S.A.
ul. Jagiellończyka 26
10-062 Olsztyn
tel. 89 522 11 00
faks 89 522 11 25
e-mail: sprint@sprint.pl
www.sprint.pl

Oddziały:
ul. Przemysłowa 15, 85-758 **Bydgoszcz**
tel. 52 365 01 01
faks 52 365 01 11

ul. Budowlanych 64E, 80-298 **Gdańsk**
tel. 58 340 77 00
faks 58 340 77 01

ul. Heyki 27C, 70-631 **Szczecin**
tel. 91 485 50 00
faks 91 485 50 12

ul. Canaletta 4, 00-099 **Warszawa**
tel. 22 826 62 77
faks 22 827 61 21

S.P.S. Trading Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. 22 518 31 50
faks 22 518 31 70
e-mail: warszawa@spstrading.pl
www.aper.com.pl

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

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

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

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

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

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

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

SYSTEM 7
ul. Krakowska 33
43-300 Bielsko-Biała
tel. 33 821 87 77
Infolinia 801 000 307
faks 33 816 91 88
e-mail: biuro@s7.pl
www.system7.pl
Internetowa Hurtownia Zabezpieczeń:
www.system7.biz

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

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

TAYAMA POLSKA
Robert Prandota, Henryk Prandota, Krystyna Prandota Spółka Jawna
ul. Słoneczna 4
40-135 Katowice
tel. 32 258 22 89
faks 32 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. 22 516 97 77
faks 22 516 97 87
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. 12 398 99 00
faks 12 398 99 01
e-mail: biuro@unicard.pl
www.unicard.pl

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

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

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
AGIS Fire and Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	–	TAK	–	–
Alarmtech Polska	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	TAK
ATLine	–	TAK	TAK	TAK	–
BOSCH	TAK	–	TAK	–	TAK
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	TAK	–	–	TAK
CBC Poland	TAK	TAK	TAK	–	TAK
CMA	–	–	–	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	TAK	TAK	TAK	TAK	TAK
DG Elpro	–	TAK	TAK	TAK	TAK
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	TAK	TAK
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
ela-compil	TAK	–	TAK	–	TAK
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
ELZA Elektro-Systemy-Instalacje	–	TAK	TAK	TAK	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	TAK	TAK	–	TAK
FES	TAK	TAK	TAK	TAK	TAK
GDE Polska	–	TAK	TAK	–	TAK
HSA	–	–	TAK	–	TAK
Insap	–	TAK	TAK	TAK	TAK
ISM EuroCenter	–	–	TAK	–	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
Janex International	–	TAK	TAK	TAK	TAK
KABE	TAK	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	–	TAK	–	–
NAPCO	–	TAK	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	–
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	–	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	TAK	TAK	TAK	TAK
RETT-POL	–	–	TAK	TAK	–
RISCO	TAK	–	–	–	–
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	TAK
SATIE	–	–	TAK	TAK	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	TAK	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	–	–	TAK	–	–
Sony	TAK	–	TAK	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	TAK	TAK	–	TAK
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	–	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	–	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
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
AGIS Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	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
Ambient System	–	–	–	TAK	–	TAK	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	TAK	TAK	–	–	TAK	TAK	TAK	TAK	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	–	–	–	TAK
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	TAK	–	–
CMA	TAK	–	TAK	TAK	TAK	TAK	TAK	TAK	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	TAK	–	–	TAK
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	TAK	TAK	–	TAK	–	–	–	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–	–	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
EBS	Transmitery IP (ethernet), GSM/GPRS/SMS, zabezpieczenia bankowe, sygnalizatory, GPS, produkcja OEM/ODM, R&D								
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	–	–	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
ELZA Elektro-Systemy-Instalacje	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	TAK	TAK	TAK	–
HSA	TAK	TAK	TAK	TAK	–	–	–	–	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
ISM EuroCenter	–	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	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	–	TAK	–	–	–	–
Nuuxe – Radioton	–	TAK	–	TAK	–	–	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	TAK
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	–	–	–	–	–	–	–	TAK	–
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	TAK	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	–	TAK	TAK	–	–	–
RETT-POL	TAK	TAK	TAK	TAK	–	–	TAK	–	–
RISCO	TAK	–	TAK	–	–	TAK	–	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	TAK	TAK	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	–	TAK	TAK	–	–	TAK	TAK	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	TAK	–	–	–	–
Tayama	–	TAK	TAK	–	–	–	TAK	–	–
Technokabel	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

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

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

Skład i łamanie
Tomasz Kaczmarczyk

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

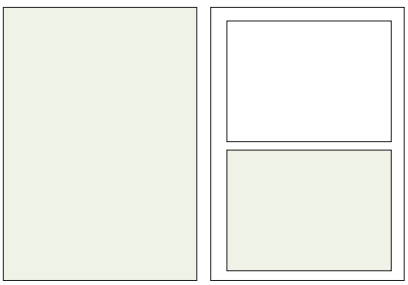
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

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



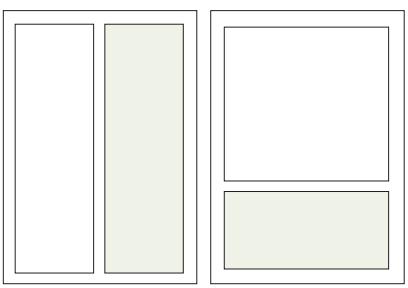
cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

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

Reklama na okładkach:

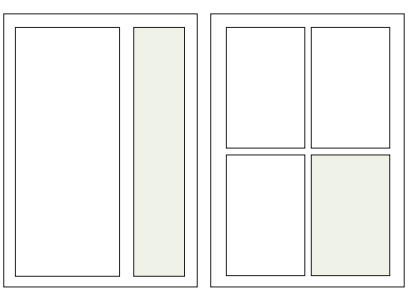
pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł



1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Spis teleadresowy:
jednorazowy wpis 70 zł



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (23%)

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

Spis reklam

PRZECHWYĆ

ZAPISZ

POKAŻ

ZŁAP

iPOLiS

Rozwiązania sieciowe firmy Samsung

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

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

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

Sieciowe rozwiązania bezpieczeństwa Samsung HD.
Inteligentniejsze bezpieczeństwo.

E **STEsecurity@samsung.com**
W **samsungsecurity.com**

Samsung Techwin Europe Ltd

SAMSUNG

Specyfikacje bez końca

Jedno rozwiązanie

Rozwiązania do migracji:

- Wyższy poziom bezpieczeństwa dzięki technologii 13,56 MHz
- Wiele aplikacji w ramach jednego systemu
- Bezproblemowa migracja z HID Prox lub MIFARE do HID iCLASS lub DESFire EV1

HID®

Nieważne, jakie wymagania pojawią się w przyszłości – nowe rozwiązania HID umożliwiają bezproblemową migrację do technologii smart card zaspokajającej przyszłościowe potrzeby z zachowaniem możliwości obsługi popularnych, starszych systemów po możliwie najniższych kosztach dla użytkownika.

Aby uzyskać informacje na temat, kiedy i jak migrować oraz aby poznać dostępne rozwiązania, należy odwiedzić stronę **hidglobal.com/onesolution-zab** i pobrać najnowszą dokumentację dotyczącą migracji.