CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 5(117)/2017

ZABEZPIECZENIA

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

W NUMERZE:

- Badania jakości ograniczników przepięć do ochrony systemów CCTV
- Prewencja przyszłością nadzoru wizyjnego
- Bogatsza wiedza na potrzeby lepszych decyzji biznesowych
- Lokalizuj, śledź i oglądaj w powiększeniu

Dużo więcej niż detekcja

z termowizyjnymi kamerami do detekcji Axis.

Dzięki dynamicznym termowizyjnym kamerom sieciowym AXIS Q8641-E i AXIS Q8642-E PT to Ty określasz tempo dozoru rozległych obszarów zewnętrznych i zwiększasz kontrolę dzięki niezakłóconemu widokowi.

www.axis.com/products/axis-q86-series

AXIS COMMUNICATIONS

FUJIFILM
Value from Innovation

Bezpieczeństwo w nowym wymiarze:

4K

Pierwszy obiektyw Fujinon typu Vari Focal

Day Night

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

kremer kommunikation®

FUJINON

SPIS TREŚCI 05 2017

NOWOŚCI PRODUKTOWE 6

WYDARZENIA, INFORMACJE 14

WYWIAD

Patrzymy w przyszłość z optymizmem. Rozmowa z Arturem Hejdyszem, prezesem zarządu C&C Partners, z okazji 25-lecia istnienia firmy 16

TELEWIZJA DOZOROWA

Badania jakości ograniczników przepięć do ochrony systemów CCTV – *dr inż. Tomasz Maksimowicz* 20

Lokalizuj, śledź i oglądaj w powiększeniu – *Bosch Security Systems* 26

Bogatsza wiedza na potrzeby lepszych decyzji biznesowych – *Axis Communications* 28

Prewencja przyszłością nadzoru wizyjnego. Inteligentne techniki termowizyjne i sieciowe systemy dozorowe poprawiają bezpieczeństwo – *dr Tristan Haage, MOBOTIX* 32

Analogowe systemy dozoru wizyjnego – *Maciej Pietrzak, Dahua Technology Poland* 36

Ograniczniki przepięć firmy RST – profesjonalna ochrona systemów sygnałowych – *dr inż. Tomasz Maksimowicz, RST sp.j. M. Zielenkiewicz, W. Nietupski, A. Wojtkowski* 38

PREZENTACJA FIRMY

25 lat największych w Polsce spotkań projektantów, rzeczoznawców, instalatorów i konserwatorów systemów sygnalizacji pożarowej (część 2)
– mgr inż. Mariusz Radoszewski, Polon-Alfa

42

OCHRONA PRZECIWPOŻAROWA

Systemy sygnalizacji pożarowej w pomieszczeniach elektronicznego przetwarzania danych (część 2)
– mgr inż. Jerzy Ciszewski, IBP NODEX

46

OCHRONA PERYFERYJNA

Od radarów wojskowych do ochrony perymetrycznej – rozwój technik wykorzystujących mikrofale
– Maciej Prelich, Firma ATLine sp.j. Sławomir Pruski

50

ZASILANIE

Profesjonalne zasilacze awaryjne marki PowerWalker
– Tomasz Lenartowicz, Impakt

52

SSWiN

Centrala alarmowa PRiMA64. Hybrydowy system o interesujących funkcjach
– Michał Konarski, GENEVO

56

MONITORING

A ty, jaki masz nadajnik alarmowy? (Część 2)
– Daniel Kamiński

62

CHMURA OBLICZENIOWA (CLOUD COMPUTING)

Bezpieczeństwo informacji w chmurze (część 3)
– Marek Blim

68

KARTY KATALOGOWE 74

SPIS TELEADRESOWY 78

SPIS REKLAM 82

NVIP-2C5000ATM – kamera IP do zadań specjalnych

Kamera **NVIP-2C5000ATM** jest przeznaczona do obserwacji urządzeń bankomatowych. Moduł kamerowy ma niewielkie rozmiary – 33 mm (szer.) x 32 mm (wys.) x 33 (dł.) mm. Obiektyw typu pinhole ma jasność F=f:2,0 i ogniskową równą 3,7 mm, i tym samym szeroki kąt widzenia równy 83 . Moduł wytwarza obraz o wysokiej rozdzielczości Full HD (1920 x 1080). Oprócz interfejsu sieciowego kamera ma wyjście BNC do integracji z systemami analogowymi AHD o wysokiej rozdzielczości. Kamera zainstalowana w urządzeniu bankomatowym jest narażona na bezpośrednie działanie promieni słonecznych. Prawidłowe zobrazowanie osób podchodzących do bankomatu jest możliwe dzięki funkcji rozszerzającej zakres dynamiki obrazu (WDR) z podwójnym skanowaniem przetwornika.

Kamera może pracować autonomicznie dzięki zapisowi strumieni wizyjnych i dźwiękowych na karcie microSD/SDHC o pojemności do 128 GB. Zapis na karcie może być realizowany w trybie ciągłym lub alarmowym (w przypadku aktywacji wejść alarmowych i detekcji ruchu). Dane zapisane na karcie SD mogą być odtwarzane bezpośrednio z interfejsu sieciowego kamery przy użyciu przeglądarki Internet Explorer. Dodatkowo, w reakcji na zdarzenia alarmowe, kamera może wysłać e-mail z załącznikiem, zapisać dane na serwerze FTP oraz aktywować wyjścia alarmowe.

Co więcej, kamera ma wejścia i wyjścia akustyczne do dwukierunkowej komunikacji dźwiękowej. Jest w pełni kompatybilna z aplikacją do nadzoru wizyjnego NMS (Novus Management System).

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Axis Communications wprowadza na rynek nową serię kamer do obserwacji dużych przestrzeni

Firma **Axis Communications** wprowadziła na rynek nową generację kamer zmiennopozycyjnych z serii **AXIS Q86** i **AXIS Q87**, które umożliwiają operatorom szybsze i bardziej precyzyjne obracanie i pochylanie urządzeń w celu obserwacji dużych obszarów czy ochrony perymetrycznej w czasie rzeczywistym. Kamery błyskawicznie reagują na wykryte alarmy i zagrożenia. Dzięki rozszerzonym funkcjom umożliwiają stały dozór w zakresie 360 stopni bez zniekształceń obrazu przy aż 135-stopniowym polu widzenia w pionie.

Wśród nowych kamer znalazły się wizyjne kamery PTZ, termowizyjne kamery PT, a także dwuprzetwornikowe kamery PTZ, które wytwarzają obraz zarówno w widmie optycznym, jak i termicznym.

Termowizyjne zmiennopozycyjne kamery sieciowe AXIS Q8641-E i AXIS Q8642-E PT wytwarzają obraz termiczny o wysokim kontraście i mają kąt widzenia równy 10, co wraz z zaawansowanymi funkcjami analitycznymi umożliwia wykrywanie zagrożeń nawet z dużej odległości i natychmiastowe powiadomienie operatora.

Kamery sieciowe AXIS Q8685-E/-LE PTZ wytwarzają obraz o rozdzielczości HDTV 1080p. Są wyposażone w obiektywy zmiennoogniskowe o krotności 30, z funkcją automatycznej regulacji ostrości. W połączeniu z funkcją Forensic WDR (od ang. *wide dynamic range*), która została stworzona przez producenta z myślą o optymalizacji dynamiki obrazu, zapewniają najwyższą z możliwych jakość i użyteczność obrazu nawet w trudnych warunkach oświetleniowych.

Dwuprzetwornikowe kamery sieciowe AXIS Q8741-E i AXIS Q8742-E Bispectral PTZ zapewniają połączenie dwóch strumieni wizyjnych tworzonych na żywo – z przetwornika termicznego (wykorzystywanego do wykrywania obiektów), a także z tradycyjnego przetwornika o wysokiej rozdzielczości (do weryfikacji wyglądu tych obiektów). Kamery są wyposażone w obiektywy zmiennoogniskowe o krotności 30, z funkcją automatycznej regulacji ostrości. W połączeniu z funkcją Forensic WDR zapewniają najwyższą z możliwych jakość i użyteczność obrazu nawet w trudnych warunkach oświetleniowych.

Dodatkowo kamery AXIS Q8741-LE, AXIS Q8742-LE i AXIS Q8685-LE mogą pracować w podczerwieni, dzięki czemu są bardziej przydatne w nocy. Urządzenia są przystosowane do użytku w miejscach, w których istnieje duże ryzyko zabrudzenia pyłem, solą, piaskiem czy sadzą, takich jak np. ruchliwe skrzyżowania, lotniska czy porty morskie, dzięki możliwości zdalnego czyszczenia przednich szyb obudowy za pomocą wbudowanych wycieraczek i myjek.

Kamery będą dostępne w sieci dystrybucyjnej firmy Axis Communications w drugim i trzecim kwartale 2017 r.

Bezpośr. inf. Axis Communications

AHD TECHNOLOGY by NOVUS®

TERAZ MOŻESZ ZOBACZYĆ WYRAŹNIEJ TO, NA CZYM CI ZALEŻY

REJESTRATORY I KAMERY 4 MPX W TECHNOLOGII AHD

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

8-dyskowy rejestrator IP marki NOVUS z inteligentnymi funkcjami

8-dyskowy rejestrator umożliwia jednoczesny zapis 32 kanałów wizyjnych o rozdzielczości 8 Mpx (3840 x 2160) oraz tej samej liczby kanałów dźwiękowych. Prędkość rejestracji dla wszystkich kanałów wynosi 960 kl./s. Łączna przepływność nagrywanych strumieni wizyjnych nie może przekraczać 256 Mb/s, co dla pojedynczego kanału daje średnią wartość na poziomie 8 Mb/s. Do rejestratora można podłączyć maksymalnie osiem dysków twardych, każdy o pojemności 6 TB, oraz dwa dodatkowe dyski poprzez złącza E-SATA, co pozwala na stworzenie archiwum o wielkości 60 TB (!). Oprócz wyjścia głównego (HDMI lub VGA) o rozdzielczości 4K rejestrator ma wyjście pomocnicze HDMI o rozdzielczości Full HD, za pomocą którego można wyświetlać obrazy pełnoekranowo, w podziale lub włączyć sekwencję.

Rejestrator odbiera zdarzenia alarmowe wynikłe z analizy treści obrazów z kamer IP serii 3000. W przypadku takich zdarzeń aktywowana jest akcja alarmowa, m.in. wysłanie e-maila, aktywacja wyjścia alarmowego lub wysłanie powiadomienia do aplikacji mobilnej. Funkcje inteligentne wybranych modeli kamer mogą również być konfigurowane z poziomu rejestratora, bez konieczności korzystania z sieciowego interfejsu kamery. Rejestrator ma dwa interfejsy sieciowe RJ-45/1000Mbit/s umożliwiające obsługę kamer z dwóch rozdzielonych podsieci lub realizację redundantnego połączenia z jedną siecią kamerową. W przypadku awarii jednego z połączeń drugie połączenie staje się aktywne automatycznie.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Wspólne inicjatywy Politechniki Łódzkiej i firmy Bosch Security Systems

Politechnika Łódzka i firma **Bosch Security Systems** zawarły 21 czerwca 2017 roku umowę dotyczącą współpracy. Współpraca ta będzie dotyczyła przede wszystkim dziedziny badawczo-rozwojowej, a także kształcenia studentów w zakresie systemów zabezpieczeń i nowoczesnych, inteligentnych rozwiązań wykorzystywanych w przestrzeni miejskiej (*smart city*).

Dokument podpisali rektor Politechniki Łódzkiej prof. Sławomir Wiak oraz dyrektor handlowy działu Bosch Security Systems Krzysztof Góra.

– *Politechnika Łódzka kładzie duży nacisk na współpracę z otoczeniem gospodarczym. Kontakt z firmami pozwala nam korygować programy kształcenia i rozwijać badania, które przynoszą realne korzyści i nie są odkładane na półkę. Prowadzimy studia m.in. w zakresie systemów sterowania inteligentnymi budynkami i zależy nam, aby ich absolwenci potrafili sprostać najnowszym wymaganiom z zakresu szeroko rozumianego inteligentnego budownictwa. Bosch Security Systems jest dla nas bardzo cennym partnerem, z którym możemy ten cel osiągnąć* – powiedział rektor Politechniki Łódzkiej prof. Sławomir Wiak.

Politechnika Łódzka i Bosch Security Systems chcą podejmować inicjatywy związane z rozwojem kompetencji studentów, które wzmocnią pozycję absolwentów na rynku pracy. Dla najlepszych studentów przewidziano praktyki zawodowe i staże naukowe w firmie Bosch. Partnerstwo obejmuje również prowadzenie zajęć z wykorzystaniem systemów zabezpieczeń firmy Bosch oraz współpracę przy organizacji warsztatów i spotkań z osobami związanymi z branżą.

Bezpośr. inf. Bosch Security Systems

Advanced
The Standard in Fire Systems

NAJWYŻSZY POZIOM OCHRONY

SYSTEM SYGNALIZACJI POŻARU

Axis EN

ZETO-PROJEKT

WYŁĄCZNY PARTNER FIRMY ADVANCED NA TERENIE POLSKI:
P.U.I. ZETO-PROJEKT SP. Z O. O.
UL. KOLEJOWA 20, 55-075 BIELANY WROCŁAWSKIE
WWW.ZETO-PROJEKT.COM.PL
BIURO@ZETO-PROJEKT.COM.PL

Systemy ePoE firmy Dahua Technology

Kwestia zasilania urządzeń w systemach nadzoru wizyjnego jest poruszana nieco rzadziej niż inne zagadnienia. Niepodważalną przewagę systemom sieciowym dawał od zawsze standard Power over Ethernet, czyli metoda umożliwiająca zarazem zasilanie i przesył strumienia danych jednym przewodem. Systemy analogowe wyróżniały się z kolei zdecydowanie dłuższymi zasięgami podczas transmisji sygnału, a zastosowanie przewodów zespolonych z żyłami zasilającymi umożliwiało również dostarczenie energii na spore odległości.

Dostrzegając zapotrzebowanie, **Dahua Technology** wprowadza system extended **Power over Ethernet** (ePoE). To innowacyjne rozwiązanie łączy zalety dwóch wymienionych typów systemów. Jakie korzyści zauważy instalator?

Przede wszystkim możliwość jednoczesnego zasilania i przesyłania sieciowych strumieni wizyjnych na dystansie do 300 m przy zachowaniu przepustowości 100 Mb/s oraz mocy zasilającej 25,4 W. W wyjątkowych sytuacjach przewidziano wariant przesyłu na odległość dochodzącą do 800 m przy przepustowości 10 Mb/s i mocy zasilającej 13 W. Wraz z wprowadzeniem zasilania metodą ePoE w ofercie pojawia się wiele wykorzystujących ją urządzeń. Należą do nich kamery o rozdzielczościach od 1080p do 4K w wielu różnych formach (tulejowe, kopułowe, kompaktowe), z obiektywami stało- i zmiennoogniskowymi. Uzupełnieniem są 2-, 4- i 8-dyskowe rejestratory z wbudowanymi przełącznikami sieciowymi z interfejsami PoE oraz wolnostojący 4-portowy przełącznik PFL2106-4ET-96, który jeszcze bardziej zwiększa elastyczność całego rozwiązania. Aby umożliwić adaptację istniejącego okablowania współosiowego, wprowadzono moduł LR1002, który przy użyciu kabla typu RG59 zapewnia przepustowość 10 Mb/s na dystansie do 1000 m, a także zasilanie metodą PoE. Wszystko to bez ekstenderów PoE czy dodatkowych przełączników sieciowych. Instalowanie jeszcze nigdy nie było tak łatwe.

Bezpośr. inf. Marian Maroszek
Dahua Technology Poland

Program partnerski
The Best Program of Dahua

Telewizory, smartwatche, laptopy, konsole do gry czy rowery – to tylko niektóre nagrody, jakie rozdaje **Dahua** w związku ze swoim nowym programem partnerskim. **The Best Program of Dahua** zapoczątkowano w czerwcu.

Podczas szkoleń prowadzonych w wielu miastach Polski pracownicy Dahua Technology byli wielokrotnie pytani o szybszy i skuteczniejszy sposób komunikacji, dlatego firma uruchomiła dla swoich partnerów The Best Program of Dahua.

Program znacznie usprawnia komunikację z firmą. Umożliwia także zbieranie punktów za zakupy, które można wymienić na atrakcyjne nagrody. Rejestracja online została uruchomiona 1 czerwca pod adresem *www.dahua.best/rejestracja*. Niedługo zacznie działać także aplikacja partnerska.

Dzięki rozbudowanej sieci sprzedaży na całym świecie Dahua Technology oferuje wsparcie sprzedażowe, projektowe, serwisowe i marketingowe. Od lipca 2016 r. w Warszawie działa polskie biuro – Dahua Technology Poland. Dzięki temu firma jest bliżej klienta i może lepiej rozumieć jego potrzeby.

Dahua Technology jest czołowym, działającym globalnie dostawcą rozwiązań z zakresu wizyjnych systemów dozorowych. W swojej ofercie ma urządzenia do nadzoru wizyjnego i termowizyjnego, systemy kontroli dostępu, systemy nadzoru ruchu ulicznego, systemy alarmowe wraz z elementami wykonawczymi oraz wideodomofony. Dopełnieniem oferty jest oprogramowanie umożliwiające tworzenie zintegrowanych systemów bezpieczeństwa.

Bezpośr. inf. Olga Dmochowska
Dahua Technology Poland

Kamery Hanwha Techwin Wisenet X
zintegrowane z systemami VMS

Hanwha Techwin ogłosiła przyspieszenie procesu integracji kamer **Wisenet X** z czołowymi rozwiązaniami **VMS**, takimi jak Genetec Security Center 5.6 i Milestone XProtect.

Kamery Hanwha zostały wyposażone w procesor Wisenet 5 – najbardziej wydajny procesor DSP, jaki kiedykolwiek zastosowano w całej linii kamer sieciowych. Dzięki temu charakteryzują się najlepszym na świecie mechanizmem pozyskiwania obrazu o szerokim zakresie dynamiki (WDR) oraz wykorzystują obiektywy przygotowane do pracy przy słabym oświetleniu zewnętrznym. Spośród 26 nowych kamer serii Wisenet X z kodekiem H.265 można wybrać optymalne urządzenia do dowolnego systemu dozoru wizyjnego – nie mają przy tym znaczenia warunki oświetleniowe i nie ma konieczności stosowania zewnętrznego doświetlenia promiennikiem IR.

Dostarczamy ROI

– *Kluczowym elementem naszej myśli przewodniej „Rozwijamy się dzięki zaufaniu" jest nasze zobowiązanie do zapewnienia użytkownikom naszych produktów pełnego zwrotu kosztów inwestycji (ROI)* – powiedział dr Bob (H.Y.) Hwang, dyrektor zarządzający Hanwha Techwin Europe. – *Współpracujemy z firmami Genetec, Milestone i innymi producentami oprogramowania VMS. Dbamy o poprawną integrację naszych kamer Wisenet X, tak aby były kompatybilne z rozwiązaniami tych producentów. Bez względu na to, którą platformę integrującą wybierze klient, zapewnione będzie optymalne wykorzystanie możliwości, jakie kryją się w Wisenet X, a dodatkowo zachowana zostanie elastyczność integracji ze specjalistycznymi aplikacjami służącymi do analizy treści obrazu i systemami kontroli dostępu.*

Integracja ze stacjami monitorowania

Najnowsze kamery sieciowe Wisenet, rejestratory sieciowe i cyfrowe rejestratory sygnałów analogowych zostały z powodzeniem zintegrowane z oprogramowaniem stacji monitorowania Immix CS firmy SureView.

Integracja kamer IP Wisenet i rejestratorów wizyjnych z Immix CS poprawia skuteczność i wydajność działania stacji monitorowania alarmów dzięki możliwości wizyjnej weryfikacji przyczyn alarmów.

Taką samą integrację przygotowano dla Immix Command Centre (CC) oraz PSIM (Physical Security Information Management) – platformy programowej wykorzystywanej przez firmy, instytucje i agencje zajmujące się monitorowaniem alarmów, sterowaniem systemami kontroli dostępu, analizą sygnałów akustycznych i wizualizacją stanu systemów dozorowych.

Bezpośr. inf. Hanwha Techwin Europe

ONVIF publikuje propozycję profilu T
dotyczącego transmisji strumieni wizyjnych

Nowy profil stanowi rozszerzenie dotychczasowej specyfikacji **ONVIF**. Dotyczy on głównie metod transmisji strumieni wizyjnych i zastosowania zaawansowanych metod kompresji obrazu, takich jak H.264 i H.265. Urządzenia zgodne z tym profilem muszą obsługiwać co najmniej jedną z tych metod kompresji.

Poza zapisami dotyczącymi różnych metod kompresji profil T zawiera informacje na temat metod wizyjnej detekcji ruchu, analizy treści obrazu i przesyłania metadanych. Istotnym elementem są zapisy standaryzujące rodzaje wydarzeń, jakie mogą być wykrywane i analizowane przez kamery.

W profilu T wprowadzony został protokół Transport Layer Security podnoszący poziom bezpieczeństwa podczas komunikacji między urządzeniami zgodnymi z tym profilem a urządzeniami klienckimi. Ponadto wprowadzone zostały zapisy pozwalające na transmisję strumieni wizyjnych wprost do przeglądarek internetowych, z pominięciem urządzeń VMS.

Istotnym fragmentem profilu T są zapisy dotyczące dwukierunkowej transmisji dźwięku, która znajduje coraz szersze zastosowanie w systemach monitoringu miejskiego, w transporcie, obsłudze parkingów etc. Dotychczas transmisji dźwięku nie dotyczyły szczegółowe zasady. Profil T zmienia tę sytuację.

Profil T w swojej obecnej formie stanowi jedynie propozycję zmian w specyfikacji ONVIF i będzie testowany przez sześć miesięcy, by producenci sprzętu oraz inne osoby zainteresowane wprowadzanymi zmianami miały czas na ustosunkowanie się do nich.

Opracował: Andrzej Walczyk
Redakcja
Źródło: https://www.onvif.org/profiles/profile-t/

Aplikacja sieciowa do obsługi systemu RACS 5

Pakiet oprogramowania **VISO** przeznaczonego do zarządzania skalowalnym systemem kontroli dostępu i automatyki budynkowej RACS 5 firmy **ROGER** został rozszerzony o aplikację VISO Web. VISO Web jest aplikacją sieciową przeznaczoną do bieżącej obsługi systemu RACS 5. Umożliwia zarządzanie użytkownikami systemu, wydawanie zdalnych komend, podgląd pracy systemu oraz przeglądanie zdarzeń historycznych zarejestrowanych w jego bazie danych. Aplikacja internetowa VISO Web została opracowana z myślą o użytkownikach końcowych systemu kontroli dostępu RACS 5, którzy, zajmując się jego obsługą, potrzebują szybkiego i skutecznego narzędzia do zarządzania użytkownikami lub monitorowania na bieżąco ruchu osób w systemie. Mogą to być zwłaszcza pracownicy działu kadr lub ochrony budynku, który został objęty działaniem systemu.

Bezpośr. inf. ROGER

Ostrzeganie osób niesłyszących
o alarmie pożarowym

Zeto-Projekt wprowadza na stałe do oferty kolejne rozwiązanie z zakresu bezpieczeństwa pożarowego. System **LifeLine**, produkowany w Wielkiej Brytanii przez firmę Advanced Electronics, jest przeznaczony do szybkiego i skutecznego przesyłania komunikatów o zdarzeniach pożarowych z wykorzystaniem transmisji radiowej. Podobnie jak wszystkie rozwiązania Advanced Electronics zapewnia szybką i łatwą instalację oraz obsługę. Posiada nadajnik o regulowanej mocy 2 W, optymalizuje zużycie energii i zapewnia precyzyjne pokrycie obszaru, nawet w skomplikowanych budynkach i na rozległych obszarach. LifeLine jest idealnym rozwiązaniem do ostrzegania osób niesłyszących i niedosłyszących o alarmie pożarowym. Może być stosowany we wszystkich rodzajach obiektów, m.in. w budynkach biurowych, szkołach, hotelach, pensjonatach, domach opieki i budynkach mieszkalnych.

System składa się z trzech podstawowych urządzeń:

– centrali Px-100, która pełni rolę nadajnika i przyjmuje sygnały z dowolnego systemu sygnalizacji pożarowej (osiem wejść dwustanowych lub poprzez port RS232 z obsługą protokołu ESPA 4.4.4),

– specjalnego odbiornika instalowanego przy łóżku osoby niesłyszącej (sygnalizacja świetlna wraz z podłączoną wibrującą wkładką do poduszki),

– trzech rodzajów pagerów do odbierania komunikatów.

System LifeLine doskonale sprawdza się również w sytuacjach, w których przesłanie precyzyjnej informacji o alarmie bezpośrednio do osoby znajdującej się w pobliżu zdarzenia zapewnia skrócenie czasu na dotarcie do miejsca zagrożenia i podjęcie szybkich działań.

Bezpośr. inf. Krzysztof Dembiński
P.U.I. Zeto-Projekt

Czytnik MIFARE do zastosowań hotelowych systemu RACS 5

MCT82M-IO-HR jest odmianą czytnika **MCT82M-IO-BK** przeznaczoną do kontroli dostępu do pokoi hotelowych funkcjonujących w ramach systemu kontroli dostępu i automatyki budynkowej **RACS 5**. Terminal umożliwia identyfikację użytkowników za pośrednictwem kart zbliżeniowych standardu ISO 14443A/B i MIFARE. Identyfikacja jest możliwa zarówno na podstawie fabrycznego numeru seryjnego karty (CSN), jak i na podstawie numeru zaprogramowanego w zaszyfrowanych sektorach karty (SSN). Na panelu frontowym czytnika znajdują się cztery wskaźniki sygnalizacyjne LED oraz przycisk dzwonka. Wskaźniki LED są przeznaczone do typowych sygnalizacji hotelowych jako formy komunikacji („nie przeszkadzać", zamówienie serwisu sprzątającego oraz gastronomicznego, prośba o asystę pracownika hotelowego). Terminal jest wyposażony w zestaw trzech linii wejściowych oraz trzech linii wyjściowych, w tym jedno wyjście przekaźnikowe. Zarówno linie wejściowe, jak i linie wyjściowe mogą być skonfigurowane w celu pełnienia dowolnych funkcji. Mogą służyć m.in. do obsługi czujnika otwarcia drzwi oraz do sterowania zamkiem. Po doposażeniu pokoju hotelowego w instalowany w nim czytnik z kieszenią MCT82M-IOCH można w ramach systemu RACS 5 uzyskać podstawowy zestaw urządzeń spełniających

typowe wymagania dotyczące kontroli dostępu i automatyki w pokojach hotelowych. Terminal MCT82M-IOHR jest zgodny z linią wzorniczą QUADRUS.

Bezpośr. inf. ROGER

14. Kongres Pożarnictwa
FIRE|SECURITY EXPO 2017
podsumowanie

27 lipca br. na PGE Narodowym w Warszawie odbył się czternasty Kongres Pożarnictwa **FIRE|SECURITY EXPO 2017**, który poświęcony był bezpieczeństwu pożarowemu obiektów budowlanych.

Uczestniczyło w nim 1104 uczestników. Wśród nich nie zabrakło osób zajmujących się projektowaniem i realizacją inwestycji, prewentystów oraz specjalistów z branży zabezpieczeń i ochrony przeciwpożarowej, którzy na co dzień spotykają się w swojej pracy zawodowej z problemami i wyzwaniami dotyczącymi ochrony przeciwpożarowej.

Podczas kongresu omówiono szereg zagadnień z wielu powiązanych ze sobą dziedzin. Pokazano nowości w systemach sygnalizacji alarmów, oddymiania i detekcji zagrożeń, nowe rozwiązania z zakresu kontroli dostępu, bierną ochronę przeciwpożarową. Swoją ofertę zaprezentowało blisko 200 przedstawicieli 70 dostawców z branży przeciwpożarowej i zabezpieczeń.

Kongres był współtworzony z ważnymi krajowymi ośrodkami naukowymi i badawczymi, m.in. z CNBOP–PIB, CIOP-PIB, SGSP, Wydziałem Inżynierii Procesowej i Ochrony Środowiska Politechniki Łódzkiej, Katedrą Telekomunikacji i Aparatury Elektronicznej Politechniki Białostockiej, PZP Ochrona, IBP NODEX, SIBP, GIG, PISA, PZU Lab, ZOSPRP, a także z wieloma organizacjami i stowarzyszeniami branżowymi. Nadzór merytoryczny nad przebiegiem bieżącej edycji pełnił zespół ekspertów w dziedzinie bezpieczeństwa pożarowego. Jak co roku, zadbano o bogaty program pokazów i testów działania systemów przygotowany przez partnerów i prelegentów.

Przed nami jubileusz 15-lecia Kongresu Pożarnictwa, dlatego już dziś serdecznie zapraszamy Państwa na jubileuszową edycję. Więcej szczegółów przekażemy już wkrótce.

Miło nam poinformować, że po raz drugi podczas Kongresu Pożarnictwa zostały przyznane trzy statuetki w kategorii *fire product* oraz po raz pierwszy przyznano nagrodę w kategorii *security product*.

Nagrody w kategorii *fire product* w tegorocznej edycji otrzymali:

– **D+H Polska** – za **TSZ-200** (centrala sterująco-zasilająca do systemów wentylacji pożarowej),
– **Bosch** – za **PAVIRO** (największa elastyczność architektury w systemach nagłośnieniowych i DSO),
– **PULSAR** – za system zasilania **DSO** do systemu Bosch PAVIRO.

Laureatem w kategorii *security product* 2017, przyznanej na Kongresie Pożarnictwa po raz pierwszy, został **MOBOTIX AG** za **Mx-M16TA-R079** – wielozadaniową dwuobiektywową kamerę termowizyjną.

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

Bezpośr. inf. DND Project
Opracowanie: Redakcja

Międzynarodowe Targi Poznańskie

securex®
POLAND

Międzynarodowe Targi Zabezpieczeń

23-26.04.2018
POZNAŃ

Zabezpiecz swój sukces!

www.securex.pl

Rozmowa z Arturem Hejdyszem,
prezesem zarządu C&C Partners, z okazji 25-lecia istnienia firmy

Patrzymy w przyszłość z optymizmem

25 lat to w przypadku firmy poważny wiek. Co uważa Pan za największy sukces C&C Partners?

Naszym największym sukcesem jest to, że przez 25 lat udawało nam się, i cały czas udaje, dostosowywać do dynamicznie zmieniającego się otoczenia biznesowego i technologicznego. Spójrzmy wstecz. Przez ten czas Polska i świat bardzo się zmieniły. Gdy zaczynaliśmy, Internet był dostępny tylko na uczelniach technicznych, a telefony komórkowe były wielkości walizki. Najbardziej dumni jesteśmy z tego, że jako firma dołożyliśmy swoją cegiełkę do wielu kluczowych i prestiżowych inwestycji. Wzięliśmy udział w tworzeniu infrastruktury sieci telekomunikacyjnych (dawniej miedzianych, obecnie światłowodowych w całej Polsce), współtworzyliśmy systemy bezpieczeństwa na Pomorskiej Kolei Metropolitalnej, w budynkach Q22 i Sky Tower, a także na największych stadionach sportowych, w szpitalach i uczelniach. Nasza praca to też nasza pasja, dzięki czemu zaufało nam duże grono klintów, którzy stali się naszymi partnerami. Serdecznie im za to dziękuję. Zawsze dbaliśmy też o ludzi, którzy tworzyli C&C Partners, i staraliśmy się być gotowi zarówno na lepsze, jak i na gorsze czasy. Przez te wszystkie lata, bez względu na wielkie zmiany, zachowywaliśmy nasze główne wartości, a jako firma cały czas się rozwijaliśmy.

A jak to wszystko się zaczęło? Jakie były początki C&C Partners?

W życiu trzeba mieć szczęście i znaleźć się w odpowiednim momencie w odpowiednim miejscu. Tak też było w naszym przypadku. C&C Partners jest owocem współpracy między dawnym województwem leszczyńskim a prowincjami w Holandii, która narodziła się w pierwszych latach po zmianie systemu politycznego w Polsce. Firma C&C Partners powstała w 1992 roku, a jej początki mają związek z osprzętem biurowym, a także centralami telefonicznymi. Chcieliśmy dostarczać nowoczesnych rozwiązań telekomunikacyjnych. W międzyczasie pojawiła się nasza słynna łączówka i nawiązana została współpraca z wówczas działającą firmą ADC KRONE. W 1994 roku zostaliśmy ich generalnym przedstawicielem, a łączówkę udało nam się wypromować w taki sposób, że dzisiaj jest standardem u wielu operatorów sieci telekomunikacyjnych. Dziś mogę z przekonaniem powiedzieć, że to był ten produkt, który zmienił bieg życia firmy.

Jak te pierwsze sukcesy wpłynęły na obecną sytuację firmy?

Ważna z dzisiejszej perspektywy okazała się możliwość przekonania klientów do tego, żeby ustandaryzowali swoje sieci telekomunikacyjne z wykorzystaniem sprzętu KRONE. To spowodowało, że w każdej szafie, na każdym ze słupków telekomunikacyjnych, które często widzimy, chodząc po polskich ulicach, są jakieś elementy, które pochodzą z Leszna. To było bardzo ważne dla naszego rozwoju. Później oczywiście wykorzystywaliśmy te wszystkie doświadczenia biznesowe, wprowadzając na rynek inne produkty i rozszerzając ofertę firmy o okablowanie strukturalne czy o systemy bezpieczeństwa.

Aż nadszedł rok 1998 i firma C&C Partners przystąpiła do holenderskiego holdingu Twentsche Kabel Holding (TKH). Jakie wypłynęły z tego korzyści?

Rzeczywiście, rok 1998 był dla nas przełomowy. C&C Partners należało do dwóch prywatnych właścicieli, którzy zdecydowali się sprzedać 100% udziałów holdingowi. Co ważne, bardzo starannie wybierali firmę, z którą chcieli robić w przyszłości interesy. TKH nie tylko był inwestorem, ale również zapewniał nam dostęp do nowoczesnych technologii i potencjału produkcyjnego, który posiadał. Dzięki temu z roli dystrybutora produktów innych producentów firma C&C Partners stała się częścią grupy firm, które działały w ramach TKH na całym świecie. Zrobiliśmy ogromny krok naprzód i uzyskaliśmy wielkie wsparcie, które procentuje do dzisiaj.

Przyłączenie się do holdingu TKH wiązało się z wprowadzeniem do oferty systemów zabezpieczeń.

Tak. C&C wpisywało się w strategię rozwoju grupy TKH, która na początku 2000 roku przyjęła sobie jako jeden z głównych celów uzyskanie pozycji lidera na rynku systemów zabezpieczeń. Tę strategię realizowano dwutorowo. Z jednej strony poprzez dołączanie do holdingu firm posiadających własne technologie w zakresie systemów bezpieczeństwa – od kontroli dostępu, systemów telewizji dozorowej i software'u do analityki obrazów czy systemów alarmowych. To rozszerzało asortyment oferowanych produktów. Z drugiej strony firmy takie jak C&C Partners zapewniały dostęp do nowych rynków, a przy okazji same także się rozwijały.

Co aktualnie oferuje C&C Partners?

Oferujemy produkowane przez nas systemy wykorzystujące osiągnięcia grupy TKH. Zapewniamy dostęp do samych produktów, a także naszą wiedzę inżynieryjną, która jest niezbędna, aby te produkty z sukcesem wdrażać już u klientów. Zaplecze inżynieryjne umożliwia nam oferowanie zintegrowanych rozwiązań zarówno w momencie sprzedaży, jak i później, tzn. już w trakcie użytkowania danego rozwiązania przez klienta końcowego. Dzięki tym kompetencjom nasze systemy współpracują z systemami firm trzecich.

Co uznaje Pan za największą zaletę firmy?

Najbardziej jestem dumny wtedy, gdy, rozmawiając z klientami, słyszę dobre słowa o naszym zespole. Ludzie byli dla nas zawsze bardzo ważni. Staramy się traktować ich uczciwie, po partnersku i dawać szanse na rozwijanie potencjałów osobistych i zawodowych. Wspieramy też ich pasje, bo nikt nie może żyć wyłącznie pracą. To wszystko owocuje profesjonalizmem inżynieryjnym, zaangażowaniem, pracowitością, pragmatyzmem w rozwiązywaniu problemów i elastycznym dostosowywaniem się do sytuacji. Jesteśmy firmą, która w pełni angażuje się we wszystko, co robi, bierze odpowiedzialność za swoje

produkty i nie zostawia klienta z problemem. Nie jesteśmy wyłącznie dystrybutorem. Nie tylko sprzedajemy, ale również bierzemy odpowiedzialność za cały proces lokowania produktu na rynku i za jego działanie u klienta końcowego.

A dzisiaj jakie branże są kluczowymi odbiorcami rozwiązań C&C Partners?

Naszą działalność koncentrujemy na rynkach, na których potencjał wzrostu jest największy. Interesują nas m.in. telekomunikacja, rozwiązania budynkowe, parkingi czy przemysł wizji maszynowej. Dzisiaj duża część firmy działa w sektorze telekomunikacji oraz skupia się na inwestycjach związanych z budową sieci szerokopasmowych. Z drugiej strony naszym celem handlowym są wszystkie instalacje budynkowe, zwłaszcza w tych obiektach, które wymagają wyższego poziomu bezpieczeństwa. Jeśli kogoś nie zadowala standardowy system bezpieczeństwa, oczekuje on dopasowania rozwiązań do swoich – często specyficznych – wymagań, to zaradzić może C&C Partners – właśnie w tym upatrujemy naszej przewagi i w takich sytuacjach chcemy działać.

Zainteresowanie zamówieniami niestandardowymi i dopasowanymi do indywidualnych potrzeb cały czas rośnie. Jak dużo właśnie takich zamówień otrzymuje firma C&C Partners?

Naszą domeną staje się głównie software. Mamy w tej dziedzinie przewagę, którą konsekwentnie utrzymujemy, wykorzystując doświadczenia i zasoby spółki córki – firmy C&C Technology zajmującej się tworzeniem oprogramowania. Dzięki temu udaje nam się dopasowywać każdy projekt do potrzeb klienta. Posiadamy też bardzo doświadczony zespół wdrożeniowy, który wspomaga naszych integratorów i instalatorów w procesie finalnego tworzenia systemów. Jeśli trzeba jeszcze bardziej ingerować w software, korzystając z zasobów C&C Technology, możemy go modyfikować i integrować z systemami firm trzecich.

Na co klienci najbardziej zwracają dziś uwagę?

Nawet i to w jakimś stopniu zmieniło się przez te wszystkie lata. Nasi klienci zawsze byli wrażliwi na cenę i cały czas jest ona ważna, ale już nie zawsze przesądza o wyborze. Coraz większa grupa inwestorów akceptuje to, że z ceną nierozerwalnie związana jest jakość i że za lepszą jakość warto zapłacić. Decyzje dotyczące wydatków CAPEX i OPEX są już świadomymi wyborami. Firmy coraz częściej współpracują z innymi przedsiębiorstwami, co ułatwia realizację zleceń i przekłada się na satysfakcję klienta.

Jaka jest dziś pozycja C&C Partners na rynku?

Bardzo dobra. Jesteśmy jednym z liderów w dziedzinie zintegrowanych systemów bezpieczeństwa na rynku polskim, litewskim, łotewskim i estońskim. Dokładamy starań, aby w najbliższym czasie umocnić naszą pozycję. Jednocześnie rozpoczynamy działania w innych krajach Europy Wschodniej, w których chcemy stać się liderem rynków wertykalnych z przeznaczonymi dla nich technologiami. Aktywnie korzystamy z zasobów w ramach grupy. Jesteśmy na trzecim miejscu wśród najszybciej rozwijających się w Europie firm z branży systemów zabezpieczeń wg rankingu TOP 50 opublikowanego przez miesięcznik a&s International.

A co Pan osobiście uważa za największy sukces firmy?

To, że tak szybko dostosowywaliśmy się do niesamowicie dynamicznych zmian, jakie następowały zarówno w dziedzinie techniki, jak i w sposobie działania firm. Dzięki temu jesteśmy w tym miejscu. Wykorzystaliśmy moment, potrafiliśmy wykreować pewne nowe modele działania. Sukcesem jest także to, że jesteśmy prekursorem pod względem technicznym, ponieważ dostarczane przez nas rozwiązania częstokroć były nowościami. Ponadto zawsze wybieraliśmy sposób działania, który pozwala nam w sposób partnerski budować relacje z klientami i wzajemnie się wspierać podczas realizacji inwestycji.

Dostarczacie rozwiązania także do krajów bałtyckich. Co spowodowało, że firma C&C Partners zdecydowała się wyjść poza Polskę?

Z jednej strony kierowała nami ciekawość i chęć spróbowania się na innym rynku, sprawdzenia, jak tam sprawdzi się nasz model biznesowy. Z drugiej strony w tamtym czasie, czyli około 2010 r., pytano o możliwości współpracy na Litwie. I tak zaczęliśmy. Później rozszerzyliśmy działalność na Łotwę i Estonię, co było naturalną konsekwencją. Obecnie na rynkach krajów bałtyckich mamy ugruntowaną pozycję. Interesują nas liczby dwucyfrowe w zakresie wzrostu obrotów.

Z jakich krajów pochodzą klienci C&C Partners? Gdzie potencjał jest większy – w Polsce czy zagranicą?

Bez dwóch zdań najważniejszy jest dla nas rynek polski. Niemniej staramy się dywersyfikować działalność firmy pod względem produktowym oraz geograficznym. Liczę na to, że w ciągu 3–4 lat około 30% obrotu firmy będzie stanowiła sprzedaż za granicą, ale mam też nadzieję, że wzrośnie globalna wartość sprzedawanych przez nas rozwiązań.

Jaka jest działalność holdingu TKH na polskim rynku?

Poza prowadzeniem działalności związanej z wprowadzaniem na nasz rynek produktów telekomunikacyjnych czy systemów bezpieczeństwa firma C&C Partners zawsze była swojego rodzaju inkubatorem i ambasadorem TKH w Polsce. Bardzo mocno zabiegaliśmy o to, aby holding korzystał ze swojego potencjału także u nas. Obecnie w ramach TKH pracuje w Polsce około 400 osób – w firmach C&C Partners, C&C Technology, TKH Kabeltechniek, VMI Polska oraz TKD Polska. Dzisiaj TKH w Lesznie jest jednym z głównych pracodawców. Rozbudowujemy swoje fabryki, a perspektywy są bardzo obiecujące.

A jakie są największe wyzwania na najbliższe lata?

Dotrzymanie kroku konkurencji. Obecnie rozwój jest niesamowicie szybki. Produkty są kreowane w dużej mierze przez klientów, adaptuje się je do ich potrzeb. Wyzwaniem jest też rozwijanie zespołu inżynierów, który daje nam przewagę podczas realizacji projektów.

Artur Hejdysz

prezes zarządu spółki C&C Partners. Związany z firmą od ponad 20 lat. Był m.in. dyrektorem ds. rozwoju, dyrektorem handlowym oraz dyrektorem operacyjnym spółki. Od 2010 roku pełnił funkcję członka zarządu w C&C Partners, a w roku 2012 został prezesem należącej do grupy C&C Partners spółki C&C Technology. W 2017 roku objął funkcję prezesa zarządu w C&C Partners.

RACS 5

System kontroli dostępu

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

Wprowadzono do oferty MCT82M-IO-HR

Czytnik zbliżeniowy MIFARE do zastosowań hotelowych w systemie RACS 5

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

roger®

Badania jakości ograniczników przepięć do ochrony systemów CCTV

dr inż. Tomasz Maksimowicz

Do stosowania środków ochrony przed przepięciami w rozbudowanych instalacjach, jakimi są systemy telewizji dozorowej, nikogo nie trzeba przekonywać. Doświadczenia związane z eksploatacją oraz koszty naprawy instalacji i wymiany uszkodzonych kamer przemawiają za zabezpieczaniem urządzeń przed skutkami wyładowań atmosferycznych najlepiej. Na rynku pojawia się coraz więcej produktów przeznaczonych do tego celu. Niestety niektóre spośród nich nie stanowią skutecznego zabezpieczenia przed przepięciami. W wielu przypadkach faktyczne parametry techniczne tych urządzeń nie odpowiadają deklarowanym, a zatem klient otrzymuje towar o jakości niższej niż oczekiwana

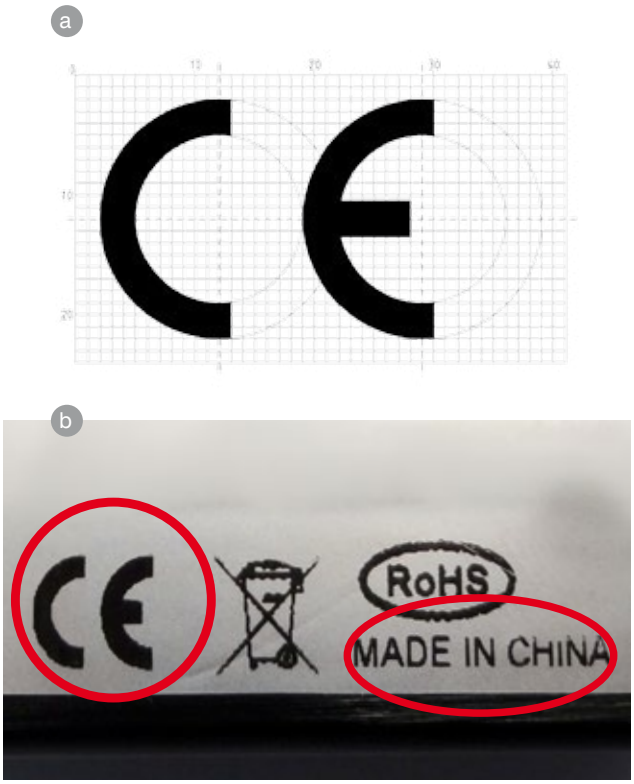
Aby podkreślić powagę problemu, przeprowadzono badania najpopularniejszych spośród dostępnych ograniczników przepięć (SPD, ang. *surge protecting device*) przeznaczonych do ochrony instalacji CCTV. Zbadano urządzenia sześciu różnych producentów i dostawców, których produkty są obecnie najczęściej stosowane. Testy przeprowadzono łącznie na 25 typach urządzeń przeznaczonych do ochrony torów transmisyjnych sygnałów wizyjnych, magistral transmisyjnych w standardzie RS485, obwodów zasilania 24 V oraz ograniczników do kamer IP zasilanych metodą PoE. Wszystkie ograniczniki przepięć były nowe i zakupione na potrzeby badań.

Zakres badań obejmował analizę parametrów technicznych podawanych przez producentów, pomiary podstawowych parametrów elektrycznych oraz próby weryfikacji deklarowanej odporności udarowej. W niniejszym artykule opisano jedynie wyniki prób udarowych.

Celem badań jest ukazanie rzeczywistej jakości ograniczników przepięć dostępnych na polskim rynku. Intencją autora jest udzielenie projektantom i inwestorom pomocy w doborze prawidłowych środków ochrony, a nie walka z konkurencją, dlatego nie ujawniono nazw badanych urządzeń ani producentów.

Wprowadzenie wyrobu do obrotu

Każdy wprowadzany do obrotu wyrób elektryczny musi spełniać wymagania zawarte w odpowiednich dyrektywach i musi być oznakowany znakiem CE (rys. 1a). Ograniczniki przepięć stosowane w obwodach sygnałowych jako wyrób elektryczny



Rys. 1. Prawidłowe oznaczenie „CE" (a) oraz znak spotykany na produktach importowanych z krajów azjatyckich (b) – za mały odstęp między znakami C i E

powinny spełniać wymagania dyrektywy niskonapięciowej (LVD) 2014/35/UE (dawniej 2006/95/WE) w zakresie, którego dotyczy norma zharmonizowana *PN-EN 61643-21 Niskonapięciowe urządzenia ograniczające przepięcia -- Część 21: Urządzenia do ograniczania przepięć w sieciach telekomunikacyjnych i sygnalizacyjnych -- Wymagania eksploatacyjne i metody badań.*

Przeprowadzenie badań według powyższej normy jest jedyną możliwością określenia rzeczywistych parametrów ogranicznika przepięć. Norma ta definiuje podstawowe wymagania odnoszące się do prawidłowego oznakowania urządzeń i niezbędnych prób elektrycznych, w tym prób udarowych. Parametry deklarowane przez producenta powinny być zatem potwierdzone stosownymi badaniami, których zakres jest zależny od konfiguracji i funkcji ogranicznika przepięć.

Dla zakupionych na potrzeby badań ograniczników przepięć deklaracje zgodności z normą PN-EN 61643-21 uzyskano dla 20 spośród 25 urządzeń. Wystawienie deklaracji zgodności przez producenta powinno być jednoznaczne z potwierdzeniem przeprowadzenia badań urządzenia. Otrzymane wyniki mogą jednak świadczyć o tym, że nie przeprowadzono takich badań.

Weryfikacja odporności udarowej

Jedną z prób, jakim poddano testowane ograniczniki przepięć, stanowiła weryfikacja deklarowanych parametrów dotyczących odporności na udary. Do badań wykorzystano generator udaru kombinowanego umożliwiający narażenie badanych urządzeń na udar prądowy o kształcie 8/20 μs i wartości szczytowej do 5 kA. Taki generator może być wykorzystywany do prób udarowych kategorii C1 i C2 według normy PN-EN 61643-21. Każdy SPD był narażony na udary o wartościach deklarowanych przez producenta (maksymalnie 5 kA 8/20 μs) i w konfiguracjach zgodnych z informacjami podanymi w instrukcjach lub kartach katalogowych. W żadnym przypadku ogranicznik nie był narażony na udar o wartości wyższej niż podane w dokumentacji parametry znamionowe lub maksymalne. W czasie prób rejestrowano jednocześnie przebiegi prądu udarowego oraz napięcia na zaciskach wyjściowych SPD po stronie chronionej. Przykładowe przebiegi zarejestrowane w czasie badań przedstawiono na rysunku 2.

Rys. 2. Przykładowy przebieg udaru prądowego 8/20 µs (kolor zielony) i napięcia zmierzonego na zaciskach wyjściowych ogranicznika przepięć (kolor pomarańczowy) zarejestrowane w czasie badań porównawczych

Wyniki przeprowadzonych prób należy uznać za zatrważające. W przypadku produktów czterech z sześciu producentów, których ograniczniki poddano próbom, co najmniej jedno urządzenie nie przeszło prób z wynikiem pozytywnym. Łącznie dziewięć spośród 25 testowanych ograniczników przepięć (dziewięć spośród 17, jeżeli uwzględni się tylko producentów, których SPD nie spełniały deklarowanych parametrów) uległo uszkodzeniu w czasie prób odporności na udary. Uszkodzeniom uległy badane SPD każdego rodzaju, przeznaczone zarówno do ochrony torów transmisji sygnałów wizji, linii zasilających, magistral RS485 oraz sieci IP z zasilaniem PoE. Należy podkreślić, że dla ośmiu z dziewięciu uszkodzonych urządzeń wystawione były przez producentów deklaracje zgodności z normą PN-EN 61643-21.

Najczęstszym typem uszkodzenia, jaki wystąpił w siedmiu z dziewięciu przypadków, było przerwanie ścieżek na laminatach PCB. Uszkodzone zostały ograniczniki trzech typów jednego z producentów przeznaczone do ochrony torów transmisji sygnałów wizyjnych, dla których w danych technicznych zamieszczono zapisy:

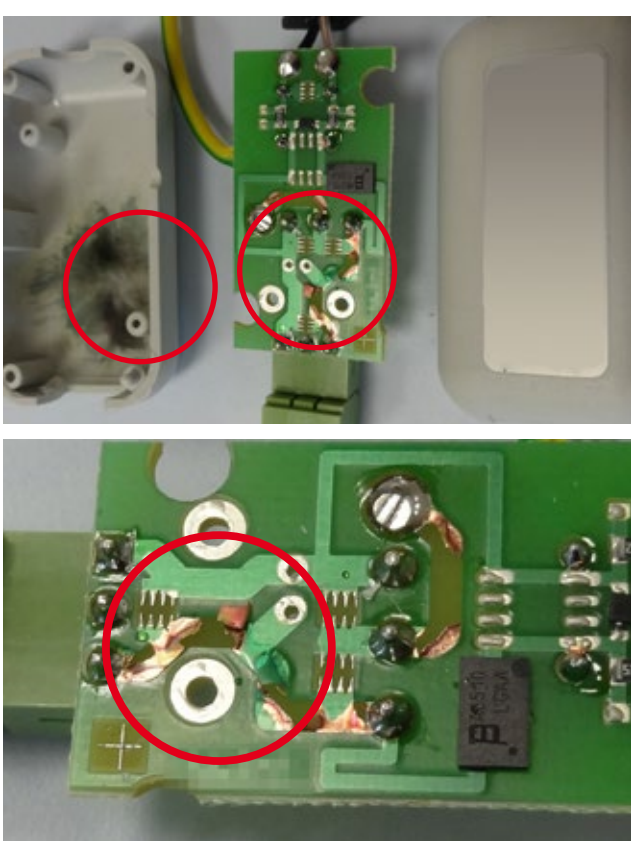
Zabezpieczenie antyprzepięciowe:
3 - Iskrownik, Ochronnik gazowy, Transil,

Ochrona linia-ziemia:
Ochronnik gazowy: 90 V, 2x10 kA @ 8/20 µS

Maksymalny poziom przepięcia:
4 kV

Taki zapis jest niejednoznaczny i wprowadza użytkownika w błąd. Informacja „Ochronnik gazowy: 90 V, 2x10 kA @ 8/20 μS" sugeruje, że SPD wytrzymuje dwukrotne narażenie na udar 10 kA 8/20 μs. Z kolei wartość przepięcia „4 kV" nie daje żadnych praktycznych informacji dotyczących odporności ogranicznika przepięć. Przykładowo, jeżeli dotyczy to udaru kombinowanego, to wartości 4 kV odpowiada prąd o wartości maksymalnej 2 kA, natomiast w przypadku generatorów udarów prądowych o kształcie 8/20 μs przy napięciu 4 kV wartość szczytowa prądu może wynosić nawet dziesiątki kA. W czasie badań przetestowano jedynie trzy typy takich ograniczników spośród kilkunastu o podobnej konstrukcji, jakie producent posiada w swojej ofercie. Urządzenia wytrzymały narażenie na udar kombinowany 4 kV/2 kA, natomiast przy udarach o wartości szczytowej 5 kA, czyli o połowie wartości podanej w specyfikacji technicznej, we wszystkich ogranicznikach całkowitemu zniszczeniu uległy ścieżki na laminacie PCB na drodze przepływu prądu udarowego od narażonej linii do miejsca przyłączenia przewodu uziemiającego (rys. 3). Przykład ten doskonale pokazuje, dlaczego parametry SPD należy określać na podstawie przeprowadzonych badań całej konstrukcji ogranicznika, a nie na podstawie danych katalogowych zastosowanych elementów.

W przypadku produktów innego producenta uszkodzenia ścieżek wystąpiły w trzech z pięciu badanych urządzeń przy udarach o wartości maksymalnej równej znamionowemu prądowi wyładowczemu (5 kA 8/20 μs). W tym przypadku należy zwrócić uwagę na fakt, że producent ten zarówno wystawia deklaracje zgodności z normą PN-EN 61643-21, jak i w prawidłowy sposób podaje parametry dotyczące odporności na udary i napięciowego poziomu ochrony, np.:



Rys. 3. Uszkodzony ogranicznik przepięć oraz laminat PCB przed narażeniem urządzenia na udar 5 kV 8/20 μs i po próbie udarowej

Poziom protekcji Up linia-linia:

≤16 V – 1 kV/μs, C3

Poziom protekcji Up linia-uziem.:

≤1000 V – 1,2/50 μs, C2

Znamionowy prąd wyładowczy i_N linia-linia:

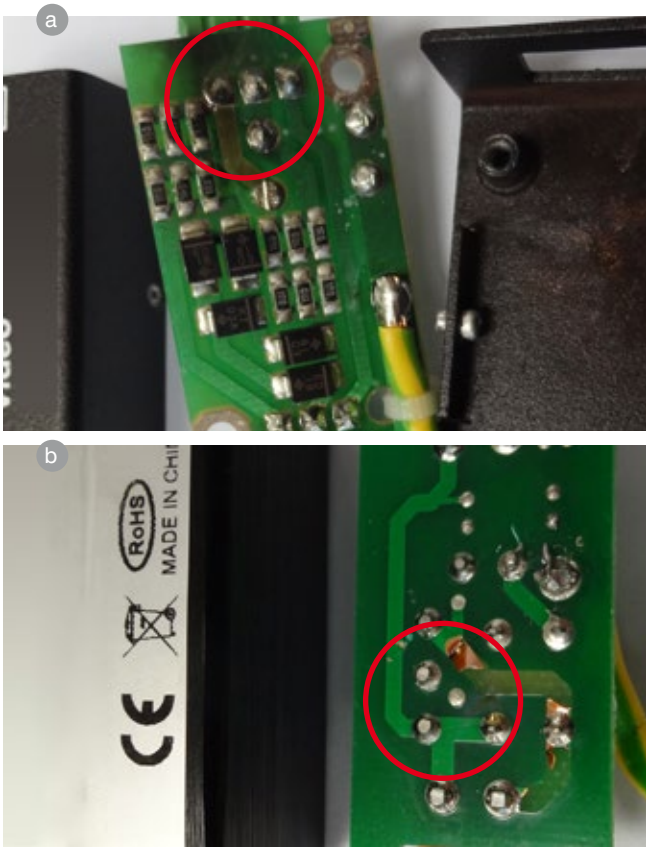
25 A – 10/1000 μs, C3

Znamionowy prąd wyładowczy i_N linia-uziem.:

5 kA – 8/20 μs, C2

Podanie znamionowej wartości prądu wyładowczego oznacza, że SPD powinien wytrzymać taki udar wielokrotnie, a w tym przypadku już pierwsza próba okazała się niszczącą (rys. 4a).

Ostatni z przypadków uszkodzenia ścieżek na laminacie PCB dotyczył ogranicznika przepięć przeznaczonego do ochrony obwodu zasilania. W danych katalogowych podano „Maksymalny prąd wyładowczy: 10 kA (8/20μs)". Uszkodzenie nastąpiło już przy wartości około 5 kA (rys. 4b).



Rys. 4. Ograniczniki przepięć podczas próby udarowej z wykorzystaniem znamionowego prądu wyładowczego

Kolejny rodzaj uszkodzenia jednego z ograniczników, jakie nastąpiło w wyniku przeprowadzanych prób, polegał na uszkodzeniu diod stanowiących drugi stopień ochrony. W katalogu podano poniższe informacje:

Nominalny prąd wyładowczy (8/20μs):

5 kA

Maksymalny prąd wyładowczy (8/20μs):

10 kA

Urządzenie powinno mieć więc stosunkowo wysoką odporność. Niestety nie było możliwości sprawdzenia, jak urządzenie zachowa się przy deklarowanej wartości nominalnego

prądu wyładowczego (5 kA 8/20 μs), ponieważ uległo uszkodzeniu już przy wstępnych próbach z zastosowaniem udaru 1 kV/0,5 kA. W wyniku braku koordynacji między elementami ogranicznika, przy doprowadzonym przepięciu odgromnik nie zadziałał odpowiednio wcześnie, aby przejąć energię udaru. W konsekwencji dioda była narażona na oddziaływanie całej energii zaburzenia, która przekraczała jej graniczną wytrzymałość, przez co nastąpiło uszkodzenie elementu i zwarcie diody. Gdyby producent przeprowadził pełne badania ogranicznika, uwzględniające próbę martwej strefy, problem ten zostałby wykryty przed wprowadzeniem elementu do sprzedaży. Próba martwej strefy ma na celu sprawdzenie koordynacji ograniczników dwustopniowych w celu zbadania, czy urządzenie wytrzymuje udary w zakresie przepięć, które nie powodują zadziałania ochrony zgrubnej pierwszego stopnia. Należy podkreślić, że konstrukcja ogranicznika była dosyć złożona – zawierał on odgromnik trójelektrodowy, warystory, szeregowe elementy indukcyjne oraz diody. Tak więc złożoność ogranicznika nie zawsze idzie w parze z jego jakością. Warto dodać, że na obudowie urządzenia zamieszczono nieprawidłowy znak CE oraz napis „Made in China".

Ostatni rodzaj uszkodzenia miał miejsce w przypadku ogranicznika przepięć do sieci IP. Ogranicznik ten wyróżniał się deklarowaną odpornością udarową wynoszącą aż 10 kA 8/20 μs (oznaczoną błędnie jako I_{imp}, które to oznaczenie jest przypisane odporności na udary o kształcie 10/350 μs):

Prąd wyładowczy C2 (8/20μS, linia-ziemia) I_{imp}

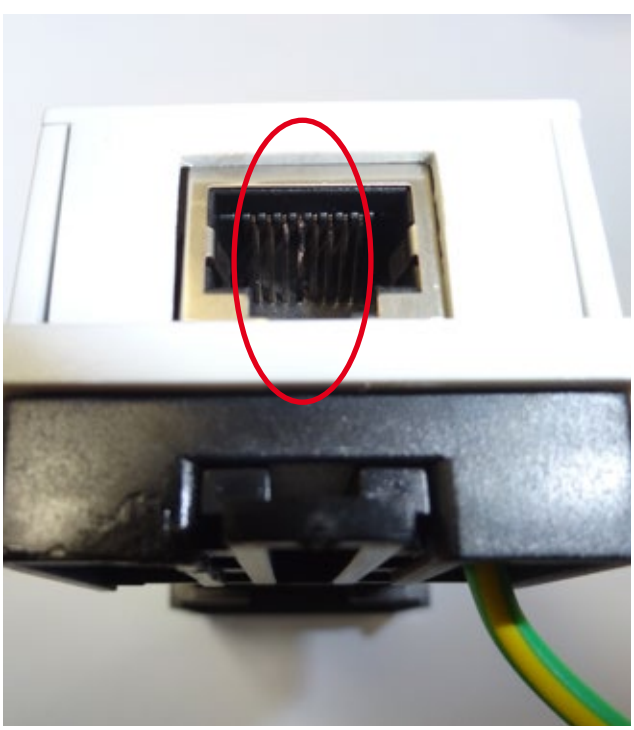
10 kA.

W przypadku pozostałych ograniczników z grupy zabezpieczeń IP deklarowane były wartości 2 kA–2,5 kA.

Ogranicznik ten, podobnie jak wszystkie pozostałe, wytrzymał udar o wartości szczytowej 2 kA. W jego przypadku próby przeprowadzono jednak również dla wyższych wartości ze względu na deklarowane parametry. Maksymalna wartość udaru prądowego, jaki kilkukrotnie jest w stanie wytrzymać złącze typu RJ45, wynosi około 2,5 kA 8/20 μs. Przy udarach o wyższych wartościach najczęściej uszkodzeniom ulegają nie elementy wewnętrzne SPD, ale złącza RJ45. Nawet jeżeli nie nastąpi przerwanie pinów gniazda RJ45 lub wtyczki, to w wyniku przepływu prądu udarowego następuje zespawanie pinów, a spaw ulega przerwaniu przy pierwszym wyjęciu wtyczki. Podobnie było w analizowanym przypadku. Przy udarze o wartości 5 kA nastąpiło uszkodzenie zarówno gniazda, jak i wtyczki RJ45 powodujące przerwanie ciągłości linii (rys. 5). W opinii autora deklarowanie wytrzymałości wyższej niż 2,5 kA w przypadku takich ograniczników jest bezpodstawne ze względu na ograniczenia związane z fizycznymi właściwościami złącz RJ45.

Podsumowanie

Wyniki przeprowadzonych badań świadczą jednoznacznie o złym stanie większości oferowanych na polskim rynku ograniczników przepięć przeznaczonych do ochrony systemów telewizji dozorowej. Jedynie w przypadku dwóch spośród sześciu producentów wszystkie testowane ograniczniki przepięć przeszły badania z wynikiem pozytywnym. Analizując 17 urządzeń czterech producentów, których urządzenia nie spełniały wymagań, w dziewięciu stwierdzono uszkodzenia na skutek narażenia na udary o deklarowanych wartościach, a w dwóch kolejnych stwierdzono niezgodność w zakresie deklarowanych prądów roboczych (ograniczenie prądu przy niższej wartości niż deklarowana). Ponadto parametry techniczne podawane w instrukcjach i kartach katalogowych są często niejasne i błędne. Otrzymane wyniki wskazują na to, że niektórzy producenci wydają deklaracje zgodności bezpodstawnie, nie przeprowadziwszy wymaganych badań w celu potwierdzenia deklarowanych parametrów. Na początku jakość urządzenia ocenia się na podstawie parametrów podawanych przez producenta w kartach katalogowych – im bardziej są szczegółowe i zgodne z wymaganiami normy PN-EN 61643-21, tym większe jest prawdopodobieństwo, że produkt został rzeczywiście przebadany. Nie jest to jednak regułą, o czym świadczy przypadek jednego z producentów – pomimo prawidłowo podanych danych trzy z pięciu ograniczników uległy uszkodzeniu przy próbach udarowych. W przypadku przebadanych urządzeń właściwym kryterium oceny jakości okazała się cena. Urządzenia dwóch producentów, które przeszły badania bez zastrzeżeń, były nawet kilkukrotnie droższe od produktów pozostałych firm, które można nabyć po cenach rynkowych (uwzględniających rabaty) wynoszących od 30 do 70 zł netto. Koszty przeprowadzenia rzetelnych badań zgodnie z normą PN-EN 61643-21 uniemożliwiają oferowanie produktów w tak niskich cenach. Projektanci i inwestorzy nie powinni zatem kierować się jak najniższą ceną przy doborze ograniczników przepięć. W celu zapewnienia skutecznej ochrony instalacji przed skutkami wyładowań atmosferycznych należy stosować produkty dobrej jakości, najlepiej firm specjalizujących się w produkcji odpowiednich urządzeń.



Rys. 5. Uszkodzenia złącz RJ45 na skutek oddziaływania udarów prądowych

dr inż. Tomasz Maksimowicz

AST DO BRAM DRZWI OKIEN

AST GWARANCJĄ DYSKRETNEJ OCHRONY OBIEKTU

SZEROKA GAMA UNIWERSALNYCH CZUJEK MAGNETYCZNYCH SKUTECZNE ZABEZPIECZENIE BRAM, DRZWI I OKIEN

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Lokalizuj, śledź i oglądaj
w powiększeniu

Bosch Security Systems

W branży systemów zabezpieczeń od kilku lat mamy do czynienia z „wojną na piksele”. Poziom szczegółowości obrazu jest siłą napędową biznesu. To zrozumiałe, gdyż szczegóły mają decydujący wpływ na bezpieczeństwo chronionych obszarów

Personel zajmujący się ochroną powinien mieć dostęp do wszystkich najważniejszych informacji, co umożliwia szybsze reagowanie i podejmowanie właściwych decyzji w przypadku zagrożenia. Poziom szczegółowości jest ważny także podczas identyfikowania osób oraz zbierania materiału dowodowego. Jak to wygląda w sytuacji, gdy poruszający się obiekt opuści pole widzenia kamery? Problem rozwiązuje seria sieciowych kamer zmiennopozycyjnych AUTODOME IP.

Fot. 1. Kamera AUTODOME IP 4000i

Kamery AUTODOME IP mają możliwość szybkiego i precyzyjnego zlokalizowania poruszającej się osoby – nawet ze znacznej odległości. Umożliwiają one użytkownikom systemów ręczne lub automatyczne sterowanie w celu śledzenia poruszających się osób. Umożliwiają także odpowiednie powiększenie obrazu potrzebne do identyfikacji obiektów lub osób także z dużej odległości. Korzyści z interpretacji materiału wizyjnego wykraczają poza cele związane z ochroną. Mogą mieć charakter biznesowy. Dzięki swoim funkcjom analitycznym wszystkie kamery sieciowe AUTODOME IP mogą dostarczać istotnych danych nadających się do dalszego wykorzystania. Egzekwowanie przepisów drogowych w strefach objętych zakazem parkowania, wykrywanie pojazdów jadących pod prąd czy dostarczanie danych statystycznych (liczba samochodów

Fot. 2. Kamera AUTODOME IP 5000i

wjeżdżających i wyjeżdżających z parkingu) umożliwia inteligentne i bardziej efektywne wykorzystanie miejsc przeznaczonych do parkowania. Inteligentne kamery sieciowe AUTODOME IP to początek rewolucji – od tej pory dozór wizyjny nie będzie kojarzył się wyłącznie z rejestracją obrazu.

Nowe możliwości wynikają z rozwoju technologii produkcji kamer. W jaki sposób możemy dalej poprawiać metody ochrony? Co jeszcze możemy zrobić z danymi generowanymi przez systemy dozoru wizyjnego? Unikatowym rozwiązaniem jest kamera sieciowa AUTODOME IP starlight 7000, która łączy technikę starlight z funkcją Intelligent Video Analytics. Bez konieczności stosowania dodatkowego oświetlenia wytwarza ona kolorowy obraz w warunkach, w których inne kamery przechodzą w monochromatyczny tryb pracy. W sposób istotny poprawia to standard ochrony, ponieważ użytkownicy mogą w pełni wykorzystywać możliwości analityczne, m.in. filtrowanie kolorów w scenach o minimalnym poziomie oświetlenia (nawet 0,0077 luksa). Wyższy standard ochrony zapewnia także funkcja Intelligent Tracking. W razie wykrycia obiektu – włącza się na podstawie określonej wcześniej reguły dotyczącej alarmu lub może być aktywowana ręcznie przez kliknięcie myszką na ekranie monitora. Po włączeniu funkcja Intelligent Tracking zapewnia ciągłe, automatyczne śledzenie poruszającego się obiektu. Dynamiczna adaptacja pola widzenia zapewnia optymalną obserwację poruszającego się obiektu. Dzięki technice starlight i zintegrowanej funkcji Intelligent Video Analytics w połączeniu z certyfikatem NEMA-TS2 kamera sieciowa AUTODOME IP starlight 7000 doskonale sprawdzi się w systemach wizyjnego nadzoru nad ruchem drogowym.

Fot. 3. Kamera AUTODOME IP starlight 7000

Kamery sieciowe AUTODOME IP 4000i oraz IP 5000i oferują funkcję Essential Video Analytics. Dzięki niej kamery analizują to, co obserwują, i powiadamiają użytkownika o potencjalnych zagrożeniach w momencie ich zaistnienia. Dzięki temu można wyszukać potrzebne nagrania w trwającym wiele godzin zapisie wizyjnym. Przede wszystkim jednak kamery te potrafią znacznie więcej niż tylko zapewniać bezpieczeństwo. Mogą dostarczać interesujących statystyk, np. dotyczących liczby osób wchodzących na dany obszar, a także pomagać w egzekwowaniu przepisów dotyczących bezpieczeństwa i higieny pracy, np. w przypadku zablokowanego wyjścia ewakuacyjnego.

Bosch Security Systems

Bogatsza wiedza na potrzeby lepszych decyzji biznesowych

Planowanie systemów bezpieczeństwa z użyciem modelu całkowitego kosztu posiadania

Axis Communications

Stworzenie projektu bezpiecznego miasta (ang. *safe city*) wiąże się z ogromnymi wyzwaniami, w tym z koniecznością zaprojektowania i wdrożenia wartego miliony dolarów systemu dozoru wizyjnego. Od czego zacząć? Jak ocenić koszty? Na których elementach systemu należy szczególnie się skupić, aby maksymalnie zwiększyć jego żywotność i wydajność bez generowania niepotrzebnych kosztów? To tylko niektóre z problemów, z którymi należy się zmierzyć w celu zminimalizowania ryzyka pojawienia się przykrych niespodzianek po wdrożeniu systemu

Całkowity koszt posiadania

Więcej informacji to lepsze decyzje biznesowe

Odkryj jak model Całkowitego Kosztu Posiadania może pomóc w podejmowaniu lepszych decyzji finansowych

1500 kamer

10 LAT długość życia

17m USD

Koszty związane z systemem dozoru wizyjnego w całym okresie jego eksploatacji

Cykl życia

Zakupu | Operacyjny | Likwidacji

Cykl życia systemu dozorowego

"Zainstalowaliśmy 4,500 kamer I nie mieliśmy najmniejszego problemu"

Partner Axis

"Nasze "ślepe testy" wykazały, że kamery Axis wykazują mniej niż 1% usterek, w porównaniu z kamerami od innych producentów, których kamery generują usterki na poziomie 4–5%"

Klient Axis

ODKRYJ co tworzy 40+ koszt w Twoim kolejnym systemie dozorowym

www.axis.com/tco

AXIS COMMUNICATIONS

Stworzenie ekonomicznego systemu dozoru wizyjnego jest trudne. Na wszystkich etapach projektowania trzeba uwzględnić wiele czynników, a następnie ponosić koszty bieżącej eksploatacji systemu. Wartość początkowej inwestycji w urządzenia jest zwykle łatwa do oszacowania. Dużo trudniej jest wyliczyć koszty projektu systemu, montażu, konserwacji, modernizacji czy wycofania systemu z eksploatacji. Pomocny w takiej sytuacji może być model całkowitego kosztu posiadania (ang. *total cost of ownership* – TCO).

TCO pozwala uwzględnić wszystkie koszty związane z systemem dozoru wizyjnego w całym okresie jego eksploatacji. TCO to narzędzie biznesowe stosowane w wielu branżach do prawidłowego oszacowania zarówno bezpośrednich, jak i pośrednich kosztów wdrożenia systemu, a także do porównywania różnych systemów o różnych charakterystykach i różnych strukturach kosztów. Dzięki niemu integratorzy i klienci mogą:

– poznać rozkład kosztów w czasie,
– zapoznać się z kosztami poszczególnych elementów systemu,
– zminimalizować ryzyko wystąpienia nieprzewidzianych kosztów,
– łatwiej objaśniać poszczególne koszty w rozmowach z zainteresowanymi stronami,
– właściwie oceniać oferty przetargowe.

tem wciąż rozbudowywany.

Model TCO pozwala uwzględnić i ocenić wiele kosztów, które występują zarówno podczas budowy, jak i w trakcie eksploatacji systemu. Oczywiście model nie jest w stanie określić, kto w rzeczywistości ma ponieść dane koszty – w niektórych przypadkach będzie to klient końcowy, natomiast w innych część kosztów będzie pokrywał integrator. Wszystko jest uzależnione od zawartych umów, zasad finansowania czy gwarancji.

Aby stworzyć proste zestawienie wszystkich kosztów, które mają wpływ na TCO systemów dozorowych, poszczególne koszty są dzielone w zależności od rodzaju i czasu występowania. Cykl życia systemu można podzielić na fazy: nabycie i montaż, eksploatacja i likwidacja. W związku z tym koszty dzieli się na trzy główne kategorie: całkowity koszt nabycia, całkowity koszt operacyjny i całkowity koszt likwidacji.

Firma Axis Communications, globalny lider w branży dozoru wizyjnego, dostrzegła potrzebę stworzenia modelu TCO przeznaczonego dla branży bezpieczeństwa. W 2015 r. firma przeprowadziła kompleksowe badanie. Opracowany w jego wyniku model TCO obejmuje 40 rodzajów kosztów związanych z różnymi elementami systemu i etapami jego realizacji, w tym m.in. inwestycje w sprzęt i oprogramowanie, gwarancje, koszty instalacji i integracji z już istniejącymi rozwiązaniami, szkoleń dla operatorów, zarządzania projektem, funkcjono-

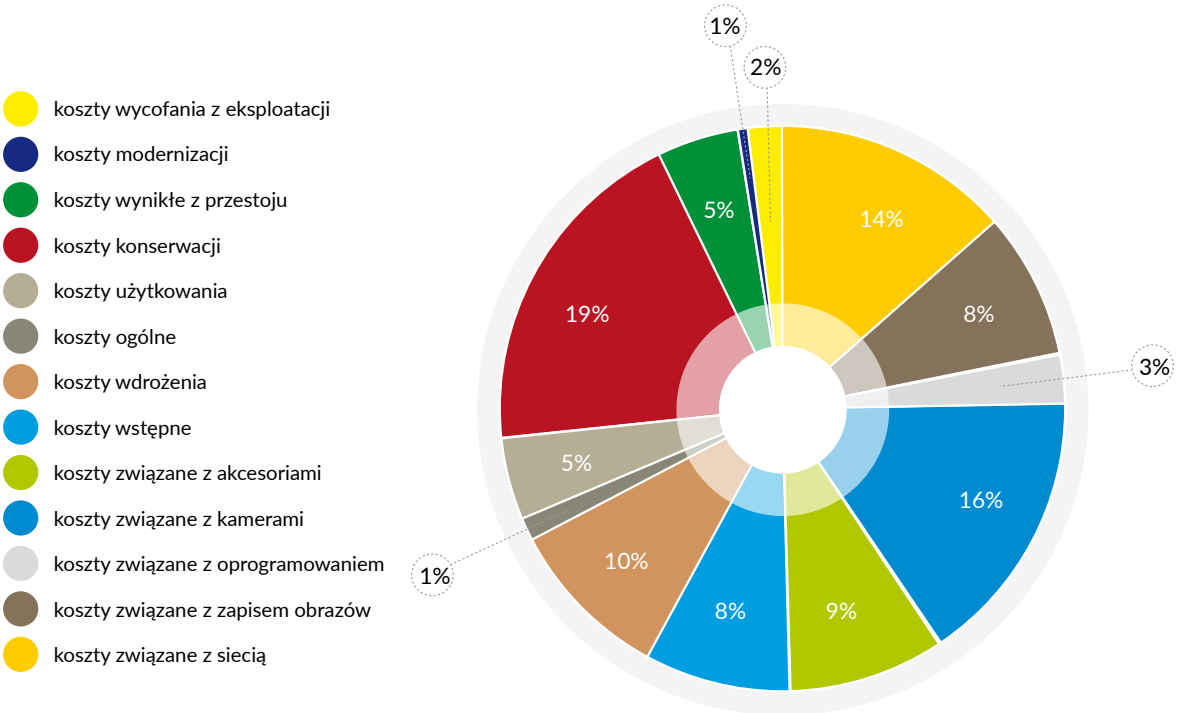
Rys. 1. Cykl życia systemu monitorowania

Warto podkreślić, że nie ma jednolitego modelu TCO, który pasuje do każdego projektu. Wręcz przeciwnie – każdy projekt jest unikatowy i wyjątkowe są determinanty wpływające na to, jak należy go analizować i wyceniać. Ważna jest specyfika monitorowanego obiektu. System tworzony z myślą o lotnisku będzie zasadniczo różny od systemu dostosowywanego do infrastruktury krytycznej czy szkoły – różny pod wieloma względami, np. pod względem wielkości czy kosztów przestoju w pracy systemu. Inną zmienną jest „czas życia" wykorzystanych rozwiązań – w niektórych zastosowaniach, np. w monitoringu miejskim, system może funkcjonować w niezmienionym stanie przez wiele lat, natomiast w innych, np. w handlu detalicznym, kamery mogą być regularnie przemieszczane, a system wciąż rozbudowywany.

wania, konserwacji, a także likwidacji systemu.

Przy opracowywaniu modelu punktem odniesienia był duży miejski system nadzoru wizyjnego zawierający 1500 kamer. Model uwzględnia koszty zarządzania projektem, użytkowania, konserwacji, wycofania z eksploatacji oraz wiele innych. Wszystkie są przedstawione graficznie, za pomocą zrozumiałych, prostych wykresów.

Model TCO opracowany przez firmę Axis może być narzędziem przydatnym przy wycenianiu projektów lub ocenie ofert. Model (rys. 2) przedstawia przykłady kosztów, których można się spodziewać na poszczególnych etapach życia systemu i wskazuje te obszary, na których należy się skupić w celu redukcji kosztów i poprawy jakości wykorzystywanych



Rys. 2. Ilustruje całkowity koszt posiadania przykładowego systemu. Szczegółowe informacje można znaleźć w pełnym raporcie, który jest dostępny na stronie https://www.axis.com/pl/pl/solutions-by-industry/total-cost-of-ownership.

rozwiązań. Należy pamiętać, że niniejszy model TCO nie jest dostosowany do wszystkich projektów – każda realizacja jest wyjątkowa i model powinien to odzwierciedlać, uwzględniając różne zmienne, np. skalę projektu, branżę czy wymagania systemowe.

W raporcie o TCO można przeczytać, jak kompleksowa analiza kosztów może pomóc w podejmowaniu lepszych decyzji biznesowych dotyczących projektów z dziedziny bezpieczeństwa.

Axis Communications

JEDNO SŁOWO, WIELE ROZWIĄZAŃ

sferica.net

SiCUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

TAM, GDZIE PRODUKTY I STRATEGIE TWORZĄ ROZWIĄZANIA

Fiera Milano, Rho

W DNIACH 15-17 LISTOPADA 2017 ROKU

www.sicurezza.it

WRAZ Z

SMART BUILDING EXPO

ZAREJESTRUJ SIĘ NA STRONIE INTERNETOWEJ
WWW.SICUREZZA.IT OSZCZĘDZAJ CZAS I PIENIĄDZE!

MIĘDZYNARODOWA SIEĆ

BRASEG BRAZILIAN TRADE SHOW FOR OCCUPATIONAL SAFETY AND HEALTH, AND FIRE PROTECTION
www.braseg.tmp.br

EXPOSEC INTERNATIONAL SECURITY FAIR
www.exposec.com.br

FISP INTERNATIONAL FAIR OF SAFETY AND PROTECTION
www.fispvirtual.com.br

POD PATRONATEM

Ministero della Difesa

Città metropolitana di Milano

CAMERA DI COMMERCIO MILANO

ZORGANIZOWANA PRZEZ

FIERA MILANO

Prewencja przyszłością nadzoru wizyjnego

Inteligentne techniki termowizyjne i sieciowe systemy dozorowe poprawiają bezpieczeństwo

dr Tristan Haage

Jak wynika z aktualnych danych Stowarzyszenia Niemieckich Towarzystw Ubezpieczeniowych GDV, w Niemczech co pięć minut płonie siedziba jakiegoś przedsiębiorstwa. Powstające w ten sposób szkody ekonomiczne sięgają co roku miliardów EUR. Równie niepokojące są aktualne statystyki dotyczące włamań, których liczba wzrosła w minionych pięciu latach o ponad 30%. Wykrywalność sprawców włamań do obiektów przemysłowych wynosi niecałe 20%. Dane te wyraźnie pokazują, jak ważna jest prewencja w zakresie wykrywania włamań i pożarów. Inteligentne systemy zabezpieczające, które wykorzystują techniki wizyjne i termowizyjne, przydają się nie tylko do wyjaśniania przyczyn w przypadku zaistnienia szkody, lecz także do zapobiegania zagrożeniom jeszcze przed ich wystąpieniem

Fot. 1. Rozwiązania firmy MOBOTIX skutecznie zapobiegają kradzieży i wandalizmowi

Ze względu na rosnącą liczbę włamań ekonomiczne i skuteczne rozwiązania zabezpieczające stają się wszechobecne. Coraz więcej firm decyduje się na zastosowanie systemów wizyjnych do monitorowania budynków, instalacji i terenu zakładów. Straty finansowe wynikające z kradzieży, wandalizmu czy pożarów mogą być dla firm bardzo dotkliwe, zwłaszcza gdy dochodzi nie tylko do powstania bezpośrednich szkód majątkowych (a w związku z tym również do wzrostu składek ubezpieczeniowych), lecz także do przestojów w produkcji. Dlatego kluczowe jest zapobieganie zagrożeniom i powstawaniu szkód. Jak jednak wykorzystać technikę wizyjną do działań prewencyjnych?

Granica nie do pokonania dla tradycyjnych systemów wizyjnych

Zwykłe kamery mogą wytwarzać materiał wizyjny, który ułatwia wyjaśnienie przyczyn zaistniałych zdarzeń – o ile system rejestracji obrazu działa niezawodnie, a jakość nagrań jest odpowiednia. Niestety wiele zainstalowanych i oferowanych obecnie systemów wizyjnych nie spełnia nawet tych minimalnych oczekiwań użytkowników. Jakość obrazu nie wystarcza do uzyskania materiału dowodowego. Większość sprzedawanych kamer w dalszym ciągu ma rozdzielczość nie przekraczającą 3 megapikseli (źródło: badanie rynku przeprowadzone przez firmę IHS Research, sierpień 2016 r.). Kolejnym ograniczeniem jest niska czułość przetworników obrazu, która przy słabym oświetleniu skutkuje rozmyciem obrazów ruchomych obiektów.

O jakości systemu wizyjnego decyduje jednak nie tylko wyraźność obrazu poruszających się obiektów, lecz także odporność na awarie. Kluczowych jest tu kilka czynników, w tym niezawodność kamer oraz możliwość zapisywania obrazu w przypadku awarii połączeń sieciowych, które zapobiega utracie danych potrzebnych do wyjaśnienia sprawy. Ze względu na bezpieczeństwo najlepszy jest system, w którym każda kamera ma jak najwięcej inteligentnych funkcji, dzięki którym przetwarzanie i analiza obrazu nie muszą odbywać się na serwerze centralnym.

Inteligentne systemy wizyjne wykrywają zagrożenia i zapobiegają szkodom

Jeśli kamery nie służą wyłącznie do tworzenia obrazu, lecz są wyposażone w wydajne procesory i inteligentne aplikacje, system wizyjny można wykorzystać skuteczniej, w szczególności do wykrywania zagrożeń i zapobiegania szkodom. Inteligentne kamery „wkraczają do akcji" tylko wtedy, gdy jest to naprawdę konieczne. Mają zainstalowane odpowiednie oprogramowanie do detekcji ruchu i umożliwiają zarządzanie alarmami. Jeśli na przykład w zdefiniowanym oknie czasowym ktoś wtargnie na chroniony teren, kamery mogą odstraszyć intruza, nadając przez głośnik komunikat głosowy i włączając dodatkowe oświetlenie. Kamery mogą także informować wybrane osoby o wtargnięciu intruzów za pośrednictwem telefonii VoIP lub wiadomości e-mail.

Aby takie nowoczesne rozwiązanie zabezpieczające było skuteczne i przydatne w praktyce, należy wyeliminować fałszywe alarmy wywoływane przez zakłócenia powodowane przez ruchome elementy otoczenia widoczne na obrazie, takie jak gałęzie drzew poruszane wiatrem, lub drgania masztów, na których umieszczone są kamery. Tradycyjne techniki zabezpieczające nie są w stanie sprostać temu zadaniu. Wiele dostępnych na rynku systemów wizyjnych ma bardzo ograniczone możliwości eliminacji zakłóceń. W najnowocześniejszych kamerach stosowane jest inteligentne oprogramowanie, dzięki któremu poruszające się obiekty są odróżniane od ruchomego tła. Dzięki zastosowaniu narzędzi do wykrywania ruchu na trójwymiarowych zobrazowaniach, takich jak MxActivitySensor 2.0, ograniczana jest liczba fałszywych alarmów powodowanych np. przez ptaki czy małe zwierzęta.

Jednoczesne wykorzystanie obrazów termowizyjnych i obrazów powstałych w widmie optycznym umożliwia skuteczną ochronę obiektów i granic terenów zamkniętych

Aby stworzyć wydajne zabezpieczenia, niezbędne są inteligentne funkcje realizowane w kamerach, inteligentne oprogramowanie do wykrywania ruchu i aktywne zarządzanie alarmami.

Fot. 2. Nowe kamery z platformy Mx6 przesyłają strumienie wideo w różnych formatach – MxPEG, M-JPEG i H.264

Nadzór wizyjny często ogranicza się jedynie do rejestracji obrazu. Połączenie technik termowizyjnych z klasycznymi technikami wizyjnymi przynosi wymierne korzyści. Za pomocą kamer dwuobiektywowych, które są wyposażone w przetwornik optyczny i przetwornik termowizyjny, można wykrywać nawet obiekty odległe i poruszające się w absolutnych ciemnościach. Przetwornik termowizyjny niezawodnie wykrywa ruch, a przetwornik optyczny tworzy obraz o rozdzielczości 6 Mpx, na którym można bez trudu rozpoznać ludzi i wykonywane przez nich czynności, co może mieć decydujące znaczenie przy ściganiu sprawców przestępstw. Aby wszystko to było możliwe również w nocy, kamery mogą włączać dodatkowe oświetlenie, gdy przetwornik termowizyjny wykryje ruch.

Kamery dwuobiektywowe z przetwornikami optycznymi i termowizyjnymi umożliwiają nie tylko skuteczną ochronę obiektów i granic terenu. Pomagają też chronić prywatność, co jest bardzo ważne zwłaszcza w miejscach publicznych, takich jak obiekty sportowe czy szpitale. Obraz termowizyjny zawiera profil termiczny, który nie umożliwia rozpoznania poszczególnych osób, ale w razie potrzeby kamery dwuobiektywowe mogą automatycznie uruchomić przetwornik optyczny zamiast termowizyjnego i wytwarzać strumień wizyjny o wysokiej rozdzielczości, gdy tylko na obserwowanym obszarze coś się poruszy.

Prewencja dzięki inteligentnemu monitorowaniu procesów

Techniki wizyjne i narzędzia termowizyjne są coraz częściej wykorzystywane przez firmy do rejestrowania niebezpiecznych sytuacji w procesach produkcyjnych. Przykładowo, w branży spożywczej kamery są wykorzystywane w procesach kontroli jakości. Często stosuje się kamery hemisferyczne o wysokiej rozdzielczości i szerokim polu widzenia, z funkcją cyfrowego przetwarzania obrazu. W zakładach produkcyjnych przydają się kamery zewnętrzne, odporne na wahania temperatury i wpływ wilgoci, które dzięki konstrukcji pozbawionej elementów ruchomych praktycznie nie wymagają konserwacji.

Kamery dwuobiektywowe, które są wyposażone zarówno w przetwornik optyczny, jak i w specjalny, skalibrowany przetwornik termiczny, mogą z kolei monitorować procesy, w których duże znaczenie ma temperatura. Również takie wykorzystanie kamer do zapobiegania szkodom w wyniku przegrzania lub pożaru wymaga użycia inteligentnego systemu, który automatycznie wygeneruje alarm, gdy temperatura spadnie poniżej lub wzrośnie powyżej zdefiniowanych granic, lub gdy wzrost temperatury będzie zbyt gwałtowny. Odpowiednia integracja z systemem SCADA pozwala zatrzymać proces produkcyjny lub włączyć chłodzenie, zanim dojdzie do powstania szkód. Kamery dwuobiektywowe umożliwiają też nakładanie obrazu optycznego na obraz termiczny co pomaga w szybkiej identyfikacji miejsc awarii, których temperatura przekracza wartość krytyczną, np. w maszynowni.

Systemy inteligentne są też opłacalne

Zainwestowanie w bazujące na niezawodnych kamerach i inteligentnym oprogramowaniu wizyjne systemy zabezpieczające jest opłacalne. Aby można było zapobiegać szkodom ekonomicznym powstającym w wyniku kradzieży, wandalizmu czy pożarów, niezbędne jest zastosowanie inteligentnych kamer, które nie tylko dostarczą czytelny obraz, lecz także przeanalizują zarejestrowane dane, rozpoznają zagrożenia i automatycznie podejmą działania ukierunkowane na ich eliminację. Inteligentny system kamer ma jeszcze jedną kluczową zaletę – koszty jego wdrożenia są niższe niż koszty instalacji tradycyjnego systemu wizyjnego, a inwestycja szybko się zwraca. Gdy przetwarzanie i analiza obrazu w kamerach oraz rejestrowanie danych w sieciowej pamięci masowej nie odbywa

Fot. 3. Dr Tristan Haage

się w trybie ciągłym, lecz jest dokonywane na skutek pewnych zdarzeń, a kamery dodatkowo zapisują dane w swoich wewnętrznych pamięciach w przypadku awarii sieci, nie jest potrzebna ani duża przepustowość łączy, ani dodatkowa infrastruktura teleinformatyczna. Takie rozwiązanie o zdecentralizowanej architekturze systemowej można bez trudu połączyć z dotychczasową infrastrukturą sieciową. Dzięki zastosowaniu techniki termowizyjnej można zmniejszyć liczbę kamer niezbędnych do zabezpieczenia rozległych obszarów, uniknąć konieczności stosowania dodatkowego oświetlenia, a tym samym zmniejszyć zużycie energii. Z niedawnego badania rynkowego (IHS Research, sierpień 2016 r.) wynika, że najbardziej popularne są tanie kamery IP o bardzo ograniczonych możliwościach. Warto jednak uświadomić sobie, że przyszłością nadzoru wizyjnego jest prewencja. Przy podejmowaniu decyzji o zakupie należy więc skupić się na zaletach inteligentnych zabezpieczeń wizyjnych, a nie tylko na ich cenie.

dr Tristan Haage
członek zarządu ds. sprzedaży w firmie MOBOTIX

dahua TECHNOLOGY

The BEST program of Dahua!

PROGRAM PARTNERSKI DAHUA TECHNOLOGY

KROK
01

Zarejestruj się
na stronie
www.dahua.best

KROK
02

Rejestruj swoje faktury
każde wydane
8 zł to 1 punkt

KROK
03

Wymieniaj punkty
na zakup
wyposażenia

ZAREJESTRUJ SIĘ NA: **WWW.DAHUA.BEST**

CE FC UL RoHS ISO 9001:2000

www.dahuasecurity.com/pl

Dahua Technology Poland Sp. z o.o.
ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

Analogowe systemy dozoru wizyjnego

Maciej Pietrzak

Obecnie jesteśmy świadkami cyfryzacji niemal wszystkich dziedzin techniki, a nieustający rozwój metod cyfrowych powoduje, że metody analogowe przechodzą do historii

Jeszcze do niedawna mówiliśmy to samo w odniesieniu do przyszłości analogowych systemów dozoru wizyjnego. To, że analogowe systemy wizyjne czeka zamiana na systemy cyfrowe, wydawało się oczywiste. W momencie pojawienia się systemów wykorzystujących sieci IP pierwszym argumentem za przewagą systemów cyfrowych nad analogowymi była jakość oferowanego przez nie obrazu. Systemy IP oferowały wyższą rozdzielczość. Drugim „za" była możliwość budowy otwartej struktury sieciowej.

Systemy dozoru wizyjnego przestały być ograniczane przez odległość, na jaką możliwa była transmisja analogowa. Od tamtej pory można było tworzyć systemy z urządzeniami oddalonymi od siebie nawet o setki kilometrów.

Obecnie obie techniki są rozwijane jednocześnie i żadnej z nich nie możemy uznać za gorszą lub przestarzałą. Obie mają nadal racjonalne zastosowanie w systemach wizyjnych. W analogowych systemach dozoru wizyjnego standardem stała się rozdzielczość 2 Mpx, ale od niedawna coraz więcej producentów oferuje kamery o jeszcze wyższej rozdzielczości. Firma Dahua Technology, lider w dziedzinie dostaw elementów systemu dozoru wizyjnego, ogłosiła niedawno opracowanie nowej linii kamer HDCVI.

Kamera HAC-HFW3802EP-Z oferuje obraz o rozdzielczości aż 8 megapikseli, a więc 4K! Ponadto cechuje się wysoką światłoczułością, która wynika z zastosowania przetwornika o rozmiarach 1/2". Kamera ma funkcję rozszerzania dynamiki obrazu realizowaną sprzętowo i jest wyposażona w obiektyw z regulowaną ogniskową, o krotności x3. Powstała również nowa seria kamer Dahua Guardian zbudowanych z wykorzystaniem znacznie większych przetworników – o rozmiarach 4/3".

Nie tylko argument dotyczący wyższej rozdzielczości obrazu w systemach IP stracił na znaczeniu. Systemy analogowe nie są już ograniczane dystansem, na jaki możliwa jest transmisja sygnału z kamery do rejestratora. Technika HDCVI pozwala na przesyłanie sygnału nawet na odległość 500 m przy wykorzystaniu okablowania koncentrycznego. Możliwe jest również wykorzystanie okablowania UTP, w przypadku którego sygnał jest transmitowany na odległość 300 m. Kolejnym krokiem do przodu w technice HDCVI było umożliwienie przesyłu sygnałów wielu typów jednym przewodem. Nie ma już potrzeby instalacji oddzielnego okablowania do transmisji obrazu, dźwięku, do sterowania i do zasilania. Wszystkie sygnały przesyłane są jednym, wspólnym przewodem. Zmiany nie ominęły drugiego końca systemu, czyli rejestratorów. Nie przypominają one już niczym analogowych poprzedników. Nowa seria rejestratorów XVR firmy Dahua Technology pokazuje, że systemy HDCVI zapewniają otwartość i elastyczność. XVR to rejestratory, które pozwalają na wykorzystanie wielu trybów analogowych, w tym CVI, TVI, AHD i SD oraz trybów IP w jednym systemie. Każdy z kanałów rejestratora może pracować w jednym z wymienionych trybów. Dzięki temu mamy możliwość zbudowania skalowalnego systemu spełniającego nawet najwyższe wymagania funkcjonalne oraz oferującego najnowocześniejsze osiągnięcia techniczne. Jednym z nowatorskich rozwiązań było wprowadzenie na rynek panoramicznych, wieloprzetwornikowych kamer IP. Szybka reakcja firmy Dahua Technology udowodniła, że również kamery analogowe sprawdzą się w tym segmencie. Kamera HDCVI HAC-PFW3601-A180 wykorzystuje trzy przetworniki Starlight, a rozdzielczość każdego z nich wynosi 2 Mpx. Widoki ze wszystkich trzech przetworników są łączone w jeden obraz. W efekcie kamera HDCVI generuje obraz o polu widzenia 180 stopni. Jeżeli to nadal za mało, to do dyspozycji mamy również kamerę wykorzystującą obiektyw typu rybie oko (ang. *fisheye*). Kamera HAC-EBW3802 daje użytkownikowi 360-stopniowe pole widzenia. Wykorzystano w niej przetwornik o rozmiarach 1/2.8", o rozdzielczości 8 Mpx.

Fot. 1. Kamera HAC-HFW3802EP-Z

Analiza treści obrazu długo była zarezerwowana wyłącznie dla systemów IP, jednak i to z czasem uległo zmianie. Seria rejestratorów HDCVI firmy Dahua Technology oferuje zaawansowaną analizę treści obrazu, w tym detekcję intruzów, informowanie o przekroczeniu linii, zliczanie ludzi i inne. Analiza treści obrazu umożliwia automatyzację procesu detekcji niepożądanych zdarzeń, co istotnie wpływa na skuteczność wykrywania incydentów.

Czy w związku z powyższym możemy stwierdzić, że można się obejść bez systemów IP? Absolutnie nie. Jest wiele czynników, które sprawiają, że preferowana jest technika IP. Gdy trzeba zaprojektować rozległy system dozoru, w skład którego będzie wchodzić kilkadziesiąt czy nawet kilkaset kamer, wybór jest prosty – należy wybrać system IP. W przypadku małych systemów wybór nie jest już oczywisty. Systemy HDCVI są tańsze i można je łatwo i szybko zainstalować oraz uruchomić. Mówimy cały czas o budowie całkowicie nowego systemu. Co jednak, gdy jesteśmy zmuszeni wykorzystać niektóre elementy już istniejącego systemu dozorowego? W takim przypadku technika HDCVI jest niezastąpiona. Umożliwia zastąpienie starych analogowych kamer i rejestratorów nowymi, oferującymi obraz o bardzo dobrej jakości (również w nocy) i o wysokiej rozdzielczości, analizę treści obrazu, obraz panoramiczny, a także przesyłanie wielu sygnałów jednym przewodem, nawet na dużych dystansach, a wszystko to z wykorzystaniem starego okablowania koncentrycznego. Dodatkowo, dzięki obsłudze protokołu POS, mamy możliwość integracji wizyjnego systemu dozorowego z terminalami fiskalnymi. Obraz uwidaczniający transakcję może być nakładany na obraz z wybranej kamery. Możemy też uzyskać zdalny dostęp do systemu. Po podłączeniu rejestratora HDCVI do sieci internetowej uzyskujemy dostęp do naszego systemu z dowolnego miejsca na ziemi, za pomocą komputera PC lub aplikacji mobilnej.

Możemy śmiało stwierdzić, że technice analogowej w wizyjnych systemach dozorowych jeszcze długo nie grozi odejście w niepamięć. Nadal znajduje ona zastosowanie w wielu przypadkach. Obie techniki, IP i analogowa, doskonale się uzupełniają i sprawiają, że nic nie stoi na przeszkodzie zbudowaniu nowoczesnego systemu bezpieczeństwa nawet tam, gdzie z różnych względów musimy wykorzystać stare okablowanie koncentryczne lub rejestratory analogowe. Dahua Technology stale pracuje nad rozwojem techniki HDCVI i z pewnością jeszcze nie raz oferta tego producenta wzbudzi zainteresowanie w branży zabezpieczeń.

Maciej Pietrzak
Dahua Technology Poland

Ograniczniki przepięć firmy RST
profesjonalna ochrona systemów sygnałowych

dr inż. Tomasz Maksimowicz

Spółka RST od ponad 20 lat specjalizuje się w ochronie wszelkiego rodzaju obiektów i instalacji przed skutkami wyładowań atmosferycznych. Swoje wieloletnie doświadczenie w tym zakresie przełożyła na produkcję ograniczników przepięć przeznaczonych do ochrony obwodów sygnałowych. Laboratorium firmy umożliwiło opracowanie, przebadanie i wdrożenie do produkcji wysokiej jakości produktów

Badania laboratoryjne ograniczników RST

Wszystkie ograniczniki przepięć produkowane przez RST są w pełni przebadane zgodnie z normą PN-EN 61643-21. Do ich konstrukcji wykorzystywane są wyłącznie podzespoły renomowanych producentów, a montaż jest realizowany w Polsce. Zakres przeprowadzanych badań obejmuje próby mechaniczne, badania środowiskowe w komorze klimatycznej, a także próby elektryczne ze szczególnym naciskiem na odporność na udary. Te ostatnie uwzględniają szczegółowe pomiary napięć ograniczania, odporności na znamionowe i maksymalne prądy udarowe, a także próby martwej strefy oraz testy przeciążeniowe prowadzące do uszkodzenia. Wszystkie ograniczniki są poddawane próbom odporności kategorii C2 (udar 8/20 μs), a także próbom odporności kategorii D1 na udary o dużej energii, symulujące częściowe prądy piorunowe (udar 10/350 μs), dzięki czemu ograniczniki te mogą być stosowane do ochrony obwodów zewnętrznych na granicach stref LPZ 0/1 i wyższych. Weryfikacji podlegają wszystkie właściwości urządzeń, takie jak największe napięcie trwałej pracy, prąd znamionowy, częstotliwość graniczna, a także parametry transmisyjne (jeżeli są istotne). W kartach katalogowych i instrukcjach obsługi produktów RST szczegółowo podane są wszystkie najistotniejsze parametry techniczne. Szeroki zakres badań umożliwia rzetelne potwierdzenie deklarowanych parametrów technicznych i wprowadzenie na rynek produktów o wysokiej jakości.

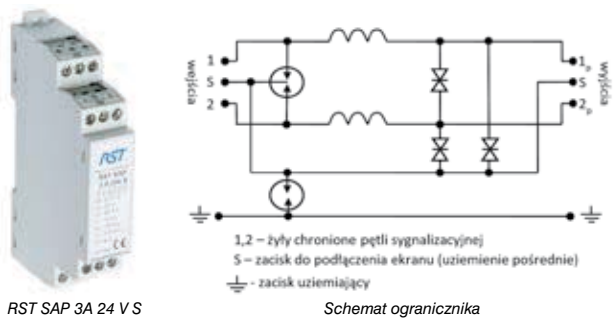
Ograniczniki przepięć ogólnego przeznaczenia

Seria ograniczników RST Guard obejmuje bogaty asortyment produktów do ochrony systemów automatyki, systemów kontrolno-pomiarowych i magistral transmisyjnych przed przepięciami. Wszystkie ograniczniki z tej serii są w obudowach montowanych na szynie 35 mm. Pod względem parametrów technicznych nie ustępują one produktom czołowych firm zachodnich specjalizujących się w produkcji SPD. Charakteryzują się wysoką odpornością na udary indukowane (na poziomie I_{max} = 20 kA 8/20 μs kategorii C2) oraz na częściowe prądy piorunowe (na poziomie I_{imp} = 3,5 kA 10/350 μs kategorii D1). Seria produktów obejmuje grupy ograniczników ogólnego przeznaczenia RST Guard i RST Guard HF przeznaczone odpowiednio do sygnałów do kilku MHz lub kilkudziesięciu MHz na różne napięcia znamionowe. Rozszerzenie serii stanowią ograniczniki przeznaczone do konkretnych zastosowań, takie jak RST Guard RS485 (uniwersalne zabezpieczenie magistral transmisyjnych), RST Guard GDT (ochrona zgrubna), RST Guard Audio (dla ochrony analogowych obwodów akustycznych) oraz RST Guard 24V S (ochrona systemów pomiarowych z pośrednim uziemieniem ekranu kabla).

Seria RST SAP

Ograniczniki RST SAP zostały opracowane z myślą o zabezpieczeniu pętli sygnalizacyjnych systemów sygnalizacji pożarowej. Dzięki bardzo małej rezystancji elementu szeregowego (0,07 Ω), dużemu prądowi znamionowemu (I_N = 3 A) oraz dużej rezystancji izolacji ogranicznik praktycznie nie wpływa na funkcjonowanie chronionego obwodu. Ograniczniki RST SAP charakteryzują się deklarowanymi parametrami w zakresie odporności udarowej jak RST Guard (I_{max} = 20 kA 8/20 μs, I_{imp} = 3,5 kA 10/350 μs), jednak dzięki zastosowaniu pracujących w drugim stopniu ochrony diod o wyższej jakości, które są w stanie pochłonąć większą energię przepięć, są produktami o najwyższej wytrzymałości. Dzięki dużym prądom roboczym, jakie wytrzymują SPD typu RST SAP, znajdują one również zastosowanie w ochronie obwodów zasilania o napięciu do 48 V prądu stałego lub 24 V prądu przemiennego.

Najnowszy produkt z tej rodziny – RST SAP 3A 24V S (rys. 1) – został opracowany z myślą o systemach ppoż., w których producent zaleca uziemienie ekranu kabla pętli sygnalizacyjnej tylko w jednym miejscu, czyli przy centrali. Dzięki dodatkowemu zaciskowi do pośredniego uziemienia ekranu ogranicznik może być zainstalowany w dowolnym miejscu, z zachowaniem wymagań producenta. W warunkach normalnej pracy ogranicznik zapewnia izolację ekranu od uziemienia poprzez odgromnik gazowy, natomiast w chwili wystąpienia przepięcia skutecznie wyrównuje potencjały. Należy tu nadmienić, iż zgodnie z wymaganiami zawartymi w normach odgromowych serii PN-EN 62305 w analizie ryzyka zagrożenia piorunowego instalacja przeciwpożarowa jest uznawana za skuteczny środek redukcji ryzyka pożaru jedynie wówczas, gdy jest zabezpieczona przed przepięciami. W innym przypadku w chwili bezpośredniego uderzenia pioruna, które może wywołać pożar w obiekcie, piorunowy impuls elektromagnetyczny może doprowadzić do uszkodzenia systemu alarmowego, który nie będzie w stanie ostrzec o zagrożeniu.

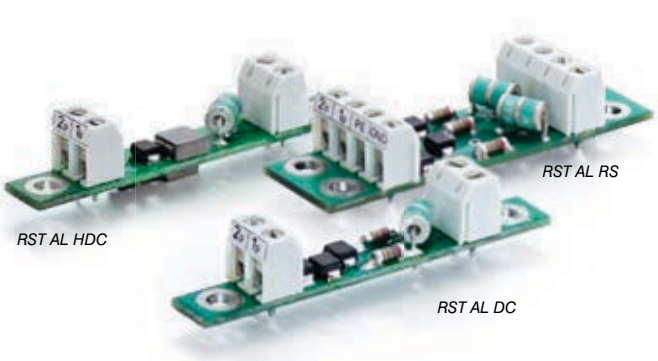


RST SAP 3A 24 V S — Schemat ogranicznika

Rys. 1. Ogranicznik przepięć RST SAP 3A 24V S do ochrony pętli sygnalizacyjnych systemów sygnalizacji pożarowej

Ochrona systemów alarmowych

Ze względu na dużą liczbę obwodów sygnalizacyjnych, jakie doprowadzane są do central alarmowych, konieczne było wypracowanie kompromisu między wymiarami SPD



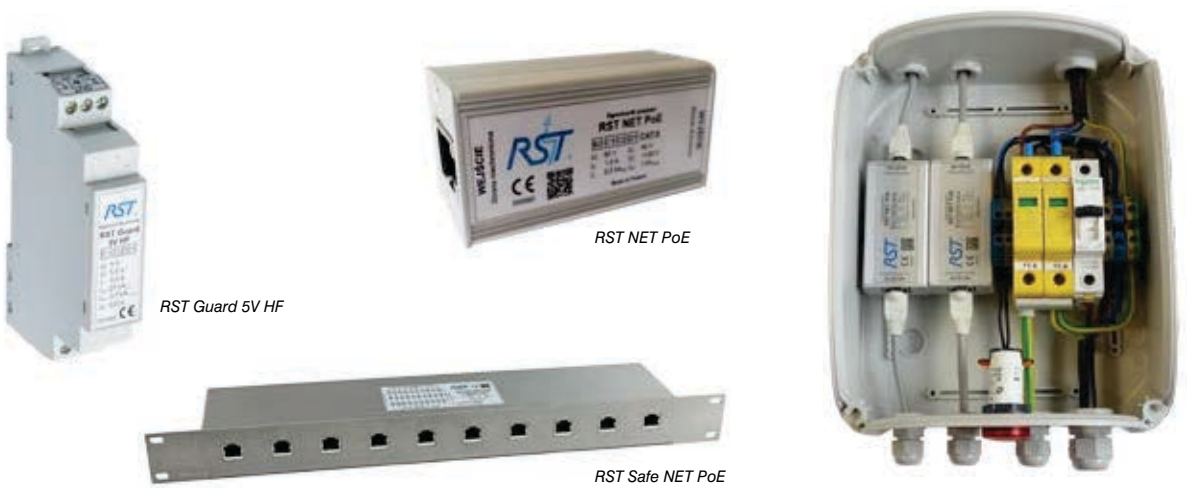
Rys. 2. Ograniczniki przepięć serii RST AL do ochrony systemów alarmowych

a odpornością udarową z jednoczesnym uwzględnieniem docelowego, niewysokiego kosztu pojedynczego modułu. Optymalne rozwiązanie przeznaczone do ochrony takich systemów jak SSWiN czy KD osiągnięto dzięki serii miniaturowych ograniczników przepięć RST AL (rys. 2). Przy niewielkich rozmiarach (wymiary pojedynczego modułu to 10 × 65 mm) uzyskano odporność udarową na poziomie I_{max} = 10 kA 8/20 μs, I_{imp} = 2,5 kA 10/350 μs. Zakres maksymalnych napięć trwałej pracy ograniczników umożliwia stosowanie ich w systemach dowolnych producentów. Z tej serii można wyróżnić następujące grupy:

– RST AL DC – dostosowane do obwodów niskoprądowych;
– RST AL HDC – dostosowane do obwodów wysokoprądowych;
– RST AL RS – dostosowane do magistral transmisyjnych.

uzyskać dla złącz typu RJ45 (I_{max} = 2,5 kA 8/20 μs), a dzięki znakomitym parametrom transmisyjnym może być skutecznie stosowany także w ochronie sieci Ethernet. Ograniczniki obu tych typów mają aluminiowe obudowy, które są instalowane i jednocześnie uziemiane za pomocą zatrzasku na szynę 35 mm. Ponadto oba ograniczniki są dostępne również w wersjach w obudowach 19" (1U) umożliwiających jednoczesne zabezpieczenie do 10 torów i ochronę serwerów, rejestratorów lub przełączników sieciowych.

Oprócz ograniczników służących do indywidualnego zabezpieczenia poszczególnych linii transmisyjnych firma RST oferuje kompleksowe układy RST TV do ochrony systemów CCTV (rys. 3). Klient otrzymuje gotowy do podłączenia układ do ochrony wszelkich obwodów zasilających i sygnałowych w konfiguracji zależnej od typu instalacji CCTV. Do ochrony



Rys. 3. Rozwiązania do ochrony systemów CCTV przed przepięciami

Kompleksowe zabezpieczenie central przy zastosowaniu ograniczników RST AL umożliwia istotne ograniczenie przestrzeni potrzebnej do montażu i znaczne obniżenie kosztów w stosunku do adekwatnej ochrony przy użyciu tradycyjnych ograniczników instalowanych na szynie montażowej.

Rozwiązania dla systemów CCTV

Specjalnością firmy RST są zabezpieczenia do systemów telewizji dozorowej. W ofercie można znaleźć ograniczniki przepięć do ochrony linii transmitujących sygnały wizyjne, sterujące oraz obwody zasilania kamer (rys. 3). Poza ogranicznikami z serii RST Guard, które znajdują zastosowanie w ochronie linii służących do transmisji sygnałów wizyjnych (np. RST Guard 5V HF) lub sygnałów do sterowania kamer (np. RST Guard 12V HF), lub ogranicznikami RST SAP do ochrony zasilania 24 V dostępne są również rozwiązania przeznaczone do innych celów. Ograniczniki RST CCTV BNC-I zapewniają skuteczną ochronę kabli koncentrycznych transmitujących analogowe sygnały wizyjne (I_{max} = 20 kA 8/20 μs, I_{imp} = 2,5 kA 10/350 μs). Pośrednie uziemienie ekranu kabla umożliwia stosowanie ograniczników przy kamerach umieszczonych w terenie bez problemów z zakłóceniami. Z kolei RST NET PoE został opracowany z myślą o ochronie kamer IP z zasilaniem PoE. Ogranicznik ten charakteryzuje się maksymalną odpornością, jaką można obwodów transmitujących sygnały wizyjne i sterujące stosowane są ograniczniki produkowane przez RST, zaś w przypadku zasilania urządzeń wizyjnych napięciem 230 V_{AC} stosowane są wysokiej jakości ograniczniki przepięć produkcji niemieckiej firmy LEUTRON. Wersje z zasilaniem 230 V_{AC} są wyposażone w zewnętrzną optyczną sygnalizację uszkodzenia ogranicznika przepięć, która pozwala na szybkie zdiagnozowanie ewentualnego uszkodzenia bez konieczności demontażu układu, co jest bardzo pomocne podczas konserwacji kamer umieszczanych na wysokich słupach lub na elewacjach budynków.

Podsumowanie

Rozwiązania oferowane przez RST to produkty o wysokiej jakości i potwierdzonych parametrach technicznych. Bogaty asortyment pozwala na dobranie zabezpieczeń do wszelkiego rodzaju instalacji. Do dyspozycji klientów dostępna jest wyspecjalizowana kadra, która pomoże w doborze optymalnych rozwiązań służących do ochrony przed skutkami wyładowań atmosferycznych.

dr inż. Tomasz Maksimowicz
kierownik Działu Badawczo-Rozwojowego
RST sp.j. M. Zielenkiewicz, W. Nietupski, A. Wojtkowski
www.rst.pl, rst@rst.pl, 85 741 08 40

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

dobrze zaprojektowane BEZPIECZEŃSTWO

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

oraz

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

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

25 lat
największych w Polsce spotkań
projektantów, rzeczoznawców, instalatorów i konserwatorów systemów sygnalizacji pożarowej (część 2)

mgr inż. Mariusz Radoszewski

W poprzednim numerze *Zabezpieczeń* przybliżyłem Państwu genezę Ogólnopolskich Warsztatów „Sygnalizacja i Automatyka Pożarowa SAP" i opisałem ich historię do roku 2000. Niniejszy artykuł przedstawia kolejne fakty

Nowy wiek przyniósł kolejny wzrost zainteresowania warsztatami. W 2001 roku zaprezentowaliśmy przygotowaną do wdrożenia centralę POLON 4800 po badaniach certyfikacyjnych. Pokazano też następną centralę konwencjonalną przeznaczoną do sterowania automatycznymi systemami gaszenia pożaru – IGNIS 1520 z osprzętem przycisków sterujących. Przedstawiono kolejne czujki szeregu 40 – jonizacyjną czujkę dymu DIO-40 i czujkę ciepła TUP-40. Czujki szeregu 40 miały wyprzeć wersje szeregu 30, dlatego przygotowano gniazdo G-3840 dla centrali CSP-38 współpracujące z nowymi czujkami szeregu 40. Zaprezentowano nowość – autonomiczną optyczną czujkę dymu ADR-20N przeznaczoną do zainstalowania w mieszkaniach i domach.

POLON-ALFA

Podczas warsztatów w roku 2002 przedstawiono ostatnią centralę z systemu IGNIS 1000 – wieloliniową centralę IGNIS 1240, już z kompletem czujek szeregu 40.

Centrala POLON 4200, która zastąpiła centralę CSP-38, była przedmiotem prezentacji w 2003 roku. Wraz z centralą pokazano komplet czujek szeregu 4043 oraz czujkę wielosensorową DOT-4046, a także wielowyjściowy element sterujący EWS-4001 i sygnalizator adresowalny SAL-4001. Zestaw był uzupełniony przez terminal sygnalizacji równoległej TSR-4001.

W roku 2004 zaprezentowano centralę POLON 4500, czteroliniową centralę systemu POLON 4000, umożliwiającą automatyczne sterowanie gaszeniem maksymalnie czterech stref. Było to pierwsze rozwiązanie, w którym moduły sterujące gaszeniem zostały na stałe umieszczone w centrali sygnalizacyjnej. Zaprezentowano też pierwszą optyczną czujkę dymu DUR-40 wykorzystującą niebieską diodę LED jako nadajnik. W teście TF1 czujka ta wykazywała czułość zbliżoną do czujki jonizacyjnej. Podobne czujki były promowane przez konkurencyjne firmy później (*UV* lub *Blu*).

W 2005 roku pokazano centralę POLON 4900 (zmodernizowaną centralę POLON 4800) i centralę IGNIS 1520M, która miała zastąpić IGNIS 1520 w związku z wprowadzeniem w PN zmian zasad sterowania gaszeniem i organizacji koincydencji. Pokazano również nowe przyciski sterujące gaszeniem, współpracujące z IGNIS 1520M.

W 2006 roku zaprezentowano pierwszą centralę sterującą urządzeniami zabezpieczającymi – UCS 4000. UCS 4000 jest centralą uniwersalną, przeznaczoną do sterowania dowolnymi urządzeniami (oprócz gaszących), szczególnie klapami dymowymi. Przedstawiono także nowatorskie konstrukcje ręcznych ostrzegaczy pożarowych ROP-63 i ROP-4001M, a także przycisków gaszenia i oddymiania. Ostrzegacze nie mają szklanej szybki działającej jednorazowo, lecz poliwęglanową szybkę wielokrotnego użycia. Pod wpływem uderzenia szybka odskakuje do góry, umożliwiając użycie przycisku. Zmiana koloru strzałek wskazujących przycisk z czarnego na żółty informuje o zadziałaniu ostrzegacza. Przywrócenie go do pozycji dozorowania wymaga użycia specjalnego klucza.

W 2007 roku zaprezentowano pierwsze czujki wielodetektorowe szeregu 40 – czujki dymu i ciepła DOT-40 oraz ciepła i płomienia TOP-40. Czujki wielodetektorowe instalowano dotychczas głównie w systemach adresowalnych.

Podczas warsztatów w 2008 roku zademonstrowano centralę IGNIS 1030. Ma ona trzy konwencjonalne linie dozorowe i jest najmniejszą centralą sygnalizacji pożarowej, która zastąpiła centralę IGNIS 1020. W tym samym roku firma Polon-Alfa stała się częścią holdingu AAT, największego w Polsce dostawcy, i od tego czasu również producenta, zabezpieczeń elektronicznych.

W roku 2009 zaprezentowano najmniejszą centralę adresowalną POLON 4100 o dwóch liniach dozorowych (po 64 adresy w każdej). Centrala wyróżnia się spośród innych central systemu POLON 4000 oryginalną szatą graficzną.

W 2011 roku zaprezentowano pierwszą modułową uniwersalną centralę sterującą UCS 6000. Centrala ta ma ogromne możliwości konfiguracyjne (może występować w niemal 40 wersjach), duże moce sterujące (do 64 A) oraz może wysterować wszystkie dostępne rodzaje siłowników i napędów.

Podczas dwudziestych warsztatów przedstawiliśmy najnowszy system sygnalizacji pożarowej POLON 6000 z centralami o architekturze rozproszonej. System ten stał się w ostatnim czasie „motorem napędowym" firmy w ramach oferty produktowej. Gdy pojawił się system POLON 6000, firma Polon-Alfa bezsprzecznie wzmocniła swoją pozycję lidera w zakresie systemów sygnalizacji pożarowej w Polsce. Cechy systemu sprawiają, że w niemalże każdym obiekcie, który podlega zabezpieczeniu tego typu instalacjami, można zastosować POLON 6000 i jego elementy liniowe.

W 2013 roku również prezentowano urządzenia systemu POLON 6000 jako uniwersalnego systemu o architekturze rozproszonej. Poza tym przedstawiono wielosensorową czujkę DTC-6046 (wykrywającą dym, ciepło i tlenek węgla). Omówiono wprowadzenie nowego systemu VENO – specjalnego oprogramowania przeznaczonego do wizualizacji i integracji dostosowanego do systemów sygnalizacji pożarowej produkowanych przez firmę Polon-Alfa.

Podczas warsztatów w 2014 roku zaprezentowano trójpasmową czujkę podczerwieni PPW-40REx przeznaczoną do wykrywania płomieni w strefach zagrożonych wybuchem. Oficjalnie przedstawiono również system POLON 6000 – już po uzyskaniu certyfikatów, wprowadzony do sprzedaży. Uzupełnieniem był nowy szereg tonowych i głosowych sygnalizatorów akustycznych SAW-6000.

Fot. 1. Uniwersalna centrala sterująca UCS 6000

W następnym roku omówiono wiele przykładowych realizacji systemu POLON 6000 i zaprezentowano zastosowane rozwiązania, m.in. funkcje synchronizacji sterowań w realnych warunkach.

Na warsztatach w 2016 roku zaprezentowano nowe funkcje urządzeń, w tym warianty pracy czujek DOT-4046 przeznaczonych do wykorzystania w garażach, dodatkowe wykonanie elementu EKS-6222P umożliwiające obciążenie wyjść prądem aż 12 A przy napięciu 230 V, uzupełnienie zestawu radiowego o ręczne ostrzegacze w wersji bezprzewodowej. Zaprezentowano też nowe podstawowe dwusensorowe czujki dymu DUO-6046/6043. Po raz pierwszy podczas warsztatów pokazano najnowszy produkt firmy Polon-Alfa – system detekcji gazów SDG 6000, który będzie stanowił rozszerzenie naszej oferty i pozwoli na kompleksowe zabezpieczenie obiektów.

Zaprezentowany przegląd ekspozycji wyrobów firmy Polon-Alfa podczas odbywających się od 25 lat warsztatów nie obejmuje wszystkich produktów, które były lub są produkowane w firmie. Ukazuje jednak historię produkcji i rozwijania urządzeń sygnalizacji pożarowej w firmie Polon-Alfa i jest dowodem intensywnych prac, które są stale prowadzone w dziale rozwoju.

Reakcja na aktualne problemy środowiska

Oprócz z góry ustalonych tematów na każdych warsztatach poruszano aktualne problemy nurtujące środowisko projektantów, instalatorów i konserwatorów systemów sygnalizacji pożarowej. Oto niektóre z nich:

- wprowadzenie wymogu przyłączania instalacji do monitorowania pożarowego w jednostkach Państwowej Straży Pożarnej;
- zmiana przepisów dotyczących postępowania z czujkami jonizacyjnymi;
- przygotowania firm projektowo-instalacyjnych do wprowadzania systemów zarządzania jakością ISO 9000;
- wprowadzanie europejskiego systemu certyfikacji wyrobów służących do ochrony przeciwpożarowej;
- przygotowanie projektów PN zgodnych z normami europejskimi, zwłaszcza w zakresie projektowania, instalowania i odbiorów;
- certyfikacja usług z zakresu ochrony przeciwpożarowej;
- aprobaty w certyfikacji urządzeń sygnalizacji pożarowej, których nie obejmują normy zharmonizowane;
- integracja automatyki pożarowej umożliwiająca realizację scenariuszy pożarowych.

Podsumowanie

Organizowane od 25 lat przez firmę Polon-Alfa warsztaty mają bardzo wysoką rangę w środowisku specjalistów zajmujących się ochroną przeciwpożarową. Często byli na nich obecni najwyżsi funkcjonariusze PSP – z komendantami głównymi włącznie – oraz wybitni specjaliści z instytucji związanych z ochroną przeciwpożarową. Wysoki poziom merytoryczny referatów i nieograniczanie się do promowania produktów firmy Polon-Alfa sprawiły, że te ogólnopolskie warsztaty są

Fot. 2. Centrala POLON 6000 o architekturze rozproszonej

opiniotwórcze w branży. Wystąpienia obejmowały i będą obejmować (także w tym roku) szeroką tematykę oraz przekazują uczestnikom ogromną wiedzę z dziedziny sygnalizacji i automatyki pożarowej. Miało to szczególne znaczenie, gdy na rynku brakowało literatury fachowej, nie było branżowych czasopism ani dostępu do zagranicznych norm. Nasi konkurenci zauważyli duże zainteresowanie warsztatami i w związku z tym próbowali organizować podobne spotkania, jednak to warsztaty firmy Polon-Alfa do dziś cieszą się największym zainteresowaniem.

Zapraszamy na kolejne edycje Ogólnopolskich Warsztatów „Sygnalizacja i Automatyka Pożarowa SAP".

mgr inż. Mariusz Radoszewski
Polon-Alfa

Systemy sygnalizacji pożarowej

w pomieszczeniach elektronicznego przetwarzania danych (część 2)

mgr inż. Jerzy Ciszewski

W pierwszej części artykułu (*Zabezpieczenia 4/2017*) wspomniałem, jak ważne jest zabezpieczenie serwerowni. W tej części opiszę podstawowe źródła zagrożeń pożarowych serwerowni, scharakteryzuję pożary oraz przedstawię kwalifikację pożarową obiektu

Kwalifikacja pożarowa obiektu

Budynek centrum przetwarzania danych (CPD) ma przeznaczenie techniczne. Z tego względu kwalifikuje się do kategorii PM. W większości pomieszczeń centrum gęstość obciążenia ogniowego nie przekracza wartości 500 MJ/m^2. Jedynie w pomieszczeniu z agregatem prądotwórczym gęstość obciążenia ogniowego może sięgać 2000 MJ/m^2.

Oczywiście odrębną strefą pożarową powinno być pomieszczenie zawierające szafy z komputerami, macierzami dyskowymi i urządzenia sieciowe, chronione stałymi urządzeniami gaśniczymi. Odrębnymi strefami pożarowymi powinny być również pomieszczenia z transformatorami, z agregatem prądotwórczym, z rozdzielnią średniego napięcia i niskiego napięcia. Gwarantuje to bezprzerwowe zasilanie serwerowni niezależnie od miejsca wybuchu pożaru.

W związku z powyższym w centrum przetwarzania danych powinny być wyodrębnione następujące strefy pożarowe:

– serwerownia,
– pomieszczenie z UPS-ami,
– pomieszczenie z agregatem prądotwórczym,
– pomieszczenie z rozdzielnią niskiego napięcia,
– pomieszczenie z rozdzielnią średniego napięcia,
– komory transformatorów,
– akumulatornia,
– magazyn.

Charakterystyka typowych pożarów serwerowni

Pożary takich obiektów jak serwerownie charakteryzują się na ogół wydzielaniem małej ilości energii i jednocześnie silnym zadymieniem. Zniszczenia spowodowane oddziaływaniem wysokiej temperatury pożaru ograniczają się praktycznie do ogniska pożaru. Najczęstszymi przyczynami pożarów są przeciążenia, zwarcia i inne awarie elementów i urządzeń elektrycznych i elektronicznych. W większości przypadków urządzenia te są instalowane w specjalnych szafach typu rack, dlatego powstałe ogniska pożarów są przeważnie ograniczone przez obudowy uszkodzonych urządzeń elektrycznych. Przyczyną pożarów – na skutek miejscowych przegrzań – mogą być również awarie lub nieprawidłowy montaż urządzeń chłodzących.

Często dużo groźniejsze są zniszczenia spowodowane dymem i oddziaływaniem produktów spalania. Produkty rozkładu tworzyw sztucznych stosowanych w urządzeniach elektrycznych są bardzo trujące i agresywne chemicznie, dlatego dym powstały w trakcie ich spalania stanowi bardzo poważne zagrożenie nie tylko dla personelu, ale także dla urządzeń elektronicznych, które w wyniku działania systemu wentylacji będą miały styczność z produktami spalania. Tworzywa sztuczne, z których budowane są podstawowe elementy urządzeń elektrycznych (izolacje przewodów, płyty elektroniki, obudowy), są w większości niepalne lub ich palność jest obniżana odpowiednimi substancjami. Z tego względu typowy rozwój pożaru w tego typu obiektach, wynikający z uszkodzeń lub nieprawidłowej pracy urządzeń, jest zwykle powolny.

Laboratoryjna demonstracja próby wykrycia dymu towarzyszącego przegrzaniu izolacji krótkiego odcinka przewodu elektrycznego wykazuje, że wobec bardzo nikłego zjawiska wynoszenia jedynym sposobem wykrycia pożaru jest zastosowanie systemu zasysającego. Taki system wykrywa wolno rozwijający się pożar z małą ilością dymu, charakteryzujący się tym, że praktycznie nie występuje zjawisko wynoszenia. Na fotografii widać, że dym równomiernie otacza przewód elektryczny w formie walca, słabo przemieszczając się ku górze. Szansę na wykrycie zagrożenia ma jedynie system zasysający o dostatecznie dużej czułości. Dym wytwarzany w procesie rozkładu termicznego elementów elektronicznych w działającym komputerze będzie jednak wyrzucany na zewnątrz obudowy (szafy) w wyniku działania wentylacji ogólnej lub indywidualnej. Dzięki temu cząstki dymu dotrą do układów detekcyjnych czujek, oczywiście z opóźnieniem i w formie silnie rozrzedzonej.

Zupełnie inny może być przebieg pożaru wywołanego sabotażem czy aktem terrorystycznym. W takim przypadku w celu uzyskania możliwie dużych zniszczeń prawdopodobnie zostaną zastosowane substancje, których pożar będzie miał przebieg płomieniowy, charakteryzujący się silnym zadymieniem i znacznym wzrostem temperatury.

Uszkodzenia w instalacji prowadzące do powstania łuku elektrycznego mogą skutkować szybko rozwijającym się pożarem płomieniowym. Wysoka energia i wysokie napięcie występują w części instalacji związanej z zasilaniem.

Podstawowe źródła zagrożeń pożarowych serwerowni

Występujące materiały palne i łatwopalne

Występujące materiały palne i łatwopalne mogą doprowadzić do powstania pożaru i być przyczyną jego rozprzestrzeniania się. Ilość materiałów palnych ma wpływ przede wszystkim na wydzielanie energii przez pożar i na korozyjność produktów spalania.

Do najczęściej występujących w serwerowniach materiałów palnych można zaliczyć tworzywa sztuczne, płyty z elementami elektronicznymi, przewody elektryczne, materiały wykończeniowe podłogi podniesionej, obudowy urządzeń elektronicznych, papier oraz wszelkiego rodzaju środki czyszczące i konserwujące. W serwerowniach pracują urządzenia biurowe i peryferyjne przetwarzające materiały palne (np. papier). W centrach przetwarzania danych archiwizuje się dane na nośnikach wykonanych z materiałów palnych opakowanych również w materiały palne (płyty, dyski, jak również papierowe formy archiwizacji).

Instalacje sygnalizacji alarmu pożarowego (SAP)

Czy sama instalacja sygnalizacji pożarowej znajdująca się w centrum przetwarzania danych może stanowić jakieś zagrożenie dla systemów komputerowych?

Zagrożenie wynikające z istnienia i funkcjonowania samej instalacji jest bardzo małe. Instalacje SAP są instalacjami niskonapięciowymi/niskoprądowymi, za wyjątkiem linii zasilających centrale 230 V.

Zagrożenie spowodowane oddziaływaniami elektromagnetycznymi linii dozorowych i samych czujek punktowych jest nikłe pod warunkiem, że aktywne czujki systemu adresowalnego nie będą instalowane bezpośrednio w szafach komputerowych. W praktyce umieszczenie czujek w szafach skutkuje natychmiastową utratą gwarancji producenta komputera. Nie dotyczy to oczywiście przypadków, w których w szafie typu rack zainstalowany jest specjalny, autonomiczny moduł

zawierający system wykrywający pożar (czujka zasysająca), a także gazowy system gaszący pożar w szafie.

Rzeczywistym problemem mogą być nieuzasadnione, fałszywe alarmy, które mogą w niektórych przypadkach uruchomić procedurę obrony obiektu. W jej wyniku (w zależności od przyjętego sposobu wentylacji serwerowni) zostaną zamknięte klapy doprowadzające świeże powietrze do klimatyzatorów, może być chwilowo wstrzymywana wentylacja ogólna, a nawet

Fot. 1. Słabe rozprzestrzenianie się dymu w czasie testu polegającego na przegrzaniu izolacji (fot. „Zabezpieczenia")

może zostać uwolniony środek gaśniczy (zmiany temperatury, zamglenie, hałas). To samo może nastąpić w przypadku niewłaściwej eksploatacji i serwisowania systemu SAP. Nieuzasadnione uruchomienie systemu kontroli dostępu otwierające drogi ewakuacyjne dla personelu może umożliwić działania sabotażowe w obiekcie. Z tego powodu eliminacja fałszywych alarmów ma najwyższy priorytet.

Dobór instalacji sygnalizacji pożarowej o zbyt niskiej czułości może powodować uruchamianie gazowego systemu gaśniczego w zbyt późnej fazie rozwoju pożaru i skutkować dużymi stratami popożarowymi oraz silną emisją toksycznych produktów spalania i rozkładu termicznego chemicznego środka gaśniczego stanowiących zagrożenie dla ludzi i sprzętu elektronicznego (jeśli taki został użyty). Najwłaściwszym systemem współpracującym z urządzeniem gaśniczym jest zasysający system wczesnej detekcji.

Pozostałe zagrożenia wynikające z faktu zainstalowania systemu SAP, takie jak uszkodzenie czujek jonizacyjnych, możliwość uwolnienia wodoru z akumulatorów itp., są do pominięcia.

Działalność człowieka

Działania człowieka stwarzające zagrożenie pożarowe serwerowni:

- działania sabotażowe wewnątrz budynku z użyciem materiałów wybuchowych lub niebezpiecznych substancji chemicznych;
- inne działania sabotażowe mające na celu zniszczenie lub uszkodzenie wybranych systemów: wentylacji, klimatyzacji, kontroli dostępu, systemu wykrywania pożaru, systemu antywłamaniowego, central sterujących, systemu zasilania i źródeł awaryjnych;
- uszkodzenia i awarie spowodowane nieumyślnie przez osoby postronne podczas serwisowania systemów i urządzeń, remontowania i innych prac, do których zatrudniany jest personel obcy (z zewnątrz);
- nieodpowiednia organizacja pracy, niewłaściwe zachowanie personelu, zwłaszcza w warunkach krytycznych, zaniedbywanie obowiązków związanych z kontrolą stanu technicznego systemów, nieprawidłowa eksploatacja systemów;
- brak kontroli, nadzoru i bieżącego rejestrowania stanu bezpieczeństwa pożarowego w obiekcie, w tym nieodpowiedni poziom organizacyjny ochrony przeciwpożarowej w przedsiębiorstwie;
- działania terrorystyczne w pobliżu budynku – wysadzenie samochodu, uwolnienie niebezpiecznych substancji chemicznych; (systemy wentylacji w ramach wielu wymian wprowadzają do przestrzeni wentylowanej kilka procent świeżego powietrza, które może zostać zanieczyszczone w wyniku takich działań);
- podejmowanie prób gaszenia pożaru przez nieprzeszkolony personel;
- uzyskanie dostępu do systemów bezpieczeństwa związanych z ochroną przeciwpożarową przez osoby nieupoważnione.

W kolejnej części artykułu opiszę techniki wykrywania pożaru w serwerowniach.

mgr inż. Jerzy Ciszewski
IBP NODEX

WIELOPUNKTOWY I WIELOGAZOWY SYSTEM DETEKCJI CO/LPG... NO_2... W GARAŻACH I PARKINGACH PODZIEMNYCH

JEŚLI MUSISZ STOSUJ ORYGINALNE

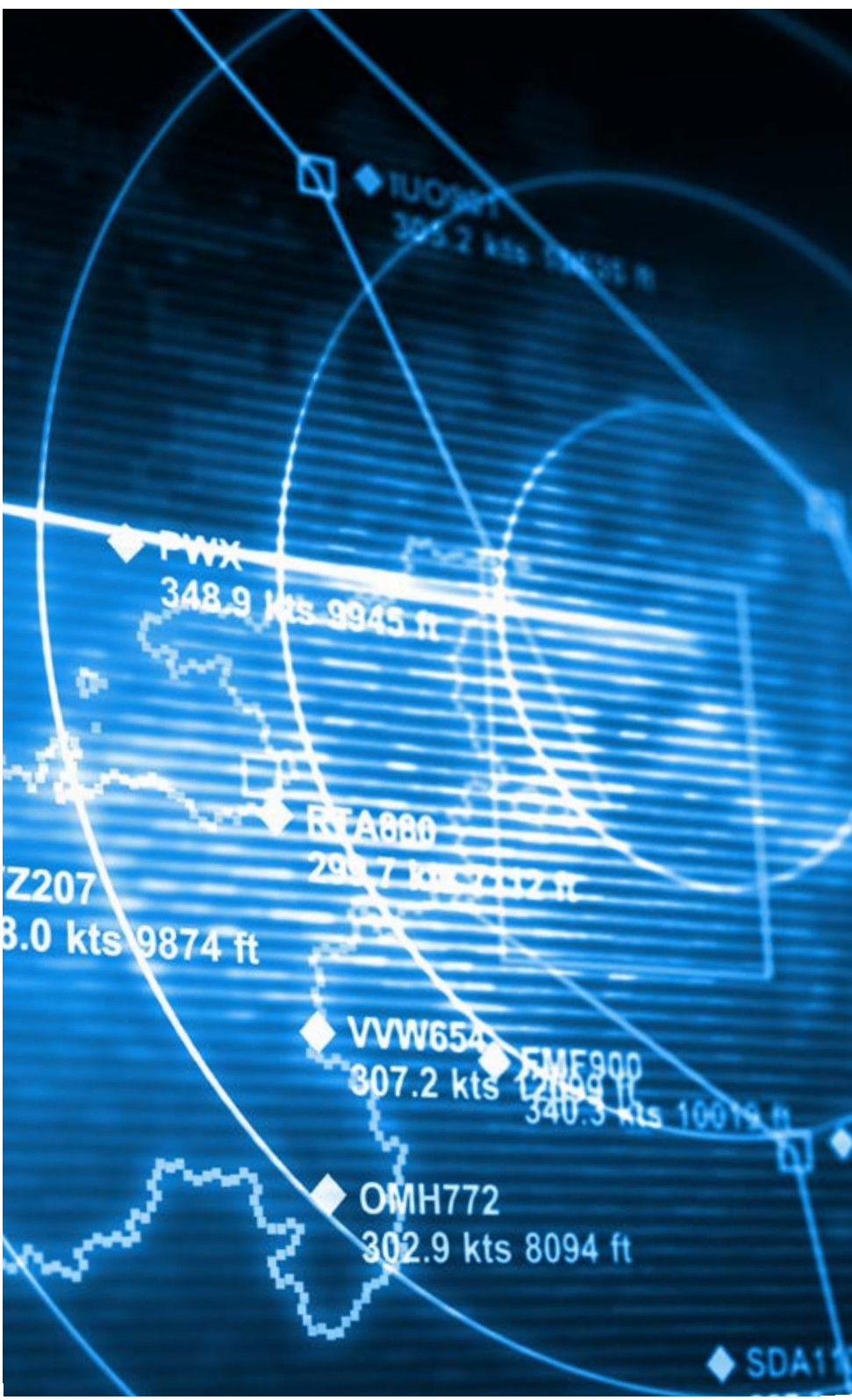
PRO-SERVICE®

Przedsiębiorstwo Wdrożeniowe Pro-Service© Sp. z o.o.
Os. Złotej Jesieni 4, 31-826 Kraków, Tel. 12 425 90 90
www.alarmgaz.com

Od radarów wojskowych
do ochrony perymetrycznej
rozwój technik wykorzystujących mikrofale

Maciej Prelich

Zaskakująco dużo technik, których używamy na co dzień, ma swoje początki w rozwiązaniach tworzonych na potrzeby wojska. Jednym z najlepszych przykładów jest system nawigacji satelitarnej GPS. Początkowo był używany tylko przez armię Stanów Zjednoczonych. Teraz jest nieodłącznym elementem codziennego życia i komunikacji. Innym przykładem może być wykorzystanie mikrofal

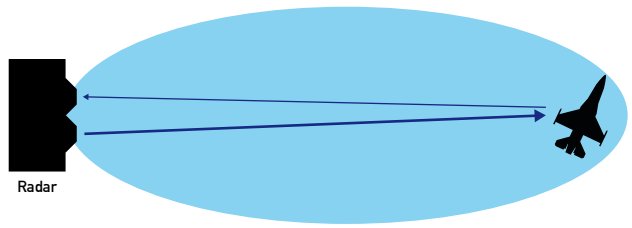


Mikrofale to po prostu promieniowanie elektromagnetyczne o częstotliwości od 1 GHz do 300 GHz – z zakresu pomiędzy poczerwienią a falami ultrakrótkimi. Już w 1864 roku James Maxwell teoretycznie przewidział istnienie mikrofal, ale dopiero prace nad radarami umożliwiły rozwój teorii oraz badań nad ich właściwościami. Mikrofale są wykorzystywane bardzo różnie, m.in. w radarach, kuchenkach mikrofalowych, telefonach komórkowych, w bezprzewodowych sieciach WLAN i Bluetooth.

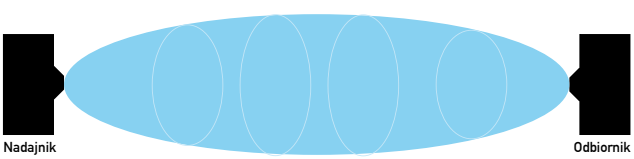
Amerykański inżynier Percy Spencer zauważył podczas badań nad wytwarzaniem fal elektromagnetycznych stosowanych w urządzeniach radarowych, że mikrofale wprawiają cząsteczki wody w drgania rotacyjne, a tym samym zwiększają jej temperaturę. Dzięki temu zjawisku w 1947 roku na rynek została wprowadzona pierwsza kuchenka mikrofalowa Raytheon Radarange, która ważyła 340 kg oraz miała 1,65 m wysokości. Była ona przydatna głównie w obiektach przemysłowych i na okrętach marynarki wojennej.

Rys. 1. Kuchenka mikrofalowa Raytheon Radarange

Skupmy się teraz na interesujących nas radarach, gdyż to one są urządzeniami wykorzystującymi mikrofale w systemach ochrony perymetrycznej. Wykrywanie obiektów polega na zjawisku odbicia fal radiowych. Rozróżniamy dwa główne typy radarów – aktywny (emituje wiązkę mikrofal na danym terenie, odbiornik umieszczony obok nadajnika szuka sygnałów odbitych od obiektów) oraz pasywny (nie emituje mikrofal, a jedynie odbiera promieniowanie odbite od obiektów, pochodzące od nadajników telekomunikacyjnych lub innych radarów). Na przykład w prędkościomierzach drogowych wykorzystujących efekt Dopplera wykrycie poruszającego się pojazdu polega na porównaniu częstotliwości fali wychodzącej oraz przychodzącej. W przypadku odbicia od nieruchomych obiektów częstotliwości będą takie same. Jeśli mikrofale odbiją się od obiektu oddalającego się od czujki, to odebrany sygnał będzie cechował się mniejszą częstotliwością. Jeśli sygnał odbije się od obiektu zbliżającego się do czujki, to częstotliwość zostanie zwiększona.



Rys. 2. Schemat działania radaru



Rys. 3. Schemat działania bariery mikrofalowej

Obecnie ta technika ma zastosowania typowo wojskowe, a także jest używana w barierach mikrofalowych, które za pomocą kolumn z nadajnikami i odbiornikami generują niewidzialne ściany i służą do detekcji intruzów. Takie systemy jak bariera Model 316 amerykańskiej firmy Southwest Microwave są z powodzeniem stosowane do ochrony budynków przemysłowych, obiektów o podwyższonym ryzyku włamania (elektrowni, rafinerii), a także terenów prywatnych.

Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski
mprelich@atline.pl

Profesjonalne zasilacze awaryjne marki PowerWalker

Tomasz Lenartowicz

Firma BlueWalker, producent zasilaczy awaryjnych marki PowerWalker, kładzie coraz większy nacisk na tworzenie profesjonalnych urządzeń jedno- i trójfazowych. Obecnie asortyment oferowanych zasilaczy awaryjnych powiększono, wprowadzając nowe modele z współczynnikiem mocy 1.0. Dostępne są też modele o większej mocy wyjściowej, w konfiguracji trójfazowej. Wszystkie zasilacze z serii profesjonalnej pracują w trybie on-line, dzięki czemu uzyskujemy całkowite odizolowanie podłączonych urządzeń od sieci energetycznej. Konwersja jest dwuetapowa. W pierwszym etapie prąd przemienny z sieci energetycznej jest konwertowany na prąd stały. Następnie, w drugim etapie, prąd stały jest z powrotem zamieniany poprzez falownik na prąd przemienny, dzięki czemu na wyjściu otrzymujemy prąd o bardzo dobrych parametrach. Zachowywany jest sinusoidalny kształt napięcia wyjściowego, o stabilnej częstotliwości, dlatego mamy pewność, że podłączone urządzenia są całkowicie odseparowane od sieci energetycznej i są zasilane napięciem o niezniekształconym przebiegu.

Do grupy profesjonalnych zasilaczy jednofazowych należą dwie nowe serie – VFI CPG PF1 oraz VFI RMG PF1.

VFI CPG PF1 to zasilacze w obudowie Tower, z najwyższym w przypadku zasilaczy dostępnych w sprzedaży współczynnikiem mocy równym 1. Oznacza to, że do zasilacza o mocy pozornej równej 1000 VA możemy podłączyć obciążenie o mocy czynnej równej aż 1000 W. Z powyższej serii wyróżniamy sześć urządzeń, które różnią się mocą wyjściową (1 kW, 1,5 kW, 2 kW, 3 kW) i są wyposażone w gniazda wyjściowe zgodne z IEC C13, oraz urządzenia większej mocy wyjściowej (równej 6 kW i 10 kW), które są wyposażone w złącze terminalowe, więc możemy je wpiąć bezpośrednio do instalacji elektrycznej. Urządzenia z serii CPG PF1 charakteryzują się wysoką sprawnością (od 89 do 94%). Opisywane zasilacze awaryjne są przeznaczone do zasilania urządzeń elektrycznych bardzo wrażliwych na stabilność zasilania, w przypadku których nawet najmniejsza niestabilność uniemożliwia prawidłową pracę.

Do drugiej serii zasilaczy jednofazowych o współczynniku mocy 1 należą modele przeznaczone do montażu w szafach RACK 19". W serii VFI RMG PF1 można wyróżnić cztery urządzenia o mocach wyjściowych równych 1 kW, 1,5 kW, 2 kW i 3 kW. Wszystkie modele są wyposażone w wydajną ładowarkę do akumulatorów, o prądzie ładowania równym 12 A, dzięki czemu po podłączeniu akumulatorów o dużej mocy znacznie skraca się czas ładowania (istnieje możliwość doboru optymalnej wartości prądu ładowania z poziomu wyświetlacza – w zakresie od 1 A do 12 A).

Firma BlueWalker jako jeden z niewielu producentów oferuje zasilacze trójfazowe przeznaczone do montażu w szafie

RACK 19". Jest to seria VFI CPR, w której skład wchodzą trzy urządzenia o mocach wyjściowych równych 10 kVA, 15 kVA i 20 kVA. Wszystkie modele mają wbudowane akumulatory. Czas podtrzymania przy pełnym obciążeniu wynosi od dwóch do trzech minut. Do wyboru jest również konfiguracja faz wyjściowych: 3/1 lub 3/3. Wysoka sprawność energetyczna i parametry techniczne to nie jedyne atuty serii CPR. Istnieje możliwość podłączenia redundantnego do trzech urządzeń o tej samej mocy wyjściowej. W najbardziej rozbudowanej konfiguracji można uzyskać moc wyjściową równą aż 60 kVA.

Zasilacze VFI CP 3/3, dzięki niewielkim rozmiarom i dużej mocy przyłączeniowej, mogą służyć do zasilania najbardziej wymagających maszyn, silników elektrycznych oraz innych urządzeń wymagających stabilnego zasilania. Dostępne urządzenia z serii CP mają następujące moce wyjściowe: 10 kVA, 15 kVA, 20 kVA, 30 kVA. Urządzenia te charakteryzują się wysokim współczynnikiem mocy równym 0,9 oraz wysoką sprawnością energetyczną. Każdy zasilacz może zostać rozbudowany przez dodanie dodatkowego modułu bateryjnego, modułu SNMP (który umożliwia sygnalizację awarii za pośrednictwem sieci LAN), modułu AS-400 (który umożliwia komunikację z serwerami IBM). W sprzedaży jest dodatkowy moduł EMD, dzięki któremu można kontrolować środowisko pracy zasilacza, co jest wymagane w niektórych projektach.

Kolejną serią zasilaczy awaryjnych do zastosowań profesjonalnych są urządzenia modułowe VFI CPM 3/3. To dziesięć modułów, z których każdy ma moc wyjściową 30 kVA. Wszystkie moduły współpracują ze sobą, dzięki czemu jednostka sterująca na bieżąco dobiera odpowiednią liczbę modułów niezbędnych do pracy w danych warunkach. Na przykład przy zainstalowanych dziesięciu modułach o mocy 30 KVA wykorzystujemy tylko połowę mocy zasilacza, a druga połowa jest dostępna w trybie rezerwowym. W przypadku modeli serii

CPM 3/3 można podłączyć zewnętrzne akumulatory w celu wydłużenia czasu zasilania w warunkach awaryjnych, gdy nie ma sprawnego, zewnętrznego zasilania. W zasilaczu został zamontowany dotykowy wyświetlacz LCD o przekątnej 10" służący do zarządzania urządzeniem i wszystkimi jego parametrami. Zasilacz tego typu sprawdza się w centrach danych, gdzie bezwzględnie musi być zachowana ciągłość pracy urządzeń teleinformatycznych.

Do wszystkich pracujących w trybie on-line zasilaczy marki PowerWalker dostępnych jest wiele akcesoriów: moduły bateryjne, karty SNMP które umożliwiają sygnalizację awarii za pośrednictwem sieci LAN, karty AS-400 (zapewniające komunikację z serwerami IBM), moduły EMD (które umożliwiają monitorowanie temperatury i wilgotności powietrza w otoczeniu urządzeń), MBS.

Tomasz Lenartowicz
Impakt

ROZWIJAMY SIĘ
dzięki zaufaniu

NAJLEPSZA NA ŚWIECIE

Seria WISENET X

ROZWIJAMY SIĘ, bo nasze urządzenia spełniają najwyższe wymagania, pracując w najtrudniejszych warunkach oświetleniowych.

- Najlepszy WDR - 150dB
- Najlepsza jakość obrazu przy minimalnym oświetleniu sceny z zastosowaniem obiektywu motozoom (F0.94)
- Najmocniejszy procesor do obróbki obrazu we wszystkich kamerach serii WISENET X

Więcej informacji na www.hanwha-security.eu/wisenet-x

Hanwha Techwin

Centrala alarmowa PRiMA64

Hybrydowy system o interesujących funkcjach

Michał Konarski

Od kilku lat na polskim rynku dynamicznie zdobywa popularność rodzina nowoczesnych central alarmowych PRiMA produkowanych przez firmę GENEVO. Urządzeniem z tej serii, które ma największe możliwości, jest centrala PRiMA64

Fot. 1. Aplikacja mobilna PRiMAgo!

Na rynku central alarmowych nie pojawia się w dzisiejszych czasach zbyt wiele innowacji. Na szczęście niektóre produkty nie są zgodne z tą tendencją. Jednym z nich jest niewątpliwie centrala alarmowa PRiMA64 firmy GENEVO.

Charakterystyka centrali PRiMA64

Centrala PRiMA64 jest przeznaczona do budowy systemów alarmowych w średniej wielkości i większych obiektach – w apartamentach, domkach, obiektach handlowo-usługowych, budynkach użyteczności publicznej: szkołach, bibliotekach, lecznicach. Umożliwia ona wykorzystanie do 64 linii dozorowych. Mogą to być zarówno tradycyjne urządzenia przewodowe, jak i czujki komunikujące się drogą radiową. System umożliwia również wykorzystanie do 16 wyjść programowalnych (również wyjść wirtualnych), które umożliwiają nie tylko powiadamianie o zagrożeniach, ale także sterowanie dowolnymi urządzeniami.

Wejścia systemu mogą być podzielone na cztery całkowicie niezależne strefy (podsystemy). Strefy mogą posiadać wejścia wspólne, dla których na etapie instalacji można wybrać rodzaj zależności – współzależność typu „AND” (typowo wykorzystywana, jeśli wystąpi „wspólny korytarz”) lub współzależność typu „OR” (np. włączanie w dozór pomieszczenia mającego dwóch różnych użytkowników). Każda z tych stref może mieć wejścia blokowane w trybie tzw. „czuwania domowego”. Jest to taki tryb załączenia strefy, w którym naruszenie części czujek systemu, wybranych przez instalatora podczas programowania, jest ignorowane przez centralę. W efekcie możliwa jest konfiguracja, zgodnie z którą domownicy załączają system na noc i mogą swobodnie poruszać się po wybranym obszarze, ale

wtargnięcie z zewnątrz wywoła sygnalizację alarmu.

Do obsługi systemu PRiMA64 można wyznaczyć 32 użytkowników, a każdemu z nich można przyznać określone uprawnienia – zarówno do dostępu do stref, jak i do korzystania z wybranych funkcji centrali. Taki sposób zarządzania uprawnieniami użytkowników daje dużo swobody przy tworzeniu instalacji w obiektach komercyjnych.

System PRiMA64 ma budowę modułową. Sercem instalacji jest płyta centrali alarmowej, jednak w celu uzyskania wszystkich funkcji urządzenia należy je wyposażyć w moduły rozszerzające oraz urządzenia peryferyjne – manipulatory, ekspandery wejść, ekspandery wyjść programowalnych, a także hub umożliwiający bezprzewodową łączność z maksymalnie 64 urządzeniami alarmowymi EvoLiNK. Do komunikacji z tymi modułami służy inteligentna czteroprzewodowa magistrala, do której można łatwo przyłączać urządzenia metodą plug and play – bez konieczności ręcznego wpisywania adresów w poszczególnych urządzeniach. Maksymalna długość magistrali to 300 m w przypadku zastosowania typowego okablowania alarmowego YTDY z żyłami miedzianymi 0,5 mm. Ze względów bezpieczeństwa komunikacja między urządzeniami przyłączonymi do magistrali jest nadzorowana oraz szyfrowana.

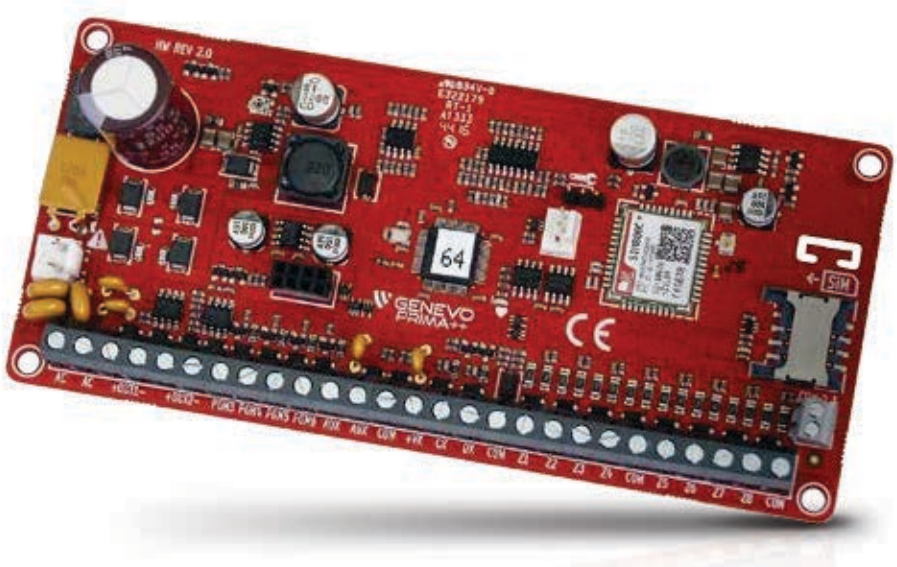
Na płycie centrali PRiMA64 zainstalowany został komunikator GSM/GPRS. Umożliwia on m.in. powiadamianie (np. poprzez SMS) i zdalne sterowanie (z użyciem prostych komend SMS oraz za pomocą specjalnych aplikacji w systemach Android oraz iOS). Centrala PRiMA64 ma także możliwość przesyłania sygnałów w wielu formatach (w tym ContactID oraz we własnym formacie GPRS Kronos) do centrum monitorowania oraz zdalnego programowania poprzez łącze GPRS.

Głównym źródłem zasilania elementów systemu alarmowego z centralą PRiMA64 jest buforowy zasilacz o łącznej wydajności prądowej 2 A, umożliwiający pracę z akumulatorami do zasilania pomocniczego o pojemności 18 Ah (prąd ładowania 600 mA). Zasilacz ma liczne zabezpieczenia, m.in. przeciążeniowe oraz przed głębokim rozładowaniem akumulatora w przypadku przedłużającej się przerwy w dostawie energii.

Obsługa systemu i funkcje komunikacyjne

System PRiMA64 obsługuje się przede wszystkim za pomocą manipulatorów LCD. Centrala PRiMA64 umożliwia przyłączenie do maksymalnie ośmiu manipulatorów LCD, co ułatwia obsługę rozbudowanego systemu z wielu miejsc. Manipulatory mogą być skonfigurowane w taki sposób, by ułatwić obsługę pojedynczego systemu podzielonego na strefy albo wyodrębnienie praktycznie niezależnych podsystemów.

Dużym atutem manipulatorów systemu PRiMA jest graficzny interfejs użytkownika, którego obsługa przypomina korzystanie z bankomatu. Dzięki temu użytkownicy intuicyjnie radzą sobie z obsługą podstawowych funkcji systemu. Nawet korzystanie z bardziej zaawansowanych funkcji nie wymaga ciągłego szukania instrukcji. Najważniejsze informacje na ekranie są przedstawiane za pomocą czytelnych piktogramów, a opisy tekstowe dodatkowo ułatwiają korzystanie z funkcji systemu.



Fot. 2. Centrala PRiMA64

Dzięki możliwościom wbudowanego komunikatora GSM/GPRS system PRiMA64 może również być obsługiwany zdalnie. Użytkownicy smartfonów i tabletów z systemem Android lub iOS mogą skorzystać z bezpłatnej aplikacji PRiMAgo! (która już jest dostępna w Google Play i wkrótce będzie dostępna w AppStore). Aplikacja ta umożliwia podstawową obsługę systemu alarmowego oraz zdalne sterowanie urządzeniami przyłączonymi do centrali (np. roletami, oświetleniem, podlewaniem ogrodu). Użytkownicy innych telefonów mogą skorzystać z funkcji sterowania za pośrednictwem SMS, które – dzięki unikatowej funkcji autoryzacji kodami potwierdzającymi – może być bezpieczniejsze niż w innych systemach.

Oprócz funkcji zdalnego sterowania wbudowany komunikator umożliwia również szczegółowe powiadamianie. Użytkownik systemu otrzymuje na telefon szczegółową informację, np. – w przypadku alarmów – o tym, które wejście wywołało alarmowanie, a w przypadku awarii – o jej przyczynie, np. braku zasilania 230 V.

Centrale serii PRiMA od początku zapewniały szereg ułatwień dla użytkowników korzystających z kart prepaid. Oprócz możliwości sprawdzenia stanu konta (za pomocą manipulatora lub zdalnie) jest też możliwość jego zasilenia przez wpisanie kodu z kuponu zasilającego (tzw. zdrapki).

Nie tylko system alarmowy – nowe funkcje Easy Home Control

Centrala PRiMA64 została zaprojektowana jako urządzenie mające dbać o bezpieczeństwo i zarazem komfort domowników. Pierwotnie umożliwiała proste sterowanie wyjściami, ale w miarę rozwoju oprogramowania i sprzętu pojawiły się nowe możliwości.

Centrala PRiMA64 ma teraz funkcję Easy Home Control, która umożliwia bardzo wygodny sposób sterowania. W ramach Easy Home Control instalator może zdefiniować do sześciu spersonalizowanych ekranów sterowania, na których dostępne są przyciski szybkiego dostępu sterujące wybranymi urządzeniami. Tytuł każdego z takich ekranów ułatwia pogrupowanie funkcji, a możliwość określenia nazw wyjść oraz wyboru piktogramu dla każdego przycisku funkcyjnego z osobna daje praktycznie nieograniczone możliwości dostosowania ich do indywidualnych potrzeb użytkownika.

Fot. 3. Menu Easy Home Control w manipulatorze

Urządzenia przyłączone do centrali mogą być sterowane również za pomocą aplikacji, a także automatycznie, z wykorzystaniem timerów. Centrala PRiMA64 umożliwia realizowanie funkcji logicznych dla wyjść, dzięki czemu można za jej pomocą realizować bardziej złożone sterowanie, łączące działania automatyczne (według timerów, w reakcji na sygnały z różnych czujek) ze sterowaniem ręcznym (z wykorzystaniem manipulatorów lub aplikacji mobilnej).

Przewodowo i bezprzewodowo

Centrala PRiMA64 umożliwia utworzenie spójnego hybrydowego systemu alarmowego zawierającego urządzenia przewodowe i bezprzewodowe urządzenia EvoLiNK. Część czujek systemu może wykorzystywać ekspandery wejść przewodowych, a część z nich łączyć się drogą radiową. Aby wykorzystać w systemie urządzenia bezprzewodowe, wystarczy wyposażyć centralę PRiMA64 w moduł bezprzewodowy EvoHUB. Moduł ten umożliwia obsługę do 64 urządzeń bezprzewodowych, zapewniając w pełni dwukierunkową, szyfrowaną i bezpieczną komunikację w pasmie 868 MHz. System EvoLiNK wykorzystuje nowoczesne, zaawansowane komponenty charakteryzujące się doskonałym zasięgiem komunikacji (w terenie otwartym ponad 0,5 km). Pobór prądu przez składowe urządzenia zasilane bateryjnie jest niski. EvoHUB jest wyposażony w system dwóch anten zapewniających dobrą jakość odbioru wewnątrz budynków, a centrala PRiMA64 może wykorzystać do czterech modułów EvoHUB w celu zapewnienia optymalnego sygnału w rozległych instalacjach. W przypadku zastosowania większej liczby modułów system automatycznie wybiera najkorzystniejszą drogę dla sygnału radiowego (podobnie jak w systemach telefonii GSM), co dodatkowo poprawia niezawodność jego działania. Praca każdego urządzenia bezprzewodowego jest indywidualnie nadzorowana, dzięki czemu użytkownik ma dostęp do pełnej informacji o poziomie sygnału radiowego czy stanie baterii w konkretnym urządzeniu bezprzewodowym. Warto również podkreślić, że czułość czujek systemu EvoLiNK można regulować zdalnie.

Dla ułatwienia instalacji i późniejszej konserwacji systemu centrala PRiMA64 oraz moduły EvoHUB są wyposażone w szereg narzędzi diagnostycznych, m.in. skaner pasma radiowego (umożliwiający ocenę jakości łączności) czy wskaźnik poziomu sygnału (wbudowany w czujki, ułatwiający dobór miejsca ich montażu, uruchamiany zworką podczas instalacji).

Łatwa konfiguracja i konserwacja

Centrala PRiMA64 jest przyjazna nie tylko dla użytkowników systemu alarmowego. Została zaprojektowana tak, by maksymalnie ułatwić pracę instalatora. Z tego właśnie powodu wyposażono ją w szereg funkcji ułatwiających jej konfigurację,

a także późniejszą konserwację systemu.

System można programować za pomocą manipulatora lub komputera. W tym pierwszym przypadku pracę ułatwia czytelne menu trybu serwisowego na dużym wyświetlaczu. Interfejs do programowania jest zbudowany w postaci menu wyborów, dzięki czemu nie trzeba zapamiętywać sekwencji kodów sterujących czy adresów poszczególnych ustawień.

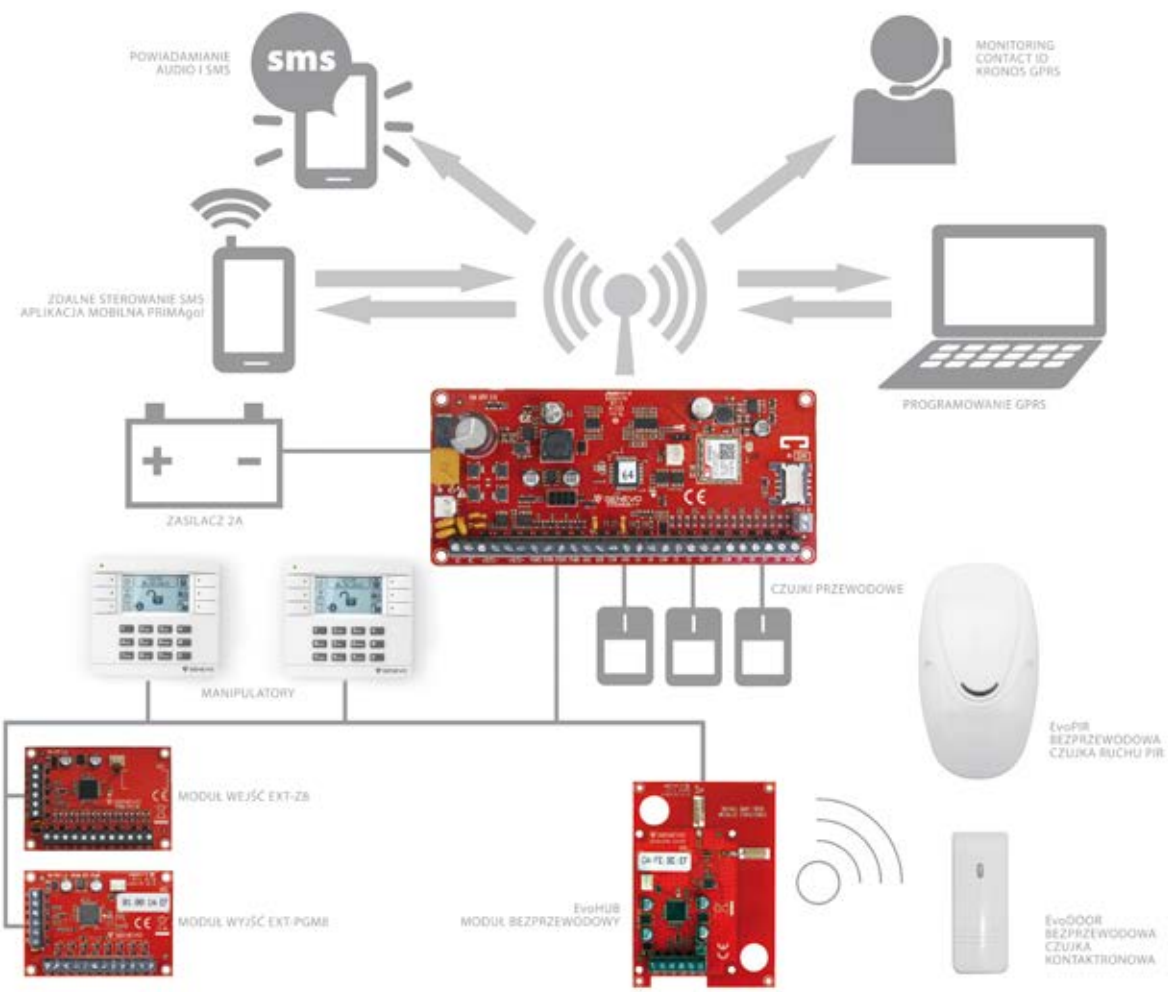
W przypadku bardziej złożonych systemów ułatwieniem jest możliwość programowania z użyciem komputera. Bezpłatny program konfiguracyjny PRiMAtool jest wszechstronnym narzędziem, które pozwala nie tylko na programowanie, ale również na aktualizację firmware'u we wszystkich urządzeniach czy korzystanie z dodatkowych narzędzi diagnostycznych.

Komputer i centrala PRiMA64 mogą być połączone za pomocą specjalnego kabla CUSB-PIN3. Do pracy z centralą można też wykorzystać popularne w branży interfejsy RS-TTL z zakończeniem PIN3.

Połączenie między centralą PRiMA64 i komputerem może też być zrealizowane zdalnie, za pośrednictwem GPRS. W tym przypadku komputer, za pomocą którego programowana jest centrala, powinien mieć dostęp do Internetu zapewniający publicznie dostępny port IP. Ułatwieniem w nawiązaniu takiej łączności jest funkcja programu PRiMAtool weryfikująca prawidłową konfigurację połączenia.

Nie tylko duże systemy

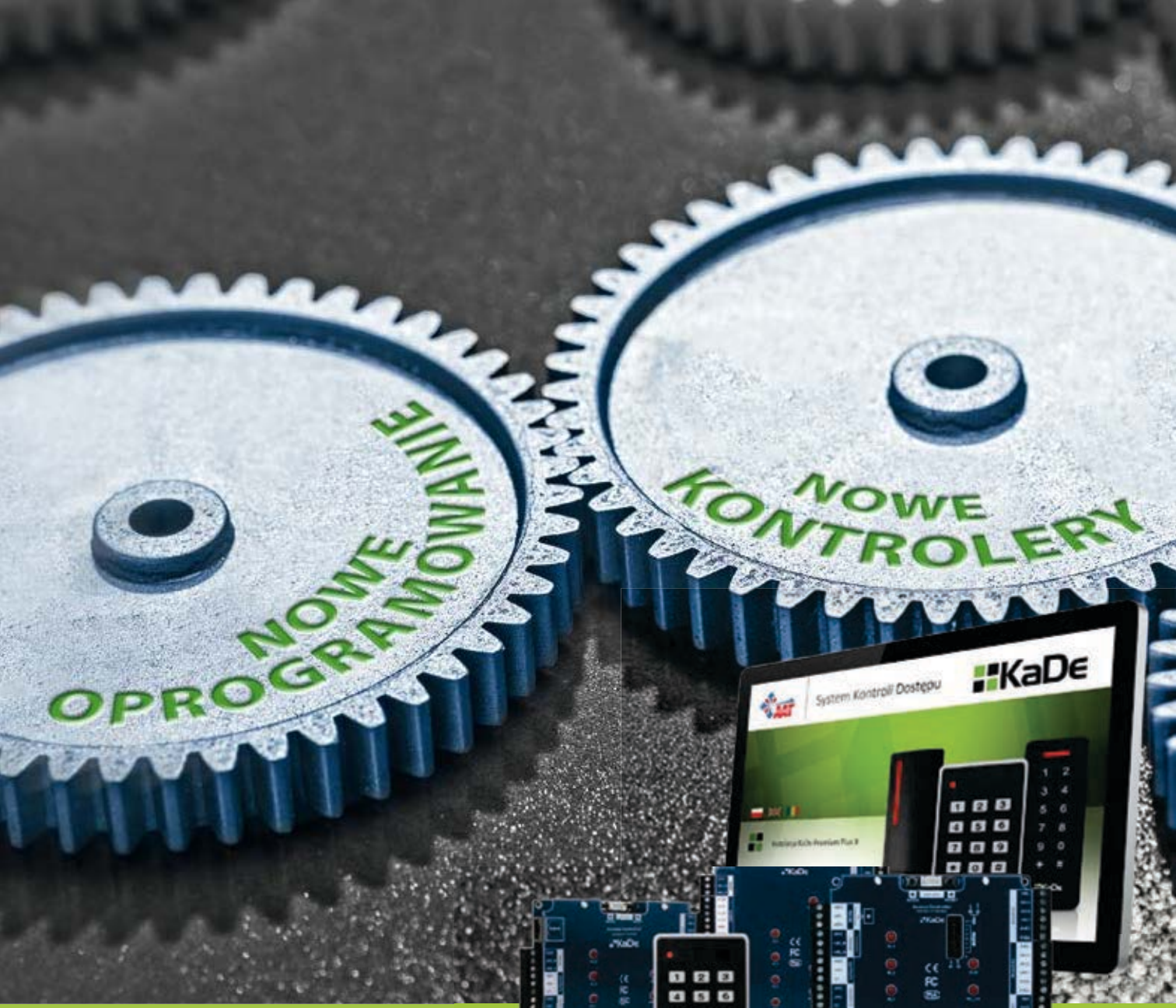
Oprócz centrali PRiMA64 w ofercie firmy GENEVO można znaleźć prostsze centrale alarmowe przeznaczone do mniejszych systemów alarmowych, w których najważniejsze są prosta obsługa i niezawodna komunikacja. Takie centrale jak PRiMA6 czy PRiMA16 mają już ugruntowaną pozycję na rynku i świetnie sprawdzają się w systemach alarmowych o podstawowych, lecz ważnych funkcjach. Bardzo istotna jest pełna unifikacja – w przypadku sprzętu GENEVO wszystkie centrale (od najmniejszej do najbardziej rozbudowanej) wykorzystują wspólne, jednolite oprogramowanie oraz wyposażenie, co ułatwia precyzyjne dopasowanie sprzętu do indywidualnych potrzeb inwestora i nie wymaga od instalatora zmiany przyzwyczajeń.



Rys. 1. Struktura systemu PRiMA64

Warto zwrócić uwagę również na jakość wsparcia technicznego, które firma GENEVO oferuje swoim Klientom i które jest szczególnie ważne dla instalatorów. Świetną okazją do poznania sprzętu firmy GENEVO są prowadzone w całej Polsce – we współpracy z dystrybutorami – szkolenia w formie warsztatów. Dzięki nim można później w pełni wykorzystać potencjał urządzeń.

Michał Konarski
GENEVO
e-mail: info@genevo.pl
www.genevo.pl



KaDe

NOWY SYSTEM KADE
IDEALNE DOPASOWANIE

MAPY OBIEKTU Z AKTYWNYMI, ANIMOWANYMI IKONAMI ELEMENTÓW SYSTEMU
GLOBALNY ANTI-PASSBACK

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

A ty, jaki masz nadajnik alarmowy? (Część 2)

Daniel Kamiński

Czy zastanawiałeś się, dlaczego niektóre firmy ochrony udostępniają swoim klientom aplikacje mobilne do zdalnego sterowania systemem alarmowym lub wyjściami nadajnika, a inne tego nie robią? Czemu niektóre firmy ochrony umożliwiają zdalne konfigurowanie urządzeń poprzez stronę WWW, a inne nie? Dlaczego tylko nieliczne firmy wykrywają, że od jakiegoś czasu nie ma łączności z obiektem, a pozostałe reagują tylko na sygnały, które do nich docierają?

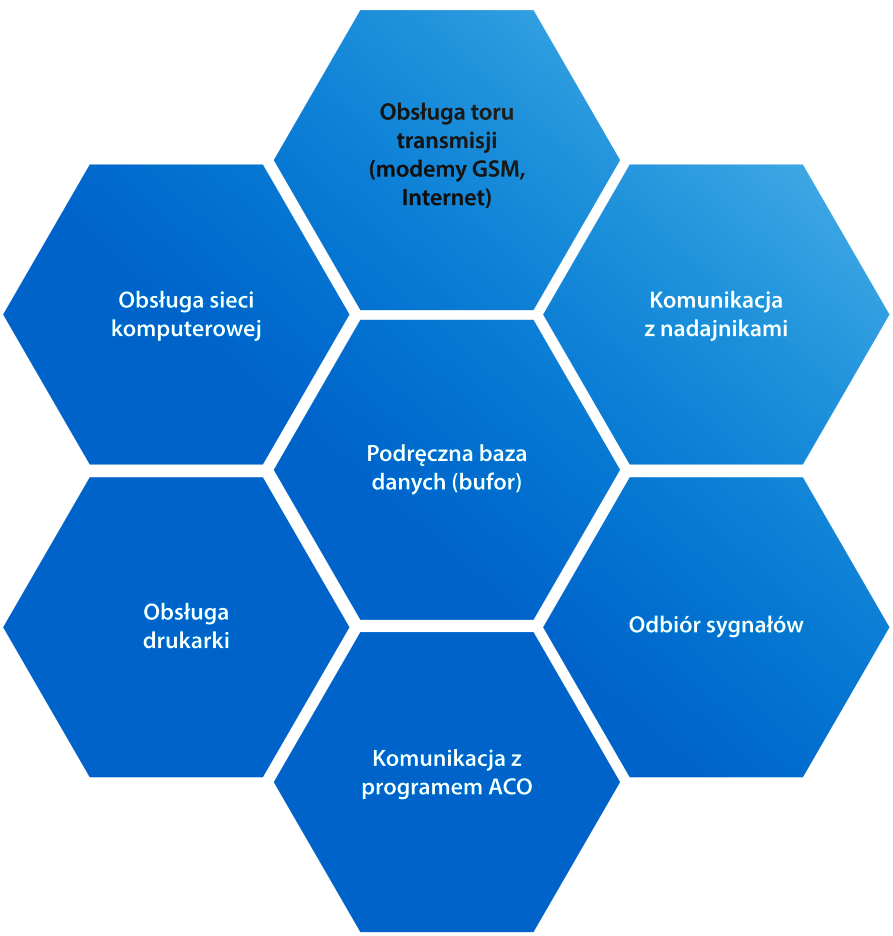
Część firm ochrony korzysta jeszcze z rozwiązań technicznych, które uniemożliwiają stosowanie nowoczesnych usług zwiększających przewagę konkurencyjną. Używają nadajników bez potwierdzeń, wykorzystują proste odbiorniki alarmów lub nie rozwijają oprogramowania służącego do obsługi alarmów. Na szczęście coraz więcej firm rozważa wprowadzenie nowoczesnych rozwiązań. Wierzę, że niniejszy artykuł ułatwi wybór docelowego rozwiązania.

Odwołania do norm

W poprzednim numerze *Zabezpieczeń* (3/2017) opisywałem różne standardy usług monitorowania wynikające ze stosowania w Polsce nadajników alarmowych (urządzeń do transmisji alarmów) i powoływałem się na normy dotyczące systemów alarmowych (w szczególności arkusz PN-EN 50131-10 dot. urządzeń nadawczo-odbiorczych w miejscu chronionym) oraz normy dotyczące systemów transmisji alarmów (w szczególności arkusz PN-EN 50136-2 dot. urządzeń nadawczo-odbiorczych w miejscu chronionym).

W niniejszym artykule skoncentruję się różnych standardach usług monitorowania wynikających z możliwości odbiorników alarmowych stosowanych w Polsce. Powołując się na normy, będę miał na myśli normy dotyczące systemów transmisji alarmów (STA), w szczególności arkusz PN-EN 50136-3 dot. urządzeń nadawczo-odbiorczych centrum odbiorczego, oraz normy dotyczące alarmowego centrum odbiorczego (ACO), w szczególności arkusz PN-EN 50518-2 zawierający wymagania dotyczące urządzeń instalowanych w ACO.

Uważny czytelnik na pewno zauważył, że normy zawierają wytyczne i wymagania dotyczące zabezpieczeń technicznych stosowanych zarówno w chronionych miejscach (obiektach), jak i w alarmowym centrum odbiorczym (ACO) zbierającym informacje z wielu chronionych miejsc. Z tego względu nie będę ich opisywał w artykule, ale polecam zapoznanie się z wymienionymi normami i stosowanie ich w praktyce.



Rys. 1. Podstawowy odbiornik

O nadajnikach raz jeszcze – różne okresy testowania

W poprzednim artykule zawarty był wniosek, że należy stosować tylko nadajniki dwukierunkowe, umożliwiające uzyskanie potwierdzenia, że sygnał alarmowy dotarł do centrum odbiorczego (ACO). Sposób skonfigurowania nadajników może jednak wpłynąć na jakość usługi monitorowania. Jednym z najbardziej różnicujących parametrów są tzw. okresowe testy łączności. Nadajniki części firm wysyłają testy co 20–30 sekund (nadajniki GPRS), ale są też firmy, których nadajniki wysyłają testy co 12–24 godziny (nadajniki radiowe, telefoniczne oraz SMS). Jest to formalnie zgodne z normą, ponieważ ze względu na czas raportowania można zaliczyć wymienione nadajniki do klasy T2 (25 godzin). Nadajniki wykorzystujące GPRS testują łączność co 60–90 sekund, a w szczególnych przypadkach co 20 sekund. W związku z tym można zaliczyć je do klasy T4 (180 sekund) czy nawet T6 (20 sekund).

Co to oznacza dla użytkownika? Centra odbiorcze firm zajmujących się monitorowaniem są automatycznie ostrzegane o braku łączności z obiektem. Najczęściej ostrzeżenie (ang. *alert*) jest generowane w przypadku niedotarcia dwóch kolejnych sygnałów testowych. Jeśli nadajnik wysyła sygnały testowe co 12 godzin (nadajniki radiowe oraz powiadomienia GSM), to obsługa centrum monitorowania otrzyma ostrzeżenie dopiero po 25 godzinach. Jeśli natomiast testy łączności są wysyłane są co 90 sekund (nadajniki GPRS), to obsługa otrzyma alert po trzech minutach (!).

W dobie łatwego dostępu do urządzeń zakłócających sygnały radiowe i GSM ważne jest to, czy o braku łączności z Twoim obiektem dowiesz się po 25 godzinach czy po trzech minutach. Przy założeniu, że czas na reakcję załogi interwencyjnej to 10–15 minut, załoga powinna jak najszybciej otrzymać wiadomość o tym, że nie ma łączności z Twoim obiektem.

Rodzaje odbiorników alarmowych

Odbiornik alarmowy jest najważniejszym elementem systemu transmisji alarmu. Dzięki niezawodności i możliwościom

nadajniki alarmowe jednych producentów są popularniejsze od produktów innych producentów. Niestety nawet specjaliści popełniają ten błąd, że przypisują nadajnikom alarmowym cechy, które wynikają z funkcjonalności odbiorników alarmowych. Aby ocenić nadajnik, przede wszystkim trzeba poznać możliwości odbiornika.

Można spotkać trzy rodzaje odbiorników:

– sprzętowe pracujące lokalnie,
– programowe pracujące lokalnie,
– programowe pracujące w chmurze.

Odbiorniki sprzętowe wywodzą się z czasów, gdy dopiero zaczynał się rozwój komputerów, a ich oprogramowanie nie było stabilne. Producenci systemów transmisji alarmu tworzyli wszystkie odbierane sygnały były drukowane na wypadek awarii komputera. Odbiorniki sprzętowe były zawsze wyposażone w źródło zasilania awaryjnego w postaci baterii akumulatorów. Obecnie odbiorniki sprzętowe są tworzone z wykorzystaniem komputerów przemysłowych i mają specjalne zastosowania, np. w wojsku.

Obecnie najczęściej spotyka się odbiorniki programowe, instalowane na lokalnych komputerach lub serwerach. Producenci systemów transmisji alarmu dostarczają oprogramowanie obsługujące ich nadajniki oraz wymieniające dane z oprogramowaniem alarmowego centrum odbiorczego. Odbiorniki programowe są dużo tańsze. Duża część ich funkcji jest obsługiwana przez sprzęt komputerowy oraz wspomagana

Rys. 2. Nowoczesny odbiornik

specjalne urządzenia wyposażone w wyświetlacz i klawiaturę, aby można było wzrokowo sprawdzić poprawność odbieranych danych. Urządzenia te miały port RS232 do komunikacji z komputerem oraz port drukarkowy LPT. Standardowo procedurami systemu operacyjnego. Z tego względu często są dystrybuowane bezpłatnie.

Część producentów zrezygnowała z własnych odbiorników i przekazała protokoły komunikacyjne do integracji

z programami służącymi do obsługi sygnałów alarmowych. Takie rozwiązanie jest korzystne ze względu na skrócenie łańcucha niezawodności (komputer pośredniczący służący do odbioru alarmów jest eliminowany) i sprawdza się przy obsłudze maksymalnie kilku tysięcy nadajników. W przypadku konieczności obsługi kilkudziesięciu tysięcy nadajników istnieje jednak duże ryzyko, że procesy związane z odbiorem sygnałów alarmowych będą obciążały (i w efekcie spowalniały) oprogramowanie służące do obsługi zdarzeń alarmowych. W takich przypadkach należy oddzielić odbiornik alarmów od oprogramowania centrum odbiorczego.

W przyszłości producenci systemów transmisji alarmów będą uruchamiać odbiorniki w chmurze. Wynika to z kierunków rozwoju teleinformatyki (IoT) oraz konieczności budowania redundantnych rozwiązań obsługujących coraz większe ilości sygnałów alarmowych (Big Data). W przypadku odbiorników pracujących w chmurze definiowane będą rodzaje sygnałów (np. techniczne, alarmowe) oraz ich odbiorcy (np. instalatorzy, firmy ochrony), a wymiana informacji będzie odbywała się pomiędzy platformami współpracujących firm.

Główne funkcje odbiorników alarmowych

Podstawowym zadaniem odbiornika alarmów jest przyjęcie sygnału alarmowego otrzymanego z nadajnika i przekazanie go programowi służącemu do obsługi zdarzeń alarmowych. Zadanie nie jest jednak tak proste, jak się wydaje. Po pierwsze odbiornik musi nawiązać i podtrzymywać połączenie z urządzeniami sieciowymi operatora telekomunikacyjnego. W tym celu musi obsługiwać modemy (radiowe, telefoniczne lub GSM) oraz routery umożliwiające wymianę danych sieciowych z centrum SMS-C i APN operatora.

Po zestawieniu łączności z siecią operatora telekomunikacyjnego odbiornik może zająć się komunikacją z nadajnikami. W tym celu identyfikuje urządzenia, rozpoznaje formaty transmisji, dekoduje zaszyfrowane wiadomości oraz potwierdza nadajnikowi otrzymanie wiadomości.

Następnie odbiornik ponownie koduje wiadomości w sposób zrozumiały dla programu służącego do obsługi alarmów, nawiązuje z nim połączenie, przekazuje otrzymane wiadomości i upewnia się, że program je odkodował i potwierdził ich otrzymanie. Jeżeli program jest zajęty lub nie odpowiada, odbiornik przechowuje dane w lokalnej bazie.

Format transmisji wykorzystywany przez nadajnik różni się od formatu wykorzystywanego do komunikacji z programem do obsługi zdarzeń. Producenci urządzeń do transmisji i odbioru alarmów wykorzystują wewnętrzne formaty transmisji pomiędzy swoimi urządzeniami, natomiast do komunikacji z programami do obsługi alarmów wykorzystują międzynarodowe standardy, takie jak Ademco lub Surgard, gdy do komunikacji tej służy łącze RS232. W przypadku komunikacji poprzez sieć komputerową najczęściej stosuje się biblioteki XML.

Odbiornik powinien mieć możliwość zasygnalizowania błędów w procesie oraz skonfigurowania współpracujących urządzeń. Z tego względu każdy odbiornik jest wyposażony w interfejs użytkownika oraz menu konfiguracyjne.

Dodatkowe funkcje odbiorników alarmowych

W ostatnich latach pojawiło się kilka nowych funkcji odbiorników alarmowych, które znacząco wpłynęły na ich niezawodność oraz funkcjonalność. Dzisiejszy odbiornik obsługuje kilka torów transmisji jednocześnie oraz komunikuje się z kilkoma programami do obsługi alarmów równolegle. W przypadku awarii umożliwia przekierowanie ruchu do innych współpracujących odbiorników alarmowych. Poza tym umożliwia zdalne zarządzanie przyłączonymi nadajnikami oraz centralami alarmowymi, automatyczną i grupową, zdalną aktualizację firmware'u współpracujących urządzeń i ma wbudowany konfigurator urządzeń.

Nowoczesny odbiornik jest również serwerem komunikacyjnym. Umożliwia służbom technicznym oraz klientom końcowym dostęp do urządzeń poprzez stronę WWW lub aplikacje mobilne w smartfonach. Klienci końcowi mogą zdalnie sterować bramami garażowymi czy załączać w dozór system alarmowy. Terenowe służby techniczne mogą natomiast zdalnie sprawdzać jakość komunikacji w przypadku konserwacji systemu bez konieczności angażowania operatorów centrum odbiorczego.

Podsumowanie

Odbiorniki alarmowe ewoluowały w ciągu ostatnich 20 lat. Rozdzieliły się role dotyczące monitorowania technicznego (testy, usterki łączności) i monitorowania alarmowego. Odbiorniki musiały przejąć część funkcji dostępnych wcześniej w programach do obsługi alarmów. Działanie programów do monitorowania skoncentrowano na obsłudze zdarzeń alarmowych otrzymywanych z dziesiątek odbiorników (setek tysięcy nadajników). Zmiany te prowadzą w kierunku chmury obliczeniowej.

Niestety nie wszyscy doceniają ważność dobrego odbiornika alarmowego. Niewiele jest odbiorników mogących obsłużyć 20–30 tys. urządzeń i nie zakłócić pracy programu do obsługi alarmów. Utrudnia to zadanie firmom, które chcą zmodernizować swoje systemy transmisji tak, aby były zgodne z normami i pozwalały na uruchamianie konkurencyjnych usług dodatkowych. Mam nadzieję, że po zapoznaniu się z tym materiałem ich oczekiwania wobec nadajników i odbiorników wzrosną.

Daniel Kamiński

Alert Control
ALARMY POD KONTROLĄ

ALERTCONTROL Daniel Kamiński
ul. Przyrodnicza 7E
05-126 Michałów-Grabina
alertcontrol@alertcontrol.pl
tel.: (+48) 784 646 386

DSC

with PowerG Technology

WYKORZYSTAJ DWUKIERUNKOWĄ KOMUNIKACJĘ BEZPRZEWODOWĄ OPARTĄ NA TECHNOLOGII PowerG

NOWA KOMPAKTOWA CENTRALA ALARMOWA WP8010

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Bezpieczeństwo informacji w chmurze (część 3)

dr inż. Marek Blim

Ostatnio w publicystyce często nadużywa się określenia „bezpieczeństwo informacji". Zamiast używać słów wytrychów powinniśmy sprecyzować nasze wymagania dotyczące bezpieczeństwa w cloud computing, odnosząc je do określonych zasobów danych oraz do obsługujących je aplikacji programowych – stosownie do rzeczywistych potrzeb oraz oczekiwań użytkownika

Różnorodność ofert z dziedziny CC na polskim rynku I&CT a problem bezpieczeństwa informacji

Dostęp do funkcji CC jest zależny od użytkownika usługi, jego potrzeb i oczekiwań, a także od zaleceń, wskazówek i możliwości jej oferenta – usługodawcy oferującego własne (czyli rekomendowane jako te najlepsze) rozwiązania CC.

Dla potencjalnego użytkownika chmura obliczeniowa jest alternatywą dla własnego centrum danych, która nie wymaga poniesienia znaczących kosztów inwestycyjnych związanych z wybudowaniem odpowiedniej infrastruktury, gdyż może on korzystać z profesjonalnie przygotowanej infrastruktury i mocy obliczeniowej urządzeń IT usługodawcy (procesorów, pamięci RAM, przestrzeni dyskowej, urządzeń sieciowych, firewalli, przepustowości łącza internetowego itp.), która będzie zwiększana lub zmniejszana w dowolnym momencie, na życzenie i stosownie do potrzeb, a jedynym ograniczeniem będzie wielkość dostępnej puli zasobów usługodawcy.

Zastosowanie przez usługodawcę wirtualizacji sprawia, że pula ta jest dostępna dla każdego użytkownika w zależności od jego chwilowych potrzeb, a opłaty są naliczane tylko i wyłączenia za faktycznie wykorzystaną moc obliczeniową w danym czasie. Użytkownik, za pomocą specjalnie przygotowanego przez usługodawcę interfejsu, jest w stanie w dowolnym momencie i w pełni automatycznie dodawać lub usuwać maszyny wirtualne lub ich zasoby.

Na polskim rynku I&CT działa szereg usługodawców krajowych i międzynarodowych, także spoza strefy Schengen, co czasami stwarza wątpliwości prawne – miejsce technicznego wykonywania usługi (serwery w Polsce, Francji, Irlandii, USA czy Indiach) wpływa bowiem istotnie na sposób egzekwowania uprawnień polskiego usługobiorcy w przypadku niedotrzymania lub naruszenia zobowiązań przez usługodawcę (właściciela CC).

CC z lokalizacją techniczną sprzętu na terenie EEA/SIS (europejskie centra komputerowe)

W pierwszej kolejności należy wskazać polskie firmy z lokalizacją zasobów CC w Polsce. Należą do nich:

1) Najstarsza na polskim rynku Atende S.A. – grupa kapitałowa od 2012 r. notowana na GPW, dawniej ATM Systemy Informatyczne (w ofercie: usługi kolokacji sprzętowej w serwerowniach ATM od 2006 r.). Firma Atende Software opracowała autorską platformę redCDN, obecnie po modernizacji redGalaxy CDN (od ang. *content delivery network*), która jest powszechnym rozwiązaniem CC tego typu w Polsce. obecnie korzystają z niej m.in. TVN, Cyfrowy Polsat oraz ITI Neovision.
2) Oktawave – konsorcjum K2 (CC w Polsce czterech subregionach, a w przyszłości w pięciu). Jest to jedyna polska firma posiadająca certyfikat bezpieczeństwa informacji w chmurze CSA STAR Certification i spełniająca wymogi bezpieczeństwa dotyczące przetwarzania danych osobowych.
3) e24cloud.com – serwis CC poznańskiej firmy Beyond.pl bazujący na dwóch współpracujących lokalizacjach (z powodu negatywnych doświadczeń z 2012 r. i w efekcie podjętych działań doskonaląco-innowacyjnych).

Inną polską firmą, której elementy techniczne, czyli fizyczne zasoby sprzętowe prawdopodobnie znajdują się w Europie, jest Cloud IQ PL współpracująca z Microsoft Azure. Według oficjalnych zapewnień polskie zasoby nie opuszczają granic EOG/EEA i są przetwarzane w dwóch dużych centrach danych Microsoftu – w Dublinie i w Amsterdamie.

Na polskim rynku CC funkcjonują też zewnętrzni co do siedziby (spoza granic EOG/EEA) usługodawcy z zasobami w Europie oferujący swoje specjalizowane usługi w chmurze:

1) Firma Adobe Systems Software Ireland oferująca usługi CC w zakresie pracy twórczej i innych zastosowań – Adobe Creative Cloud. W ofercie dostępne są standardy branżowe oraz najnowsze wersje programów Photoshop CC i Lightroom (na komputery i urządzenia przenośne). Bezpieczeństwo usług tej firmy jest jednak dyskusyjne.
2) Ogólnoświatowa firma Rackspace oferująca CC Uptime Network. W Europie firma ma zasoby techniczne w Wielkiej Brytanii (w Londynie i Slough). Ponadto posiada centra w Chicago, Dallas, Wirginii Północnej, Hongkongu i Sydney. Bezpieczeństwo informacji zapewnia zespół wysoko wykwalifikowanych inżynierów wspieranych przez własne Cyber Security Operations Center (CSOC) funkcjonujące całodobowo, całotygodniowo i całorocznie, certyfikowane przez BSI.
3) CC-Mega Corp. (USA) oferuje darmową przestrzeń 50 GB bazując na usłudze rdzeniowej. Usługa ta jest polecana przez spiderweb.pl. Ponoć dane są przechowywane gdzieś w Europie (we współpracy ze SpiderOak). Nie ma pewności, czy są bezpieczne (zaleca się szyfrowanie danych programami Viva lub Boxcrypter).
4) Dropbox Business amerykańskiej spółki Dropbox, która działa także na rynku europejskim. Jej usługa bazuje na Amazon Simple Storage Service (Amazon S3). Dropbox Business jest objęty certyfikatem w ramach programu Tarcza Prywatności UE-USA (*Private Shield EU-USA*), ale przechowywanie danych w Europie (Data Center Dublin) jest dostępne dla klientów posiadających ponad 250 stanowisk.

Usługi CC, w przypadku których zasoby techniczne są fizycznie zlokalizowane poza Europą (na fermach komputerowych w USA i Indiach)

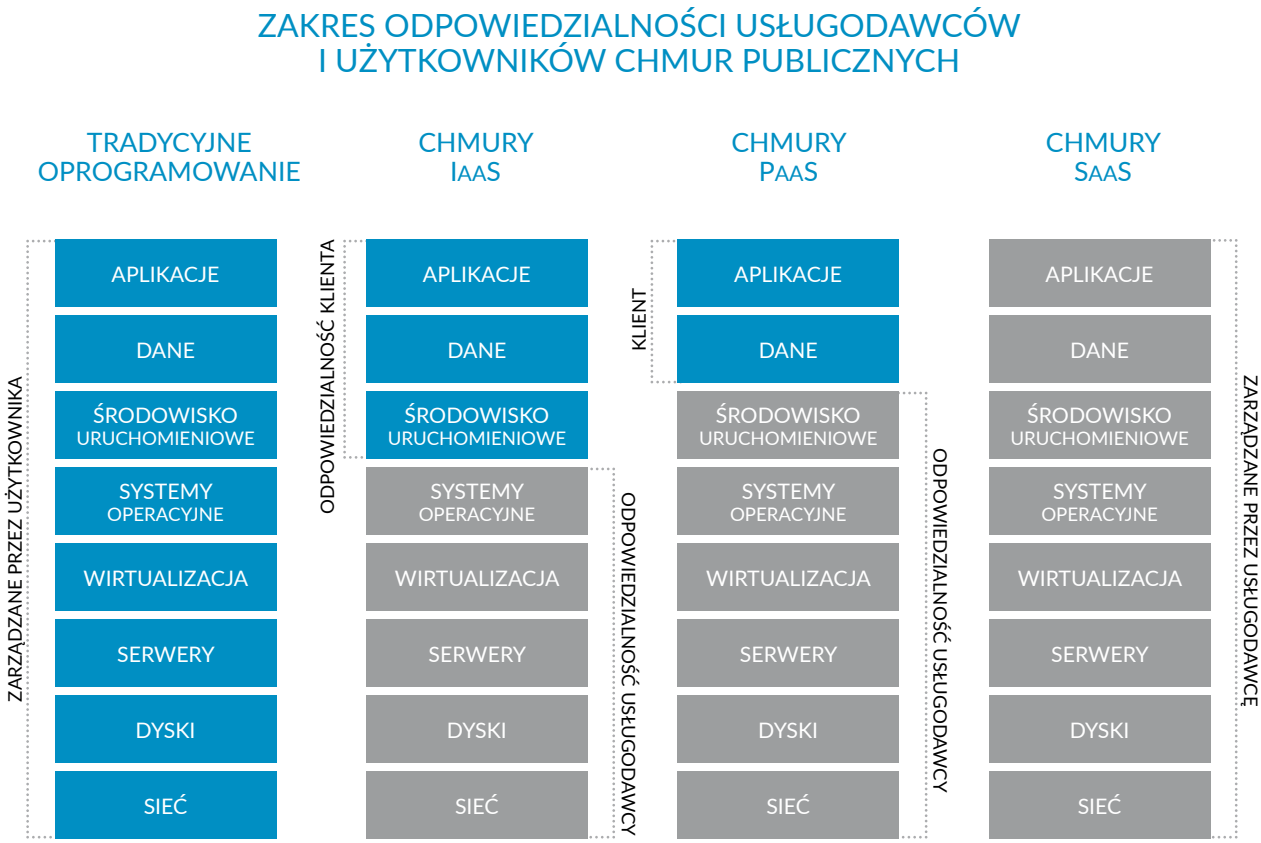
Możemy wskazać działające w Polsce firmy – przedstawicielstwa usługodawców z zasobami CC zlokalizowanymi poza Europą – oferujące usługi indywidualne i firmowe w Polsce. Do usług tych należą:

1) Amazon Cloud Drive (Unlimited Photos i Unlimited Everything) dla użytkowników prywatnych, firm i instytucji publicznych. W jej zakres wchodzą:
   – Amazon Web Services (zakres IaaS),
   – Amazon EC2 (zakres IaaS i elementy PaaS),
   – Amazon DaaS (centrum danych jako usługa – lokacja z organizacją),
   – Amazon (wirtualna chmura prywatna – chmura przypisana do firmy/organizacji).
2) Microsoft Azure (zakres IaaS).
3) Microsoft Azure Function (zakres SaaS).
4) Microsoft Onlive Desktop (usługa PaaS/SaaS zapewniająca użytkownikom tabletów dostęp do zdalnego pulpitu

systemu Windows wraz z pakietem Office).
5) Windows Azure API (zakres PaaS).
6) Google App Engine (zakres PaaS).
7) Force.Com (zakres PaaS).
8) Ruby on Rails (zakres PaaS).
9) Salesforce.com (zakres SaaS).
10) Apple Cloud – chmura dla użytkowników systemów Apple (komputer, iPhone, iPad). Dostępny jest bezpłatny wirtualny dysk iCloud Drive (do 5 GB).

W przypadku największych usługodawców oferujących usługi w chmurze, takich jak Google, Microsoft i Amazon, zasoby chmury pochodzą z centrów danych rozmieszczonych

Opis dobrych praktyk dotyczących SZBI/ISMS jest zawarty w rodzinie norm ISO 27k, a w szczególności w normach (i ich polskich edycjach):
– ISO/IEC 27001:2013 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania;
– ISO/IEC 27002:2013 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji;
– ISO/IEC 27005:2011 – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.



Rys. 1. Wskazanie, kto i za co odpowiada w chmurze publicznej (na podstawie PE 474.104 – Chmury obliczeniowe. Ekspertyza, http://www.europarl.europa.eu/committees/en/supporting-analyses-search.html)

na całym świecie. Gdzie dokładnie? Tego typu informacje ze względów bezpieczeństwa nigdy nie są podawane w pełni, ale ze względu na dostępność usług zasadna jest rozległa (kontynentalnie – Ameryka Płn. i Płd., Australia, Europa, Indie) dyslokacja poszczególnych centrów danych/ferm komputerowych usługodawców.

Audyt bezpieczeństwa informacji w chmurze

Bezpieczeństwo informacji nie jest trwałe. Jest to proces podlegający zróżnicowanym oddziaływaniom wewnętrznym (operacyjnym) i zewnętrznym (biznesowym) występującym zarówno w samej organizacji/firmie/instytucji/korporacji, jak i w jej bliższym oraz dalszym otoczeniu systemowym.

Organizację bezpieczeństwa informacji opisuje zestaw zasad, reguł, procedur i instrukcji postępowania nazywany ogólnie systemem zarządzania bezpieczeństwem informacji (SZBI/ISMS – Information Security Management System).

Aby SZBI/ISMS był zrealizowany zgodnie z ww. normami, wymaga on objęcia pełną kontrolą zarządczą całości posiadanych zasobów informacji, jak również środków ich przetwarzania (ze szczególnym zwróceniem uwagi na utylizację danych oraz sprzętu przetwarzającego), o co w przypadku korzystania z usług w chmurze bywa czasem bardzo trudno (rys. 1), chyba że chmura jest prywatna.

SZBI wg normy ISO 27001 – zalety i ułomności oceny

Mimo iż zalety stosowania SZBI/ISMS w zlokalizowanym systemie (firmowe centrum danych/prywatna chmura użytkownika) są oczywiste, posiadanie przez oferującego CC usługodawcę certyfikatu ISO/IEC 27001 nie stanowi dla usługobiorcy pełnej gwarancji bezpieczeństwa przetwarzanych danych (dotyczy to szczególnie danych chronionych, np. wrażliwych danych osobowych przetwarzanych przez ich gestora, gdyż nie

ma możliwości zawarcia z procesorem wymaganej ustawowo umowy dotyczącej powierzenia danych osobowych). Odrębnymi problemami są tutaj:

– kwestia lokalizacji bazy sprzętowej oraz sposobów jej zabezpieczenia fizycznego i technicznego;
– zakres oferowanych usług i dostępność dostawców/usługodawców właściciela chmury (dla potrzeb wykonania przez użytkownika audytu II strony u oferenta CC ;
– zakres i możliwość prawnej egzekucji zobowiązań podstawowych oraz zależnych wynikające z różnic systemów prawnych, którym podlegają klient i dostawca usługi (prawo stanowione nie równa się prawu zwyczajowemu – wbrew oczekiwaniom szeregu użytkowników CC).

SZBI z nakładką CSA STAR – model doskonałości systemu wg CCM CSA

Rozwiązaniami szczególnymi dot. bezpieczeństwa informacji w chmurze obliczeniowej zajmuje się od grudnia 2008 roku Cloud Security Alliance (CSA). Organizacja CSA została założona przez grupę osób zajmujących się I&CT, którzy widzieli potrzebę dostarczenia użytkownikowi chmury obliczeniowej narzędzi umożliwiających sprawne kierowanie bezpieczeństwem chmury, jako stowarzyszenie non profit, otwarte na udział wolontariuszy – specjalistów i użytkowników w zakresie rozwijających się usług CC. Pierwszym efektem działania CSA było upublicznione w połowie 2009 roku opracowanie systemowe „Kierowanie Bezpieczeństwem dla Krytycznych Obszarów w Informatyce Chmury Obliczeniowej". Inicjatywy i prace CSA na rzecz unormowania praktyk związanych z ochroną informacji w chmurze poparło szereg instytucji oraz organizacji będących globalnymi decydentami w dziedzinie bezpieczeństwa: National Institute of Standards and Technology w USA, Komisja UE, rząd Singapuru i liczne krajowe władze odpowiedzialne za ochronę danych (BSI RFN, BSIG UK, BSP AS/NZ).

Sposób oceny funkcjonowania CC oparto na analizie pięciu głównych czynników wpływających na wydajność usługi, którymi w każdym analizowanym przypadku są:

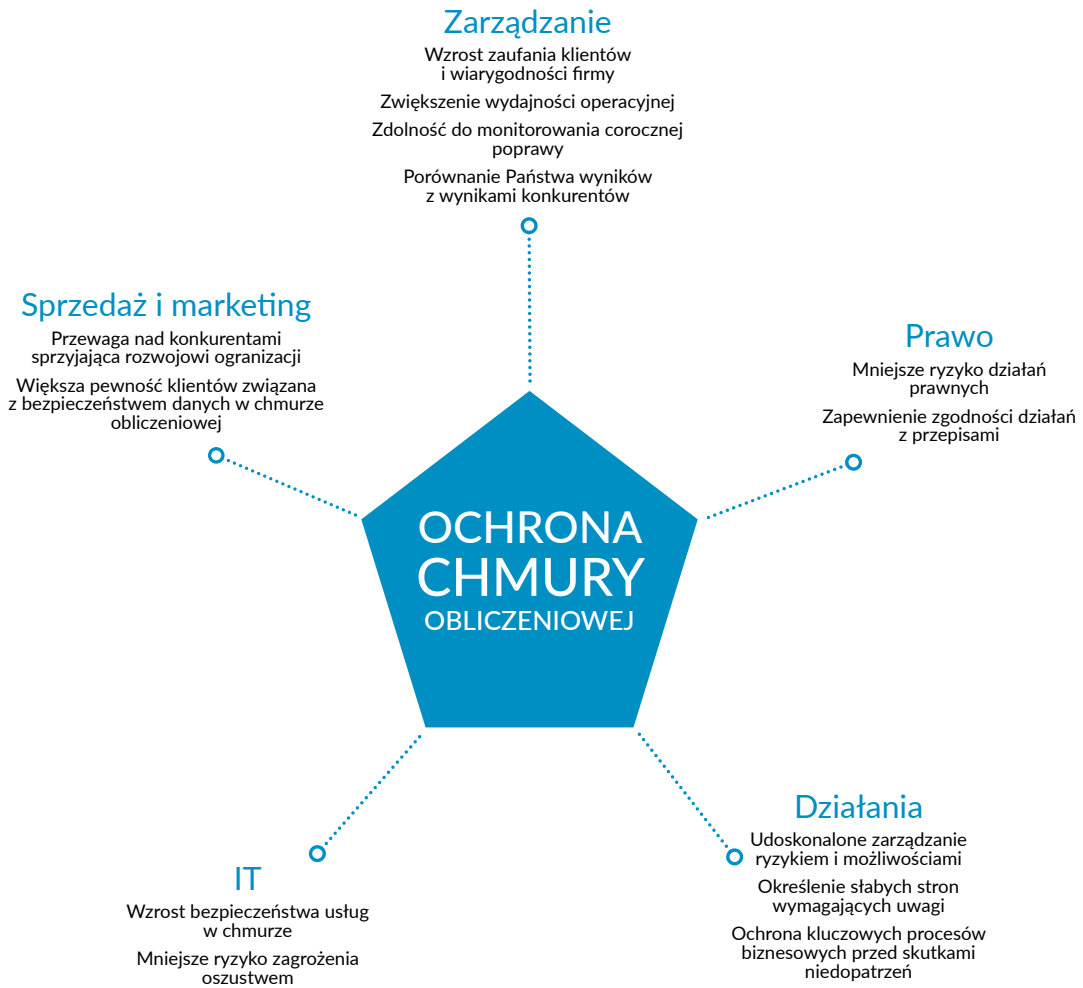
– komunikacja i zaangażowanie interesariuszy,
– polityki, plany i procedury oraz podejście systemowe,
– umiejętności i wiedza fachowa,
– własność, przywództwo i zarządzanie,
– monitorowanie i dokonywanie pomiarów.

Usługa CC jest sprawdzana z uwzględnieniem następujących kryteriów:

1) Zgodność (*compliance*). Planowany jest audyt wewnętrzny (SZBI) oraz niezależne audyty przeprowadzane przez strony trzecie. Sprawdzane są regulacje związane z zachowaniem własności intelektualnej.
2) Zarządzanie danymi (*data governance*). Sprawdzenie dotyczy ogólnego zarządzania dostępnością, użytecznością, rzetelnością procesów i bezpieczeństwem danych w firmie oferującej CC.
3) Ochrona obiektu (*facility security*). Sprawdzane są polityki i procedury dotyczące bezpieczeństwa w obiekcie (wymagane jest bezpieczne środowisko pracy w firmie oferującej CC).
4) Zasoby ludzkie (*human resources*). Sprawdza się, czy pracownicy mający kontakt z danymi wykonują swoje obowiązki w taki sposób, by ograniczyć ryzyko kradzieży, oszustwa lub nadużyć w firmie oferującej CC.
5) Bezpieczeństwo informacji (*information security*). Sprawdzenie ma na celu m.in. zapewnienie opracowania, udokumentowania, zatwierdzenia i wdrożenia systemu zarządzania bezpieczeństwem informacji SZBI/ISMS (deklaracja stosowania – Statement of Applicability) obejmującego zabezpieczenia administracyjne, techniczne i fizyczne.
6) Zgodność z prawem (*legal*). Sprawdzane jest przestrzeganie przepisów, obowiązków ustawowych, regulacyjnych lub kontraktowych i wymogów dotyczących bezpieczeństwa.
7) Zarządzanie operacjami (*operations managment*). Sprawdza się, czy zapewniono poprawne i bezpieczne funkcjonowanie obiektów służących przetwarzaniu informacji u dostawców usług.
8) Zarządzanie ryzykiem (*risk management*). Sprawdza się, czy dostawcy usług opracowali i utrzymują ramy zarządzania ryzykiem w przedsiębiorstwie służące zarządzaniu ryzykiem na dopuszczalnym poziomie.
9) Zarządzanie publikacjami (*release management*). Sprawdza się, czy zapewniono należytą kontrolę zarządzania i autoryzowania w ramach opracowywania lub pozyskiwania nowych aplikacji, systemów, baz danych, infrastruktury, usług, operacji i obiektów.
10) Odporność (*resilience*). Sprawdza się, czy zapewniono systemy zapobiegające zakłóceniom działań biznesowych i czy kluczowe procesy biznesowe są należycie chronione przed skutkami poważnych niedopatrzeń.
11) Struktura bezpieczeństwa (*security architecture*). Sprawdza się, czy w firmie oferującej usługi CC jest odpowiednia kontrola dostępu i system zarządzania bezpieczeństwem informacji – SZBI/ISMS (wymagany zgodnie z normą ISO/IEC 27001). Zastosowanie Cloud Controls Matrix opracowanej przez CSA i uzyskanie certyfikatu bezpieczeństwa informacji w chmurze CSA STAR są dodatkowymi atutami.

Na bazie dwuletnich badań, analiz i udostępnionych informacji środowiskowych stowarzyszenie CSA opracowało koncepcję użytkową macierzy sprawdzającej zależności – Cloud Controls Matrix (CCM) oraz model dojrzałości jako elementy służące do dokonywania oceny stosowania się do wymagań zawartych w CCM, co w połączeniu z wymaganiami normy ISO 27001 pozwala dostosowywać działania w chmurze do wymagań dotyczących SZBI/ISMS.

STAR (Security, Trust & Assurance Registry) jest bezpłatnym, publicznie dostępnym rejestrem, który dokumentuje kontrole zabezpieczeń dla usług udostępnianych w chmurze obliczeniowej. Firma STAR została powołana i uruchomiona w sierpniu 2011 roku przez CSA w celu prowadzenia (publikacji i autoryzacji) rejestru umożliwiającego zachowanie większej przejrzystości działań dostawców usług w chmurze. Klienci korzystający z CC mogą skorzystać z usługi STAR, by zbadać praktyki mające związek z bezpieczeństwem danych u dostawców usług w chmurze. Ci ostatni mogą składać raport udowadniający zgodność ich zabezpieczeń z matrycą kontrolną



Rys. 2. Ocena działań w CC na podstawie rejestru CSA STAR (źródło : https://www.bsigroup.com/pl-PL/Certyfikacja-CSA-STAR/CSA-STAR-Certification-Korzysci/)

Cloud Controls Matrix, która stanowi ramy kontroli. Alternatywnie dostawcy mogą zdecydować się na wypełnienie i przedłożenie opracowanego przez CSA kwestionariusza CAIQ (Consensus Assessments Initiative Questionnaire) zawierającego 140 pytań, tzn. udzielenie odpowiedzi na zawarte w nim pytania dotyczące usługi. Odpowiedzi te będą stanowić źródło informacji dla usługobiorców.

Nakładka CSA STAR Certification na SZBI/ISMS w chmurze jest aktualnie jedyną formą pełnej weryfikacji bezpieczeństwa informacji przetwarzanych w ramach usługi CC.

Przewidywania eksperckie dotyczące zmian na polskim rynku I&CT w 2017 roku

Jak wynika ze wstępnych szacunków firmy IDC, w 2016 r. polski rynek chmury publicznej wzrósł o ponad 25% w porównaniu z rokiem 2015. Firma prognozuje, że – o ile nie nastąpi nic niespodziewanego – w 2017 roku wartość chmury publicznej w Polsce powinna przekroczyć 200 milionów USD. – *Szacujemy, że do 2019 r. polski rynek chmury publicznej będzie rósł średnio pięć razy szybciej niż rynek tradycyjnych usług IT, co oznacza, że nie odstajemy pod względem inwestycji w cloud computing od światowej średniej. Średnie tempo inwestycji w chmurę publiczną – do 2019 r., globalnie wyniesie 21,5%, gdy tymczasem w Polsce sięgnie ono 18,6%* – zwraca uwagę Ewa Zborowska z IDC.

Podsumowanie

Oferta firmy Oktawave na rynku polskim i jej poziom bezpieczeństwa potwierdzony posiadanymi certyfikatami ISO 27001 oraz CSA STAR Certification może służyć jako przykład dalszego rozwoju polskich usług w chmurze. Oktawave oferuje następujące usługi w chmurze:

1) Oktawave Cloud Instances (OCI). Jest to usługa, która pozwala łatwo wykorzystać zasoby chmury obliczeniowej (wirtualnych serwerów nazywanych instancjami) do stworzenia i rozwoju skalowalnych serwisów i aplikacji internetowych, systemów przypisanych czy gier online. Dzięki rozliczaniu jedynie za wykorzystane zasoby ograniczone są koszty związane z IT i jednocześnie zachowana zostaje zdolność do szybkiego dostosowania infrastruktury do zmieniających się potrzeb klientów i rynku.
2) Oktawave Volume Storage (OVS). Usługa ta umożliwia trwały zapis danych dla instancji, dzięki czemu można

zarządzać wolumenami dyskowymi bez względu na to, które instancje z nich korzystają, a także przypisać jeden wolumen wielu instancjom jednocześnie, budując np. klastry SQL czy rozwiązania High Performance Computing (HPC). OVS jest standardowym urządzeniem blokowym pracującym w jednym z trzech standardów, które gwarantują następujące parametry:
– Tier-1: do 1000 IOPS oraz do 300 MB/s ciągłego transferu,
– Tier-2: do 20 000 IOPS oraz do 2 GB/s ciągłego transferu,
– Tier-3: do 50 000 IOPS oraz 3 GB/s ciągłego transferu,
– Tier-4: do 100 000 IOPS oraz 3 GB/s ciągłego transferu,
– Tier-5: do 200 000 IOPS oraz 3 GB/s ciągłego transferu.

Każdy wolumen OVS może w dowolnym momencie zostać poddany migracji do innej klasy. Kopie migawkowe (tzw. snapshot) są wykonywane w kontekście instancji, do której wolumen został przypisany.

3) Oktawave Cloud Storage (OCS). Jest to wysoko wydajny, niezawodny i bezpieczny sposób wymiany plików pomiędzy różnymi systemami i aplikacjami w Internecie. Ułatwia tworzenie skalowalnych środowisk bez względu na wykorzystywane technologie. Interfejs sieciowy umożliwia dostęp do statystyk stworzonych wolumenów dyskowo-sieciowych i dokonywanie na nich zmian. Udostępnione są również zaawansowane API klasy REST dzięki którym możliwa jest integracja różnych platform.
4) Oktawave Relational Databases (ORDB). Jest to sieciowa usługa służąca do uruchamiania i zarządzania systemami relacyjnych baz danych w chmurze obliczeniowej. Zapewnia elastyczny model utrzymania baz danych w zakresie ich wydajności, zwalniając użytkownika z konieczności dbania o kopie zapasowe, migracje danych czy optymalizację. ORDB umożliwia uruchomienie popularnych baz MySQL oraz PostgreSQL, oferując pełen zakres funkcji relacyjnych baz danych i zapewniając bezpieczeństwo oraz łatwość w zarządzaniu – wszystkie operacje na bazach oraz zmiany dotyczące obsługujących je instancji można wykonywać zarówno poprzez sieciowy interfejs użytkownika, jak i w pełni transakcyjne API Oktawave (XML SOAP).

Mamy więc dobre i polskie. Warto z tego korzystać i jest na czym się wzorować. Warto też sprawdzać:
– kto jest właścicielem, a kto obsługującym oferowaną chmurę;
– jak dana chmura reaguje na test obciążenia wykonany za pomocą aplikacji LoadStorm;
– jaką opinię na temat funkcjonowania danej chmury i jej obciążenia ma CloudHarmony;
– gdzie fizycznie lokowane są centra danych/fermy komputerowe obsługujące oferowane usługi CC (w Polsce, na terenie UE, gdzie indziej);
– jaka jest pewność, że po zaprzestaniu korzystania z usługi w danej chmurze wszelkie wcześniej powierzone dane zostaną definitywnie zutylizowane.

Opracował dr inż. Marek Blim

Bibliografia

1) Bezpieczeństwo biznesu w XXI wieku, praca zbiorowa, wyd. SASMA EUROPE, Warszawa 2014.
2) Handzel Z., Cloud computing – czyli chmura obliczeniowa i możliwości jej wykorzystania w mediach, „Problemy Zarządzania" vol. 11, nr 4 (44), wyd. UW, Warszawa 2013.
3) Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, wyd. Difin, Warszawa 2004.
4) Kępa L., Tomasik P., Dobrzyński S., *Bezpieczeństwo systemu e-commerce*, wyd. Helion, Gliwice 2012.
5) Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*, wyd. Helion, Gliwice 2011.
6) Michalak A., *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, wyd. Kantor Wydawniczy ZAKAMYCZE, Kraków 2006.
7) Siwicki M., *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy komunikacyjnej w chmurach obliczeniowych*, „Prokuratura i Prawo" nr 5/2015, s. 109–127.
8) Spraul V. A., *Jak działa oprogramowanie*, wyd. Helion, Gliwice 2016.

Netografia

1) http://it-manager.pl/chmura-obliczeniowa-w-polskim-e-biznesie-raport-e24cloud/ (stan z 14.05.2017).
2) www.3s.pl/pl/17,serwery-i-cloud.html (stan z 14.05.2017).
3) www.computerworld.pl/news/Dlaczego-chmura-sie-w-Polsce-nie-udaje,405741.html (stan z 14.05.2017).
4) www.cyberdefence24.pl/526022,jak-chronic-infrastrukture-krytyczna-nowe-rekomendacje-nist (stan z 14.05.2017).
5) www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf (stan z 14.05.2017).
6) www.giodo.gov.pl/259/id_art/6271/j/pl (stan z 14.05.2017).
7) www.hbrp.pl/a/chmura-obliczeniowa-bilans-korzysci-i-zagrozen/36ypu9gW (stan z 14.05.2017).
8) www.piit.org.pl/documents/10181/268830/Definicja_rodzaje_chmur_obliczeniowych_oraz_poziomy_uslug_-_Dorota_Grudzien-Molenda_HP.pdf (stan z 14.05.2017).
9) www.spidersweb.pl/2013/11/tencent-10-tb-za-darmo.html (stan z 14.05.2017).
10) www.spidersweb.pl/2015/11/jaka-chmure-wybrac-dysk-google-mega.html (stan z 14.05.2017).

KDH-CDZ900 - Czytnik kart dalekiego zasięgu

Czytnik dalekiego zasięgu **KDH-CDZ900** przeznaczony jest do pracy w systemach kontroli dostępu. Można go instalować wewnątrz i na zewnątrz pomieszczeń. Najczęściej umieszczany jest na wjazdach/wyjazdach z parkingów, garaży i posesji prywatnych oraz wszędzie tam, gdzie potrzebny jest duży zasięg odczytu identyfikatorów. Zasięg ten zależy od rodzaju karty UHF oraz ustawień i wynosi od 1 do 8 m. Czytnik może współpracować z kontrolerami z interfejsem Wiegand. Odczytuje różne rodzaje identyfikatorów w formie kart plastikowych, breloków, naklejek, kart dualnych oraz innych z chipem Alien Higgs 3. Również specjalne identyfikatory przeznaczone do montażu na powierzchniach metalowych. Ma obudowę z tworzywa ABS w kolorze IVORY. Pracuje w paśmie 860 MHz.

Model	KDH-CDZ900
Rodzaj karty	UHF
Klawiatura	nie
Częstotliwość pracy	860 MHz
Zasięg odczytu	od 1 do 8 m (domyślnie 5 m)
Porty do połączenia z kontrolerem	Interfejs Wiegand: 26/34 bit
Pobór prądu	350 mA
Zasilanie	12 V_{DC}
Temperatura pracy	-20°C do 80°C
Wilgotność względna	20% – 95%
Środowisko montażu	do instalacji wewnątrz i na zewnątrz pomieszczeń (przy pomocy wspornika dołączonego do zestawu)
Wymiary (mm)	227 x 227 x 60

Producent:

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. +48 22 546 05 46
e-mail: kontakt@aat.pl
www.aat.pl

8-dyskowy rejestrator IP marki NOVUS - NVR-6332-H8

Rejestrator 32-kanałowy do rejestracji strumieni wizyjnych z kamer o rozdzielczości do 8 Mpx (3840 x 2160) i kompresji metodą H.264, H.264+ oraz H.265. W urządzeniu można zamontować do 8 dysków twardych o pojemności 6 TB każdy. Rejestrator we współpracy z kamerami serii 3000 obsługuje funkcje inteligentnej analizy obrazu. Urządzenie ma wyjścia monitorowe główne (HDMI lub VGA) oraz pomocnicze (HDMI).

Nazwa parametru lub funkcji	Wartość parametru lub opis funkcji
Wideo	
Kamery IP	do 32 kanałów w rozdzielczości 3840 x 2160 (obraz i dźwięk)
Obsługiwana rozdzielczość	maks. 3840 x 2160
Kompresja	H.264, H.264+, H.265
Wyjścia monitorowe	główne (podział, pełny ekran, sekwencja): 1 x VGA, 1 x HDMI (4K UltraHD)
Nagrywanie	
Prędkość nagrywania	960 kl./s (32 x 30 kl./s dla 3840 x 2160)
Odtwarzanie	
Prędkość odtwarzania	480 kl./s (16 x 30 kl./s dla 3840 x 2160) **
Dyski	
Wewnętrzne do rejestracji	możliwość montażu: 8 x HDD 3.5” 6 TB SATA *
Maksymalna łączna pojemność	48 TB
Alarmy	
Wejścia/wyjścia alarmowe lokalne	8/4 typu przekaźnik
Wejścia/wyjścia alarmowe w kamerach	obsługa wejść/wyjść dostępnych w kamerach*
Detekcja ruchu	obsługa detekcji ruchu dostępnej w kamerach*
Reakcja na zdarzenia alarmowe	sygnał dźwiękowy, e-mail, aktywacja wyjścia alarmowego, aktywacja nagrywania, zmiana ustawienia PTZ
Inteligentna analiza obrazu	
Obsługiwane funkcje	wykrywanie obiektów, sabotaż, zmiana sceny, utrata ostrości, zmiana kolorystyki, przekroczenie linii, naruszenie strefy
Sieć	
Interfejs sieciowy	2 x Ethernet - złącze RJ-45, 10/100/1000 Mb/s
Zgodność z ONVIF	Profile S (ONVIF 2.2 lub wyższy)
Programy na PC/MAC	Internet Explorer, NVR-6000 Viewer/Safari
Programy na Smartphone	SuperLive Plus (iPhone, Android)
Maks. liczba połączeń z rejestratorem	4

* Funkcja uzależniona od protokołu komunikacji (szczegółowe dane znajdują się w tabeli kompatybilności dostępnej w zakładce PLIKI DO POBRANIA na stronie produktu na www.aat.pl)

** Przy wykorzystaniu dwustrumieniowości

Producent:

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. +48 22 546 05 46
e-mail: kontakt@aat.pl
www.aat.pl

MCT62E
Terminal dostępu do systemu RACS 5

MCT62E jest terminalem dostępu przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej **RACS 5**. Terminal umożliwia identyfikację użytkowników za pośrednictwem kart zbliżeniowych standardu EM 125 kHz. MCT62E jest wyposażony w interfejs komunikacyjny RS485, za pośrednictwem którego jest podłączony do kontrolera dostępu. Urządzenie może być instalowane na zewnątrz budynków bez konieczności stosowania dodatkowych zabezpieczeń. Terminal jest zgodny z linią wzorniczą RADIUS.

Charakterystyka

- Terminal dostępu do systemu RACS 5
- Czytnik kart EM 125 kHz
- 3 LED-y sygnalizacyjne
- Buzzer
- RS485
- Tamper
- Praca na zewnątrz
- Wymiary: 100 x 40 x 25 mm
- Linia wzornicza RADIUS
- CE

Producent: roger®

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

MCT88M-IO
Terminal dostępu do systemu RACS 5

MCT88M-IO jest terminalem dostępu przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej **RACS 5**. Terminal ma kolorowy wyświetlacz matrycowy, klawiaturę dotykową z 4 przyciskami funkcyjnymi oraz czytnik MIFARE Ultralight/Classic/DESFire/Plus/NFC/Bluetooth. MCT88M-IO może być podłączony do kontrolera dostępu za pośrednictwem magistrali RS485 lub sieci Ethernet (LAN). Czytnik zwykle jest wykorzystany jako punkt kontroli dostępu oraz terminal do sterowania systemem. Dodatkowo, ze względu na dostępność wyświetlacza i programowanych przycisków funkcyjnych, może on być wykorzystany jako terminal rejestracji czasu pracy. Wbudowane linie wej./wyj. mogą być użyte do obsługi przejścia, realizacji automatyki budynkowej lub innych, dostępnych w systemie funkcji. Logowanie użytkowników na terminalu może odbywać się za pomocą kart zbliżeniowych, kodów PIN lub z poziomu urządzeń mobilnych wyposażonych w technologię NFC lub Bluetooth. Terminal MCT88M-IO jest zgodny z linią wzorniczą QUADRUS.

Charakterystyka

- Terminal dostępu do systemu RACS 5
- Kolorowy wyświetlacz matrycowy
- Czytnik MIFARE Ultralight/Classic/DESFire/Plus
- Identyfikacja mobilna NFC
- Identyfikacja mobilna Bluetooth
- Klawiatura dotykowa
- 4 klawisze funkcyjne
- 3 wejścia parametryczne
- 2 wyjścia tranzystorowe
- 1 wyjście przekaźnikowe
- RS485
- Ethernet (LAN)
- Wymiary: 155,5 x 85,0 x 21,5 mm
- Linia wzornicza QUADRUS
- CE

Producent: roger®

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

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

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46; faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

D PROD S

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. Antoniuk Fabryczny 22, 15-741 **Białystok**
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@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, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 **Kraków**
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

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

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

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

Al. Niepodległości 606/610, 81-855 **Sopot**
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

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

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

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

D PROD PROJ

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

D PROD PROJ S

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

D PROD PROJ S

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

I PROD PROJ

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
www.assaabloy.com.pl

D I PROJ S

FIRMA ATLINE SPÓŁKA JAWNA SŁAWOMIR PRUSKI
ul. Franciszkańska 125
91-845 Łódź
tel. 42 236 30 19; faks 42 655 20 99
e-mail: biuro@atline.pl
www.atline.pl

D I PROD PROJ

BOSCH SECURITY SYSTEMS
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 40 00
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

D S

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

D I PROJ

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

I PROD PROJ S

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

D PROD PROJ S

CMA Monitoring Group Sp. z o.o.
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. Składowa 2, 41-902 Bytom
tel. 32 388 09 50; faks 32 388 09 60

ul. Zatorska 36, 51-215 **Wrocław**
tel. kom. 697 972 558
faks 71 341 16 26

Biura handlowe:
ul. Nowy rynek 2, 62-002 **Suchy Las k/Poznania**
tel. kom. 601 203 664, 601 410 979
faks 61 861 40 51

ul. Hallera 140, lok. 124, 80-416 **Gdańsk**
tel kom. 693 694 339

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17/18; faks 22 855 00 19
e-mail: cs@cs.pl
www.cs.pl

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2, Lisbon Building, Lobby II
02-823 Warszawa
tel. 22 395 74 00; faks 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

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

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

PHU ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel. kom. 606 270 756
tel. 22 398 96 53
e-mail: elproma@elproma.pl
www.elproma.pl

ELSTECH
os. Złota Podkowa 6/4
31-352 Kraków
tel. kom. 570 400 537, 570 400 538; faks 12 350 45 03
e-mail: info@elstech.pl
www.elstech.pl

Eltrox.pl
ul. Główna 23
42-280 Częstochowa
tel. 34 341 14 61
tel. kom. 517 015 471
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Hynka 6/2, 80-465 **Gdańsk**
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. 6 sierpnia 14, 90-416 **Łódź**
tel. 42 632 31 24
e-mail: lodz@eltrox.pl

ul. Brynowska 65/4, 40-584 **Katowice**
tel. 32 203 50 73
e-mail: katowice@eltrox.pl

ul. Wybickiego 42A, 31-302 **Kraków**
tel. kom. 501 945 239
e-mail: krakow@eltrox.pl

ul. Dmowskiego 2/1, 45-365 **Opole**
tel. kom. 501 945 246
e-mail: opole@eltrox.pl

ul. Stablewskiego 31/3, 60-223 **Poznań**
tel. kom. 504 904 710
e-mail: poznan@eltrox.pl

ul. Wyszyńskiego 26, 70-203 **Szczecin**
tel. 91 434 78 72
e-mail: szczecin@eltrox.pl

ul. Remiszewska 1/7B, 03-550 **Warszawa**
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Łopuszańska 22, 02-220 **Warszawa**
tel. kom. 506 601 006
e-mail: warszawa2@eltrox.pl

ul. Komandorska 53R, 50-258 **Wrocław**
tel. kom. 503 127 533
e-mail: wroclaw@eltrox.pl

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
ul. Wilcza 54a lok. 1
00-679 Warszawa
tel. 22 629 53 49
e-mail: kontakt@estpolska.pl
http://europeansecuritytrading.com/pl

EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

D PROD PROJ S

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

D I PROJ S

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

D PROJ S

HANWHA TECHWIN
Diamond Business Park
ul. Posag 7 Panien 1
02-495 Warszawa
e-mail: hte.poland@hanwha.com
www.hanwha-security.eu

D S

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

D PROJ S

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

I PROJ

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

D PROJ S

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

C D S

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59; faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

D I PROJ

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
02-672 Warszawa
tel. 22 549 23 30
e-mail: info@legrand.com.pl
www.legrand.pl

D PROD PROJ S

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

PROD

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

D

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

PROD

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

D PROJ S

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

D I PROD PROJ S

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

D

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

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

D PROD S

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

PROD PROJ S

Oddziały:
ul. M. Gomółki 2, 80-279 **Gdańsk**
tel. 58 526 35 70
e-mail: gdansk@schrack-seconet.pl

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

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

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

TAP- Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel./faks 61 677 48 00
e-mail: tap@tap.com.pl
www.tap.com.pl

D PROJ S

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
e-mail: techom@techom.com
www.techom.com

B C S

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

B D PROD PROJ

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
faks 65 525 58 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

D PROD

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie *www.zabezpieczenia.com.pl*

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner

Skład i łamanie
Piotr Przybylski

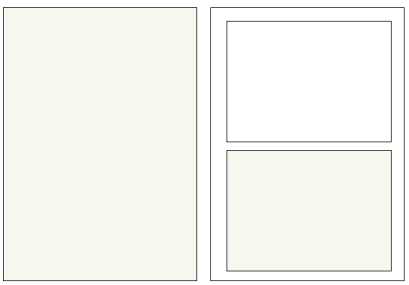
Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

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

Dostępne formy reklamy

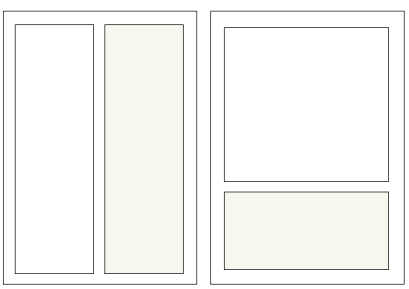
Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona



cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)

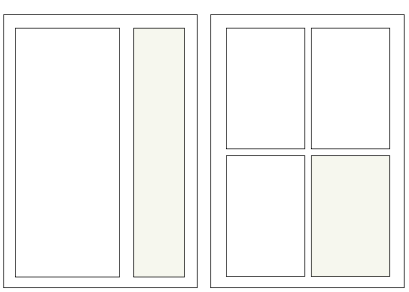
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

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

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



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

AAT HOLDING	7, 25, 61, 67, 74, 75
Axis Communications Poland	2
Bosch Security Systems	83
C&C Partners	1
Dahua Technology	10, 35
Firma ATline	30
Fujifilm	3
Genevo	45
Gunnebo	13
Hanwha Techwin Europe	55
P.U.I. Zeto-Projekt	9
Polon-Alfa	41
Przedsiębiorstwo Wdrożeniowe PRO-SERVICE	49
ROGER	19, 76, 77
Securex	15
SICUREZZA	31
Videotec	84

BOSCH
Technologia bliżej nas

Dla innych centrum handlowe to rozrywka.

Ty widzisz inteligentne dane, które pomogą zwiększyć sprzedaż.

Znajdź nas na **www.boschsecurity.pl**

BE READY FOR AN EXTRA-ORDINARY NEW WORLD

- Extra-competitive
- Extra-light
- Extra-compact
- Extra-flexible

Nowe kamery MAXIMUS MMX pozwolą na realizację nawet najbardziej skomplikowanych zadań w portach, na nabrzeżach i pokładach okrętów oraz w instalacjach przemysłowych, w których panują bardzo trudne warunki eksploatacyjne.

MAXIMUS MMX CAMERA

ATEX

LISTED

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy

VIDEOTEC