20 lat
ZABEZPIECZENIA
CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3(121)/2018

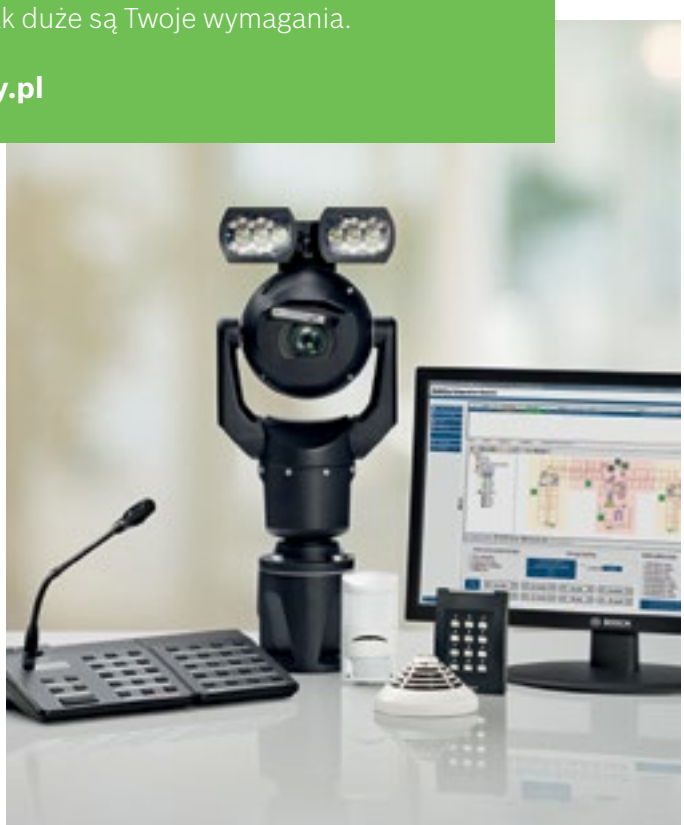
BOSCH
Technologia bliżej nas

Jedni widzą duże miasto.

Ty widzisz miasto pełne zintegrowanych rozwiązań w zakresie bezpieczeństwa i ochrony.

Dzięki firmie Bosch jesteś w stanie zbudować bezpieczniejszy świat i zapewnić mu lepszą ochronę. Praktyczne rozwiązania współpracują ze sobą, by zapewnić Ci spokój umysłu, bez względu na to, jak duże są Twoje wymagania.

Dowiedz się więcej na **boschsecurity.pl**



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 MS SQL
- 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

RWL-3

Bezprzewodowy zamek szafkowy

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

roger®

SPIS TREŚCI

Ochrona fizyczna

Telewizja dozorowa

Wywiad

SSWiN

Ochrona informacji

Eliminacja nieuzasadnionych alarmów
w systemach AHD marki NOVUS z funkcją detekcji ruchu

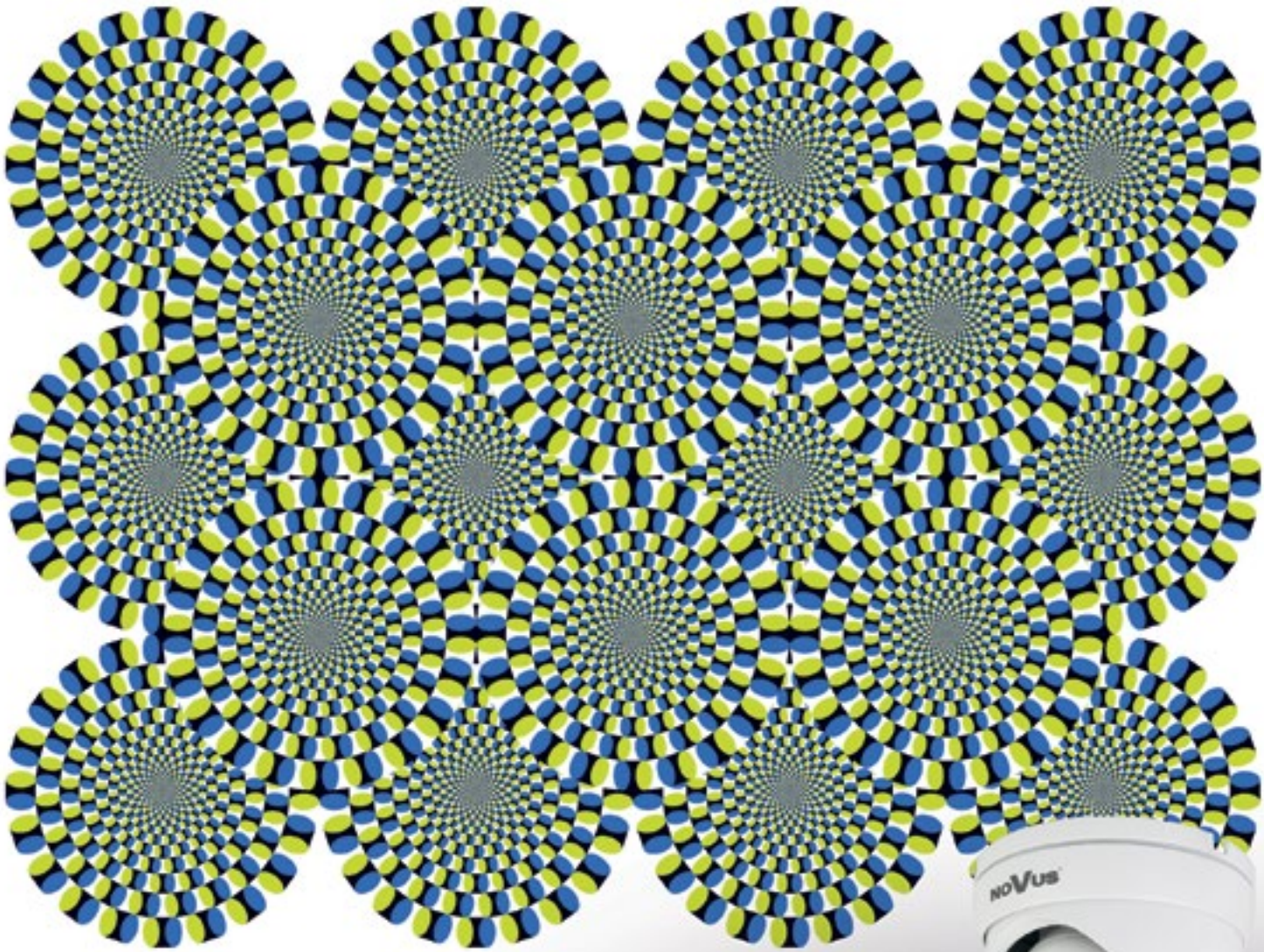
Asortyment multistandardowych kamer **AHD** marki **NOVUS** został wzbogacony w nowe modele z wbudowanymi **czujkami PIR**. Pasywne czujki podczerwieni są szeroko wykorzystywane w systemach alarmowych i służą do wykrywania poruszających się osób. Działanie czujki opiera się na precyzyjnym pomiarze temperatury obiektów przemieszczających się na określonym obszarze. Za sprawą zintegrowanych układów elektronicznych każda zmiana temperatury jest interpretowana jako ruch i generuje alarm.

Znaczne ograniczenie liczby nieuzasadnionych alarmów (wywołanych rozbłyskami światła, opadami śniegu czy przełączaniem trybu pracy kamery z dziennego na nocny lub odwrotnie) w systemach wizyjnych z funkcją detekcji ruchu jest możliwe dzięki temu, że alarm jest generowany dopiero po jednoczesnym wykryciu ruchu przez czujkę PIR i funkcję wizyjnej detekcji ruchu.

Ogromną zaletą dla administratorów systemów jest konfiguracja czujki PIR i odbieranie zdarzeń alarmowych bezpośrednio z rejestratora marki NOVUS. Po podłączeniu kamery z czujką PIR, do rejestratora zostaje ona automatycznie rozpoznana i dodana do listy kamer, a jej konfiguracja przebiega analogicznie jak w przypadku funkcji detekcji ruchu – należy określić strefę detekcji, czułość, czas postalarmu, dostępne opcje reakcji oraz włączyć nagrywanie.

Nagrania zdarzeń wykrywanych przez czujkę PIR są wyróżnione na grafie nagrań. Zarówno kamera kopułowa NVAHD-2DN3201MV/IR-1-PIR, jak i kamera w obudowie NVAHD-2DN3201MH/IR-1-PIR mają obiektyw szerokokątny o ogniskowej 2,8 mm, zaś wbudowana czujka PIR ma zasięg dochodzący do ośmiu metrów.

Bezpośr. inf. Patryk Gańko
AAT HOLDING



AHD TECHNOLOGY by NOVUS® 3000 SERIA AHD MULTI STANDARD

OKO MOŻNA OSZUKAĆ
KAMER PIR - NIE

PODWÓJNA DETEKCJA RUCHU
OGRANICZENIE FAŁSZYWYCH ALARMÓW
ZASIĘG PIR DO 8 M

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

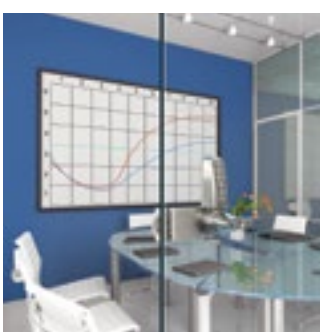
Centrala detekcji gazów CDG 6000

nowość w ofercie firmy POLON-ALFA

Adresowalna centrala detekcji gazów **CDG 6000** jest przeznaczona do sygnalizowania wycieku gazów palnych (**CNG, LPG**) oraz niebezpiecznych stężeń tlenku węgla (**CO**) po odebraniu informacji od współpracujących z nią detektorów gazów typu **PSG-6000**. Centrala uruchamia alarmową sygnalizację akustyczną i optyczną, umożliwia uruchomienie wentylacji w celu usunięcia nadmiaru szkodliwych gazów z pomieszczenia oraz może wysłać sygnał sterujący zaworem odcinającym dopływ gazu. Wbudowane linie kontrolne zapewniają kontrolę stanu sterowanych zewnętrznych urządzeń sygnalizacyjnych i wykonawczych. Centrala CDG 6000 może przekazać informację o alarmie do zainstalowanych w obiekcie systemów sygnalizacji pożarowej **POLON 4000/POLON 6000**. Może zasygnalizować wykrycie stężenia gazów odpowiadającego jednemu z trzech stopni alarmowych. Informacje o alarmach i uszkodzeniach są zapisywane w wewnętrznej, nieulotnej pamięci centrali w postaci rejestru zdarzeń. Jego pojemność wynosi 1000 zdarzeń. Konfigurowanie i programowanie centrali, a także odczyt historii zdarzeń przeprowadza się za pomocą aplikacji komputerowej Konfigurator CDG6000.

Bezpośr. inf. AAT HOLDING

Nowe zamki szyfrowe



Jedną z najważniejszych nowości w naszej ofercie są niewątpliwie zamki szyfrowe **Codelocks**. Wyróżniamy obecnie trzy główne kategorie zamków: klasyczne mechaniczne (serie od **CL100** do **CL4000GD**), klasyczne elektroniczne (serie **CL4500** oraz **CL5500**) oraz te zastępujące zamki baskwilowe, przeznaczone do szafek (serie **KLxxxx**).

Zamki szyfrowe są jednym z podstawowych zabezpieczeń, na które decydują się zarówno instytucje państwowe czy przedsiębiorstwa, jak i właściciele prywatnych posesji. Nawet w przypadku najbardziej skomplikowanych zamków tego typu instalacja jest łatwa, a koszty są niskie.

Duży wybór zamków jest odpowiedzią na zapotrzebowanie na skuteczne i proste rozwiązania. Oczywiście stanowią przede wszystkim zabezpieczenie, ale są wybierane również po to, by wyeliminować ryzyko zgubienia lub kradzieży klucza, a także ze względu na wygodę – szczególnie w przypadku, gdy z zamka korzysta wiele osób, w tym osoby mające czasowy dostęp do mieszkania (np. zajmujące się opieką nad dziećmi albo sprzątaniem). Ponadto wzrasta liczba zastosowań zamków w lokalach przeznaczonych do wynajmu. Nowoczesne rozwiązania umożliwiają pełną kontrolę dostępu, a także przegląd zarejestrowanych otwarć i prób włamania.

Zamki z serii KLxx pozwalają zabezpieczyć nawet pojedyncze szafki lub szuflady zawierające cenne przedmioty lub dokumenty. Są stosowane z powodzeniem zarówno w szpitalach, jak i w obiektach sportowych, spa i prywatnych gabinetach lekarskich.

Zachęcamy do odwiedzenia naszej strony internetowej, na której przedstawione są wszystkie zamki z naszej oferty.

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

SAIK TUBE

nowoczesne rozwiązanie dla administracji budynków

Jesteśmy firmą, która zajmuje się produkcją systemów automatycznej identyfikacji kluczy (**SAIK**). Użytkownicy dotychczasowych produktów tego typu poszukiwali sposobu na ograniczanie dostępu do kluczy służących do otwarcia drzwi głównych w budynkach oraz na stworzenie możliwości pobierania tych kluczy bez konieczności oczekiwania na osobę nimi dysponującą.

W wielu firmach i instytucjach zarządcy ustalają dyżury dla pracowników, którzy mają za zadanie przyjechać do pracy wcześniej i umożliwić wejście pozostałym pracownikom do budynku, a po zakończeniu pracy, po wyjściu wszystkich pracowników, zamknąć budynek. Jeśli z jakichś powodów osoby odpowiedzialne za otwarcie i zamknięcie budynku spóźnią się, pozostali pracownicy będą musieli czekać, marnując czas swój i pracodawcy.

W 2017 roku stworzyliśmy urządzenie **SAIK TUBE**, które spełnia oczekiwania naszych klientów. SAIK TUBE służy do przechowywania kluczy do budynku i umożliwia zdalne zarządzanie prawami dostępu pracowników do tego urządzenia. Dodatkowo wymusza dwustopniową weryfikację pracownika. Najpierw pracownik przykłada kartę zbliżeniową do czytnika i odblokowuje pierwsze zabezpieczenie. Następnie wpisuje indywidualny numer PIN, czym odblokowuje drzwi będące główną barierą – głównym zabezpieczeniem przed osobami niepowołanymi.

Zarówno pierwsze, jak i drugie drzwi urządzenia SAIK TUBE są wyposażone w czujniki otwarcia, dlatego każda próba ingerencji osób nieuprawnionych jest sygnalizowana. Drugie, wewnętrzne drzwi mają podwyższoną odporność na włamanie (klasy RC3) zgodnie z wymaganiami normy PN-EN 1627:2012.

W przypadku banków obsługiwanych przez konwojentów SAIK TUBE daje możliwość zrezygnowania z przyjazdu konwoju w celu pobrania czy zwrotu kluczy do oddziału, co pozwala znacznie ograniczyć koszty.

Zastosowanie urządzenia SAIK TUBE umożliwia korzystanie z tylko jednego zestawu kluczy do otwierania głównych drzwi budynku. Z punktu widzenia pracodawcy to przede wszystkim większa wygoda, która ma przełożenie na jakość i czas pracy, a w konsekwencji przynosi zysk.

Więcej informacji o naszym produkcie SAIK TUBE, jak również o pozostałych produktach z linii SAIK znajdziecie Państwo na stronie www.bte.pl.

Bezpośr. inf. Dawid Czaja
dawid.czaja@bte.pl
BT Electronics

Podwójne bramki obrotowe

Centurion Twin i Bastion Twin firmy CartPoland

Firma **CartPoland** została założona w 1992 r. Obecnie jesteśmy jednym z czołowych producentów kart plastikowych w Polsce. Posiadamy własny park maszynowy oraz rozbudowane zaplecze produkcyjne, dzięki któremu jesteśmy w stanie w krótkim czasie zrealizować zróżnicowane i złożone zamówienia, np. dostarczyć karty magnetyczne, karty zbliżeniowe, zdrapki lub identyfikatory na kartach plastikowych. Nasze karty, za pośrednictwem naszych partnerów, trafiają do niemal wszystkich krajów Europy oraz do kilkunastu innych krajów, m.in. do Stanów Zjednoczonych, Zjednoczonych Emiratów Arabskich, Brazylii, na Martynikę czy na Jamajkę.

Potrzeba ciągłego rozwoju zaowocowała powiększeniem asortymentu. Poza kartami produkujemy również bramki stadionowe, obrotowe, uchylne i rozsuwane – do których podłączamy systemy kontroli dostępu oraz rejestracji czasu pracy. Produkujemy też bramki do wykrywania metali, ręczne wykrywacze metali oraz certyfikowane bariery antyzderzeniowe, zapory drogowe i kolczatki.

W ostatnich latach nastąpił ogromny wzrost zainteresowania urządzeniami zabezpieczającymi. Do naszych najciekawszych produktów z tej dziedziny należą podwójne bramki obrotowe **Centurion Twin i Bastion Twin**. Po raz pierwszy mieliśmy okazję zaprezentować je większemu gronu zainteresowanych na Międzynarodowych Targach Zabezpieczeń SECUREX 2018. Są to bramki dwukierunkowe, wyposażone w serwonapęd, obsługujące dwa niezależne przejścia.

Użycie zasilacza buforowego pozwala na podtrzymywanie napięcia w przypadku awarii sieci energetycznej, a opcjonalnie montowany podgrzewacz umożliwia instalację bramek na zewnątrz budynków. Bramki Centurion Twin i Bastion Twin świetnie sprawdzą się jako bramki kontrolujące dostęp pieszych do budynków i stref wymagających zabezpieczenia. Możliwość połączenia z systemem kontroli dostępu, systemem rejestracji czasu pracy i alkomatem, a także integracja z wizyjnym systemem dozorowym czyni z podwójnych bramek świetne rozwiązanie dla zakładów pracy, w których wymagana jest kontrola ruchu pracowników.

Bezpośr. inf. Maciej Twardowski
maciej@cartpoland.pl
CartPoland

Panoramiczna kamera 4K HDCVI

Zastosowanie urządzeń o rozdzielczości **4K** we współczesnych systemach dozoru wizyjnego nie zaskakuje. Stosowane są powszechnie i mają wysokoczułe przetworniki, co przekłada się na bardzo dobrą jakość obrazu nawet w trudnych warunkach oświetleniowych. Tak wysoka rozdzielczość jest kojarzona z kamerami sieciowymi.

Ciekawym wyjątkiem od powyższej reguły są kamery 4K generujące sygnał analogowy, które pojawiły się na rynku dzięki firmie **Dahua Technology**. Asortyment oferowanych urządzeń tego typu jest coraz większy, jednakże jedno z nich zdecydowanie wyróżnia się na tle innych, dzięki czemu zdobyło Złoty Medal Międzynarodowych Targów Poznańskich podczas targów SECUREX 2018.

Chodzi o 3-przetwornikową kamerę panoramiczną **HAC-PFW3601-A180** – produkt ze wszech miar unikatowy i innowacyjny. Sygnał z trzech wysokoczułych przetworników Sony STARVIS jest przetwarzany i łączony w jeden obraz o rozdzielczości 3840x2160, w przypadku którego pole widzenia kamery wynosi 180°. Aby zapewnić wysoką rozróżnialność szczegółów obrazu nawet w ciemnościach, model ten wyposażono w promiennik IR o zasięgu 20 m. Wysokie kontrasty redukuje funkcja WDR o dynamice 120 dB czy funkcja HLC. Dostępne są także funkcje 3DNR oraz AGC. Urządzenie ma dwa wejścia i jedno wyjście alarmowe, wejście dźwiękowe oraz wyjście serwisowe. Obudowa o klasie szczelności IP67 i klasie odporności na udary IK10 umożliwia montaż tych kamer w wielu miejscach.

Bezpośr. inf. Marian Maroszek
Dahua Technology Poland

Rejestrator Dahua XVR5216AN-4KL-16P

Od roku 2015 do chwili obecnej trwa ponowny rozkwit analogowych systemów dozoru wizyjnego. Pokusa dziesięciokrotnego zwiększenia liczby szczegółów w obrazie bez konieczności wymiany starej infrastruktury na nową poskutkowała powstaniem wielu zamkniętych i ograniczonych systemów, ponieważ okazało się, że standardy CVI, TVI i AHD nie są ze sobą kompatybilne, a rozbudowa systemów wykorzystujących te techniki wcale nie jest łatwa.

Aby rozwiązać ten problem, **Dahua Technology** opracowała nową serię urządzeń. Ostatecznie pojęcie uniwersalnego rejestratora hybrydowego nabrało materialnego kształtu. **XVR5216AN-4KL-16P** umożliwia rejestrację sygnałów z szesnastu kanałów analogowych w dowolnym standardzie (HDCVI/AHD/TVI/CVBS), z rozdzielczością do 4K włącznie. Nic nie stoi na przeszkodzie, aby dodatkowo rejestrować strumienie wizyjne z kamer IP. Wszechstronność zastosowań omawianego urządzenia zapewnia menu OSD służące do obsługi kamer, umożliwiające sterowanie PTZ, transmisję dźwięku, zasilanie oraz obsługę wejść/wyjść alarmowych. Dopełnieniem jest obsługa inteligentnej analizy treści obrazu IVS, integracja z czujkami ruchu i temperatury, a także wyjście HDMI o rozdzielczości 4K.

XVR5216AN-4KL-16P jest rozwiązaniem stworzonym w związku z zapotrzebowaniem na prawdziwie uniwersalny serwer zapisu danych.

Bezpośr. inf. Marian Maroszek
Dahua Technology Poland

Innowacyjne zabezpieczenie terenu budowy dzięki systemowi WES+

SECUREX już za nami. Dziękujemy za odwiedzanie stoiska firmy **GEO-KAT** – oficjalnego dystrybutora systemu **WES+** w Polsce.

W czasie targów mieliśmy przyjemność zaprezentować Państwu nową wersję systemu WES+, w której ręczny ostrzegacz pożarowy został rozbudowany przez dodanie dodatkowego przycisku medycznego służącego do powiadomienia o wypadku na budowie.

Nawet przy zachowaniu ostrożności w środowisku pracy o wysokim ryzyku, jakie jest na placu budowy, stale występuje zagrożenie życia i zdrowia. W związku z tym konieczne jest natychmiastowe udzielenie pomocy w razie wypadku.

Nowa wersja systemu – WES^3 – zawiera wszelkie udogodnienia systemu WES+, a także ma dodatkowe funkcje, np. opóźnienie procedury ewakuacji ze zgłoszonej strefy, dzięki któremu jest czas na weryfikację zdarzenia. Po uruchomieniu wstępnego alarmu dźwiękowego osoby odpowiedzialne za ochronę terenu budowy będą mogły same zadecydować o wszczęciu procedury ewakuacji lub o odwołaniu alarmu, jeżeli niewielkie zagrożenie zostanie wyeliminowane przez pracowników budowy czy odpowiednie służby ratunkowe.

Przycisk medyczny systemu WES^3 zapewnia pracownikom możliwość zgłoszenia alarmu (bez konieczności ewakuacji), jeżeli potrzebna jest pomoc medyczna. Dodatkowo, dzięki wbudowanej pamięci urządzenia w stacji bazowej, zawsze jesteśmy w stanie odczytać miejsce i czas zdarzenia.

Podstawową zaletą bezprzewodowego systemu sygnalizacji pożarowej jest to, że w miarę postępu prac budowlanych można bardzo łatwo zmienić położenie ręcznych ostrzegaczy pożarowych. Nie ma potrzeby prowadzenia okablowania, które wymaga montażu czy programowania.

Przewodowe systemy sygnalizacji pożarowej mogą uniemożliwić podwykonawcom zamknięcie poszczególnych części budynku. Przed każdą kolejną fazą budowy trzeba dokonać zmiany tras przewodów, co wiąże się z tymczasowym wyłączeniem systemu alarmowego. Tego problemu nie ma tam, gdzie stosuje się bezprzewodowe systemy alarmowe. Zdobywają one coraz większą popularność, dają nowe możliwości, a dzięki ich mobilności łatwiej dostosować je do pracy na chronionym obszarze.

Szczegółowe informacje znajdują się na stronie www.wesfire.com.pl.

Bezpośr. inf. Marcin Malinowski
GEO-KAT
e-mail: info@wesfire.com.pl

Detektor FLA-07i
do systemów ochrony obwodowej

Detektor FLA-07i jest przeznaczony do pracy w systemach ochrony obwodowej **Varya Perimeter** i może być zastosowany na dowolnym ogrodzeniu lub płocie. Akcelerometr w detektorze wykrywa dynamiczne zmiany położenia przeplotu ogrodzenia. Detektor wykrywa próby przechodzenia przez płot lub jego przecinania. Dzięki funkcji **WAV** (Weather Alarm Verification) jest odporny na zmienne warunki atmosferyczne, tj. silny wiatr, gradobicie, śnieg, mgła czy wyładowania atmosferyczne. Detektor FLA-07i automatycznie dostosowuje swoje działanie do właściwości mechanicznych chronionego ogrodzenia.

Ten sam detektor można zastosować również do tzw. ochrony przedmiotowej za pomocą systemu Anarya Alarm. Urządzenie FLA-07i jest wyposażone w trzyosiowy akcelerometr oraz żyroskop. Ma też dwa wejścia cyfrowe służące do podłączenia innych urządzeń. Detektor może być stosowany na wszystkich rodzajach ogrodzeń. Uzyskał certyfikat Grade 4. Czas działania baterii może wynosić nawet osiem lat. Detektor w systemie Varya Perimeter ma funkcję automatycznej, okresowej kontroli poprawnego działania akcelerometru. Dodatkową funkcją systemu Varya Perimeter jest automatyczna rejestracja patrolowania wzdłuż ogrodzenia.

Bezpośr. inf. Marek Majchrzak
m.majchrzak@rcse.pl
RCS Engineering

Publikacja oprogramowania systemu
RACS w wersji 5.4

W kolejnej wersji oprogramowania systemu kontroli dostępu i automatyki budynkowej **RACS 5** dodano wiele nowych funkcji. Do najważniejszych z nich należy zaliczyć możliwość wydruku etykiet do kart z poziomu programu zarządzającego systemem, integracji kamer CCTV z funkcją rozpoznawania numerów tablic rejestracyjnych, zezwalania na dostęp pod warunkiem autoryzacji zewnętrznej oraz potwierdzania tożsamości użytkowników za pomocą telefonów z systemem iOS lub Android.

Najnowsza wersja programu do konfiguracji i obsługi systemu oferuje prosty moduł projektowania graficznego nadruku na kartach i umożliwia wydrukowanie ich na dowolnej drukarce, która jest przystosowana do wydruku obrazów.

Funkcja rozpoznawania numerów tablic rejestracyjnych dzięki wykorzystaniu kamer CCTV jest kolejną możliwą formą uwierzytelniania użytkowników systemu.

Kolejną nową funkcją systemu, uzyskiwaną dzięki nowej wersji oprogramowania, jest możliwość zezwalania na dostęp albo odmawiania dostępu z różnych poziomów – stacji roboczej (decyzję podejmuje operator), terminalu dostępowego (decyzję podejmuje inny użytkownik) lub zewnętrznego oprogramowania wykorzystującego serwer integracji systemu RACS 5.

Aby ułatwić potwierdzanie tożsamości użytkowników za pomocą telefonów komórkowych, wprowadzono do oferty terminal zbliżeniowy MCT88M-IO z kolorowym wyświetlaczem oraz miniaturowy czytnik zbliżeniowy MCT80M-BL.

Bezpośr. inf. ROGER

SPRAWDŹ
JAK ZMIENIAMY
SIĘ DLA CIEBIE

NOWA STRONA INTERNETOWA

OPROGRAMOWANIA NMS

www.nms.aat.pl

www.nms.aat.pl

Autonomiczna kamera IP marki NOVUS
do odczytu numerów z tablic rejestracyjnych

Wykorzystanie kamer **NVIP-2DN5021H/IRH-1P/LPR** pracujących autonomicznie, bez konieczności stosowania dodatkowego, licencjonowanego oprogramowania oraz sprzętu komputerowego umożliwia szybkie i proste tworzenie systemów kontroli dostępu dla pojazdów. Kamery rozpoznają tablice rejestracyjne ze wszystkich państw Unii Europejskiej i byłych krajów WNP, a także Turcji, Izraela, Szwajcarii i Norwegii, i odczytują z nich numery.

Rozwiązanie to pozwala na odczyt numerów z tablic rejestracyjnych pojazdów poruszających się z prędkością do 50 km/h. Kamerę konfiguruje się w pełni za pomocą przeglądarki internetowej. Umożliwia to utworzenie list pojazdów, których dostęp do chronionej strefy jest dozwolony lub zabroniony, wraz z harmonogramami obowiązywania praw dostępu. Sterowanie szlabanem lub bramą odbywa się za pośrednictwem wyjścia przekaźnikowego. Ponadto następuje zapis obrazu na serwerze FTP oraz wysłanie e-maila wraz z załącznikiem na wskazany adres.

Kamera jest wyposażona w wewnętrzną bazę pięciuset ostatnio rozpoznanych tablic z następującymi atrybutami: data oraz czas rozpoznania, numer z tablicy rejestracyjnej, zdjęcie tablicy, kierunek przemieszczania się pojazdu, obecność na „białej liście" lub „czarnej liście", kraj pochodzenia tablicy rejestracyjnej. Baza danych może być filtrowana według powyższych atrybutów oraz eksportowana do pliku. Kamera z obiektywem o ogniskowej regulowanej w zakresie od 7 mm do 22 mm jest zintegrowana z aplikacją NMS.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Dekada kamer sieciowych
w transporcie publicznym

Dziesięć lat temu zaczęto stosować wizyjne systemy dozorowe w środkach komunikacji miejskiej, pociągach i autobusach dalekobieżnych. Dzięki dynamicznemu rozwojowi techniki pojawiły się nowe funkcje, takie jak liczenie ludzi czy rozpoznawanie twarzy, które poprawiają bezpieczeństwo pasażerów i efektywność transportu publicznego. Wzrosła także niezawodność elementów mechanicznych kamer, a także pojawiła się możliwość przetwarzania obrazów. Dodano również funkcje, które pomagają w przypadku pracy kamer w zmiennych warunkach oświetlenia czy konieczności wykorzystania pamięci o relatywnie niewielkiej objętości, a także ułatwiają transmisję danych. Należą do nich Forensic WDR – Forensic Capture oraz Axis Lightfinder. Obie te funkcje gwarantują możliwość wytwarzania kolorowych obrazów nawet w niemal całkowitej ciemności.

Istotną wadą starszych systemów analogowych była ich niezdolność do kompresji obrazów. Aby sprostać temu wyzwaniu, w kamerach IP wprowadzono funkcję Zipstream, która umożliwia kompresję bez uszczerbku dla jakości i użyteczności zarejestrowanego materiału wizyjnego. Flagowym produktem jest kamera sieciowa **Axis P3905-R Mk II** przeznaczona do dozoru w pojazdach kołowych i szynowych.

Coraz powszechniejsze w użyciu stają się kamery pokładowe z wbudowanymi mikrofonami. Możliwość rejestracji dźwięku poprawia efektywność działania kamery i ułatwia postępowanie wyjaśniające po zaistniałym zdarzeniu, np. utarczce słownej między pasażerami. Standardem są już kamery z aplikacjami kontrolującymi zachowanie kierowcy, które pomagają ustalić przyczynę zdarzenia – błąd ludzki albo okoliczności zewnętrzne. Kamery zainstalowane na zewnętrz pojazdów komunikacji miejskiej, które umożliwiają wyświetlanie obrazów na ekranach umieszczonych na deskach rozdzielczych maszynistów, mogą działać jak cyfrowe lusterka.

– Dzisiejsze kamery sieciowe to już nie tylko urządzenia optyczne, ale również komputery o dużej mocy obliczeniowej, pozwalające na inteligentną analizę rejestrowanych obrazów. Zaawansowane algorytmy analityczne umożliwiają firmom transportowym wykrywanie pozostawionych przedmiotów oraz dostęp do istotnych danych na temat liczby pasażerów i ich zachowań, a nawet analizę pod kątem demograficznym. Ze względu na tempo rozwoju techniki i rosnący popyt na tego rodzaju usługi sieciowe kamery pokładowe z pewnością staną się kluczową częścią naszej wspólnej przyszłości – powiedział Jakub Kozak, dyrektor handlowy na Polskę, Ukrainę i kraje bałtyckie w firmie Axis Communications.

Bezpośr. inf.
Axis Communications

Kamery ruchome Bosch MIC IP fusion 9000i
przeznaczone do zadań specjalnych

Kamery ruchome **MIC IP fusion 9000i** zaprojektowano z myślą o pracy w niemal każdych warunkach eksploatacyjnych. Zastosowano w nich przetwornik optyczny i termowizyjny, mają wytrzymałą obudowę, a dodatkowym atutem jest funkcja **Intelligent Video Analytics**. Dzięki temu kamery mogą być wykorzystane do wykonywania złożonych zadań, nawet o znaczeniu krytycznym.

Kamery dostarczają szczegółowych informacji na temat bieżącej sytuacji i umożliwiają wczesne wykrywanie obiektów i ludzi nawet w całkowitej ciemności, także w warunkach zadymienia ograniczającego widoczność w świetle białym. Możliwe jest także wykrywanie obiektów i ludzi znajdujących się w gęstych zaroślach.

Kamera korzysta z wyjątkowej funkcji łączącej metadane z dwóch przetworników – optycznego i termowizyjnego. Dzięki temu użytkownicy mogą dostrzec istotne szczegóły, które są ukryte. Alarm jest wyzwalany także w razie wykrycia zdarzenia, które nie jest widoczne w aktualnie oglądanym strumieniu wizyjnym. Dzięki temu kamery MIC IP fusion 9000i dostarczają dokładnych informacji o sytuacji na obserwowanym terenie całodobowo, niezależnie od panujących warunków atmosferycznych.

Bezpośr. inf. Michał Małek
Bosch Security and Safety

Bezprzewodowy zamek szafkowy RWL-3

Zamek szafkowy **RWL-3** umożliwia bezprzewodową kontrolę dostępu do szafek i różnego rodzaju skrytek. Zamek RWL-3 może pracować w trybie autonomicznym (offline) lub sieciowym (online).

W trybie autonomicznym zamek RWL-3 steruje dostępem do szafki na podstawie danych konfiguracyjnych wprowadzonych do jego pamięci w trakcie programowania, które może być przeprowadzone manualnie, za pomocą karty programującej lub zdalnie, po nawiązaniu połączenia z poziomu programu **RogerVDM**.

W trybie sieciowym zamek jest połączony bezprzewodowo z kontrolerem, który zarządza dostępem do szafki i rejestruje na bieżąco zdarzenia związane z obsługą zamka, w tym stany alarmowe.

W scenariuszu online konfiguracja uprawnień dostępu jest realizowana z poziomu oprogramowania zarządzającego systemem RACS 5, które umożliwia elastyczne określanie zasad dostępu do szafek z uwzględnieniem kalendarzy, harmonogramów, poziomów dostępu i innych zaawansowanych mechanizmów stosowanych powszechnie w systemach kontroli dostępu.

Zamek RWL-3 składa się z czytnika zbliżeniowego montowanego na zewnątrz szafki oraz zasobnika na baterie zespolonego z mechanizmem ryglującym, który jest montowany wewnątrz szafki. Zamek jest wyposażony w czujnik położenia rygla oraz wejście do podłączenia zewnętrznego czujnika otwarcia drzwiczek. W przypadku wyczerpania baterii zamek może być zasilany za pomocą zewnętrznego zasilacza podłączonego do czytnika zbliżeniowego.

Bezpośr. inf. ROGER

ULISSE COMPACT z funkcją DELUX

do pracy w trybie dzień/noc

Firma **Videotec** wprowadza na rynek kamery z nową funkcją **DELUX** usprawniającą tworzenie i kodowanie obrazów w kamerach zainstalowanych na zewnątrz budynków, pracujących w trybie dzień/noc. Dzięki zwiększonej światłoczułości kamer można uzyskać czytelne obrazy i poprawną reprodukcję barw w warunkach bardzo słabego oświetlenia, na poziomie 0,006 luksa, a także poprawną pracę w trybie monochromatycznym już przy 0,0006 luksa.

Zalety wynikające z zastosowania funkcji DELUX stają się szczególnie widoczne w wizyjnych systemach dozorowych służących do całodobowej ochrony rozległych terenów o strategicznym znaczeniu, gdzie trzeba ciągle obserwować i identyfikować ludzi, rozpoznawać poruszające się pojazdy i oceniać nietypowe zdarzenia, zarówno w dzień jak i w nocy.

DELUX – nowa metoda tworzenia i kodowania obrazów, opracowana przez dział badawczo-rozwojowy firmy Videotec, została użyta w punktach kamerowych ULISSE COMPACT PTZ stosowanych na całym świecie do nadzoru nad terenami miejskimi, ochrony perymetrycznej obiektów przemysłowych należących do infrastruktury krytycznej, ochrony granic państwowych i kontroli ruchu drogowego.

ULISSE COMPACT z funkcją DELUX to punkt kamerowy, który pracuje w trybie dzień/noc z rozdzielczością FullHD 1080p i prędkością 60 klatek na sekundę, co umożliwia precyzyjną obserwację szybko poruszających się obiektów. Moduł kamerowy jest wyposażony w obiektyw zmiennoogniskowy zapewniający trzydziestokrotne powiększenie obrazu na drodze optycznej.

Funkcja DELUX zapewnia lepszą niż dotychczas czułość na światło, skuteczniejszą redukcję szumów, bardzo dobrą reprodukcję barw, a także znaczną poprawę funkcjonalności punktów kamerowych ULISSE COMPACT. Prędkość ruchu punktu kamerowego została uzależniona od ogniskowej obiektywu. Usprawniono tworzenie zamaskowanych stref prywatności.

Wytrzymała konstrukcja mechaniczna punktów kamerowych ULISSE COMPACT gwarantuje ich bezawaryjną pracę w każdych warunkach pogodowych, w zakresie temperatur od -40°C do + 60°C. Maksymalna prędkość obrotowa wynosi 200°/s. Pozycjonowanie z użyciem wcześniej przygotowanych ustawień PTZ jest bardzo precyzyjne. Dostępne są funkcje poprawiające jakość obrazu podczas obserwacji we mgle. Obudowa modułu kamerowego jest wyposażona w wycieraczkę i oświetlacz pracujący w podczerwieni.

Dzięki zachowaniu dużej staranności na wszystkich etapach projektowania urządzeń z funkcją DELUX możliwa była znaczna redukcja kosztów produkcji nowego modelu punktu kamerowego ULISSE COMPACT. Poprawa jakości obrazu oraz usprawnione działanie zwiększyło konkurencyjność nowego modelu na światowym rynku wizyjnych systemów dozorowych.

Bezpośr. inf. Videotec
www.videotec.com
sales@videotec.com
Tłumaczenie: Redakcja

Tegoroczna konferencja firmy EBS

Wpływ IoT na branżę zabezpieczeń

Tematem przewodnim konferencji, która odbyła się w dniach **8–9 marca**, był wpływ **Internetu rzeczy** (**IoT**) na branżę zabezpieczeń. Zakres zastosowań IoT jest szeroki, dlatego w ramach wprowadzenia organizatorzy wyjaśnili, że będą się odwoływać do trzech głównych obszarów tych zastosowań: łączności z urządzeniami, przetwarzania danych w chmurze oraz wykorzystywania aplikacji mobilnych.

Co ciekawe, zaproponowany podział był widoczny również we wnioskach z badań rynkowych przeprowadzonych przez firmę IHS, według której w ciągu 4–6 lat tradycyjne zabezpieczenia zostaną zastąpione zabezpieczeniami inteligentnymi, umożliwiającymi klientom zdalną obsługę systemów alarmowych za pomocą aplikacji mobilnych instalowanych na smartfonach. Aby to było możliwe, użytkowane systemy alarmowe musiałyby być na stałe podłączone do Internetu.

Wpływ IoT został ukazany na przykładach produktów służących do ochrony mienia i osób. Wpasowuje się w obecne trendy łączenia ochrony fizycznej i zabezpieczeń technicznych, a także zdalnego zarządzania systemami ochrony.

Zmiany odbywają się szybko i to, co kiedyś było tradycyjne, obecnie jest przestarzałe, dlatego konferencje organizowane przez firmę EBS mają pomóc uczestnikom przewidywać kierunki rozwoju produktów.

Patronat nad konferencją objęły trzy izby branżowe – PZPO, PIO i PISA – oraz inni, w tym czasopismo *Zabezpieczenia*.

W trakcie konferencji zostały zaprezentowane produkty naszych partnerów technologicznych – firm Hikvision, Linc Polska, DMSI, AdInfo oraz Plus. Zaprezentowano programy do obsługi systemów alarmowych pracujące w chmurze, systemy detekcji intruzów wykorzystujące analizę treści obrazu już w kamerach, systemy transmisji obrazów wizyjnych oraz wiele innych ciekawych rozwiązań.

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

Bezpośr. inf. EBS

I Forum Bezpieczeństwa Zakładów Wytwórczych Energii

podsumowanie

W dniach **13–14 marca 2018 r.** odbyło się **I Forum Bezpieczeństwa Zakładów Wytwórczych Energii** zorganizowane przez **PZU Lab** oraz **TUW Polski Zakład Ubezpieczeń Wzajemnych**. W pierwszej edycji forum wzięło udział prawie 200 uczestników, wśród których przeważali przedstawiciele czołowych polskich grup energetycznych: PGE, Tauron, Enea i Energa.

W spotkaniu wzięli udział również przedstawiciele innych branż, m.in. reprezentanci Polskiej Grupy Górniczej, Grupy Azoty, Grupy Lotos, PCC Rokita oraz kilkunastu innych firm współpracujących z branżą energetyczną.

Forum uświetnili swym udziałem partnerzy instytucjonalni, a mianowicie Urząd Dozoru Technicznego oraz uczelnie – AGH, Politechnika Gdańska, Politechnika Warszawska i Politechnika Łódzka.

Celem konferencji była promocja wiedzy i wymiana doświadczeń z zakresu szeroko rozumianego bezpieczeństwa w przemyśle energetycznym. Przedstawiciele największych firm w Polsce, instytucji publicznych i ośrodków akademickich starali się odpowiedzieć na kluczowe pytania dotyczące przyszłości branży energetycznej oraz sposobów jej przygotowania na nowe formy zagrożeń, takie jak cyberataki i terroryzm.

Jak wiadomo, tylko bezpieczna i innowacyjna energetyka jest gwarantem dynamicznej i nowoczesnej gospodarki, a ciągłość dostaw energii jest filarem działalności całego państwa. To właśnie w dużej mierze od bezpieczeństwa realizowanych procesów wytwórczych i niezawodności dostaw energii zależy funkcjonowanie całego kraju.

Podczas dwudniowego forum zaprezentowano również najlepsze międzynarodowe rozwiązania z zakresu bezpieczeństwa działalności operacyjnej przedsiębiorstw, ochrony środowiska oraz ochrony ludzi.

Prezentacje eksperckie były poświęcone kierunkom rozwoju

oraz sposobom unowocześniania branży energetycznej w Polsce tak, aby jej funkcjonowanie było efektywne, innowacyjne i zgodne z wymogami środowiskowymi.

Eksperci omawiali m.in. zagadnienia związane ze znaczeniem bezpieczeństwa w działalności operacyjnej przedsiębiorstw, z tworzeniem systemu identyfikacji zagrożeń i oceny ryzyka procesowego w elektrowni, z doświadczeniami brytyjskimi dotyczącymi zdarzeń awaryjnych w energetyce. Podczas jednego z wystąpień omówiono warsztaty Piramida Kompetencji, których tematem były strategie pożarowe. Warsztaty zostały zorganizowane przez PZU Lab we współpracy z Politechniką Łódzką w lipcu 2017 r. w zakładzie Enea Połaniec. Uczestnikami byli naukowcy, osoby z branży energetycznej oraz eksperci z PZU Lab.

Uczestnicy forum mogli wymienić się swoimi doświadczeniami podczas debat i rozmów kuluarowych. W specjalnie przygotowanych „pokojach innowacji" uczestnicy mogli zapoznać się z nowoczesnymi rozwiązaniami z zakresu Internetu rzeczy (IoT), wirtualnej rzeczywistości, przetwarzania dużych zbiorów danych oraz technik uczenia się przez maszyny lub systemy (ang. *machine learning*). Uczestnicy forum mieli również możliwość skorzystania z doświadczeń i dobrych praktyk wypracowanych przez RWE – jedną z czołowych firm z branży energetycznej.

Forum było również znakomitą okazją do rozmów o możliwościach doskonalenia działań związanych z minimalizacją ryzyka i poprawy standardów bezpieczeństwa procesowego w sektorze energetycznym.

Bezpośr. inf. Robert Kuczkowski
PZU Lab

Zasilacze

gwarantowanego napięcia przemiennego i stałego ZUP-230V w instalacjach bezpieczeństwa ochrony przeciwpożarowej

Dariusz Cygankiewicz

Instalacje systemów przeciwpożarowych [1] muszą niezawodnie działać w czasie normalnej eksploatacji (dozoru), a przede wszystkim w czasie pożaru. Innowacyjne zasilacze ZUP-230V są źródłami gwarantowanych napięć 230 V_{AC} i 24 V_{DC}. Są one zgodne z wymaganiami norm [2, 3] i przepisów prawnych obowiązujących w ochronie przeciwpożarowej, w tym także z rozporządzeniem MSWiA z 20 czerwca 2007 r. [4] oraz z rozporządzeniem UE Nr 305/2011 (CPR) z 9 marca 2011 r. [5]

Cechy charakterystyczne i podstawowe zastosowania

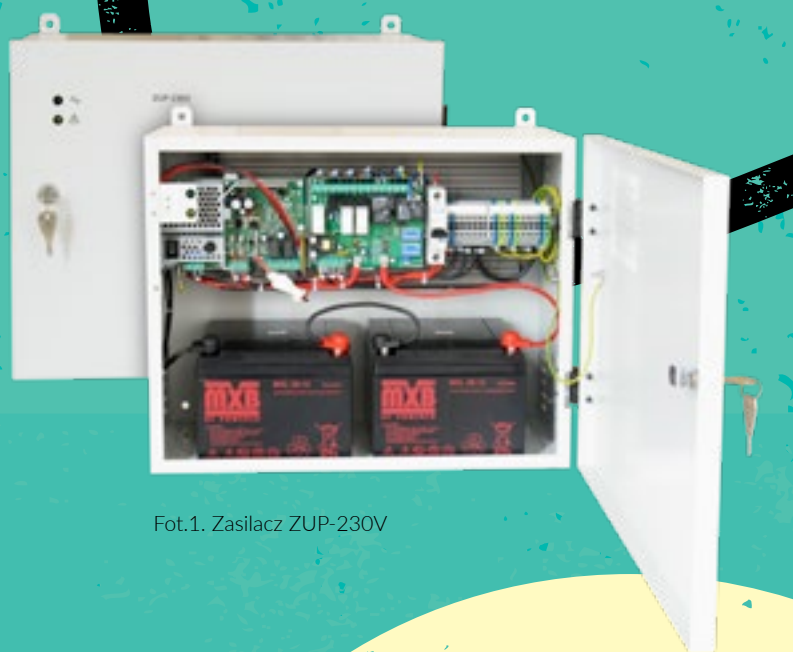
Zasilacz umożliwia rozdział napięcia 230 V pomiędzy cztery różne typy odbiorników wymagających podania, przełączenia lub odłączenia zasilania w określonym czasie i zależnie od realizowanej funkcji, po otrzymaniu sygnału z zewnątrz. Czasy reakcji dla poszczególnych typów wyjść mogą być ustawiane przez użytkownika w szerokim zakresie za pomocą przełączników suwakowych [6].

Zasilacz ZUP-230V nie jest UPS-em. Większość urządzeń przeciwpożarowych zasilanych napięciem 230 V podczas dozoru pozostaje w bezruchu, czyli nie pobiera mocy. Uwzględniono to w działaniu zasilacza przez wprowadzenie konkretnych czasów aktywności inwertera, który pobiera energię z baterii. Poza tymi czasami bateria jest odciążona w oczekiwaniu na ewentualny alarm pożarowy. Umożliwia to wydłużenie czasu dozoru do 72 h przy jednoczesnym utrzymaniu gotowości do obsługi zasilanych urządzeń z pełną mocą (400÷1500 W, zależnie od odmiany) [6].

Zasilacze ZUP-230V są stosowane przede wszystkim do zasilania:

- bram napowietrzających,
- wzrostowych wyzwalaczy przeciwpożarowych wyłączników prądu,
- samohamownych, dwukierunkowych siłowników klap odcinających wentylacji pożarowej,
- napędów bram oddzielających strefy pożarowe,
- siłowników sprężynowych przeciwpożarowych klap odcinających,
- rolety podsufitowych zbiorników dymu,
- wentylatorów kanałów oddymiania, uruchamianych po przejściu klapy odcinającej w pozycję otwarcia,
- samohamownych, dwukierunkowych siłowników klap odcinających wentylacji pożarowej, zamykanych po zatrzymaniu wentylatora,
- urządzeń uruchamianych kaskadowo w celu zmniejszenia prądu rozruchowego.

Dodatkowo zasilacz dostarcza napięcia gwarantowanego 24 V_{DC} o mocy 100 W do zasilania innych urządzeń przeciwpożarowych [6]. Wyjście to jest zabezpieczone przed zwarciem.



Fot.1. Zasilacz ZUP-230V

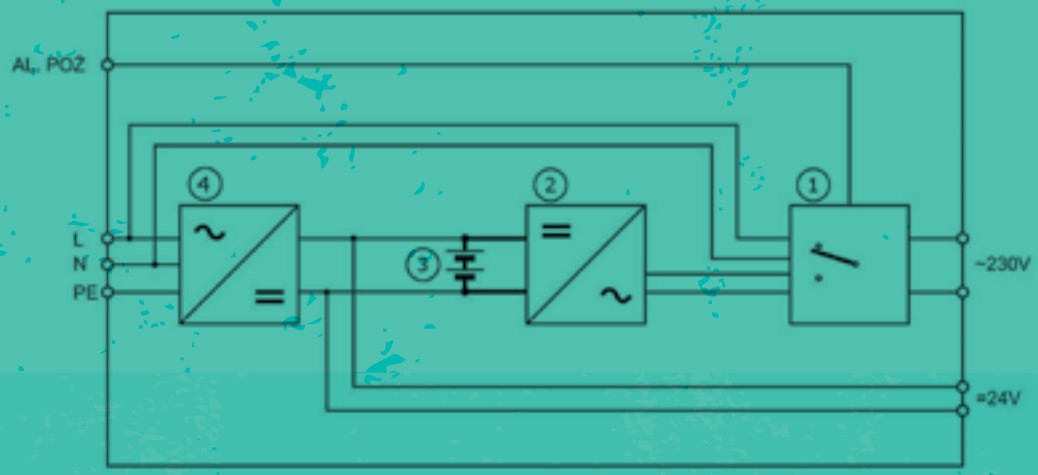
Schemat blokowy

Na rysunku 1 przedstawiono uproszczony schemat blokowy zasilacza ZUP-230V.

Funkcje dodatkowe

Zasilacz jest wyposażony w świetlną sygnalizację stanu pracy na drzwiach szafki i wewnętrzną sygnalizację diagnostyczną. Może przyjąć sygnał alarmu pożarowego z CSP lub układu oddymiania. Może również zostać ręcznie wysterowany z wielu lokalizacji.

ZUP-230V ma układ kontroli linii sterującej, którą można włączyć albo wyłączyć. Jest on wyposażony w wewnętrzny przycisk testu oraz wewnętrzny przycisk umożliwiający uruchomienie zasilacza z wykorzystaniem samych baterii, bez zasilania sieciowego. Zbiorcze uszkodzenie zasilacza [2] jest sygnalizowane na zewnątrz za pomocą przekaźników. Zasilacz zapewnia pełną obsługę baterii



Rys. 1. Schemat blokowy zasilacza
1 – główny blok rozdziału zasilania 230 V_{AC} (ZUP)
2 – inwerter 24 V_{DC}/230 V_{AC}
3 – bateria akumulatorów 24 V
4 – zasilacz ZSP121N-DR, którego podstawową funkcją jest ładowanie baterii akumulatorów i nadzór nad nią, dostarczanie energii do wyjścia 24 V_{DC} oraz zasilanie układów elektronicznych bloku rozdziału zasilania 230 V

Typ zasilacza	Maks. moc wyjściowa 230 V_{AC}	Maks. poj. baterii akumulatorów	Wymiary korpusu – SxWxG [mm]	Ciężar z baterią
ZUP-230V-400	400 W	45 Ah	455×406×207	42 kg
ZUP-230V-700	700 W	45 Ah	455×406×207	42 kg
ZUP-230V-1000	1000 W	45 Ah	455×406×207	42 kg
ZUP-230V-1500	1500 W	75 Ah	555×456×207	65 kg

Tab. 1. Podstawowe parametry eksploatacyjne zasilaczy

akumulatorów, łącznie z ochroną przed głębokim rozładowaniem i kontrolą rezystancji obwodu bateryjnego.

Certyfikacja

Na podstawie rozporządzenia CPR [5] CNBOP-PIB wydało dla zasilaczy ZUP-230V certyfikat stałości właściwości użytkowych nr 1438-CPR-0593, który upoważnia producenta do wystawienia deklaracji właściwości użytkowych. Zgodnie z rozporządzeniem MSWiA [4] wystawił także, wymagane w Polsce (oprócz certyfikatu), świadectwo dopuszczenia do użytkowania nr 3183/2018.

Wykaz norm zharmonizowanych z rozporządzenia CPR [5] oraz rozporządzenie MSWiA [4] nie obejmują norm dla „systemów bezprzerwowego zasilania UPS" (PN-EN 62040). Z powyższego wynika, że urządzenia typu UPS nie mogą uzyskać na ich podstawie zarówno certyfikatu stałości właściwości użytkowych dla celów stosowania w systemach ochrony przeciwpożarowej, jak również świadectwa dopuszczenia do użytkowania. Brak wymienionych dokumentów uniemożliwia stosowanie rozwiązań typu UPS w systemach ochrony przeciwpożarowej, natomiast zasilacz ZUP-230V może być w takich przypadkach legalnie używany.

Podsumowanie

Zasilacz ZUP-230V jest nowością na rynku, gdyż większości jego funkcji nie mają żadne urządzenia zasilające urządzenia przeciwpożarowe. Zasilacz wypełnia więc pewną lukę jako urządzenie służące do gwarantowanego zasilania napięciem 230 V (w zakresie dysponowanych mocy) urządzeń stosowanych w instalacjach systemów przeciwpożarowych.

Bibliografia

1. PN-HD 60364-5-56:2013 *Instalacje elektryczne w obiektach budowlanych. Dobór i montaż wyposażenia elektrycznego. Instalacje bezpieczeństwa.*
2. PN-EN 54-4:2001+A1:2004+A2:2007 *Systemy sygnalizacji pożarowej. Część 4: Zasilacze.*
3. PN-EN 12101-10:2007+AC:2007 *Systemy kontroli rozprzestrzeniania dymu i ciepła. Część 10: Zasilacze.*
4. Rozporządzenie MSWiA z dnia 20 czerwca 2007 r. *w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania* (Dz. U. z 2007 r. Nr 143, poz. 1002, zm. Dz. U. z 2010 r. Nr 85, poz. 553).
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 305/2011 z dnia 9 marca 2011 r. *ustanawiające zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych i uchylające dyrektywę Rady 89/106/EWG (Dziennik Urzędowy Unii Europejskiej L88).*
6. Instrukcja obsługi zasilaczy ZUP-230V (www.merawex.com.pl).

Dariusz Cygankiewicz
MERAWEX

Techniki pożarowych zabezpieczeń
obiektów zabytkowych i muzealnych

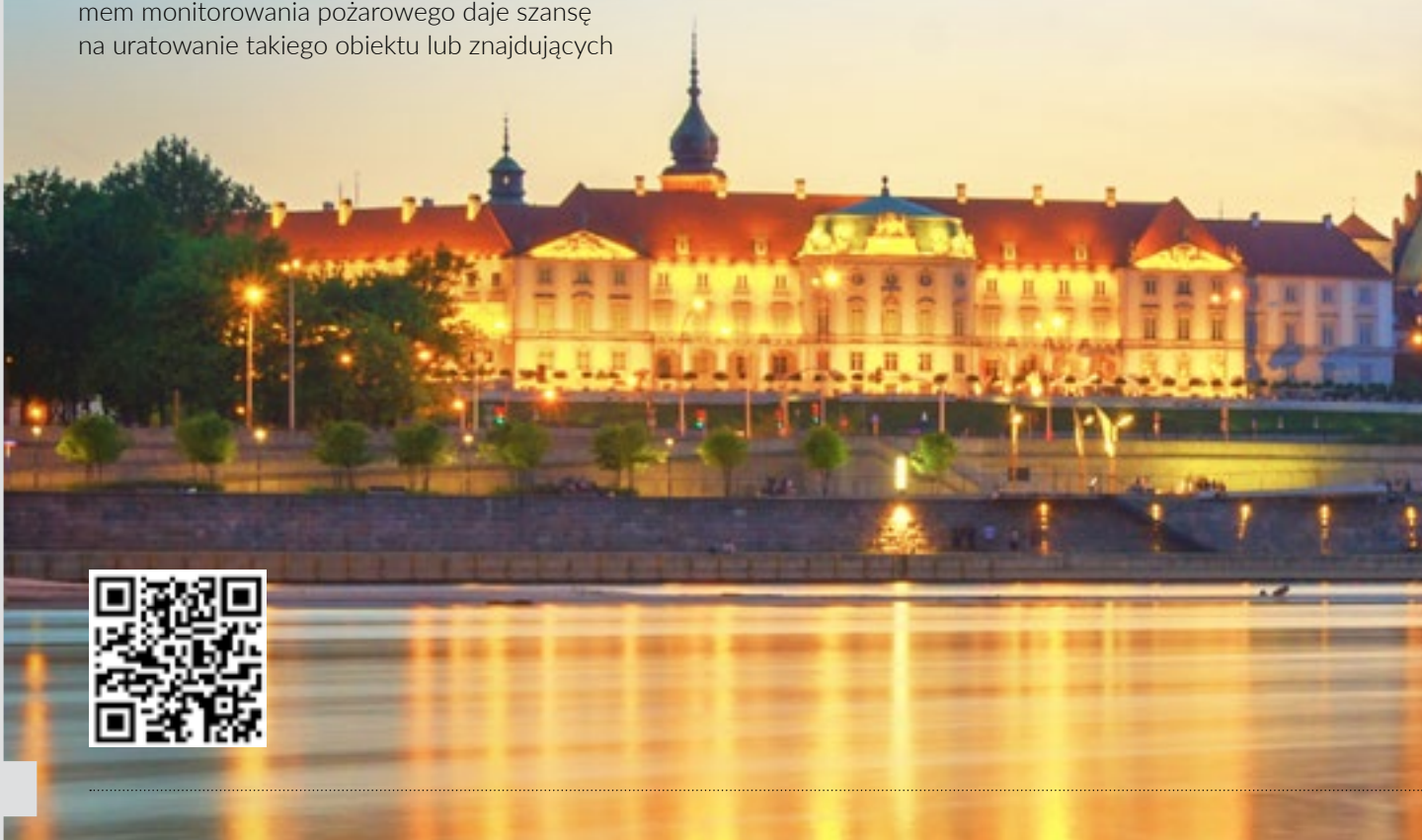
mgr inż. Józef Seweryn

Ochrona dziedzictwa narodowego nie jest na co dzień przedmiotem zainteresowania większości ludzi. Przypominają sobie o konieczności zabezpieczania zabytkowych obiektów i eksponatów dopiero wtedy, gdy destrukcji ulegnie kolejny z nich. Nie powinniśmy ograniczać się do zapewnienia wyłącznie tego, co narzucają przepisy. Warto wykorzystać najnowsze metody ochrony przeciwpożarowej

Podstawową formą ochrony jest wykonanie systemu sygnalizacji pożarowej sprzęgniętego z systemem monitorowania pożarowego. Z doświadczenia wynika jednak, że ograniczenie się do tego typu działania niestety nie wystarcza, a czasami wręcz szkodzi, jeżeli ma się w takim przypadku przekonanie o pełnym zabezpieczeniu pożarowym obiektu.

W przypadku wystąpienia zarzewia pożaru wewnątrz budynku dobrze wykonana instalacja systemu sygnalizacji pożarowej wraz z systemem monitorowania pożarowego daje szansę na uratowanie takiego obiektu lub znajdujących się w nim eksponatów. Musi być jednak spełnionych wiele warunków, takich jak bliskość straży pożarnej, dobry dojazd, odpowiednie warunki atmosferyczne itp.

Obecnie dostępne są detektory, które mogą bardzo wcześnie wykryć dym, temperaturę czy ogień. Zastosowanie mikroprocesorów i innych zaawansowanych elementów elektronicznych pozwala niezawodnie określić te parametry i odpowiednio wysterować urządzenia do gaszenia pożarów.



Wymienione sposoby ochrony zupełnie zawodzą w przypadku rozwiniętych pożarów wewnętrznych lub pożarów zewnętrznych, powstałych najczęściej na skutek wyładowań atmosferycznych bądź działań ludzkich, często celowych. Zastosowanie stałych urządzeń gaśniczych sterowanych przez systemy sygnalizacji pożarowej pozwala zdecydowanie podnieść poziom zabezpieczenia przed pożarami. Współczesna technika umożliwia skuteczne zabezpieczenie przed ogniem obiektów zabytkowych lub muzealnych, a jednocześnie nie ma znaczącego destrukcyjnego wpływu na wartość obiektu lub eksponatów. Jak wiemy, bardzo skutecznym środkiem gaśniczym jest woda, lecz ze względu na powodowanie znacznych strat popożarowych przez instalacje tryskaczowe i zraszaczowe jej stosowanie jest ograniczone. Zastosowanie gazowych urządzeń gaśniczych jest jak najbardziej wskazane, lecz niestety ograniczone do małych kubatur i, co istotne, są to urządzenia stosunkowo drogie. Do skutecznego gaszenia pożarów zarówno wewnątrz, jak i na zewnątrz obiektów stosuje się w ostatnich latach mgłę wodną. Mgła wodna doskonale nadaje się również do zabezpieczenia galerii muzealnych i innych muzealiów.

Obecnie znane są trzy techniki zabezpieczenia mgłą wodną:

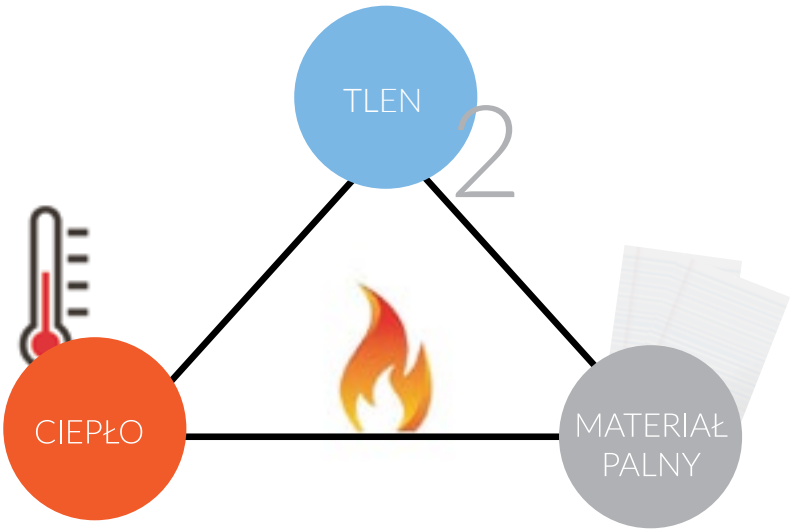
- zastosowanie urządzeń wytwarzających wysokociśnieniową mgłę wodną (powyżej 100 barów),
- zastosowanie urządzeń wytwarzających niskociśnieniową mgłę wodną (od 5 do 12 barów),
- zastosowanie urządzeń hybrydowych (mieszaniny wody i gazu).

Zastosowanie mgły wodnej pozwala w zasadzie wyeliminować problemy związane z doborem dużych pomp, zbiorników z zapasem wody gaśniczej i przekrojów rur, a także uniknąć dużych strat popożarowych związanych z zalaniem wodą gaśniczą pomieszczeń. Ma to oczywiście wpływ na koszty.

Systemy gaśnicze na bazie wody

Mgłowe systemy gaśnicze na bazie wody wykorzystują wodę w formie kropel. Krople są bardzo małe w przypadku systemów wysokociśnieniowych, a stosunkowo duże w systemach zalewowych lub tryskaczowych. Główne efekty zwalczania pożaru za pomocą wody (w zależności od rozmiarów kropel):

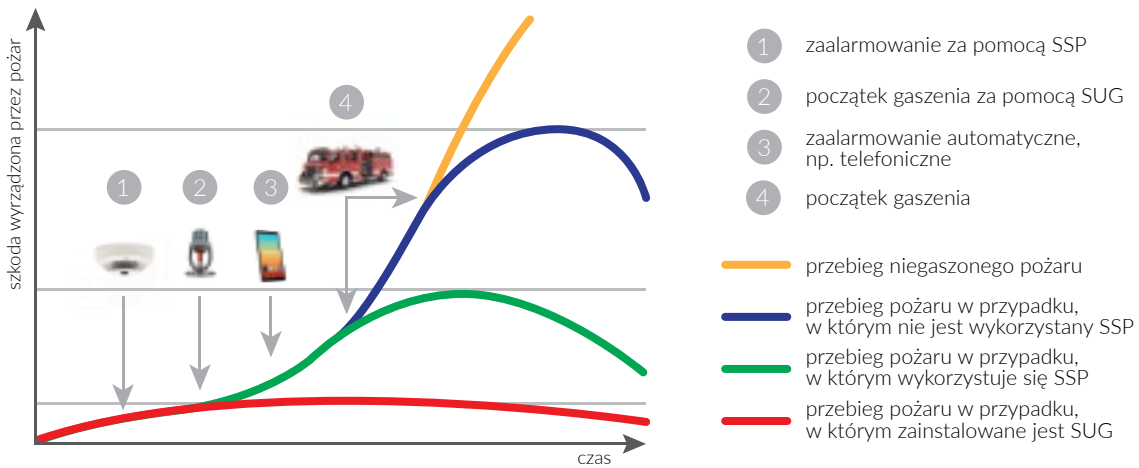
1. Dławienie pożaru. Podczas parowania wody jej objętość wzrasta 1640 razy, co prowadzi do redukcji zawartości tlenu w powietrzu przy źródle pożaru. W efekcie pożar jest dławiony, a przynajmniej tłumiony na skutek



Rys. 1. Trójkąt spalania (źródło: http://stankowa.osp.org.pl/pozar.html)

braku wystarczającej ilości tlenu potrzebnego do spalania. Uwaga: redukcja zawartości tlenu w powietrzu na skutek tworzenia się pary występuje jedynie w miejscach, gdzie temperatura jest bardzo wysoka, dlatego będzie występować w pobliżu pożaru, a nie na drogach ewakuacyjnych.

2. Efekt separacji. Kropelki wody znajdują się pomiędzy płomieniem i powierzchnią paliwa. Ograniczają one nagrzewanie się powierzchni paliwa na skutek promieniowania, skutecznie odbijając to promieniowanie. Dzięki temu zmniejsza się szybkość spalania oraz ciepło promieniowania w innych miejscach w tunelu. Zmniejsza to ryzyko rozprzestrzeniania się ognia. Efekt odbijania promieniowania zależy od wystarczającej liczby małych kropelek – skuteczność rośnie wraz ze zmniejszaniem rozmiarów kropelek.
3. Efekt tarczy. Jak opisano powyżej, kropelki wody redukują ciepło promieniowania, jakie dociera do obiektów w pobliżu pożaru w tunelu. Ten „efekt tarczy" pomaga zapobiegać rozprzestrzenianiu się pożaru i chronić ewakuujących się z tunelu ludzi i służby bezpieczeństwa próbujące dotrzeć do tunelu.
4. Chłodzenie. Na skutek rozbicia wody na kropelki tworzy się powierzchnia reakcji, przez którą absorbowane jest ciepło z pożaru. Na rozgrzanie jednego litra wody o temperaturze 20°C do temperatury 100°C potrzeba 335 kJ energii, a dodatkowe 2257 kJ jest potrzebnych do przetworzenia wody w parę. Woda jest więc środkiem gaśniczym o najwyższej znanej zdolności absorpcji ciepła. Im większa powierzchnia reakcji, co zależy od widma rozpylenia kropel, tym większy potencjalny efekt chłodzenia. Im mniejszy średni rozmiar kropel, tym większy efekt chłodzenia. Ten efekt dotyczy powietrza i gazów dookoła pożaru, a nie samego pożaru, w którego przypadku decydującym czynnikiem jest powierzchnia



Rys. 2. Szkoda wyrządzona przez pożar w zależności od momentu jego wykrycia

nim objęta. Chłodzenie jest bardziej wydajne, jeśli kropelki znajdują się w powietrzu. Mniejsze krople, które spadają wolniej niż większe, będą skuteczniej chłodzić otoczenie w tunelu.

Wysokociśnieniowa mgła wodna

Systemy wytwarzające wysokociśnieniową mgłę wodną pozwalają skutecznie zabezpieczyć obiekty zabytkowe i muzealne, ale są dość drogie, dlatego stosuje się je w obiektach o szczególnym znaczeniu. Warto wspomnieć, że takie rozwią-

Fot. 1. Przykład zastosowania wysokociśnieniowej mgły wodnej (sanktuarium „Maria Śnieżna" na Górze Iglicznej)

Fot. 2. Przykład zastosowania wysokociśnieniowej mgły wodnej (sanktuarium „Maria Śnieżna" na Górze Iglicznej)

zanie zastosowano w kościele Marii Śnieżnej na Górze Iglicznej w Sudetach, jak również na Kasprowym Wierchu, przy okazji modernizacji kolejki, oraz w budynku Międzynarodowego Centrum Kultury na Rynku Głównym w Krakowie.

Fot. 3. Przykład zastosowania wysokociśnieniowej mgły wodnej (kolejka na Kasprowy Wierch)

Wysokociśnieniowa mgła wodna była pierwotnie stosowana do zabezpieczenia statków morskich i stopniowo wprowadzana do zabezpieczeń obiektów lądowych. Ma ona wiele zalet, takich jak mała ilość wody potrzebnej do gaszenia pożarów (dzięki temu szkody powstałe na skutek pożaru są mniejsze), bardzo duża efektywność gaśnicza, niewielkie koszty medium gaśniczego, jakim jest woda, wielość zastosowań, a także jedną zasadniczą wadę, jaką jest koszt wykonania instalacji. Potrzeba stosowania osprzętu odpornego na wysokie ciśnienie (do 200 barów), wykonanego ze stali nierdzewnej, oraz zastosowanie specjalnych pomp wysokociśnieniowych sprawia, że systemy wytwarzające wysokociśnieniową mgłę wodną są drogie – czasem kilkakrotnie droższe od innych. Z tego powodu opracowano podobne instalacje gaśnicze wykorzystujące do gaszenia mgłę wodną, o podobnych cechach użytkowych, ale tańsze. W Polsce została opracowana technika gaszenia mgłą wodną pod niskim ciśnieniem, która, mając możliwości gaśnicze podobne jak wysokociśnieniowa mgła wodna, jest od niej znacznie tańsza. Technika ta zostanie zaprezentowana w kolejnej części materiału.

mgr inż. Józef Seweryn
Ośrodek Badawczo-Szkoleniowy Techniki Pożarowej

Systemy sygnalizacji pożarowej
w serwerowniach (część 4)

mgr inż. Jerzy Ciszewski

W pierwszej części artykułu (*Zabezpieczenia* nr 4/2017) wspomniałem, jak ważne jest zabezpieczenie serwerowni. W części drugiej (nr 5/2017) opisałem podstawowe źródła zagrożeń pożarowych dotyczących serwerowni, scharakteryzowałem pożary oraz przedstawiłem kwalifikację pożarową obiektu. W części trzeciej (nr 6/2017) opisałem techniki wykrywania pożaru w serwerowniach. Niniejsza część dotyczy ochrony obiektów, od których zależy właściwe zasilanie serwerowni w energię – akumulatorni, nastawni, rozdzielni i stacji transformatorowych

Jak napisałem w poprzednich artykułach, obiekty serwerowni wymagają pewnego, praktycznie bezprzerwowego źródła zasilania. W związku z tym w okresie, w którym nie ma zasilania podstawowego, uruchamiane są zespoły prądotwórcze, do których odnoszą się bardzo wysokie wymagania eksploatacyjne dotyczące urządzeń klasy G3 (określonej w normie PN-ISO8528-1). Zespół prądotwórczy powinien być odpowiednio dobrany do rodzajów obciążenia, powinien być zsynchronizowany z ogólną siecią zasilającą i mieć zapas paliwa wystarczający na 30 h nieprzerwanej pracy (wymaganie dotyczące instalacji przeciwpożarowych w obiekcie).

W czasie, w którym dokonuje się wymaganych przełączeń i uruchamia zespoły prądotwórcze, energia elektryczna jest pobierana z baterii akumulatorów kwasowych, a następnie przetwarzana za pomocą systemów falowników na wymagane napięcie. Odpowiednio dobrana pojemność baterii akumulatorów pozwala na podtrzymanie zasilania najważniejszych obiektów serwerowni przez kilkadziesiąt minut.

Akumulatornia

Wymagania dotyczące bezpieczeństwa pracy i instalowania akumulatorów są zawarte w normie PN-EN62485-3:2014. W praktyce należy przyjąć, że ładowanie akumulatorów kwasowych, nawet żelowych lub AGM, może wytworzyć

Fot. 1. Widok czujki gazu zainstalowanej pod stropem akumulatorni

mieszaninę wybuchową wskutek wydzielania się wodoru. Dolna granica wybuchowości dla wodoru wynosi 4%. Ilość wytwarzanego w tym procesie wodoru jest zależna od liczby i typu ogniw w bateriach, a także od parametrów pracy systemu ładowania akumulatorów. Podstawowym warunkiem bezpieczeństwa jest zastosowanie odpowiednio wydajnej wentylacji obniżającej koncentrację wodoru, chłodzącej ogniwa, a także usuwającej skutki mogącego wystąpić przeładowania ogniw. Oczywiście wymagany jest również system wykrywania niebezpiecznych stężeń tego gazu. Dlatego w pobliżu stropu powinny być zainstalowane detektory, tak jak na fot. 1.

Warunki środowiskowe, występujące zagrożenia
Środowisko korozyjne jest w przypadku zastosowania akumulatorów o tradycyjnej budowie. W normalnych warunkach normalnych nie ma silnej wentylacji. Temperatura jest większa niż 0°C. Źródłem pożaru może być niesprawna instalacja elektryczna.

Sposób nadzoru
Pomieszczenie należy nadzorować za pomocą rozproszeniowych czujek optycznych przy założeniu zasięgu 6,2 m (zgodnie z Fpr CEN/TS54-14:2015). Czujki powinny być rozmieszczone z uwzględnieniem sposobu wentylacji pomieszczenia. Na zewnątrz, nad drzwiami pomieszczenia, powinien być wyprowadzony wskaźnik zadziałania.

Nastawnie, rozdzielnie niskiego napięcia, pomieszczenie z falownikami

Warunki środowiskowe, występujące zagrożenia
W nastawni, rozdzielni niskiego napięcia lub pomieszczeniu z falownikami, w szeregach znajdu-

Fot. 2. Pomieszczenie z aparaturą kontrolną

jących się pod ścianami szaf, zainstalowana jest aparatura elektryczna służąca do rozdziału energii elektrycznej i sterowania elementami rozdzielni. Przewidywana wczesna faza pożaru to rozkład termiczny oraz tlenie się izolacji aparatury elek-

trycznej lub elektronicznej. Istnieje możliwość wystąpienia pożaru płomieniowego w przypadku wyładowań łukowych. Pomieszczenie jest suche. Nie ma silnej wymiany powietrza w przestrzeni głównej oraz w przestrzeni podpodłogowej (<10 wymian/h, v<10 m/s). Środowisko nie zagraża powstawaniem korozji. Obudowy szaf aparaturowych silnie ograniczają możliwość

Fot. 3. Oznaczenia miejsca instalowania czujek

wskazania miejsca wystąpienia zagrożenia pożarem. Powolna wymiana powietrza w szafie także utrudnia wykrycie pożaru z wymaganą czułością.

Nadzór pomieszczenia

Do nadzoru pomieszczenia należy zastosować umieszczone na stropie punktowe czujki pożarowe, dymowe, optyczne rozproszeniowe, pracujące przy długości fali promieniowania wynoszącej ok. 400–470 nm. Maksymalny zasięg pojedynczej czujki nie powinien przekraczać 6,2 m wg Fpr CEN/TS54-14:2015 (fot. 2).

Przestrzeń podpodłogowa, przestrzeń międzystropowa

Przestrzeń podpodłogowa i przestrzeń międzystropowa jest nadzorowana za pomocą optycznych czujek rozproszeniowych. Jeżeli przestrzeń podpodłogowa występuje pod całym pomieszczeniem, to powierzchnia objęta dozorem przez czujkę powinna być dwukrotnie mniejsza niż powierzchnia dozorowania przyjmowana dla czujek instalowanych na stropie. Jeżeli kable są rozprowadzane tylko w duktach kablowych pod szafami, to czujki należy rozmieszczać wzdłuż duktów co 5 m (wg Fpr CEN/TS54-14:2015).

Instalując czujki w przestrzeniach międzystropowych oraz podpodłogowych, należy pamiętać o oznakowaniu miejsc instalacji, a także o zastosowaniu wskaźników zadziałania niezależnie od ewentualnego adresowania elementów liniowych zastosowanego systemu wykrywania pożaru. Na fot. 3 pokazano przykładowe oznakowanie.

Nadzór szaf

W zależności od tego, czy zastosowane szafy są wyposażone w indywidualny system wymuszonej wentylacji, należy dobrać skuteczny sposób ich nadzoru.

Jeżeli obudowa urządzenia (szafa) ma otwory wentylacyjne (a także wewnętrzny system wentylacyjny), istnieje możliwość dozorowania urządzenia poprzez kontrolę powietrza wyrzucanego na zewnątrz obudowy przez wentylator. W pomieszczeniach o długości większej niż 10 m, z dużą liczbą szeregowo ustawionych szaf można nad każdym szeregiem zastosować czujkę liniową umieszczoną w odległości nieprzekraczającej jednego metra od szafy. Takie rozwiązanie umożliwia

zrezygnowanie z nadzorowania pozostałej części pomieszczenia za pomocą czujek punktowych. Jeżeli czujki punktowe są zainstalowane na stropie w odległości nie większej niż jeden metr od szafy, to powierzchnia nadzorowana przez czujkę nie powinna przekraczać 15 m^2 (wg CRP. Electronic data processing installations and similar facilities. Planning of fire detection systems. Doc. e592a. Edition 02.92. CERBERUS).

Jeżeli szafy nie są wyposażone w systemy wentylacji wymuszonej, to praktycznie nie jest możliwe skuteczne wykrycie pożaru aparatury elektrycznej zainstalowanej w szafie. Jedynym prawidłowym i skutecznym rozwiązaniem jest zastosowanie systemu zasysającego nadzorującego poszczególne szafy za pomocą rurek próbkujących.

Jeżeli w górnej części szafy jest otwór wentylacyjny bez wentylatora, to skuteczny nadzór zapewni czujka zasysająca zainstalowana na stropie, nad szeregiem szaf. Jednocześnie istnieje możliwość nadzoru pozostałej części pomieszczenia – pod warunkiem, że odległość między punktem zasysającym a dowolnym miejscem na stropie nie przekracza 6,2 m.

Zabezpieczenie stacji transformatorowych

Zgodnie z §182 rozporządzenia Ministra Infrastruktury w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie, pomieszczenie stacji transformatorowej może być usytuowane w budynku o innym przeznaczeniu, jeżeli spełnione są warunki określone w §96 tego rozporządzenia oraz zostanie zachowana pozioma i pionowa odległość od pomieszczeń przystosowanych do stałego pobytu ludzi wynosząca co najmniej 2,8 m, a ściany i stropy będą stanowiły oddzielenia przeciwpożarowe i będą miały zabezpieczenia przed przedostawaniem się cieczy i gazów.

Odpowiednio zaprojektowane pomieszczenia mogą stanowić stacje transformatorowe, w których instalowane są transformatory olejowe, żywiczne, suche. W zależności od zastosowanego transformatora mogą występować różne zagrożenia pożarowe.

W przypadku transformatora olejowego głównym problemem jest zawarta w kadzi transfor-

matora duża ilość oleju, który ma bardzo dobre właściwości izolacyjne i bardzo dobrze odprowadza ciepło, ale ma niską temperaturę zapłonu. W przypadku wyładowania łukowego między zwojami transformatora nastąpi intensywny rozkład termiczny, powstaną palne gazy powodujące silny wzrost ciśnienia w kadzi, a w konsekwencji nastąpi wyrzut gorącego oleju na zewnątrz.

Suche transformatory żywiczne, w których uzwojenia są zalewane lub impregnowane żywicą epoksydową, są przeznaczone przede wszystkim do zastosowań wnętrzowych. Charakteryzują się odpornością na korozyjność środowiska E2, odpornością na szoki termiczne C2 i odpornością ogniową F1, a więc są trudno zapalne lub niepalne. W czasie palenia się w małym stopniu wydzielają się trujące gazy.

Problemy związane z zastosowaniem czujek pożarowych

- utrudniony dostęp do punktowych czujek pożarowych w celu ich czyszczenia i konserwacji ze względu na występujące wysokie napięcie,
- silne zakłócenia elektromagnetyczne podczas przeprowadzania operacji załączania i wyłączania instalacji,
- zagrożenie dla środowiska w przypadku uwolnienia czynnika chłodzącego transformator (dotyczy to przede wszystkim transformatorów olejowych).

Fot. 4. Transformator suchy nieskutecznie nadzorowany za pomocą uszkodzonego, zwisającego systemu zasysającego

Nadzorowanie komory transformatora – przykładowe rozwiązania

Do nadzoru może być wykorzystany system zasysający. W takim przypadku rury z otworami próbkującymi powinny zostać zainstalowane bezpośrednio nad transformatorem. Transformator wytwarza duże ilości ciepła. Dym występujący na początku rozkładu termicznego jest szybko unoszony w kierunku otworów próbkujących. Zainstalowana na zewnątrz pomieszczenia jednostka pomiarowa czujki umożliwia łatwy dostęp w celu serwisowania. System zasysania ma bardzo małą podatność na wpływ zakłóceń elektromagnetycznych. W przypadku występowania różnic ciśnień w pomieszczeniach należy wykonać rurowe połączenie wyrównawcze. W żadnym razie nie należy stosować rurek przewodzących, metalowych, charakteryzujących się małą podatnością na wyboczenia w przypadku podwyższonej temperatury. Na fot. 4 pokazano przykładowe zabezpieczenie transformatora suchego za pomocą systemu zasysającego, w którym prawidłowo zastosowano nieprzewodzące rurki z tworzywa sztucznego, jednak zbyt mała liczba elementów przymocowujących rurki do stropu spowodowała uszkodzenie instalacji.

Do nadzoru może służyć zespolona czujka liniowa na światło przechodzące. Takie rozwiązanie umożliwia odpowiednie serwisowanie instalacji w przypadku, w którym długość (lub szerokość) pomieszczenia jest większa niż 10 m.

Niezależnie od rodzaju zastosowanych czujek w pomieszczeniu powinien znajdować się przycisk pożarowy ROP umieszczony w miejscu umożliwiającym bezpieczne wykonywanie czynności serwisowych. W przypadku komór transformatorowych przycisk pożarowy należy zainstalować na zewnątrz.

Do skutecznej ochrony obiektów, w których znajdują się źródła zasilania, potrzebne są samoczynne systemy gaszenia (podobnie jak w przypadku przestrzeni roboczej w serwerowni). Do gaszenia powinno się stosować gazowe środki gaśnicze lub mgłę wodną.

Aby zastosować samoczynne systemy gaśnicze, należy zadbać o prawidłową organizację alarmowania. W przypadku czujek punktowych, które umożliwiają precyzyjną lokalizację wykrytego

alarmu, niezbędne jest zapewnienie koincydencji, czyli równoczesnego pobudzenia co najmniej dwóch czujek umieszczonych w sąsiedztwie tak, by uruchomienie systemu gaśniczego następowało w wyniku zadziałania czujek, a nie przypadkowego impulsu. W przypadku zastosowania drugiego, równoległego systemu zasysającego należy ustawić różne poziomy czułości w taki sposób, aby system równoległy potwierdzał wykrycie pożaru. Poza tym w systemach samoczynnych należy zastosować przyciski uruchamiające procedurę gaszenia, przyciski blokujące procedurę gaszenia, a w przypadku gaszenia wodą należy zapewnić jej odpływ do studzienki.

Podsumowanie

Nie sposób w krótkim, czteroczęściowym artykule opisać uniwersalny sposób projektowania systemu wykrywania pożaru w obiektach serwerowni. Podano więc jedynie bardzo ogólne zasady i wskazówki dotyczące postępowania w trakcie projektowania. Każdy z wymienionych wcześniej obiektów powinien być dokładnie sprawdzony pod kątem:

- panujących warunków środowiskowych, a więc wibracji, drgań, wahań temperatur, przepływów powietrza, różnic ciśnień występujących w poszczególnych pomieszczeniach i częściach pomieszczeń,
- możliwości wystąpienia oddziaływań elektromagnetycznych (przewodzonych i polowych),
- występowania nadmiernej wilgoci lub atmosfery grożącej korozją,
- możliwości zakłócania przez instalację sygnalizacji pożarowej prawidłowego działania aparatury pracującej w obiekcie,
- konfiguracji architektonicznej poszczególnych pomieszczeń.

Mając potrzebne informacje, można dobrać właściwy sposób nadzoru poszczególnych obiektów na podstawie opracowanego scenariusza pożarowego. Dominującym systemem wykrywania pożaru w głównych obiektach serwerowni jest niewątpliwie system zasysający. Jego najważniejsze cechy to bardzo wysoka czułość i zarazem – w przypadku systemów wykorzystujących kilka długości fal promieniowania – duża odporność na czynniki środowiskowe, np. kurz, zapylenie, mgłę i parę wodną. Główną wadą jest brak możliwości określenia miejsca zagrożonego pożarem. Projektant musi więc odpowiednio zaprojektować orurowanie i zastosowanie niestandardowego sposobu alarmowania.

mgr inż. Jerzy Ciszewski
IBP NODEX

Bibliografia

1. R. Chybowski, *Zabezpieczenia przeciwpożarowe transformatorów energetycznych*, *elektro.info* nr 10/2010.
2. Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. *w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie* (Dz. U. z 2002 r., nr 75, poz. 690 z późn. zm.).
3. *CRP. Electronic data processing installations and similar facilities. Planning of fire detection systems.* Doc. E592A Edition 02.92. CERBERUS.
4. *CRP. Telecommunications equipment. Planning of fire detection systems.* Doc. E803. Edition 12.90. CERBERUS.
5. Applications Guide. *Aspirating Smoke Detection. FAAST. System Sensor.* 800/736-7672. 2015.
6. FHSD700. *Air Sampling Pipe Networks. Installation and design manual.* GE Security. Version 1-1/January 2005.
7. BS 6266:1992 (i następne). *Code of practice for fire protection for electronic data processing installations.*
8. PN-ISO 8528-1. *Zespoły prądotwórcze prądu przemiennego napędzane silnikiem tłokowym. Zastosowanie, klasyfikacja i wymagania eksploatacyjne.*
9. PN-EN 62485-3:2014. *Wymagania bezpieczeństwa dotyczące akumulatorów i ich instalowania. Część 3: Akumulatory trakcyjne.*
10. PKN-CEN/TS54-14:2004. *Systemy sygnalizacji pożarowej. Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji.*
11. FprCEN/TS54-14:2015. *Systemy sygnalizacji pożarowej. Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji.*

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

PROJEKTUJEMY
zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

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

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

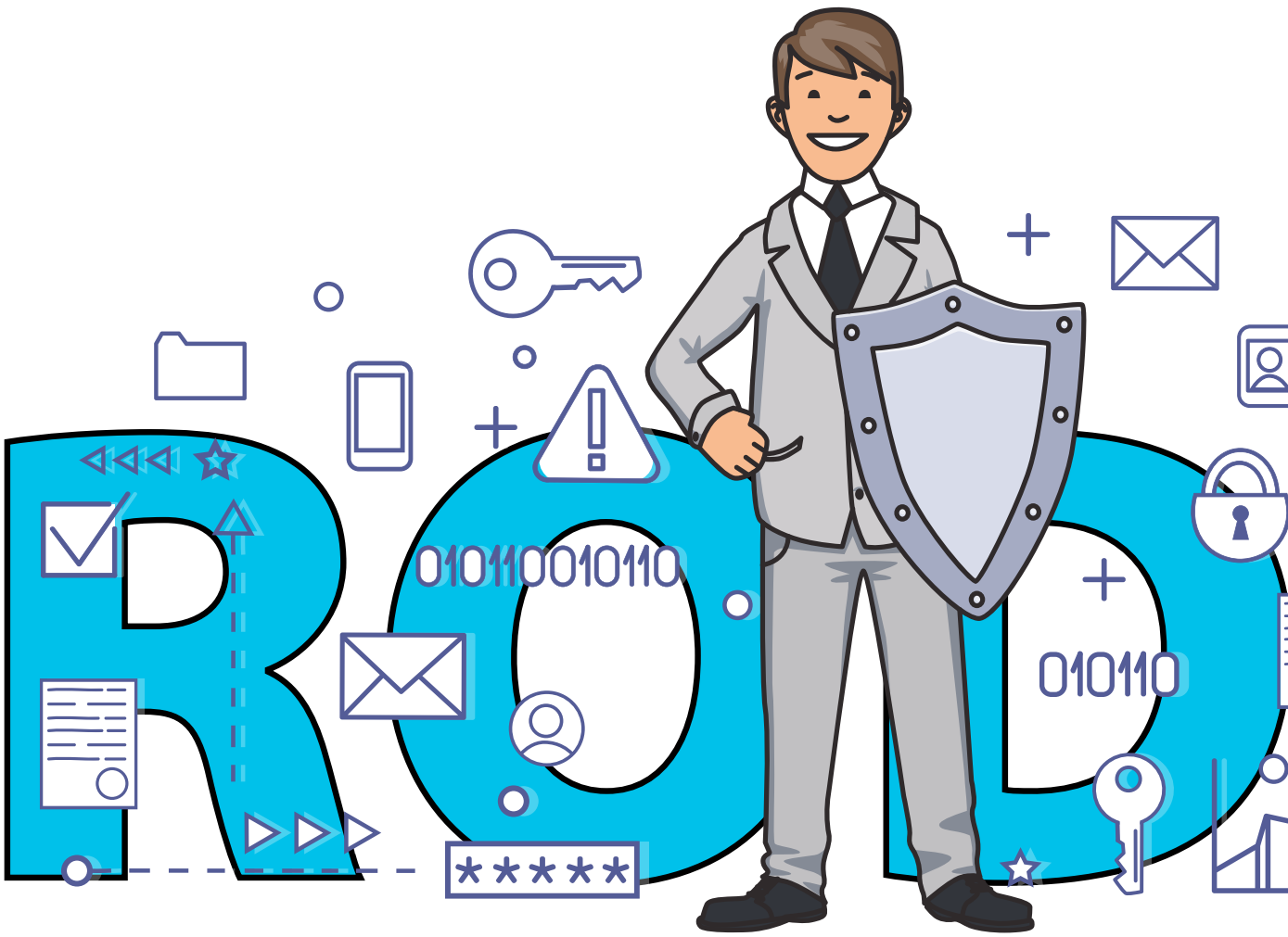
SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A. (dawniej Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.)
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

RODO w branży ochrony

Cezary Młotek

25 maja 2018 roku wchodzi w życie Rozporządzenie o Ochronie Danych Osobowych (RODO), czyli kompleksowa regulacja na poziomie unijnym, która dotyczy ochrony danych osobowych. Już od dawna jesteśmy informowani o konieczności uwzględnienia nowych wymogów. Wiele osób zastanawia się, czy jest już za późno na przygotowanie się na zmiany. Moim zdaniem nie, mimo iż w mediach już od prawie pół roku ogłasza się, że to już ostatnia chwila i straszy się wielomilionowymi karami



Biorąc pod uwagę to, że przedsiębiorcy z branży ochrony (jak z każdej innej) są nagabywani przez rozmaite podmioty gospodarcze oferujące jedyną słuszną (i dość kosztowną) opcję wdrożenia zmian, pewnie zaczynasz się zastanawiać, czy dotyczy to również Twojego przedsiębiorstwa. Czy coś mi w ogóle grozi? A może wszyscy wokół to naciągacze i nie muszę nic robić i niczym się przejmować? Takie pytania narzucają się same.

Czy w ochronie osób i mienia w ogóle przetwarza się jakiekolwiek dane osobowe? Tak, dane osobowe w agencji ochrony są przetwarzane cały czas, niezależnie od tego, czy Twoje przedsiębiorstwo świadczy usługi z zakresu ochrony bezpośredniej czy z zakresu zabezpieczenia technicznego. Podam kilka przykładów. Pracownicy ochrony na posterunkach w biurowcu mają obowiązek legitymować wchodzących interesantów. Zażądał tego klient w umowie. Spisują imię, nazwisko, adres, serię i numer dowodu osobistego. Co robią? Przetwarzają dane osobowe. Agencja ochrony monitoruje bezpieczeństwo obiektu za pomocą kilku kamer znajdujących się w kluczowych miejscach. Nagrywa wszystkich wchodzących, rejestruje ich wizerunki i, co więcej, przechowuje nagrania przez minimum trzy miesiące. Co robi? Przetwarza dane osobowe. Przedsiębiorca zatrudnia kilkunastu pracowników ochrony rozmieszczonych w kilku obiektach. Aby zawrzeć z nimi umowy, ubezpieczyć ich w ZUS-ie i odprowadzić za nich podatki, wymaga podania niezbędnych informacji w kwestionariuszu osobowym. Musi, ma prawny obowiązek, ale co w ten sposób robi? Przetwarza dane osobowe.

Tak więc, zajmując się ochroną, przetwarzasz dane osobowe – niezależnie od rodzaju świadczonych usług. Musisz zatem chronić te dane przed osobami nieuprawnionymi, przed ich wyciekiem. Temu właśnie ma służyć RODO.

Przejdźmy do kolejnej istotnej kwestii. Czy należy obawiać się milionowych kar? Teoretycznie tak. Kary są określone w rozporządzeniu i są wysokie, jednak przepisy, które o nich mówią, określają stawki maksymalne, a nie są w nich podane stawki minimalne. Oznacza to, że kara najprawdopodobniej będzie znacznie niższa niż podana – uzależniona od stopnia winy i wielu innych czynników.

Warto dodać, że niedawno rozmawiałem z inspektorem zajmującym się GIODO i dowiedziałem się, że obecnie na całą Polskę, czyli na 38 milionów obywateli, przypada osiemnastu takich inspektorów...

Czy RODO dotyczy branży ochrony? Tak, dotyczy. Czy musisz wprowadzić zmiany, aby uzyskać zgodność ze standardami wskazanymi w RODO? Tak, powinieneś. Czy już 26 maja do Twoich drzwi zapuka inspektor i zapłacisz w związku z tym milionową karę? Jest to prawdopodobne, ale tak samo jak to, że wygrasz w totka lub trafi Cię piorun. Nie wpadaj zatem w panikę i po prostu zastanów się nad dotychczasowym poziomem ochrony danych osobowych w swoim przedsiębiorstwie. Zastanów się, co powinieneś poprawić. RODO nie daje gotowych rozwiązań – nie określa, co musisz zrobić, aby się dostosować. Określono w nim prawa, obowiązki i sankcje, ale wszystkie poziomy zabezpieczeń i możliwą dokumentację musisz dobrać sam. Jest to podejście

oparte na ryzyku. W poradniku chcę wskazać niezbędne moim zdaniem minimum, o którym warto pomyśleć w agencji ochrony.

Najpierw zastanów się, jakiego rodzaju dane osobowe przetwarzasz w ramach działalności swojego przedsiębiorstwa i w jakim celu to robisz. Z mojego dotychczasowego doświadczenia wynika, że najczęściej przetwarza się następujące dane osobowe:

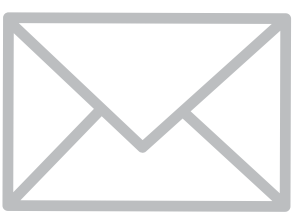
- dane własnych pracowników i zleceniobiorców (na potrzeby zatrudnienia),
- dane kontrahenta i jego pracowników (w celu realizacji umowy),
- dane osób legitymowanych przez ochronę fizyczną (w celu realizacji umowy oraz zapewnienia bezpieczeństwa w chronionym obiekcie),
- dane w postaci wizerunku danej osoby utrwalone na nagraniach z systemu nadzoru wizyjnego (w celu realizacji umowy oraz zapewnienia bezpieczeństwa w monitorowanym obiekcie).

Zbieranie tych danych jest konieczne. Jeśli nie dysponujesz danymi pracowników i zleceniobiorców, nie możesz ich zarejestrować w ZUS-ie, NFZ-cie i US-ie. Jeśli brak Ci danych pracowników klienta, możesz mieć problemy z kontaktowaniem się z nimi. Z kolei legitymowanie osób wchodzących do obiektu bądź zastosowanie kamer i przechowywanie nagrań przez wiele miesięcy jest częstym wymogiem zawartym w umowie, wymaganiem klienta mającym na celu zapewnienie określonego poziomu bezpieczeństwa. Jeśli się nie zgodzisz, to w zasadzie możesz pakować manatki.

Zastanów się, kto ma dostęp do danych osobowych. W ten sposób ograniczysz do niezbędnego minimum liczbę osób lub podmiotów, które go mają, i uniemożliwisz dostęp tym spośród nich, które go nie potrzebują do wykonywania swoich obowiązków.

Zweryfikuj także sposób przechowywania danych osobowych w swoim przedsiębiorstwie. Trzymasz je na zewnętrznym serwerze czy w pomieszczeniu serwerowym gdzieś na zapleczu? A może wystarcza Ci jeden komputer? Jak zabezpieczasz dostęp do komputerów? Jeśli gromadzisz dokumenty w formie papierowej, to czy przechowujesz dane w szafie zamykanej na klucz, w szafie pancernej lub sejfie? Zastanów się nad sposobem przechowywania tych danych. Możesz usprawnić wiele rzeczy, zwłaszcza jeśli dotychczas nie przywiązywałeś wagi do szczegółów.

Zastanów się nad ewentualnym powołaniem inspektora ochrony danych. Będzie on pełnił podobne funkcje jak dotychczasowi administratorzy bezpieczeństwa informacji, ale nie znaczy to, że wszyscy tacy administratorzy staną się automatycznie inspektorami. Inspektor powinien posiadać odpowiednie kwalifikacje zawodowe, ale także wiedzę praktyczną. Może być zatrudniony w firmie albo działać w ramach outsourcingu na podstawie umowy o świadczenie usług. W przypadku działalności w branży ochrony osób i mienia z reguły nie ma obowiązku powoływania inspektora, jednak większe firmy powinny go zatrudniać nie tylko ze względu na przepisy. W końcu wraz z rozwojem przedsiębiorstwa prędzej czy później może pojawić się jakiś problem z ochroną danych osobowych.



Kiedy już przeanalizujesz wszystko, co zostało wyżej zasygnalizowane, pora pomyśleć o formalnościach, czyli o niezbędnej dokumentacji. Na początek przygotuj w formie dokumentu politykę bezpieczeństwa, czyli wewnętrzne zasady przetwarzania oraz ochrony danych osobowych. W takim dokumencie powinny być przed-

stawione m.in. informacje o tym, gdzie i w jaki sposób przechowywane są dane, zasady przesyłania danych osobowych i sposoby zabezpieczania danych (wymóg stosowania loginów i haseł, konieczność zabezpieczania danych przesyłanych elektronicznie, zasady instalowania oprogramowania na komputerach, wymóg zastosowania programów zabezpieczających i ich aktualizacji, zasady dotyczące podłączania urządzeń zewnętrznych, zasady przechowywania dokumentacji papierowej). Należy pamiętać o tym, że że polityka bezpieczeństwa nie może być opublikowana na stronie internetowej! Nie pomyl jej z polityką prywatności. Opis zasad bezpieczeństwa w formie dokumentu firmowego musi być dostępny wyłącznie dla pracowników, tzn. tylko dla osób z wewnątrz.

Kolejnym koniecznym dokumentem jest umowa dotycząca powierzenia danych osobowych. Jeśli na przykład trzymasz dane firmowe na serwerach firmy hostingowej, powinieneś jako administrator danych osobowych zawrzeć z tym podmiotem umowę, która określi zasady powierzania danych osobowych, same kategorie powierzanych danych, cel ich powierzania, a także zasady ich ochrony. Podobne umowy zawrzyj ze wszystkimi swoimi podwykonawcami.

Umowy dotyczące powierzenia danych osobowych powinieneś zawrzeć także ze wszystkimi kontrahentami, dla których wykonujesz usługi ochrony fizycznej bądź monitorowania. Zapewne część klientów przekazała Ci już do podpisania swoje wzory umów. Bardzo dobrze – masz jedną sprawę z głowy. Gorsze jest to, że ze wszystkimi pozostałymi musisz zawrzeć podobne umowy.

Przyjmij od swoich pracowników i zleceniobiorców oświadczenia dotyczące przetwarzania danych osobowych. Musisz ich pisemnie poinformować o tym, jakie ich dane osobowe przetwarzasz, w jakim celu i przez jaki okres, a także o wszelkich przysługujących im prawach związanych z przetwarzaniem danych osobowych. Osobnym oświadczeniem, które należy przyjąć, powinno być oświadczenie o zapoznaniu się z zasadami bezpieczeństwa – wszak pracownik musi mieć świadomość, że i on ma pewne obowiązki związane z wykorzystywaniem cudzych danych osobowych w swojej pracy.

Rekomenduję prowadzenie rejestru czynności związanych z przetwarzaniem danych. Nie jest on obowiązkowy w przypadku przedsiębiorców zatrudniających mniej niż 250 osób, chyba że przetwarzanie może naruszać prawa osób, których dane dotyczą, obejmuje szczególne kategorie danych lub dane dotyczące wyroków skazujących, lub nie ma charakteru sporadycznego. Moim zdaniem będziesz musiał rejestrować co najmniej czynności związane z przetwarzaniem danych zatrudnianych przez siebie osób, niezależnie od liczby osób zatrudnionych.

Reasumując, powinieneś zadbać o:
- politykę bezpieczeństwa,
- umowy dotyczące powierzenia danych osobowych,
- oświadczenie o prawach pracownika wynikających z RODO,
- oświadczenie o zachowaniu poufności,
- rejestr czynności związanych z przetwarzaniem danych.

Potrzebnych w związku z wejściem w życie RODO dokumentów może być znacznie więcej. Zależy to od zasad obowiązujących w przedsiębiorstwie. Nic nie stoi na przeszkodzie, abyś był lepiej przygotowany. Jeśli chcesz osiągnąć przynajmniej niezbędne minimum, to postaraj się skorzystać z podanych przeze mnie wskazówek.

Oczywiście ten poradnik nie wyczerpuje tematu. Unikam zamieszczania w nim skomplikowanych definicji ustawowych czy szczegółowych wyjaśnień. O tym możesz przeczytać w wielu publikacjach dostępnych w Internecie. Wolałem zwrócić uwagę na konkrety. Mam nadzieję, że moje porady będą pomocne.

Cezary Młotek
radca prawny
expert PZPO

Opracowanie: Redakcja

Polski Związek Pracodawców Ochrona
1992

Nasobny wizyjny system dozorowy
marki NOVUS

Patryk Gańko

Nasobne systemy telewizji użytkowej są rekomendowane przede wszystkim policji i Straży Miejskiej. Wynika to z konieczności rejestrowania interwencji, które bardzo często są przedmiotem kontrowersji i skarg, a także sporów sądowych. Wydanie wiarygodnej opinii w takich przypadkach bywało niemożliwe, gdyż nie było możliwości bezstronnego odtworzenia jego przebiegu i wszystko sprowadzało się do przedstawienia przez obie strony swoich wersji wydarzeń. Systemy nasobne mogą również być stosowane przez inne grupy zawodowe, które muszą dokumentować swoje czynności, np. przez pracowników agencji ochrony, pogotowia ratunkowego i straży pożarnej, przez osoby odpowiedzialne za prowadzenie imprez masowych czy ochronę konwojów, a także osoby zagrożone przemocą i agresją w kontakcie z petentami, np. przez pracowników socjalnych. Spektrum grup społecznych mogących z korzyścią stosować takie rozwiązania stale się powiększa. Dotyczy to również kierowców jednośladów dokumentujących wykroczenia drogowe innych użytkowników dróg

W podstawowej konfiguracji system tworzą kamery nasobne wraz z dodatkowymi akcesoriami. Każda z tych kamer ma niewielkie rozmiary, masę 200 g i jest wyposażona w uchwyt nośny. Kamery mają klasę szczelności IP67 i mogą pracować w temperaturach od -30°C do 70°C. Można je wykorzystać w każdych warunkach pogodowych. Każda z kamer ma wbudowaną baterię o pojemności 2700 mAh, co umożliwia ciągłą pracę urządzenia przez okres jednej zmiany, czyli przez około 8 h. Kamery mają przetworniki CMOS o rozdzielczości 1920x1080 i generują dwa strumienie wizyjne z kompresją H.264 lub H.265. Rejestrują także dźwięk. Wbudowane głośniki oraz mikrofony mogą

Rys. 1. Kamera nasobna NVBWS-C01

być wykorzystywane do komunikacji z centrum nadzoru. Pierwszy strumień wizyjny o wysokiej rozdzielczości jest zapisywany na wewnętrznej karcie pamięci o pojemności 32 GB (gwarantowany jest zapis przez okres jednej zmiany) oraz może być transmitowany do centrum nadzoru. Drugi strumień wizyjny o niższej rozdzielczości jest nieprzerwanie transmitowany do centrum nadzoru. Ponadto w każdej z kamer może być zainstalowana karta SD o pojemności do 128 GB. Kamery mają wbudowane dwie diody LED pracujące w podczerwieni, o zasięgu do 15 m, co umożliwia wykorzystanie ich w całkowitej ciemności. Dwie inne diody LED, które oświetlają światłem widzialnym, mogą być wykorzystywane jako latarki.

Nagrania są opatrzone znakiem wodnym identyfikującym operatora. Mogą być dodatkowo oznaczone jako kluczowe, co umożliwia ich szybkie odnalezienie w zgromadzonym materiale. Kamery można skonfigurować za pomocą wbudowanego dotykowego wyświetlacza o przekątnej 2,2". Dostęp do menu może być autoryzowany kodem lub wzorem. Kamery mogą pracować w trybie autonomicznym bez komunikacji sieciowej z centrum nadzoru, ale dzięki interfejsom Wi-Fi (802.11 a/b/g/n 2,4 GHz + 5 GHz) oraz 3G/4G możliwa jest ciągła transmisja i zdalny nadzór nad podejmowanymi czynnościami.

W wersji kamuflowanej dostępne są dodatkowe akcesoria, takie jak kamery guzikowe NVBWS-C01/BC oraz kamery nauszne NVBWS-C01/EC komunikujące się kablowo z „kamerą matką" poprzez gniazdo microUSB.

Stacja dokująca pozwala na zarządzanie danymi zapisanymi na kamerach nasobnych. Jest w niej sześć gniazd dla kamer, w tym jedno gniazdo priorytetowe. Przy pełnym obsadzeniu wszystkich gniazd kamerami nasobnymi prędkość zgrywania danych wynosi maksymalnie 4,6 Mb/s i maksymalnie 15 Mb/s w przypadku gniazda priorytetowego. Stacja dokująca, wyposażona w system operacyjny Windows 10 i ekran o przekątnej 13,3", może być rozbudowana w zależności od potrzeb – mogą być w niej maksymalnie 24 gniazda.

Po włożeniu kamery do gniazda następuje automatyczne pobieranie i kasowanie z pamięci zarejestrowanych nagrań oraz ładowanie akumulatorów. Kamery mają mechaniczną blokadę zabezpieczającą je przed nieautoryzowanym użyciem. Ponowne uruchomienie kamery wymaga podania identyfikatora i hasła lub użycia klucza mechanicznego używanego przez administratora systemu.

W stacji dokującej można dodatkowo zamontować dwa dyski twarde o łącznej pojemności 24

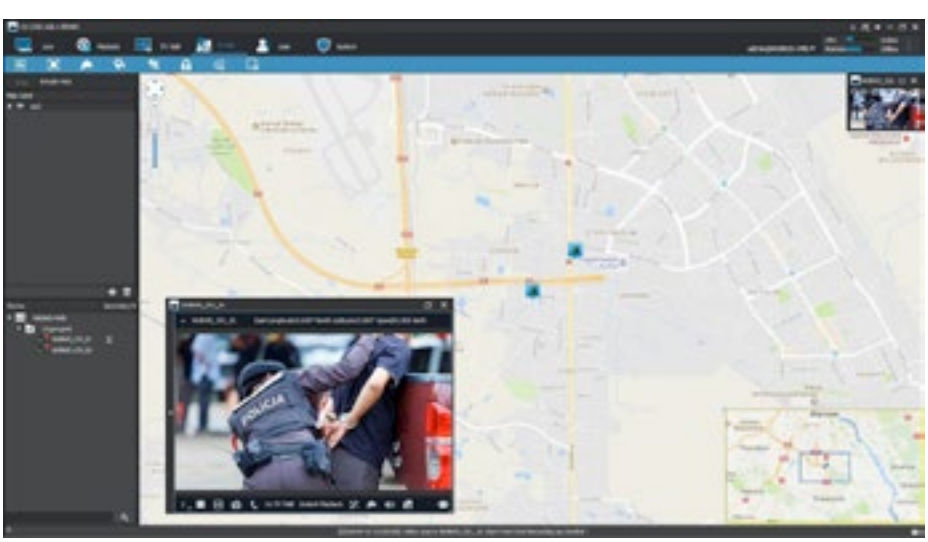
Rys. 2. Stacja dokująca NVBWS-DDS

Rys. 3. Architektura systemu nasobnego marki NOVUS

Uzupełnieniem systemu i podstawowym narzędziem do jego obsługi w czasie rzeczywistym jest stacja zarządzania NVBWS-VMS. Stacja umożliwia bieżące odbieranie strumieni wizyjnych z kamer i zapisywanie ich na dyskach twardych. Istnieje możliwość połączenia z macierzami iSCSI, a także zwizualizowanie położenia kamer na mapie Google Maps. Analizując przebieg patrolu, możemy odtworzyć materiał zapisany w dowolnym momencie, w dowolnym miejscu. Ponadto w sytuacjach krytycznych nadzorca systemu może zdalnie uruchomić zapis na dowolnej z kamer, wyręczając tym samym operatora. VMS oraz kamery mają dupleksowy system komunikacji głosowej. Każdy z operatorów kamer nasobnych cały czas ma kontakt głosowy z centrum dozorowym.

Należy spodziewać się, że w miarę upływu czasu popularność takich rozwiązań będzie rosła i kamery nasobne staną się codziennym narzędziem pracy poprawiającym bezpieczeństwo personelu przebywającego w terenie, pozwalającym na lepszą ocenę aktualnej sytuacji, a także stwarzającym możliwość dokumentowania podejmowanych czynności.

Patryk Gańko
AAT HOLDING



Rys. 4. Interfejs graficzny stacji zarządzającej systemem wizyjnym (NVBWS-VMS)

Kamery z serii MIC

do wykrywania pożarów lasu

Przemysław Pierzchała | Michał Borzucki

Już ponad 125 000 ha lasów w trzynastu leśnictwach jest dozorowanych przez kamery Bosch MIC 7000 HD wchodzące w skład zestawów Forester. System Forester – autorstwa gliwickiej firmy MWM – jest specjalistycznym narzędziem do obserwacji rozległych obszarów zielonych i zaawansowanego wykrywania pożaru. Forester składa się z kamer, unikatowego układu służącego do analizy treści obrazu w celu wykrycia dymu oraz systemu do wizualizacji i efektywnego zarządzania przez operatorów

Wykorzystanie kamer w nadzorze przeciwpożarowym lasów powoduje, że sprzęt i systemy informatyczne muszą spełniać wiele wymagań. Po pierwsze należy wspomnieć o odpowiedniej odporności środowiskowej. Kamery służące do nadzoru przeciwpożarowego są montowane na szczytach dostrzegalni pożarowych lub specjalnych masztów pożarowych, a są to konstrukcje o wysokościach dochodzących do 60 metrów. W takich miejscach niczym nie osłonięte kamery często muszą opierać się potężnym podmuchom wiatru i są narażone na bezpośrednie oddziaływanie promieni słonecznych, które rozgrzewają stalowe konstrukcje wież do temperatury kilkudziesięciu stopni Celsjusza.

Praca kamery służącej do nadzoru pożarowego różni się znacznie od pracy kamery służącej do nadzoru przestrzeni publicznej. Monitorowanie przestrzeni leśnych polega na stałym, powolnym ruchu obrotowym kamery, która ma umożliwić wykrycie oznak pożaru lasu w polu jej widzenia. Taka ciągła, jednostajna praca stanowi duże wyzwanie dla układów przeniesienia napędu kamer, gdyż kamera wykonuje nierzadko pięćset obrotów dookoła osi na dobę, zawsze w tym samym kierunku i zazwyczaj z tą samą prędkością.

Istotne jest też precyzyjne odczytywanie azymutu osi optycznej kamery. Te wszystkie wymagania są spełnione przez kamery MIC 7000. Są one specjalistycznymi urządzeniami, których parametry techniczne i konstrukcja umożliwiają nieprzerwany, długotrwały i precyzyjny nadzór wizyjny w niesprzyjających warunkach atmosferycznych. Wszystko w tych urządzeniach – od układów napędowych i elektroniki do obudowy wykonanej z ciśnieniowo formowanego aluminium – jest bardzo trwałe, „stworzone, by trwać".

Obudowa kamery ma klasę szczelności IP68 NEMA 6P i klasę odporności mechanicznej IK10. Dodajmy jeszcze, że urządzenia są objęte trzyletnią gwarancją producenta z możliwością wymiany urządzenia w przypadku usterki.

Do innych, wymaganych funkcji systemów nadzoru pożarowego należy:
- precyzyjne informowanie o aktualnym azymucie osi optycznej kamery (tym samym system zarządzający dokonuje precyzyjnej lokalizacji zagrożenia, a operator może szybko skierować strażaków we właściwe miejsce),
- pozycjonowanie kamery zgodnie z określonym azymutem z dokładnością do 0,06 stopnia,
- pokazywanie na obrazie z kamery informacji niezbędnych dla operatora, w tym podawanie azymutu kamery, nazwy aktualnie nadzorowanego obszaru (we współpracy z systemem mapy cyfrowej wbudowanej w oprogramowanie Forester) czy wyświetlanie „celownika" pomagającego w precyzyjnym ustawianiu kamery przez wskazanie celu obserwacji.

Dzięki udziałowi firmy MWM w programie Bosch Integration Partner Program i wykorzystaniu możliwości pakietów SDK udostępnianych przez firmę Bosch dokonano integracji kamer MIC z systemem VMS Forester w szerokim zakresie, udostępniając użytkownikowi między innymi:
- odczyt aktualnego azymutu osi optycznej kamery (cztery razy na sekundę),
- pozycjonowanie kamery zgodnie z określonym azymutem z dokładnością do 0,06 stopnia,
- korekcja gamma obrazu kamery,
- wyświetlanie na ekranie dowolnych ciągów znaków w różnych kolorach,
- wyświetlanie „celownika" na obrazie z kamery,
- zmiana prędkości ruchu rotacyjnego w aplikacji systemu Forester.

Więcej informacji na temat systemu można znaleźć na stronie www.forester.com.pl.

Przemysław Pierzchała
MWM
Michał Borzucki
Bosch Security and Safety Systems

Wygrywamy dzięki wartościom

Rozmowa z Rayem Mauritssonem – dyrektorem generalnym w firmie Axis Communications

Jaką strategię rozwoju w najbliższych latach przyjmuje Axis Communications?

Jesteśmy dynamicznie rozwijającą się firmą, która w ciągu ostatnich czterech lat podwoiła liczbę pracowników. Obecnie zatrudniamy 3000 osób, które wnoszą do organizacji talent, pasję i najwyższe kompetencje. Aby utrzymać wzrost sprzedaży na poziomie 15% rocznie, będziemy systematycznie poszerzać ofertę o nowe produkty i aplikacje oraz zwiększać ich funkcjonalność. Kamery sieciowe nadal pozostaną w centrum zainteresowania, jednak sporo uwagi poświęcimy też innowacjom w sektorze dźwięku. Podstawą naszych działań jest wolność eksperymentowania, jaką dajemy naszym młodym, utalentowanym inżynierom, a także niemałe środki, jakie inwestujemy w dział badań i rozwoju. W minionym roku przeznaczyliśmy na ten cel 17% zysku osiągniętego w 2016 roku. Jednocześnie bacznie obserwujemy rynek i staramy się spełniać oczekiwania klientów.

Jak bardzo zmieniły się i będą się zmieniać kamery sieciowe?

Od czasu stworzenia przez Martina Grena kamery sieciowej AXIS w 1996 roku minęło ponad dwadzieścia lat charakteryzujących się niezwykłą dynamiką zmian i rozwojem techniki. Obecne kamery sieciowe nie są już zwykłymi urządzeniami optycznymi, lecz procesorami o dużej mocy obliczeniowej, dzięki której szybko i sprawnie analizują wytwarzany obraz. Kamery sieciowe wpiszą się w miejski krajobraz, będą wszechobecne. Dlatego tak ważna jest edukacja społeczeństwa mającą na celu uświadomienie korzyści płynących z zastosowania takich zabezpieczeń. Sądzę, że nowoczesne kamery będą wtapiać się

w otoczenie, będą działać dyskretnie i nie będą razić wyglądem. Pole do popisu mają projektanci, którzy, bazując na tradycji szwedzkiego wzornictwa, mogą zaproponować rozwiązania łączące funkcjonalność z estetyką.

Nadzór wizyjny nierozerwalnie wiąże się z ograniczeniem prywatności. W maju wchodzi w życie rozporządzenie RODO. Czy jesteście przygotowani na nowe regulacje?

Klienci mogą być pewni, że firma dostosuje się do nowych zaleceń. Jest to wyzwanie, a jednocześnie okazja do tego, by zacząć opracowywać jak najlepsze rozwiązania chroniące wizerunek twarzy i nie magazynujące danych przez zbyt długi czas.

Na czym skoncentrujecie się w tym roku? Jakie trendy w branży dozoru wizyjnego uważacie za najważniejsze?

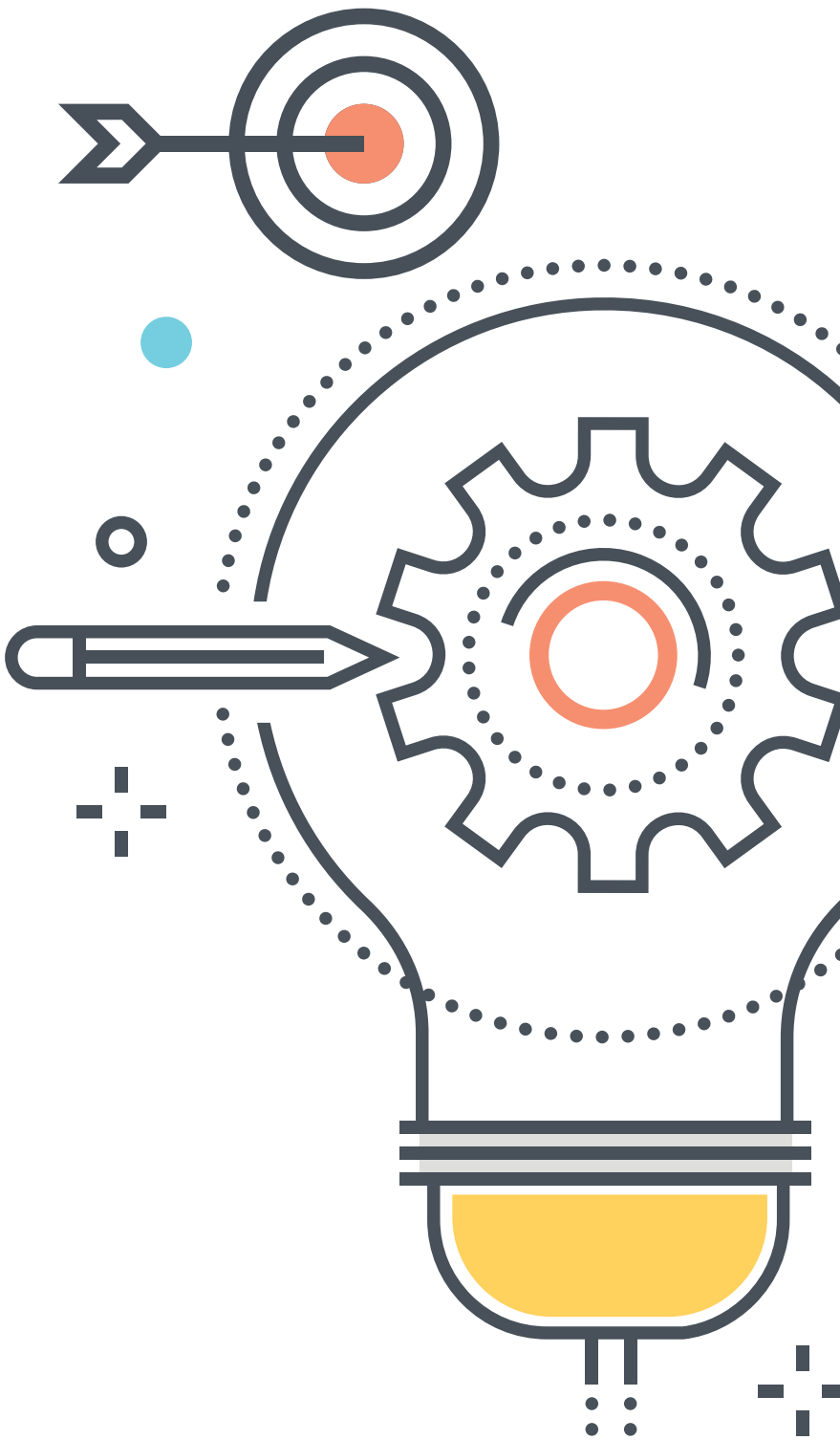
Szczególnie istotna będzie dla nas koncepcja inteligentnego miasta (ang. *smart city*) oraz nadzór wizyjny w transporcie publicznym. Chcemy proponować nasze nowatorskie rozwiązania i być jak najbardziej „widoczni". Koncepcja inteligentnego miasta to ważny trend i będzie ona coraz bardziej rozwijana, gdyż dotyczy wszystkich mieszkańców zurbanizowanych obszarów. Jej celem jest podniesienie jakości życia, w tym poprawa bezpieczeństwa, np. w drodze do pracy lub szkoły, podczas spędzania wolnego czasu w publicznej przestrzeni miejskiej. Wykorzystanie nowoczesnych kamer sieciowych w transporcie publicznym poprawia efektywność dozoru wizyjnego i bezpieczeństwo pasażerów. Możliwe jest liczenie ludzi czy rozpoznawanie twarzy. Większość analitycznej obróbki danych będzie odbywała się w kamerze, a reszta na zewnętrznych serwerach sieciowych. Przykładem mogą być systemy służące do wykrywania ruchu, które jednocześnie umożliwiają liczenie osób. W związku z coraz szerszym wykorzystaniem kamer o rozdzielczości 4K powstaje problem magazynowania ogromnych ilości danych. Tu z pomocą przychodzi produkt Axis zwany Zipstream, umożliwiający kompresję obrazu bez utraty jakości i użyteczności zarejestrowanego materiału wizyjnego. W efekcie magazynowane są tylko istotne informacje, a zapotrzebowanie na przepustowość sieci i zasoby pamięci masowej zostaje ograniczone nawet o połowę.

Na rynku działa wiele konkurencyjnych firm. Czy macie przygotowany sposób na odparcie ofensywy z Azji?

To prawda, że bierzemy udział w nieustannym wyścigu, głównie z chińskimi firmami, których produkty są po prostu tańsze. Naszym asem w rękawie są zintegrowane rozwiązania zapewniające klientowi cały zestaw usług dodatkowych, takich jak obsługa posprzedażowa, ścisła współpraca partnerska, bogaty system regularnych szkoleń, a także nasza wiedza, doradztwo i ekspertyza, którymi chętnie się dzielimy. Stawiamy na rozwój, inwestujemy w talenty i pomysły, dbamy o bezpieczeństwo danych osobowych. Nie chcemy wygrywać dzięki cenie, lecz dzięki wartościom.

Pod koniec stycznia odbyło się huczne otwarcie większego biura w Warszawie? Czy to nowy etap w rozwoju firmy w tej części Europy?

Tak, zdecydowanie. To bardzo ważny dla nas rynek z ogromnym potencjałem i jednocześnie świetna lokalizacja. W Warszawie mogą spotykać się pracownicy Axis Communications z całego regionu, w tym z Ukrainy i krajów bałtyckich. Zorganizowaliśmy tutaj Akademię Axis, zapewniając powierzchnię oraz sprzęt, które będą wykorzystywane w regularnie prowadzonych szkoleniach.



15 LAT

lipiec FIRE 2018

FIRE|EXPO SECURITY 2018

KONGRES POŻARNICTWA

PGE NARODOWY

26 lipca 2018 WARSZAWA

Świętuj z nami 15 - lecie Kongresu DZIEŃ Z BEZPIECZEŃSTWEM POŻAROWYM na PGE Narodowy

WSTĘP BEZPŁATNY

Główny Patron Medialny FIRE | SECURITY EXPO 2018

CZASOPISMO ZABEZPIECZENIA

Główny Partner Technologiczny Wystawy SECURITY|EXPO 2018

BOSCH

PATRONAT HONOROWY

Mazowsze. WIPOS Politechnika Łódzka SIBP NODEX PIARC PISA IFOA

DND project

Rejestracja na Kongres ROZPOCZĘTA

Już dziś ZAREZERWUJ miejsce!

www.fire-expo.pl

Zabezpieczanie prywatnego mieszkania lub lokalu

przeznaczonego do wynajmu

Maciej Prelich

Bardzo często w naszych artykułach poruszamy kwestie zabezpieczania terenów przemysłowych i fabryk. Tym razem chcielibyśmy skoncentrować się na zabezpieczaniu prywatnych mieszkań lub apartamentów przeznaczonych do wynajmu

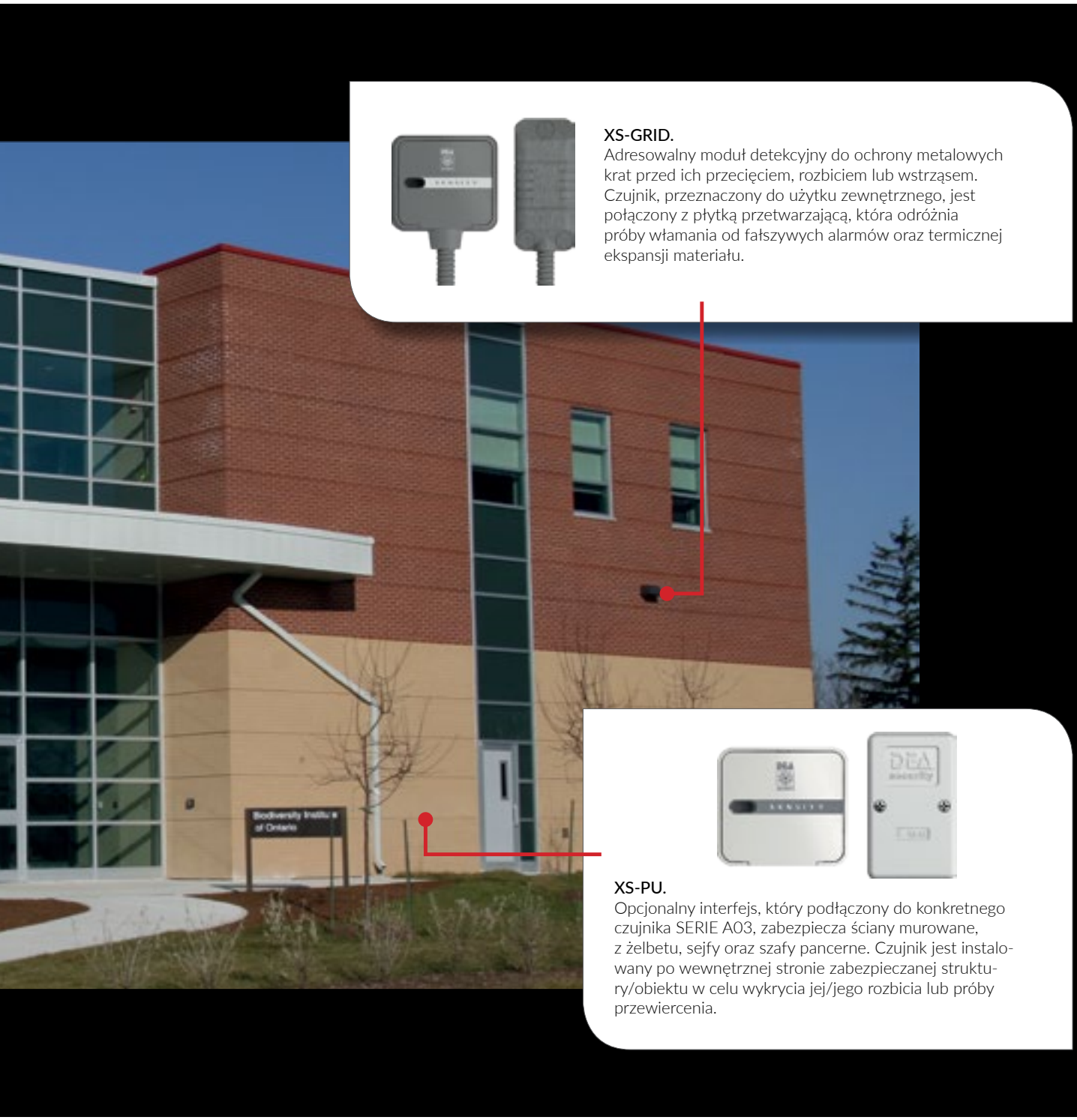
Ciągły rozwój techniki oraz rosnąca popularność idei wynajmu mieszkań, apartamentów, domów i posiadłości, również za pośrednictwem platform takich jak AirBnB, sprawia, że właściciele nieruchomości szukają rozwiązań, które pozwolą zabezpieczyć ich cenne mienie. Najbardziej klasycznym i oczywistym zabezpieczeniem mieszkania są zamki, jednak te klasyczne, bębenkowe, narażają właściciela na ryzyko podrobienia lub zgubienia kluczy. Ponadto nawet przy zwykłym użytkowaniu klucze mogą ulec uszkodzeniu, co powoduje dodatkowe koszty i problemy.

Zamki szyfrowe opisane w numerze 02/2018 *Zabezpieczeń* pozwalają ominąć ten problem, ponieważ klucz jest zastąpiony kodem lub kartą dostępu, a także dają wiele dodatkowych korzyści. Jedną z nich jest możliwość przeglądania dziennika dostępu dla każdego indywidualnego zamka.

Rys.1. Zamek szyfrowy CL5510

Rys. 2. Mnogość zastosowań systemu DEA Xensity

Co więcej, zamki z funkcją NetCode umożliwiają dostęp do specjalnego portalu internetowego, za pomocą którego można generować kody dostępu w określonzych ramach czasowych. W razie potrzeby można nawet zablokować już istniejący kod. Przykładem takiego zamka szyfrowego jest Codelocks CL 5510, pokazany na rys. 1. Jest to dobre rozwiązanie w nowoczesnym domu ze względu na możliwość konfiguracji zamka za pomocą smartfonu. Takie rozwiązanie ułatwia życie nie tylko właścicielom, lecz również tym, którzy wynajmują mieszkanie lub przebywają w nim tylko w niektórych dniach i godzinach, np. osobom opiekującym się dziećmi albo sprzątającym – nie jest potrzebny dodatkowy kluczy i w związku



XS-GRID.
Adresowalny moduł detekcyjny do ochrony metalowych krat przed ich przecięciem, rozbiciem lub wstrząsem. Czujnik, przeznaczony do użytku zewnętrznego, jest połączony z płytką przetwarzającą, która odróżnia próby włamania od fałszywych alarmów oraz termicznej ekspansji materiału.

XS-PU.
Opcjonalny interfejs, który podłączony do konkretnego czujnika SERIE A03, zabezpiecza ściany murowane, z żelbetu, sejfy oraz szafy pancerne. Czujnik jest instalowany po wewnętrznej stronie zabezpieczanej struktury/obiektu w celu wykrycia jej/jego rozbicia lub próby przewiercenia.

z tym nie ma ryzyka jego zgubienia. Sami lokatorzy, a szczególnie małe lub nastoletnie dzieci, narażeni są na zgubienie lub kradzież kluczy. Dzięki możliwości otwarcia drzwi za pomocą telefonu lub bransoletki zamki te mogą być atrakcyjne dla ludzi, którzy chcieliby mieć tzw. inteligentny dom. Mogą spodobać się również tym, którzy chcą zminimalizować wagę oraz objętość noszonych ze sobą rzeczy.

Do zabezpieczania lokali mieszkalnych wykorzystuje się różne rozwiązania. Niektóre techniki detekcyjne stosowano pierwotnie w obiektach wojskowych i w obiektach należących do infrastruktury krytycznej, np. w elektrowniach czy elektrociepłowniach. Przykładem może

Rys. 3. System DEA SISMA CA instalowany pod chronioną powierzchnią

być DEA Xensity (rys. 2). System Xensity wykorzystuje pojedyncze czujki alarmowe instalowane w wybranych miejscach w obiekcie oraz przetwarza wytwarzane przez nie sygnały z wykorzystaniem inteligentnych algorytmów zwiększających skuteczność wykrywania zagrożeń, minimalizując ryzyko wystąpienia nieuzasadnionych alarmów. System jest w stanie odróżnić faktyczną próbę włamania od prób manipulacji przy czujkach.

Kolejne możliwe rozwiązanie to wykorzystanie posadzki przed drzwiami, na balkonach, na tarasach lub w ogrodach zimowych jako czujki w systemie DEA SISMA CA. Inny system, DEA SISMA CA PF,

Rys. 4. Sorhea Biris II – bariera podczerwieni do zabezpieczenia terenu wokół okna, bramy lub na dachu

wykrywa wejście intruza na podłogę wewnątrz budynku. Znajdzie zastosowanie raczej w prywatnych posiadłościach i domach, a nie w apartamentach w blokach ze względu na niezbędne prace instalacyjne. Oba wymienione systemy sprawdzą się zarówno w klasycznych lokalach mieszkalnych, jak i w takich lokalach, w których jedno pomieszczenie pełni funkcję lokalu użytkowego (np. biura, gabinetu lekarskiego).

Specyfika zabezpieczanych prywatnych obiektów nie wyklucza możliwości wykorzystania popularnych technik detekcji, nierzadko wywodzących się z obiektów wojskowych. Czołowi producenci barier podczerwieni produkują urządzenia przystosowane do ochrony obiektów prywatnych, a nawet tylko ich fragmentów, takich jak wnęka okna, fasada czy brama posesji (rys. 4.). Przykładem może być Uniris II i Biris II firmy Sorhea. Obszary wokół budynku mogą być chronione z użyciem systemów peryferyjnych, kabli sensorycznych, klasycznych barier podczerwieni i barier mikrofalowych.

Mnogość technik detekcji oraz systemów alarmowych sprawia, że obecnie można znaleźć dobry sposób na poprawę swojego bezpieczeństwa oraz komfortu życia nawet przy ograniczonym budżecie.

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

GENEVO na targach
SECUREX 2018

Michał Konarski

SECUREX 2018 był dla firmy GENEVO wyjątkowy, i to z wielu względów. Przede wszystkim firma mogła po raz pierwszy samodzielnie przedstawić swoją ofertę na tych największych w Polsce targach branżowych. Udział w nich był istotny również ze względu na możliwość zaprezentowania licznych nowości – wprowadzanych do oferty lub tych, które lada moment powiększą asortyment oferowanych produktów. Oczywiście znaczącym wyróżnieniem była również statuetka Acanthus Aureus, przyznana przez Kapitułę MTP za atrakcyjny sposób przedstawienia swojej wizji marketingowej

Możemy mówić o dużym sukcesie firmy GENEVO na targach. Dzięki prostemu, „lekkiemu" i ciekawemu wzornictwu jej stoisko przyciągało uwagę odwiedzających. Ich duża część znała już firmę oraz słyszała o jej produktach. To dowód na to, że działania prowadzone w terenie – zarówno szkolenia, jak i spotkania z dystrybutorami oraz instalatorami – przynoszą zamierzony efekt. Odwiedzający mówili również, że już sama obecność firmy na targach jest dla nich potwierdzeniem jej dynamicznego rozwoju.

Klienci, którzy już znali produkty z oferty GENEVO, chętnie dzielili się swoimi doświadczeniami i zadawali liczne i trafne pytania świadczące o ich profesjonalnym podejściu do wykonywanego zawodu.

Dla tej grupy odwiedzających najbardziej istotne były informacje o nowościach wprowadzanych do oferty oraz zapowiedzi określające planowane działania zespołu badawczo-rozwojowego firmy. Trzeba dodać, że tegoroczna ekspozycja na targach SECUREX obfitowała w nowe produkty.

Swoją premierę miała rodzina nowych manipulatorów do systemów alarmowych GENEVO – modele PRIMA LCD SL, PRIMA LCD SL-HUB oraz EvoKPD. Pierwsze dwa to tradycyjne manipulatory podłączane przewodowo do central alarmowych PRIMA. PRIMA LCD SL jest nowoczesnym manipulatorem mającym sprostać oczekiwaniom najbardziej wymagających klientów. Jest wyposażony w graficzny ekran z kolorowym podświetleniem RGB i mieści się w bardzo smukłej obudowie mierzącej zaledwie 15 mm. Wygląda lekko, efektownie i będzie ozdobą każdego pomieszczenia. Dopełnieniem efektu wizualnego jest powierzchnia wykończona na wysoki połysk, śnieżnobiała płyta czołowa manipulatora, a także dyskretny wskaźnik diodowy ukryty w podświetlanym logotypie na płycie czołowej urządzenia.

Model z dopiskiem *HUB* w nazwie ma dodatkowo wbudowany kontroler urządzeń bezprzewodowych EvoLiNK, dzięki czemu stanowi doskonałe rozwiązanie przeznaczone do rozbudowy tradycyjnego systemu przez dodanie elementów bezprzewodowych i stworzenia w ten sposób systemu hybrydowego. Warto podkreślić, że firma GENEVO jest pierwszym polskim producentem wprowadzającym w swoim manipulatorze takie udogodnienie dla instalatorów.

EVOKPD to z kolei bezprzewodowy manipulator zaprojektowany z myślą o systemach, w przypadku których nie ma możliwości poprowadzenia przewodu pomiędzy centralą i manipulatorem. Tworząc to urządzenie, również zastosowano rozwiązanie, którego nie oferuje żaden inny polski producent – manipulator bezprzewodowy można zasilić za pomocą dopuszkowego zasilacza 14 V_{DC} lub – jeżeli nie ma takiej możliwości –wykorzystać go w trybie całkowicie autonomicznym, w którym zasilanie jest wyłącznie bateryjne.

Ze względu na to, że nowe manipulatory były najbardziej istotną premierą ze względu na strategię rozwoju oferty firmy GENEVO, to właśnie tym urządzeniom podporządkowany został wystrój całego stoiska targowego. Zaokrąglone narożniki ścian, pulpitu oraz ozdobnego daszku nawiązywały do ukształtowania narożników nowych manipulatorów. Lekki i prosty, wręcz minimalistyczny projekt stoiska miał odzwierciedlić czystą i prostą formę manipulatorów z rodziny SL. Efektowne połyskujące wykończenie panelu przedniego zostało odzwierciedlone w błyszczącej lakierowanej podłodze stoiska targowego oraz w elementach dekoracyjnych. W ten sposób udało się nadać odpowiednią rangę tej istotnej premierze produktowej.

To jednak nie koniec listy nowości. Manipulatory wyposażone w interfejs radiowy są dowodem na to, że firma GENEVO poważnie traktuje swój system bezprzewodowy, który ma doskonałe parametry i – pomimo obecności na rynku od niedawna – już zdążył wykazać się niezawodnością,

jak przystało na solidny dwukierunkowy system pracujący w paśmie 868 MHz.

Moduł EVOHUB-NANO stanowi znaczący krok w stronę rozwoju systemu całkowicie bezprzewodowego. Wpinając go do płyty głównej centrali PRiMA, można uzyskać centralę bezpośrednio obsługującą urządzenia komunikujące się drogą radiową – manipulatory, czujki czy sygnalizatory. Dużą zaletą modułu EVOHUB-NANO jest to, że można go dołączyć do istniejącego systemu alarmowego PRIMA.

Uzupełnieniem asortymentu bezprzewodowych urządzeń zaprezentowanych na tegorocznych targach SECUREX był EVOSOUND – bezprzewodowy zewnętrzny sygnalizator optyczno-akustyczny przeznaczony do pracy w systemie EVOLINK. Ma on atrakcyjną obudowę, znaną z sygnalizatora BLADE z oferty GENEVO, i bardzo spodobał się odwiedzającym. W ten sposób asortyment oferowanych urządzeń EVOLINK staje się coraz bardziej kompletny i spełnia większość typowych oczekiwań mających związek z instalacją.

Na tegorocznych targach SECUREX firma GENEVO zaprezentowała nie tylko nowe urządzenia bezprzewodowe. Również zwolennicy przewodowych systemów alarmowych mogli znaleźć coś dla siebie. Moduł EXT-Z8PS-R jest rozwinięciem modułów I/O do central PRiMA, a zwłaszcza centrali PRiMA64. Oprócz ośmiu programowalnych wejść posiada on również dwa wyjścia przekaźnikowe oraz wbudowany zasilacz buforowy zapewniający poprawny bilans energetyczny w instalacji alarmowej.

Na targach zaprezentowany został również odbiornik monitoringu MSR-XC. Urządzenie to zostało zaprojektowane z myślą o współpracy central PRIMA i modułów GSM-8 – w zakresie monitorowania z wykorzystaniem sieci IP – z praktycznie dowolnym systemem stacji monitorujących obsługujących format SURGARD. MSR-XC umożliwia odbieranie sygnałów z systemów i przekazuje je dalej, do oprogramowania zarządzającego stacją.

Wspominając o zaprezentowanych nowościach, nie sposób pominąć również nowych programów. W trakcie targów SECUREX zaprezentowano funkcję zdalnego programowania wszystkich central GENEVO z wbudowanym modułem GSM/GPRS za pośrednictwem tzw. chmury, w dowolnym miejscu, w którym jest dostęp do Internetu. Jest to olbrzymie udogodnienie dla tych instalatorów, którzy chcą mieć szybki i łatwy wgląd w obsługiwane przez siebie instalacje bez dojeżdżania do chronionego obiektu.

Również GSM-8 ma zupełnie nowe możliwości. Jego przydatność jako modułu komunikacyjnego znacznie wzrosła – zwiększona została liczba numerów telefonów uwzględnianych w czasie powiadamiania o alarmach, umożliwiono sterowanie systemem podzielonym na strefy i wprowadzono wiele innych udogodnień. Moduł GSM-8 może także pełnić rolę samodzielnego modułu alarmowego PICO-8 w ekonomicznych, uproszczonych instalacjach alarmowych. Umożliwia on podłączenie czujek, sygnalizatorów oraz – z użyciem EVOHUB NANO – urządzeń bezprzewodowych EVOLINK, w tym manipulatora bezprzewodowego. Dzięki temu staje się obecnie najbardziej funkcjonalnym w swojej klasie urządzeniem na rynku.

W trakcie tegorocznych targów SECUREX wspomniano o niektórych planach dotyczących rozwoju linii produktów GENEVO. Nowa seria central XL, mająca uzupełnić obecną linię PRIMA o urządzenia dla jeszcze bardziej wymagających klientów, umożliwi budowanie dwukrotnie większych (pod względem liczby linii) systemów alarmowych. Seria XL zapewni nie tylko większą liczbę wejść, wyjść i stref. Docelowo ma dać więcej możliwości w zakresie integracji systemów alarmowych z elementami inteligentnego domu, co usatysfakcjonuje nawet najbardziej wymagających instalatorów.

Dla firmy GENEVO tegoroczna edycja targów SECUREX była bardzo owocna. Nic nie motywuje do dalszego wytężonego wysiłku lepiej niż zadowolenie klientów i partnerów biznesowych. „Naładowaliśmy baterie" i możemy działać dalej – z pasją tworzyć łatwe i wygodne w codziennej obsłudze, niezawodne urządzenia zapewniające poczucie bezpieczeństwa.

Michał Konarski
GENEVO

EVIX®

MADE IN EU

NOWY WYMIAR OCHRONY
CZUJKI DUALNE PIR + MW

IDEALNE UZUPEŁNIENIE KAŻDEGO SYSTEMU ALARMOWEGO

AAT HOLDING S.A.

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

Nowy wymiar ochrony

Nowa rodzina czujek EVIX

Bartłomiej Kwiatkowski

Dzięki nowej serii czujek dualnych EVIX zabezpieczenie trudno dostępnych miejsc staje się prostsze. Urządzenia te mogą mieć różne charakterystyki detekcji – dookolną i kurtynową – i są przeznaczone do zastosowań specjalistycznych

Każdy model nowej serii wyróżnia się czymś unikatowym, o czym będzie mowa w dalszej części tego artykułu. Detekcja bazuje na wykorzystaniu podczerwieni oraz mikrofal (technik PIR i MW), dzięki czemu jest niezawodna. Na serię składają się urządzenia do zastosowania zarówno wewnątrz, jak i na zewnątrz obiektów. Modele EV-CL4D oraz EV-CL360D to czujki przeznaczone do instalacji wewnątrz pomieszczeń, a modele EV-CL6DAM, EV-WL12DAM oraz EV-WL24DAM są przystosowane do instalacji zewnętrznych.

EV-CL4D to czujka dualna o charakterystyce kurtynowej. Jej obudowa ma bardzo małe rozmiary. Jest to cecha umożliwiająca np. bezproblemowe zabezpieczenie wnęk okiennych i drzwiowych. W takich miejscach czujka powinna być instalowana od góry. Urządzenie będzie mało widoczne i nie będzie przeszkadzać w normalnym użytkowaniu chronionych obszarów. Maksymalna wysokość mierzona od podłoża, na jakiej może być zainstalowana czujka, wynosi aż cztery metry, dzięki czemu czujka ta może znaleźć zastosowanie również w kontroli przejść do poszczególnych stref w wysokich pomieszczeniach.

Fot. 1. Wewnętrzne czujki dualne EVIX (EV-CL4D i EV-CL360D)

EV-CL360D to czujka dualna o charakterystyce dookolnej (360°). Maksymalna wysokość instalacji urządzenia wynosi aż 4,8 m, przy tej wysokości średnica pola detekcji wynosi około dziesięć metrów. Czujka może pracować w trybie *AND* lub *OR*. Sprawdzi się w miejscach, w których tradycyjne czujki o charakterystyce szerokokątnej nie pokrywają w pełni obszarów dozorowanych. Przykładem takich miejsc są magazyny, gdzie regały często zasłaniają pole widzenia czujek szerokokątnych. Kolejnym atutem czujki jest wbudowana funkcja braku reakcji na małe zwierzęta (do 12 kg), dzięki której czujka nie będzie generować fałszywych alarmów, np. na skutek obecności gryzonia w składzie, na hali czy w magazynie. Warunkiem jej działania jest instalacja urządzenia na wysokości powyżej 3,5 m. Czujki EV-CL4D i EV-CL360D umożliwiają zabezpieczenie obiektu w stopniu drugim (*Grade 2* według PN-EN 50131-2-4).

Modele EV-CL6DAM, EV-WL12DAM oraz EV-WL24DAM to czujki o charakterystyce kurtynowej, przystosowane do instalacji na zewnątrz obiektów. Gwarantują doskonałą niezawodność działania nawet w najtrudniejszych warunkach środowiskowych, ponieważ elektronika urządzeń została poddana procesowi tropikalizacji. Proces ten polega na wygrzaniu elektroniki w celu pozbycia się całej wilgoci, a następnie polakierowaniu jej odpowiednim środkiem. Ciekawostką jest fakt, że podobnym zabiegom poddaje się elektronikę urządzeń instalowanych na statkach morskich.

Wspomniane modele mają również zaawansowane funkcje, które na ogół trudno znaleźć w urządzeniach wykorzystywanych do ochrony zewnętrznej – funkcję blokady urządzenia oraz funkcję pamięci alarmów. Obie są ze sobą powiązane i aktywuje się je przez podanie odpowiedniego sygnału na wyznaczone wejście czujki. Proces ten można zautomatyzować, wykorzystując wyjścia programowalne oraz funkcję centrali alarmowej. Działanie funkcji polega na tym, że jeżeli czujka wykryje intruza, próbę jej zasłonięcia lub naruszenie jednego z sensorów PIR/MW, to po aktywacji wyznaczonego wejścia zablokuje swoje działanie i wyświetli zapamiętane zdarzenia za pomocą odpowiednich diod LED. Jeżeli urządzenie nie wykryło wcześniej żadnego zdarzenia, a funkcja zostanie zaktywowana, czujka zablokuje swoje działanie, ale żadna z diod nie będzie świecić. Podczas aktywnej blokady czujka będzie w dalszym ciągu wykrywać próby zasłonięcia.

Czujki wyposażono także w zaawansowany system dualnego antymaskingu, dzięki czemu umożliwiają one zabezpieczenie obiektu w stopniu trzecim (*Grade 3* zgodnie z PN-EN 50131-2-4). Antymasking oznacza, że czujki wykorzystują układy oraz algorytmy wykrywające obiekty

Fot. 2. Zewnętrzne czujki dualne EVIX (EV-CL6DAM, EV-WL12DAM i EV-WL24DAM)

zasłaniające ich pole detekcji. Dualny antymasking polega na tym, że urządzenia mogą wykryć zasłonięcie zarówno czujników PIR, jak i czujników MW. Za pomocą odpowiednich przełączników można dowolnie określać, który z układów antymaskingu będzie aktywny (PIR, MW lub obydwa). Zasięg działania antymaskingu wynosi siedem centymetrów od obudowy dla obu sensorów. Umożliwia to wykrycie nie tylko takiego obiektu zasłaniającego, który przylega do obudowy, ale również takiego, który znajduje się przed czujką (nie ma fizycznego kontaktu). Urządzenia mogą pracować w trybie *AND* lub *OR*, a ich zasięgi detekcji są regulowane za pomocą potencjometrów (dla PIR i MW).

Fot. 3. Przykład zabezpieczenia okien wielkoformatowych

Dzięki stosunkowo niewielkim rozmiarom można z powodzeniem instalować czujki EV-CL6DAM i EV-WL12DAM wewnątrz obiektów. Mogą być wykorzystane np. do ochrony ekspozycji w muzeach, do ochrony korytarzy w archiwach, do zabezpieczenia przestrzeni między regałami w magazynach.

EV-CL6DAM to czujka, która może być zamontowana na wysokości do sześciu metrów. Przy takiej wysokości długość kurtyny wynosi osiem metrów. Czujka jest przeznaczona do ochrony drzwi i okien, a dzięki specyficznemu kształtowi może być zainstalowana np. pomiędzy roletą a oknem. Tak jak w przypadku EV-CL4D urządzenie to powinno być zainstalowane u góry, a jego soczewka powinna być skierowana w stronę chronionej przestrzeni. W zestawie z czujką są uchwyty dwóch rodzajów – płaski oraz kątowy (90°). Prawidłowe wykorzystanie uchwytów zapobiegnie przedostawaniu się owadów do wnętrza urządzenia. Uchwyt kątowy umożliwia zainstalowanie czujki na ścianie lub nadprożach, co zwiększa zakres zastosowań urządzenia.

EV-WL12DAM to czujka, która powinna być instalowana na wysokości około 2,1 m. Przy takiej wysokości jej zasięg wynosi 12 metrów. Do urządzenia dołączony jest uchwyt płaski oraz uchwyt kątowy (90°). Dostępne są również opcjonalne akcesoria, takie jak pokrywa chroniąca przed deszczem i nasłonecznieniem, a także uchwyt umożliwiający skierowanie czujki w dowolnym kierunku. EV-WL24DAM to czujka zbudowana z dwóch czujek EV-WL12DAM dzięki wykorzystaniu specjalnej obudowy. Wewnątrz niej znajduje się płytka elektroniki łącząca sygnały z obu czujek, dzięki czemu urządzenia możemy podłączyć na jednej linii dozorowej. Czujka ma zasięg 24 metrów i powinna być instalowana centralnie na elewacji, na której znajdują się okna i drzwi. Opcjonalny uchwyt przeznaczony do montażu czujki na ścianie umożliwi dostosowanie jej położenia. Urządzenia EV-WL12DAM i EV-WL24DAM sprawdzą się w ochronie zewnętrznej bram garażowych, bram wjazdowych, tarasów, balkonów, elewacji budynków, fragmentów ogrodzeń itp.

Wszystkie czujki wyróżniają się ciekawym, minimalistycznym wzornictwem oraz różnymi charakterystykami detekcji umożliwiającymi ochronę obszarów, które do tej pory były trudne do zabezpieczenia. Zaimplementowana cyfrowa analiza sygnałów z czujek PIR i MW sprawia, że urządzenia są stabilne i nie generują fałszywych alarmów.

Bartłomiej Kwiatkowski
AAT HOLDING

Przeprowadzanie audytu

dotyczącego zarządzania bezpieczeństwem organizacyjno-technicznym obiektów. Część 4 Wpływ postępowania z ryzykiem na zabezpieczenie obiektów

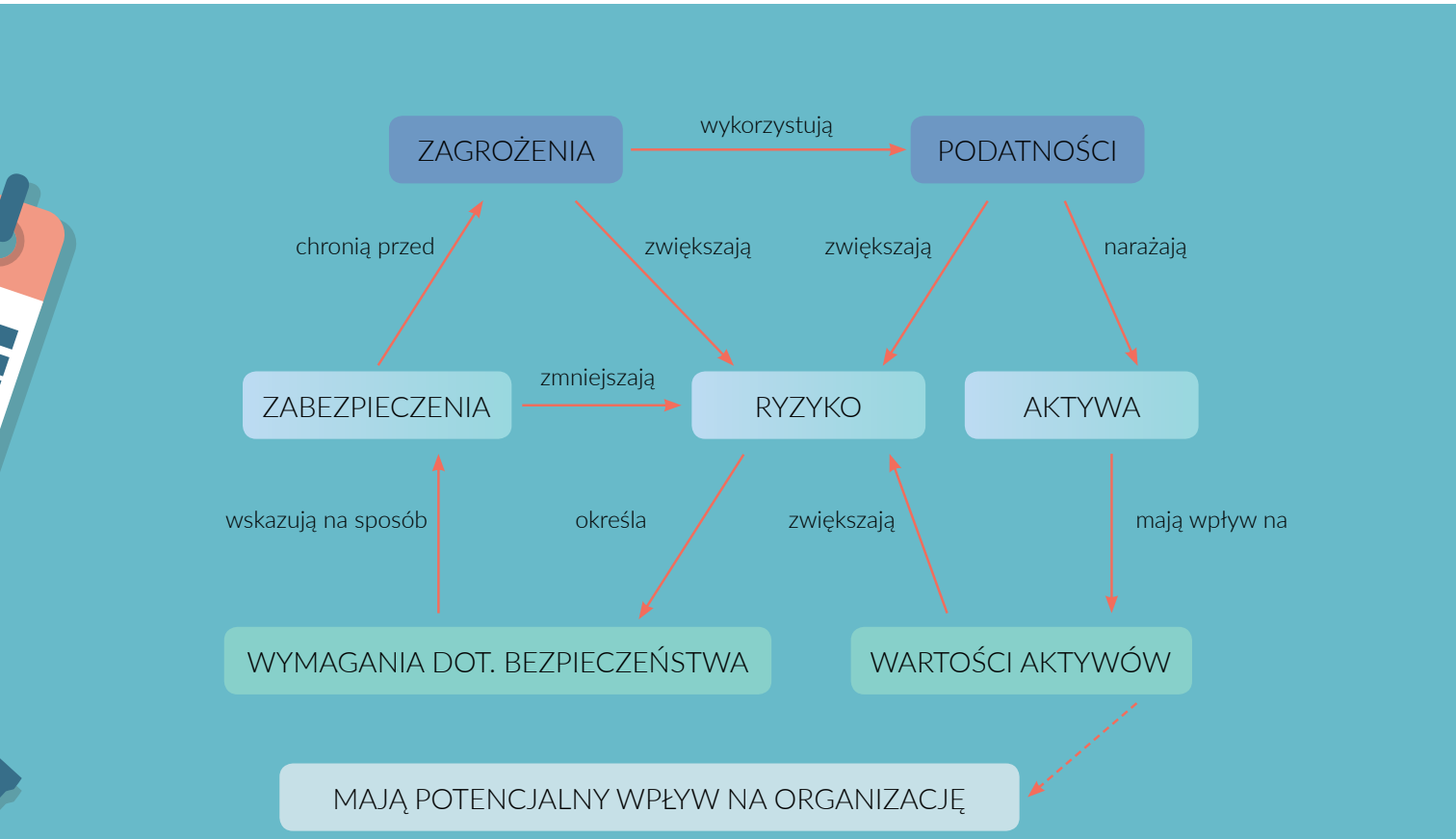
dr inż. Andrzej Wójcik

Plan postępowania z ryzykiem podczas zabezpieczania obiektów

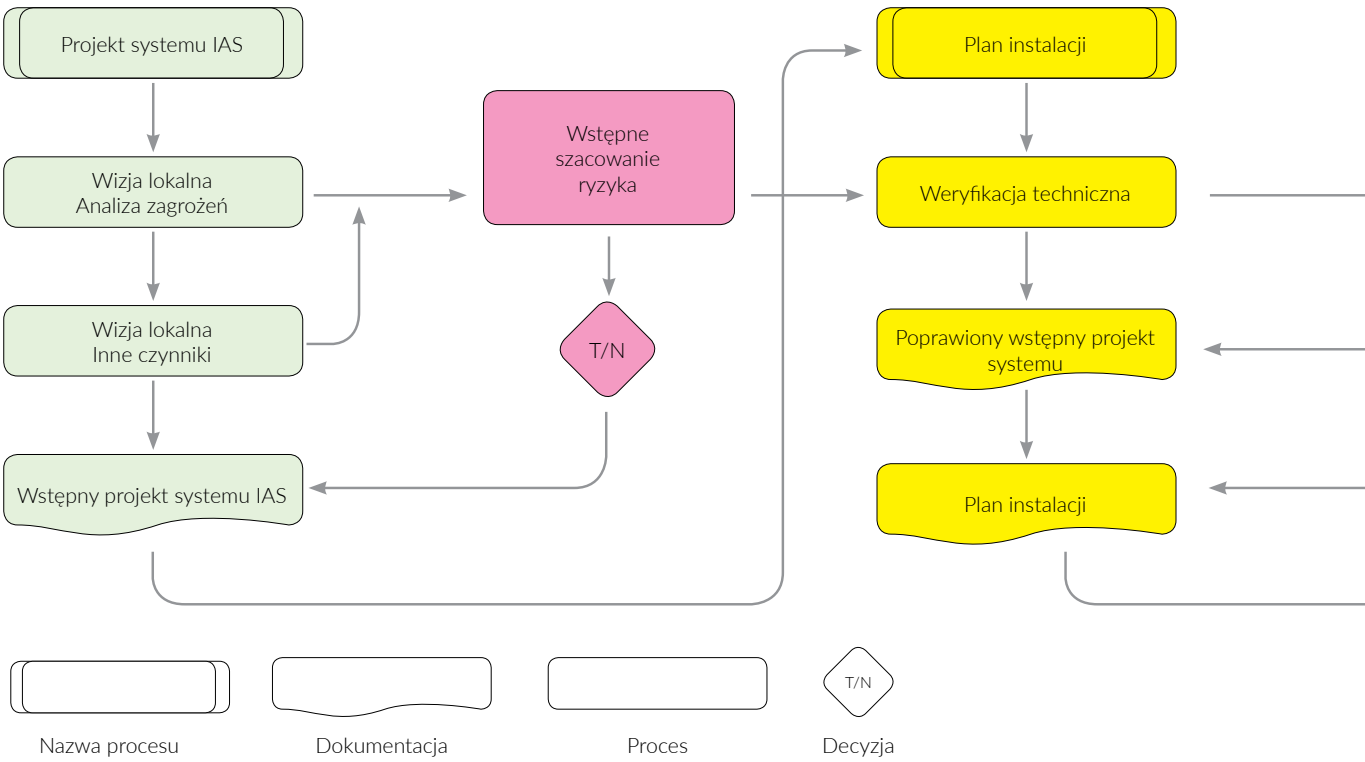
Niniejsza część artykułu dotyczy wyboru sposobu postępowania z ryzykiem, wpływu analizy ryzyka na wybór sposobów zabezpieczenia procesów w organizacji, sposobów pomiaru efektywności zabezpieczenia oraz tego, co należy sprawdzić podczas audytu w związku z szacowaniem ryzyka.

Załączony schemat prezentuje wpływ wyników analizy ryzyka na wybór sposobu zabezpieczenia obiektu. Podstawę tej analizy stanowi analiza zagrożeń oraz podatności aktywów/zasobów na zagrożenia (ich słabości). Trafne określenie zagrożeń oraz ich podział według istotności na podstawie przewidywanych strat dla organizacji jest podstawą dalszych wytycznych do dalszych działań. Ważne jest prawdopodobieństwo niepożądanych zdarzeń mających wpływ na bezpieczeństwo obiektu. Należy też uwzględnić wpływ mogących spowodować zagrożenie słabości (podatności) aktywów na bezpieczeństwo.

Organizacja powinna być świadoma ryzyka potencjalnych strat na skutek zagrożenia i jego konsekwencji – nie tylko finansowych, ale również prawnych, a także możliwości doprowadzenia przez nie do niepodpisania ważnych umów czy do odpływu fachowej kadry. Uświadomienie ryzyka i jego konsekwencji umożliwia działanie zapobiegawcze w organizacji, a mianowicie określenie adekwatnych do potrzeb i poziomu ryzyka wymagań dotyczących bezpieczeństwa (w omawianym przypadku wymagań dotyczących zabezpieczenia obiektów).



Rys. 1. Zależność zabezpieczenia obiektu od wyników szacowania ryzyka



Rys. 2. Proces szacowania ryzyka podczas realizacji zabezpieczenia obiektu

Opracowane wytyczne dotyczące zabezpieczenia obiektów, oparte na okresowo analizowanej i modyfikowanej metodyce, pozwalają wskazać najodpowiedniejsze sposoby zabezpieczenia i tym samym zapobiegać potencjalnym zagrożeniom oraz ograniczyć liczbę niekorzystnych dla funkcjonowania organizacji zdarzeń.

Jedną z podstawowych metod utrzymania ryzyka na odpowiednim, akceptowalnym dla organizacji poziomie jest przeprowadzanie systematycznych analiz ryzyka oraz aktualizowanie planów postępowania z ryzykiem. Powinno się to czynić nie tylko w zaplanowanych odstępach czasowych, np. minimum raz w roku, ale także wtedy, kiedy pojawią się przesłanki wskazujące na to, że zagrożenia urzeczywistniły się lub mogą niekorzystnie wpłynąć na stopień zabezpieczenia obiektu. Jak już wspomniano, duży wpływ na działania zapobiegające zagrożeniom ma przeprowadzany regularnie, a także w wyżej wymienionych sytuacjach audyt dotyczący stanu zabezpieczenia obiektu.

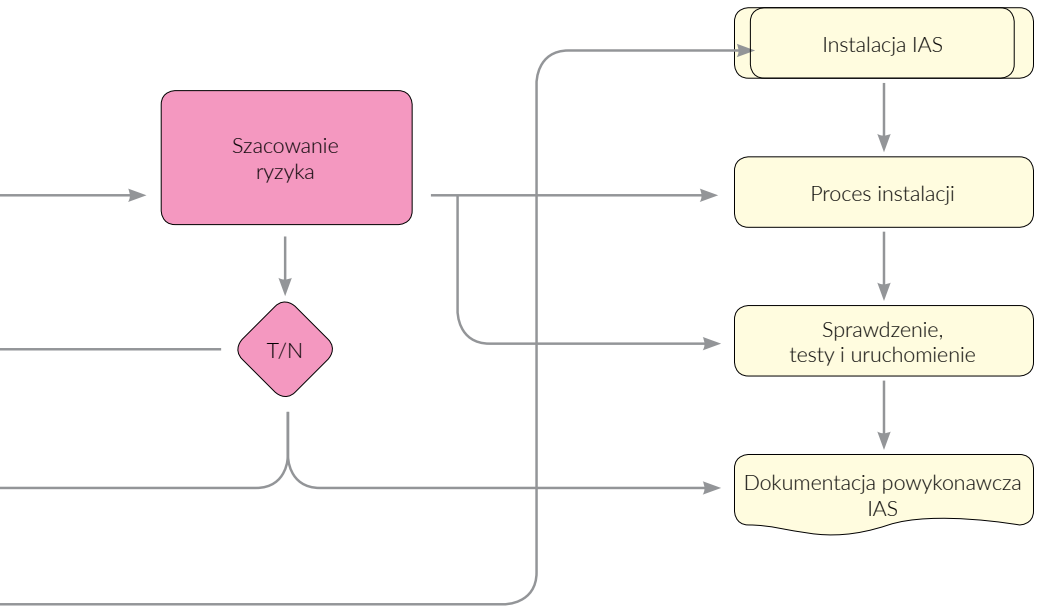
Monitorowanie ryzyka

Ocena ryzyka i analiza dobranych środków zapobiegającym potencjalnym zagrożeniom powinna być prowadzona regularnie. Wytyczne powinny być zawarte w procedurach szacowania ryzyka opracowanych na podstawie opisanych w poprzednich artykułach standardów, np. ISO 27005 czy ISO 3100.

Dane do ponownego szacowania ryzyka powinny wynikać z procesu ciągłego monitorowania bezpieczeństwa obiektu, regularnych audytów, ekspertyz itd.

Należy podjąć takie działania, aby monitorowanie i przegląd odnosiły się (lecz nie były ograniczone) do:

- kontekstu prawnego i środowiskowego (zmiany w prawie lub normach mają wpływ na to, co jest podstawą wymaganego zabezpieczenia obiektu);
- wystąpienia incydentów i zagrożeń (np. skutecznego włamania do obiektu);
- wyników audytu bezpieczeństwa wskazujących słabe punkty lub nieprawidłowości w zabezpieczenia obiektu;
- przekroczonego czasu resursu technicznego stosowanych zabezpieczeń (minął okres, w którym sprzęt powinien działać prawidłowo i spełnia założone funkcje użytkowe, a jego eksploatacja była bezpieczna);
- zmian organizacyjnych oraz przeznaczenia



chronionego obiektu (zmienił się status biznesowy);
- zmiany firmy zajmującej się fizyczną ochroną obiektu;
- zmiany firmy zajmującej się serwisem i konserwacją systemu technicznych zabezpieczeń obiektu;
- podejścia do szacowania ryzyka, np. zmiany metodyki szacowania;
- wartości i kategorii aktywów, np. wprowadzenia nowej technologii w zabezpieczeniach obiektów;
- kryteriów skutków zmaterializowania się potencjalnych zagrożeń na bezpieczeństwo obiektu;
- kryteriów oceny ryzyka, np. podniesienia lub obniżenia poziomu akceptowalnego ryzyka, czyli decyzji, że obiekt jest właściwie chroniony dzięki istniejącym środkom zabezpieczenia;
- kryteriów akceptowania ryzyka;
- całkowitego kosztu utrzymania, np. wzrostu kosztów eksploatacji systemów alarmowych;
- koniecznego zwiększenia zasobów, np. konieczności rozbudowy systemu alarmowego.

Monitorowanie ryzyka może skutkować modyfikacją lub uzupełnieniem podejścia, metodyki lub używanych narzędzi w zależności od:
- zidentyfikowanych zmian w konfiguracji, w oprogramowaniu urządzeń itp.;
- iteracji szacowania ryzyka, np. podjęcia decyzji, kiedy akceptujemy ryzyko;
- celu procesu zarządzania ryzykiem w bezpieczeństwie informacji, którym może być na przykład ciągłość działania, odporność na incydenty czy zgodność z wymaganiami prawnymi i normami zabezpieczenia technicznego;
- przedmiotu zarządzania ryzykiem (np. organizacji, jednostki organizacyjnej, procesu informacyjnego, jego technicznego wdrożenia, aplikacji, połączenia z centrum monitorowania, utrzymania skuteczności systemu alarmowego na najwyższym poziomie).

Szacowanie ryzyka podczas realizacji planu zabezpieczenia obiektu

Podczas zabezpieczania obiektu, gdy wydaje się, że posiadamy wystarczające dane do wykonania zaplanowanego systemu ochrony, należy także uwzględnić potencjalne ryzyko wystąpienia nieprawidłowości. Najczęstsze przyczyny to m.in.:
- brak dostatecznych wytycznych dotyczących realizacji projektu zabezpieczenia albo zbyt dokładne zapisy (zawężające lub wręcz wskazujące konkretne rozwiązania techniczne), albo zbyt ogólnikowe wskazówki – nawet bez powołania się na standardy techniczne i wymagania prawne dotyczące zabezpieczenia obiektów;
- nieaktualna dokumentacja projektowa albo brak dokumentacji projektowej;
- niedostateczny nadzór nad przebiegiem realizacji projektu systemu zabezpieczeń obiektu

albo brak nadzoru;
- brak protokołów odbioru częściowych prac instalacyjnych i odpowiednich pomiarów elektrycznych;
- brak potwierdzenia wykonania funkcjonalno-użytkowych testów zainstalowanych systemów technicznych zabezpieczeń obiektu;
- nieuzgodnione z zamawiającym, wprowadzone przez wykonawcę zmiany sprzętowe i konfiguracyjne systemu zabezpieczeń;
- dokumentacja powykonawcza nieodpowiadająca stanowi rzeczywistemu lub wręcz mająca wady (np. brakuje dokładnego spisu zainstalowanych urządzeń).

Wymienione braki i wady stanowią typowe słabości zastosowanego w obiekcie systemu zabezpieczeń, które mogą być przyczyną wielu zagrożeń dotyczących obiektu i prowadzonej w nim działalności biznesowej (innymi słowy stanowią podatności na zagrożenia).

Zabezpieczając obiekt, należy uwzględnić szacowanie ryzyka na następujących etapach:

1. Projekt wstępny/koncepcja systemu zabezpieczeń. Po wizji lokalnej należy przeanalizować zagrożenia i wstępnie oszacować ryzyko. Informacji powinien udzielić również użytkownik obiektu-zleceniodawca. Po realizacji wstępnego projektu zabezpieczenia obiektu należy ponownie oszacować ryzyko i przedstawić wyniki użytkownikowi obiektu, który musi zadecydować, czy je akceptuje.
2. Projekt wykonawczy. Na tym etapie tworzy się projekt wykonawczy, w tym wskazuje rozwiązania techniczne i sposób zabezpieczenia z uwzględnieniem funkcjonalności systemu zabezpieczeń. Na tym etapie również powinna być możliwość oszacowania ryzyka, aby sprawdzić, czy zostały zachowane założone, adekwatne do zagrożeń poziomy zabezpieczenia obiektu.
3. Szacowanie ryzyka podczas realizacji zabezpieczenia obiektu. Obejmuje ono sprawdzenie prawidłowości zabezpieczenia obiektu i zgodności z zatwierdzoną dokumentacją projektową oraz zaakceptowanymi zmianami.
4. Szacowanie ryzyka podczas eksploatacji odebranego systemu zabezpieczenia obiektu – ciągłe monitorowanie stanu systemu zabezpieczeń obiektu w opisanych wyżej sytuacjach.

Przykładowe czynniki mające wpływ na podatność na zagrożenie

Oszacowanie ryzyka wymaga wskazania zagrożeń, ale także podatności na nie (słabości, które mogą być przyczyną zagrożeń). W cytowanej w poprzednich częściach artykułu normie ISO27001 wymienionych jest w załączniku wiele przykładów takich podatności, które mogą dotyczyć m.in.:

- sprzętu (np. wrażliwość na zmiany temperatury),
- sieci (np. złe połączenie kabli),
- personelu (np. nieobecność personelu),
- siedziby (np. brak fizycznej ochrony budynku),
- procedur w organizacji dotyczących bezpieczeństwa (np. brak regularnych audytów lub nieodpowiedni serwis).

W praktyce przy ustalaniu poziomu zagrożenia i adekwatności zabezpieczenia obiektu należy uwzględnić takie czynniki jak:

- kontekst organizacyjny i prawny obiektu – np. przeznaczenie obiektu, procesy biznesowe, jakie realizowane są w obiekcie, zasoby informacyjne, które wymagają ochrony ze względu na wymagania prawne;
- lokalizacja obiektu, środowisko naturalne, aspekty społeczne (np. możliwe manifestacje), lokalny ruch mogący utrudnić dojazd służb ratunkowych i interwencyjnych, lokalizacja innych obiektów mogących mieć wpływ na powstanie potencjalnych zagrożeń (np. stacji benzynowej), ewentualna obecność ogrodzenia wokół obiektu i stan tego ogrodzenia, lokalizacja obiektu na obszarze zagrożonym powodzią, możliwa obecność interesantów (także z firm trzecich) poruszających się po obiekcie, obsługa (serwis realizowany przez firmy zewnętrzne na terenie obiektu);
- konstrukcja głównego budynku, jego odporność na włamanie, cechy konstrukcyjne i architektoniczne budynku, które ułatwiają włamanie (stanowią podatności budynku na włamanie), np. niski parter, obecność gzymsu, dach połączony z dachem sąsiedniego budynku, nienadzorowane włazy techniczne, wejścia i klatki schodowe;
- to, czy stosowana jest ochrona fizyczna (osobowa), a także sposób takiego chronienia obiektu (np. ochrona czasowa, ochrona zapewniana przez pracowników firmy posia-

dającej koncesję na usługi ochrony fizycznej, dodatkowa ochrona grup interwencyjnych);
- funkcjonowanie zabezpieczeń elektronicznych i budowlano-mechanicznych w obiekcie, umożliwiających zdalne przesyłanie sygnałów alarmowych do lokalnych lub zdalnych centrów nadzoru;
- brak systemu alarmowego chroniącego obiekt;
- zagrożenie pożarem, zastosowane zabezpieczenie techniczne i wymagania prawne w tym zakresie, np. ewentualny brak zabezpieczenia systemem sygnalizacji pożarowej w miejscach o dużej podatności;
- inne zagrożenia – w tym środowiskowe, przestępcze i terrorystyczne.

Audyt zabezpieczenia technicznego obiektów powinien uwzględniać wyżej wymienione podatności, ale także procedury i wymagania. Ich zakres obejmuje m.in.:

1. Zabezpieczenia techniczne, specyfikę funkcjonalno-użytkową systemów alarmowych oraz zabezpieczenia budowlano-mechaniczne adekwatne do poziomu zidentyfikowanych zagrożeń.
2. Standardy i wymagania dotyczące ochrony obiektów, plany ochrony, specyficzne wymagania prawne, np. odnoszące się do utrzymania infrastruktury krytycznej, ochrony informacji niejawnych, ochrony danych osobowych, wymagania prawne w zakresie projektowania, instalacji i serwisowania systemów zabezpieczeń technicznych, wymagania prawne dotyczące bezpieczeństwa obsługi, instalacji i projektowania systemów przetwarzania danych.
3. Bezpieczeństwo zasobów ludzkich. Należy sprawdzić m.in. procedury, umowy i regulaminy dotyczące oświadczenia o zachowaniu poufności dotyczące pracowników zajmujących się ochroną fizyczną, portierów, pracowników zajmujących się serwisem technicznym, pracowników patrolujących lub interweniujących oraz innych pracowników i współpracowników uczestniczących bezpośrednio lub pośrednio w procesie bezpieczeństwa obiektu, a także zaangażowanie kierownictwa, tj. w zapewnienie bezpieczeństwa tej świadomości kierownictwa w zakresie bezpieczeństwa czy też podejmowanie decyzji w zakresie finansowania bezpieczeństwa obiektu;
4. Zabezpieczenia organizacyjne. Należą do nich procedury dotyczące eksploatacji i serwisu zabezpieczeń technicznych, ruchu osobowo-materiałowego, reagowania na zagrożenia (scenariusze działań), ochrony informacji, szacowania ryzyka i określania poziomu zagrożeń, zachowania ciągłości działania, stref ochrony i inne wymagania organizacyjne.

Mierniki skuteczności zabezpieczenia

Ocena skuteczności zabezpieczenia (jego efektywności) nie jest zadaniem łatwym, a wyniki mogą budzić kontrowersje. Przy określaniu mierników efektywności stosowanego zabezpieczenia organizacyjno-technicznego obiektów pomocne mogą być poniższe wskazówki zawarte w normie PN-ISO/IEC 27001.

„Organizacja powinna ocenić wyniki działań na rzecz bezpieczeństwa informacji oraz skuteczność systemu zarządzania bezpieczeństwem informacji. Organizacja powinna określić:

a) co należy monitorować i mierzyć, włączając w to procesy związane z bezpieczeństwem informacji i zabezpieczenia;
b) metody monitorowania, pomiaru, analizy i oceny, stosownie do potrzeb, w celu zapewnienia poprawności wyników;
c) kiedy należy monitorować i wykonywać pomiary;
d) kto powinien monitorować i wykonywać pomiary;
e) kiedy należy analizować i oceniać wyniki monitorowania i pomiarów;
f) kto powinien analizować i oceniać te wyniki.

Organizacja powinna zachować odpowiednie udokumentowane informacje jako dowód wyników monitorowania i pomiarów”[1].

Aby wybrane metody pomiarów zostały uznane za poprawne, ich wyniki powinny być porównywalne i powtarzalne.

Jedną z metod pomiarów skuteczności zabezpieczeń jest stosowanie różnych procedur ich testowania, takich jak:

[1] PN-ISO/IEC 27001 – *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

– zastosowanie narzędzi sprawdzających podatność czujek, central alarmowych i innych urządzeń zabezpieczających,
– wykonanie włamaniowych testów systemów zabezpieczeń – zasymulowanie włamania,
– dokonanie technicznych przeglądów urządzeń pod kątem funkcjonalno-użytkowym,
– przeanalizowanie skuteczności przekazywania przez system informacji o zagrożeniach lub informacji technicznych do centrów zarządzania bezpieczeństwem.

Należy wspomnieć o podstawowej zasadzie projektowania systemów zabezpieczeń: „przewidywany czas reakcji użytkownika systemu na zaistniałe zagrożenie powinien być krótszy od czasu, jaki jest potrzebny intruzowi na działania prowadzące do przejęcia kontroli nad chronionym dobrem”[2].

Matematycznie można to zaprezentować w następujący sposób:
tr < ta
tr = tb + td + ti +tn
ta= twe + trca + twy
gdzie:
tr – czas reakcji systemu ochrony na zaistniałe zagrożenie
ta – czas realizacji ataku na chroniony obiekt
tb – czas bezwładności systemu nadzoru
td – czas wykrywania zagrożenia przez elementy detekcyjne systemu alarmowego
ti – czas potrzebny na przekazanie informacji o zaistniałym zagrożeniu przez komórki systemu nadzoru
tn – czas fizycznej neutralizacji zagrożenia lub podjęcia kroków mających na celu przeciwdziałanie zaistniałemu zagrożeniu
twe – czas związany z koniecznością forsowania fizycznych zabezpieczeń systemu ochrony przez intruza podczas atakowania chronionego obiektu (etap wstępny)
trca – czas związany z realizacją konkretnych, zaplanowanych celów ataku na chroniony obiekt (etap zasadniczy)
twy – czas potrzebny intruzowi na sforsowanie fizycznych zabezpieczeń systemu ochrony podczas opuszczania chronionego obiektu

[2] Marcin Buczaj, *Strefowa organizacja systemów alarmowych w aspekcie realizacji założonych zadań ochrony w obiektach budowlanych*, *Zabezpieczenia* 5/2011.

Istnieją inne metody oceny skuteczności zabezpieczeń, które polegają na analizie matematycznej[3], ale w praktyce wykorzystuje się raczej proste, intuicyjne sposoby opisane wcześniej. Systematyczne przeprowadzanie audytu zabezpieczeń jest jedną ze skutecznych metod i powinien on być stałym elementem monitorowania stanu zabezpieczenia technicznego obiektu.

Podsumowanie

W tej części artykułu poruszone zostały kwestie, które są często pomijane podczas przeprowadzania audytu dotyczącego bezpieczeństwa czy ekspertyzy dotyczącej stanu zabezpieczenia obiektu. Jedna z nich to potrzebą posiadania danych wyjściowych, jakimi są wyniki oszacowania ryzyka i plan postępowania z ryzykiem. Takie dane powinien otrzymać projektant, aby przygotować projekt zabezpieczenia obiektu adekwatnie do poziomu potencjalnych zagrożeń. Kolejna kwestia, która jest bardziej związana z wykonaniem zabezpieczeń, to wskazanie w procesie realizacyjnym momentów, w których należy oszacować ryzyko w celu weryfikacji działań projektanta i wykonawcy. Podczas analizowania ryzyka należy zwrócić uwagę na podatności obiektu na zagrożenia. Bardzo ważna jest również ocena skuteczności zastosowanych w obiekcie zabezpieczeń. Następna część artykułu będzie dotyczyła sposobu monitorowania i utrzymywania odpowiedniego poziomu bezpieczeństwa, przeciwdziałania incydentom i reagowania na nie, a także infrastruktury technicznej służącej do zabezpieczania obiektów.

Andrzej Wójcik

Opracował
dr inż. Andrzej Wójcik
ekspert i rzeczoznawca ds. bezpieczeństwa technicznego i ochrony informacji
audytor ds. bezpieczeństwa biznesu
andrzejw@esinstal.pl

[3] Marek Szulim, Marek Kuchta, *Metoda analizy skuteczności systemu bezpieczeństwa obiektu*, Biuletyn Wojskowej Akademii Technicznej vol. LIX, nr 4/2010.

Osiągnij nieosiągalne

ePoE

800 m ePoE redukuje okablowanie i zmniejsza koszty

Technologia ePoE

- Rozszerzona transmisja PoE: 800 m; 10 Mbps; 13 W lub 300 m; 100 Mbps; 24,4 W
- Automatyczna konfiguracja - Plug & Play
- Duży wybór kamer IP, rejestratorów i switchy posiadających możliwości ePoE
- Migracja z technologii analogowej do IP: obraz IP, dźwięk, zarządzanie i zasilanie przez kabel koncentryczny

Produkty ePoE

Kamery kompaktowe
IPC-HF5231E-E
IPC-HF5431E-E

Kamera tulejowa IR
IPC-HFW5231E-ZE/Z5E/Z12E
IPC-HFW5431E-ZE/Z5E
IPC-HFW5631E-ZE/Z5E
IPC-HFW5831E-ZE/Z5E

Kamery wandaloodporne
IPC-HDBW5231E-ZE/Z5E
IPC-HDBW5431E-ZE/Z5E
IPC-HDBW5631E-ZE/Z5E
IPC-HDBW5831E-ZE/Z5E

Rejestratory IP
NVR5216-16P-4KS2E
NVR5416-16P-4KS2E
NVR5816-16P-4KS2E

Switch
PFL2106-4ET-96

ePoE przez kabel koncentryczny
LR1002

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

EV-WL12DAM

Zewnętrzna czujka dualna o charakterystyce kurtynowej z dualnym antymaskingiem

Czujka (**PIR + MW**), dzięki niewielkim rozmiarom, idealnie nadaje się do ochrony elewacji oraz otworów drzwiowych, okiennych, balkonowych itp. Zastosowane materiały oraz poddanie procesowi tropikalizacji umożliwiają jej pracę w zmiennych warunkach zewnętrznych. Czujka tworzy wąską kurtynę (o szerokości 7,5°) oraz ma regulowany zasięg detekcji (maks. 12 m). Solidna konstrukcja i cyfrowa analiza sygnału z czujników PIR i MW sprawiają, że urządzenie jest wyjątkowo stabilne i odporne na fałszywe alarmy.

Charakterystyka	
Wyjścia alarmowe	alarm, sabotaż, antymasking
Stopień zabezpieczenia	Grade 3
Zasilanie	10-15 V_{DC}
Płaszczyzna pozioma	PIR=7,5°, MW=32°
Płaszczyzna pionowa	PIR=90°, MW=80°
Pobór prądu	25 mA
Pobór prądu w czasie czuwania	11 mA
Metoda detekcji	PIR + MW
Zasięg detekcji (m)	12
Charakterystyka detekcji	kurtynowa
Funkcje antymaskingu	antymasking MW + antymasking PIR
Wskaźnik LED	tak
Pamięć alarmów	tak
Regulacja czułości	tak
Wybór logiki AND/OR	tak/tak
Styk sabotażowy	tak
Zakres temperatury pracy	-20°C ~ 60°C
Klasa ochrony obudowy	IP54 (IP55 z osłoną EV-RAINCOVERWL12)
Wysokość montażu (m)	2,1
Montaż	ściana, otwór okienny
Kolor	biały
Wymiary (mm)	129 x 40 x 48 (z uchwytem ściennym), 129 x 45 x 52 (z uchwytem kątowym)
Akcesoria	uchwyt kątowy (w zestawie), uchwyt ścienny (w zestawie), uchwyt ścienny EV-BRACKETWL12 (opcjonalny), osłona EV-RAINCOVERWL12 (opcjonalna)

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

NVAHD-2DN3201MH/IR-1-PIR

Kamera AHD marki NOVUS z czujką PIR

NOVUS

Kamera **NVAHD-2DN3201MH/IR-1-PIR** została wyposażona w **czujkę PIR** o zasięgu do 8 m. Rekomendowana jest do obserwacji obszarów o dużym poziomie fałszywych alarmów generowanych przez funkcję detekcji ruchu, wywoływanych przez rozbłyski czy padające snopy światła. Alarm aktywowany jest przy jednoczesnym wystąpieniu wizyjnej i PIR-owskiej detekcji ruchu. Ogranicza to pojawianie się fałszywych alarmów i oszczędza przestrzeń dyskową poprzez rejestrację tylko faktycznych naruszeń chronionego obszaru.

Obraz	
Przetwornik obrazu	matryca CMOS 1/2.7" SMARTSENS
Liczba efektywnych pikseli	1936 (H) x 1096 (V)
Czułość	0,01 lx/F2.0 - tryb kolorowy 0 lx (IR wł.) - tryb czarno-biały
Obiektyw	
Typ obiektywu	standardowy, f=2,8 mm/F2.0
Dzień/noc	
Rodzaj przełączania	mechanicznie odsuwany filtr podczerwieni
Pozostałe funkcje	
Zdalne sterowanie	tak (protokół COAX)
Czujka PIR	zasięg do 8 m
Oświetlacz IR	
Liczba diod IR	18
Zasięg	20 m
Kąt świecenia	60°
Interfejsy	
Wyjście wizyjne	BNC, 1.0 V_{p-p}, 75 Ohm
Parametry instalacyjne	
Obudowa	aluminiowa, w kolorze białym, uchwyt ścienny z przepustem kablowym w zestawie
Zakres temperatury pracy	-30°C ~ 55°C

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

RWL-3
Bezprzewodowy zamek szafkowy

Zamek szafkowy **RWL-3** umożliwia bezprzewodową kontrolę dostępu do szafek i różnego rodzaju skrytek. Zamek RWL-3 może pracować w trybie autonomicznym (offline) lub sieciowym (online). W trybie autonomicznym RWL-3 steruje dostępem do szafki na podstawie danych konfiguracyjnych wprowadzonych do jego pamięci w trakcie programowania, które może być przeprowadzone manualnie, za pomocą karty programującej lub zdalnie, po nawiązaniu połączenia z poziomu programu RogerVDM. W trybie sieciowym zamek jest połączony bezprzewodowo z kontrolerem, który zarządza dostępem do szafki i rejestruje na bieżąco zdarzenia związane z obsługą zamka, w tym stany alarmowe. W scenariuszu online konfiguracja uprawnień dostępu jest realizowana z poziomu oprogramowania zarządzającego systemem RACS 5, które umożliwia elastyczne określenie zasad dostępu do szafek z uwzględnieniem kalendarzy, harmonogramów, poziomów dostępu i innych zaawansowanych mechanizmów stosowanych powszechnie w systemach kontroli dostępu. Zamek RWL-3 składa się z czytnika zbliżeniowego montowanego na zewnątrz szafki oraz zasobnika na baterie zespolonego z mechanizmem ryglującym, który jest montowany wewnątrz szafki. Zamek jest wyposażony w czujnik położenia rygla oraz wejście do podłączenia zewnętrznego czujnika otwarcia drzwiczek. W przypadku wyczerpania baterii zamek może być zasilany za pomocą zewnętrznego zasilacza podłączonego do czytnika zbliżeniowego.

Charakterystyka

- Bezprzewodowy zamek szafkowy
- Wbudowany czujnik położenia rygla
- Wejście do podłączenia zewnętrznego czujnika stanu drzwiczek
- Komunikacja bezprzewodowa - IEEE 802.15.4/2.4 GHz
- Zasięg komunikacji 10 m w otwartej przestrzeni
- Identyfikacja użytkowników przy użyciu kart zbliżeniowych ISO/IEC 14443A/MIFARE Ultralight/Classic/Plus/DESFire
- 4 wskaźniki LED oraz głośnik sygnalizacyjny
- Zasilanie z trzech baterii AA
- Typowy czas pracy 1 rok przy 10 odczytach dziennie
- Raportowanie stanu baterii do systemu kontroli dostępu
- Lokalna sygnalizacja niskiego stanu baterii
- Konfiguracja niskopoziomowa poprzez połączenie przewodowe lub bezprzewodowe z poziomu aplikacji RogerVDM
- Wymiary panelu zewnętrznego: 113,0 x 44,0 x 20,0 mm (wys. x szer. x grub.)
- Wymiary panelu wewnętrznego: 132,0 x 65,0 x 22,0 mm (wys. x szer. x grub.)
- Obsługa drzwi lewych i prawych
- Ochrona IP40
- Masa: ≈400,0 g
- Znak CE

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

MCT80M

Terminal dostępu do systemu RACS 5

MCT80M jest miniaturowym terminalem identyfikacji przeznaczonym do wykorzystania w systemie kontroli dostępu i automatyki budynkowej RACS 5. Terminal umożliwia rozpoznawanie użytkowników za pośrednictwem kart zbliżeniowych standardu 13,56 MHz MIFARE Ultralight i MIFARE Classic. MCT80M jest wyposażony w interfejs komunikacyjny RS485, dzięki któremu jest podłączony do kontrolera dostępu. Urządzenie może być instalowane na zewnątrz budynków bez konieczności stosowania dodatkowych zabezpieczeń. Ze względu na relatywnie małe wymiary czytnik może być montowany na drzwiczkach do różnego rodzaju szafek i schowków. Terminal jest zgodny z linią wzorniczą QUADRUS.

Charakterystyka

- Terminal dostępu do systemu RACS 5
- Czytnik 13,56 MHz MIFARE Ultralight/Classic
- 3 LED-y sygnalizacyjne
- Buzzer
- RS485
- Tamper
- Praca na zewnątrz
- Wymiary:
  100,0 x 45,0 x 16,0 mm (wys. x szer. x grub.)
- Linia wzornicza QUADRUS
- Znak CE

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 I

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

I 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

ALARM-TECH Systemy Zabezpieczeń s.c.
ul. Graniczna 4
32-086 Boleń
tel. kom. 775 453 453
e-mail: sklep@napad.pl
www.napad.pl

Oddział:
os. Jagiellońskie 19, 31-834 Kraków
tel. kom. 609 197 800

D PROD S

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

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

D

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

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: info@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

D I PROD PROJ

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; faks 22 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2
02-823 Warszawa
tel. 22 395 74 00
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 38/P1
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
ul. Główna 23
42-280 Częstochowa
tel. 34 333 57 04
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Św. Rocha 87, 42-202 Częstochowa
tel. 34 333 57 13
e-mail: czestochowa@eltrox.pl

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

ul. Myśliborska 2-6, 66-400 Gorzów Wlkp.
tel. 95 766 65 16
e-mail: gorzow@eltrox.pl

ul. Wybickiego 42a, 31-302 Kraków
tel. 12 210 06 25
e-mail: krakow@eltrox.pl

ul. 6 sierpnia 14, 90-416 Łódź
tel. 42 233 49 96
e-mail: lodz@eltrox.pl

ul. Orla 7/I, 41-205 Sosnowiec
tel. kom. 501 945 219
e-mail: sosnowiec@eltrox.pl

ul. ks. kard. S. Wyszyńskiego 22
70-203 Szczecin
tel. 91 443 56 36
e-mail: szczecin@eltrox.pl

ul. Joachima Lelewela 33, 87-100 Toruń
tel. 56 645 94 24
e-mail: torun@eltrox.pl

ul. Radzymińska 308, 03-694 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Komandorska 53R, 50-258 Wrocław
tel. kom. 504 904 689
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
www.estpolska.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

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 EUROPE LTD.
Biuro w Polsce
ul. Posag 7 Panien 1
02-495 Warszawa
e-mail: hte.poland@hanwha.com
www.hanwha-security.eu

B C D PROD 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

C D I PROD 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 S.A.
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
Paweł Karczmarzyk
Andrzej Walczyk

Korekta
Paweł Karczmarzyk

Dział marketingu i reklamy
Ela Końka

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

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, 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

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

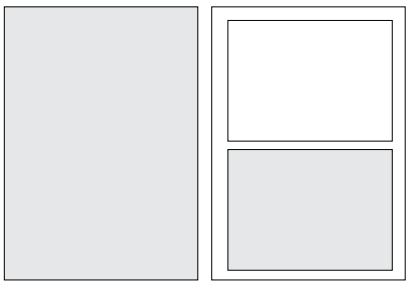
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

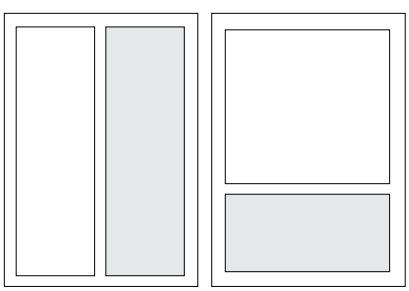
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

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



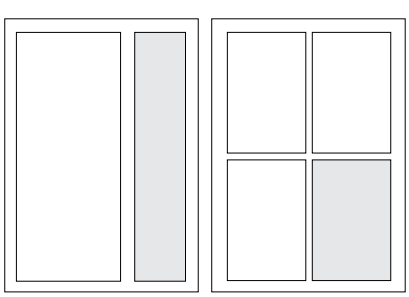
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

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

GENEVO

Systemy alarmowe nowej generacji

PRiMA 64

Hybrydowy system alarmowy z komunikatorem GSM/GPRS

- 64 wejścia - przewodowe i bezprzewodowe
- Programowalne wyjścia z funkcjami logicznymi
- Aplikacje dla urządzeń mobilnych iOS i Android
- Zdalne programowanie przez chmurę
- Wsparcie techniczne dla instalatorów

POLSKI PRODUCENT ◦ POLSKI PRODUKT

+48 58 380 07 05 · +48 605 919 926
www.genevo.pl · info@genevo.pl