DLA TYCH, KTÓRZY CHCĄ WYMIENIĆ SYSTEM ZABEZPIECZEŃ, ALE WSTYDZĄ SIĘ ZAPYTAĆ

Andrzej TOMCZAK

„Ludzie mają wrodzony talent do wybierania właśnie tego, co dla nich najgorsze"
J.K. Rowling

Truizmem zdaje się być, iż podjęcie prawidłowej decyzji o wymianie lub wyborze elektronicznego systemu zabezpieczeń (ESZ) wymaga dogłębnej wiedzy, dotyczącej zarówno spraw technicznych, zasad sztuki i dobrej praktyki tworzenia sytemu ochrony, jak i uwarunkowań lokalnych, związanych z chronionym obiektem. Rozsądnym jest więc sięgnięcie w takiej sytuacji do wiedzy eksperckiej. Wielokrotnie proszono mnie o przekazanie wskazówek, dotyczących wymiany na nowy aktualnie użytkowanego systemu sygnalizacji włamania i napadu (SSWiN), kontroli dostępu (SKD) lub dozoru wizyjnego (CCTV[1], VSS[2]). Najczęściej pada sakramentalne pytanie: jaki system wybrać i dlaczego? Oferta rynku systemów zabezpieczeń jest dość obszerna, jednakże nie do każdego obiektu łatwo dopasować nowe rozwiązanie. Często ograniczenia wynikające ze specyficznych wymagań bardzo zawężają możliwości prawidłowego wyboru sprzętu. Niestety wielu inwestorów polega na wiedzy firm sprzedających systemy, a handlowcy nie zawsze rzetelnie doradzają w tym zakresie. Poniżej kilka uwag i przemyśleń na ten temat, napisanych w formie popularnonaukowej.

[1] **CCTV** – telewizja w sieci zamkniętej (ang. *Closed Circuit TeleVision*)
[2] **VSS** – system dozoru wizyjnego (ang. *Video Surveillance System*)

Struktura i rodzaje okablowania wewnętrznego systemów zabezpieczeń

Transmisja po magistrali RS-485

Ponad 30 lat temu powstał przemysłowy standard komunikacji szeregowej RS-485, który z powodzeniem jest wykorzystywany do dzisiaj. Co więcej, tworzy się na jego podstawie specjalistyczne standardy komunikacji pomiędzy urządzeniami, takie jak MODBUS RTU czy DMX512. Również większość systemów alarmowych i kontroli dostępu wykorzystywała transmisję po magistrali RS-485 (aktualnie można przyjąć, że część systemów w dalszym ciągu wykorzystuje magistralę RS-485, a pozostałe korzystają z transmisji po komputerowej sieci Ethernet). Magistrala zrealizowana w przemysłowym standardzie komunikacyjnym RS-485, której długość może osiągnąć 1200 m, jest przede wszystkim bardzo odporna na zakłócenia i pozwala na podłączanie od 1 do 32 urządzeń adresowalnych. Ze względu na stosunkowo niską prędkość transmisji ≥ 100 Kb/s (ale w zupełności wystarczającą na potrzeby systemów alarmowych i kontroli dostępu) przewodom nie są stawiane zbyt wygórowane wymagania – wystarczy np. skrętka telekomunikacyjna kat. 3. Poglądowy schemat przyłączania urządzeń do magistrali RS-485 pokazano na rys. 1. Podłączanym urządzeniem adresowalnym może być np. podcentrala alarmowa, centrala kontroli dostępu (kontroler), czy też czujka alarmowa, wykonana w wersji magistralowej. Jakie są zalety systemów wykorzystujących magistralę RS-485?

1. Ze względu na magistralowy charakter połączeń można ułożyć znacznie mniej przewodów.

2. Instalację można układać tańszymi przewodami, przy zachowaniu bardzo wysokiej odporności na zakłócenia.

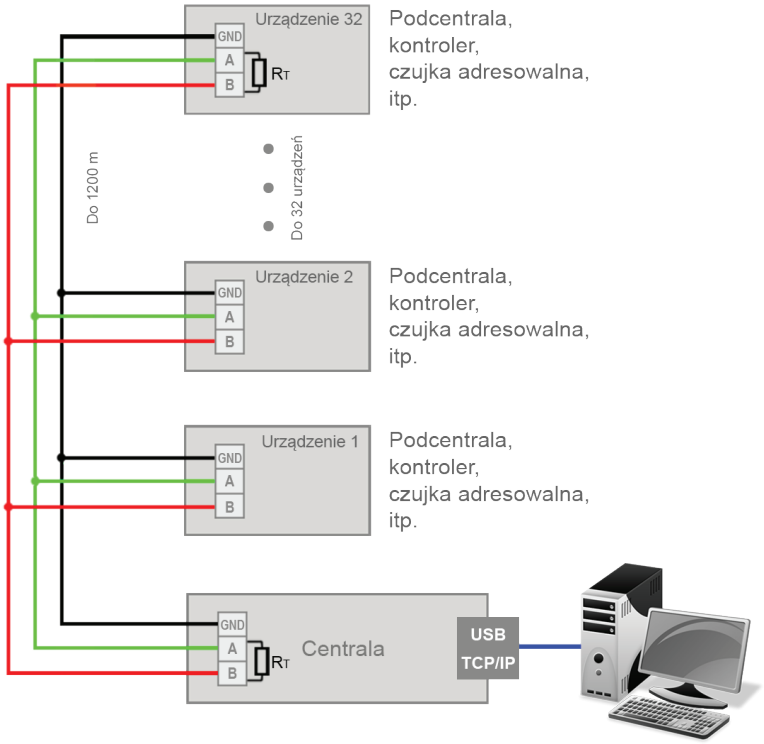
3. Długość magistrali może przekroczyć 1 km.

4. Rozwiązanie jest energooszczędne i bez problemu można spełnić wymogi zagwarantowania podtrzymania zasilania na wypadek zaniku napięcia sieci energetycznej zasilającej system.

5. Producent dostarcza urządzenia adresowalne odpowiadające za funkcje wykonawcze oraz za transmisję wewnętrzną pomiędzy urządzeniami, a więc gwarantuje bezpieczeństwo działania całego systemu. Dzięki temu może też bez problemu wykonać pełną certyfikację systemu, a nie tylko poszczególnych urządzeń (co ma miejsce w przypadku systemów wykorzystujących transmisję po sieci Ethernet). Do tematu certyfikacji wrócimy pod koniec artykułu.

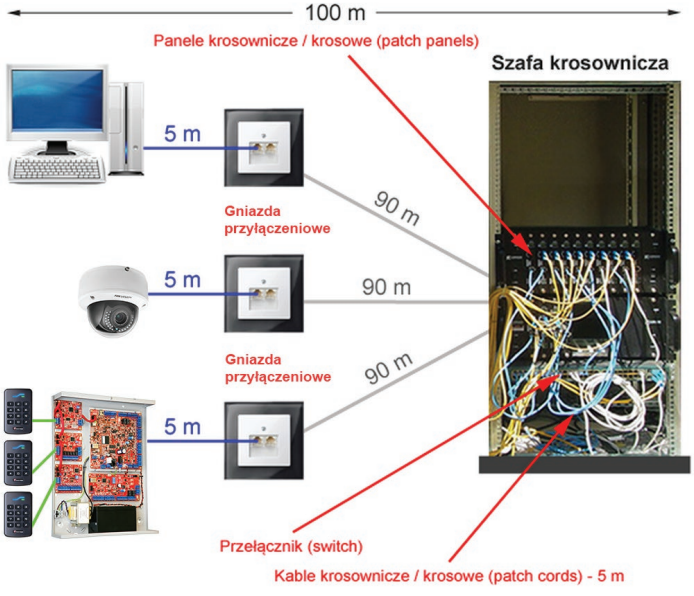
Transmisja po sieci Ethernet

Od kilkunastu lat coraz popularniejsze staje się wykorzystywanie sieci Ethernet do transmisji danych, również w systemach zabezpieczeń. Niewątpliwą wartością, jaką przedstawia sobą tego typu transmisja, jest możliwość przekazywania informacji z dużą prędkością, co ma znaczenie przy transmitowaniu dużej ilości danych, tak jak to ma miejsce w przypadku przesyłaniu wizji, a co nie ma już takiego znaczenia w przypadku systemów kontroli dostępu, czy też sygnalizacji włamania i napadu, w których transmituje się stosunkowo mało danych. Zalety transmisji po sieci Ethernet można również wykorzystać przy przesyłaniu danych na duże odległości. W tym momencie kończą się zalety w wykorzystywania sieci komputerowej na potrzeby systemów zabezpieczeń. Żeby lepiej zrozumieć problem, należy oddzielnie od innych analizować systemy transmitujące wizję i systemy przekazujące dane na duże odległości.

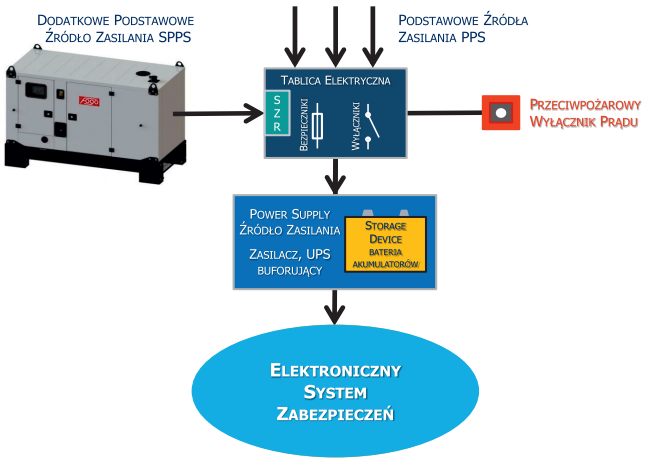


Rys. 1. Przykładowy schemat podłączania urządzeń do magistrali RS-485

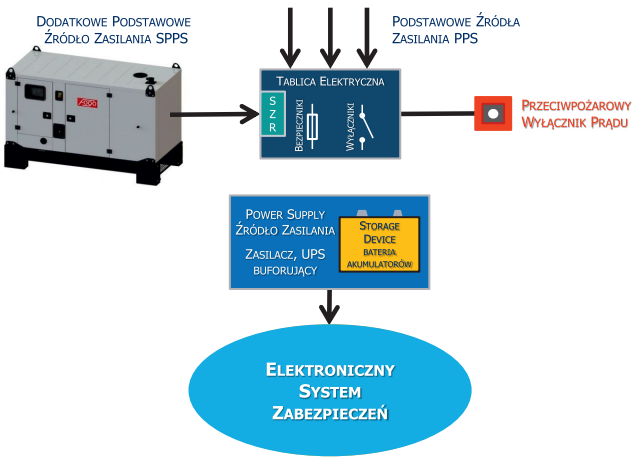
W przypadku najpopularniejszych przewodów miedzianych bezpośrednia transmisja w sieci Ethernet ma zasięg maks. 100 m. Aby dane mogły powędrować na większe odległości potrzebne będą dodatkowe urządzenia, zainstalowane w sieci, np. przełączniki sieciowe (rys. 2).



Rys. 2. Przykładowy schemat podłączania urządzeń do sieci Ethernet



Rys. 3a. Zasada prawidłowego zasilania systemu zabezpieczeń, wyposażonego w agregat prądotwórczy lub centralny UPS



Rys. 3b. Mimo zastosowania agregatu prądotwórczego lub centralnego zasilacza typu UPS, w momencie zaniku lub wyłączenia zasilania zewnętrznego, system powinien działać z buforowanego zasilania lokalnego przez min. 4 h

W momencie podjęcia decyzji wykorzystania systemu zabezpieczeń wykorzystującego Ethernet do transmisji wewnętrznej, sytuacja inwestora ulega dramatycznej zmianie. W przypadku magistrali RS-485 wszystkie urządzenia potrzebne do wykonania systemu dostarczał producent, natomiast w przypadku rozwiązań sieciowych do działania systemu konieczny jest element obcy – sieć komputerowa.

W przypadku magistrali RS-485 wszystkie urządzenia potrzebne do wykonania systemu dostarczał producent, natomiast w przypadku rozwiązań sieciowych do działania systemu konieczny jest element obcy – sieć komputerowa.

Patrząc pod tym kątem widzimy, że producenci systemów sieciowych idą, w pewnym sensie, na łatwiznę, w porównaniu z dostawcami systemów wykorzystujących magistralę RS-485. Ich systemy nie mogą działać bez obcego medium transmisyjnego, jakim jest sieć komputerowa. Ma to proste odzwierciedlenie w kosztach systemu. W przypadku systemu opartego na RS-485 kosztem dodatkowym jest kabel magistralowy, zaś w przypadku rozwiązań wykorzystujących sieć komputerową, kosztem dodatkowym jest okablowanie, układane w gwiazdę pomiędzy urządzeniem a węzłem sieci, oraz sama sieć komputerowa, której cena może czasami wielokrotnie przekraczać koszt systemu zabezpieczeń.

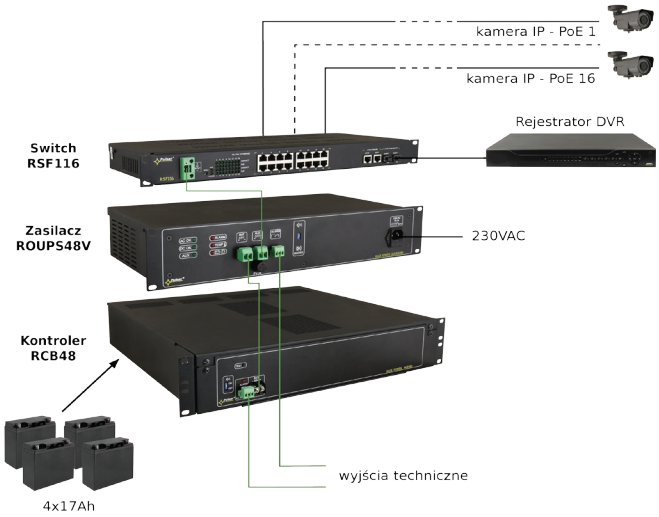
Powyższa analiza powinna być zrozumiała nawet dla osób niezagłębiających się w techniczne zawiłości prawidłowego tworzenia systemów zabezpieczeń. Obrazowo przedstawiając sytuację, producent systemu zabezpieczeń z komunikacją wewnętrzną opartą na RS-485 daje gotowe, bezpieczne rozwiązanie „pod klucz", zaś dostarczający system wykorzystujący do komunikacji wewnętrznej sieć komputerową przerzuca na inwestora stworzenie medium komunikacyjnego, którego bezpieczeństwo zależy od wielu czynników, np. od nakładów poniesionych na projektowanie i budowę sieci, od rzetelnej pracy wyspecjalizowanych administratorów, których zatrudnienie będzie stałym kosztem eksploatacji systemu, jak również od tego, czy sieć została wydzielona wyłącznie na potrzeby systemu zabezpieczeń, czy też system zabezpieczeń współdzieli sieć z innymi systemami.

Tu kończy się wiedza popularnonaukowa. Kolejnym elementem układanki są zasady tworzenia systemów zabezpieczeń określone w przepisach i normach. Trzeba pamiętać „o tym, że w momencie podłączenia do sieci Ethernet urządzeń ESZ sieć komputerowa staje się częścią systemu zabezpieczeń, a więc obowiązują dla niej takie same wymagania, jak dla innych elementów danego systemu zabezpieczeń. Dotyczy to ograniczenia dostępu, zabezpieczenia mechanicznego przed dostępem, ochrony antysabotażowej i oczywiście… zasilania"[3]. Zainteresowanych szczegółami odsyłam do [1], [2] i [3] pozycji literatury.

Trzeba pamiętać o tym, że w momencie podłączenia do sieci Ethernet urządzeń elektronicznego systemu zabezpieczeń (ESZ), sieć komputerowa staje się częścią systemu zabezpieczeń, a więc obowiązują dla niej takie same wymagania, jak dla innych elementów danego systemu zabezpieczeń. Dotyczy to ograniczenia dostępu, zabezpieczenia mechanicznego przed dostępem, ochrony antysabotażowej i oczywiście… zasilania.

W momencie, gdy sieć komputerowa przestanie prawidłowo działać traci się komunikację wewnętrzną w systemie zabezpieczeń, co jest poważnym zagrożeniem dla bezpieczeństwa. Dlatego tak ważne jest prawidłowe zaprojektowanie sieci komputerowej na potrzeby systemu zabezpieczeń, biorąc pod uwagę jej redundancyjność oraz prawidłowe zasilanie urządzeń aktywnych sieci. Nie wchodząc głęboko w szczegóły, opisane w poz. [1], [2]

[3] A. Tomczak: *Zasilanie sieciowych systemów zabezpieczeń na cenzurowanym.* SEC&AS, nr 5/2018, s. 72.



Zespół zasilający VSS IP: 16-portowy przełącznik sieciowy PoE – RSF116; zasilacz buforowy 54 V – ROUPS48V; kontroler akumulatorów – RCB48V (w środku kontrolera znajduje się pakiet akumulatorów 4 x 17 Ah / 12 V)

Rys. 3c. Wymóg 4-godzinnego podtrzymania, przedstawiony na rys. 3b, dotyczy również urządzeń aktywnych sieci odpowiedzialnych za transmisję wewnątrz systemu, zasilanych lokalnie np. za pomocą zasilaczy wyposażonych w baterię akumulatorów

Na podstawie poz. [2] i [3] literatury

i [3] literatury, należy przyjąć do wiadomości, że zgodnie z normami i przepisami prawa sieć komputerowa powinna być zasilana w taki sposób, aby po zaniku napięcia sieci energetycznej podtrzymać transmisję wewnątrz systemu przez określony czas. Jeżeli jest to np. 12 h, to zasilanie każdego urządzenia sieciowego, biorącego udział w transmisji danych wewnątrz systemu powinno być podtrzymywane awaryjnie przez 12 h. Jeżeli do tego celu zastosuje się agregat prądotwórczy lub centralny UPS, to wówczas każde urządzenie powinno mieć dodatkowo lokalne podtrzymanie przez min. 4 h. Wymóg ten dotyczy również zasilania aktywnych urządzeń sieci komputerowej, odpowiedzialnych za transmisję wewnątrz systemu np. przełączników-sieciowych (rys. 3).

Jeżeli do zagwarantowania zasilania ESZ zastosuje się agregat prądotwórczy lub centralny UPS, to wówczas każde urządzenie powinno mieć dodatkowo lokalne podtrzymanie przez min. 4 h. Wymóg ten dotyczy również zasilania aktywnych urządzeń sieci komputerowej, odpowiedzialnych za transmisję wewnątrz systemu np. przełączników sieciowych.

Reasumując, tworzenie systemów zabezpieczeń wykorzystujących do transmisji sieć komputerową może przy pierwszym spojrzeniu wydawać się atrakcyjne, jednakże rzeczywiste koszty stworzenia i eksploatacji prawidłowo zbudowanego systemu wykorzystującego do transmisji sieć Ethernet mogą być bardzo wysokie i nie mieć żadnego uzasadnienia ekonomicznego.

Wybieranie ESZ na wymianę

Podchodząc do tego problemu metodycznie, jasnym się staje, że pierwszym wyborem powinien być system o podobnej strukturze okablowania do poprzedniego. Oczywistym jest, że jeżeli wybierzemy nowy system o podobnej strukturze i rodzaju okablowania, a nasze „stare" kable są w dobrym stanie (jeżeli instalacja była prowadzona wewnątrz budynku, to zapewne zwykle będzie to prawda), wymiana systemu będzie sprowadzała się głównie do wymiany starego sprzętu na nowy. Nie trzeba będzie kuć ścian i wykonywać w szerokim zakresie dodatkowego remontu budowlanego. Jeżeli nasz „stary" system miał komunikację wewnętrzną wykorzystującą magistralę RS-485 to w pierwszym podejściu szukamy systemu o podobnej strukturze, nie dając się zwieść „nowoczesności" i „przyszłości" rozwiązań wykorzystujących do transmisji wewnętrznej sieć komputerową. Jeżeli nasz dotychczasowy system wykorzystywał transmisję po sieci Ethernet, wówczas sytuacja się komplikuje. Jeżeli bezpieczeństwo jest naszym priorytetem, to warto rozważyć możliwość odejścia od transmisji po sieciowej komputerowej, bo i tak rzadko taka instalacja była prawidłowo wykonana. Albo zainwestować dodatkowe środki (z reguły niemałe) w dostosowanie sieci komputerowej do wymogów prawa i norm.

Certyfikacja i poświadczanie zgodności systemów

Zatrzymajmy się na chwilę przy tematach certyfikacji, a właściwie potwierdzania zgodności. Brzmi trochę tajemniczo, ale dotyczy dość oczywistej czynności. Inwestorowi bardzo często zależy, aby system spełniał jakieś wymagania i normy. Na przykład był wykonany w konkretnym stopniu zabezpieczenia[4], powiedzmy w 3. stopniu zabezpieczenia. Wówczas (w uproszczeniu) instalator po zakończeniu prac powinien dostarczyć dokument potwierdzający wykonanie systemu w 3. stopniu zabezpieczenia.
W przypadku systemu wykorzystującego magistralę RS-485 może to zrobić bez problemu. Jeżeli producent przebadał swój system i dostarczył odpowiedni dokument np. deklarację zgodności systemu w 3. stopniu zabezpieczenia, a wykonawca zastosował zalecane przez producenta

[4] Normy na elektroniczne systemy zabezpieczeń (sygnalizacji włamania i napadu, kontroli dostępu, dozoru wizyjnego) wprowadzają klasyfikację systemów wg tzw. stopni zabezpieczenia, od stopnia 1. (najniższego), do stopnia 4. (najwyższego).

okablowanie i zainstalował system zgodnie z instrukcją, potwierdzenie zgodności będzie czystą formalnością. W przypadku systemów wykorzystujących sieć komputerową, sytuacja jest dużo bardziej skomplikowana. Producent może dostarczyć np. deklaracje wykonania urządzeń w 3. stopniu zabezpieczenia, ale nie może być to jedyną podstawą dla wykonawcy do zadeklarowania zgodności wykonania systemu w 3. stopniu zabezpieczenia. Producent nie jest bowiem w stanie przewidzieć, do jakiej sieci komputerowej jego urządzenia zostaną podłączone. Czyli na podstawie tego, że producent zadeklarował wykonanie urządzeń w 3. stopniu zabezpieczenia, instalator nie ma prawa uznać, że podłączając je do obcego medium transmisyjnego (sieci komputerowej), które tym samym zostało włączone w system zabezpieczeń, system spełnia wymagania określonego stopnia zabezpieczenia.

Na podstawie tego, że producent zadeklarował wykonanie urządzeń w określonym stopniu zabezpieczenia, instalator nie ma prawa uznać, że podłączając je do obcego medium transmisyjnego (sieci komputerowej), które tym samym zostało włączone w system zabezpieczeń, cały system spełnia wymagania danego stopnia zabezpieczenia.

Należy przeprowadzić badania całego systemu, opisane w odpowiednich normach, i dopiero po pozytywnej weryfikacji wyników badań określić stopień zabezpieczenia wykonanego systemu. Wydaje się trudne i kosztowne? Zapewne dlatego w czasie wieloletniej praktyki eksperta nie natrafiłem na system wykorzystujący do komunikacji wewnętrznej sieć komputerową, który byłby po wykonaniu prawidłowo zweryfikowany.

Zamiast podsumowania

A co z systemami dozoru wizyjnego opartego na kamerach IP? Tu sytuacja również się komplikuje. Kiedyś mieliśmy wybór zerojedynkowy. Albo instalacja z kamerami PAL, o maksymalnej rozdzielczości ok. 0,4 Mpx, albo system z megapikselowymi kamerami IP, ze wszystkimi wadami i zaletami takiego rozwiązania. Od kilku lat sytuacja nie jest już tak jednoznaczna. Wprowadzenie na rynek rozwiązań z analogowymi kamerami HD dało instalatorom alternatywę. Nie można się więc dziwić, że tam gdzie tylko jest to możliwe, wielu inwestorów na świecie i w Polsce coraz częściej rezygnuje ze stosowania kamer IP. I na koniec uwaga, dotycząca podtrzymania zasilania systemów dozoru wizyjnego w przypadku zaniku zasilania z sieci energetycznej – w niektórych obiektach obowiązują normy i wytyczne wielogodzinnego awaryjnego podtrzymania zasilania takiego systemu. Dotychczas w trakcie żadnej z wykonanych przeze mnie ekspertyz nie stwierdziłem wykonania prawidłowego podtrzymania awaryjnego sieci komputerowej wykorzystywanej do transmitowania danych wewnątrz systemu zabezpieczeń. Daje to dużo do myślenia.

A hasło pod tytułem „masz telewizję IP, dołącz inne systemy zabezpieczeń do sieci wykorzystywanej przez kamery" należy, w kontekście powyższego tekstu, traktować co najmniej jako nieżyczliwą radę, dobrze pasującą do motta tego artykułu.

Literatura:

[1] W. Kessler: *Stosowanie sieciowych systemów zabezpieczeń w obiektach IK i nie tylko…* SEC&AS, nr 5/2018, s. 56.

[2] A. Tomczak: *Zasilanie sieciowych systemów zabezpieczeń na cenzurowanym.* SEC&AS, nr 5/2018, s. 72.

[3] M. Dzioch: *Zasilacz buforowy. Źródło zasilania rezerwowego systemów z kamerami IP.* SEC&AS, nr 5/2018, s.77.

Andrzej TOMCZAK
Ekspert Polskiej Izby Systemów Alarmowych, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym