ZASILANIE SIECIOWYCH SYSTEMÓW ZABEZPIECZEŃ NA CENZUROWANYM

Andrzej TOMCZAK

Zagrożenia terrorystyczne, które spotęgowały się w ostatnich latach, nakłaniają do wnikliwej analizy stosowania elektronicznych systemów zabezpieczeń (ESZ). Specjaliści zaczęli zwracać baczniejszą uwagę na to, czy stosowane systemy mogą skutecznie zabezpieczać, czy też np. w sytuacjach ekstremalnych nie okażą się tylko bardzo drogimi i jednocześnie zupełnie nieprzydatnymi zabawkami. Skoncentrujemy się na wąskiej, acz witalnej tematyce, dotyczącej zasilania ESZ, a w szczególności sieciowych systemów zabezpieczeń. Nie będzie chyba odkrywczym stwierdzenie, że bez prądu zabezpieczenia elektroniczne nie będą działać. Po kilku latach prosperity sieciowych ESZ światowe statystyki notują spadki inwestycji w systemy oparte na sieciach komputerowych, co szczególnie jest widoczne w przypadku kamer IP. Coraz chętniej stosowane się kamery analogowe HD, często również w systemach hybrydowych z kamerami IP[1].

Źródło: materiały techniczne firmy Dell

O CZYM ZDAJĄ SIĘ ZAPOMINAĆ ZWOLENNICY WYKORZYSTANIA SIECI KOMPUTEROWYCH W ELEKTRONICZNYCH SYSTEMACH ZABEZPIECZEŃ?

Przede wszystkim o tym, że w momencie podłączenia do niej 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. Jeżeli jakiś system ma niezawodnie działać np. przez 12 h, to muszą działać wówczas zarówno urządzenia systemu, jak i komunikacja między nimi. A za tę komunikację w tym przypadku odpowiada sieć komputerowa (rys. 1). Bo jak sieć przestanie działać, np. w przypadku zaniku zasilania, to utraci się komunikację wewnątrz systemu. Można to wyjaśnić na prostym, ale dobitnym przykładzie – nie będzie można obserwować obrazu z kamer IP, bo najzwyczajniej w świecie nie będzie z nimi połączenia. Tak jakby ktoś poprzecinał przewody w tradycyjnym systemie (rys. 2).

[1] Zob. M. Maroszek: *Telewizja analogowa HD. Przegląd rynku*. SEC&AS, nr 4/2018, s. 94.

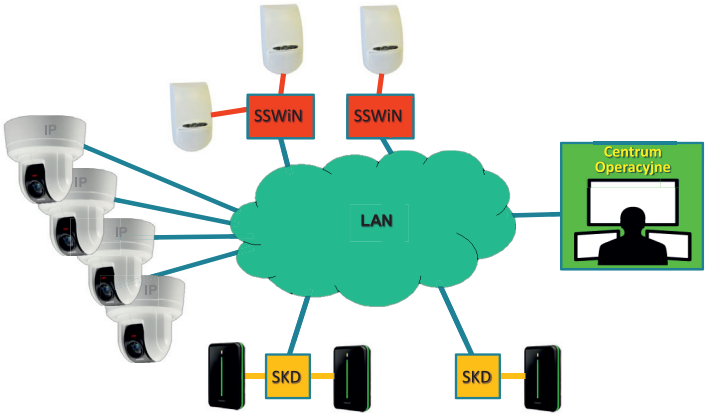
Jak wówczas wysłać zdalną informację o odblokowaniu przejść lub odwrotnie, o ich zablokowaniu w momencie ataku terrorystycznego? Nikogo chyba nie trzeba przekonywać, że taka sytuacja jest niedopuszczalna, szczególnie gdy zabezpieczane są ważne obiekty, np. infrastruktury krytycznej państwa (IK). Dlatego w sprawozdaniu *Zespołu zadaniowego do spraw opracowania standardów zabezpieczeń antyterrorystycznych i reguł współdziałania dotyczących infrastruktury krytycznej oraz zasad dokonywania sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej zgodnie z przepisami ustawy o działaniach antyterrorystycznych*, w którym określone zostały minimalne, ujednolicone wymagania m.in. w zakresie zapewnienia bezpieczeństwa fizycznego, przyjętym 28 czerwca 2018 r. przez Międzyresortowy Zespół ds. Zagrożeń Terrorystycznych, wiele miejsca poświęcono kwestii zgodnego z zasadami sztuki zasilania elektronicznych systemów zabezpieczeń.

> *Zaprojektowanie i wykonanie zasilania elektronicznych systemów zabezpieczeń zgodnie z zasadami sztuki jest szczególnie istotne, gdy zabezpieczane są ważne obiekty, np. infrastruktury krytycznej państwa.*

Te zasady zostały oparte na zapisach norm polskich, będących wprowadzeniem norm europejskich, oraz norm obronnych. Uznano, że w zakresie zasilania ESZ szczególnie wymagania norm obronnych będą dobrym wyznacznikiem standardów dla obiektów IK.

ZASADY SZTUKI PROJEKTOWANIA I WYKONYWANIA ZASILANIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

Zasilanie ESZ należy tak projektować, aby systemom zagwarantować bezprzerwowe dostarczanie energii, niezależnie od niekontrolowanego lub celowego działania czynników zewnętrznych, np. zaniku napięcia podstawowego źródła zasilania, wyłączenia obwodu zasilającego ESZ w tablicy elektrycznej czy też użycia przeciwpożarowego wyłącznika prądu. Podstawowe źródło zasilania (PPS – ang. *Prime Power Source*) to źródło energii umożliwiające długotrwałe zasilanie ESZ, np. sieć elektroenergetyczna. Dla poprawy niezawodności zasilania w obiektach wrażliwych stosuje się PPS dwustronne, a nawet wielostronne. W bardzo wrażliwych miejscach wykorzystuje się dodatkowe podstawowe źródło zasilania (SPPS – ang. *Supplementary Prime Power Source*) – niezależne w stosunku do PPS źródło energii, umożliwiające długotrwałe zasilanie ESZ, np. rezerwowy generator prądotwórczy. Należy jednak pamiętać, że w przypadku ESZ rozwiązanie zawierające PPS i SPPS nie jest wystarczające, ponieważ zasilanie ESZ nie jest uniezależnione od wpływów



Rys. 1. Połączenia wewnętrzne elektronicznych systemów zabezpieczeń, zrealizowane za pośrednictwem sieci komputerowej

Rys. 2. Zanik połączeń wewnętrznych elektronicznych systemów zabezpieczeń, zrealizowanych za pośrednictwem sieci komputerowej, w przypadku uszkodzenia lub braku zasilania sieci komputerowej

zewnętrznych. Omówione wyżej źródła zasilania określane są jako źródła zasilania zewnętrznego (EPS – ang. *External Power Source*). W przypadku zasilania elementów systemów napięciem 12 VDC[2], 24 VDC lub PoE[3] stosuje się zasilacze sieciowe AC[4]/DC, które są wyposażone w dodatkowe rezerwowe źródła zasilania APS (ang. *Alternative Power Source*) w postaci baterii akumulatorów. W przypadku konieczności zasilania elementów ESZ napięciem 230 VAC zamiast zasilaczy stosuje się lokalne UPS-y. Należy zwrócić uwagę na wymogi zapisów § 183. 1.6, § 183.2, § 183.3 oraz § 183.4 rozporządzenia Ministra Infrastruktury z dnia 12 kwietnia 2002 r. *w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie* (Dz.U. 2002, nr 75, poz. 690 z późn. zm.) oraz wpływ użycia przeciwpożarowego wyłącznika prądu, które powinno wyeliminować w budynku wszelkie napięcia wyższe niż napięcia dotykowe dopuszczalne długotrwale, nazywane też napięciami bezpiecznymi (z wyłączeniami określony-

[2] DC (ang. *Direct Current*) – prąd stały.

[3] PoE (ang. *Power over Ethernet*) – system zasilania urządzeń podłączanych do sieci komputerowej za pośrednictwem przewodu, którym następuje komunikacja z urządzeniami aktywnymi sieci.

[4] AC (ang. *Alternating Current)* – prąd przemienny.

mi w powyższym rozporządzeniu), na elektroniczne systemy zabezpieczeń (w tym na transmisję danych ESZ po sieci komputerowej).

Gdy przewidziano dodatkowe podstawowe źródło zasilania z automatycznym przełączaniem podstawowego źródła zasilania na dodatkowe podstawowe źródło zasilania, okres gotowości rezerwowego źródła wymagany do zasilania elektronicznych systemów zabezpieczeń może być zredukowany do 4 h.

Powyższe fachowe i lakoniczne zapisy wynikające z przepisów prawa i norm można wyjaśnić w sposób bardziej opisowy. Otóż podstawową ideą zasilania ESZ jest wprowadzenie, pomiędzy źródło zasilania a poszczególne zasilane elementy systemu, dodatkowego urządzenia zasilającego, buforowanego baterią akumulatorów. Urządzenia, które niezależnie od czynników zewnętrznych, zamierzonych lub niezamierzonych, zasilą przez założony czas elektroniczne systemy zabezpieczeń. I nie ma w tym nic odkrywczego dla specjalistów zajmujących się ESZ. Należy jednakże pamiętać, że sieci komputerowe, ze wszystkimi elementami aktywnymi, koniecznymi do ich prawidłowego działania, powinny być zasilane identycznie, jak reszta ESZ. A o tym już nie wszyscy, niestety, wiedzą.

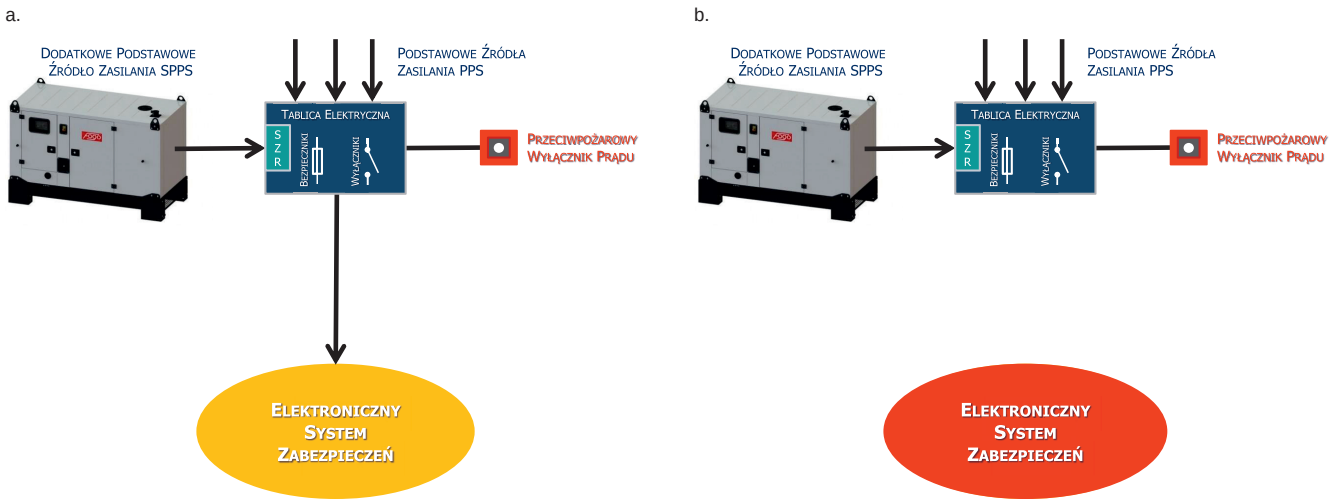
Należy pamiętać, że sieci komputerowe wykorzystywane w ESZ, ze wszystkimi elementami aktywnymi, koniecznymi do ich prawidłowego działania, powinny być zasilane identycznie, jak reszta elektronicznych systemów zabezpieczeń.

Na rys. 3 przedstawiono przykład standardu realizacji zasilania sieci komputerowych za pomocą tzw. napięcia gwarantowanego. Zastosowanie dodatkowo UPS-ów centralnych lub UPS-ów centralnych i rezerwowych agregatów prądotwórczych nie zmieni faktu, że dostarczanie energii zasilającej elektroniczny system zabezpieczeń lub sieć komputerową wykorzystywaną przez ESZ nie jest uniezależnione od wpływów zewnętrznych, będących np. wynikiem zamierzonych działań sabotażowych lub zgodnych z prawem działań mających miejsce w trakcie akcji ratowniczo-gaśniczej.

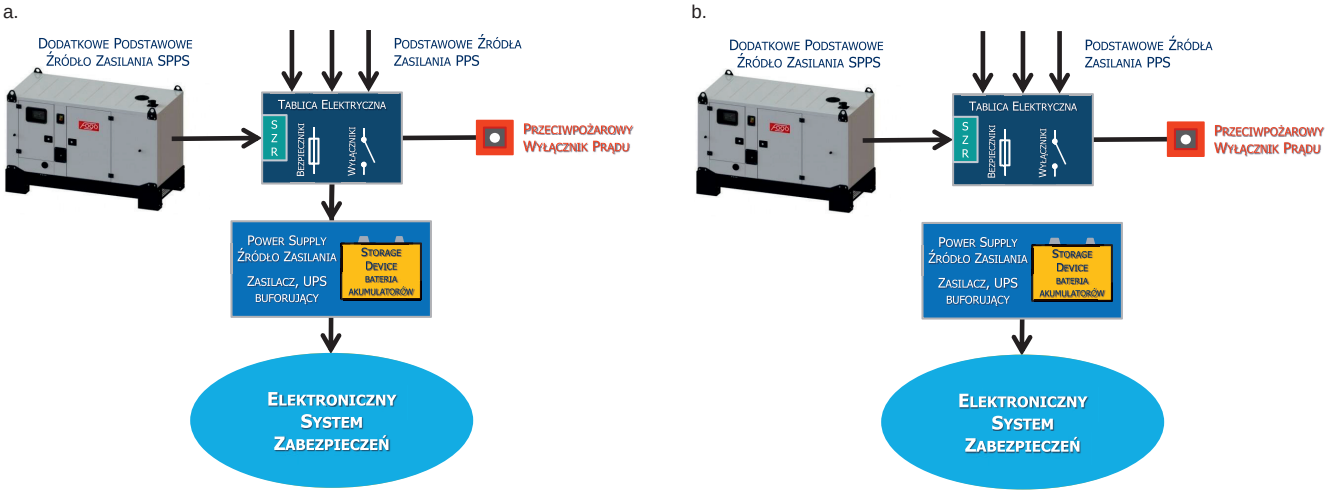
Na rys. 4 przedstawiono poprawny sposób realizacji zasilania elektronicznych systemów zabezpieczeń, jak również elementów aktywnych sieci komputerowych, wykorzystywanych do realizowania połączeń w ramach ESZ. Przy takiej konfiguracji, oczywistej dla branżowych specjalistów, system zabezpieczeń jest maksymalnie uniezależniony od wszelkich zamierzonych lub niezamierzonych działań zewnętrznych.

Z przedstawionych zasad sztuki realizowania zasilania ESZ wynika wprost, jak należy zasilać elementy aktywne, niezbędne do prawidłowego działania sieci komputerowej, wykorzystywanej do komunikacji wewnątrz elektronicznych systemów zabezpieczeń. Wynika z tego prosty wniosek, iż, tam, gdzie to tylko jest możliwe, należy unikać wykorzystywania sieci komputerowych do komunikacji wewnątrz ESZ. A szczególnie jest istotne, aby o tym pamiętać w przypadku ważnych obiektów, np. należących do infrastruktury krytycznej państwa.

W przypadku systemów sygnalizacji włamania i napadu (SSWiN) oraz systemów kontroli dostępu (SKD) na rynku jest wielu dostawców, którzy połączenia wewnętrzne realizują nie korzystając z sieci komputerowych. Z punktu widzenia powyższych systemów transmituje się tak mało informacji, że wykorzystanie szerokopasmowej sieci komputerowej nie ma technicznego uzasadnienia. To tak, jakby zastosować tira jako taksówkę osobową – olbrzymie koszty i wiele problemów. Powyższy przykład dobrze ilustruje podejście



Rys. 3. Nieprawidłowy sposób zasilania, mimo zastosowania rezerwowego agregatu prądotwórczego (a.) – ESZ przestaje działać w momencie ręcznego lub automatycznego wyłączenia zasilania zewnętrznego na poziomie tablic elektrycznych (b.)



Rys. 4. Prawidłowy sposób zasilania elektronicznych systemów zabezpieczeń i sieci komputerowych wykorzystywanych na potrzeby ESZ (a.) – w momencie ręcznego lub automatycznego wyłączenia zasilania zewnętrznego na poziomie tablic elektrycznych ESZ dalej działa (b.)

producentów tego typu systemów: ponieważ w obiektach z reguły występuje sieć komputerowa, można przecież dołożyć aplikacje, które mają odpowiadać za bezpieczeństwo osób i mienia – nie trzeba będzie układać dodatkowych przewodów, czyli: ponieważ tiry i tak jeżdżą, wykorzystajmy je przy okazji do wożenia pasażerów – na drogach będzie mniej taksówek.

W systemach SWiN oraz KD od dawna są wykorzystywane technologie pozwalające na bezpieczną transmisję sygnałów wewnętrznych w systemach zabezpieczeń na odległości powyżej 1 km. Dla przypomnienia maksymalny bezpośredni zakres transmisji w przypadku sieci komputerowej to, w uproszczeniu, tylko 100 m. Dalej zaczynają się urządzenia aktywne i kłopoty z zasilaniem realizowanym zgodnie z normami dla elektronicznych systemów zabezpieczeń. Na czym te kłopoty polegają? Oczywiście na nieuzasadnionych kosztach inwestycyjnych i eksploatacyjnych. Większość urządzeń aktywnych w sieciach komputerowych jest zasilana napięciem 230 VAC. Z tego wynika konieczność zastosowania do zasilania urządzeń, takich jak np. przełączniki sieciowe, lokalnych UPS-ów, działających przez minimum 4 h. Resztę czasu podtrzymania można zapewnić stosując rezerwowe agregaty prądotwórcze. Należy pamiętać, że czas życia akumulatorów stosowanych np. w UPS-ach to 3–5 lat i trzeba przewidzieć budżet na ich systematyczną konserwację oraz wymianę. W przypadku systemów SWiN oraz KD nie ma uzasadnienia stosowania w obiektach, szczególnie IK, lokalnych rozwiązań opartych na sieciach komputerowych, ponieważ powoduje to występowanie dodatkowych kosztów inwestycyjnych i eksploatacyjnych w momencie, gdy można zastosować dostępne od wielu lat rozwiązania, które nie mają tych wad.

WYKORZYSTYWANIE TRANSMISJI ZA POŚREDNICTWEM SIECI KOMPUTEROWYCH W ESZ

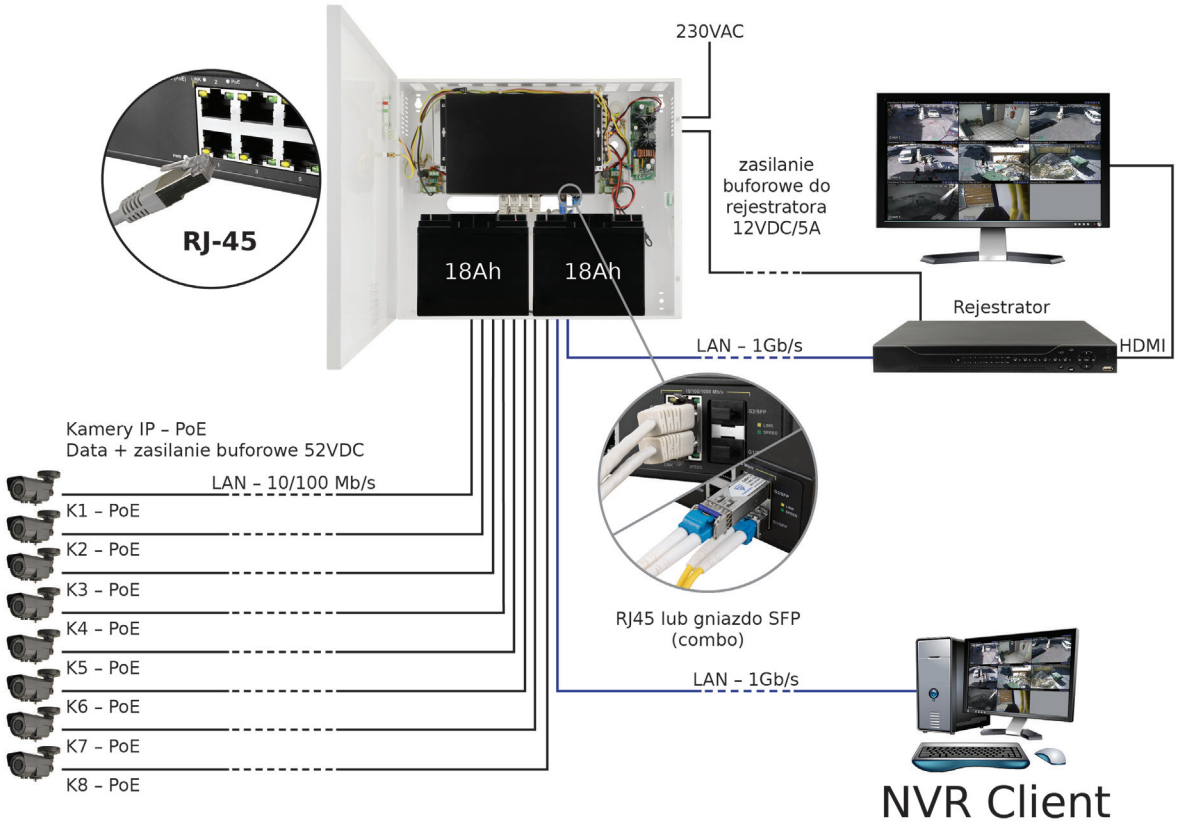
Do tej pory wykazano, że stosowanie transmisji za pośrednictwem sieci komputerowej nie ma uzasadnienia w przypadku systemów SWiN oraz KD, instalowanych w obiektach lokalnych, w których zachowanie bezpieczeństwa jest priorytetem. Inaczej sytuacja wygląda w przypadku sieciowych systemów dozoru wizyjnego. W odróżnieniu od SSWiN i SKD trzeba wówczas transmitować tak dużo informacji, że często nawet przepustowości sieci komputerowych okazują się niewystarczające. W tym przypadku z pomocą przychodzą nowe technologie analogowe, pozwalające przekazywać obraz HD za pośrednictwem przewodów stosowanych w tradycyjnych systemach, które wykorzystywały kamery PAL. Mają przy okazji dodatkową zaletę – brak opóźnień, co nie jest bez znaczenia przy zdalnym sterowaniu kamerami obrotowo-uchylnymi (PTZ). Oczywiście nie każdą kamerę IP da się zastąpić analogową kamerą HD. Producenci urządzeń zasilających przewidzieli możliwość zgodnego z zasadami sztuki realizowania systemów za pomocą kamer IP. Na rys. 5 pokazano przykład zasilacza do przełącznika sieciowego PoE, buforowanego baterią akumulatorów.

Wykorzystując przykład z tirami – w systemach dozoru wizyjnego mamy tyle „towaru", że do „transportu" musimy korzystać z ciężarówek, ze wszystkimi negatywnymi skutkami ich stosowania.

Gdzie jeszcze nie da się uniknąć stosowania sieci komputerowych w systemach zabezpieczeń? Na przykład w przypadku integrowania systemów czy też realizowania systemów rozproszonych. Ale wówczas albo wydzielamy sieć na potrzeby systemów zabezpieczeń i zasilamy ją zgodnie z zasadami sztuki, albo wykorzystujemy sieć komputerową do transmisji pomiędzy ESZ. A na tego typu rozwiązania obowiązują już zupełnie inne normy.

PODSUMOWANIE

Zasady zasilania urządzeń aktywnych sieci komputerowych wykorzystywanych na potrzeby ESZ są dobrze znane specjalistom z branży zabezpieczeń. Jednak codzienna praktyka pokazuje, że świadomość wśród inwestorów jest w tym zakresie niewystarczająca,



Rys. 5. Przykład zasilacza, buforowanego baterią akumulatorów, przeznaczonego do zasilania kamer IP, przełącznika sieciowego PoE i rejestratora NVR
Źródło: materiały techniczne firmy Pulsar

szczególnie wśród operatorów infrastruktury krytycznej państwa. Dlatego w dokumencie *Standardy zapewnienia bezpieczeństwa infrastruktury krytycznej. Zapewnienie bezpieczeństwa fizycznego – wymagania minimalne* poświęcono kilka stron na opisanie zasad prawidłowego zasilania elektronicznych systemów zabezpieczeń. I nie ma też w tym nic dziwnego, że skorzystano z zasad zasilania określonych w normach obronnych, wychodząc z założenia, że obiekt infrastruktury krytycznej państwa powinien w tym zakresie podlegać obowiązkom podobnym jak w przypadku obiektów wojskowych. A w normach obronnych najkrótszy czas podtrzymania zasilania systemów w przypadku zaniku napięcia podstawowego wynosi 12 h (maks. to 72 h), z czego min. 4 h muszą zapewnić lokalne urządzenia zasilające, buforowane bateriami akumulatorów.

Powyższy artykuł został dla ułatwienia percepcji napisany w sposób opisowy, unikając odnoszenia się do przepisów prawa oraz norm. Dociekliwi czytelnicy mogą zapoznać się ze szczegółami w literaturze, której wykaz został załączony.

Literatura:

[1] PN-EN 50131-1:2009 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe.* (PN-EN 50131-1:2009/A1:2010, PN-EN 50131-1:2009/A2:2017-07).
[2] PN-EN 50131-6:2017-12 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 6: Zasilacze.*
[3] PN-EN 50398-1:2017-10 *Systemy alarmowe. Systemy alarmowe łączone i zintegrowane. Część 1: Wymagania ogólne.*
[4] PN-EN 62676-1-1:2014-06 *Systemy dozorowe CCTV stosowane w zabezpieczeniach. Część 1-1: Wymagania systemowe. Postanowienia ogólne.*
[5] PN-EN 60839-11-1:2014-01 *Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i części składowych.*
[6] PN-EN 50518-1: 2014-07 *Centrum monitoringu i odbioru alarmu. Część 1: Wymagania dotyczące rozmieszczenia i konstrukcji.*
[7] NO-04-A004-1: 2016 *Obiekty wojskowe. Systemy alarmowe. Część 1: Wymagania ogólne.*
[8] NO-04-A004-6: 2016 *Obiekty wojskowe. Systemy alarmowe. Część 6: Wymagania dotyczące systemów kontroli dostępu.*
[9] NO-04-A004-7: 2016 *Obiekty wojskowe. Systemy alarmowe. Część 7: Wymagania dotyczące telewizyjnych systemów nadzoru.*
[10] NO-04-A004-8: 2016 *Obiekty wojskowe. Systemy alarmowe. Część 8: Eksploatacja.*
[11] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dn. 7 września 2010 r. *w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.* Dz.U. 2010, poz. 1128. z późn. zm.
[12] Sprawozdanie zespołu zadaniowego do spraw opracowania standardów zabezpieczeń antyterrorystycznych i reguł współdziałania dotyczących infrastruktury krytycznej oraz zasad dokonywania sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej, zgodnie z przepisami ustawy o działaniach antyterrorystycznych: *Standardy zapewnienia bezpieczeństwa infrastruktury krytycznej. Zapewnienie bezpieczeństwa fizycznego – wymagania minimalne.*

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym, redaktor naczelny SEC&AS