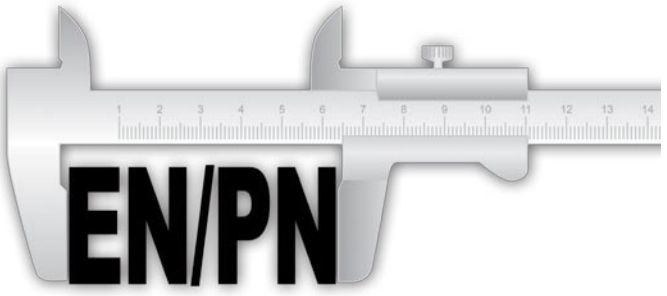
„Systemy Alarmowe" nr 2/2011
Czasopismo branży security



Nowe normy

na systemy i urządzenia transmisji alarmów włamaniowych i napadowych (1)

Jerzy W. Sobstel
CENELEC TC79/WG5

W poprzednim artykule opublikowanym na łamach SA [1] przedstawiłem aktualny stan normalizacji europejskiej w obszarze dotyczącym systemów monitoringu włamaniowego i napadowego oraz jej kontekst historyczny. Obecnie chciałbym omówić nowe normy, niedawno przyjęte przez CENELEC, a także dopiero opracowywane w grupach roboczych Komitetu Technicznego TC79 Alarm Systems tej organizacji.

Zacznę jednak od wyjaśnienia, dlaczego piszę o normach, które jeszcze nie zostały opublikowane po polsku lub nawet niezatwierdzone przez CENELEC, i to w sytuacji, gdy Polski Komitet Normalizacyjny tak agresywnie przekonuje wszystkich, że stosowanie norm jest nieobowiązkowe, a ich przywoływanie w aktach prawa często bywa (przynajmniej w interpretacji PKN) sprzeczne z prawem.

Porównując serię norm dotyczących monitoringu włamaniowego i napadowego (które omawiałem w [1]) z nowymi normami opracowywanymi w CENELEC, łatwo zauważyć istotną różnicę. Dostępne obecnie normy mają charakter przewodników dla konstruktorów systemów i urządzeń oraz ich użytkowników, wskazując, jak te systemy lub urządzenia należy poprawnie budować. Nowa seria norm jest nastawiona na odróżnianie rozwiązań dobrych od najlepszych lub tylko poprawnych.

Są to normy umożliwiające certyfikację urządzeń i systemów. Oczywiście certyfikację dobrowolną, wymuszaną jedynie przez grę rynkową prowadzoną przez konkurujące podmioty.

W wielu krajach oferowanie profesjonalnej usługi monitorowania bez takich certyfikatów jest już niemożliwe. Wymuszają to zarówno regulacje prawne, policja, ubezpieczyciele, jak i organizacje biznesowe, które inicjowały opracowanie niektórych norm. Wkrótce również w Polsce takimi certyfikatami będą się musiały wykazywać firmy, które chcą się liczyć na rynku, np. monitorować obiekty infrastruktury krytycznej. Jeszcze wcześniej wymaganiami powinny zainteresować się firmy, które zamierzają produkować urządzenia i systemy, eksportować swój sprzęt, oprogramowanie lub usługi. Te, które zdążą „przed premierą", będą miały szansę na rentę dodatkową nowości.

Cykl opracowywania nowej normy jest długi i bardzo często przekracza trzyletni okres normatywny. Zwykle w jego połowie już wiadomo, do czego nowe opracowanie zmierza, i pierwsza wersja projektu jest dostępna, zanim zostanie on skierowany do ankiety powszechnej. W niektórych krajach takie projekty są publikowane jako prenormy i można je nabyć (jak zwykłe normy). Po zakończeniu prac nad normą i jej zatwierdzeniu w głosowaniu powszechnym upływa jeszcze co najmniej pół roku, zanim zostanie ona ratyfikowana i opublikowana. W tym momencie firmy, które zaryzykowały i oparły swoje prace rozwojowe na prenormach, mają już dwa lata wyprzedzenia wobec firm, które czekały na publikację normy.

Nowa norma jest publikowana w języku angielskim (w przypadku norm CEN także po francusku i niemiecku). W języku polskim nawet tak ważne normy, jak EN 50131-1:2006, bywają udostępniane dopiero po trzech latach od publikacji oryginału. Czekające na nie firmy mają już pięć lat opóźnienia w porównaniu ze swoimi aktywnymi konkurentami. Wprawdzie nasze dwie wspaniałe organizacje: POLALARM oraz PISA trochę się ostatnio obudziły i wspierają tłumaczenie norm, jednak opóźnienia w udostępnianiu norm ciągle występują. Warto brać je pod uwagę przy wszystkich dyskusjach o (nie)innowacyjności naszej gospodarki.

Nowy garnitur norm dla monitoringu włamaniowego

Prace nad nowymi normami europejskimi dotyczącymi monitorowania systemów SSWN są prowadzone przez grupy robocze komitetu technicznego TC79 CENELEC. Wszystkie te normy powinny być dostępne w 2012 r. i wtedy zostaną przekazane do IEC do publikacji jako normy międzynarodowe.

Można je umownie podzielić na cztery grupy *(rys. 1)*, gdzie podano numery norm oraz scharakteryzowano ich przedmiot.

W dalszej części artykułu poszczególne normy zostaną omówione.

Systemy transmisji alarmów

Prace nad nową wersją normy na systemy transmisji alarmów są prowadzone przez grupę roboczą CLC/TC79 WG5 od 2004 r. Autor artykułu uczestniczy w nich od 2005 r. W tym czasie grupa robocza zdążyła się podzielić na dwie i z powrotem połączyć, został powołany trzeci z kolei przewodniczący.

Najnowszy projekt tej normy prEN 50136-1:2010 [2] przesłano właśnie do trzeciej ankiety powszechnej, chociaż wewnętrzny regulamin CENELEC dopuszcza tylko dwukrotne zastosowanie takiej procedury. Taka sytuacja powstała wskutek trudności

Normy Technologiczne	Normy podstawowe na systemy i urządzenia transmisji alarmów	Normy aplikacyjne dla monitoringu włamaniowego	Normy na budowę, wyposażenie i działanie centrów odbiorczych
EN 50136-1-7 Protokoły transmisji	EN 50136-1 Systemy transmisji alarmów	EN 50131-1 (nowa edycja) Określenie kategorii systemów	EN 50136-4 Urządzenia powiadamiające
	EN 50136-2 Nadajniki/odbiorniki chronionych obiektów	EN 50131-N Nadajnik/odbiornik dla monitoringu włamaniowego	EN 50518-1 Lokalizacja i budowa centrum
	EN 50136-3 Nadajniki/odbiorniki centrów odbiorczych		EN 50518-2 Wymagania techniczne
	EN 50136-7 Zalecenia aplikacyjne		EN 50518-3 Procedury oraz wymagania dotyczące funkcjonowania

Rys. 1.

w rozstrzygnięciu kilku kwestii spornych:
– czy norma powstająca jako nowa wersja normy istniejącej ma wprowadzać zasadnicze zmiany, czy raczej być kontynuacją poprzedniej,
– czy powinna być to norma dotycząca tylko systemów włamaniowych i napadowych, czy też norma podstawowa dla wszystkich systemów transmisji alarmów,
– czy powinna obejmować tylko rozwiązania spełniające wysokie wymagania, czy też wszystkie konstrukcje aktualnie stosowane.

Dały o sobie także znać różnice w organizacji systemów monitorowania w poszczególnych krajach, wynikające z uwarunkowań historycznych, stosowanych rozwiązań biznesowych oraz prawnych – koncesji, licencji certyfikatów itd.

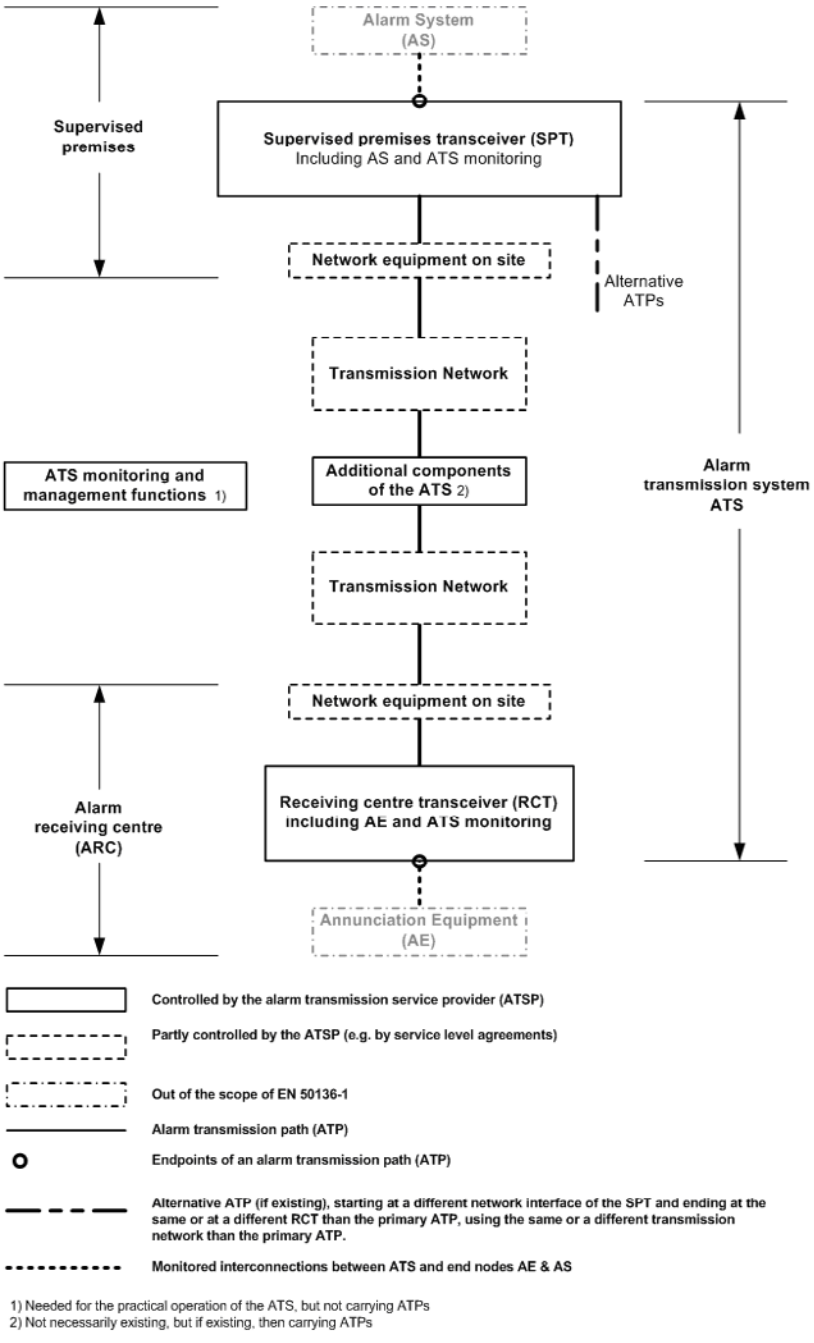
Przyjęto ostatecznie, że będzie to norma podstawowa, na podstawie której powstaną normy aplikacyjne, np. dla transmisji alarmów pożarowych, socjalnych itd., oraz neutralna technologicznie, czyli że nie będzie kolejnych norm dotyczących systemów wykorzystujących różne sieci transmisji. W praktyce jednak projekt normy zdecydowanie preferuje systemy wykorzystujące systemy telekomunikacyjne z komutacją pakietów, takie jak Internet i GPRS, oraz definiuje ograniczoną liczbę kategorii systemów, co umożliwi bezpośrednie wykorzystanie tej normy do certyfikacji systemów.

Ogólny schemat systemu transmisji alarmów wg prEN 50136-1:2010 przedstawiono na *rys. 2.* W porównaniu z ciągle aktualną wersją normy [3] można zauważyć dwie istotne zmiany: pojawienie się funkcji monitorowania pracy systemu i realizujących ją urządzeń pośredniczących oraz urządzeń sieciowych w zabezpieczanych obiektach i stacjach odbiorczych, które nie są urządzeniami transmisji alarmów, ale nie są także elementami sieci transmisji. Taka sytuacja występuje bardzo często, szczególnie (ale nie wyłącznie) w przypadku transmisji przez Internet. Urządzenia transmisji alarmów są podłączane do firmowych sieci lokalnych lub choćby tylko ruterów, które pozostają pod nadzorem „lokalnych informatyków", często niezbyt zorientowanych w zagadnieniach ochrony i bezpieczeństwa obiektów. W wielu przypadkach urządzenia takie są pozbawione zasilania rezerwowego. Problem ten pozostawiono do rozwiązania w normach aplikacyjnych lub w bezpośrednich umowach z użytkownikami.

Projekt normy przewiduje dziesięć kategorii systemów transmisji alarmów oraz znacznie większą liczbę ocenianych cech użytkowych. Są wśród nich wszystkie cechy klasyfikowane w dotychczasowej wersji normy: • czas transmisji D • maksymalny czas transmisji M • czas raportowania T • dostępność A • ochrona informacji I • ochrona przed podmianą S.

Sześć kategorii, oznaczonych jako S1 ... S6, dotyczy systemów z pojedynczym torem transmisji. Cztery pozostałe: D1 ... D4 obejmują systemy z dwoma torami transmisji. W *tablicy 1* podano konfigurację systemów poszczególnych kategorii.

Jeżeli norma zostanie przyjęta w obecnej postaci, umożliwi bezpośrednią certyfikację systemu transmisji alarmów na zgodność z jedną z dziesięciu przewidzianych kategorii, co może być konieczne w przypadku systemów, dla których nie będzie norm aplikacyjnych. Twórcy norm aplikacyjnych (np. dla transmisji alarmów pożarowych lub socjalnych) mogą do swoich projektów wstawić wy-



Rys. 2. Ogólny schemat systemu transmisji alarmów wg prEN 50136-1:2010

Tablica 1

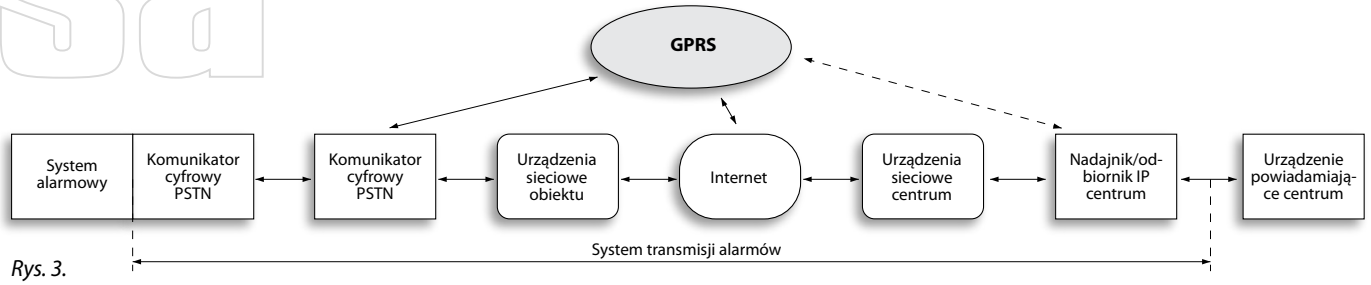
	S1	S2	S3	S4	S5	S6	D1	D2	D3	D4
Interfejs UTA do podstawowej sieci transmisji[a)]	M	M	M	M	M	M	M	M	M	M
Interfejs UTA do dodatkowej sieci transmisji [a)]	Op	Op	Op	Op	Op	Op	M	M	M	M
Alternatywny odbiornik w centrum odbiorczym[b)]	Op	Op	Op	Op	Op	Op	M	M	M	M
Interfejs odbiornika w centrum odbiorczym do podstawowej sieci transmisji[c)]	M	M	M	M	M	M	M	M	M	M
Interfejs odbiornika w centrum odbiorczym do dodatkowej sieci transmisji[c)]	Op	Op	Op	Op	Op	Op	M	M	M	M

Objaśnienia: M = obowiazkowy; Op = opcjonalny

[a)] UTA może zawierać jeden lub więcej interfejsów do sieci transmisji wykorzystujących różne technologie.

[b)] Każdy odbiornik centrum odbiorczego powinien zawierać jeden lub więcej interfejsów do sieci transmisji.

[c)] Każdy odbiornik w centrum odbiorczym może posiadać kilka interfejsów do sieci transmisyjnych



Rys. 3.

magania dotyczące systemów jednej lub kilku kategorii lub utworzyć nową kategorię C systemów o cechach użytkowych odpowiadających danemu zastosowaniu. Zapewne stanie się tak w przypadku nowej normy na systemy transmisji alarmów pożarowych i sygnałów uszkodzeniowych, nad którą prace rozpoczną się w 2011 r.

Przewiduje się, że w nowej edycji normy EN 50131-1 (lub zmianie do niej) systemom SSWN stopni 1 ... 4 zostaną przyporządkowane odpowiednie kategorie systemów transmisji alarmów.

Uwagi do projektu normy prEN 50136-1:2010 mogły być zgłaszane do 2011-02-18. Z Polski takie uwagi nie zostały przesłane.

Protokoły transmisji alarmów

Protokoły transmisji alarmów mają znacznie większą żywotność niż wykorzystujące je urządzenia transmisji. Do dziś można w chronionych obiektach znaleźć nadajniki stosujące protokoły, procedury i metody modulacji wprowadzone jeszcze w latach 50. ub. wieku. Nie udało się wprowadzić norm międzynarodowych na protokoły transmisji informacji alarmowych, a normy opracowane przez IEC nie zostały zaakceptowane przez rynek zabezpieczeń [1]. Wśród „klasycznych" protokołów transmisji najbardziej popularne są obecnie protokoły firmowane przez SIA *(Security Industry Association)*: „Contact ID"[4] oraz „SIA Format"[5], ale wiele dostępnych na rynku odbiorników obsługuje nawet kilkadziesiąt innych protokołów, formatów i metod modulacji.

Komunikatory cyfrowe są przez wielu producentów montowane bezpośrednio na płytach głównych central SSWN lub podłączane do magistrali tych central, a z reguły montuje się je we wspólnej obudowie z centralami. Komunikatory te są zwykle przeznaczone do pracy w publicznych sieciach telefonicznych PSTN, jednak w wielu dozorowanych obiektach analogowe łącza telefoniczne są obecnie całkowicie likwidowane lub zastępowane przez łącza VoIP. Czasami użytkownicy końcowi (np. najemcy lokali w dużych obiektach) nie są nawet świadomi takiej zmiany.

Komunikatory przeznaczone do przesyłania informacji alarmowych przez analogowe łącza PSTN nie zapewniają poprawnej transmisji „klasycznych" protokołów alarmowych przez łącza VoIP. Ze względu na dużą różnorodność rozwiązań kryjących się pod ogólną nazwą „VoIP" nie jest celowe opracowywanie i stosowanie urządzeń dopasowujących komunikatory do współpracy z sieciami VoIP. W nowych obiektach można oczywiście do transmisji wykorzystać inne łącza, jednak trudno sobie wyobrazić masową wymianę systemów sygnalizacji z wbudowanymi komunikatorami tylko z powodu zmiany łącza analogowego na łącze VoIP.

Problem ten jest praktycznie rozwiązywany poprzez instalację w obiekcie dodatkowego nadajnika/odbiornika, który symuluje centralę PSTN, odbiera przesyłkę alarmową, np. w DTMF zgodnie z protokołem Contact ID, a następnie wiadomości w formacie zgodnym z tym protokołem przesyła przez Internet i/lub GPRS *(rys. 3)*.

Przy takiej symulacji łącza telefonicznego zachowuje się strukturę protokołu wyjściowego i zawartość stosowanych ramek. Nie zmieniają się także interfejsy początkowe i końcowe systemu transmisji alarmów. Oznacza to, że czas transmisji D definiowany w normie obejmuje także czas nawiązywania przez komunikator połączenia z nieistniejącą centralą PSTN oraz czas transmisji sygnałów DTMF.

Opisane rozwiązanie jest wprawdzie tymczasowe i wymuszone, jednak ma istotny wpływ na rozwój protokołów w sieciach AoIP *(Alarm over Internet Protocol)* oraz ich standaryzację, sprzyjając dalszemu wykorzystywaniu „klasycznych" protokołów, stosowanych w nich formatów i metod kodowania informacji alarmowych.

Nie ma jeszcze standardów międzynarodowych czy choćby de facto standardów przemysłowych na systemy AoIP, stosowane w nich protokoły i procedury transmisji. Dominują rozwiązania firmowe umożliwiające współpracę nadajników/odbiorników tej samej firmy lub co najwyżej kilku firm.

Podejmowane próby opracowania oraz wdrożenia norm krajowych i środowiskowych na systemy klasy AoIP zazwyczaj ograniczają się do opisu sposobu enkapsulacji ramek „klasycznych" protokołów transmisji informacji alarmowych IP. Przykładem mogą być specyfikacje opracowane przez VEBON [6] oraz VdS [7]. Ta ostatnia dopuszcza wprawdzie enkapsulację ramek takich protokołów dodatkowych, jak TAS czy też TELENOT, jednak obligatoryjne jest stosowanie protokołu VdS 2465 [8]

Formalnie normą otwartą i udostępnioną w Internecie do swobodnego wykorzystania jest norma amerykańska opracowana przez SIA i opublikowana jako ANSI/SIA DC-09 Digital Communication Standard – Internet Protocol Event Reporting [9]. Wykorzystuje ona formaty i procedury wymiany danych opisane w innej normie SIA o symbolu DC-07 [10] (niedostępnej w Internecie – do kupienia w cenie 100 dol.), dotyczącej komunikacji pomiędzy odbiornikiem a komputerem centrum odbiorczego alarmów.

Zgodnie z normą DC-09 do przesyłania informacji alarmowych można wykorzystywać protokół UDP lub TCP, a także oba te protokoły. Jeżeli można wykorzystywać tylko jeden protokół, preferowany jest protokół UDP. Informacje mogą być przesyłane bez szyfrowania lub szyfrowane, z wykorzystaniem szyfrów blokowych lub AES i klucza o długości 128, 192 lub 256 bitów. Odbiornik centrum odbiorczego powinien mieć stały adres IP, urządzenie transmisji alarmów natomiast może mieć adres statyczny lub przydzielany dynamicznie.

Norma ANSI/SIA DC-09 powstała już przed kilkoma laty i ma charakter ogólnego przewodnika budowy urządzeń i sieci AoIP*.

W Szwecji organizacja SOS Alarm Sverige AB obsługująca numer alarmowy 112 oraz koordynująca akcje ratownicze opracowała i wykorzystuje protokół SOS Access Version 4 [11], który może być swobodnie stosowany przez producentów systemów i urządzeń pod warunkiem zachowania pełnej zgodności z oryginalną specyfikacją oraz przywołaniem jej nazwy w dokumentacji wyrobu. To jeden ze stosowanych obecnie protokołów transmisji alarmów w języku XML. Przewiduje on m.in. możliwość przekazywania informacji o położeniu obiektu w formacie WGS84.

Pakiet norm dotyczących systemów transmisji alarmów opracowywany w CENELEC przez grupę roboczą TC79/WG5 obejmuje także normę europejską na protokół transmisji alarmów w sieciach IP v4 oraz IP v6. Projekt tej normy EN 50136-1-7:2010 [12] przeszedł już pomyślnie ankietę powszechną i wkrótce zostanie skierowany do formalnego głosowania, kończącego procedurę opracowywania tej nowej normy. Jej przedmiotem jest specyfikacja protokołu

* W marcu 2011 r. The Security Industry Association (SIA) rozpoczęła prace nad nową normą *DC-10 Digital IP Communication Protocol for Electronic Security*. Autor artykułu wraz z zaproszeniem na pierwsze posiedzenie grupy roboczej otrzymał projekt tej normy. Zostanie on omówiony w następnej części artykułu.

transmisji w zakresie umożliwiającym zapewnienie kompatybilności urządzeń nadawczych i odbiorczych różnych producentów oraz ich certyfikację. Stąd też norma jest znacznie obszerniejsza (prawie 50 stron) od wyżej wymienionych i bardziej szczegółowa. Jest w niej definiowany protokół transmisji z punktu do punktu pomiędzy nadajnikiem/odbiornikiem chronionego obiektu a nadajnikiem/odbiornikiem centrum odbiorczego. Wykorzystuje protokół UDP i obejmuje warstwy transportową oraz aplikacji (patrz *Vademecum sieci komputerowych* (9) 1/2011 SA). Szczególną uwagę zwrócono na zapewnienie bezpieczeństwa przesyłanych informacji, uwierzytelnianie i ochronę przed podstawieniem oraz zabezpieczenie przed niektórymi metodami ataków internetowych. Wykorzystywane są zarówno fizyczne adresy urządzeń, jak i indywidualne identyfikatory nadawane urządzeniom w czasie włączania obiektu do systemu.

Do weryfikacji informacji jest wykorzystywana funkcja skrótu SHA-256 lub RIPEMD-256. Norma przewiduje zastosowanie symetrycznych szyfrów blokowych AES-128 lub AES-256. Transmisja bez szyfrowania może być stosowana tylko w czasie prac rozwojowych lub testowania. Klucz powinien być zmieniany nie rzadziej niż co tydzień. Norma opisuje procedurę pierwszego włączenia urządzenia obiektowego do systemu, w tym przekazywania kluczy oraz identyfikatorów przez obsługę systemu, jak też przy wykorzystaniu metodyki klucza publicznego zgodnie z X.509 i protokołu DTLS.

Zgodnie z projektem normy EN 50136-1-7 rozwiązanie kompatybilne z definiowanym protokołem musi umożliwiać przesyłanie w warstwie aplikacji przynajmniej dwóch rodzajów informacji:

- transparentnej komunikacji pomiędzy systemem alarmowym a urządzeniem powiadamiającym w centrum odbiorczym,
- wiadomości przesyłanych zgodnie z protokołem SIA DC-03 dotyczących:
  - sygnałów przekazywanych przez system alarmowy poprzez styk równoległy,
  - sygnałów wewnętrznych generowanych przez nadajniki/odbiorniki zainstalowane w obiektach i stacji odbiorczej.

Zdefiniowano identyfikatory takich protokołów, jak Ademco Contact ID, VdS 2465, SOS Access v4, CEI ABI 79 5/6, Scancom FF, F1COM oraz SurGard. Lista będzie powiększana stosownie do potrzeb. Producent może zdefiniować własny format przesyłanych informacji alarmowych i do czasu nadania mu formalnego identyfikatora w czasie aktualizacji normy powinien posługiwać się numerem identyfikacyjnym 254.

O losach protokołu wprowadzanego przez CENELEC jak zwykle zdecydują użytkownicy. Złośliwi twierdzą, że jest on dostatecznie skomplikowany, aby mogli go zaakceptować „big boys", utrudniając życie małym dostawcom i operatorom.

Literatura

[1] J. Sobstel: Normy i certyfikaty na systemy monitoringu włamaniowego i napadowego. SA 6/2010

[2] Alarm systems – Alarm transmission systems and equipment – Part 1: General requirements for alarm transmission systems

[3] PN-EN 50136-1-1:2007 Systemy alarmowe. Systemy i urządzenia transmisji alarmu Część 1-1: Wymagania ogólne dotyczące systemów transmisji

[4] SIA DC-05-1999. Digital Communication Standard-Ademco® Contact ID Protocol-for Alarm System Communications

[5] SIA DC-03-1990 (R2000). Digital Communication Standard – "SIA Format" Protocol for Alarm System Communication

[6] Specification Proposal: Alarm Signaling over IP Rev. 1.2.2. VEBON 2007

[7] VdS 2465en-S2 : 2006 guidelines for Alarm Systems (AS)-Transmission protocol for Alarm Systems (AS) Version 2 Amendment S2: Protocol extension for connection to networks of the TCP protocol family

[8] VdS 2465 : 1999-03 Übertragungsprotokoll für Gefahrenmeldeanlagen Version 2

[9] ANSI/SIA DC-09-2007 – SIA DCS - IP Event Reporting

[10] SIA DC-07-2001 - SIA Digital Communications Standard - Receiver-to-Computer Interface Protocol (Type 2) - for Central Station Equipment Communications

[11] SOS Access Version 4.0.1 Protocol description. SOS Alarm AB 2007

[12] prEN 50136-1-7:2010 Alarm systems - Alarm transmission systems and equipment - Part 1-7: Requirements for common protocol for alarm transmission using packet switched network