Koncepcja metody bezpiecznej transmisji danych w sieci KNX na potrzeby systemu zdalnego nadzoru

Michał Porzeziński

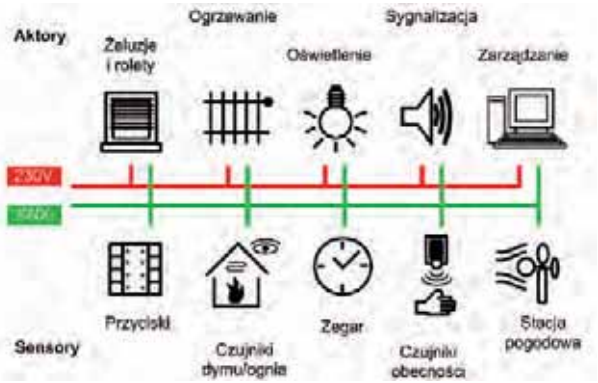
Wydział Elektrotechniki i Automatyki, Politechnika Gdańska

Streszczenie: W pracy omówiono wymagania stawiane kanałom komunikacyjnym wykorzystywanym do realizacji funkcji związanych z bezpieczeństwem oraz zaproponowano metodę bezpiecznej transmisji danych w sieci KNX opracowaną na potrzeby systemu zdalnego nadzoru. Metoda definiuje dodatkową warstwę stosu protokołu komunikacyjnego KNX umożliwiającą spełnienie wymagań dotyczących niezawodność i bezpieczeństwa transmisji danych bez konieczności wprowadzania zmian w istniejącym systemie KNX.

Słowa kluczowe: system KXN, bezpieczeństwo funkcjonalne, bezpieczeństwo transmisji danych

1. Wprowadzenie

Na przestrzeni ostatnich lat można zaobserwować gwałtowny rozwój systemów automatyki budynków. Znajdują one zastosowanie zarówno w dużych budynkach użyteczności publicznej, jak i w małych hotelach, domach jednorodzinnych, czy nawet mieszkaniach. Systemy te umożliwiają sterowanie i monitorowanie stanu wybranych urządzeń i wielkości fizycznych przyczyniając się do wzrostu bezpieczeństwa, obniżenia kosztów eksploatacji i zwiększenia komfortu użytkowania obiektów. Obecnie stosowane rozwiązania są przeważnie systemami rozproszonymi, w których brak jest centralnego sterownika, a każdy z elementów systemu komunikuje się z pozostałymi za pomocą specjalnej magistrali komunikacyjnej (rys. 1).



Rys. 1. Idea rozproszonego systemu automatyki budynków na przykładzie systemu KNX

Fig. 1. The idea of a distributed building automation system shown on the example of the KNX system

W niektórych rozwiązaniach sieć przewodowa może być zastąpiona transmisją radiową lub komunikacją polegającą na przesyłaniu odpowiedniego sygnału za pomocą istniejącej instalacji elektrycznej 230 V.

Spośród wielu systemów automatyki budynków szczególnie dużą popularnością cieszą się systemy bazujące na standardach otwartych, takich jak: KNX [1], LonWorks [2] oraz BACnet [3]. Podstawowe funkcje realizowane przez te systemy to sterowanie ogrzewaniem i klimatyzacją, sterowanie oświetleniem, sterowanie żaluzjami i roletami oraz centralne monitorowanie i zarządzanie tymi zasobami [4]. Systemy te są z powodzeniem stosowane od wielu lat. Jak wynika z doświadczeń tysięcy użytkowników, wystarczająco niezawodnie pełnią swoje funkcje.

Znacznie większe wymagania stawiane są systemom realizującym funkcje związane z bezpieczeństwem, takim jak: System Sygnalizacji Pożaru (SSP), System Sygnalizacji Włamania i Napadu (SSWiN), System Kontroli Dostępu (SKD). Muszą być one odporne nie tylko na przypadkowe zakłócenia, ale również na celowe działania osób trzecich, chcących zakłócić ich działanie.

Obecnie większość systemów bezpieczeństwa realizowana jest jako obwody autonomiczne, niezintegrowane z pozostałymi systemami automatyki. Pociąga to za sobą duże koszty inwestycyjne wynikające z konieczności budowy niezależnej infrastruktury sieciowej dla każdego z tych systemów. W związku z tym uzasadnione jest poszukiwanie rozwiązań umożliwiających bezpieczne współdzielenie infrastruktury sieciowej zarówno przez urządzenia związane z bezpieczeństwem, jak i typowe urządzenia automatyki. Rozwiązania tego typu są dopuszczalne i coraz częściej spotykane w systemach automatyki przemysłowej. Takie podejście wymusza jednak szereg dodatkowych wymagań, które muszą spełniać urządzenia związane z bezpieczeństwem w zakresie niezawodności i bezpieczeństwa transmisji danych.

W przypadku rozproszonych systemów automatyki budynków szczególnego znaczenia nabiera problem zapewnienia bezpieczeństwa transmitowanych danych. Wynika to z faktu, że sieci tego typu, z powodu ich rozległości, trudno

jest ochronić przed fizycznym dostępem osób niepowołanych. Analiza istniejących rozwiązań pokazuje, że spośród trzech najważniejszych standardów otwartych systemów automatyki budynków jedynie system BACnet udostępnia w miarę skuteczne mechanizmy bezpieczeństwa, podczas gdy system KNX nie ma ich praktycznie wcale [5]. Skłania to do poszukiwania rozwiązań, które potrafią tę lukę uzupełnić.

W dalszej części artykułu przedstawiono wymagania stawiane systemom związanym z bezpieczeństwem oraz zaproponowano prostą metodę bezpiecznej transmisji danych w systemie KNX, która może być wykorzystana do monitorowania stanu obiektów i urządzeń krytycznych z punktu widzenia bezpieczeństwa budynku.

2. Wymagania dotyczące kanałów komunikacyjnych związanych z bezpieczeństwem

Wymagania dotyczące bezpieczeństwa funkcjonalnego domowych i budynkowych systemów elektronicznych określa norma PN-ISO/IEC 14762:2010 [6]. Przedstawiono w niej m.in. wymagania dotyczące: zachowania się urządzeń po zaniku i wznowieniu zasilania, metod konfiguracji i ładowania programów aplikacyjnych oraz odporności urządzeń na warunki środowiskowe. Wymagania dotyczące sposobu komunikowania się urządzeń są przedstawione bardzo ogólnie. Dotyczą m.in. problemów: ograniczania obciążenia sieci komunikacyjnej wprowadzanego przez poszczególne urządzenia, unikania hazardów podczas odbioru wiadomości z wielu źródeł oraz odporności na zakłócenia transmisji. Bardziej szczegółowe wymagania dotyczące kanałów komunikacyjnych wykorzystywanych do realizacji funkcji związanych z bezpieczeństwem można znaleźć w literaturze i dokumentach normatywnych dotyczących bezpieczeństwa funkcjonalnego systemów automatyki przemysłowej. W efekcie analizy można sformułować dwie podstawowe klasy wymagań: wymagania dotyczące niezawodności przesyłu danych oraz wymagania dotyczące bezpieczeństwa transmitowanych danych.

2.1. Wymagania dotyczące niezawodności

Pod pojęciem zapewnienia niezawodności przesyłu danych należy rozumieć zagwarantowanie, że dane nadane przez nadawcę zostaną w zadanym czasie z odpowiednio wysokim prawdopodobieństwem poprawnie przesłane do odbiorcy, pomimo działania różnego rodzaju przypadkowych zakłóceń oraz obecności w oprogramowaniu błędów systematycznych, które mogą się ujawniać w szczególnych warunkach pracy systemu.

W przypadku projektowania systemów realizujących funkcje związane z bezpieczeństwem najczęściej stosowane jest podejście przedstawione w normie PN-EN 61508-1 [7]. Norma ta operuje pojęciem poziomu nienaruszalności bezpieczeństwa SIL (ang. *Safety Integrity Level*) określanym dla danej funkcji bezpieczeństwa na podstawie analizy ryzyka i zagrożeń dla danego obiektu/systemu. Każdy z czterech poziomów SIL determinuje m.in. architekturę systemu bezpieczeństwa, sposób projektowania oprogramowania oraz maksymalne dopuszczalne prawdopodobieństwo niewypełnienia danej funkcji bezpieczeństwa (tab. 1). Dodatkowo wymagania normy PN-EN 61784-3 [9] dotyczącej magistral komunikacyjnych bezpiecznych funkcjonalnie zakładają, aby dla danego poziomu SIL prawdopodobieństwo wystąpienia niebezpiecznego błędu transmisji stanowiło nie więcej niż 1 % dopuszczalnego prawdopodobieństwa niewypełnienia danej funkcji bezpieczeństwa, określonego w tab. 1.

Na niezawodność mają również wpływ błędy systematyczne, które mogły zostać wprowadzone na etapie projektowania i konfigurowania systemów, a nie zostały wykryte w fazie testowania. Aby minimalizować liczbę tych błędów, wymaga się m.in., żeby oprogramowanie poszczególnych warstw protokołu zostało zaprojektowane i wykonane zgodnie z wytycznymi normy PN-EN 61508-3 [8] dla zakładanego poziomu nienaruszalności bezpieczeństwa. Tak zaprojektowany kanał komunikacyjny nazywany jest kanałem „białym" i można go bezpośrednio zastosować do realizacji funkcji związanych z bezpieczeństwem.

Tab. 1. Dopuszczalne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa dla określonych poziomów nienaruszalności bezpieczeństwa SIL

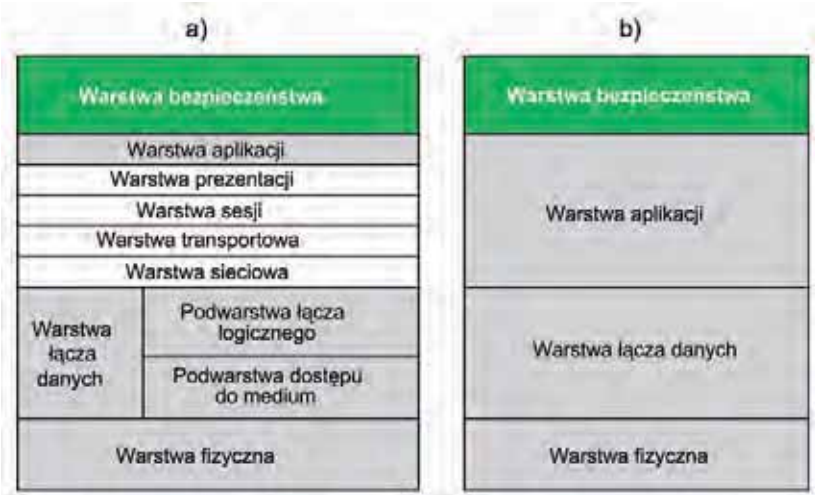
Tab. 1. The acceptable probability of failure of the safety function for certain levels of SIL

SIL	Prawdopodobieństwo niezadziałania na przywołanie (tryb rzadkiego przywołania)	Prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego na 1 h (tryb częstego przywołania lub pracy ciągłej)
1	$\geq 10^{-2} \div < 10^{-1}$	$\geq 10^{-6} \div < 10^{-5}$
2	$\geq 10^{-3} \div < 10^{-2}$	$\geq 10^{-7} \div < 10^{-6}$
3	$\geq 10^{-4} \div < 10^{-3}$	$\geq 10^{-8} \div < 10^{-7}$
4	$\geq 10^{-5} \div < 10^{-4}$	$\geq 10^{-9} \div < 10^{-8}$

Dopuszcza się również wykorzystanie protokołów komunikacyjnych, które nie zostały opracowane zgodnie z wytycznymi normy PN-EN 61508-3, lub których szczegóły realizacji po prostu nie są znane [9]. Kanał tego typu określany jest jako kanał „czarny" i wymaga dodania na górze istniejącego stosu protokołu dodatkowej warstwy nazywanej warstwą bezpieczeństwa (rys. 2). Warstwa bezpieczeństwa korzysta z interfejsu udostępnianego przez warstwę aplikacji wprowadzając własne, niezależne od pozostałych warstw, mechanizmy kontroli poprawności przesyłanych danych. Oprogramowanie obsługujące tą warstwę musi być ponadto zaprojektowane, wykonane i przetestowane zgodnie z wymaganiami stawianymi w normie PN-EN 61508-3 dla obowiązującego poziomu SIL.

2.2. Wymagania dotyczące bezpieczeństwa

Pod pojęciem zapewnienia bezpieczeństwa przesyłu danych należy rozumieć zapewnienie odporności systemu na celowe działania osób nieuprawnionych. Sprowadza się to do następujących wymagań: poufności danych, aktualności danych



Rys. 2. Model stosu protokołów komunikacyjnych z dodaną warstwą bezpieczeństwa: a) model OSI, b) model uproszczony wg PN-EN 61784-3 [9]

Fig. 2. The model of the communication protocol stack with the additional security layer: a) the OSI model, b) a simplified PN-EN 61784-3 model [9]

oraz wymagania integralności danych wiązanego często z wymaganiem autentyczności danych [10].

Zapewnienie poufności danych jest istotne w sieciach, których nie można zabezpieczyć przed fizycznym dostępem osób nieuprawnionych. W sieciach przemysłowych i sieciach automatyki budynków, w których przesyłanymi danymi są zwykle dane z czujników pomiarowych i polecenia sterujące, zapewnienie poufności wydaje się zbyt daleko posuniętą ostrożnością. Szyfrowanie może być jednak potrzebne do zapewnienia pozostałych wymagań bezpieczeństwa, takich jak: integralność, aktualność czy autentyczność danych. Poufność można zapewnić przez szyfrowanie przesyłanych danych z użyciem tajnych kluczy za pomocą powszechnie znanych i sprawdzonych w działaniu algorytmów kryptograficznych.

Warunek integralności danych wymaga, aby nie było możliwe zmodyfikowanie przesyłanych danych, bez zauważenia tego przez odbiorcę. Najpopularniejszym rozwiązaniem pozwalającym na wykrycie zmiany danych jest stosowanie tzw. funkcji skrótu. Umożliwiają one wygenerowanie swoistego podpisu w postaci sekwencji bitów dołączanej do wysyłanej wiadomości, zależnej od liczby i wartości wysyłanych bajtów danych. Znajomość algorytmu wyliczania skrótu umożliwia jednak osobie nieuprawnionej zmodyfikowanie i ponowne podpisanie zmodyfikowanych danych, dlatego w celu zapewnienia ich autentyczności podczas wyliczania funkcji skrótu często uwzględniany jest dodatkowy ciąg danych, znany tylko uprawnionym stronom, lub dane wraz ze skrótem się dodatkowo szyfruje.

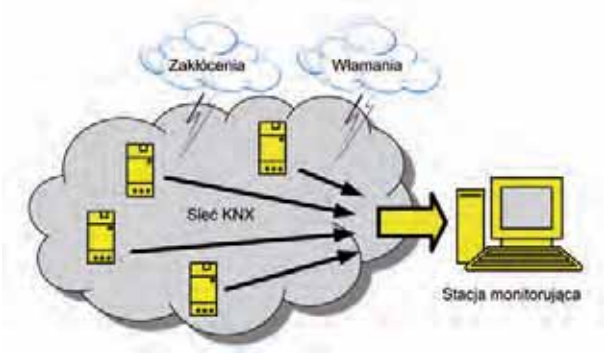
W sieciach przemysłowych szczególnie istotnym wymaganiem jest zapewnienie aktualności przesyłanych danych. Weryfikacja aktualności danych zapobiega możliwości wykorzystania przez osobę nieuprawnioną do sterowania wcześniej „podsłuchanych" i zapamiętanych sekwencji danych, nadawanych przez inne uprawnione węzły. Samo szyfrowanie danych nie rozwiązuje tego problemu. Konieczne są dodatkowe mechanizmy polegające na użyciu tzw. stempla czasu lub odpowiedniej sekwencji numeracji wiadomości.

Omawiając wymagania dotyczące bezpieczeństwa transmisji danych, warto wspomnieć o dokumentach normatywnych dotyczących bezpieczeństwa systemów informatycznych. Obecnie dostępne są dwie rodziny norm: normy z rodziny ISO/IEC 27000 oraz normy z rodziny ISO/IEC 15408. Obie grupy norm traktują zagadnienia bezpieczeństwa na bardzo dużym poziomie ogólności. Normy z rodziny ISO/IEC 27000 zawierają wymagania dotyczące systemów zarządzania bezpieczeństwem informacji w przedsiębiorstwach oraz zbiór dobrych praktyk, porad i zaleceń dotyczących projektowania takich systemów. Z kolei grupa norm z rodziny ISO/IEC 15408 opisuje sposób oceny bezpieczeństwa systemów informatycznych bazujący na metodyce CC (ang. *Common Criteria*). Pozwala on w obiektywny sposób, za pomocą poziomów EAL (ang. *Evaluation Assurance Level*) oceniać poziom zaufania do zadeklarowanych zabezpieczeń. Posiadanie certyfikatu CC nie gwarantuje jednak, że produkt jest bezpieczny pod każdym względem, zapewnia jedynie o poprawnym działaniu wszystkich zadeklarowanych przez producenta zabezpieczeń określonych w tzw. profilu ochrony.

3. Koncepcja metody bezpiecznej transmisji danych

3.1. Założenia systemu nadzoru

Opracowana metoda bezpiecznej transmisji danych w systemie KNX ma służyć bezpiecznemu i niezawodnemu przekazywaniu danych na potrzeby systemu nadzoru. Idea tego systemu została pokazana na rys. 3. Składa się on ze stacji monitorującej dołączonej do istniejącej sieci KNX za pomocą odpowiedniego interfejsu oraz szeregu „inteligentnych" czujników przesyłających za pośrednictwem tej sieci informacje o stanie nadzorowanego obiektu. Mogą to być urządzenia pełniące rolę czujników wykorzystywanych w systemach sygnalizacji włamania i napadu, czujników sys-



Rys. 3. Idea systemu nadzoru

Fig. 3. The idea of the supervisory system

temów przeciwpożarowych, czy też urządzenia do pomiaru i rozliczania zużycia mediów energetycznych.

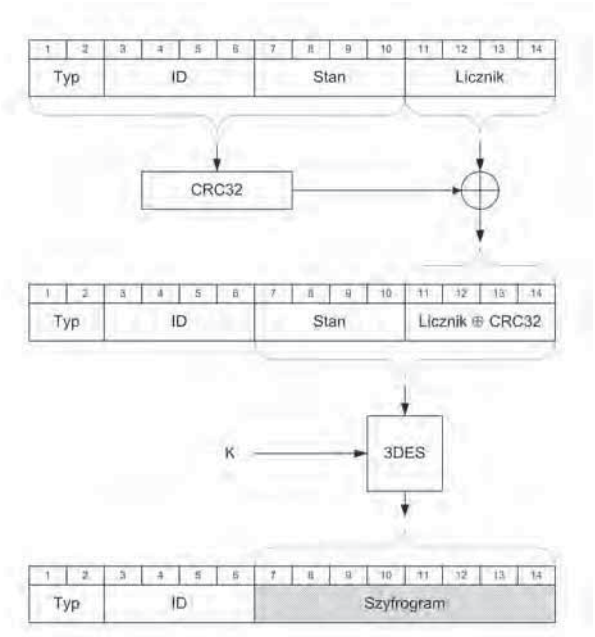
Rolą stacji monitorującej jest rejestrowanie otrzymanych od czujników informacji oraz sygnalizowanie operatorowi stanów nieprawidłowych. W większych systemach zamiast stacji monitorującej może zostać użyty odpowiedni agent nadzoru przekazujący informacje do centralnego serwera alarmów, z którego danych może korzystać wiele stacji operatorskich [11]. Przyjęto ponadto, że system zdalnego nadzoru powinien spełniać następujące dodatkowe wymagania:

- Urządzenia nadzoru powinny współdzielić magistralę KNX z innymi urządzeniami automatyki budynku i być pełnoprawnymi węzłami tego systemu, tzn. powinny być widziane i obsługiwane przez standardowe narzędzia KNX, takie jak program ETS służący do konfiguracji i diagnostyki tego systemu.
- Zastosowana metoda transmisji powinna zapewnić: integralność, autentyczność, aktualność i poufność przesyłanych danych dotyczących stanu urządzenia oraz zapewnić odporność na zakłócenia przypadkowe.
- Synchronizacja stanów odbiorcy i nadawcy informacji powinna odbywać się przy założeniu jednokierunkowej transmisji danych na poziomie warstwy aplikacji (od urządzenia do stacji monitorującej).
- Stan danego urządzenia będzie wyrażony za pomocą maksymalnie 32 bitów informacji przekazywanej do stacji nadzoru.
- W jednym systemie może pracować maksymalnie 65 535 nadzorowanych urządzeń.
- Urządzenia będą przekazywać swój stan cyklicznie, nie częściej jednak, niż co 1 s.
- Zostaną wykorzystane standardowe metody kryptograficzne, które są dostępne w postaci bloków sprzętowych wybranych mikrokontrolerów.

3.2. Koncepcja warstwy bezpieczeństwa

Standard KNX wprowadza szereg typów danych, które mogą zostać wykorzystane do przekazywania stanu pomiędzy czujnikami a stacją monitorującą za pomocą tzw. telegramów. W protokole KNX istnieją już mechanizmy zwiększające niezawodność transmisji danych. Są to procedury kontroli integralności przesyłanych danych opierające się na zastosowaniu bitu parzystości w każdym z przesyłanych bajtów oraz dodatkowej ośmiobitowej sumy kontrolnej [1]. Wysoką niezawodność transmisji zapewnia również używany na poziomie warstwy łącza danych mechanizm potwierdzania odebrania danych wraz z ewentualną retransmisją, odbywającą się w przypadku braku potwierdzenia. Z punktu widzenia normy PN-EN 61784-3, kanał komunikacyjny wykorzystujący stos protokołów KNX należy jednak do kategorii kanałów „czarnych", tym samym nie może być bezpośrednio użyty do realizacji funkcji bezpieczeństwa. Standard KNX nie oferuje ponadto żadnych mechanizmów zapewniających poufność, autentyczność ani aktualność danych [5].

Problem bezpieczeństwa sytemu KNX został już wcześniej zauważony, czego efektem jest opracowanie kompleksowych mechanizmów bezpieczeństwa w postaci protokołu

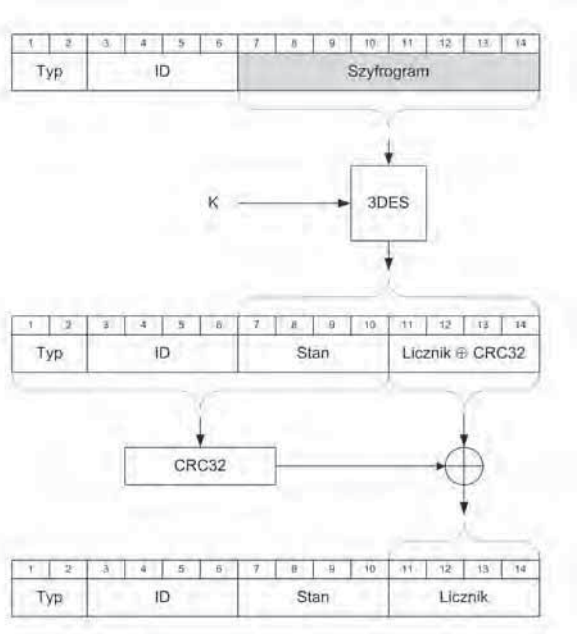


Rys. 4. Proces przetwarzania danych po stronie nadawcy
Fig. 4. The process of data conversion at the sender side

EIBsec [10]. Metoda ta wymaga jednak zastosowania dodatkowych urządzeń pełniących w systemie KNX rolę zaufanego centrum dystrybucji kluczy. W metodzie tej szyfrowane są nie tylko dane użytkowe, lecz również pola ramki związane z warstwą aplikacji i warstwą transportową protokołu, co po części wymuszone jest 16-bitowym rozmiarem bloku danych w użytym do szyfrowania algorytmie AES (a maksymalna długość pola danych w telegramach KNX wynosi 14 bajtów). Przez to nie jest możliwe wykorzystanie dostępnych na rynku standardowych komponentów KNX. Uniemożliwia to również wykorzystanie standardowych narzędzi konfiguracyjnych i diagnostycznych. Ograniczeniem jest również znaczący wzrost obciążenia sieci wykorzystującej protokół EIBsec, wynikający z konieczności przesyłania dodatkowych informacji potrzebnych do wymiany kluczy i synchronizacji urządzeń [12].

W związku z powyższym zaproponowano alternatywną metodę bezpiecznej transmisji danych, która jest wystarczająca na potrzeby przedstawionego systemu nadzoru, zapewniając jednocześnie poufność, integralność i aktualność przesyłanych danych. Metoda zakłada wykorzystanie: funkcji skrótu CRC-32 w celu weryfikacji integralności danych, numerowania wiadomości w celu zapewnienia ich aktualności oraz popularnego algorytmu szyfrowania symetrycznego 3DES, który pozwala na szyfrowanie bloków o długości 8 bajtów. Mechanizmy te są obsługiwane przez dodatkową warstwę bezpieczeństwa umieszczoną nad warstwą aplikacji zgodnie z wytycznymi normy PN-EN 61784-3.

Proces przetwarzania danych przez czujnik podczas wysyłania wiadomości do stacji monitorującej został pokazany na rys. 4. Wiadomość związana z warstwą bezpieczeństwa ma długość 14 bajtów, co odpowiada w systemie KNX obiektowi typu DPT16 (łańcuch znaków) i stanowi najdłuższą możliwą wiadomość, jaka może zostać przesłana w pojedynczym telegramie KNX.



Rys. 5. Proces przetwarzania danych po stronie odbiorcy
Fig. 5. The process of data conversion at the receiver side

Wiadomość rozpoczyna się od 16-bitowego pola Typ, w którym może być zakodowany format wiadomości oraz format danych pola Stan, które może być np. 32-bitową liczbą zmiennoprzecinkową określającą wartość mierzonej wielkości fizycznej lub zestawem bitów sygnalizujących stany alarmowe urządzenia.

Kolejnym polem jest 32-bitowy identyfikator czujnika, który pozwala na jego jednoznaczne zidentyfikowanie. Może to być np. numer seryjny lub inny unikalny adres, niezależny od adresu fizycznego w sieci KNX. Identyfikator ten, przekazywany w formie jawnej, umożliwia po stronie stacji monitorującej wybranie skojarzonego z czujnikiem klucza szyfrującego w celu odszyfrowania dalszej części wiadomości.

Kolejne 32-bitowe pole zawiera stan czujnika przekazywany do stacji monitorującej. Razem z wcześniejszymi polami jest ono uwzględniane podczas wyliczania 32-bitowej wartości CRC32. Algorytm CRC-32 cechuje się bardzo wysoką skutecznością wykrywania przekłamań dla krótkich wiadomości. Dla wiadomości o długości 10 bajtów pozwala wykryć wszystkie przekłamania o maksymalnym odstępie Hamminga równym aż 15 (zostaną wykryte wszystkie wiadomości, w których nastąpiło mniej niż 15 przekłamań dowolnych bitów) [13].

Ostatnim polem jest wartość 32-bitowego licznika, indywidualnego dla każdego z czujników, którego stan jest zwiększany o jeden po każdej wysłanej wiadomości. Licznik ten jest wykorzystywany do zapewnienia aktualności danych i jego wartość nigdy nie może się powtórzyć. Mając na uwadze, że wiadomości są wysyłane nie częściej niż co 1 s, licznik przepełni się najwcześniej za 136 lat, co w praktyce wydaje sie być wystarczające.

Podczas wysyłania danych warstwa bezpieczeństwa zastępuje wartość pola Licznik różnicą symetryczną (funkcja XOR) wartości CRC32 oraz wartości licznika. Następnie szyfruje algorytmem 3DES to pole wraz z polem stanu i całość wiadomości jest wysyłana do stacji monitorującej jako ciąg znaków (typ DPT16 w standardzie KNX).

Stacja monitorująca będąca odbiorcą wiadomości dokonuje procesu odwrotnego (rys. 5). Na podstawie pola Typ oraz unikalnego identyfikatora czujnika odszukuje właściwy klucz kryptograficzny i dokonuje odszyfrowania zaszyfrowanego bloku danych. Następnie oblicza CRC32, co pozwala uzyskać pierwotną wartość licznika na podstawie symetrycznej różnicy wartości CRC32 i ostatniego 32-bitowego pola wiadomości.

Wartość pola Licznik porównywana jest z analogicznym licznikiem przechowywanym dla każdego czujnika po stronie stacji monitorującej. Akceptowane są tylko te wiadomości, dla których wartości obu liczników zgadzają się. Zapewnia to spełnienie warunku aktualność danych, gdyż próba wykorzystania wcześniej podsłuchanych i zarejestrowanych wiadomości spowoduje ich odrzucenie. Jednocześnie weryfikowana jest integralność pozostałych danych, gdyż uzyskanie poprawnej wartości licznika wymaga uzyskania tej samej wartości CRC32, która była wyliczona podczas procesu wysyłania danych.

Kolejnym ważnym mechanizmem jest mechanizm synchronizacji liczników nadawcy i odbiorcy wiadomości. Licznik odbiorcy jest inkrementowany po każdej poprawnie odebranej wiadomości. Jeżeli jednak któraś z kolejnych wiadomości nie dotrze do odbiorcy, nastąpi rozsynchronizowanie się liczników. Mając na względzie jednokierunkowy charakter transmisji wiadomości oraz jej cykliczność, przyjęto, że do ponownego zsynchronizowania liczników można wykorzystać odebranie dwóch kolejnych wiadomości, spełniających kryterium niepowtarzalności wartości liczników. W celu ograniczenia częstości zdarzeń polegających na rozsynchronizowaniu się liczników na skutek utraty pojedynczej wiadomości spowodowanej zakłóceniami lub chwilową utratą łączności proponuje się ponadto akceptowanie wiadomości, których liczniki mieszczą się w pewnym przedziale wartości od n do $n + m$, gdzie n jest stanem licznika po stronie stacji monitorującej, a m odpowiada liczbie kolejnych wiadomości, które mogą zostać „zgubione”, nie powodując utraty synchronizacji.

Ostatnim niezbędnym mechanizmem jest mechanizm przeterminowania, który pozwala wykryć utratę łączności pomiędzy czujnikiem a stacją monitorującą. Polega on na zastosowaniu po stronie stacji monitorującej okna czasowego o ustalonej szerokości, rozpoczynającego się w chwili odebrania ostatniej poprawnej wiadomości od danego czujnika. Jeżeli kolejna wiadomość nie nadejdzie w zadanym czasie, uruchamiany jest odpowiedni alarm.

4. Podsumowanie

Zaproponowana metoda bezpiecznej transmisji danych ma na celu umożliwienie wykorzystania infrastruktury systemu KNX do monitorowania urządzeń/czujników związanych z bezpieczeństwem budynków. Uzupełnia ona standardowy protokół transmisji wykorzystywany w systemie KNX o dodatkową warstwę zapewniającą poufność przesyłanych danych oraz kontrolującą ich aktualność i integralność. Warstwa ta, po uwzględnieniu dodatkowych wymagań doty-

czących projektowania oprogramowania pozwala również spełnić wymagania normy PN-EN 61508 w zakresie niezawodności kanału komunikacyjnego.

W odróżnieniu od innych opracowanych rozwiązań metoda ta nie wymaga żadnych dodatkowych urządzeń, zachowuje zgodność z istniejącymi narzędziami konfiguracyjnymi KNX i pozwala wykorzystać istniejące standardowe komponenty systemu. Pozwala to na znaczne obniżenie kosztów ewentualnej certyfikacji na zgodność urządzeń ze standardem KNX oraz kosztów wykonania i uruchomienia systemu.

Na ukończeniu są prace nad budową prototypu. Po stronie stacji monitorującej wykorzystano dostarczaną bezpłatnie przez organizację KNX bibliotekę Falcon zapewniającą aplikacjom pracującym pod systemem operacyjnym Windows dostęp do danych przesyłanych poprzez magistralę KNX. Do budowy prototypu czujników wykorzystano moduły SIM-KNX współpracujące z komputerami PC za pośrednictwem interfejsu RS-232 lub USB. Docelowo zostaną one zastąpione mikrokontrolerami z obsługą stosu KNX. Prototyp umożliwi oszacowanie zapotrzebowania na zasoby mikrokontrolera (wielkość pamięci, moc obliczeniowa) oraz pozwoli na ostateczną weryfikację koncepcji w praktyce.

Planuje się również opracowanie modelu niezawodnościowego systemu wykorzystującego zaproponowaną metodę, który pozwoliłby na ilościowe oszacowanie prawdopodobieństwa wystąpienia niewykrywalnego błędu transmisji przy zastosowaniu przedstawionej metody. W szczególnie wymagających zastosowaniach pożądane może być również przeprowadzenie formalnego dowodu odporności metody na kryptoanalizę. Co prawda sam algorytm szyfrowania jest dobrze znany i jak dotąd uważany za bezpieczny, nie mniej znajomość struktury szyfrowanych danych oraz charakteru zmienności niektórych pól może siłę tego algorytmu obniżać.

Bibliografia

1. Miller F.P., Vandome A.F., McBrewster J., *KNX* (standard), Alphascript Publishing, Aurora, IL, USA 2010.
2. Loy D., Dietrich D., Schweinzer H.-J., *Open Control LonWorks/EIA 709 Technology*, Kluwer Academic Publishers, 2001.
3. BACnet – A Data Communication Protocol for Building Automation and Control Networks, ANSI/ASHRAE Standard 135, 2010.
4. Porzeziński M., *Inteligentny budynek – obecne technologie i kierunki rozwoju*, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, nr 29, 49–52, Gdańsk 2011.
5. Granzer W., Kastner W., *Security Analysis of Open Building Automation Systems*, Proc. 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP '10), 2010, 303–316.
6. PN-ISO/IEC 14762: *Technika informatyczna – Wymagania bezpieczeństwa funkcjonalnego dla domowych i budynkowych systemów elektronicznych* (HBES), PKN 2010.
7. PN-EN 61508-1: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne, PKN 2010.
8. PN-EN 61508-3: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 3: Wymagania dotyczące oprogramowania, PKN 2010.
9. PN-EN 61784-3: Przemysłowe sieci komunikacyjne – Profile – Część 3: Magistrale miejscowe bezpieczne funkcjonalnie – Ogólne zasady i definicje profili, PKN 2010.
10. Granzer W., Kastner W., Neugschwandtner G., Praus F., *Security in Networked Building Automation Systems*, 6th IEEE International Workshop on Factory Communication Systems, 2006, 283–292.
11. Mazur L., Porzeziński M., *Rozproszony system zdalnego nadzoru urządzeń telekomunikacyjnych*, „Pomiary Automatyka Kontrola", 7/2011, 806–809.
12. Kohler W., *Simulation of a KNX network with EIBsec protocol extensions*, VDM Verlag Dr. Müller, 2010.
13. Koopman P., *32-bit cyclic redundancy codes for internet applications*, Int. Conf. Dependable Systems and Networks (DSN), Washington DC, 2002, 459–468.

The conception of secure data transmission method in the KNX network for remote supervision system

Abstract: The paper presents the requirements for communication channels used for implement safety-related functions and proposes a method of secure data transmission in the KNX system. The method was developed for the remote supervision system and does not require any changes to existing KNX protocol. It involves the use of an additional layer over the KNX protocol stack to enable compliance with the requirements of data transmission safety and security.

Keywords: KNX system, functional safety, data transmission security

Artykuł recenzowany, nadesłany 24.06.2013, przyjęty do druku 17.09.2013.

dr inż. Michał Porzeziński

Adiunkt w Katedrze Automatyki Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej. Jego zainteresowania naukowe dotyczą zagadnień związanych z projektowaniem komputerowych systemów pomiarowo-sterujących oraz rozproszonych systemów automatyki budynków ze szczególnym uwzględnieniem problemów niezawodności i bezpieczeństwa.

e-mail: mporz@ely.pg.gda.pl