XXIV Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2014

Oddział Gdański PTETiS

WYBRANE ZAGADNIENIA NIEZAWODNOŚCI I BEZPIECZEŃSTWA TRANSMISJI DANYCH W PRZEMYSŁOWYCH SIECIACH KOMPUTEROWYCH

Michał PORZEZIŃSKI

Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
tel: 583486311 fax: 583471270 e-mail: mporz@ely.pg.gda.pl

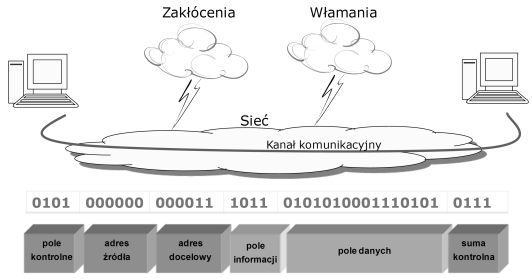
Streszczenie: W referacie przedstawiono problemy dotyczące bezpieczeństwa i niezawodności transmisji danych w przemysłowych sieciach komunikacyjnych wykorzystywanych do realizacji funkcji związanych z bezpieczeństwem. Omówiona została koncepcja kanałów komunikacyjnych bezpiecznych funkcjonalnie oraz związane z nimi wymagania niezawodnościowe określone w normach PN-EN 61508-3 oraz PN-EN 61784-3. Przedstawione zostały również zagrożenia dotyczące bezpieczeństwa transmisji danych w sieciach przemysłowych i stosowane metody ochrony oraz metodyka zarządzania bezpieczeństwem informacji w ujęciu norm z rodziny ISO/IEC 27000 i ISO/IEC 15408.

Słowa kluczowe: przemysłowe sieci komputerowe, niezawodność, bezpieczeństwo transmisji danych

1. WPROWADZENIE

W przemysłowych systemach sterowania i zabezpieczeń powszechnie stosowane są systemy rozproszone wykorzystujące do komunikacji przemysłowe sieci komputerowe. Zastosowanie rozwiązań sieciowych pozawala na uzyskanie znacznych oszczędności przy automatyzacji rozległych obiektów sterowania, takich jak: instalacje wodociągowe, petrochemiczne, elektroenergetyczne czy budynkowe. Systemy rozproszone charakteryzują się ponadto znacznie większą elastycznością i skalowalnością niż systemy scentralizowane, co ułatwia ich rozbudowę i dopasowanie do bieżących potrzeb.

Niezależnie od rodzaju sieci podstawą wymiany danych pomiędzy węzłami sieci są tzw. kanały komunikacyjne, którymi przesyłane są pakiety danych (rys. 1). Kanały komunikacyjne stanowią logiczne połączenie pomiędzy nadawcą i odbiorcą informacji i należy je traktować jako jeden z elementów biorących udział w realizacji danej funkcji sterowania lub bezpieczeństwa. Muszą one zapewnić wykonanie danej funkcji z odpowiednio wysokim prawdopodobieństwem, pomimo działania różnego rodzaju przypadkowych zakłóceń oraz celowych działań. Kanały są elementem sieci, które mogą być również narażone na różnego rodzaju „włamania" mające na celu ingerencję w proces transmisji danych. Możliwość takich ataków należy przewidzieć i się przed nimi odpowiednio zabezpieczyć.

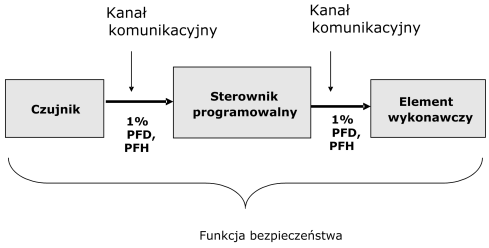


Rys. 1. Idea kanału komunikacyjnego jako logicznego połączenia węzłów sieci

2. WYMAGANIA DOTYCZĄCE NIEZAWODNOŚCI TRANSMISJI DANYCH

W przypadku projektowania systemów realizujących funkcje związane z bezpieczeństwem najczęściej stosowane jest podejście przedstawione w normie PN-EN 61508-1 [1]. Norma ta operuje pojęciem poziomu nienaruszalności bezpieczeństwa SIL (Safety Integrity Level) określanym dla danej funkcji bezpieczeństwa na podstawie analizy ryzyka i zagrożeń dla danego obiektu/systemu. Każdy z 4 poziomów SIL determinuje m.in. architekturę systemu bezpieczeństwa, sposób projektowania oprogramowania oraz maksymalne dopuszczalne prawdopodobieństwo niewypełnienia danej funkcji bezpieczeństwa. W nawiązaniu do tych informacji norma PN-EN 61784-3 [2] dotycząca magistral komunikacyjnych bezpiecznych funkcjonalnie zaleca, aby dla danego SIL prawdopodobieństwo wystąpienia niebezpiecznego błędu transmisji w każdym z wykorzystywanych kanałów stanowiło nie więcej niż 1% maksymalnego dopuszczalnego prawdopodobieństwa niewypełnienia danej funkcji bezpieczeństwa określonego dla danego poziomu SIL. Zostało to zobrazowane na rys. 2 [2]. PFD oznacza maksymalne dopuszczalne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na żądanie i jest rozpatrywane, gdy układ pracuje trybie rzadkiego przywołania. W przypadku pracy ciągłej rozpatrywany jest parametr PFH, który określa prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na godzinę. Prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa z rys. 2 jest obliczane jako suma prawdopodobieństw niezadziałania wszystkich elementów biorących udział w jej realizacji (łącznie z

kanałami komunikacyjnymi) i nie może przekroczyć maksymalnej wartości dopuszczalnej dla danego poziomu SIL.



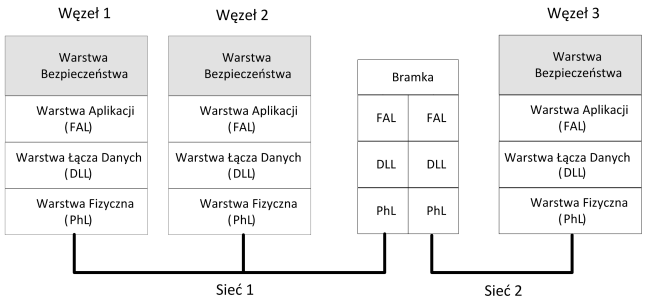
Rys. 2. Wymagania dotyczące niezawodności kanału komunikacyjnego

Punktem wyjścia do oceny ilościowej niezawodności kanału komunikacyjnego jest współczynnik BER (Bit Error Ratio) nazywany również elementową stopą błędu. Definiuje się go jako stosunek liczby przekłamanych bitów do liczby wszystkich przesłanych bitów. Oceny niezawodności kanału komunikacyjnego nie można jednak opierać tylko na BER, gdyż w procesie komunikacji wykorzystuje się szereg mechanizmów, których zadaniem jest wykrywanie różnego rodzaju błędów i ich naprawa. Są one zdefiniowane w opisie protokołu komunikacyjnego, który jest wykorzystywany do przesyłania informacji w danej sieci. Zestawienie najczęstszych błędów występujących w kanałach komunikacyjnych oraz metod ich wykrywania i naprawy przedstawiono w tabeli 1.

Tabela 1. Podstawowe rodzaje błędów oraz metody ich wykrywania [2, 4]

Metoda wykry-wania/ obrony / Rodzaj błędu	Numerowanie wiadomości	Stempel czasu	Przeterminowanie	Kody kontrolne i korekcyjne	Potwierdzanie	Powtarzanie/ powielanie	Sekwencja zmian wiadomości
Przekłamanie danych				x	x	x	x
Utrata wiadomości	x		x		x	x	x
Powtórzenie wiadomości	x	x					x
Opóźnienie		x	x		x		
Niepoprawna kolejność	x	x					x
Wtrącona wiadomość	x				x	x	x

Należy pamiętać, że na niezawodność kanału komunikacyjnego mają również wpływ błędy systematyczne, które mogły zostać wprowadzone do oprogramowania obsługującego protokół komunikacyjny na etapie projektowania i konfigurowania systemów i 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 [3] dla zakładanego poziomu nienaruszalności bezpieczeństwa. Tak zaprojektowany kanał komunikacyjny nazywany jest kanałem „białym". Dopuszcza się również wykorzystanie protokołów komunikacyjnych, które nie zostały opracowane w oparciu o wytyczne normy PN-EN 61508-3 lub których szczegóły realizacji po prostu nie są znane. Kanał tego typu określany jest jako kanał „czarny" i wymaga dodania na górze istniejącego stosu protokołu dodatkowej warstwy nazywanej warstwą bezpieczeństwa, co pokazano na rys. 3.



Rys. 3. Koncepcja warstwy bezpieczeństwa

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. Przy takim podejściu istnieje możliwość łączenia różnych podsieci za pomocą zwykłych przełączników, routerów i bramek, gdyż kontrola poprawności transmisji danych odbywa się tyko w punkcie początkowym i końcowym (powyżej warstwy aplikacji). Jeżeli wymagana niezawodność transmisji danych nie może być osiągnięta w oparciu o wymienione wcześniej mechanizmy należy wprowadzić redundancję kanałów komunikacyjnych. Redundancja może być również wymogiem wynikającym z przyjętego poziomu SIL. Przykładowe rozwiązania redundancji węzłów i magistral komunikacyjnych są opisane w [2].

Aby ułatwić pracę projektantom rozproszonych systemów automatyki realizujących funkcje bezpieczeństwa w normie PN-EN 61784-3 zdefiniowano szereg rodzin profili komunikacyjnych (CPF) magistral miejscowych bezpiecznych funkcjonalnie (tabela 2).

Tabela 2. Rodziny profili komunikacyjnych posiadające profile bezpiecznie funkcjonalnie [2]

Numer CPF	Nazwa profilu
1	FOUNDATION Fieldbus
2	CIP
3	PROFIBUS& PROFINET
6	INTERBUS
8	CC-Link
11	TCnet
12	EtherCAT
13	ETHERNET Powerlink
18	SafetyNET p

Są to przeważnie definicje standardów rozszerzających istniejące profile sieci przemysłowych o dodatkowe mechanizmy kontrolne. Mechanizmy te zaimplementowane są w postaci opisywanej wcześniej dodatkowej warstwy bezpieczeństwa. W przypadku niektórych rodzajów sieci (np. INTERBUS – Profil 6) umożliwia to zredukowanie ryzyka wystąpienia błędu komunikacji do poziomu mniejszego niż 10^{-7}. Pozwala to na stosowanie tego typu sieci do realizacji funkcji bezpieczeństwa, dla których wymagany poziom SIL wynosi 3 (maksymalne dopuszczalne ryzyko niewypełnienia

funkcji bezpieczeństwa wynosi 10^{-5}). Lista profili jest otwarta i należy liczyć się z kolejnymi aktualizacjami normy PN-EN 61784 uwzględniającymi nowo pojawiające się rozwiązania.

3. WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA TRANSMISJI DANYCH

3.1. Zagrożenia i typowe metody obrony

Kanały komunikacyjne mogą być również narażone na intencyjne działanie osób trzecich próbujących zakłócić działanie systemu. Dotyczy to zwłaszcza sieci, w których trudno jest zabezpieczyć medium komunikacyjne przed fizycznym dostępem osób niepowołanych (np. sieci bezprzewodowe, sieci stosowane w rozproszonych systemach automatyki budynków, czy rozlegle sieci akwizycji danych). Projektując takie systemy należy więc rozważyć możliwe ataki na sieć komunikacyjną i zabezpieczyć się przed nimi.

Podstawowe rodzaje zagrożeń bezpieczeństwa transmisji danych to: podsłuchiwanie, modyfikacja danych, podstawienie danych i ataki na dostępność danych.

Podsłuchiwanie (sniffing) jest formą ataku biernego [5], w którym zagrożona jest poufność przesyłanych danych. Atakujący poprzez dołączenie się do sieci w trybie nasłuchu może rejestrować wszystkie przekazywane przez dany segment sieci dane. Atakujący nie modyfikuje ani nie wprowadza do sieci danych, dlatego atak tego typu jest bardzo trudny do wykrycia. Obroną jest najczęściej wprowadzenie mechanizmów zapewnienia poufności danych działających w oparciu o algorytmy szyfrowania. Najczęściej wykorzystuje się do tego celu szyfry symetryczne, takie jak np. AES (Advanced Encryption Standard), opierające się na poufnym kluczu szyfrującym znanym tylko nadawcy i odbiorcy. Są one stosowane m.in. w protokołach komunikacyjnych ZigBee, BACnet, EIBsec. Co prawda w przypadku zastosowań przemysłowych poprzez sieć przekazywane są głównie informacje pomiarowe i sterujące, nie przedstawiające przeważnie większej wartości dla atakującego, szyfrowanie może być jednak potrzebne do funkcjonowania innych mechanizmów bezpieczeństwa np. mechanizmu zapewnienia integralności i autentyczności danych. Przykładem może być protokół EIBsec [6], w którym wraz z danymi szyfrowana jest obliczona na ich podstawie suma kontrolna, chroniąc w ten sposób dane przed nieautoryzowaną modyfikacją.

Modyfikacja danych jest formą ataku aktywnego, w którym atakujący przechwytuje dane, modyfikuje je i ponownie wprowadza do sieci. Modyfikacja może mieć na celu wprowadzenie w błąd operatora, aktywowanie określonego obwodu sterowania, uzyskanie dostępu do zasobów itp. Ta forma ataku jest znacznie trudniejsza do przeprowadzania od podsłuchiwania gdyż wymaga wprowadzenia do sieci nowych danych z zachowaniem mechanizmów arbitrażu i reżimów czasowych obowiązujących w danej sieci.

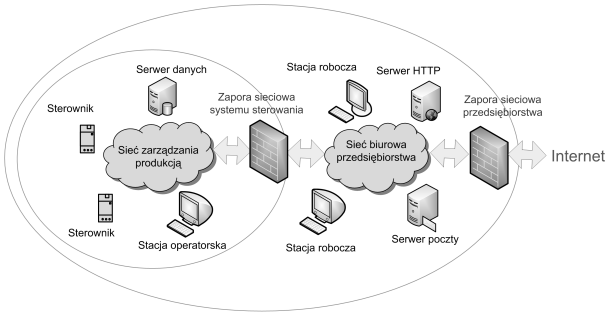
Przed nieautoryzowaną modyfikacją danych można się zabezpieczyć stosując mechanizmy zapewniające integralność i autentyczność danych. Mechanizmy te powinny uniemożliwiać zmodyfikowanie przesyłanych danych, bez zauważenia tego przez odbiorcę. Najpopularniejszym rozwiązaniem zapewniającym integralność danych jest stosowanie tzw. funkcji skrótu. Przekształcają one dane bitowe o dowolnej długości na dane o ustalonej długości zwane skrótem. Charakteryzują się przy tym cechami uniemożliwiającymi odtworzenie danych wejściowych na podstawie znajomości skrótu. Odbiorca może wyliczyć tę wartość według tego samego algorytmu i porównać z dołączonym skrótem. Funkcja skrótu może być parametryzowana kluczem kryptograficznym znanym tylko uprawnionym stronom, co jest najczęściej wykorzystywane do zabezpieczania danych przed nieautoryzowaną modyfikacją. Ze względu na ograniczone zasoby pamięci i mocy obliczeniowej urządzeń pracujących w sieciach kontrolno-pomiarowych opracowano dla nich specjalne dedykowane algorytmy weryfikacji integralności i autentyczności przesyłanych danych. Przykładem może być SCPM (Secure Communication Protocol for Middleware) [7], zastosowany m.in. w rozszerzeniu protokołu komunikacyjnego sieci KNX [8].

Podstawienie danych jest formą ataku, w którym atakujący wprowadza do sieci dane podszywając się często pod innego uprawnionego nadawcę. Do tego typu ataku są często wykorzystywane zarejestrowane wcześniej oryginalne dane innego nadawcy. W ten sposób atakujący może próbować np. zmienić stan sterowanego obiektu za pomocą zarejestrowanej wcześniej sekwencji danych sterujących, bez konieczności jakiejkolwiek ich modyfikacji. Do ochrony przed tego typu atakami służą mechanizmy zapewnienia aktualności (świeżości) przesyłanych danych. Najczęściej sprowadzają się one do użycia tzw. stempla czasu lub odpowiedniej sekwencji numeracji wiadomości w połączeniu z mechanizmem zapewnienia integralności i autentyczności danych, dzięki któremu nie jest możliwa niezauważona zmiana tych znaczników.

Ataki na dostępność danych są najczęstszą i najtrudniejszą do obrony formą ataków. Są atakami aktywnymi, których celem jest zakłócenie pracy sieci, tak aby zablokować możliwość normalnego przekazywania danych. Atak taki można zrealizować na bardzo wiele sposobów, takich jak: fizyczne uszkodzenie magistrali, generowanie bardzo dużego ruchu blokującego dostęp do magistrali innym węzłom, modyfikowanie przesyłanych danych powodujące ich niszczenie lub wprowadzanie do sieci specjalnie spreparowanych danych, których przetwarzanie przeciąża węzły do których są kierowane. Często jedynym skutecznym sposobem zapobiegania tego typu atakom (jak również innym wcześniej wymienionym) jest uniemożliwienie fizycznego dostępu do medium komunikacyjnego osobom nieupoważnionym i izolowanie chronionej sieci od innych sieci mogących być źródłem ataku.

W przypadku sieci polowych stosowanych na najniższym poziomie struktury systemu automatyki i zabezpieczeń jest to zwykle łatwe do wykonania, gdyż sieci te obejmują najczęściej niewielki obszar pokrywający się z obszarem sterowanego obiektu technologicznego, który sam w sobie jest chroniony. Trudniejsze jest izolowanie sieci zarządzania, często wykonywanej w standardzie Ethernet, która integruje sterowniki z systemami SCADA i może być łączona z siecią biurową przedsiębiorstwa lub nawet z sieciami publicznymi w celu umożliwienia wybranym osobom dostępu do danych procesowych i informacji o zdarzeniach. W takim przypadku izolowanie sieci wymaga użycia tzw. zapór sieciowych czyli specjalizowanych bramek i routerów filtrujących ruch międzysieciowy (rys. 4). Filtracja może polegać np. na kontroli wybranych parametrów przekazywanych wiadomości, takich jak: typ wiadomości, adres nadawcy, adres odbiorcy itp. W

przypadku sieci Ethernet opartej na przełącznikach zarządzanych istnieje również możliwość utworzenia sieci wirtualnych (VLAN). Mechanizm ten pozwala na takie skonfigurowanie przełączników, aby wybrane węzły sieci, mogły wymieniać dane tylko pomiędzy sobą.



Rys. 4. Przykład odseparowania sieci komputerowych w przedsiębiorstwie

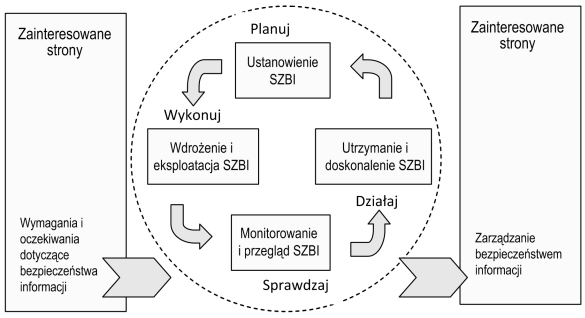
Należy przy tym pamiętać, że skuteczność ochrony zależy od poprawności działania urządzeń zabezpieczających. Niedostateczna ochrona może być wynikiem zastosowania nieodpowiednich metod zabezpieczeń, błędów konfiguracyjnych jak również ukrytych błędów tkwiących w oprogramowaniu, dlatego też elementy te powinny być przedmiotem odpowiedniej oceny skuteczności zabezpieczeń.

3.2. Zarządzanie bezpieczeństwem

Normy z rodziny PN-EN 61784 dotyczące sieci bezpiecznych funkcjonalnie nie zawierają, jak do tej pory, żadnych szczegółowych wytycznych dotyczących ochrony kryptograficznej przesyłanych danych. Zapowiedziane zostało opracowanie czwartej części tej normy poświeconej bezpieczeństwu transmisji danych w sieciach przemysłowych (IEC 61784-4 Secure communications for fieldbuses), ale do tej pory nie została ona wydana. Aktualnie pomocą przy projektowaniu i ocenie mechanizmów ochrony informacji w rozproszonych systemach sterowania i zabezpieczeń mogą być normy z rodzin: ISO/IEC 27000 oraz ISO/IEC 15408.

Normy z rodziny ISO/IEC 27000 dotyczą głównie organizacji wdrażających, eksploatujących i przeglądających systemy zarządzania bezpieczeństwem informacji. Najważniejsze z nich to normy ISO/IEC 27001 [9], oraz ISO/IEC 27002 zastępująca ISO/IEC 17799. Pierwsza z nich jest ogólną normą zawierającą wymagania dotyczące Systemów Zarządzania Bezpieczeństwem Informacji (Information Security Management Systems - ISMS) . Opiera się ona na procesach wykorzystujących model „Planuj-Wykonuj-Sprawdzaj-Działaj” (rys. 5), w skrócie nazywany PDCA (Plan-Do-Check-Act) [9], [10].

Planowanie obejmuje ustanowienie polityki SZBI, celów procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa informacji, tak by uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji. Wykonywanie jest rozumiane jako wdrażanie i eksploatacja polityki SZBI, zabezpieczeń, procesów i procedur. Sprawdzanie obejmuje szacowanie i pomiar wydajności procesów w odniesieniu do polityki SZBI, celów i doświadczenia praktycznego oraz dostarczanie kierownictwu raportów do przeglądu. Działanie to podejmowanie działań korygujących i zapobiegawczych w oparciu o wyniki wewnętrznego audytu SZBI i przeglądu realizowanego przez kierownictwo lub innych istotnych informacji, w celu zapewnienia ciągłego doskonalenia SZBI [9]. Z kolei norma ISO/IEC 17799 [11] (ISO/IEC 27002) jest zbiorem dobrych praktyk, porad i zaleceń dotyczących projektowania systemów wymagających zarządzania bezpieczeństwem informacji.



Rys. 5. Model PDCA (Plan-Do-Check-Act) [9]

Grupa norm z rodziny ISO/IEC 15408 „Information technology - Security techniques - Evaluation criteria for IT security” opisuje z kolei sposób oceny bezpieczeństwa systemów informatycznych oparty o metodykę Jednolitych Kryteriów (CommonCriteria, CC). CC udostępnia procedury pozwalające na zdefiniowanie istniejących zagrożeń oraz wymaganych zabezpieczeń, które na te zagrożenia odpowiadają, a następnie przeprowadzenie formalnej weryfikacji ich faktycznego działania. Wynikiem procesu certyfikacji powinien być tzw. "profil ochrony" (PP - protection profile), który definiuje zabezpieczenia stosowane przez produkt oraz certyfikat potwierdzający ich faktyczną skuteczność. Proces certyfikacji może być prowadzony według różnych poziomów szczegółowości i weryfikacji formalnej (EAL - Evaluation Assurance Level), począwszy od EAL1 (tylko testy funkcjonalne) aż do EAL7 (formalna weryfikacja projektu oraz testy) [12], [13], [14], [15]. Należy przy tym zaznaczyć, że posiadanie certyfikatu CC nie gwarantuje, że produkt jest bezpieczny pod każdym względem. Certyfikat zapewnia jedynie o poprawnym działaniu wszystkich zadeklarowanych przez producenta zabezpieczeń określonych w profilu ochrony.

Kompleksowe ujęcie problemów bezpieczeństwa systemów automatyki jest przedmiotem przygotowywanej do wydania rodziny norm ISA/IEC 62443. Opisane w niej będą zasady tworzenia i wdrażania programu bezpieczeństwa przemysłowych systemów automatyki i sterowania oraz sposób formułowania wymagań dla tego typu systemów. Przedstawione będą również możliwe do zastosowania technologie bezpieczeństwa takie jak: metody uwierzytelniania i autoryzacji użytkowników, konfiguracja zapór sieciowych, sieci wirtualne, metody kryptograficzne oraz monitoring i detekcja zagrożeń.

4. PODSUMOWANIE

Zastosowanie rozproszonych systemów automatyki wiąże się z wykorzystaniem sieci komputerowych, które z racji swojej rozległości są elementem szczególnie narażonym na działanie różnego rodzaju zakłóceń. Na niezawodność ich działania mają wpływ takie elementy, jak: rodzaj medium komunikacyjnego, struktura i topologia sieci, konstrukcja i jakość sprzętu elektronicznego wykorzystywanego w węzłach, zastosowany protokół wymiany danych. W przypadku systemów związanych z bezpieczeństwem pomocą w doborze

odpowiedniego rozwiązania sieci komunikacyjnej mogą być zalecenia zawarte w normie PN-EN 61784-3. Podstawowym wymaganiem jest takie zaprojektowanie lub dobranie kanału komunikacyjnego, żeby prawdopodobieństwo wystąpienia niewykrywalnego niebezpiecznego błędu transmisji było co najmniej 100 razy mniejsze od maksymalnego dopuszczalnego prawdopodobieństwa niewypełnienia związanej z nim funkcji bezpieczeństwa. Zaleca się ponadto, aby sprzęt i oprogramowanie realizujące transmisję danych było zaprojektowane, wykonane i zweryfikowane zgodnie z wymaganiami normy PN-EN 61508. Możliwe jest również wykorzystanie istniejących protokołów komunikacyjnych, nie spełniających tych wymagań, jeżeli zostaną one uzupełnione dodatkową specjalnie zaprojektowaną warstwą bezpieczeństwa. Praktyka pokazuje, że takie rozwiązanie jest powszechnie stosowane, a dla wielu popularnych przemysłowych sieci komunikacyjnych istnieją tzw. profile sieci bezpiecznych funkcjonalnie.

Obecnie coraz większą wagę przywiązuje się również do zagadnień bezpieczeństwa informacji przesyłanej w przemysłowych sieciach komputerowych. Niestety, protokoły wielu popularnych polowych sieci przemysłowych nie posiadają wbudowanych mechanizmów ochrony informacji i wykorzystywane są przy założeniu, że sieć wraz ze sterowanym obiektem jest chroniona przed fizycznym dostępem osób niepowołanych i odseparowana od innych sieci za pomocą odpowiednich zapór sieciowych.

Istotnym zagadnieniem jest również odpowiednie zarządzanie bezpieczeństwem w całym cyklu życia systemów wykorzystujących przemysłowe sieci komputerowe oraz ocena skuteczności stosowanych zabezpieczeń. W pierwszym wypadku pomocą mogą być normy z rodziny ISO 27000 wprowadzające ogólny model zarządzania bezpieczeństwem oraz opis dobrych praktyk inżynierskich stosowanych do zapewnienia bezpieczeństwa systemów. W drugim przypadku można się oprzeć na metodologii wspólnych kryteriów wprowadzonej w normie ISO/IEC 15408, bazującej na profilach ochrony oraz formalnie zdefiniowanych poziomach zaufania do zabezpieczeń EAL. Dla rozproszonych systemów sterowania i zabezpieczeń kluczowy wydaje się jednak być powstający zbiór norm ISA/IEC 62443 dotyczący bezpośrednio zagadnień bezpieczeństwa przemysłowych systemów automatyki i sterowania.

5. BIBLIOGRAFIA

1. PN-EN 61508-1: 2010, Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne.
2. PN-EN 61784-3: 2010, Przemysłowe sieci komunikacyjne – Profile – Część 3: Magistrale miejscowe bezpieczne funkcjonalnie - Ogólne zasady i definicje profili.
3. PN-EN 61508-3: 2010, Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 3: Wymagania dotyczące oprogramowania.
4. Herard J., Hedberg J., Kivipuro M, Malm T.,Edler H., Sjostrom H., Strawinski T.: Validation of communication in safety-critical controls system. Nordtest Tekniikantie 2003.
5. Karpiński M.: Bezpieczeństwo informacji, Wydawnictwo PAK, Warszawa 2012.
6. Granzer W., Kastner W., Neugschwandtner G., Praus F.: Security in networked building automation systems. In Proc. WFCS, 283–292, 2006.
7. ISO/IEC 24767-2: 2009. Information technology - Home network security - Secure Communication Protocol for Middleware (SCPM).
8. Application Note 158/13 v02 - KNX Data Security Draft Proposal, KNX Standard Version 2.1, KNX Association, October 2013.
9. PN-ISO/IEC 27001: 2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania. PKN, Warszawa 2007.
10. Evans, R.; Tsohou, A.; Tryfonas, T.; Morgan, T.: Engineering secure systems with ISO 26702 and 27001, System of Systems Engineering (SoSE), pp.1-6, 22-24 June 2010.
11. ISO/IEC 17799: 2000, Information technology — Code of practice for information security management.
12. Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria, praca zbiorowa pod redakcją A. Białasa, Instytut Technik Innowacyjnych EMAG, 2011.
13. ISO/IEC 15408-1: 2009, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.
14. ISO/IEC 15408-2: 2008, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components.
15. ISO/IEC 15408-3: 2008, Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components.

SELECTED ISSUES OF SAFETY AND SECURITY OF DATA TRANSMISSION IN INDUSTRIAL COMPUTER NETWORKS

Key-words: industrial computer networks, safety, security of data transmission

The paper presents security and reliability issues of data transmission in industrial communication networks used to implement safety functions. The concept of functional safety communication profiles and associated reliability requirements specified in the standards PN/EN 61508-3 and PN/EN 61784-3 are described. It also includes security risks of data transmission in industrial networks, the methods of data protection and information security management methodology in terms of ISO/IEC 27000 and ISO/IEC 15408 standards.