Marcin BEDNAREK [1], **Tadeusz DĄBROWSKI** [2], Michał WIŚNIOS [2]
[1] KATEDRA INFORMATYKI I AUTOMATYKI, POLITECHNIKA RZESZOWSKA, Al. Powstańców Warszawy 12, 35-959 Rzeszów
[2] INSTYTUT SYSTEMÓW ELEKTRONICZNYCH, WOJSKOWA AKADEMIA TECHNICZNA, ul. Kaliskiego 2, 00-908 Warszawa

Koncepcja zabezpieczenia transmisji pomiędzy stacjami diagnostycznymi

Dr inż. Marcin BEDNAREK

Pracuje na stanowisku adiunkta w Katedrze Informatyki i Automatyki Wydziału Elektrotechniki i Informatyki Politechniki Rzeszowskiej. Główny obszar zainteresowań to: diagnostyka systemów antropotechnicznych, komunikacja w rozproszonych systemach sterowania, niezawodność i bezpieczeństwo systemów. Jest autorem/współautorem ponad 80 publikacji.

e-mail: bednarek@prz.edu.pl

Dr hab. inż. Tadeusz DĄBROWSKI

Dyrektor Instytutu Systemów Elektronicznych na Wydziale Elektroniki WAT. Zasadniczy obszar zainteresowań naukowych i działalności dydaktycznej to: diagnostyka systemów antropotechnicznych, niezawodność eksploatacyjna, techniczne systemy bezpieczeństwa. Jest autorem/współautorem ponad 70 artykułów, 150 drukowanych referatów konferencyjnych, 12 pozycji książkowych.

e-mail: tdabrowski@wat.edu.pl

Streszczenie

W artykule rozpatrywany jest przypadek komunikacji pomiędzy stacjami systemu, które są dwufunkcyjne. Pierwszą z funkcji jest sterowanie procesem przemysłowym (stacja procesowa). Funkcja druga – to diagnozowanie procesu (stacja diagnostyczna). Istotnym aspektem komunikacji w tak zbudowanym systemie diagnostycznym jest konieczność bezpiecznego przesyłania wartości zmiennych diagnostycznych. Przedstawiono elementy rozwijające koncepcję zabezpieczenia transmisji pomiędzy stacjami systemu diagnostycznego. Proponowane rozwiązania programowe obejmują m.in. ochronę kryptograficzną transmisji pomiędzy lokalną i odległą stacją diagnostyczną.

Słowa kluczowe: bezpieczeństwo, komunikacja, sterownik przemysłowy, system diagnostyczny.

A conception of transmission security between diagnostic stations

Abstract

The paper presents the case of communication carried out using the Ethernet computer network. This network connects bi-functional stations of the system. The first function is an industrial process control (process station), the second - a diagnosing process, and more specifically – supervision. Therefore, from the point of view of the diagnostic system it will be called a diagnostic station. The most important aspect of communication in this integrated diagnostic system is the necessity of secure, uninterrupted transmission of diagnostic and process variables, between the stations of the system. In order to secure transmission of diagnostic variables, there should be introduced cryptographic protection of the transmitted data at the stage of sending the data from the diagnostic stations. The paper presents elements expanding the conception of transmission security between the stations of the diagnostic system. The proposed software solutions, among others the use of asymmetric encryption and hash function, have an effect on the security of transmission between the local and remote diagnostic stations.

Keywords: security, communication, industrial controller, diagnostic system.

Mgr inż. Michał WIŚNIOS

Absolwent Wojskowej Akademii Technicznej (w 2010r. ukończył studia na Wydziale Elektroniki). Obecnie doktorant i pracownik naukowo-dydaktyczny w Instytucie Systemów Elektronicznych WAT. Jego zainteresowania naukowe skupione są wokół metod wiarygodnego rozpoznawania osób na podstawie cech biometrycznych, a w szczególności identyfikacji na podstawie obrazu twarzy.

e-mail: mwisnios@wat.edu.pl

1. Wprowadzenie

W artykule rozpatrywany jest przypadek komunikacji wykorzystującej sieć komputerową pracującą wg standardu Ethernet. Sieć ta łączy ze sobą dwufunkcyjne stacje systemu. Pierwszą z funkcji jest sterowanie procesem przemysłowym przebiegającym w obiekcie dołączonym do wejść/wyjść obiektowych stacji. W tym kontekście stację systemu można nazwać stacją procesową (rys. 1). Drugą z funkcji jest diagnozowanie procesu, a dokładniej jego dozorowanie. Z punktu widzenia systemu diagnostycznego stacja ta może być nazywana stacją diagnostyczną (rys. 1). Zarówno zadania sterowania procesem, jak i zadania dozorowania implementowane są w tych samych urządzeniach, dlatego w dalszej części opracowania nazwy te będą używane zamiennie.

Ważnym zagadnieniem, w kontekście realizacji funkcji dozorowania, jest wiarygodność diagnozy. Biorąc pod uwagę rozproszenie między stacjami systemu składowych etapów-operacji procesu diagnozowania, tj. badania i wnioskowania, wpływ na wiarygodność diagnozy będą miały m.in.:

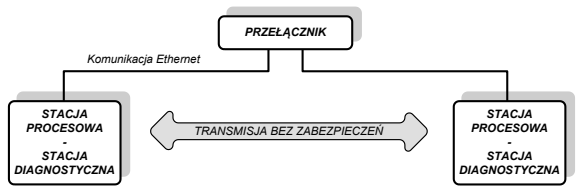
- wiarygodność procesu pozyskiwania informacji diagnostycznych w stacji lokalnej (m.in. wystarczająco dokładny pomiar);
- wiarygodność procesu generowania diagnozy w stacji odległej (istotne są tu: forma, głębokość i szczegółowość diagnozy);
- wiarygodność i niezawodność przesyłu danych diagnostycznych pomiędzy stacjami (czyli ogólnie: bezpieczeństwo transmisji).

Istotnym aspektem komunikacji, w tak interpretowanym systemie diagnostycznym, jest konieczność zapewnienia bezpiecznego, niezakłóconego przesyłania, pomiędzy stacjami systemu, pewnych zmiennych diagnostycznych i procesowych. Proces i jego dozorowanie odbywa się w układzie kilku stacji, na ogół odległych względem siebie [1, 2]. Na rysunkach niniejszego opracowania, dla lepszej czytelności, zrezygnowano z zamieszczania wielu urządzeń – ograniczono się najczęściej do dwóch stacji, ilustrujących dwie strony komunikacji.

W sytuacji przedstawionej na rys. 1, stacje systemu komunikują się za pomocą sieci komputerowej niezabezpieczonym kanałem komunikacyjnym. Jest on podatny na ingerencję intruza, zmierzającą do zakłócenia procesu komunikacji, w konsekwencji - procesu sterowania i diagnozowania. Domyślnie należy uważać jedną ze stron za lokalną stację diagnostyczną, drugą – za odległą stację diagnostyczną.

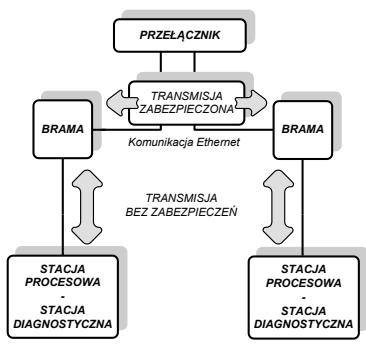
Ze względu na konieczność przesyłania pomiędzy stacjami wartości zmiennych diagnostycznych/procesowych, ważną cechą jest bezpieczność systemu komunikacji. Oznacza ona zdolność systemu do utrzymania się w stanie bezpieczeństwa. Bezpieczeństwo komunikacji jest warunkiem niezbędnym do uzyskania niezakłóconego transportu zmiennych diagnostycznych i w konsekwencji – wiarygodnej diagnozy. Żeby to osiągnąć, należy zadbać o ochronę przesyłanej informacji przed nieuprawnionym dostępem lub modyfikacją ze strony potencjalnych intruzów. Ze względu na zastosowanie sterowników przemysłowych jako stacji diagnostycznych, komunikacja pomiędzy nimi odbywa się według mechanizmów standardowo implementowanych przez producentów.

Nacisk w zakresie bezpieczeństwa przemysłowych systemów sterowania skierowany jest głównie na bezpieczeństwo z ich strony dla otoczenia (ang. *safety*). W tym kontekście należy wymienić np. rozwiązania Siemens [3]. Można też znaleźć publikacje dotyczące bezpieczeństwa sieci rozpatrywanego pod kątem wymagań czasowych [4]. Ochrona transmisji danych przed nieuprawnionym ujawnieniem lub naruszeniem ich integralności, czy też autentyczności stanowi jednak problem z dziedziny bezpieczeństwa danych, rozumiany jako ochrona (ang. *security*) przed zewnętrznymi czynnikami destrukcyjnymi, wprowadzającymi system komunikacji w stan niezdatności – tu interpretowany jako stan niebezpieczeństwa. Proces komunikacji pomiędzy stacjami należy więc w pewien sposób chronić przed zagrożeniami z zewnątrz [5]. Wśród firmowych rozwiązań z zakresu bezpieczeństwa przesyłu w kontekście *security* można wymienić np. [6-8].



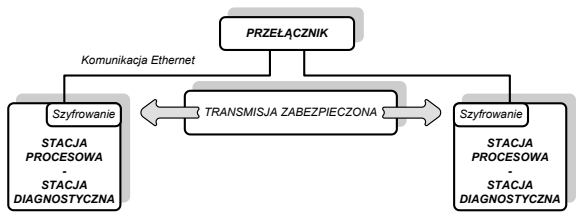
Rys. 1. Standardowa komunikacja Ethernet
Fig. 1. Standard Ethernet communication

Niektóre z proponowanych rozwiązań firmowych można nazwać częściowym zabezpieczeniem transmisji. Opierają się one na zasadzie umieszczenia dodatkowych, sprzętowych elementów pośredniczących w procesie komunikacji (rys. 2). Urządzenia te – nazywane w uproszczeniu „bramami" – odpowiednio skonfigurowane mogą komunikować się poprzez sieć komputerową, tworząc wirtualne kanały podlegające szyfrowaniu (ang. *VPN – Virtual Private Network*). Jednak mankamentem takich rozwiązań jest niepełne zabezpieczenie całej „trasy", którą są przesyłane dane. W dalszym ciągu pozostają niezabezpieczone fragmenty sieci komunikacyjnej. Oznaczone są one na rysunku 2 pionowymi strzałkami. Są to połączenia pomiędzy stacjami diagnostycznymi a bramami.



Rys. 2. Komunikacja częściowo zabezpieczona
Fig. 2. Partially secured communication

Na podstawie przedstawionych rozważań nasuwa się zatem pewien wniosek, że należy zabezpieczyć całą ścieżkę, którą przemieszczają się wartości zmiennych diagnostycznych, tzn. należy wprowadzić kryptograficzną ochronę przesyłanych danych już na etapie ich wysyłania ze stacji diagnostycznych (rys. 3).



Rys. 3. Komunikacja zabezpieczona
Fig. 3. Secured communication

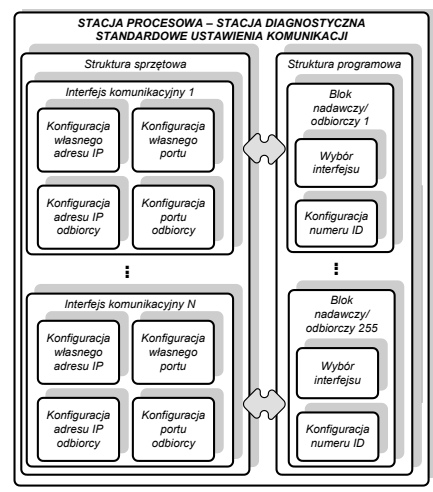
Nie ma wtedy konieczności używania urządzeń pośredniczących, szyfrujących transmisję. Cały proces szyfrowania i deszyfrowania danych można umieścić w programach sterujących stacji diagnostycznych. Może tu być stosowany symetryczny algorytm szyfrujący z identycznym kluczem do szyfrowania i deszyfrowania danych. Zabezpieczenie przesyłanych danych algorytmami symetrycznymi poruszano już w [9, 10]. W kolejnych punktach przedstawione zostaną elementy uzupełniające ww. koncepcję zabezpieczenia transmisji.

2. Komunikacja standardowa

Standardowe ustawienia transmisji Ethernet polegają na skonfigurowaniu kilku zasobów programowych związanych z komunikacją. Czynności przygotowawcze, przeprowadzane z poziomu lokalnej i odległej stacji diagnostycznej można ująć w kilku punktach (rys. 4):

1. Dodanie do zasobów sprzętowych odpowiedniego modułu (interfejsu komunikacyjnego) nadawczo/odbiorczego.
2. Skonfigurowanie własnego (stacji diagnostycznej lokalnej) adresu IP oraz numeru własnego portu, na którym prowadzona będzie komunikacja.
3. Wprowadzenie adresu IP rozmówcy (odległej stacji diagnostycznej) oraz numeru portu, na którym będzie prowadził komunikację.
4. Wybranie różnych ustawień dotyczących kierunku przepływu danych (klient lub serwer).
5. Ustawienie czasów cyklicznego wysyłania/odbierania komunikatów, oddzielnie dla zadania nadawcy i odbiorcy.
6. Dołączenie do bloku nadawczego identyfikatora (nazwy) wysyłanej zmiennej diagnostycznej oraz do bloku odbiorczego identyfikatora (nazwy) zmiennej odbieranej.
7. Wybór wykorzystywanego interfejsu komunikacyjnego (dodanego w punkcie 1).
8. Ustawienie ID bloku odbiorczego oraz nadawczego – a co za tym idzie – „sparowanie" bloków nadawczo-odbiorczych.

Można zauważyć, że wśród ww. etapów nie występują żadne ustawienia znacząco utrudniające dostęp do transmitowanych zmiennych diagnostycznych. Jakimś „quasi" zabezpieczeniem mógłby być numer ID bloku nadawczego lub odbiorczego, gdyby był poddawany szyfrowaniu przed wysłaniem.



Rys. 4. Standardowe ustawienia komunikacyjne stacji procesowej
Fig. 4. Process station standard settings

3. Rozszerzone zabezpieczenia

Z powodu braku w standardzie możliwości ustawienia zabezpieczeń, zdecydowano o wprowadzeniu do struktury programowej stacji diagnostycznej odpowiednich mechanizmów zmierzających do zabezpieczenia transmisji przed intruzami. Ich realizacja pole-

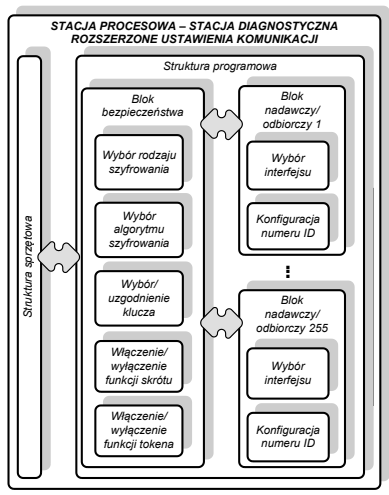
ga na odpowiednim skonfigurowaniu bloku funkcyjnego - tzw. bloku bezpieczeństwa (rys. 5) uaktywniającego odpowiednie algorytmy. Stacja diagnostyczna jest implementowana jako zadanie stacji procesowej. Z kolei stacja procesowa umożliwia tworzenie programów sterowania w jednym z języków normy PN-EN 61131-3, np FBD (ang. *Function Block Diagram*). Polega to, w uproszczeniu, na: wyborze odpowiednich bloków funkcyjnych z dostępnych bibliotek; parametryzacji bloków poprzez dostępne okna konfiguracyjne; połączeniu liniami przepływu sygnałów wejść i wyjść odpowiednich bloków, tworzących strukturę schematu realizującego określone zadanie (tutaj: zadanie bloku bezpieczeństwa) oraz wprowadzeniu odpowiednich zmiennych wejściowych i wyjściowych oraz połączeniu ich z pozostałymi elementami schematu FBD.

Tak utworzony schemat jest elementem większej struktury – zadania użytkownika. W niektórych przypadkach istnieje możliwość utworzenia tzw. bloków funkcyjnych użytkownika (ang. *user function block*). Wtedy cały schemat z bloków można „zamknąć" w jednym bloku funkcyjnym użytkownika, definiując dodatkowo tylko zewnętrzne (widziane z zewnątrz) wejścia i wyjścia.

Na rysunku 5 pokazano schematycznie rozszerzenie ustawień komunikacyjnych. Struktura sprzętowa pozostaje bez większych zmian. Konieczne jest tylko zdefiniowanie dodatkowych interfejsów komunikacyjnych – indywidualnie do obsługi każdego adresu odległej stacji diagnostycznej. Na poziomie struktury programowej stacji diagnostycznej zostaje zastosowany blok bezpieczeństwa (rys. 5).

W ramach parametrów konfiguracyjnych należy dokonać ustawień:
- rodzaju szyfrowania, szyfrowanie symetryczne lub asymetryczne:
  - wybranie szyfrowania symetrycznego (ustawiane jest na cały okres trwania komunikacji);
  - wybranie szyfrowania asymetrycznego w celu nawiązania komunikacji i uzgodnienia parametrów transmisji szyfrowanej symetrycznie;
- algorytmu szyfrującego:
  - dla szyfrowania symetrycznego algorytm będzie obowiązywał podczas całej sesji komunikacyjnej;
  - dla szyfrowania asymetrycznego wybrany algorytm będzie obowiązywał tylko do czasu przejścia na szyfrowanie symetryczne (por. wyżej);
- klucza:
  - jeżeli wybrano wcześniej szyfrowanie symetryczne, można wybrać klucz szyfrujący spośród proponowanych, wcześniej wprowadzonych przez operatora lub wprowadzić nowy, zgodny dla obydwu komunikujących się stacji diagnostycznych;
  - jeżeli wybrano wcześniej szyfrowanie asymetryczne, można wybrać długość klucza szyfrowania;
- włączenia lub wyłączenia jednokierunkowej funkcji skrótu przesyłanych danych;
- włączenia lub wyłączenia mechanizmu „żetonu" programowego (ang. *token*).

Konfiguracja wymienionych, rozszerzonych ustawień powinna odbywać się z poziomu:
1. *Stacji diagnostycznej (stacji procesowej)* – mogą to być przełączniki konfiguracyjne dołączone do binarnych wejść obiektowych, odpowiednio ustawiające parametry w kodzie dwójkowym – metoda wymagająca zastosowania jedynie zabezpieczenia w postaci fizycznej kontroli dostępu. Może to być np. zabezpieczenie dostępu do obiektu za pomocą biometrycznych technik kontroli dostępu.
2. *Stacji inżynierskiej* – dołączanej na określony, krótki czas stacji umożliwiającej utworzenie, sparametryzowanie i przesłanie programu stacji diagnostycznej. Należy zachować ostrożność ze względu na połączenie stacji w standardzie Ethernet. Dla zachowania poufności dokonywanych ustawień należy wykorzystać bezpośrednie, obserwowane połączenie przewodowe pomiędzy interfejsami stacji inżynierskiej i diagnostycznej (procesowej).
3. *Stacji operatorskiej* – dołączonej podobnie jak wyżej, z zachowaniem wspomnianych wymagań bezpieczeństwa. Należy wtedy wykorzystać standardowy obraz graficzny z dynamicznymi, aktywnymi elementami graficznymi pozwalającymi na ingerencję decydenta systemu w ustawienia bezpieczeństwa transmisji.



Rys. 5. Rozszerzone ustawienia programowe stacji procesowej
Fig. 5. Expanded software settings of process stations

W celu poprawnej komunikacji, stacje diagnostyczne powinny korzystać z kilku kanałów komunikacyjnych, czyli sparowanych ze sobą bloków nadawczych i odbiorczych:
- kanału uzgadniania parametrów transmisji (rozszerzonej o elementy zabezpieczające);
- kanału wymiany informacji o żetonie programowym;
- kanału wymiany kluczy szyfrujących;
- właściwego kanału wymiany danych (wartości zmiennych procesowych).

Tab. 1. Tryby pracy układu komunikacji
Tab. 1. Operating modes of the communication system

Tryb pracy	Znaczenie
T1	- komunikacja normalna bez zabezpieczeń
T2	- komunikacja normalna szyfrowana symetrycznie
T3	- komunikacja normalna szyfrowana asymetrycznie
T4	- zarezerwowany dla przyszłych zastosowań
T5	- transmisja klucza asymetrycznego publicznego
T6	- transmisja klucza asymetrycznego prywatnego
T7	- zarezerwowany dla przyszłych zastosowań
T8	- transmisja danych uwierzytelniających stację odległą bez zabezpieczeń
T9	- transmisja danych uwierzytelniających stację odległą z dołączoną wartością funkcji skrótu)
T10	- transmisja danych uwierzytelniających stację odległą z wartością funkcji skrótu szyfrowana symetrycznie
T11	- transmisja danych uwierzytelniających stację odległą z wartością funkcji skrótu szyfrowana asymetrycznie
T12	- zarezerwowane dla przyszłych zastosowań
T13	- transmisja danych z wartością funkcji skrótu szyfrowana symetrycznie
T14	- transmisja danych z wartością funkcji skrótu szyfrowana asymetrycznie
T15	- transmisja danych z wartością funkcji skrótu
T16	- zarezerwowany dla przyszłych zastosowań

Ważnym elementem zabezpieczonej transmisji jest protokół uzgadniania parametrów transmisji. Na podstawie analizy 16-bitowej wartości zmiennej całkowitej (słowa sterującego przesyłanego właśnie kanałem uzgadniania parametrów transmisji) stacja odbierająca może właściwie interpretować otrzymywane pozostałymi trzema kanałami dane. Można rozróżnić 16 (12 zdefiniowanych i 4 zarezerwowane dla przyszłych zastosowań) różnych trybów pracy układu komunikacji (tabela 1). Wartości 16 bitów zmiennej sterującej przedstawia tabela 2. Pominięto w niej nieużywane, przeznaczone dla przyszłych zastosowań tryby. Dla każdego trybu inny bit zmiennej przyjmuje wartość logiczną „1" (*TRUE*). Zabezpieczona transmisja zapewniająca poufność wymiany danych pomiędzy stacjami diagnostycznymi odbywa się wg. poniższego algorytmu:

1. Stacja lokalna zgłasza się do stacji odległej z prośbą o rozpoczęcie transmisji szyfrowanej. Znany musi być oczywiście adres zmiennej i format pytania. Komunikat transmitowany jest za pomocą modułów o znanych wcześniej numerach ID.
2. Stacja odległa potwierdza wybrany rodzaj komunikacji wysyłając odpowiedź zawierającą własny klucz publiczny.
3. Stacja odległa oczekuje na określonym porcie na nadejście zwrotne komunikatów od stacji lokalnej: z kluczem publicznym stacji lokalnej (I) i kluczem przeznaczonym do szyfrowania symetrycznego (II). Są do tego przeznaczone odpowiednie zmienne i bloki odbierające o określonych numerach ID.
4. Stacja lokalna wysyła swój klucz publiczny szyfrując go otrzymanym (w p.2) kluczem publicznym stacji odległej.
5. Stacja lokalna dokonuje wyboru (generuje) klucza symetrycznego używanego w dalszej części procesu komunikacji (punkt 11).
6. Stacja lokalna ekstrahuje klucz publiczny stacji odległej z odebranego komunikatu.
7. Stacja lokalna za jego pomocą i własnego klucza prywatnego szyfruje pierwszą przesłaną wiadomość.
8. Stacja lokalna wysyła tak przygotowany komunikat zawierający klucz symetryczny (tzw. klucz sesji) zaszyfrowany otrzymanym, publicznym kluczem od stacji odległej.
9. Stacja odległa odszyfrowuje dane przesłane w p. 4 i 8.
10. Stacja odległa generuje komunikat-potwierdzenie przełączenia się w stan transmisji zabezpieczonej kluczem symetrycznym.
11. Stacja lokalna rozpoczyna cykliczną transmisję zabezpieczoną kluczem sesji (do chwili przekroczenia ustawionego czasu *timeout* lub zakończenia transmisji).

Tab. 2. Tryby pracy układu komunikacji
Tab. 2. Operating modes of the communication system

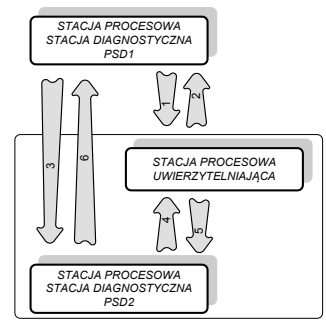
Nr bitu	Ustawienie bitów komunikatu sterującego wskazującego na wybrany tryb pracy (T) układu komunikacji											
	T1	T2	T3	T5	T6	T8	T9	T10	T11	T13	T14	T15
1	1	0	0	0	0	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	1	0	0	0	0	0	0	0	0
6	0	0	0	0	1	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	1	0	0	0	0	0	0
9	0	0	0	0	0	0	1	0	0	0	0	0
10	0	0	0	0	0	0	0	1	0	0	0	0
11	0	0	0	0	0	0	0	0	1	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	1	0	0
14	0	0	0	0	0	0	0	0	0	0	1	0
15	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0

Dodatkowym zabezpieczeniem transmisji od strony zapewnienia integralności komunikatów jest zastosowanie kontroli przesłanej informacji przy pomocy funkcji skrótu. Obliczana wartość funkcji skrótu na danych wysyłanych w stacji wysyłającej, przesyłana odrębnym, logicznym kanałem komunikacyjnym (odrębny numer ID modułu odbierającego) obliczana ponownie w stacji odbierającej (na podstawie równolegle wysyłanego komunikatu) może potwierdzać integralność tak przesłanych danych. Drugim z zabezpieczeń jest wspomniany wyżej mechanizm żetonu (znacznika) programowego. Program generowania żetonu na podstawie przesyłanej informacji, a także kilku innych parametrów (np. czasowych) pozwala na wygenerowanie liczby, która po przesłaniu weryfikowana jest także po drugiej stronie partnera komunikacji, służąc tym samym do dodatkowego uwierzytelniania.

4. Podsumowanie

W artykule przedstawiono elementy rozwijające koncepcję zabezpieczenia transmisji pomiędzy stacjami systemu diagnostycznego. Proponowane rozwiązania programowe wpływają na bezpieczeństwo transmisji pomiędzy lokalną i odległą stacją diagnostyczną:

- pozostawiony wybór rodzaju szyfrowania na symetryczne lub asymetryczne uelastycznia system pod względem zależności czasowych, nawiązanie połączenia asymetrycznego wymaga większych nakładów obliczeniowych i dłuższego oczekiwania na przesył kolejnych danych diagnostycznych;
- rozpoczęcie transmisji za pomocą algorytmu niesymetrycznego umożliwia tajną dystrybucję kluczy symetrycznych;
- wprowadzenie odrębnych kanałów komunikacyjnych dla przesyłanych wiadomości zawierających dane diagnostyczne i dla wiadomości sterujących utrudnia orientację intruza w samym sposobie komunikacji;
- przesył wartości zmiennych zabezpieczających (wartość funkcji skrótu, żetonu) służy do potwierdzenia integralności oraz autentyczności odebranych danych.



Rys. 6. Uwierzytelnianie z udziałem stacji procesowej uwierzytelniającej
Fig. 6. Authentication using the authentication station

Kolejnym etapem rozwojowym proponowanej koncepcji może być wykorzystanie tzw. trzeciej strony w celu potwierdzenia tożsamości (rys. 6). Można tego dokonać instalując (na rys. 6 - lokalnie względem stacji diagnostycznej PSD2) uwierzytelniającą stację diagnostyczną, stanowiącą centrum dystrybucji kluczy. Stacja ta, jako zaufana trzecia strona komunikacji, mogłaby udostępniać klucze publiczne innych stacji (rys. 6, strzałka 2 i 5) zwracających się do niej stacji diagnostycznych (rys. 6, strzałka 1 i 4) wykorzystywane w asymetrycznie szyfrowanej transmisji (rys. 6, strzałka 3 i 6).

5. Literatura

[1] Bednarek M., Będkowski L., Dąbrowski T.: Komparacyjno-progowe diagnozowanie w systemie transmisji komunikatów. Przegląd Elektrotechniczny, nr 5, s. 320-324, 2008.
[2] Bednarek M., Dąbrowski T., Będkowski L.: Diagnozowanie bezpiecznościowe wybranego systemu transportowego. Zeszyty Naukowe Politechniki Warszawskiej, seria Transport, zeszyt 73, s. 5-17, 2010.
[3] SIMATIC Distributed I/O System Fail-Safe Engineering ET 200S Distributed I/O System, Siemens, 2007.
[4] Kwiecień A., Gaj P.: Bezpieczeństwo transmisji w sieciach przemysłowych, Sotel, Gliwice 1999.
[5] Bednarek M., Dąbrowski T., Wiśnios M.: Diagnozowanie bezpieczeństwa komunikacji w przemysłowym systemie sterowania. MWK 2014, Waplewo 27-30.05.2014.
[6] SCALANCE W. Przemysłowa komunikacja bezprzewodowa - niezawodna, odporna, bezpieczna, Katalog skrócony, Siemens, 03/2007.
[7] Programowanie przez Internet: Konfiguracja modułów SCALANCE S 612 V2 do komunikacji z komputerem przez VPN, www.siemens.pl/simatic, 16/11/2007
[8] Inteligentna i bezpieczna komunikacja radiowa w systemie SCADA, Aprisa SR.
[9] Bednarek M., Dąbrowski T., Wiśnios M.: Bezpieczeństwo komunikacji w rozproszonym systemie sterowania. Przegląd Elektrotechniczny, nr 9, s. 72-74, 2013.
[10] Bednarek M., Dąbrowski T.: Koncepcja bezpiecznej transmisji danych w mobilnym systemie rozproszonym. Prace Naukowe Politechniki Warszawskiej, seria Transport, zeszyt 96, s. 69-76, 2013.

otrzymano / received: 06.06.2014
przyjęto do druku / accepted: 01.08.2014 *artykuł recenzowany / revised paper*