Biuletyn WAT
Vol. LXVI, Nr 1, 2017

Trójpoziomowe zabezpieczanie integralności i poufności przesyłanych danych w sieci przemysłowej

MARCIN BEDNAREK[1], TADEUSZ DĄBROWSKI[2]

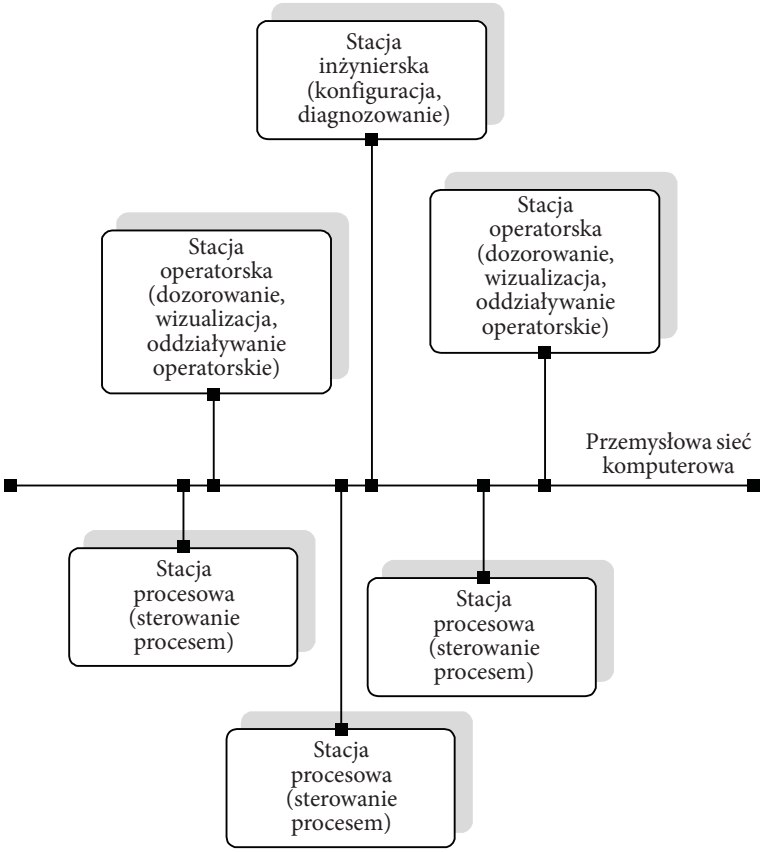
[1]Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki,
35-959 Rzeszów, ul. W. Pola 2,
[2]Wojskowa Akademia Techniczna, Wydział Elektroniki,
00-908 Warszawa, ul. gen. S. Kaliskiego 2,
bednarek@prz.edu.pl, tadeusz.dabrowski@wat.edu.pl

Streszczenie. W artykule rozpatruje się rozproszony minisystem sterowania złożony ze stacji procesowych, operatorskich i inżynierskich. Stacje procesowe prowadzą sterowanie procesem. Stacje operatorskie przeznaczone są do wizualizacji procesu przebiegającego w stacjach procesowych, a także do oddziaływania operatorskiego. Z poziomu stacji inżynierskich jest realizowana konfiguracja systemu oraz dozorowanie procesu komunikacji. Pomiędzy stacjami systemu przesyłane są dane procesowe. Zdatność procesu sterowania zależy od poprawnego przesyłu danych zawierających wartości zmiennych procesowych. Za poprawność otrzymanych danych odpowiadają działania przeciwdestrukcyjne realizowane w systemie komunikacji. Od zdatności systemu komunikacji zależy zdatność całego systemu sterowania. Artykuł zawiera rozważania odnoszące się do zależności integralności i poufności przesyłanych danych od poziomu zdatności układu komunikacji łączącego stacje systemu.
Słowa kluczowe: zdatność, integralność, poufność
DOI: 10.5604/01.3001.0009.9486

1. Wprowadzenie

Rozpatrywany w artykule system komunikacji rozproszonego mini-systemu sterowania (ang. *mini-DCS*) łączy wszystkie stacje [1]. Wzajemnie komunikujące się stacje systemu można zaliczyć do jednego z trzech rodzajów. Pierwszym rodzajem jest stacja inżynierska (rys. 1). To za jej pomocą możliwe jest zaprogramowanie pozostałych stacji systemu — przesyłanie programów sterujących. Za pomocą

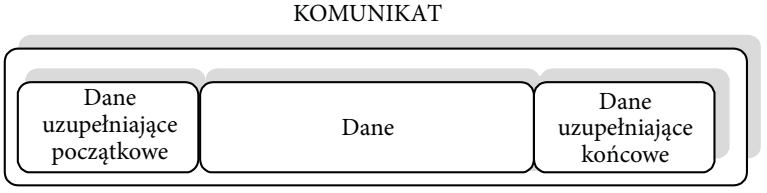
odpowiedniego oprogramowania stacji inżynierskiej przeprowadzany jest także proces uruchamiania oraz ewentualnego podglądu on-line wykonywania programów stacji procesowych. Drugi rodzaj to stacje procesowe prowadzące sterowanie procesem — sterowniki przemysłowe. Po zaprogramowaniu wykonują program sterowania obiektem. Trzecim rodzajem są stacje operatorskie. Za pomocą zaprojektowanych, wykonanych wcześniej i przesłanych ze stacji inżynierskiej obrazów operator ma możliwość oddziaływania lub dozorowania procesu przebiegającego w stacjach procesowych. Stacje systemu komunikują się wzajemnie, przesyłając wartości zmiennych procesowych niezbędnych do ich wzajemnego, prawidłowego funkcjonowania, a więc do pozostawania w stanie zdatności funkcjonalnej.



Rys. 1. Komunikujące się stacje systemu sterowania

2. Komunikacja standardowa w systemie

Każdy rodzaj stacji systemu może być producentem lub konsumentem wartości określonych zmiennych. Dla uproszczenia — wartości zmiennych przesyłanych w systemie, bez względu na rodzaj stacji, która je wyprodukowała, nazywamy wartościami zmiennych procesowych. Są one przesyłane w komunikatach. Każdy komunikat oprócz właściwych danych zawierających zazwyczaj wartość zmiennej procesowej (rys. 2 — pole *Dane*) przenosi także dane uzupełniające. Dane uzupełniające są niezbędne w standardowym procesie przesyłu. Odpowiadają one m.in. za adresację (*Dane uzupełniające początkowe*) oraz prostą detekcję błędów (*Dane uzupełniające końcowe*) [2].



Rys. 2. Struktura standardowego komunikatu

Zdatność procesu sterowania zależy od poprawnego przesyłu danych zawierających wartości zmiennych procesowych. Od zdatności systemu komunikacji zależy zdatność całego systemu sterowania. Kluczową rolą jest więc właściwe spreparowanie przesyłanej informacji zapewniające zachowanie odpowiedniego poziomu bezpieczeństwa [3]. W klasycznym procesie komunikacji wśród danych uzupełniających, oprócz początkowego pola nagłówka komunikatu zawierającego m.in. adres docelowej stacji (*Dane uzupełniające początkowe*), znajdują się dane (*Dane uzupełniające końcowe*) z wartością cyklicznej sumy kontrolnej (CRC) [4] przesyłanych danych (CRC pola *Dane*). Zwróćmy jednak uwagę, że cykliczna suma kontrolna umożliwia jedynie detekcję przypadkowych błędów transmisji. Mając na uwadze możliwość celowych działań destrukcyjnych skierowanych na proces komunikacji, można stwierdzić, że jest ona tylko „namiastką" kontroli integralności przesyłanych danych. Podrobienie zawartości pola *Dane* w celu otrzymania tożsamej z oryginalną wartości CRC nie jest działaniem skomplikowanym.

3. Procesy przeciwdestrukcyjne

W wieloprocesowym ujęciu procesu eksploatacji systemu komunikacji [5] wyróżnia się dwie antagonistycznie działające grupy procesów. Oprócz procesu użytkowania wyróżnić można procesy destrukcyjne i procesy przeciwdestrukcyjne.

Działania procesów destrukcyjnych prowadzą system do stanu niezdatności, natomiast efektem działania procesów przeciwdestrukcyjnych jest utrzymanie stanu zdatności systemu komunikacji oraz neutralizacja skutków działania tych pierwszych procesów. W zależności od poziomu zaawansowania (intensywności przeciwdziałania procesom destrukcyjnym), można wyróżnić trzy podprocesy procesu przeciwdestrukcyjnego [6]:

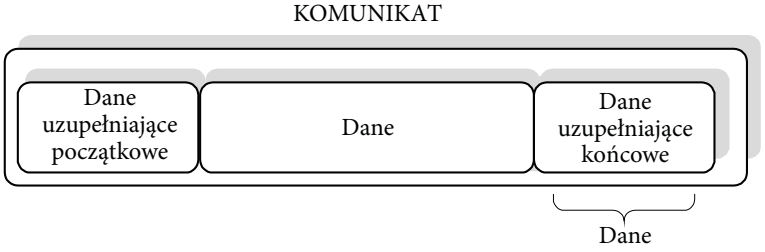
— osłonowy,
— interwencyjny,
— ratunkowy,

a także odpowiadające im poziomy utrzymania lub przywrócenia istniejącego lub prognozowanego funkcjonalnego stanu systemu:

— poziom I — pełnej zdatności,
— poziom II — niepełnej zdatności,
— poziom III — częściowej niezdatności.

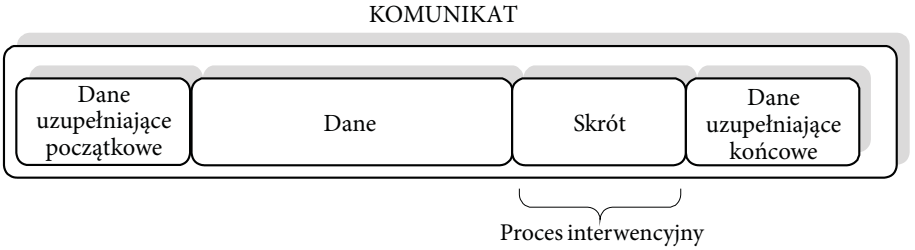
Każdy kolejny poziom poszerza (nie zastępując poprzedniego) wachlarz działań przeciwdestrukcyjnych, intensyfikując działania zmierzające do neutralizacji procesów destrukcyjnych.

W standardowym przesyle komunikatów, w rozproszonym przemysłowym systemie sterowania, stosuje się tylko działania osłonowe (**poziom I**). Odpowiadają za to procedury obliczeniowe generujące właśnie wymienione wcześniej dane uzupełniające końcowe zawierające cykliczną sumę kontrolną, obliczoną dla transmitowanych danych (rys. 3).



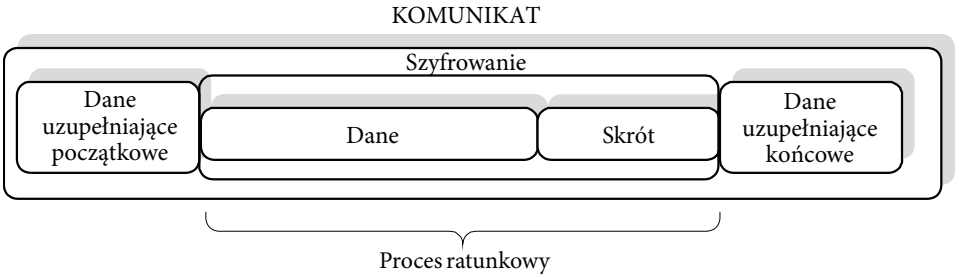
Rys. 3. Komunikat standardowy — działania osłonowe na poziomie I

Jak wspomniano wyżej, ze względu na słabe efekty działania funkcji cyklicznej sumy kontrolnej dotyczące zachowania integralności komunikatu w przypadku celowych prób destrukcyjnych należy wprowadzić dodatkowe zabezpieczenie. Jest ono niezbędne do przeciwstawienia się celowej ingerencji w treść przesyłanych danych. Uaktywniając podproces interwencyjny (**poziom II**), proponuje się wprowadzenie dodatkowego pola komunikatu z wartością jednokierunkowej funkcji skrótu [7]. W tym przypadku zamiast pola danych występuje para pól: *Dane* i *Skrót* (rys. 4).



Rys. 4. Komunikat — działania interwencyjne na poziomie II

Za sytuację zmierzającą do awarii systemu uznaje się — w rozpatrywanym przypadku — celowe działanie intruza polegające na podrobieniu danych wraz z wyliczoną na ich podstawie wartością skrótu. Uaktywnić należy wtedy procedury ratunkowe (**poziom III**) bazujące na szyfrowaniu. W ramach działań ratunkowych (przeciwawaryjnych) w dotychczasowych pracach autorów odnoszących się do zagadnień związanych z wieloprocesowym ujęciem eksploatacji systemu komunikacji proponowano m.in. przełączanie się na alternatywny kanał komunikacji [8]. Nie uwzględniano tu jednak uporczywych, celowych działań intruza. Obecnie proponuje się zaszyfrowanie przesyłanych danych symetrycznym algorytmem szyfrującym (rys. 5). Ewentualny problem dystrybucji klucza szyfrującego poruszano już m.in. w [9]. W zależności od wymaganej intensywności działania na poziomie częściowej niezdatności zabezpieczeniu kryptograficznemu podlegać może pole danych lub pole skrótu, lub razem: pole danych i skrótu. Działania na poziomie pełnej zdatności (I) są wykonywane przez standardowe mechanizmy obsługi komunikacji, natomiast na poziomach niepełnej zdatności oraz częściowej niezdatności (II i III) — przez dodatkowe zadania stacji procesowych lub skrypty stacji operatorskich.



Rys. 5. Komunikat — działania ratunkowe na poziomie III

Syntetyczne zestawienie poziomów utrzymania lub przywrócenia pożądanego funkcjonalnego stanu systemu komunikacji wraz z odpowiadającymi im podprocesami procesu destrukcyjnego i przeciwdestrukcyjnego przedstawiono w tabeli 1.

Tabela 1
Poziomy utrzymania lub przywrócenia pożądanego funkcjonalnego stanu systemu komunikacji

Lp.	Poziom zdatności	Proces przeciwdestrukcyjny	Realiz. procedura (przykład)	Mechanizm realizujący
I	poziom I — pełnej zdatności	osłonowy	suma kontrolna	wbudowany
II	poziom II — niepełnej zdatności	interwencyjny	funkcja skrótu	dodatkowy (zadanie, skrypt)
III	poziom III — częściowej niezdatności	ratunkowy wariant 1 wariant 2 wariant 3	szyfrowanie: skrótu danych skrótu i danych	dodatkowy (zadanie, skrypt)

4. Dyskusja dotycząca rezerwy czasowej

W rozpatrywanym systemie przeważająca liczba wymian komunikatów realizowana jest w sposób cykliczny. Należy zauważyć, że zastosowanie dodatkowych procedur poziomu II i III wymaga odpowiedniego czasu. Wobec tego układ komunikacji powinien dysponować dostateczną rezerwą czasową. Rezerwa ta spożytkowywana jest na:

— obliczenia wartości jednokierunkowej funkcji skrótu z wartości zmiennej procesowej potwierdzające integralność przesyłanych danych (II) — czas t_{II},
— operację wykonania algorytmu szyfrującego pozwalającego na zachowanie tajności danych (III) — czas t_{III},
— przygotowanie komunikatu składającego się z odpowiednio konkatenowanych kolejnych bajtów preparowanych danych (II, III) — czasy $t_{prep\mathrm{II}}$ i $t_{prep\mathrm{III}}$,
— przesłanie dodatkowych wartości związanych z wynikiem obliczeń w ramach procesów przeciwdestrukcyjnych (II lub/i III) — czas t_{trdod};
— przesłanie standardowych danych uzupełniających poziomu I — czas t_{I}.

Czas niezbędny na aktualizację wartości zmiennej przesyłanej pomiędzy dwiema stacjami (t_{akt}) jest sumą czasów (1):

$$t_{akt} = t_{\mathrm{II}} + t_{\mathrm{III}} + t_{prep\mathrm{II}} + t_{prep\mathrm{III}} + t_{trdod} + t_{\mathrm{I}}. \tag{1}$$

Minimalny niezbędny czas od chwili wytworzenia do chwili wykorzystania poprawnej wartości przesyłanych danych, uwzględniający procesy odbiorcze realizowane w ramach poziomów II i III, wynosi (2):

$$t_{prez} = 2(t_{\mathrm{II}} + t_{\mathrm{III}}) + t_{prep\mathrm{II}} + t_{prep\mathrm{III}} + t_{trdod} + t_{\mathrm{I}}. \tag{2}$$

Zakładając dla uproszczenia, że:
- po magistrali komunikacyjnej system transmisji przesyła dane dotyczące tylko jednej wartości zmiennej procesowej,
- nie występują inne wymiany danych (serwisowe, konfiguracyjne, diagnostyczne itp.),
- proces przesyłu kolejnej wartości następuje po zakończeniu odbierania danych przez stację docelową,
- transmisja odbywa się bez potwierdzania.

to czas cyklu wymian danych powinien być większy niż pełny czas dostarczenia wartości zmiennej poddanej zabiegom poziomu II i III (3):

$$t_{cykl} \geq t_{akt} + t_{\varepsilon}, \tag{3}$$

gdzie: t_{ε} — czas konieczny do zachowania technologicznej przerwy pomiędzy kolejnymi komunikatami.

Zwiększenie liczby przesyłanych wartości zmiennych (przesyłanych w oddzielnych komunikatach) do liczby k powinno wiązać się z zapewnieniem dodatkowej rezerwy czasowej na przesył (t_{rez}):

$$t_{rez} \geq (k - 1)(t_{akt} + t_{\varepsilon}). \tag{4}$$

Zwiększanie wartości czasu związanego z aktualizacją wartości zmiennej pomiędzy stacjami systemu może wydawać się tendencją niepożądaną. Należy tu jednak podkreślić, że w systemach komunikacji sterowników przemysłowych stosuje się detekcję i korekcję błędów z opóźnieniem. Nie przesyła się zazwyczaj informacji nadmiarowej pozwalającej na odtworzenie poprawnego komunikatu na podstawie przekłamanego. Korektę ewentualnych błędów przeprowadza się poprzez retransmisję komunikatu. Dodając do ww. czasów transmisji czasy oczekiwania na reakcję drugiej strony procesu komunikacji (*timeout*), wydaje się, że czas potrzebny na realizację procedur poziomu II i III relatywnie nie jest zbyt duży.

5. Czas realizacji procedur przeciwdestrukcyjnych

Zapewnienie zdatności układu komunikacji za pomocą procedur poziomu II i III pozwala jednocześnie na zwiększenie bezpieczeństwa przesyłanych danych w zakresie zapewnienia:
- integralności — poprzez obliczenie wartości jednokierunkowej funkcji skrótu z wartości zmiennej procesowej (poziom II),
- poufności — wynikającej z wykonywania algorytmu szyfrującego dane (poziom III).

Z punktu widzenia czasochłonności obliczeń ważne są dwa parametry czasowe wymienione we wzorze (2), tj. odpowiednio t_{II}, t_{III}. Zastosowane do obliczeń mogą być dowolne algorytmy gwarantujące odpowiedni, satysfakcjonujący decydenta systemu poziom bezpieczeństwa. W tabeli 2 przedstawiono wyniki eksperymentu pomiaru czasu realizacji procedury obliczania funkcji jednokierunkowej funkcji skrótu SHA-2(256) [7] dla poziomu II oraz asymetrycznego algorytmu kryptograficznego RSA [10].

Tabela 2

Wyniki badania czasu wykonania procedur poziomu II i III

Lp.	Czas cyklu zadania (t_{ask} cycle) [ms]	Poziom II[1] t_{II} [ms]	Poziom III[1,2] t_{III} [ms]
1	5	65,8	56,2
2	50	67,6	57,0
3	100	101,2	100,4
4	200	200,4	200,2

[1]wartości średnie czasu z 5 pomiarów, wartość wejściowa 100000
[2]dla klucza (n = 37969; e = 877; d = 34045)

Obliczenia wykonywane są jako program umieszczony w oddzielnym zadaniu użytkownika, napisany w języku ST sterownika przemysłowego AC800F. Należy zaznaczyć, że każdy z programów zgodnie z wybranym algorytmem zawiera w sobie kilkanaście pętli — iteracji. Wymaga więc iteracyjnego wykonania pewnych podobnych sekwencji działań. W tym celu badany program sterowania korzysta z możliwości stosowania tzw. bloków użytkownika, które zawierają realizację powtarzających się fragmentów algorytmu i wywoływane są iteracyjnie. Dzięki temu zmniejsza się kilkukrotnie objętość programu obliczającego procedury proponowanych poziomów. Na podstawie wartości średnich z wartości pomiarów czasu wykonania procedur (tab. 2) widać, że:

— dla pomiarów 3 i 4 czasy wykonania procedur są zbliżone do czasów cyklu obliczeń, tj. 100 ms i 200 ms, a więc obliczenia kończą się wcześniej niż czas przeznaczony na nie i sterownik czeka bezczynnie do końca zadania,
— dla pomiarów 1 i 2 szacunkowy czas potrzebny na obliczenia dla poziomu zachowania zdatności II wynosi prawie 70 ms, natomiast dla poziomu III — prawie 60 ms (dla czasu cyklu zadania 5 ms i 50 ms).

Akceptując te wartości czasu, uprawnione jest stwierdzenie, że możliwa jest komunikacja zapewniająca najwyższy stopień zdatności systemu komunikacji z czasem cyklu komunikacji większym od sumy ww. czasów obliczeń, powiększonym o pozostałe czasy zgodnie z (1). W przypadku zastosowania obliczeń w języku bloków funkcyjnych (FBD) przedstawione czasy wykonania ulegają zwiększeniu nawet kilkadziesiąt razy ze względu na sekwencyjne wykonywanie kolejnych bloków.

6. Podsumowanie

Przedstawione powyżej mechanizmy zachowania integralności i poufności wykorzystywane w sieciach komputerowych powszechnego użytku nie są stosowane w większości protokołów sieci przemysłowych [11, 12]. Spotykane rozwiązania sprowadzają się do wykorzystania, podczas transmisji danych pomiędzy stacjami, standardowych protokołów sieci komputerowych [13] implementujących mechanizmy zabezpieczające protokołu TLS [14]. Na przykład stosowane są tu metody tunelowania, np. komunikatów OPC [15] bezpiecznym kanałem. Podejmowane są też próby wprowadzenia mechanizmów uwierzytelniania lub szyfrowania [16, 17]. Z kolei innym stosowanym rozwiązaniem jest wprowadzenie stref bezpieczeństwa oraz traktowanie sieci przemysłowej jako zamkniętej o sterowanym dostępie poprzez zastosowanie bramy (*Gateway*) [18-21] lub wykorzystanie stref DMZ [22].

Należy podkreślić, że tego typu rozwiązania nie zawsze zapewniają spełnienie wymaganego, charakterystycznego dla rozwiązań przemysłowych warunku determinizmu czasowego. Natomiast proponowane w artykule działania, w ramach kolejnych poziomów utrzymania lub przywracania pożądanego funkcjonalnego stanu systemu komunikacji, można bez problemu zaimplementować do większości protokołów komunikacyjnych stacji systemu, rozszerzając (poziom II) i modyfikując (poziom III) pole *Dane* komunikatu.

Źródło finansowania publikacji: fundusz statutowy (PBS – WAT, DS – PRZ).

Artykuł wpłynął do redakcji 27.01.2017 r. Zweryfikowaną wersję po recenzjach otrzymano 10.02.2017 r.

LITERATURA

[1] Dokumentacja techniczna: AC800F, Engineering Manual, IEC 61131-3 Programming.

[2] Dokumentacja techniczna: Modicon Modbus Protocol Reference Guide, PI-MBUS-300 Rev. J., Modicon Inc.

[3] Anderson Ross J., *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, Willey, Hoboken, 2008.

[4] Stigge M., Plötz H., Müller W., Redlich J., *Reversing CRC — Theory and Practice*, HU Berlin Public Report SAR-PR-2006-05, Humboldt University, Berlin, May 2006.

[5] Będkowski L., Dąbrowski T., *Podstawy eksploatacji*, cz. 2. *Podstawy niezawodności eksploatacyjnej*, Wydawnictwo WAT, Warszawa, 2006.

[6] Dąbrowski T., *Diagnozowanie systemów antropotechnicznych w ujęciu potencjałowo-efektowym*, Wydawnictwo WAT, Warszawa, 2001.

[7] *Secure Hash Standard (SHS)* (Federal Information Processing Standards Publication 180-3), U.S. Department of Commerce, National Institute of Standards and Technology, 2008.

[8] Bednarek M., Będkowski L., Dąbrowski T., *Wieloprocesowe ujęcie eksploatacji układu komunikacji*, Diagnostyka, 34, 2005, s. 37-42.

[9] Dąbrowski T., Bednarek M., *Układ dozorująco-terapeutyczny wymiany kluczy w systemie transmisji danych procesowych*, Przegląd Elektrotechniczny, 11, 2015, s. 2014-2019.

[10] *Public-Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002.

[11] *Modbus Application Protocol Specification V1.1b3*, modbus.org, April 26, 2012.

[12] *Simatic Net. Profibus Network Manual*, System Manual, Siemens, Edition O4, 2009.

[13] Hayes G., El-Khatib K., *Securing Modbus Transactions Using Hash-based Message Authentication Codes and Stream Transmission Control Protocol*, Third International Conference on Communications and Information Technology (ICCIT), Beirut, 2013, pp. 179-184.

[14] Dierks T., Rescorla E., *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, 08.2008.

[15] *OPC Tunnel manual – System Freelance ABB*, July 2015, ABB.

[16] Phan R.C.W., *Authenticated Modbus Protocol for Critical Infrastructure Protection*, IEEE Transactions on Power Delivery, vol. 27, no. 3, July 2012, pp. 1687-1689.

[17] Cheminod M., Pironti A., Sisto R., *Formal Vulnerability Analysis of a Security System for Remote Fieldbus Access*, IEEE Transactions on Industrial Informatics, vol. 7, no. 1, Feb. 2011, pp. 30-40.

[18] *PROFINET technologie i informacje. Opis systemu standard dla zastosowań w automatyce, Profibas, 2005.*

[19] Fovino I.N., Carcano A., Masera M., *A Secure and Survivable Architecture for SCADA Systems*, Second International Conference on Dependability, Athens, Glyfada, 2009, pp. 34-39.

[20] Zhou Y., Chai D., Liu M., *Research on the Security Mechanism for Interconnection Between PROFIBUS and Internet*, Proceeding of the 11th World Congress on Intelligent Control and Automation, Shenyang, 2014, pp. 5972-5976.

[21] Schwaiger C., Sauter T., *A Secure Architecture for Fieldbus/Internet Gateways*, ETFA 2001, 8th International Conference on Emerging Technologies and Factory Automation. Proceedings, Antibes-Juan les Pins, France, 2001, vol. 1, pp. 279-285.

[22] *Freelance and Cyber Security. How to implement "Defense In-Depth Concept" in cyber strategies with Freelance DCS system*, ABB 2013.

M. BEDNAREK, T. DĄBROWSKI

Integrity and confidentiality three-level protection of the transmitted data in the industrial network

Abstract. Mini-DCS containing process stations, operator stations, and engineering stations are considered in the paper. Process stations provide the control of the process. Operator stations are designed to process visualization, as well as to the operator interaction. Configuration of the system and supervision of the communication process are carried out at the engineering stations. Between the stations of the system, the process data are transmitted. The fitness of the control process depends on correct transmission of the data with process values. Anti-destructive processes are responsible for the correctness of the received data. Fitness of the communication system determines the fitness of the entire control system. The article contains considerations relating to dependency of integrity and confidentiality of the transmitted data on the level of fitness of communication system connecting the stations.

Keywords: fitness, integrity, confidentiality
DOI: 10.5604/01.3001.0009.9486