Marcin BEDNAREK[1], Tadeusz DĄBROWSKI[2]

Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki (1), Wojskowa Akademia Techniczna, Wydział Elektroniki (2)

doi:10.15199/48.2015.11.52

Diagnozowanie bezpieczeństwa przesyłu danych w przemysłowym systemie sterowania

Streszczenie. *Rozpatruje się dwa przypadki komunikacji w przemysłowym rozproszonym systemie sterowania. W pierwszym wariancie testuje się zabezpieczenie komunikacji pomiędzy sterownikami przemysłowymi. W drugim wariancie – diagnozuje się bezpieczeństwo komunikacji pomiędzy stacją procesową i stacją operatorską. Komunikacja w systemach testowych oparta jest na standardzie Ethernet. W rozpatrywanych konfiguracjach rozproszonego systemu sterowania komunikacja odbywa się na poziomie procesowym, łączącym stacje procesowe i stacje operatorskie przy pomocy protokołu z rodziny TCP/IP. W referacie przedstawiono eksperymenty diagnozowania zagrożeń bezpieczeństwa komunikacji.*

Abstract*. Two cases of the communication in an industrial distributed control system are considered. In the first variant communication security between industrial controllers is tested. In the second option - vulnerability between process station and operator station is tested. The communication in the test systems is based on Ethernet standard. In the analyzed configurations of distributed control system, communication takes place at the process level connecting process stations and operator station using TCP/IP family protocol. (**Diagnosing data transmission security in the industrial control system**).*

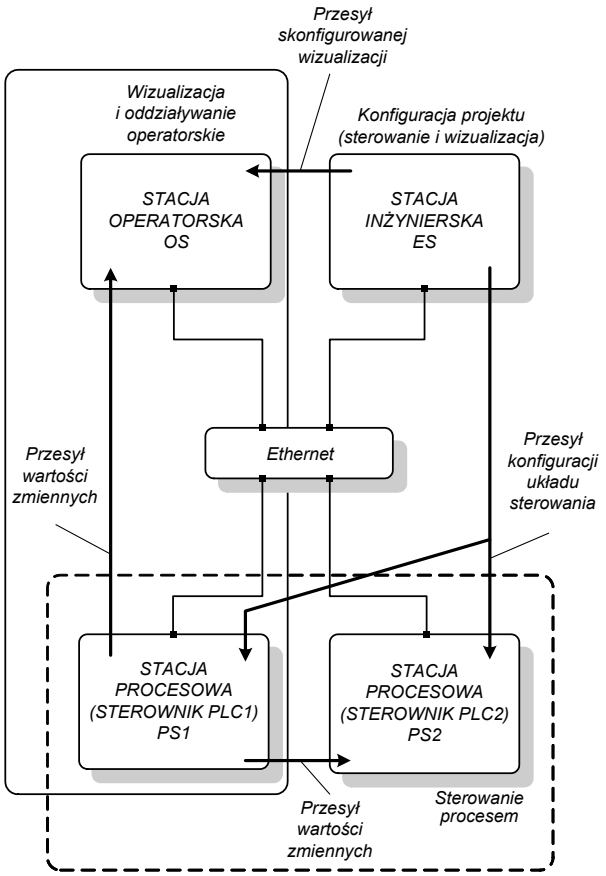
Słowa kluczowe: przemysłowy system sterowania, diagnozowanie bezpieczeństwa, komunikacja, sieć przemysłowa.
Keywords: industrial control system, diagnosing of the security, communication, fieldbus.

Wstęp

Przesył danych w ramach prezentowanego w artykule rozproszonego mini systemu sterowania odbywa się na poziomie procesowym [1], wykorzystującym standard Ethernet [2], łączącym stacje systemu przy pomocy protokołu TCP/IP. Stacjami tymi są trzy rodzaje urządzeń:

- Stacje procesowe (*ang. PS – Proces Station*), będące sterownikami przemysłowymi realizującymi programy sterowania procesami (rys. 1).
- Stacje operatorskie (ang. *OS – Operator Station*). Za pośrednictwem odpowiednio skonfigurowanych standardowych obrazów wizualizacyjnych stacji operatorskich prowadzi się oddziaływania operatorskie, wykorzystując do tego celu aktywne animowane elementy graficzne. Służą one także do graficznej prezentacji obrazu toczącego się procesu sterowania.
- Stacja inżynierska (ang. *ES - Engineering Station* [3]). Stacja operatorska i procesowa realizują zadania zdefiniowane i zaprogramowane a'priori przez projektanta-inżyniera systemu na poziomie stacji inżynierskiej. Ze stacji inżynierskiej, po odpowiednim skonfigurowaniu projektu stacji PS i OS, przeprowadza się konfigurację sprzętową, przesył i uruchomienie całego systemu.

Stacje systemu komunikują się pomiędzy sobą wg firmowych, zamkniętych protokołów komunikacyjnych. Zazwyczaj protokoły te są nieudokumentowane lub niewystarczająco udokumentowane. Projektanci liczą być może na to, iż nieznany sposób wymiany danych może być zabezpieczeniem przesyłu danych. W rzeczywistości jest to tylko złudne przekonanie o bezpieczeństwie transmisji. Nie ukrywanie sposobu działania algorytmu bowiem, a jego mechanizm szyfrowania wraz z utajnionym kluczem szyfrującym powinny gwarantować bezpieczeństwo [4]. Producenci sprzętu skupiają się często na zabezpieczeniach urządzeń w kontekście bezpieczeństwa ze strony urządzeń dla otaczającego środowiska [5]. Natomiast, jeśli rozpatrywane jest bezpieczeństwo przesyłu w kontekście ochrony przed intruzami – pojawiają się najczęściej rozwiązania bazujące na wirtualnych sieciach prywatnych (ang. *VPN*) [6, 7] lub zastosowaniu dodatkowych pośredniczących elementów do zestawienia bezpiecznego kanału [8]. Przesył pomiędzy stacjami systemu wykorzystujący standardowe firmowe mechanizmy często opiera się na protokole UDP, którego użycie podyktowane jest łatwością implementacji, jest okupione większą podatnością na odkrycie treści komunikatu przez osoby nieuprawnione.



Rys.1. Diagnozowanie bezpieczeństwa

Jak ważnym zagadnieniem jest zabezpieczenie transmisji pomiędzy stacjami systemu mogą świadczyć przypadki ingerencji intruza w systemy krytyczne ze względu na wypełniane funkcje. Przykładem mogą być ataki opisane w publikacjach [9,10]. Atakowanym systemem był system sygnalizacji świetlnej. Wykorzystując dedykowane urządzenia (karty sieciowe) można było zaingerować w

ustawienia sygnalizatorów na skrzyżowaniach. Nie dotyczy to wprawdzie przypadku spowodowania stanu katastrofy polegającej na jednoczesnym włączeniu zielonego światła dla dwóch kierunków, lecz jedynie uruchamiania odpowiedniej sekwencji zmiany świateł.

Artykuł niniejszy jest kolejną, po publikacji [11], próbą zwrócenia uwagi na istotne znaczenie zabezpieczenia transmisji. Uwidocznieniu tego ważnego aspektu służą dwa kolejne, diagnozowane przypadki komunikacji (zaznaczone na rysunku 1 ramkami):

(I) stacja procesowa – stacja procesowa (rys. 1, ramka - linia przerywana)

(II) stacja procesowa – stacja operatorska (rys. 1, ramka - linia ciągła).

Test pierwszy (I) polega na podszyciu się, zmianie oryginalnego komunikatu i wysłaniu polecenia ze stacji PS1 zmieniającego ustawienie wyjść binarnych stacji PS2.

Drugi przypadek (II) to także udana próba podszycia się i zafałszowanie informacji wyświetlanej na obrazie graficznym stacji operatorskiej oraz wprowadzenie operatora w błąd. Jako diagnozę dotyczącą niezdatności lub zdatności systemu komunikacji, a tym samym bezpieczeństwa systemu transmisji danych poddanemu atakowi powtórzeniowemu, można uznać odpowiedź na pytania:

(I) Czy można za pomocą ingerencji w standardową transmisję pomiędzy stacjami PS1 i PS2 podszyć się pod stację PS1 i zmienić ustawienia wyjść binarnych stacji PS2?

(II) Czy można za pomocą ingerencji w standardową transmisję pomiędzy stacją PS1 a stacją operatorską OS wprowadzić operatora w błąd prezentując na ekranie inny stan procesu niż toczący się aktualnie w stacji PS1?

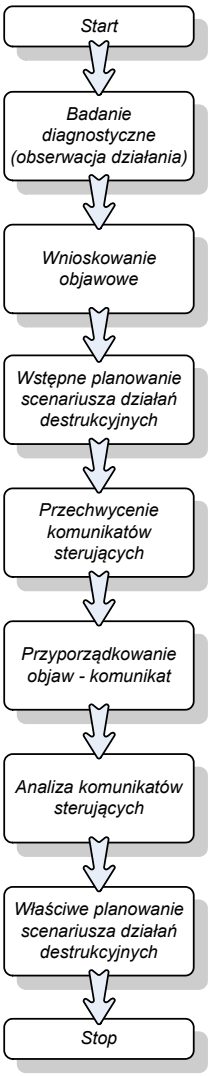
Przedstawione poniżej testy powinny dać odpowiedź na postawione pytania.

System destrukcyjny – planowanie scenariusza ataku

Na system destrukcyjny, za pomocą którego można naruszyć bezpieczeństwo systemu komunikacji składa się kilka elementów, których współdziałanie może okazać się sukcesem (z punktu widzenia systemu destrukcyjnego), czyli wprowadzeniem błędnego, fałszywego komunikatu do systemu transmisji. Przede wszystkim musi istnieć zainteresowany działaniami destrukcyjnymi intruz – operator-decydent systemu destrukcyjnego. Powinien on posiadać wystarczającą wiedzę do dokonania ataku. Udany atak może mieć miejsce tylko wtedy, gdy intruz dysponuje pewnym arsenałem środków technicznych, czyli właściwymi narzędziami do podsłuchu (ang. *sniffer*). Przydatne są tu także wszelkie metody socjotechniczne stosowane wobec operatorów atakowanego systemu, pozwalające na uzyskanie i zgromadzenie wiedzy niezbędnej do ataku. Pożądany jest też wcześniejszy dostęp do atakowanego systemu lub możliwość wykonania laboratoryjnego odpowiednika lub fragmentu atakowanego systemu przemysłowego i odtworzenia warunków rzeczywistych. Dodatkowo, zatem, dochodzi kwestia dość znacznego kosztu całego przedsięwzięcia. Bardzo przydatne może być także doświadczenie w projektowaniu systemów podobnych do atakowanego. Podsumowując - wszystkie wyżej wymienione elementy systemu destrukcyjnego: intruz, wiedza, arsenał środków technicznych i narzędzi, umiejętności socjotechniczne, doświadczenie projektowe sprzyjają zakończeniu sukcesem etapów planowania scenariusza działań destrukcyjnych (rysunek 2).

Na rysunku 2 przedstawiono przykład schematu przygotowania kilkuetapowego scenariusza ataku:

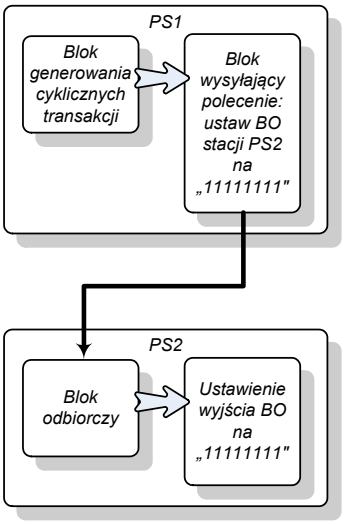
1. Badania diagnostycznego – obserwacji działania rzeczywistego, niezakłóconego systemu przemysłowego, podsłuchu transmisji komunikatów (a jeśli to nie jest możliwe - budowy laboratoryjnego odpowiednika).
2. Wnioskowania objawowego – na tym etapie możliwe jest zaobserwowanie wpływu komunikatów przesyłanych z jednej ze stacji na działanie drugiej.
3. Wstępnego planowania działań destrukcyjnych – decyzji dotyczącej celów cząstkowych intruza (wybór atakowanego zasobu).
4. Przechwycenia wszystkich transmitowanych komunikatów wysyłanych do atakowanej stacji.
5. Dokonania wyboru i przyporządkowania komunikatów sterujących powodujących wywołanie stanu, który intruz zamierza zakłócić (przyporządkowanie komunikat - powodowany objaw).
6. Analizy pola danych wybranych w punkcie 5. komunikatów i zlokalizowania wartości, które mają być zmienione przez intruza.
7. Właściwego zaplanowania scenariusza podszycia się pod nadawcę prowadzącego do zaburzenia pracy stacji atakowanej – decyzji dotyczących nowych, podmienionych wartości rozpoznanych pól danych komunikatu.



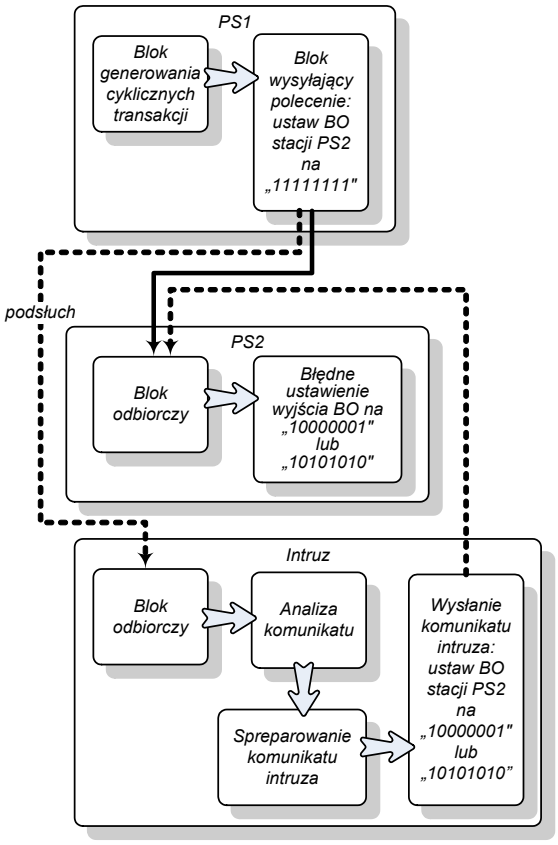
Rys.2. Planowanie scenariusza ataku

Test 1 – diagnozowanie bezpieczeństwa przesyłu pomiędzy stacjami procesowymi

Na rysunku 3 przedstawiono schematycznie standardową, niezakłóconą komunikację pomiędzy dwiema stacjami procesowymi rozproszonego systemu sterowania. Komunikacja odbywa się za pomocą protokołu UDP, wykorzystując technologię Ethernet. Stacja PS1 za pomocą specjalnych bloków komunikacyjnych wysyła do bloku odbiorczego PS2 komunikat ustawienia na kolejnych kanałach (0-7) wyjścia binarnego BO stacji PS2 wartości logicznej jedynki („11111111"). Komunikat wysyłany jest cyklicznie co 5 sekund. Stan niezakłócony przedstawia rysunek 5a.



Rys.3. Standardowa transmisja danych PS1-PS2



Rys.4. Transmisja zakłócona PS1-PS2

Stanowisko diagnozowania bezpieczeństwa komunikacji (rysunek 4) jest modyfikacją układu z rysunku 3. Składa się, oprócz stacji PS1 i PS2, ze stacji intruza z odpowiednim oprogramowaniem pozwalającym na obserwację ruchu sieciowego (ang. *sniffer*) [12] oraz umożliwiającym wysłanie dowolnie spreparowanego komunikatu.

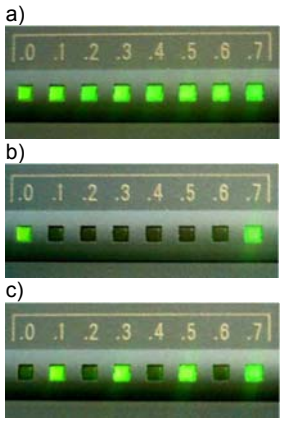
Przebieg diagnozowania bezpieczeństwa transmisji PS1 – PS2, czyli sprawdzenia podatności systemu na atak powtórzeniowy przebiega wg następującego schematu:

1. Podsłuch komunikatu wysłanego ze stacji PS1 oraz analiza pola danych (tabela 1, wiersz nr 1).
2. Rozpoznanie przesyłanej wartości ustawiającej wyjście BO PS2 (wartość 0xff - heksadecymalnie)
3. Skopiowanie całości komunikatu i zapis do pliku.
4. Użycie aplikacji pozwalającej na wysyłanie dowolnie spreparowanych komunikatów.
5. Wczytanie pliku ze skopiowanym komunikatem.
6. Podmiana pola danych na wartość 0xaa (tabela 1, wiersz 2) ustawiającą kolejne kanały wyjścia BO na „10101010".
7. Wymuszenie cyklicznego wysyłania, z czasem cyklu kilkadziesiąt razy mniejszym od założonego, komunikatu z nową wartością pola danych.
8. Obserwacja zachowania stacji PS2 (rys. 5b).
9. Podmiana pola danych na wartość 0x81 (tabela 1, wiersz 2) ustawiających kolejno kanały wyjścia BO na „10000001".
10. Wymuszenie cyklicznego wysyłania, z czasem cyklu kilkadziesiąt razy mniejszym od założonego, komunikatu z nową wartością pola danych.
11. Obserwacja zachowania stacji PS2 (rys. 5c).

Na podstawie przeprowadzonego eksperymentu można odpowiedzieć twierdząco na pytanie (I) dotyczące możliwości podszycia się pod stację PS1 i zmiany ustawienia wyjść binarnych stacji PS2 za pomocą ingerencji w standardową transmisję pomiędzy stacjami PS1 i PS2.

Tabela 1. Wartości pola danych komunikatu ustawiającego BO

Lp.	Stan	Bity BO (7..0)	Komunikat (pole danych)
1	Niezakłócony	11111111	ff:00:00:00:00:00
2	Ingerencja	10101010	aa:00:00:00:00:00
3	Ingerencja	10000001	81:00:00:00:00:00

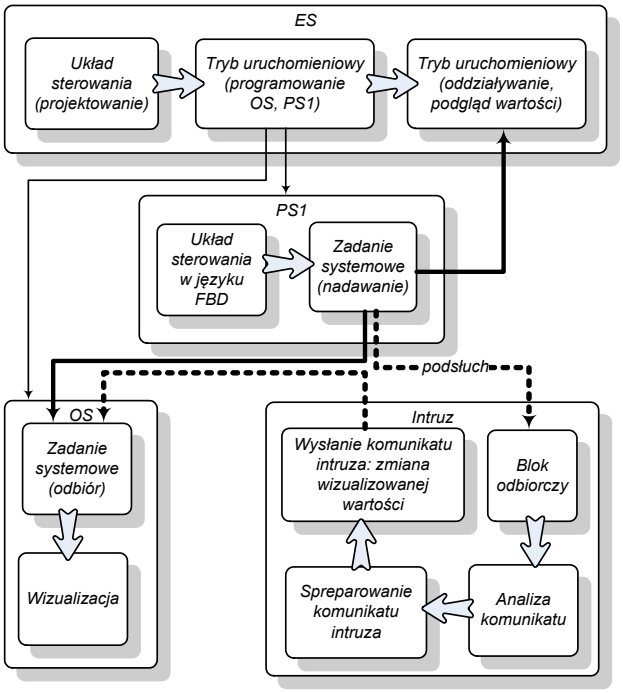


Rys.5. Wynik działania: a) prawidłowego; b, c) intruza

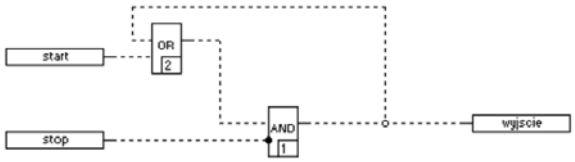
Test 2 – diagnozowanie bezpieczeństwa przesyłu pomiędzy stacją procesową i operatorską

Na rysunku 6 przedstawiono schematycznie sposób przeprowadzenia testu polegającego na podmianie wartości przesyłanej zmiennej pomiędzy stacją procesową PS1 i stacją operatorską OS. Stacja inżynierska ES wykorzystywana jest do konfiguracji projektu układu sterowania oraz projektu wizualizacji. Po jego wykonaniu, do każdej ze stacji zostaje załadowana odpowiednia część.

Zostało to oznaczone na rysunku 6 cienkimi liniami zakończonymi strzałkami wychodzącymi od ES. Stacja inżynierska uczestniczy także w trybie uruchomieniowym – służącym m.in. do śledzenia i obserwacji zmian wartości zmiennych. Można to zaobserwować np. w postaci zmian wyglądu linii przepływu sygnałów na schemacie w języku FBD [3] lub też w zdefiniowanych oknach trendu i wartości. Do stacji procesowej PS1 zostaje przesłany prosty program sterowania (rys. 7). Jest to tzw. układ „start-stop" działający analogicznie do przerzutnika RS, umożliwiający za pomocą przycisków monostabilnych (logiczne zmienne „start" i „stop") odpowiednio włączenie i wyłączenie urządzenia wykonawczego (logiczna zmienna „wyjscie").



Rys.6. Transmisja zakłócona PS1-OS



Rys.7. Układ sterowania PS1 – wersja 1

Stacja PS1 przesyła informacje do stacji inżynierskiej oraz do stacji operatorskiej w celu wizualizacji pracy układu. Stanowisko diagnozowania bezpieczeństwa przesyłu stacja PS1 – stacja OS początkowo służy do analizy komunikatów przesyłanych wg protokołu UDP.

Test dotyczy możliwości nieuprawnionej zmiany przez intruza wartości przesyłanych zmiennych, w taki sposób, aby mimo prawidłowego wykonania programu sterowania operator stacji OS otrzymał błędną informację i tym samym został wprowadzony w błąd, podejmując niepotrzebne działania zaradcze.

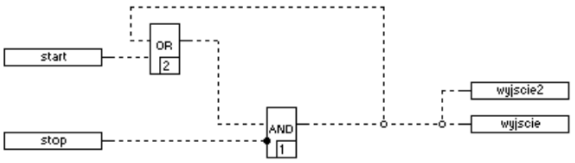
Nie jest znana a'priori struktura komunikatu służącego do przesyłu wartości zmiennych procesowych do stacji OS. Oprogramowanie podsłuchujące stacji intruza całą przechwyconą informację traktuje jako „dane". Proces diagnozowania polega na obserwacji kolejnych pól przechwyconych danych, przed i po zmianie wysyłanej wartości zmiennej oraz na wnioskowaniu dotyczącym miejsca w polu danych komunikatu, na którym dokonała się zmiana (miejsca, na którym jest transmitowana wartość). Informacja o położeniu bajtu pola danych zawierającego określone informacje może być z łatwością wykorzystana do podsłuchu oraz ataku powtórzeniowego służącego pozornej zmianie wartości.

Wymuszając z poziomu stacji inżynierskiej zmianę stanu wyjścia układu (wyjscie=0 → wyjscie=1) zaobserwowano zmianę w polu danych zaznaczoną ramką (tab. 2).

Tabela 2. Wartości pola danych komunikatu do OS dla wariantu z pojedynczym wyjściem (zmienna „wyjscie")

Lp.	Stan	Komunikat (pole danych)
1	wyjscie=0	20:00:1c:00:6c:04:10:00:16:01:01:04:ff:ff:08:00:00:00:00:00:54:47:54:47:54:47:54:47:54:47:54:47:10:04:10:00:08:00:1c:00:00:00:00:00:01:00:54:47:54:47:01:00:01:01:01:01:01:00:03:01:01
2	wyjscie=1	20:00:1c:00:96:06:10:00:16:01:01:04:ff:ff:08:00:00:00:00:00:54:47:54:47:54:47:54:47:54:47:54:47:10:04:10:00:08:00:1c:00:00:00:00:00:01:00:54:47:54:47:01:00:01:01:01:01:01:01:03:01:01

Następnym krokiem było przesłanie do stacji procesowej PS1 zmodyfikowanego programu sterowania (rys. 8). Jest to wspomniany układ „start-stop" uzupełniony o drugie, zdublowane wyjście (logiczna zmienna „wyjscie2").



Rys.8. Układ sterowania PS1 – wersja 2

Wymuszając z poziomu stacji inżynierskiej zmianę stanu obydwu wyjść układu (wyjscie=0→wyjscie=1, wyjscie2=0→wyjscie2=1) zaobserwowano zmiany w polu danych zaznaczoną ramkami (tab. 3). Pogrubione (na szarym tle) wartości odpowiadają kolejnym wartościom zmiennej „wyjscie2".

Tabela 3. Wartości pola danych komunikatu do OS dla wariantu ze zdublowanym wyjściem (zmienne „wyjscie", „wyjscie2")

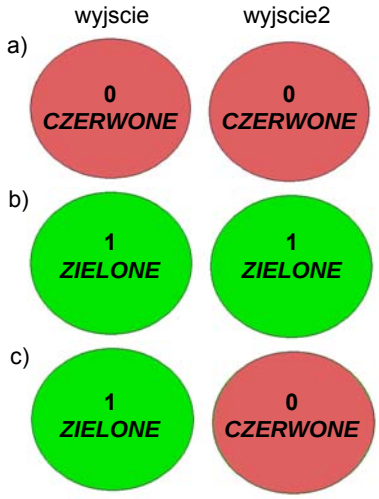
Lp.	Stan	Komunikat (pole danych)
1	wyjscie=0 **wyjscie2=0**	20:00:28:00:1f:04:10:00:15:02:01:04:ff:ff:24:00:00:00:00:00:54:47:54:47:54:47:54:47:54:47:54:47:10:04:69:00:24:00:28:00:00:00:00:00:68:00:54:47:54:47:04:00:01:01:01:01:00:03:01:01:00:01:03:01:00:01:03:01:**00**:01:03:01
2	wyjscie=1 **wyjscie2=1**	20:00:20:00:7f:05:10:00:16:01:01:04:ff:ff:1b:00:00:00:00:00:54:47:54:47:54:47:54:47:54:47:54:47:10:04:59:01:1b:00:20:00:00:00:00:00:01:00:54:47:54:47:02:00:01:01:01:01:01:03:01:01:**01**:01:03: 01
3	wyjscie=1 **wyjscie2=0** (ingerencja intruza)	20:00:1c:00:6c:04:10:00:16:01:01:04:ff:ff:08:00:00:00:00:00:54:47:54:47:54:47:54:47:54:47:54:47:10:04:10:00:08:00:1c:00:00:00:00:00:01:00:54:47:54:47:01:00:01:01:01:01:**00**:03:01:01

W ten sposób intruz mógł poznać miejsce przesyłania wartości zmiennych w komunikacji pomiędzy stacją

procesową i operatorską. Podobnie do testu 1. czynności polegające na:

- skopiowaniu wybranego komunikatu zawierającego pole danych przedstawione w tabeli 3 (wiersz 2);
- wczytaniu zapisanego komunikatu do aplikacji umożliwiającej wygenerowanie dowolnego komunikatu;
- podmianie pola danych na zawarte w tab. 3 (wiersz 3);
- wysłaniu tak spreparowanego komunikatu do stacji operatorskiej OS z częstością większą od standardowej;

spowodują błędną interpretację przez operatora sytuacji jako nieprawidłową, awaryjną. Będą się różniły wartości zmiennych wyjściowych sterowanych za pomocą wspólnej linii sygnałowej (por. rys. 8), co jest stanem niedozwolonym i niemożliwym do uzyskania w stanie zdatności układu transmisji PS1 - OS. Będzie to skutek interpretacji przez operatora sposobu prezentacji elementów graficznych na ekranie wizualizacyjnym (rys. 9c), Stanem uważanym za właściwy jest wyświetlenie elementów graficznych symbolizujących wyjścia w takim samym kolorze (rys. 9a, 9b).



Rys.9. Wynik działania układu „start-stop": a, b) prawidłowego; c) nieprawidłowego - poddanego działaniu intruza

Na podstawie przeprowadzonego testu można odpowiedzieć twierdząco także na pytanie (II), postawione we wstępie, dotyczące możliwości ingerencji w standardową transmisję pomiędzy stacją PS1 a stacją operatorską OS i wprowadzenia operatora w błąd poprzez prezentację na ekranie stanu procesu różniącego się od rzeczywistego, prowadzonego przez stację PS1.

Podsumowanie

W artykule przedstawiono diagnozowanie bezpieczeństwa transmisji dotyczące sprawdzenia możliwości:

- próby podszycia się, zmiany oryginalnego komunikatu i wysłania polecenia ze stacji PS1 zmieniającego ustawienie wyjść binarnych stacji PS2.
- próby podszycia się i zafałszowania informacji wyświetlanej na obrazie graficznym stacji operatorskiej, tym samym wprowadzenia operatora w błąd.

Diagnozy uzyskane w wyniku przeprowadzonych, zaprezentowanych testów, dotyczące niezdatności lub zdatności systemu komunikacji, a tym samym bezpieczeństwa systemu transmisji danych poddanemu atakowi powtórzeniowemu dają twierdzącą odpowiedź na postawione we wstępie pytania. Jednoznacznie wskazują także na konieczność dodatkowego zabezpieczenia transmisji. Można to osiągnąć stosując dodatkowe programowe metody ochrony danych, implementując np. algorytmy kryptograficzne pozwalające na szyfrowanie przesyłanych danych [13, 14].

LITERATURA

[1] Kwiecień A., Analiza przepływu informacji w komputerowych sieciach przemysłowych, Wydawnictwo Politechniki Śląskiej, Gliwice 2002
[2] Haudahl S., Diagnozowanie i utrzymanie sieci. Księga eksperta, Helion, Gliwice 2001
[3] Bednarek M., Wizualizacja procesów. Laboratorium, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2004
[4] Stinson D.R., Cryptography. Theory and Practice, Chapman& Hall/CRC, Boca Raton 2006
[5] Safety Integrated for Process Automation. Reliable, Flexible, Easy, Technical Brochure, Siemens
[6] Serafin M., Sieci VPN, Helion, Gliwice 2008
[7] Konfiguracja połączenia VPN (Virtual Private Network). Beckoff Automation Sp.z.o.o., 2007
[8] Programowanie przez Internet: Konfiguracja modułów SCALANCE S 612 V2 do komunikacji z komputerem przez VPN, www.siemens.pl/simatic, 16/11/2007
[9] Ghena B., Beyer W., Hillaker A., Pevarnek J., Alex J., HaldermanGreen Lights Forever: Analyzing the Security of Traffic Infrastructure, Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14), August 2014
[10] Zetter K., Hackers can mess with traffic lights to jam roads and reroute cars. Wired, Apr. 2014
[11] Bednarek M., Dąbrowski T., Wiśnios M., Diagnozowanie zagrożeń komunikacji w przemysłowym systemie sterowania, Przegląd Elektrotechniczny, nr 8/2014, 138-143
[12] Szmit M., Gusta M., Tomaszewski M., 101 zabezpieczeń przed atakami w sieci komputerowej, Helion, Gliwice 2005
[13] Bednarek M., Dąbrowski T., Koncepcja zabezpieczenia transmisji danych w mobilnym systemie diagnostycznym, *Journal Of KONBiN*, z.2(26)/2013, 61-70
[14] Bednarek M., Dąbrowski T.: Bezpieczeństwo komunikacji w rozproszonym systemie sterowania, *Przegląd Elektrotechniczny*, nr 9/2013, 72-74

***Autorzy**: dr inż. Marcin Bednarek, Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki, Katedra Informatyki i Automatyki, al. Powstańców Warszawy 12, 35-959 Rzeszów, E-mail: bednarek@prz.rzeszow.pl; dr hab. inż. Tadeusz Dąbrowski, prof. WAT Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, ul. Kaliskiego 2, 00-908 Warszawa; E-mail: tdabrowski@wat.edu.pl,*