Marcin BEDNAREK[1], Tadeusz DĄBROWSKI[2], Michał WIŚNIOS[2]

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

Diagnozowanie zagrożeń komunikacji w przemysłowym systemie sterowania

Streszczenie. *W rozpatrywanym, rozproszonym systemie sterowania komunikacja odbywa się na dwóch poziomach: procesowym - łączącym stacje procesowe przy pomocy protokołu TCP/IP (Ethernet) oraz obiektowym - łączącym stację procesową z rozproszonymi modułami wejść/wyjść, wykorzystującym magistralę CAN. W referacie przedstawiono kilka eksperymentów diagnozowania zagrożeń bezpieczeństwa komunikacji dotyczących poziomu procesowego i obiektowego.*

Abstract*. In the discussed distributed control system communication carried out at two levels: process level - linking process stations using TCP/IP (Ethernet), and object level - connecting the process station with distributed I/O modules, using the CAN bus. This paper presents some experiments diagnosing the security threats of communications concerning the process level and object (sensor) level. (**Diagnosing the Communication Threats in Industrial Control System**).*

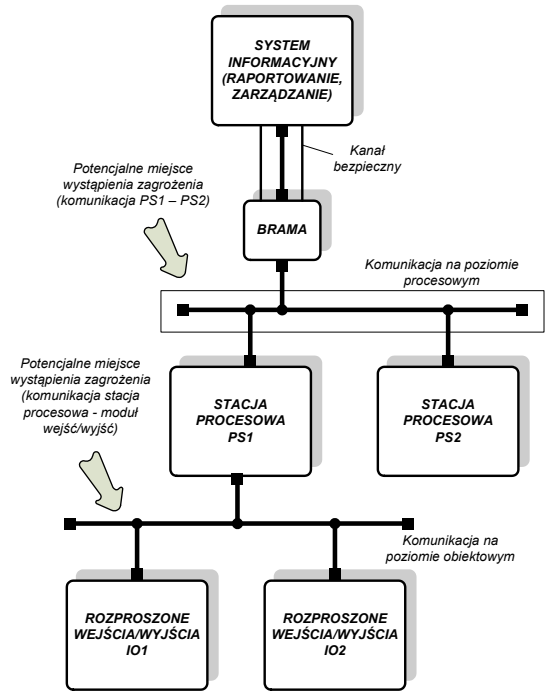
Słowa kluczowe: rozproszony system sterowania, diagnozowanie bezpieczeństwa, komunikacja, sieć przemysłowa.
Keywords: distributed control system, diagnosing of the security, communication, fieldbus.

doi:10.12915/pe.2014.08.32

Wstęp

W skład rozproszonego systemu sterowania wchodzi kilka rodzajów urządzeń. Są to m.in.:

- stacje procesowe (ang. *PS – Process Station*), czyli sterowniki przemysłowe, sterujące procesami (rys. 1);
- stacje operatorskie (ang. *OS – Operator Station*) realizujące wizualizację i oddziaływania operatorskie;
- stacje inżynierskie (ang. *ES - Engineering Station* [1]), z poziomu których przeprowadza się konfigurację i uruchomienie systemu sterowania.



Rys.1. Miejsca występowania zagrożeń komunikacji w rozproszonym systemie sterowania

W rozpatrywanym systemie (rysunek 1) komunikacja odbywa się na dwóch poziomach [2, 3]:

- na poziomie procesowym, wykorzystującym standard Ethernet [4], łączącym stacje procesowe przy pomocy protokołu TCP/IP;
- na poziomie obiektowym, wykorzystującym magistralę CAN [5], łączącym stację procesową z rozproszonymi modułami wejść/wyjść.

Aspekty bezpieczeństwa systemu zazwyczaj rozpatrywane są jako:

- zapewnienie bezpieczeństwa ze strony systemu dla otaczającego go środowiska (ang. *safety*);
- zapewnienie bezpieczeństwa dla systemu przed wpływem negatywnych czynników destrukcyjnych (ang. *security*)[19].

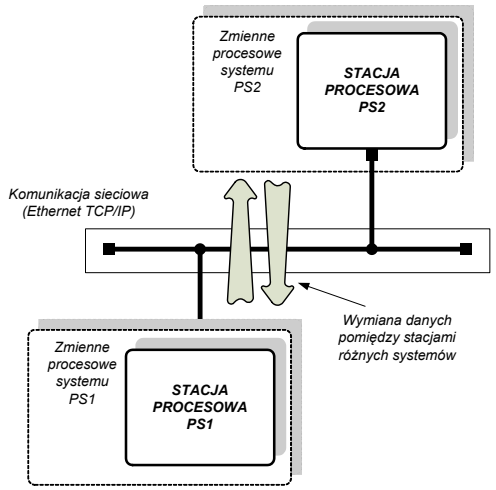
Większość rozwiązań koncentruje się na zapewnieniu bezpieczeństwa dla otaczającego środowiska ze strony systemu. Są to na przykład rozwiązania [6-9]. Mniej miejsca poświęca się problemom ochrony danych przesyłanych przez sieci komunikacyjne rozproszonych systemów sterowania. Zazwyczaj bazują one na zastosowaniu dodatkowych urządzeń wprowadzających możliwość zabezpieczenia transmisji (np. [10]). Nasuwają się więc wątpliwości, dotyczące zagrożeń bezpieczeństwa transmisji w rozproszonym systemie sterowania (rys. 1), w którym nie są implementowane dodatkowe funkcje zabezpieczające, a transmisja prowadzona jest wg firmowych, zamkniętych i nieudokumentowanych protokołów komunikacyjnych:

- czy można stworzyć zagrożenie poufności komunikacji, a tym samym - ingerencji w komunikację pomiędzy urządzeniami rozproszonego systemu sterowania – w taki sposób, aby pozyskać transmitowane informacje w sposób nieuprawniony?
- czy można podszyć się pod jedną z komunikujących się stron i stworzyć zagrożenie integralności komunikacji, tak aby w pewien sposób zmienić wartości przesyłanych zmiennych procesowych, a tym samym wprowadzić sterowany proces w stan niezdatności?

W dalszej części rozważań zostaną przedstawiony opis eksperymentów diagnozowania zagrożeń bezpieczeństwa komunikacji, których wyniki dadzą odpowiedź na postawione pytania.

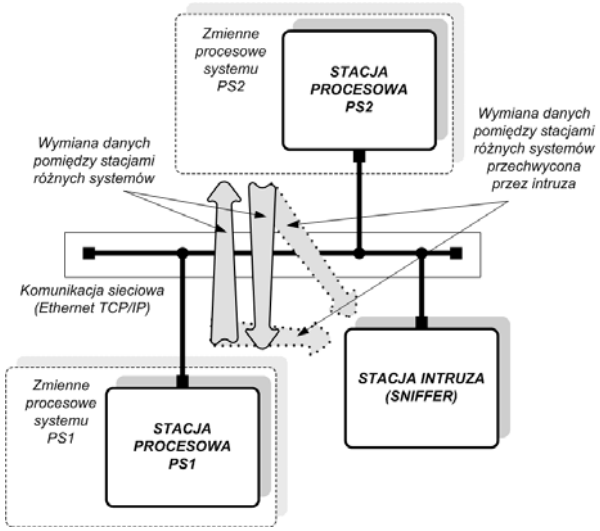
Diagnozowanie bezpieczeństwa transmisji pomiędzy stacjami procesowymi

Na rysunku 2 przedstawiono schematycznie komunikację pomiędzy dwiema stacjami procesowymi rozproszonego systemu sterowania. Komunikacja odbywa się za pomocą protokołu TCP/IP, wykorzystując technologię Ethernet. Stacje wymieniają wzajemnie komunikaty z zastosowaniem specjalnych bloków komunikacyjnych. Standardowa konfiguracja takiego połączenia polega na ustawieniu interfejsu sieciowego, numeru portu komunikacyjnego, doboru identyfikatora nadawanej zmiennej. Skonfigurować należy odpowiednio blok nadawczy w stacji PS1 oraz odbiorczy w stacji PS2. W celu zwrotnego przesyłu danych należy analogicznie postąpić dodając blok nadawczy do PS2 i odbiorczy do PS1.



Rys.2. Komunikacja pomiędzy stacjami różnych systemów

Stanowisko diagnozowania zagrożeń bezpieczeństwa komunikacji (rysunek 3) składa się ze stacji intruza z odpowiednim oprogramowaniem pozwalającym na obserwację ruchu sieciowego. W przypadku wykorzystania np. komputerowego symulatora stacji procesowej można wykorzystać do nasłuchu ruchu sieciowego tę samą maszynę. W przypadku dodatkowego komputera wymaganych jest kilka ustawień, za pomocą których można „oszukać" urządzenia sieciowe i cały ruch zmierzający do konkretnej stacji przekierować przez interfejs komunikacyjny intruza [11].



Rys.3. Podsłuch komunikacji pomiędzy stacjami

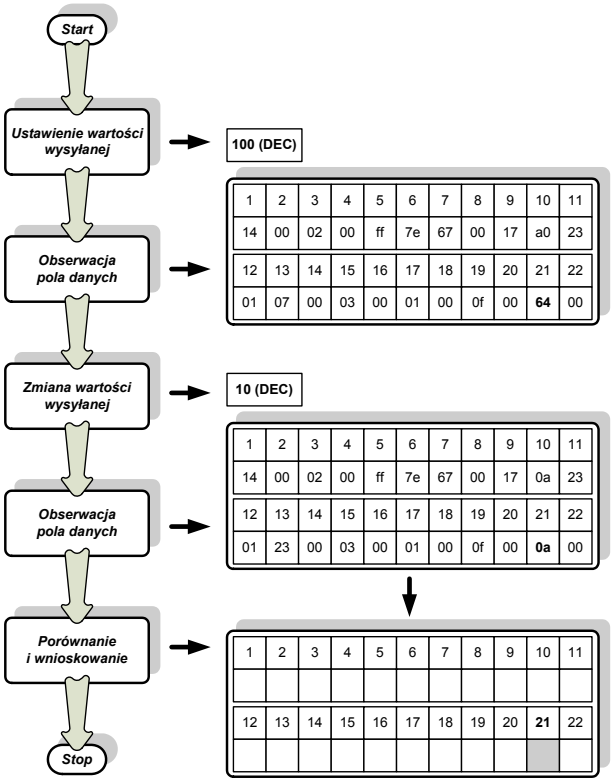
Uzyskanie informacji o przesyłanej wartości – przykład 1

Należy podkreślić, iż nie jest znana a'priori struktura protokołu warstw wyższych, służącego do przesyłu wartości zmiennych procesowych. Przed rozpoczęciem procesu diagnozowania stanowi ona „czarną skrzynkę". Oprogramowanie podsłuchujące (ang. sniffer) 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 (numeru bajtu), na którym jest transmitowana wartość. Informacja o numerze bajtu pola danych zawierającym określone informacje może być wówczas z łatwością wykorzystana do podsłuchu.

Celem eksperymentu było uzyskanie informacji o numerze bajtu pola danych przechowującego przesyłaną wartość zmiennej procesowej. W tym celu wykonano kolejne czynności (rysunek 4):

1. Ustawiono wartość zmiennej wysyłanej na 100 (DEC).
2. Przechwycono dane i obserwowano miejsce pojawienia się w polu danych ustawionej wartości (bajt nr 21).
3. Ustawiono wartość zmiennej wysyłanej na 10 (DEC).
4. Przechwycono dane i potwierdzono miejsce pojawienia się w polu danych ustawionej nowej wartości (bajt nr 21).
5. Porównano odpowiedzi i sformułowano diagnozę dotyczącą numeru bajtu pola danych niosącego informację o wartości zmiennej procesowej (21).

W toku dalszych badań sprawdzono także przesył zmiennych o większych wartościach (zajmujących kolejne bajty nr 21, 22 ...), zmiennoprzecinkowych i struktur zmiennych.



1	2	3	4	5	6	7	8	9	10	11
14	00	02	00	ff	7e	67	00	17	a0	23
12	13	14	15	16	17	18	19	20	21	22
01	07	00	03	00	01	00	0f	00	**64**	00

1	2	3	4	5	6	7	8	9	10	11
14	00	02	00	ff	7e	67	00	17	0a	23
12	13	14	15	16	17	18	19	20	21	22
01	23	00	03	00	01	00	0f	00	**0a**	00

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	**21**	22

Rys.4. Analiza przesyłanych danych – pole wartości

Uzyskanie informacji o numerze modułu odbierającego – przykład 2

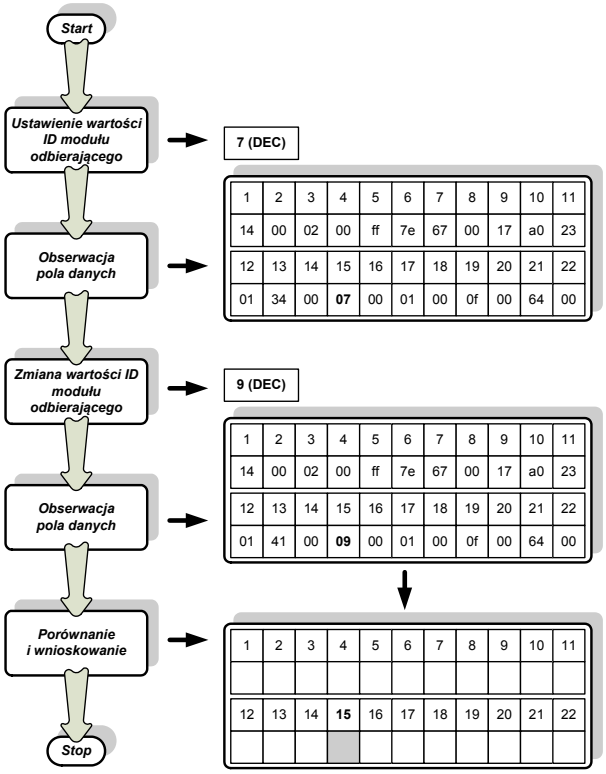
Uzyskana informacja o numerze bajtu pola danych, niosącego informację o wartości zmiennej procesowej jest dla intruza niekompletna. Dopełnieniem jest informacja o numerze ID modułu odbierającego, do którego kierowane są dane. Jak wspomniano wcześniej, każdy moduł odbierający ma odpowiednio nadany numer porządkowy. Jest to także identyfikator transmitowanej wartości zmiennej procesowej. Pozwala on na otrzymywanie wielu komunikatów z wartościami różnych zmiennych przez jeden interfejs komunikacyjny (o danym adresie IP) stacji procesowej oraz identyfikację i odpowiednie przyporządkowanie otrzymanych wartości zmiennych.

W celu uzyskania informacji o miejscu położenia, w polu danych, numeru ID zmiennej (modułu) wykonano następujące czynności (rysunek 5):

1. Ustawiono wartość zmiennej wysyłanej na 100 (DEC), wartość numeru ID na 7 (DEC).
2. Przechwycono dane i obserwowano miejsce pojawienia się w polu danych ustawionej wartości numeru ID (bajt nr 15).

3. Ustawiono wartość ID modułu na 9 (DEC).
4. Przechwycono dane i potwierdzono miejsce pojawienia się w polu danych ustawionej nowej wartości numeru ID (bajt nr 15).
5. Porównano odpowiedzi i sformułowano diagnozę dotyczącą numeru bajtu pola danych niosącego informację o numerze ID modułu odbierającego (15).

W wyniku wyżej opisanych i przeprowadzonych eksperymentów można potwierdzić pierwszą z wątpliwości, sformułowanych we wprowadzeniu, tzn., że w nieskomplikowany i nieuprawniony sposób można pozyskać informacje transmitowane w rozpatrywanym systemie, zaburzając tym samym poufność transmitowanych danych.



1	2	3	4	5	6	7	8	9	10	11
14	00	02	00	ff	7e	67	00	17	a0	23
12	13	14	15	16	17	18	19	20	21	22
01	34	00	**07**	00	01	00	0f	00	64	00

1	2	3	4	5	6	7	8	9	10	11
14	00	02	00	ff	7e	67	00	17	a0	23
12	13	14	15	16	17	18	19	20	21	22
01	41	00	**09**	00	01	00	0f	00	64	00

1	2	3	4	5	6	7	8	9	10	11
12	13	14	**15**	16	17	18	19	20	21	22

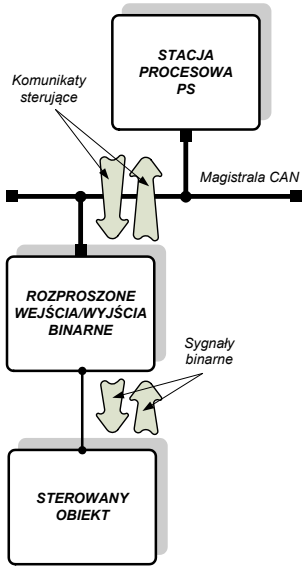
Rys.5. Analiza przesyłanych danych – pole ID modułu odbierającego

Diagnozowanie bezpieczeństwa transmisji pomiędzy modułami wejść/wyjść

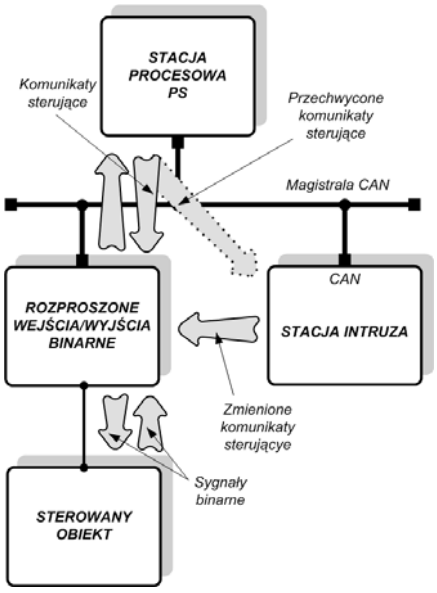
W poprzednich punktach omówiono diagnozowanie bezpieczeństwa komunikacji na poziomie procesowym pomiędzy stacjami procesowymi. Teraz zajmiemy się opisem procesu diagnozowania bezpieczeństwa transmisji na poziomie obiektowym (na poziomie komunikatów sterujących – por. rysunek 6). Stacja procesowa badanego systemu (rysunek 6) porozumiewa się poprzez magistralę komunikacyjną, w standardzie CAN, z zewnętrznymi modułami wejść/wyjść. Komunikacja pomiędzy stacją procesową a modułami wejść/wyjść odbywa się bez jakichkolwiek czynności przygotowawczych. System samodzielnie inicjuje, zarządza i dokonuje transakcji w protokole zbliżonym do CanOpen [12].

Stanowisko diagnozowania bezpieczeństwa komunikacji na poziomie obiektowym (rysunek 7) składa się ze stacji intruza z odpowiednio oprogramowaną kartą komunikacyjną CAN pozwalającą na:

- obserwację komunikatów sterujących transmitowanych do modułu wyjść binarnych;
- wygenerowanie komunikatu o podobnej, jak obserwowane komunikaty strukturze, różniącego się tylko polem danych.



Rys.6. Komunikacja pomiędzy stacją procesową a modułem wejść/wyjść



Rys.7. Ingerencja w komunikację z modułami wejść/wyjść

Rys.8. Sortownica – sortowanie prawidłowe

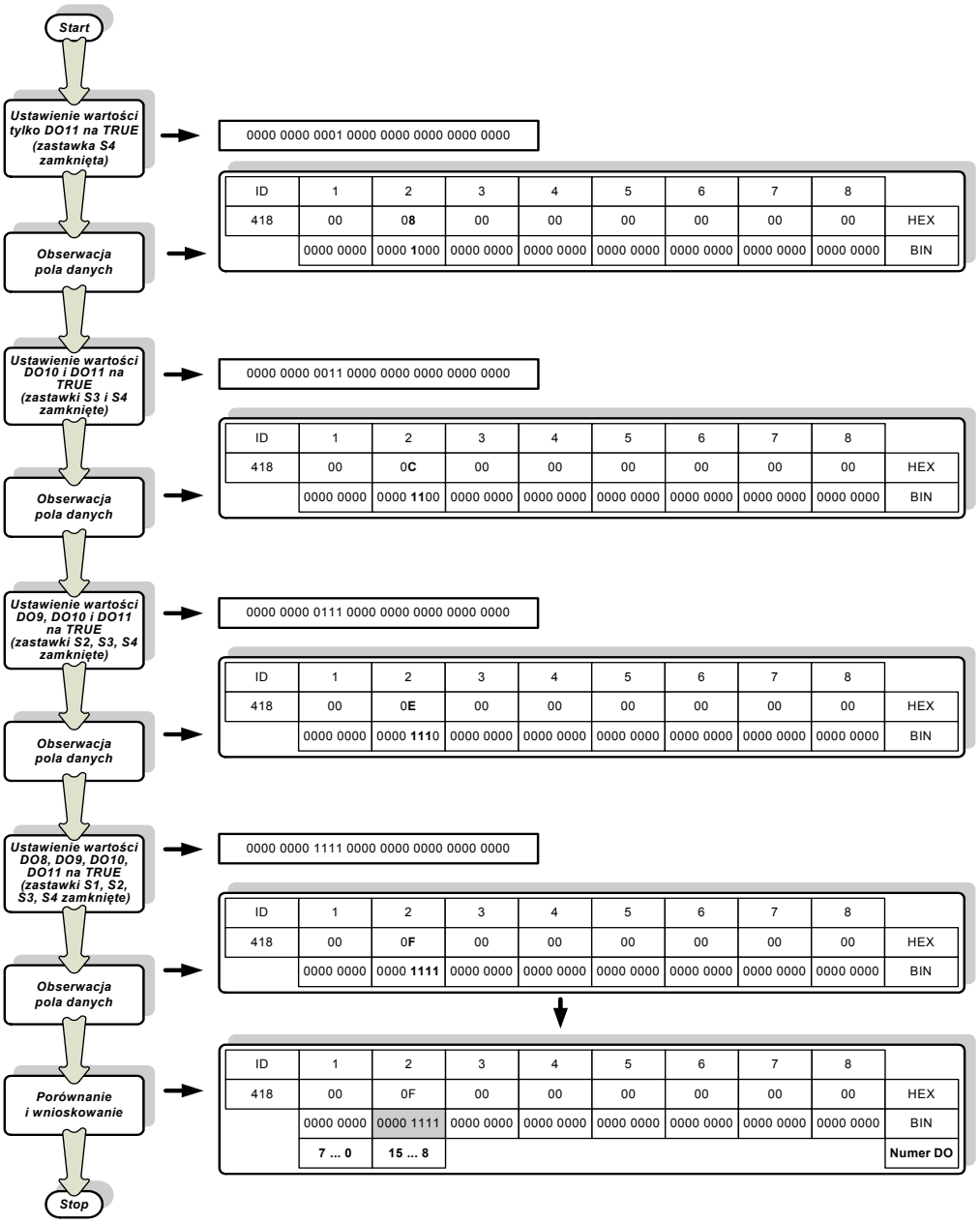
Przykładowym sterowanym obiektem jest sortownica różnobarwnych elementów [1, 13]. Obiekt służy, w tym przypadku odwrócony, do sortowania nagromadzonych w kanaliku dolotowym kulek do dwóch zbiorników (na białe i

czarne). Rysunek 8 przedstawia prawidłowo przebiegający proces sortowania, pożądany ze względów bezpieczeństwa. Za pomocą sygnału z czujnika koloru i czujnika przelatującej kulki, program sterowania stacji procesowej odpowiednio steruje wartościami wyjść binarnych zastawek:

- zastawka 4 – blokująca ruch kulek, otwierana tylko na kilka milisekund, w celu przepuszczenia jednej kulki;
- zastawka 3 – kierująca kulki do odpowiedniego zbiornika na podstawie odczytanego stanu czujnika koloru;
- zastawki 1 i 2 – dolotowe do zbiorników, permanentnie otwarte podczas niezakłóconego procesu sortowania.

Sygnały sterujące zastawkami są przyłączone, w strukturze sprzętowej stacji procesowej, do kanałów wyjść binarnych o numerach:

- zastawka 1 – kanał wyjściowy DO08;
- zastawka 2 – kanał wyjściowy DO09;
- zastawka 3 – kanał wyjściowy DO10;
- zastawka 4 – kanał wyjściowy DO11.



Rys.9. Rozpoznanie pola odpowiedzialnego za sterowanie kanałami wyjść binarnych 8-15

Uzyskanie informacji o miejscu położenia w ramce wartości zmiennych sterujących – przykład 3

Podobnie jak w poprzednich przykładach, nie jest znana a'priori struktura protokołu warstw wyższych, służącego do przesyłu wartości zmiennych procesowych.

Proces diagnozowania polega na:

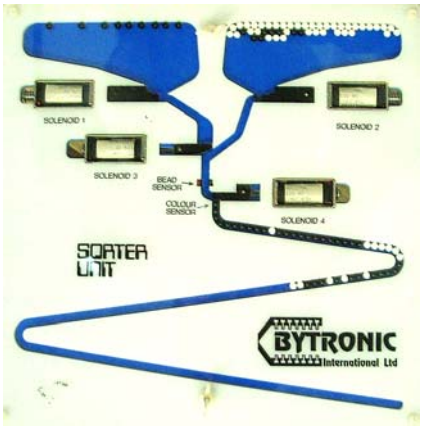
- zmianie (wymuszeniu wartości TRUE) z poziomu programu sterującego, stanu wyjść binarnych kolejno: DO11; DO10, DO11; DO9, DO10, DO11; D08, DO9, DO10, DO11
- obserwacji kolejnych pól danych, przed i po zmianie wartości zmiennej oraz wnioskowaniu dotyczącym miejsca w ramce, na którym jest transmitowana wartość. Informacja o miejscu położenia ww. wartości w polu danych zostanie wykorzystana do ingerencji w proces sterowania.

Celem eksperymentu było uzyskanie informacji o miejscach położenia w ramce wartości zmiennych sterujących procesem. Pożądaną informacją diagnostyczną są miejsca transmisji w ramce wartości sterujących zastawkami: S4 – blokującą kulki (kanał DO11), S3 - kierującą kulki do zbiorników (kanał DO10). S2, S1 - dolotowe do zbiorników (kanały odpowiednio DO9 i DO8). W celu ich uzyskania wykonano kolejne czynności (rysunek 9):

1. Ustawiono wartość wysyłanej zmiennej DO11 (zastawka S4) na TRUE (logiczna „1”).
2. Przechwycono dane i obserwowano miejsce pojawienia się w polu danych ustawionej wartości (por. rysunek 9 – pogrubione).
3. Ustawiono wartości wysyłanych zmiennych DO11 i DO10 (dodatkowo zastawka kierująca kulki S3) na TRUE (logiczna „1”).
4. Ponownie przechwycono dane i obserwowano miejsce pojawienia się w polu danych ustawionej nowej wartości (por. rysunek 9 – pogrubione w kolejnym kroku).
5. Ustawiono wartości wysyłanych zmiennych DO11, DO10, DO9 (dodatkowo zastawka dolotowa do zbiornika białych kulek S2) na TRUE (logiczna „1”).
6. Znowu przechwycono dane i obserwowano miejsce pojawienia się w polu danych ustawionej nowej wartości (por. rysunek 9 – pogrubione w kolejnym kroku).
7. Ustawiono wartości wysyłanych zmiennych DO11, DO10, DO9, DO8 (dodatkowo zastawka dolotowa do zbiornika czarnych kulek S1) na TRUE (logiczna „1”).
8. Kolejno przechwycono dane i obserwowano miejsce pojawienia się w polu danych ustawionej nowej wartości (por. rysunek 9 – pogrubione w kolejnym kroku).
9. Porównano odpowiedzi i sformułowano diagnozę dotyczącą miejsca położenia w ramce informacji odpowiadających poszczególnym kanałom wyjść binarnych DO1-15 (pogrubiona linia Kanały DO).

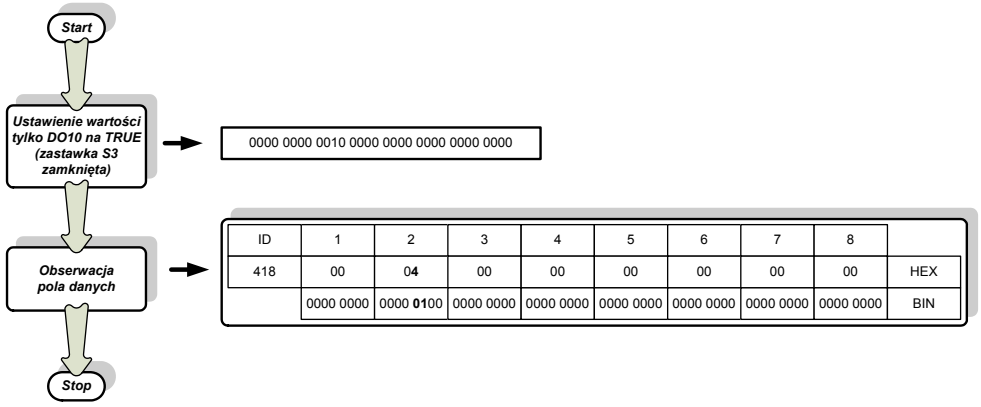
Wariant 1 wymuszenia stanu niebezpiecznego – przykład 4

Ingerencja w sterowany proces polegała na wygenerowaniu ramki z poziomu stacji intruza pozwalającej na zamknięcie zastawki sterującej S3 (kierującej) w chwili, gdy powinna ona być otwarta. Skutkiem takiego działania jest powstanie stanu niebezpiecznego, polegającego na błędnym sortowaniu (rysunek 10). Wysyłanie cykliczne specjalnie spreparowanego komunikatu na magistralę CAN z częstością większą od ustawionej w sterowniku, spowodowało powstanie zaburzenia procesu sterowania (rysunek 10).



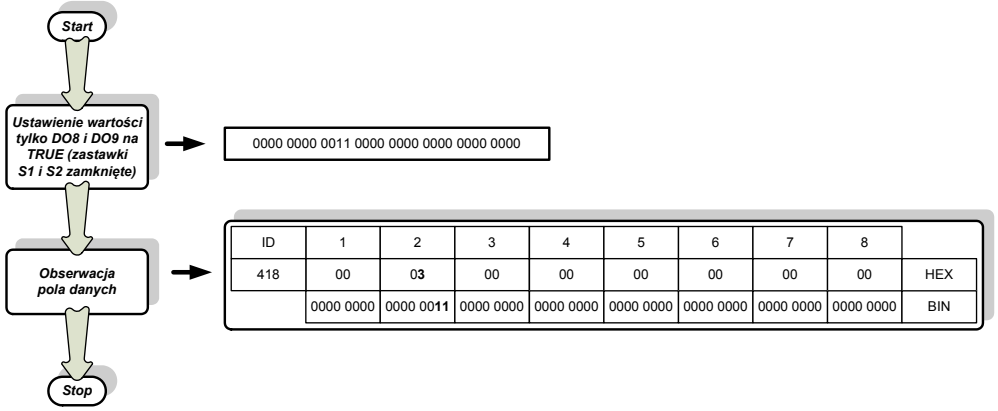
Rys.10. Sortownica – sortowanie błędne (zastawka kierująca)

Wygenerowany komunikat został przedstawiony na rysunku 11.



ID	1	2	3	4	5	6	7	8	
418	00	0**4**	00	00	00	00	00	00	HEX
	0000 0000	0000 **01**00	0000 0000	0000 0000	0000 0000	0000 0000	0000 0000	0000 0000	BIN

Rys.11. Wymuszenie zamknięcia zastawki kierującej S3



ID	1	2	3	4	5	6	7	8	
418	00	0**3**	00	00	00	00	00	00	HEX
	0000 0000	0000 00**11**	0000 0000	0000 0000	0000 0000	0000 0000	0000 0000	0000 0000	BIN

Rys.12. Wymuszenie zamknięcia zastawek S1 i S2 (dolotowych)

Wariant 2 wymuszenia stanu niebezpiecznego – przykład 5

W wariancie drugim ingerowano w sterowany proces podobnie. Ze stacji intruza cyklicznie, co kilka milisekund, na magistralę CAN był generowany komunikat zawierający „spreparowane" wartości zmiennych (ramkę pokazano na rysunku 12) wymuszających zamknięcie zastawek dolotowych do zbiorników S1 i S2. Pomimo, iż program sterujący prawidłowo sterował zastawką kierującą S3, zablokowane kanały dolotowe powodowały spiętrzenie elementów. W konsekwencji doprowadziło to do powstania niebezpiecznego stanu polegającego na blokadzie procesu sortowania (rysunek 13).

W wyniku przeprowadzonych eksperymentów (przykład 4 i 5), można odpowiedzieć twierdząco na wątpliwość drugą, postawioną we wprowadzeniu. Oznacza to, że można w pewien sposób zmienić wartości przesyłanych zmiennych procesowych, tym samym wprowadzając sterowany proces w stan niezdatności.

Rys.13. Sortownica – sortowanie błędne (zamknięte zastawki nad zbiornikami)

Podsumowanie

W artykule przedstawiono eksperymenty dotyczące dozorowania zmian przesyłanych danych pomiędzy:

- stacjami procesowymi rozproszonego systemu sterowania z wykorzystaniem boków komunikacyjnych umożliwiających transmisję wg protokołu TCP;
- sterownikiem przemysłowym i oddalonymi modułami wejść/wyjść obiektowych w standardzie magistrali CAN.

Dzięki diagnozie dotyczącej miejsca położenia danych transmitujących wartości zmiennych procesowych w ramce komunikatu, przeprowadzono kolejne eksperymenty polegające na ingerencji w przesyłaną informację, prowadzące do wywołania stanu niebezpiecznego w procesie sortowania elementów. Było to wymuszenie wartości przesyłanych zmiennych prowadzące do stanu:

- nieprawidłowego sortowania;
- blokady procesu sortowania.

Przedstawione eksperymenty dają twierdzącą odpowiedź na sformułowane we wstępie wątpliwości. W stosunkowo nieskomplikowany sposób można pozyskać informacje dotyczące jawnie przesyłanych wartości zmiennych procesowych. Podobnie, dla przypadku ingerencji w przesyłane dane, można dokonać niebezpiecznej ingerencji powodującej błędne wykonanie zadania użytkowego. A zatem: ważnymi działaniami wpływającymi na stan bezpieczeństwa komunikacji są następujące rozwiązania:

- zastosowanie odpowiednich modułów sprzętowych pozwalających na tunelowanie ruchu sieciowego [10];
- użycie procedur kontroli dostępu fizycznego do obiektu z zastosowaniem np. metod biometrycznych [14-16];
- wykorzystanie szyfrowania przesyłanych danych na poziomie stacji procesowych [17,18].

LITERATURA

[1] Bednarek M., Wizualizacja procesów. Laboratorium, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2004
[2]. Kwiecień A., Analiza przepływu informacji w komputerowych sieciach przemysłowych, Wydawnictwo Politechniki Śląskiej, Gliwice 2002
[3] Kwiecień A., Analiza przepływu informacji w komputerowych sieciach przemysłowych, Wydawnictwo Pracowni Jacka Skalmierskiego, 1999
[4] Haudahl S., Diagnozowanie i utrzymanie sieci. Księga eksperta, Helion, Gliwice 2001
[5] Bosch R., Sieci wymiany danych w pojazdach samochodowych, WKiŁ, Warszawa 2008
[6] Cyganik A., SIMATIC Safety Integrated, część 1, *Elektronika Praktyczna*, 4/2007, 138-140
[7] Cyganik A, SIMATIC Safety Integrated, część 2, *Elektronika Praktyczna*, 5/2007, 139-141
[8] Bezpieczeństwo funkcjonalne, Siemens Safety Tour, 09/2009
[9] Safety Integrated, Functional Examples, Siemens, March 2007
[10] Programowanie przez Internet: Konfiguracja modułów SCALANCE S 612 V2 do komunikacji z komputerem przez VPN, www.siemens.pl/simatic, 16/11/2007
[11] Szmit M., Gusta M., Tomaszewski M., 101 zabezpieczeń przed atakami w sieci komputerowej, Helion, Gliwice 2005
[12] www.can-cia.org
[13] Bytronic Educational Technology. Sorter Unit, Bytronic Ltd
[14] Wiśnios M., Dąbrowski T., Bednarek M., Credibility analysis of a multi-biometric identification system for fingerprints, *Problemy Eksploatacji*, nr 2/2013
[15] Wiśnios M., Dąbrowski T., Bednarek M., Badania weryfikacyjne metody rozpoznawania twarzy, *Biuletyn Wojskowej Akademii Technicznej*, nr 4/2013, 205-218
[16] Ślot K., Wybrane zagadnienia biometrii, Wydawnictwa Komunikacji i Łączności, Warszawa 2008
[17] Bednarek M., Dąbrowski T., Koncepcja zabezpieczenia transmisji danych w mobilnym systemie diagnostycznym, *Journal Of KONBiN*, z.2(26)/2013, 61-70
[18] Bednarek M., Dąbrowski T., Wiśnios M.: Bezpieczeństwo komunikacji w rozproszonym systemie sterowania, *Przegląd Elektrotechniczny*, nr 9/2013, 72-74
[19] Dąbrowski T., Bednarek M., Fokow K., Wiśnios M.: The method of threshold-comparative diagnosing insensitive on disturbances of diagnostic signals, Przegląd Elektrotechniczny - Electrical Review, vol.88, issue: 11A, 2012. pp. 93-97

***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, mgr inż. Michał Wiśnios, Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Systemów Elektronicznych, ul. Kaliskiego 2, 00-908 Warszawa; E-mail: tdabrowski@wat.edu.pl, michal.wisnios@wat.edu.*