Marcin BEDNAREK[1], Tadeusz DĄBROWSKI[2]

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

doi:10.15199/48.2015.11.51

Układ dozorująco-terapeutyczny wymiany kluczy w systemie transmisji danych procesowych

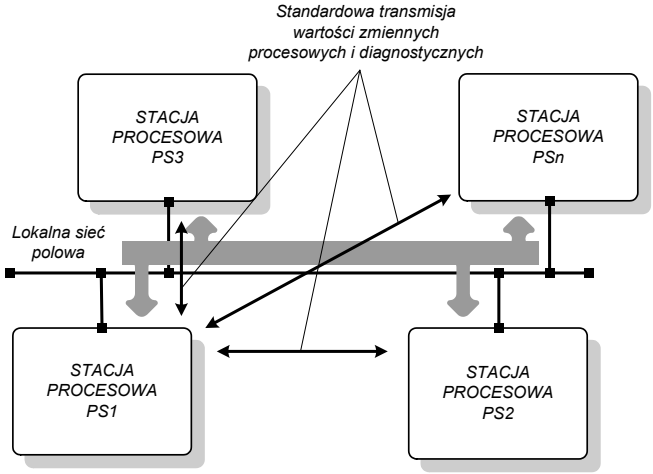
Streszczenie. *W rozpatrywanym, rozproszonym systemie sterowania komunikacja odbywa się na poziomie procesowym - łączącym stacje procesowe przy pomocy protokołu TCP/IP (Ethernet). Transmisja danych procesowych jest zabezpieczona programowo. Elementami zabezpieczającymi są: uwierzytelnianie, przesył kluczy asymetrycznych, przesył kluczy symetrycznych, właściwa - zabezpieczona transmisja danych procesowych. W artykule przedstawiono sposób działania układu dozorująco-terapeutycznego odpowiedzialnego za etap związany z wymianą kluczy szyfrujących pomiędzy stacjami procesowymi i przygotowaniem stacji do transmisji danych procesowych.*

Abstract*. In the discussed distributed control system communication carried out at process level - linking process stations using TCP/IP (Ethernet). Process data transmission is software protected. Authentication, transmission of asymmetric keys, symmetric keys transmission, secure data transmission process are security features. The article presents behavior of the supervising and therapeutic system responsible for the step associated with the exchange of encryption keys between process stations and station preparation for data transmission process. (**Supervising and therapeutic system of the key exchange in process data transmission system**).*

Słowa kluczowe: rozproszony system sterowania, bezpieczeństwo, komunikacja, sieć przemysłowa, układ dozorująco-terapeutyczny.
Keywords: distributed control system, security, communication, fieldbus, supervising and therapeutic system.

Wstęp

Problem poruszany w opracowaniu dotyczy przedstawienia wariantów działania układu dozorująco-terapeutycznego (UDT) systemu wymiany kluczy szyfrujących w rozproszonym systemie sterowania. W skład takiego systemu wchodzą stacje procesowe (ang. *PS – Process Station*), czyli sterowniki przemysłowe, sterujące procesami (rys. 1); stacje operatorskie (ang. *OS – Operator Station*) realizujące wizualizację i oddziaływania operatorskie oraz stacje inżynierskie (ang. *ES - Engineering Station* [1]), z poziomu których przeprowadza się konfigurację i uruchomienie systemu sterowania. Rysunek 1 przedstawia standardowy system transmisji danych w rozproszonym systemie sterowania złożonym tylko ze stacji procesowych. Dla uproszczenia na rysunku pominięto pozostałe elementy tj. stacje operatorskie i inżynierską.



Rys.1. Standardowa transmisja danych pomiędzy stacjami procesowymi rozproszonego systemu sterowania

W rozpatrywanym systemie (rys. 1) komunikacja odbywa się na poziomie procesowym, wykorzystującym standard Ethernet [2], łączącym stacje procesowe przy pomocy protokołu TCP/IP. Do transmisji danych pomiędzy stacjami procesowymi system sterowania oferuje standardowe bloki komunikacyjne umożliwiające jawny przesył danej określonego typu. Nie ma możliwości zastosowania mechanizmów szyfrowania używanych powszechnie w transmisji opartej na rodzinie protokołów TCP/IP. Nie pozwala na to zamknięty charakter sposobu komunikowania się zastosowany przez producenta systemu. Standardowo, bez zastosowania opisanych w artykule rozwiązań, transmisja nie jest w żaden sposób zabezpieczona, co stwarza podatność na ataki naruszające integralność lub poufność przesyłanych danych [3, 4]. W celu zapewnienia bezpiecznej transmisji danych procesowych i diagnostycznych pomiędzy stacjami systemu zastosowano szyfrowaną transmisję danych, szerzej opisaną w [5-7]. Zakłada się, iż transmisja prowadzona jest wg standardowych, firmowych protokołów komunikacyjnych producenta sprzętu oraz z wykorzystaniem standardowych bloków komunikacyjnych implementowanych w języku FBD (*ang. Function Block Diagram*) sterownika przemysłowego. Troska o zabezpieczenie danych spoczywa na inżynierze, odpowiednio dobierającym zaawansowanie implementowanych mechanizmów zabezpieczających. W rozpatrywanym systemie zostały zastosowane mechanizmy szyfrowania asymetrycznego oraz symetrycznego. Nad poprawnością wymiany zabezpieczonych danych czuwają układy dozorująco-terapeutyczne (UDT) sterujące kolejnymi etapami procesu. Należy podkreślić, że w założeniu (i w praktyce omawianego systemu) nie ma możliwości skorzystania ze standardowych sposobów zabezpieczenia transmisji, takich jak np. tunelowanie ruchu sieciowego czy też wymuszenie szyfrowania z użyciem protokołu SSL. W tego typu systemie sterowania nie ma, w standardowym repertuarze ustawień, możliwości włączenia opcji szyfrowania, czy też wymuszenia zastosowania do komunikacji rozwiązań oferowanych przez protokoły z rodziny TCP/IP. Wszystkie zastosowane i opisane tu mechanizmy zabezpieczające wykorzystują opisane dalej warianty pracy przesyłając dane szyfrowane „zapakowane" do wartości zmiennych procesowych określonego typu za pomocą bloków komunikacyjnych sterownika (stacji procesowej). Proces zabezpieczania transmisji przed podsłuchem czy też ingerencją odbywa się zatem na etapie przygotowania danych do wysyłki, jeszcze w zadaniu użytkownika wykonywanym przez sterownik równolegle z zadaniem realizującym algorytm sterowania procesem.

Układ dozorująco-terapeutyczny wymiany kluczy

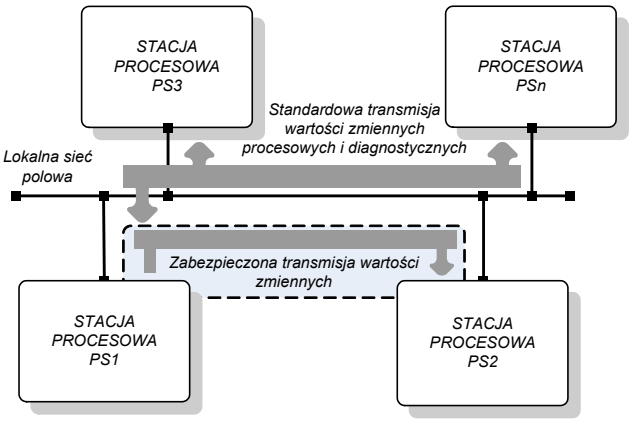
Na rysunku 2 przedstawiono schematycznie komunikację pomiędzy dwiema stacjami procesowymi

rozproszonego systemu sterowania (PS1 i PS2). Komunikacja odbywa się za pomocą protokołu TCP/IP, wykorzystując technologię Ethernet. Stacje wymieniają wzajemnie komunikaty z zastosowaniem standardowych interfejsów komunikacyjnych. Konfiguracja takiego połączenia polega na ustawieniu interfejsu sieciowego, numeru portu komunikacyjnego, doboru identyfikatora nadawanej zmiennej. Skonfigurować należy także odpowiednio blok nadawczy w stacji PS1 oraz odbiorczy w stacji PS2. Dodatkowo zmienne gotowe do wysłania do PS2 są poddawane procesowi szyfrowania w programie zadania użytkownika sterownika i umieszczane w standardowej zmiennej określonego typu wysyłanej przez bloki komunikacyjne nie dające możliwości standardowego szyfrowania. System zabezpieczonej transmisji korzysta z 3 rodzajów kanałów komunikacyjnych (kanały komunikacyjne tworzą z punktu widzenia programu sterownika sparowane ze sobą bloki nadawczo-odbiorcze na diagramach stacji PS1 i PS2 w języku FBD):

- *Kanału sterującego*, za pomocą którego przesyłane są komunikaty sterujące procesem transmisji. Dzięki niemu układy dozorująco-terapeutyczne stacji mają możliwość wzajemnego informowania się o kolejnych etapach procesu zabezpieczonej transmisji.
- *Kanału wymiany kluczy*, którym przesyłane są informacje o kluczach szyfrujących.
- *Kanału wymiany danych*, dzięki któremu odbywa się szyfrowana transmisja danych procesowych i diagnostycznych.

W zależności od potrzeb, liczba kanałów wymiany danych może być zwielokrotniona, zgodnie z wymaganą liczbą przesyłanych zmiennych diagnostycznych. Każdej zmiennej procesowej lub diagnostycznej powinien odpowiadać unikalny kanał wymiany danych.

Właściwa komunikacja jest zabezpieczona algorytmem kryptograficznym symetrycznym [8]. Oznacza to wykorzystanie identycznego klucza szyfrującego po obydwu stronach kanału wymiany danych. Korzystanie przez układy dozorująco-terapeutyczne stacji PS1 i PS2 z identycznego klucza szyfrującego stwarza problem z jego dystrybucją. Należy bowiem tak przekazać klucz z jednej strony kanału transmisyjnego na drugą aby zachować poufność danych.

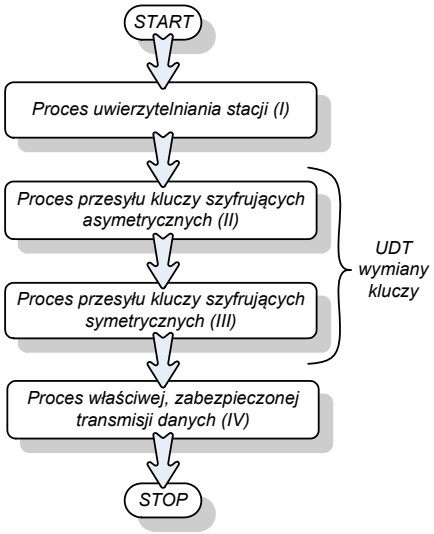


Rys.2. Zabezpieczona transmisja danych procesowych pomiędzy stacjami PS1 i PS2

M.in. z tego powodu układy dozorująco-terapeutyczne przesyłu kluczy wpisują się swoim działaniem w 4 etapowy proces przesyłu danych procesowych (rys 3). Etapami tymi są:

- proces uwierzytelniania stacji (I);
- proces przesyłu kluczy szyfrujących asymetrycznych (II);
- proces przesyłu kluczy szyfrujących symetrycznych (III);
- proces właściwej, zabezpieczonej transmisji danych (IV).

Niniejsze opracowanie, ze względu na ograniczoną objętość, nie poświęca uwagi równie ważnemu, także implementowanemu przez autorów w rozpatrywanym systemie, procesowi uwierzytelniania stacji (I), zmniejszającemu podatność na ataki MITM (ang. *Man In The Middle* [3]. Proces uwierzytelniania stacji w omawianym systemie ze względu na złożoność i objętość, jest przedmiotem przygotowywanego, odrębnego opracowania.



Rys.3. Ilustracja etapów procesu przesyłania danych

Zadaniem układu dozorująco-terapeutycznego wymiany kluczy zlokalizowanego w komunikujących się stacjach procesowych jest „czuwanie" nad prawidłowym przebiegiem podprocesów (II) i (III) odpowiedzialnych za wymianę kluczy (rys. 3). Najpierw strony wymieniają pomiędzy sobą klucze publiczne (jawne), a następnie tajny klucz transakcji przesyłają z wykorzystaniem kryptografii asymetrycznej. Tak dostarczony tajny klucz symetryczny umożliwia rozpoczęcie właściwej zabezpieczonej wymiany danych procesowych. W kolejnych punktach opracowania przedstawione są warianty rozwiązania układów dozorująco-terapeutycznych wymiany kluczy podprocesów (II) i (III) w ujęciu eksploatacyjnym (zaznaczone klamrą na rysunku 3).

Warianty układu dozorująco-terapeutycznego przesyłu kluczy szyfrujących

Elementy układu dozorująco-terapeutycznego (UDT) wymiany kluczy w systemie transmisji danych procesowych są rozmieszczone w programach sterujących komunikujących się stacji procesowych. Ich zadaniem jest dozorowanie procesu transmisji kluczy oraz właściwe sterowanie kolejnymi etapami procesu wymiany kluczy. UDT wymiany kluczy jest wykonany w pięciu wariantach (tab. 1).

Tabela 1. Układ dozorująco-terapeutyczny wymiany kluczy - warianty

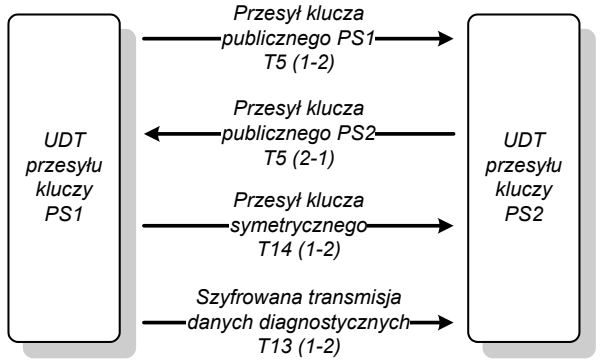
Wariant nr	Nazwa - oznaczenie
Wariant 1.	Uproszczony układ dozorująco-terapeutyczny
Wariant 2.	Podstawowy układ dozorująco-terapeutyczny
Wariant 3.	Standardowy układ dozorująco-terapeutyczny
Wariant 4.	Uzupełniony układ dozorująco-terapeutyczny
Wariant 5.	Rozszerzony układ dozorująco-terapeutyczny

Zadaniem każdego z wariantów układu dozorująco-terapeutycznego przesyłu kluczy jest odpowiednie sterowanie procesem wymiany kluczy. W kolejnych modyfikacjach układu inaczej rozwiązane jest m.in. potwierdzanie dostarczenia kluczy drugiej stronie.

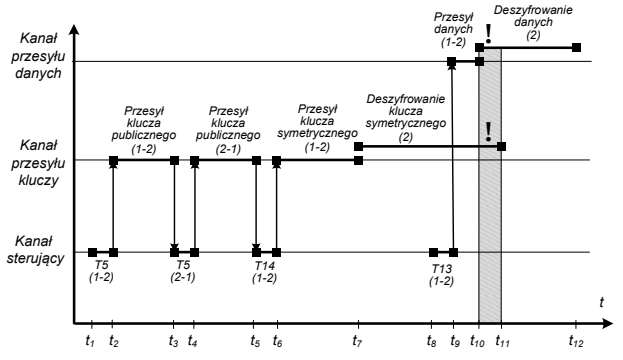
Układ dozorująco-terapeutyczny przesyłu kluczy szyfrujących - wariant 1.

Stany eksploatacyjne i funkcjonowanie układu w wariancie 1 przedstawiono na rysunkach 4 i 5:

1. Układ dozorująco-terapeutyczny stacji PS1 wysyła komunikat sterujący T5 ($t_1;t_2$) informujący PS2 o rozpoczęciu transmisji klucza asymetrycznego [9] i wysyła klucz publiczny stacji PS1 do stacji PS2 ($t_2;t_3$).
2. Zwrotnie układ dozorująco-terapeutyczny stacji PS2 nadaje komunikat sterujący T5 ($t_3;t_4$) informujący PS1 o rozpoczęciu transmisji klucza asymetrycznego i wysyła klucz publiczny stacji PS2 do stacji PS1 ($t_4;t_5$).
3. Układ dozorująco-terapeutyczny PS1 przesyła komunikat sterujący T14 ($t_5;t_6$) i klucz symetryczny ($t_6;t_7$).
4. Po odczekaniu pewnego czasu (3-4 cykli przetwarzania zadania sterownika, ($t_7;t_8$)) następuje wystawienie komunikatu sterującego T13 przez PS1 ($t_8;t_9$) i przełączenie na transmisję szyfrowaną z użyciem klucza symetrycznego.
5. Układ dozorująco-terapeutyczny stacji PS1 transmituje komunikat z danymi procesowymi ($t_9;t_{10}$) i rozpoczyna się właściwa zabezpieczona transmisja danych procesowych z PS1 do PS2.



Rys.4. Schematyczne przedstawienie działania UDT przesyłu kluczy w wariancie 1.



Rys.5. Grafik stanów eksploatacyjnych systemu transmisji kluczy w wariancie 1.

Do przedstawienia szczegółowego przebiegu sterowania procesem wymiany kluczy przyjęto przebywanie układu dozorująco-terapeutycznego w trzech stanach eksploatacyjnych:

- wykorzystanie kanału sterującego (oznaczenie na rysunkach 5, 7, 9, 11 i 13: *Kanał sterujący*);
- użycie kanału przesyłu kluczy (oznaczenie na rysunkach 5, 7, 9, 11 i 13: *Kanał przesyłu kluczy*);
- przesył danych kanałem transmisji danych (oznaczenie na rysunkach 5, 7, 9, 11 i 13: *Kanał przesyłu danych*).

Rysunek 5 przedstawia schematycznie wykorzystanie kanałów transmisyjnych przez układ dozorująco-terapeutyczny. Wyróżnione są na nim trzy stany, w których może znajdować się układ transmisji kluczy. Poziomymi odcinkami zaznaczono przebywanie układu transmisji w jednym ze stanów: wysyłanie komunikatu sterującego, wysyłanie kluczy, przesył danych. Dodatkowo na wykresie z rysunku 5 oraz 7, 9, 11 i 13 - poza liniami oznaczającymi przebywanie systemu transmisji w określonym stanie - są umieszczone odcinki nie związane bezpośrednio z transmisją. Są to odcinki symbolizujące czas potrzebny na przetwarzanie otrzymanej informacji. W nawiasach umieszczono numeryczne informacje dotyczące kierunku przepływu komunikatów wg zasady nadawca-odbiorca. Np. przesył danych z PS1 do PS2 oznaczono symbolem (*1-2*).

Zaletą wersji uproszczonej układu dozorująco-terapeutycznego wymiany kluczy jest jego mały stopień skomplikowania. To z kolei wpływa na dużą szybkość, dzięki niewielu wymianom danych na etapie przygotowawczym do właściwej transmisji. Wadą jest natomiast brak kontroli układu stacji PS1 nad chwilą rozpoczęcia transmisji zabezpieczonej. Układ dozorująco-terapeutyczny stacji PS1 może w przypadku wystąpienia chwilowej niezdatności stacji PS1, a tym samym - wydłużenia czasu dekodowania przesłanego klucza wysłać dane zbyt wcześnie. Zaznaczono to na rysunku 5 zakreskowanym polem ($t_{10};t_{11}$). W takim przypadku układ dozorująco-terapeutyczny stacji PS2 rozpoczął by deszyfrowanie nadchodzących danych z użyciem niewłaściwej, tymczasowej wartości klucza, przed zakończeniem jego deszyfracji ($t_{11};t_{12}$). Należy liczyć się zatem z otrzymaniem w PS2 kilku pierwszych wartości zmiennych procesowych deszyfrowanych niewłaściwym kluczem, pobranym ze zmiennej przed zakończeniem jego „wyłuskiwania". Można temu zapobiec wydłużając czas zwłoki stacji PS1 ($t_7;t_8$) lub stosując układ dozorująco-terapeutyczny w wariancie 2. (podstawowym).

Układ dozorująco-terapeutyczny przesyłu kluczy szyfrujących - wariant 2.

Podstawowy układ dozorująco-terapeutyczny działa podobnie do opisanego wariantu 1. Z tą jednak różnicą, iż stacja inicjująca połączenie (PS1) otrzymuje potwierdzenie kodem T14 przesyłanym kanałem sterującym informujące o odebraniu klucza symetrycznego. Działanie podstawowego algorytmu układu jest następujące (rys. 6):

1. Układ dozorująco-terapeutyczny stacji PS1 wysyła komunikat sterujący T5 ($t_1;t_2$) informujący PS2 o rozpoczęciu transmisji klucza asymetrycznego i wysyła klucz publiczny stacji PS1 do stacji PS2 ($t_2;t_3$).
2. Zwrotnie układ dozorująco-terapeutyczny stacji PS2 nadaje komunikat sterujący T5 ($t_3;t_4$) informujący PS1 o rozpoczęciu transmisji klucza asymetrycznego i wysyła klucz publiczny stacji PS2 do stacji PS1 ($t_4;t_5$).
3. Układ dozorująco-terapeutyczny PS1 przesyła komunikat sterujący T14 ($t_5;t_6$) oraz w kolejnym kroku klucz symetryczny ($t_6;t_7$).

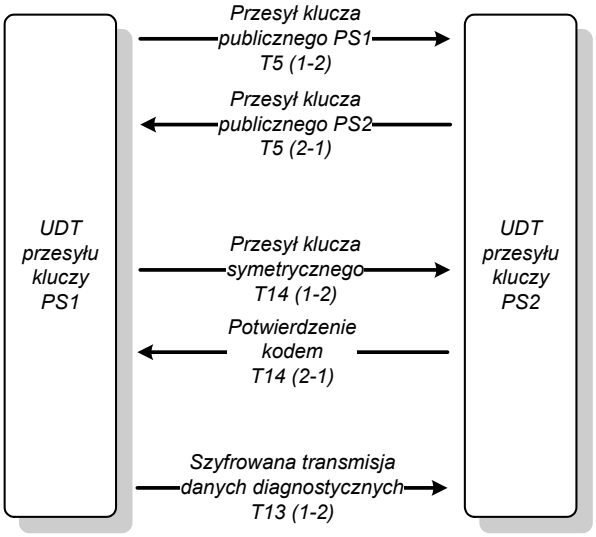
Od chwili t_7 są możliwe dwa scenariusze działania układu, w zależności od wybranego podprogramu.

W pierwszym z nich (rys. 7a):

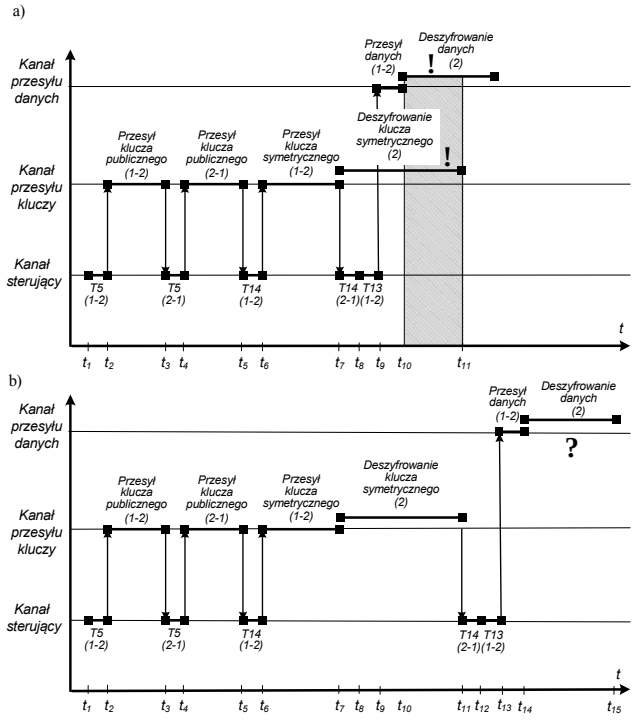
4a. Stacja PS2 potwierdza niezwłocznie otrzymanie klucza symetrycznego komunikatem sterującym T14 ($t_7;t_8$).

W drugim ze scenariuszy (rys. 7b):

4b. Potwierdzenie T14 jest wysyłane kanałem sterującym ($t_{11};t_{12}$) dopiero po zakończeniu procesu deszyfrowania, trwającego przez okres ($t_7;t_{11}$).



Rys.6. Schematyczne przedstawienie działania UDT przesyłu kluczy w wariancie 2.



Rys.7. Grafik stanów eksploatacyjnych systemu transmisji kluczy w wariancie 2.: a) z niedomiarem czasu; b) z rezerwą czasową

Od chwili t_8 (scenariusz 1, rys. 7a) lub od chwili t_{12} (scenariusz 2, rys. 7b) transmisja przebiega ponownie według podobnego scenariusza:

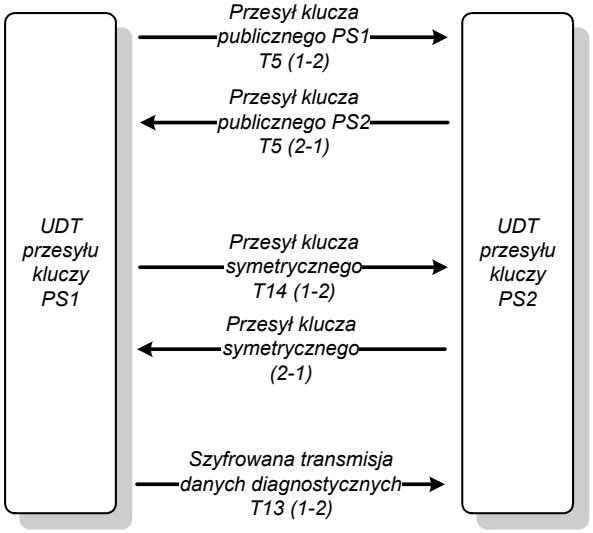
5. Następuje wystawienie komunikatu sterującego T13 przez PS1 (wg scenariusza 1 w czasie ($t_8;t_9$) lub wg scenariusza 2 w czasie ($t_{12};t_{13}$)) i przełączenie na transmisję szyfrowaną z użyciem klucza symetrycznego.
6. Układ dozorująco-terapeutyczny stacji PS1 transmituje komunikat z danymi procesowymi (wg scenariusza 1 w czasie ($t_9;t_{10}$) lub wg scenariusza 2 w czasie ($t_{13};t_{14}$)) i rozpoczyna się właściwa zabezpieczona transmisja danych procesowych z PS1 do PS2.

W obydwu przypadkach przedstawionych na rysunku 7 stacja PS1 otrzymuje od stacji PS2 potwierdzenie otrzymania klucza symetrycznego. Jest to istotną zaletą, ponieważ inicjator połączenia – stacja PS1 dysponuje potwierdzeniem odebrania klucza sesji. Istotnym problemem w scenariuszu pierwszym (rys 7a) jest rozpoczęcie procesu deszyfrowania otrzymanej wartości przed zakończeniem obliczeń PS2 nad kluczem szyfrującym ($t_{10};t_{11}$). Obszar zaznaczono na rysunku 7a obszarem zakreskowanym.

Scenariusz drugi eliminuje tę niedogodność. Proces przesyłu ($t_{13};t_{14}$) i deszyfrowania ($t_{14};t_{15}$) danych procesowych rozpoczyna się po zakończeniu obliczeń i uzyskaniu przez PS2 klucza symetrycznego. Układ dozorująco-terapeutyczny stacji PS1 nie ma jednak potwierdzenia czy PS2 przeprowadziła proces deszyfrowania danych poprawnie obliczonym kluczem. Nie ma zatem także pewności, czy stacja PS2 przetwarza wiarygodną wartość zmiennej procesowej. Eliminuje to wariant 3. wykonania układu dozorująco-terapeutycznego.

Układ dozorująco-terapeutyczny przesyłu kluczy szyfrujących - wariant 3.

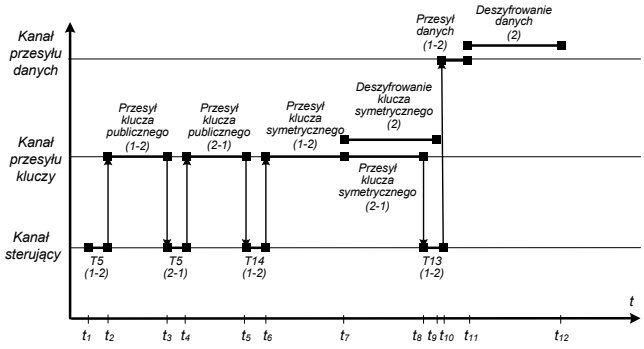
W wariancie standardowym wprowadzono zwrotny przesył przez układ dozorująco-terapeutyczny PS2 otrzymanego klucza symetrycznego (rys. 8). Oznaczone jest to odcinkiem ($t_7;t_8$) na rysunku 9. Dzięki temu została wyeliminowana niepewność PS1 co do poprawności otrzymania klucza przez PS2. Stacja PS2 po odebraniu odsyła klucz w identycznej postaci. Dzięki temu cały proces potwierdzenia przebiega bez zbędnych opóźnień spowodowanych obliczeniami matematycznymi na otrzymanych wartościach klucza.



Rys.8. Schematyczne przedstawienie działania UDT przesyłu kluczy w wariancie 3.

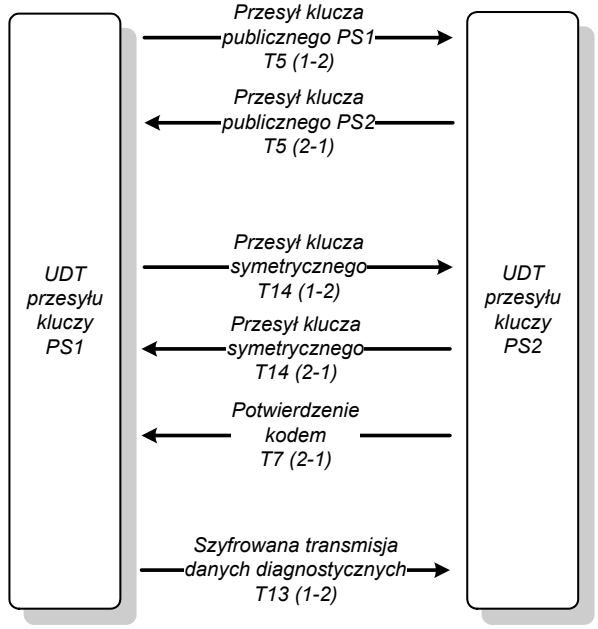
Zarówno przesyłany klucz symetryczny z PS1 do PS2 (służący do szyfrowania i deszyfrowania późniejszych cyklicznych wymian danych procesowych), jak i potwierdzenie, jest szyfrowane kluczem publicznym stacji PS2. Komparator układu dozorująco-terapeutycznego stacji PS1 może stwierdzić jedynie, iż odesłany komunikat ze stacji PS2 jest tożsamy z wysłanym. Istotną zaletą jest szybkość procesu weryfikacji dostarczenia klucza symetrycznego. Za wadę takiego rozwiązania można uznać brak informacji zwrotnej o deszyfrowaniu przez PS2 klucza. Układ dozorująco-terapeutyczny w kolejnym wariancie –

uzupełnionym - może generować dodatkowe potwierdzenia eliminujące tę niedogodność.

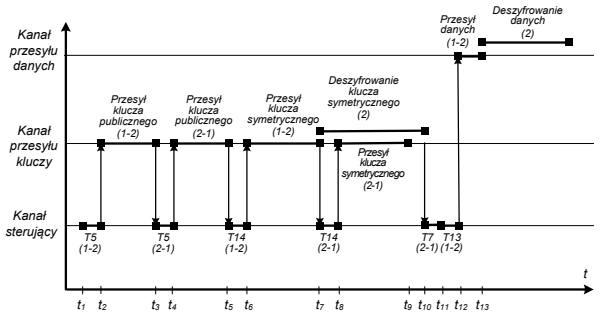


Rys.9. Grafik stanów eksploatacyjnych systemu transmisji kluczy w wariancie 3.

Układ dozorująco-terapeutyczny przesyłu kluczy szyfrujących - wariant 4.



Rys.10. Schematyczne przedstawienie działania UDT przesyłu kluczy w wariancie 4.



Rys.11. Grafik stanów eksploatacyjnych systemu transmisji kluczy w wariancie 4.

W wariancie uzupełnionym układ dozorująco-terapeutyczny generuje dwa niezależne potwierdzenia otrzymania przez PS2 klucza symetrycznego (rys. 10):

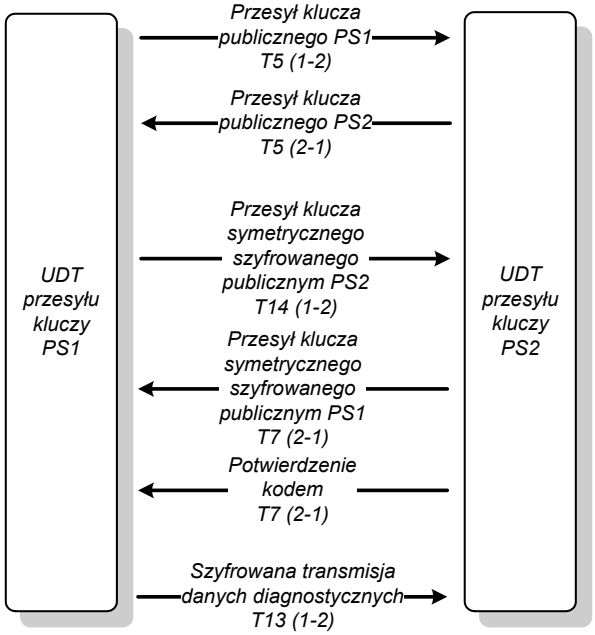
- Pierwsze potwierdzenie jest podobne do opisanego wyżej wariantu 3. Jest to zwrotny przesył otrzymanego komunikatu. Ilustruje to rysunek 11. Na odcinku ($t_7;t_8$) PS2 wystawia komunikat sterujący T14 i przesyła zwrotnie otrzymany klucz w identycznej formie, jak otrzymana ($t_8;t_9$).
- Drugie potwierdzenie następuje w chwili zakończenia deszyfrowania przez PS2 klucza symetrycznego (t_{10}).

Dzięki dwukrotnemu potwierdzeniu układ dozorująco-terapeutczny stacji PS1 jest informowany o zakończeniu kolejnych etapów procesu przesyłu klucza sesji – zakończenia jego odbioru i zakończenia deszyfrowania. Wyeliminowana jest zatem niepewność UDT stacji PS1 w odniesieniu do chwili zakończenia deszyfrowania klucza przez PS2.

Układ dozorująco-terapeutyczny przesyłu kluczy szyfrujących - wariant 5.

Proces użytkowania układu w wersji rozszerzonej (rys. 12) jest podobny do opisanego dla wariantu 1. (uproszczonego) i 2. (podstawowego) na odcinku ($t_1;t_7$). Kolejnymi krokami są (rys.13):

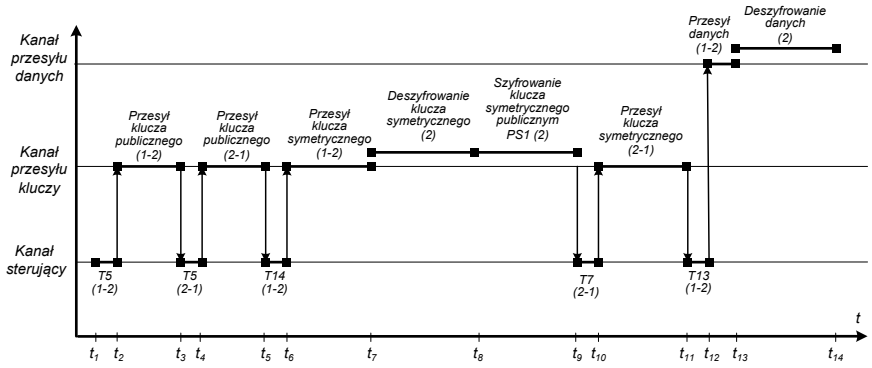
- deszyfrowanie otrzymanego od PS1 klucza symetrycznego kluczem prywatnym PS2 ($t_7;t_8$);
- szyfrowanie otrzymanego klucza dotychczas nieużywanym, wcześniej przesłanym, kluczem publicznym stacji PS1 ($t_8;t_9$);
- wystawienie komunikatu potwierdzającego T7 ($t_9;t_{10}$) i przesył zaszyfrowanego asymetrycznie kluczem PS1 klucza symetrycznego ($t_{10};t_{11}$)
- rozpoczęcie transmisji szyfrowanej kluczem symetrycznym (od chwili t_{12}).



Rys.12. Schematyczne przedstawienie działania UDT przesyłu kluczy w wariancie 5.

Układ dozorująco-terapeutyczny przesyłu kluczy w wariancie rozszerzonym pozwala na pełne dozorowanie procesu wymiany kluczy szyfrujących. Układ dozorująco-terapeutyczny inicjatora połączenia PS1 jest w stanie kontrolować przebieg procesu otrzymując (lub nie - w stanie niezdatności systemu wymiany kluczy) odpowiednie komunikaty kanałem sterującym i kanałem wymiany kluczy. Precyzyjność działania uzyskana jest niestety kosztem kilkukrotnego wydłużenia czasu procesu przygotowawczego, niezbędnego do właściwej transmisji zabezpieczonych danych pomiędzy stacjami. Otrzymuje się jednak pewność, że klucz symetryczny, wykorzystywany do dalszej komunikacji dotarł do PS2 w niezmienionej postaci (integralność), został poprawnie zdekodowany, zakończył

się proces jego deszyfrowania i stacja PS2 jest gotowa na otrzymywanie właściwych komunikatów z danymi procesowymi.



Rys.13. Grafik stanów eksploatacyjnych systemu transmisji kluczy w wariancie 5.

Podsumowanie

W artykule przedstawiono pięć wariantów wykonania układu dozorująco-terapeutycznego przesyłu kluczy w zabezpieczonym procesie przesyłania danych procesowych. Należy podkreślić, iż przedstawione - w ujęciu eksploatacyjnym - opisy algorytmów UDT przesyłu kluczy nie wykorzystują standardowych mechanizmów zabezpieczenia transmisji oferowanych w sieciach opartych na TCP/IP. Funkcjonalność taka nie jest bowiem dostępna dla inżyniera projektującego i konfigurującego system sterowania. Wszystkie z przedstawionych wariantów są realizowane jako zadania użytkownika (ang. *User Task*). Wraz z implementacją w sterowniku przemysłowym coraz wyższej wersji UDT uwidaczniają się dwie tendencje:

- zwiększa się stopień skomplikowania UDT, co skutkuje wydłużeniem oczekiwania na właściwą transmisję danych procesowych;
- zwiększa się precyzja działania UDT oraz dokładność dozorowania, co wpływa na większą wiarygodność otrzymywanych danych procesowych.

LITERATURA

[1] Bednarek M., Wizualizacja procesów. Laboratorium, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2004

[2] Haudahl S., Diagnozowanie i utrzymanie sieci. Księga eksperta, Helion, Gliwice 2001

[3] Alcorn W., Frichot C., Orru M.:The Browser Hacker Handbook's, John Willey&Sons, Indianapolis 2014

[4] Bednarek M., Dąbrowski T., Wiśnios M.: Bezpieczeństwo komunikacji w rozproszonym systemie sterowania, Przegląd Elektrotechniczny, nr 9/2013, 72-74

[5] Bednarek M., Dąbrowski T., Koncepcja zabezpieczenia transmisji danych w mobilnym systemie diagnostycznym, *Journal Of KONBiN*, z.2(26)/2013, 61-70

[6] Bednarek M., Dąbrowski T.: Koncepcja bezpiecznej transmisji danych w mobilnym systemie rozproszonym, Prace Naukowe Politechniki Warszawskiej „Bezpieczeństwo i analiza ryzyka w transporcie", seria Transport, zeszyt 96/2013, 69-76

[7] Bednarek M., Dąbrowski T., Wiśnios M.: Koncepcja zabezpieczenia transmisji pomiędzy stacjami diagnostycznymi, Pomiary Automatyka Kontrola, Wydawnictwo PAK, nr 9/2014, 749-752

[8] Stamp M.: Information Security. Principles and Practice, John Willey & Sons, Hoboken, New Jersey 2006

[9] Bednarek M., Dąbrowski T., Wiśnios M.: Elementy koncepcji zabezpieczenia transmisji pomiędzy stacjami diagnostycznymi, X Szkoła-konferencja „Metrologia wspomagana komputerowo", Waplewo, 27-30.05.2014, s. 38

[10] 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

[11] Igure VM, Laughter SA, Williams RD: Security issues in SCADA networks, Computers & Security, 2006, 25(7),1-9

[12] Zetter K., Hackers can mess with traffic lights to jam roads and reroute cars. Wired, Apr. 2014

[13] Nicholson A., Webber S., Dyer S., Patel T., Janicke H.: SCADA security in the light of Cyber-Warfare, Computers & Security, vol. 31(4), 06.2012, 418-436

***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,