Marcin BEDNAREK[1], Tadeusz DĄBROWSKI[2]

Politechnika Rzeszowska, Katedra Informatyki i Automatyki (1), Wojskowa Akademia Techniczna, Instytut Systemów Elektronicznych (2)

doi:10.15199/48.2019.11.42

Układ dozorująco-terapeutyczny systemu transmisji danych w sieci przemysłowej

Streszczenie. *W artykule przedstawiono zasadę działań przeciwdestrukcyjnych układu dozorująco-terapeutycznego (UDT), realizowanych w stacji operatorskiej/diagnostycznej przy pomocy wbudowanych funkcjonalności pakietu SCADA. Działania te mają postać procedur wykonywanych w języku skryptowym pakietu wizualizacji. Polegają one m.in. na dynamicznej zmianie pól zmiennych. W opracowaniu udowadnia się, że pomimo dużych ograniczeń funkcjonalności języka skryptowego, można wykonać właściwie reagujący UDT.*

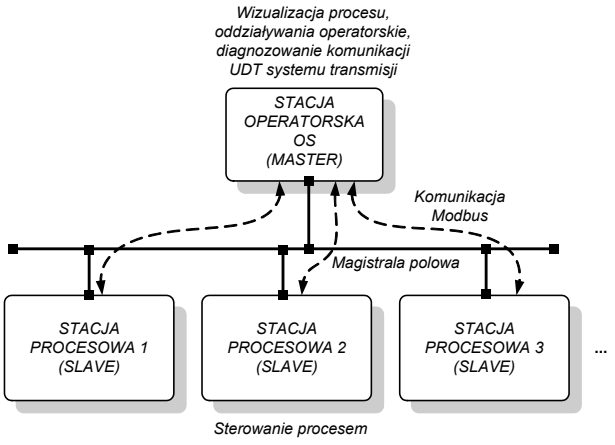
Abstract*. The paper presents the principle of anti-destructive actions of supervising and therapeutic system, carried out in the operator/diagnostic station using the built-in functionalities of the SCADA package. These activities take the form of procedures executed in the scripting language of the visualization package. They, among others, are based on dynamic change of variable fields. The study proves that despite the large limitations of the scripting language functionality, it is possible to perform a properly responsive supervising and therapeutic system. (**Data transmission supervising and therapeutic system in an industrial network**).*

Słowa kluczowe: sieć przemysłowa, układ dozorująco-terapeutyczny, diagnozowanie, działania przeciwdestrukcyjne.
Keywords: industrial network, supervising and therapeutic system, diagnosis, anti-destructive actions.

Wstęp

W referacie przedstawiono sposób implementacji układu dozorująco-terapeutycznego systemu transmisji danych w sieci przemysłowej wykorzystując wbudowane mechanizmy oprogramowania wizualizacyjnego. Sieć przemysłowa łączy elementy rozproszonego systemu sterowania. W skład rozpatrywanego mini-systemu wchodzą [1]:

- stacje procesowe – sterowniki przemysłowe sterujące procesem;
- stacja operatorska – komputery przeznaczone do wizualizacji i oddziaływań operatorskich, z oprogramowaniem dedykowanym lub uniwersalnym pakietem SCADA (ang. *Supervisory Control And Data Acquisition*) [2];
- stacja inżynierska – najczęściej komputer przenośny wykorzystywany m.in. do programowania stacji procesowej oraz przesyłu programu sterującego do pozostałych stacji systemu;
- stacja diagnostyczna – prowadząca dozorowanie procesu komunikacji oraz, w razie konieczności, uruchamiająca odpowiednie działania terapeutyczne (oddzielne urządzenie lub dodatkowe funkcje stacji operatorskiej).



Rys.1. Rozpatrywany system transmisji danych

W przedstawionym układzie stacja diagnostyczna nie jest oddzielnym urządzeniem. Jej funkcje zostały zaimplementowane w stacji operatorskiej. Rysunek 1. przedstawia uproszczony system. Dla większej czytelności pominięto tutaj stację inżynierską, podłączaną do systemu okazjonalnie w celu rekonfiguracji systemu.

Komunikacja w przedstawionym systemie odbywa się na zasadzie mechanizmu odpytywania (ang. *polling*). Stacja operatorska (*master*) wysyła komunikaty-polecenia, na które reagują stacje procesowe (typu *slave*). Przykładem protokołu działającego na takiej zasadzie jest Modbus RTU [3, 4], dla którego w pracy przedstawiono realizację działań dozorująco-terapeutycznych. Stacje procesowe nie mogą samodzielnie inicjować wymian komunikatów. Zarezerwowane jest to dla stacji nadrzędnej – stacji operatorskiej. Wyróżnia się dwa główne rodzaje wymian komunikatów z danymi:

- *Komunikat-polecenie*, w odpowiedzi na który stacja podrzędna (procesowa) wykonuje polecenie (najczęściej jest to ustawienie określonej wartości zmiennej procesowej, znajdującej się pod odpowiednim adresem wewnętrznym) i odsyła do nadawcy *komunikat-odpowiedź* identyczny z otrzymanym. Pozwala to na szybką weryfikację przez stację operatorską (tutaj także diagnostyczną) poprawności komunikacji.
- *Komunikat-pytanie*, w odpowiedzi na który stacja procesowa odsyła do nadawcy komunikat-odpowiedź zawierający wartość żądanej, określonej zmiennej procesowej, znajdującej się pod odpowiednim adresem wewnętrznym.

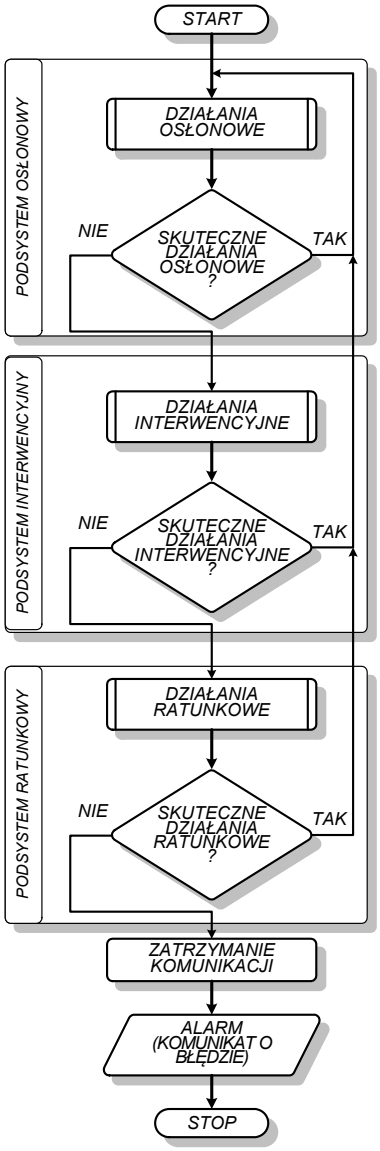
Ww. schemat działania obowiązuje tylko w warunkach pełnej zdatności systemu transmisji danych. Aby system transmisji działał poprawnie, w przypadku pojawiających się czynników zakłócających transmisję, stosuje się odpowiednie działania dozorująco-terapeutyczne przywracające zdatność systemu.

Układ dozorująco-terapeutyczny systemu komunikacji

Na system transmisji danych działają czynniki destrukcyjne, które mogą wywoływać jego niezdatność. Niezdatność systemu transmisji danych może stać się przyczyną groźnej w skutkach niezdatności całego rozproszonego systemu sterowania. Nad prawidłowym przebiegiem procesu komunikacji czuwa układ dozorująco-terapeutyczny systemu transmisji danych. Dla uproszczenia zapisu, dalej będzie używany skrót $UDT_{(SK)}$ oznaczający **u**kład **d**ozorująco-**t**erapeutyczny **s**ystemu **k**omunikacji. Dozoruje on proces komunikacji i podejmuje stosowne

działania terapeutyczne. W referacie przedstawiono działania podejmowane przez $UDT_{(SK)}$ w zależności od intensywności procesu destrukcyjnego [5,6]:

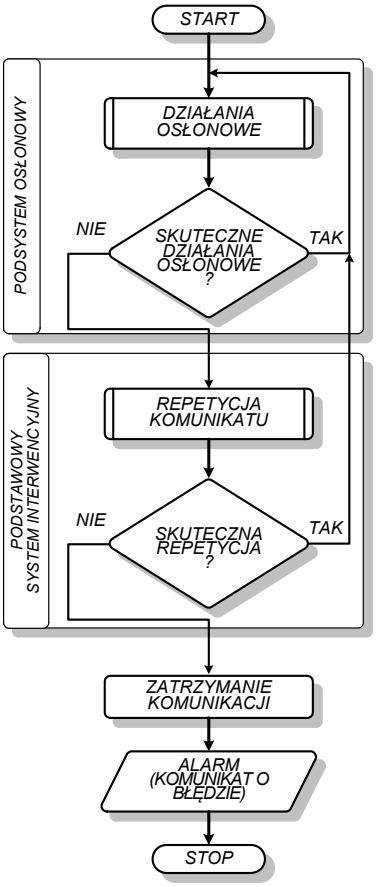
- osłonowe (poziom osłonowy):
  - obliczenie bitów parzystości;
  - sprawdzenie sum kontrolnych;
- interwencyjne (poziom interwencyjny):
  - analiza pojawiających się błędów transmisji;
  - wykrywanie przekroczeń czasów *timeout*;
  - analiza odpowiedzi urządzenia podrzędnego (obsługa błędów);
  - zmiana długości bloków danych (dostosowanie parametrów przesyłu do możliwości stacji procesowej);
  - zmiana wartości czasu cyklu;
  - repetycja komunikatów;
- ratunkowe (poziom ratunkowy):
  - przełączenie na alternatywny kanał komunikacji
  - zabezpieczenie kryptograficzne transmisji



Rys.2. Pełne działania przeciwdestrukcyjne realizowane przez $UDT_{(SK)}$

Jak sugeruje ww. lista, działania pogrupowane są zgodnie z przyjętymi [5,6] poziomami intensywności działań dozorująco-terapeutycznych. Dlatego, odpowiednio, dla trójprocesowego ujęcia procesu eksploatacji systemu transmisji danych przyjęto, że (rys. 2):

- poziom osłonowy działania $UDT_{(SK)}$ zapobiega lub neutralizuje uaktywniające się czynniki inicjujące proces destrukcyjny;
- poziom interwencyjny $UDT_{(SK)}$ przeciwdziała rozwijającemu się (w dalszym ciągu) niepożądanemu procesowi destrukcyjnemu;
- poziom ratunkowy $UDT_{(SK)}$ powoduje neutralizację lub minimalizację skutków intensywnie rozwijającego się procesu awaryjnego (prowadzącego - w przypadku braku działań przeciwdestrukcyjnych - do niezdatności systemu transmisji danych, a w konsekwencji - niezdatności całego systemu przemysłowego).



Rys.3. Podstawowe działania przeciwdestrukcyjne realizowane przez $UDT_{(SK}$

Stacja operatorska, pracująca pod kontrolą okienkowego systemu operacyjnego, wyposażona jest w oprogramowanie wizualizacyjne. W rozpatrywanym przypadku opisane tu działania implementowane były w oprogramowaniu Intouch [7], będącym częścią składową dużego pakietu SCADA (ang. *Supervisory Control And Data Acquisition*).

Standardowo, diagnozowanie komunikacji przebiega na poziomie podstawowym, obejmującym działania osłonowe (rys. 3) oraz fragment działań interwencyjnych, polegających na repetycji błędnie przesłanych komunikatów. Krotność powtórzeń określa się a priori, podczas konfiguracji systemu. Nie wymaga się przy tym większych zabiegów operatora systemu, oprócz odpowiedniego zaprojektowania scenariusza wymian komunikatów.

Proponowane w pracy rozwinięcie systemu $UDT_{(SK)}$ opiera się na ww. schemacie trójprocesowego ujęcia eksploatacji [6] systemu transmisji danych w sieci przemysłowej. Kolejne podsystemy systemu przeciwdestrukcyjnego neutralizują czynniki destrukcyjne

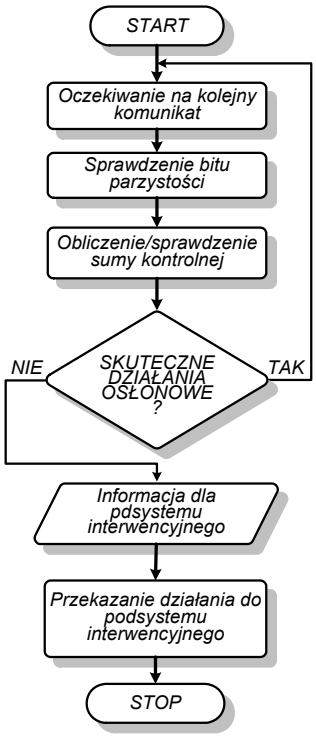
lub, w przypadku braku możliwości odparowania zagrożenia albo niewystarczająco silnych procedur zapobiegawczych, przekazują działanie do następnego podsystemu przeciwdestrukcyjnego.

Działania osłonowe

Działania osłonowe standardowo realizowane są także bez zastosowania układu dozorująco-terapeutycznego. Z tą jednak różnicą, że sprawdzanie bitu parzystości oraz sum kontrolnych ma powodować akceptację tylko prawidłowych, nieprzekłamanych odpowiedzi ze strony urządzeń podrzędnych. Nie są tu stosowane (por. rys. 2) żadne działania terapeutyczne. System transmisji danych, po nieudanej kilkukrotnej próbie przesłania, przechodzi do kolejnego komunikatu z listy wysyłkowej (scenariusza wymian komunikatów).

Na rysunku 4 przedstawiono schemat działania podsystemu osłonowego proponowanego $UDT_{(SK)}$:

1. Po nadejściu *komunikatu-odpowiedzi* następuje sprawdzenie poprawności bitu parzystości oraz sumy kontrolnej;
2. W przypadku braku komunikatu (po odczekaniu czasu *timeout*) lub obliczonych, nieprawidłowych wartości „parametrów osłonowych", proces przekazywany jest do podsystemu interwencyjnego z informacją o przyczynie przekazania.
3. W przypadku poprawnego zadziałania procedur osłonowych podproces osłonowy wraca do oczekiwania na następny odebrany *komunikat-odpowiedź*.



Rys.4. Działania osłonowe realizowane przez $UDT_{(SK)}$

Działania interwencyjne

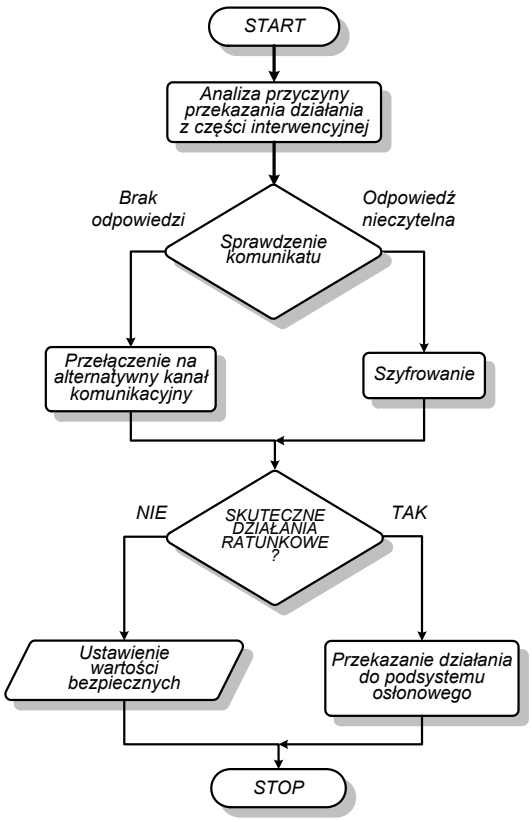
Podsystem interwencyjny uruchamiany jest, gdy podsystem osłonowy nie jest w stanie zneutralizować pojawiających czynników destrukcyjnych (por. rys. 4). Następuje wtedy przekazanie czynności dozorowania do podsystemu interwencyjnego $UDT_{(SK)}$. W efekcie analizy nadesłanego *komunikatu-odpowiedzi* następuje sprawdzenie jego zawartości (oczywiście tylko wtedy, gdy odpowiedź nadeszła). Działania interwencyjne prowadzone przez $UDT_{(SK)}$ można podzielić na trzy oddzielne wątki (rys.5), uruchamiane w zależności od genezowanej przyczyny niezdatności systemu transmisji danych:

- (I) repetycja *komunikatu-polecenia* w przypadku braku odpowiedzi ze strony stacji procesowej;
- (II) zwiększenie czasu cyklu, wg którego cyklicznie odpytywane jest urządzenie podrzędne, włączane w chwili zauważenia „gubienia" odpowiedzi lub osiągnięcia wartości czasu opóźnienia otrzymania odpowiedzi bliskiej ustawionej wartości czasu *timeout*;
- (III) obsługa błędu, realizowana dla przypadku otrzymania odpowiedzi od urządzenia podrzędnego zawierającej numer błędu, polegająca na zmianie wybranych parametrów transmisji: długość bloku danych, adres komórki z danymi, wartość przesyłanych danych, częstość odpytywania, zmiana numeru funkcji służącej do uzyskania danych.

Dla uproszczenia, w zgrubnym schemacie działania części interwencyjnej $UDT_{(SK)}$ przedstawionym na rys. 5, nie umieszczono szczegółów związanych z ewentualnym powrotem algorytmu do etapu ponownego sprawdzenia komunikatu i zastosowania innej ścieżki (I-III). W przypadku, gdy działania interwencyjne przyniosły oczekiwany skutek, sterowanie przekazywane jest z powrotem do części osłonowej $UDT_{(SK)}$ z zachowaniem ostatnio dokonanych korekt ustawień odpytywania urządzenia podrzędnego. W przeciwnym przypadku, następuje przekazanie sterowania działaniami przeciwdestrukcyjnymi do części ratunkowej systemu $UDT_{(SK)}$.

Działania ratunkowe

Działania ratunkowe $UDT_{(SK)}$ polegają na analizie otrzymanego komunikatu i podjęciu odpowiednich czynności terapeutycznych zapobiegających awarii.



Rys.5. Działania ratunkowe realizowane przez $UDT_{(SK)}$

Dostępne są tu dwie ścieżki postępowania (rys. 5):

- (I) przełączenie się na szyfrowanie komunikacji w przypadku, gdy odpowiedzi urządzenia podrzędnego wskazują na ingerencję intruza (są to m.in.: niedopuszczalny zakres wartości danych, zbyt duża prędkość narastania wartości zmiennych procesowych, niewiarygodne dane) [9-11];
- (II) przełączenie komunikacji na alternatywny kanał komunikacji (por. [12]).

Przełączenie na połączenie szyfrowane odbywa się w sytuacji, gdy stacja operatorska otrzymuje pewne zwrotne odpowiedzi. Zawierają one jednak wartości niezrozumiałe, np. wskazujące na za szybką zmianę ich wartości w czasie lub niewiarygodne z punktu widzenia przyjmowanego zakresu wartości zmiennych procesowych. Może to świadczyć o celowej zewnętrznej ingerencji intruza w system transmisji danych w sieci przemysłowej. Działanie ratunkowe polegające na przełączeniu się na kanał szyfrowany odbywa się po serii sprawdzeń, gdy wszystkie niżej wymienione działania nie przyniosą rezultatu:

1. kilkakrotna repetycja komunikatu;
2. zmiana prędkości przesyłu;
3. zmiana numeru zastosowanej funkcji;
4. zmiana liczby przesyłanych zmiennych w jednym komunikacie;
5. zmiana częstości wysyłania danych (czasu cyklu);

oraz po wysłaniu wiadomości rozgłoszeniowej (*broadcast*) do wszystkich stacji procesowych zawierającej numer klucza szyfrującego stosowanego w kolejnych wymianach danych [9, 13].

Podsumowanie

W artykule przedstawiono ideę działań przeciwdestrukcyjnych podejmowanych $UDT_{(SK)}$, realizowanych w stacji operatorskiej (diagnostycznej) przy pomocy wbudowanych funkcjonalności pakietu SCADA. Działania te mają postać procedur wykonywanych w języku skryptowym pakietu wizualizacji. Polegają one m.in. na dynamicznej zmianie pól zmiennych. Należy podkreślić, że wszystkie przedstawione tu procedury przeciwdestrukcyjne, możliwe są do zaimplementowania w dowolnym pakiecie SCADA, spełniającym nw. warunki:

- wspierającym język skryptowy [14];
- umożliwiającym zmianę parametrów wykorzystywanego połączenia komunikacyjnego;
- pozwalającym na dostęp do pól zmiennych wejściowych/wyjściowych, umożliwiającym dostęp do dodatkowych informacji ich opisujących;
- wyposażonym w mechanizmy wywoływania skryptów sterowane zdarzeniami.

W opracowaniu pokazano, że pomimo dużych ograniczeń funkcjonalności pakietu wizualizacji SCADA, można wykonać właściwie reagujący układ dozorująco-terapeutyczny systemu transmisji danych w sieci przemysłowej za pomocą standardowych mechanizmów oferowanych przez pakiet wizualizacji.

***Autorzy**: prof. dr hab. inż. Tadeusz Dąbrowski, Wojskowa Akademia Techniczna, Instytut Systemów Elektronicznych, ul. Kaliskiego 2, 01-476 Warszawa,*
E-mail: tadeusz.dabrowski@wat.edu.pl;
dr inż. Marcin Bednarek, Politechnika Rzeszowska, Katedra Informatyki i Automatyki, ul. Skłodowskiej 8, 35-959 Rzeszów, E-mail: bednarek@prz.edu.pl.

LITERATURA

[1] Bednarek M., *Wizualizacja procesów. Laboratorium*, Oficyna Wydawnicza Politechniki Rzeszowskiej, Wydanie II, Rzeszów 2004
[2] Grega W., Information Technologies Supporting Control and Monitoring of Power Systems, *Przegląd Elektrotechniczny*, 88 (2012), nr 5a, 193-197
[3] MODBUS over Serial Line Specification and Implementation Guide, Modbus.org, 2005, [http://www.modbus.org/docs/ Modbus_over_serial_line_V1_02.pdf]
[4] Szulim R., Zastosowanie rozwiązań programowych standardu IEC 61850 typu Open – Source do integracji systemów pomiarowo – sterujących, *Przegląd Elektrotechniczny*, 90 (2014), nr 11, 48-50
[5] Dąbrowski T., *Diagnozowanie systemów antropotechnicznych w ujęciu potencjałowo-efektowym*, Wyd. Wojskowej Akademii Technicznej, Warszawa, 2001
[6] Bednarek M., Będkowski L., Dąbrowski T., Metody i układy przeciwdestrukcyjne oraz diagnostyczne w systemach transmisji informacji, *Diagnostyka*, 46 (2008), nr 2, 137-142
[7] Dokumentacja elektroniczna pakietu Wonderware Intouch
[8] Wonderware FactorySuite InTouch, *Opis funkcji, pól i zmiennych systemowych*, Invensys Systems, Inc., 2005
[9] Stinson D.R., *Cryptography. Theory and Practice*, Chapman& Hall/CRC, Boca Raton, 2006
[10] Bednarek M., Dąbrowski T., Bezpieczeństwo komunikacji w rozproszonym systemie sterowania, *Przegląd Elektrotechniczny*, (2013), nr 9, 72-74
[11] Bednarek M., Dąbrowski T., Układ dozorująco-terapeutyczny wymiany kluczy w systemie transmisji danych procesowych, *Przegląd Elektrotechniczny*, (2015), nr 1, 214-219
[12] Bednarek. M, Dąbrowski T., Wybrane aspekty diagnozowania komunikacji w sieciach przemysłowych, *Materiały konferencji DIAG'2019*, Augustów, 20-25.05.2019
[13] Rome E., Bloomfield R. (eds.), *Critical Information Infrastructures Security*, Springer-Verlag, Berlin-Heidelberg 2010
[14] Anwar M.W., Azam F., Proposing a Novel Architecture of Script Component to Incorporate the Scripting Language Support in SCADA Systems. In: Saeed K., Snášel V. (eds) *Computer Information Systems and Industrial Management. CISIM 2015*. Lecture Notes in Computer Science, vol. 8838 (2014). Springer, Berlin, Heidelberg