

WIELOPROCESOWE UJĘCIE EKSPLOATACJI UKŁADU KOMUNIKACJI

Marcin BEDNAREK*, Lesław BĘDKOWSKI**, Tadeusz DĄBROWSKI**

*Katedra Informatyki i Automatyki, Wydział Elektrotechniki i Informatyki
Politechnika Rzeszowska, ul. W. Pola 2, 35-959 Rzeszów, fax (17) 8542910, e-mail: bednarek@prz.rzeszow.pl

**Instytut Systemów Elektronicznych, Wydział Elektroniki
Wojskowa Akademia Techniczna, ul. S. Kaliskiego 2, 00-908 Warszawa, fax (22) 6839125,
e-mail: lbedkowski@wel.wat.edu.pl, tdabrowski@wel.wat.edu.pl

Streszczenie

W artykule przedstawiono eksploatację układu komunikacji w ujęciu wieloprosowym. Układ komunikacji łączy stację procesową i stację operatorską (diagnostyczną) rozproszonego systemu sterowania. Scharakteryzowano komunikację pomiędzy komputerem nadrzędnym (master) a sterownikiem (slave). W procesie eksploatacji układu komunikacji wyróżniono trzy współbieżne procesy: proces użytkowania, który prowadzi do osiągnięcia wymaganego efektu użytkowego; proces destrukcyjny prowadzący do utraty zdolności i proces przeciwdestrukcyjny zapobiegający inicjacji i hamujący lub przerywający proces destrukcyjny. Przedstawiono procedury przeciwdestrukcyjne systemu dozorująco-terapeutycznego z uwzględnieniem podprocesów procesu przeciwdestrukcyjnego: osłonowego, interwencyjnego i przeciwwawaryjnego.

Słowa kluczowe: proces destrukcyjny, proces przeciwdestrukcyjny, system dozorująco-terapeutyczny.

A MULTIPROCESS APPROACH TO AN OPERATION OF COMMUNICATION SYSTEM

Summary

The operation of a communication system in a multiprocess approach is presented in the article. The communication system connects a process station and an operator station (diagnostic) of a distributed control system. The communication between a host computer (master) and a controller (slave) is briefly characterized. During the operation of the communication system three concurrent processes are differentiated: a usage process leading to a required effect of use; a destructive process causing loss of the fitness and an anti-destructive process preventing or stopping the destructive process. The anti-destructive procedures of supervision and therapeutic system are given, considering sub-processes of the anti-destructive process: protective, intervention and anti-breakdown ones.

Keywords: destructive process, anti-destructive process, supervision and therapeutic system.

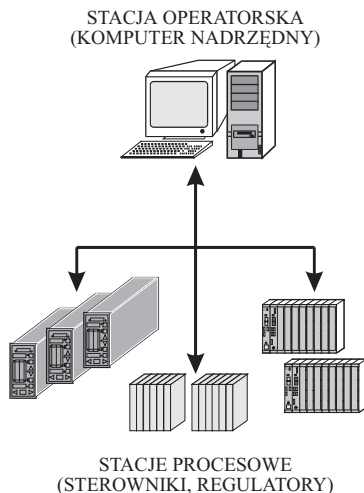
1. WPROWADZENIE

1.1. Układ komunikacji

W rozproszonym systemie sterowania można wydzielić dwie kategorie urządzeń: stacje procesowe (sterowniki - realizujące procesy sterowania) oraz stacje operatorskie (umożliwiające wizualizację i oddziaływanie operatorskie). W zależności od rodzaju uruchomionego oprogramowania stacja operatorska może pełnić rolę stacji diagnostycznej (dozorowanie stanu procesu), a także stacji inżynierskiej (konfiguracja systemu). W każdym rozproszonym systemie sterowania ma miejsce komunikacja pomiędzy urządzeniami połączonymi w sieć przemysłową (rys. 1). Pomiędzy stacją operatorską a stacjami procesowymi dokonuje się cykliczna wymiana informacji. Sieci przemysłowe powinny spełniać wymagania dotyczące przede wszystkim zdeterminowanego czasu wymiany danych, możliwości przekazywania dużej liczby

komunikatów i wysokiej niezawodności [7]. Aby spełnić pierwsze, najważniejsze spośród ww. wymagań stosuje się mechanizmy pozwalające na uniknięcie kolizji w sieci (skutek jednoczesnego nadawania przez stacje systemu). W mniejszych systemach DCS (*Distributed Control System*) [6] stosowany jest mechanizm odpytywania, polegający na cyklicznej (także na sporadycznej – np. na żądanie operatora) wymianie informacji na zasadzie *master-slave* [8]. Stacja operatorska (komputer nadrzędny – *master*) wysyła *komunikaty-pytania* do stacji procesowych (*slave*), które „nasłuchują” i oczekują na nadejście *komunikatu-pytania*. Po jego otrzymaniu stacja procesowa odpowiada komputerowi nadrzdnemu. Sterowniki obiektowe nie mogą samodzielnie inicjować wymian danych. Popularnym przedstawicielem tego typu komunikacji jest protokół *Modbus* [8]. Podane przykłady rozwiązań komunikacyjnych są wzorowane na możliwościach oferowanych przez mechanizmy protokołu *Modbus*.

W artykule przedstawione jest wieloprotocowe podejście do eksploatacji układu komunikacji realizującego wymianę informacji wg protokołu działającego na zasadzie *master-slave* (stosunkowo łatwo implementowanego). Najpierw proces komunikacji jest potraktowany (por. p. 2.1) jako proces użytkownika, a w kolejnych punktach - jako proces użytkownika i obsługiwanie kolejno uzupełnianego o mechanizmy osłonowe, interwencyjne i przeciawawaryjne [4].



Rys. 1. Rozproszony system sterowania (fragment)

1.2. Eksploatacja układu komunikacji w ujęciu wieloprotocowym

Podczas eksploatacji układu komunikacji najważniejszym zadaniem (wg podejścia bezpieczeństwa), jest utrzymanie go w stanie bezpieczeństwa (w stanie braku zagrożenia awarią lub katastrofą) [5]. Utrzymanie procesu komunikacji w stanie stabilnej zdolności nabiera znaczenia w przypadku uwzględnienia powiązania układu komunikacji z procesami przebiegającymi w stacji operatorskiej i procesowej (np. brak dostarczenia wartości zmiennej procesowej może spowodować ich niezdatność).

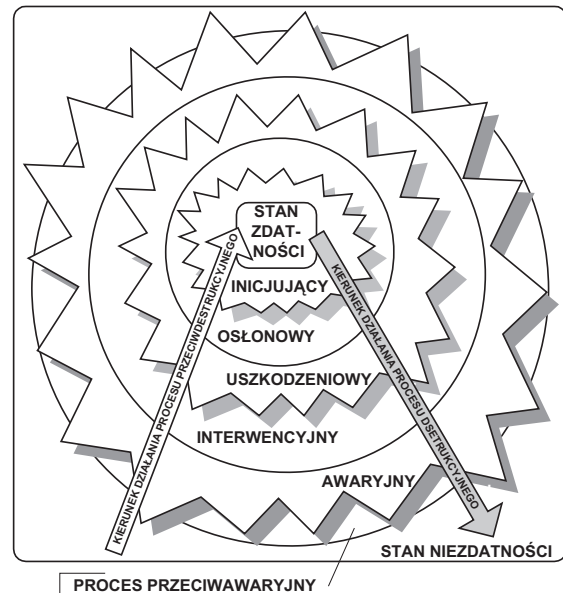
W **użytkowej fazie procesu eksploatacji** układu komunikacji (podobnie jak w każdym systemie technicznym) można wyróżnić **proces użytkownika** (proces komunikacji dostarczający dane) oraz **dwa przeciwstawne procesy: destrukcyjny i przeciawdestrukcyjny**. Sam protokół komunikacyjny oferuje mechanizmy przeciawdestrukcyjne. Sposób ich wykorzystania w dużym stopniu zależy od projektanta i/lub operatora-inżyniera.

Zadaniem systemu dozorująco-terapeutycznego (SDT), w który wyposaża się układ komunikacji (UK), jest wykrycie w odpowiedniej chwili symptomów pojawiającego się stanu niestabilnej zdolności (skutki pojawiającego się procesu destrukcyjnego). Rys. 2 przedstawia graficzną ilustrację opozycyjnych podprocesów procesu destrukcyjnego oraz przeciawdestrukcyjnego [1, 2, 3]:

- inicjującego (uaktywniającego czynniki wyzwalające) oraz osłonowego (deaktywującego czynniki inicjujące);
- uszkodzeniowego (prowadzącego do stanu niezdatności) oraz interwencyjnego (generującego czynniki interwencyjne);
- awaryjnego (niszczącego wytworzony efekt) oraz przeciawawaryjnego (ograniczającego negatywne skutki awarii).

Ostro zakończone „chmurki” (rys. 2) przedstawiają podprocesy destrukcyjne – z kolei otaczające je okręgi to podprocesy przeciawdestrukcyjne (hamujące działania destrukcyjne).

Kolejne punkty artykułu zawierają rozważania dotyczące ww. wieloprotocowego ujęcia procesu eksploatacji komunikacji pomiędzy komputerem nadrzędnym (stacją operatorską) a urządzeniem wielofunkcyjnym (sterownikiem, stacją procesową).



Rys. 2. Ilustracja działania wieloprotocowego destrukcyjnego i przeciawdestrukcyjnego

2. PROCES KOMUNIKACJI

2.1. Komunikacja pozbawiona mechanizmów przeciawdestrukcyjnych

Rozpatrzmy tylko użytkową fazę eksploatacji (bez obsługiwanie) procesu komunikacji. Na rys. 3 przedstawiono graf eksploatacyjny układu komunikacji dla urządzenia *master* (a) i *slave* (b). Odpowiednio tab. 1 i tab. 2 zawierają opis stanów.

Master cyklicznie, kolejno wysyła *komunikaty-pytania* do urządzeń podrzędnych (odpowiednio adresowanych stacji procesowych – *slave*) zawarte we wcześniej ułożonym „scenariuszu” (rys. 3). Po każdym wysłaniu przechodzi w stan oczekiwania. W tym czasie *slave* „nasłuchuje” i odbiera *komunikat-pytanie* (sprawdzając czy jest ono adresowane do niego) oraz wysyła *komunikat-*

odpowieź. Następuje odbiór, a później interpretacja i prezentacja odpowiedzi w stacji operatorskiej (*master*). W tym czasie urządzenie podrzędne przechodzi w stan oczekiwania. Taki sposób funkcjonowania układu komunikacji (pozbawiony zabezpieczeń) szybko doprowadza do stanu niezdatności. Dlatego użytkowe protokoły mają wbudowane mechanizmy ochrony przed czynnikami destrukcyjnymi. Polegają one np. na:

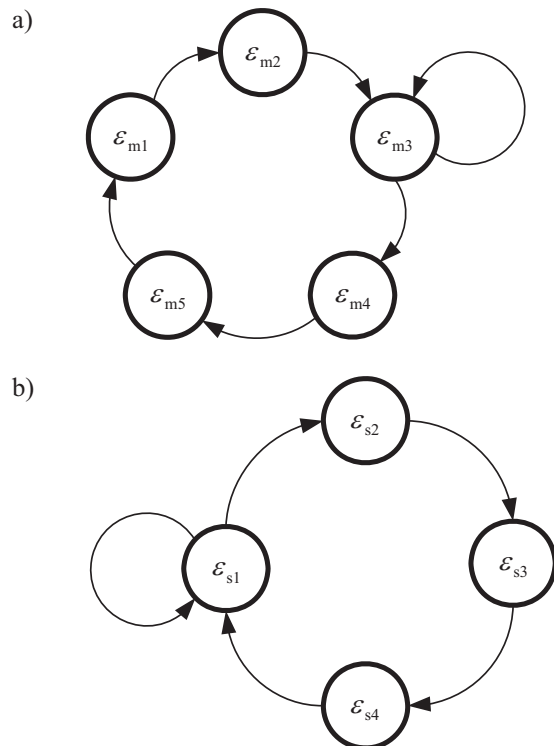
- dodawaniu bitu parzystości,
- obliczaniu sumy kontrolnej.

Tab. 1. Opis stanów procesu komunikacji pozbawionej informacji diagnostycznych - *master*

Stan	Opis
ϵ_{m1}	Wybór komunikatu do wysłania
ϵ_{m2}	Nadawanie <i>komunikatu-pytania</i>
ϵ_{m3}	Oczekiwanie na <i>komunikat-odpowieź</i>
ϵ_{m4}	Odbiór <i>komunikatu-odpowiezi</i>
ϵ_{m5}	Interpretacja, prezentacja <i>kom.-odp.</i>

Tab. 2. Opis stanów procesu komunikacji pozbawionego informacji diagnostycznych - *slave*

Stan	Opis
ϵ_{s1}	Oczekiwanie na <i>komunikat-pytanie</i>
ϵ_{s2}	Odbiór <i>komunikatu-pytania</i>
ϵ_{s3}	Interpretacja <i>komunikatu-pytania</i>
ϵ_{s4}	Nadawanie <i>komunikatu-odpowiezi</i>



Rys. 3. Grafy eksploatacyjne procesu komunikacji bez uwzględnienia informacji diagnostycznych:

a) *master*, b) *slave*

Projektant systemu komunikacyjnego decyduje o wykorzystaniu w działaniach przeciwdestrukcyjnych dostępnej informacji (na różnych poziomach wieloprotocowego modelu komunikacji).

Układ komunikacji działający wg powyższego opisu nie spełnia ostrych warunków narzucanych sieciom przemysłowym. Każde pojawienie się czynników destrukcyjnych powoduje w takim układzie mniejsze lub większe problemy komunikacyjne. Sytuacjami, z którymi nie radzi sobie układ komunikacji nieposiadający systemu dozorująco-terapeutycznego są m.in.:

- brak odpowiedzi urządzenia *slave* – zatrzymanie odpytywania w fazie oczekiwania na odpowiedź,
- brak sprawdzenia poprawności pytania – zignorowanie go lub niewłaściwa interpretacja przez *slave* oraz zatrzymanie j.w.,
- brak sprawdzenia poprawności odpowiedzi i błędna interpretacja oraz prezentacja niewiarygodnej wartości.

W celu osiągnięcia wysokiej niezawodności komunikacji rzeczywiste systemy wyposaża się w mechanizmy dozorująco-terapeutyczne, których wykorzystanie umożliwi utrzymanie układu w stanie zdadności stabilnej.

2.2. System dozorująco-terapeutyczny układu komunikacji

W warunkach komunikacji pomiędzy urządzeniami pracującymi w sieci przemysłowej (zachowanie determinizmu dotyczącego warunków dostarczenia wartości zmiennej) system powinien być uzupełniony mechanizmami przeciwdestrukcyjnymi. Poprawna komunikacja zależy w dużej mierze od ich zastosowania przez projektanta systemu (a także od możliwości oferowanych przez konkretny protokół). Zwiększenie niezawodności komunikacji leży również częściowo po stronie operatora systemu i wykorzystania przez niego rozwiązań proponowanych przez projektanta. Rolę narzędzia zapobiegania i minimalizacji skutków ewentualnej awarii spełnia system dozorująco-terapeutyczny układu komunikacji.

Pod pojęciem **systemu dozorująco-terapeutycznego układu komunikacji** (SDT_{UK}) należy rozumieć zespół mechanizmów i działań udostępnianych przez protokół komunikacyjny, które wykorzystuje (lub może wykorzystać) interfejs sieciowy komunikującego się urządzenia, a także odpowiednio dobranych przez projektanta (lub operatora) funkcji i procedur oprogramowania, pozwalających przeciwdziałać procesom destrukcyjnym [4].

SDT_{UK} można podzielić na trzy podsystemy:

- **podsystem osłonowy**, oferujący tylko działania osłonowe zapobiegające powstawaniu czynników wyzwalających podproces inicjujący (SDT_{UK-O}),
- **interwencyjny**, rozpoznający proces uszkodzeniowy i generujący czynniki interwencyjne (SDT_{UK-I}),

- **przeciawaryjny**, wykrywający przejście w stan awarii i minimalizujący jej skutki (SDT_{UK-PA}).

3. EKSPLOATACJA UKŁADU KOMUNIKACJI UWZGLĘDNIAJĄCA MECHANIZMY PRZECIWDESTRUKCYJNE

3.1. Mechanizmy osłonowe

Graf eksploatacyjny procesu komunikacji z uwzględnieniem informacji pochodzących z SDT_{UK-O} przedstawia rys. 4 (tab. 3 i tab. 4 zawierają opis stanów, odpowiednio dla *master* i *slave*). Układ komunikacji wyposażony w podsystem osłony SDT_{UK-O} dodaje do procesu komunikacji procedurę osłonową obliczającą i sprawdzającą sumę kontrolną nadchodzącego komunikatu (*master* i *slave*):

- w razie stwierdzenia niezgodności pomiędzy otrzymaną i obliczoną wartością, stacja ignoruje polecenie i przechodzi w stan oczekiwania (stacja procesowa) lub w stan wybierania kolejnego komunikatu do wysłania (stacja operatorska);
- w przypadku poprawnego odbioru komunikatu wysyłana jest odpowiedź zawierająca żądane dane (*slave*) lub (po pozytywnym wyniku sprawdzenia zawierania się otrzymanej wartości w wymaganym przedziale – tzn. po dodatkowym działaniu osłonowym) następuje prezentacja odpowiedzi (*master*).

Tab. 3. Opis stanów eksploatacji procesu komunikacji wzbogaconego o informacje SDT_{UK-O} - *master*

Stan	Opis
ε_{m1}	Wybór komunikatu do wysłania
ε_{m2}	Nadawanie <i>komunikatu-pytania</i>
ε_{m3}	Oczekiwanie na <i>komunikat-odpowieź</i>
ε_{m4}	Odbiór <i>komunikatu-odpowieź</i>
ε_{m5}	Sprawdzenie sumy kontrolnej <i>kom.-odp.</i>
ε_{m6}	Sprawdzenie poprawności <i>kom.-odp.</i>
ε_{m7}	Interpretacja, prezentacja <i>kom.-odp.</i>
Warunki przejść:	$\varepsilon_{m5} \rightarrow \varepsilon_{m1}$ i $\varepsilon_{m6} \rightarrow \varepsilon_{m1}$ - przy błędnym wyniku sprawdzenia

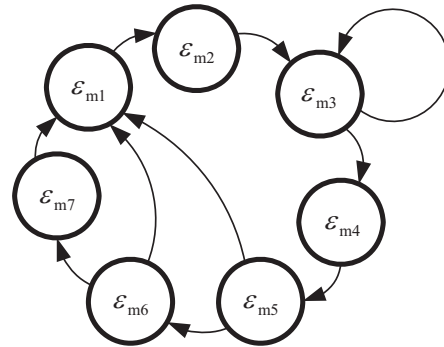
W przypadku korzystania jedynie z informacji SDT_{UK-O}, ograniczeniem funkcjonalności systemu komunikacji jest zatrzymanie procesu komunikacji w przypadku braku odpowiedzi z urządzenia podrzędnego. Aby tego uniknąć układ komunikacji należy wzbogacić o SDT_{UK-I}.

Tab. 4. Opis stanów eksploatacji procesu komunikacji wzbogaconego o informacje SDT_{UK-O} - *slave*

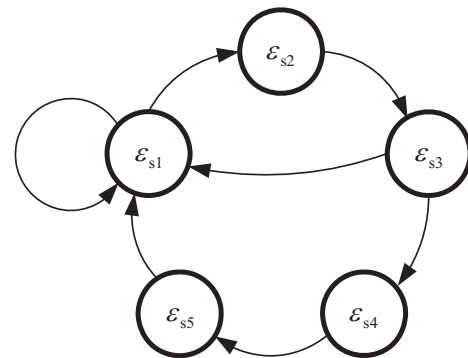
Stan	Opis
ε_{s1}	Oczekiwanie na <i>komunikat-pytanie</i>
ε_{s2}	Odbiór <i>komunikatu-pytania</i>
ε_{s3}	Sprawdzenie sumy kontrolnej <i>kom.-pyt.</i>
ε_{s4}	Interpretacja <i>komunikatu-pytania</i>

ε_{s5}	Nadawanie <i>komunikatu-odpowieź</i>
Warunki przejść:	$\varepsilon_{s3} \rightarrow \varepsilon_{s1}$ - przy błędnym wyniku sprawdzenia

a)



b)



Rys. 4. Proces komunikacji wzbogacony o informacje SDT_{UK-O}: a) *master*, b) *slave*

3.2. Mechanizmy interwencyjne

Podsystem interwencyjny (SDT_{UK-I}) zapewnia dodatkowe procedury podtrzymujące ciągłość procesu komunikacji oraz umożliwiające dostarczenie do stacji operatorskiej informacji diagnostycznej o reakcji stacji procesowej (patrz: grafy eksploatacyjne - rys. 5, opis stanów – tab. 5 i tab. 6). Aby komputer nadrzędny reagował na brak odpowiedzi ze strony stacji procesowej wprowadza się w driverze komunikacyjnym kryteria (parametry), które pozwalają na przerwanie oczekiwania na odpowiedź i podjęcie dalszych działań. Standardowe drivery dają możliwość wprowadzenia następujących kryteriów [4]:

- maksymalnej liczby repetycji pytania k_{max} , po przekroczeniu której (przy braku odpowiedzi w czasie nie większym niż t_{max}) komputer nadrzędny przechodzi do wyboru następnego pytania z listy;
- maksymalnego czasu oczekiwania na odpowiedź (*timeout* t_{max}), po przekroczeniu którego (o ile nie przekroczono maksymalnej liczby powtórzeń) stacja operatorska powtarza pytanie.

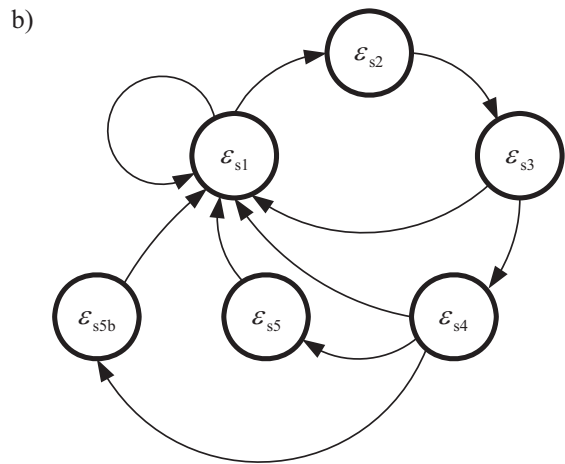
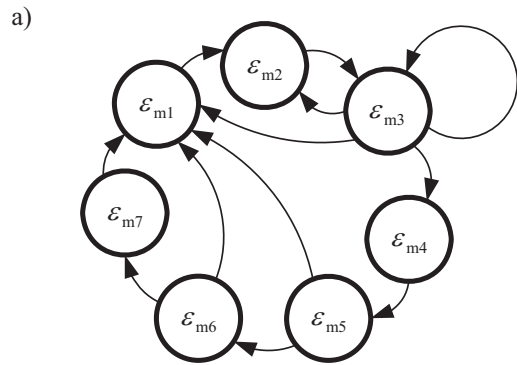
Proces interwencyjny w urządzeniu podrzędnym sprowadza się do sprawdzenia poprawności polecenia przesłanego z komputera nadrzędnego i (w razie błędu) poprawności odpowiedzi zawierającej numer błędu (będącego objawem jednego ze stanów: adres poza zakresem, dane poza zakresem, błędny kod funkcji, urządzenie zajęte itp. - w przypadku rozpoznawalnego błędu). Umożliwia to diagnozowemu (np. oprogramowaniu stacji operatorskiej) dokonanie wniosku diagnostycznego dotyczącego stanu układu komunikacji.

Tab. 5. Opis stanów eksploatacji procesu komunikacji wzbogaconego o informacje SDT_{UK-I} - master

Stan	Opis
ϵ_{m1}	Wybór komunikatu do wysłania
ϵ_{m2}	Nadawanie komunikatu-pytania z inkrementacją liczby powtórzeń k
ϵ_{m3}	Oczekiwanie na kom.-odp. z uwzgl. czasu oczekiwania t i liczby powtórzeń k
ϵ_{m4}	Odbiór komunikatu-odpowiedzi
ϵ_{m5}	Sprawdzenie sumy kontrolnej kom.-odp.
ϵ_{m6}	Sprawdzenie poprawności kom.-odp.
ϵ_{m7}	Interpretacja, prezentacja kom.-odp.
<u>Warunki przejść:</u>	
$\epsilon_{m5} \rightarrow \epsilon_{m1}$ i $\epsilon_{m6} \rightarrow \epsilon_{m1}$ - przy błędnym wyniku sprawdzenia	
$\epsilon_{m3} \rightarrow \epsilon_{m4}$ - $t \leq t_{max} \wedge k \leq k_{max}$ (nadejście kom.-odp.)	
$\epsilon_{m3} \rightarrow \epsilon_{m1}$ - $t > t_{max} \wedge k > k_{max}$ (brak kom.-odp.)	
$\epsilon_{m3} \rightarrow \epsilon_{m2}$ - $t > t_{max} \wedge k \leq k_{max}$ (brak kom.-odp.)	

Tab. 6. Opis stanów eksploatacji procesu komunikacji wzbogaconego o informacje SDT_{UK-I} - slave

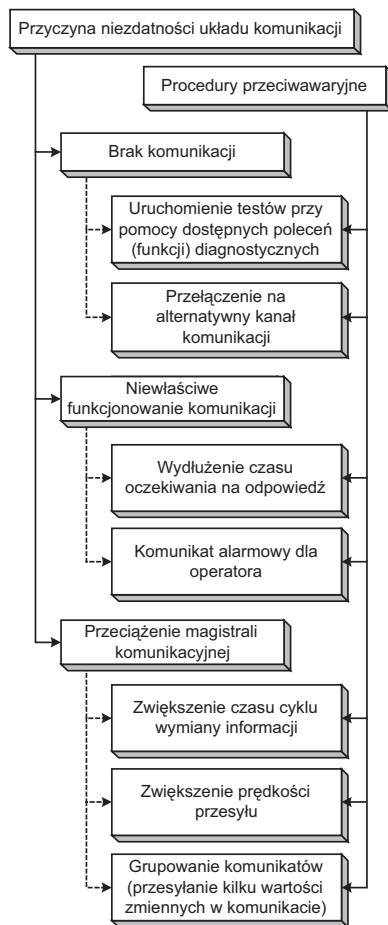
Stan	Opis
ϵ_{s1}	Oczekiwanie na komunikat-pytanie
ϵ_{s2}	Odbiór komunikatu-pytania
ϵ_{s3}	Sprawdzenie sumy kontrolnej kom.-pyt.
ϵ_{s4}	Interpretacja i sprawdzenie poprawności komunikatu-pytania
ϵ_{s5}	Nadawanie komunikatu-odpowiedzi
ϵ_{s5b}	Nadawanie komunikatu-odpowiedzi z informacją o rodzaju (numerze) błędu
<u>Warunki przejść:</u>	
$\epsilon_{s3} \rightarrow \epsilon_{s1}$ - przy błędnym wyniku sprawdzenia	
$\epsilon_{s4} \rightarrow \epsilon_{s1}$ - przy błędnym wyniku sprawdzenia, jeśli błąd nie jest identyfikowany przez SDT _{UK-I}	
$\epsilon_{s4} \rightarrow \epsilon_{s5b}$ - przy błędnym wyniku sprawdzenia, jeśli błąd jest identyfikowany przez SDT _{UK-I}	



Rys. 5. Proces komunikacji wzbogacony o informacje SDT_{UK-I}: a) master, b) slave

3.3. Mechanizmy przeciawaryjne

W przypadku niewystarczających działań systemu osłonowego i interwencyjnego, dochodzi do sytuacji awaryjnej. Można wtedy mówić o braku komunikacji lub niewłaściwym jej funkcjonowaniu (np. bez gwarancji dostarczenia oczekiwanej informacji – wartości zmiennej procesowej). Proponowane działania SDT_{UK-PA} służą do zminimalizowania strat wynikających z tej sytuacji. Działania te są wykonywane sporadycznie (nie należą do cyklu normalnej pracy układu komunikacji). Rys. 6 przedstawia przykłady mechanizmów przeciawaryjnych. Wybór wykonywanej procedury przeciawaryjnej zależy od przyczyny, która spowodowała niezdatność układu komunikacji.



Rys. 6. Procedury przeciwwawaryjne

4. PODUMOWANIE

Stan układu komunikacji wpływa pośrednio na stan „porozumiewających się” stacji systemu sterowania. Niezdatność układu komunikacji prowadzi do błędów sterowania procesem technologicznym, a w konsekwencji – do strat ekonomicznych. Wprowadzenie elementów SDT pozwala na wcześniejsze wykrywanie i odpowiednie przeciwdziałanie zagrożeniom.

Przedstawione mechanizmy osłonowe i interwencyjne oferowane są zazwyczaj przez rzeczywiste protokoły. Jednak nie wszyscy producenci urządzeń je wykorzystują. Dlatego większość procedur zabezpieczających (realizowanych programowo) powinien zapewnić projektant systemu.

LITERATURA

- [1] Będkowski L., Dąbrowski T., Bednarek M.: Niedomiary potencjalności przeciwdestrukcyjnej systemu katalizatorem niezdatności. Materiały XXXIII Zimowej Szkoły Niezawodności. Szczyrk, 10÷15.01.2005, str. 32-43.
- [2] Będkowski L., Dąbrowski T.: Model eksploatacyjny obiektu technicznego w ujęciu wieloprotocowym. Materiały II Międzynarodowej

Konferencji Explo-Diesel & Gas Turbine'2003. Międzyzdroje-Lund, 05÷09.05.2003, str. 45-52.

- [3] Będkowski L.: System dozoru i terapeutyczny w ujęciu wieloprotocowym. Materiały V Krajowej Konferencji DIAG'2003. Ustroń, 13÷17.10.2003, str. 30-39.
- [4] Bednarek M., Będkowski L., Dąbrowski T.: Procedury przeciwdestrukcyjne układu komunikacji w ujęciu wieloprotocowym. Materiały XXXII Ogólnopolskiego Sympozjum „Diagnostyka Maszyn”, Węgierska Górka, 28.02÷05.03.2005.
- [5] Będkowski L.: Elementy diagnostyki technicznej. WAT, wyd. 2, Warszawa 1992, rozdział 4.
- [6] Trybus L.: Kierunki rozwoju regulatorów i sterowników aparaturowych. Materiały XIII KKA, Opole, 21÷24.09.1999, tom 1, str. 349-356.
- [7] Sacha K.: Systemy czasu rzeczywistego. Oficyna Wydawnicza PW, wyd. 2, Warszawa 1999
- [8] Modbus Protocol Reference Guide. Modicon, June 1996.

Informacje o Autorach znajdują się na stronie 36