



Symulacyjne środowisko dla testowania elementów sieci telemetrycznych

WOJCIECH SULEJ, JAN CHUDZIKIEWICZ

Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Teleinformatyki i Automatyki,
00-908 Warszawa, ul. S. Kaliskiego 2

Streszczenie. W artykule zaprezentowano problematykę dotyczącą realizacji procesu symulacyjnego testowania elementów sieci telemetrycznych z zastosowaniem metod diagnostyki systemowej. Omówiono podstawy zagadnienia z zakresu wykorzystywanych metod diagnostyki systemowej. Przedstawiono zarysy projektu sieci telemetrycznej do badań w zakresie diagnostyki i bezpieczeństwa, a także opracowywane dla niej środowisko symulacyjne dla potrzeb testowania elementów tej sieci. Na bazie środowiska symulacyjnego zaprezentowano przykładową realizację procesu diagnozowania elementów sieci telemetrycznej.

Słowa kluczowe: diagnostyka systemowa, sieci telemetryczne, metody testowania sieci przemysłowych, standardy komunikacyjne

1. Wstęp

Problematyka diagnozowania procesów przemysłowych — w tym również sieci przemysłowych — jest szeroko analizowana w literaturze światowej. Znana autorom artykułu literatura z wybranego zakresu tematycznego porusza problem diagnozowania elementów sieci przemysłowych czy np. procesów przemysłowych. Problematyka diagnozowania procesów przemysłowych jest szczegółowo zaprezentowana w publikacji [8]. Autor tej publikacji porusza zagadnienia diagnozowania procesów przemysłowych z uwzględnieniem wymogów nakładanych na systemy czasu rzeczywistego.

Inne podejście zostało zaprezentowane w pracy [10], gdzie przedstawiono rozwiązanie bazujące na wykrywaniu uszkodzeń w elementach komunikacyjnych sieci przemysłowych. Realizacja procesu wykrywania uszkodzeń bazuje na metodach

i technikach diagnostyki systemowej. Autorzy proponują wykorzystanie do diagnostyki między innymi protokołu SNMP.

Podobnie w pracy [13] poruszana jest problematyka detekcji oraz diagnozowania błędów w sieciach przemysłowych bazujących na standardzie Ethernet. Przedstawiono modele błędów, które mogą być zaimplementowane w tego typu rozwiązaniach.

Jak można zaobserwować, problematyka diagnozowania poszczególnych elementów sieci przemysłowych traktowana jest rozłącznie. Istotne jest więc połączenie problematyki diagnozowania zarówno procesów, jak również elementów i mechanizmów przesyłowych i zaproponowanie wspólnej metodyki ich diagnozowania. Stąd też celem realizacji badań, których fragment przedstawiono w artykule, jest rozwinięcie podstaw teoretycznych metod diagnostyki systemowej sieci teleinformatycznych i sieci przemysłowych, ich praktyczna weryfikacja oraz zaproponowanie jednolitej metody oceny stanu bezpieczeństwa i niezawodności całego systemu.

2. Elementy diagnostyki systemowej

Zależnie od rodzaju zastosowanego modelu diagnostycznego, wyniki wzajemnego testowania się elementów sieci można przedstawić za pomocą podanych poniżej zależności. Największe znaczenie praktyczne znalazły modele PMC oraz BGM [1, 2, 9, 10, 12].

W przypadku przyjęcia modelu PMC interpretacja wyników testowania przedstawiana jest za pomocą następujących zależności:

$$[n(e_s) = n_0(e_s)] \Rightarrow \left[d_{st} = \begin{cases} 0 & \text{dla } n(e_t) = n_0(e_t) \\ 1 & \text{dla } n(e_t) \neq n_0(e_t) \end{cases} \right] \quad (1)$$

oraz:

$$[n(e_s) \neq n_0(e_s)] \Rightarrow [d_{st} = x] \quad (x \in \{0, 1\}), \quad (2)$$

gdzie: $n(e_s)$ — stan niezawodnościowy elementu, który w grafie reprezentowany jest przez węzeł e_s ;

$n_0(e_s)$ — stan zdadności komputera e_s ;

d_{st} — opinia elementu testującego e_s o elemencie testowanym e_t ,

przy czym $d_{st} = 0$ oznacza, że komputer e_s opiniuje jako zdadny element e_t natomiast $d_{st} = 1$ oznacza, że element e_s opiniuje jako niezadny element e_t .

Jeżeli przyjęty zostanie model BGM, wówczas wynik testowania się elementów przedstawiany jest za pomocą następującej zależności:

$$[n(e_s) \neq n_0(e_s)] \Rightarrow \left[d_{st} = \begin{cases} x & \text{dla } n(e_t) = n_0(e_t) \\ 1 & \text{dla } n(e_t) \neq n_0(e_t) \end{cases} \right]. \quad (3)$$

Zwykle w systemach o zwiększonej odporności na uszkodzenia uwarunkowanych czasowo bierze się pod uwagę dwie strategie diagnostyczne, pierwsza dotyczy diagnozy dokładnej (jednoznacznej), druga związana jest z diagnozą nadmiarową. W przypadku systemów jednoznacznie diagnozowalnych chodzi o precyzyjną identyfikację wszystkich niezdatnych jednostek (komputerów) w systemie na podstawie uzyskanych wyników testów wzajemnych tych jednostek przy założeniu, że liczba niezdatnych jednostek systemu nie przekroczy ustalonego parametru t . W systemach jednoznacznie diagnozowalnych stosowane są dwie metody: opiniowanie diagnostyczne i dialog diagnostyczny.

Metoda opiniowania diagnostycznego zalicza się do grupy scentralizowanych metod diagnozowania systemów komputerowych. Cechą charakterystyczną tej metody jest to, że identyfikacji niezdatnych jednostek systemu (sieci komputerowej) dokonuje się po zgromadzeniu wszystkich wyników testowań elementów, zgodnie z założonym przydziałem testów.

Metoda dialogu diagnostycznego należy do grupy rozproszonych metod diagnozowania systemów (sieci). W przypadku tych metod proces testowania inicjowany jest przez dowolny element sieci i obejmuje zazwyczaj pewien podzbiór elementów sieci przyległych do elementu inicjującego. Możliwe, pomiędzy elementami biorącymi udział w testowaniu, dialogi diagnostyczne opisane są grafem nazywanym grafem dialogów diagnostycznych, który jest tożsamy grafowi opisującemu strukturę logiczną sieci. Uzyskane w procesie testowania wyniki wykorzystywane są do oceny stanu niezawodnościowego zarówno elementów (łącznie z elementem inicjującym), jak i linii transmisji danych należących do badanego podzbioru elementów sieci.

Systemy jednoznacznie diagnozowalne są systemami o ograniczonej diagnozowalności, wynikającej głównie z topologii połączeń między elementami, która określa możliwości wzajemnego testowania się elementów. Problem ten może być bardzo istotny w przypadku systemów (sieci) o dużej liczbie elementów.

W systemach nadmiarowo diagnozowalnych pewna liczba elementów systemu może być diagnozowana niepoprawnie (zdatne elementy mogą być diagnozowane jako niezdatne). Przy takim podejściu istnieje możliwość określenia takiego zbioru elementów, który zawierać będzie wszystkie niezdatne elementy systemu oraz być może niewielką liczbę elementów zdatnych. Pozwala to na szybką izolację wszystkich niezdatnych jednostek systemu w ramach tak określonego zbioru, kosztem utraty niewielkiej liczby jednostek zdatnych. Dalej dokonuje się rekonfiguracji systemu z udziałem pozostałych elementów systemu.

3. Sieci telemetryczne

Telemetria to dziedzina telekomunikacji obejmująca różne techniki przesyłania wartości wielkości mierzonych na odległość. Telesterowanie to zdalne sterowanie obiektami zautomatyzowanymi. Sieć telemetryczna — inaczej system telemetryczny — to urządzenia pomiarowe i sterujące rozmieszczone na większym obszarze (w terenie lub w budynkach), połączone siecią telekomunikacyjną, realizujące założenia telemetrii i telesterowania. Do przesyłania informacji w sieciach telemetrycznych używa się sieci telefonicznych, drogi radiowej, komunikacyjnych sieci przemysłowych, przewodowych, bezprzewodowych i światłowodowych sieci komputerowych oraz sieci mobilnych (komórkowych).

Sieci telemetryczne znajdują zastosowanie przede wszystkim w energetyce, przedsiębiorstwach wodno-kanalizacyjnych i gazowych. Obecnie sieci telemetryczne mają coraz większe zastosowanie także w innych dziedzinach, takich jak:

- nadzór i zarządzanie wszystkimi urządzeniami technicznymi wykorzystywanymi w dziedzinie:
 - produkcji wody (odwierty, ujęcia wody, stacje uzdatniania, pompownie);
 - magazynowania i dystrybucji (zbiorniki ciśnieniowe, zasobniki, komory obliczeniowe);
- nadzór i zarządzanie obiektami wchodzącymi w skład sieci kanalizacyjnych i deszczowych:
 - oczyszczalniami ścieków;
 - przepompowniami;
 - przelewami burzowymi;
- przewidywanie wylewów rzek i kanałów;
- kontrola jakości wody;
- monitorowanie magazynów z odpadami;
- monitorowanie poziomu wód gruntowych;
- monitorowanie kotłowni i sieci ciepłowniczych;
- nadzór i zapis pomiarów dotyczących urządzeń chłodniczych;
- zarządzanie zakładami produkującymi energię odnawialną (słoneczną, wiatrową);
- techniczne zarządzanie budynkami:
 - monitoring i optymalizacja zużycia energii elektrycznej;
 - zdalne odczyty liczników wody, gazu, prądu;
 - zarządzanie ogrzewaniem/klimatyzacją w zależności od zaplanowanych założeń;
 - nadzór pracy wind;
 - kontrola dostępu;
- oświetlenie publiczne:

- kontrola szaf i stacji;
 - sterowanie oświetleniem;
 - monitorowanie działania;
 - optymalizacja zużycia energii;
- optymalizacja zużycia wody, elektryczności, gazu, ogrzewania w przemyśle;
 - alarmy techniczne;
 - nadzór nad odpadami wprowadzanymi do środowiska.

Pomimo różnorodności zastosowań systemy telemetryczne zazwyczaj realizują następujące podstawowe funkcje:

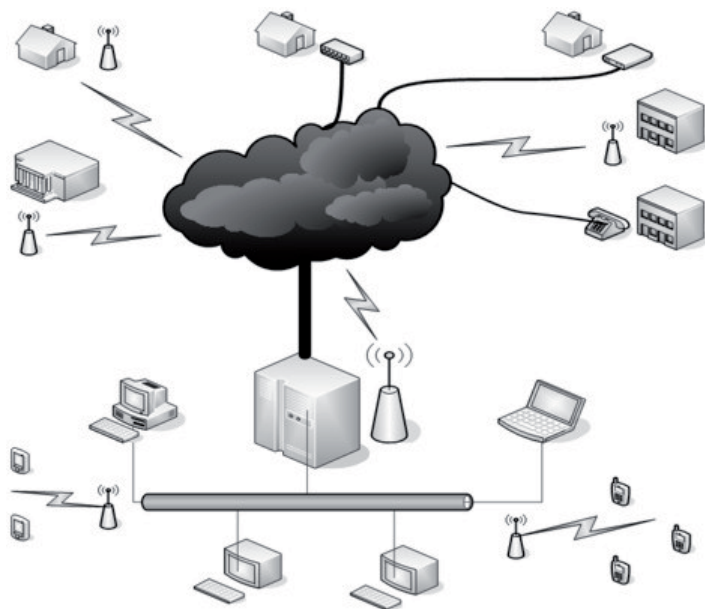
- automatyczny odczyt wartości z urządzeń pomiarowych zgodnie z zadanymi harmonogramami;
- przekazywanie informacji między odległymi obiektami, umożliwiające zdalny nadzór i zarządzanie;
- zdalne sterowanie i oddziaływanie na odległość na monitorowane urządzenia;
- automatyczne i ręczne sterowanie działaniem urządzeń;
- automatyczne nadawanie komunikatów alarmowych w razie awarii lub usterki urządzenia;
- zapis informacji pozwalający na analizę, optymalizację i zarządzanie odległymi obiektami.

Dodatkowo sieci telemetryczne spełniają następujące zadania:

- rejestrują wyniki pomiarów, umożliwiając dostęp do danych historycznych;
- obliczają wartości średnie oraz udostępniają parametry związane z dokładnością;
- opracowują wyniki pomiarów, określają wskaźniki oraz porządkują je;
- generują sygnały przeznaczone do regulacji, samorekonfiguracji i ostrzegawcze;
- dostarczają danych o aktualnej wartości wielkości mierzonej lub kontrolowanej;
- opracowują rozliczenia finansowe w zależności od zużycia dla różnych parametrów.

Ogólna idea budowy sieci telemetrycznej została przedstawiona na rysunku 1. Urządzenia pomiarowe, czujniki lub urządzenia sterujące rozmieszczone są w różnych budynkach na znacznym obszarze. Odpowiednie przetworniki umożliwiają odczytanie i przesyłanie wartości mierzonych wielkości lub poleceń sterujących przy pomocy różnych mediów komunikacyjnych do centrum monitoringu (sterowania) i w odwrotną stronę.

W centrum dane mogą być w dowolny sposób obrabiane i dostarczane upoważnionym do ich odbioru użytkownikom. Z centrum przesyłane są też odpowiednie dane konfiguracyjne i polecenia sterujące do urządzeń.



Rys. 1. Ogólna idea budowy sieci telemetrycznej

4. Badana sieć telemetryczna

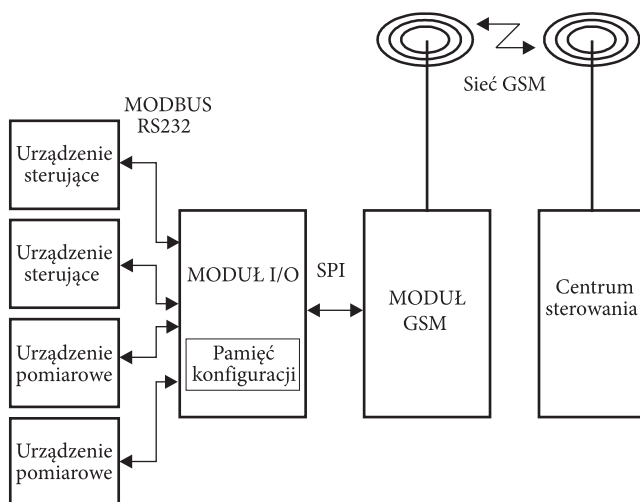
Celem realizowanych badań jest wykorzystanie diagnostyki systemowej do kompleksowego diagnozowania systemów przemysłowych, w szczególności sieci telemetrycznych.

Do tych badań został opracowany przez autorów artykułu przykładowy system telemetryczny (sieć telemetryczna). Przygotowany system jest przykładem realizacji sieci przemysłowej. Umożliwia on zdalny odczyt wartości wielkości mierzonych przez podłączone do systemu różne urządzenia pomiarowe oraz zdalne sterowanie różnymi urządzeniami sterującymi.

Istotą opracowanych testów jest weryfikacja poprawności działania modułu wejścia-wyjścia tego systemu (moduł I/O z rysunku 2). Moduł ten ma za zadanie odczytywanie i zapamiętywanie danych z urządzeń oraz zapisywanie danych do urządzeń sterujących. Z drugiej strony moduł I/O zapewnia poprzez moduł GSM przekazywanie danych do Centrum sterowania i odbieranie poleceń sterujących.

Mierzone wielkości są zamieniane na sygnał elektryczny w urządzeniu pomiarowym lub czujniku pomiarowym. Moduł I/O przechowuje odczytane informacje w odpowiednim formacie.

Moduł I/O użyty w badanym systemie umożliwia zarządzanie 4 urządzeniami pomiarowymi lub sterującymi jednocześnie.



Rys. 2. Schemat blokowy badanej sieci telemetrycznej

W założeniu system powinien współpracować z urządzeniami pomiarowymi i urządzeniami sterującymi różnych typów. Stąd też opracowany zestaw testów pozwala na sprawdzenie poprawności pracy modułu I/O w różnych konfiguracjach.

W jednej z badanych konfiguracji do modułu I/O podłączony był regulator pogodowy (urządzenie sterujące) oraz licznik ciepła (urządzenie pomiarowe). Identyfikacja urządzeń realizowana jest poprzez podział na grupy, przy czym jedno urządzenie stanowi jedną grupę i podłączane jest do końcówek odpowiadających danej grupie. W danej chwili może być obsługiwanych od jednej do czterech grup. Grupy nieobsługiwane są programowo wyłączane poprzez wprowadzenie opisu konfiguracji do pamięci konfiguracji.

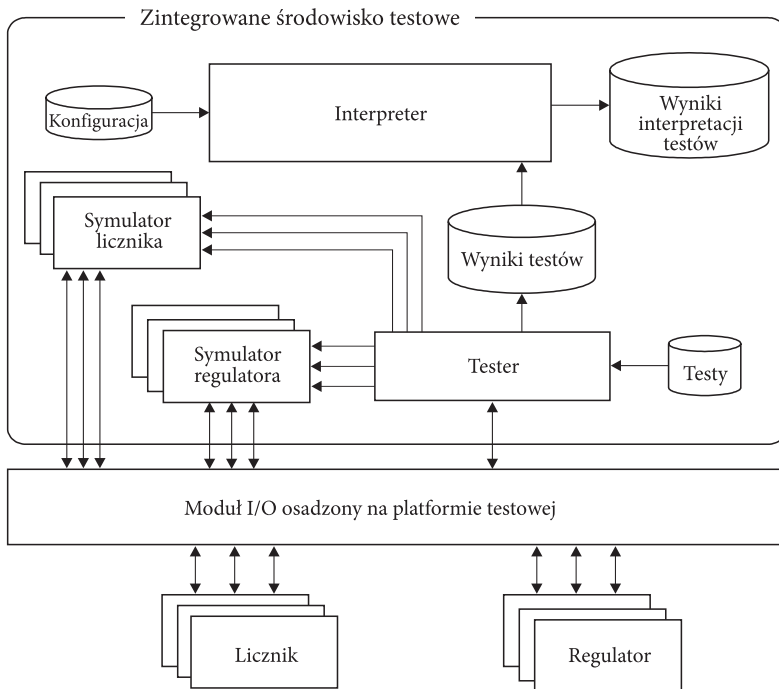
Komunikacja pomiędzy modułem GSM oraz modułem I/O realizowana jest z wykorzystaniem standardu SPI (ang. *Serial Peripheral Interface*). Natomiast komunikacja pomiędzy modułem I/O a urządzeniami wykorzystuje standard MODBUS (w przypadku regulatora pogodowego) lub rozwiązanie firmy, która urządzenie wyprodukowała (w przypadku licznika ciepła). Proces diagnozowania zależy silnie od właściwości wykorzystywanych w systemie interfejsów komunikacyjnych.

5. Symulacyjne środowisko dla testowania elementów sieci telemetrycznej

Stworzenie środowiska symulacyjnego dla potrzeb testowania elementów sieci telemetrycznych ma na celu znaczne zmniejszenie kosztów przygotowania niezawodnej pod względem funkcjonalnym i spełniającej wymogi bezpieczeństwa sieci

telemetrycznej gotowej do wdrożenia w warunkach rzeczywistych. Środowisko symulacyjne pozwala w łatwy i tani sposób przetestować nowo projektowane elementy sieci telemetrycznej w pierwszych etapach projektowania nowego systemu rzeczywistego, a także przy rozszerzaniu funkcjonalności już istniejącej sieci.

Schemat blokowy środowiska symulacyjnego dla testowania elementów systemu telemetrycznego został przedstawiony na rysunku 3.



Rys. 3. Schemat blokowy środowiska symulacyjnego dla testowania elementów sieci telemetrycznej

Zadaniem środowiska symulacyjnego sieci przemysłowej jest pełna automatyzacja procesu testowania systemu telemetrycznego na poziomie modułu I/O i na poziomie całego systemu. Środowisko umożliwia sprawdzanie poprawności działania modułu I/O po dokonaniu w nim zmian lub rozszerzeń funkcjonalnych.

Dodatkowo stworzone środowisko testowe umożliwia przeprowadzanie testów nie tylko na etapie konstrukcyjnym, ale także na etapie produkcyjnym, gdzie w szczególności może zostać wykorzystane do sprawdzenia każdego modułu I/O systemu telemetrycznego przed jego zainstalowaniem w rzeczywistym systemie u odbiorcy końcowego.

Wykonane oprogramowanie ma budowę modułową. Każdy moduł realizuje funkcje w zależności od jego roli w systemie testującym.

Tester realizuje zadania związane z przesyłaniem kolejnych testów wybranej sekwencji testowej na wejście modułu I/O w postaci odpowiednich poleceń sterujących i pobieranie wyniku wykonania testu z wyjścia modułu I/O w postaci odpowiedzi na polecenia sterujące. Wszystkie wyniki dla wybranej sekwencji testowej są automatycznie oznaczane odpowiednimi znacznikami i zostają zapisane w pliku tekstowym lub pliku XML.

Poniżej przedstawiona została przykładowa realizacja automatycznego wykonywania testów z wybranej sekwencji testowej dla jednej z konfiguracji.

```
SEKWENCJA TESTOWA: 20000
```

```
>>START TEST 20001<<
```

```
17:50:44.67 Moduł IO Gotowy!
```

```
17:50:44.67 RCON:1C SVer:0E MTyp:06030001
```

```
17:50:49.40 GR:01T:01
```

```
17:50:49.42 RMet:1DB2012F00000510852410F13A01000C00000000D00000000  
046B150000FF05FAA10000FF092337000018312319F60A1A3B18130000FF14000  
000150000FF300000
```

```
17:50:49.51 GR:03T:03
```

```
17:50:49.51 RMet:1E000000001F0000000022002300240E
```

```
17:50:49.59 GR:04T:06
```

```
17:50:49.60 RMet:1D0006351B0036BE00373C0038AF003900003A00003B14003C  
00003D03003E00003F0000402B12410415422324
```

```
>>END TEST 20001<<
```

```
>>START TEST 20002<<
```

```
17:51:08.59 I:40007C034401010101010101010101000000000000000000010100  
0000000000000000000101000000000000000000000001010000000000000000  
10100000000000000000002340101FF01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  
FFFFFFFFFFFFFFFFFFFF0A
```

```
17:51:08.96 EEst:00
```

```
17:51:08.96 EEd:0101FF01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  
FFFF7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

```
17:51:09.07 EEa:01010101010101010101010000000000000000000101000000000  
000000000001010000000000000000000101000000000000000000010100000  
0000000000000000
```

```
17:51:09.20 ACT:00 MI:00 MA:00
```

```
17:51:09.21 O:FEC00000
```

```
>>END TEST 20002<<
```

```

>>START TEST 20003<<
17:52:16.59 I:40003602340101FF01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FF0A141E40
17:52:16.76 EEst:00
17:52:16.76 EEd:0101FF01FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFF7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
17:52:16.87 ACT:00 MI:00 MA:00
17:52:16.89 O:FEC00000
>>END TEST 20003<<

>>START TEST 20004<<
17:52:38.43 I:0020000A141E40
17:52:38.45 ACT:00 MI:00 MA:00
17:52:38.46 O:FE800000
>>END TEST 20004<<

```

Interpreter realizuje zadania związane z automatyczną oceną wszystkich testów każdej sekwencji testowej w celu określenia, czy dany test dał w odpowiedzi prawidłowy wynik (T_PASS), czy też dał wynik nieprawidłowy (T_FAIL).

Interpretacja odbywa się po wczytaniu danych z pliku tekstowego lub pliku XML zawierającego odpowiednio oznaczone wyniki testów. Wyniki interpretacji zapisywane są w zwykłym pliku tekstowym lub pliku HTML.

Poniżej przedstawiony został wynik automatycznej interpretacji wyników testów dla wybranej sekwencji testowej dla jednej z konfiguracji.

```

SEKWENCJA TESTOWA: 20000

>>START TEST 20001<<
////////////////////////////////////
WŁĄCZENIE ZASILANIA                               ---> Test
////////////////////////////////////
0E --> Testowana wersja oprogramowania Modułu IO.
Konfiguracja: 06 03 00 01
Grupa 1: Licznik ciepła
Grupa 2: GRUPA WYŁĄCZONA
Grupa 3: Wejścia dodatkowe

```

Grupa 4: Regulator pogodowy

Odpytanie grupa 1:

dane w postaci heksadecymalnej

Odpytanie grupa 3:

dane w postaci heksadecymalnej

Odpytanie grupa 4:

dane w postaci heksadecymalnej

---> Wynik testu T_PASS (zostały odczytane dane po włączeniu zasilania)

>>END TEST 20001<< ---> T_PASS

(...)

>>START TEST 20005<<

Polecenie SPI: 00 22 00 0A 14 1E 40 ---> Test

Pobierz dane

Polecenie dotyczy grup: 1

Stan alarmów: ACT:00 MI:00 MA:00

---> Aktualny stan do analizy ---<

Informacje do interpretacji-----
Konfiguracja: 06 03 00 01

---> Analiza odpowiedzi i ocena wyniku testu ---<

Interpretacja odpowiedzi SPI

FE --> Wersja modułu IO

01 --> Identyfikator grupy danych

1 grupa, Licznik ciepła

1D --> 29 Typ miernika (0x01 + wersja softu CC) (uint, 2 bajty)

B2 01 --> 434

Ostatni RMet: B2 01 (434) --> Zgodne z ostatnim RMet --> T_PASS

04 --> 4 Energia (str5, 5 bajtów)

6B 15 00 00 FF --> 548,3

Ostatni RMet: 6B 15 00 00 FF (548,3) --> Zgodne z ostatnim RMet --> T_PASS

05 --> 5 Przepływ (str5, 5 bajtów)

FA A1 00 00 FF --> 4146,6

Ostatni RMet: FA A1 00 00 FF (4146,6) --> Zgodne z ostatnim RMet --> T_PASS

18 --> 24 Temperatura zasilania (uint, 2 bajty)

31 23 --> 9009

```

Ostatni RMet: 31 23 (9009) --> Zgodne z ostatnim RMet --> T_PASS
19 --> 25 Temperatura powrotu (uint, 2 bajty)

    F6 0A --> 2806
Ostatni RMet: F6 0A (2806) --> Zgodne z ostatnim RMet --> T_PASS
1A --> 26 Różnica temperatur (uint, 2 bajty)
    3B 18 --> 6203
Ostatni RMet: 3B 18 (6203) --> Zgodne z ostatnim RMet --> T_PASS
13 --> 19 Moc chwilowa (str3, 3 bajty)
    00 00 FF --> 0
Ostatni RMet: 00 00 FF (0) --> Zgodne z ostatnim RMet --> T_PASS
14 --> 20 Przepływ chwilowy (str3, 3 bajty)
    00 00 00 --> 0
Ostatni RMet: 00 00 00 (0) --> Zgodne z ostatnim RMet --> T_PASS
>>END TEST 20005<< --> T_PASS

```

---> Ocena uzyskanych wyników sekwencji testowej ---<

STATYSTYKA SEKWENCJI TESTOWEJ: 20000

Liczba wszystkich testów: 69

Liczba testów T_PASS: 69

Liczba testów T_FAIL: 0

Ocena sekwencji testowej: PASS

Symulator realizuje zadania związane z symulowaniem funkcjonalności wybranego licznika lub regulatora na poziomie obsługi interfejsu komunikacyjnego. Każdy moduł *Symulatora* musi poprawnie realizować protokół wymiany danych tak jak pomiędzy rzeczywistym urządzeniem a modułem I/O. Moduł I/O może jednocześnie obsługiwać zarówno prawdziwe urządzenia jak i ich symulatory.

6. Realizacja procesu diagnozowania elementów sieci telemetrycznej w środowisku symulacyjnym

Na bazie środowiska symulacyjnego można przeprowadzić testowanie elementów sieci przemysłowej. Dla potrzeb niniejszego artykułu został przedstawiony tylko fragment badań. Szczegółowy opis został zaprezentowany w publikacji [3].

Istotne z punktu widzenia efektywności i skuteczności realizowanych testów jest przyjęcie odpowiedniej strategii testowania. W założonym procesie testowym przyjęto przeprowadzanie testów dla wybranej grupy elementów systemu stanowiącej rdzeń testowania. Rdzeń testowania zawiera elementy newralgiczne sieci przemysłowej (systemu). Od poprawności działania tych elementów zależy poprawność działania pozostałych elementów systemu. Jako rdzeń testowania w testowanym systemie przyjęty zostaje moduł I/O.

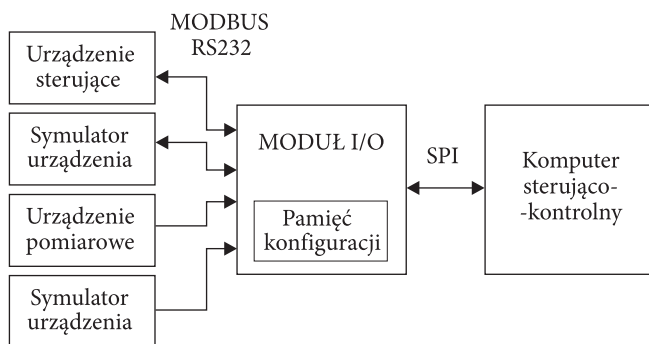
Proces generacji testów oparty został o założone klasy błędów, które mogą wystąpić w systemie. Dla badanego systemu określono następujące klasy błędów:

- odczytu grup i ich parametrów (odczyt pogrupowanych dla każdego urządzenia zestawów wartości wielkości mierzonych przez urządzenia, zapamiętanych i przetwarzanych w module I/O);
- odpytywania urządzeń (proces odczytywania przez modułu I/O wartości wielkości mierzonych przez urządzenia);
- identyfikacji alarmów (wykrywanie przekroczenia ustalonej wcześniej wartości minimalnej lub maksymalnej);
- interpretacja danych niedozwolonych (dopuszczalnych, ale niezgodnych z protokołami komunikacyjnymi);
- harmonogramów czasowych (wykonywanie odczytów urządzeń);
- zapisu danych (poleceń sterujących) do urządzeń sterujących.

Jako metodę testowania systemu wybrano metodę zapamiętanej odpowiedzi. Polega ona na zadawaniu wymuszeń dla testowanego układu i porównywaniu odpowiedzi układu z wartościami uznanymi za wzorcowe.

Testy na poziomie modułu wejścia-wyjścia mają za zadanie sprawdzenie poprawności działania rdzenia testowania, czyli samego modułu I/O. Schemat układu testowego przedstawiono na rysunku 4.

Taki układ testowy pozwala na odłączenie od modułu I/O wszystkich innych elementów systemu (w porównaniu z układem pracującym w rzeczywistych warunkach), które mogłyby powodować nieprawidłowe działanie modułu.



Rys. 4. Schemat układu testowego na poziomie modułu I/O

Dzięki temu na podstawie uzyskanych wyników testów możemy wnioskować, że stwierdzone błędy są generowane przez sam moduł I/O, a nie jakkolwiek inny element systemu.

Komputer sterująco-kontrolny wraz z oprogramowaniem diagnostycznym jest podłączony do modułu I/O poprzez przejściówkę RS232 do SPI. Zadaniem tego komputera jest zadawanie testów oraz weryfikacja reakcji układu na zadane testy. Weryfikacja otrzymanych wyników jest realizowana w sposób automatyczny lub półautomatyczny. Wstępnie uzyskane sekwencje wyjściowe są przetwarzane z rozbiciem na poszczególne wartości: parametrów oraz danych identyfikacyjnych przy pomocy opracowanego oprogramowania. Część wyników testów wymaga dodatkowo ręcznej interpretacji.

W przypadku stwierdzenia błędów w otrzymanej sekwencji wyjściowej test powodujący jej wygenerowanie jest powtarzany 10 razy w celu eliminacji błędów przypadkowych.

Dla przykładu przedstawiona została klasa błędów dotyczących identyfikacji błędów odczytu grup i ich parametrów. W tej klasie założono możliwość wystąpienia następujących błędów: odczyt innej grupy niż podana w zapytaniu (G_INNA), odczyt innego parametru dla grupy niż podany w zapytaniu (GP_INNY), niepoprawna interpretacja danej określonego typu (B_TYP). Opis sekwencji testowej dla tej klasy błędów przedstawiono w tabeli 1.

TABELA 1

Opis sekwencji testowej błędów odczytu grup i parametrów

Test	Wysłanie polecenia pobrania danych dla określonych w teście grup i konfiguracji parametrów w grupach dobranych tak, aby pozwalały na identyfikację założonych klas błędów: G_INNA, GP_INNY, B_TYP.
Wzorzec testowy	Określone dla każdego testu identyfikatory grup i konfiguracja parametrów dla każdej grupy.
Sposób weryfikacji wyniku	Porównanie uzyskanej odpowiedzi na polecenie pobrania danych z wzorcem testowym.
Możliwe oceny uzyskanych wyników testów	T_PASS — uzyskana odpowiedź na polecenie pobrania danych jest zgodna z wzorcem testowym. T_FAIL_G_INNA — w uzyskanej odpowiedzi są parametry z innej grupy niż określone we wzorcu testowym. T_FAIL_GP_INNY — w uzyskanej odpowiedzi są inne parametry dla co najmniej jednej z grup niż określone we wzorcu testowym. T_FAIL_B_TYP — w uzyskanej odpowiedzi jest co najmniej jeden parametr z dowolnej grupy złego typu.
Powtarzalność testu	Przeprowadzenie wielokrotnej operacji odczytu poszczególnych grup z założoną wartością testową.

cd. tabeli 1

Możliwe oceny uzyskanych wyników sekwencji testowej	PASS — wszystkie testy sekwencji testowej mają ocenę wyniku T_PASS FAIL_X — X% testów sekwencji testowej ma ocenę jednego z wyników T_FAIL, a (100-X)% testów ma ocenę wyniku T_PASS ERROR — wszystkie testy sekwencji testowej mają ocenę jednego z wyników T_FAIL.
---	--

Testy na poziomie systemu stanowią ostatni etap procesu testowania, mający na celu wykrycie błędów przesyłania danych przez sieć GSM (poprawność interpretacji pakietów) oraz zapisu odbieranych informacji w bazie danych. Przeprowadzane są wtedy, kiedy testy na poziomie modułu I/O wykażą prawidłowe działanie modułu. Dzięki temu na tym etapie możemy już przyjąć, że pojawiające się błędy nie będą błędami w działaniu samego modułu I/O, ale błędami spowodowanymi nieprawidłowym działaniem innych elementów sieci przemysłowej. Jednocześnie testy te pozwalają zbadać reakcję modułu I/O na błędy generowane poza nim. Newralgicznym elementem są tutaj urządzenia sterujące, bo błędy w procesie przekazywania do nich sygnałów sterujących mogą mieć bardzo duże konsekwencje.

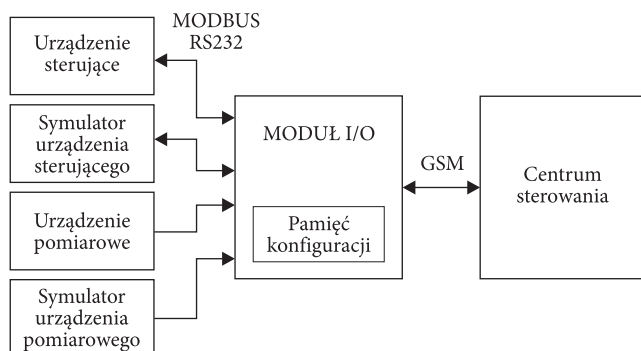
Na poziomie systemu przeprowadzane są testy z wykorzystaniem symulatora urządzenia sterującego lub pomiarowego, co pozwala na weryfikację danych przekazywanych do Centrum sterowania, jak również testy z wykorzystaniem urządzeń rzeczywistych dla weryfikacji zależności czasowych.

Istotnym elementem tego etapu testów jest weryfikacja poprawności generowania zapytań do urządzeń oraz generowania odpowiedzi przez urządzenia i przesyłania jej do Centrum sterującego z zapisem do bazy danych. Na tym etapie ważna jest weryfikacja założeń czasowych przyjętych w systemie dla realizacji audytu danych pochodzących z urządzeń pomiarowych. Schemat układu testowanego przedstawiono na rysunku 5.

Na poziomie systemu przeprowadzone są testy pozwalające na identyfikację założonych klas błędów z poziomu interfejsu Centrum sterowania. Zmianie ulega więc przede wszystkim sposób wykonywania testów dla poszczególnych sekwencji testowych.

Dla przykładu przedstawiona została klasa błędów dotyczących identyfikacji błędów na poziomie systemu zapisu do urządzenia sterującego (regulatora).

Zestaw testów dla tej sekwencji testowej został tak dobrany, aby umożliwił sprawdzenie z poziomu Centrum sterowania możliwości zapisu w regulatorze danych dozwolonych (wynikających ze skrajnych wartości danego parametru), jak również wartości dopuszczalnych (wynikających ze skrajnych wartości dla danego typu parametru). Opis sekwencji testowej na poziomie systemu dla tej klasy błędów przedstawiono w tabeli 2.



Rys. 5. Schemat układu testowego na poziomie systemu

TABELA 2

Opis sekwencji testowej na poziomie systemu błędów zapisu do urządzenia sterującego (regulatora)

Test	Zapis do regulatora z Centrum sterowania wartości parametrów z założonego przedziału wartości dopuszczalnych oraz wartości dozwolonych.
Wzorzec testowy	Wartość zapisana do regulatora.
Sposób weryfikacji wyniku	Porównanie wartości parametru uzyskanej po odpytaniu regulatora z wzorcem testowym.
Możliwe oceny uzyskanych wyników testów	T_PASS — wartość parametru uzyskana podczas odpytania regulatora jest zgodna z wzorcem testowym. T_FAIL — wartość parametru uzyskana podczas odpytania regulatora nie jest zgodna z wzorcem testowym.
Powtarzalność testu	Przeprowadzenie wielokrotnej operacji zapisu do regulatora różnych wartości testowych sterowanej z Centrum sterowania.
Możliwe oceny uzyskanych wyników sekwencji testowej	PASS — wszystkie testy sekwencji testowej mają ocenę wyniku T_PASS FAIL_X — X% testów sekwencji testowej ma ocenę wyniku T_FAIL, a (100-X)% testów ma ocenę wyniku T_PASS ERROR — wszystkie testy sekwencji testowej mają ocenę wyniku T_FAIL.

Testy na poziomie systemu umożliwiają zastosowanie obydwu metod diagnozowania: opiniowania diagnostycznego i dialogu diagnostycznego. Dzięki temu, mając tylko środowisko symulacyjne rzeczywistej sieci telemetrycznej, poprzez odpowiednie połączenie wielu modułów I/O, możemy testować sieć, korzystając z całej wiedzy dotyczącej diagnostyki systemowej.

7. Podsumowanie

Niniejszy artykuł porusza problematykę realizacji procesu symulacyjnego testowania elementów sieci telemetrycznych z zastosowaniem metod diagnostyki systemowej. Obszar rozwoju przemysłu teleinformatycznego zajmujący się zastosowaniem diagnostyki systemowej do diagnozowania sieci przemysłowych zaczyna się cieszyć w ostatnich latach coraz większą popularnością. Niniejszy artykuł łącznie z innymi publikacjami dotyczącymi m.in. ochrony informacji i obiektów w połączonych sieciach przemysłowych i teleinformatycznych przedstawia fragment prac zainicjowanych w Instytucie Teleinformatyki i Automatyki WAT z zakresu technik diagnostyki systemowej.

Zaprezentowane w artykule rozwiązanie stanowi rozwinięcie podstaw teoretycznych metod diagnostyki systemowej sieci teleinformatycznych oraz sieci mikroprocesorowych i zastosowanie ich dla potrzeb diagnostyki sieci przemysłowych. Realizacja pracy pozwoliła na weryfikację wspomnianych założeń teoretycznych w praktyce.

Stworzone środowisko symulacyjne dla testowania elementów sieci telemetrycznych pozwala w łatwy i tani sposób przetestować nowo projektowane elementy sieci telemetrycznej w pierwszych etapach projektowania nowego systemu rzeczywistego, a także przy rozszerzaniu funkcjonalności już istniejącej sieci. Środowisko to umożliwia przeprowadzanie testów nie tylko na etapie konstrukcyjnym, ale także na etapie produkcyjnym.

Następnie może ono zostać wykorzystane w szczególności do sprawdzenia każdego elementu systemu telemetrycznego przed jego zainstalowaniem w rzeczywistym systemie.

Zastosowaniem środowiska jest też badanie nowych metod diagnostyki, a także zastosowanie środowiska w dydaktyce. Wykorzystując stworzone środowisko symulacyjne i pracując nad dalszym jego rozwojem, można testować różne moduły współpracujące z całą gamą przeróżnych mierników, czujników i urządzeń sterujących.

Sieci telemetryczne znajdują coraz większe zastosowanie nie tylko w przemyśle, ale także w wojsku w obszarze bezpieczeństwa narodowego (sieciocentryczność). Stąd też niezawodność działania i bezpieczeństwo tych sieci jest niezwykle newralgicznym problemem.

Kierunki dalszych prac będą zmierzały między innymi do opracowania narzędzia programowego wspierającego proces generacji testów oraz testowania elementów sieci telemetrycznej przy zastosowaniu strategii on-line. Pozwoli to na zmniejszenie kosztów tego procesu, zwłaszcza że testowane elementy mogą być rozmieszczone na dużym obszarze. Strategia on-line zapewni także możliwość wcześniejszego wykrywania niezdatności elementów sieci telemetrycznej — co umożliwi ich wcześniejszą naprawę lub wymianę — zanim zostanie wykryta niezdatność sieci telemetrycznej podczas realizacji jej podstawowych (niezwiązanych z diagnostyką) funkcji.

Artykuł wpłynął do redakcji 14.12.2009 r. Zweryfikowaną wersję po recenzji otrzymano w grudniu 2010 r.

LITERATURA

- [1] J. CHUDZIKIEWICZ, *Sieci komputerowe o strukturze logicznej typu hipersześcianu*, Instytut Automatyki i Robotyki, Wydział Cybernetyki WAT, Warszawa, 2002.
- [2] J. CHUDZIKIEWICZ, Z. ZIELIŃSKI, *Wyznaczanie m-diagnozowalnych struktur typu PMC w systemach o zwiększonej odporności na uszkodzenia*, Materiały X Konferencji SCR' 2003, Ustroń, 15-18 września 2003.
- [3] J. CHUDZIKIEWICZ, W. SULEJ, *Diagnozowanie elementów sieci przemysłowych*, Biuletyn Instytut Automatyki i Robotyki, Wydział Cybernetyki WAT, 25, 2008.
- [4] S. CHUTANI, J.-D. DECOTIGNE, *A Perspective on Fault Diagnosis of Industrial Communication Networks*, IEEE International Workshop, 4-6 Oct 1995, 91-96.
- [5] H. KRAWCZYK, *Analiza i synteza samo diagnozowalnych systemów komputerowych*, Zeszyty Naukowe Politechniki Gdańskiej, Elektronika, 64, Gdańsk, 1987.
- [6] J. M. KOŚCIELNY, M. SYFERT, P. WNUK, *System zaawansowanego monitorowania i diagnostyki procesów przemysłowych AMandD*, Diagnostyka, 3, 39, 2006.
- [7] J. M. KOŚCIELNY, *Diagnostyka zautomatyzowanych procesów przemysłowych*, wyd. I, Akademicka Oficyna Wydawnicza EXIT, 2001.
- [8] J. KORBICZ, J. M. KOŚCIELNY, Z. KOWALCZUK, W. CHOLEWA, *Diagnostyka procesów. Modele. Metody sztucznej inteligencji. Zastosowania*, WNT, Warszawa, 2002.
- [9] R. KULESZA, *Podstawy diagnostyki sieci logicznych i komputerowych*, wyd. II, Instytut Automatyki i Robotyki, Wydział Cybernetyki WAT, Warszawa, 2000.
- [10] R. KULESZA, *Niektóre własności grafów opiniowania diagnostycznego*, Materiały z Krajowego Kongresu Metrologii KKM'98, Gdańsk, t. 5, 15-18.09.1998, 81-88.
- [11] R. S. WILLIAM, W. JOHN, *System Test and Diagnosis*, Kluwer Academic Publishers, Norwell, MA, 1994.
- [12] Z. ZIELIŃSKI, *Model symulacyjny procedur diagnostycznych w rozproszonych systemach sieciowych*, Diagnostyka, 3, 39, 2006.
- [13] Y. J. WON, MI-JUNG CHOI, J. W. K. HONG, et al., *Fault Detection and Diagnosis in IP-Based Mission Critical Industrial Process Control Networks*, 46, May 2008, 172-180.
- [14] Z. SUSKI, W. SULEJ, *Mechanizmy typu fault tolerance w multimedialnym systemie konferencyjnym STIAR*, Biuletyn Instytut Automatyki i Robotyki, Wydział Cybernetyki WAT, 14, 2000.

W. SULEJ, J. CHUDZIKIEWICZ

The simulation environment for testing elements of telemetry networks

Abstract. This paper describes the implementation of a process of simulation testing elements of telemetry networks on the basis of system diagnostics methods. A project of telemetry networks to diagnostics researches was presented. Moreover, fundamental theory of system diagnostics, theoretical basis of the process tests generation, a model set of tests, worked out for the examined network and a way of interpretation of get results are given.

Keywords: system diagnostics, telemetry networks, testing methods industrial control systems, communication standards