

# Diagnozowanie elementów sieci przemysłowych

**Jan CHUDZIKIEWICZ**

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,  
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa

**Wojciech SULEJ**

Zakład Automatyki, Instytut Teleinformatyki i Automatyki WAT,  
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa

**STRESZCZENIE:** W artykule przedstawiono sposób realizacji procesu diagnozowania elementów sieci przemysłowej. Przedstawiono przykłady standardów komunikacyjnych wykorzystywanych w sieciach przemysłowych. Przedstawiono podstawy teoretyczne procesu generacji testów. Zaprezentowano przykładowy zbiór testów, opracowany dla badanej sieci oraz sposób interpretacji uzyskanych wyników.

**SŁOWA KLUCZOWE:** metody testowania, sieci przemysłowe, sieci telemetryczne, standardy komunikacyjne.

## 1. Wstęp

W niniejszym artykule przedstawiono częściowe wyniki badań prowadzonych w Instytucie Teleinformatyki i Automatyki m.in. w ramach grantu KBN<sup>1</sup>: „Techniki diagnostyki systemowej w ocenie i poprawianiu stanu bezpieczeństwa sieci teleinformatycznych i mikroprocesorowych”.

Problematyka diagnozowania procesów przemysłowych – w tym również

---

<sup>1</sup> Praca naukowa finansowana ze środków na naukę w latach 2008-2011 jako projekt badawczy nr O N514 051135

sieci przemysłowych – jest szeroko analizowana w literaturze światowej.

Znana autorom artykułu literatura, z wybranego zakresu tematycznego, porusza problem diagnozowania, czy to elementów sieci przemysłowych, czy też procesów przemysłowych. Problematyka diagnozowania procesów przemysłowych jest szczegółowo zaprezentowana w publikacji [9]. Autor tej publikacji porusza zagadnienia diagnozowania procesów przemysłowych z uwzględnieniem wymogów nakładanych na systemy czasu rzeczywistego.

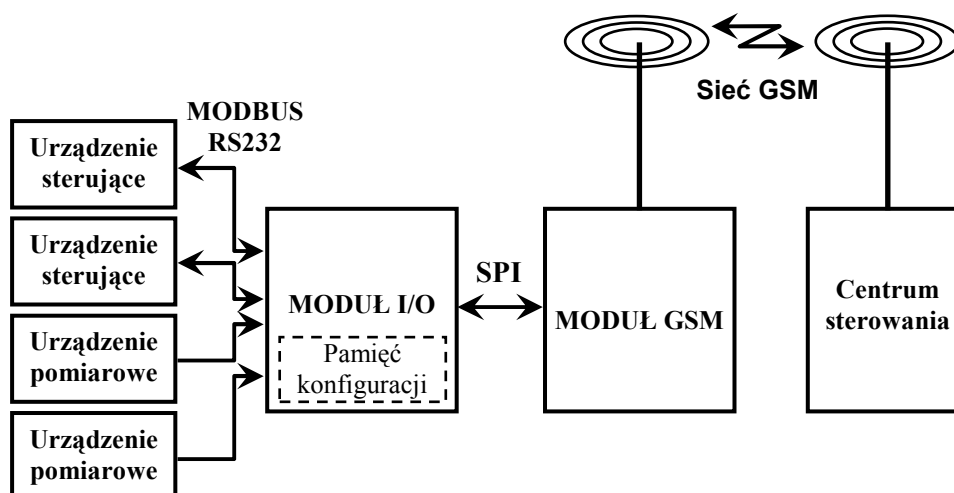
Inne podejście zostało zaprezentowane w pracy [10], gdzie Autorzy przedstawiają rozwiązanie bazujące na wykrywaniu uszkodzeń w elementach komunikacyjnych sieci przemysłowych. Realizacja procesu wykrywania uszkodzeń bazuje na metodach i technikach diagnostyki systemowej. Autorzy proponują wykorzystanie do diagnostyki, między innymi protokołu SNMP.

Podobnie w pracy [11] poruszana jest problematyka detekcji oraz diagnozowania błędów w sieciach przemysłowych bazujących na standardzie Ethernet. Autorzy przedstawiają modele błędów, które mogą być zaimplementowane w tego typu rozwiązaniach.

Jak można zaobserwować problematyka diagnozowania poszczególnych elementów sieci przemysłowych traktowana jest rozłącznie. Istotnym 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.

Zrealizowana część badań dotyczyła opracowania zestawu testów oraz przeprowadzenia na ich bazie procesu testowania opracowanego w Instytucie modelu systemu telemetrycznego (sieci telemetrycznej). Opracowany 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 miała być weryfikacja poprawności działania modułu wejścia-wyjścia tego systemu (moduł I/O z rysunku 1). 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.



Rys. 1. Schemat blokowy testowanego systemu

W założeniu system powinien współpracować z urządzeniami pomiarowymi i urządzeniami sterującymi różnych typów. Stąd też opracowany zestaw testów powinien pozwolić na sprawdzenie poprawności pracy modułu I/O w różnych konfiguracjach. W artykule zaprezentowano wyniki uzyskane dla jednej z konfiguracji, w której do modułu 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 diagnostowania zależy silnie od właściwości wykorzystywanych w systemie interfejsów komunikacyjnych, stąd też zostały one bardziej szczegółowo opisane w punkcie 2.

Realizacja procesu diagnostowania elementów sieci przemysłowej zgodnie z opracowaną i zaproponowaną przez autorów artykułu metodyką została przedstawiona w punkcie 3. W rozdziale tym przedstawiono opisy: sekwencji testowych, sposobu generacji testów i procesu testowania dla wspomnianej wcześniej konfiguracji oraz przykładowe wyniki testów.

## 2. Wybrane standardy komunikacyjne dla sieci przemysłowych

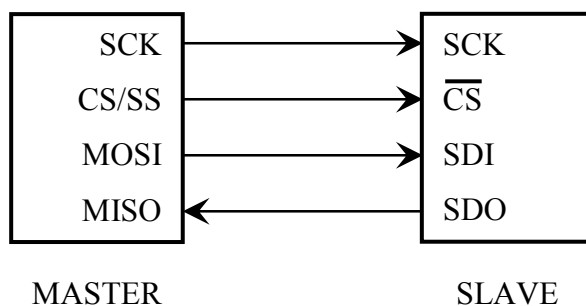
W punkcie przedstawiono standardy komunikacyjne wykorzystywane do połączenia pomiędzy współpracującymi elementami sieci przemysłowych. Ograniczono się do dwóch standardów, a mianowicie SPI oraz MODBUS. Przedstawione standardy zostały wykorzystane do komunikacji w badanym systemie. Producenci sprzętu sterująco-pomiarowego wykorzystują również własne standardy komunikacyjne. Nie są one jednak przedstawiane w artykule ze względu na ograniczenia narzucane przez producentów.

### 2.1. Standard SPI

SPI jest czteroprzewodowym, dwukierunkowym, synchronicznym interfejsem szeregowym wykorzystywanym do komunikacji pomiędzy układem kontrolera a układami wykonawczymi. Opracowany przez firmę Motorola dla mikroprocesorów rodziny MC68HCxx, obecnie jest implementowany w wielu układach mikrokontrolerów.

Z założenia w systemie wykorzystującym interfejs SPI może występować jeden układ kontrolera i jeden lub kilka układów wykonawczych. Transmisję na szynie inicjuje i zarządza nią układ kontrolera. Transmisja może być realizowana w dwóch kierunkach jednocześnie. Szybkość transmisji zależy od sygnału zegara, generowanego przez układ kontrolera i wynosi 1-bit danych w jednym takcie zegara.

Standard wymaga dwóch linii sterujących SCK oraz CS i dwóch linii danych SDI oraz SDO. Sposób połączenia układów przedstawiono na rysunku 2.



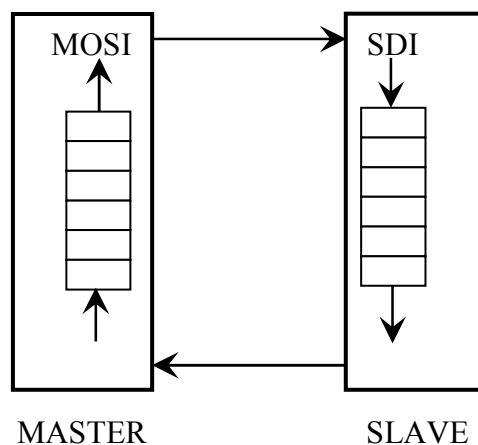
Rys. 2. Linie interfejsu SPI [4]

Znaczenie poszczególnych linii jest następujące:

- SCK (*ang. Serial Clock*) – linia zegara systemowego;
- CS/SS (*ang. Chip Select/Slave Select*) – linia wyboru układu wykonawczego;
- MOSI/SDI (*ang. Master Output Slave Input/Serial Data In*) – linia danych przesyłanych od układu kontrolera do układu wykonawczego;
- MISO/SDO (*ang. Master Input Slave Output/Serial Data Out*) – linia danych przesyłanych od układu wykonawczego do układu kontrolera.

Wybór układu wykonawczego realizowany jest za pomocą linii CS. Linia ta jest aktywna poziomem niskim. W niektórych kontrolerach jest dedykowane wyjście wyboru układu oznaczane jako Slave Select. Układ wykonawczy, który nie jest wybrany ma ustawione wyjście SDO w stan wysokiej impedancji.

Wewnątrz układy kontrolera i wykonawczy mają wbudowane szeregowo rejestry przesuwne. Sposób podłączenia rejestrów przesuwnych do linii sygnałowych przedstawia rysunek 3.

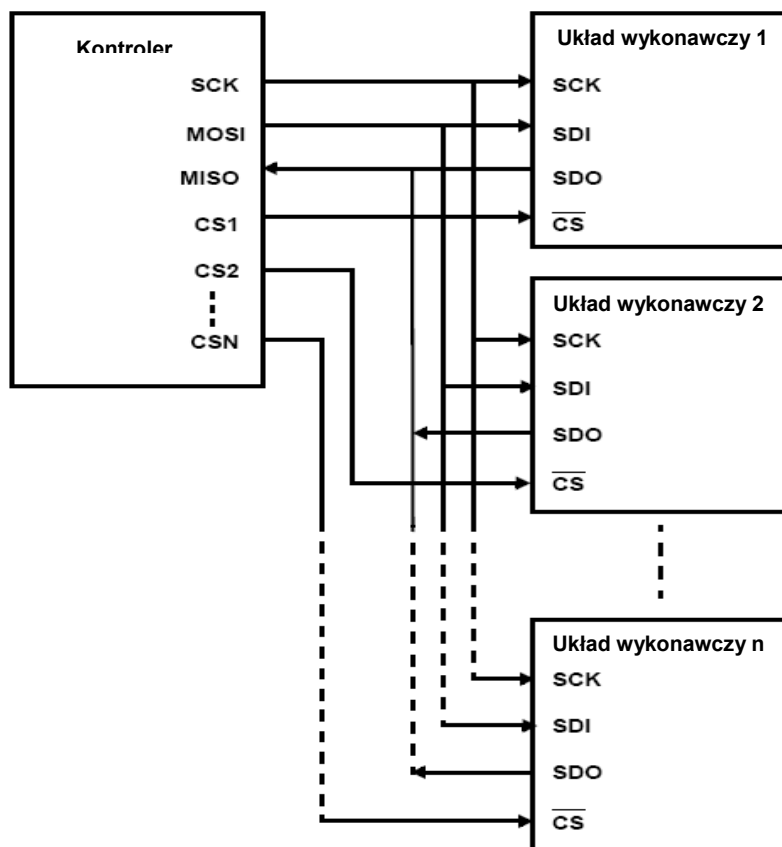


Rys. 3. Przesyłanie danych za pomocą interfejsu SPI [4]

Transmisja danych rozpoczyna się po ich wprowadzeniu do rejestru przesuwne przez układ kontrolera. W przypadku, gdy transmisja ma być dwukierunkowa układ wykonawczy powinien umieścić dane w swoim rejestrze przesuwne. Po zainicjowaniu transmisji układy współpracujące odpowiednio: pobierają bity z wejść MISO oraz SDI, przesyłając jednocześnie wartości z rejestrów na wyjścia MOSI oraz SDO.

W przypadku, gdy w systemie będzie występować więcej niż jeden układ wykonawczy, mogą one pracować w jednej z dwóch konfiguracji. Wybór konfiguracji zależny jest od układów wykonawczych.

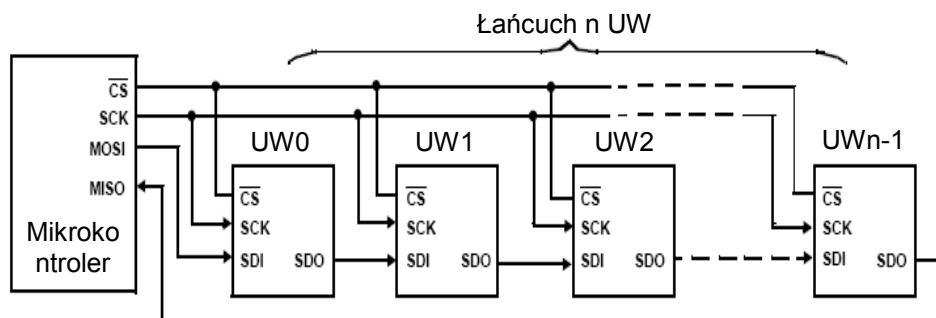
Na rysunku 4 przedstawiono przykład jednej z tych konfiguracji, która określana jest mianem równoległej. W tej konfiguracji wyjścia układu kontrolera: SCK łączone jest do wejść zegarowych, natomiast MOSI łączone jest do wejść SDI wszystkich układów wykonawczych w sposób równoległy.



Rys. 4. Przykład konfiguracji równoległej dla systemu bazującego na interfejsie SPI [3]

Podobnie podłączane jest wejście MISO do wyjść SDO wszystkich układów wykonawczych. Zgodnie z założeniami wybór układu realizowany jest poprzez sygnał CS, stąd też w tej konfiguracji układ kontrolera musi być podłączony do poszczególnych wejść CS układów wykonawczych niezależnie.

Drugą z konfiguracji, w której mogą pracować układy wykorzystujące interfejs SPI jest – przedstawiona na rysunku 5 – konfiguracja typu łańcuch (ang. *Daisy Chain*).



Rys. 5. Przykład konfiguracji typu łańcuch dla systemu bazującego na interfejsie SPI [3]

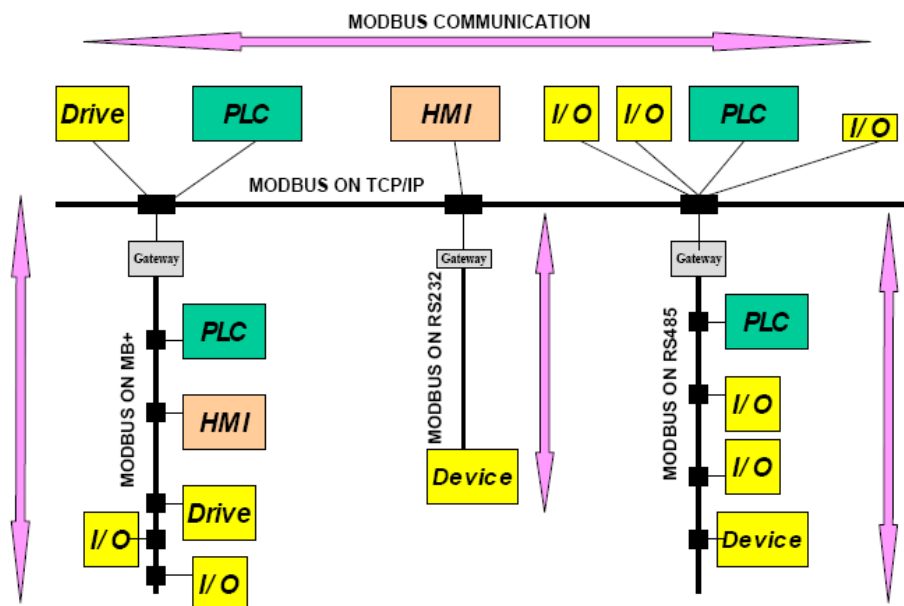
W tej konfiguracji wyjścia CS oraz SCK układu kontrolera podłączone są w sposób równoległy do odpowiadających im wejść układów wykonawczych. Wyjście MOSI układu kontrolera podłączone jest do wejścia SDI pierwszego w łańcuchu układu wykonawczego. Wejście MISO podłączone jest do wyjścia SDO ostatniego w łańcuchu układu wykonawczego. Wyjście SDO układu wykonawczego podłączone jest do wejścia SDI kolejnego układu. Zaletą tej konfiguracji jest uproszczenie sposobu połączenia poszczególnych układów wykonawczych poprzez ograniczenie liczby linii przesyłu danych. Wadą natomiast jest wymuszenie jednoczesnej realizacji przez wszystkie układy wykonawcze operacji zapisu lub odczytu.

Można przyjąć założenie, że wszystkie układy w łańcuchu są elementami szeregowego rejestru przesuwanego, w którym dane muszą przejść przez poszczególne układy. Układ sterujący wprowadza ciągi bitów rozpoczynając od przeznaczonych dla ostatniego układu w łańcuchu.

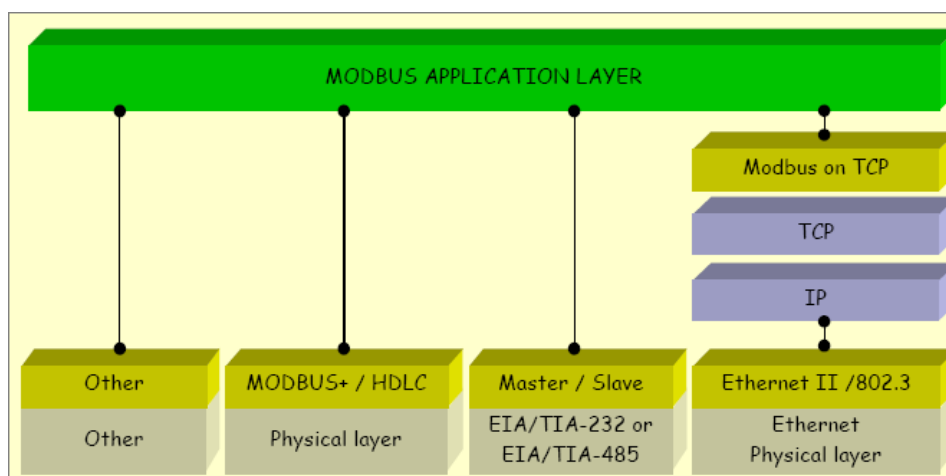
## 2.2. Standard MODBUS

MODBUS jest opracowanym przez firmę Modicon – zorientowanym na transmisję bajtową – protokołem dla transmisji szeregowej. Został opracowany dla zapewnienia prostego sposobu wymiany danych pomiędzy sterownikiem, a układem wykonawczym przy wykorzystaniu interfejsu RS232. Za standard przemysłowy został uznany w 1979 roku. W komunikacji pomiędzy układem sterującym a układami wykonawczymi wykorzystywany jest model klient-serwer. Obecnie jest implementowany na wielu mediach

transmisyjnych, włączając standard Ethernet (patrz rysunek 6), gdzie pracuje na poziomie warstwy aplikacji (7 warstwa modelu ISO/OSI) (patrz rysunek 7).



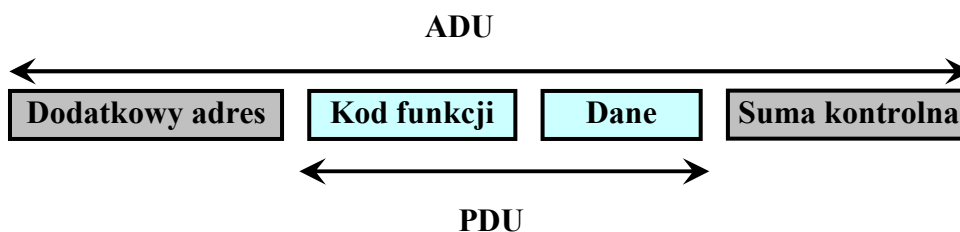
Rys. 6. Przykłady architektur wykorzystujących protokół MODBUS [2]



Rys. 7. Umieszczenie protokołu MODBUS w stosie protokołów [2]



Postać ramki protokołu – PDU (*ang. Protocol Data Unit*) – przedstawia rysunek 8. Mapowanie protokołu MODBUS na specyficzne media transmisyjne może wymagać wprowadzenia dodatkowych pól. Powoduje to wbudowanie ramki protokołu MODBUS (PDU) w ramkę lub pakiet danej sieci. Na rysunku 8 oznaczono ten przypadek jako ADU (*ang. Application Data Unit*).



Rys. 8. Ramka protokołu MODBUS [2]

Ramka ADU jest tworzona przez klienta, który inicjuje transmisję, natomiast jej postać jest zgodna ze specyfikacją dla wykorzystywanego medium transmisyjnego. Rozmiar ramki PDU jest efektem przyjętych założeń konstrukcyjnych dla pierwszej implementacji protokołu bazującej na standardzie RS485. Dla RS485 rozmiar ADU wynosi 256 bajtów. Przyjmując dla pola adresu 1-bajt oraz 2-bajty dla pola sumy kontrolnej, na ramkę PDU pozostaje 253 bajty.

Pole – Kod funkcji – jest polem 1-bajtowym, określającym rodzaj operacji, jaka ma zostać wykonana. Dopuszczalny przedział wartości dla tego pola wynosi od 1 do 255, przy czym wartości z zakresu od 128 do 255 są zarezerwowane dla obsługi wyjątków. Niektóre funkcje mogą być złożone (zawierać podfunkcje), wówczas w polu danych pojawia się kod funkcji dodatkowej.

Pole – Dane – w przypadku przesyłania wiadomości od klienta do serwera, zawiera dodatkowe informacje niezbędne do wykonania przez serwer określonej funkcji. Może to być, np. adres rejestru lub liczba bajtów danych, które powinien przesłać w odpowiedzi. Dla niektórych funkcji pole to jest zbędne i wówczas, w wiadomości przesyłanej do serwera, ma ono długość zero bajtów. W przypadku, gdy obsługa żądania przebiegnie bez błędów pole to zawiera (w wiadomości przesyłanej od serwera do klienta) wymagane dane. Jeżeli natomiast wystąpi błąd obsługi danego żądania, to w polu tym zwrótnie przekazywany jest jego kod.

Informacja o sposobie zakończenia obsługi żądania przekazywana jest w polu – Kod funkcji. Jeżeli obsługa żądania zakończy się powodzeniem, pole to zawiera kod operacji, którą serwer miał zrealizować. W przypadku, gdy obsługa żądania zakończy się niepowodzeniem pole to zawiera pierwotny kod funkcji z ustawionym najbardziej znaczącym bitem na 1.

Pole – Suma kontrolna – zawiera wartość umożliwiającą weryfikację poprawności przesyłanych w ramce danych. Proces weryfikacji może być realizowany z wykorzystaniem dwóch metod: kontroli parzystości oraz kontroli na poziomie ramki. Kontrola parzystości (lub nieparzystości) może być zastosowana do każdego przesyłanego znaku. Kontrola integralności danych na poziomie ramki może być zrealizowana poprzez zastosowanie metod: LRC (*ang. Longitudinal Redundancy Check*) lub CRC (*ang. Cyclic Redundancy Check*) [2].

Standardowo protokół MODBUS implementowany jest w rozwiązaniach opartych o RS232. W takim systemie występuje układ sterujący (*ang. Master*) oraz układ wykonawczy (*ang. Slave*). Układ sterujący pełni rolę klienta, natomiast układ wykonawczy – serwera. Protokół daje możliwość przesłania żądania do pojedynczego układu wykonawczego lub do grupy układów. W przypadku rozsyłania grupowego pole adresu jest ustawiane na wartość 0.

W przypadku pracy bazującej na RS232 układ sterujący może pracować w jednym z dwóch trybów: ASCII oraz RTU (*ang. Remote Terminal Unit*) [1]. Wybór trybu pracy określany jest w momencie programowania układów. W przypadku trybu ASCII każdy bajt jest przesyłany jako dwa znaki ASCII. Zaletą tego rozwiązania jest możliwość przesyłania znaków z opróżnieniami przekraczającymi 1 sekundę, bez powodowania błędów. Jest to szczególnie istotne w przypadku wolnych układów. W przypadku trybu RTU każdy bajt przysłany jest jako dwie wartości szesnastkowe. Transmisja musi być realizowana jako ciągły strumień danych, dlatego też realizowana jest ona szybciej niż w przypadku trybu ASCII.

W protokół została wbudowana seria funkcji diagnostycznych. Pozwalają one na przetestowanie komunikacji pomiędzy układem sterującym oraz układami wykonawczymi oraz sprawdzenie błędów wewnętrznych generowanych przez układy wykonawcze. Funkcje te nie obsługują transmisji grupowej. Funkcje diagnostyczne inicjowane są poprzez podanie w polu – Kod funkcji – wartości 08 hex. Wykorzystują one dwubajtowe kody podfunkcji, które określają rodzaj testów. Układ wykonawczy w odpowiedzi na żądanie diagnostyczne przesyła zwrótnie echo całej ramki. Przy pomocy tych funkcji nie ma możliwości uruchomienia w układzie wykonawczym programu użytkownika.

### 3. Realizacja procesu diagnozowania elementów sieci przemysłowej

Istotnym 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 w systemie mogą wystąpić. Dla badanego systemu zostały określone następujące klasy błędów:

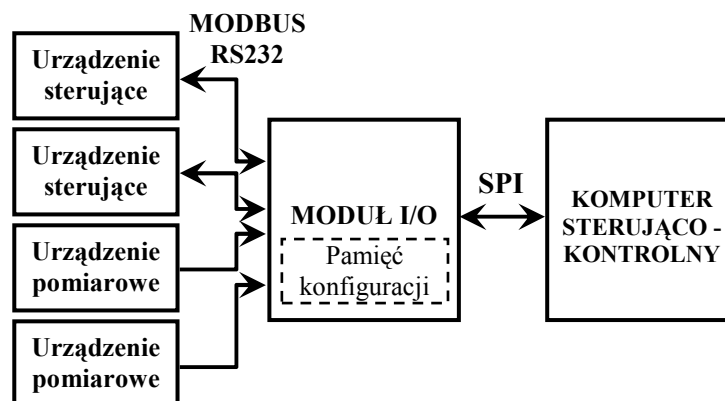
- odczytu grup i ich parametrów (odczyt pogrupowanych dla każdego urządzenia zestawu wartości wielkości mierzonych przez urządzenia, zapamiętanych i przetwarzanych w module I/O);
- odpytywania urządzeń (proces odczytywania przez modułu I/O wartości wielkości mierzonych przez urządzenia);
- identyfikacji 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 metodą zapamiętanej odpowiedzi. Metoda ta polega na zadawaniu wymuszeń dla testowanego układu i porównywanie odpowiedzi układu z wartościami uznanymi za wzorcowe.

#### 3.1. Testy na poziomie modułu wejścia-wyjścia

Testy na tym poziomie mają za zadanie sprawdzenie poprawności działania rdzenia testowania, czyli samego modułu I/O. Schemat układu testowego przedstawiono na rysunku 9.

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. 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.



Rys. 9. Schemat układu testowego

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 rozbiem 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. W dalszej części tego punktu przedstawiono sekwencje testowe dla założonych klas błędów.

### 3.1.1. Identyfikacja 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.

Tab. 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.
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

### 3.1.2. Identyfikacja błędów odpytywania urządzeń

Testy identyfikujące błędy tej klasy opierają się na inicjowaniu sekwencji odczytu danych z urządzeń poprzez: reset urządzenia oraz wymuszenie odczytu za pomocą impulsów taktujących, jak również poprzez wywołanie odpowiedniej komendy diagnostycznej. Opis sekwencji testowej dla tej klasy błędów przedstawiono w tabeli 2.

Tab. 2. Opis sekwencji testowej odpytywania urządzeń

Test	Wymuszanie odpytywań urządzeń.
Wzorzec testowy	Zestaw rzeczywistych wartości parametrów odczytanych z ekranu urządzenia lub ustawionych w symulatorze urządzenia.
Sposób weryfikacji wyniku	Porównanie zestawu wartości parametrów uzyskanego podczas odpytania urządzeń z wzorcem testowym.
Możliwe oceny uzyskanych wyników testów	T_PASS – zestaw wartości parametrów uzyskany podczas odpytania urządzeń jest zgodny z wzorcem testowym. T_FAIL – zestaw wartości parametrów uzyskany podczas odpytania urządzeń nie jest zgodny z wzorcem testowym.
Powtarzalność testu	Przeprowadzenie wielokrotnej operacji inicjowania urządzeń, wymuszania impulsów taktujących i ponawiania polecenia diagnostycznego.
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.

### 3.1.3. Identyfikacja błędów identyfikacji alarmów

Sekwencja testowa dla tej klasy błędów obejmuje ustawienie każdego z 5-ciu mogących wystąpić alarmów, dla parametrów różnych typów (7 typów parametrów), które mogą wystąpić w danej konfiguracji. Dla wartości wzorcowych zmieniane będą zakresy przedziałów alarmowych tak, aby sprawdzić sygnalizację alarmu dla wszystkich możliwych kombinacji ustawień. Klasa błędów obejmuje błędy typu: brak sygnalizacji alarmu przy jego wystąpieniu (A\_BRAK\_MIN, A\_BRAK\_MAX), sygnalizacji alarmu przy poprawnych danych (A\_ZLE\_MIN, A\_ZLE\_MAX). Opis sekwencji testowej dla tej klasy błędów przedstawiono w tabeli 3.

Tab. 3. Opis sekwencji testowej błędów identyfikacji alarmów

Test	Modyfikacja zakresów alarmów oraz ustawianie wartości w zakresie lub poza zakresami alarmów dla różnych typów danych. Testy zostaną tak dobrane, aby istniała możliwość identyfikacji założonych klas błędów: A_BRAK_MIN, A_BRAK_MAX, A_ZLE_MIN, A_ZLE_MAX.
Wzorzec testowy	Określone dla każdego testu konfiguracje poszczególnych alarmów.
Sposób weryfikacji wyniku	Analiza bitów odpowiedzi informujących o zaistnieniu alarmu.
Możliwe oceny uzyskanych wyników testów	<p>T_PASS – w uzyskanej odpowiedzi jest informacja o zaistnieniu alarmu i powinna ona być lub nie ma informacji o zaistnieniu alarmu i nie powinno jej być.</p> <p>T_FAIL_A_BRAK_MIN – w uzyskanej odpowiedzi nie ma informacji o zaistnieniu alarmu przekroczenia wartości minimalnej, a powinna ona być.</p> <p>T_FAIL_A_BRAK_MAX – w uzyskanej odpowiedzi nie ma informacji o zaistnieniu alarmu przekroczenia wartości maksymalnej, a powinna ona być.</p> <p>T_FAIL_A_ZLE_MIN – w uzyskanej odpowiedzi jest informacja o zaistnieniu alarmu przekroczenia wartości minimalnej, a nie powinno jej być.</p> <p>T_FAIL_A_ZLE_MAX – w uzyskanej odpowiedzi jest informacja o zaistnieniu alarmu przekroczenia wartości maksymalnej, a nie powinno jej być.</p>
Powtarzalność testu	Przeprowadzenie wielokrotnej operacji ustawiania alarmów.
Możliwe oceny uzyskanych wyników sekwencji testowej	<p>PASS – wszystkie testy sekwencji testowej mają ocenę wyniku T_PASS.</p> <p>FAIL_X – X% testów sekwencji testowej ma ocenę jednego z wyników T_FAIL, a (100-X)% testów ma ocenę wyniku T_PASS.</p> <p>ERROR – wszystkie testy sekwencji testowej mają ocenę jednego z wyników T_FAIL.</p>

### 3.1.4. Identyfikacja błędów interpretacji przez system danych niedozwolonych

Sekwencja testowa dla tej klasy błędów ma za zadanie weryfikację reakcji systemu na niepoprawne formaty przesyłanych ramek. Zgodnie z założeniem system powinien odrzucić tego typu ramki. Opis sekwencji testowej dla tej klasy błędów przedstawiono w tabeli 4.

**Tab. 4. Opis sekwencji testowej błędów interpretacji przez system danych niedozwolonych**

Test	Naprzemienne wygenerowanie ramki niedozwolonej i ramki poprawnej przez symulator urządzenia oraz komputer kontrolno-sterujący.
Wzorzec testowy	Zmodyfikowana wartość ramki poprawnej.
Sposób weryfikacji wyniku	Sprawdzenie czy system odpowiedział, gdy wysłane do niego polecenie miało postać ramki niedozwolonej oraz sprawdzenie czy dane przesyłane za pomocą ramki niepoprawnej zostały zaakceptowane przez system. Następnie sprawdzenie czy system zaakceptował kolejne polecenie mające już postać ramki poprawnej.
Możliwe oceny uzyskanych wyników testów	T_PASS – odpowiedź układu jest prawidłowa (zignorowanie ramki niepoprawnej i odpowiedź na ramkę poprawną). T_FAIL – odpowiedź układu jest nieprawidłowa (odpowiedź na ramkę niepoprawną lub przyjęcie danych z ramki niepoprawnej oraz brak odpowiedzi na ramkę poprawną).
Powtarzalność testu	Przeprowadzenie wielokrotnej operacji zapisu danych oraz wielokrotnej operacji pobrania danych z modułu I/O przy pomocy kolejnych ramek niedozwolonych.
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.



### 3.1.5. Identyfikacja błędów harmonogramów czasowych

Sekwencja testowa dla tej klasy błędów ma za zadanie sprawdzenie poprawności działania zegara systemowego. Dla weryfikacji harmonogramów czasowych przyjęto następujące przedziały czasowe: 15, 30, 45 minut. Opis sekwencji testowej dla tej klasy błędów przedstawiono w tabeli 5.

Tab. 5. Opis sekwencji testowej błędów harmonogramów czasowych

Test	Automatyczne odpytywanie urządzeń zgodnie z harmonogramem czasowym określonym w konfiguracji dla każdej grupy.
Wzorzec testowy	Określona dla każdego testu konfiguracja harmonogramów odpytywania dla każdej grupy.
Sposób weryfikacji wyniku	Interpretacja uzyskanych sygnatur czasowych odpytywania urządzeń na podstawie wzorca testowego.
Możliwe oceny uzyskanych wyników testów	T_PASS – z interpretacji sygnatur czasowych odpytywania urządzeń na podstawie wzorca testowego wynika prawidłowa realizacja harmonogramu. T_FAIL – z interpretacji sygnatur czasowych odpytywania urządzeń na podstawie wzorca testowego wynika nieprawidłowa realizacja harmonogramu.
Powtarzalność testu	Kolejne automatyczne odpytywanie urządzeń zgodnie z różnymi harmonogramami czasowymi określonymi w konfiguracji dla różnych grup.
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.

### 3.1.6. Identyfikacja błędów zapisu danych do urządzenia sterującego (regulatora)

Zestaw testów dla tej sekwencji testowej został tak dobrany, aby umożliwił sprawdzenie możliwości zapisu do urządzenia sterującego danych dozwolonych (wynikających ze skrajnych wartości danego parametru), jak również wartości dopuszczalnych (wynikających ze skrajnych wartości dla danego typu parametru). Opis sekwencji testowej dla tej klasy błędów przedstawiono w tabeli 6.

Tab. 6. Opis sekwencji testowej błędów zapisu danych do urządzenia sterującego (regulatora)

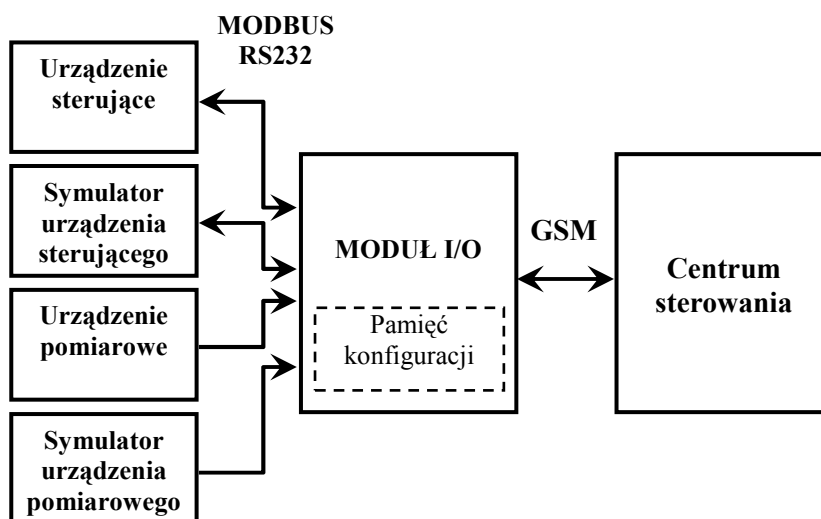
Test	Zapis do regulatora wartości parametrów z założonego przedziału wartości dopuszczalnych oraz wartości dozwolonych.
Wzorzec testowy	Wartość zapisana do regulatora.
Sposób weryfikacji wyniku	Porównanie wartości parametru uzyskanej po odpytaniu regulatora z wzorcem testowym.
Możliwe oceny uzyskanych 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.
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.

### 3.2. Testy na poziomie systemu

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 wykazują 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 10.



Rys. 10. Schemat układu testowego

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. W dalszej części tego punktu przedstawiono sekwencje testowe na poziomie systemu dla założonych klas błędów.

### 3.2.1. Identyfikacja na poziomie systemu 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 na poziomie systemu dla tej klasy błędów przedstawiono w tabeli 7.

Tab. 7. Opis sekwencji testowej na poziomie systemu błędów odczytu grup i parametrów

Test	Wysłanie polecenia z Centrum sterowania 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 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 na żądanie 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 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.

### 3.2.2. Identyfikacja na poziomie systemu błędów identyfikacji alarmów

Sekwencja testowa na poziomie systemu dla tej klasy błędów obejmuje ustawienie i przesłanie z Centrum sterowania każdego z 5-ciu mogących wystąpić alarmów, dla parametrów różnych typów (7 typów parametrów), które mogą wystąpić w danej konfiguracji. Dla wartości wzorcowych zmieniane będą zakresy przedziałów alarmowych tak, aby sprawdzić sygnalizację alarmu dla wszystkich możliwych kombinacji ustawień. Klasa błędów obejmuje błędy typu: brak sygnalizacji alarmu przy jego wystąpieniu (A\_BRAK\_MIN, A\_BRAK\_MAX), sygnalizacji alarmu przy poprawnych danych (A\_ZLE\_MIN, A\_ZLE\_MAX). Opis sekwencji testowej na poziomie systemu dla tej klasy błędów przedstawiono w tabeli 8.

**Tab. 8. Opis sekwencji testowej na poziomie systemu błędów identyfikacji alarmów**

Test	Modyfikacja zakresów alarmów oraz ustawianie wartości w zakresie lub poza zakresami alarmów dla różnych typów danych. Testy zostaną tak dobrane, aby istniała możliwość identyfikacji założonych klas błędów: A_BRAK_MIN, A_BRAK_MAX, A_ZLE_MIN, A_ZLE_MAX.
Wzorzec testowy	Określone dla każdego testu konfiguracje poszczególnych alarmów.
Sposób weryfikacji wyniku	Analiza odpowiedzi informującej o zaistnieniu alarmu.
Możliwe oceny uzyskanych wyników testów	T_PASS – w uzyskanej odpowiedzi jest informacja o zaistnieniu alarmu i powinna ona być lub nie ma informacji o zaistnieniu alarmu i nie powinno jej być. T_FAIL_A_BRAK_MIN (_MAX) – w uzyskanej odpowiedzi nie ma informacji o zaistnieniu alarmu przekroczenia wartości minimalnej (maksymalnej), a powinna ona być. T_FAIL_A_ZLE_MIN (_MAX) – w uzyskanej odpowiedzi jest informacja o zaistnieniu alarmu przekroczenia wartości minimalnej (maksymalnej), a nie powinno jej być.
Powtarzalność testu	Przeprowadzenie wielokrotnej operacji ustawiania alarmów sterowanej z Centrum sterowania.
Możliwe oceny uzyskanych wyników sekwencji testowej	PASS – wszystkie testy sekwencji 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

### 3.2.3. Identyfikacja 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 9.

Tab. 9. 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.

### 3.3. Przykładowe wyniki testów

Do przeprowadzenia testów zostało stworzone specjalne oprogramowanie diagnostyczne składające się w szczególności z Testera i Interpretera testów.

Zadaniem Testera jest przesyłanie 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.

Natomiast zadaniem Interpretera testów jest automatyczna ocena 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 zawierającego odpowiednio oznaczone wyniki testów. Wyniki interpretacji zapisywane są w zwykłym pliku tekstowym lub pliku HTML. Poniżej dla kilku sekwencji testowych opisanych w punkcie poprzednim przedstawione są fragmenty plików z wynikami testów i ich interpretacją.

#### 3.3.1. Identyfikacja błędów odczytu grup i ich parametrów

```
SEKWENCJA TESTOWA: 20000
>>START TEST 20001<<

////////////////////////////////////
WŁĄCZENIE ZASILANIA                               ---> Test
IO-Ext - moduł z obsługą regulatorów pogodowych
////////////////////////////////////

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 2005<<  
  
Polecenie SPI: 00 22 00 0A 14 1E 40    ---> Test  
Pobierz dane  
Polecenie dotyczy grup: 1  
  
Stan alarmów: ACT:00 MI:00 MA:00        ---> I odpowiedź na test  
  
        ---> Aktualny stan do analizy ---<  
  
-----  
Informacje do interpretacji  
-----  
  
Konfiguracja: 06 03 00 01  
  
Konfiguracja parametrów w grupach:  
Grupa 1: Parametry: dane w postaci heksadecymalnej  
Grupa 2: Parametry: dane w postaci heksadecymalnej  
Grupa 3: Parametry: dane w postaci heksadecymalnej  
Grupa 4: Parametry: dane w postaci heksadecymalnej  
  
        ---> Analiza odpowiedzi i ocena wyniku testu ---<  
  
*****  
Interpretacja stanu alarmów  
*****  
  
00 --> Informacja o zmianie stanu alarmu  
  
        0000 0000  1 na danej pozycji oznacza zmianę stanu alarmu z tej  
                pozycji, np. wystąpiło przekroczenie lub powrót do  
                sytuacji normalnej  
  
        0 --> nieużywany  
        0 --> nieużywany  
        0 --> nieużywany  
        0 --> stan alarmu 5  
  
        0 --> stan alarmu 4  
        0 --> stan alarmu 3  
        0 --> stan alarmu 2  
        0 --> stan alarmu 1  
  
00 --> Informacja o aktualnie aktywnych przekroczeniach alarmów na  
        wartościach minimalnych  
  
        0000 0000  1 na danej pozycji oznacza, że monitorowana przez ten  
                alarm wartość jest poniżej MIN  
  
        0 --> nieużywany  
        0 --> nieużywany  
        0 --> nieużywany  
        0 --> stan alarmu 5          NIEAKTYWNY --> T_PASS
```



```

0 --> stan alarmu 4      NIEAKTYWNY --> T_PASS
0 --> stan alarmu 3      NIEAKTYWNY --> T_PASS
0 --> stan alarmu 2      NIEAKTYWNY --> T_PASS
0 --> stan alarmu 1      NIEAKTYWNY --> T_PASS

00 --> Informacja o aktualnie aktywnych przekroczeniach alarmów na
      wartościach maksymalnych

      0000 0000 1 na danej pozycji oznacza, że monitorowana przez ten
      alarm wartość jest powyżej MAX

0 --> nieużywany
0 --> nieużywany
0 --> nieużywany
0 --> stan alarmu 5      NIEAKTYWNY --> T_PASS

0 --> stan alarmu 4      NIEAKTYWNY --> T_PASS
0 --> stan alarmu 3      NIEAKTYWNY --> T_PASS
0 --> stan alarmu 2      NIEAKTYWNY --> T_PASS
0 --> stan alarmu 1      NIEAKTYWNY --> T_PASS

////////////////////////////////////
////////////////////////////////////

Odpowiedź SPI: FE 80 62 4E 01 7F 14 35 18 30 01 1D B2 01 2F 00 00 05 10 85
24 10 F1 3A 01 00 0C 00 00 00 0D 00 00 00 04 6B 15 00 00 FF 05 FA A1
00 00 FF 09 23 37 00 00 18 31 23 19 F6 0A 1A 3B 18 13 00 00 FF 14 00 00 00
15 00 00 FF 30 00 00 0E 0A 14 1E 40

      ---> II odpowiedź na test

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

-----
Informacje do interpretacji
-----

Konfiguracja: 06 03 00 01

Konfiguracja parametrów w grupach:
Grupa 1: Parametry: dane w postaci heksadecymalnej
Grupa 2: Parametry: dane w postaci heksadecymalnej
Grupa 3: Parametry: dane w postaci heksadecymalnej
Grupa 4: Parametry: dane w postaci heksadecymalnej

Ostatni RMet grupa 1:
1D B2 01 2F 00 00 05 10 85 24 10 F1 3A 01 00 0C 00 00 00 00 0D 00 00 00 00
04 6B 15 00 00 FF 05 FA A1 00 00 FF 09 23 37 00 00 18 31 23 19 F6 0A 1A 3B
18 13 00 00 FF 14 00 00 00 15 00 00 FF 30 00 00

Ostatni RMet grupa 3:
1E 00 00 00 00 1F 00 00 00 00 22 00 23 00 24 0E

Ostatni RMet grupa 4:
1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14 00 3C
00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24

Prawidłowa kolejność grup w odpowiedzi: 01

```

```
---> Analiza odpowiedzi i ocena wyniku testu ---<
*****
Interpretacja odpowiedzi SPI
*****

FE --> Wersja płytki IO

80 --> Identyfikator danych

      1000 0000

      1 --> zawsze 1
      0 --> zaktualizowano konfigurację płytki IO
            (CONFIG IO, CONFIG DATA, CONFIG ALARMS)
      0 --> zaktualizowano konfigurację części komunikacyjnej
            (CONFIG COM)
      0 --> wykryto alarm, w ramce są dane o alarmie
            (rozpoczęcie lub zakończenie alarmu)

      0 --> nieużywany
      0 --> nieużywany
      0 --> nieużywany
      0 --> nieużywany

62 --> Identyfikator grupy/akcji

      0110 0010

      0 --> dane zaktualizowane (wysłano dane niezaktualizowane
            i rozpoczęto proces ich aktualizacji)
      1 --> alarmy sprawdzone (nastąpiła weryfikacja wystąpienia
            stanów alarmowych dla wszystkich grup danych)
      1 --> dane pobrane (dołączone są wszystkie dane z grup
            określonych poniżej jako odpowiedź na zapytanie)
      0 --> w ramce są wszystkie dane określone w EEPROM z grupy 4

      0 --> w ramce są wszystkie dane określone w EEPROM z grupy 3
      0 --> w ramce są wszystkie dane określone w EEPROM z grupy 2
      1 --> w ramce są wszystkie dane określone w EEPROM z grupy 1
      0 --> w ramce są dane z grupy 0

4E --> Długość danych od następnego bajtu do końca ramki w bajtach
      (78 bajtów)

01 --> Identyfikator grupy danych

      1 grupa, Licznik ciepła

7F --> Identyfikator CRC i konfiguracji

      14 35

      18 30 01 --> 06 03 00 01 --> Konfiguracja zgodna --> T_PASS
```

```
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
2F --> 47 Numer seryjny (bcd, 6 bajtów)
      00 00 05 10 85 24 --> 000005108524
      Ostatni RMet: 00 00 05 10 85 24 (000005108524) -->
      Zgodne z ostatnim RMet --> T_PASS
10 --> 16 Data (ulong, 4 bajty)
      F1 3A 01 00 --> 80625
      Ostatni RMet: F1 3A 01 00 (80625) -->
      Zgodne z ostatnim RMet --> T_PASS
0C --> 12 Dodatkowe wejście impulsowe In-A (ulong, 4 bajty)
      00 00 00 00 --> 0
      Ostatni RMet: 00 00 00 00 (0) -->
      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
15 --> 21 Moc szczytowa (str3, 3 bajty)
      00 00 FF --> 0
      Ostatni RMet: 00 00 FF (0) --> Zgodne z ostatnim RMet --> T_PASS
30 --> 48 Info code (error) (uint, 2 bajty)
      00 00 --> 0 --> Praca prawidłowa.
      Ostatni RMet: 00 00 (0) --> Zgodne z ostatnim RMet --> T_PASS
0E --> Identyfikator czasu (czas ostatniego odczytu urządzenia)
      0A 14 1E 40
>>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
-----
-----
```

### 3.3.2. Identyfikacja błędów odpytywania urządzeń

```

SEKWENCJA TESTOWA: 10000
>>START TEST 10001<<

////////////////////////////////////
WŁĄCZENIE ZASILANIA                               ---> Test
IO-Ext - moduł z obsługą regulatorów pogodowych
////////////////////////////////////

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

                ---> Odpowiedź na test ---<

RMet: 1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14
00 3C 00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24

                ---> Spodziewany wynik testu (wzorzec) ---<

Wzorzec:
1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14 00 3C
00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24

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

*****
Interpretacja i porównanie z wzorcem
*****

1D --> 29 Typ miernika (uint, 2 bajty)

    00 06 --> 1536

    Wzorzec: 00 06 (1536) --> Zgodne z wzorcem. --> T_PASS

35 --> 53 Temperatura zewnętrzna (int, 2 bajty)

    1B 00 --> 27

    Wzorzec: 1B 00 (27) --> Zgodne z wzorcem. --> T_PASS
    
```

```
36 --> 54 Temperatura zasilania CO (int, 2 bajty)
      BE 00 --> 190
      Wzorzec: BE 00 (190) --> Zgodne z wzorcem. --> T_PASS
37 --> 55 Temperatura powrotu CO (int, 2 bajty)
      3C 00 --> 60
      Wzorzec: 3C 00 (60) --> Zgodne z wzorcem. --> T_PASS
38 --> 56 Temperatura CWU (int, 2 bajty)
      AF 00 --> 175
      Wzorzec: AF 00 (175) --> Zgodne z wzorcem. --> T_PASS
39 --> 57 Ciśnienie zasilania WP (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
3A --> 58 Ciśnienie powrotu WP (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
3B --> 59 Ciśnienie zładu (int, 2 bajty)
      14 00 --> 20
      Wzorzec: 14 00 (20) --> Zgodne z wzorcem. --> T_PASS
3C --> 60 Temperatura CO wyliczana przez regulator (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
3D --> 61 Położenie siłownika CO (int, 2 bajty)
      03 00 --> 3
      Wzorzec: 03 00 (3) --> Zgodne z wzorcem. --> T_PASS
3E --> 62 Położenie siłownika CWU (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
3F --> 63 REZERWOWY (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
```

```

40 --> 64 Słowo stanu (int, 2 bajty)
      2B 12 --> 4651
      Wzorzec: 2B 12 (4651) --> Zgodne z wzorcem. --> T_PASS
41 --> 65 Temperatura zadana CWU (int, 2 bajty)
      04 15 --> 5380
      Wzorzec: 04 15 (5380) --> Zgodne z wzorcem. --> T_PASS
42 --> 66 Przesunięcie krzywej grzania (int, 2 bajty)
      23 24 --> 9251
      Wzorzec: 23 24 (9251) --> Zgodne z wzorcem. --> T_PASS
*****
>>END TEST 10001<< --> T_PASS
(...)
>>START TEST 10017<<
Polecenie SPI: 82                               ---> Test
Polecenie protokołu serwisowego
0x02 - uruchom test podłączonych liczników

      ---> Odpowiedź na test ---<

Odpowiedź SPI: 55

////////////////////////////////////
////////////////////////////////////

Odpytanie grupa 1:
      dane w postaci heksadecymalnej

Odpytanie grupa 3:
      dane w postaci heksadecymalnej

Odpytanie grupa 4:
      dane w postaci heksadecymalnej

RMet: 1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14
00 3C 00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24

      ---> Spodziewany wynik testu (wzorzec) ---<

Wzorzec:
1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14 00 3C
00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24
    
```

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

*****
Interpretacja i porównanie z wzorcem
*****

1D --> 29 Typ miernika (uint, 2 bajty)
      00 06 --> 1536
      Wzorzec: 00 06 (1536) --> Zgodne z wzorcem. --> T_PASS

35 --> 53 Temperatura zewnętrzna (int, 2 bajty)
      1B 00 --> 27
      Wzorzec: 1B 00 (27) --> Zgodne z wzorcem. --> T_PASS

36 --> 54 Temperatura zasilania CO (int, 2 bajty)
      BE 00 --> 190
      Wzorzec: BE 00 (190) --> Zgodne z wzorcem. --> T_PASS

37 --> 55 Temperatura powrotu CO (int, 2 bajty)
      3C 00 --> 60
      Wzorzec: 3C 00 (60) --> Zgodne z wzorcem. --> T_PASS

38 --> 56 Temperatura CWU (int, 2 bajty)
      AF 00 --> 175
      Wzorzec: AF 00 (175) --> Zgodne z wzorcem. --> T_PASS

3B --> 59 Ciśnienie zładu (int, 2 bajty)
      14 00 --> 20
      Wzorzec: 14 00 (20) --> Zgodne z wzorcem. --> T_PASS

3C --> 60 Temperatura CO wyliczana przez regulator (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS

3D --> 61 Położenie siłownika CO (int, 2 bajty)
      03 00 --> 3
      Wzorzec: 03 00 (3) --> Zgodne z wzorcem. --> T_PASS
```



```
3E --> 62 Położenie siłownika CWU (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
3F --> 63 REZERWOWY (int, 2 bajty)
      00 00 --> 0
      Wzorzec: 00 00 (0) --> Zgodne z wzorcem. --> T_PASS
40 --> 64 Słowo stanu (int, 2 bajty)
      2B 12 --> 4651
      Wzorzec: 2B 12 (4651) --> Zgodne z wzorcem. --> T_PASS
41 --> 65 Temperatura zadana CWU (int, 2 bajty)
      04 15 --> 5380
      Wzorzec: 04 15 (5380) --> Zgodne z wzorcem. --> T_PASS
42 --> 66 Przesunięcie krzywej grzania (int, 2 bajty)
      23 24 --> 9251
      Wzorzec: 23 24 (9251) --> Zgodne z wzorcem. --> T_PASS
>>END TEST 10017<< --> T_PASS
```

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

```
-----
-----
STATYSTYKA SEKWENCJI TESTOWEJ: 10000
Liczba wszystkich testów: 17
Liczba testów T_PASS: 17
Liczba testów T_FAIL: 0
Ocena sekwencji testowej: PASS
-----
```

### 3.3.3. Identyfikacja błędów identyfikacji alarmów

```
SEKWENCJA TESTOWA: 30000
>>START TEST 30001<<

////////////////////////////////////
WŁĄCZENIE ZASILANIA                               ---> Test
IO-Ext - moduł z obsługą regulatorów pogodowych
////////////////////////////////////

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 30001<< --> T PASS

(...)
>>START TEST 30007<<

                               ---> Test ---<

Polecenie SPI: 40 00 46 03 44 01 01 01 01 01 01 01 01 01 C4 41 44 16 00 00 00
70 17 00 00 00 C4 41 94 11 00 00 00 70 17 00 00 00 C4 41 04 15 00 00 00 7C
15 00 00 00 C4 41 94 11 00 00 00 04 15 00 00 00 C4 41 04 15 00 00 00 04 15
00 00 00 0A 14 1E 40
Zmiana konfiguracji płytki IO
CONFIG ALARMS - dane konfiguracyjne progów alarmowych i częstotliwości
sprawdzania ich przekroczenia.
01 01 01 01 01 01 01 01 01 C4 41 44 16 00 00 00 70 17 00 00 00 C4 41 94 11 00
00 00 70 17 00 00 00 C4 41 04 15 00 00 00 7C 15 00 00 00 C4 41 94 11 00 00
00 04 15 00 00 00 C4 41 04 15 00 00 00 04 15 00 00 00

Status zapisu do EEPROM: (00) IO_UPDATE_OK --> Zapis ukończony
powodzeniem.

Stan alarmów: ACT:17 MI:01 MA:00           ---> I odpowiedź na test
```

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

-----  
Informacje do interpretacji  
-----

Konfiguracja: 06 03 00 01

Konfiguracja parametrów w grupach:

Grupa 1: Parametry: dane w postaci heksadecymalnej

Grupa 2: Parametry: dane w postaci heksadecymalnej

Grupa 3: Parametry: dane w postaci heksadecymalnej

Grupa 4: Parametry: dane w postaci heksadecymalnej

Ostatni RMet grupa 1:

1D B2 01 2F 00 00 05 10 85 24 10 F1 3A 01 00 0C 00 00 00 00 0D 00 00 00 00  
04 6B 15 00 00 FF 05 FA A1 00 00 FF 09 25 37 00 00 18 32 23 19 F7 0A 1A 3B  
18 13 00 00 FF 14 00 00 00 15 00 00 FF 30 00 00

Ostatni RMet grupa 3:

1E 00 00 00 00 1F 00 00 00 00 22 00 23 00 24 0E

Ostatni RMet grupa 4:

1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14 00 3C  
00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24

Konfiguracja alarmów:

Alarm 1: Grupa: 4, Parametr monitorowany: 41 (65), Wartość MIN: 44 16 00  
00 00 (5700), Wartość MAX: 70 17 00 00 00 (6000)

Alarm 2: Grupa: 4, Parametr monitorowany: 41 (65), Wartość MIN: 94 11 00  
00 00 (4500), Wartość MAX: 70 17 00 00 00 (6000)

Alarm 3: Grupa: 4, Parametr monitorowany: 41 (65), Wartość MIN: 04 15 00  
00 00 (5380), Wartość MAX: 7C 15 00 00 00 (5500)

Alarm 4: Grupa: 4, Parametr monitorowany: 41 (65), Wartość MIN: 94 11 00  
00 00 (4500), Wartość MAX: 04 15 00 00 00 (5380)

Alarm 5: Grupa: 4, Parametr monitorowany: 41 (65), Wartość MIN: 04 15 00  
00 00 (5380), Wartość MAX: 04 15 00 00 00 (5380)

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

\*\*\*\*\*  
Interpretacja stanu alarmów  
\*\*\*\*\*

17 --> Informacja o zmianie stanu alarmu

0001 0111 1 na danej pozycji oznacza zmianę stanu alarmu z tej  
pozycji, np. wystąpiło przekroczenie lub powrót do  
sytuacji normalnej

0 --> nieużywany

0 --> nieużywany

0 --> nieużywany

1 --> stan alarmu 5

```
0 --> stan alarmu 4
1 --> stan alarmu 3
1 --> stan alarmu 2
1 --> stan alarmu 1

01 --> Informacja o aktualnie aktywnych przekroczeniach alarmów na
wartościach minimalnych

0000 0001 1 na danej pozycji oznacza, że monitorowana przez ten
alarm wartość jest poniżej MIN

0 --> nieużywany
0 --> nieużywany
0 --> nieużywany
0 --> stan alarmu 5      Parametr 41: 5380 = MIN: 5380
                        --> T_PASS
0 --> stan alarmu 4      Parametr 41: 5380 > MIN: 4500
                        --> T_PASS
0 --> stan alarmu 3      Parametr 41: 5380 = MIN: 5380
                        --> T_PASS
0 --> stan alarmu 2      Parametr 41: 5380 > MIN: 4500
                        --> T_PASS
1 --> stan alarmu 1      Parametr 41: 5380 < MIN: 5700
                        --> T_PASS

00 --> Informacja o aktualnie aktywnych przekroczeniach alarmów na
wartościach maksymalnych

0000 0000 1 na danej pozycji oznacza, że monitorowana przez ten
alarm wartość jest powyżej MAX

0 --> nieużywany
0 --> nieużywany
0 --> nieużywany
0 --> stan alarmu 5      Parametr 41: 5380 = MAX: 5380
                        --> T_PASS
0 --> stan alarmu 4      Parametr 41: 5380 = MAX: 5380
                        --> T_PASS
0 --> stan alarmu 3      Parametr 41: 5380 < MAX: 5500
                        --> T_PASS
0 --> stan alarmu 2      Parametr 41: 5380 < MAX: 6000
                        --> T_PASS
0 --> stan alarmu 1      Parametr 41: 5380 < MAX: 6000
                        --> T_PASS

////////////////////////////////////
////////////////////////////////////

Odpowiedź SPI: FE D0 40 0F 04 7F A2 F4 18 30 01 41 04 15 0E 00 00 00 00

                        ---> II odpowiedź na test
```

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

-----
Informacje do interpretacji
-----

Konfiguracja: 06 03 00 01

Konfiguracja parametrów w grupach:
Grupa 1: Parametry: dane w postaci heksadecymalnej
Grupa 2: Parametry: dane w postaci heksadecymalnej
Grupa 3: Parametry: dane w postaci heksadecymalnej
Grupa 4: Parametry: dane w postaci heksadecymalnej

Ostatni RMet grupa 1:
1D B2 01 2F 00 00 05 10 85 24 10 F1 3A 01 00 0C 00 00 00 00 0D 00 00 00 00
04 6B 15 00 00 FF 05 FA A1 00 00 FF 09 25 37 00 00 18 32 23 19 F7 0A 1A 3B
18 13 00 00 FF 14 00 00 00 15 00 00 FF 30 00 00

Ostatni RMet grupa 3:
1E 00 00 00 00 1F 00 00 00 00 22 00 23 00 24 0E

Ostatni RMet grupa 4:
1D 00 06 35 1B 00 36 BE 00 37 3C 00 38 AF 00 39 00 00 3A 00 00 3B 14 00 3C
00 00 3D 03 00 3E 00 00 3F 00 00 40 2B 12 41 04 15 42 23 24

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

*****
Interpretacja odpowiedzi SPI
*****

FE --> Wersja płytki IO

D0 --> Identyfikator danych

    1101 0000

    1 --> zawsze 1
    1 --> zaktualizowano konfigurację płytki IO
        (CONFIG IO, CONFIG DATA, CONFIG ALARMS)
    0 --> zaktualizowano konfigurację części komunikacyjnej
        (CONFIG COM)
    1 --> wykryto alarm, w ramce są dane o alarmie
        (rozpoczęcie lub zakończenie alarmu)

    0 --> nieużywany
    0 --> nieużywany
    0 --> nieużywany
    0 --> nieużywany

40 --> Identyfikator grupy/akcji

    0100 0000

    0 --> dane zaktualizowane (wysłano dane niezaktualizowane
        i rozpoczęto proces ich aktualizacji)
```

```
1 --> alarmy sprawdzone (nastąpiła weryfikacja wystąpienia
      stanów alarmowych dla wszystkich grup danych)
0 --> dane pobrane (dołączone są wszystkie dane z grup
      określonych poniżej jako odpowiedź na zapytanie)
0 --> w ramce są wszystkie dane określone w EEPROM z grupy 4

0 --> w ramce są wszystkie dane określone w EEPROM z grupy 3
0 --> w ramce są wszystkie dane określone w EEPROM z grupy 2
0 --> w ramce są wszystkie dane określone w EEPROM z grupy 1
0 --> w ramce są dane z grupy 0

0F --> Długość danych od następnego bajtu do końca ramki w bajtach
      (15 bajtów)

(*****)
(*****)

04 --> Identyfikator grupy danych

      4 grupa, Regulator pogodowy

7F --> Identyfikator CRC i konfiguracji

      A2 F4

      18 30 01 --> 06 03 00 01 --> Konfiguracja zgodna --> T_PASS

41 --> 65 Temperatura zadana CWU (int, 2 bajty)

      04 15 --> 5380

      Ostatni RMet: 04 15 (5380) --> Zgodne z ostatnim RMet --> T_PASS

0E --> Identyfikator czasu (czas ostatniego odczytu urządzenia)

      00 00 00 00

>>END TEST 30007<< --> T PASS

(...)

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

-----
-----
STATYSTYKA SEKWENCJI TESTOWEJ: 30000

Liczba wszystkich testów: 11

Liczba testów T PASS: 11
Liczba testów T FAIL: 0

Ocena sekwencji testowej: PASS
-----
-----
```

#### 4. Podsumowanie

Niniejszy artykuł porusza problematykę diagnozowania sieci przemysłowych. Ten obszar rozwoju przemysłu teleinformatycznego zaczyna się cieszyć w ostatnich latach coraz większą popularnością. Artykuł łącznie z publikacją K. Lidermana – *Ochrona informacji i obiektów w połączonych sieciach przemysłowych i teleinformatycznych – przegląd zagadnień* – 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.

Zgodnie z zaproponowanym w artykule podejściem należy przyjąć odpowiednią strategię testowania. Strategia ta zakłada zainicjowanie procesu testowania od określenia newralgicznego elementu systemu zwanego *rdzeniem testowania*. Kolejnym krokiem jest określenie klas błędów, które mogą w systemie wystąpić. Określenie klas błędów – a co się z tym bezpośrednio wiąże ich modeli – zależne jest od poziomu, na którym będzie realizowany proces testowania. W badanej sieci proces testowania realizowany był na poziomie modułu I/O oraz całego systemu i miał za zadanie weryfikację działania systemu pod kątem poprawności realizowania przez niego założonych funkcji. W dalszej kolejności – dla założonych klas błędów – przeprowadza się proces generacji testów i następnie proces testowania.

Kierunki dalszych prac będą zmierzały między innymi do opracowania narzędzia programowego wspierającego proces: generacji testów oraz testowania elementów sieci przemysłowej stosując strategię 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 przemysłowej – co umożliwi ich wcześniejszą naprawę lub wymianę – zanim zostanie wykryta niezdatność sieci przemysłowej podczas realizacji jej podstawowych (niezwiązanych z diagnostyką) funkcji.

## Literatura

- [1] *Modicon: Modbus Protocol Reference Guide*, ([www.modbus-ida.com/docs/PI\\_MBUS\\_300.pdf](http://www.modbus-ida.com/docs/PI_MBUS_300.pdf)).
- [2] *Modbus Application Protocol Specification V1.1b*, ([www.modbus-ida.com/docs/Modbus\\_Application\\_Protocol\\_V1\\_1b.pdf](http://www.modbus-ida.com/docs/Modbus_Application_Protocol_V1_1b.pdf)).
- [3] *Intersil: SPI Protocol and Bus Configuration of Multiple DCPs, Application Note*, August 20, 2007 ([www.intersil.com/data/an/an1340.pdf](http://www.intersil.com/data/an/an1340.pdf)).
- [4] *Serial Peripheral Interface – SPI Bus overview*, (<http://www.scienceprog.com/serial-peripheral-interface-spi-bus-overview/>).
- [5] HASAN URAL, PROBERT R. L., VON BOCHMANN G., *Testing of Communicating Systems Tools and Techniques*, Kluwer Academic Publishers, Norwell, MA, 2000.
- [6] WILLIAM R. S., JOHN W., *System Test and Diagnosis*, Kluwer Academic Publishers, Norwell, MA, 1994.
- [7] SACHA K., *Sieci przemysłowe - Profibus*, Mikom, 1998.
- [8] LIDERMAN K., *Ochrona informacji i obiektów w połączonych sieciach przemysłowych i teleinformatycznych – przegląd zagadnień*, Biuletyn ITA, Nr 25, 2008.
- [9] KOŚCIELNY J. M., *Diagnostyka zautomatyzowanych procesów przemysłowych*, Akademicka Oficyna Wydawnicza EXIT, Wydanie 1, 2001.
- [10] CHUTANI, S.; DECOTIGNIE, J.-D., *A Perspective on Fault Diagnosis of Industrial Communication Networks*, *IEEE International Workshop*, Page(s):91 – 96, 4-6 Oct 1995.
- [11] WON Y.J., MI-JUNG CHOI, HONG J.W.-K., MYUNG-SUP KIM, HWAWON HWANG, JUN-HYUB LEE, SUNG-GYOO LEE, *Fault Detection and Diagnosis in IP-Based Mission Critical Industrial Process Control Networks*, Volume: 46, Page(s): 172-180, May 2008.



## **Fault diagnosis of elements of industrial control systems**

ABSTRACT: In the paper the method of process diagnosis of elements of industrial control systems was presented. More over in the paper was presented: examples of communications standards used in industrial control systems, 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.

KEY WORDS: testing methods industrial control systems, telemetry networks, communications standards.

*Praca wpłynęła do redakcji: 06.10.2008 r.*