



PROGRAM ROZWOJOWY POLITECHNIKI WARSZAWSKIEJ



Dokument:

SIECI PRZEMYSŁOWE I INTELIGENTNE URZĄDZENIA POLOWE

MATERIAŁY DO WYKŁADU

Wersja: 0.9

Data: 2010.12.05

Autor: Michał Bartyś



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓŁNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

SPIS TREŚCI

| | |
|--|----|
| 1. Wprowadzenie do systemów sieciowych..... | 6 |
| 1.1. Charakterystyka i klasyfikacja sieci | 6 |
| 1.2. Warstwowy model referencyjny sieci | 9 |
| 1.1.1. Warstwy niższe modelu ISO/OSI..... | 10 |
| 1.2.2. Warstwy wyższe modelu ISO/OSI | 12 |
| 1.3. Literatura | 13 |
| 2. Sieć analogowa 4-20mA | 14 |
| 2.1. Charakterystyka sieci analogowych..... | 14 |
| 2.2. Topologia sieci | 15 |
| 2.3. Wykorzystanie sieci analogowej 4-20mA do celów diagnostycznych | 17 |
| 2.4. Sieć analogowa 4-20mA w urządzeniach inteligentnych..... | 17 |
| 2.5. Właściwości analogowej sieci prądowej..... | 19 |
| 2.5.1. Odporność na zwarcia i rozwarcia sieci | 19 |
| 2.6. Ekonomia sieci analogowej..... | 24 |
| 3. Izkrobeszczeństwo urządzeń pomiarowych i wykonawczych | 27 |
| 3.1. Podstawowe definicje..... | 27 |
| 3.2. Strefy zagrożenia wybuchem | 28 |
| 3.3. Klasyfikacja urządzeń | 29 |
| 3.3.1. Grupy urządzeń | 29 |
| 3.3.2. Kategoria bezpieczeństwa urządzenia | 30 |
| 3.3.3. Klasyfikacja temperaturowa urządzeń..... | 31 |
| 3.3.4. Klasyfikacja urządzeń ze względu na pole powierzchni..... | 31 |
| 3.3.5. Oznakowanie urządzeń elektrycznych..... | 32 |
| 3.4. Obwody izkrobeszczeńcze | 34 |
| 3.4.1. Definicje | 34 |
| 3.4.2. Poziomy izkrobeszczeństwa urządzeń elektrycznych..... | 35 |
| 3.4.2.1. Poziom izkrobeszczeństwa „ia” | 35 |
| 3.4.2.2. Poziom izkrobeszczeństwa „ib” | 36 |
| 3.4.2.3. Poziom izkrobeszczeństwa „ic” | 36 |
| 3.4.3. Ocena warunków do powstania iskry..... | 36 |
| 3.4.3.1. Ocena warunków do powstania zapłonu w wyniku efektów cieplnych | 37 |
| 3.5. Przykłady oceny izkrobeszczeńności urządzeń..... | 38 |
| 3.5.1. Ocena nieuszkadzalności ścieżek na płytach obwodów drukowanych | 38 |
| 3.5.2. Ocena nieuszkadzalności zespołu diod w obwodzie izkrobeszcznym klasyfikowanym do grupy IIC na poziomie „ia” | 39 |
| 3.5.3. Ocena nieuszkadzalności rezystora w obwodzie izkrobeszcznym klasyfikowanym do grupy IIC na poziomie „ia” | 41 |
| 3.5.4. Ocena izkrobeszczeństwa w obwodzie izkrobeszcznym z pojemnością..... | 43 |
| 3.6. Literatura | 44 |
| 4. Diagnostyka urządzeń inteligentnych | 45 |
| 4.1. Wprowadzenie..... | 45 |
| 4.1.1. Pojęcia podstawowe | 46 |
| 4.1.2. Fazy wnioskowania diagnostycznego | 49 |
| 4.2. Diagnostyka typu <i>on-</i> i <i>off-line</i> | 49 |

| | | |
|--------|---|-----|
| 4.3. | Diagnostyka rozproszona..... | 51 |
| 4.3.1. | Detektory uszkodzeń | 52 |
| 4.3.2. | Sensory uszkodzeń..... | 54 |
| 4.3.3. | Analizatory uszkodzeń | 55 |
| 4.4. | Diagnostyka wbudowana..... | 56 |
| 4.5. | Tolerowanie uszkodzeń | 59 |
| 4.6. | Redundancja analityczna | 62 |
| 4.7. | Podsumowanie | 64 |
| 4.8. | Literatura | 64 |
| 5. | Elektropneumatyczny inteligentny element wykonawczy automatyki | 65 |
| 5.1. | Rola i miejsce elementów wykonawczych w układach automatyki | 65 |
| 5.2. | Zagadnienia diagnozowania stanu elementów wykonawczych | 67 |
| 5.3. | Elektropneumatyczny element wykonawczy | 71 |
| 5.3.1. | Ustawnik pozycyjny i siłownik pneumatyczny..... | 71 |
| 5.3.2. | Zawór sterujący..... | 73 |
| 5.4. | Instalacja elektropneumatycznych elementów wykonawczych..... | 75 |
| 5.5. | Przykład konstrukcji inteligentnego elektropneumatycznego ustawnika pozycyjnego | 77 |
| 12.5.1 | Konstrukcja części mechanicznej | 77 |
| 5.5.1. | Model funkcjonalny | 79 |
| 5.5.2. | Badania laboratoryjne modelu funkcjonalnego | 81 |
| 5.5.3. | Oprogramowanie | 84 |
| 5.5.4. | Testy przemysłowe modelu funkcjonalnego | 84 |
| 5.6. | Podsumowanie | 86 |
| 5.7. | Literatura | 86 |
| 6. | Sieci komunikacyjne | 87 |
| 6.1. | Sieci lokalne | 88 |
| 7. | Sieć Modbus | 90 |
| 7.1. | Rys historyczny..... | 90 |
| 7.2. | Wymiana wiadomości pomiędzy jednostkami | 91 |
| 7.3. | Tryby transmisji..... | 93 |
| 7.4. | Struktura ramki | 94 |
| 7.4.1. | Adres | 95 |
| 7.4.2. | Kod funkcji..... | 95 |
| 7.4.3. | Pole danych..... | 97 |
| 7.4.4. | Pole kontroli błędów..... | 99 |
| 7.5. | Odpowiedzi wyjątkowe..... | 101 |
| 7.6. | Schemat realizacji transakcji sieciowej przez jednostkę podległą | 103 |
| 7.7. | Wymagania czasowe..... | 104 |

| | | |
|----------|---|-----|
| 7.8. | Przykłady typowych funkcji Modbus | 104 |
| 7.8.1. | Odczyt pola bitowego - 01 Read Coil Status | 105 |
| 7.8.2. | Odczyt rejestru – 03 Read Holding Registers..... | 106 |
| 7.8.3. | Zapis do rejestrów - 16 Preset Multiple Regs | 106 |
| 7.9. | Podsumowanie | 107 |
| 8. | Sieć AS-i | 109 |
| 8.1. | Rys historyczny..... | 109 |
| 8.2. | Sieć AS-i a model odniesienia ISO/OSI..... | 109 |
| 8.3. | Warstwa fizyczna sieci AS-i | 111 |
| 8.3.1. | Medium transmisyjne | 111 |
| 8.3.2. | Układ zasilania..... | 113 |
| 8.3.3. | Modulacja sygnału | 114 |
| 8.3.4. | Topologia sieci..... | 115 |
| 8.4. | Warstwa danych sieci AS-i | 116 |
| 8.4.1. | Format ramki..... | 116 |
| 8.4.2. | Transmisja danych | 118 |
| 8.4.3. | Funkcjonalność magistrali..... | 119 |
| 8.5. | Warstwa aplikacji sieci AS-i..... | 121 |
| 8.5.1. | Komunikaty | 121 |
| 8.5.1.1. | Komunikaty proste..... | 122 |
| 8.5.1.2. | Komunikaty złożone..... | 123 |
| 8.5.2. | Profile | 125 |
| 8.5.3. | Przepływ informacji w sieci AS-i | 125 |
| 8.6. | Bezpieczna sieć AS-i | 126 |
| 9. | Sieć CAN | 127 |
| 9.1. | Rys historyczny..... | 127 |
| 9.2. | Standaryzacja | 127 |
| 9.3. | CAN – charakterystyka ogólna | 127 |
| 9.4. | Rozwój sieci CAN..... | 130 |
| 9.5. | Przykład zastosowania sieci CAN | 131 |
| 9.6. | Sieć CAN a model odniesienia ISO/OSI | 132 |
| 9.7. | Podstawowe wiadomości o sieci CAN | 134 |
| 9.7.1. | Przepływ informacji w sieci..... | 134 |
| 9.7.2. | Przepływ informacji w obrębie węzła | 135 |
| 9.8. | Warstwa fizyczna | 135 |
| 9.8.1. | Technika kodowania informacji..... | 135 |
| 9.8.2. | Taktowanie i synchronizacja | 136 |
| 9.8.3. | Zależność prędkości transmisji od długości magistrali | 136 |
| 9.8.4. | Kanał podkładowy transmisji danych | 136 |

| | | |
|-----------|---|-----|
| 9.8.5. | Topologia sieci..... | 137 |
| 9.8.6. | Dostęp do magistrali | 138 |
| 9.8.7. | Unormowania w zakresie warstwy fizycznej | 138 |
| 9.9. | Warstwa łącza danych | 139 |
| 9.9.1. | Wprowadzenie | 139 |
| 9.9.2. | Podstawowe definicje | 140 |
| 9.9.2.1. | Wiadomość | 140 |
| 9.9.2.2. | Zarządzanie przepływem informacji | 140 |
| 9.9.2.3. | Predkość transmisji | 141 |
| 9.9.2.4. | Priorytet wiadomości | 141 |
| 9.9.2.5. | Żądanie transmisji danych | 141 |
| 9.9.2.6. | Tryb MULTIMASTER | 141 |
| 9.9.2.7. | Arbitraż | 141 |
| 9.9.2.8. | Bezpieczeństwo przesyłanych informacji | 142 |
| 9.9.2.9. | Kontrola błędów transmisji..... | 142 |
| 9.9.2.10. | Skuteczność mechanizmu detekcji błędów | 142 |
| 9.9.2.11. | Sygnalizacja błędów i czas powrotu do normalnej pracy | 142 |
| 9.9.2.12. | Automatyczne wykluczanie uszkodzeń trwałych (Fault Confinement) | 142 |
| 9.9.2.13. | Połączenia | 142 |
| 9.9.2.14. | Wartości/Poziomy sygnału magistrali..... | 143 |
| 9.9.2.15. | Sygnalizacja potwierdzenia odbioru ACK (Acknowledgement) | 143 |
| 9.9.2.16. | Tryb uśpienia węzła (Sleep Mode / Wake-up)..... | 143 |
| 9.9.3. | Transmisja wiadomości..... | 143 |
| 9.9.3.1. | Format ramki..... | 143 |
| 9.9.3.2. | Rodzaje ramek | 143 |
| 9.9.3.3. | Ramka danych (DATA FRAME)..... | 144 |
| 9.9.3.4. | Początek ramki SOF (START OF FRAME) | 144 |
| 9.9.3.5. | Pole arbitrażu (ARBITRATION FIELD) | 144 |
| 9.9.3.6. | Identyfikator | 145 |
| 9.9.3.7. | Pole kontrolne (CONTROL FIELD)..... | 146 |
| 9.9.3.8. | Pole danych (DATA FIELD)..... | 147 |
| 9.9.3.9. | Pole sumy kontrolnej (CRC FIELD)..... | 147 |
| 9.9.3.10. | Pole potwierdzenia ACK (ACK FIELD) | 148 |
| 9.9.3.11. | Koniec ramki (END OF FRAME) | 149 |
| 9.9.4. | Ramka żądania transmisji (REMOTE FRAME) | 149 |
| 9.9.5. | Ramka sygnalizacji błędu (ERROR FRAME) | 150 |

| | | |
|----------|--|-----|
| 9.9.6. | Ramka przepełnienia (OVERLOAD FRAME) | 151 |
| 9.9.7. | Przerwa między ramkami (INTERFRAME SPACING)..... | 152 |
| 9.10. | Wymagania stawiane budowie ramki..... | 154 |
| 9.11. | Nadajnik i odbiornik..... | 154 |
| 9.12. | Filtrowanie wiadomości | 154 |
| 9.13. | Klasyfikacja wiadomości | 154 |
| 9.14. | Kodowanie ciągu bitów..... | 155 |
| 9.15. | Zarządzanie błędami (ERROR HANDLING) | 155 |
| 9.15.1. | Wykrywanie błędów..... | 155 |
| 9.15.2. | Sygnalizacja błędów (ERROR SIGNALING)..... | 156 |
| 9.16. | Ograniczanie wpływu uszkodzeń (FAULT CONFINEMENT) | 156 |
| 9.17. | Częstotliwość generatora podstawy czasu | 158 |
| 9.18. | Wymagania dotyczące taktowania (BIT TIMING REQUIREMENTS) | 158 |
| 9.19. | Warstwa aplikacyjna | 161 |
| 9.19.1. | CANopen – wprowadzenie | 161 |
| 9.19.2. | Model urządzenia | 161 |
| 9.19.3. | Słownik obiektów | 162 |
| 9.19.4. | Model komunikacji..... | 163 |
| 9.19.5. | Współpraca typu master-slave..... | 163 |
| 9.19.6. | Współpraca typu klient - serwer | 164 |
| 9.19.7. | Współpraca typu producent - konsument | 164 |
| 9.19.8. | Obiekty komunikacji..... | 165 |
| 9.19.9. | Obiekt PDO (Process Data Object) | 165 |
| 9.19.10. | Rodzaje trybów komunikacyjnych | 165 |
| 9.19.11. | Typy wymiany danych | 165 |
| 9.19.12. | Obiekt SDO (Service Data Object) | 166 |
| 9.19.13. | Transmisja segmentowa..... | 166 |
| 9.19.14. | Transmisja blokowa..... | 167 |
| 9.19.15. | Obiekt synchronizujący SYNC..... | 167 |
| 9.19.16. | Obiekt typu Time Stamp..... | 167 |
| 9.19.17. | Obiekt awaryjny EMCY | 167 |
| 9.19.18. | Obiekt NMT | 167 |
| 9.19.19. | Zarządzanie trybem pracy | 168 |
| 9.19.20. | Nadzór | 168 |
| 9.19.21. | Obiekt Boot-Up..... | 169 |
| 10. | Literatura | 170 |

1. WPROWADZENIE DO SYSTEMÓW SIECIOWYCH

1.1. CHARAKTERYSTYKA I KLASYFIKACJA SIECI

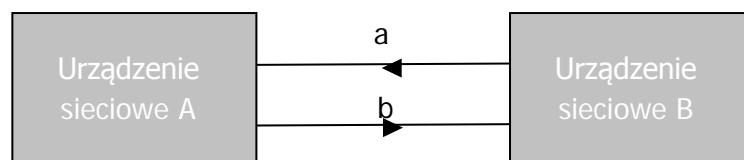
Nie wnikając nadmiernie w szczegóły realizacyjne należy przyjąć, że zdolności komunikacyjne należą do podstawowych i koniecznych cech funkcjonalnych urządzeń, które określane są jako urządzenia intelligentne. Warunek ten można próbować odwrócić twierdząc, że każde urządzenie, które nie posiada możliwości komunikacyjnych jest nieintelligentne. „Inteligencja” techniczna jest zatem współokreślona przez funkcje komunikacyjne, a te zaś stanowią jej warunek konieczny.

Ponieważ współczesne systemy automatyzacji i sterowania korzystają głównie z urządzeń intelligentnych, to szczególnej wagi nabierają także systemy komunikacyjne stosowane w tych systemach. Obecnie stosowane są w praktyce zarówno systemy komunikacji **analogowej jak i cyfrowej**. Jednak od wielu lat obserwowany jest wyraźny trend rozwojowy systemów komunikacji cyfrowej.

Podstawową zaletą komunikacji analogowej jest jej prostota, akceptowalność techniczna, niska cena, prosty serwis, duża odporność na zaburzenia elektromagnetyczne, możliwość stosowania (z uwzględnieniem określonych warunków) w strefach zagrożonych wybuchem. Do podstawowych wad komunikacji analogowej należy zaliczyć: ograniczoną przepustowość informacyjną sieci, brak możliwości realizacji złożonych topologii sieciowych i jednokierunkowość przesyłania informacji.

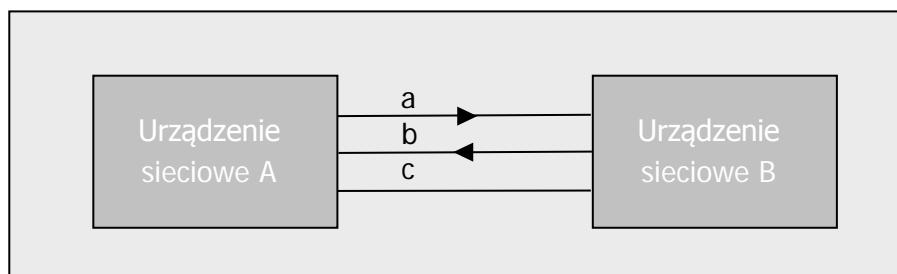
Cyfrowe systemy komunikacji posiadają zdolności komunikacji dwukierunkowej o znacznej przepustowości informacyjnej.

Zarówno sieci analogowe jak i cyfrowe mogą być konstruowane jak tzw. **sieci dwuprzewodowe**. Sieci dwuprzewodowe (rys 1.1), to takie sieci, które są zdolne przy pomocy wyłącznie jednej pary przewodów nie tylko przenosić informację pomiędzy urządzeniami sieciowymi, ale także służyć do zasilania tych urządzeń. Należy zwrócić uwagę, że sieci dwuprzewodowe należą do grupy sieci, które szczególnie chętnie są stosowane w strefach zagrożonych wybuchem. Wynika to między innymi z faktu, że urządzenia takie są budowane zwykle w taki sposób, że ich zapotrzebowanie na moc elektryczną zwykle nie przekracza 40mW. Dzięki temu moc elektryczna wprowadzana przez sieć w strefę iskrobezpieczną jest stosunkowo niewielka. Dwuprzewodowe sieci analogowe, w których wykorzystywany jest nośnik informacji w postaci prądu nazywane są tzw. **pętlami prądowymi**. Oprócz sieci dwuprzewodowych stosowane są również sieci trzy i czteroprzewodowe.



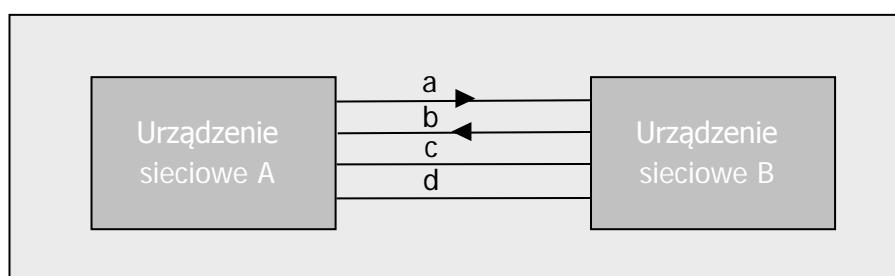
Rys. 1.1 Idea dwuprzewodowego sieciowego systemu komunikacyjnego. Oznaczenia: a, b- linie sygnałowe i zasilające.

Sieci trójprzewodowe to takie sieci, w których jedna para przewodów jest wykorzystywana jako podkładowy kanał komunikacyjny i służy do przesyłania sygnału, natomiast druga para jest wykorzystywana do zasilania urządzenia. Obie pary przewodów mają jeden przewód wspólny (por. rys. 1.2).



Rys. 1.2 Idea trójprzewodowego sieciowego systemu komunikacyjnego. Oznaczenia: a,b- linie sygnalowe, b,c- linie zasilające.

Sieci czteroprzewodowe to takie sieci, które wykorzystują dwie rozdzielne pary przewodów, z których pierwsza służy do celów komunikacyjnych, natomiast druga para jest wykorzystywana do zasilania urządzenia.



Rys. 10.4. Idea czteroprzewodowego sieciowego systemu komunikacyjnego.
Oznaczenia: a,b- linie sygnalowe, c,d- linie zasilające.

We współczesnych systemach automatyzacji i sterowania stosowane są coraz częściej cyfrowe systemy komunikacji sieciowej. Umożliwiają one tworzenie sieci lokalnych, a także sieci globalnych. Ze względu jednak na konieczność zapewnienia bezpieczeństwa sterowanego procesu, co do zasady stosowane są środki ograniczające nieautoryzowany dostęp do przemysłowych sieci komunikacyjnych. Stąd, szczególnie chętnie stosowane są w takich zastosowaniach **sieci lokalne** (LAN). Sieci lokalne stosowane w automatyzacji procesów nazywane są również **sieciami polowymi** lub sieciami typu **fieldbus**. Cechą charakterystyczną tych sieci jest ograniczony zasięg terytorialny (do kilkunastu kilometrów) oraz ograniczone prędkości transmisji (do kilkunastu Mb/s).

Rozległe sieci komunikacyjne typu WAN stosowane są do obsługi warstw zarządzania i planowania przedsiębiorstw, w których nie jest w zasadzie wymagany **determinizm** sieci. Determinizm jest szczególną cechą sieci polegającą na terminowej i przewidywalnej czasowo realizacji **transakcji sieciowych**. Sieci posiadające cechę determinizmu nazywane są

czasami **sieciami czasu rzeczywistego**. O sieciach czasu rzeczywistego mówimy również, że są przeznaczone do pracy w trybie **on-line**.

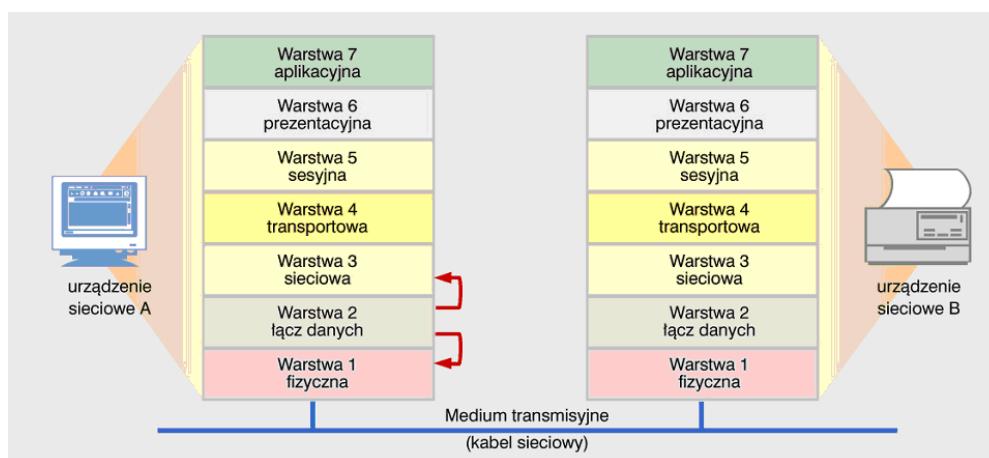
Transakcja sieciowa jest realizacją techniczną sformalizowanej procedury przesłania informacji w sieci. Zasady formalne opisujące możliwe transakcje sieciowe są specyfikowane w postaci odpowiednich dokumentów. Każda sieć komunikacyjna ma swoją własną, unikalną specyfikację sieciową. Specyfikacja zasad wymiany informacji w sieci nazywana jest często **protokołem sieciowym**. Rozróżniamy otwarte i zamknięte protokoły komunikacyjne. **Otwarte** protokoły komunikacyjne, to protokoły, których specyfikacja jest dostępna w domenie publicznej. **Zamknięte** protokoły komunikacyjne zwane czasami protokołami firmowymi, są protokołami o niejawnej specyfikacji. W praktyce protokoły zamknięte mają znaczenie marginalne. Protokoły otwarte są rozwijane i wspierane przez specjalnie utworzone ponadnarodowe organizacje zrzeszające użytkowników i producentów elementów sieciowych. Organizacje te zapewniają również wsparcie dla producentów elementów sieciowych polegające między innymi na opracowaniu jednolitych procedur pozwalających na realizację procesu certyfikacji produkowanych urządzeń sieciowych.



1.2. WARSTWOWY MODEL REFERENCYJNY SIECI

Sieciowe systemy komunikacyjne opisywane są w wymiarze funkcjonalnym w postaci wirtualnego modelu siedmiowarstwowego zwanego modelem odniesienia ISO/OSI¹ [3]. Model ten prezentuje szkieletową strukturę sieci wirtualnej. W modelu przyjęto zasadę, że każda warstwa świadczy usługi, ale wyłącznie warstwom bezpośrednio z nimi sąsiadującym. Warstwowy model ISO/OSI zaimplementowany w odpowiednim sterowniku komunikacyjnym urządzenia nosi często nazwę **stosu komunikacyjnego**. Co do zasady nie wszystkie warstwy modelu ISO/OSI muszą być zaimplementowane. Wyróżniamy **warstwy wyższe** protokołu (warstwy: sesyjna, prezentacyjna i aplikacyjna) oraz **warstwy niższe** protokołu (warstwy: fizyczna, łącza danych, sieciowa i transportowa).

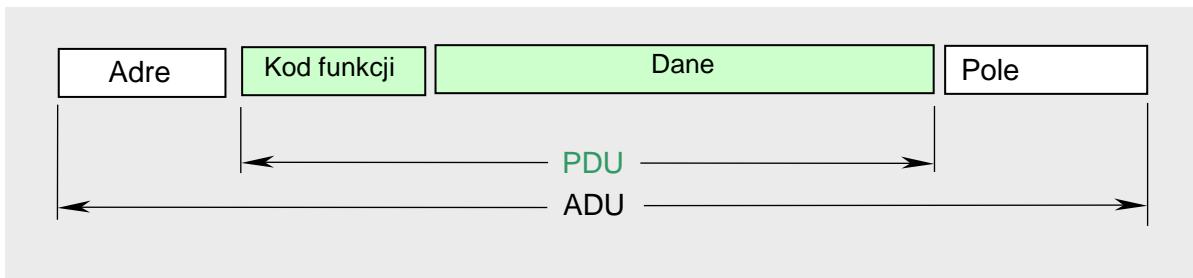
Rys. 1.5. Przykład komunikacji pomiędzy urządzeniami sieciowymi zgodny z



siedmiowarstwowym modelem komunikacyjnym ISO/OSI.

Niższe warstwy modelu są odpowiedzialne za fizyczną realizację procesu transportu informacji w sieci. W tym celu, nadajnik informacji dokonuje podziału strumienia danych przeznaczonych do wysłania na fragmenty zwane PDU (*Protocol Data Units*). Jednocześnie odbiornik informacji dokonuje procesu odwrotnego, tzn. odtwarza strumień danych na podstawie procesu defragmentyzacji jednostek PDU. W warstwie niższej następuje również uzupełnienie jednostek PDU o dodatkowe informacje (pola) zależne od typu stosowanej sieci. Jednostka PDU łącznie z dodatkowymi polami nosi nazwę jednostki ADU (*Application Data Unit*). W jednostce ADU w stosunku do jednostki PDU są zawarte dodatkowe informacje pozwalające na prawidłowe skierowanie jednostki ADU w sieci (np. adres docelowy lub i adres źródła informacji) oraz informacje pozwalające na formalną kontrolę poprawności transmisji jednostki ADU przez jednostkę sieciową, do której kierowana jest ADU (pole kontrolne).

¹ International Organisation for Standardisation/Open System Interconnection



Rys 1.6. Pola jednostek PDU i ADU w specyfikacji sieci MODBUS [4].

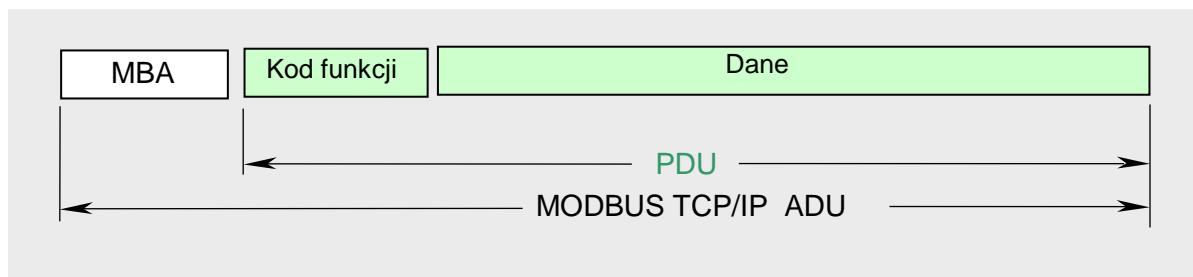
1.1.1. WARSTWY NIŻSZE MODELU ISO/OSI

Warstwa transportowa jest odpowiedzialna za segmentację danych do postaci jednostek PDU w procesie nadawania informacji i jest odpowiedzialna za proces odwrotny tzn. za składanie jednostek PDU do postaci strumienia danych w procesie odbioru informacji. Warstwa transportowa jest również odpowiedzialna za nadzór nad prawidłowością realizacji transportu ADU do sieciowej jednostki docelowej. W tym celu warstwa transportowa w procesie nadawania informacji korzysta z informacji zwrotnych kierowanych przez jednostkę docelową i informującą ją o fakcie dotarcia i poprawności formalnej wysłanej jednostki ADU. Informacja ta może być interpretowana jako potwierdzenie odbioru. W przypadku braku potwierdzenia warstwa transportowa może zlecić ponowną wysyłkę kopii tej samej jednostki ADU, której oryginał najprawdopodobniej zaginął lub uległ uszkodzeniu w sieci.

W większości sieci stosowanych do automatyzacji procesów przemysłowych stosowane są sieci LAN, w których warstwa transportowa nie jest z reguły implementowana. Zadania tej warstwy są wówczas przenoszone do warstwy aplikacyjnej i realizowane przez aplikację użytkową.

Warstwa sieciowa jest odpowiedzialna za utworzenie prawidłowych połączeń komunikacyjnych (kanałów komunikacyjnych) pomiędzy źródłem i ujęciem informacji. Inaczej mówiąc warstwa sieciowa odpowiedzialna jest za ruch w sieci i prawidłowe skierowanie jednostek PDU. W związku z tym musi posiadać wiedzę dotyczącą **topologii** sieci. Na podstawie znajomości topologii sieci w warstwie sieciowej następuje rozpoznanie tras (kanałów), po których mogą być realizowane transfery sieciowe oraz następuje dystrybucja przesyłanej informacji pomiędzy tymi kanałami. Warstwa sieciowa odgrywa również rolę regulatora ruchu sieciowego. W przypadku gdy przepustowość dysponowanych kanałów komunikacyjnych jest zbyt mała, warstwa sieciowa ma prawo wyselekcyjnować ze strumienia przesyłanej informacji tylko tę jej część, która może być realnie przesłana. W takim przypadku dochodzi do strat w strumieniu przesyłanej informacji. Warstwa sieciowa nie bierze odpowiedzialności za te straty. Są one kontrolowane i kompensowane przez

wyższe warstwy protokołu np. warstwę transportową. W warstwie sieciowej stosowane są między innymi implementacje: IPv4 i IPv6.



Rys 10.7 Pola jednostek PDU i ADU dla specyfikacji sieci MODBUS TCP/IP [5]. Oznaczenia: MBAP – *Modbus Application Protocol Header* - nagłówek jednostki ADU zawierający informacje o: identyfikatorze jednostki sieciowej, długości przesyłanego pola danych w bajtach, identyfikatorze protokołu inicjowanego przez klienta i identyfikatorze transakcji pozwalającym na realizację operacji scalania jednostek ADU w strumień danych.

W większości sieci stosowanych do automatyzacji procesów przemysłowych stosowane są sieci LAN, w których warstwa sieciowa nie jest z reguły implementowana. Zadania tej warstwy są wówczas realizowane przez aplikację użytkową.

Warstwa łącza danych zwana warstwą liniową pełni dwie podstawowe role: logistyczną i kontrolną. Zasadniczą rolą tej warstwy polega w przypadku nadawania na podziale przekazywanej informacji na fragmenty i uzupełnianie tej informacji o pole kontrolne. W przypadku odbioru, warstwa łącza sprawdza poprawność formalną odbieranych jednostek ADU. Warstwa łącza danych może również parametryzować właściwości warstwy fizycznej w taki sposób, aby obniżyć liczbę transferów z błędami. W warstwie łącza danych następuje również operacja **enkapsulacji** informacji w ramki LPDU (*data Link Protocol Data Unit*) o strukturze zgodnej ze specyfikacją wykorzystywanego protokołu sieciowego. W warstwie łącza danych wydzielane są dwie podwarstwy: LLC (*Logical Link Control*) i MAC (*Media Access Control*). Warstwa LLC odpowiedzialna jest za kontrolę poprawności transmisji. Warstwa MAC zapewnia dostęp warstwy łącza danych do podkładowego kanału komunikacyjnego (medium komunikacyjnego) obsługiwany przez warstwę fizyczną.

W większości sieci stosowanych do automatyzacji procesów przemysłowych stosowane są sieci LAN, w których warstwa łącza jest z reguły implementowana lub realizowana sprzętowo przez odpowiedni kontroler warstwy łącza danych np. kontroler CAN 2.0B.

Warstwa fizyczna definiuje wszystkie składniki materialne i funkcjonalne, które są konieczne do fizycznej realizacji procesu komunikacji. Jest warstwą konieczną do realizacji procesu komunikacyjnego. Należy zwrócić uwagę, że procesy komunikacyjne

wykorzystywane obecnie w systemach sieciowych wykorzystują tryb transmisji szeregowej. W związku z tym w warstwie fizycznej w procesie nadawania realizowana jest transformacja informacji z postaci równoległej do szeregowej. Podobnie w procesie odbioru pokonywana konwersja odwrotna tzn. konwersja z postaci szeregowej do równoległej. Dodatkowo szeregowe bitowe strumienie informacji podlegają dodatkowemu kodowaniu w celu dostosowania do właściwości stosowanego kanału podkładowego. Stosowane są np. techniki kodowania częstotliwościowego z kluczowaniem fazy (FSK), techniki kodowania czasowego takie jak np. bifazowy kod Manchester czy kod NRZ z techniką *bit stuffing*.

Informacja pomiędzy jednostkami sieciowymi wymieniana jest w warstwie fizycznej w trybie szeregowej **transmisji jednoczesnej** (*full duplex*) lub **naprzemiennej** (*half duplex*). Może odbywać się synchronicznie lub **asynchronicznie**. Sposób i tryb realizacji transmisji w warstwie fizycznej jest zależny od konkretnego protokołu komunikacyjnego. Warstwa fizyczna specyfikuje również parametry elektryczne stosowanego kanału komunikacyjnego. Należy zwrócić uwagę, że dla wielu protokołów sieciowych istnieje możliwość wyboru warstwy fizycznej. W tym sensie warstwa fizyczna nie jest warstwą unikalną dla danego protokołu komunikacyjnego. Znane są specyfikacje protokołów, które nie definiują warstwy fizycznej np. MODBUS i takie, które korzystają z tej samej specyfikacji np. Profibus PA i Foundation Fieldbus H1. Zgodność warstw fizycznych sieci gwarantuje jedynie kompatybilność tych sieci na poziomie elektrycznym i mechanicznym. Nie gwarantuje natomiast zgodności na poziomie warstw wyższych, a więc kompatybilności informacyjnej.

Warstwa fizyczna jest warstwa obligatoryjną dla wszystkich sieci stosowanych do automatyzacji procesów przemysłowych. Należy jednak zaznaczyć, że ze względu na zapewnienie odporności tych sieci na zaburzenia elektromagnetyczne charakterystyczne dla środowiska przemysłowego, stosowanie są w tych sieciach relatywnie niskie prędkości transmisji w porównaniu z sieciami stosowanymi do innych celów.

1.2.2. WARSTWY WYŻSZE MODELU ISO/OSI

Warstwa sesyjna nadzoruje kanały komunikacyjne wytworzzone w warstwie transportowej zapewniając prawidłowe połączenie pomiędzy jednostkami sieciowymi na poziomie aplikacji sieciowych. Dokonuje kojarzenia strumieni przesyłanych danych z realizowanymi aplikacjami zapewniając nadzór zarówno nad kierunkiem, jak i ciągłością transmisji.

Ze względu na lokalny zasięg, w większości sieci stosowanych do automatyzacji procesów przemysłowych warstwa sesyjna nie jest implementowana. Zadania tej warstwy, jeśli występują, są realizowane przez aplikację użytkową obsługującą proces komunikacji.

Warstwa prezentacji w procesie nadawania nadzoruje proces przetwarzania danych pochodzących z warstwy aplikacyjnej do formatu kanonicznego (*canonnical representation*)

zgodnego ze specyfikacją OSI. Warstwa prezentacji dokonuje procesu odwrotnego w procesie odbioru. Warstwa ta odpowiada między innymi za kodowanie i szyfrowanie przesyłanych danych, a także za operacje ich dekodowania i deszyfrowania. W warstwie tej może być np. realizowana konwersja formatów graficznych JPEG, MPEG, GIF. Warstwa prezentacji odgrywa szczególną rolę w systemach komunikacji z zabezpieczeniami.

W większości sieci stosowanych do automatyzacji procesów przemysłowych warstwa prezentacji nie jest implementowana. Zadania tej warstwy, jeśli występują, są realizowane przez aplikację użytkową obsługującą proces komunikacji.

Warstwa aplikacji jest warstwą najwyższą stosu komunikacyjnego mającą bezpośrednie połączenie z aplikacjami użytkowymi obsługującymi proces komunikacji. W warstwie tej definiowany jest język oraz zasady syntaktyczne umożliwiające sieciową komunikację aplikacji użytkowych. Typowymi funkcjami definiowanymi w tej warstwie są funkcje otwarcia, zamknięcia, odczytu i zapisu plików, funkcje uruchamiania zdalnego zadań, funkcje pozwalające na monitorowanie dostępnych zasobów sieciowych. Warstwa ta daje narzędzia programowe do tworzenia aplikacji obsługujących proces komunikacji.

W większości systemów sieciowych stosowanych do automatyzacji procesów przemysłowych warstwa aplikacyjna jest realizowana. Warstwa aplikacyjna nie jest wyróżnikiem sieci komunikacyjnej. Oznacza to, że ta sama sieć może mieć zaimplementowanych kilka różnych warstw aplikacyjnych. Dla przykładu w sieci CAN stosowane są warstwy aplikacyjne: CanOpen, Kingdom, J1939.

1.3. LITERATURA

- [1] J. Ułasiewicz: Systemy czasu rzeczywistego QNX6 Neutrino. Wydawnictwo BTC, ISBN 978-83-60233-27-6, str. 301 Warszawa 2007.
- [2] K. Sacha: *Systemy czasu rzeczywistego*, Oficyna Wydawnicza Politechniki Warszawskiej, ISBN 83-7207-124-1, str. 135, Warszawa, 2006.
- [3]. ISO s7498-1:1994: *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- [4]. <http://www.modbus.org/specs.php>. MODBUS Protocol Specification.
- [5]. <http://www.modbus.org/specs.php>. MODBUS TCP/IP Protocol Specification.
- [6]. A. Tanenbaum: *Sieci komputerowe*, Helion, 2004, ISBN 83-7361-557-1.

2. SIEĆ ANALOGOWA 4-20mA

2.1. CHARAKTERYSTYKA SIECI ANALOGOWYCH

W naturalny sposób sieci analogowe były pierwotnymi sieciami komunikacyjnymi. Umożliwiały przesyłanie informacji kodowanej w sposób ciągły przy wykorzystaniu dowolnych technik modulacji amplitudowej, częstotliwościowej, czasowej, PWM, a także bezpośrednio w postaci sygnałów prądowych i napięciowych. Szczególnego znaczenia w zastosowaniach przemysłowych nabraly zwłaszcza te sieci analogowe, w których wykorzystywano bezpośrednie kodowanie informacji w postaci napięcia lub prądu proporcjonalnego do wartości przesyłanej wielkości. O rozpowszechnieniu tych metod kodowania informacji zdecydowały przede wszystkim czynniki mające ostatecznie wymiar ekonomiczny, takie jak: niska cena realizacji, prosty montaż i uruchomienie, prosty i szybki serwis, brak konieczności stosowania złożonych narzędzi diagnostycznych.

Sieci analogowe stosowane w automatyzacji procesów realizowane są głównie w postaci:

- sieci z kodowaniem napięciowym informacji i
- sieci z kodowaniem prądowym informacji.

Istnieje wiele standardów określających zakresy zmienności sygnałów napięciowych i prądowych wykorzystywanych w komunikacji analogowej. Stosowane są zarówno sygnały unipolarne jak i bipolarne.

W przypadku kodowania informacji w postaci napięciowej stosowane są zakresy napięciowe:

- 0..1V
- 0..5 V
- 0..10V
- ± 1V
- ± 5V
- ± 10V

W przypadku kodowania informacji w postaci prądowej stosowane są zakresy prądowe:

- 0..5mA
- 0..20mA
- 4..20mA
- 4..12mA
- 12-20mA

Najbardziej rozpowszechnionymi sieciami analogowymi o bezpośrednim kodowaniu napięciowym są sieci wykorzystujące sygnał napięciowy z zakresu 0..10V. W przypadku sieci analogowych o bezpośrednim kodowaniu prądowym najbardziej rozpowszechnione są sieci wykorzystujące sygnał prądowy z zakresu 4..20mA.

Zdecydowaną wadą systemów komunikacji analogowej jest brak prostej, taniej i niezawodnej możliwości realizacji wielu kanałów komunikacyjnych w tym samym kanale podkładowym. Oznacza to w praktyce, że jeden analogowy kanał komunikacyjny może być wykorzystywany w zasadzie do przesyłania informacji wyłącznie o jednej zmiennej procesowej, którą reprezentuje. Dodatkowo analogowe kanały komunikacyjne są kanałami

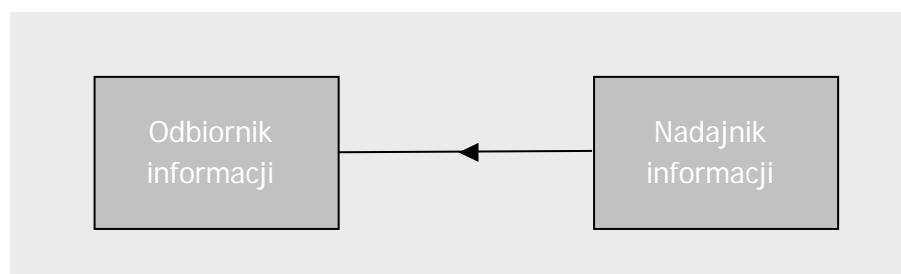
jednokierunkowymi. Oznacza to, że informacja przesyłana jest pomiędzy nadajnikiem i odbiornikiem, ale obie role nie są zamienne, tzn. odbiornik nie może pełnić roli nadajnika.

2.2. TOPOLOGIA SIECI

Niewątpliwą wadą sieci analogowych liczba jest bardzo ograniczona liczba dostępnych topologii sieciowych. Ponadto, w stosunku do niektórych z nich istnieją silne ograniczenia stosownalności. Zasadniczo sieć analogowa wykorzystywana jest w trzech topologiach:

- połączenia bezpośredniego,
- gwiazdy,
- łańcucha.

Topologia połączenia bezpośredniego zwana również topologią punkt do punktu (*point-to-point*) jest najprostszą topografią sieciową pozwalającą na bezpośredni, wyłączne i jednokierunkowe połączenie dwóch urządzeń sieciowych. Przykład takiej topologii podano na rys. 2.1.

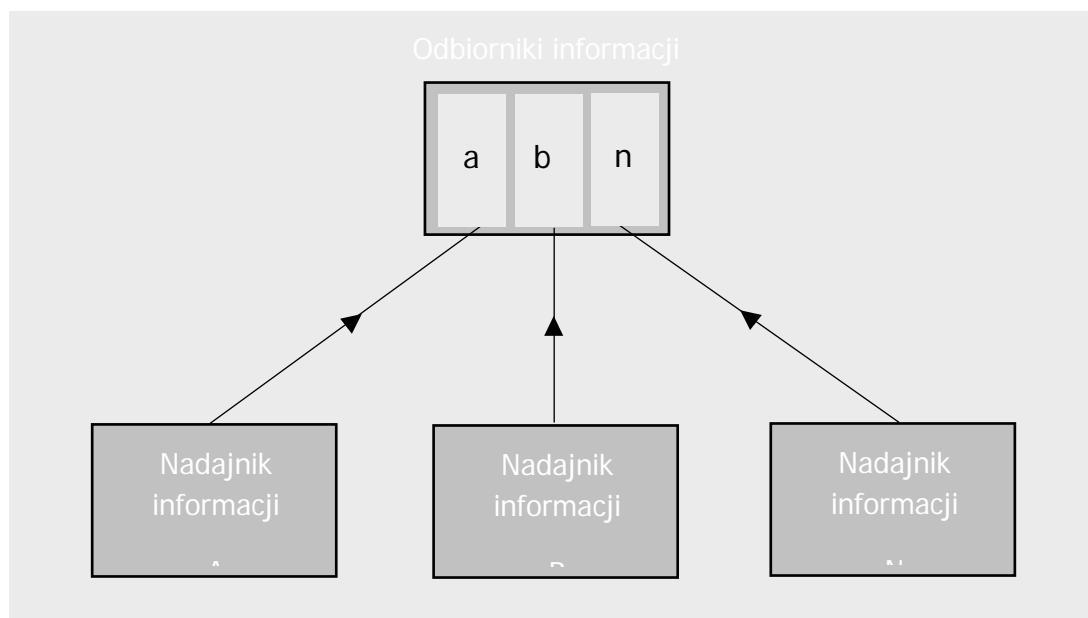


Rys. 2.1. Przykład topologii w postaci połączenia bezpośredniego (*point-to-point*)

W przypadku sieci z kodowaniem napięciowym nadajnik informacji pełni rolę sterowanego źródła napięcia o niskiej impedancji wyjściowej, natomiast odbiornik informacji charakteryzuje się wysoką impedancją wejściową. W tym przypadku stosowana jest sieć trójprzewodowa (rys. 1.2) lub czteroprzewodowa (rys. 1.3). Sieć dwuprzewodowa nie jest możliwa do zastosowania, co jest ewidentną wadą sieci z kodowaniem napięciowym.

W przypadku sieci z kodowaniem prądowym nadajnik informacji pełni rolę sterowanego źródła prądowego. W związku z tym impedancja wyjściowa nadajnika informacji jest wysoka. Prąd generowany przez nadajnik jest nośnikiem przesyłanej informacji. Odbiornik informacji ma elektryczną charakterystykę zbliżoną do idealnego źródła napięcia. Charakteryzuje się niską wartością impedancji wyjściowej. W sieci z kodowaniem prądowym stosowana jest sieć dwuprzewodowa (rys. 1.1), trójprzewodowa (rys. 1.2) lub czteroprzewodowa (rys. 1.3). W przypadku zastosowania sieci dwuprzewodowej rolę urządzenia zasilającego sieć pełni nadajnik lub odbiornik. Odbiornik informacji zasila bezpośrednio nadajnik informacji w przypadku gdy nadajnikiem jest urządzenie wejściowe np. przetwornik pomiarowy. Z kolei nadajnik informacji zasila bezpośrednio odbiornik informacji w przypadku gdy odbiorikiem jest urządzenie wyjściowe np. element wykonawczy automatyki.

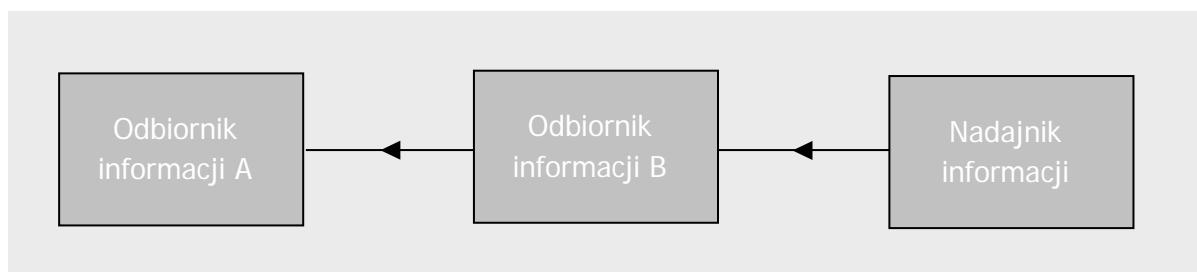
Topologia gwiazdy jest w istocie mnożnikową topologią połączenia bezpośredniego. Topologia ta stosowana jest w układach bezpośredniego sterowania DDC i w modułach rozproszonych wejścia-wyjście analogowych. W takich przypadkach koncentracja sieci w umownym wspólnym punkcie wirtualnym jest realizowana zwykle po stronie cyfrowej a nie analogowej. Przykład takiej topologii podano na rys. 2.2.



Rys. 2.2 Przykład topologii gwiazdy

W analogowej sieci o topologii gwiazdy stosowane są połączenia urządzeń w konfiguracji dwu-, trzy- i czteroprzewodowej.

Topologia łańcucha jest stosowana wyłącznie w sieciach z prądowym kodowaniem informacji analogowej. Topologia ta stosowana jest stosunkowo rzadko. Umożliwia przesyłanie tej samej informacji do kilku urządzeń sieciowych połączonych szeregowo. W praktyce stosowane są połączenia dwóch lub trzech urządzeń. Topologia ta wykorzystywana jest np. w przypadku, gdy potrzebny jest lokalny wyświetlacz wartości wielkości mierzonej przez przetwornik pomiarowy. Wówczas lokalny wyświetlacz wartości wielkości mierzonej łączony jest szeregowo w tor komunikacji analogowej pomiędzy nadajnikiem i odbiornikiem informacji. Przykład topologii łańcucha przedstawiono na rys. 2.3.



Rys. 2.3 Przykład topologii łańcucha

2.3. WYKORZYSTANIE SIECI ANALOGOWEJ 4-20mA DO CELÓW DIAGNOSTYCZNYCH

Typowym przykładem uszkodzenia toru komunikacji analogowej jest zerwanie linii komunikacyjnej. Zerwanie linii komunikacyjnej wiąże się z zanikiem sygnału prądowego. Zero wartość sygnału prądowego jest dopuszczalna w przypadku wykorzystywania komunikacji analogowej w zakresie prądowym 0-20mA i jest niedopuszczalna w przypadku stosowania zakresu 4-20mA. Zatem zero wartość prądu w przypadku stosowania komunikacji prądowej w zakresie 4-20mA może być wykorzystana do celów diagnostycznych ponieważ przenosi dodatkową informację o uszkodzeniu połączenia lub urządzenia komunikacyjnego.

W niektórych przypadkach urządzenia prądowej komunikacji sygnalizują mogą sygnalizować dodatkowo pewne stany np. stany alarmowe w postaci wyróżnionych wartości prądu leżących poza standardowym zakresem 4-20mA np. 3,75mA lub 21,25mA. W tym przypadku komunikacja analogowa umożliwia transmisję jednej wartości analogowej (ciągłej) w zakresie 4-20mA i przesyłanie 3 wartości dyskretnych (nieciągłych) kodowanych wartościami prądu {0mA, 3,75mA, 21,25mA}.

2.4. SIEĆ ANALOGOWA 4-20mA W URZĄDZENIACH INTELIGENTNYCH

W zasadzie każde urządzenie intelligentne wyposażone jest, w co najmniej jeden wbudowany mikrokontroler cyfrowy. Nie oznacza to bynajmniej, że urządzenia intelligentne mogą być stosowane wyłącznie w sieciach cyfrowych. Istnieje szeroka gama intelligentnych urządzeń pomiarowych i wykonawczych, które komunikują się wyłącznie w sposób analogowy.

Istotną zaletą zastosowania prądowej sieci analogowej o zakresie 4-20mA w urządzeniach intelligentnych jest możliwość realizacji dwuprzewodowych połączeń sieciowych. W takim przypadku intelligentne urządzenia sieciowe muszą być w stanie operatywnym już wówczas, gdy prąd sieci jest równy 4mA. Ze względów bezpieczeństwa przyjmuje się, że urządzenia takie powinny być w pełni funkcjonalnie już wówczas, gdy prąd w sieci przyjmuje wartość 3,6mA lub 3,2mA w przypadku sieci HART. Jeśli założymy, że wartość napięcia na zaciskach wejściowych takiego urządzenia zwykle nie przekracza 10V, to maksymalna moc pobierana przez urządzenie intelligentne nie może przekraczać wartości 40mW. Tak mała wartość dysponowanej mocy stanowi istotne wyzwanie dla konstruktorów dwuprzewodowych intelligentnych urządzeń sieciowych. Należy zaznaczyć w tym miejscu, że podobne ograniczenia obowiązują również w przypadku zastosowania sieci cyfrowych takich jak: HART, Profibus PA czy Foundation Fieldbus H1.

Poniżej rozważymy dwa przykłady typowych urządzeń inteligentnych, akcentując jednocześnie ograniczenia jakie są wnoszone przez sieć analogową.

Przykład 1: Przetwornik pomiarowy

Inteligentny przetwornik pomiarowy dokonuje pomiaru wartości ciśnienia hydrostatycznego w zbiorniku wykorzystując do tego celu czujnik ciśnienia w postaci scalonego mostka piezorezystancyjnego. Napięcie niezrównoważenia tego mostka jest zależne od wartości wielkości mierzonego ciśnienia. Niestety napięcie to jest również funkcją temperatury samego mostka. Stąd, dla uzyskania poprawnego wskazania należy dokonać kompensacji temperaturowej napięcia niezrównoważenia mostka. Do tego celu konieczny jest dodatkowy pomiar temperatury struktury mostka piezorezystancyjnego. Kompensacja wpływu temperatury na wartości mierzonego ciśnienia jest realizowana w sposób cyfrowy przez wbudowany mikrokontroler. W rezultacie w przetworniku dokonywane są dwa pomiary: ciśnienia i temperatury. Jeśli wartości obu wielkości fizycznych będą przesyłane w sposób analogowy, to konieczne jest dołączenie do przetwornika dwóch kanałów analogowych. W przypadku zastosowania komunikacji cyfrowej, obie wielkości mogą być przesyłane przy wykorzystaniu tylko i wyłącznie jednego kanału.

Przykład 2: Element wykonawczy

Inteligentny element wykonawczy automatyki steruje strumieniem objętościowym cieczy dopływającej do zbiornika. Poziom cieczy w zbiorniku jest mierzony przy wykorzystaniu czujnika ciśnienia z przykładu 1. Sterowanie dopływem cieczy odbywa się przez zastosowanie w torze zasilania zbiornika zaworu sterującego. Zawór ten dławia strumień sterowanej cieczy w stopniu zależnym między innymi od stopnia jego zamknięcia. Stopień zamknięcia zaworu sterowany jest sygnałem analogowym z zewnętrznego systemu sterowania. Sygnał ten przekształcany jest w układzie pozycjonującym elementu wykonawczego na proporcjonalny sygnał przemieszczenia grzyba zaworu, a więc przekłada się bezpośrednio na stopień dławienia zaworu. Układ pozycjonujący grzyb zaworu dokonuje pomiaru przemieszczenia grzyba zaworu. Pomiar ten jest wykorzystywany wewnątrz elementu wykonawczego, ale jest jednocześnie niezwykle użyteczny z punktu widzenia diagnostycznego. Znajomość wartości aktualnej przemieszczenia grzyba zaworu w zestawieniu z jego aktualną wartością zadaną pozwala na ocenę nie tylko właściwości dynamicznych samego elementu wykonawczego, ale także na ocenę jego stanu technicznego. W ten sposób można łatwo wykryć np. zacięcie grzyba zaworu. Dodatkowa informacja o przemieszczeniu grzyba zaworu wymaga niestety zastosowania dodatkowego analogowego kanału komunikacyjnego.

2.5. WŁAŚCIWOŚCI ANALOGOWEJ SIECI PRĄDOWEJ

Analogowa sieć prądowa stosowana jest powszechnie w praktyce przemysłowej. Posiada ona szereg istotnych zalet eksploatacyjnych, z których najważniejsze zostaną omówione poniżej.

2.5.1. ODPORNOŚĆ NA ZWARCIA I ROZWARCIA SIECI

W czasie eksploatacji systemów sieciowych z komunikacją analogową dochodzi do uszkodzeń połączeń pomiędzy urządzeniami. Uszkodzenia te mogą mieć różną naturę, ale zdecydowana większość z nich może być klasyfikowana do dwóch kategorii, a mianowicie jako zwarcia i rozwarcia linii komunikacyjnych. Rozważymy skutki tego typu uszkodzeń osobno dla sieci analogowych z napięciowym i prądowym kodowaniem informacji.

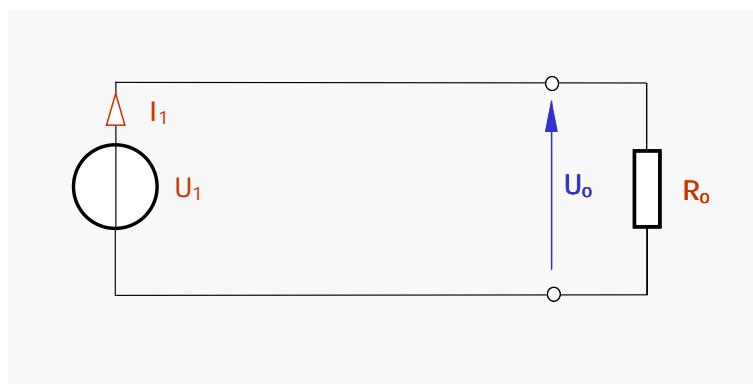
Przypadek 1: Zwarcie linii komunikacyjnych

W przypadku zwarcia linii komunikacyjnych popłynie prąd zwarciovy. Wartość tego prądu może być różna dla sieci z napięciowym i prądowym kodowaniem informacji.

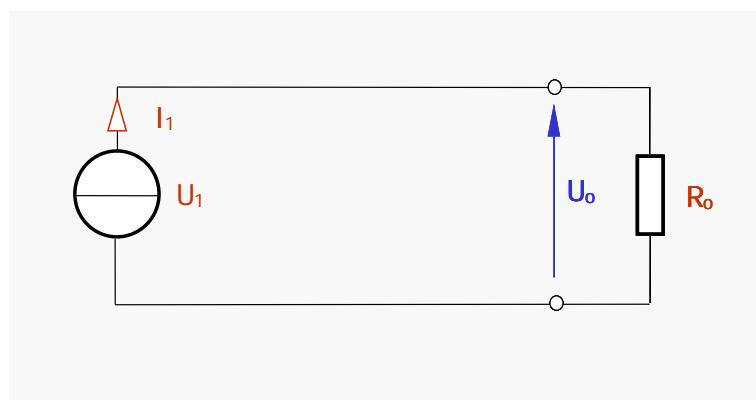
W przypadku sieci z napięciowym kodowaniem informacji (por. rys. 2.4) popłynie prąd zwarcia teoretycznie o nieskończonym wielkości wartości. W rzeczywistych urządzeniach sieciowych prąd zwarcia będzie ograniczony przez rezystancję kabli, rezystancję wewnętrzną źródła napięcia i ewentualnie przez układ zabezpieczenia przetężeniowego urządzenia sieciowego. Wystąpienie zwarcia powoduje paraliż informacyjny sieci i wywołuje przepływ nadmiernego prądu.

W przypadku sieci z prądowym kodowaniem informacji (por. rys. 2.5) i połączeniu trzy- lub czteroprzewodowym, w wyniku zwarcia linii sygnałowych popłynie prąd zwarcia równy dokładnie wartości prądu generowanego przez źródło prądowe nadajnika. W odróżnieniu od sieci z kodowaniem napięciowym, zwarcie nie wywoła żadnej zmiany prądu nadajnika. Prąd ten będzie przepływał przez zworę i w związku z tym nie będzie przepływał przez odbiornik informacji. W związku z tym wystąpienie zwarcia przewodów sygnałowych powoduje również paraliż informacyjny sieci jednakże nie wywołuje zmiany wartości płynącego prądu przez nadajnik.

W przypadku sieci z prądowym kodowaniem informacji i połączeniu dwuprzewodowym, w wyniku zwarcia obu przewodów popłynie przez zworę prąd zwarcia źródła odbiornika. Prąd ten w rzeczywistych odbiornikach sieciowych jest ograniczany przez układ przetężeniowy. W rezultacie zwarcia napięcie na zaciskach nadajnika informacji spadnie do zera i w związku z tym prąd nadajnika spadnie również do zera. W związku z tym wystąpienie zwarcia powoduje również paraliż informacyjny sieci i powoduje spadek do zera wartości prądu generowanego przez nadajnik.



Rys. 2.4. Schemat zastępczy napięciowego źródła informacji. Oznaczenia: U_1 – sygnał napięciowy nadajnika informacji, I_1 - prąd w pętli napięciowej, R_o - rezystancja wejściowa odbiornika, U_o – napięcie wejściowe odbiornika.



Rys. 2.5 Schemat zastępczy prądowego źródła informacji.

Przypadek 2: Wpływ rezystancji kabli

Połączenia kablowe pomiędzy urządzeniami sieciowymi nie są bezrezystancyjne. Rezystancja kabli przyłączeniowych i rezystancja przyłączycy tych kabli może mieć wpływ na wartość przesyłanego sygnału.

W przypadku sieci z napięciowym kodowaniem informacji (por. rys. 2.6) wartość sygnału napięciowego U_o na zaciskach odbiornika nie jest dokładnie równa napięciu U_1 generowanemu przez nadajnik. Jeśli pominiemy rezystancję wewnętrzną źródła sygnału, to wartość napięcia na zaciskach odbiornika zależy od wartości napięcia sygnału U_1 , rezystancji kabli R_1 , i rezystancji wejściowej odbiornika R_o . W sieciach analogowych odległości pomiędzy nadajnikiem i odbiornikiem informacji są na tyle znaczne, że wartość rezystancji kabli nie jest bez znaczenia. Spróbujmy oszacować ten wpływ na następującym prostym przykładzie:

Założymy, że,

$$R_1 = 50\Omega, \\ R_o = 100k\Omega.$$

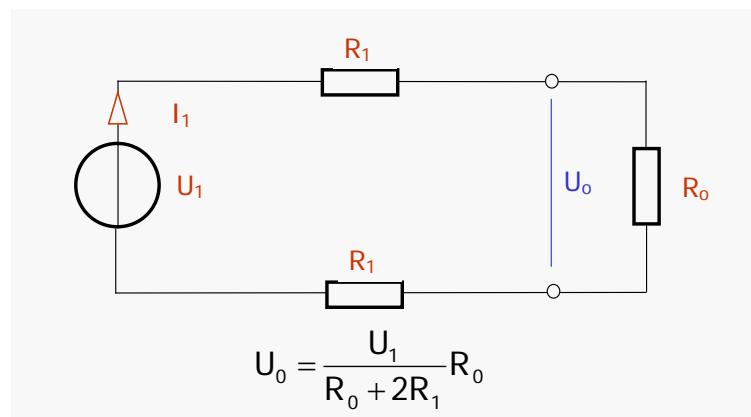
Względny spadek napięcia U_0 w stosunku do napięcia U_1 wynosi:

$$\frac{U_1 - U_0}{U_1} = 1 - \frac{R_o}{R_o + 2R_1} = 1 - \frac{100k\Omega}{100k\Omega + 100\Omega} \cong 0,1\%$$

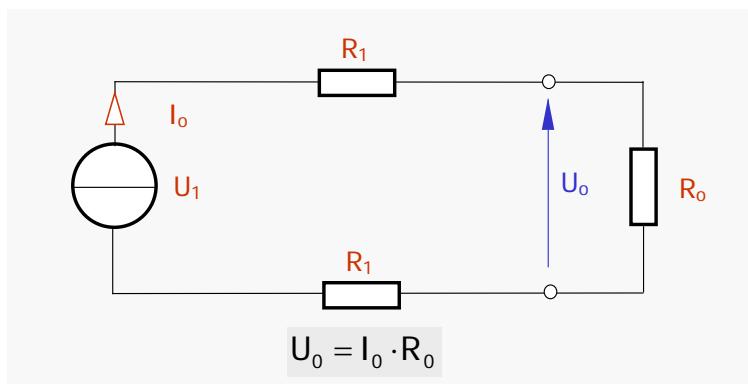
Gdybyśmy założyli, że rezystancja wejściowa odbiornika byłaby mniejsza i równa $R_o = 10k\Omega$, to dla tej samej wartości rezystancji kabli $R_1 = 50\Omega$ względny spadek napięcia U_0 w stosunku do napięcia U_1 wynosiłby aż 1%.

W przypadku sieci z prądowym kodowaniem informacji (por. rys. 2.7) wartość sygnału napięciowego U_0 na zaciskach odbiornika jest wyłącznie zależna od jego rezystancji wejściowej R_o i prądu źródła informacji. Zatem wartość U_0 nie zależy od rezystancji kabli i nie zależy również od zmian tej rezystancji wynikającej ze zmian temperatury, procesów starzenia, korozji itp.

Przeprowadzona analiza wskazuje na istotną zaletę analogowych sieci z sygnalizacją prądową w stosunku do sieci z sygnalizacją napięciową polegającą na braku wrażliwości przesyłanego sygnału na wartość rezystancji linii komunikacyjnych.



Rys. 2.6 Uproszczony schemat zastępczy napięciowego źródła informacji z uwzględnieniem rezystancji kabli. Oznaczenia: R_1 – rezystancja pojedynczego kabla.



Rys. 2.7 Uproszczony schemat zastępczy prądowego źródła informacji z uwzględnieniem rezystancji kabli.

Przypadek 3: Odporność na zakłócenia

Dokonajmy prostej analizy polegającej na zbadaniu odporności na zakłócenia sieci analogowych z kodowaniem napięciowym i prądowym. W analizie tej założymy, że zaburzenia elektromagnetyczne oddziaływujące na obie sieci są zaburzeniami tej samej mocy. Analizę będziemy prowadzić wykorzystując uproszczone schematy przedstawione na rys. 2.8 i 2.9. Na schematach tych przyjęto, że zakłócenia mogą być reprezentowane w postaci źródła napięcia U_z włączonego szeregowo w obwód z kodowaniem napięciowym lub w postaci źródła prądowego I_z włączonego równolegle w obwód z kodowaniem prąдовym.

Przypadek 3.1: Analogowa sieć z sygnałem napięciowym

Napięcie wejściowe U_o odbiornika informacji będzie zależało w tym przypadku zarówno od napięcia źródła informacji U_1 , napięcia szczytowego źródła zakłócającego U_z , oraz rezystancji wejściowej odbiornika R_o i rezystancji kabli $2R_1$. Wrażliwość sygnału użytecznego U_o na zakłócenia o maksymalnej wartości szczytowej U_z i rezystancję kabli w może być wyrażony w postaci:

$$\frac{U_1 - U_o}{U_1} = 1 - \frac{R_o(U_1 + U_z)}{(R_o + 2R_1) \cdot U_1} \quad (2.1)$$

natomiast szczytowa wartość mocy sygnału zakłócającego P_z w postaci:

$$P_z = \left(\frac{U_1 + U_z}{R_o + 2R_1} \right) \cdot U_z \quad (2.2)$$

Spróbujmy wyznaczyć wartość stosunku sygnału do zakłócenia na przykładzie liczbowym, który odzwierciedla dość typowy przypadek praktyczny. W przykładzie tym przyjęto następujące dane:

$$P_z = 0,1mW,$$

$$U_1 = 10,00V,$$

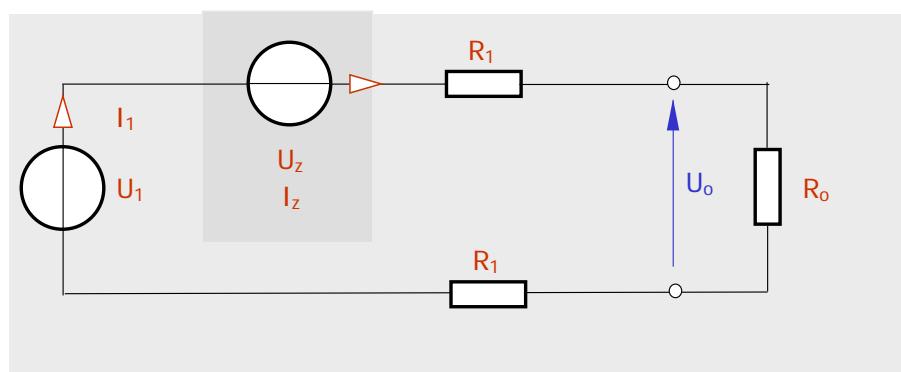
$$R_0 = 100k\Omega,$$

$$R_1 = 50\Omega.$$

Po podstawieniu danych do wzoru 2.2 wyznaczamy ekwiwalentną wartość szczytową U_z źródła napięcia zakłócającego $U_z = 0,46V$. Po podstawieniu wartości U_z do wzoru 2.1 wyznaczamy wrażliwość sygnału w odbiorniku na rezystancję kabli i zakłócenie napięciowe o wartości szczytowej U_z .

$$\frac{U_1 - U_0}{U_1} = 1 - \frac{100000\Omega \cdot 10,46V}{100100\Omega \cdot 10,00V} = -4,5\%$$

Jak łatwo zauważyc (przypadek 2, rozdział 2.4.1) wpływ rezystancji kabli na ten współczynnik jest relatywnie mały.



Rys. 2.8 Uproszczony schemat zastępczy napięciowego źródła informacji z uwzględnieniem rezystancji kabli i zastępczym szeregowym źródłem zakłóceń.

Oznaczenia: U_z – napięcie źródła zakłóceń.

Przypadek 3.2: Analogowa sieć z sygnałem prądowym

Napięcie wejściowe U_0 odbiornika informacji będzie zależało w tym przypadku zarówno od prądu źródła informacji I_1 , prądu szczytowego źródła zakłócającego I_z . Nie będzie natomiast zależało od rezystancji kabli $2R_1$. Wrażliwość sygnału użytecznego I_0 na zakłócenia o maksymalnej wartości szczytowej I_z na zakłócenia może być wyrażony w postaci:

$$\frac{I_1 - I_0}{I_1} = \frac{-I_z}{I_1} \quad (2.3)$$

natomiast szczytowa wartość mocy sygnału zakłócającego P_z w postaci:

$$P_z = R_0 \cdot (I_1 + I_z) \cdot I_z \quad (2.4)$$

Spróbujmy wyznaczyć wartość stosunku sygnału do zakłócenia na przykładzie liczbowym, który odzwierciedla dość typowy przypadek praktyczny. W przykładzie tym przyjęto następujące dane:

$$P_z = 0,1mW,$$

$$I_1 = 20mA,$$

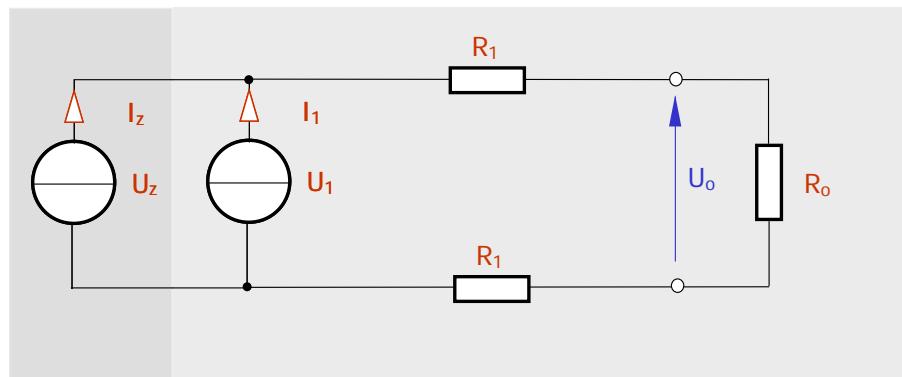
$$R_0 = 100\Omega,$$

$$R_1 = 50\Omega,$$

Po podstawieniu danych do wzoru 2.4 wyznaczamy ekwiwalentną wartość szczytową I_z źródła prądu zakłócającego $I_z = 0,05mA$. Po podstawieniu wartości I_z do wzoru 10.4 wyznaczamy wrażliwość sygnału w odbiorniku na rezystancję kabli i zakłócenie prądowe o wartości szczytowej I_z .

$$\frac{I_1 - I_0}{I_1} = -\frac{0,05mA}{20mA} = -0,25\%$$

Jak łatwo zauważyc, w tym przypadku wpływ zakłócenia o tej samej mocy na sygnał odbiornika jest ewidentnie mniejszy w układzie komunikacji analogowej z kodowaniem prądowym sygnału niż w układzie komunikacji analogowej z kodowaniem napięciowym.

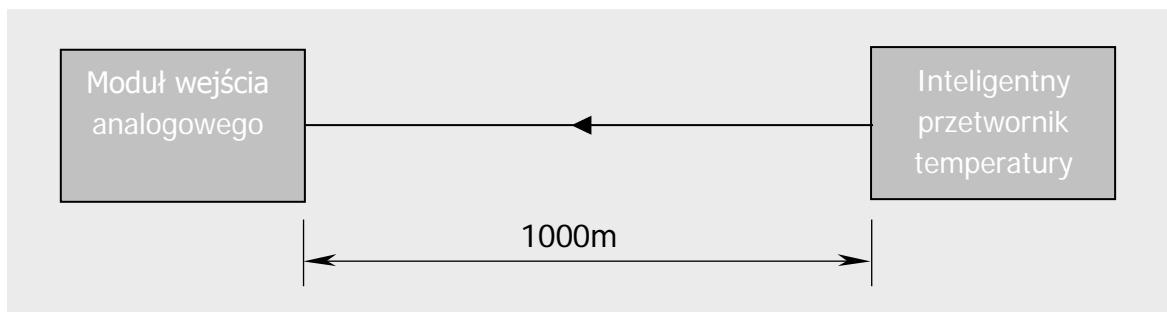


Rys. 2.9 Uproszczony schemat zastępczy prądowego źródła informacji z uwzględnieniem rezystancji kabli i zastępczym równoległy źródłem zakłóceń. Oznaczenia: I_z – prąd źródła zakłóceń.

2.6. EKONOMIA SIECI ANALOGOWEJ

Sukces aplikacyjny sieci analogowych wynika z korzystnej oceny ich właściwości technicznych, użytkowych i ekonomicznych. Z punktu widzenia ekonomicznego tzw. całkowity koszt posiadania TCO (*total cost of ownership*) sieci analogowych należy do najniższych. Na koszt ten składają się wszystkie składniki kosztowe, które są związane z siecią. Do składników tych należą między innymi: koszt projektu sieci, koszt urządzeń sieciowych, koszt sieci kablowej, koszt jej instalacji, koszty serwisu i energii, koszty amortyzacji i utrzymania pomieszczeń, w których znajdują się sieci, a także koszt utylizacji

sieci. Świadomość tych kosztów, a także relacji pomiędzy nimi jest istotna dla podejmowania właściwych decyzji. W rozdziale tym przedstawiony jedynie uproszczoną i wycinkową oceną relacji kosztowych jakie zachodzą pomiędzy kosztami urządzeń sieciowych i kosztami jego okablowania, oraz pomiędzy kosztami urządzeń a kosztami energii, którą zużywają.



Rys. 2.10. Szkic do analizy relacji pomiędzy kosztami urządzeń sieciowych i kosztami okablowania.

Przykład:

Przeanalizujemy relacje pomiędzy kosztami urządzeń sieciowych i kosztami okablowania dla przypadku sieci analogowej wykorzystywanej do zdalnego pomiaru temperatury. W skład sieci wchodzą dwa urządzenia sieciowe: jeden kanał modułu wejść analogowych sterownika programowalnego oraz inteligentny przetwornik temperatury. Oba urządzenia są połączone dwuprzewodową prądową siecią analogową. Do analizy przyjmiemy dane, które odzwierciedlają spodziewany i prawdopodobny poziom kosztów.

Dane:

| | |
|--|-------------|
| Koszt jednego kanału modułu wejścia analogowego | - 350 zł |
| Koszt inteligentnego przetwornika temperatury | - 450 zł |
| Koszty instalacji modułów sieciowych | - 200 zł |
| Koszt 1 m kabla wraz z jego ułożeniem i wykonaniem prowadnic | - 10 zł |
| Łączny koszt urządzeń sieciowych i ich instalacji | - 1000 zł |
| Łączny koszt realizacji połączenia kablowego (1000m) | - 10 000 zł |

Wniosek 1:

W podanym przykładzie koszt realizacji połączenia kablowego w stosunku do kosztów urządzeń sieciowych i ich instalacji jest **dominujący**.

Wniosek 2:

Dominujący koszt realizacji połączeń kablowych w stosunku do kosztów urządzeń sieciowych jest raczej regułą niż wyjątkiem.

Wniosek 3:

Modernizacja sieci analogowej jest ekonomicznie uzasadniona zwłaszcza wtedy gdy nie wymaga wymiany połączeń kablowych.

Wniosek 4:

Istnieją przemysłowe sieci komunikacji cyfrowej, które mogą wykorzystywać istniejące połączenia kablowe wykorzystywane do komunikacji analogowej.

Podstawowymi zaletami komunikacji analogowej są: jej prostota, akceptowalność techniczna, niska cena, prosty serwis, duża odporność na zaburzenia elektromagnetyczne, możliwość stosowania (z uwzględnieniem określonych warunków) w strefach zagrożonych wybuchem.

Do podstawowych wad komunikacji analogowej należy zaliczyć: ograniczoną przepustowośćą informacyjną sieci, brak możliwości realizacji złożonych topologii sieciowych i jednokierunkowość przesyłania informacji.



3. ISKROBEZPIECZEŃSTWO URZĄDZEŃ POMIAROWYCH I WYKONAWCZYCH

Projektowanie urządzeń i realizacja zadań automatyzacji w obszarach o zwiększym zagrożeniu wybuchem jest zadaniem trudnym i odpowiedzialnym. W zakresie stosowanych środków automatyzacji konieczne jest spełnienie specjalnych wymagań formułowanych w odpowiednich uregulowaniach normatywnych [1, 1]. Uregulowania te dotyczą wszystkich stosowanych środków automatyzacji, a więc zarówno urządzeń klasycznych jak i inteligentnych. Generalnie rzecz ujmując, stosowanie tych wymagań nie wyklucza jednak możliwości powstania wybuchu. Istnieje bardzo nikt, ale jednak skończone prawdopodobieństwo zaistnienia sytuacji, w której do takiego wybuchu dojść może. I odwrotnie, nie stosowanie tych wymagań zwiększa istotnie prawdopodobieństwo zaistnienia wybuchu. Standardy iskrobezpieczeństwa dotyczą wszystkich urządzeń, które mogą wytwarzać jedno lub więcej potencjalnych źródeł zapłonu, do których zaliczamy między innymi:

- iskry elektryczne,
- łuki elektryczne,
- płomienie,
- gorące powierzchnie,
- ładunek elektrostatyczny,
- reakcje chemiczne,
- uderzenia mechaniczne,
- tarcie mechaniczne,
- zapłon,
- energię akustyczną,
- promieniowanie jonizacyjne,
- promieniowanie elektromagnetyczne.

3.1. PODSTAWOWE DEFINICJE

Dla zapewnienia właściwego zrozumienia przedstawionego w tym rozdziale materiału zdefiniujmy podstawowe pojęcia z szeroko rozumianej sfery zagadnień związanych z iskrobezpieczeństwem.

Eksplozja to przebiegająca w sposób gwałtowny reakcja spalania dowolnej substancji palnej w otoczeniu tlenu powodująca uwolnienie dużej ilości energii.

Substancja palna może występować w postaci dowolnego stanu skupienia np. w postaci gazowej, zawiesiny, oparów, pyłu, cieczy, częstek ciała stałego, ciała stałego, itp.

Czynnikami warunkującymi powstanie eksplozji jest wystąpienie warunków, w których dochodzi do bezpośredniego kontaktu: substancji palnej, atmosfery zawierającej tlen i źródła zapłonu. Nie każdy zapłon substancji palnej może być uznany za eksplozję. Warunkiem koniecznym wystąpienia eksplozji jest propagacja przestrzenna zapłonu.

Gazowa atmosfera wybuchowa to mieszanina substancji palnych w postaci gazowej lub mieszanina par substancji palnych z powietrzem, w której po zapaleniu, proces spalania rozprzestrzenia się na całą nie spaloną mieszaninę.

Punkt parowania cieczy palnej to najniższa temperatura, w której nad poziomem cieczy palnej formuje się gazowa atmosfera wybuchowa. Punkt parowania jest nieco wyższy od temperatury parowania cieczy i zależy od jej właściwości fizycznych. Dla potrzeb technicznych ciecze palne zostały podzielone na cztery **klasy wybuchowości** (Tab.3.1).

| Klasa wybuchowości | Punkt parowania |
|--------------------|--|
| AI | <21°C |
| All | 21..55°C |
| AIII | >55..100°C |
| B | <21°C dla cieczy rozpuszczonych w wodzie w temperaturze 15°C |

Tab. 3.1 Klasa wybuchowości cieczy palnych

Maksymalna temperatura powierzchni to najwyższa temperatura osiągana przez urządzenie w czasie pracy przez dowolną jego część lub powierzchnię w warunkach najbardziej niekorzystnych (lecz dopuszczalnych) mogąą zainicjować zapłon otaczającej urządzenie gazowej atmosfery wybuchowej. Maksymalna temperatura powierzchni może być określana jako wewnętrzna lub zewnętrzna, w zależności od rodzaju stosowanej budowy przeciwwybuchowej.

Rodzaj budowy przeciwwybuchowej to określone środki techniczne, które są stosowane w urządzeniach elektrycznych w celu uniknięcia zapłonu otaczającej atmosfery wybuchowej.

Temperatura pracy to temperatura pracy urządzenia osiąganego w znamionowych warunkach pracy urządzenia.

3.2. STREFY ZAGROŻENIA WYBUCHEM

W obszarze, w którym może wystąpić zagrożenie wybuchem wyodrębniane są strefy zagrożenia. Kryterium podziału obszaru występowania na strefy zagrożenia wybuchem jest czas, w którym w danej strefie mogą pojawić się substancje palne. Strefy zagrożenia wybuchem oznaczone są symbolami numerycznymi. Symbole te jednocześnie identyfikują rodzaj substancji palnej. Podział na strefy zagrożenia wybuchem i kryteria klasyfikacyjne podano w Tab. 3.2.

| Strefy zagrożenia wybuchem | | |
|-----------------------------------|-----|---|
| Gaz | Pył | Kryterium klasyfikacji |
| 0 | 20 | Obszar, w którym substancje wybuchowe występują w sposób trwały |
| 1 | 21 | Obszar, w którym substancje wybuchowe występują sporadycznie |
| 2 | 22 | Obszar, w którym niebezpieczeństwo wybuchu może wystąpić bardzo rzadko i nie występuje w czasie normalnej pracy |

Tab. 3.2 Podział na strefy zagrożenia wybuchem

Rozległość stref zagrożenia wybuchem jest związana ze specyfiką konstrukcji i rozplanowania przestrzennego urządzeń i instalacji pracujących w tych strefach. Między innymi rozległość tych stref zależy od takich czynników jak: temperatura, ciśnienie, wilgotność, występowanie i intensywność prądów powietrznych, itp. Szczegółowy opis poszczególnych stref podany jest w [7].

3.3. KLASYFIKACJA URZĄDZEŃ

3.3.1. GRUPY URZĄDZEŃ

Urządzenia elektryczne przeznaczone do pracy w gazowych atmosferach wybuchowych są podzielone na dwie następujące grupy:

- grupa I – obejmująca urządzenia przeznaczone do stosowania w zakładach górniczych, w których występuje metanowa (NH_3) atmosfera wybuchowa,
- grupa II – obejmująca urządzenia przeznaczone do stosowania poza miejscami zdefiniowanymi w grupie I.

Osią podziału obu grup jest zakres stawianych wymagań konstrukcyjnych w stosunku do obudów urządzeń elektrycznych. Urządzenia grupy I muszą być wyposażone w odpowiednią obudowę uniemożliwiającą przedostanie się na zewnątrz iskry, która może potencjalnie powstać w urządzeniu elektrycznym. Rygor ten nie obejmuje obudów stosowanych dla grupy II.

Urządzenia grupy II podzielone są na trzy grupy zwane grupami wybuchowymi. Kryterium podziału jest ocena stopnia zagrożenia wybuchem.

| Grupa wybuchowa II | | | | |
|---------------------------|---------------------|--|--------------------------|--|
| Urządzenia grupy II | Zagrożenie wybuchem | | Wymagania wobec urządzeń | |
| IIA | niskie | | niskie | |
| IIB | średnie | | średnie | |
| IIC | wysokie | | wysokie | |

Tab. 3.3 Klasyfikacja urządzeń elektrycznych grupy II.



Urządzenia elektryczne przeznaczone do pracy w gazowych atmosferach wybuchowych powinny być odpowiednio oznakowane. Oznakowanie to powinno obejmować wskazanie grupy, podgrupy, zastosowane budowy iskrobezpieczne, maksymalną temperaturę powierzchni a także **grupę wybuchową**. W tabeli 3.3 podano charakterystykę określającą w sposób jakościowy stopień zagrożenia wybuchem i wymagania formułowane w stosunku do urządzeń elektrycznych należących do tych grup. Szczegółowe wymagania są formułowane w odpowiednich dokumentach normatywnych [4, 5].

W Tab. 3.4 przedstawiono typowe przykłady i stopień zagrożenia wybuchem.

| Grupa urządzeń | | |
|-----------------------|---|-----------|
| Grupa | Przykłady zagrożeń wybuchem | Grupa |
| I | Zagrożenie wybuchem metanu lub pyłu węglowego | metanowa |
| IIA | Zagrożenie wybuchem propanu, acetolu, alkoholu metylowego, alkoholu etylowego | propanowa |
| IIB | Zagrożenie wybuchem etylenu, siarkowodoru | etylenna |
| IIC | Zagrożenie wybuchem acetylu, wodoru, hydrazyny | wodorowa |

Tab. 3.4 Przykłady zagrożeń wybuchem

3.3.2. KATEGORIA BEZPIECZEŃSTWA URZĄDZENIA

Urządzenia elektryczne pracujące w strefach zagrożenia wybuchowego są kategoryzowane. Kategoria urządzenia jest klasą związaną z poziomem jego bezpieczeństwa w zastosowaniach w strefach zagrożonych wybuchem. Każda kategoria ma sformułowane wymagania co do sposobu zabezpieczenia w przypadku awarii. W Tab. 3.5 przedstawiono podstawowe wymagania konstrukcyjne na środki ochronne stawiane urządzeniom elektrycznym pracujących w strefach zagrożenia wybuchowego. W praktyce urządzenia kategorii 1 są stosowane w strefach zagrożenia 0 i 20, urządzenia kategorii 2 w strefach zagrożenia 1 i 21, natomiast urządzenia kategorii 3 są stosowane w strefach 2 i 22. Badania statystyczne wykazują, że ok. 95% urządzeń przeznaczonych do zastosowań w strefach zagrożonych wybuchem jest instalowane w strefach 1 i 21 a zaledwie ok. 5% w strefach 0 i 20.

| Grupa wybuchowa II | | |
|---------------------------|---|---|
| Kategoria | Opis kategorii | Wymagana ochrona |
| 1 | Ekstremalnie wysoki poziom bezpieczeństwa | Co najmniej dwa środki ochronne na wypadek, gdyby jeden zawiódł |
| 2 | Wysoki poziom bezpieczeństwa | Co najmniej jeden środek ochronny |
| 3 | Normalny poziom bezpieczeństwa | Brak dodatkowych środków ochronnych |

Tab. 3.5 Kategorie bezpieczeństwa urządzeń dla grupy wybuchowej II.



3.3.3. KLASYFIKACJA TEMPERATUROWA URZĄDZEŃ

Klasifikacja temperaturowa urządzeń jest odrębna dla każdej grupy urządzeń elektrycznych przeznaczonych do pracy w gazowych atmosferach wybuchowych. Kryterium klasycyfikacyjnym w obu przypadkach jest maksymalna temperatura powierzchni i rodzaj atmosfery wybuchowej.

W przypadku urządzeń elektrycznych należących do grupy I w oznakowaniu urządzenia powinna być podana wartość maksymalnej rzeczywistej temperatury powierzchni. W urządzeniach tych maksymalna temperatura powierzchni nie powinna przekraczać:

- 150°C dla dowolnej powierzchni, na której może osadzić się warstwa pyłu węglowego,
- 450°C dla dowolnej powierzchni, na której osadzenie pyłu węglowego jest wykluczone np. w wyniku zastosowania odpowiednich uszczelnień.

W przypadku urządzeń elektrycznych należących do grupy II stosowany jest podział na sześć klas temperaturowych oznaczanych symbolem T i odpowiednią cyfrą. Kryterium klasycyfikacyjnym jest maksymalna temperatura powierzchni. Ogólnie, im wyższa jest klasa temperaturowa, tym niższa jest maksymalna temperatura maksymalna powierzchni. Klasycyfikację temperaturową urządzeń elektrycznych grupy II podano w Tab. 3.6. przedstawiono:

| Klasa temperaturowa | Maksymalna temperatura powierzchni w [°C] |
|----------------------------|--|
| T1 | 450 |
| T2 | 300 |
| T3 | 200 |
| T4 | 135 |
| T5 | 100 |
| T6 | 85 |

Tab. 3.6 Klasycyfikacja temperaturowa urządzeń elektrycznych grupy II

3.3.4. KLASYFIKACJA URZĄDZEŃ ZE WZGLĘDU NA POLE POWIERZCHNI

Urządzenia elektryczne przeznaczone do pracy w atmosferach wybuchowych powinny być zaprojektowane w taki sposób, aby zarówno w normalnych warunkach użytkowania jak również podczas napraw, konserwacji i czyszczenia nie występowało niebezpieczeństwo zapłonu otaczającego gazu. Niebezpieczeństwo to może być spowodowane przez przeskok iskry elektrycznej pomiędzy elementami niemetalowymi urządzenia w wyniku różnicy potencjałów tych elementów spowodowanej nagromadzeniem na nich ładunków elektrostatycznych. W stosunku do urządzeń elektrycznych, które są zbudowane w taki sposób, że możliwy jest dostęp do ich elementów wykonanych z materiałów niemetalicznych stosowana jest klasycfikacja, której kryterium jest powierzchnia materiałów niemetalicznych.

Procedura wyznaczenia pola powierzchni jest następująca:

- dla elementów płaskich polem powierzchni jest pole powierzchni eksponowanej, która może ulec naładowaniu ładunkiem elektrostatycznym,
- dla elementów o powierzchniach przestrzennych, za pole powierzchni uznaje się największe pole dowolnego rzutu tego elementu,
- w przypadku elementów niemetalowych rozdzielonych elementami przewodzącymi i uziemionymi, ich pola powierzchni powinny być wyznaczane niezależnie.

Klasyfikację urządzeń ze względu na pole powierzchni przedstawiono w Tab. 3.7.

| Maksymalne pole powierzchni w [mm²] | | | | |
|---|-----------------------------------|-----------|-----------|-----------|
| Urządzenia grupy I | Urządzenia grupy II | | | |
| | Strefa (zgodnie z PN-EN 60079-10) | Grupa IIA | Grupa IIB | Grupa IIC |
| 1000 | 0 | 5000 | 2500 | 400 |
| | 1 | 10000 | 10000 | 2000 |
| | 2 | 10000 | 10000 | 2000 |

Tab. 3.7 Klasyfikacja budowy iskrobezpiecznej ze względu na powierzchnię elementów niemetalowych.

Inteligentne urządzenia pomiarowe i wykonawcze dzięki wbudowanym funkcjom diagnostycznym i możliwości realizacji zdalnej parametryzacji i konfiguracji są chętnie stosowane w strefach zagrożonych wybuchem. Urządzenia te w przeciwieństwie do urządzeń konwencjonalnych nie wymagają w zasadzie żadnej obsługi bezpośredniej. Dzięki temu możliwe jest zwiększenie stopnia bezpieczeństwa zarówno samego procesu jak i operatorów procesu. Stąd też znaczna część inteligentnych urządzeń pomiarowych i wykonawczych przeznaczonych jest do zastosowań w strefach zagrożenia 0 i 1 i jest klasyfikowana w grupie wybuchowej IIC.

3.3.5. OZNAKOWANIE URZĄDZEŃ ELEKTRYCZNYCH

Urządzenia elektryczne przeznaczone do pracy atmosferze wybuchowej powinny być odpowiednio oznakowane. Jest to szczególnie ważne z punktu widzenia zapewnienia warunków bezpieczeństwa. Oznakowanie powinno być umieszczone w widocznym miejscu i powinno zawierać:

- nazwę producenta lub jego zarejestrowany znak handlowy,
- oznaczenie typu urządzenia ustalone przez producenta,
- symbol Ex wskazujący, że urządzenie elektryczne odpowiada jednemu lub wielu rodzajom budowy przeciwwybuchowej spełniających wymagania norm
- symbol zastosowanego rodzaju (rodzajów) budowy przeciwwybuchowej:



| Symbol rodzaju budowy | Rodzaj budowy przeciwybuchowej |
|------------------------------|---|
| d | osłona ognioszczelna |
| e | budowa wzmacniona |
| ia | iskrobezpieczeństwo, poziom zabezpieczenia „ia” |
| ib | iskrobezpieczeństwo, poziom zabezpieczenia „ib” |
| ma | hermetyzacja, poziom zabezpieczenia „ma” |
| mb | hermetyzacja, poziom zabezpieczenia „mb” |
| nA | rodzaj n, sposób zabezpieczenia „nA” |
| nC | rodzaj n, sposób zabezpieczenia „nC” |
| nL | rodzaj n, sposób zabezpieczenia „nL” |
| nR | rodzaj n, sposób zabezpieczenia „nR” |
| o | osłona olejowa |
| px | osłona gazowa z nadciśnieniem, poziom zabezpieczenia „px” |
| py | osłona gazowa z nadciśnieniem, poziom zabezpieczenia „py” |
| pz | osłona gazowa z nadciśnieniem, poziom zabezpieczenia „pz” |
| q | osłona piaskowa |

Tab. 3.8 Klasyfikacja i rodzaje budowy przeciwybuchowej

- symbol grupy urządzenia elektrycznego (I, II, IIA, IIB, IIC),
- symbol klasy temperaturowej (T1, T2, T3, T4, T5, T6),
- numer fabryczny,
- nazwę wydawcy oraz oznaczenie certyfikatu iskrobezpieczeństwa,
- opcjonalne wskazanie warunków bezpiecznego użytkowania (symbol X),

Przykład oznakowania urządzenia:

II 2G Ex d ia IIC T5

| | |
|-----|---|
| II | Grupa urządzenia. Urządzenie przeznaczone do stosowania poza zakładami górnictwymi, w których występuje metanowa atmosfera wybuchowa. |
| 2G | Kategoria urządzenia. Urządzenie zapewniające wysoki stopień bezpieczeństwa (2) przeznaczone do pracy w gazowej atmosferze wybuchowej (G) |
| Ex | Ochrona wybuchowa zgodna z zharmonizowanymi normami europejskimi |
| d | Rodzaj budowy przeciwybuchowej. Urządzenie jest wyposażone w obudowę ognioszczelną. |
| ia | Rodzaj iskrobezpieczeństwa. Poziom zabezpieczenia „ia” określa stopień bezpieczeństwa elektrycznych obwodów wejściowych i wyjściowych urządzenia. Obwody wejściowe i wyjściowe urządzeń przenoszą sygnały elektryczne o ograniczonej mocy. Obwody wejściowe i wyjściowe mogą być wprowadzane do stref zagrożenia wybuchem 0, 1 i 2. |
| IIC | Grupa wybuchowa. Urządzenie może być stosowane w warunkach wysokiego zagrożenia wybuchem. |
| T5 | Klasa temperaturowa. Maksymalna temperatura powierzchni urządzenia nie może być wyższa niż 100°C. |

Tab. 3.8 Przykład oznakowania urządzenia elektrycznego.



3.4. OBWODY ISKROBEZPIECZNE

3.4.1. DEFINICJE

Iskrobezpieczeństwo „i” to sposób budowy przeciwwybuchowej, który ogranicza ilość energii rozpraszanej lub magazynowanej wewnątrz urządzenia elektrycznego i w jego okablowaniu do poziomu niższego niż ten, przy którym w atmosferze wybuchowej mogłoby dojść do zapłonu wywołanego przez iskrę lub ogrzanie jego powierzchni.

Urządzenie iskrobezpieczne to urządzenie elektryczne, którego wszystkie obwody są obwodami iskrobezpiecznymi.

Obwód iskrobezpieczny to obwód, w którym dowolna iskra lub dowolny efekt cieplny wywołyany w obwodzie w określonych warunkach nie jest zdolny do wywołania zapłonu w gazowej atmosferze wybuchowej. Obwód iskrobezpieczny zachowuje cechę iskrobezpieczeństwa zarówno w warunkach nominalnych jego pracy jak również w warunkach z określonymi uszkodzeniami obwodu.

Uszkodzenie to dowolny defekt dowolnego elementu, oddzielenia izolacyjnego lub połączenia pomiędzy elementami od którego zależy iskrobezpieczeństwo obwodu i który jest nieuszkadzalny.

Element lub zespół nieuszkadzalny to element lub zespół, którego prawdopodobieństwo **uszkodzenia** w trakcie pracy lub składowania urządzenia jest na tyle niskie, że może nie być brane pod uwagę.

Nieuszkadzalne połączenie to połączenie lub złącze, lub okablowanie lub ścieżka obwodu drukowanego, których prawdopodobieństwo **przerwania** w trakcie pracy lub składowania urządzenia jest na tyle niskie, że może nie być brane pod uwagę.

Nieuszkadzalne oddzielenie izolacyjne lub separacja to oddzielenie izolacyjne lub separacja pomiędzy elementami przewodzącymi obwodu, których prawdopodobieństwo **zwarcia** w trakcie pracy lub składowania urządzenia jest na tyle niskie, że może nie być brane pod uwagę.

Uszkodzenie zliczane to uszkodzenie w częściach urządzenia elektrycznego, których budowa jest zgodne ze specyfikacją normy [5], a więc dotyczy przypadku uszkodzenia elementów praktycznie nieuszkadzalnych.

Maksymalna pojemność zewnętrzna C_0 to największa pojemność, która może być przyłączona do zacisków urządzenia bez naruszania rodzaju budowy przeciwwybuchowej.

Maksymalna indukcyjność zewnętrzna L_0 to największa indukcyjność, która może być przyłączona do zacisków urządzenia bez naruszania rodzaju budowy przeciwwybuchowej.

Maksymalne napięcie wyjściowe U_0 to największe napięcie (szczytowe przemienne lub stałe), które może się pojawić na zaciskach urządzenia przy napięciu zasilania nie przekraczającym wartości maksymalnej.

Maksymalny prąd wyjściowy I_0 to największy prąd (szczytowy przemienny lub stały), który może być pobrany z zacisków urządzenia.

Maksymalna moc wyjściowa P_o to największa moc, którą można pobrać z urządzenia.

Maksymalna pojemność wewnętrzna C_i to całkowita wypadkowa pojemność wewnętrzna urządzenia uznana za pojemność występującą na jego zaciskach.

Maksymalna indukcyjność wewnętrzna L_i to całkowita wypadkowa indukcyjność wewnętrzna urządzenia uznana za indukcyjność występującą na jego zaciskach.

Maksymalny prąd wejściowy I_i to największy prąd (szczytowy przemienny lub stały), który można doprowadzić do zacisków urządzenia bez naruszania rodzaju budowy przeciwwybuchowej.

Maksymalne napięcie wejściowe U_i to największe napięcie (szczytowe przemienne lub stałe), który można doprowadzić do zacisków urządzenia bez naruszania rodzaju budowy przeciwwybuchowej.

Maksymalna moc wejściowa P_i to największa moc, którą można doprowadzić do zacisków urządzenia bez naruszania rodzaju budowy przeciwwybuchowej.

Maksymalna wartość skuteczna napięcia przemiennego lub stałego U_m to największe napięcie, które można doprowadzić do zacisków urządzenia towarzyszącego i przeznaczonych dla obwodu, którego energia nie jest ograniczona, nie naruszając rodzaju budowy przeciwwybuchowej.

Diodowa bariera ochronna to zespół złożony z równolegle połączonych diod (zawierających diody Zenera) zabezpieczony przez szeregowo dołączone bezpieczniki lub/i rezystory lub ich kombinacje. Diodowa bariera ochronna jest zwykle wykonywana w postaci odrębnego urządzenia.

3.4.2. POZIOMY ISKROBEZPIECZEŃSTWA URZĄDZEŃ ELEKTRYCZNYCH

Urządzenia iskrobezpieczne klasyfikowane są w trzech poziomach iskrobezpieczeństwa: „ia”, „ib” lub „ic”.

3.4.2.1. . POZIOM ISKROBEZPIECZEŃSTWA „IA”

Poziom iskrobezpieczeństwa „ia” posiadają te urządzenia elektryczne, które po zasilaniu napięciami U_i i U_m , nie są zdolne do zapłonu atmosfery wybuchowej w przypadku zaistnienia każdej z niżej wymienionych okoliczności:

- w warunkach pracy normalnej i w warunkach pracy z uwzględnieniem wszystkich najbardziej niekorzystnych uszkodzeń niezliczanych,
- w warunkach pracy normalnej i w warunkach pracy z uwzględnieniem jednego uszkodzenia zliczanego i wszystkich możliwych najbardziej niekorzystnych uszkodzeń niezliczanych,
- w warunkach pracy normalnej i w warunkach pracy z uwzględnieniem dwóch uszkodzeń zliczanych i wszystkich możliwych najbardziej niekorzystnych uszkodzeń niezliczanych.

3.4.2.2. . POZIOM ISKROBEZPIECZEŃSTWA „IB”

Poziom iskrobezpieczeństwa „ib” posiadają te urządzenia elektryczne, które po zasileniu napięciami U_i i U_m , nie są zdolne do zapłonu atmosfery wybuchowej w przypadku zaistnienia każdej z niżej wymienionych okoliczności:

- a) w warunkach pracy normalnej i w warunkach pracy z uwzględnieniem wszystkich najbardziej niekorzystnych uszkodzeń nieszczelnich,
- b) w warunkach pracy normalnej i w warunkach pracy z uwzględnieniem jednego uszkodzenia zliczanego i wszystkich możliwych najbardziej niekorzystnych uszkodzeń nieszczelnich,

3.4.2.3. POZIOM ISKROBEZPIECZEŃSTWA „IC”

Poziom iskrobezpieczeństwa „ic” posiadają te urządzenia elektryczne, które po zasileniu napięciami U_i i U_m , nie są zdolne do zapłonu atmosfery wybuchowej w warunkach pracy normalnej.

W przypadku oceny iskrobezpieczeństwa urządzenia na poziomie „ic” nie są zatem wymagane rozważania dotyczące analizy zdolności do zapłonu atmosfery wybuchowej z założeniem o nieuszkadzalności elementów i zespołów. Wówczas istotne są rozważania dotyczące energii rozpraszanej i magazynowanej przez te elementy i efektów termicznych z tym związanych.

3.4.3. OCENA WARUNKÓW DO POWSTANIA ISKRY

Obwody elektryczne powinny być oceniane oraz ewentualnie testowane na przypadek zastosowanych środków ograniczenia energii iskier, które w przypadku powstania w obwodzie, miałyby zdolność do zapłonu atmosfery wybuchowej. Ocena lub test warunków powstawania iskry dotyczy badania każdego punktu w obwodzie, w którym może nastąpić zwarcie lub rozwarcie elektryczne.

Testy służące do oceny energii iskry są przeprowadzane w warunkach normalnych pracy urządzenia, a także w warunkach z symulowanymi uszkodzeniami. Badania są przeprowadzane z użyciem odpowiednich aparatów zwanych iskiernikami. Iskiernik składa się z układu elektrod umieszczonych w komorze o objętości co najmniej 250 cm^3 . Iskiernik wytwarza iskry zwierając i przerywając badany obwód elektryczny zanurzony w odpowiedniej probiercej mieszaninie wybuchowej. Przerwy i zwarcia dotyczą również obwodów uziemień obwodu. Skład mieszaniny wybuchowej jest zależny od deklarowanej grupy wybuchowej badanych urządzeń elektrycznych oraz współczynnika bezpieczeństwa. Do testów ze współczynnikiem bezpieczeństwa 1,0 stosowane są mieszanki metanowo-powietrzne, propanowo-powietrzne, etylenowo-powietrzne i wodorowo-powietrzne. Do testów ze współczynnikiem bezpieczeństwa 1,5 stosowane są mieszanki tlenowo-wodorowo-powietrzne i tlenowo-wodorowe.

W przypadku oceny warunków do powstania iskry dla poziomów iskrobezpieczeństwa „ia” i „ib” testy z iskiernikiem powinny być prowadzone dla nominalnych warunków pracy urządzenia w jego stanie normalnym i w stanie z jednym lub dwoma uszkodzeniami zliczanymi zależnie od deklarowanego poziomu iskrobezpieczeństwa urządzenia. Testy powinny być prowadzone w warunkach obciążenia badanego obwodu maksymalnymi wartościami zewnętrznych pojemności C_o , indukcyjności L_o , lub stosunku L_o/R_o . Uszkodzenie wprowadzane przez iskiernik jest traktowane jako niezliczane dla wszystkich złącz elektrycznych i wszystkich połączeń wewnętrznych. Zastosowanie iskiernika nie jest nieograniczone. W szczególności, iskiernik nie powinien byćłączany równolegle do elementów separujących spełniających wymogi nieuszkadzalności i nie może byćłączany szeregowo z połączonymi nieuszkadzalnymi.

Typowo, iskiernik wyposażony jest w wirujący uchwyt umożliwiający zamocowanie do czterech elektrod z tungstenu. Elektrody mają postać odcinków drutu o długości 11mm i średnicy 0,2 mm. Uchwyt elektrod jest napędzany silnikiem elektrycznym i wiruje z prędkością 80 obr/min. Ten sam silnik, przez redukcyjną przekładnię mechaniczną, napędza rowkowaną tarczę wykonaną z kadmu. Stosunek prędkości obrotowej uchwytu z elektrodami do prędkości obrotowej tarczy kadmowej wynosi 50:12. W wyniku wzajemnego względnego ruchu elektrod po rowkowanej powierzchni tarczy kadmowej następują okresowe zwarcia i rozwarcia elektrod i dysku.

Obwód elektryczny uznaje się za spełniający wymagania dotyczące ograniczenia energii iskry jeśli w czasie testów z iskrownikiem nie wystąpi ani jeden przypadek zapłonu testowej mieszanki wybuchowej. Test jest realizowany:

- a) dla obwodów prądu stałego przez 5 minut (po 200 obrotów tarczy dla każdej polaryzacji elektrod),
- b) dla obwodów prądu przemiennego przez 12,5 minuty (1000 obrotów tarczy).

3.4.3.1. OCENA WARUNKÓW DO POWSTANIA ZAPŁONU W WYNIKU EFEKTÓW CIEPLNYCH

Na ocenę warunków powstawania zapłonu w wyniku efektów cieplnych ma wpływ wiele czynników. Wśród nich należy wymienić:

- temperaturę otoczenia,
- zewnętrzne źródła powodujące nagrzewanie lub chłodzenie,
- temperaturę pracy,
- maksymalną temperaturę powierzchni.

Jeśli urządzenie elektryczne jest zaprojektowane do użytkowania w zakresie temperatur otoczenia od -20°C do +40°C to nie jest wymagane żadne specjalne oznakowanie temperatur pracy. Jeśli urządzenie jest zaprojektowane do użytku w innym zakresie temperatur, to w oznaczeniu przyrządu powinien znaleźć się symbol „Ta” wraz z wyszczególnionym zakresem temperatur użytkowania.

3.5. PRZYKŁADY OCENY ISKROBEZPIECZNOŚCI URZĄDZEŃ

3.5.1. OCENA NIEUSZKADZALNOŚCI ŚCIEŻEK NA PŁYTKACH OBWODÓW DRUKOWANYCH

Obwód drukowany pewnego urządzenia przeznaczonego do zastosowania w strefach zagrożonych wybuchem wykonany jest na laminacie szklano-epoksydowym FR4 o nominalnej grubości 1,6 mm grubości i pokrytym dwustronnie warstwą miedzi o nominalnej grubości 35 μ m. Nominalna szerokość najczęstszych ścieżek tego obwodu wynosi 0,254mm. Nominalny prąd zasilania obwodów elektrycznych płytki w wynosi 20mA, natomiast maksymalny prąd wejściowy I ; obwodów elektrycznych płytki w warunkach jej uszkodzenia wynosi 100mA. Urządzenie, w którym będzie zamontowana płytka obwodu drukowanego będzie pracowało w warunkach zewnętrznych, w których maksymalna temperatura otoczenia będzie wynosiła 80°C.

Procedura klasyfikacji temperaturowej zakłada uwzględnienie w procesie oceny nieuszkadzalności zasady najgorszego przypadku. W tym celu muszą być wyznaczone parametry graniczne konieczne do zdefiniowania takiego przypadku. W naszym przykładzie:

- minimalna grubość płytki wynosi 1,5mm,
- minimalna grubość warstwy miedzi wynosi 33 μ m,
- minimalna szerokość ścieżek drukowanych wynosi 0,20mm
- na płytce występują ścieżki przebiegające pod elementami rozpraszającymi moc o wartości $\geq 0,25W$,
- maksymalna temperatura otoczenia płytki będzie wynosiła 80°C.

Ponieważ ścieżki są wykonane z miedzi, to do klasyfikacji temperaturowej ścieżek na obwodach drukowanych ma zastosowanie tabela 4 normy EN 60079-11:2007.

| Klasa temperaturowa | Maksymalny dopuszczalny prąd w [A] |
|---------------------|------------------------------------|
| T1 do T4 | 1,8 |
| T5 | 1,4 |
| T6 | 1,2 |

Tab. 3.9. Klasyfikacja temperaturowa ścieżek na płytach drukowanych jednostronne o grubości 0,2 mm w maksymalnej temperaturze otoczenia równej 40°C.

W celu dokonania oszacowania iskrobezpieczności ścieżek zastosowano następujące współczynniki korekcyjne:

- a) współczynnik 1,2 (uwaga nr 3 w tablicy 4 normy EN 60079-11:2007) wynikająca z faktu, że grubość płytki drukowanej mieści się w granicach [0,5 .. 1,6]mm),
- b) współczynnik 1,5 (uwaga nr 4 w tablicy 4 normy EN 60079-11:2007) wynikająca z faktu, że płytka drukowana jest płytka laminowaną dwustronnie),

- c) współczynnik 1,5 (uwaga nr 8 w tablicy 4 normy EN 60079-11:2007) wynikająca z faktu, że na płytce drukowanej występują ścieżki pod elementami rozpraszającymi energię o wartości $\geq 0,25\text{W}$),
- d) współczynnik 2,0 (uwaga nr 9 w tablicy 4 normy EN 60079-11:2007) wynikająca z faktu, że na płytce drukowanej występują elementy, które mogą rozproszyć energię $\geq 0,25\text{W}$ w warunkach pracy normalnej lub z uszkodzeniami.
- e) współczynnik 1,3 (uwaga nr 11 w tablicy 4 normy EN 60079-11:2007) wynikająca z faktu, że temperatura otoczenia może osiągnąć temperaturę 80°C .
- f) współczynnik bezpieczeństwa 1,5.

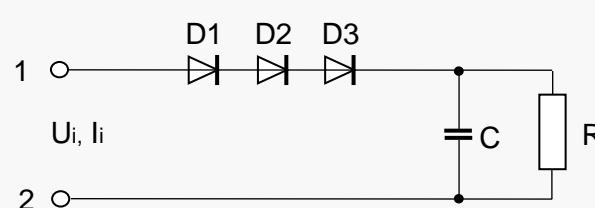
Iloczyn współczynników korekcyjnych a)..f) wynosi: $1,2 \cdot 1,5 \cdot 1,5 \cdot 2,0 \cdot 1,3 \cdot 1,5 = 10,53$

Maksymalny prąd zasilania obwodów wynosi $I_i = 100\text{mA}$. Maksymalny obliczeniowy prąd dla klasyfikacji temperaturowej ścieżek obwodów drukowanych wynosi $100\text{mA} \cdot 10,53 = 1,053\text{A}$ i nie przekracza maksymalnej wartości prądu w tabeli 3.8 dla żadnej klasy temperaturowej.

Wniosek: wszystkie ścieżki obwodu drukowanego mają klasyfikację temperaturową T6.

3.5.2. OCENA NIEUSZKADZALNOŚCI ZESPOŁU DIOD W OBWODZIE ISKROBEZPIECZNYM KLASYFIKOWANYM DO GRUPY IIC NA POZIOMIE „IA”

W obwodzie wejściowym obwodu elektronicznego zastosowano zespół trzech połączonych szeregowo diod zabezpieczających zewnętrzne źródło zasilania przed prądem rozładowania pojemności wewnętrznej zasilanego obwodu w przypadku gdyby polaryzacja zacisku nr 1 była dodatnia w stosunku do polaryzacji zacisku nr 2 (rys. 3.1). Tego typu prosty zespół zabezpieczeń jest dość często stosowany w konstrukcjach obwodów iskrobezpiecznych w celu ograniczenia wartości pojedynczej wejściowej C_i obwodu widzianej od strony zacisków 1 i 2. Warunkiem uznania iskrobezpieczności takiego zespołu jest wykazanie jego nieuszkadzalności w warunkach granicznych jego pracy, włączając w to pracę w warunkach z uszkodzeniami. W przypadku poziomu iskrobezpieczeństwa „ia” należy wykazać nieuszkadzalność takiego zespołu w przypadku wystąpienia dwóch uszkodzeń zliczalnych, których skutki są najgorsze z punktu widzenia oceny iskrobezpieczności. W związku z tym jeśli założymy, że jednocześnie uszkodzeniom (np. zwarciom) uległy dwie dowolne diody np. D2 i D3, to dioda D1 powinna spełnić funkcje ochronne.



Rys.3.1. Uproszczony schemat elektryczny do oceny obwodu elektrycznego.

W obwodzie zastosowano diody typu S1M. Podstawowe parametry diod przedstawiono w tabeli 3.10.

| Dioda typ S1M | | | | | |
|----------------------------------|--|------------|-------------|--------------------|---|
| Podstawowe parametry elektryczne | | | | | |
| Lp. | Parametr | Symbol | Wartość | Jednostka fizyczna | Uwagi |
| 1 | Maksymalne napięcie wsteczne | U_{RRM} | 1000 | V | |
| 2 | Maksymalny prąd w kierunku przewodzenia | I_F | 1,0 | A | 100°C |
| 3 | Maksymalna temperatura złącza | T_{JMAX} | 150 | °C | |
| 4 | Rezystancja termiczna złącze - otoczenie | R_{9JA} | 85 | K/W | |
| 5 | Dopuszczalna moc diody | P_{MAX} | 1 1 0 | W W W | $T_a=100^\circ\text{C}$ $T_a=100^\circ\text{C}$ $T_a=150^\circ\text{C}$ |

Tab. 3.9 Podstawowe parametry diod typu S1M.

| Lp | Parametr | Symbol | Wartość | Sposób wyznaczenia |
|----|---|---------------|---------|---|
| 1 | Maksymalna moc wydzielana na diodzie | P_D | 82 mW | $P_D=0,1\text{A}\cdot0,82\text{V}=82\text{mW}$ |
| 2 | Maksymalna moc wydzielana na diodzie ze współczynnikiem bezpieczeństwa 1,5 | $P_{D1,5}$ | 123 mW | $P_{D1,5}=82\text{mW}\cdot1,5=123\text{mW}$ |
| 3 | Maksymalny przyrost temperatury złącza | ΔT | 10,5 K | $\Delta T = R_{9JA} \cdot P_{D1,5} = 85\text{K/W} \cdot 0,123\text{W} = 10,5\text{K}$ |
| 4 | Maksymalna temperatura złącza w temperaturze $T_a=80^\circ\text{C}$ | T_J | 90,5°C | $T_{JMAX}=80^\circ\text{C}+10,5^\circ\text{C}=90,5^\circ\text{C}$ |
| 5 | Maksymalna dopuszczalna moc diody ze współczynnikiem bezpieczeństwa 1,5 | $P_{DMAX1,5}$ | 0,667 W | $T_a=80^\circ\text{C}$ |
| 6 | Maksymalne napięcie robocze diody ze współczynnikiem bezpieczeństwa 1,5 | $U_{D1,5}$ | 45V | $T_a=80^\circ\text{C}$ |
| | Wniosek: Dioda S1M jest nieuszkadzalna dla $T_a=80^\circ\text{C}$. | | | $P_{D1,5} < P_{MAX}$ $I_{D1,5} < I_F$ $U_{D1,5} < U_{RRM}$ $T_J < T_{JMAX}$ |

Tab. 3.11 Ilustracja kolejnych kroków procedury oceny iskrobezpieczeństwa diody S1M zastosowanej w zespole ochronnym jak na rys. 3.1.

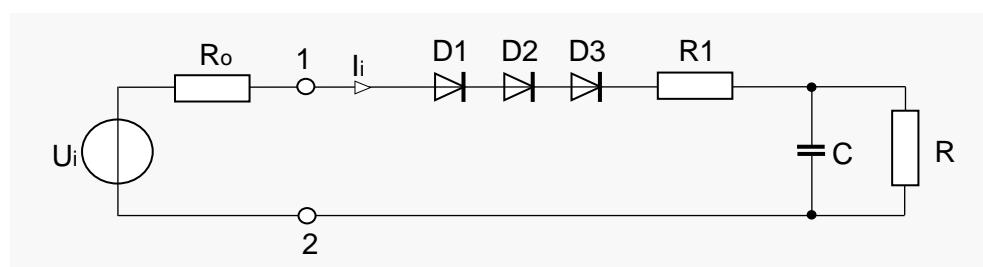


Ocenę nieuszkodzalności diody S1M w obwodzie jak na rysunku 3.1 przedstawiono w tabeli 3.11. W ocenie tej założono, że:

- maksymalna wartość prądu diody będzie równa $I_i = 100\text{mA}$,
- maksymalna napięcia wejściowego będzie równa $C_i = 30\text{V DC}$,
- współczynnik bezpieczeństwa ma wartość 1,5.
- maksymalna temperatura otoczenia będzie wynosiła 80°C .

3.5.3. OCENA NIEUSZKADZALNOŚCI REZYSTORA W OBWODZIE ISKROBEZPIECZNYM KLASYFIKOWANYM DO GRUPY IIC NA POZIOMIE „IA”

W obwodzie wejściowym obwodu elektronicznego zastosowano zespół trzech połączonych szeregowo diod zabezpieczających zewnętrzne źródło zasilania obwodu przed prądem rozładowania pojemności wewnętrznej obwodu (jak na rys 3.1) i dodatkowo rezystor szeregowy R_1 ograniczający prąd w obwodzie. Należy dokonać oceny nieuszkadzalności tego rezystora.



Rys.3.3. Uproszczony schemat elektryczny do oceny nieuszkadzalności rezystora R_1 .

Ocenę nieuszkadzalności rezystora R_1 w obwodzie jak na rysunku 3.2 przedstawiono w tabeli 3.12. W ocenie tej założono, że:

- maksymalna wartość prądu wejściowego będzie równa $I_i = 100\text{mA}$,
- maksymalna napięcia wejściowego będzie równa $C_i = 30\text{V DC}$,
- minimalna wartość rezystancji wyjściowej źródła zasilania będzie wynosiła $R_o = 300\Omega$,
- nominalna wartość rezystancji rezystora R_1 będzie wynosiła 20Ω ,
- minimalny odstęp pomiędzy polami lutowniczymi rezystora R_1 nie będzie mniejszy niż $d = 2 \text{ mm}$.
- minimalny spadek napięcia na nieuszkadzalnym szeregowym prądowym ograniczniku diodowym (D1, D2, D3) wynosi $0,82\text{V}$,
- nominalna moc rezystora będzie wynosiła 1W w temperaturze 25°C ,
- współczynnik bezpieczeństwa ma wartość 1,5,
- maksymalna temperatura otoczenia będzie wynosiła 80°C .

W analizie założymy, że uszkodzeniom uległa dowolna para diod w nieuszkadzalnym zespole trzech diod (D1, D2, D3). Zespół spełnia rolę ogranicznika szeregowego prądu, ponieważ zmniejsza napięcie na rezystancji obciążenia. Wówczas należy wykazać nieuszkadzalność rezystora R1. Analizę nieuszkadzalności rezystora R1 przedstawiono w tabeli 3.12.

| Rezystor | R1 |
|--|--|
| Typ | RC-6432-J -100 |
| Producent | Samsung |
| Oznaczenie handlowe | 2512-1W-10R-5% |
| Wartość nominalna rezystancji | 20 Ω |
| Wartość nominalna tolerancji | 5 % |
| Napięcie graniczne | 200V |
| Moc nominalna (70°C) | 1,0W |
| Wymiary | 6,4 x 3,2mm |
| Temperaturowy współczynnik rezystancji | $\pm 200 \cdot 10^{-6} / ^\circ C$ |
| Współczynnik spadku mocy (powyżej 70°C) | $-1/(125-70)K = \approx 1,82\% / K$ |
| Maksymalna temperatura pracy | 125°C |
| Nieuszkadzalność rezystora | |
| Technologia wykonania rezystora | grubowarstwowa |
| Minimalna odległość pomiędzy polami lutowniczymi rezystora | D=4,5mm |
| Wartość maksymalna rezystancji | $R_{max} = 21 \Omega$ |
| Wartość minimalna rezystancji | $R_{min} = 19 \Omega$ |
| Maksymalny prąd rezystora | $I_R = \frac{30V - 0,82V}{300\Omega + 19\Omega} \approx 91,5mA$ |
| Maksymalna moc wydzielana na rezystorze | $P_{max} = (I_R)^2 * R_{min}$ $P_{max} = (0,0915A)^2 * 19 \Omega \approx 0,160W$ |
| Wartość mocy maksymalnej rozpraszanej przez rezistor w temperaturze otoczenia 80°C | $P_{max(80C)} = 1W * [1 - 0,0182 * (80 - 70)] = 0,818W$ |
| Wartość mocy maksymalnej rozpraszanej przez rezistor w temperaturze otoczenia 80°C ze współczynnikiem bezpieczeństwa 1,5 | $P_{max(80C)1,5} = 0,818 / 1,5 \approx 0,545W$ |
| Warunki nieuszkadzalności rezystora R1 w temperaturze otoczenia $T_a = 80^\circ C$ | $P_{max} < P_{max(80C)1,5}$ $d < D$ $0,160W < 0,545W$ |
| Wniosek | Warunek nieuszkadzalności rezystora R1 w temperaturze otoczenia $T_a = 80^\circ C$ spełniony |

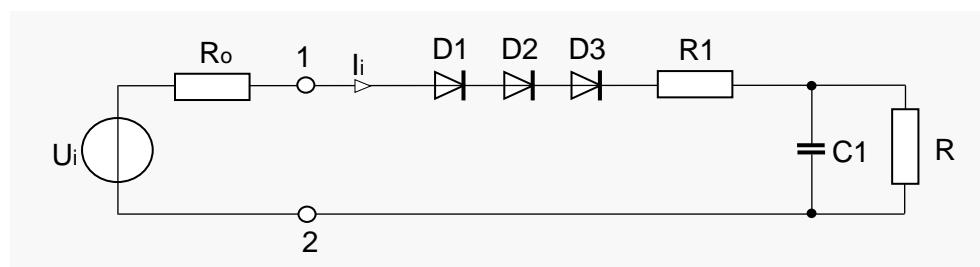
Tab. 3.12 Ilustracja kolejnych kroków procedury oceny nieuszkadzalności rezystora R1 zastosowanego w obwodzie jak na rys. 3.2.

Komentarz: Zgodnie z analizą przedstawioną w tablicy 3.12., rezystor R1 jest nie uszkadzalny w założonych warunkach pracy. Nie jest zatem konieczne uwzględnienie tego uszkodzenia w ocenie iskrobezpieczości obwodu przedstawionego na rys 3.2. Rezystor R1 jest elementem nie uszkadzalnym, tzn. takim, którego prawdopodobieństwo uszkodzenia w układzie jest pomijalnie małe.

W rzeczywistości nie można jednak wykluczyć uszkodzenia rezystora R1. W rzeczywistych układach może on ulec uszkodzeniu np. w przypadku wystąpienia zaburzeń elektromagnetycznych w postaci wysokoenergetycznych zaburzeń indukowanych lub przewodzonych. Wówczas należy założyć, że wartość rezystancji rezystora R1 może przyjąć wartość dowolną. Ze względu na temperaturę powierzchni małego elementu jakim jest rezystor, istotne jest wyznaczenie takiej jego rezystancji R1, dla której moc wydzielana na nim w stanie uszkodzenia będzie największa. Przypadek ten ma miejsce gdy występuje dopasowanie energetyczne: obwodów wejściowego i wyjściowego tzn. gdy $R_o=R_i$. Jeśli dla uproszczenia przyjmiemy, że zastępca rezystancja statyczna nieuszkadzalnego zespołu diod jest pomijalna, a rezystor R uległ zwarciu to na rezystorze R1 może wydzielić się moc równa czwartej części mocy źródła tzn. 0,75W.

3.5.4. OCENA ISKROBEZPIECZEŃSTWA W OBWODZIE ISKROBEZPIECZNYM Z POJEMNOŚCIĄ

W obwodzie wejściowym obwodu elektronicznego zastosowano zespół trzech szeregowo połączonych diod zabezpieczających zewnętrzne źródło zasilania obwodu przed prądem rozładowania pojemności wewnętrznej obwodu C1 (jak na rys 3.1). Dodatkowo włączono nie uszkadzalny rezystor szeregowy R1 ograniczający prąd w obwodzie. Należy dokonać oceny iskrobezpieczeństwa tego obwodu pod kątem analizy dopuszczalnej pojemności.



Rys.3.3. Uproszczony schemat elektryczny do oceny iskrobezpieczeństwa obwodu.

Ocenę iskrobezpieczości obwodu w grupie IIC z pojemnością wewnętrzną jak na rysunku 3.3 przedstawiono w tabeli 3.12. W ocenie tej założono, że:

- maksymalna wartość napięcia wejściowego będzie równa $C_i = 30V$ DC,
- napięcie znamionowe kondensatora będzie równe $U_n = 100V$ DC,
- nominalna wartość pojemności wewnętrznej będzie wynosiła $C1 = 30nF$,
- tolerancja wartości pojemności $\pm 20\%$,

- współczynnik bezpieczeństwa ma wartość 1,5,
- maksymalna temperatura otoczenia będzie wynosiła 80°C.

| Lp. | Oznaczenie schematowe | Pojemność nominalna [nF] | Pojemność maksymalna [nF] | Napięcie znamionowe [V] | Uwagi |
|-----|--|-----------------------------|------------------------------|----------------------------|---|
| 1 | C1 | 30,0 | 36 | 100 | |
| | Maksymalna dopuszczalna wartość pojemności dla napięcia zasilania 30V ze współczynnikiem bezpieczeństwa równym 1,5 | 66,0 | | | Tablica A2, grupa IIC normy PN-EN 60079-11:2007 |
| | Warunek iskrobezpieczeństwa ze względu na pojemność wewnętrzną | spełniony | | | 36nF<66nF |
| | Maksymalna dopuszczalna wartość napięcia zasilania kondensatora bezpieczeństwa równym 1,5 | 66,7V | | | Tablica A2, grupa IIC normy PN-EN 60079-11:2007 |
| | Warunek iskrobezpieczeństwa ze względu na nieprzekroczenie napięcia zasilania kondensatora | spełniony | | | 30V<66,7V |

Tab. 3.13. Ilustracja procedury oceny iskrobezpieczności obwodu z pojemnością klasyfikowanego do grupy IIC

Uwaga: Ze względu na zastosowanie nie uszkadzalnego zespołu diod (D1, D2, D3) pojemność wejściowa obwodu widziana od strony zacisków 1 i 2 jest pomijalnie mała.

3.6. LITERATURA

- [1] PN-EN 60079-0:2004. *Urządzenia elektryczne w przestrzeniach zagrożonych wybuchem gazów- Część 0: Wymagania ogólne*, Polski Komitet Normalizacyjny, str. 72, Warszawa, 2006.
- [2] PN-EN 60079-11:2007. *Atmosfery wybuchowe - Część 11: Urządzenia przeciwwybuchowe iskrobezpieczne „i”*. Polski Komitet Normalizacyjny, ICS 29.260.20, str. 233, Warszawa, 2007.
- [3] A. Cyganik: *Strefy Ex*, Wydawnictwo SIGMA-NOT, Maszyny Technologie Materiały, No 2, ISSN 0137-3730, str. 11-16, Warszawa, 2006.
- [4] PN-EN 60079-10:2003. *Urządzenia elektryczne w przestrzeniach zagrożonych wybuchem - Część 10: Klasifikacja obszarów niebezpiecznych*. Polski Komitet Normalizacyjny, ICS 29.260.20, str. 62, Warszawa, 2003.

4. DIAGNOSTYKA URZĄDZEŃ INTELIGENTNYCH

4.1. WPROWADZENIE

Bez wątpienia podstawą diagnostyki jest logika. Diagnostyka rozpoznaje bowiem badany stan rzeczy na podstawie pewnych przesłanek i związków logicznych (relacji) zachodzącymi pomiędzy tymi przesłankami a wnioskami z nich wypływającymi. W tym miejscu warto zwrócić uwagę na pewną istotną i wyróżniającą cechę mechanizmu wnioskowania diagnostycznego. W przypadku typowego wnioskowania przyczynowo-skutkowego, wnioskowanie o skutkach następuje na podstawie analizy relacji pomiędzy przyczynami a skutkami. W diagnostyce stosowany jest **mechanizm wnioskowania odwrotnego**. Na podstawie obserwowanych skutków dociekane są przyczyny, które je wywołyły. Różnice w sposobie wnioskowania zostały zilustrowane schematycznie na rys. 4.1.

a



b



Rys. 4.1. Schemat wnioskowania przyczynowo-skutkowego (a) i odwrotnego (b)

Różnica w sposobie wnioskowania ma istotne konsekwencje. Jak łatwo zauważyc te same skutki (uszkodzenia) mogą być wywołane przez różne przyczyny. Stąd możemy wywieść prosty wniosek, że rozwiązywanie problemu diagnozowania w ogólności jest niejednoznaczne i w tym sensie niewyznaczalne. Tę cechę będziemy dalej określali terminem **nierozróżnialności przyczyn**. W szczególności w odniesieniu do diagnostyki technicznej będziemy mówili o **nierozróżnialności uszkodzeń**.

Powstaje pytanie o co należy rozumieć pod pojęciem uszkodzenia. W dalszej części tego rozdziału będziemy stosowali następującą prostą i ogólną definicję uszkodzenia:

Def. 4.1. *Uszkodzeniem lub defektem jest każde zdarzenie destrukcyjne powodujące pogorszenie jakości działania obiektu diagnozowania.*

W diagnostyce technicznej stosowana jest często praktyczna subiektywna ale i zawężająca definicja uszkodzenia:

Def. 4.2. *Uszkodzeniem lub defektem jest każde zdarzenie destrukcyjne powodujące pogorszenie jakości działania obiektu diagnozowania i takie, które powinno być wykrywane w procesie diagnozowania.*

Definicja 4.2 zawęża pojęcie uszkodzenia do takiego ich podzbioru, które spełnia pewne postulatywne kryterium subiektywne.

Obie definicje odnoszą się do bliżej niezdefiniowanych zdarzeń, co do których domyślnie zakłada się, że odnoszą się zarówno do **składników materialnych** procesów takich jak np.:

- uszkodzeń urządzeń
- uszkodzeń urządzeń pomiarowych i wykonawczych
- uszkodzeń instalacji technologicznych
- wystąpienie pasożytniczych reakcji w reaktorze chemicznym
- uszkodzeń przemysłowych magistral komunikacyjnych
 - lub **energetyczno-surowcowych** np.:
 - zaników zasilania elektrycznego, pneumatycznego, hydraulicznego
 - wystąpienie braku surowców na wejściu aparatu technologicznego
- lub **niematerialnych** np.:
 - niewłaściwe sterowanie np.: przestawienie przez operatora zaworu sterowanego ręcznie na niewłaściwą pozycję
 - niezamierzona nieskończona pętla programowa w oprogramowaniu sterującym

Def. 4.3. Uszkodzenia szczególnie groźne w skutkach nazywane są **awariami**.

Diagnostyka urządzeń inteligentnych jest częścią **diagnostyki procesów przemysłowych**. Diagnostyka procesów przemysłowych zajmuje się rozpoznawaniem zmian stanów procesów ciągłych występujących w przemyśle chemicznym, petrochemicznym, energetycznym, spożywczym, farmaceutycznym i innych. Jako przyczyny zmian stanów rozpatrywane są uszkodzenia. Zasadniczym zadaniem diagnostyki procesów przemysłowych jest wczesne wykrywanie i dokładne rozpoznawanie (rozróżnianie) powstających uszkodzeń.

4.1.1. POJĘCIA PODSTAWOWE

Wprowadźmy obecnie kilka pojęć podstawowych dotyczących diagnostyki procesów [4.1], które będą przydatne w dalszej części rozdziału.

Na początku zdefiniujmy pewien hipotetyczny obiekt diagnozowania, w którym wyróżniono K uszkodzeń. Zatem

Def. 4.4. *Zbiorem uszkodzeń F obiektu będziemy nazywali zbiór wszystkich jego K uszkodzeń:*

$$F = \{f_k : k = 1, 2, \dots, K\} \quad (4.1)$$

Definicja 4.4 nie odzwierciedla faktu, że proces powstawania uszkodzeń jest w istocie procesem dynamicznym. Uszkodzenia, co jest oczywiste, mogą się zarówno pojawiać jak i zanikać (być naprawiane). W związku z tym definiowane jest pojęcie stanu diagnostycznego obiektu. W tym miejscu należy zaznaczyć, że pojęcie stanu diagnostycznego obiektu jest definiowane odmiennie niż w przypadku definicji stanu w automatyce. O ile bowiem w automatyce przyjmuje się, że stan obiektu jest zdefiniowany przez minimalny zbiór współrzędnych stanu pozwalających na projekcję stanu obiektu w przyszłość na podstawie znajomości stanu aktualnego i przeszłego, to w diagnostyce przyjmuje się, że stan diagnostyczny obiektu złożonego określony jest przez zbiór stanów z

uszkodzeniami elementów tego obiektu. Uszkodzenia mogą mieć charakter uszkodzeń pojedynczych lub wielokrotnych. Maksymalna krotność uszkodzeń wynosi K . Liczba stanów obiektu z uszkodzeniami n -krotnymi jest równa $2^n - 1$. Zatem:

Def. 4.5. Stanem diagnostycznym $Z(t)$ obiektu będziemy nazywali zbiór wszystkich jego stanów $z_n(t)$ z uszkodzeniami n -krotnymi:

$$Z(t) = \{z_n(t) : n = 1..2^K - 1\} \quad (4.2)$$

Zatem stan diagnostyczny jest zbiorem stanów obiektu diagnozowania z uszkodzeniami pojedynczymi, podwójnymi, potrójnymi, ..., i K -tymi. Przyczyną zmian stanu są pojawiające się uszkodzenia oraz powroty obiektu do stanu normalnego (zdolności). Stąd wypływa prosty wniosek, że stan diagnostyczny obiektu jest funkcją uszkodzeń: $z(t) = z(f(t))$, a zatem ma charakter dynamiczny.

Rozpoznawanie stanu obiektu na podstawie aktualnie dostępnych informacji o tym obiekcie, można rozpatrywać jako:

- diagnozowanie** - którego celem jest określenie aktualnego stanu obiektu
- genezowanie** - którego celem jest określenie wcześniejszych (przeszłych) stanów obiektu
- prognozowanie** (przewidywanie) - którego celem jest określenie przyszłych stanów obiektu.

Wyniki tych działań nazywamy odpowiednio: **diagnozą**, **genezą** i **prognozą** stanu obiektu. Domeną diagnostyki procesów jest głównie diagnozowanie. Proces diagnozowania traktowany będzie jako proces wykrywania i rozróżniania uszkodzeń obiektu w wyniku zbierania, przetwarzania, analizy i oceny sygnałów diagnostycznych. Proces rozróżniania uszkodzeń jest procesem wnioskowania i wymaga znajomości przesłanek diagnostycznych oraz związków tych przesłanek z uszkodzeniami. Przesłanki diagnostyczne noszą nazwę **symptomów uszkodzeń**. Symptomy uszkodzeń uzyskiwane są zazwyczaj w procesie ostrej lub rozmytej oceny wartości tzw. sygnałów diagnostycznych.

Def. 4.6. Sygnałem diagnostycznym będziemy nazywali dowolny sygnał s_j będący nośnikiem informacji o stanie obiektu diagnozowania

$$S = \{s_j : j = 1, 2, \dots, J\} \quad (4.3)$$

Związki pomiędzy sygnałami diagnostycznymi a uszkodzeniami określa relacja diagnostyczna R_{FS} , która definiujemy w postaci iloczynu kartezjańskiego.

$$R_{FS} \subset S \times F. \quad (4.4)$$

W przypadku, gdy rozważane są jedynie związki binarne pomiędzy j -tym sygnałem diagnostycznym a k -tym uszkodzeniem, to mamy do czynienia z przypadkiem, w którym dany sygnał diagnostyczny s_j wskazuje (wartość 1) lub nie (wartość 0) na wystąpienie uszkodzenia f_k .

Relacja diagnostyczna z definicji ma bardzo prostą interpretację w postaci dwuwymiarowej **macierzy diagnostycznej**.



Def. 4.7. Binarną macierzą diagnostyczną będziemy nazywali taką macierz diagnostyczną której elementy przyjmują wyłącznie wartości binarne tzn:

$$r_{jk} = \{0,1\}; j = 1,2..J, k = 1,2, K. \quad (4.5)$$

Przykład 19.1.

Rozważmy binarną diagonalną macierz diagnostyczną o postaci:

| F S | f₁ | f₂ | f₃ | f₄ | f₅ | f₆ | f₇ | f₈ | f₉ |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <i>s₁</i> | 1 | | | | | | | | |
| <i>s₂</i> | | 1 | | | | | | | |
| <i>s₃</i> | | | 1 | | | | | | |
| <i>s₄</i> | | | | 1 | | | | | |
| <i>s₅</i> | | | | | 1 | | | | |
| <i>s₆</i> | | | | | | 1 | | | |
| <i>s₇</i> | | | | | | | 1 | | |
| <i>s₈</i> | | | | | | | | 1 | |
| <i>s₉</i> | | | | | | | | | 1 |

Rys. 4.2. Przykład binarnej diagonalnej macierzy diagnostycznej

W macierzy tej mamy dziewięć uszkodzeń i dziewięć sygnałów diagnostycznych o wartości 1. Jak łatwo zauważać, każde k -te uszkodzenie f_k jest w sposób jednoznaczny wskazywane przez k -tą wartość sygnału diagnostycznego s_k . Taka postać macierzy zapewnia zatem pełną rozróżnialność uszkodzeń. Niestety macierz ta w praktyce **jest nierealizowalna**. Przyczyna jest prosta. Testy diagnostyczne wymagają użycia sygnałów pomiarowych pochodzących z torów pomiarowych, które też są uszkadzalne. Zatem liczność potencjalnych uszkodzeń rośnie i zwykle istotnie przekracza liczbę dysponowanych testów diagnostycznych. W diagnostyce intelligentnych urządzeń pomiarowych i wykonawczych stosowane są zabiegi polegające na projektowaniu macierzy diagnostycznych o postaci zbliżonej do macierzy diagonalnej

Przykład 4.2.

Rozważmy binarną macierz diagnostyczną o postaci:

| F S | f₁ | f₂ | f₃ | f₄ | f₅ | f₆ | f₇ | f₈ | f₉ |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <i>s₁</i> | 1 | | | 1 | 1 | | | | |
| <i>s₂</i> | 1 | 1 | | 1 | | 1 | | | 1 |
| <i>s₃</i> | | | 1 | | 1 | | 1 | | |
| <i>s₄</i> | | | | 1 | | | | 1 | |
| <i>s₅</i> | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 |
| <i>s₆</i> | | | 1 | | | | 1 | | |
| <i>s₇</i> | | 1 | | 1 | | 1 | 1 | | |
| <i>s₈</i> | | | | | 1 | | | 1 | |
| <i>s₉</i> | | | 1 | 1 | 1 | | | | 1 |

Rys. 4.3. Przykład binarnej macierzy diagnostycznej



W macierzy tej, podobnie jak w macierzy z przykładu 4.1 mamy dziewięć uszkodzeń i dziewięć sygnałów diagnostycznych. Jak łatwo zauważać, do każdego k -tego uszkodzenia f_k można przyporządkować wektor kolumnowy wartości binarnych wszystkich sygnałów diagnostycznych. I tak, np. uszkodzeniu f_1 można przyporządkować wektor $v_1=[1,1,0,0,1,0,0,0,0]^T$, a uszkodzeniu f_2 wektor $v_2=[0,1,0,0,1,0,1,0,0]^T$. Wektory kolumnowe zawierające wartości wszystkich sygnałów diagnostycznych danego uszkodzenia f_k nazywać będziemy **sygnaturą uszkodzenia f_k** . Sygnatury pozwalają na rozróżnienie przynajmniej części uszkodzeń. Jak można zauważać w przykładzie 4.2 sygnatury wszystkich uszkodzeń za wyjątkiem v_2 i v_6 są różne. Macierz ta nie pozwala zatem na rozróżnienie tych uszkodzeń.

4.1.2. FAZY WNIOSKOWANIA DIAGNOSTYCZNEGO

Diagnozowanie jest sekwencyjnym procesem wielofazowym. Do podstawowych etapów tego procesu należą: detekcja, lokalizacja i identyfikacja uszkodzenia.

Detekcja uszkodzenia jest etapem pierwotnym. Detekcja polega na wykryciu uszkodzenia i określeniu momentu jego detekcji. W tej fazie istotne jest wyłącznie wskazanie, że wystąpiło co najmniej jedno uszkodzenie. W diagnostyce procesów stosowane są różne metody detekcji uszkodzeń począwszy od najprostszych związanych z przekroczeniem granic alarmowych po znacznie bardziej złożone bazujących na modelach fizycznych, behawioralnych, sztucznej inteligencji i hybrydowych [4.1]. Stosowane są zarówno podejścia jakościowe jak i ilościowe.

Lokalizacja (wyodrębnienie) uszkodzenia jest fazą, w której następuje określenie rodzaju, miejsca i czasu wystąpienia uszkodzenia. Lokalizacja jest realizowana po detekcji uszkodzenia. Lokalizacja jest etapem diagnozowania, w którym istotne jest zapewnienie możliwie dużej rozróżnialności uszkodzeń, wykrywanie uszkodzeń pojedynczych i krotnych. W tej fazie określana bywa również niepewność diagnozy. Jest też fazą, która często kończy proces diagnozowania.

Identyfikacja uszkodzenia jest fazą, w której następuje określenie rozmiaru i charakteru zmienności uszkodzenia w czasie. Identyfikacja uszkodzenia następuje po lokalizacji uszkodzenia.

4.2. DIAGNOSTYKA TYPU ON- I OFF-LINE

Diagnostyka urządzeń pomiarowych i wykonawczych realizowana jest podobnie jak diagnostyka procesów ciągłych w dwóch zasadniczych trybach:

- diagnostyki serwisowej zwanej powszechnie diagnostyką *off-line* i
- diagnostyki bieżącej zwanej diagnostyką *on-line*.

Różnice pomiędzy tymi podejściami wyjaśnimy na przykładzie elementu wykonawczego automatyki. Szczegółowo urządzenie to zostało przedstawione w rozdziale 17, a jego schemat ideowy został przedstawiony na rys 17.4. Element ten składa się z: zaworu sterującego, ustawnika pozycyjnego i siłownika pneumatycznego. Uszkodzenia elementu wykonawczego dotyczą oczywiście każdego z jego elementów składowych.

W tym przypadku nieinteligentnego urządzenia automatyki, diagnostyka serwisowa polega na wykonaniu szeregu pracochłonnych czynności takich jak:



- przejście na awaryjne sterowanie ręczne procesu,
- demontaż zespołu wykonawczego,
- montaż zespołu wykonawczego na stanowisku testowym,
- realizacja testów diagnostycznych urządzenia,
- realizacji ewentualnej naprawy zespołu wykonawczego,
- demontaż zespołu wykonawczego ze stanowiska testowego,
- montaż zespołu wykonawczego w instalacji technologicznej,
- przełączenie sterowania zespołu wykonawczego w tryb pracy automatycznej.

Opisany wyżej scenariusz diagnostyki off-line jest niezmiernie pracochłonny, długotrwały i kosztowny. Wymaga przejścia na sterowanie ręczne, co zazwyczaj skutkuje obniżeniem jakości procesu sterowania i w konsekwencji również jakości produktu finalnego. Jest wykonywany okresowo niezależnie od tego, czy jego uszkodzenie nastąpiło czy też nie. Ma jednak podstawową zaletę. Do celów diagnostycznych możliwe jest bowiem wprowadzanie specjalnych pobudzeń testowych. Wprowadzenie tych pobudzeń pozwala na zwiększenie liczności zbioru sygnałów diagnostycznych, co w konsekwencji prowadzi do zwiększenia rozróżnialności uszkodzeń.

Znacznie wygodniej, szybciej i taniej jest realizowana **diagnostyka typu off-line intelligentnego urządzenia wykonawczego**. W tym przypadku nie jest konieczny demontaż i ponowny montaż tego urządzenia w fazie jego diagnozowania. Przebieg diagnozowania serwisowego składa się wówczas z następujących faz:

- przejście na awaryjne sterowanie ręczne procesu,
- realizacja testów diagnostycznych urządzenia przy wykorzystaniu specjalistycznego oprogramowania testowego klasy AMS (Asset Management System).
- realizacji ewentualnej naprawy zespołu wykonawczego,
- przełączenie sterowania zespołu wykonawczego w tryb pracy automatycznej.

W tym przypadku diagnostyka serwisowa pozwala na stwierdzenie, czy i w jakim zakresie nastąpiło uszkodzenie elementu wykonawczego. Tutaj bardzo istotna z punktu widzenia realizacji naprawy uszkodzenia jest jego lokalizacja. Pozwala ona bowiem na zaplanowanie czasu i sposobu realizacji naprawy. Realizacja testów diagnostycznych wymaga zastosowania specjalistycznego oprogramowania diagnostycznego, które jest zazwyczaj rozwijane i dostarczane przez producentów elementów wykonawczych. W tym miejscu należy zaznaczyć, że również specyfikacje współczesnych przemysłowych sieci komunikacyjnych w warstwie łączą danych uwzględniają wsparcie dla realizacji zadań diagnostycznych (np. sieć HART).

Z punktu widzenia ekonomiki procesu oraz jego ciągłości, znacznie bardziej atrakcyjna jest metoda zdalnego diagnozowania urządzeń w trybie on-line. Metoda ta dotyczy wyłącznie urządzeń intelligentnych. W odróżnieniu od metod diagnostyki typu on-line, metoda ta jest **metodą pasywną** w tym sensie, że bazuje na analizie dostępnych sygnałów (wartości zmiennych procesowych) bez możliwości wprowadzania testowych wymuszeń diagnostycznych. Brak możliwości wprowadzania wymuszeń testowych w istotny sposób osłabia zdolności rozróżniania uszkodzeń, ale jednocześnie diagnostyka on-line nie wpływa na jakość procesu sterowania, co jest wartością samą w sobie.

Diagnostyka ta jest realizowana współbieżnie z procesem w czasie rzeczywistym lub pseudo-rzeczywistym.

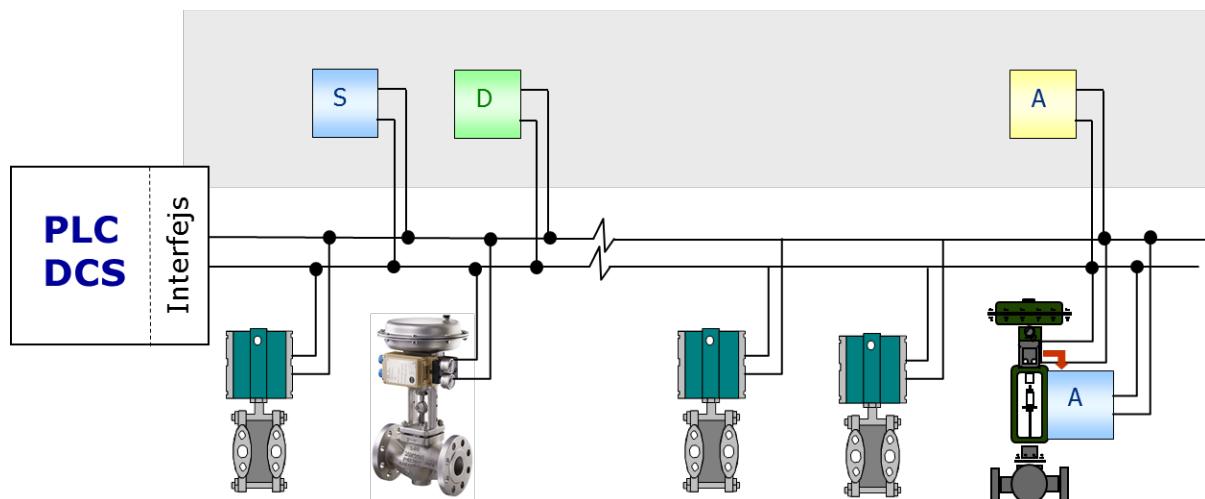
W przypadku analizowanego przez nas elementu wykonawczego, diagnostyka on-line wymaga:

- uaktywnienia trybu zdalnej diagnostyki typu on-line w urządzeniu wykonawczym,
- monitorowanie i analiza wartości wielkości procesowych związanych z elementem wykonawczym,
- realizacji wnioskowania diagnostycznego przy wykorzystaniu specjalistycznego oprogramowania diagnostycznego.
- realizacji ewentualnej naprawy zespołu wykonawczego.

W tym przypadku, w trybie off-line realizowana jest jedynie naprawa uszkodzonego elementu wykonawczego. Istotną zaletą tego diagnozowania on-line jest fakt, że naprawy są wykonywane tylko wtedy, gdy zostały wykryte uszkodzenia, a niekoniecznie wtedy, gdy minął resurs urządzenia lub jego podzespołów. Istotną wadą diagnostyki on-line jest silne obciążenie systemu sterowania zadaniami diagnostycznymi i transakcjami sieciowymi związanymi z zadaniami diagnostycznymi. W przypadku systemów sterowania dużej skali projektowane są specjalne specjalizowane stacje diagnostyczne np. jednostki master klasy 2 w sieci PROFIBUS DP, które odciążają jednostki sterujące od zadań diagnostycznych. W innych rozwiązaniach stosowane są specjalizowane dedykowane stacje procesowe realizujące zadania diagnostyczne.

4.3. DIAGNOSTYKA ROZPROSZONA

Rozważmy typowy segment rozproszonego systemu sterowania złożonego z magistrali komunikacyjnej, interfejsu komunikacyjnego systemu sterowania rozproszego DDC oraz inteligentnych elementów pomiarowych i wykonawczych (rys. 19.4). W tym przypadku implementacja diagnostyki realizowanej centralnie pozostaje w sposób oczywisty w kontradyscyplinie do idei rozproszenia systemu.



Rys. 4.4. Idea diagnostyki rozproszonej

Można jednak bez trudu wyobrazić sobie możliwość realizacji specjalizowanych fizycznych lub wirtualnych węzłów sieciowych pełniących funkcje diagnostyczne. Ze względu na zakres funkcjonalności, wyodrębniamy trzy rodzaje takich urządzeń, a mianowicie:

- detektory uszkodzeń,
- sensory uszkodzeń i
- analizatory uszkodzeń.

Urządzenia te zostały na rys. 4.4 oznaczone odpowiednio symbolami S, D i A.

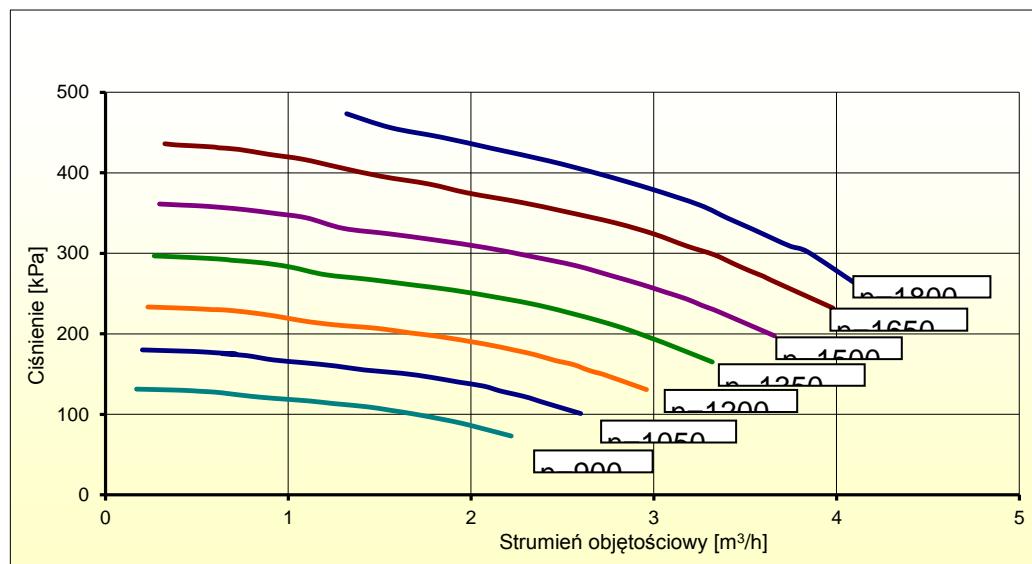
4.3.1. DETEKTORY USZKODZEŃ

Detektory uszkodzeń są węzłami sieciowymi (autonomicznymi lub wbudowanymi) ukierunkowanymi na detekcję uszkodzenia określonego urządzenia lub grupy urządzeń.

Z definicji, urządzenia te realizują wyłącznie pierwszą fazę procesu diagnozowania, a mianowicie fazę detekcji. Ponadto należy zaznaczyć, że urządzenia te pełnią wyspecjalizowane funkcje detekcyjne ukierunkowane na konkretne urządzenie procesowe. Detektory oferowane są w wersjach uniwersalnych i dedykowanych. Te pierwsze, przed włączeniem funkcjonalnym do sieci wymagają przeprowadzenia złożonego procesu konfiguracji. W tym przypadku konfiguracja polega na projekcie, implementacji i parametryzacji odpowiedniej programowej struktury diagnostycznej w urządzeniu. Przeprowadzana jest przez inżyniera procesu. Tego typu detektory uszkodzeń stosowane są rzadko, gdyż ich konfiguracja wymaga doświadczenia, wysokiego stopnia kwalifikacji i specjalizacji. Znacznie częściej stosowane są specjalizowane detektory uszkodzeń oferowane bezpośrednio przez producentów urządzeń i aparatów technologicznych. W tym przypadku konfiguracja detektora jest bardzo uproszczona i w zasadzie sprowadza się do wyboru określonych opcji jego pracy oraz naturalnej konfiguracji do pracy w przemysłowej sieci komunikacyjnej. Cechą charakterystyczną detektorów jest to, że dokonują zazwyczaj detekcji **uszkodzenia zintegrowanego**. Uszkodzeniem zintegrowanym jest nazywali uszkodzenie przypisywane całemu urządzeniu lub aparatu technologicznemu niezależnie od faktycznego wewnętrznego lub zewnętrznego źródła tego uszkodzenia. Dla przykładu, pęknięcie membrany silownika wcześniej analizowanego elektropneumatycznego elementu wykonawczego automatyki jest traktowane jako uszkodzenie całego zespołu wykonawczego.

Przykład 4.3. Detektor uszkodzenia zespołu pompy.

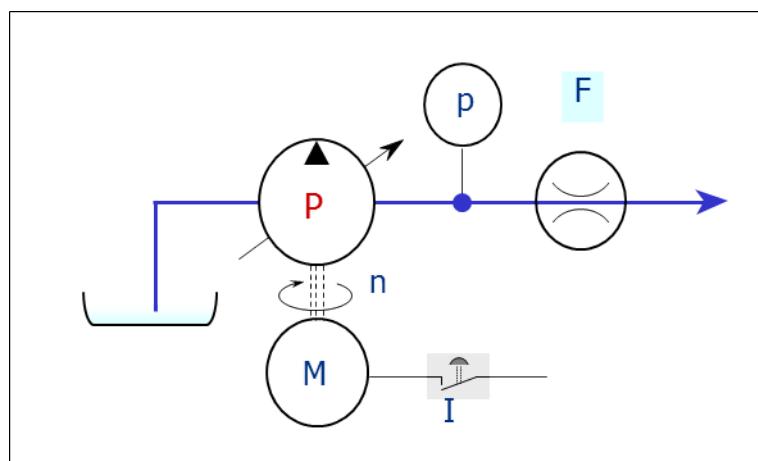
Podstawową charakterystyką roboczą pompy jest jej charakterystyka mechaniczna (rys. 4.5) odzwierciedlająca relację pomiędzy strumieniem objętościowym F tłoczonego medium i ciśnieniem tłoczenia p . Parametrem tej charakterystyki jest prędkość obrotowa n silnika napędzającego pompę.



Rys. 4.5. Przykładowa rodzina charakterystyk roboczych pompy śrubowej

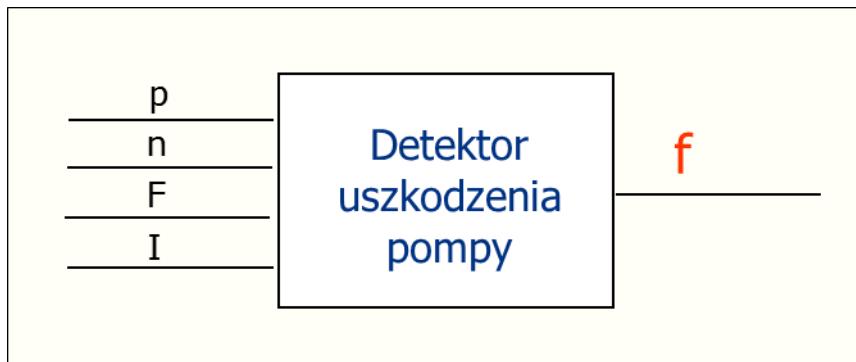
Detektorem uszkodzenia zespołu pompy będzie w tym przypadku wyspecjalizowany układ monitorujący jej charakterystykę roboczą $p(F)$ i wyznaczający stopień spadku sprawności wolumetrycznej pompy. Monitorowanie charakterystyki roboczej pompy wymaga znajomości co najmniej 4 wartości wielkości procesowych (rys. 4.6), a mianowicie;

- binarnego stanu włącznika silnika I
- prędkości obrotowej wału silnika napędowego pompy n ,
- ciśnienia tłoczenia p ,
- strumienia objętościowego F .



Rys. 4.6. Zbiór sygnałów monitorowanych przez detektor uszkodzenia zespołu pompy. Zespół pompy tworzą: P- pompa śrubowa, M- silnik napędowy pompy, I –wyłącznik pompy, p - przetwornik pomiarowy ciśnienia, F- przetwornik pomiarowy strumienia objętościowego.

Detektor uszkodzenia generuje sygnał diagnostyczny f (rys. 4.7) interpretowany jako zagregowany sygnał uszkodzenia.



Rys. 4.7. Zbiór sygnałów monitorowanych przez detektor uszkodzenia zespołu pompy.

Faktycznie, w obrębie zespołu pompy potencjalnych uszkodzeń jest więcej. Ich listę przedstawiono w Tab. 4.5. Uszkodzenie zespołu pompy jest uszkodzeniem zagregowanym, ponieważ każde z uszkodzeń wymienionych w tabeli 4.5 ma na nie wpływ.

Tab. 4.5. Lista potencjalnych uszkodzeń zespołu pompy

| Zbiór uszkodzeń zespołu pompy | | |
|--------------------------------------|-------------------------------------|---|
| f_1 | Uszkodzenie pompy | P |
| f_2 | Uszkodzenie silnika pompy | M |
| f_3 | Uszkodzenie czujnika ciśnienia | p |
| f_4 | Uszkodzenie przepływomierza | F |
| f_5 | Uszkodzenie obrotomierza | n |
| f_6 | Uszkodzenie włącznika silnika pompy | I |
| f_7 | Przeciek zewnętrzny | I |

4.3.2. SENSORY USZKODZEŃ

Sensory uszkodzeń są urządzeniami sieciowymi (autonomicznymi lub wbudowanymi) ukierunkowanymi na lokalizację pojedynczego uszkodzenia określonego urządzenia lub grupy urządzeń.

Sensory uszkodzeń realizują dwa etapy procesu diagnozowania: etap detekcji i lokalizacji wybranego uszkodzenia. Ukierunkowane są na detekcję szczególnie groźnych uszkodzeń np. wycieków substancji toksycznych, uszkodzenie łopatek turbin turbogeneratorów parowych, wystąpienie mechanicznych zjawisk rezonansowych, wystąpienie chemicznych reakcji pasożytniczych, itp.

Przykład 4.4. Sensor przecieku zewnętrznego zespołu pompy.

W tabeli 4.5 przedstawiono siedem potencjalnych uszkodzeń zespołu pompy śrubowej. Uszkodzenie f_7 dotyczy uszkodzenia polegającego na wycieku zewnętrznym z pompy. Przeciek ten może być wywołany np. pęknięciem jej obudowy, nieszczelnością kołnierzy łączących pompę z rurociągiem, korozją rurociągu lub jego uszkodzeniem mechanicznym. Przeciek może stanowić potencjalne zagrożenie dla zdrowia ludzi i stanu środowiska wskutek wycieku toksycznego lub agresywnego chemicznie medium. W tym przypadku zastosowanie wyspecjalizowanego sensora przecieku jest jak najbardziej uzasadnione.

4.3.3. ANALIZATORY USZKODZEŃ

Analizator uszkodzeń jest urządzeniem sieciowym (autonomicznym lub wbudowanym) ukierunkowanym jednocześnie na **detekcję i lokalizację uszkodzeń** określonego urządzenia lub grupy urządzeń.

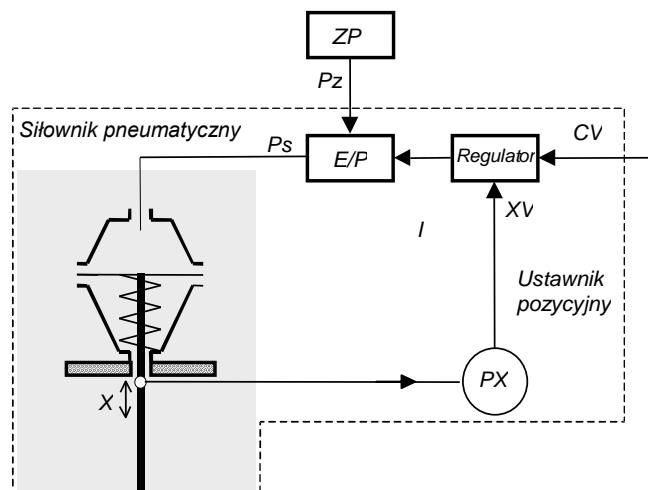
Wynika stąd, że analizator uszkodzeń może być traktowany funkcjonalnie jako zbiór sensorów uszkodzeń. I odwrotnie, sensorem uszkodzenia jest taki szczególny analizator, który dokonuje detekcji i lokalizacji wybranego uszkodzenia.

Przykład 4.5. Analizator wbudowany uszkodzeń zespołu pozycjonera

Przykładem realizacji analizatora uszkodzeń może być blok funkcjonalny (realny lub wirtualny) pozycjonera realizującego zadania detekcji i lokalizacji uszkodzeń na podstawie wartości zadanej CV, prądu sterującego I wewnętrzny przetwornik elektropneumatyczny E/P, ciśnienia sterującego w komorze siłownika Ps, ciśnienia zasilania Pz, przemieszczenia tłoczyska siłownika X.

Schemat blokowy pozycjonera wraz ze współpracującym membranowym siłownikiem pneumatycznym jednostronnego działania o ruchu posuwistym trzpienia przedstawiono na rys. 4.8.

W tym przypadku analizator korzysta także z dostępnych sygnałów wewnętrznych ustawnika takich jak np. prąd sterujący I. Sygnał ten normalnie nie jest udostępniany przez ustawnik w postaci sieciowej zmiennej procesowej. Jego wykorzystanie ma jednak istotne znaczenie diagnostyczne, ponieważ ma wpływ na rozróżnialność uszkodzeń. Stąd, w tym przypadku celowa jest realizacja analizatora uszkodzeń w wersji wbudowanej. Ze względów ekonomicznych oraz występujących ograniczeń w zasilaniu dwuprzewodowych urządzeń inteligentnych analizator wbudowany realizowany jest głównie na drodze programowej. Zaletą realizacji takiego analizatora jest szybki dostęp do wszystkich wewnętrznych zmiennych analizowanego urządzenia. W tym przypadku analizator dokonuje detekcji i lokalizacji uszkodzeń: przetwornika elektropneumatycznego E/P i przetwornika przemieszczenia PX gdyż oba elementy są szczególnie podatne na uszkodzenia. Dla przykładu średni czas pomiędzy uszkodzeniami (MTBF) dla typowych przetworników E/P stosowanych w ustawnikach wynosi zaledwie ok. 20000h, a dla przetworników przemieszczenia ok. 50000h.



Rys. 4.8. Schemat blokowy elektropneumatycznego ustawnika pozycyjnego wraz z siłownikiem pneumatycznym jednostronnego działania o ruchu liniowym. Oznaczenia: **ZP** – źródło zewnętrznego zasilania pneumatycznego podające do elementu powietrze pod ciśnieniem **Pz**, **E/P**- przetwornik elektropneumatyczny, **PX**- przetwornik pomiarowy przemieszczenia, **CV** – sygnał sterujący, **I**- sygnał prądowy sterujący przetwornik elektropneumatyczny, **Ps**- ciśnienie sterujące komory siłownika pneumatycznego, **X**- sygnał przemieszczenia tłoczyka siłownika pneumatycznego, **XV** – sygnał pomiarowy przemieszczenia tłoczyka siłownika.

4.4. DIAGNOSTYKA WBUDOWANA

Przykład zastosowania idei diagnostyki wbudowanej w postaci analizatora uszkodzeń ustawnika pozycyjnego przedstawiono w przykładzie 4.5. Teraz, zajmiemy się zagadnieniem diagnostyki wbudowanej nieco szerzej.

Rozpatrzmy na początku wady i zalety diagnostyki scentralizowanej i rozproszonej.

Diagnostyka scentralizowana typu on-line:

- ❑ korzysta ze zbioru dostępnych zmiennych procesowych zwykle wykorzystując mechanizm udostępniania OPC. Ten sposób dostępu do bazy (archiwum) zmiennych procesowych ma zasadnicze wady: wprowadza opóźnienia wynikające z zastosowania samego mechanizmu OPC i dodatkowo opóźnienia transportowe wynikające z transferu zmiennych sieciami komunikacyjnymi. Ponadto możliwe jest korzystanie wyłącznie z podzbioru zmiennych procesowych udostępnianych przez mechanizm dostępowy.
- ❑ realizuje zadania diagnostyczne dla wszystkich elementów systemu automatyki. Wobec zróżnicowania tych elementów i po uwzględnieniu ich liczby (często liczba zmiennych przekracza 10^6) wymaga to zaangażowania znacznych mocy obliczeniowych.

- wymaga zastosowania specjalnych systemów oprogramowania diagnostycznego. Ponieważ z natury rzeczy systemy te są przeznaczone do zastosowań uniwersalnych, to konfiguracja takiego systemu i jego pielęgnacja jest bardzo czasochłonna i kosztowna, a ponadto wymaga bardzo wysokich kwalifikacji inżynierów procesu.
- zaletą takiej diagnostyki jest możliwość dostępu do tych zmiennych procesowych, do których nie mają dostępu systemy diagnostyki rozproszonej, a które mają wpływ na proces detekcji i lokalizacji uszkodzeń.

System diagnostyki rozproszonej:

- prowadzi diagnostyką lokalną o zasięgu ograniczonym zwykle do jednego segmentu sieci przemysłowej.
- elementy funkcjonalne systemu diagnostycznego skoncentrowane są głównie na detekcji i ewentualnie lokalizacji szczególnie groźnych uszkodzeń.
- wykorzystywane są prekonfigurowane fabrycznie detektory, sensory i analizatory uszkodzeń. Dzięki temu czas konfiguracji jest krótki i nie wymaga od personelu bardzo wysokich kwalifikacji.
- Może zawierać **elementy wbudowane** w urządzenia procesowe. Pozwala to na istotne skrócenie czasu dostępu do zmiennych procesowych oraz umożliwia dostęp do zmiennych nie udostępnianych publicznie. Dzięki temu możliwe uzyskanie dodatkowej wiedzy diagnostycznej.

Dwupoziomowy hybrydowy system diagnostyki:

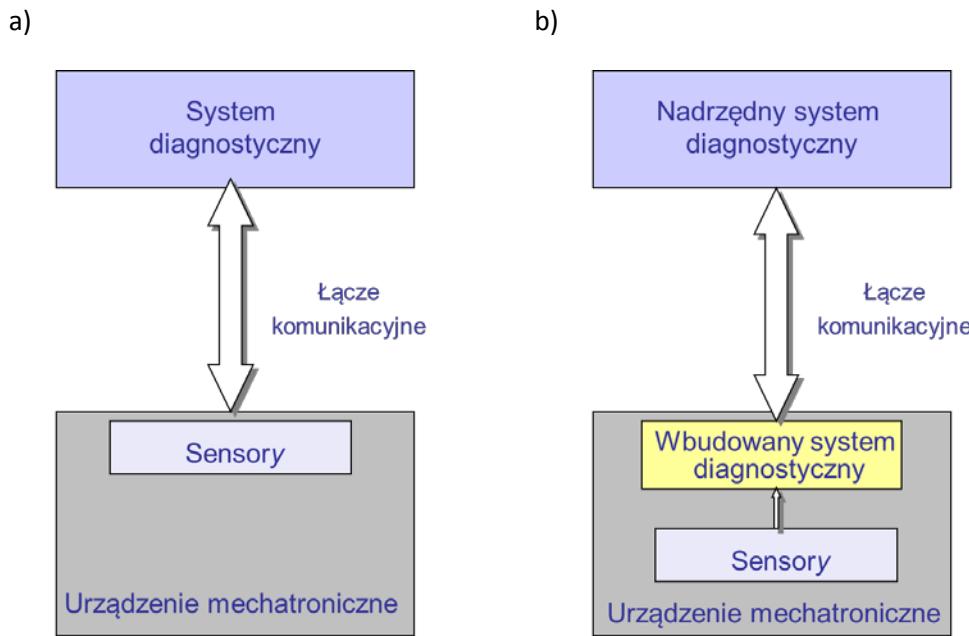
- prowadzi diagnostyką rozproszoną na poziomie lokalnym i diagnostykę scentralizowaną na poziomie globalnym.
- wypracowuje diagnozy globalne wykorzystując zagregowane informacje diagnostyczne dostarczane przez systemy diagnostyki rozproszonej.
- rozszerza zbiór zmiennych procesowych o zmienne diagnostyczne. Mimo to operuje na silnie zredukowanej liczbie zmiennych procesowych w stosunku do systemu diagnostyki scentralizowanej.
- jest znacznie prostszy w konfiguracji w stosunku do zcentralizowanego systemu diagnostyki.

Przykłady takich systemów diagnostycznych przedstawiono poglądowo na rysunku 4.9.

Realizacja diagnostyki wbudowanej w urządzenia inteligentne wymaga zastosowania w tych urządzeniach jednostek obliczeniowych o odpowiednich mocach obliczeniowych i zasobach pamięciowych, bowiem co do zasady diagnostyka wbudowana jest realizowana na drodze programowej. W tym miejscu należy zaznaczyć, że w wielu przypadkach w urządzeniach realizowanych w technice dwuprzewodowej (por. rozdz. 1), ze względu na ograniczoną dysponowaną moc zasilania, wolne moce obliczeniowe mogą nie być dostępne. Dotyczy to w większej mierze złożonych inteligentnych elementów wykonawczych niż przetworników

pomiarowych. Na szczęście postęp w technologii wytwarzania układów mikrokontrolerów o ultra niskim poborze energii pozwala obecnie na pokonanie tego ograniczenia. Diagnostyczne oprogramowanie wbudowane tworzone jest na etapie konstrukcji urządzenia, a więc z wykorzystaniem szczegółowej i bardzo przydatnej na tym etapie wiedzy konstruktorskiej.

Diagnostyka wbudowana realizowana jest w trybie on-line. Nie wyklucza to oczywiście przełączenia tej diagnostyki w tryb pracy off-line np. w celu realizacji funkcji **autodiagnostycznych**.



Rys. 4.9. Przykładowe uproszczone schematy możliwej współpracy inteligentnych urządzeń automatyki z zewnętrznymi systemami diagnostycznymi: a) z centralnym systemem diagnostycznym, b) w systemie rozproszonym z diagnostyką wbudowaną i nadzorowanym systemem diagnostycznym.

Warto zapamiętać:

Diagnostyka wbudowana:

- ❑ zwiększa dyspozycyjność urządzeń,
- ❑ zwiększa bezpieczeństwo funkcjonalne,
- ❑ umożliwia realizację funkcji rekonfiguracji urządzenia,
- ❑ zmniejsza obciążenie przemysłowych sieci komunikacyjnych,
- ❑ zmniejsza obciążenie centralnego systemu diagnostyki,
- ❑ daje możliwość wykorzystania w diagnozowaniu sygnałów wewnętrznych urządzenia,
- ❑ daje możliwość wykorzystania w diagnozowaniu wiedzy konstruktora urządzenia,
- ❑ zmniejsza nieroróżnialność uszkodzeń.

4.5. TOLEROWANIE USZKODZEŃ

Istotnym zadaniem diagnostyki urządzeń procesowych jest jej zastosowanie do realizacji procedur tolerowania uszkodzeń. Pod pojęciem **tolerowania uszkodzeń** należy rozumieć zdolność urządzenia do wypełniania swoich funkcji mimo zaistnienia uszkodzenia jednego lub wielu jego elementów składowych. Od urządzenia lub systemu wykonawczego pracującego w trybie tolerowania uszkodzeń nie wymaga się najczęściej spełnienia wszystkich kryteriów oceny jakości wypełnianych funkcji. Inaczej jest w przypadku urządzeń pomiarowych, gdzie w trybie tolerowania uszkodzeń powinna być zachowana nominalna niepewność pomiaru.

Zastosowanie metod tolerowania uszkodzeń w istotny sposób zwiększa tzw. **bezpieczeństwo funkcjonalne** urządzenia. Ogólna miara bezpieczeństwa funkcjonalnego jest intensywność uszkodzeń. Zastosowanie podejścia konstrukcyjnego polegającego na tolerowaniu, a więc maskowaniu uszkodzeń, wpływa w sposób oczywisty na zmniejszenie tej intensywności. Ze względu na techniczną i praktyczną wagę problemu należy zaznaczyć, że metody i algorytmy tolerowania uszkodzeń należą obecnie do grupy najszybciej rozwijanych dziedzin diagnostyki.

Ideę oraz praktykę tolerowania uszkodzeń elementów pomiarowych i wykonawczych przedstawimy na dwóch przykładach.

Przykład 4.6. Inteligentny przetwornik pomiarowy tolerujący uszkodzenia

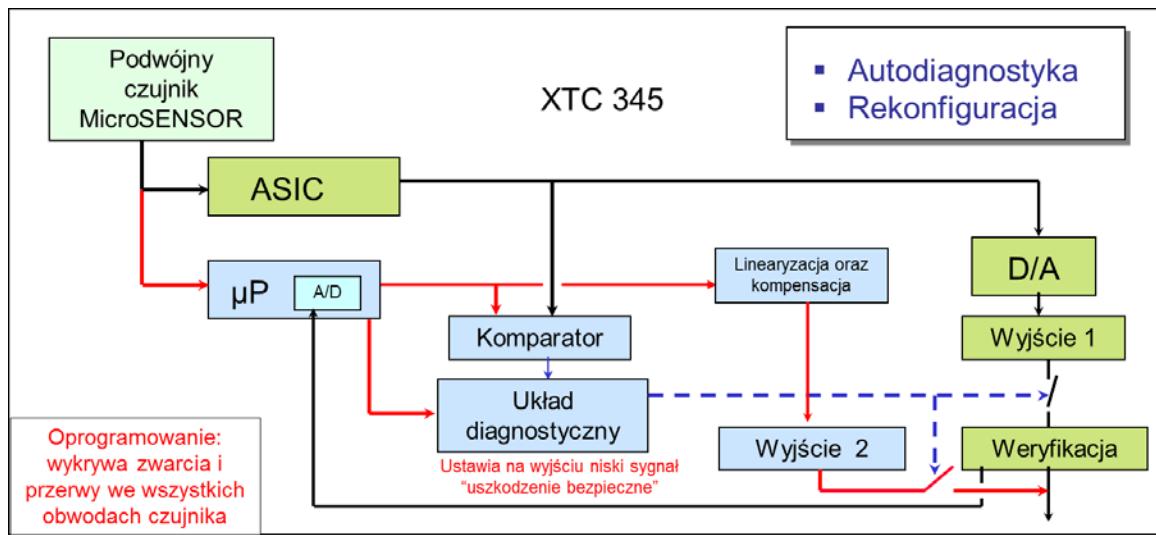
Na rysunku 4.10 przedstawiono uproszczoną strukturę inteligentnego przetwornika ciśnienia tolerującego uszkodzenia. W jego konstrukcji przyjęto tzw. zasadę redundancji funkcjonalnej kanałów. Polega ona na rozdzieleniu torów przetwarzania wartości wielkości wejściowej na co najmniej dwa kanały realizowane w taki sposób aby nie mogły ulec uszkodzeniu wskutek zaistnienia tzw. wspólnej przyczyny. Podejście to wyjaśnimy nieco bliżej. Jego realizacja w uproszczeniu polega na zaprojektowaniu zróżnicowanych sprzętowo i programowo torów przetwarzania informacji.

W przypadku interesującego nas przetwornika zastosowano:

- dwie różne struktury czujnika ciśnienia (strukturę piezorezystancyjną na podłożu krzemowym i mostek tensometryczny)
- dwa różne układy przetwarzania sygnału pomiarowego (specjalizowany układ ASIC i uniwersalny mikrokontroler współpracujący z integracyjnym przetwornikiem analogowo-cyfrowym wysokiej rozdzielczości)
- komparator umożliwiający ocenę wiarygodności pomiarów w obu torach przez porównanie wyników przetwarzania w obu torach,
- układ diagnostyczny oceniający wiarygodność pomiarów i przełączający wyjście z przetwornika na tor wiarygodny
- układ dwóch wyjściowych przetworników cyfrowo-analogowych.

W tym przypadku wbudowane oprogramowanie diagnostyczne:

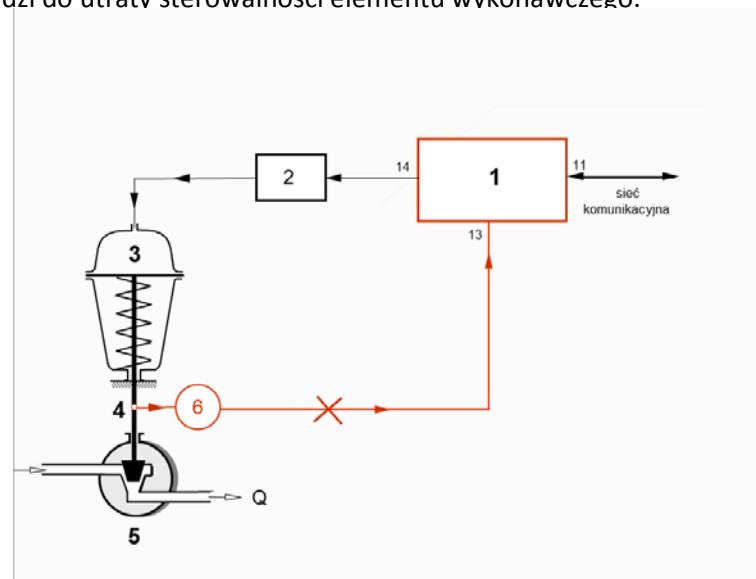
- dokonuje oceny wiarygodności pomiarów
- wykrywa zwarcia i przerwy w obwodach czujników pomiarowych,
- realizuje funkcje przełączania toru wyjściowego, a więc funkcje tolerowania uszkodzenia.



Rys. 4.10. Przykład struktury inteligentnego przetwornika ciśnienia tolerującego uszkodzenia.

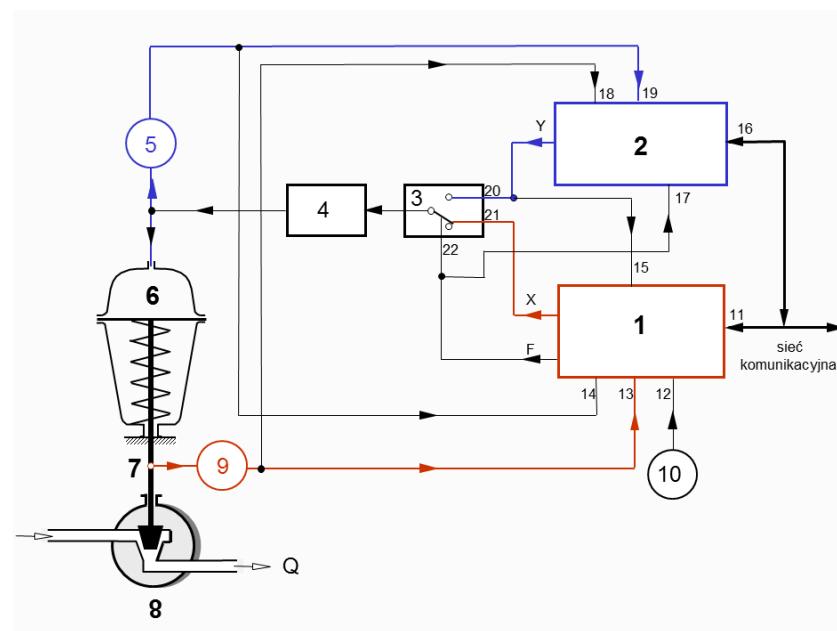
Przykład 4.7. Inteligentne urządzenie wykonawcze tolerujące uszkodzenia toru sprężenia zwrotnego.

Rozważmy urządzenie inteligentne wykonawcze o strukturze jak na rysunku 4.11 i którego szczegółowy opis znajduje się w rozdziale 5. Urządzenie to pełni rolę nadążnego zamkniętego układu regulacji przemieszczenia tłoczyska siłownika (4) śledząc sygnał nastawiający regulatora zewnętrznego przesyłany kanałem komunikacji cyfrowej. Sygnał sprężenia zwrotnego jest podawany lokalnie do wewnętrznego regulatora ustawnika (1) przez przetwornik pomiarowy (6) przemieszczenia liniowego tłoczyska siłownika (3). Przetwornik pomiarowy przemieszczenia konstrukcyjnie składa się z części mechanicznej przetwarzającej ruch posuwisto-zwrotny tłoczyska siłownika na ruch obrotowy osi potencjometru pomiarowego. Część mechaniczna przetwornika jest sprzężona mechanicznie z tłoczkiem i narażona na uszkodzenia wynikające z pracy części mechanicznej w ciężkich warunkach środowiskowych. Uszkodzenie toru sprężenia zwrotnego przekształca zamknięty układ regulacji w układ otwarty, co wobec całkującego charakteru toru głównego prowadzi do utraty sterowalności elementu wykonawczego.



Rys. 4.11. Przykład struktury inteligentnego elementu wykonawczego

Rozważmy teraz strukturę układu sterowania ustawnika pozycyjnego jak na rys. 4.2. W tej strukturze zastosowano dodatkowy przetwornik ciśnienia powietrza w komorze siłownika (5), oraz dodatkowy układ regulacji ze sprzężeniem od sygnału ciśnienia (2). W normalnym trybie pracy ustawnik pracuje z regulatorem (1) i sygnałem sprzężenia zwrotnego generowanym przez przetwornik przemieszczenia (9). Wbudowany sensor diagnostyczny służy do detekcji i lokalizacji uszkodzenia przetwornika przemieszczenia. Po wykryciu tego uszkodzenia następuje przełączenie układu sterowania na obwód z regulatorem (2). W tym przypadku wartość przemieszczenia tłoczyska siłownika wynika z charakterystyki mechanicznej siłownika $X=f(p)$. Charakterystyka ta nie jest jednak ani liniowa ani jednoznaczna. Dodatkowo jej parametry podlegają ewolucji reologicznej. Stąd należy przypuszczać, że w trybie tolerowania uszkodzenia toru sprzężenia zwrotnego wystąpi znacznie większa odchyłka regulacji niż w przypadku układu regulacji ze sprzężeniem od położenia trzpienia siłownika. W wielu zastosowaniach nie ma to jednak zasadniczego znaczenia, ponieważ element wykonawczy dodatkowo objęty jest zewnętrzną pętlą sprzężenia zwrotnego. Dzięki temu, możliwa jest kompensację wpływu odchyłki regulacji elementu wykonawczego.



Rys.4.12. Przykład struktury inteligentnego z wbudowaną funkcją tolerowania uszkodzenia toru sprzężenia zwrotnego.

Warto zapamiętać:

Urządzenia tolerujące uszkodzenia:

- dokonują detekcji i lokalizacji uszkodzeń,
- tolerują uszkodzenia wypełniając swoje funkcje pomimo istniejącego uszkodzenia,
- zmieniają swój stan diagnostyczny,
- sygnalizują ten stan systemowi monitorowania i nadzoru procesu wymagając obsługi serwisowej.

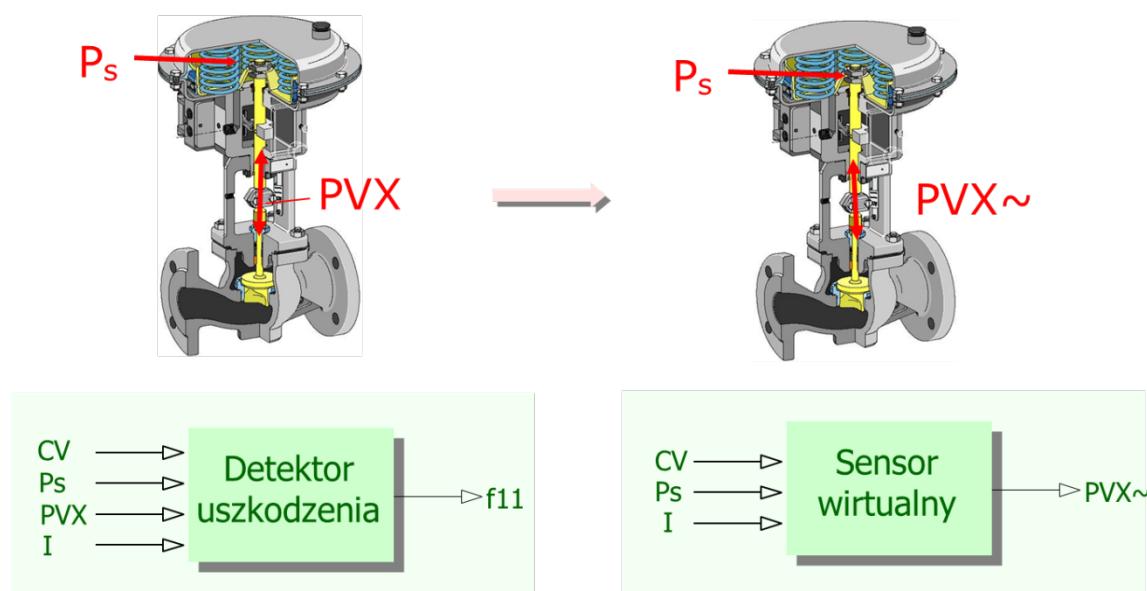
4.6. REDUNDANCJA ANALITYCZNA

Nie wchodząc nadmiernie w szczegóły, redundancja analityczna pozwala na rekonstrukcję wartości wielkości niemierzalnych lub utraconych np. na skutek wystąpienia uszkodzenia. Rekonstrukcja jest możliwa tylko wówczas, gdy dysponujemy wiarygodnymi zmiennymi procesowymi o istotnej korelacji ze zmienną rekonstruowaną.

Rozważmy teraz nieco inne podejście do problemu tolerowania uszkodzenia toru sprzężenia zwrotnego elementu wykonawczego niż to, które zostało przedstawione w przykładzie 4.7. Zamiast budowania redundantnego układu regulacji spróbujmy odtworzyć utraconą zmienną procesową (przemieszczenie tłoczyska siłownika X) i wykorzystać estymatę tej zmiennej w procesie sterowania ustawnika w trybie tolerowania uszkodzenia toru sprzężenia zwrotnego. Przemieszczenie tłoczyska siłownika zostanie odtworzone na podstawie znajomości:

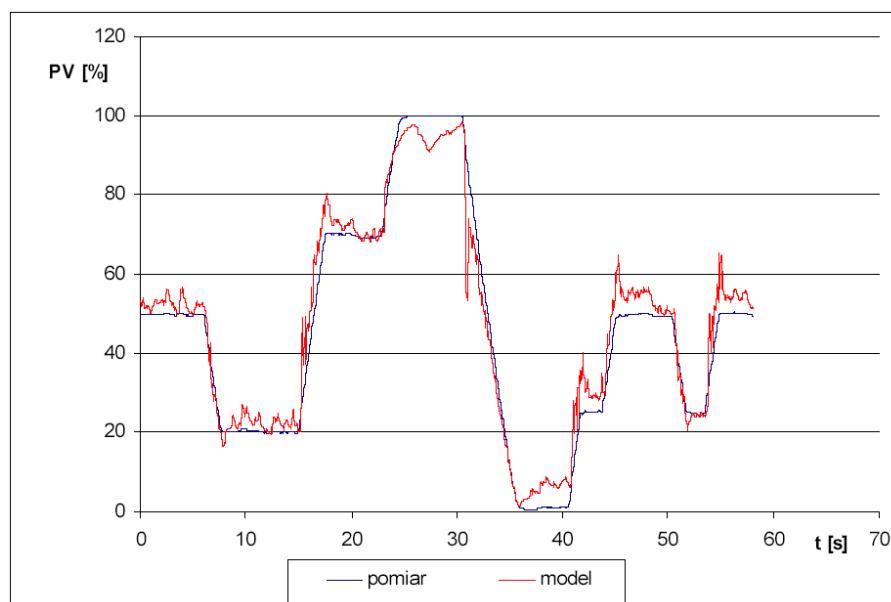
- sygnału nastawiającego CV ,
- sygnału ciśnienia Ps w komorze siłownika,
- wartości prądu sterującego / przetwornik elektropneumatyczny.

Ideę zastosowania redundancji analitycznej przedstawiono na rys. 4.13. W istocie polega ona na konstrukcji modelu sygnału pomiarowego. Model ten nosi alternatywną nazwę **sensora wirtualnego**. Jak łatwo zauważyc, na podstawie modelu jakościowego, bez pogłębionej analizy zależności fizycznych, sygnał przemieszczenia tłoczyska siłownika jest skorelowany ze wszystkimi trzema wyżej wymienionymi sygnałami. Stąd istnieją przesłanki do budowy modelu tego sygnału. W praktyce modele analityczne stosowane są rzadko. Znacznie częściej stosowane są modele w postaci sieci neuronowych, rozmytych sieci neuronowych lub modele rozmyte. W intelligentnych urządzeniach automatyki poszukiwane są modele statyczne i dynamiczne o prostej strukturze i możliwe niewielkiej złożoności obliczeniowej.



Rys. 4.13. Ilustracja zastosowania redundancji analitycznej do rekonstrukcji sygnału sprzężenia zwrotnego.

Liczba sensorów tej samej wielkości fizycznej może być różna. W przypadku rekonstrukcji sygnału sprzężenia zwrotnego ustawnika pozycyjnego możliwe jest zbudowanie zarówno modeli statycznych jak i dynamicznych. Przykład weryfikacji jednego z nich a mianowicie skrajnie uproszczonego neuronalnego modelu statycznego o postaci $PVX=f(Ps)$ przedstawiono na rys. 4.14. I choć rekonstrukcja zmiennej PV nie jest zbyt perfekcyjna, to model ten może być brany pod uwagę w zastosowaniu praktycznym.



Rys. 4.14. Ilustracja dokładności statycznego modelu neuronowego przemieszczenia trzpienia siłownika o postaci $PVX=f(Ps)$.

Zmienna rekonstruowana może być wykorzystywana w procesie detekcji uszkodzenia. Istotna rozbieżność pomiędzy wartościami zmiennej mierzonej i zmiennej rekonstruowanej świadczy o wystąpieniu uszkodzenia lub w niektórych przypadkach o niedoskonałości modelu. Zmienna rekonstruowana może być również wykorzystywana w zastępstwie zmiennej czasowo lub nawet trwale niedostępnej. Dotyczy to np. układów tolerujących uszkodzenia.

Przykład 4.8. Pomiary zawartości NO_x w spalinach.

W elektrowniach zawodowych poziom zawartości NO_x w spalinach podlega ścisłej kontroli i monitorowaniu. W tym celu wykorzystywane są sprzętowe analizatory gazów. Muszą być one jednak okresowo (np. co godzinę) wyłączone i poddawane procedurze kalibracyjnej. W okresie realizacji kalibracji poziom zawartości NO_x może być rekonstruowany przez zastosowanie sensora wirtualnego.

Warto zapamiętać:

Redundancja analityczna:

- jest użyteczna do rekonstrukcji zmiennych procesowych,
- jest wykorzystywana do badania wiarygodności pomiarów,
- jest wykorzystywana w procesie detekcji uszkodzeń,
- jest wykorzystywana w systemach tolerujących uszkodzenia.

4.7. PODSUMOWANIE

W niniejszym rozdziale przedstawiono w skrócie rolę i miejsce diagnostyki w budowie urządzeń intelligentnych automatyki. Jej rola we współczesnych systemach automatyki jest nie do przecenienia, ponieważ jej zastosowanie umożliwia zapewnienie większego bezpieczeństwa funkcjonalnego urządzeń, zmniejszenia kosztów serwisu i eksploatacji oraz racjonalizację działań służb utrzymania ruchu.

4.8. LITERATURA

[4.1] Korbicz J., J.M. Kościelny, Z. Kowalcuk, W. Cholewa (2004). *Fault Diagnosis. Models. Artificial intelligence. Applications*, Springer Verlag, 2004, ISBN: 3-540-40767-7, s. 918.

5. ELEKTROPNEUMATYCZNY INTELIGENTNY ELEMENT WYKONAWCZY AUTOMATYKI

Inteligentny elektropneumatyczny element wykonawczy automatyki należy do klasy urządzeń mechatronicznych. Można powiedzieć więcej, że jest wręcz typowym przykładem zintegrowanego urządzenia mechatronicznego. Pełna realizacja jego funkcji wymaga bowiem rozwiązania problemów dotyczących znajomości zarówno teorii jak i wiedzy praktycznej w zakresie takich dziedzin jak: mechanika, technologia, elektronika, elektrotechnika, automatyka, diagnostyka i informatyka.

W rozdziale tym zostaną przedstawione podstawowe informacje dotyczące konstrukcji i zastosowania inteligentnych elektropneumatycznych elementów wykonawczych automatyki. Przedstawione zostaną również podstawowe cechy funkcjonalne takich elementów. Zostaną podane wybrane przykłady zastosowań elementów wykonawczych do silowników jednostronnego działania o ruchu liniowym.

5.1. ROLA I MIEJSCE ELEMENTÓW WYKONAWCZYCH W UKŁADACH AUTOMATYKI

W procesach technologicznych elementy wykonawcze automatyki stosowane są do bezpośredniego sterowania strumieni materiałowo-energetycznych. W strukturze układów sterowania pełnią rolę elementów pośredniczących pomiędzy *regulatorami* a *obiekty sterowania* (Rys. 5.1). Jest oczywiste, że właściwości statyczne i dynamiczne elementu wykonawczego mają wpływ na właściwości całego układu regulacji. Zatem w fazie projektowania układu regulacji automatycznej fakt ten powinien być uwzględniony i przeanalizowany. Jeśli stosunek zastępczych stałych czasowych modeli uproszczonych opisujących element wykonawczy i obiekt regulacji jest dostatecznie mały (np. mniejszy od 0,01), to w pierwszej fazie projektowania układu regulacji przyjmuje się, że dopuszczalne jest pominięcie właściwości dynamicznych elementów wykonawczych. W uproszczeniu można wówczas przyjąć, że element wykonawczy w interesującym paśmie częstotliwości, wprowadza pomijalne małe przesunięcie fazowe sygnału wyjściowego w stosunku do przesunięcia fazowego wnoszonego przez obiekt. Jeśli dodatkowo jego charakterystyka statyczna w zakresie roboczym jest charakterystyką liniową, to element taki ma właściwości zbliżone do właściwości elementu proporcjonalnego. W takim przypadku element wykonawczy może być traktowany jako element proporcjonalny o wzmacnieniu 1.

Idealny element wykonawczy ma charakterystykę idealnego członu proporcjonalnego o wzmacnieniu 1.

Wówczas rola elementu wykonawczego polega nie tylko na wzmacnieniu sygnału (traktowanego w kategoriach bezwymiarowych), ale na wzmacnieniu mocy i zmianie postaci fizycznej sygnału sterującego. Dla uzyskania odpowiedniego wzmacnienia mocy, do elementu wykonawczego musi być dostarczana dodatkowa energia. W przypadku elektropneumatycznych elementów wykonawczych energia ta dostarczana jest z sieci sprężonego powietrza.

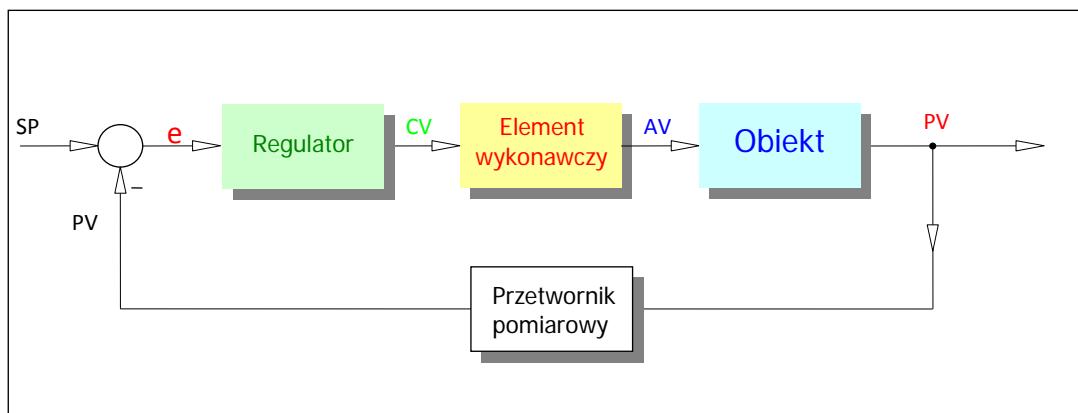
Przykład 5.1:

Załóżmy, że fizycznym sygnałem wyjściowym regulatora jest sygnał prądowy w znormalizowanym zakresie prądowym 4-20 mA o mocy maksymalnej równej 200 mW. Sygnał ten jest sygnałem

wejściowym elektropneumatycznego elementu wykonawczego o ruchu liniowym, którego zadaniem jest sterowanie strumienia objętościowego medium. Sygnałem wyjściowym elementu wykonawczego jest sygnał przestawienia jego organu ruchomego. W trakcie przestawienia, organ ruchomy pokonuje siły bezwładności, siły tarcia oraz siły oddziaływania hydrostatycznego i hydrodynamicznego sterowanego medium. Jeśli w dużym uproszczeniu założymy, że suma sił pokonywanych przez organ ruchomy elementu wykonawczego wykonujący przemieszczenie 20 mm ruchem jednostajnym w ciągu 2 s jest stała i równa 2000 N, to moc konieczna do realizacji tego przemieszczenia jest równa 20W. Energia potrzebna do pokonania tych sił znacznie przewyższa poziom energii elektrycznej sygnału wejściowego. Pokonanie tych sił wymaga dostarczenia mocy z zewnątrz. W tym przypadku wzmacnienie mocy w układzie wykonawczym wynosi 100.

Elekropneumatyczne elementy wykonawcze wymagają zasilania energią sprężonego powietrza.

Istotną zaletą elektropneumatycznych elementów wykonawczych, w stosunku do elektrycznych elementów wykonawczych, jest możliwość łatwiejszego spełnienia wymagań iskrobezpieczeństwa zgodnie z normą ATEX [5.1].



Rys. 1: Miejsce elementu wykonawczego w strukturze prostego jednoobwodowego układu automatyki. Oznaczenia: SP - sygnał wartości zadanej (zewnętrzny sygnał sterujący), e - odchyłka regulacji, CV - sygnał sterujący regulatora, AV - sygnał wyjściowy z elementu wykonawczego, PV - sygnał wielkości regulowanej.

Właściwości dynamiczne elementu wykonawczego są zależne nie tylko od konstrukcji samego elementu, ale także od wartości parametrów jego wewnętrznego układu regulacji. Parametry te nazywane są w praktyce przemysłowej **nastawami**. W przypadku inteligentnych elementów wykonawczych nastawy są programowalne. Układy sterowania inteligentnych elementów wykonawczych są układami automatycznej regulacji nadążnej.

Typowy element wykonawczy automatyki posiada wbudowany układ realizujący funkcje nadążnego układu regulacji automatycznej.

W takim przypadku sygnał wyjściowy elementu wykonawczego AV nadąża za sygnałem sterującym CV regulatora. Zmiana parametrów wewnętrznego regulatora ma wpływ na właściwości całego elementu wykonawczego. W szczególności zmiana tych parametrów umożliwia kształtowanie pożądanych właściwości dynamicznych elementu. Właściwości te są charakteryzowane między innymi przez wartości wskaźników jakości regulacji elementu wykonawczego, do których należą

między innymi: przeregulowanie, czas regulacji, całkowy wskaźnik jakości regulacji czy pasmo częstotliwości.

Postulowana wartość przeregulowania k dla elementów wykonawczych automatyki wynosi 0%.

Niewłaściwy dobór parametrów może prowadzić do powstania drgań tłumionych organu ruchomego elementu wykonawczego lub nawet do utraty stabilności. Organia organu ruchomego elementu wykonawczego prowadzą do szybszego zużycia samego organu jak i współpracujących z nim elementów obniżając w sposób istotny ich trwałość. Ponadto drgania te przenoszą się na sterowany proces i wywołują niekorzystne zaburzenia w sterowanych przez elementy wykonawcze strumieniach mas i energii. W wielu przypadkach prowadzi to do powstawania drgań mechanicznych elementów instalacji obiektu (np. rur) i wywołuje efekty akustyczne. W związku z tym w stosunku do zdecydowanej większości elementów wykonawczych automatyki pierwszoplanowym wskaźnikiem jakości regulacji jest wartość przeregulowania k.

Pomijanie właściwości dynamicznego elementu wykonawczego w procesie projektowania układów automatyki jest błędem, nawet jeśli stosunek zastępczych stałych czasowych modeli uproszczonych opisujących element wykonawczy i obiekt regulacji jest dostatecznie mały.

5.2. ZAGADNIENIA DIAGNOZOWANIA STANU ELEMENTÓW WYKONAWCZYCH

Elementy wykonawcze należą do grupy elementów układów automatyki podlegających najczęstszym uszkodzeniom. Szacuje się, że wśród uszkodzeń elementów pomiarowych, wykonawczych i komponentów technologicznych, udział awarii elementów wykonawczych przekracza 40%. Wynika to z ciężkich warunków pracy tych urządzeń. Urządzenia wykonawcze pracują często w warunkach wysokiej temperatury, zapylenia, wilgoci, silnych drgań czy w otoczeniu atmosfery agresywnej chemicznie (Rys. 2 i 3).

Uszkodzenie elementów wykonawczych może prowadzić do pogorszenia jakości produktu finalnego, a nawet może prowadzić do zatrzymania sterowanego procesu. Wszystkie te czynniki powodują zmniejszenie stopnia bezpieczeństwa procesu i ludzi, a także pogorszenie wskaźników ekonomicznych przedsiębiorstwa. Z tego powodu coraz większego znaczenia nabiera aspekt zapewnienia możliwie bezawaryjnej pracy takich urządzeń lub przynajmniej minimalizacji wpływu występujących uszkodzeń na jakość sterowanego procesu. W tym kontekście, istotne stają się zagadnienia dotyczące przewidywania i diagnozowania uszkodzeń, a także sposobów ich tolerowania. Realizacja tych zadań może odbywać się np. na drodze analizy diagnostycznej dostępnych sygnałów w zewnętrznym systemie sterowania typu DCS czy SCADA lub przy wykorzystaniu funkcji autodiagnostycznych samych elementów wykonawczych.



Rys. 5.2. Fotografia przedstawiająca warunki pracy ustawnika pozycyjnego elementu wykonawczego przeznaczonego do sterowania dyszami OFFA w kotle energetycznym bloku elektroenergetycznego w elektrowni. Dysze OFFA odgrywają istotną rolę w sterowaniu poziomu emisji NO_x. Fotografia została wykonana po okresie dwóch miesięcy od daty instalacji ustawnika. Widoczne jest silne zapylenie otoczenia miejsca pracy. Temperatura otoczenia wynosi od 40°C do 60°C i jest zależna od pory roku.



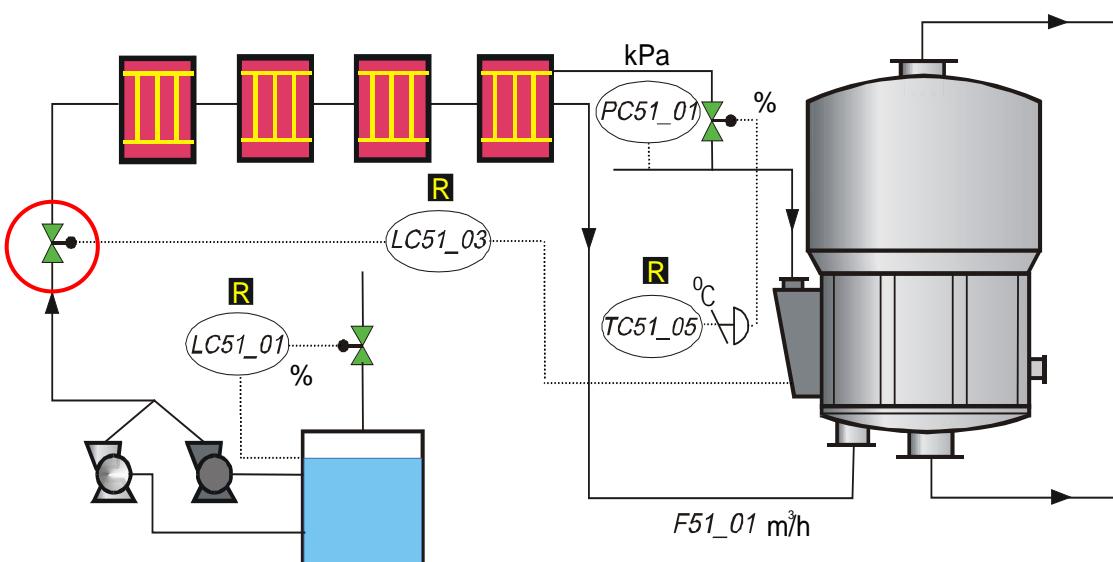
Rys. 5.3. Fotografia przedstawiająca warunki pracy elementu wykonawczego zainstalowanego w układzie regulacji poziomu wody chłodzącej w zbiorniku buforowym w cukrowni. Fotografia została wykonana w momencie wymiany ustawnika pozycyjnego w zespole elementu wykonawczego. Widoczne jest silne korozyjne oddziaływanie środowiska pracy na element wykonawczy. Temperatura otoczenia wynosi od 15°C do 40°C natomiast wilgotność względna waha się w granicach: 50-95%.

W pierwszym przypadku mówimy o **diagnostyce zdalnej** realizowanej okresowo (w trybie off-line) bądź na bieżąco (w trybie on-line). W drugim przypadku mówimy o **diagnostyce wbudowanej**. Realizacja wbudowanych funkcji diagnostycznych wymaga wyposażenia elementu wykonawczego w funkcje komunikacyjne. Element wykonawczy realizujący funkcje komunikacyjne nazywany jest powszechnie, choć nieprecyzyjnie elementem intelligentnym.

Immanentnym atrybutem intelligentnych elementów wykonawczych są funkcje komunikacyjne.

Funkcje komunikacyjne należą do ważnych, ale nie są najważniejszymi funkcjami realizowanymi przez intelligentne elementy wykonawcze. Najważniejsza funkcja spełniana przez elementy intelligentne jest identyczna jak w przypadku nieintelligentnych elementów wykonawczych. Tą funkcją jest funkcja pierwotna polegająca na realizacji wzmacnienia mocy. Funkcja ta jest realizowana przez wbudowany, a więc autonomiczny układ regulacji elementu wykonawczego. Zwykle intelligentne elementy wykonawcze realizują także funkcje autonastawcze (autostrojenie), pomiarowe, diagnostyczne, funkcje umożliwiające tolerowanie niektórych uszkodzeń wewnętrznych, itd. Niektóre intelligentne urządzenia wykonawcze mają wbudowany dodatkowy regulator, który np. może pełnić rolę regulatora procesu. Aspekt bezpieczeństwa procesu i przydatności funkcji diagnostycznych zostanie przedstawiony na poniższym przykładzie.

Przykład 2. Na rysunku 5.4 przedstawiono układ regulacji poziomu soku rzadkiego w pierwszym stopniu wyparnym w cukrowni. Element wykonawczy (w kółku) steruje strumieniem objętościowym soku rzadkiego podawanego ze zbiornika buforowego przez jedną z dwóch pomp pracujących w równoległym układzie redundantnym. Po wstępnych podgrzaniu w serii podgrzewaczy, sok jest podawany do aparatu wyparnego, gdzie podlega częściowemu zagęszczaniu przez odparowanie i następnie jest przekazywany do następnego aparatu wyparnego. Sok w aparacie wyparnym podgrzewany jest parą. Założmy, że wskutek uszkodzenia zaworu regulacyjnego elementu wykonawczego, dopływ soku rzadkiego do aparatu wyparnego w pewnym momencie zostanie zablokowany. W wyniku zamknięcia dopływu soku do aparatu wyparnego następuje odparowanie soku w aparacie wyparnym, co prowadzi do karmelizacji powierzchni wewnętrznych aparatu i wzrostu ciśnienia w aparacie. Proces odparowania soku jest na tyle procesem dynamicznym, że odparowanie soku w aparacie wyparnym może nastąpić w ciągu zaledwie kilkudziesięciu sekund. W tym przypadku uzyskanie szybkiej i dostatecznie wiarygodnej informacji diagnostycznej o zaistniałym uszkodzeniu pozwala na podjęcie odpowiednich działań zapobiegawczych. Informacja taka może być wypracowana np. w zewnętrznym systemie sterowania procesu na podstawie analizy rozbieżności pomiędzy sygnałami wartości sygnału sterującego regulatora procesu i wartością wyjściową elementu wykonawczego. W tym przypadku realizowany jest tryb diagnostyki zdalnej. Ta sama informacja może być wypracowana także przez inteligentny element wykonawczy, ponieważ w tym przypadku dysponuje on tymi samymi sygnałami. W tym przypadku realizowany jest tryb diagnostyki wbudowanej. Ponieważ element wykonawczy jest generatorem swojego sygnału wyjściowego, to sygnał ten pojawi się wcześniej w samym elemencie wykonawczym niż w zewnętrznym systemie sterowania. Zatem diagnostyka wbudowana może generować diagnozy wcześniej niż diagnostyka zdalna.



Rys. 5.4. Przykład elementu wykonawczego zainstalowanego w układzie regulacji poziomu soku rzadkiego w aparacie wyparnym w cukrowni.

5.3. ELEKTROPNEUMATYCZNY ELEMENT WYKONAWCZY

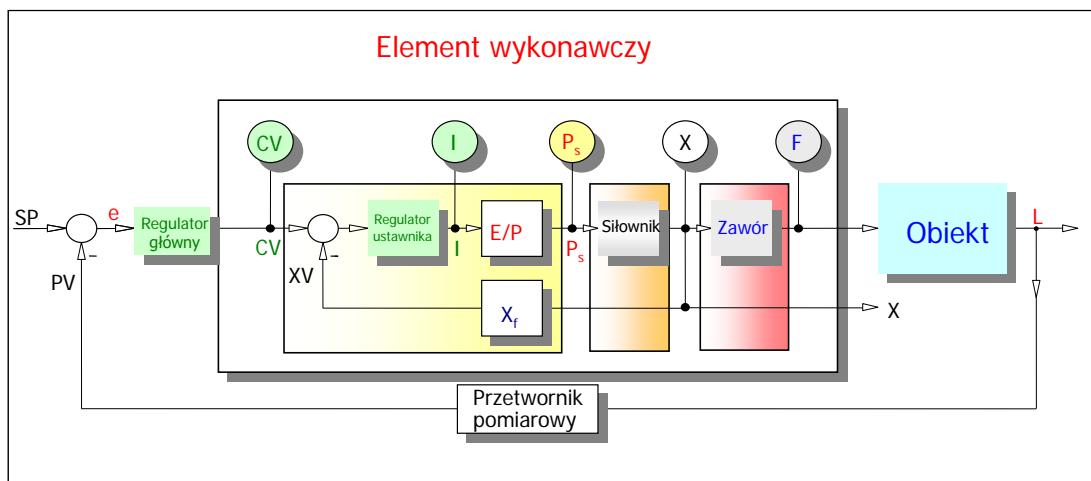
Istnieje wiele odmian konstrukcyjnych elektropneumatycznych elementów wykonawczych. W tym rozdziale zajmiemy się wyłącznie pewną ich klasą, mającą duże znaczenie praktyczne, a mianowicie elektropneumatycznymi elementami wykonawczymi jednostronnego działania o ruchu liniowym. Typowy przemysłowy elektropneumatyczny element wykonawczy należący do tej klasy został przedstawiony na rys. 5.5. Element wykonawczy przedstawiony na rysunku 5.5 składa się z: siłownika pneumatycznego, ustawnika pozycyjnego oraz zaworu regulacyjnego.



Rys. 5.5. Typowy elektropneumatyczny element wykonawczy automatyki i jego konstrukcja mechaniczna.

5.3.1. USTAWNIK POZYCYJNY I SIŁOWNIK PNEUMATYCZNY

Ustawnik pozycyjny, nazywany również pozycjonerem, w połączeniu z siłownikiem pneumatycznym, pełni rolę układu regulacji przemieszczenia tłoczyka siłownika (Rys. 5.6).



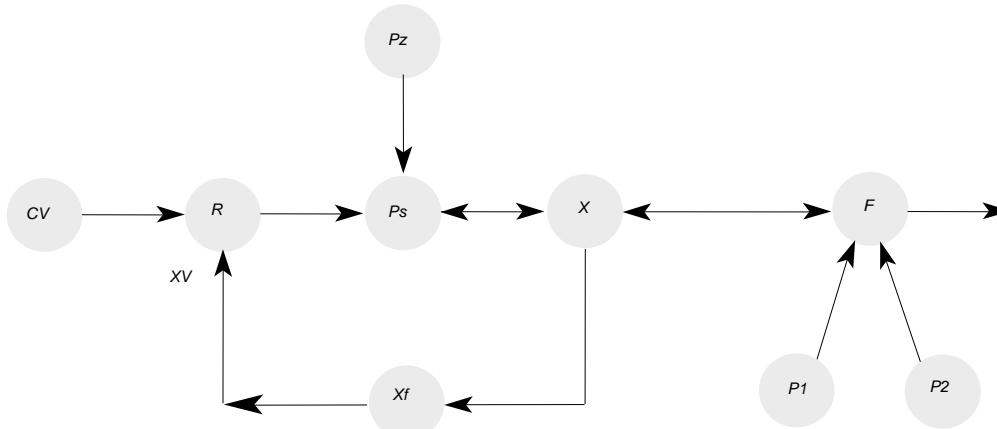
Rys. 5.6. Schemat blokowy jednoobwodowego układu regulacji automatycznej z elektropneumatycznym elementem wykonawczym. Oznaczenia: SP - sygnał wartości zadanej (zewnętrzny sygnał sterujący), PV – sygnał wielkości regułowanej (wielkość mierzona), e – odchyłka regulacji, CV – sygnał sterujący regulatora, XV – wartość mierzona w układzie regulatora wewnętrznego ustawnika, I – wewnętrzny sygnał sterowania przetwornika elektropneumatycznego E/P, P_s – sygnał ciśnienia podawanego z przetwornika E/P na siłownik, X - sygnał przemieszczenia trzpienia siłownika, X_f – element dynamiczny toru sprężenia zwrotnego w regulatorze wewnętrznym ustawnika, F – sygnał wyjściowy z elementu wykonawczego, L – wielkość regulowa

Ustawnik pozycyjny pełni rolę lokalnego układu regulacji przemieszczenia elementu dławiącego zaworu sterującego.

Wejściowym sygnałem ustawnika jest sygnał sterujący CV generowany najczęściej przez zewnętrzny regulator główny obwodu regulacyjnego. Z punktu widzenia lokalnego układu regulacji realizowanego przez ustawnik, sygnał ten traktowany jest jako sygnał wartości zadanej. Sygnałem wyjściowym układu regulacji przemieszczenia tłoczyka siłownika jest sygnał przemieszczenia X . Na podstawie różnicy pomiędzy wartością zadaną (CV) i wartością mierzoną przemieszczenia tłoczyka siłownika XV , regulator wewnętrzny ustawnika pozycyjnego generuje sygnał sterujący I . Sygnał ten jest przekształcany w przetworniku elektropneumatycznym E/P do postaci sygnału ciśnieniowego P_s . Sygnał ciśnieniowy P_s podawany jest do komory siłownika pneumatycznego. Siłownik pneumatyczny przekształca sygnał ciśnieniowy na przemieszczenie tłoczyka X . Z kolei tłoczyko powoduje przemieszczanie grzyba zaworu regulacyjnego i zmianę jego powierzchni przepłybowych. Zmiana powierzchni przepłybowych zaworu regulacyjnego wywołuje zmianę strumienia objętościowego przepływającego przez zawór medium.

Funkcjonalnie tłoczyko siłownika zmienia stopień otwarcia zaworu sterującego.

Na rys. 5.7 przedstawiono uproszczony graf przyczynowo-skutkowy elementu wykonawczego. Należy zwrócić uwagę na złożoność zjawisk fizycznych zachodzących w elemencie. Z jednej strony zawór sterujący oddziaływa na strumień medium, z drugiej strony strumień medium oddziaływał na zawór w wyniku działania sił hydrostatycznych i hydrodynamicznych. Oddziaływanie to wywołuje zmiany przemieszczenia tłoczyka siłownika, co z kolei ma wpływ na wartość ciśnienia P_s w komorze siłownika. Warto również zauważyć, że na wartość strumienia objętościowego medium przepływającego przez zawór sterujący ma wpływ nie tylko stopień jego otwarcia (X), ale również różnica ciśnień (P_1-P_2) na zaworze.



Rys. 5.7. Graf przyczynowo-skutkowy ustawnika pozycyjnego o schemacie blokowym jak na rysunku 6. Oznaczenia: CV – sygnał sterujący regulatora zewnętrznego, XV – wartość mierzona w układzie regulatora wewnętrznego Ps – ciśnienie w komorze siłownika, X - sygnał przemieszczenia trzpienia siłownika, XF – element dynamiczny toru sprzężenia zwrotnego w regulatorze wewnętrznym ustawnika, F – strumień medium, Pz - ciśnienie zasilania ustawnika, P1 - ciśnienie medium przed zaworem sterującym, P2 - ciśnienie medium za zaworem sterującym.

5.3.2. ZAWÓR STERUJĄCY

Zawór regulacyjny steruje strumieniem objętościowym zgodnie ze swoją konstrukcyjną charakterystyką przepływową. Charakterystyki przepływowo zaworów są zależne od konstrukcji i geometrii zaworów. Charakterystyki te przedstawiają zależność współczynnika konstrukcyjnego K_v zaworu w funkcji stopnia otwarcia zaworu (Rys. 5.8). Miarą stopnia otwarcia zaworu jest przemieszczenie względne X jego organu ruchomego (np. grzyba). Współczynnik K_v zaworu (zgodnie z normą DIN IEC 60534 [5.2]) jest liczbowo równy wartości strumienia objętościowego wody o temperaturze 5-40°C przepływającej przez zawór przy statycznym spadku ciśnienia na zaworze równym 1 bar. Wartość strumienia objętościowego wody wyrażana jest w [m^3/h]. Wartość tego współczynnika jest podawana w specyfikacji zaworu regulacyjnego w warunkach pełnego otwarcia zaworu. Specyfikacja zaworu regulacyjnego zawiera ponadto informację o jego konstrukcyjnej charakterystyce przepływowej.

Strumień objętościowy medium przepływającego przez zawór sterujący zależy nie tylko od stopnia jego otwarcia. Wynika stąd, że element wykonawczy nie ma pełnego wpływu na wartość strumienia objętościowego sterowanego medium.

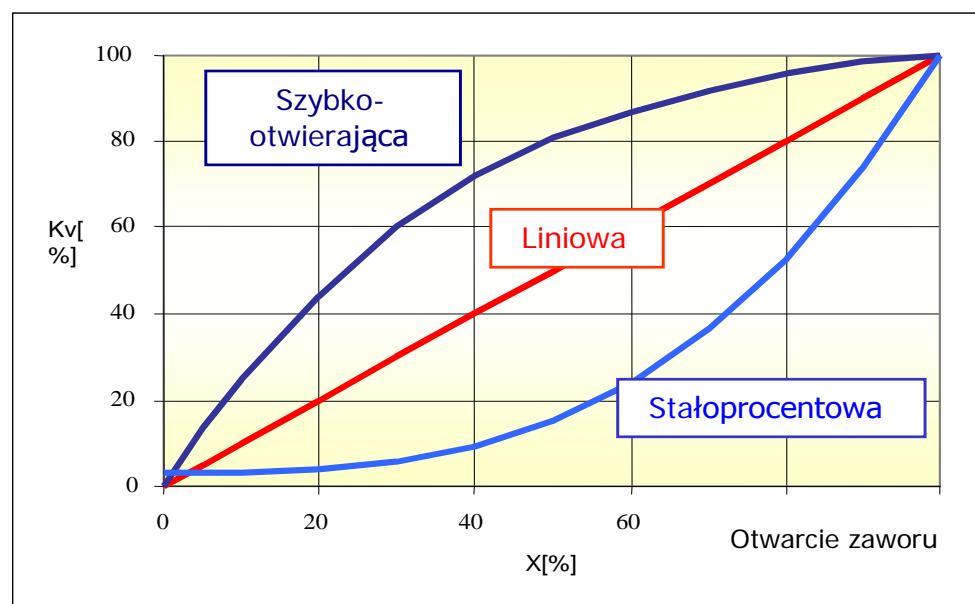
Wartość strumienia objętościowego medium przepływającego przez zawór sterujący zależy od: stopnia otwarcia zaworu, charakterystyki konstrukcyjnej zaworu, różnicy ciśnień na zaworze, rodzaju przepływu (podkrytyczny, nadkrytyczny) stanu skupienia medium, objętości lub gęstości właściwej medium przed i za zaworem, temperatury, współczynnika rozszerzalności cieplnej medium, itd.

W praktyce stosowane są zawory o charakterystykach:

- liniowej, w której tym samym zmianom stopnia otwarcia zaworu odpowiadają te same zmiany współczynnika przepływu,
- stałoprocentowej, w której tym samym względnym zmianom stopnia otwarcia zaworu odpowiadają te same względne zmiany współczynnika przepływu,
- szybko otwierającej, w której tym samym zmianom stopnia otwarcia zaworu w pobliżu pełnego otwarcia i w pobliżu pełnego zamknięcia zaworu towarzyszą odpowiednio mniejsze i większe zmiany współczynnika przepływu.

Wybór rodzaju charakterystyki przepływowej zaworu jest uzależniony między innymi od charakterystyki statycznej obiektu regulacji. Odpowiedni dobór tej charakterystyki pozwala na przynajmniej częściowe skompensowanie nieliniowości łącznej charakterystyki statycznej zaworu i obiektu regulacji. Z tego między innymi powodu, w zaworach regulacyjnych stosowanych np. do sterowania procesami cieplnymi stosowane są częściej zawory o charakterystykach stałoprocentowych niż liniowych.

Niektóre inteligentne elementy wykonawcze pozwalają na swobodne, programowe kształtowanie charakterystyki statycznej. Pozwala to między innymi na wygodną korekcję nieliniowości charakterystyk statycznych obiektów regulacji.



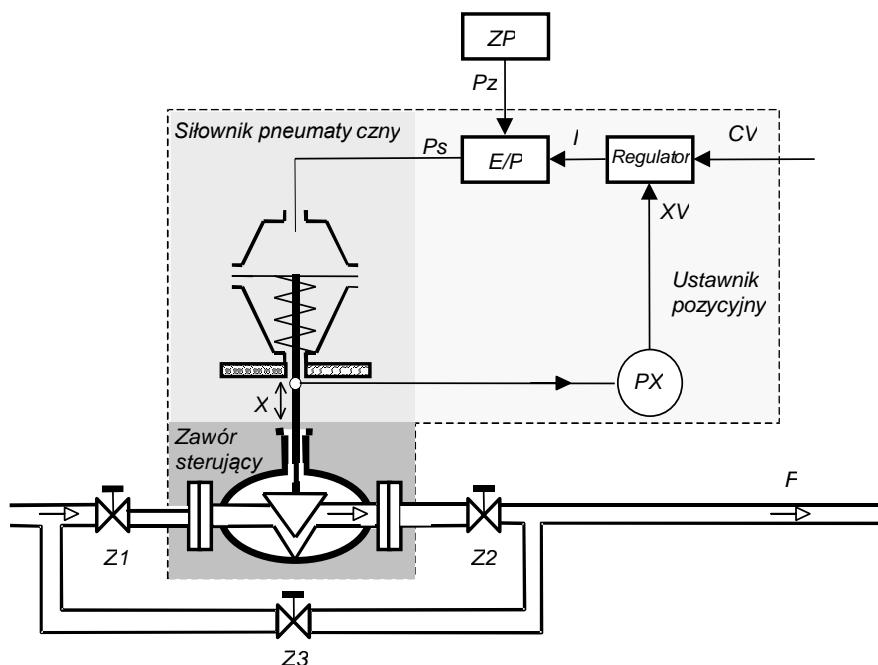
Rys. 5.8: Standardowe charakterystyki przepływowe zaworów regulacyjnych

5.4. INSTALACJA ELEKTROPNEUMATYCZNYCH ELEMENTÓW WYKONAWCZYCH

Istnieje wiele sposobów instalacji elektropneumatycznych elementów wykonawczych. W przypadku instalacji technologicznych pracujących w ruchu ciągłym, stosowany jest często schemat instalacji pokazany schematycznie na rysunku 9. Przemysłowy przykład realizacyjny tego układu pokazano na rysunku 5.10. W układzie tym, oprócz zaworu regulacyjnego, stosowane są dodatkowo trzy zawory odcinające sterowane ręcznie (Z1, Z2 i Z3) oraz rurociąg obejściowy. W stanie normalnej pracy zawory Z1 i Z2 są otwarte natomiast zawór Z3 jest zamknięty. Wymiana zaworu regulacyjnego w ruchu ciągłym wymaga sterowania przepływu medium w trybie ręcznym przy pomocy zaworu Z3 i zamknięcia zaworów Z1 i Z2. Należy przyjąć, że taka zmiana trybu pracy zaworu jest zwykle związana z wprowadzeniem istotnego zakłócenia do regulowanego procesu. Ponadto, wymaga dalszego prowadzenia procesu w trybie ręcznym, co zwykle prowadzi do pogorszenia wartości wskaźników jakości regulacji. Wymiana zaworu regulacyjnego powinna być więc zrealizowana możliwie w jak najkrótszym czasie. W wielu przypadkach jest to o tyle trudne, że np. zawory pracujące w wysokich temperaturach muszą najpierw ulec ochłodzeniu (np. w technologicznych ciągach parowych zawory mogą osiągać temperatury rzędu 400-500°C). Układ instalacji przedstawiony na rysunku 5.9 jest wygodny także do realizacji przeglądów technicznych i napraw elementów wykonawczych w fazach odstawienia lub zatrzymania procesu. Po dokonaniu odpowiednich czynności naprawczych i montażowych, otwierane są zawory Z1 i Z2, a następnie zamknięty jest zawór Z3. Czynności te wprowadzają również zakłócenia procesu, podobnie jak w przypadku demontażu zaworu.

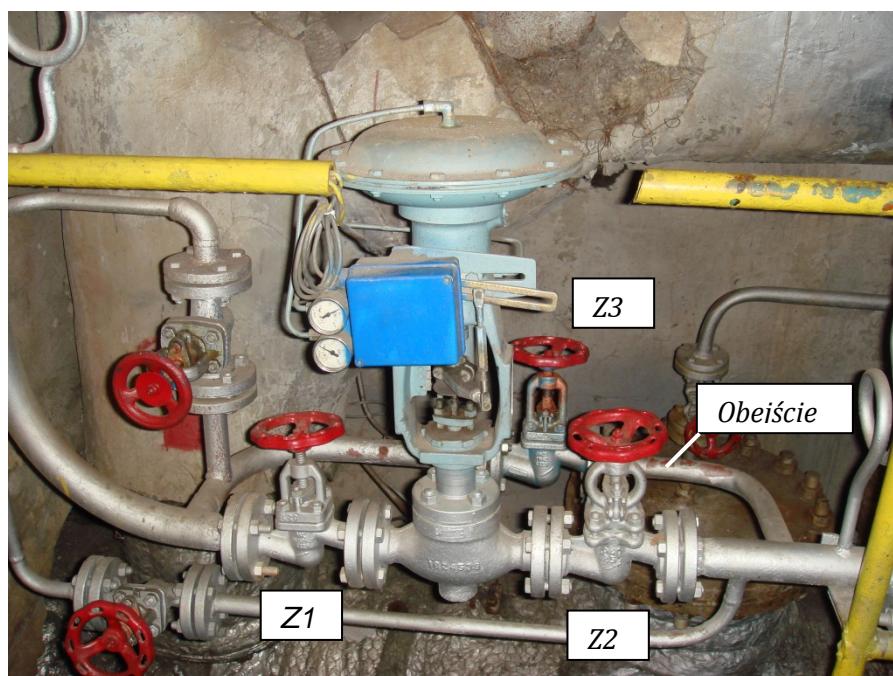
Ogólnie rzecz biorąc, wymiana zaworu sterującego zwłaszcza w ruchu ciągłym jest kłopotliwa. Jak wskazuje praktyka, w wielu przypadkach wymiana zaworu regulacyjnego w ogóle nie jest konieczna. Przyczyną niesprawności lub uszkodzenia elementu wykonawczego może być poza uszkodzeniem zaworu, także każde inne uszkodzenie w tym uszkodzenie siłownika pneumatycznego, ustawnika pozycyjnego, a nawet może wystąpić przyczyna niezależna np. uszkodzenie przewodu zasilania pneumatycznego. Z punktu widzenia prawidłowości podejmowania odpowiednich decyzji naprawczych, istotna jest przynajmniej informacja, czy uszkodzenie dotyczy zaworu regulacyjnego, czy siłownika pneumatycznego, czy też ustawnika pozycyjnego. Jakkolwiek wymiana siłownika czy ustawnika wymaga również przejścia w tryb pracy ręcznej elementu wykonawczego, ze wszystkimi tego konsekwencjami. Dzięki informacji o potencjalnej lokalizacji uszkodzenia proces naprawy lub wymiany uszkodzonego elementu może być zrealizowany znacznie szybciej i sprawniej. Informacje diagnostyczne lokalizujące uszkodzenie elementu wykonawczego są szczególnie przydatne zwłaszcza w układach, w których element wykonawczy jest montowany bezpośrednio na rurociągu, a więc bez rurociągu obejściowego i zaworu Z3.

Jedną z cech opcjonalnych inteligentnych elementów wykonawczych są wbudowane funkcje autodiagnostyczne.



Rys. 5.9. Schemat instalacji elementu wykonawczego.

Oznaczenia: ZP – zasilanie pneumatyczne, P_z - ciśnienie zasilania, P_s - ciśnienie sterowania siłownika pneumatycznego, PX – przetwornik pomiarowy przemieszczenia tłoczyka siłownika, $Z1$, $Z2$, $Z3$ - zawory odcinające sterowane ręcznie



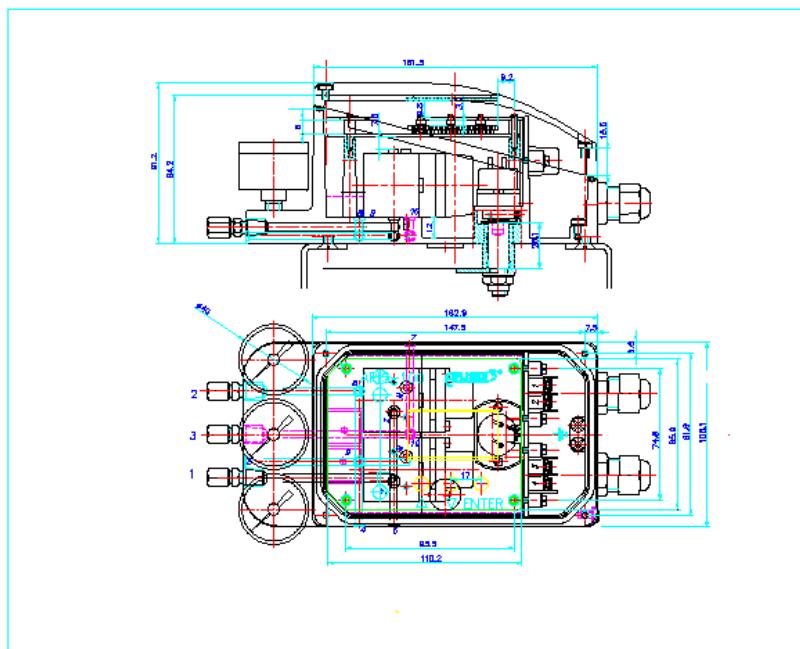
Rys. 5.10. Przykład praktyczny instalacji elementu wykonawczego

5.5. PRZYKŁAD KONSTRUKCJI INTELIGENTNEGO ELEKROPNEUMATYCZNEGO USTAWNIAKA POZYCYJNEGO

Ustawnik pozycyjny stanowi jeden z trzech podstawowych składników konstrukcyjnych elementu wykonawczego (**por. rysunek 5.5**). Proces konstrukcji ustawnika, jak również wielu podobnych mu urządzeń jest procesem długotrwałym i wymagającym znacznych nakładów finansowych. Proces projektowania obejmuje etapy: koncepcyjny, formułowania wymagań konstrukcyjnych, tworzenia modelu, badania eksperymentalne, przygotowanie do produkcji i działania marketingowe. W rozdziale tym zostaną przedstawione główne etapy konstrukcyjne intelligentnego elekropneumatycznego ustawnika pozycyjnego.

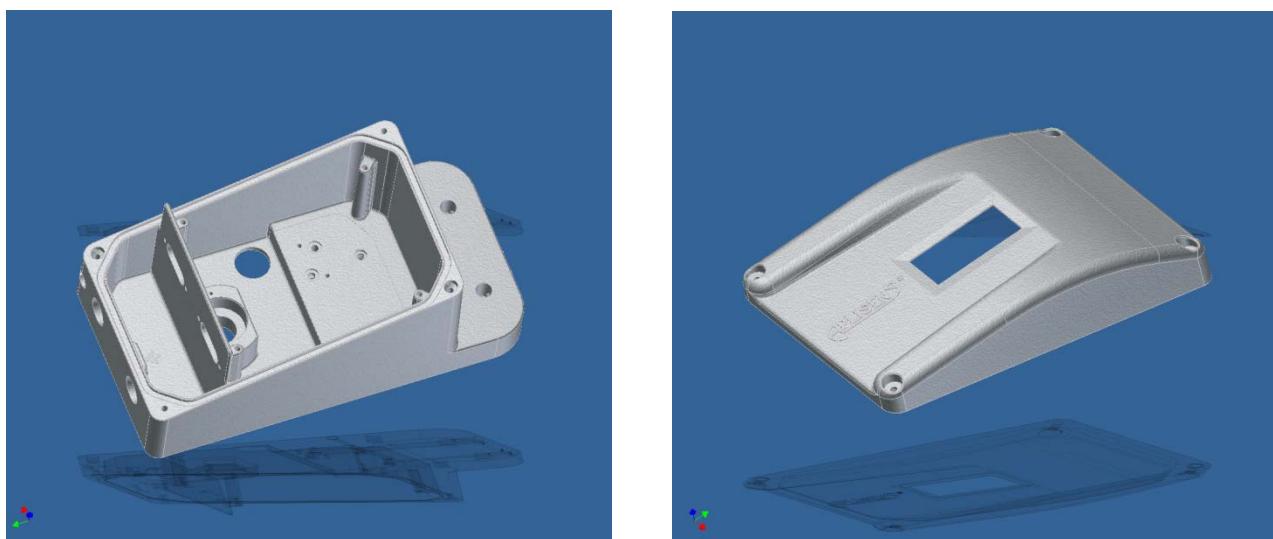
12.5.1 KONSTRUKCJA CZĘŚCI MECHANICZNEJ

Ustawniki pozycyjne przeznaczone są do pracy w warunkach przemysłowych. Warunki te są zwykle warunkami ciężkimi, w których występują często: wysokie temperatury, zapalenie, wstrząsy, wilgoć, agresywne atmosfery chemiczne, niebezpieczeństwo wybuchu, silne zakłócenia elektromagnetyczne, naprężenia mechaniczne, itd. W związku z tym w stosunku do obudowy mechanicznej ustawnika wymaga się: wytrzymałości mechanicznej, zwartości konstrukcyjnej, odporności na korozję, szczelności, wytrzymałości na wpływ wysokich temperatur. Praktycznie wymagania te są możliwe są do spełnienia przez obudowy odlewane ze stopów lekkich metodą ciśnieniową. Technologia wykonywania odlewów metoda ciśnieniowa wymaga wykonania odpowiednich form ciśnieniowych. Formy są elementami bardzo drogimi. Konieczne jest więc sprawdzenie poprawności konstrukcji obudowy jeszcze przed samym wykonaniem form ciśnieniowych. Obecnie stosowana jest w praktyce konstrukcyjnej powszechnie technologia tzw. szybkiego prototypowania. Polega ona na wytworzeniu zastępczych modeli konstruowanych wyrobów w celu sprawdzenia przynajmniej niektórych ich cech oraz uchwycenia ewentualnych błędów konstrukcyjnych. Modele mogą mieć charakter zarówno fizyczny jak i wirtualny. W przypadku konstrukcji obudowy do ustawnika wybrano metodę szybkiego prototypowania polegającą na wykorzystaniu technologii drukowania przestrzennego (3D). Przygotowanie do wydruku przestrzennego może być realizowane w różny sposób. W najprostszym przypadku możliwe jest wykonanie rysunków konstrukcyjnych odlewu w przestrzeni 2D przy pomocy popularnych programów do komputerowego wspierania projektowania np. AutoCAD (rysunek 5.11).



Rys. 5.11. Projekt obudowy ustawnika pozycyjnego w projekcji dwuwymiarowej (za zgodą firmy Aplisens S.A.)

Następnie przy pomocy odpowiedniego oprogramowania rysunki w przestrzeni 2D zostają przekształcone do postaci przestrzennej 3D (**rysunek 5.12**). Dzięki temu możliwe jest oglądanie zaprojektowanej konstrukcji z dowolnej strony oraz zobrazowanie przestrzenne kanałów pneumatycznych krzyżujących się wewnątrz obudowy. Na tym etapie następuje pierwsza korekcja zauważonych błędów konstrukcyjnych.



Rys. 5.12. Projekt obudowy ustawnika pozycyjnego w projekcji trójwymiarowej (za zgodą firmy Aplisens S.A.)

W celu ostatecznej weryfikacji projektu, generowany jest kod wydruku przestrzennego obudowy na specjalną drukarkę 3D. Drukarka ta tworzy wydruk przestrzenny obudowy warstwa po warstwie przy pomocy odpowiednich żywic chemoutwardzalnych. Grubość każdej warstwy wydruku wynosi 0,1mm. Dzięki temu w procesie wydruku uzyskiwane jest precyzyjne odwzorowanie kształtu zaprojektowanej konstrukcji. Żywice stosowane do wydruku mogą być barwione, dzięki czemu wydruk przestrzenny jest bardzo realistyczny. Wytrzymałość mechaniczna oraz parametry skrawania stosowanych do wydruku żywic są na tyle wysokie, że możliwe jest dołączenie do obudowy dodatkowych elementów mocujących. Ze względu na możliwość pracy ustawników w otoczeniu agresywnym chemicznie, elementy mocujące i złączne wykonywane są z materiałów nierdzewnych. Na rysunku 5.13 przedstawiono wydrukowaną obudowę zamontowaną na pneumatycznym siłowniku membranowym jednostronnego działania zainstalowanymi mechanicznymi elementami wewnętrz obudowy i zewnętrz obudowy. Na tym etapie następuje pierwsza druga korekcja zauważonych błędów konstrukcyjnych.



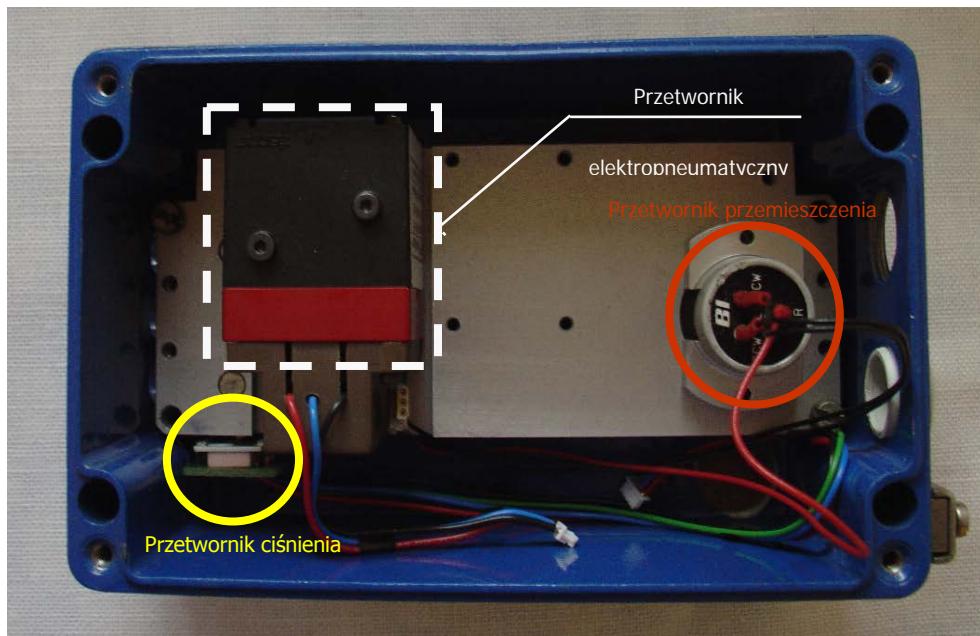
Rys. 5.13. Wydruk trójwymiarowy obudowy ustawnika pozycyjnego. Wydrukowana obudowa została zamontowana na kolumnowym pneumatycznym siłowniku membranowym jednostronnego działania. W obudowie zainstalowano mechaniczne elementy wewnętrzne i zewnętrzne.

Po wydrukowaniu i zweryfikowaniu modelu obudowy ustawnika możliwe jest skorygowanie zauważonych błędów i uruchomienie procesu wytwarzania formy wysokosiągniętej.

5.5.1. MODEL FUNKCJONALNY

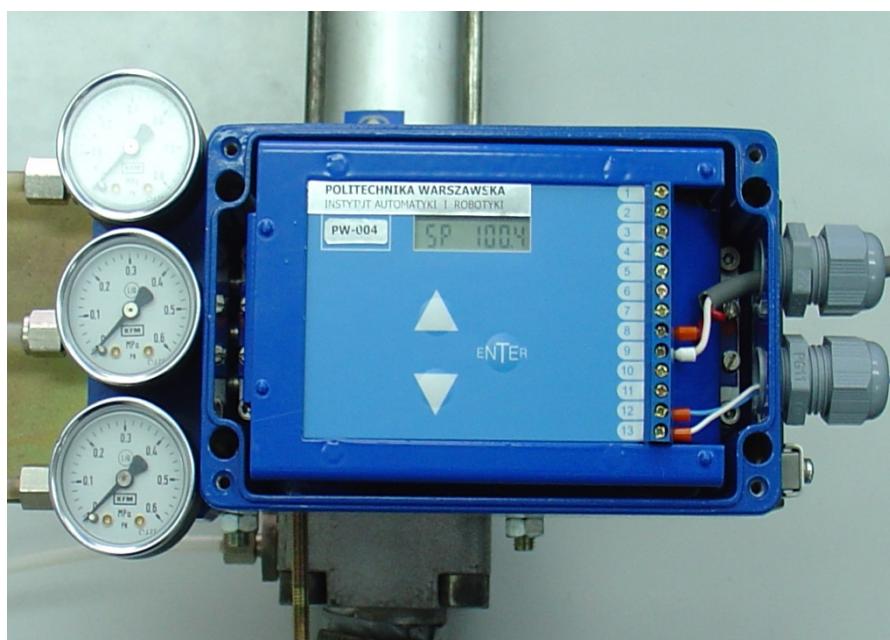
Model funkcjonalny budowany jest w celu weryfikacji podstawowych założeń konstrukcyjnych. Model funkcjonalny jest modelem fizycznym, w którym stosowane są zastępcze elementy mechaniczne i elektroniczne. Elementy te dobierane są w taki sposób, aby ich zastąpienie przez elementy docelowe nie wpłynęło w zasadniczy sposób na podstawowe funkcje projektowanego urządzenia. Dzięki temu możliwe jest przeprowadzenie wstępnych badań funkcjonalnych. Takie podejście pozwala na istotne skrócenie okresu projektowania urządzenia. Dla przykładu badania funkcjonalne ustawnika mogą być prowadzone równolegle z projektowaniem i weryfikacją jego obudowy docelowej. Na rysunku 5.14 przedstawiono model funkcjonalny inteligentnego ustawnika pozycyjnego bez części elektronicznej. Model ten składa się z zastępczej obudowy z zamontowanymi zastępczymi elementami mocującymi wewnętrz obudowy, zastępczego przetwornika ciśnienia,

docelowego przetwornika elekropneumatycznego i docelowego potencjometru służącego do pomiaru przemieszczenia tłocyska siłownika.



Rys. 5.14. Model funkcjonalny inteligentnego ustawnika pozycyjnego bez części elektronicznej. Model ten składa się z zastępczej obudowy z zamontowanymi zastępczymi elementami mocującymi wewnętrz obudowy, zastępczego przetwornika ciśnienia, docelowego przetwornika elekropneumatycznego i docelowego potencjometru służącego do pomiaru przemieszczenia tłocyska siłownika.

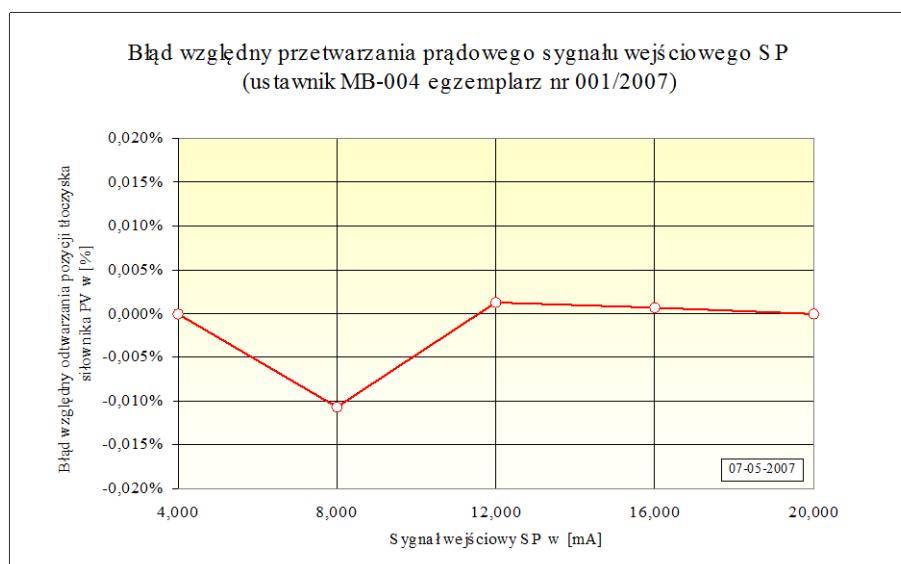
Na rysunku 5.15 przedstawiono pełny model funkcjonalny ustawnika zamontowanego na siłowniku tłokowym. W takiej postaci model umożliwia przeprowadzenie badań eksperymentalnych.



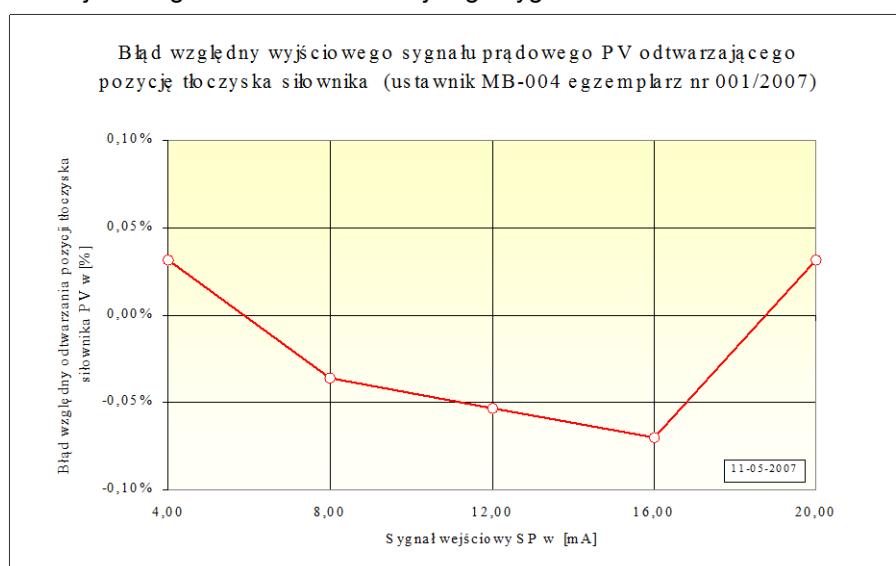
Rys. 5.15. Pełny model funkcjonalny inteligentnego ustawnika pozycyjnego zamontowany na siłowniku tłokowym działania.

5.5.2. BADANIA LABORATORYJNE MODELU FUNKCJONALNEGO

Badania laboratoryjne modelu funkcjonalnego polegają na sprawdzeniu stopnia spełnienia założeń funkcjonalnych stawianych na etapie formułowania wymagań konstrukcyjnych. Przeprowadzane są starannie zaplanowane badania, których celem jest analiza cech funkcjonalnych badanego urządzenia i wypracowania wniosków prowadzących do udoskonalenie jego konstrukcji w części mechanicznej, elektronicznej, sensorycznej, elektrotechnicznej i oprogramowaniu wewnętrznym. Przedstawimy tutaj kilka wybranych wyników badań rzeczywistego modelu funkcjonalnego ustawnika intelligentnego. Na rysunku 5.16 przedstawiono przykład wyniku badania błędu przetwarzania wejściowego prądowego sygnału sterującego modelu funkcjonalnego ustawnika w funkcji tego sygnału. Jak widać z wykresu, maksymalny błąd przetwarzania wynosi 0,011% i spełnia z nadmiarem stawiane wymagania konstrukcyjne (0,05%). Wynik tego badania należy ocenić jako pozytywny.



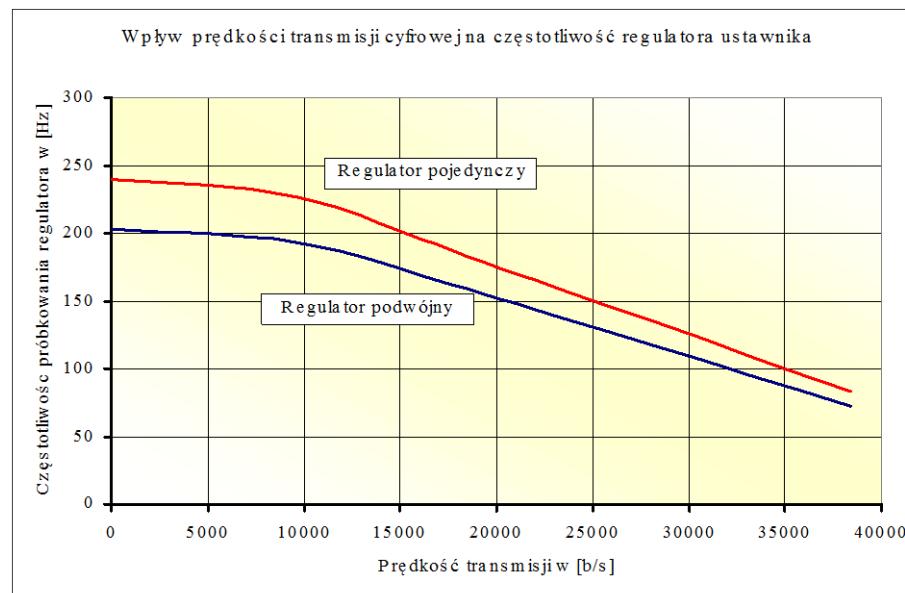
Rys. 5.16.Wynik badania błędu przetwarzania wejściowego prądowego sygnału sterującego modelu funkcjonalnego ustawnika w funkcji tego sygnału.



Rys. 5.17 Wynik badania błędu liniowości modelu funkcjonalnego ustawnika w funkcji prądowego sygnału wejściowego.

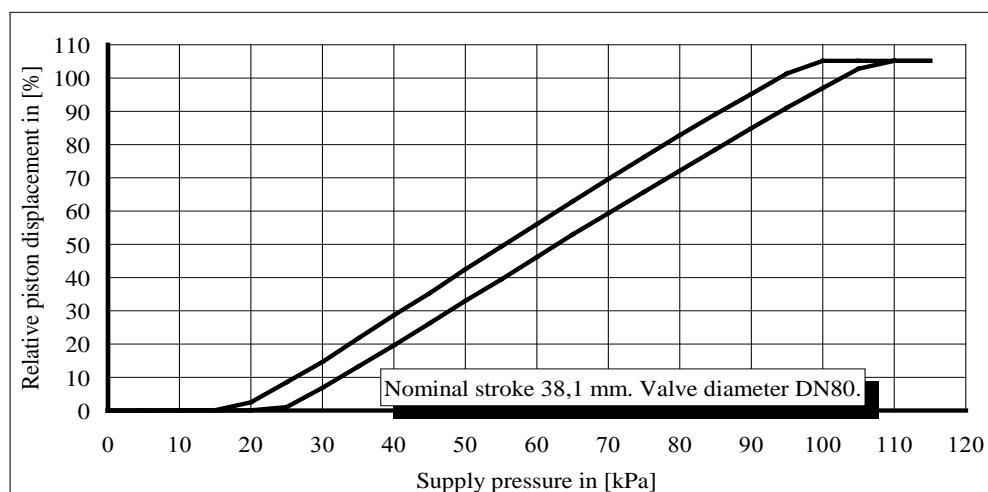
Na rysunku 5.16 przedstawiono przykład wyniku badania błędu liniowości charakterystyki statycznej modelu funkcjonalnego ustawnika. Charakterystyka statyczna odtwarza zależność pomiędzy sygnałem wyjściowym i wyjściowym w stanie ustalonym. W większości ustawników intelligentnych charakterystyka ta może być programowana. Standardową charakterystyką statyczną jest jednak charakterystyka liniowa. W celu oceny rozbieżności pomiędzy idealną i rzeczywistą charakterystyką statyczną tworzona jest różnica tych charakterystyk. Różnica ta nazywana jest błędem liniowości. Na rysunku 5.16 przedstawiono zależność błędu liniowości modelu funkcjonalnego ustawnika w funkcji wejściowego sygnału sterującego. Jak widać z wykresu, maksymalny błąd liniowości nie przekracza 0,07% i spełnia z nadmiarem stawiane wymagania konstrukcyjne (0,20%). Wynik tego badania należy ocenić jako pozytywny.

Regulator wewnętrzny ustawnika realizowany jest w sposób programowy zgodnie z odpowiednim algorytmem regulacyjnym. Algorytm ten na podstawie aktualnych i przeszłych wartości sygnałów wejściowych (sterujących i pomiarowych) oraz przeszłych wartości sygnału wyjściowego okresowo (z tzw. okresem próbkowania) wyznacza nową wartość wyjściową sterowania. Ważne jest aby okres ten był dostatecznie krótki. W przypadku ustawników elektropneumatycznych okres ten nie powinien przekraczać 10ms. Mikrokontroler realizujący oprogramowanie wewnętrzne ustawnika oprócz funkcji regulacyjnych realizuje w czasie rzeczywistym wiele innych współbieżnych zadań, w tym między innymi zadania komunikacyjne. Zadania komunikacyjne absorbują znaczne moce obliczeniowe, tym większe im większe są prędkości komunikacyjne. W niektórych przypadkach udział mocy obliczeniowych wewnętrzne układu mikrokontrolera przeznaczony na obsługę zadań komunikacyjnych jest wyższy niż udział przeznaczony na realizację zadań regulacyjnych. W takich przypadkach zachowanie maksymalnego dopuszczalnego okresu próbkowania regulatora może stanowić istotny problem. Na rysunku 5.18 przedstawiono zależność pomiędzy prędkością transmisji i częstotliwością próbkowania (odwrotnością okresu próbkowania) regulatora. Jak widać z wykresu dla badanej wersji oprogramowania, przy prędkości transmisji 19200 b/s okres ten jest w przybliżeniu równy 6,5 ms. Wartość krytyczną (10ms) osiąga okres próbkowania przy prędkości komunikacji rzędu 32000 b/s.

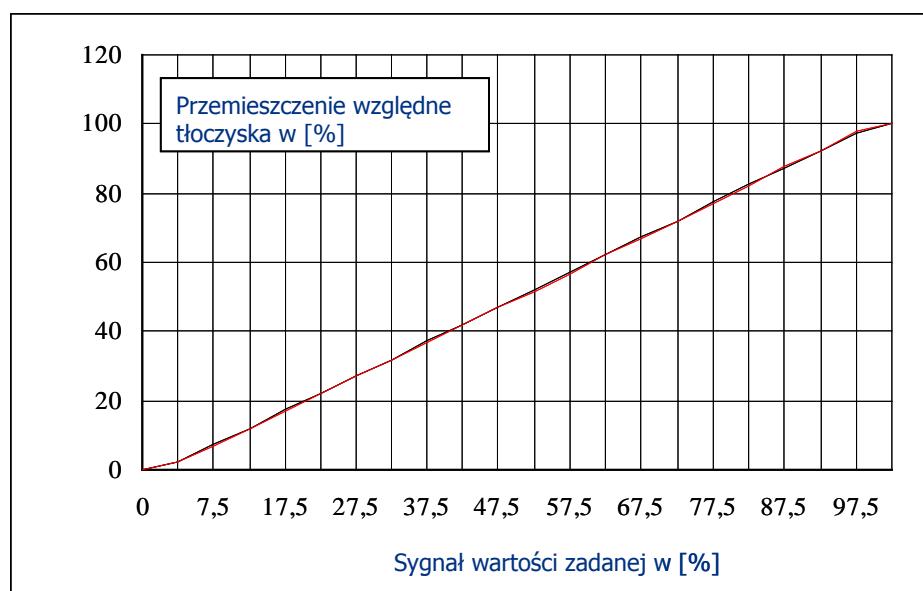


Rys. 5.18 Wpływ prędkości komunikacji cyfrowej na częstotliwość próbkowania regulatora wewnętrznego ustawnika.

Jednym z podstawowych zadań ustawnika pozycyjnego jest kompensacja nieliniowej i niejednoznacznej charakterystyki statycznej zespołu siłownik pneumatyczny-zawór regulacyjny. Gdyby nie stosowano ustawnika pozycyjnego w elemencie wykonawczym automatyki, to charakterystyka sterowania (względne przemieszczenie tłoczyska siłownika w funkcji wejściowego ciśnienia sterującego siłownika) mogłyby wyglądać jak na rysunku 5.19. Szerokość pętli histerezy nie jest stała. Zarówno szerokość jak i położenie histerezy zmieniają się w trakcie eksploatacji elementu wykonawczego. W rzeczywistych układach szerokość pętli histerezy waha się w granicach od 4 do 40%. Szerokość pętli histerezy pokazanej na rysunku 5.19 wynosi ok. 10%. Taka niejednoznaczność charakterystyki sterowania elementu wykonawczego jest niedopuszczalna w większości układów regulacji automatycznej stosowanych w procesach ciągłych.



Rys. 5.19 Charakterystyka statyczna pneumatycznego siłownika membranowego jarzmowego jednostronnego działania z zamocowanym zaworem regulacyjnym.



Rys. 5.20. Charakterystyka statyczna zespołu wykonawczego automatyki składającego się z ustawnika pozycyjnego, pneumatycznego siłownika membranowego jarzmowego jednostronnego działania i zaworu regulacyjnego.

Zastosowanie ustawnika pozycyjnego pozwala na linearyzację charakterystyki statycznej całego elementu wykonawczego. Na **rysunku 20** przedstawiono charakterystykę statyczną elementu wykonawczego zawierającego siłownik i zawór regulacyjny o charakterystyce przedstawionej na rysunku 19 i zawierającego dodatkowo ustawnik pozycyjny. W tym przypadku sygnałem sterującym jest sygnał wartości zadanej podawany na ustawnik, a nie na siłownik. Siłownik jest sterowany przez ustawnik w zamkniętej pętli regulacyjnej ze sprzężeniem od przemieszczenia tłoczyska siłownika. Jak łatwo zauważyć została radykalnie poprawiona liniowość tej charakterystyki i zmniejszona szerokość strefy histerezy do akceptowalnego poziomu nie przekraczającego wartości 0,5%.

5.5.3. OPROGRAMOWANIE

Urządzenia inteligentne posiadają bardzo rozbudowane oprogramowanie wewnętrzne. W znacznej mierze właściwości funkcjonalne takiego urządzenia są pochodną jakości tego oprogramowania. Oprogramowanie to ma zwykle budowę modułową. Każdy moduł realizuje określoną funkcję. Podstawowymi modułami programowymi są moduły:

- komunikacyjny – odpowiedzialny za komunikację ustawnika ze światem zewnętrznym,
- regulacyjny – odpowiedzialny za realizację algorytmu sterowania w wewnętrznej pętli regulacyjnej ustawnika,
- pomiarowy – odpowiedzialny za współpracę z przetwornikami pomiarowymi
- diagnostyczny – odpowiedzialny za detekcję i lokalizację uszkodzeń wewnętrznych,
- logistyczny – odpowiedzialny za koordynację współpracy pomiędzy modułami

Oprogramowanie wewnętrzne w urządzeniach inteligentnych nazywane jest mianem oprogramowania wbudowanego lub firmware.

Należy zwrócić uwagę, że oprogramowanie wewnętrzne ustawnika realizuje obsługę współbieżnych zadań programowych realizowanych w czasie rzeczywistym. Narzuca to szczególne wymagania na obsługę tzw. wątków krytycznych czasowo. Wątki krytyczne czasowo powinny być obsługiwane z wysokim priorytetem, a czas obsługi optymalizowany czasowo. Z tego powodu oprogramowanie wewnętrzne ustawników konstruowane jest w całości lub przynajmniej w części przy wykorzystaniu języków adresów symbolicznych.

5.5.4. TESTY PRZEMYSŁOWE MODELU FUNKCJONALNEGO

Po zakończeniu fazy badań laboratoryjnych, dokonaniu analizy uzyskanych wyników i wprowadzeniu niezbędnych poprawek zarówno po stronie sprzętowej jak i programowej możliwe jest zrealizowanie testów przemysłowych. Testy przemysłowe mają za zadanie weryfikację przydatności projektowanego urządzenia do zastosowań przemysłowych. Prawidłowe przeprowadzenie testów przemysłowych polega na takim doborze obiektów, aby testowane urządzenia poddawane były skrajnym narażeniom środowiskowym. Do testowania modelu funkcjonalnego został wybrany układ regulacji dysz OFFA w kotle energetycznym opalany na węgiel kamienny w bloku energetycznym w jednej z elektrowni zawodowej w Polsce (rysunek 5.22). Ulokowanie zespołu wykonawczego w tak ważnym obwodzie regulacyjnym wymagało uprzedniego przeprowadzenia odpowiednich badań laboratoryjnych dotyczących badania odporności urządzenia na testowe zaburzenia elektromagnetyczne. Pozytywny wynik tych badań upoważniał do wydania tzw. deklaracji zgodności CE (rysunek 5.21), która jest podstawowym dokumentem wymaganym od urządzeń tego typu.



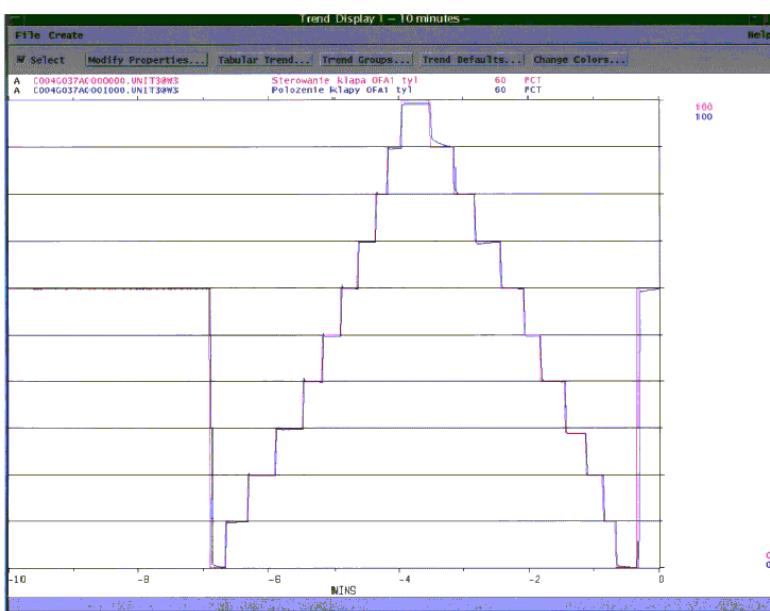
| | | |
|---|---|---|
| POLITECHNIKA WARSZAWSKA WYDZIAŁ MECHATRONIKI Instytut Automatyki i Robotyki 02-525 Warszawa, ul. Św. A. Boboli 8 tel. 022 849 96 16, fax: 022 849 03 98 | | |
| Declaration of conformity | | |
| Konformitätserklärung | | |
| Déclaration de conformité | | |
| confirming the correspondence with the requirements of the European guidelines for low-voltage facilities and electromagnetic compatibility (89/336/EEC; 73/23/EEC) zur Bestätigung der Übereinstimmung mit den Anforderungen der europäischen Richtlinien für Niederspannungs- einrichtungen und EMV(89/336/EWG; 73/23/EWG); | | |
| avec les exigences des directives européennes «Basse tension» et «Compatibilité électromagnétique» (89/336/EWG; 73/23/EWG); | | |
| POLITECHNIKA WARSZAWSKA WYDZIAŁ MECHATRONIKI Instytut Automatyki i Robotyki 02-525 Warszawa, ul. Św. A. Boboli 8 | | |
| declare to their own responsibility that the product | erklärt, in alleiniger Verantwortung, daß das Produkt | déclare sous sa seule responsabilité que le(s) produit(s) |
| PW-004*) | | |
| *) and possible versions to which this declaration refers, is in line with the following harmonised standards: | | |
| *) und etwaige Ausführungen auf die sich diese Erklärung bezieht, mit den/den Bestimmungen folgender harmonisierter Normen übereinstimmt | | |
| *) et les variantes éventuelles objets de cette déclaration, est (sont) conforme(s) aux exigences des normes suivantes: | | |
| EN 61000-4-3:2002 EN 61000-4-4:1999 EN 61000-4-5:1998 EN 61000-4-8:1998 EN 61514-6.6.11:2002 | | |
| Warszawa, 31-05-2007 | | |
| /dr inż. Michał Bartysi/ | | |

Rys. 5.21. Deklaracja zgodności z dyrektywą kompatybilności elektromagnetycznej CE.



Rys. 5.22. Obiekt: klapa regulacyjna w układzie regulacji poziomu emisji NOx w kotle energetycznym turbiny w elektrowni węglowej.

Czas trwania testów przemysłowych nie powinien być zbyt krótki. Jego czas trwania jest umowny. W przypadku ustawnika przyjęto czas testów równy 1 rok. W czasie trwania testów przemysłowych ustawnik podlega ciągłe monitorowaniu oraz dodatkowo co 2 tygodnie dokonywane są jego testy realizowane przez operatorów w trybie ręcznym. Przykład takiego testu (testu nadążania za wymuszeniem skokowym) pokazano na rysunku 5.23. Należy podkreślić, że opisywany w tym miejscu model funkcjonalny przeszedł pomyślnie testy przemysłowe i połużył do opracowania wersji przemysłowej ustawnika.



Rys. 5.23. Przykładowy wynik testu przemysłowego zespołu wykonawczego z testowanym ustawnikiem prowadzony w trybie sterowania ręcznego.

5.6. PODSUMOWANIE

W rozdziale przedstawiono w sposób ogólny rolę i miejsce elektropneumatycznych elementów wykonawczych w układach regulacji. Wskazano zestaw podstawowych cech funkcjonalnych inteligentnych urządzeń wykonawczych. W szczególności zaliczyć do nich należy funkcje: regulacyjne, komunikacyjne, autodiagnostyczne, autonastawcze, programowalność charakterystyk statycznych i funkcje tolerowania uszkodzeń. Podano również ogólne informacje dotyczące budowy i zastosowania inteligentnych elektropneumatycznych elementów wykonawczych automatyki.

5.7. LITERATURA

[5.1] PN-EN 60079 –11:2007: Atmosfery wybuchowe – Część 11: Urządzenia przeciwwybuchowe iskrobezpieczne „i”.

[5.2] DIN IEC 60534: Industrial-Process Control Valves

6. SIECI KOMUNIKACYJNE

Sieci komunikacyjne stanowią obecnie podstawowy element infrastruktury informacyjnej społeczeństw i systemów gospodarczych. Stanowią powszechną i akceptowaną platformę wymiany informacji. Dzięki rozproszeniu i redundancji pozwalają na uzyskanie wysokiego bezpieczeństwa nie tylko przesyłania, ale także przechowywania informacji. Komputerowe sieci komunikacyjne (Internet) stworzyły możliwość prostego i powszechnego dostępu do wiedzy. Dało to szansę na szybszy rozwój gospodarczy, kulturalny i społeczny w skali globalnej. Społeczność skupiona wokół sieci komunikacyjnych nosi nazwę społeczności informacyjnej. W wymiarze globalnym, sieci odgrywają zatem funkcje integracyjne. Sieci komunikacyjne mają nie tylko wymiar globalny, ale także, a może przede wszystkim lokalny. Służą zadaniom szeroko rozumianej komunikacji informacyjnej. Wykorzystywane są do wymiany danych, komunikacji multimedialnej, sterowania i nadzorowania procesami wytwórczymi i montażowymi. Urządzenia techniczne, które są wzajemnie powiązane siecią komunikacyjną będziemy określali mianem urządzeń sieciowych. Urządzenia sieciowe są zwykle rozlokowane przestrzennie i połączone wzajemnie komunikacyjną infrastrukturą sieciową tworzącą kanały komunikacyjne. Z punktu widzenia zasięgu sieci komunikacyjne zalicza się do dwóch zasadniczych grup:

- sieci rozległych i
- sieci lokalnych

Rozległe sieci komunikacyjne (WAN) umożliwiają realizację komunikacji na znaczne odległości przy praktycznie nieograniczonym zasięgu i praktycznie nieograniczonej liczbie urządzeń sieciowych. Z kolei sieci lokalne (LAN) są sieciami o ograniczonym zasięgu i ograniczonej liczbie urządzeń sieciowych. Zadania realizowane przez sieci należące do obu grup są zasadniczo odmienne. Sieci rozległe nie posiadają cech sieci deterministycznych tzn. takich, w których czas realizacji zadania komunikacyjnego jest przewidywalny. Z tego powodu sieci rozległe nie są stosowane do realizacji zadań sterowania i monitorowania procesów wytwórczych i montażowych. Procesy takie realizowane są zazwyczaj współbieżnie lub sekwencyjnie w czasie rzeczywistym, a więc wymagają pewnego rygoru czasowego następstw zdarzeń, w tym także zdarzeń komunikacyjnych. Domeną zastosowań przynajmniej części sieci lokalnych są między innymi zadania sterowania, nadzoru i monitorowania zarówno ciągłych jak i dyskretnych procesów wytwórczych i montażowych. Sieci lokalne mogą podlegać integracji tworząc większe zespoły sieci lokalnych (np. Intranet) lub mogą być integrowane z sieciami rozległymi. Zakres i forma tej integracji zależy od specyficznych wymagań stawianych tym sieciom.

6.1. SIECI LOKALNE

Sieci o ograniczonym zasięgu i ograniczonej liczbie urządzeń sieciowych nazywane są sieciami lokalnymi LAN (ang. *Local Area Network*). Struktury sieci lokalnych są zróżnicowane i zależne od ich zadań, zasięgu i technologii. W odróżnieniu od sieci globalnych WAN, sieci lokalne są z reguły realizowane przez bezpośrednich użytkowników np. przedsiębiorstwa produkcyjne. Zasadniczo zasięg sieci lokalnej ogranicza się do: urządzenia technologicznego, procesu technologicznego, budynku lub grupy budynków, czy przedsiębiorstwa.

W sieciach lokalnych, do zadań komunikacyjnych stosowane są głównie sieci przewodowe. W niektórych przypadkach stosowane są również sieci bezprzewodowe oparte np. na protokołach WiFi czy ZigBee określonych przez standardy grupy IEEE 802.11. Do zadań przesyłu informacji w komunikacji przewodowej stosowany jest powszechnie kabel miedziany i światłowód. W lokalnych sieciach przewodowych stosowna jest coraz powszechniej sieć **Ethernet**. Znajduje ona także coraz to szersze zastosowanie w sieciach przeznaczonych do zastosowań przemysłowych (Industrial Ethernet). Sieci lokalne łączone są do sieci globalnych np. Internetu przy wykorzystaniu łącz takich jak: SDI (obecnie rzadko stosowane), DSL, ADSL lub przy wykorzystaniu modemów kablowych.

Pierwszorzędnym wymaganiem stawianym sieciom lokalnym stosowanym w przemyśle jest bezpieczeństwo personelu i procesu. Ze względu na możliwe ataki, a także wycieki danych, z reguły, sieci takie nie są dołączane do sieci o zasięgu globalnym.

Struktury sieci lokalnych są dość różnorodne. Sieci lokalne mogą być budowane w oparciu o różne **topologie**, takie jak np: magistrala, gwiazda, pierścień, drzewo czy siatka. Topologia sieci jest uzależniona od rodzaju sieci i konkretnego zastosowania. Sieć lokalna jest definiowana przez odpowiednią, tzw. **specyfikację** sieci. Specyfikacja sieci obejmuje sformalizowany opis wymagań dotyczących wymiany informacji w sieci. Opis ten jest najczęściej zgodny z **modelem referencyjnym ISO/OSI**. Specyfikacja taka nosi też nazwę **protołu komunikacyjnego** lub czasami **stosu komunikacyjnego**. Liczba różnych rodzajów sieci lokalnych jest znaczna (przekracza 100). Niektóre z tych sieci są sieciami **zamknietymi** tzn. takimi sieciami, których specyfikacja nie jest dostępna w domenie publicznej. Są one stosowane do zadań specjalnych. Większość sieci ma cechy sieci **otwartych**, tzn. sieci o dostępnej specyfikacji. Są one stosowane powszechnie. Do najczęściej stosowanych sieci lokalnych stosowanych w automatyzacji procesów ciągłych i dyskretnych należą: HART, Foundation Fieldbus, CAN, MODBUS, AS-i, InterBus, PROFIBUS, LonWorks, EIB itd. Mnogość dostępnych systemów sieciowych wynika z różnorodności procesów produkcyjnych i wymagań stawianych tym systemom.

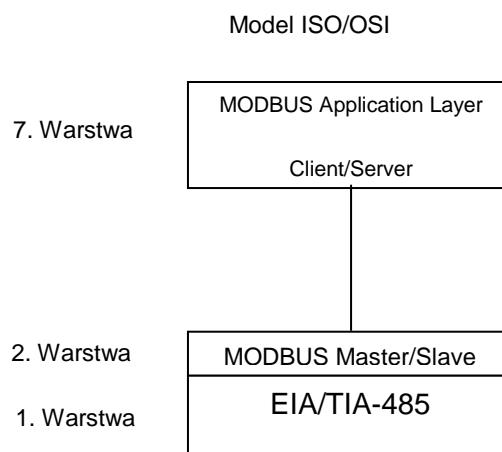
Osobnym zagadnieniem jest integracja sieci lokalnych. Integracja pozwala na tworzenie bardziej kompleksowych struktur sieciowych. Integracja sieci pozwala na zbudowanie szerokiej infrastruktury informatycznej zaspalającej sieci lokalne w przedsiębiorstwach produkcyjnych wykorzystywanych do realizacji zadań: zarządzania, sterowania i wytwarzania. Integracja sieci może przebiegać zarówno w układzie poziomym jak i pionowym. Integracja jest realizowana zarówno na poziomie sprzętu jak i oprogramowania. Sprzężenie dwóch lub więcej sieci wymaga użycia urządzeń fizycznych (np. interfejsów

sieciowych, przełączników, mostków, bramek, wzmacniaków oraz zastosowania specjalnego oprogramowania, które pozwala na dwukierunkowy przepływ informacji pomiędzy różnymi sieciami. Na odpowiednio wysokim poziomie np. na poziomie wymiany informacji pomiędzy poszczególnymi oddziałami danego przedsiębiorstwa wymiana danych realizowana jest najczęściej przy pomocy sieci światłowodowych.

7. SIEĆ MODBUS

7.1. RYS HISTORYCZNY

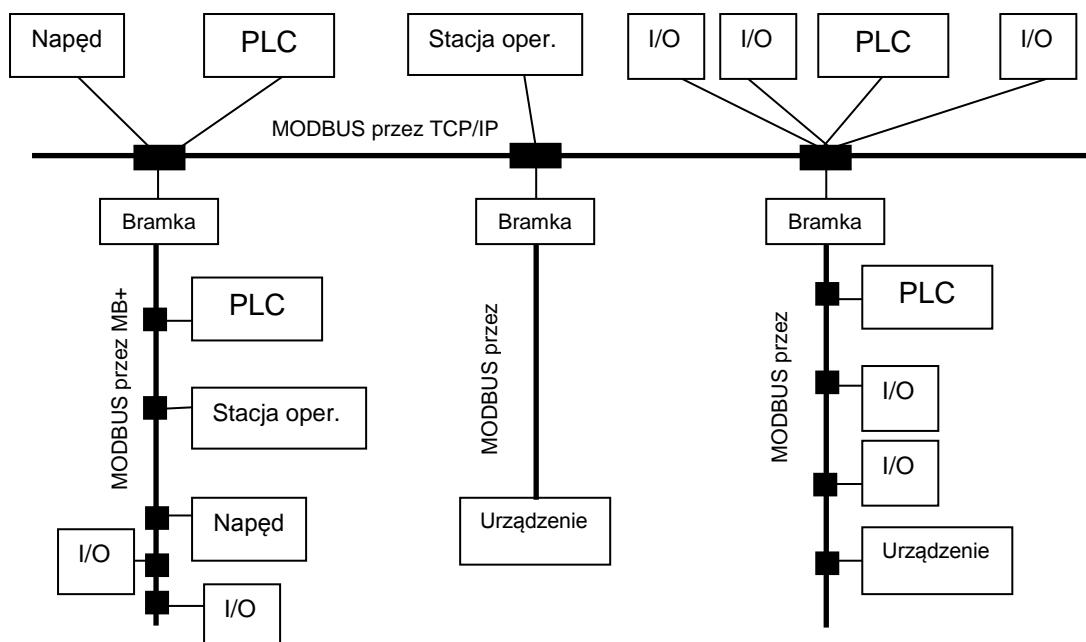
Modbus był pierwszym, powszechnie zaakceptowanym przemysłowym systemem komunikacji sieciowej. Jego historia sięga późnych lat siedemdziesiątych poprzedniego wieku. W roku 1979 producent sterowników PLC firma Modicon opublikowała protokół komunikacyjny przeznaczony dla sieci wieloelementowych, oparty na architekturze typu master/slave. Komunikacja pomiędzy urządzeniami odbywała się za pomocą wiadomości. Warstwa fizyczna interfejsu Modbus była dowolna. Pierwotna postać protokołu wykorzystywała komunikację szeregową RS-232, lecz kolejne implementacje używały RS-485 ze względu na większe dopuszczalne odległości, wyższe prędkości transmisji oraz większą liczbę urządzeń w systemie. W krótkim czasie, pomimo tego, że protokół nie był promowany przez żadne konsorcjum lub organizację standaryzacyjną, setki twórców zaczęło stosować Modbus w swoich urządzeniach. Stał się on *de facto* standardem dla sieci przemysłowych.



Rys. 7.1. Struktura warstwowa protokołu Modbus w odniesieniu do modelu ISO/OSI

Modbus ściśle definiuje strukturę wiadomości, która umożliwia komunikację między urządzeniami. Określa więc sposób adresowania jednostek, interpretację i przetwarzanie wiadomości, ewentualnie proces konstruowania odpowiedzi. Protokół opisuje też wykrywanie i sygnalizację błędów, zarówno tych wynikających z transmisji w kanale komunikacyjnym, jak i tych, których skutkiem jest błędna składnia wiadomości.

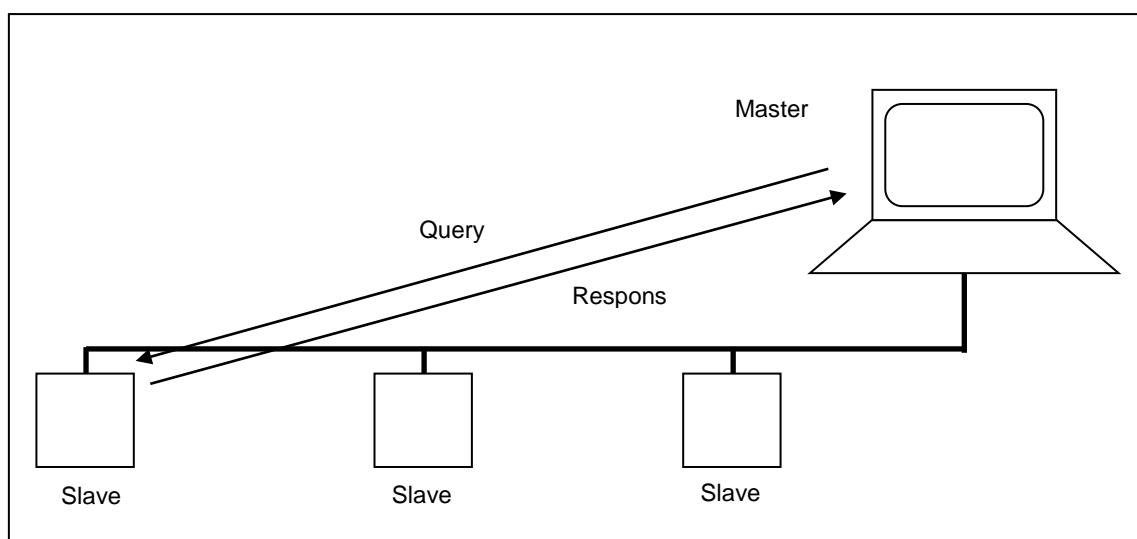
Modbus jest protokołem prostym, łatwym w implementacji a jednocześnie bardzo elastycznym. Pomimo tego, że Modbus jest używany głównie w tradycyjnej asynchronicznej transmisji szeregowej, istnieją także jego rozszerzenia pozwalające na komunikację bezprzewodową oraz przez Ethernet. Istnieje również Modbus Plus – sieć o wysokich prędkościach transmisji, oparta na przekazywaniu znacznika (token). Szeroka gama możliwych warstw fizycznych i identyczna konstrukcja ramki komunikacyjnej niezależna od rodzaju sieci Modbus, pozwalają na tworzenie struktur sieci hierarchicznych.



Rys. 7.2. Hybrydowa struktura hierarchiczna sieci Modbus

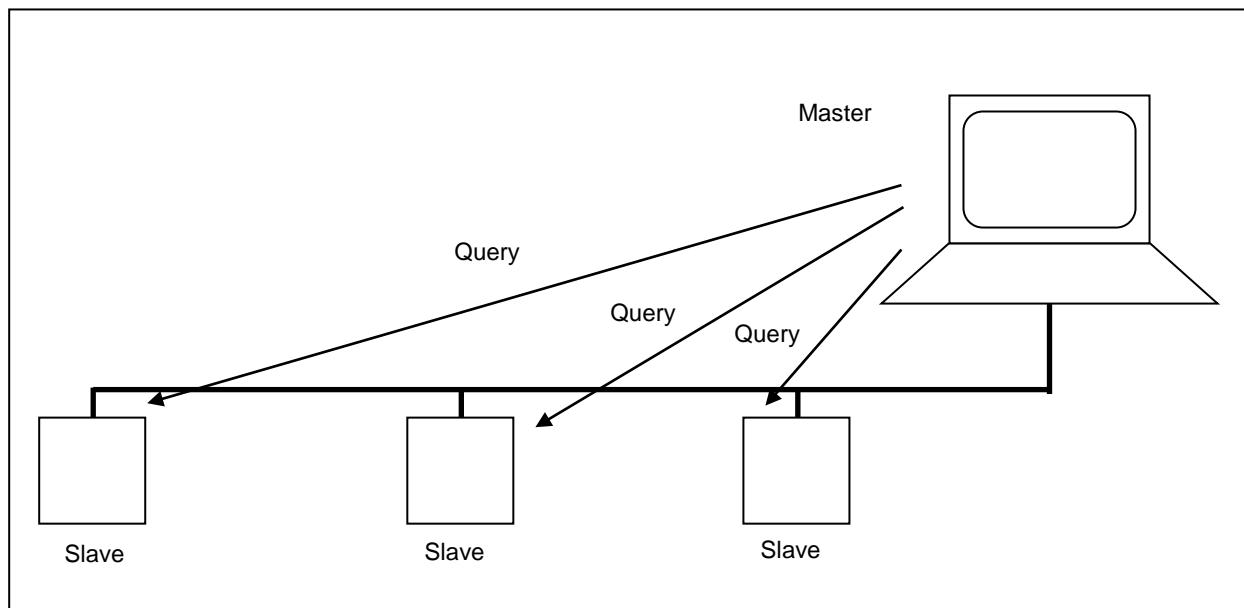
7.2. WYMIANA WIADOMOŚCI POMIĘDZY JEDNOSTKAMI

Urządzenia wykorzystujące interfejs RS-232C komunikują się używając techniki master-slave, w której tylko jedna jednostka nadziedzona (master) może zainicjować wymianę wiadomości, wysyłając zapytanie (query) do urządzeń podporządkowanych (sklave). Urządzenia slave odpowiadają przekazując wymagane dane do jednostki nadziedznej lub podejmując określone w zapytaniu działania. Jednostka master może adresować pojedyncze jednostki podziedne lub wysłać jedną wspólną wiadomość jednocześnie do wszystkich urządzeń (broadcast). Jednostki podziedne odpowiadają zawsze (response) na zapytania, które zostały skierowane indywidualnie do nich. Odpowiedzi na zapytania typu broadcast nie są udzielane.

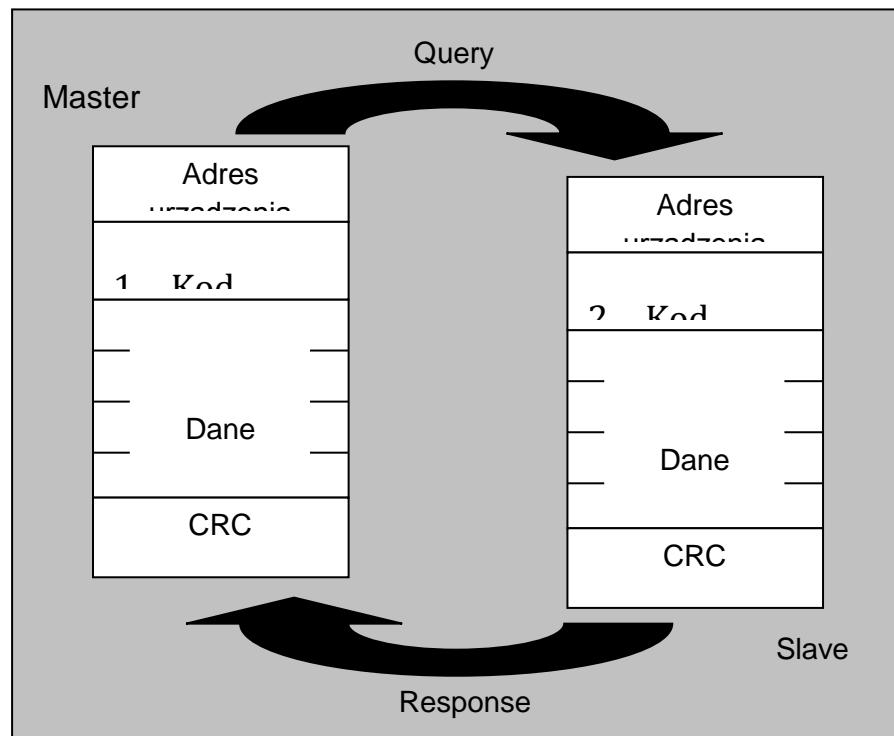


Rys 7.3. Schemat transakcji sieciowej typu zapytanie-odpowiedź w sieci Modbus

Protokół Modbus określa format zapytania. Zapytanie składa się z adresu jednostki podrzędnej (lub adresu broadcast), kodu funkcji, danych wysłania i pola kontrolnego (CRC). Odpowiedź jednostki podrzędnej ma zbliżoną strukturę. Zawiera pole potwierdzające wykonanie wymaganych czynności, dane oraz pole kontrolne. Jeśli w strukturze zapytania pojawi się błąd lub jeśli urządzenie podporządkowane nie jest w stanie wykonać polecenia, to jednostka slave wygeneruje odpowiedź sygnalizującą wystąpienie błędu (exception response).



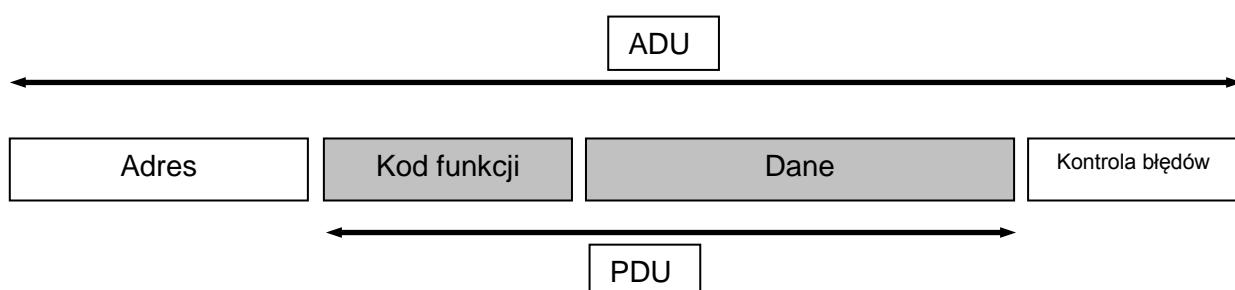
Rys 7.4. Schemat transakcji sieciowej typu rozpowszechniania (broadcast) w sieci Modbus



Rys 7.5. Schemat typowej transakcji sieciowej w sieci Modbus

Urządzenia korzystające z warstw fizycznych takich jak Ethernet, MB+ komunikują się wykorzystując technikę *peer-to-peer*, w której każda jednostka może zainicjować transakcję z inną, dowolną i równorzędną jednostką. W tym przypadku obowiązuje także profil współpracy urządzeń sieciowych zgodny z protokołem master-slave. Urządzenie wysyłające zapytanie przejmuje rolę jednostki nadzorowanej i oczekuje odpowiedzi od jednostki podporządkowanej. Podobnie, jeśli dowolne urządzenie sieciowe odbierze zapytanie, to wygeneruje odpowiedź i wyśle ją do jednostki nadzorowanej.

W ogólnym przypadku protokół Modbus definiuje podstawową ramkę danych PDU (Protocol Data Unit). Dodatkowe pola w ramce zależne są od typu sieci i dopełniają PDU do ADU (Application Data Unit).



Rys 7.6. Schemat ramki w sieci Modbus

Rozmiar PDU jest ograniczony przez maksymalną liczbę bajtów, wynikającą z pierwszej implementacji protokołu przy wykorzystaniu w warstwie fizycznej standardu RS485. W tym przypadku, maksymalny rozmiar ADU wynosi 256 bajtów, natomiast maksymalna liczba bajtów pola PDU wynosi:

$$\text{MODBUS PDU} = 256 - \text{Adres (1 bajt)} - \text{CRC (2 bajty)} = 253 \text{ bajty.}$$

7.3. TRYBY TRANSMISJI

W warstwie fizycznej sieci MODBUS wykorzystywane są dwa standardy komunikacji szeregowej. Są one zgodne ze specyfikacjami RS-232C i RS-485. W obu przypadkach możliwe jest stosowanie w warstwie łącza danych dwóch specyfikacji ADU zwanymi trybami transmisji. Nosią one nazwy odpowiednio: ASCII i RTU. Tryb transmisji definiuje sposób kodowania poszczególnych pól ramki komunikacyjnej. W każdej sieci MODBUS dla wszystkich urządzeń sieciowych tryb transmisji musi być jednakowy.

Tryb ASCII

Każdy bajt ramki danych (8 bitów) jest kodowany w tym trybie w postaci dwóch znaków kodu ASCII (*American Standard Code for Information Interchange*). W trybie tym są dopuszczalne długie przerwy czasowe (do 1s) pomiędzy kolejnymi znakami, nie powodujące powstania błędu integralności przesyłanej ramki.



Format znaku w trybie ASCII:

System kodowania: heksadecymalny, dopuszczalne znaki ASCII: 0–9, A–F

Przykład:

Dana (bajt) **9A** zostanie przesłana w postaci dwóch znaków kodu ASCII tzn. **9** i **A**.

- Znak składa się z:**
- 1 bitu startu
 - 7 bitów danych, najmniej znaczący bit wysyłany jako pierwszy
 - 1 opcjonalny bit kontroli parzystości lub nieparzystości
 - 1 bitu stopu, jeśli włączona jest kontrola parzystości; jeśli nie to 2 bity stopu

Kontrola błędów: Longitudinal Redundancy Check (LRC).

Tryb RTU

W trybie RTU (Remote Terminal Unit) każdy bajt ramki jest przekształcany do postaci jednego znaku o 8-mio bitowym polu danych. Dzięki temu możliwe jest uzyskanie w przybliżeniu dwukrotnie większego stopnia upakowania informacji w porównaniu z trybem ASCII. W odróżnieniu od trybu ASCII, przerwy czasowe pomiędzy sukcesywnymi bajtami podlegają nie mogą przekraczać 1,5 czasu transmisji jednego znaku.

Format znaku w trybie RTU:

System kodowania: binarny 8-bitowy

- Znak składa się z:**
- 1 bitu startu
 - 8 bitów danych, najmniej znaczący bit wysyłany jako pierwszy
 - 1 opcjonalny bit kontroli parzystości lub nieparzystości
 - 1 bitu stopu, jeśli włączona jest kontrola parzystości; jeśli nie to 2 bity stopu

Kontrola błędów: Cyclical Redundancy Check (CRC).

7.4. STRUKTURA RAMKI

W przypadku obu trybów transmisji (ASCII i RTU), nadajnik wiadomości (urządzenie master lub slave) komponuje ramkę transmisyjną składającą się z pola danych oraz pól dodatkowych pozwalających między innymi na kontrolę poprawności przesyłanej wiadomości oraz na jednoznaczne określenie długości ramki.

Ramka w trybie ASCII

W trybie ASCII ramka rozpoczyna się znakiem dwukropka ':' (kod ASCII: $3A_h$), a kończy parą znaków: <CR>, <LF> (odpowiednie kody ASCII: $0D_h$ i $0A_h$). Dla pozostałych pól ramki, dozwolonymi znakami są jedynie znaki: 0..9 i A..F.



| START | ADRES | KOD FUNKCJI | DANE | LRC | KONIEC |
|------------|---------|-------------|----------|---------|-----------------|
| 1 znak ‘:’ | 2 znaki | 2 znaki | N znaków | 2 znaki | 2 znaki CRLF |

Rys 7.7. Schemat ramki w trybie ASCII

Ramka w trybie RTU

W trybie RTU, wysłanie ramki poprzedza przerwa w transmisji. Przerwa ta nie może być krótsza niż 3,5 krotność czasu transmisji pojedynczego znaku. Pierwszym informacyjnym polem ramki jest adres urządzenia, do którego kierowana jest ramka. Następnie przesyłany jest kod funkcji, dane oraz suma kontrolna. Po sumie kontrolnej następuje przerwa w transmisji o czasie trwania nie krótszym niż 3,5 krotny czas transmisji jednego znaku. Bezpośrednio po tej przerwie może zostać wysłana następna ramka. W obrębie ramki przerwy czasowe pomiędzy transmisją kolejnych znaków nie mogą być dłuższe niż 1,5 czasu trwania pojedynczego znaku. Naruszenie tej zasady uznawane jest za dezintegrację ramki komunikacyjnej. Taka ramka musi być odrzucona przez odbiornik informacji.

| START | ADRES | KOD FUNKCJI | DANE | CRC | KONIEC |
|-------------|---------|-------------|-------------|----------|-------------|
| T1-T2-T3-T4 | 8 bitów | 8 bitów | n x 8 bitów | 16 bitów | T1-T2-T3-T4 |

Rys 7.8. Schemat ramki w trybie RTU

7.4.1. ADRES

Pole adresowe ramki składa się z dwóch znaków (ASCII) lub 1 znaku (RTU). Poprawne adresy MODBUS mogą przyjmować wartości w zakresie od 0 do 247. Urządzenia podporządkowane przyjmują adresy z zakresu 1..247. Adres 0 jest zarezerwowany dla trybu rozpuszczania (*broadcast*).

Adres umieszczany jest w polu adresowym zarówno przez jednostkę nadzorową w ramce rozkazowej jak również przez jednostkę podrzędną w ramce odpowiedzi.

7.4.2. KOD FUNKCJI

Kod funkcji składa się z dwóch znaków (ASCII) lub 1 znaku (RTU). Poprawne kody funkcji zawierają się w przedziale od 1 do 127. Zestawy funkcji realizowanych przez różne urządzenia mogą być różne.

Istnieją trzy rodzaje kodów funkcji MODBUS:

Kody publiczne:

- zdefiniowane,
- niepowtarzalne,
- zatwierdzone przez społeczność MODBUS-IDA.org,
- udokumentowane,
- zgodne dla wszystkich urządzeń.



Kody użytkownika:

- to kody o wartościach z przedziałów: 65..72 i 100..110,
- użytkownik może wybrać i zaimplementować własną funkcję o kodzie, którego nie ma w specyfikacji MODBUS,
- nie ma gwarancji, że kod i znaczenie funkcji użytkownika będzie unikalne w sieci,
- użytkownik może starać się o włączenie funkcji do grupy funkcji publicznych,

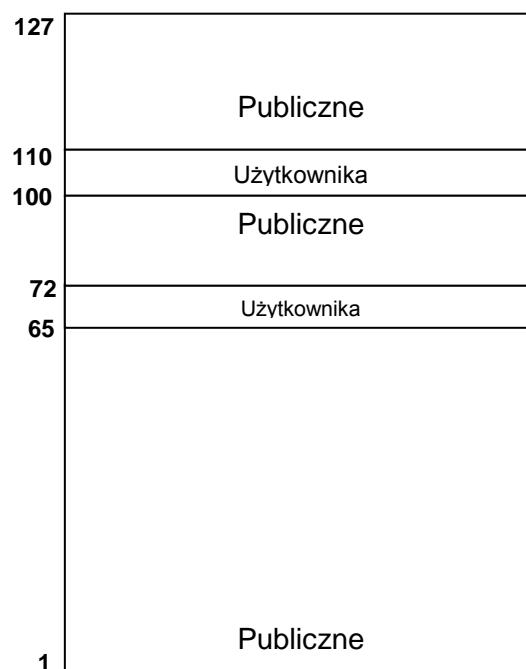
Kody zastrzeżone:

- kody stosowane przez konkretne firmy i niedostępne publicznie.

Kod funkcji umieszczony w ramce rozkazowej określa czynności, jakie musi wykonać jednostka podrzędna. Kod funkcji umieszczony w ramce odpowiedzi informuje jednostkę nadzorującą o przyjęciu lub odrzuceniu ramki rozkazowej. Jeśli kod funkcji w ramce odpowiedzi jest zgodny z kodem funkcji ramki rozkazowej, to oznacza, że urządzenie podporządkowane przyjęło rozkaz do realizacji. Jeśli jest inaczej, to oznacza, że urządzenie podporządkowane odrzuciło rozkaz. Wówczas w odpowiedzi oryginalny kod funkcji zostaje uzupełniony jedynką na najstarszej pozycji bitowej.

Przykład:

Kod rozkazu w ramce rozkazowej ma kod 03_h (rozkaz odczytu rejestrów). Jeśli ramka ta zostanie przyjęta przez urządzenie slave (nie wystąpią błędy), to w ramce odpowiedzi zostanie zwrocony taki sam kod funkcji. W przeciwnym przypadku kod funkcji w ramce odpowiedzi przyjmie wartość: 83_h . Stąd wynika, że kody funkcji z przedziału 128-255 są zarezerwowane dla odpowiedzi wyjątkowych. Niektóre funkcje wymagają podania także kodów dodatkowych (*sub-function codes*).



Rys 7.9. Mapa legalnych kodów funkcji MODBUS

7.4.3. POLE DANYCH

Zależnie od trybu transmisji, pole danych ramki składa się z par znaków ASCII lub pojedynczych znaków RTU. Pole danych w ramce rozkazowej wysyłanej przez jednostkę nadzorującą, zawiera ponadto dodatkowe informacje niezbędne jednostce podrzędnej do wykonania operacji wskazanych przez kod funkcji. Dane te mogą zawierać adresy rejestrów i pół bitowych, liczbę bajtów zawartych w polu, itp. W niektórych rozkazach pole danych może być polem pustym.

Model danych MODBUS

Model danych Modbus definiuje cztery typy danych:

| Typ | Postać | Rodzaj | Interpretacja |
|-------------------|-------------|------------|---|
| Discrete Inputs | Single bit | Read-Only | Pole jednabitowe przeznaczone jedynie do odczytu. Modyfikacja pola nie może być dokonana przy pomocy funkcji Modbus. |
| Coils | Single bit | Read-Write | Pole jednabitowe przeznaczone do zapisu i odczytu. Możliwa jest modyfikacja tego przy pomocy funkcji Modbus. |
| Input Registers | 16-bit-word | Read-Only | Rejestr szesnastobitowy przeznaczony jedynie do odczytu. Modyfikacja tego typu rejestru nie może być dokonana przy pomocy funkcji Modbus. |
| Holding Registers | 16-bit-word | Read-Write | Rejestr szesnastobitowy przeznaczony do zapisu i odczytu. Możliwa jest modyfikacja tego typu rejestrów przy pomocy funkcji Modbus. |

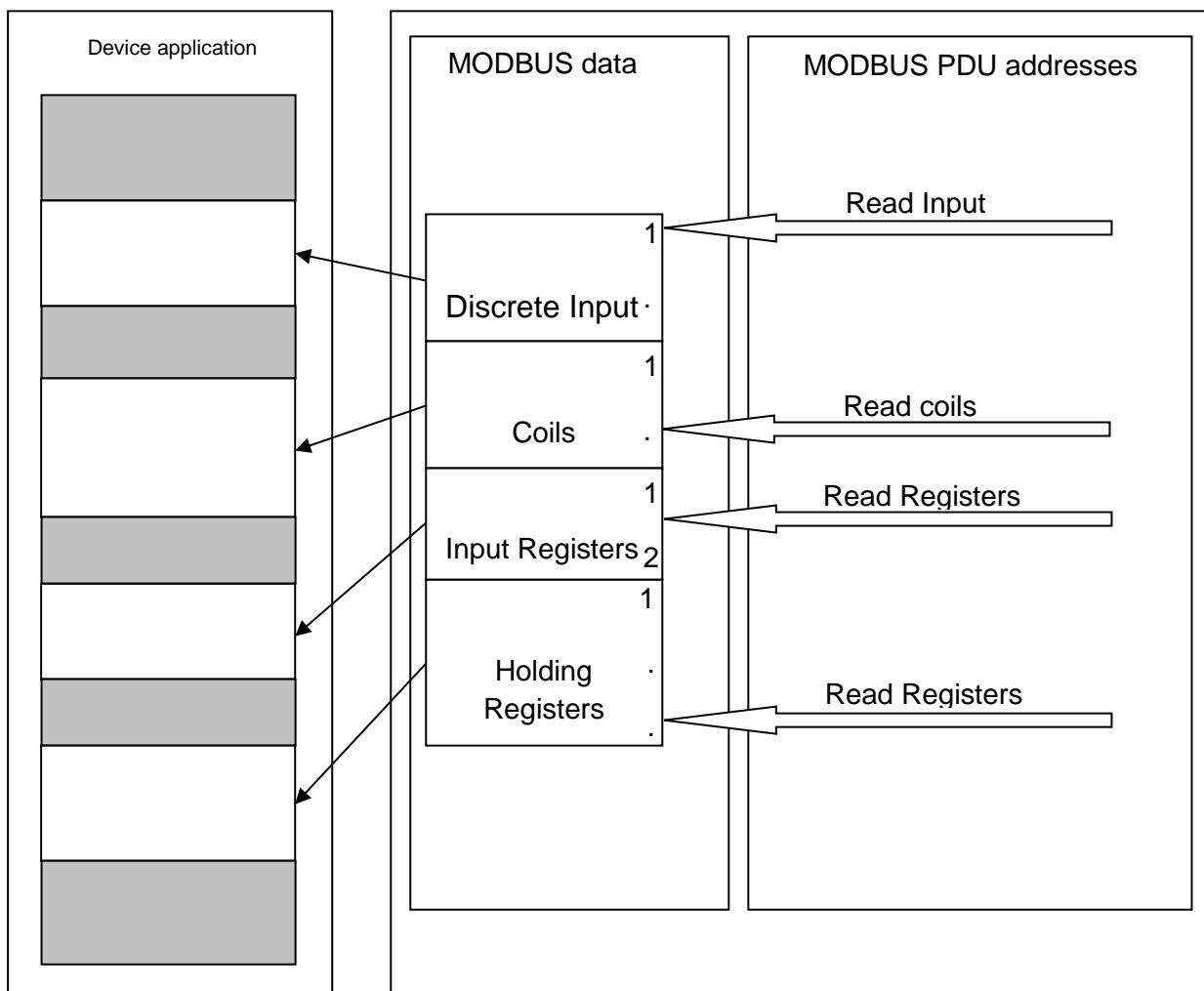
Rys 7.10. Typy danych MODBUS

Specyfikacja Modbus dopuszcza możliwość adresowania do 2^{16} elementów każdego typu danych. Typ danych jest wskazywany przez numer kod funkcji. Zatem kod funkcji niesie nie tylko informację o realizowanym rozkazie, ale również o typie danych w polu danych.

Adresy danych

Należy odróżnić adresy urządzeń i adresy danych. Adres urządzenia służy do zaadresowania (wskazania) urządzenia podporządkowanego przez jednostkę nadzorującą. Adresy danych dotyczą adresów zasobów pamięci wskazanego urządzenia. W specyfikacji Modbus przyjęto, że adresy początkowe wszystkich struktur danych w pamięci urządzeń podporządkowanych będą rozpoczynały się od zera. Stąd np. pierwsze pole bitowe o będzie miało przyporządkowany adres 0 a 127 pole bitowe – adres 126, a rejestr (holding register o numerze 40108 będzie miał przyporządkowany adres 0107.





Rys 7.11. Mapowanie struktur danych w pamięci urządzenia MODBUS

Oczywisty jest fakt, że adresy fizyczne w pamięci wewnętrznej urządzeń MODBUS nie powinny być mylone z adresami struktur zdefiniowanymi zgodnie z modelem danych (MODBUS data model).

Notacja

Specyfikacja Modbus wykorzystuje system kodowania danych zgodną z notacją „big-Endian”. Oznacza to, że jeśli przesyłana jest dana o długości przekraczającej jeden bajt, to najbardziej znaczący bajt wysyłany jest jako pierwszy. Na przykład, szesnastobitowe słowo 0x1234 zostanie przesłane w postaci sekwencji bajtów: 0x12 i 0x34.

| Notacja | Kolejność bajtów |
|---------------------------------|---------------------|
| big-Endian | 0x10 0x20 0x30 0x40 |
| big-Endian with byte-swapped | 0x20 0x10 0x40 0x30 |
| little-Endian | 0x40 0x30 0x20 0x10 |
| little-Endian with byte-swapped | 0x30 0x40 0x10 0x20 |

Rys 7.12. Typy notacji

7.4.4. POLE KONTROLI BŁĘDÓW

Modbus wykorzystuje dwa niezależne rodzaje kontroli poprawności transmisji. Stosowana jest zarówno kontrola parzystości w odniesieniu do każdego pojedynczego znaku ramki jak również stosowana kontrola poprawności całej ramki.

Tryb ASCII

W trybie ASCII kontrola ramki oparta jest na metodzie LRC (*Longitudinal Redundancy Check*). Pole LRC stanowi liczba ośmiobitowa, przesyłana jako dwa znaki ASCII, w dwóch oddzielnych ramkach transmisji szeregowej. LRC weryfikuje poprawność wiadomości, a więc do jej wyznaczenia nie sąbrane znaki startu <:> i końca <CRLF> ramki.

Wartość LRC jest obliczana i dodawana do ramki zawsze przez urządzenie nadające. Odbiornik informacji wyznacza własne LRC na podstawie zawartości odebranej ramki i porównuje ją z wartością odebranej LRC. Błąd zostaje wykryty, gdy obie wartości nie są identyczne.

Wartość LRC jest obliczana przez sumowanie kolejnych bajtów ramki. Wszystkie przeniesienia są ignorowane. Na koniec zawartość LRC jest dopełniana do dwóch. Procedura tworzenia LRC jest następująca:

1. Sumuj wszystkie bajty ramki w arytmetyce stałoprzecinkowej ośmiobitowej,
2. Dokonaj uzupełnienia dwójkowego uzyskanego wyniku.

Funkcja generująca LRC może wyglądać następująco:

```
unsigned char LRC(unsigned char *pWiadomosc, unsigned short LiczbaBajtow)
{
    unsigned char LRC = 0x00 ;
    while (LiczbaBajtow--)
        LRC += *pWiadomosc++;
    return (~LRC + 0x01) ;
}
```

Pole LRC jest przesyłane w postaci dwóch znaków ASCII. Znak zawierający cztery starsze bity jest wysyłany jako pierwszy.

Tryb RTU

W trybie RTU kontrola poprawności transmisji oparta jest na metodzie CRC (*Cyclical Redundancy Check*). CRC służy do weryfikacji całej ramki i jest wyznaczane niezależnie od opcjonalnej kontroli parzystości każdego znaku.

Pole CRC jest polem 16-bitowym, generowanym zawsze przez urządzenie nadające ramkę. Odbiornik informacji wyznacza własne CRC na podstawie zawartości odebranej ramki i porównuje ją z wartością odebranej CRC. Błąd zostaje wykryty, gdy obie wartości nie są identyczne.

Procedura wyznaczania CRC jest następująca:

1. Załaduj do 16-bitowego rejestru CRC liczbę 0xFFFF.
2. Wykonaj operację XOR młodszego bajtu rejestru CRC z pierwszym bajtem ramki.



3. Przesuń rejestr CRC o jeden bit w prawo i wstaw 0 na miejsce najbardziej znaczącego bitu (MSB).
4. Jeśli najmniej znaczący bit (LSB) jest równy 0 – to należy wykonać powtórnie czynność z p. Jeśli LSB jest równy 1, to należy wykonać operację XOR rejestrów CRC z wartością A001_h.
5. Czynności z punktów 3 i 4 powtórzyć aż do osiągnięcia 8 przesunięć.
6. Powtórzyć czynności z punktów od 2 do 5 dla wszystkich kolejnych bajtów ramki.
7. Dołączyć do wysyłanej ramki CRC zamieniając miejscami bajty (młodszy bajt jest wysyłany jako pierwszy).

Funkcja generująca CRC może wyglądać następująco:

```
unsigned short CRC(unsigned char *pMessage, unsigned int NumberOfBytes)
{
    register unsigned short reg16 = 0xFFFF;
    unsigned char reg8;
    unsigned char i;

    while (NumberOfBytes--)
    {
        reg16 ^= *pMessage++;
        i = 8;
        while(i--)
        {
            if (reg16 & 0x0001)
            {
                reg16 >>= 1;
                reg16 ^= 0xA001;
            }
            else
                reg16 >>= 1;
        }
        reg8 = reg16 >> 8;
        return (reg16 << 8 | reg8);
    }
}
```

Powyższy algorytm okazuje się często zbyt wolny w rzeczywistych zastosowaniach. Dlatego też wykorzystywana jest tablicowa metoda generacji CRC. Wartość CRC wyznacza się z dwóch tablic, w których znajdują się wszystkie możliwe starsze i młodsze bajty CRC.

```
unsigned short CRC(unsigned char *pMessage, unsigned int NumberOfBytes)
{
    static unsigned char aCRCHi[] =
    {
        0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81,
        0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0,
        0x80, 0x41, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01,
        0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x01, 0xc0, 0x80, 0x41,
        0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81,
```



```

0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x01, 0xc0,
0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x01,
0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40,
0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81,
0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0,
0x80, 0x41, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01,
0xc0, 0x80, 0x41, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41,
0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81,
0x40, 0x01, 0xc0, 0x80, 0x41, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0,
0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x01,
0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41,
0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80,
0x41, 0x00, 0xc1, 0x81, 0x40, 0x00, 0xc1, 0x81, 0x40, 0x01, 0xc0, 0x80, 0x41, 0x00, 0xc1,
0x40
};

static unsigned char aCRCLo[] =
{
0x00, 0xc0, 0xc1, 0x01, 0xc3, 0x03, 0x02, 0xc2, 0xc6, 0x06, 0x07, 0xc7, 0x05, 0xc5, 0xc4,
0x04, 0xcc, 0x0c, 0x0d, 0xcd, 0x0f, 0xcf, 0xce, 0x0e, 0x0a, 0xca, 0xcb, 0x0b, 0xc9, 0x09,
0x08, 0xc8, 0xd8, 0x18, 0x19, 0xd9, 0x1b, 0xdb, 0xda, 0x1a, 0x1e, 0xde, 0xdf, 0x1f, 0xdd,
0x1d, 0x1c, 0xdc, 0x14, 0xd4, 0xd5, 0x15, 0xd7, 0x17, 0x16, 0xd6, 0xd2, 0x12, 0x13, 0xd3,
0x11, 0xd1, 0xd0, 0x10, 0xf0, 0x30, 0x31, 0xf1, 0x33, 0xf3, 0xf2, 0x32, 0x36, 0xf6, 0xf7,
0x37, 0xf5, 0x35, 0x34, 0xf4, 0x3c, 0xfc, 0xfd, 0x3d, 0xff, 0x3f, 0x3e, 0xfe, 0xfa, 0x3a,
0x3b, 0xfb, 0x39, 0xf9, 0xf8, 0x38, 0x28, 0xe8, 0xe9, 0x29, 0xeb, 0x2b, 0x2a, 0xea, 0xee,
0x2e, 0x2f, 0xef, 0x2d, 0xed, 0xec, 0x2c, 0xe4, 0x24, 0x25, 0xe5, 0x27, 0xe7, 0xe6, 0x26,
0x22, 0xe2, 0xe3, 0x23, 0xe1, 0x21, 0x20, 0xe0, 0xa0, 0x60, 0x61, 0xa1, 0x63, 0xa3, 0xa2,
0x62, 0x66, 0xa6, 0xa7, 0x67, 0xa5, 0x65, 0x64, 0xa4, 0x6c, 0xac, 0xad, 0x6d, 0xaf, 0x6f,
0x6e, 0xae, 0xaa, 0x6a, 0x6b, 0xab, 0x69, 0xa9, 0xa8, 0x68, 0x78, 0xb8, 0xb9, 0x79, 0xbb,
0x7b, 0x7a, 0xba, 0xbe, 0x7e, 0x7f, 0xbf, 0x7d, 0xbd, 0xbc, 0x7c, 0xb4, 0x74, 0x75, 0xb5,
0x77, 0xb7, 0xb6, 0x76, 0x72, 0xb2, 0xb3, 0x73, 0xb1, 0x71, 0x70, 0xb0, 0x50, 0x90, 0x91,
0x51, 0x93, 0x53, 0x52, 0x92, 0x96, 0x56, 0x57, 0x97, 0x55, 0x95, 0x94, 0x54, 0x9c, 0x5c,
0x5d, 0x9d, 0x5f, 0x9f, 0x9e, 0x5e, 0x5a, 0x9a, 0x9b, 0x5b, 0x99, 0x59, 0x58, 0x98, 0x88,
0x48, 0x49, 0x89, 0x4b, 0x8b, 0x8a, 0x4a, 0x4e, 0x8e, 0x8f, 0x4f, 0x8d, 0x4d, 0x4c, 0x8c,
0x44, 0x84, 0x85, 0x45, 0x87, 0x47, 0x46, 0x86, 0x82, 0x42, 0x43, 0x83, 0x41, 0x81, 0x80,
0x40
};

unsigned char HiByte = 0xFF;
unsigned char LoByte = 0xFF;
unsigned char Index;
while (NumberOfBytes--)
{
    Index = HiByte ^ *pMessage++;
    HiByte = LoByte ^ aCRCHi[Index];
    LoByte = aCRCLo[Index];
}
return (HiByte << 8 | LoByte);
}

```

7.5. ODPOMIEDZI WYJĄTKOWE

Po wysłaniu zapytania, jednostka nadziedna oczekuje odpowiedzi ze strony zaadresowanej jednostki podporządkowanej. Odpowiedzi nie są udzielane przez jednostki podporządkowane w przypadku



wysłania przez jednostkę nadziedną wiadomości typu broadcast. Istnieją cztery typy sytuacji, które mogą wystąpić po wysłaniu wiadomości przez urządzenie nadziedne:

- ❑ Jeśli urządzenie podporządkowane odbierze wiadomość bez błędów transmisji i będzie w stanie przeprowadzić zażądane działania to wygeneruje odpowiedź standardową.
- ❑ Jeśli urządzenie podporządkowane nie odbierze wiadomości z powodu błędów w komunikacji, to nie zostanie wygenerowana żadna odpowiedź.
- ❑ Jeśli urządzenie podporządkowane odbierze wiadomość, ale wykryje w niej błędy (przez kontrolę parzystości, LRC lub CRC) to nie zostanie wygenerowana żadna odpowiedź.
- ❑ Jeśli urządzenie podporządkowane odbierze wiadomość bez błędów w transmisji, ale nie będzie w stanie zrealizować funkcji (np. odczytu nieistniejącego rejestru), to zwróci odpowiedź wyjątkową, informującą o rodzaju błędu.

Odpowiedź wyjątkowa posiada dwa pola, odróżniające ją od odpowiedzi standardowej.

Kod funkcji: W przypadku odpowiedzi standardowej, jednostka podziedna wysyła taki sam kod funkcji, jaki odebrała w rozkazie. Wszystkie standardowe kody funkcji mają zerowy najbardziej znaczący bit (MSB). W odpowiedzi wyjątkowej, jednostka podziedna ustawia 1 w miejscu MSB kodu funkcji, co pozwala urządzeniu nadziednemu na łatwe rozpoznanie odpowiedzi wyjątkowej i interpretację kodu wyjątku (w polu danych).

Pole danych: W przypadku odpowiedzi standardowej w polu danych znajdują się dane żądane przez jednostkę nadziedną. W odpowiedzi wyjątkowej, jednostka podziedna wykorzystuje to pole do przesłania kodu wyjątku, określającego rodzaj błędu.

| ADRES | KOD FUNKCJI | DANE | CRC lub LRC |
|-------|--------------------------------|-------------|-------------|
| | Normalny kod + 80 _h | Kod wyjątku | |

Rys. 7.13. Ramka odpowiedzi wyjątkowej

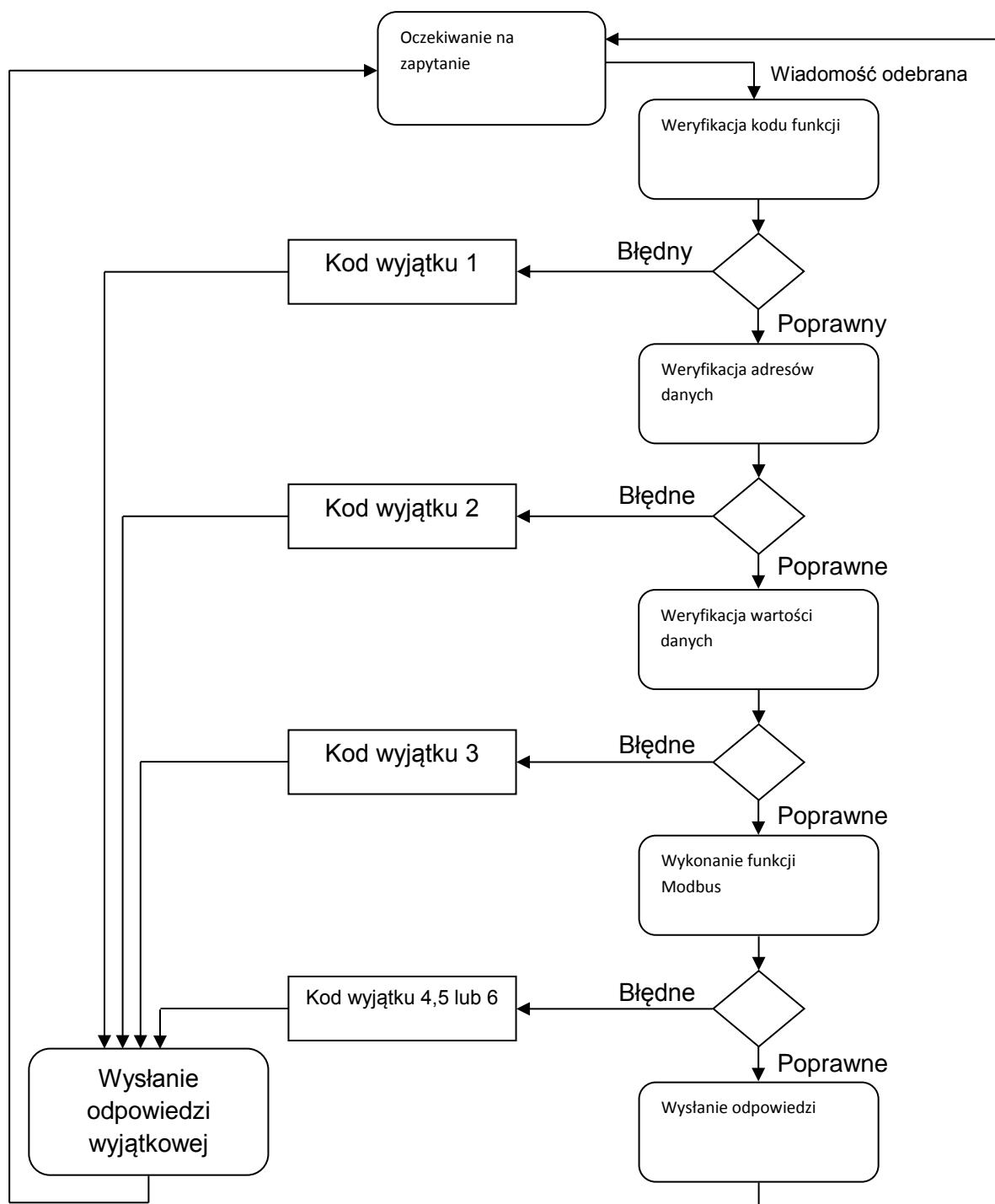
| Kod | Nazwa | Opis |
|-----|-----------------------------|--|
| 01 | Niedozwolona funkcja | Kod funkcji odebrany w zapytaniu nie jest obsługiwany przez jednostkę podziedną. |
| 02 | Niedozwolony adres danych | Próba odczytu lub zapisu nieistniejącego rejestru lub pola bitowego. |
| 03 | Niedozwolona wartość danych | Próba wpisania do rejestru lub pola bitowego niewłaściwej wartości. |
| 04 | Niepowodzenie | Wystąpienie nieokreślonego błędu podczas próby wykonania operacji. |
| 05 | Potwierdzenie | Potwierdzenie przyjęcia i rozpoczęcia realizacji funkcji. Proces wymagać jednak będzie długiego czasu. |
| 06 | Jednostka podziedna zajęta | Jednostka podziedna jest zajęta wykonywaniem czasochłonnej funkcji. Zapytanie powinno zostać wysłane ponownie później. |
| 08 | Błąd parzystości pamięci | Błąd parzystości pamięci przy próbie odczytu. |

Rys. 7.14. Kody wyjątków (dla sieci standardowych):



7.6. SCHEMAT REALIZACJI TRANSAKCJI SIECIOWEJ PRZEZ JEDNOSTKĘ PODRZĘDΝĄ

Schemat na rys. 7.15 przedstawia sposób realizacji transakcji sieciowej przez jednostkę podrzedną. Schemat dotyczy wyłącznie przypadków, gdy nie zostały wykryte błędy transmisji. W przypadku wystąpienia błędów transmisji, urządzenie podporządkowane nie udziela żadnej odpowiedzi.



Rys. 7.15. Sposób realizacji transakcji sieciowej przez jednostkę podrzedną

7.7. WYMAGANIA CZASOWE

Komunikacja zgodna ze specyfikacją Modbus podlega rygorom terminowości. Analizując przebieg procesów komunikacyjnych zachodzących pomiędzy rzeczywistymi urządzeniami należy zwrócić uwagę na:

- skończony i zdeterminowany czas transmisji ramki przez jednostkę nadzorowaną i czas odbioru ramki przez jednostkę podrzijną,
- okresy czasu konieczne dla właściwego przebiegu transmisji kolejnych ramek wiadomości,
- czas przeterminowania transakcji. Jednostka nadzorowana oczekuje na odpowiedź urządzenia podporządkowanego tylko i wyłącznie przez ścisłe określony czas.

Czas przesłania pojedynczego znaku ramki można obliczyć następująco:

$$t_{byte} = \frac{1000 \cdot BPC}{BR} [ms]$$

gdzie:

BPC – liczba bitów znaku

BR – prędkość transmisji w [b/s].

Czas transmisji całej ramki Modbus (wraz z okresem koniecznej przerwy):

$$t_{frame} = (n + 4) \cdot t_{byte} = \frac{1000 \cdot (n + 4) \cdot BPC}{BR} [ms]$$

gdzie:

n – liczba znaków ramki Modbus.

Czas przeterminowania transakcji (*timeout*) to maksymalny czas, w którym jednostka nadzorowana oczekuje na rozpoczęcie odpowiedzi przez jednostkę podrzijną. Czas jaki upływa od momentu zakończenia ramki rozkazowej do momentu rozpoczęcia wysyłania ramki odpowiedzi zależy od rodzaju i konstrukcji urządzenia podporządkowanego. Zależy również od kontekstu ramki rozkazowej (rodzaju funkcji i liczby danych, które mają być przesłane).

7.8. PRZYKŁADY TYPOWYCH FUNKCJI MODBUS

Zestaw i rodzaj realizowanych funkcji zależy od typu urządzenia sieciowego. Do standardowych rozkazów Modbus należą:

- 01 Read Coil Status
- 02 Read Input Status
- 03 Read Holding Registers
- 04 Read Input Registers
- 05 Force Single Coil
- 06 Preset Single Register
- 07 Read Exception Status
- 11 Fetch Comm Event Ctr
- 12 Fetch Comm Event Log
- 15 Force Multiple Coils
- 16 Preset Multiple Regs
- 17 Report Slave ID
- 20 Read General Reference



- 21 Write General Reference
- 22 Mask Write 4X Register
- 23 Read/Write 4X Registers
- 24 Read FIFO Queue

7.8.1. ODCZYT POLA BITOWEGO - 01 READ COIL STATUS

Funkcja służy do odczytu stanu binarnego pól bitowych (*coils – discrete outputs*) jednostki podrzędnej. Funkcja ta nie jest możliwa w trybie rozgłoszeniowym (*tryb broadcast*).

Rozkaz

Przykład żądania odczytu pól bitowych 20..56 z urządzenia 17.

| Nazwa pola | Przykład (hex) |
|------------------------|----------------|
| Adres urządzenia | 11 |
| Funkcja | 01 |
| Adres startowy Hi | 00 |
| Adres startowy Lo | 13 |
| Liczba pól bitowych Hi | 00 |
| Liczba pól bitowych Lo | 25 |
| Kontrola (LRC lub CRC) | xx |

Odpowiedź

Stany binarne pól są upakowane w taki sposób, że najmniej znaczący bit pierwszego bajtu zawiera stan binarny pola o adresie startowym podanym w zapytaniu.

Jeśli liczba pól nie jest wielokrotnością ośmiu, to pozostałe bity w ostatnim bajcie zostaną wypełnione zerami.

| Nazwa pola | Przykład (hex) |
|------------------------|----------------|
| Adres urządzenia | 11 |
| Funkcja | 01 |
| Liczba bajtów | 05 |
| Dane (Coils 27-20) | CD |
| Dane (Coils 35-28) | 6B |
| Dane (Coils 43-36) | B2 |
| Dane (Coils 51-44) | 0E |
| Dane (Coils 56-52) | 1B |
| Kontrola (LRC lub CRC) | xx |

Stan pól 27-20 określony jest w pierwszym bajcie danych (CD_h lub 11001101_b). Stan logiczny pola 27 reprezentuje najbardziej znaczący bit.

7.8.2. ODCZYT REJESTRU – 03 READ HOLDING REGISTERS

Funkcja służy do odczytu zawartości rejestrów (*holding registers*) jednostki podporządkowanej. Funkcja ta nie jest możliwa w trybie rozgłoszeniowym (*tryb broadcast*).

Rozkaz

Przykład żądania odczytu rejestrów 40108..40110 z urządzenia 17.

| Nazwa pola | Przykład (hex) |
|------------------------|----------------|
| Adres urządzenia | 11 |
| Funkcja | 03 |
| Adres startowy Hi | 00 |
| Adres startowy Lo | 6B |
| Liczba rejestrów Hi | 00 |
| Liczba rejestrów Lo | 03 |
| Kontrola (LRC lub CRC) | xx |

Odpowiedź

Zawartość każdego rejestru jest reprezentowana w odpowiedzi w postaci dwóch znaków.

| Nazwa pola | Przykład (hex) |
|-------------------------|----------------|
| Adres urządzenia | 11 |
| Funkcja | 03 |
| Liczba bajtów | 06 |
| Dane Hi (rejestr 40108) | 02 |
| Dane Lo (rejestr 40108) | 2B |
| Dane Hi (rejestr 40109) | 00 |
| Dane Lo (rejestr 40109) | 00 |
| Dane Hi (rejestr 40110) | 00 |
| Dane Lo (rejestr 40110) | 64 |
| Kontrola (LRC lub CRC) | xx |

7.8.3. ZAPIS DO REJESTRÓW - 16 PRESET MULTIPLE REGS

Funkcja dokonuje zapisu grupy rejestrów (*holding registers*). W trybie *broadcast* następuje zapisanie rejestrów o tym samym adresie we wszystkich urządzeniach.

Rozkaz

Przykład wpisania do rejestrów 40002 i 40003 kolejno wartości $000A_h$ i 0102_h .

| Nazwa pola | Przykład (hex) |
|------------------------|----------------|
| Adres urządzenia | 11 |
| Funkcja | 10 |
| Adres startowy Hi | 00 |
| Adres startowy Lo | 01 |
| Liczba rejestrów Hi | 00 |
| Liczba rejestrów Lo | 02 |
| Liczba bajtów | 04 |
| Dane Hi | 00 |
| Dane Lo | 0A |
| Dane Hi | 01 |
| Dane Lo | 02 |
| Kontrola (LRC lub CRC) | xx |

Odpowiedź

Standardowa odpowiedź zawiera: adres urządzenia, kod funkcji, adres początkowy oraz liczbę rejestrów.

| Nazwa pola | Przykład (hex) |
|------------------------|----------------|
| Adres urządzenia | 11 |
| Funkcja | 10 |
| Adres startowy Hi | 00 |
| Adres startowy Lo | 01 |
| Liczba rejestrów Hi | 00 |
| Liczba rejestrów Lo | 02 |
| Kontrola (LRC lub CRC) | xx |

7.9. PODSUMOWANIE

Implementacja protokołu Modbus pozwala na tworzenie sieci deterministycznych i scentralizowanych. Pomimo pewnych niewątpliwych zalet, rozwiązanie to posiada też szereg ograniczeń. Ograniczenia te wynikają zarówno z konstrukcji samego protokołu, jak i z właściwości warstwy fizycznej.

Do zalet protokołu Modbus należą:

- otwartość i dostępność specyfikacji protokołu Modbus,
- prostota i łatwość implementacji,
- niska cena realizacji warstwy fizycznej
- elastyczność – właściwie brak jest ograniczeń, co do typu urządzeń, które mogą wykorzystywać protokół. Istnieje możliwość tworzenia własnych funkcji.
- silne zabezpieczenie przed błędami transmisji przez zastosowanie mechanizmów kontroli parzystości i sum kontrolnych,
- wbudowany algorytm powiadamiania o sytuacjach wyjątkowych,
- determinizm osiągany dzięki wyeliminowaniu możliwości wystąpienia kolizji sieciowych,

- łatwa modyfikacja sieci – sieć oparta na strukturze magistrali pozwala na łatwe dodawanie i usuwanie kolejnych jednostek.

Do wad protokołu Modbus należą:

- ograniczona liczba urządzeń,
- ograniczona prędkość transmisji,
- ograniczony rozmiar pola danych
- brak możliwości komunikacji pomiędzy jednostkami podporządkowanymi
- brak możliwości generowania ramek rozkazowych przez urządzenia podporządkowane.

8. SIEĆ AS-I

8.1. RYS HISTORYCZNY

Sieć AS-i (ang. *Actuator Sensor Interface*) jest międzynarodowym otwartym² standardem komunikacyjnym przeznaczonym głównie do stosowania w zadaniach automatyzacji przemysłowych procesów dyskretnych³ [5]. Sieć AS-i została opracowana na początku lat dziewięćdziesiątych ubiegłego wieku i wprowadzona do praktyki przemysłowej w 1994 roku. Sieć ta została zaprojektowana głównie dla realizacji zadań sterowania binarnego w warstwie obiektowej procesu⁴. W trakcie opracowania założeń technicznych sieci przyjęto, na wzór rozwiązań spotykanych w projektach programistycznych, że sieć będzie charakteryzowała się wysokim stopniem „przyjazności” w stosunku do użytkownika. O stopniu realizacji tej cechy świadczy rosnąca w dużym tempie liczba zastosowań tej sieci zwłaszcza w zautomatyzowanych procesach montażu, pakowania i dystrybucji. Sieć AS-i jest rozwijana przez międzynarodową organizację AS International Association.

8.2. SIEĆ AS-I A MODEL ODNIESIENIA ISO/OSI

Sieć AS-i, podobnie jak sieć MODBUS, jest typową siecią o modelu komunikacyjnym typu master-slave. Sieć AS-i jest siecią typu monomaster, co oznacza, że w sieci dopuszczalna jest jedna i tylko jedna jednostka nadzędna. Jednostka nadzędna komunikuje się z urządzeniami podrzędnymi w trybie tzw. odpytywania (ang. *polling*). Prawo do odpytywania jednostek podporządkowanych przysługuje tylko i wyłącznie jednostce nadzędnej. Odpytanie odbywa się w pewnym, stale powtarzanym cyklu (p. 3.4) trwającym 5ms dla specyfikacji 2.0 i 10ms dla specyfikacji 2.11. Liczba jednostek podporządkowanych w sieci jest ograniczona i uzależniona od numeru specyfikacji sieci. W sieci o specyfikacji 2.0 maksymalna liczba urządzeń podporządkowanych wynosi 31, natomiast maksymalna liczba urządzeń podporządkowanych w sieci o specyfikacji 2.11 wynosi 62. Urządzenia podporządkowane w sensie informacyjnym są pasywne. Oznacza to, że nie mają prawa samodzielnego inicjowania jakichkolwiek transakcji komunikacyjnych. Niemożliwa jest również jakakolwiek bezpośrednia wymiana informacji pomiędzy jednostkami podporządkowanymi. Każda z jednostek podporządkowanych ma swój własny unikalny adres sieciowy. Adres ten pozwala na jednoznaczne rozróżnienie przez jednostkę nadzędną wszystkich dołączonych do sieci urządzeń podporządkowanych. Adresy urządzeń są liczbami całkowitymi o wartościach z zakresu 1..31 w specyfikacji 2.0 i 1..31 oraz 33..62 w specyfikacji 2.11. Adres 0 jest adresem zarezerwowanym i jest nadawany urządzeniom AS-i w procesie ich wytwarzania. Adres ten należy traktować jako zarezerwowany adres tymczasowy. Adres ten zostanie zmodyfikowany bezpośrednio po dołączeniu urządzenia do

² Pod pojęciem otwartego standardu komunikacyjnego rozumiany jest taki standard, którego specyfikacja jest ogólnie dostępna w domenie publicznej.

³ Przemysłowy proces dyskretny dotyczy procesu, w którym można wyróżnić skończoną liczbę zdarzeń i stanów.

⁴ Warstwa obiektowa procesu złożona jest z: urządzeń pomiarowych (sensorów), elementów wykonawczych (aktuatorów) i instalacji technologicznej (komponentów technologicznych).

sieci. Adres tymczasowy wykorzystywany jest w procesie automatycznego rozpoznawania nowych urządzeń sieciowych przez jednostkę nadzorującą. Lista adresów wszystkich urządzeń sieciowych jest przechowywana w pamięci jednostki nadzorującej w postaci list adresowych urządzeń. Jednostka ta prowadzi dwie listy adresowe. Pierwsza lista jest tzw. listą konfiguracyjną i zawiera adresy wszystkich urządzeń, które powinny być dołączone do sieci. Lista ta przechowywana jest w sposób trwały w pamięci nieulotnej jednostki nadzorującej. Druga lista jest listą dynamiczną i zawiera adresy urządzeń, które są oczywiście dołączone do sieci. Na podstawie oceny stanu i rodzaju rozbieżności obu list, jednostka nadzorująca podejmuje odpowiednie decyzje. Pozwalają one miedzy innymi na: wykrycie dołączenia nowego urządzenia podporządkowanego do sieci, wykrycie uszkodzeń urządzeń sieciowych, realizację funkcji automatycznego adresowania nowych urządzeń sieciowych itp.

Komunikacja pomiędzy stacjami oraz definicja zasad transmisji i interfejs w sieci AS-i opisany jest za pomocą warstwowego modelu referencyjnego ISO/OSI⁵. Model ISO/OSI definiuje elementy, strukturę i zadania związane z komunikacją (rys.3.1). W modelu ISO/OSI zostało wyróżnionych siedem warstw. Mają one charakter opcjonalny. Charakterystyczną cechą większości sieci polowych (sieci typu fieldbus), do których zalicza się sieć AS-i, jest to, że nie definiują warstw: sieciowej, transportowej, sesyjnej i prezentacyjnej.

| Nadajnik | Odbiornik | Opis i zastosowanie danej warstwy | |
|----------------------|-----------|-----------------------------------|--|
| 7 | 7 | Warstwa aplikacji | Warstwa usługowa. Definiuje interfejs dostępu do sieci przez programy aplikacyjne. |
| 6 | 6 | Warstwa prezentacji | Definiuje struktury i sposoby kodowania danych. |
| 5 | 5 | Warstwa sesyjna | Opisuje metody tworzenia oraz anulowania sesji komunikacyjnych. Odpowiada za synchronizację procesu komunikacji. |
| 4 | 4 | Warstwa transportowa | Opisuje metody przygotowania logicznych kanałów komunikacyjnych w tym kontroli przesyłanych informacji. |
| 3 | 3 | Warstwa sieciowa | Definiuje procesy nawiązania oraz anulowania połączenia sieciowego, określa sposoby rozwiązywania konfliktów w sieci. |
| 2 | 2 | Warstwa danych | Opisuje protokół dostępu do warstwy fizycznej (Medium Access Control, MAC) oraz definiuje ramkę komunikacyjną i sposób zabezpieczenia przesyłanych informacji. |
| 1 | 1 | Warstwa fizyczna | Definiuje medium komunikacyjne, sposób kodowania informacji, określa prędkość transmisji informacji. |
| Medium komunikacyjne | | | |

Rys.8.1. Komunikacyjny model odniesienia ISO/OSI

⁵ Open System Interconnection Reference Model - model komunikacyjny zdefiniowany przez Międzynarodową Organizację Standardyzacji (International Standard Organisation) w 1983 roku

Sieć komunikacyjna AS-i wykorzystuje jedynie warstwę fizyczną, warstwę danych i warstwę aplikacyjną. Implementacja tych warstw w sieci AS-i została przedstawiona na rys. 8.2.

| Warstwa | Implementacja w sieci AS-i |
|-------------------------|---|
| Warstwa 7: aplikacyjna | Komunikaty, cykle, profile, adresowanie automatyczne |
| Warstwa 6: prezentacji | |
| Warstwa 5: sesyjna | |
| Warstwa 4: transportowa | |
| Warstwa 3: sieciowa | |
| Warstwa 2: danych | Ramka danych, bit startu, bit stopu, zabezpieczenie, przetwarzanie błędów |
| Warstwa 1: fizyczna | Kable, zasilanie, odpręganie danych, modulacja PE, APM |

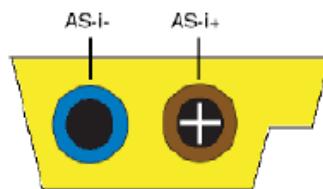
Rys.8.2. Implementacja modelu warstwowego ISO/OSI w sieci AS-i

8.3. WARSTWA FIZYCZNA SIECI AS-I

Warstwa fizyczna definiuje wymagania techniczne dotyczące parametrów medium transmisyjnego, metody kodowania informacji oraz zasilania sieci.

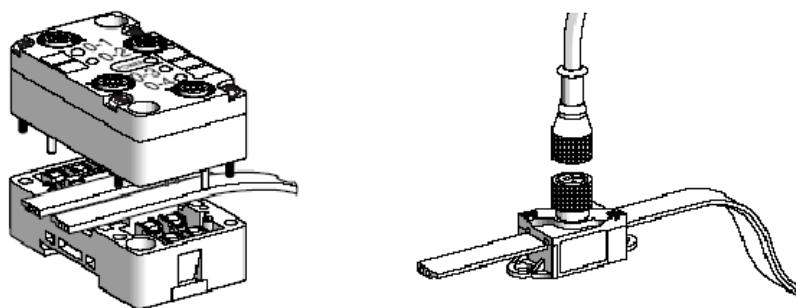
8.3.1. MEDIUM TRANSMISYJNE

W sieci AS-i wykorzystywane jest kablowe łącze transmisyjne. Kabel komunikacyjny AS-i jest wykonany w postaci specjalnego profilowanego dwużyłowego nieekranowanego kabla o przekroju żył $2 \times 1,5\text{mm}^2$ (rys. 8.3).



Rys.8.3. Przekrój kabla AS-i.

Kabel AS-i łączy wszystkie urządzenia sieciowe. Proces realizacji fizycznych połączeń pomiędzy urządzeniami sieciowymi został w sieci AS-i zaprojektowany w taki sposób, aby zapewnić możliwość bardzo szybkiej realizacji dołączenia lub odłączenia poszczególnych urządzeń. W tym celu urządzenia sieciowe zazwyczaj mają specjalną konstrukcję mechaniczną obudowy (rys. 8.4). Obudowa jest dzielona na dwie części: górną i dolną. Zazwyczaj w dolnej części obudowy znajdują się profilowane prowadnice umożliwiające ułożenie kabla AS-i. Specjalny kształt kabla i prowadnic wyklucza jego błędne ułożenie. Górną część obudowy zawiera dwa ostrza

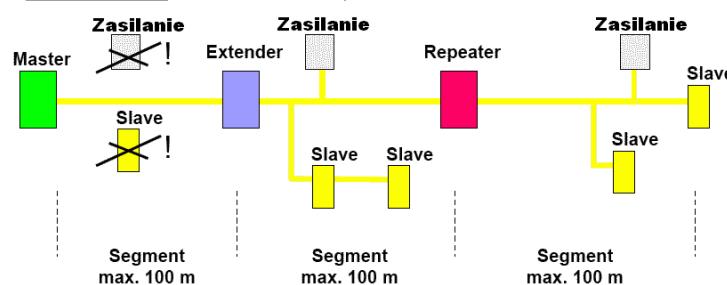


Rys.8.4. Sposób dołączania urządzeń sieciowych do kabla AS-i.

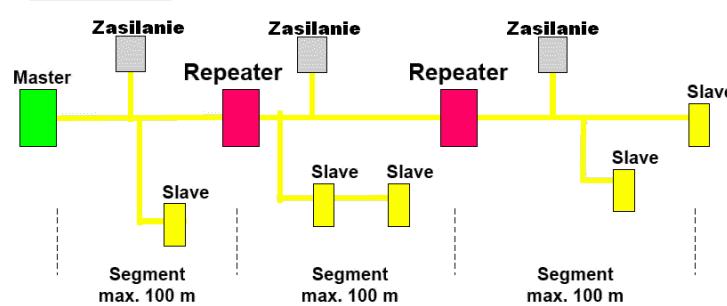
kontaktowe. W czasie skręcania obu części obudowy styki te przecinają izolację kabla i dokonują połączeń elektrycznych z żyłami kabla. Izolacja kabla jest wykonana z materiału zapewniającego szczelność tak wykonanego połączenia na akceptowanym w warunkach przemysłowych poziomie IP65. Przecięcie izolacji kabla w trakcie montażu urządzenia sieciowego nie oznacza jego definitivego zniszczenia. Po demontażu urządzenia sieciowego nadcięcie izolacji kabla ulega samoregeneracji. W ten sposób możliwe jest wykonywanie wielokrotnych dołączeń urządzeń sieciowych w tym samym miejscu tego samego kabla, co jest istotne zwłaszcza w przypadku konieczności dokonania wymiany uszkodzonego urządzenia.

Ponieważ kabel jest nieekranowany oraz prowadzony w postaci równoległej pary przewodów, to jego odporność na zakłócenia elektromagnetyczne nie jest wysoka. Z tego między innymi powodu ograniczona jest łączna długość użytego przewodu do realizacji sieci. Maksymalna długość kabla sieciowego wynosi 100m. W niektórych przypadkach, przy zastosowaniu wzmacniaczy (ang. repeater) oraz przedłużaczy (ang. extender) możliwe jest wydłużenie sieci do 300m (rys. 8.5).

Rozwiązanie 1: 1 extender + 1 repeater



Rozwiązanie 2: 2 x repeater



Rys.8.5. Możliwości rozszerzenia zasięgu sieci AS-i

Topologia połączeń sieciowych jest dowolna. Możliwa jest topologia magistrali, gwiazdy, drzewa, pierścienia, siatki lub topologie mieszane. Daje to wyjątkową wygodę w projektowaniu i realizacji sieci. Ze względu na ograniczenie długości maksymalnej kabla w sieci AS-i nie występuje konieczność stosowania tzw. terminatorów. Terminatorzy są specjalnymi urządzeniami dołączanymi na końcach sieci, których głównym zadaniem jest efektywne tłumienie zjawisk odbiciowych w sieci. Terminatorzy są najczęściej realizowane w postaci dwójników pasywnych o odpowiednio dobranej impedancji. Terminatorzy stosowane są między innymi w sieciach: MODBUS, CAN, PROFIBUS PA, FOUNDATION FIELDBUS H1.

8.3.2. UKŁAD ZASILANIA

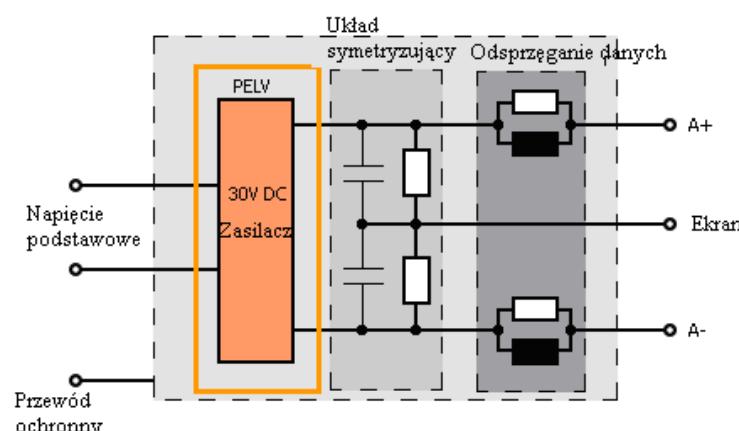
Kabel AS-i służy do jednoczesnego przesyłania informacji i zasilania urządzeń sieciowych. Z tego względu specyfikacja sieci AS-i w warstwie fizycznej definiuje także wymagania na układ zasilania. Zgodnie ze specyfikacją, napięcie na zaciskach zasilacza AS-i wynosi 29,5..31,6V. Napięcie to jest zgodne z odpowiednimi standardami zasilania niskonapięciowego (IEC64, DIN VDE 0100-410, DIN VDE 0106-101, IEC 60364-4-41). Zazwyczaj napięcie znamionowe zasilacza AS-i wynosi 30V, a jego obciążalność znamionowa wynosi 2,4A. W wyniku przepływu prądu przez sieć i skończonej rezystancji kabla AS-i, napięcie na zaciskach urządzeń sieciowych różni się od napięcia na zaciskach zasilacza. Zakłada się, że napięcie na zaciskach urządzeń nie powinno być niższe niż 20V. W przypadku, gdy obciążenie zasilacza przez urządzenia sieciowe jest na tyle duże, że powyższy warunek nie może być dochowany, to stosowane są zasilacze AS-i z dodatkowym wyjściem mocy. To dodatkowe wyjście służy wyłącznie do zasilania stopni końcowych urządzeń sieciowych o dużym poborze mocy (zwykle są to urządzenia wykonawcze). Wyjście to nie służy do przesyłania informacji. Dodatkowe wyjście zasilacza łączone jest z urządzeniami sieciowymi w podobny sposób jak kabel AS-i (rys. 3.4). Zewnętrznie kabel zasilający różni się od kabla AS-i kolorem. Kabel AS-i jest żółty, kabel zasilający jest czarny.

Uwagi:

- do jednego segmentu sieci AS-i może być dołączony tylko jeden zasilacz AS-i,
- użycie dodatkowego kabla zasilającego jest opcjonalne,
- zasilanie sieci AS-i z zasilacza uniwersalnego jest niedopuszczalne.

Układ zasilania AS-i realizuje następujące zadania:

- zasilania sieci,
- separację sygnału AS-i ,
- symetryzację sygnału,
- odpręganie danych.



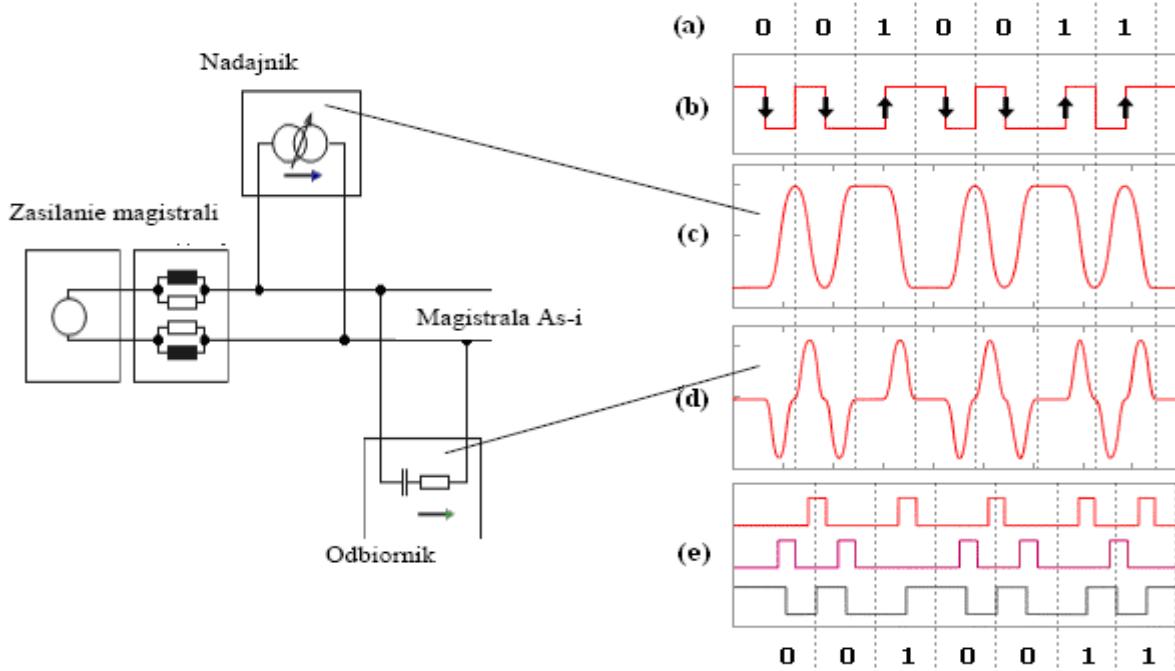
Rys.8.6. Schemat układu zasilania AS-i

Układ symetryzujący pozwala na uniknięcie potrzeby ekranowania kabla AS-i. Efekt tłumienia zakłóceń jest osiągany przez podłączenie końcówki ekranu (rys 8.6) do zacisku uziemienia.

Tak zwany układ odpręgania danych składa się z dwóch cewek o indukcyjności 50 μH każda połączonych równolegle z dwoma rezystorami o rezystancji 39 Ω każdy. W trakcie trwania komunikacji w sieci AS-i, nadajnik informacji generuje zmiany prądu. Zmiany prądu indukują odpowiednie zmiany napięcia w cewkach układów odpręgających wszystkich odbiorników. Na podstawie tych zmian odtwarzana jest w sieciowych urządzeniach odbiorczych binarna postać informacji przesyłanej przez nadajnik. W rzeczywistych sieciach AS-i zmiany prądu w czasie transmisji wahają się w granicach 55..68mA. Zmiany te indukują napięcia o wartości $\pm 2\text{V}$.

8.3.3. MODULACJA SYGNAŁU

W sieci AS-i transmisja informacji realizowana jest w paśmie podstawowym. Z uwagi na nienajlepsze właściwości transmisyjne naturalnego kodu binarnego (składowa stała, nieograniczona liczba występujących kolejno elementów „0” i „1”) stosowany jest specjalny sposób kodowania informacji. Do kodowania informacji stosowany jest kod PE (ang. *Phase Encoding*), nazywany też kodem Manchester. Kodowanie to polega na tym, że spadek poziomu sygnału koduje wartość logicznego „0”, a wzrost poziomu sygnału koduje wartość logicznej „1”. Zarówno spadki jak i wzrosty poziomów sygnału przypadają na środkowe części przedziału czasowego przeznaczonego na przesłanie jednego bitu. Zaletą takiego sposobu kodowania jest to, że przesłanie każdego bitu związane jest z co najmniej jedną zmianą poziomu sygnału. Ilustrację sposobu kodowania przedstawiono na rys. 8.7.



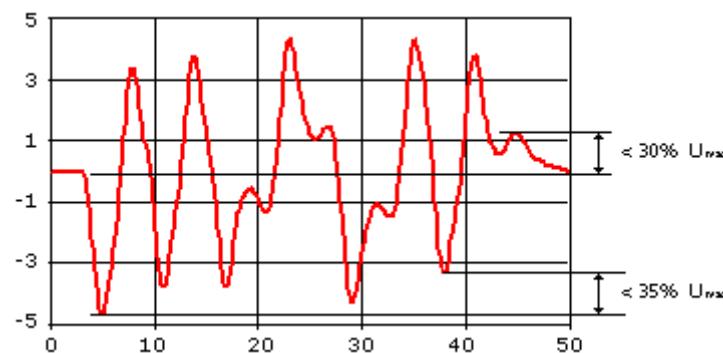
Rys.8.7. Sposób kodowania informacji w sieci AS-i.

- Sekwencja przesyłanych bitów w kodzie binarnym naturalnym
- Kodowanie typu Manchester
- Nadawany sygnał prądowy
- Napięcie na zaciskach odbiornika informacji
- Sekwencja bitów odebranych

Na początku informacja zakodowana w naturalnym kodzie binarnym (rys. 8.7 wykres a), kodowana jest zgodnie z regułami kodu PE (rys. 8.7, wykres b). Następnie uzyskany przebieg podawany na filtr dolnoprzepustowy i przekształcany do postaci sygnału prądowego w przetworniku napięciowo-prądowym (rys. 8.7, wykres c). Sygnał prądowy indukuje napięcie na elementach indukcyjnych w układzie odprzegającym zasilacza, co prowadzi do uzyskania naprzemiennej modulacji impulsowej APM (ang. **Alternate Pulse Modulation**) napięcia zasilającego (rys. 8.7, wykres d).

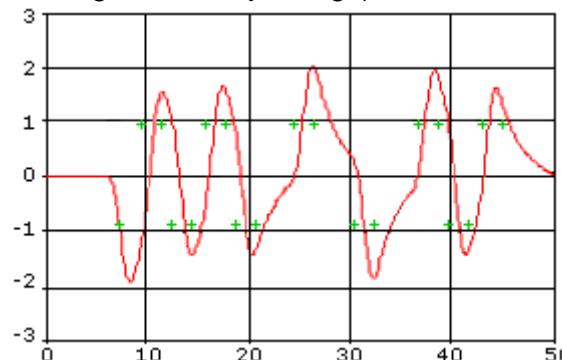
Dla modulacji APM zostały ustalone następujące ograniczenia:

- maksymalne dopuszczalne odchylenie amplitudy wynoszące 35% U_{max}
- dopuszczalne przepięcie wynoszące maksymalnie 30% amplitudy U_{max}



Rys.8.8. Ograniczenia modulacji APM w dziedzinie amplitudy

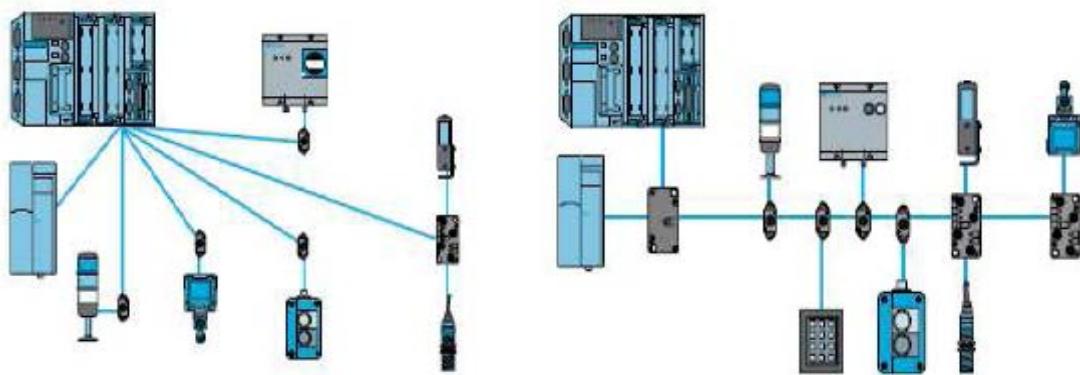
- dopuszczalne odchylenia czasowe zboczy impulsów wynoszące $(n + 3 \mu s) + 1/-0,5 \mu s$ (mierzone od pierwszego zbocza ujemnego).



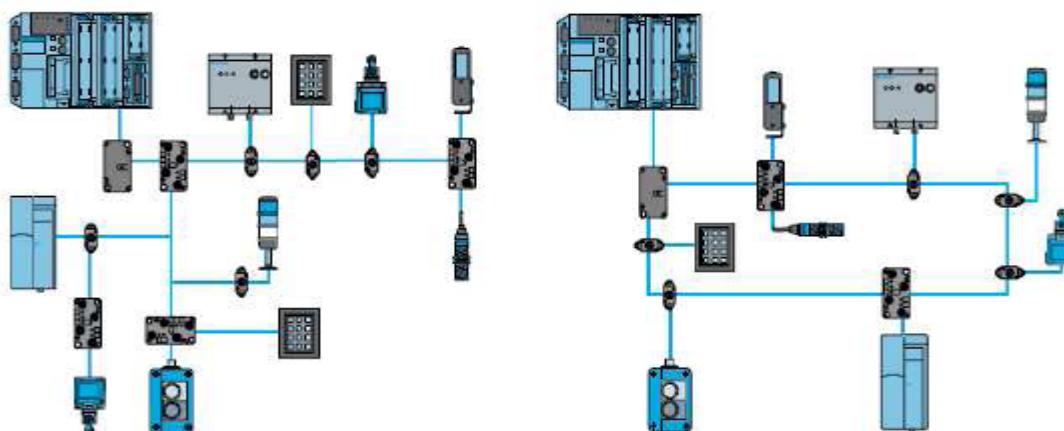
Rys.8.9. Ograniczenia modulacji APM w dziedzinie czasu

8.3.4. TOPOLOGIA SIECI

Sieć AS-i może mieć postać sieci o topologii liniowej (magistralowej), gwiazdzistej, drzewiastej, pierścieniowej lub typu punkt do punktu. Dopuszczalne są również topologie mieszane. Przykłady realizacji sieci o różnych topologiiach przedstawiono na rys. 8.10 i 8.11. Należy jednak pamiętać, że w przypadku konieczności dostarczenia do pojedynczego węzła sieci prądu o wartości przekraczającej 200 mA wymagane jest zainstalowanie dodatkowego kabla zasilającego (w kolorze czarnym).



Rys.8.10. Przykłady topologii sieci AS-i: z lewej strony- topologia punkt do punktu, z prawej strony- topologia magistrali.



Rys.3.11. Przykłady topologii sieci AS-i: z lewej strony- topologia drzewa, z prawej strony- topologia pierścienia.

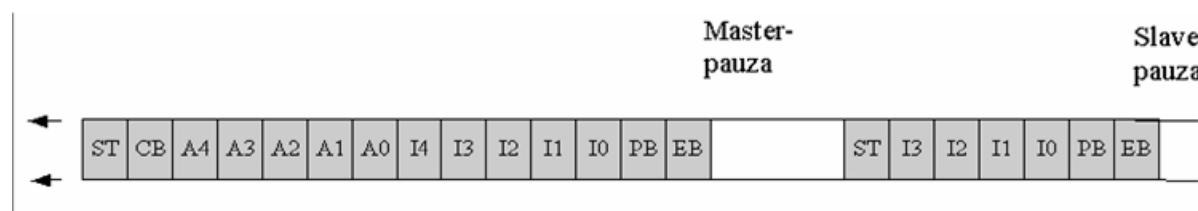
8.4. WARSTWA DANYCH SIECI AS-I

Jak już wspomniano wyżej, w sieci AS-i przyjęto model komunikacyjny typu master-slave. Wyłączne prawo inicjacji transferów informacji należy w sieci AS-i do jednostki nadzędnej. Jednostka nadzędna wysyła w sieć odpowiednio sformatowaną informację zwaną ramką lub telegramem. Informacja ta zawiera między nimi adres jednostki podporządkowanej, do której jest skierowana. Najczęściej informacja ta ma znaczenie rozkazu lub zapytania. Zaadresowane urządzenie podporządkowane interpretuje uzyskaną informację z jednostki nadzędnej, a następnie udziela odpowiedzi w postaci odpowiednio sformatowanej ramki informacyjnej. Cykl zapytanie-odpowiedź nazywany jest również transakcją.

8.4.1. FORMAT RAMKI

Ramka w sieci AS-i jest ramką bardzo małej długości, jeśli porówna się ją z długością ramek spotykanych w innych sieci komunikacyjnych np. z ramką sieci MODBUS czy PROFIBUS. Ramka ta ma ściśle zdefiniowaną strukturę. Składa się z szeregu pól o długości

od jednego do kilku bitów. Format ramki jest zależny od tego czy jest to ramka generowana przez urządzenie nadzędne czy przez urządzenie podrzędne. W pierwszym przypadku ramka liczy 14 bitów, w drugim przypadku ramka liczy 7 bitów. Po zakończeniu przesyłania każdej ramki dodawane są dodatkowe przerwy zwane pauzami. Pauza po wysłaniu ramki przez jednostkę nadziedną jest równa czasowi trwania transmisji od 3 bitów do 10 bitów informacji (18..60μs), natomiast pauza po wysłaniu ramki przez jednostkę podporządkowaną jest równa czasowi trwania transmisji jednego bitu informacji (6μs). Łącznie, pojedyncza transakcja polega na wymianie 25..32 bitów i trwa od 150..192 μs. W czasie jednej transakcji przesyłane są zaledwie 4 bity danych. Zatem sprawność informacyjna pojedynczej transakcji jest niewielka i wynosi co najwyżej 16%. Format ramki informacyjnej w sieci AS-i jest przedstawiony na rysunku 8.12.

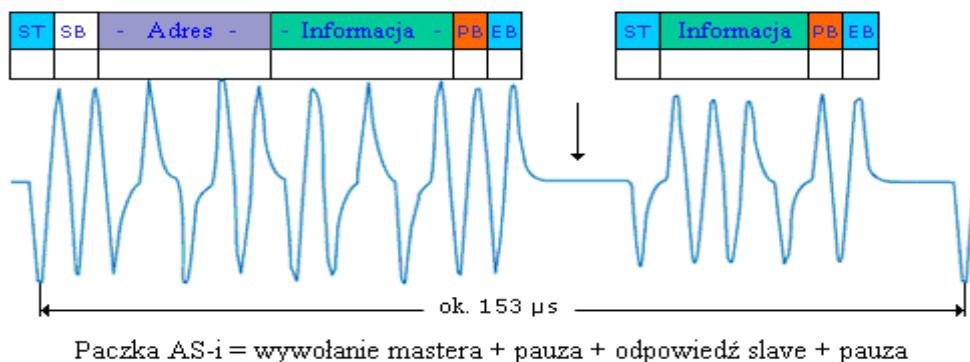


Rys.8.12. Format ramki informacyjnej w sieci AS-i.

Opis rysunku 8.12.:

- ST – bit startu, bit ST zawsze = 0,
- CB – bit sterujący, 0 - transmisja danych lub parametrów, 1 – instrukcja sterująca,
- A0...A4 – adres jednostki podporządkowanej, 01H...1FH
- I0...I4 – bity informacyjne interpretowane zależne od typu transakcji,
- PB – bit parzystości dotyczący całej ramki z wyłączeniem bitów ST i EB; wartość 0 określa parzystą liczbę w ramce '1',
- EB – bit stopu, bit EB zawsze =1

W sieci AS-i przyjęto elementową podstawę czasu równą 6μs, co odpowiada przepływności binarnej równej 167kb/s. Długość pauzy po wysłaniu ramki przez jednostkę nadziedną jest zależna od stopnia synchronizacji odbiornika jednostki podporządkowanej. Jeśli urządzenie podporządkowane jest zsynchronizowane, to rozpoczyna nadawanie już po upływie czasu równego transmisji trzech bitów. W przypadku braku synchronizacji wymagane jest wydłużenie pauzy o czas potrzebny na transmisję dodatkowych dwóch bitów. Jeśli jednostka nadziedna nie otrzyma odpowiedzi w czasie trwania równym czasowi transmisji dziesięciu bitów, to automatycznie przechodzi do realizacji transakcji z nastepnym urządzeniem podporządkowanym. Czas trwania pauzy po ramce odpowiedzi urządzenia podporządkowanego jest stały i równy czasowi transmisji jednego bitu. Typowy czas trwania pojedynczej transakcji wynosi 150μs. Maksymalny czas trwania pojedynczej transakcji wynosi 192μs. Minimalny czas trwania pojedynczej transakcji bez udzielonej odpowiedzi wynosi 144μs. Jednostka nadziedna realizuje cykle transakcyjne sekwencyjnie ze wszystkimi dołączonymi do sieci urządzeniami podrzędnymi. Typowy, łączny czas trwania cykli transakcyjnych w sieci złożonej z 31 urządzeń podporządkowanych wynosi ok. 5 ms. Łączny maksymalny czas trwania tej sekwencji w sieci złożonej z 31 urządzeń podporządkowanych wynosi 6,144ms. Czas trwania jednej sekwencji transakcji sieciowych jest zależny od liczby urządzeń podporządkowanych dołączonych do sieci. Czas ten nazywany jest również czasem dostępu do urządzenia.



Rys.8.13. Interpretacja graficzna sygnału ramki pakietu przesyłanych bitów w sieci AS-i

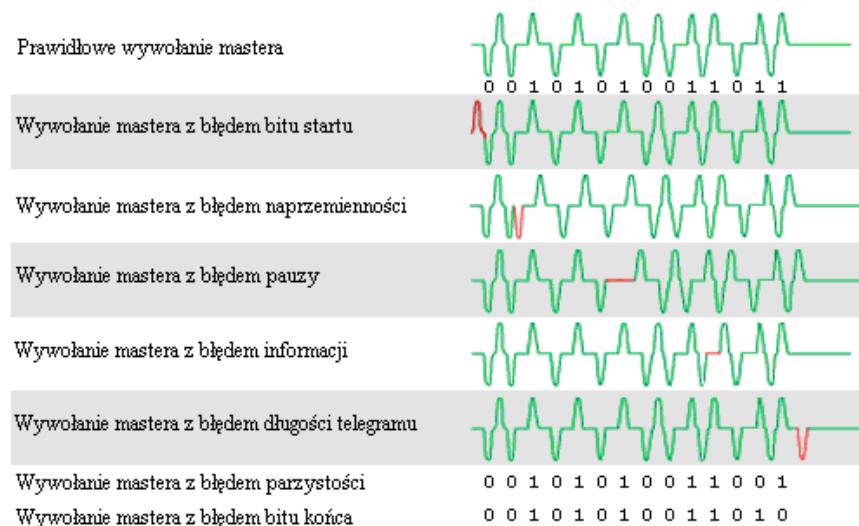
8.4.2. TRANSMISJA DANYCH

W systemach sterowania istotnym problemem jest zapewnienie wysokiej wiarygodności przekazywanych informacji. Kontrola wiarygodności transmitowanych w sieci AS-i ramek jest możliwa dzięki wprowadzeniu mechanizmu kontrolnego bitu parzystości oraz dzięki wprowadzeniu kodowania transmisyjnego PE i modulacji APM. Informacja o wartości składowej zmiennej sygnału APM wykorzystywana jest także do wykrycia stanu braku transmisji.

Przyjmuje się następujące kryteria kontroli wiarygodności ramek transmitowanych z wykorzystaniem modulacji APM:

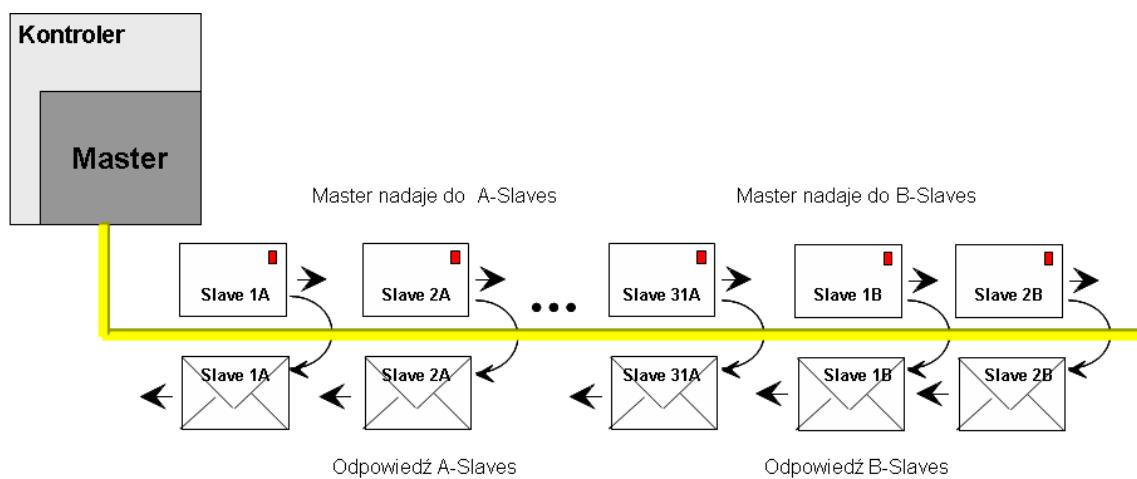
- pierwszy impuls ramki musi być impulsem ujemnym,
- kolejne pary impulsów muszą mieć przeciwną polaryzację,
- odstęp czasowy między sąsiednimi impulsami nie może przekraczać 0,5 okresu zegara taktującego transmisję,
- w drugiej połowie nadawanego bitu (w odniesieniu do nadawanej informacji) musi zawsze wystąpić impuls,
- liczba dodatnich impulsów (bez uwzględnienia bitów ST i EB) musi być parzysta,
- ostatni impuls ramki musi być dodatni,
- bezpośrednio po bicie stopu (EB) nie mogą wystąpić żadne impulsy

Po przekodowaniu informacji z kodu PE na kod binarny, realizowana jest kontrola parzystości odebranej ramki.



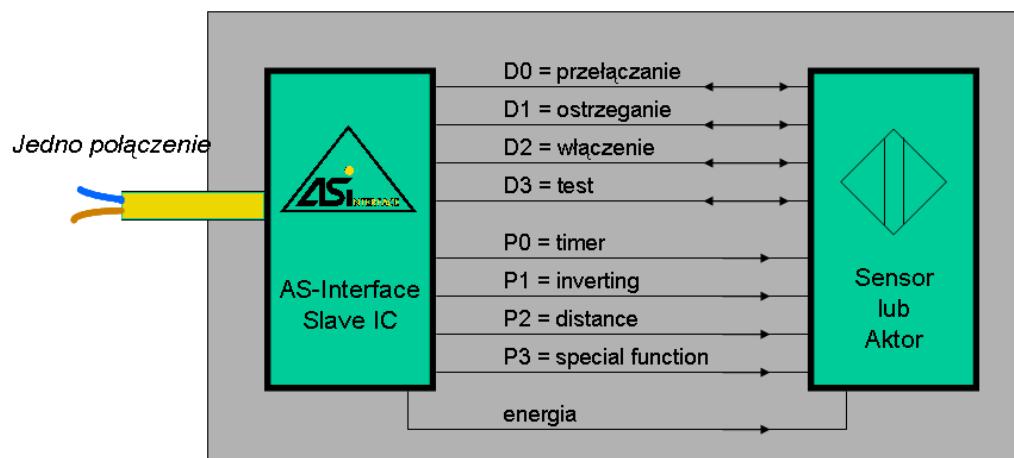
Rys.8.14. Przykłady możliwych błędów występujących w czasie transmisji informacji

8.4.3. FUNKCJONALNOŚĆ MAGISTRALI



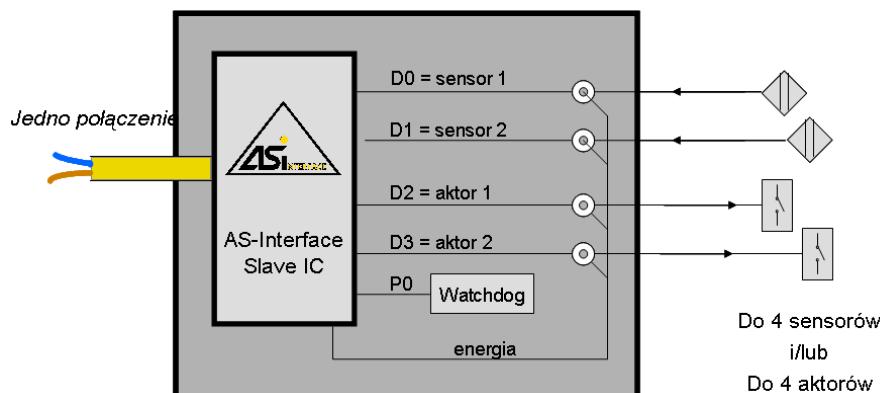
Rys.8.15. Rozszerzona sieć AS-i (62 urządzenia podporządkowane do jednego urządzenia nadzorowanego)

Maksymalna liczba urządzeń podporządkowanych w sieci AS-i zgodnej ze specyfikacją 2.0 wynosi 31. Specyfikacja 2.11 rozszerza tę liczbę do 62 urządzeń. Z punktu widzenia jednostki nadzorowanej każde urządzenie podległe jest widziane jako zespół trzech programowalnych rejestrów 4-bitowych. Pierwszy register jest rejestrem przeznaczonym na przechowywanie danych wejściowych, drugi register jest rejestrem przeznaczonym na przechowywanie danych wyjściowych, trzeci register jest przeznaczony do przechowywania wartości parametrów urządzenia. Rejestr parametrów (rys. 3.16) pozwala na rozszerzenie funkcji urządzenia (konfiguracja, diagnostyka itp.).



Rys.8.16. Profil funkcjonalny urządzenia podporządkowanego sieci AS-i

Warstwa danych sieci AS-i, podobnie jak w sieci CAN, obsługiwana jest sprzętowo. W tym celu produkowane są specjalizowane kontrolery sieci wykonywane najczęściej w postaci układów programowalnych ASIC (ang. *Application Specific Integrated Circuit*). Kontrolery te są wbudowywane bezpośrednio do sensorów i urządzeń wykonawczych. Z siecią mogą również współpracować konwencjonalne sensory i elementy wykonawcze. Produkowane są bowiem specjalne aktywne moduły przyłączeniowe sieci AS-i (rys. 8.18) o funkcji rozproszonych modułów wejść/wyjść binarnych. Typowy aktywny moduł przyłączeniowy umożliwia dołączenie do 4 urządzeń.

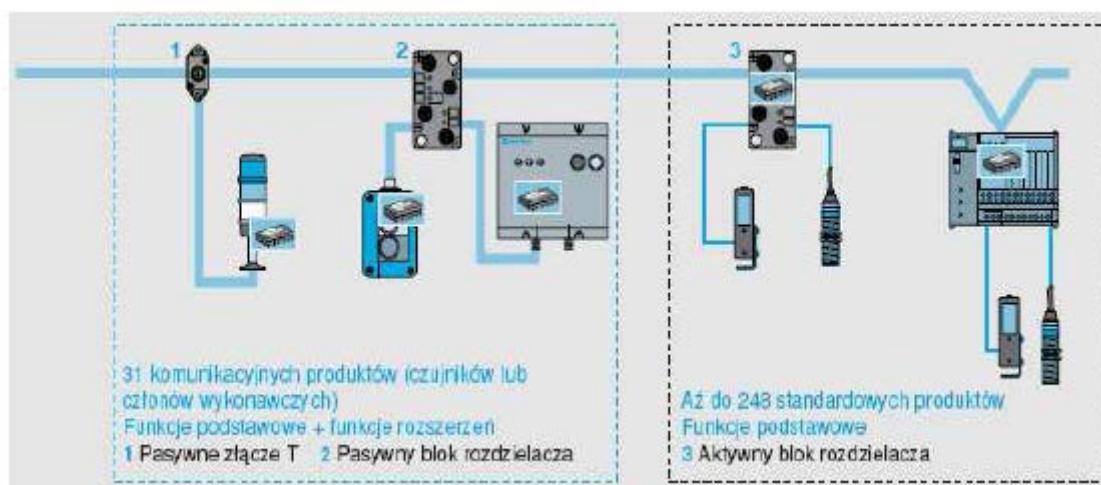


Rys.3.18. Schemat podłączenia konwencjonalnych sensorów i elementów wykonawczych



Rys.8.18. Aktywny moduł przyłączeniowy sieci AS-i z modułem ASIC

Produkowane są również pasywne przyłącza sieci AS-i nazywane przyłączaniami typu T (rys. 8.19). Przyłącza te nie zawierają kontrolera AS-i. Pozwalają jedynie na rozgałęzienie kabla AS-i w celu uzyskania łatwiejszego dostępu do urządzeń sieciowych.



Rys.8.19. Ilustracja sposobów przyłączania urządzeń podporządkowanych do sieci AS-i.

8.5. WARSTWA APLIKACJI SIECI AS-i

Warstwa aplikacji sieci AS-i obejmuje zestaw gotowych protokołów, które są wykorzystywane przez aplikacje użytkowe do przesyłania różnego typu informacji w sieci. Do podstawowych zadań warstwy aplikacji w sieci AS-i należą: obsługa komunikatów AS-i, obsługa programów funkcjonalnych jednostek podporządkowanych oraz definiowanie profili funkcjonalnych.

W sieci AS-i każde urządzenie podporządkowane posiada swój własny programowalny adres sieciowy. Ponadto każde urządzenie podporządkowane ma zdefiniowany profil funkcjonalny w postaci odpowiedniego kodu identyfikacyjnego. Adres sieciowy jest przydzielany poszczególnym urządzeniom podporządkowanym w czasie procesu produkcji urządzenia lub w fazie konfiguracji sieci zazwyczaj przy pomocy specjalnego programatora. Fabrycznie nowe urządzenie podporządkowane ma zawsze adres równy 0. Jeśli adres ten nie zostanie zmieniony, a urządzenie dołączone do sieci AS-i, to wówczas jednostka nadziedna przypisze temu urządzeniu adres tymczasowy według zasady „pierwszy wolny”. Dzięki temu urządzenia bez fizycznie przypisanego adresu mogą być podłączane w dowolnym momencie w dowolnym miejscu sieci AS-i. Ponadto jest rozpoznawane przez jednostkę nadziedną dzięki swojemu identyfikatorowi określającemu jego profil funkcjonalny. Rozpoznawanie nowo dołączonych urządzeń jest realizowane przez jednostkę nadziedną w końcowej fazie każdego cyklu sekwencji transakcji.

8.5.1. KOMUNIKATY

W sieci AS-i wyróżniamy dwa rodzaje komunikatów:

- komunikaty proste, w których przesyłane są maksymalnie 4 bity informacji z jednostki nadziednej do jednostki podrzędnej (informacja wyjściowa) oraz jednostki podrzędnej do jednostki nadziednej (informacja wejściowa),

- komunikaty złożone, w których przesyłane jest więcej niż 4 bity informacji., Komunikaty złożone składają się z serii wywołań jednostki nadzędnej i odpowiedzi jednostki podporządkowanej o zdefiniowanej treści.

8.5.1.1. KOMUNIKATY PROSTE

Komunikaty proste dzielimy na cztery grupy:

- wymiana danych lub wymiana parametrów,
- wymiana informacji ze urządzeniem o adresie zerowym,
- polecenia,
- nadawanie.

Strukturę komunikatów prostych przedstawiono na rysunkach:

- wymiana danych lub wymiana parametrów – rys. 8.20.,
- wymiana informacji ze urządzeniem o adresie zerowym – rys. 8.21.,
- polecenia – rys. 8.22. oraz rys. 8.23.,
- nadawanie – rys. 8.24.

Podczas wymiany danych i parametrów wartość bitu sterującego CB przyjmuje wartość 0.

Wywołanie mastera

| | ST | CB | 5 bitów adresu | 5 bitów informacji | PB | EB |
|------------------------|----|----|----------------|--------------------|----|----|
| Wywołanie danych | 0 | 0 | A4 A3 A2 A1 A0 | 0 D3 D2 D1 D0 | PB | 1 |
| Wywołanie danych 1) | 0 | 0 | A4 A3 A2 A1 A0 | 0 Sel D2 D1 D0 | PB | 1 |
| Wywołanie parametru | 0 | 0 | A4 A3 A2 A1 A0 | 1 D3 D2 D1 D0 | PB | 1 |
| Wywołanie parametru 1) | 0 | 0 | A4 A3 A2 A1 A0 | 1 Sel D2 D1 D0 | PB | 1 |

1) Rozszerzony tryb adresu

Rys.8.20. Struktura komunikatu prostego typu: wymiana danych lub wymiana parametrów

Dostępne są tylko dwa komunikaty, które mogą być skierowane w stronę urządzenia o adresie zerowym

Wywołanie mastera

| | ST | CB | 5 bitów adresu | 5 bitów informacji | PB | EB |
|---|----|----|----------------|--------------------|----|----|
| Przypisanie adresu: | 0 | 0 | 0 0 0 0 0 | A4 A3 A2 A1 A0 | PB | 1 |
| Wywołanie polecenia: Zapisywane: ID1 | 0 | 0 | 0 0 0 0 0 | 0 ID3 ID2 ID1 ID0 | PB | 1 |

Rys.8.21. Struktura komunikatu prostego typu: przypisanie adresu lub zapis kodu ID1

Podczas realizacji polecenia wartość bitu sterującego CB przyjmuje wartość 1.



Wyrobowanie mastera

| | ST | CB | 5 bitów adresu | 5 bitów informacji | PB | EB |
|-------------------------|----|----|----------------|--------------------|----|----|
| Wywołanie polecenia: | 0 | 1 | A4 A3 A2 A1 A0 | C4 C3 C2 C1 C0 | PB | 1 |
| Wywołanie polecenia: 1) | 0 | 1 | A4 A3 A2 A1 A0 | C4 Sel C3 C2 C1 C0 | PB | 1 |

1) Rozszerzony tryb adresu

Rys.8.22. Struktura komunikatu prostego typu: polecenie

Dostępnych jest siedem możliwych poleceń przedstawionych na rysunku 8.23.

| Czynność | Zadanie | Odpowiedź slave'a |
|-----------------------|------------------------------|--------------------|
| Konfiguracja sieci | Wykasowanie adresu | 0 |
| | Zresetowanie slave'a | 6 |
| Identyfikacja slave'a | Wczytanie konfiguracji We/Wy | Konfiguracja We/Wy |
| | Wczytanie kodu ID | Kod ID |
| | Wczytanie kodu ID1 | Kod ID1 |
| | Wczytanie kodu ID2 | Kod ID2 |
| Diagnostyka | Wczytanie statusu slave'a | Status slave'a |

Rys.8.23. Lista poleceń prostych

Komunikat nadawania jest kierowany do wszystkich urządzeń podporządkowanych jednocześnie.

| | ST | CB | 5 bitów adresu | 5 bitów informacji | PB | EB |
|---------------------|----|----|----------------|--------------------|----|----|
| Nadawanie: Reset | 0 | 1 | 1 1 1 1 1 | 1 0 1 0 1 | PB | 1 |

Rys.8.24. Struktura komunikatu prostego typu: nadawanie

8.5.1.2. KOMUNIKATY ZŁOŻONE

Komunikaty złożone są wykorzystywane do transmisji informacji o długości przekraczającej 4 bity. Z przypadkiem takim mamy do czynienia np. wówczas, gdy chcemy przesłać w postaci cyfrowej wynik pomiaru wielkości analogowej przetwornikiem analogowo-cyfrowym o rozdzielczości 12 bitów. W sieci AS-i zdefiniowano pięć odmian komunikatów złożonych CTT (ang. **Combined Transaction Types**).

Typowymi urządzeniami wykorzystującymi komunikaty złożone są:



- przetworniki analogowe do pomiaru wartości wielkości mechanicznych, termodynamicznych, elektrycznych, itp.
- analogowe urządzenia wykonawcze sterujące położeniem, kątem, obrotem, prędkością, itp.,
- urządzenia sieciowe wymagające transferu znacznej ilości parametrów w fazie uruchomienia lub podczas normalnej pracy,
- urządzenia sieciowe dostarczające dane diagnostyczne,
- skanery, panele przyciskowe, wyświetlacze.

Wyrołanie mastera

| | ST | CB | 5 bitów adresu | 5 bitów informacji | | | PB | EB |
|------------------------|-----------|-----------|-----------------------|---------------------------|-----|---------|-----------|-----------|
| 1-sze wywołanie danych | 0 | 0 | A4 A3 A2 A1 A0 | 0 | Sel | 0 01 00 | PB | 1 |
| 2-gie wywołanie danych | 0 | 0 | A4 A3 A2 A1 A0 | 0 | Sel | 0 07 06 | PB | 1 |
| 3-cie wywołanie danych | 0 | 0 | A4 A3 A2 A1 A0 | 0 | Sel | 0 05 04 | PB | 1 |
| 4-te wywołanie danych | 0 | 0 | A4 A3 A2 A1 A0 | 0 | Sel | 0 03 02 | PB | 1 |

Odpowiedź slave'a

| ST | 4 bity informacji | PB | EB |
|-----------|--------------------------|-----------|-----------|
| 0 | 0 0 E7 E6 | PB | 1 |
| 0 | 0 1 E5 E4 | PB | 1 |
| 0 | 1 0 E3 E2 | PB | 1 |
| 1 | 1 1 E1 E0 | PB | 1 |

Rys.8.25. Struktura transakcji złożonej, typ 3 (CTT3), profil S-7.A.A.

Profile urządzeń określają typy urządzeń uczestniczących w wymianie złożonych komunikatów AS-i.

| Profil urządzenia | Typ komunikatu | Profil mastera | Zastosowanie |
|-------------------|----------------|----------------|--|
| S-7.3 | CTT1 | M3 | 16 bitów wejściowych lub wyjściowych |
| S-7.4 | CTT1 | M3 | Złożone urządzenia polowe |
| S-7.5.5 | CTT2 | M4 | Połączenie urządzeń polowych |
| S-7.A.5 | CTT2 | M4 | Połączenie urządzeń polowych |
| S-B.A.5 | CTT2 | M4 | Urządzenia polowe |
| S-7.A.7 | CTT3 | M4 | 4 We/4 Wy w rozszerzonym trybie adresu |
| S-7.A.A | CTT3 | M4 | 8 We/8 Wy w rozszerzonym trybie adresu |
| S-7.A.8 | CTT4 | M4 | 16 bitów wejściowych w rozszerzonym trybie adresu |
| S-7.A.9 | CTT4 | M4 | Podwójny kanał 16 bitów wejściowych w rozszerzonym trybie adresu |
| S-6.0 | CTT5 | M4 | 16 szybkich bitów wejściowych i wyjściowych |

Rys.8.26. Typy komunikatów złożonych



8.5.2. PROFILE

W sieci AS-i profil urządzenia podporządkowanego określa:

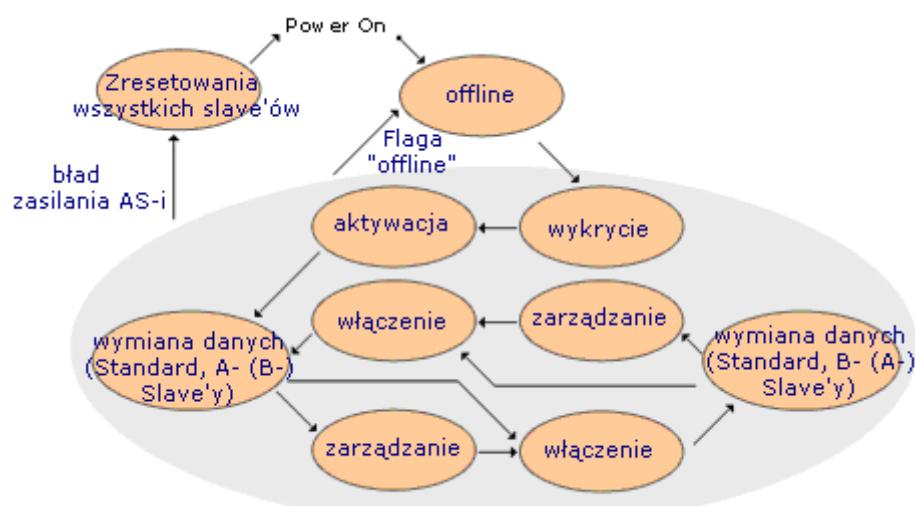
- treść informacji przekazywanej przez bity danych,
- czy zostały użyte parametry, jeśli tak - to ich ważność,
- który tryb adresowania został użyty,
- czy zewnętrzny bit błędu może być umieszczony w rejestrze statusu,
- który typ komunikatu złożonego został zaimplementowany.

8.5.3. PRZEPŁYW INFORMACJI W SIECI AS-I

W sieci AS-i wyróżniane są fazy wymiany informacji i zarządzania sieci. Podczas fazy wymiany informacji następuje sekwencyjna realizacja komunikatów prostych i złożonych, natomiast w fazie zarządzania mogą być wymieniane komunikaty acykliczne, takie jak:

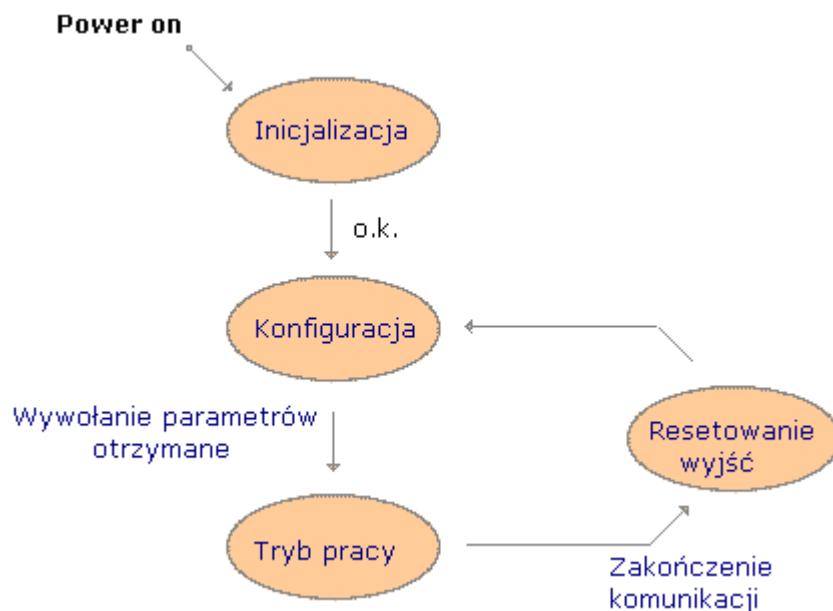
- transfer parametrów,
- polecenia (włączając komunikację ze urządzeniem o adresie zerowym),
- wywołania diagnostyczne,
- nadawanie.

Aby nie wydłużać czasu trwania cyklu, podczas każdej fazy zarządzania jest wysyłany tylko jeden pojedynczy komunikat. Jeśli jest to konieczne, możliwe jest podzielenie sekwencji na kilka cykli.



Rys.8.27. Diagram przepływu informacji w urządzeniu nadzorowanym

W przypadku, gdy urządzenia sieciowe A i B (specyfikacja rozszerzona) mają te same adresy sieciowe, to faza wymiany informacji różni się od fazy zarządzania. W tym przypadku w fazie wymiany informacji następuje komunikacja z urządzeniem sieciowym A, natomiast w fazie zarządzania komunikacja z urządzeniem B.



Rys.8.28. Diagram przepływu informacji w urządzeniu podrzędnym

8.6. BEZPIECZNA SIEĆ AS-i

Sieć AS-i została pierwotnie zaprojektowana do wymiany krótkich informacji binarnych. Nie wyklucza to możliwości przesyłania dłuższych ciągów danych (np. wartości cyfrowych wielkości analogowych). W praktyce stawiany jest problem, czy możliwe jest wykorzystanie sieci AS-i do przesyłania istotnych dla bezpieczeństwa personelu i procesu sygnałów pochodzących z wyłączników bezpieczeństwa. Obecnie do przesyłania tego typu sygnałów stosowane muszą być specjalne systemy niezależne od systemów sieciowych.

W sieci AS-i dostępne są urządzenia podporządkowane o wysokim stopniu bezpieczeństwa, które można wykorzystać do transmisji informacji z wyłączników bezpieczeństwa. Dodatkowo do takiej sieci musi być dołączony specjalne urządzenie zwane monitorem bezpieczeństwa. Monitor ten nadzoruje komunikację pomiędzy bezpiecznymi urządzeniami podporządkowanymi i urządzeniem nadzorującym. W przypadku wykrycia błędu komunikacji lub uszkodzenia, ustawia sterowane urządzenie lub proces w stan bezpieczny. Zastosowanie monitora bezpieczeństwa pozwala na podniesienie klasy bezpieczeństwa całej sieci.

9. SIEĆ CAN

9.1. RYS HISTORYCZNY

Sieć CAN (ang. Controller Area Network) jest międzynarodowym otwartym⁶ standardem komunikacyjnym przeznaczonym głównie do stosowania w zadaniach sterowania i pomiarów w technice samochodowej oraz w przemyśle elektromaszynowym. Prace związane z opracowaniem sieci CAN zostały rozpoczęte w 1983 roku przez firmę Bosch. Do prac nad projektem nowej sieci dołączyła wkrótce firma Mercedes-Benz oraz firma Intel. W 1986 roku sieć CAN została oficjalnie zaprezentowana w Detroit na kongresie SAE (Society of Automotive Engineers) pod nazwą: Automotive Serial Controller Area Network. W połowie lipca 1987 roku firma Intel dostarczyła pierwszy zintegrowany układ kontrolera sieci CAN.

9.2. STANDARYZACJA

We wczesnych latach 90-tych firma Bosch przedłożyła specyfikację protokołu CAN (w wersji 2.0) w celu jej międzynarodowej standaryzacji. W wyniku dyskusji uwzględniającej między innymi sieć VAN (Vehicle Area Network) w listopadzie 1993 roku opublikowana została pierwsza norma dotycząca sieci CAN (ISO 11898). W wyniku dalszych prac rozwojowych unormowano sieć CAN tolerującą uszkodzenia (ang. *fault-tolerant*), która została opisana w specyfikacji ISO 11519-2. W roku 1995 norma ISO 11898 została rozszerzona o dodatek opisujący wykorzystanie 29-bitowego identyfikatora CAN.

Aby zapewnić zgodność implementacji sieci CAN, opracowano standardowe testy zgodności opublikowane w normie ISO 16845. W wyniku prowadzonych dalszych prac dokonano weryfikacji pierwotnego brzmienia normy ISO 11898. Obecnie obowiązują następujące normy:

- ISO 11898-1 opisuje warstwę danych
- ISO 11898-2 opisuje warstwę fizyczną
- ISO 11898-3 opisuje warstwę fizyczną odporną na uszkodzenia
- ISO 11992 opisuje interfejs dla samochodów ciężarowych i przyczep

9.3. CAN – CHARAKTERYSTYKA OGÓLNA

CAN jest lokalną siecią komunikacyjną typu *fieldbus*, a więc przeznaczoną głównie do zastosowań i realizacji zadań tzw. warstwy obiektoowej modelu procesu produkcji i zarządzania. W warstwie obiektoowej zlokalizowane są głównie urządzenia pomiarowe i wykonawcze. Ze względu na ekonomiczność implementacji - podobnie zresztą jak w większości innych sieci typu *fieldbus* – stosowana jest komunikacja szeregowa o maksymalnej prędkości transmisji równej 1Mb/s. Należy zaznaczyć, że prędkość transmisji jest funkcją długości sieci. Ogólnie im większa długość sieci tym mniejsza dopuszczalna prędkość transmisji. Na przykład dla sieci CAN o topologii magistrali maksymalna prędkość transmisji spada do ok. 20kb/s dla sieci o długości 1000m.

⁶ Specyfikacje: ISO 11898, ISO 11519-2, ISO 11992

Typowymi topologiami sieci CAN są topologie: magistrali lub łańcucha. Nie są natomiast stosowane topologie: rozgałęzionego drzewa, pierścienia, gwiazdy czy siatki.

Sieć CAN złożona jest z urządzeń sieciowych zwanych węzłami. Węzły połączone są wzajemnie wspólną magistralą. Magistrala umożliwia wymianę informacji w sieci (dwie linie danych) i ewentualne zasilanie urządzeń sieciowych (2 dodatkowe linie zasilania). Sposób wymiany informacji w sieci CAN ma zupełnie odmienny charakter w stosunku do sposobu właściwego dla sieci typu *master-slave* (np. MODBUS RTU czy AS-i). Sieć CAN jest siecią typu rozgłoszeniowego. Oznacza to, że każdy węzeł ma prawo inicjacji transakcji sieciowych. W tym wypadku informacje przesyłane w wyniku realizacji transakcji sieciowych nazywane są wiadomościami. W przypadku sieci typu master-slave prawo do inicjacji transakcji sieciowych przysługiwało wyłącznie jednostce lub jednostkom nadzorującym. Wynika stąd, że w sieci CAN nie ma wyróżnionej jednostki nadzorującej, lub wszystkie węzły mogą (przynajmniej teoretycznie) taką rolę pełnić. Z tego powodu sieć CAN zaliczana jest do klasy sieci typu *multimaster*. Należy jednak wyraźnie zaznaczyć, że sieć CAN nie wyklucza możliwości wymiany informacji zgodnej z modelem sieci master-slave. Zależy to wyłącznie od implementacji warstwy aplikacyjnej. Międzynarodowe normy, o których była mowa w p. 4.2 definiują wyłącznie dwie pierwsze warstwy modelu komunikacyjnego ISO/OSI i nie dotyczą tej warstwy. Na przykład międzynarodowa organizacja CiA (ang. *CAN in Automation*) czuwająca nad rozwojem sieci zdefiniowała implementację tej warstwy o nazwie CanOpen, a firma Allen-Bradley produkująca sprzęt głównie do zastosowań elektroenergetycznych zdefiniowała implementację o nazwie DeviceNet.

Prawo inicjacji transferów sieciowych przez wszystkie węzły sieci wprowadza możliwość wystąpienia konfliktów (kolizji) informacyjnych na magistrali. Kolizje te mają miejsce wówczas, gdy dwa lub więcej węzłów sieciowych zainicjują jednocześnie transakcje sieciowe. Kolizje sieciowe rozstrzygane są w wyniku realizacji odpowiednich procedur zwanych procedurami arbitrażowymi. W przypadku sieci typu master-slave arbitraż nie jest konieczny, ponieważ organizacja wymiany informacji w takiej sieci nie pozwala na występowanie kolizji. Jeśli kolizje takie wystąpią w wyniku np. zakłóceń, to są rozstrzygane np. przez mechanizmy retransmisyjne realizowane w warstwie aplikacyjnej. W przypadku sieci o charakterze rozgłoszeniowym konflikty rozstrzygane są zasadniczo na dwa sposoby.

Pierwszy sposób (CSMA/CD⁷) polega na unieważnieniu bieżącej transakcji i przydzieleniu węzłom będącym w konflikcie losowych czasów oczekiwania na możliwość reinitiacji unieważnionej transakcji. Istnieje wówczas stosunkowo wysokie prawdopodobieństwo uniknięcia ponownego konfliktu. Niemniej jednak, istnieje również prawdopodobieństwo powstania konfliktu z informacjami generowanymi przez nowe węzły sieci w czasie reinitializacji transakcji wcześniej skonfliktowanych węzłów. Taki sposób rozwiązywania konfliktów nazywamy arbitrażem niszczącym, a sieć wykorzystująca ten sposób arbitrażu nie może być uznana za sieć deterministyczną.

Drugi sposób (CSMA/CA⁸) rozwiązywania konfliktów, zwanych arbitrażem nieniszczącym polega na jednoznaczny rozstrzygnięciu w początkowym okresie trwania konfliktu, które z urządzeń komunikacyjnych będących w konflikcie uzyska prawo do dalszej transmisji, a które urządzenia muszą

⁷ CSMA/CD (ang. *Carrier Sense Multiple Access / with Collision Detect*) = protokół wielodostępu CSMA ze śledzeniem stanu dostępności medium transmisyjnego i wykrywaniem kolizji

⁸ CSMA/CA (ang. *Carrier Sense Multiple Access /with Collision Avoidance*) = protokół wielodostępu do magistrali ze śledzeniem stanu nośnika i unikaniem kolizji

wycofać żądanie rozpowszechniania własnych wiadomości. Taki sposób rozwiązywania konfliktów sprzyja zwiększeniu sprawności informacyjnej sieci, a także determinizmowi sieci. Sieć CAN korzysta z metody arbitrażu nieniszczącego.

Istotną cechą sieci rozgłoszeniowych jest zmiana sposobu sygnalizacji źródła pochodzenia informacji. W przypadku sieci typu monomaster każdemu urządzeniu podlegającemu nadawany jest unikalny adres. Jednostka nadzorująca zwraca się z odpowiednim rozkazem do jednostki podporządkowanej wskazując jej adres. Jednostka nadzorująca musi zatem prowadzić listę adresów urządzeń podporządkowanych. Urządzenie podporządkowane odpowiada na zapytanie lub rozkaz jednostki nadzorującej umieszczając w ramce odpowiedzi swój własny adres jako wskaźnik źródła pochodzenia informacji. Ponieważ w sieci CAN wszystkie urządzenia sieciowe mają prawo inicjowania transakcji sieciowych, to ważne jest nie to, która jednostka jest źródłem informacji, ale sama informacja jako taka. Dla porządku informacjom przypisano odpowiednie identyfikatory. Identyfikatory te często są mylnie utożsamiane z adresami. Co do zasady, identyfikatory wiadomości w sieci CAN muszą być unikalne. Identyfikatorem jest opatrywana każda wiadomość. Odgrywa ona rolę prioritetu wiadomości. Im niższa wartość binarna identyfikatora, tym wyższy jest prioritet wysyłanej informacji. Procedura arbitrażu jest realizowana w czasie transmisji identyfikatora. Prawo kontynuacji transakcji sieciowej uzyskuje węzeł generujący wiadomości o najwyższej wartości binarnej identyfikatora. Ze względów technicznych dla skutecznej realizacji procedury arbitrażu konieczne jest stosowanie w CAN trybu transmisji synchronicznej.

Konstrukcja ramki danych CAN ma w zasadzie organizację bitową. Oznacza to, że podstawowymi elementami składowymi ramki CAN są pola bitowe. Od tej zasady istnieje jednak wyjątek – jest nim pole danych o organizacji bajtowej. Maksymalna długość pola danych w sieci CAN jest ograniczona do zaledwie 8 bajtów. Jest to znaczco mniej w porównaniu do innych sieci. Na przykład w przypadku sieci MODBUS RTU maksymalna długość pola danych wynosi 256 bajtów, w sieci PROFIBUS PA, DP i FMS – 244 bajty. Należy stąd wnioskować, że sieć CAN jest siecią przeznaczoną do efektywnego (organizacja bitowa), przesyłania stosunkowo krótkich informacji (0..8 bajtów).

Obecnie, w skali globalnej około 40 producentów układów scalonych dostarcza gotowe układy realizujące sprzętowo wymagania specyfikacji CAN na poziomach: warstwy fizycznej i warstwy wymiany danych. Pozwala to na skoncentrowanie uwagi konstruktorów węzłów CAN na implementacji warstwy aplikacyjnej modelu ISO/OSI. W związku z tym, praktycznie jedynymi zadaniami użytkownika jest realizacja przepływu strumieni informacji. Wszystkie inne niezbędne procedury związane z realizacją protokołu komunikacyjnego (takie jak np. kompozycja ramki, detekcja błędów czy retransmisja błędnych ramek) są przeprowadzane automatycznie przez sprzęt bez ingerencji użytkownika.

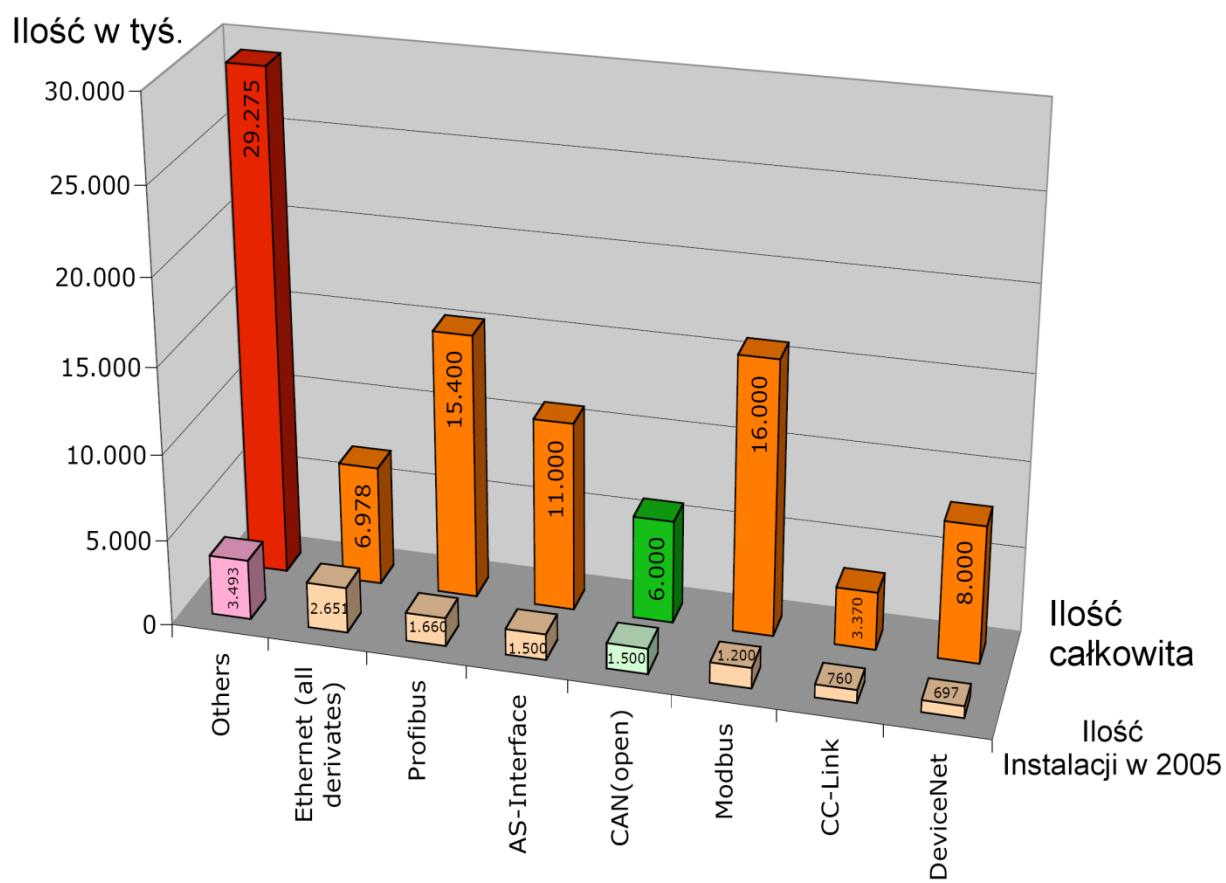
Podsumowując, podstawowymi cechami sieci CAN są:

- ❑ organizacja typu multimaster. Organizacja tego typu pozwala na budowę sieci o właściwościach redundancyjnych, w której awaria jednego z węzłów nie powoduje blokady pracy sieci całej sieci,
- ❑ komunikacja rozgłoszeniowa (ang. broadcast). Każda wiadomość pojawiająca się w sieci jest dostępna dla wszystkich urządzeń sieciowych. To urządzenia sieciowe decydują o wykorzystaniu tej wiadomości lub decydują czy wiadomość jest skierowana jest do nich,
- ❑ zaawansowane metody detekcji błędów. Metody te gwarantują spójność i poprawność transmitowanych i odbieranych wiadomości.

9.4. ROZWÓJ SIECI CAN

Ze względu na otwarty charakter sieci oczywistą stała się potrzeba powołania organizacji, która będzie czuwać nad jej rozwojem. W 1992 powstała organizacja zrzeszająca użytkowników sieci CAN o nazwie CiA (ang. *CAN in Automation*). Głównym celem organizacji jest promowanie i rozwój sieci. Obecnie organizacja zrzesza około 460 użytkowników i producentów sieci CAN.

Na zlecenie organizacji CiA firma IMS Research wykonała w 2007 roku badania liczby zainstalowanych węzłów różnych rodzajów sieci. Na rys. 9.1 uwidoczniony jest wynik tej analizy.



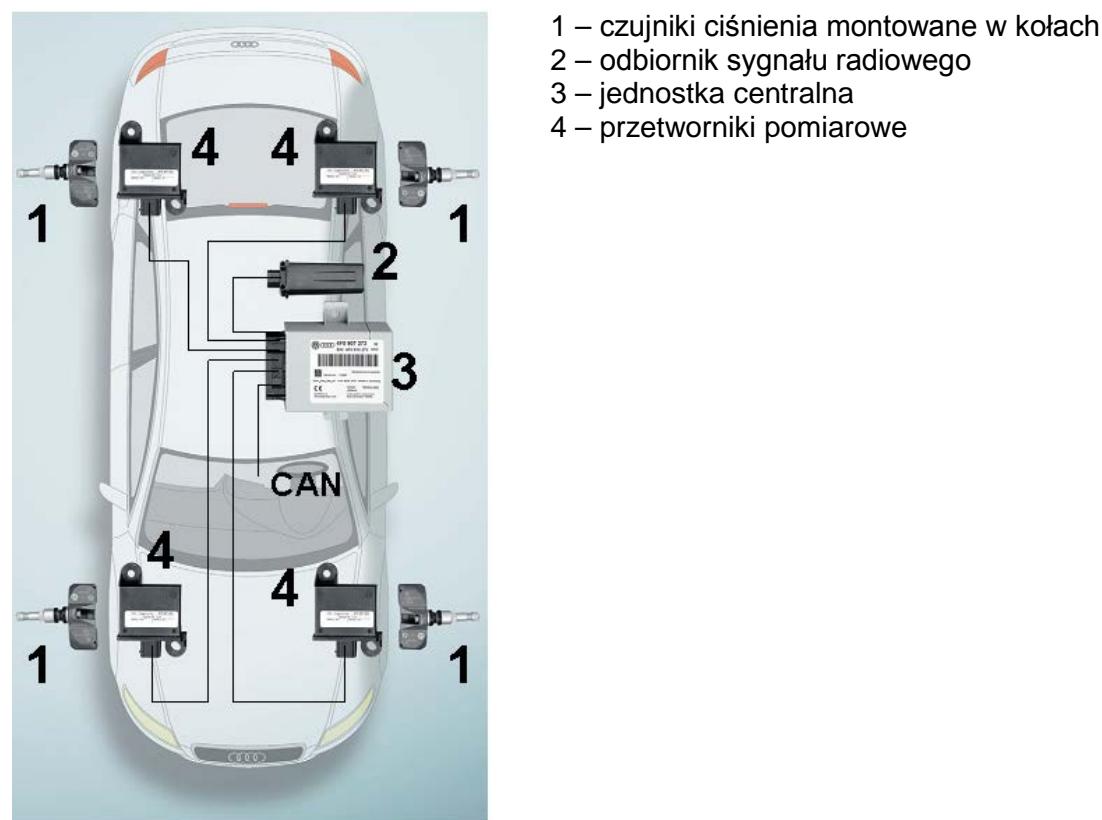
Rys. 9.1 Liczba zainstalowanych węzłów różnych systemów sieciowych w samym 2005 roku i ich ogólna liczba według stanu z 2005 roku

Wykres uwidacznia całkowitą liczbę instalacji w skali globalnej bez podziału na poszczególne dziedziny przemysłu. Sieci wykorzystujące specyfikację CAN (*CANopen*, *DeviceNet*) zajmują znaczące miejsce w ogólnej liczbie zainstalowanych węzłów. Liczba zainstalowanych węzłów sieci wykorzystujących CAN w 2005 roku jest tylko nieco ustępuje liczbie węzłów sieci Ethernet. Głównym powodem ekspansji sieci CAN jest jej powszechnie zastosowanie w przemyśle samochodowym.

9.5. PRZYKŁAD ZASTOSOWANIA SIECI CAN

Utrzymywanie ciśnienia powietrza w oponach na odpowiednim poziomie jest ważnym elementem wpływającym na bezpieczeństwo jazdy, komfort podróży, zużycie opon oraz zużycie paliwa. Firma Beru stworzyła system kontroli ciśnienia w oponach, który został dość powszechnie zaaprobowany przez producentów samochodów. System oferuje ciągłą kontrolę ciśnienia w oponach zarówno podczas postoju jak i w czasie jazdy. Ponadto system umożliwia:

- wcześnie ostrzeganie przed zbytnim spadkiem ciśnienia
- wspomaganie doboru ciśnienia podczas pompowania
- kontrolę parametrów ciśnienia podczas diagnostyki oraz napraw auta



Rys. 9.2 Ilustracja systemu kontroli ciśnienia w oponach

Czujnik ciśnienia wbudowany jest w zawór znajdujący się w kole (1). Zasilany jest baterijnie a transmisja odbywa się drogą radiową. Dla zapewnienia jednoznaczności pomiarów każde koło, w tym również koło zapasowe posiada swój własny identyfikator. Monitorowane jest aktualne ciśnienie w oponie oraz jego spadki. Możliwe jest zaprogramowanie ciśnienia nominalnego dla danego auta (może tego dokonywać producent auta lub jego użytkownik). W skład zestawu wchodzą 4 zawory, 4 układy elektroniczne montowane w kole, 4 przetworniki pomiarowe, odbiornik sygnału radiowego oraz jednostka centralna. Jednostka centralna jest jednocześnie węzłem sieci CAN, co umożliwia jej bezpośrednią współpracę z samochodową siecią CAN.

9.6. SIEĆ CAN A MODEL ODNIESIENIA ISO/OSI

Podobnie jak większość współczesnych systemów komunikacyjnych, w tym również sieć CAN, została zaprojektowana zgodnie z wzorcowym modelem sieci otwartych zdefiniowanym przez ISO⁹. Model ISO/OSI opisuje sposób wymiany informacji w sieci. Definiuje 7 warstw protokołu oraz ich wzajemne relacje (logiczne, elektryczne, fizyczne). Co do zasady, kolejne warstwy modelu mogą komunikować się wzajemnie wyłącznie w układzie pionowym. Oznacza to, że warstwy świadczą usługi komunikacyjne wyłącznie w stosunku do swoich najbliższych warstw sąsiednich.

| Numer warstwy | Nazwa warstwy | Realizacja w sieci CAN |
|---------------|----------------------|--|
| 7 | Warstwa aplikacji | CANopen, DeviceNet, J1939 |
| 6 | Warstwa prezentacji | |
| 5 | Warstwa sesji | |
| 4 | Warstwa transportowa | |
| 3 | Warstwa sieciowa | |
| 2 | Warstwa danych | Zgodna z ISO 11898-1 |
| 1 | Warstwa fizyczna | Zgodna z: ISO 11898-2, ISO 11898-3, SAE J2411, ISO 11992 |

Rys. 9.3 Specyfikacja CAN w stosunku do modelu odniesienia ISO/OSI

W sieci CAN, podobnie jak dla większości sieci typu LAN, definiowane są tylko 3 warstwy modelu (rys 9.3). Należą do nich: warstwa fizyczna (1), warstwa danych zwana również warstwą łącza danych (2) oraz warstwa aplikacji (7). Pozostałe warstwy z modelu nie zostały zdefiniowane. Warstwy 1 i 2 zostały ujęte w odpowiednich międzynarodowych uregulowaniach standaryzacyjnych.

Warstwa fizyczna

Warstwa ta definiuje mechaniczne i elektryczne aspekty fizycznego dostępu do realnej sieci komunikacyjnej. Fizyczny kanał komunikacyjny zwany jest również kanałem podkładowym lub medium komunikacyjnym. W warstwie tej zdefiniowane są sposoby kodowania i dekodowania informacji oraz zastosowana technika synchronizacji sieci. Przedmiotem opisu warstwy fizycznej jest również specyfikacja standardowych rodzajów złącz.

⁹ Model sieci otwartej ISO/OSI (ang. *Open System Interconnection*) jest zgodny z normą międzynarodową ISO7498 i często jest nazywany modelem ISO/OSI.

W przypadku sieci CAN informacja kodowana jest w postaci napięciowego sygnału różnicowego pomiędzy dwoma przewodami elektrycznymi sieci. Medium fizycznym w tym przypadku jest para skręconych przewodów o odpowiedniej impedancji charakterystycznej zakończonych dwoma rezystorami zwierającymi tzw. terminatorami. Rezystancja terminatorów jest dobrana, aby możliwe było optymalne tłumienie odbić w magistrali.

Warstwa łącza danych

Warstwa ta definiuje strukturę logiczną ramki komunikacyjnej. Warstwa ta jest odpowiedzialna za odbiór i wysyłanie informacji z i do warstwy fizycznej oraz za komunikację z warstwą aplikacji. W przypadku sieci CAN zadania warstwy łącza danych są realizowane sprzętowo. W celu sprzętowej realizacji zadań warstwy łączącej danych zaprojektowano odpowiednie układy scalone zwane kontrolerami CAN. Kontrolery CAN są również integrowane z systemami mikroprocesorowymi w postaci specjalizowanych modułów. Kontroler CAN realizuje dostęp do medium komunikacyjnego za pośrednictwem sprzętowego sterownika spełniającego wymagania stawiane w warstwie fizycznej. Dzięki temu zapewniono prostą, taną i wygodną implementację sieci. Podobne podejście zastosowano między innymi w sieci AS-i. W wielu innych sieciach zadania warstwy drugiej modelu ISO/OSI realizowane są programowo (np. w sieci MODBUS RTU czy w sieci PROFIBUS PA).

Warstwa aplikacji

Specyfikacja CAN zawarta w odpowiednich normach opisujących warstwy pierwszą i drugą nie definiuje szeregu aspektów istotnych z punktu widzenia praktycznej realizacji sieci. Należą do nich między innymi takie aspekty jak: ustalenie schematu adresowania węzłów, kontrola przepływu informacji, ustalanie prędkości transmisji w sieci i procedur startowych, definicji sposobów przesyłania danych o objętości przekraczających objętość jednej ramki komunikacyjnej itp. Zagadnienia te są realizowane i rozstrzygane przez protokoły warstwy 7 modelu OSI zwane też prokółami warstwy wyższej HLP (ang. *High Level Protocol*).

Do najbardziej popularnych protokołów warstwy wyższej HLP należą:

- CANopen – protokół utworzony, spopularyzowany i rozwijany przez organizację CiA. Zyskał największą popularność w automatyce przemysłowej i w przemyśle budowy maszyn.
- DeviceNet – opracowany przez firmę Allen-Bradley(Rockwell). Obecnie jest rozwijany jest przez organizację ODVA (*Open DeviceNet Vendors Association*). Wykorzystywany jest w automatyce przemysłowej, i elektroenergetycznej,
- CAN Kingdom – opracowany przez Szwedzką firmę Kvaser AB. Wykorzystywany jest głównie w zadaniach sterowania maszyn,
- J1939 – opracowany i rozwijany przez stowarzyszenie SAE (*Society of Automotive Engineers*). Stosowany jest w automatyzacji aut osobowych i ciężarowych oraz maszyn budowlanych.

9.7. PODSTAWOWE WIADOMOŚCI O SIECI CAN

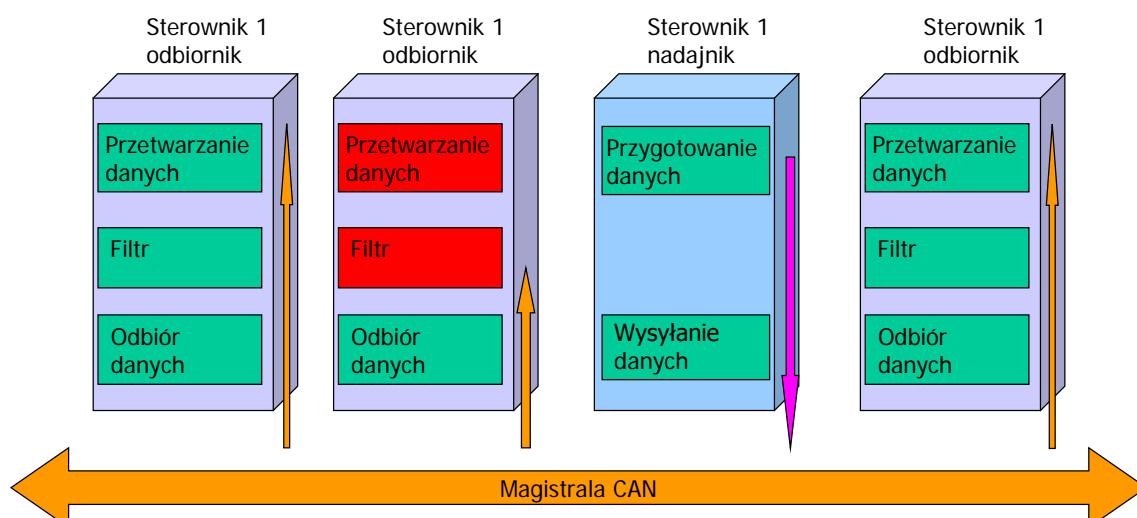
Komunikacja w sieci oparta jest na modelu rozgłoszeniowym (ang. *broadcast*). W modelu tym istotna jest wiadomość i jej treść, a nie źródło jej pochodzenia. Każdej wiadomości przypisywany jest identyfikator. Identyfikator musi być bezwzględnie unikalny w skali całej sieci. Identyfikatory pozwalają jednocześnie na:

- zachowanie porządku w sieci,
- wskazanie stopnia ważności wiadomości (priorytety wiadomości),
- realizację procedury arbitrażu.

Jest jasne, że jeśli identyfikatory wiadomości będą miały charakter unikalny w skali globalnej to zapewnić to może bardzo prostą obsługę i rozbudowę istniejącej sieci. Dzięki temu, w prosty sposób można dodawać nowe węzły do magistrali bez konieczności głęboko idących ingerencji w jej ustawienia. Także wymiana uszkodzonego węzła sieci jednostki nie powoduje konieczności jakichkolwiek zmian w oprogramowaniu czy też ustawieniach sprzętowych.

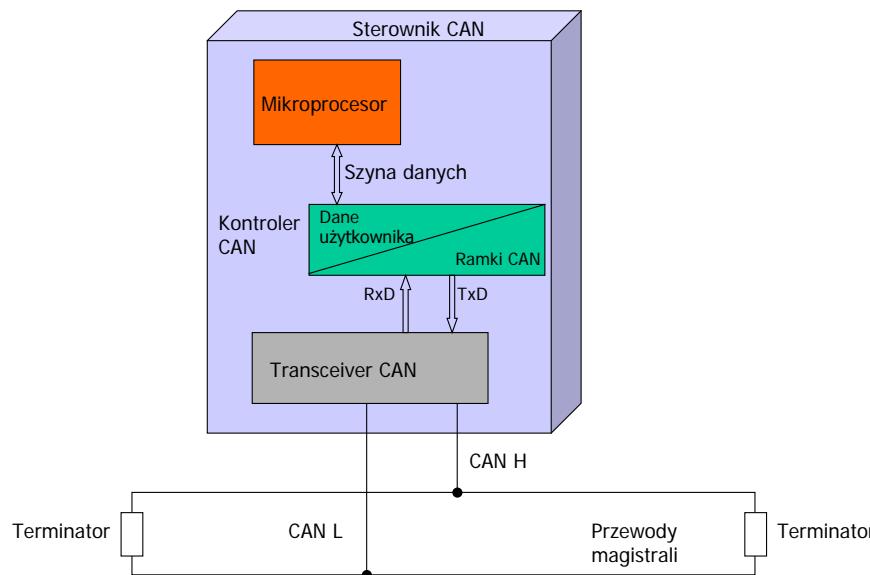
9.7.1. PRZEPŁYW INFORMACJI W SIECI

Każda wiadomość rozsyłana w sieci jest dostępna dla każdego węzła w sieci, w tym oczywiście także dla węzła, który jest jej źródłem. Każdy węzeł, przy pomocy odpowiedniego filtra (maski), może decydować o przyjęciu wiadomości i przekazaniu jej do dalszego przetwarzania lub o jej odrzuceniu. Akceptacja wiadomości realizowana jest na podstawie analizy zawartości identyfikatora wiadomości. Urządzenia wysyłające wiadomości akceptują je jednocześnie niezależnie od identyfikatora. Schemat przepływu informacji w sieci przedstawiono na rys. 9.4.



Rys. 9.4 Przepływ informacji w obrębie magistrali

9.7.2. PRZEPŁYW INFORMACJI W OBRĘBIE WĘZŁA



Rys. 9.5 Przepływ informacji w obrębie węzła

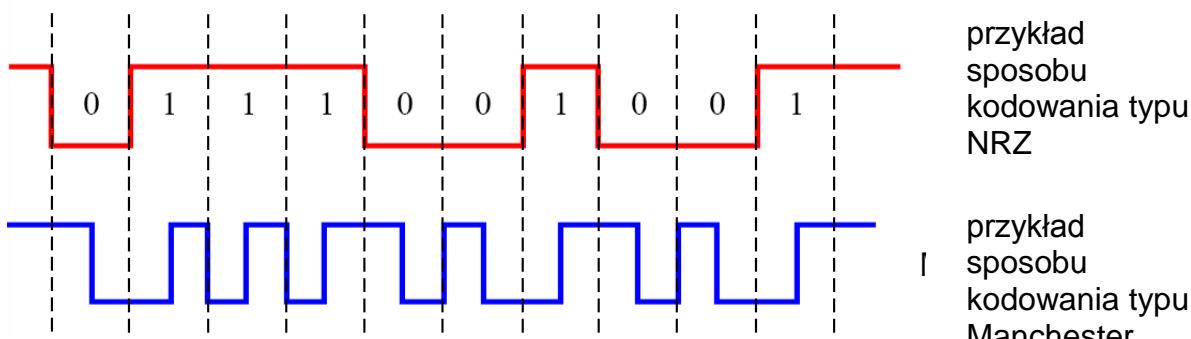
Przepływ informacji w obrębie węzła sieci CAN przedstawiono na rys. 9.5. Kontroler CAN oraz sterownik magistrali (transceiver) realizują zadania warstwy 1 i warstwy drugiej modelu ISO/OSI. Wyróżniona jednostka mikroprocesorowa realizuje programowo zadania warstwy aplikacyjnej. Przepływ informacji w węźle jest dwukierunkowy realizowany równolegle na poziomie wyższym i szeregowo na poziomie niższym. Należy jednak zaznaczyć, że przepływ informacji w kanale podkładowym (w magistrali CAN) odbywa się dwukierunkowo ale w trybie komunikacji szeregowej naprzemiennej.

9.8. WARSTWA FIZYCZNA

Warstwa fizyczna opisuje między innymi rodzaj medium transmisyjnego, rodzaje okablowania, poziomy napięć, sposoby przyporządkowanie stanów logicznych, sposób synchronizacji, prędkość transmisji, itp.

9.8.1. TECHNIKA KODOWANIA INFORMACJI

Magistrala CAN jest magistralą dwukierunkową i synchroniczną. Zastosowano w niej sposób kodowania informacji metodą NRZ (ang. *Non Return to Zero*). W metodzie tej stan logiczny jest reprezentowany przez stały poziom sygnału fizycznego. Ten sposób kodowania jest bardziej efektywny niż metodą Manchester (rys. 9.6). W metodzie kodowania typu Manchester stany logiczne kodowane są nie tyle poziomami sygnałów fizycznych, co przez zmiany (zbocza) tych sygnałów. Istotną wadą techniki kodowania NRZ jest możliwość utraty synchronizmu sieci, w przypadku przesyłania długich ciągów bitowych o tej samej wartości. W CAN problem ten rozwiązano w ten sposób, że w przypadku występowania ciągów bitowych składających się z samych zer lub samych jedynek i jednocześnie dłuższych niż 5 bitów następuje automatyczna krótkotrwała zmiana stanu na przeciwny (technika: *bit stuffing*). Zmiana ta pozwala na zachowanie synchronizacji węzłów. Dodatkowe bity synchronizujące są usuwane przez kontroler CAN odbiornika wiadomości. Z punktu widzenia warstwy aplikacyjnej technika dodawania i usuwania bitów synchronizacyjnych jest całkowicie przezroczysta.



Rys. 9.6 Porównanie sposobów kodowania typu NRZ i typu Manchester

9.8.2. TAKTOWANIE I SYNCHRONIZACJA

Wykorzystanie transmisji synchronicznej pozwala na znacznie zwiększenie przepływności binarnej w kanale podkładowym w stosunku do transmisji asynchronicznej. Wymaga to jednak zastosowania określonych metod zapewniających synchronizację procesów komunikacyjnych. W przypadku transmisji asynchronicznej, synchronizacja jest realizowana przez bit startu dołączany do każdego transmitowanego znaku. W przypadku komunikacji synchronicznej w sieci CAN stosowany jest tylko jeden bit startu na początku całej ramki komunikacyjnej. Zatem zapewnienie właściwego odbioru transmitowanej wiadomości wymaga właściwej synchronizacji nadajnika wiadomości z jej odbiornikami w czasie trwania transmisji całej wiadomości.

9.8.3. ZALEŻNOŚĆ PRĘDKOŚCI TRANSMISJI OD DŁUGOŚCI MAGISTRALI

Prędkość transmisji w sieci CAN zależy od właściwości elektrycznych samego kanału podkładowego i wejściowych parametrów elektrycznych węzłów sieciowych. Istotnym parametrem sieci umożliwiającym określenie maksymalnej prędkości transmisji jest czas propagacji sygnału w sieci pomiędzy dwoma najbardziej od siebie oddalonymi węzłami sieci. Czas propagacji uwzględnia:

- czas potrzebny na przesłanie sygnału pomiędzy najbardziej oddalonymi węzłami sieci,
- czas opóźnienia w układach nadajnika i odbiornika,
- czas potrzebny na uzyskanie synchronizmu,
- czas niezbędny na powrót sygnału.

Wynika stąd, że im dłuższa magistrala, tym większa jej pojemność i indukcyjność oraz większe opóźnienie i tłumienie sygnału. W związku z tym wzrasta czas propagacji i zmniejsza się dopuszczalna prędkość komunikacji w sieci. Należy zaznaczyć, że dla prawidłowego działania sieci konieczne jest przyjęcie jednej wspólnej prędkości komunikacji dla wszystkich węzłów sieci. W tym przypadku prędkość sieci ustalana jest w oparciu o zasadę analizy najgorszego przypadku.

9.8.4. KANAŁ PODKŁADOWY TRANSMISJI DANYCH

Aby medium fizyczne mogło być użyte do transmisji wiadomości zgodnych ze specyfikacją protokołu CAN musi posiadać zdolność reprezentowania stanu dominującego i recesywnego. Jak dotąd udało się to uzyskać za pomocą medium elektrycznego i optycznego. Stanem dominującym jest taki stan logiczny magistrali, który ma w stosunku

do stanu recesywnego tę przewagę, że ich jednoczesna zaistnienie w tym samym medium fizycznym spowoduje powstanie stanu dominującego. W przypadku medium elektrycznego jest to stan 0 logicznego.

Dla medium elektrycznego poziomy napięcia różnicowego oraz stany dominujące i recesywne zostały zdefiniowane w normach: ISO 11898-2, ISO 11898-3, SAE J2411 i ISO 11992. Dla medium optycznego poziom recesywny jest reprezentowany przez brak sygnału świetlnego „dark” zaś poziom dominujący reprezentuje sygnał świetlny „light”.

Najczęściej używanym kanałem fizycznym transmisji w sieciach CAN jest symetryczna skręcona, ekranowana para przewodów. W pojazdach samochodowych stosowany jest pojedynczy przewód. Prowadzone są też badania nad możliwością komunikacji CAN z wykorzystaniem linii zasilających urządzenia (na wzór sieci AS-i).

Dobór medium fizycznego wymaga uwzględnienia takich parametrów jak: czas propagacji sygnału, rezystancja, przekrój poprzeczny przewodów czy spadek napięcia na przewodach. W procesie doboru medium obliczana jest średnica przewodu elektrycznego sieci tak aby nie został przekroczyony maksymalny dopuszczalnego spadku napięcia pomiędzy najbardziej oddalonymi węzłami. Obliczenia te uwzględniają nie tylko rezystancje przewodów sieci, ale również rezystancje wszystkich podłączonych odbiorników. Maksymalny spadek napięcia w sieci musi być na tyle mały by zapewnić prawidłowy poziomu sygnału w każdym węźle.

9.8.5. TOPOLOGIA SIECI

W celu eliminowania skutków odbicia sygnałów elektrycznych od końca linii, stosowane są tzw. terminatory. Terminatory zwierają obie linie sieci na jej obu końcach. Zasadniczą topografią sieci CAN jest topologia magistrali. Magistrala posiada linię główną i relatywnie krótkie odgałęzienia. Najkorzystniejszą relację pomiędzy prędkością komunikacji, a długością magistrali można uzyskać w topologii sieci jak najbardziej zbliżonej do prostoliniowej zakończonej terminatorami. Taka topologia nazywana jest również topografią łańcuchową.

Podobnie jak w innych sieciach także i w sieciach CAN stosowane są urządzenia pozwalające na wydłużenie zasięgu sieci, oraz umożliwiają integrację sieci CAN z innymi sieciami. Do urządzeń tych należą: wzmacniacze (ang. *repeaters*), mostki (ang. *bridges*) oraz bramy (ang. *gateways*).

Wzmacniacz (wzmacniak)

Zadaniem wzmacniacza jest regeneracja sygnału elektrycznego tłumionego i zniekształconego w medium komunikacyjnym. Wzmacniacz umożliwia zwiększenie zasięgu tej samej sieci. Z punktu widzenia przepływu informacji jest urządzeniem całkowicie pasywnym. Należy pamiętać, że wzmacniacz jest dodatkowym źródłem opóźnienia w propagacji sygnału. Wzmacniacz łączy sieci na poziomie warstwy 1 modelu ISO/OSI.

Mostek

Mostek łączy (zespala) odseparowane informacyjnie sieci na poziomie warstwy drugiej modelu ISO/OSI. Istotne w tym przypadku jest, aby identyfikatory wiadomości w obu sieciach były globalnie unikalne. Mostek jest elementem aktywnym sieci i może sterować przepływem informacji pomiędzy zespołonymi sieciami.

Brama

Brama łączy sieci o różnych rodzajach protokołów komunikacyjnych na poziomie warstwy 7 modelu ISO/OSI (warstwa aplikacji). Brama jest, podobnie jak mostek, elementem aktywnym, którego zadaniem jest translacja protokołów komunikacyjnych.

9.8.6. DOSTĘP DO MAGISTRALI

Bezpośredni dostęp do medium fizycznego (magistrali dwuprzewodowej) realizowany jest przy pomocy specjalnych układów zwanych sterownikami magistrali lub transceiverami¹⁰. Układ sterownika składa się z nadajnika oraz odbiornika. Sterownik w czasie nadawania wiadomości spełnia następujące zadania:

- dokonuje translacji poziomów napięć do poziomów zdefiniowanych dla stanów: recesywnego i dominującego
- zapewnia odpowiednią pojemność wyjściową układu,
- chroni układ nadajnika przed przeciążeniem prądowym i napięciowym,
- ogranicza poziom emisji elektromagnetycznej.

W czasie odbioru sterownik:

- zapewnia odpowiedni poziom sygnału w stanie recesywnym
- chroni układ komparatora wejściowego przed przepięciami na magistrali

Dodatkowo odbiornik wykrywa usterki na magistrali takie jak przerwanie linii, zwarcie przewodów, zwarcie do masy itd. Sterownik pozwala również na izolację galwaniczną węzła sieci CAN od magistrali.

9.8.7. UNORMOWANIA W ZAKRESIE WARSTWY FIZYCZNEJ

ISO 11898-2 (Sieć CAN o dużej prędkości)

Jest to najczęściej spotykany standard specyfikujący wymagania w stosunku do warstwy fizycznej. Zgodnie z tym standardem maksymalna możliwa do uzyskania prędkość transmisji wynosi 1Mbit/s przy długości magistrali nie dłuższej niż 40m. Do transmisji wykorzystywana jest magistrala dwuprzewodowa. Jeden przewód oznaczany jest symbolem CAN_H, drugi jest oznaczany symbolem CAN_L. Liczba węzłów jest ograniczona dopuszczalnym obciążeniem magistrali. Impedancja falowa przewodów wynosi 120Ω . Zakres dopuszczalnych napięć względem wspólnego potencjału odniesienia zawiera się w przedziale od -2V do +7V. Nominalny czas propagacji sygnału w sieci nie powinien przekraczać 5ns/m.

ISO 11898-3 (sieć CAN tolerująca uszkodzenia)

Ten standard jest najbardziej popularny w zastosowaniach w technice samochodowej. Ponieważ z założenia jest to sieć o krótkim zasięgu, to problem odbić sygnałów od końców przewodów nie jest istotny. Możliwa jest więc praca tej sieci zgodnej z tą specyfikacją bez konieczności stosowania terminatorów.

¹⁰ transceiver jest neologizmem powstały ze złożenia słów angielskich transmitter i receiver oznaczających odpowiednio nadajnik i odbiornik.

Pozwala to na użycie sterowników magistrali niskiej mocy, a co za tym idzie obniżenie poboru mocy. Specyfikacja ta dopuszcza stosowanie dowolnej topologii sieci. Sieć ma zdolności komunikacyjne nawet wówczas, gdy uszkodzeniu ulegnie jedna z linii magistrali. Norma ISO 11898-3 ogranicza maksymalną prędkość transmisji do 125kb/s. Określa również zależność dopuszczalnej długości magistrali jest zależna prędkości transmisji i obciążenia sieci. Zakres dopuszczalnych napięć względem wspólnego potencjału odniesienia zawiera się w przedziale od -2V do +7V. Dopuszczalne jest stosowanie do 32 węzłów w jednej sieci.

SAE J2411 (jednoprzewodowa sieć CAN)

Standard SAE J2411 definiuje sieci o niskich wymaganiach dotyczących zarówno prędkości transmisji jak i maksymalnej długości magistrali. Komunikacja odbywa się tylko przy użyciu jednego przewodu z prędkością 33,3kb/s (dla celów diagnostycznych dostępna jest też prędkość 83,3kb/s). Maksymalna liczba urządzeń sieciowych wynosi 32. Standard ten stosowany jest zwłaszcza do sterowania układami elektronicznymi służącymi do podniesienia komfortu jazdy w samochodach. Medium transmisyjnym jest jeden nie ekranowany przewód. Topologia sieci jest dowolna. Standard dopuszcza komunikację pomiędzy aktywnymi węzłami w sytuacji, gdy pozostałe pozostają w stanie uśpienia.

ISO 11992 (sieć CAN typu punkt-punkt)

Standard ten definiuje połączenie typu punkt-punkt np. pomiędzy ciągnikiem a przyczepą. W przypadku gdy jeden ciągnik posiada dwie przyczepy, to stosowane jest połączenie łańcuchowe (ang. *daisy-chain*). Nominalna prędkość transmisji w tej sieci jest ograniczona do 125 kbit/s przy maksymalnej dopuszczalnej długości magistrali o topologii łańcuchowej równej 40 m. Standard opisuje sposoby zarządzanie błędami oraz definiuje napięcie zasilania (12VDC lub 24VDC). Jako medium transmisyjne stosowana jest para nie ekranowanych przewodów.

Pozostałe standardy

Magistrala CAN wykorzystująca światłowody jako medium transmisyjne nie została jak dotąd objęta żadnym standardem. Głównym powodem są występujące problemy z silnym tłumieniem sygnału i stratami sygnału na złączach. Zalety sieci wykorzystujących światłowody polegają między innymi na tym, że są one odporne na zewnętrzne zakłócenia elektromagnetyczne oraz same ich nie emitują. Pozwala to na zastosowanie sieci światłowodowych w środowiskach o wysokim poziomie zakłóceń elektromagnetycznych. Całkowite odseparowanie galwaniczne pozwala również na stosowanie tego rodzaju sieci w środowiskach zagrożonych wybuchem.

9.9. WARSTWA ŁĄCZA DANYCH

9.9.1. WPROWADZENIE

W celu osiągnięcia przejrzystości i elastyczności w projektowaniu sieci, w warstwie łączącej danych w specyfikacji CAN zostały wyróżnione dwie podwarstwy zgodne z modelem ISO/OSI.



- Podwarstwa logicznego sterowania komunikacją LLC (*Logical Link Control*)
- Podwarstwa sterowania dostępem do warstwy fizycznej MAC (*Medium Access Control*)

| Warstwa łącza danych | |
|---|--|
| LLC | Filtrowanie wiadomości Informacja o przeciążeniach Zarządzanie odtwarzaniem inf. |
| MAC | Przygotowanie danych Kodowanie ramki (Stuffing / Destuffing) Wykrywanie błędów Sygnalizacja błędów Sygnalizacja potwierdzenia odbioru |
| Warstwa fizyczna | |
| Kodowanie / Dekodowanie bitów Taktowanie Synchronizacja | |
| Charakterystyki nadajnika / odbiornika | |

Zadania podwarstwy LLC są następujące:

- wspomaganie transmisji danych,
- filtrowanie wiadomości,
- zarządzanie powrotem do pracy w sieci (RECOVERY MANAGEMENT) oraz
- informowanie w przypadku wystąpienia przeciążenia.

Podwarstwa MAC odpowiada głównie za realizację procesu transmisji danych, a w szczególności za:

- podział danych na ramki,
- prowadzenie arbitrażu,
- kontrolę błędów,
- sygnalizację błędów,
- ograniczanie wpływu uszkodzeń na pracę sieci.

Na poziomie tej podwarstwy podejmowane są decyzje o możliwości podjęcia nowej transmisji lub odbioru. Również tu zdefiniowane są pewne wymagania dotyczące warunków taktowania procesu komunikacyjnego.

Rys. 9.7 Podstawowe funkcje realizowane przez podwarstwy LLC i MAC

9.9.2. PODSTAWOWE DEFINICJE

9.9.2.1. WIADOMOŚĆ

Wiadomość jest podstawowym obiektem wymiany informacji. Wiadomość jest generowana przez węzły sieci zgodnie ze specyfikacją warstwy łącza danych. Tworzona jest zgodnie z określonymi zasadami i ustalonym formatem. Wiadomość jest ograniczona co do swojej długości. Wiadomości mogą być transmitowane wówczas, gdy magistrala komunikacyjna nie jest zajęta.

9.9.2.2. ZARZĄDZANIE PRZEPŁYWEM INFORMACJI

Węzły w sieci CAN nie posiadają i nie przechowują żadnych informacji dotyczących konfiguracji sieci. Jest kilka istotnych konsekwencji takiego stanu rzeczy.

Elastyczność

Sieć CAN może być rozbudowywana o nowe węzły bez konieczności dokonywania jakichkolwiek zmian w oprogramowaniu czy też konfiguracji sprzętowej żadnego z istniejących już węzłów. Nie są konieczne również zmiany w warstwie aplikacyjnej.



Selektywność

Każda wiadomość posiada IDENTYFIKATOR. Identyfikator odwołuje się do stopnia istotności wiadomości. Identyfikator nie zawiera informacji dotyczących miejsca (adresu) przeznaczenia wiadomości. Dzięki temu każdy węzeł sieci może sam decydować (przy użyciu funkcji filtrowania wiadomości) czy transmitowana wiadomość jest mu przydatna, czy też nie.

Tryb pracy równoległej węzłów (multicast)

Dzięki zastosowaniu mechanizmu filtrowania wiadomości, dowolna liczba węzłów może jednocześnie odbierać, przetwarzać i wykonywać polecenia zawarte w tej samej wiadomości.

Gwarancja zgodności danych

Specyfikacja sieci CAN gwarantuje, że wewnątrz sieci wiadomość będzie zaakceptowana przez wszystkie węzły albo nie zaakceptuje jej żaden z nich. Taką właściwość udało się uzyskać dzięki wykorzystaniu trybu MULTICAST oraz odpowiedniemu zarządzaniu błędami.

9.9.2.3. PRĘDKOŚĆ TRANSMISJI

Prędkość transmisji w sieciach CAN może być różna. Prędkość ta musi być jednak identyczna dla wszystkich węzłów w obrębie tej samej sieci.

9.9.2.4. PRIORYTET WIADOMOŚCI

IDENTYFIKATOR określa priorytet wiadomości. Priorytet wiadomości jest istotny w początkowej fazie wysyłania wiadomości, ponieważ w tej fazie rozgrywany jest arbitraż. W przypadku zaistnienia konfliktu w sieci będzie rozpowszechniona wiadomość o najwyższym priorytecie.

9.9.2.5. ŻĄDANIE TRANSMISJI DANYCH

W przypadku, gdy określony węzeł sieci potrzebuje wiadomości (danych) z innego węzła sieci, to może wysłać odpowiednio sformatowaną wiadomość zwaną żądaniem transmisji lub ramką żądania transmisji (REMOTE FRAME). W odpowiedzi generowana jest wiadomość z żądaną informacją w postaci ramki danych (DATA FRAME). Identyfikatory obu tych wiadomości są identyczne.

9.9.2.6. TRYB MULTIMASTER

Każdy węzeł ma prawo rozpoczęć transmisję wiadomości, o ile medium transmisyjne jest niezajęte. Dostęp do magistrali uzyskuje węzeł generujący wiadomość o najwyższym priorytecie.

9.9.2.7. ARBITRAŻ

Jeżeli dwa lub więcej węzłów sieci rozpoczęte transmisję wiadomości w tym samym momencie, to wystąpi konflikt dostępu do medium. Konflikt ten jest rozstrzygany w procesie nieniszczącego arbitrażu. W przypadku jednoczesnego rozpoczęcia transmisji ramek wiadomości o tym samym identyfikatorze (ramki danych i żądania transmisji) arbitraż wygrywa ramka danych. Podczas arbitrażu, każdy nadajnik każdego węzła dla każdego wysyłanego bitu porównuje wartość stanu logicznego wysyłanej wiadomości ze stanem logicznym odbieranym z sieci. Jeżeli obie wartości są identyczne, to węzeł może kontynuować nadawanie. W przypadku przeciwnym węzeł automatycznie zawiesza tryb

nadawania i przechodzi w tryb odbioru informacji. Arbitraż rozgrywany jest wyłącznie w czasie trwania transmisji identyfikatorów wiadomości.

9.9.2.8. BEZPIECZEŃSTWO PRZESYŁANYCH INFORMACJI

Każdy węzeł posiada zaimplementowane procedury służące do detekcji, sygnalizacji i kontroli błędów transmisji.

9.9.2.9. KONTROLA BŁĘDÓW TRANSMISJI

Kontrola błędów transmisji jest wieloetapowa. Służą jej:

- porównanie stanu logicznego wysyłanego bitu ze stanem logicznym w medium,
- generowanie cyklicznej redundancyjnej sumy kontrolnej CRC (**Cyclic Redundancy Check**),
- technika kodowania bitów synchronizacyjnych (*bit stuffing*),
- kontrola integralności ramki.

9.9.2.10. SKUTECZNOŚĆ MECHANIZMU DETEKCJI BŁĘDÓW

Mechanizm detekcji błędów ma następujące właściwości:

- wykrywa wszystkie błędy globalne,
- wykrywa wszystkie błędy lokalne nadajnika,
- wykrywanych jest do 5 przypadkowo zaistniałych błędów w wiadomości,
- wykrywane są błędy ciągu danych o długości mniejszej niż 15 bitów,
- wykrywana jest każda nieparzysta liczba błędnych bitów.

Prawdopodobieństwo p nie wykrycia uszkodzonej ramki jest mniejsze niż

$$p = x \cdot 4,7 \cdot 10^{-11}$$

gdzie: x jest stopą błędu wiadomości.

9.9.2.11. SYGNALIZACJA BŁĘDÓW I CZAS POWROTU DO NORMALNEJ PRACY

Zadaniem węzła, który wykryje uszkodzoną wiadomość jest natychmiastowe zasygnalizowanie takiego zdarzenia. Uszkodzona wiadomość jest anulowana i automatycznie transmitowana ponownie. Maksymalny interwał czasowy upływający pomiędzy wykryciem błędu i ponownym rozpoczęciem transmisji jest równy czasowi transmisji 31 bitów (o ile nie pojawią się kolejne błędy).

9.9.2.12. AUTOMATYCZNE WYKLUCZANIE USZKODZEŃ TRWAŁYCH (FAULT CONFIRMATION)

Węzły sieci CAN mają możliwość odróżnienia krótkich zakłóceń od uszkodzeń trwałych. Uszkodzone węzły mogą być wyłączane.

9.9.2.13. POŁĄCZENIA

Szeregowa sieć CAN pozwala na dołączenie teoretycznie nieograniczonej liczby urządzeń. Praktycznie, liczba dołączonych urządzeń jest limitowana przez dopuszczalne czasy opóźnienia sygnału w sieci oraz dopuszczalne obciążenie prądowe tranceiverów.

9.9.2.14. WARTOŚCI/POZIOMY SYGNAŁU MAGISTRALI

Sygnal CAN może przyjmować tylko jeden z dwóch komplementarnych stanów logicznych: dominujący lub recesywny. W przypadku jednoczesnej transmisji bitu recesywnego i dominującego stan logiczny magistrali przyjmuje wartość bitu dominującego. Parametry techniczne (np. poziomy napięć) reprezentujące stany logiczne nie są przedmiotem ogólnej specyfikacji i są specyficzne dla wybranej warstwy fizycznej.

9.9.2.15. SYGNALIZACJA POTWIERDZENIA ODBIORU ACK (ACKNOWLEDGEMENT)

Każdy odbiornik wiadomości sprawdza jej zawartość i potwierdza jej zgodność lub sygnalizuje błąd.

9.9.2.16. TRYB UŚPIENIA WĘZŁA (SLEEP MODE / WAKE-UP)

W celu zmniejszenie zużycia energii, węzły sieci CAN mogą przechodzić w stan uśpienia. W tym stanie zostaje zawieszona zarówno komunikacja z medium transmisyjnym jak i wewnętrzna aktywność węzła. Węzeł może być wprowadzony ze stanu uśpienia w wyniku wystąpienia określonej aktywności w sieci lub też w wyniku działania układu sterowania węzła. Bezpośrednio po wyjściu ze stanu uśpienia, warstwa MAC rozpoczyna proces przygotowania węzła do pracy w sieci. W czasie przygotowania warstwa MAC oczekuje najpierw na ustabilizowanie się generatora podstawy czasu węzła, a następnie dokonuje synchronizacji węzła z magistralą sprawdzając 11 kolejnych bitów recesywnych. Dopiero po realizacji tych operacji następuje logiczne dołączenie węzła i definitive zakonczenie trybu uśpienia węzła.

9.9.3. TRANSMISJA WIADOMOŚCI

9.9.3.1. FORMAT RAMKI

Rozróżniane są dwa formaty ramki różniące się między sobą polem IDENTYFIKATORA (IDENTIFIER).

- Ramka z identyfikatorem 11 bitowym – oznacza ramkę standardową
- Ramka z identyfikatorem 29 bitowym - oznacza ramkę rozszerzoną

9.9.3.2. RODZAJE RAMEK

Rozróżniane są cztery rodzaje ramek transmitujących wiadomości:

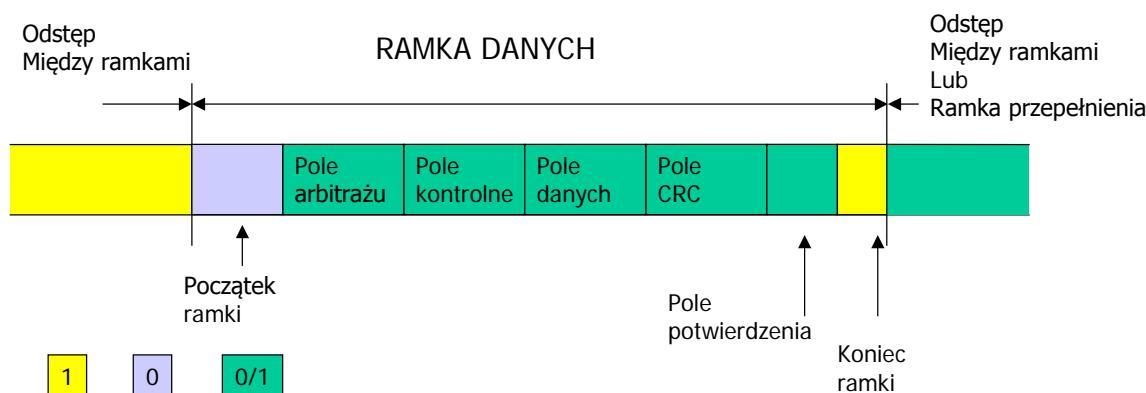
- Ramka danych (*DATA FRAME*) przeznaczona do transmisji wiadomości przez węzeł nadawczy do węzłów odbiorczych,
- Ramka żądania transmisji (*REMOTE FRAME*) przeznaczona do zainicjowania transmisji ramki danych z węzła o wskazanym przez nią identyfikatorze,
- Ramka sygnalizacji błędu (*ERROR FRAME*) przeznaczona do sygnalizacji błędu. Może być transmitowana przez każdy węzeł sieci, który dokonał detekcji błędu transmisji,
- Ramka przepełnienia (*OVERLOAD FRAME*) przeznaczona do generacji w sieci dodatkowego opóźnienia (zwłoki czasowej) pomiędzy kolejnymi ramkami danych lub ramkami żądania transmisji.

Ramka danych oraz ramka żądania transmisji mogą występować w obu formatach ramek, a więc zarówno w przypadku formatu standardowego jak i w przypadku formatu rozszerzonego. Pomiędzy ramkami transmisyjnymi wprowadzane są przerwy czasowe (INTERFRAME SPACE).

9.9.3.3. RAMKA DANYCH (DATA FRAME)

Ramka danych składa się z siedmiu pól:

- | | |
|-------------------------|-------------------|
| 1. Początek ramki | START OF FRAME |
| 2. Pole arbitrażu | ARBITRATION FIELD |
| 3. Pole kontrolne | CONTROL FIELD |
| 4. Pole danych | DATA FIELD |
| 5. Pole sumy kontrolnej | CRC FIELD |
| 6. Pole potwierdzenia | ACK FIELD |
| 7. Koniec ramki | END OF FRAME |



Rys. 9.8 Ramka danych

9.9.3.4. POCZĄTEK RAMKI SOF (START OF FRAME)

Początek ramki występuje zarówno w przypadku transmisji ramki standardowej i rozszerzonej. SOF oznacza początek ramki danych i ramki żądania transmisji. SOF jest realizowany w postaci pojedynczego stanu dominującego.

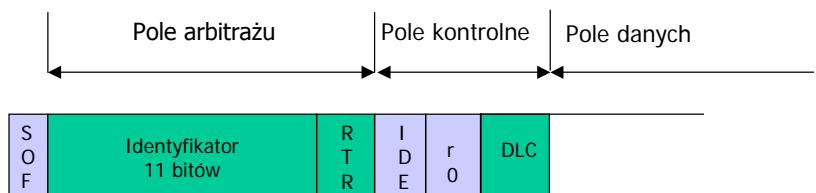
Dowolny węzeł sieci może rozpoczęć transmisję tylko wówczas, gdy magistrala znajduje się w stanie czuwania. Wszystkie węzły sieci muszą zsynchronizować się z narastającym zboczem sygnału SOF tego węzła, który jako pierwszy rozpoczyna proces nadawania ramki danych lub ramki żądania transmisji.

9.9.3.5. POLE ARBITRAŻU (ARBITRATION FIELD)

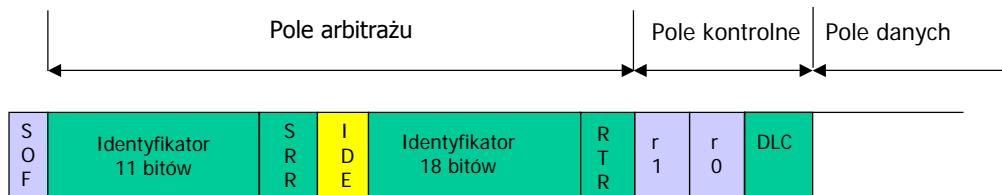
Format pola arbitrażu jest zależny od formatu ramki (standardowa czy rozszerzona).

- W transmisji ramki w formacie standardowym pole to składa się z 11 bitowego identyfikatora oraz bitu zwanego *RTR-BIT*. Bit identyfikatora oznaczane są kolejno *ID-28...ID-18*,
- W transmisji ramki w formacie rozszerzonym pole to składa się z 29 bitowego identyfikatora oraz bitów zwanych *SRR-BIT*, *IDE-BIT* i *RTR-BIT*. Kolejne bity identyfikatora oznaczane są *ID-28...ID-0*.

Standardowy format ramki



Rozszerzony format ramki



Rys. 9.9 Pole arbitrażu w ramce w formacie standardowym i rozszerzonym

9.9.3.6. IDENTYFIKATOR

RAMKA STANDARDOWA

Długość identyfikatora w ramce standardowej wynosi 11 bitów i odpowiada tak zwanej bazie (ang. *base ID*) w ramce rozszerzonej. Transmisja identyfikatora rozpoczyna się począwszy od bitu ID-28 i kończy się na bicie ID-18. ID-18 jest najmniej znaczącym bitem LSB (ang. *Least Significant Bit*).

Uwaga: Identyfikator nie może przyjmować wartości recesywnych jednocześnie na siedmiu najbardziej znaczących bitach (ID-28 .. ID-22).

RAMKA ROZSZERZONA

Ramka rozszerzona składa się z 29 bitów. Podzielona jest na następujące pola

- Identyfikator podstawowy (ang. *base ID*) – 11 bitów
- Identyfikator rozszerzony (ang. *extended ID*) – 18 bitów

Identyfikator podstawowy odpowiada identyfikatorowi ramki w formacie standardowym. W ramce rozszerzonej decyduje o podstawowym priorytecie wiadomości.

Identyfikator rozszerzony zawiera pozostałe 18 bitów, transmitowanych w kolejności od ID-17 do ID-0.

W ramce standardowej po **IDENTYFIKATORZE** występuje zawsze bit RTR. Bit RTR występuje zarówno w ramce standardowej jak i rozszerzonej.

Bit RTR (ang. *Remote Transmission Request* – zdalne żądanie transmisji)

- W ramce danych bit RTR musi być *dominujący*
- W ramce zdalnego żądania transmisji REMOTE FRAME bit RTR musi być *recesywny*

W przypadku ramki rozszerzonej najpierw transmitowane jest *Base ID*, a po nim występują dwa bity: SRR (ang. **S**ubstitute **R**emote **R**equest) oraz IDE (ang. **I**dentifier **E**xtension **B**it).

Bit SRR (ramka rozszerzona)

Bit SRR jest bitem recesywnym. W ramce rozszerzonej transmitowany jest na pozycji bitu RTR ramki standardowej, dlatego też nazywany jest jego substytutem. Pozwala to na uniknięcie kolizji w przypadku, gdy ramka standardowa i rozszerzona mają identyczną bazę *Base ID*. W tym przypadku w ramka standardowa wygrywa arbitraż (RTR jest bitem dominującym).

Bit IDE

Dodatkowy bit identyfikatora IDE w zależności od rodzaju ramki znajduje się w:

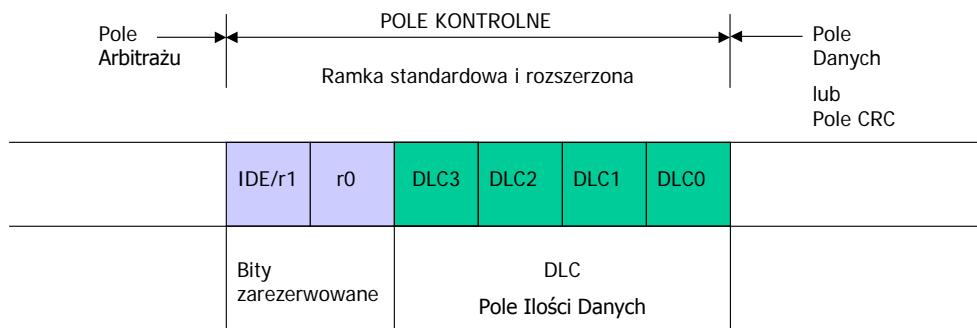
- polu arbitrażu, w przypadku ramki rozszerzonej, lub
- polu kontrolnym w przypadku ramki standardowej.

Bit IDE w ramce standardowej jest „dominujący” zaś w rozszerzonej „recesywny”.

9.9.3.7. POLE KONTROLNE (CONTROL FIELD)

Pole kontrolne występuje zarówno w ramce rozszerzonej jak i w standardowej. Pole to składa się z sześciu bitów (rys. 4.10).

- W ramce standardowej pole to zawiera kod długości pola danych DLC (ang. **D**ata **L**ength **C**ode), bit IDE (dominujący) oraz bit rezerwowy r0.
- W ramce rozszerzonej pole to zawiera kod długości pola danych DLC, dwa rezerwowe bity r1 i r0. Podczas nadawania obydwa bity rezerwowe powinny być dominujące. Jakkolwiek odbiornik wiadomości musi zaakceptować dowolną ich kombinację.



Rys. 9.10 Pole kontrolne

Kod *długości pola danych* *DLC* jest czterobitowym polem określającym liczbę bajtów występujących w *polu danych* (ang. **DATA FIELD**). Sposób kodowania liczby bajtów w DLC podano w tabeli 9.1.

Tabela 9.1 Sposób kodowania liczby bajtów w polu kontrolnym

| Liczba bajtów danych | Wartości poszczególnych bitów DLC | | | |
|----------------------|-----------------------------------|------|------|-------|
| | DLC3 | DLC2 | DLC1 | DLC0: |
| 0 | d | d | d | d |
| 1 | d | d | d | r |
| 2 | d | d | r | d |
| 3 | d | d | r | r |
| 4 | d | r | d | d |
| 5 | d | r | d | r |
| 6 | d | r | r | d |
| 7 | d | r | r | r |
| 8 | r | d | d | d |

Oznaczenia:

d - bit dominujący

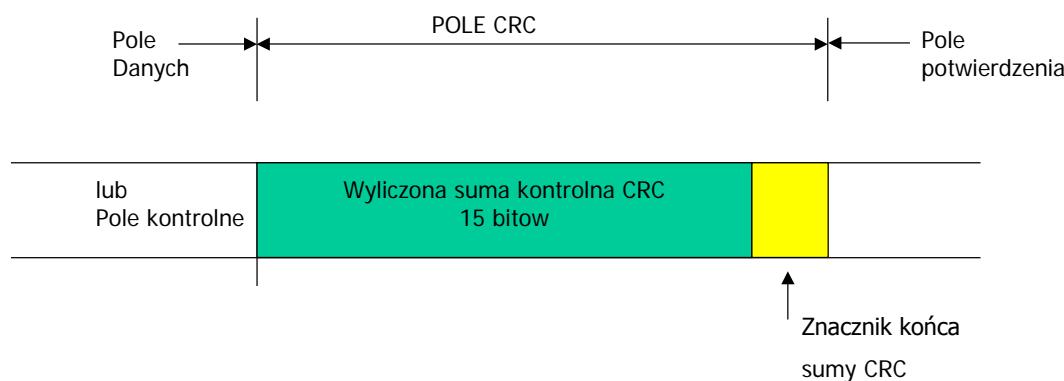
r – bit recesywny

9.9.3.8. POLE DANYCH (DATA FIELD)

Pole danych (ang. *DATA FIELD*) występuje zarówno w ramce standardowej jak i w rozszerzonej. POLE DANYCH zawiera informacje, które są transmitowane w RAMCE DANYCH. Może zawierać od 0 do 8 bajtów. Każdy bajt liczy 8 bitów. Najbardziej znaczący bit MSB (ang. *Most Significant Bit*) w każdym bajcie jest nadawany jako pierwszy.

9.9.3.9. POLE SUMY KONTROLNEJ (CRC FIELD)

Pole sumy kontrolnej CRC występuje zarówno w ramce standardowej jak i w rozszerzonej. Pole to zawiera wyliczoną sumę kontrolną w części: *CRC SEQUENCE* oraz bit końca sumy kontrolnej *CRC DELIMITER* (rys. 4.11) zwany również znacznikiem końca sumy CRC.



Rys. 9.11. Pole sumy kontrolnej CRC

Algorytm wyznaczania wartości sumy kontrolnej jest algorymem cyklicznej kontroli nadmiarowej CRC przeznaczonym dla ramek liczących nie więcej niż 127 bitów. W celu wyliczenia wartości CRC zdefiniowano najpierw wielomian generacyjny. Następnie tworzony jest wielomian składający się utworzonego z kolejnych bitów nadowanej ramki tzn. składający się z: SOF, ARBITRAION FIELD, CONTROL FIELD, DATA FIELD oraz dodatkowych piętnastu bitów o wartości zerowej. Bity dodatkowe uzupełniające wtrącone w

procesie nadawania informacji (*bit stuffing*) nie są brane pod uwagę. Wielomian ten jest dzielony (operacja dzielenia modulo 2) przez wielomian generacyjny:

$$x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^4 + x^3 + x^1$$

W wyniku podziału obu wielomianów uzyskiwana jest wartość CRC SEQUENCE. Do implementacji można zastosować algorytm podany poniżej.

Algorytm wyznaczania CRC

Niech *CRC_RG(14:0)* oznacza rejestr przechowujący wartość sumy kontrolnej CRC, natomiast *NXTBIT* oznacza kolejny bit transmitowanego ciągu bitów począwszy od SOF i skończywszy na DATA FIELD. Suma CRC obliczana jest następująco:

```

CRC_RG = 0;
REPEAT
    CRCNXT = NXTBIT EXOR CRC(14)
    CRC_RG(14:1) = CRC_RG(13:0);
    CRC_RG(0) = 0;
    IF CRCNXT THEN
        CRC_RG(14:0) = CRC_RG(14:0) EXOR (4599hex);
    ENDIF
UNTIL (zostanie osiągnięte CRC SEQUENCE lub wystąpi jeden z błędów transmisji)

```

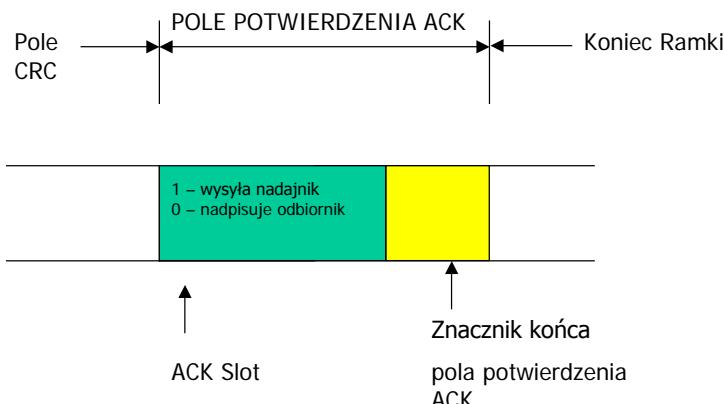
Po transmisji lub odebraniu ostatniego bitu pola danych DATA FIELD rejestr CRC_RG zawiera sekwencję CRC SEQUENCE.

Znacznik końca pola CRC (ang. *CRC DELIMITER*) występuje zarówno w ramce standardowej jak i rozszerzonej. Znacznik końca pola CRC jest transmitowany po sekwencji CRC SEQUENCE i m zawsze wartość bitu recesywnego.

9.9.3.10. POLE POTWIERDZENIA ACK (ACK FIELD)

Pole potwierdzenia odebrania wiadomości ACK FIELD występuje zarówno w ramce zwykłej jak i rozszerzonej. Pole ACK FIELD składa się z dwóch bitów (rys. 4.12). Pole to składa się bitu potwierdzenia ACK SLOT oraz bitu znacznika końca pola ACK ACK DELIMITER. W polu ACK FIELD węzeł nadający transmituje dwa bity recesywne. Węzeł odbiorczy, który odbierze prawidłową ramkę potwierdza odbiór wysyłając bit dominujący w przedziale czasu przeznaczonym na ACK SLOT.





Rys. 9.12 Pole potwierdzenia ACK

ACK DELIMITER

ACK DELIMITER jest znacznikiem końca dwubitowego pola ACK FIELD. Przyjmuje stan recesywny. W rezultacie, okno ACK SLOT jest otoczone przez dwa bity recesywne (CRC DELIMITER oraz ACK DELIMITER).

9.9.3.11. KONIEC RAMKI (END OF FRAME)

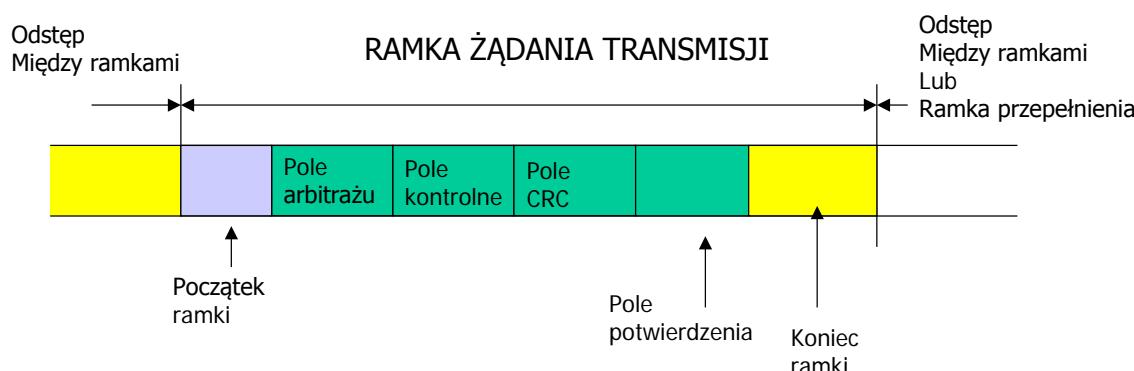
Koniec ramki EOF (ang. **END OF FRAME**) występuje w ramce standardowej oraz w ramce rozszerzonej. Każda ramka (zarówno ramka danych, jak i ramka żądania transmisji) jest zakończona polem EOF składającym się z sekwencji 7 bitów recesywnych.

9.9.4. RAMKA ŻĄDANIA TRANSMISJI (REMOTE FRAME)

Węzły sieci pracujące w trybie odbiorczym mogą inicjować transfery niezbędnych im danych pochodzących z innych węzłów wysyłając *Ramkę Żądania Transmisji* (ang. **REMOTE FRAME**). Ramka żądania transmisji występuje w zarówno w trybie transmisji ramki standardowej jak również w trybie transmisji ramki rozszerzonej. W obydwu przypadkach składa się 6 różnych pól bitowych (rys. 9.14):

1. Pole początku ramki – START OF FRAME
2. Pole arbitrażu – ARBITRATION FIELD
3. Pole kontrolne – CONTROL FIELD
4. Pole sumy kontrolnej – CRC FIELD
5. Pole potwierdzenia odbioru – ACK FIELD
6. Pole końca ramki – END OF FRAME.

W przeciwieństwie do *ramki danych*, bit RTR w ramce żądania transmisji przyjmuje stan recesywny. Nie występuje również pole danych DATA FIELD i to bez względu na wartość jaką przyjmuje pole *DLC* (dopuszalne są wartości od 0 do 8). W tym przypadku wartość pola *DLC* odpowiada *DLC* ramki danych, która będzie odpowiedziała na żądanie transmisji.



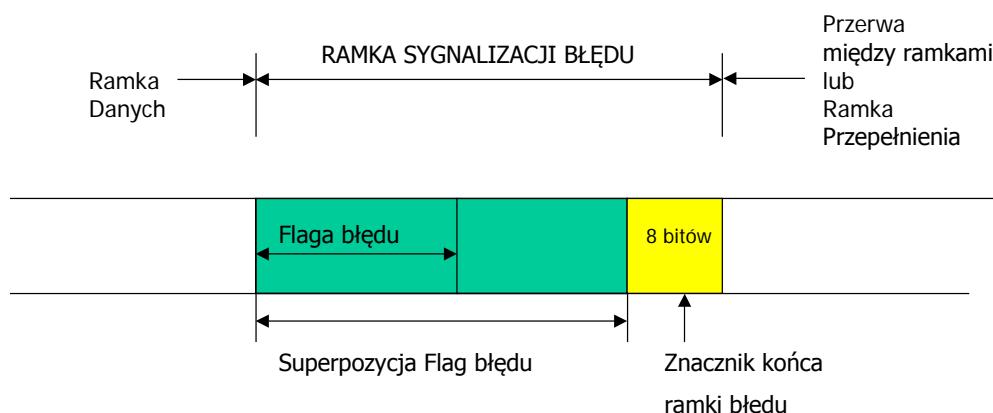
Rys. 9.13 Ramka żądania transmisji

O tym czy ramka jest *ramką danych* czy też *ramką żądania transmisji* decyduje wartość bitu RTR, który jest:

- recesywny – w ramce zdalnego żądania transmisji (REMOTE FRAME),
- dominujący – w ramce danych (DATA FRAME).

9.9.5. RAMKA SYGNALIZACJI BŁĘDU (ERROR FRAME)

Ramka sygnalizacji błędu (ang. *ERROR FRAME*) (rys. 9.14) składa się z dwóch pól. Pierwsze z nich powstaje jako superpozycja znaczników błędu *ERROR FLAGS* pochodzących z różnych węzłów. Drugie pole jest znacznikiem końca ramki (ang. *ERROR DELIMITER*).



Rys. 9.14 Ramka sygnalizacji błędu transmisji

W celu poprawnego zakończenia ramki błędu *ERROR FRAME*, węzeł pracujący w trybie *error passive* wymaga aby magistrala znajdowała się w trybie czuwania przez czas potrzebny na transmisję przynajmniej 3 bitów, co ma np. miejsce w przypadku wystąpienia lokalnego błędu w tym węźle. Z tego powodu sieć CAN nie powinna nigdy pracować przy 100% obciążeniu.

Flaga błędu (*ERROR FLAG*)

Rozróżniane są 2 rodzaje flag błędów:

1. aktywna (ACTIVE ERROR FLAG) – składająca się z sześciu kolejnych bitów dominujących.
2. pasywna (PASSIVE ERROR FLAG) – składająca się z sześciu kolejnych bitów recesywnych (chyba że zostaną one zdominowane przez dominujący bit innego węzła).

Węzeł pracujący jako *error active* sygnalizuje wykrycie błędu wysyłając aktywną flagę błędu. Flaga błędu narusza reguły kodowania danych (*bit stuffing*) stosowane dla wszystkich pól począwszy od SOF do CRC DELIMITER lub też niszczy ustaloną postać ACK FIELD lub EOF. W wyniku takiego działania wszystkie węzły sieci wykrywają błąd i rozpoczynają transmisje ERROR FLAGS. Stąd właśnie pole ERROR FLAG jest superpozycją bitów dominujących pochodzących z różnych węzłów. Faktyczna długość tej sekwencji bitów waha się w przedziale <6..12>.

Węzeł pracujący w trybie *error passive* sygnalizuje wykrycie błędu transmitując PASSIVE ERROR FLAG. Flaga ta uznawana jest za kompletną wtedy, gdy urządzenie transmitujące ją wyśle i jednocześnie odczyta 6 kolejnych bitów o tej samej wartości.

Znacznik końca ramki (ERROR DELIMITER)

Znacznik końca ramki składa się z 8 kolejnych bitów recesywnych. Po transmisji flagi błędu ERROR FLAG, każde urządzenie transmituje bit recesywny i jednocześnie monitoruje magistralę czy taki bit na niej się pojawił, a następnie transmituje pozostałe 7 bitów recesywnych.

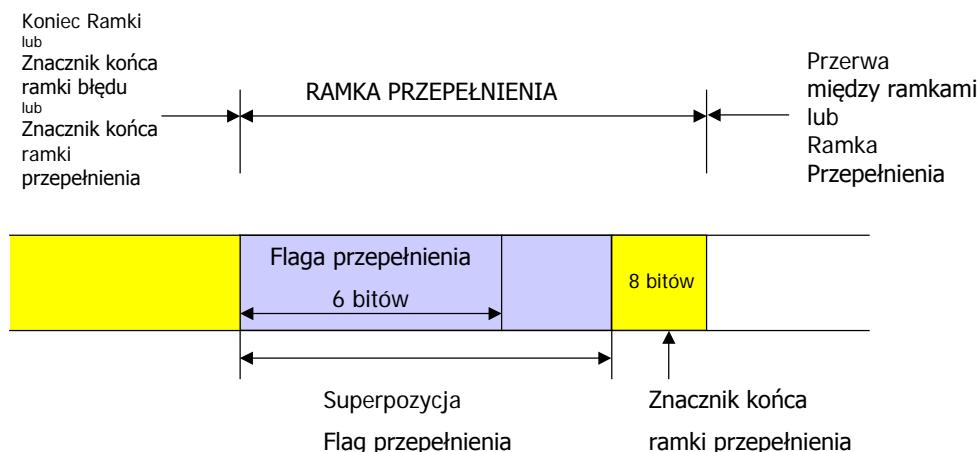
9.9.6. RAMKA PRZEPEŁNIENIA (OVERLOAD FRAME)

Ramka przepełnienia (OVERLOAD FRAME) składa się z dwóch pól: OVERLOAD FLAG oraz OVERLOAD DELIMITER (rys. 4.15). Rozróżniane są trzy przypadki przepełnienia prowadzące do wysłania OVERLOAD FLAG:

1. stan, w którym węzeł odbierający dane wymaga czasu przed odebraniem kolejnej ramki danych lub ramki żądania transmisji,
2. stan, w którym wykryty zostanie bit dominujący w pierwszym i drugim bicie INTERMISSION,
3. jeżeli węzeł pracujący w sieci CAN zarejestruje w ramce ERROR DELIMITER lub też OVERLOAD DELIMITER ósmy bit jako dominujący i rozpoczęcie transmisję ramki przepełnienia OVERLOAD FRAME zamiast ramki błędu ERROR FRAME. Wówczas nie zwiększy się także wartość licznika błędów.

W przypadku wystąpienia sytuacji opisanej w punkcie 1 rozpoczęcie transmisji ramki przepełnienia jest możliwe tylko z pierwszym bitem oczekiwanej przerwy (INTERMISSION). W pozostałych dwóch przypadkach transmisja rozpoczyna się w z przerwą jednobitową po zarejestrowaniu bitu dominującego.

Dopuszczalne jest wygenerowanie, co najwyżej 2 ramek przepełnienia w celu opóźnienia transmisji kolejnych ramek danych lub ramki żądania transmisji.



Rys. 9.15 Ramka przepełnienia

OVERLOAD FLAG

Flaga przepełnienia składa się z sześciu bitów dominujących i jest zgodna z ACTIVE ERROR FLAG. Kolejność w jakiej w ramce przepełnienia transmitowane są bity niszczy ustalony schemat pola przerwy INTERMISSION. W konsekwencji tego wszystkie węzły sieci również rejestrują warunek przepełnienia i rozpoczynają transmisje flagi przepełnienia. Wykrycie bitu dominującego jako trzeciego bitu podczas przerwy (INTERMISSION) interpretowane jest jako start (SOF) nadawania nowej ramki.

UWAGI:

Kontrolery, które mają zaimplementowany moduł CAN w wersji protokołu 1.0 lub 1.1 w odmienny sposób interpretują trzeci bit w polu przerwy (INTERMISSION). W przypadku wykrycia bitu dominującego następuje przyjęcie pierwszego bitu z sekwencji sześciu, jako bitu startu nowej ramki SOF. Szósty bit dominujący naruszy reguły kodowania bitów i spowoduje wystąpienie błędu.

Znacznik końca ramki przepełnienia (ang. OVERLOAD DELIMITER) składa się z 8 bitów recesywnych. Znacznik końca ramki przepełnienia ma taką samą budowę jak znacznik końca ramki błędu ERROR DELIMITER. Po wysłaniu flagi przepełnienia OVERLOAD FLAG, węzły monitorują sieć dopóki nie zarejestrują zmiany bitu dominującego na recesywny. Od tej chwili wszystkie sieciowe kończą nadawanie flagi przepełnienia OVERLOAD FLAG i jednocześnie rozpoczynają transmisję siedmiu kolejnych bitów recesywnych.

9.9.7. PRZERWA MIEDZY RAMKAMI (INTERFRAME SPACING)

Ramki danych DATA FRAME oraz ramki żądania transmisji REMOTE FRAME są oddzielane od poprzedzających je (bez względu na rodzaj ramki poprzedzającej) ciągiem bitów zwanym INTERFRAME SPACE. Przerwa ta nie występuje przed ramkami przepełnienia oraz błędu (OVERLOAD oraz ERROR FRAME). Nie oddziela też ona występujących po sobie kolejno dwóch ramek przepełnienia OVERLOAD FRAME (w przypadku, gdy taka transmisja wystąpi). Przerwa między ramkami (ang. INTERFRAME SPACE) składa się z pola przerwy (ang. INTERMISSION) oraz pola czuwania (ang. BUS IDLE) (rys. 9.16) i pola zawieszenia transmisji (ang. SUSPEND TRANSMISSION) dla węzłów pracujących w trybie pasywnym (*error passive*).

Dla węzłów, które nie pracują w trybie *error passive* lub były odbiorcą poprzedniej wiadomości obowiązuje przerwa jak na rys. 9.16.



Rys. 9.16 Przerwa pomiędzy ramkami I

Dla węzłów, które pracują w trybie *error passive* i były nadawcą poprzedniej wiadomości obowiązuje przerwa jak na rys. 9.17.



Rys. 9.17 Przerwa między ramkami II

INTERMISSION

Pole przerwy *INTERMISSION* składa się z kolejnych 3 bitów recesywnych. Jedyną akcją, jaka może być podjęta w czasie trwania przerwy *INTERMISSION* jest sygnalizacja przepelenienia *OVERLOAD*. Rozpoczęcie transmisji danych lub żądania transmisji, jest w takiej sytuacji niedozwolone.

Uwaga: Jeżeli węzeł sieci CAN, który posiada wiadomość oczekującą na wysłanie, wykryje bit dominujący na trzeciej pozycji pola *INTERMISSION*, to zinterpretuje go jako *SOF* i rozpoczęcie nadawanie poczynając od pierwszego bitu pola *IDENTIFIER* (z pominięciem bitu *SOF*).

Tryb czuwania magistrali (BUS IDLE)

Czas przebywania sieci w trybie czuwania nie jest możliwy do zdefiniowania. Jeżeli węzły wykryją, że sieć jest w stanie czuwania, to mogą w każdej chwili rozpocząć transmisję. Wiadomość, która oczekuje na wysłanie, jest transmitowana bezpośrednio po wystąpieniu przerwy *INTERMISSION*.

Zawieszenie transmisji (SUSPEND TRANSMISSION)

Węzeł, który pracuje w trybie *error passive*, po wysłaniu wiadomości, wysyła dodatkowo osiem bitów recesywnych zaraz po wystąpieniu przerwy INTERMISSION, a przed rozpoczęciem kolejnej transmisji lub wykryciu trybu czuwania w sieci. Jeżeli w tym czasie jakiś węzeł rozpoczęnie nadawanie, to węzeł pracujący w trybie *error passive* rozpocznie odbiór tej wiadomości.

9.10. WYMAGANIA STAWIANE BUDOWIE RAMKI

Opisany powyżej format ramki standardowej jest zgodny ze specyfikacją CAN 1.2. Ponieważ pojawiła się również specyfikacja ramki rozszerzonej, to ze względu na zachowanie zgodności wstępnej wymaga się aby:

- każdy nowy kontroler CAN wspierał bezwzględnie standardowy format ramki,
 - każdy nowy kontroler CAN mógł odbierać wiadomości formatu rozszerzonego,
 - ramki rozszerzone nie były uznawane za błędne z powodu swojego formatu,
- Nie jest jednak wymagane, aby nowe kontrolery CAN wspierały ramki rozszerzone.

9.11. NADAJNIK I ODBIORNIK

NADAJNIK

Nadajnik jest węzłem tworzącym wiadomość. Węzeł pozostaje nadajnikiem tak długo jak długo sieć nie przejdzie w tryb czuwania lub też przegra arbitraż.

ODBIORNIK

Odbiornik jest węzłem, który nie jest nadajnikiem wiadomości, a sieć nie znajduje się w trybie czuwania.

9.12. FILTROWANIE WIADOMOŚCI

Wiadomości filtrowane są w oparciu o pełny identyfikator wiadomości. Dzięki zastosowaniu opcjonalnego rejestru maskującego możliwe jest skonfigurowanie operacji filtrowania w taki sposób, żeby przepuszczane były wszystkie wiadomości lub wybrane grupy wiadomości. W przypadku gdy w węźle zostanie zaimplementowany rejestr maskujący, to wymaga się, aby każdy bit tego rejestru był w pełni programowalny (musi istnieć możliwość zablokowania lub odblokowania operacji filtrowania). Długość rejestru maski powinna odpowiadać calementu identyfikatorowi bądź tylko jego fragmentom.

9.13. KLASYFIKACJA WIADOMOŚCI

W zależności od aktualnego trybu pracy węzła (nadajnik czy odbiornik) moment w którym wiadomość zostaje uznana za poprawną jest różny.

Nadajnik

Nadajnik uznaje wiadomość za poprawną, jeżeli nie zostanie zarejestrowany żaden błąd do momentu transmisji EOF. Jeżeli wiadomość zostanie uznana za błędnią, to automatycznie zostanie przeprowadzona retransmisja wiadomości. Retransmisja musi być przeprowadzona natychmiast po przejściu sieci wejdzie w tryb czuwania, tak aby umożliwić oczekującej wiadomości rywalizację o dostęp do sieci z pozostałymi wiadomościami.

Odbiornik

Odbiornik uznaje wiadomość za poprawną, jeżeli nie zarejestruje żadnego błędu aż do przedostatniego bitu pola EOF. Ostatni bit pola EOF nie jest brany pod uwagę.

9.14. KODOWANIE CIĄGU BITÓW

Kodowanie ciągu bitów

Ciąg obejmujący bity pól: SOF, ARBITRATION FIELD, CONTROL FIELD, DATA FIELD, oraz CRC FIELD jest kodowany metodą zwaną *bit stuffing*. Metoda ta polega na tym, że jeżeli podczas transmisji zostanie wykryta sekwencja 5 kolejnych bitów o takiej samej wartości logicznej, to wstawiany jest dodatkowy bit przeciwniej wartości logicznej. Pozostałe pola wchodzące w skład ramek DATA FRAME i REMOTE FRAME (CRC DELIMTER, ACK FIELD oraz EOF) nie podlegają tej metodzie kodowania. ERROR FRAME oraz OVERLOAD FRAME mają stałą i zdefiniowaną strukturę i w związku z tym nie podlegają procedurze kodowania metodą *bit stuffing*. Do kodowania poszczególnych bitów w warstwie fizycznej stosowana jest metoda NRZ (ang. *Non-Return-to-Zero*). Została ona zilustrowana na rys. 9.6.

9.15. ZARZĄDZANIE BŁĘDAMI (ERROR HANDLING)

9.15.1. 4.15.1. WYKRYWANIE BŁĘDÓW

Rozróżnia się 5 różnych rodzajów błędów, które nie wykluczają się wzajemnie:

Błąd pojedynczego bitu (BIT ERROR)

Węzeł, który nadaje wiadomość jednocześnie ją monitoruje. Błąd BIT ERROR występuje w przypadku, gdy wartość bitu odczytana z sieci jest inna niż aktualnie transmitowana. Wyjątek stanowią sytuacje, w których transmitowany jest bit recesywny w polu ARBITRATION FIELD oraz podczas trwania ACK SLOT. W tych przypadkach nie jest sygnalizowany błąd, gdy zostanie odczytany bit dominujący. Nadajnik, który wykryje bit dominujący podczas transmisji PASSIVE ERROR FLAG nie interpretuje tego jako BIT ERROR.

Błąd kodowania (STUFF ERROR)

Błąd kodowania występuje, gdy podczas transmisji pola ramki, które powinno być kodowane metodą *bit stuffingu* w sieci zostanie wykrytych 6 kolejnych bitów o takiej samej wartości logicznej.

Błąd sumy kontrolnej (CRC ERROR)

Błąd ten występuje, gdy pole sumy kontrolnej CRC obliczone na podstawie odebranej wiadomości przez odbiornik, nie zgadza się z polem CRC dołączonym do wiadomości przez nadajnik.

Błąd formatu ramki (FORM ERROR)

Błąd ten występuje w przypadku, gdy naruszona zostanie ustalony format pola bitowego transmitowanej ramki (sytuacja w której odbiornik wykryje bit dominujący w miejscu ostatniego bitu pola EOF nie jest traktowana jako błąd formatu ramki)

Błąd potwierdzenia ramki (ACKNOWLEDGEMENT ERROR)

Błąd ten wykrywany jest przez nadajnik w przypadku braku odczytania bitu dominującego podczas transmisji pola ACK SLOT.



9.15.2. SYGNALIZACJA BŁĘDÓW (ERROR SIGNALING)

Węzeł dołączony do sieci CAN sygnalizuje wykrycie błędu transmitując flagę błędu ERROR FLAG. Dla urządzeń pracujących w trybie *error active* jest to ACTIVE ERROR FLAG i odpowiednio dla węzłów pracujących w trybie *error passive* jest to PASSIVE ERROR FLAG.

Dla błędów typu:

- BIT ERROR
- STUFF ERROR
- FORM ERROR
- ACKNOWLEDGEMENT ERROR

Flaga błędu ERROR FLAG jest transmitowana począwszy od kolejnego bitu następującego po jego wykryciu.

W przypadku wykrycia błędu sumy kontrolnej CRC, transmisja flagi błędu rozpoczyna się począwszy od bitu następującego po transmisji sekcji ACK DELIMITER, chyba że rozpoczęta została już transmisja flagi błędu wynikająca z innego warunku.

9.16. OGRANICZANIE WPŁYWU USZKODZEŃ (FAULT CONFINEMENT)

Z uwagi na sposób obsługi błędów, węzeł sieci CAN może znajdować się w jednym z 3 trybów pracy:

- error active,
- error passive,
- bus off,

Węzeł pracujący w trybie *error active* może brać udział w komunikacji w sieci, a w przypadku wykrycia błędu wysyłać ACTIVE ERROR FLAG.

Węzeł pracujący w trybie *error passive* może brać udział w komunikacji w sieci, ale w przypadku wykrycia błędu może wysyłać tylko PASSIVE ERROR FLAG. Ponadto po zakończeniu transmisji węzeł pracujący w tym trybie rozpoczyna okres oczekiwania przed rozpoczęciem kolejnej transmisji (zobacz SUSPEND TRANSMISSION).

Węzeł pracujący w trybie *bus off* nie może mieć żadnego wpływu na działanie sieci. Tryb taki występuje np. w przypadku wyłączenia (zablokowania) tranceivera (sterownika magistrali) węzła.

W celu kontroli i ograniczania błędów, każdy węzeł CAN posiada dwa liczniki:

1. licznik błędów transmisji (TRANSMIT ERROR COUNT)
2. licznik błędów odbioru (RECEIVE ERROR COUNT)

Stany tych liczników są zmieniane wg następujących reguł:

1. W przypadku wykrycia błędu przez *odbiornik*, wartość rejestru licznika błędów odbioru jest zwiększana o 1, poza przypadkami wykrycia błędu pojedynczego bitu BIT ERROR podczas transmisji ACTIVE ERROR FLAG bądź OVERLOAD FLAG.
2. Jeżeli *odbiornik* wykryje bit dominujący jako pierwszy po wysłaniu flagi błędu ERROR FLAG, wartość rejestru licznika błędów odbioru przyrasta o 8.

3. Jeżeli *nadajnik* wysyła flagę błędu ERROR FLAG, to oznacza, że jednocześnie stan licznika błędów transmisji ulegnie zwiększeniu o 8.
4. Jeżeli *nadajnik* wykryje błąd pojedynczego bitu podczas wysyłania ACTIVE ERROR FLAG lub OVERLOAD FLAG, to wartość licznika błędów transmisji ulegnie zwiększeniu o 8.
5. Jeżeli *odbiornik* wykryje błąd pojedynczego bitu podczas wysyłania ACTIVE ERROR FLAG lub OVERLOAD FLAG, to wartość licznika błędów odbioru ulegnie zwiększeniu o 8.
6. Każdy węzeł toleruje wystąpienie do 7 kolejnych bitów dominujących po wysłaniu ACTIVE i PASSIVE ERROR FLAG lub OVERLOAD FLAG. W przypadku wykrycia 14-stego kolejnego bitu dominującego (dla ACTIVE ERROR FLAG lub OVERLOAD FLAG) lub po wykryciu 8-go kolejnego bitu dominującego występującego po PASSIVE ERROR FLAG, oraz po każdej dodatkowej sekwencji ośmiu kolejnych bitów dominujących każdy *nadajnik* zwiększa wartość swojego rejestru licznika błędów transmisji o 8. Analogicznie *odbiornik* o 8 zwiększa wartość swojego licznika błędów odbioru.
7. Po każdej udanej transmisji wiadomości (odczytanie potwierdzenia ACK oraz brak wystąpienia błędów aż do końca EOF) wartość licznika błędów transmisji jest zmniejszana o 1 chyba że już wynosi 0.
8. Po udanym odbiorze wiadomości (bez wystąpienia błędów aż do ACK SLOT oraz po udanym nadaniu bitu potwierdzenia ACK) wartość licznika błędów odbioru jest zmniejszana o 1, jeśli jego wartość mieści się w przedziale od 1 do 127. Jeżeli jego wartość wynosi 0, to pozostaje 0, a gdy była większa niż 127 zostaje ona ustaliona na wartość z przedziału 119-127.
9. Węzeł pracuje w trybie *error passive*, jeżeli wartość jego licznika błędów transmisji jest równa lub przekroczy 128 lub, gdy wartość jego licznika błędów odbioru jest równa lub przekroczy 128. Błąd, za przyczyną którego węzeł przechodzi w tryb *error passive* powoduje wygenerowanie ACTIVE ERROR FLAG.
10. Węzeł pracuje w trybie wyłączonej magistrali *bus off*, kiedy wartość rejestru jego licznika błędów transmisji jest większa niż 256.
11. Węzeł może przejść z trybu *error passive* do *error active*, gdy oba jego liczniki (błędów transmisji oraz błędów odbioru) mają wartości mniejsze lub równe 127.
12. Układ pracujący w trybie *bus off* może ponownie przejść do trybu *error active* z wartością liczników błędów równą 0 po zarejestrowaniu 128 wystąpień 11 bitowych ciągów bitów recesywnych na magistrali.

Uwagi:

- Jeżeli wartości rejestrów liczników błędów przekraczają 96, to oznacza, że występują silne zakłócenia w sieci. Powinno to być jednocześnie sygnałem do przeprowadzenia dokładnego monitorowania magistrali w celu lokalizacji źródeł problemu.
- Wyjątki, w których licznik błędów transmisji nie ulega zmianie
 - Jeżeli *nadajnik* pracuje w trybie *error passive* i rozpozna błąd potwierdzenia ramki (ACKNOWLEDGEMENT ERROR) polegający na braku dominującego bitu ACK oraz nie wykryje bitu dominującego podczas nadawania własnej flagi PASSIVE ERROR FLAG.
 - W przypadku, gdy nadajnik wysyła flagę błędu ERROR FLAG spowodowaną błędem kodowania STUFF ERROR podczas arbitrażu.
- Jeżeli podczas uruchamiania sieci tylko 1 węzeł jest w trybie *online* i transmituje jakąkolwiek wiadomość, to nie otrzyma on żadnego potwierdzenia. W związku z tym wykryje błąd i powtórzy transmisję. W takiej sytuacji może on przejść do trybu *error passive*, ale nie jest dozwolone jego przejście do trybu *bus off*.

9.17. Częstotliwość generatora podstawy czasu

Maksymalna tolerancja częstotliwości generatora podstawy czasu jest równa 1,58%. W związku z tym możliwe jest stosowanie rezonatora ceramicznego taktującego węzeł CAN dla prędkości transmisji do 125 kb/s.

W przypadku sieci CAN pracującej z pełną prędkością wymagane jest zastosowanie oscylatora kwarcowego. Węzły CAN zgodne ze specyfikacjami 1.0 i 1.1 pracujące wspólnie w jednej sieci muszą być wyposażone w oscylator kwarcowy.

Węzły CAN zgodne ze specyfikacjami 1.2 lub późniejszymi mogą być wyposażone w oscylator ceramiczny.

9.18. WYMAGANIA DOTYCZĄCE TAKTOWANIA (BIT TIMING REQUIREMENTS)

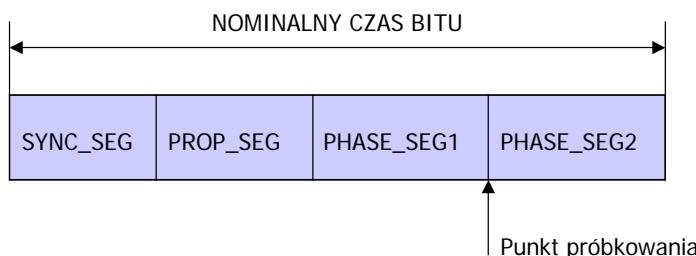
Nominalna prędkość transmisji N (NOMINAL BIT RATE) jest liczbą bitów transmitowanych w ciągu sekundy przy założeniu wykorzystania idealnego nadajnika oraz braku desynchronizacji.

Okres czas trwania transmisji pojedynczego bitu T (BIT TIME) jest definiowany jako:

$$T = \frac{1}{N}$$

Nominalny czas trwania transmisji pojedynczego bitu można podzielić teoretycznie na kilka nie zachodzących na siebie segmentów czasowych (rys. 9.18):

- segment synchronizacji (SYNC_SEG)
- segment propagacji (PROP_SEG)
- segment fazy 1 (PHASE_SEG1)
- segment fazy 2 (PHASE_SEG2)



Rys. 9.18 Nominalny czas bitu

SYNC_SEG

Segment SYNC_SEG wykorzystywany jest do synchronizowania różnych węzłów podłączonych do magistrali. W tym segmencie powinno znajdować się zbocze sygnału kodującego przesyłany bit.

PROP_SEG

W tym segmencie następuje buforowanie skutków wystąpienia fizycznych opóźnień występujących w medium. Czas opóźnienia sygnału w medium jest równy podwojonej sumie czasu propagacji sygnału na magistrali, opóźnienia w układzie wejściowym i opóźnieniu w układzie wyjściowym tranceivera.

PHASE_SEG1, PHASE_SEG2

Segmenty te wykorzystywane są do kompensacji błędów synchronizacji. Mogą się one być wydłużane lub skracane w wyniku operacji resynchronizacji.

Punkt próbkowania (SAMPLE POINT)

Chwila (punkt) próbkowania jest momentem czasowym, w którym jest odczytywany poziom elektryczny sygnału medium, i w którym przypisywana jest wartość logiczna temu poziomowi. Chwila próbkowania występuje na końcu segmentu PHASE_SEG1.

Czas przetwarzania informacji

Czas przetwarzania informacji jest czasem liczonym od momentu próbkowania i koniecznym na analizę poziomu odbieranego bitu.

Kwant czasu τ_q – TIME QUANTUM

Kwant czasu jest elementarną jednostką czasu pochodną względem okresu generatora podstawy czasu. Istnieje programowalny przelicznik o całkowitych wartościach z przedziału 1 do 32. Począwszy od minimalnego czasu kwantu, czas ten może mieć długości:

$$\tau_q = m \cdot \tau_{\min}$$

gdzie: τ_{\min} - minimalny czas trwania kwantu

m - multiplikator (1..32).

Czasy trwania segmentów czasowych wynoszą odpowiednio:

- SYNC_SEG – 1 τ_q
- PROP_SEG – jest programowalny w zakresie 1-8 τ_q
- PHASE_SEG1 – jest programowalny w zakresie 1-8 τ_q
- PHASE_SEG2 – równy jest maksymalnej długości czasu PHASE_SEG1 oraz czasu przetwarzania informacji
- Czas przetwarzania informacji – jest krótszy lub równy dwukrotnej wartości τ_q

Całkowita liczba kwantów w okresie bitu musi być programowalna w zakresie co najmniej od 8 do 25.

Częstą i celową praktyką jest konstruowanie węzłów CAN w taki sposób, aby nie było konieczności stosowania różnych generatorów dla potrzeb układu komunikacji i jednostki centralnej CPU węzła. W celu uzyskania odpowiedniej częstotliwości generatora podstawy czasu dla celów komunikacyjnych, niezbędna jest w tym przypadku programowa możliwość zmiany czasu trwania transmisji bitu (*bit timing*).



Dopasowanie chwili próbkowania w sieci, w której wszystkie węzły mają programowalne czasy transmisji bitu nie jest problemem. W przypadku braku możliwości programowania czasu trwania kwantu, czas trwania transmisji jednego bitu węzłów CAN powinien być zgodny z definicją przedstawioną na rys. 9.19.



Rys. 9.19 Podział bitu na segmenty

Synchronizacja sprzętowa - HARD SYNCHRONIZATION

W sieci CAN stosowana jest transmisja synchroniczna. Oznacza to, że rozpoczęcie odbioru informacji w odbiorniku jest synchronizowane z nadajnikiem. Odbiornik czeka z wygenerowaniem segmentu synchronizacyjnego SYNC_SEG tak długo jak nie nadaje odpowiednie zbocze synchronizujące generowane przez nadajnik.

RESYNCHRONIZATION JUMP WIDTH

W wyniku wystąpienia ponownej synchronizacji okres PHASE SEG1 może się wydłużyć lub też PHASE SEG2 może ulec skróceniu. Całkowita zmiana długości trwania segmentu fazy PHASE BUFFER SEGMENT jest ograniczona od góry przez parametr RESYNCHRONIZATION JUMP WIDTH.

Wartość RESYNCHRONIZATION JUMP WIDTH powinna być programowalna w zakresie od 1 do min. 4 PHASE SEG1. Do celów synchronizacji wykorzystywane są zbocza odbieranego sygnału. Ponieważ maksymalna liczba bitów o takiej samej wartości występujących w trakcie transmisji jest ograniczona to istnieje możliwość realizacji resynchronizacji węzła także w trakcie odbioru informacji. Maksymalna odległość czasowa pomiędzy kolejnymi zboczami synchronizującymi przejściami, które mogą być wykorzystane do ponownej synchronizacji wynosi 29 okresów transmisji jednego bitu.

Błąd fazy zbocza sygnału – PHASE ERROR

Błąd fazowy zbocza odbieranego sygnału wyznaczany jest względem segmentu synchronizacji SYNC_SEG i mierzony jest w kwantach czasu. Znak błędu fazowego określany jest w następujący sposób:

- $e=0$ jeżeli zbocze leży wewnętrz SYNC_SEG,
- $e>0$ jeżeli zbocze leży przed punktem próbkowania SAMPLE POINT,
- $e<0$ jeżeli zbocze leży za punktem próbkowania danego bitu.



Ponowna synchronizacja

W przypadku, gdy wartość błędu fazy PHASE ERROR zbocza sygnału, który wywołuje ponowną synchronizację jest mniejsza lub równa programowalnej wartości RESYNCHRONIZATION JUMP WIDTH to w efekcie mamy do czynienia z sytuacją podobną do synchronizacji sprzętowej.

Jeżeli wielkość błędu fazy jest większa niż RESYNCHRONIZATION JUMP WIDTH

- oraz, gdy błąd fazy jest dodatni, wtedy PHASE_SEG1 jest wydłużany o wartość równą RESYNCHRONIZATION JUMP WIDTH,
- oraz, gdy błąd fazy jest ujemny, wtedy PHASE_SEG2 jest skracany do wartości równej RESYNCHRONIZATION JUMP WIDTH

Zasady synchronizacji

1. Dozwolona jest tylko jedna synchronizacja w czasie trwania transmisji danego bitu.
2. Zbocze sygnału może być użyte do synchronizacji tylko wówczas, gdy wartość sygnału kodującego stan logiczny bitu zarejestrowana w poprzedzającym punkcie próbkowania jest różna od wartości sygnału zaraz po wystąpieniu tego zbocza.
3. W stanie czuwania medium, synchronizacja sprzętowa jest realizowana przez każde zbocze polegające na zmianie stanu z recesywnego na dominujący. Pozostałe zbocza występujące przy zmianach stanów medium z recesywnego do dominującego mogą być wykorzystane do ponownej synchronizacji, gdy spełniają punkty 1 i 2 z wyjątkiem gdy: węzeł nadający stan dominujący nie będzie przeprowadzał ponownej synchronizacji w wyniku dodatniego błędu fazy.

9.19. WARSTWA APLIKACYJNA

9.19.1. CANOPEN – WPROWADZENIE

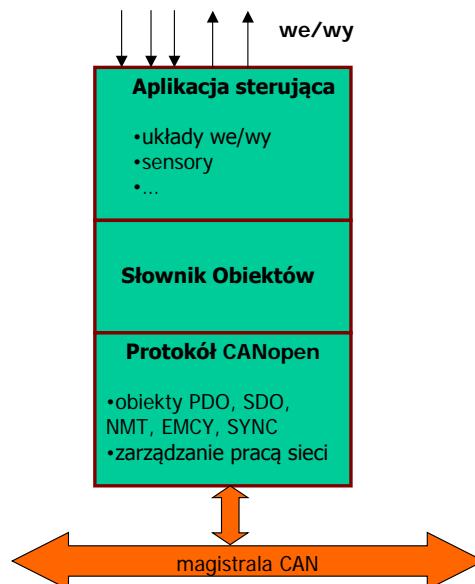
CANopen jest jednym z protokołów komunikacji warstwy wyższej wykorzystujących specyfikację sieci CAN. Został on zaprojektowany z myślą o zastosowaniach do automatyzacji przemysłowych procesów wytwórczych. Z biegiem czasu CANopen znalazł zastosowanie w wielu innych dziedzinach w tym także w budownictwie i transporcie.

Prace nad tym protokołem prowadzone były początkowo pod nadzorem firmy Bosch. Od 1995 roku rozwojem CANopen zajmuje się organizacja CiA (ang. CAN in Automation). Specyfikacje CiA obejmują warstwę aplikacji, profile komunikacyjne, strukturę urządzeń programowalnych, profile sprzętowe, zalecenia dotyczące okablowania oraz złącz. Aktualna wersja protokołu CANopen (CiA DS. 301) została objęta standardem i normą EN50325-4.

9.19.2. MODEL URZĄDZENIA

Urządzenie pracujące zgodnie z protokołem CANopen przedstawiane jest zazwyczaj w postaci modelu złożonego z trzech modułów:

- modułu odpowiedzialnego za komunikację (protokół CANopen),
- modułu zawierającego wiedzę o urządzeniu (słownik obiektów),
- aplikacji odpowiedzialnej za poprawną pracę urządzenia.



Rys. 9.20 Schemat modelu urządzenia

9.19.3. SŁOWNIK OBIEKTÓW

Słownik obiektów jest najważniejszym elementem modelu urządzenia. Zawiera niezbędne informacje potrzebne do poprawnej pracy urządzenia i daje dostęp do:

- definicji wykorzystywanych typów danych w urządzeniu,
- parametrów komunikacji,
- danych i konfiguracji aplikacji.
-

W tab. 9.3 przedstawiono strukturę słownika obiektów.

Tab. 9.3 Struktura słownika obiektów

| Indeks (hex) | Obiekt |
|--------------|---|
| 0000 | Wolny |
| 0001 – 001F | Statyczne typy danych |
| 0020 – 003F | Złożone typy danych |
| 0040 – 005F | Charakterystyczne dane producenta |
| 0060 – 007F | Charakterystyczne dane urządzenia (statyczne) |
| 0080 – 009F | Charakterystyczne dane urządzenia (złożone) |
| 00A0 – 0FFF | Zarezerwowany |
| 1000 – 1FFF | Profil komunikacyjny |
| 2000 – 5FFF | Profil charakteryzujący producenta |
| 6000 – 9FFF | Znormalizowany profil urządzenia |
| A000 – FFFF | Zarezerwowany |

Słownik obiektów może zawierać maksymalnie 65536 obiektów. Każdy obiekt jest adresowalny przez tzw. indeks. Zastosowane adresowania 16 bitowego pozwala na dostęp do prostych zmiennych. W przypadku adresowania złożonych struktur danych takich jak rekordy czy tablice, indeks odwołuje się wyłącznie do adresu danej struktury. Dostęp do obiektów złożonych możliwy jest dzięki zastosowaniu *subindeksu*. W takim przypadku indeks jest wskaźnikiem złożonej struktury danych, a subindeks wskazuje jej elementy.

9.19.4. MODEL KOMUNIKACJI

Protokół CANopen wykorzystuje różne modele komunikacji pomiędzy urządzeniami w sieci. Wykorzystywane są różne obiekty komunikacji i usług, a także różne typy obiektów wyzwalania transmisji. Stosowana jest zarówno transmisja w trybie synchronicznym jak i asynchronicznym.

W przypadku transmisji w trybie synchronicznym nadawany jest specjalny obiekt synchronizacji (obiekt SYNC), który określa momenty, w których możliwa jest wymiana wiadomości.

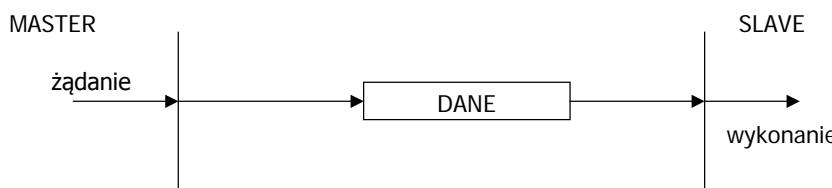
Transmisja asynchroniczna pozwala na transmisję wiadomości w dowolnym momencie. W takim przypadku transmisja wyzwalana jest odpowiednio zdefiniowanym zdarzeniem lub chwilą czasową.

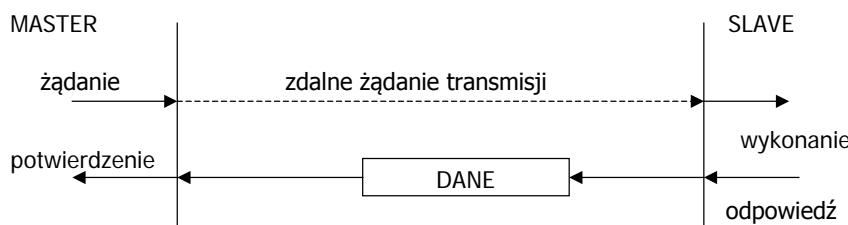
Niezależnie od tego wyróżniane są trzy następujące schematy współpracy urządzeń w sieci z protokołem CANopen:

- master-slave,
- klient-serwer,
- producent-konsument.

9.19.5. WSPÓŁPRACA TYPU MASTER-SLAVE

W przypadku schematu współpracy urządzeń typu master-slave, w każdym momencie czasowym występuje w sieci tylko i wyłącznie jedno urządzenie nadrzędne typu master. Pozostałe urządzenia traktowane są jako urządzenia podporządkowane. Urządzenie typu master wysyła żądanie do jednego lub wielu urządzeń podporządkowanych. Urządzenie podporządkowane odpowiada na żądanie urządzenia typu master. Ten model współpracy urządzeń jest podobny do modelu stosowanego np. w sieci MODBUS RTU (rozdział 7).

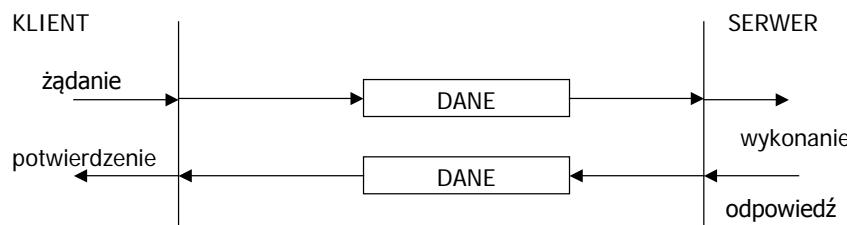




Rys. 9.21 Model komunikacji typu master-slave

9.19.6. WSPÓŁPRACA TYPU Klient - SERWER

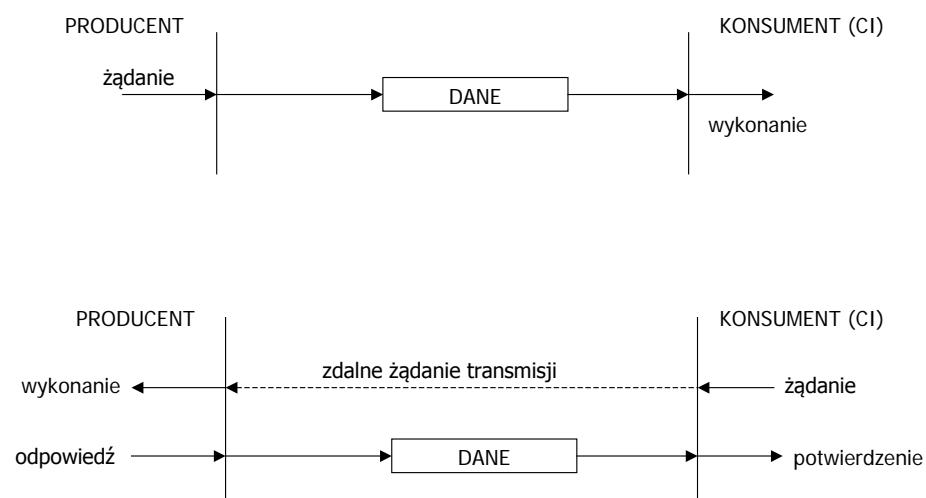
Ten model współpracy urządzeń polega na komunikacji pomiędzy jednym klientem i jednym serwerem. Klient wysyła do serwera żądanie wykonania określonej funkcji. Po jej wykonaniu, serwer wysyła odpowiedź potwierdzającą do klienta.



Rys. 9.22 Model komunikacji typu klient - serwer

9.19.7. WSPÓŁPRACA TYPU PRODUCENT - KONSUMENT

Współpraca typu producent - konsument nazywana jest również współpracą typu *push-pull*. W tego typu komunikacji bierze udział jeden producent i od 0 do n konsumentów. Model *push* charakteryzuje się brakiem konieczności potwierdzenia odebrania wiadomości. W modelu *pull* komunikacja inicjowana jest przez konsumenta, a producent odpowiada. W tym przypadku potwierdzeniem odebrania żądania jest wysłanie odpowiedzi przez producenta.



Rys. 9.23 Model komunikacji typu producent - konsument

9.19.8. OBIEKTY KOMUNIKACJI

Protokół CANopen na poziomie warstwy aplikacji korzysta z różnych sposobów wymiany informacji. Stosowane do tego tzw. obiekty komunikacyjne, które w zależności oferują różnego rodzaju funkcje i usługi takie jak np.: transmisja danych procesowych, zarządzanie i monitorowanie pracy sieci czy zdalna konfiguracja węzłów sieci.

Wszystkie obiekty i usługi oferowane przez CANopen działają przy założeniu poprawnej pracy sieci w warstwie łącza danych i poprawnej implementacji warstwy aplikacyjnej. Specyfikacją protokołu CANopen nie obejmuje przypadków, w których to założenie nie jest spełnione.

9.19.9. OBIEKT PDO (PROCESS DATA OBJECT)

Obiekty PDO służą do dynamicznej wymiany danych procesowych między urządzeniami sieci. Obiekty te mają wysoki priorytet i mogą zawierać do 8 bajtów danych w jednej wiadomości. Stosowana jest tu komunikacja typu producent-konsument.

Rozróżnia się dwa rodzaje obiektów PDO. Jeden służy do nadawania TPDO (ang. *Transmit-PDO*), a drugi do odbioru wiadomości RPDO (ang. *Receive-PDO*). Urządzenie wspierające transmisję obiektów TPDO pełni funkcję producenta natomiast, urządzenie wspierające odbiór obiektów RPDO pełni rolę konsumenta. Zazwyczaj urządzenia pracujące zgodnie z protokołem CANopen wspierają oba te tryby pracy. Odpowiednie parametry komunikacyjne umieszczone są w słowniku obiektów danego urządzenia.

9.19.10. RODZAJE TRYBÓW KOMUNIKACYJNYCH

Rozróżnić można następujące rodzaje komunikacji:

- asynchroniczna – transmisja może rozpocząć się w dowolnym momencie czasowym i może być:
 - wyzwalana zdarzeniem – transmisja następuje po wystąpieniu określonego zdarzenia np. po zmianie wartości wejściowej,
 - wyzwalana czasem – transmisja następuje po upływie określonego czasu,
 - inicjowana zdalnym żądaniem transmisji – transmisja inicjowana jest przez żądanie transmisji wysłane przez konsumenta PDO.
- Synchroniczna – transmisja może nastąpić tylko w określonym przedziale czasowym, po wystąpieniu obiektu synchronizującego SYNC nadawanego przez jedno z urządzeń w sieci i może być:
 - cykliczna – transmisja odbywa się okresowo po każdym n -tym obiekcie SYNC (n jest zmiennym parametrem)
 - acykliczna – transmisja następuje po wystąpieniu obiektu SYNC, ale wcześniej musi być ona:
 - wyzwolona zdarzeniem lub
 - wyzwolona zdalnym żądaniem transmisji.

9.19.11. TYPY WYMIANY DANYCH

Z obiektem PDO skojarzone są dwa tryby wymiany danych – zapis i odczyt.

Tryb: zapis PDO

Producent PDO wysyła w obiekcie PDO dane. Dane te są odbierane przez 0 lub n węzłów. Konsument PDO nie wysyła żadnego potwierdzenia odbioru. Ten typ wymiany danych podobny jest do transmisji rozgłoszeniowej (broadcast). Jest to model wymiany danych typu *push*.

Tryb: odczyt PDO

W tym trybie jeden lub więcej konsumentów PDO wysyła żądanie zdalnej transmisji do producenta PDO. W odpowiedzi producent przesyła żądane dane. Ich odbiorcą może być od 0 do n konsumentów PDO. Jest to model wymiany danych typu *pull*.

9.19.12. OBIEKT SDO (SERVICE DATA OBJECT)

Obiekty SDO umożliwiają zapis i odczyt danych bezpośrednio do i ze słownika obiektów. Obiekty SDO przesyłane są zazwyczaj asynchronicznie z priorytetem niższym niż obiekty PDO, gdyż prędkość wymiany danych nie ma tu tak wielkiego znaczenia.

W tego typu komunikacji stosowany jest model wymiany danych typu punkt do punktu (ang. *peer to peer*), a więc zgodny ze specyfikacją klient-serwer. Klientem SDO jest w tym przypadku węzeł żądający wymiany danych (odczyt lub zapis z lub do słownika obiektów) natomiast serwerem SDO jest aplikacja udostępniająca swój słownik obiektów. Urządzeniem inicjującym wymianę danych (tworzącym tzw. kanał komunikacyjny) jest zawsze klient. Tego typu transmisja wymaga potwierdzenia, dlatego każde połączenie wymaga użycia dwóch wiadomości CAN (żądanie klienta i odpowiedź serwera). W zależności od liczby danych przeznaczonych do przesłania, stosowane są dwa typy transmisji:

- segmentowy (standardowy) – podstawowy typ transmisji,
- blokowy (opcjonalny) – wykorzystywany przy transmisji dużych bloków danych.

W obydwu typach transmisji stosowane są różne procedury wymiany danych.

9.19.13. TRANSMISJA SEGMENTOWA

Z punktu widzenia klienta SDO transmisję segmentową można podzielić na:

- Odczyt SDO
 - inicjacja odczytu SDO,
 - odczyt danych SDO.
- Zapis SDO
 - inicjacja zapisu SDO,
 - zapis danych SDO.
- Anulowanie transmisji.

W transmisji segmentowej w jednym segmencie transmitowane może być maksymalnie 7 bajtów danych. Gdy liczba bajtów danych jest większa, dokonywany jest ich podział na segmenty.

Jeżeli liczba danych nie przekracza 4 bajtów, to dane te mogą być zawarte już w ramce inicjującej transmisję. Jest to tzw. transfer przyspieszony (ang. *expedited transfer*).

9.19.14. TRANSMISJA BLOKOWA

Z punktu widzenia klienta SDO transmisję blokową możemy podzielić na:

- Odczyt blokowy SDO
 - inicjacja odczytu bloku,
 - odczyt bloku,
 - zakończenie odczytu bloku.
- Zapis blokowy SDO
 - inicjacja zapisu bloku,
 - zapis bloku,
 - zakończenie zapisu bloku.
- Anulowanie transmisji.

9.19.15. OBIEKT SYNCHRONIZUJĄCY SYNC

W celu synchronizacji pracy elementów sieci CANopen stosuje się rozgłoszeniową transmisję obiektów typu SYNC. Obiekt SYNC jest transmitowany w regularnych odstępach czasu przez jeden z węzłów sieci zwany producentem SYNC. Okres transmisji jest określony przez parametr zwany okresem cyklu komunikacji (ang. *Communication Cycle Period*) i zapisany jest w słowniku obiektów urządzenia pod adresem 1006h. Parametr ten może być zmieniany w podczas procedury uruchamiania urządzenia.

Aby zapewnić obiekowi SYNC możliwie szybki dostęp do sieci nadawany jest mu odpowiednio wysoki priorytet. Obiekt SYNC nie zawiera żadnych danych. Transmisja odbywa się zgodnie z modelem producent - konsument. Producent w zdefiniowanych odstępach czasu wysyła obiekt SYNC do sieci. Wszystkie urządzenia (konsumenti SYNC), które tego potrzebują mogą być odbiorcą tych obiektów i za ich pomocą synchronizować swoją pracę z pozostałymi węzłami sieci.

9.19.16. OBIEKT TYPU TIME STAMP

Obiekt typu Time Stamp służy do przesyłania informacji o aktualnym czasie. Jest to transmisja rozgłoszeniowa. Obiekt o długości 6 bajtów z wysokim priorytetem wysyłany jest do sieci CAN przez producenta. Wysyłana jest liczba milisekund jakie upłynęły od północy oraz liczba dni począwszy od 1 stycznia 1984 roku.

9.19.17. OBIEKT AWARYJNY EMCY

Obiekt typu EMCY (ang. *emergency*) służy do sygnalizowania wystąpienia awarii w urządzeniu. W przypadku zaistnienia awarii nadawana jest jedna ramka CAN z 8 bajtami danych. Posiada ona wysoki priorytet. Dane zawierają kod błędu. Obiekt EMCY implementowany jest opcjonalnie.

Wystąpienie błędu sygnalizowane jest tylko raz. Kody błędów są zawarte w słowniku obiektów urządzenia. Poza standardowymi kodami błędów istnieje możliwość definiowania własnych kodów przez poszczególnych producentów.

9.19.18. OBIEKT NMT

Zarządzanie siecią CANopen (ang. *Network Management*) polega na nadzorowaniu poszczególnych węzłów sieci i oparte jest na współpracy typu master - slave. Do

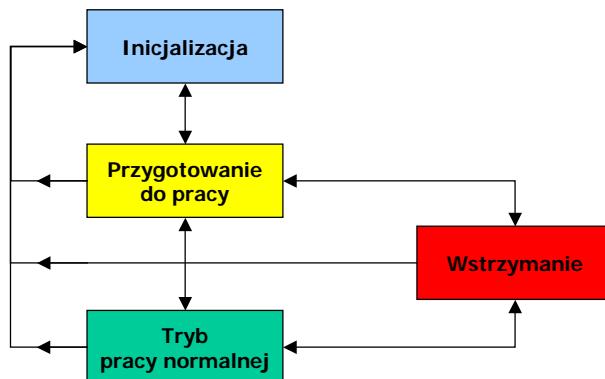
zarządzania stosuje się obiekty NMT. Za ich pomocą możliwa jest inicjalizacja pracy urządzenia, jego uruchomienie, monitorowanie, czy też zatrzymanie.

Każde urządzenie pracujące w sieci CANopen musi umożliwiać pracę w trybie *slave* NMT. Urządzenia typu *slave* adresowane są za pomocą identyfikatorów węzłów NODE-ID. W sieci musi być też zdefiniowany jeden moduł zarządzający pracujący jako master. Zarządzanie siecią skupia się głównie na dwóch zadaniach. Jedno z nich to zarządzanie trybem pracy poszczególnych węzłów i sieci. Drugie to nadzór nad urządzeniem polegające głównie na kontroli jego aktywności.

9.19.19. ZARZĄDZANIE TRYBEM PRACY

Każde urządzenia w sieci CANopen może znajdować się jednym z 4 stanów:

- | | |
|---|---|
| 1. STOPPED 2. Pre-operational 3. Operational 4. Initializing | – wstrzymania pracy, - gotowości do pracy, – pracy normalnej, – inicjalizacji. |
|---|---|



Rys. 9.24 Zależności między trybami pracy

Urządzenie master NMT odpowiedzialne jest za sterowanie trybem pracy sieci i jej poszczególnych urządzeń. Obiekt NMT steruje procesem uruchomienia sieci oraz zarządza trybem pracy poszczególnych węzłów.

Do komunikacji wykorzystywany jest obiekt NMT o długości 2 bajtów, z których pierwszy zawiera adres węzła, a drugi polecenie trybu pracy węzła, do którego ma on przejść. Możliwe jest też wysłanie poleceń do wszystkich węzłów jednocześnie.

9.19.20. NADZÓR

W specyfikacji protokołu CANopen wyróżnione są 2 rodzaje usług umożliwiających ciągłe nadzorowanie pracy sieci. Są nimi: dozór węzłów (starszy sposób) oraz nowszy i zalecany w nowych implementacjach w postaci tzw. sygnału *heartbeat*.

Dozór aplikacji nad węzłami pracującymi w trybie *slave* realizowany przez odpytywanie (wysłanie zapytania o tryb pracy) w ustalonych odstępach czasu. Jeżeli urządzenie typu *slave* nie odpowie w określonym czasie, to sygnalizowane jest to w aplikacji sterującej pracą urządzenia typu *master*.

Jeżeli urządzenie *slave* nie zostanie zapytane o stan w przeciągu określonego czasu, to również zostanie zasygnalizowane to aplikacji nim zarządzającej.

Działanie usługi *heartbeat* polega na cyklicznym wysyłaniu informacji o trybie swojej pracy do sieci. Jest to typowy przykład współpracy sieciowej typu producent -konsument. Producent wysyła sygnał potwierdzający jego obecność w sieci w regularnych odstępach czasu. Odbiorcami mogą być wszystkie urządzenia w sieci. Jeżeli w określonym czasie konsument nie otrzyma obiektu *heartbeat* z konkretnego węzła, to generowane jest zdarzenie informujące o tym lokalną aplikację zarządzającą pracą konsumenta.

9.19.21. OBIEKT BOOT-UP

Obiekt typu *Boot-up* transmitowany jest do sieci w celu przesłania informacji, że obiekt który ją wysłał osiągnął stan gotowości do pracy (pre-operational). Dzieje się tak zawsze po starcie lub restarcie urządzenia. Obiekt typu *Boot-up* ma ten sam identyfikator co obiekt *heartbeat*, ale nie przenosi żadnych danych.



10. LITERATURA

- [1]. Jędrzej Ułasiewicz (2007). Systemy czasu rzeczywistego QNX6 Neutrino, Wydawnictwo BTC, Warszawa 2007, ISBN 978-83-60233-27-6, s.301.
- [2]. Krzysztof Sacha (2006). Systemy czasu rzeczywistego, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa, 2006, ISBN 83-7207-124-1, s. 135.
- [3]. Standard Computer Dictionary, IEEE Std. 610,1990.
- [4]. Modbus Protocol Reference Guide. PI-MBUS-300. Rev. J, 1996, Modicon,
http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf,
http://modbus.org/docs/PI_MBUS_300.pdf, s.121.,
http://www.wingpath.co.uk/modbus/modbus_protocol.php
- [5]. Tadeusz Mikulczyński (2006). Automatyzacja procesów produkcyjnych Metody modelowania procesów dyskretnych i programowania sterowników PLC, ISBN: 83-204-3177-8, WNT, s.216