Protokół Modbus

1. Protokół Modbus

1.1. Wstęp

Protokół Modbus, opracowany w firmie Modicon, jest standardem przyjętym przez większość producentów sterowników przemysłowych dla asynchronicznej komunikacji pomiędzy urządzeniami systemów znakowo-kontrolnych. Podstawowe zalety protokołu to:

- dostęp do łącza na zasadzie „master-slave”
- zabezpieczenie przesyłanych komunikatów przed błędami
- potwierdzenie wykonania rozkazów zdalnych i sygnalizacja błędów
- mechanizmy zabezpieczające przed zawieszeniem systemu
- wykorzystanie asynchronicznej transmisji znakowej zgodnej ze standardem RS-232C

1.2. Opis transakcji

W systemie *Modbus* urządzenia komunikują się przy wykorzystaniu protokołu typu *master-slave*: tylko jedno urządzenie może być *masterem*, tzn. inicjować transakcję, pozostałe (*slave*) odpowiadają jedynie na jego zdalne zapytania. Transakcja składa się z zapytania (query) wysyłanego przez układ *master* oraz z odpowiedzi (response) wysyłanej do niego przez jednostki *slave*. W skład odpowiedzi wchodzą dane żądane przez master lub potwierdzenie realizacji jego polecenia.
Master może przesyłać wiadomości dwojakiego rodzaju:

- skierowane do indywidualnych odbiorców, identyfikowanych na podstawie przypisanego im adresu,
- przeznaczone dla wszystkich urządzeń typu slave w systemie (tzw. wiadomości rozgłoszeniowe – broadcast); w tym przypadku jednostki slave nie przesyłają odpowiedzi

Format wiadomości przesyłanych w protokole Modbus z master do slave zawiera:

- adres odbiorcy
- kod funkcji reprezentujący żądane polecenie
- dane
- słowo kontrolne zabezpieczające przesyłaną wiadomość

Odpowiedź urządzenia slave zawiera:

- pole potwierdzenia realizacji rozkazu
- dane żądane przez master
- słowo kontrolne zabezpieczające odpowiedź przed błędami

Jeżeli urządzenie slave wykryje błąd przy odbiorze wiadomości, albo nie jest w stanie wykonać polecenia, przygotowuje specjalny komunikat o wystąpieniu błędu i przesyła go w formie odpowiedzi do jednostki master.

1.3. Tryby pracy

Protokół Modbus posiada dwa tryby transmisji: ASCII i RTU, różniące się miedzy sobą formatem ramki komunikacyjnej. Określony format ramki pozwala urządzeniu odbierającemu na odrzucenie ramek niekompletnych i sygnalizację związanych z tym błędów.

1.3.1. Tryb ASCII

W ramce komunikacyjnej w trybie ASCII każdy bajt jest zakodowany w postaci dwóch znaków ASCII. Format przesyłanego znaku jest następujący:

- kodowanie: kod heksadecymalny, znaki ASCII 0-9, A-F; jeden znak heksadecymalny jest zawarty w każdym znaku ASCII wiadomości
- jednostka informacyjna: 10-bitowa, ograniczona znakami start i stop

Jako zabezpieczenie części informacyjnej ramki przed przekłamaniami stosuje się kod LRC (Longitudinal Redundancy Check).
Dokładny format ramki w trybie ASCII jest przedstawiony na poniższym rysunku. Znakiem początku jest dwukropek („:” – ASCII 3Ah). Urządzenie po wykryciu znacznika początku ramki sprawdza, czy pole adresowe zawiera jego adres własny. Jeżeli tak, to odczytuje zawartość pola funkcji i związaną z nim zawartość pola danych Dopuszczalnymi znakami dla pozostałych pól (za wyjątkiem znacznika końca ramki) są 0-9, Ah-Fh. Część informacyjną ramki zabezpiecza pole kontrolne LRC. Ramka jest zakończona przesłaniem dwóch znaków: CR i LF.

ZNACZNIK POCZĄTKU	ADRES	FUNKCJA	DANE	KONTROLA LRC	ZNACZNIK KOŃCA
1ZNAK	2 ZNAKI	2 ZNAKI	n ZNAKÓW	2 ZNAKI	2 ZNAKI CR LF

1.3.2. Tryb RTU

W tym trybie wiadomości rozpoczynają się odstępem czasowym będącym wielokrotnością przesyłu minimum 3,5 pojedynczego znaku, w którym panuję cisza na łączu. Podobnie odstęp czasowy pomiędzy kolejnymi znakami przesyłanymi w ramce nie może przekroczyć wielokrotności przesyłu 1,5 pojedynczego znaku. Gdy powyższe wymagania nie zostaną spełnione, to urządzenie odczyta ramkę błędnie (np. potraktuje początek następnej ramki jako kontynuację obecnej), co zostanie uwidocznione błędem sumy kontrolnej CRC, stosowanej w trybie RTU do zabezpieczenia ramki przed przekłamaniami.

Ramka jest przedstawiona na poniższym rysunku. Dopuszczalnymi znakami są 0-9, A-F.

ZNACZNIK POCZĄTKU	ADRES	FUNKCJA	DANE	KONTROLA CRC	ZNACZNIK KOŃCA
T1-T2-T3-T4	8 BITÓW	8 BITÓW	n x 8 BITÓW	16 BITÓW	T1-T2-T3-T4

1.4. Charakterystyka pól ramki

1.4.1. Pole adresowe

Zawiera dwa znaki (ASCII) lu 8 bitów (RTU). Zakres adresów slave wynosi 0-247. Master adresuje jednostkę slave umieszczając jej adres na polu adresowym ramki. Kiedy urządzenie slave wysyła odpowiedź, umieszcza swój własny adres na polu adresowym ramki, co pozwala jednostce master sprawdzić, z którą jednostką realizowana jest transakcja.
Adres O jest wykorzystywany jako adres rozgłoszeniowy, rozpoznawany przez wszystkie jednostki slave podłączone do magistrali.

1.4.2. Pole funkcji

Zawiera dwa znaki (ASCII) lu 8 bitów (RTU). Zakres kodów wynosi 1-255. Pole funkcji zawiera kod rozkazu określający działanie, które ma podjąć slave na żądanie mastera, np. zapis i odczyt rejestrów, odczyt statusu, forsowanie wyjść itp.

Slave odpowiadając masterowi wykorzystuje pole funkcji do:
- potwierdzenia wykonania polecenia – wtedy umieszcza na polu funkcji kod wykonanego rozkazu,
- sygnalizacji błędu, jeżeli nie może wykonać rozkazu – wtedy umieszcza na polu funkcji „szczególną odpowiedź" (exception response), która stanowi kod funkcji z ustawionym na 1 najstarszym bitem.

Za obsługę błędów jest odpowiedzialny program wykonywany przez jednostkę master. Typową reakcją na wystąpienie błędu jest powtórzenie ramki polecenia, odczyt informacji statusowych umożliwiających diagnostykę błędów i powiadomienie operatora.

1.4.3. Pole danych

Zawiera zestaw dwucyfrowych licz heksadecymalnych w zakresie 00-FF. Są one przy transmisji w trybie ASCII reprezentowane dwoma znakami, a przy RTU jednym.
Pole danych ramki polecenia zawiera dodatkowe informacje potrzebne jednostce slave do wykonania rozkazu określonego kodem funkcji, np. adresy rejestrów, liczba bajtów w polu danych, dane itp. Jeżeli nie wystąpi błąd, pole danych odpowiedzi zawiera żądane informacje. Wykrycie błędu powoduje zapisanie przez jednostkę slave kodu błędu na polu danych ramki odpowiedzi, co umożliwia adekwatną reakcję mastera.
W niektórych ramkach polecenia pole danych może posiadać zerowa długość. Tak jest zawsze w sytuacji, gdy operacja określona kodem funkcji nie wymaga żadnych parametrów.

1.4.4. Pole kontrolne

Zależy od zastosowanego trybu transmisji.

W trybie ASCII składa się z dwóch znaków ASCII, będących wynikiem obliczenie LRC na zawartości części informacyjnej ramki. Są one dołączane jako ostatnie pole ramki, bezpośrednio przed znacznikiem końca (znaki CR i LF).

W trybie RTU pole kontrolne jest 16-bitowe i powstaje w rezultacie obliczenia CRC na zawartości ramki. Zajmuje ono dwa bajty dołączane na końcu ramki. Pierwszy jest przesyłany młodszy bajt, ostatni starszy, który jest jednocześnie znakiem kończącym ramkę.

1.5. Funkcje protokołu Modbus

Nr funkcji	Funkcja
1h	Odczyt stanu cewek (odczyt wyjść cyfrowych)
2h	Odczyt wejść cyfrowych
3h	Odczyt rejestrów
4h	Odczyt wejść analogowych
5h	Wymuszenie pojedynczej cewki (zapis wyjścia cyfrowego)
6h	Zapis do pojedynczego rejestru
7h	Odczyt statusu
Fh	Wymuszenie wielu cewek
10h	Zapis do wielu rejestrów
11h	Odczyt ID jednostki slave
14h	Odczyt zawartości rejestrów w pamięci rozszerzonej
15h	Zapis do rejestrów w pamięci rozszerzonej
16h	Maskowanie grupy 4 rejestrów
17h	Odczyt/zapis grupy 4 rejestrów
18h	Odczyt kolejki FIFO

1.6. Generacja słów zabezpieczających

1.6.1. Generacja LRC

Wartość LRC (8-bitowa) jest obliczana przez urządzenie nadające, dołączana do wiadomości i przesyłana na końcu ramki w postaci dwóch znaków ASCII. Urządzenie odbierające oblicza LRC w trakcie odbioru ramki i porównuje wyznaczoną przez siebie wartość ze słowem kontrolnym w odebranej ramce. Jeżeli obie ramki są różne, wystąpił błąd.

Obliczanie LRC polega na sumowaniu kolejnych 8-bitowych bajtów wiadomości, odrzuceniu przeniesień, a na koniec wyznaczeniu uzupełnienia dwójkowego wyniku. Sumowanie obejmuje całą wiadomość za wyjątkiem znaczników początku i końca ramki.

1.6.2. Wyznaczanie CRC

Słowo kontrolne CRC to16-bitowa wartość wyznaczona przez urządzenie nadające, dołączające ją na końcu ramki w postaci dwóch 8-bitowych znaków. Urządzenie odbierające dokonuje analogicznego obliczenia podczas odbioru ramki, następnie porównuje wyznaczoną przez siebie wartość z odebranym słowem kontrolnym CRC. Gdy obie wartości są różne, wystąpi błąd