WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 3, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v3n3.27
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Communication Scheme of Modbus-Profibus Motor Protection Controller Based on STM32

Ze Run

College of Electronic Information, Xinan Minzu University, Chengdu, China
*Corresponding Author: Jixiang Zeng

ABSTRACT

Motor protection as one of the protection measures of power electronic system, has always been conservative attention, the content of this paper is based on the communication process of low-voltage motor protection. This paper discusses from the perspective of cost reduction and efficiency enhancement and industrial capability enhancement. Therefore, VPC3 chip of Siemens is not used as the protocol package of Profibus communication, and its packet and decoding are both using MCU internal resources. Modbus, as a simple and easy to understand communication mode, is used as the underlying data exchange library of Profibus. Profibus communication protocol only needs to encapsulate Modbus for motor protection, and realizes two communication protocols for motor protection controller. In this connection, a communication scheme based on STM32 Modbus-PROFIBUS motor protection controller is proposed.

KEYWORDS

Modbus; Profibus; Motor protection; STM32

1. INTRODUCTION

DCS system as an industrial commonly used automation control system, has the characteristics of "information centralized, control decentralized", a complete DSC system is usually composed of the following five parts: controller, control node, man-machine interface, communication network, data storage and processing. The research content of this paper is mainly aimed at the communication network and data storage, the controller, the control node and the man-machine interface module are not discussed. At present, domestic manufacturers generally use MODBUS communication protocol for motor protection controller communication standards, which is simple and easy to use, low cost, suitable for many small and medium-sized systems, but its reliability is low, lack of data encryption and authentication mechanism, and limited scalability, for large-scale systems have certain limitations. Profibus communication protocol, as the earliest communication protocol, has many advantages such as high flexibility, good reliability, strong openness and so on. It has a strong universality among mature foreign products, but it also has many disadvantages, such as complex configuration and high cost. At present, VPC3 chip of Siemens is usually used as the communication protocol encapsulation chip. However, its price is high and it is not friendly to low-cost products. Therefore, for cost consideration, this paper uses MODBUS as the bottom layer and adds Profibus communication protocol module to complete the motor protection controller supporting dual communication protocols.

2. OVERVIEW OF DUAL COMMUNICATION PROTOCOLS

2.1. Principle Analysis of Modbus Technology

2.1.1. Overview of Modbus

In 1979, the German Modcion company released the Modbus communication protocol, its simple and easy to use characteristics immediately received extensive attention, the international standardization organization I.S.O in the open system interconnection reference model will network system structure planning for 7 layers of ISO/OSI model [1], and Modbus communication protocol only occupies its 3 layers. Physical layer, data connection layer and application layer, which also makes Modbus has a very simple working environment and low cost, the OSI model diagram and the OSI model comparison diagram are shown in Figure 1.1, 1.2.

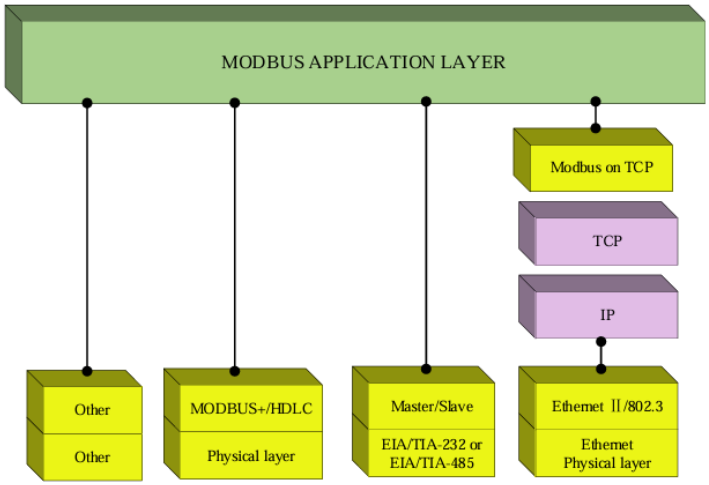

Figure 1.1. OSI model diagram of Modbus

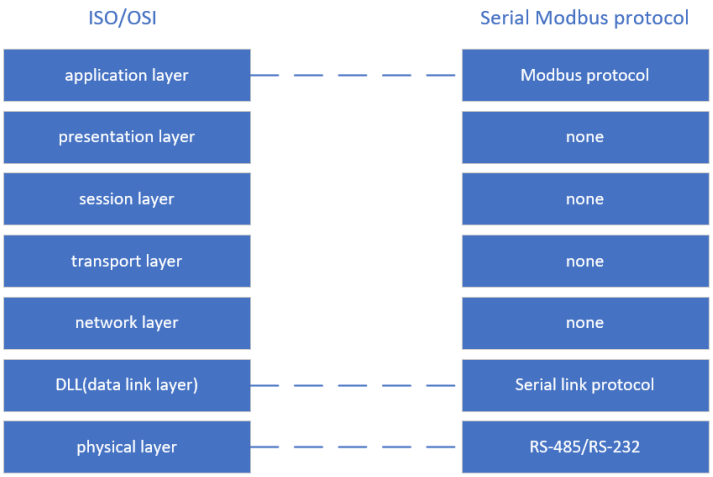

Figure 1.2. Comparison between Modbus model and OSI

At the early stage of design, Modbus protocol was used for data transmission through RS-232 protocol, but due to the limitations of short transmission distance and slow transmission speed, by the early 1980s, RS-485, which can support multiple node loads, communication distance and maximum transmission rate up to 10Mbps, replaced RS-232 in the Modbus communication system [2-4]. And Modbus communication uses the "call-answer" mode, perfectly fit the RS-485 communication protocol, the current Modbus protocol is allowed to communicate in a variety of network architecture, including PLC, HMI and various I/O interfaces [5-8].

2.1.2. Modbus communication principle

Modbus communication adopts the communication principle of "one master and many slaves". In the whole communication network, there are 247 slave devices at most. Each device has a separate slave address, that is, the "name" of each slave address. The host can call the slave through broadcast. After receiving the message, it can judge the communication object of the host according to the address, and then carry out the next operation. The specific communication network is shown in Figure 1.3.

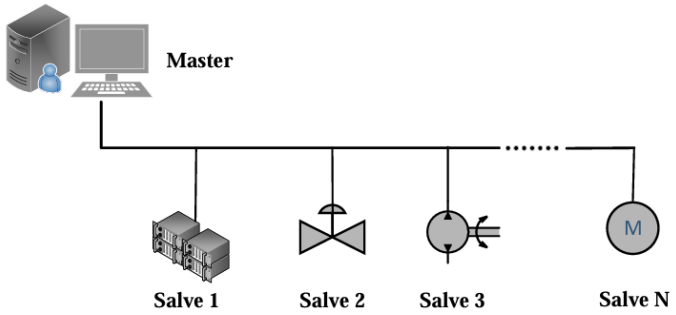

Figure 1.3. Modbus network topology diagram

The Modbus packet is divided into four parts: address field, function code, data field, and check field. The structure of the information frame is shown in Figure 1.4.

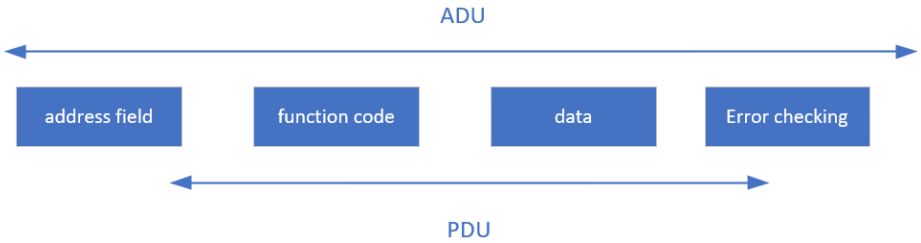

Figure 1.4. Modbus information frame

Address domain [9]: The "name" area used by the host to domain the communication between slave devices. Its size range is 0-255. Each slave has its own unique address. After receiving the host packet, it parses the packet content and returns to the host.

Function code [10]: The function code is generally two bytes, the first must be 0, and the last 7 bits are the specific function of the function code, that is, it can represent a maximum of 127 functions. The function code not only has the function of expressing effect, but also constitutes the second packet inspection layer. If the function code of the return message to the host is different from the function code of the host to send, the frame of the packet is invalid. Table 1.1 shows some function codes of Modbus.

Table 1.1. Modbus partial function codes

Function codes	Function
0x01	Read coil register
0x02	Read the discreteinput register
0x03	Read hold register
0x04	Read input register
0x05	Write a single coil register
0x06	Write a single hold register
0x0F	Write multiple coil registers
0x10	Write multiple hold registers

Data domain: The data domain stores the data content returned to the host for query, generally for values, setting points or device addresses.

Check domain [11]: Noise and interference is an unavoidable existence in the process of communication. CRC check is generally used in Modbus communication protocol to judge whether this frame message is complete and error-free, so as to improve the stability of the overall communication.

2.1.3. Frame communication in Modbus-RTU

In the whole communication process, if the concept of time is abandoned, it will be found that all the packets will become a series of bytes of data with uncertain length, and it is impossible to judge the start bit and end bit of the frame. In order to solve this series of problems, the concept of packet frame interval is introduced. Modbus-ASCII uses longitudinal redundancy check (LRC check), which stipulates that the transmission time between single byten is T, the calculation formula is as follows:

$$T = \frac{1}{\text{Baud}} \tag{1-1}$$

Where Baud represents the baud rate and has two important intervals in Modbus-RTU, namely T1.5 and T3.5. T1.5 represents the maximum transmission time interval between bytes in a frame. If the time exceeds 1.5T, packet loss will be determined for this frame data, and the system will discard this frame data by default. The specific description of 1.5T frame interval is shown in Figure 1.5.

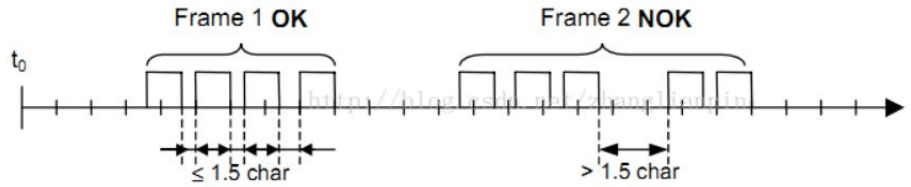

Figure 1.5. 1.5T frame interval

T3.5 interval represents the minimum interval time between two frames of data. Modbus-RTU stipulates that when a serial port receives a series of packets, when the two-byte interval time is greater than 3.5T, it will be judged as two frames of packets on the left and right ends. The description of the 3.5T interval is shown in Figure 1.6.

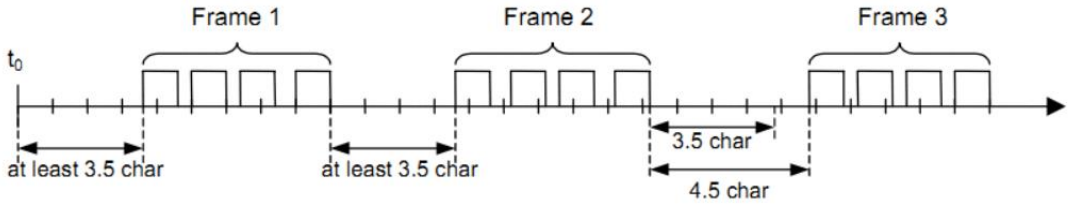

Figure 1.6. 3.5T frame interval

2.2. Profibus Technical Principle Analysis

2.2.1. Profibus Overview

Profibus originated from a communication protocol developed by the German Association of Electrical and Electronic Manufacturers in 1989 to solve the communication problem between different devices, Currently has been widely used in the field of industrial automation, the most widely used Profibus protocol is divided into three categories: Profibus-DP(Distributive Peripheral), Profibus-PA(Process Automation) and Profibus-FMS(Fieldbus Message Specification) [12], They are used in different scenarios in the industrial field, and each protocol is introduced below.

(1) Profibus-DP

Profibus-DP is mainly used in field level industrial bus communication. DP stands for "Distributed Peripherals", so Profibus-DP is often referred to as a distributed device bus [13]. It enables simple, fast, and stable periodic information exchange between master and slave stations. Profibus-DP usually uses RS485 twisted pair wire, optical cable and cable as the transmission medium, the communication rate is between 9.6k-12M, and the diagnosis, alarm and communication function between the master station and the slave station can be realized through simple configuration. As a high-speed industrial bus, the speed, reliability and real-time requirements are very high, so Profibus-DP will sacrifice the transmission distance to improve the communication rate.

(2) Profibus-PA

Profibus-PA is a communication protocol suitable for the field of process automation, using the bus power supply method in the physical layer, supporting long-distance transmission, up to 32 devices can be linked on a kilometer bus, and its communication rate is fixed at 31.25Kbps, so compared with Profibus-DP, it has a stable transmission, The advantages of anti-interference ability are strong, and it is used for information interaction between devices, such as pressure and temperature sensors.

(3) Profibus-FMS

Profibus-FMS is the predecessor of Profibus-DP, used to complete the workshop monitoring level communication requirements, the use of asynchronous communication transmission mode, support a variety of data transmission rates, and from the perspective of the amount of data transmission is much higher than the field series transmission, while using the error detection and correction mechanism to ensure the reliability of the transmitted data. To sum up, PA communication protocol is mostly used for data interaction communication between slave stations, while FMS communication protocol can only be used for workshop information interaction between master and master stations, and is not applicable to the master-slave station communication of motor protection controller studied in this paper. Therefore, the application of Profibus-DP communication protocol in click protection control and protocol messages will be introduced in the following sections.

2.2.2. Profibus-DP communication principle

Profibus-DP adopts the communication mode of communication between master and slave stations, and the master stations are divided into a class I master station and a class II master station. The first type of master station is the central processor, which sends the command of collecting message to the slave station and analyzes the message. The typical one type of slave station has PC and PLC. The second type of master station plays the role of selecting and installing the slave station. On the whole bus, each device sends back data and the format of the message is different. The second type of master station interprets the information of the slave station device through the configuration file, and then upload the first type of master station to play the role of intermediate monitoring. As the contact point of the whole communication network, each information is collected and stored by the slave station equipment, and sent to the master station after the master station sends a request signal, or the master station sends a control signal to the slave station to control the device.

In the process of communication between the slave station and the master station, the bottom layer adopts the UART format to transmit the data. Each character has a start bit, eight data bits, one check bit and one stop bit.

2.2.3. Profibus-DP communication mechanism

In the process of communication, Profibus supports data transmission between multiple master stations and multiple slave stations, and the master stations pass the control right through token. When the master station No. 1 sends the message to each slave station, the slave station will judge the command sent by the master station to the slave station according to the message address, and then make corresponding actions. However, there is only one token in the master station from a macro

perspective, which is transmitted through the way of time polling, and only the master station with the token has the permission to search down. If the master station does not establish communication with the slave station within the time when it holds the token, it can only communicate with the slave station again when it holds the token next time.

In the process of master-slave station communication, the industrial level communication process needs high real-time and stability, so the communication time between the master and slave station has strict control. Each time before the master station and the slave station communication need to wait for a certain time to ensure that there is no data flow at both ends of the communication device, this time is called synchronization time TSYN, the typical value is 33TBIT, after the master station sends a frame to the slave station, the slave station waits for a response time TSDR of the slave station and then returns the response frame to the master station, the typical value is 11TBIT. If the master station has not received the response frame from the slave station within a certain time T, it is determined that a packet loss has occurred, and the time of T time is the transmission time of the master and slave station plus the delay time of the slave station.

2.2.4. Profibus-DP communication message

In the process of communication, packets are an essential medium. In Profibus-DP, packets are mainly divided into the following five categories:

(1) Fixed-length packet SD1

The main purpose of the SD1 packet is to establish the communication relationship between the master and slave stations, and there is no data transmission in the content. When the communication between the master and slave stations is established, the master station will send the communication packet until the slave station responds. The format of the packet is as follows.

Table 1.2. SD1 packet format

SD1	DA	SA	FC	FCS	ED
0x10	XX	XX	XX	XX	0x16

(2) Variable Data field message SD2

SD2 message is the main data transmission message in the whole Profibus-DP communication.

Table 1.3. SD2 packet format

SD2	LE	LEr	SDr	DA	SA	FC	DU	FCS	ED
0x68	XX	XX	0x68	XX	XX	XX	X..X	XX	0x16

(3) Fixed data field SD3

Table 1.4. SD3 packet format

SD3	DA	SA	FC	DU	FCS	ED
0xA2	XX	XX	XX	X..X	XX	0x16

(4) Token frame SD4

Table 1.5. SD4 packet format

SD4	DA	SA
0xDC	XX	XX

(5) Respond to frame SC

Table 1.6. SC packet format

SC
0xE5

The meanings of each internal parameter are as follows:

Table 1.7. Parameter meaning

LE	The value is LE=DA+SA+FC+DU. The length cannot exceed 250. LEr is the same as LE
DA	Destination address of the packet, with the lowest seven bits representing the real address and the highest being the extended address. 0: no DSAP, 1: DSAP.
SA	Source address of a packet. The lowest seven bits indicate the actual address, and the highest bits indicate the extended address. 0: no SSAP, 1: SSAP.
FC	Function code
FCS	The frame check bit, which is the binary algebraic sum of DA, SA, FC, DU
DU	The data field, which is the most important part of the packet

FC function code description:

Table 1.8. FC meaning

B7	B6	B5	B4	B3	B2	B1	B0
0	1: Reques t frame	FCB, FCVflag		Function code			
	0: Respon se frame						

FCB, FCV sign meaning description:

Table 1.9. FCB, FCV meaning

B6	B5	B4	Meaning
0	0	0	Slave station
	0	1	The main station is not ready
	1	0	Master station ready, no token
	1	1	Master station ready with token
B6	B5	B4	Meaning
1	0		FCB is unavailable
	1		FCB available
	X		Determine FCB based on FCV

The FC function code is defined with the lower four digits:

Table 1.10. The fourth bit of FC function code is defined

Function code	Request frame B6=1	Response frame B6=0
0		Positive confirmation: OK
1		Negative confirmation: Error
2		Negative confirmation: no corresponding source
3		Negative confirmation: SAP is not active
4	Low SDN	
5		
6	SDN high	
7	SRD multicast	
8		SRD Low priority response
9	FDL to be answered	Negative confirmation: No response
A		High priority response from SRD
B		
C	Low SRD	SRD Low priority Response: passive
D	High SRD	SRD High priority Response: Passive
E	ID request to be answered	
F		

3. PROFIBUS PROGRAMMING

3.1. Overall Framework Analysis

At present, Profibus has been applied in many industrial systems, but it has not been used on a large scale due to cost and complexity. The current PROFIBUS-DP uses VPC3 chip of Siemens as the package of the protocol. As of May 2024, the price of VPC3 chip is floating at 150 yuan. It is already a very high price for a product development. The click protection controller designed in this paper based on Modbus-Profibus adopts STM32 internal resources to package the protocol, which reduces the cost to a large extent. The program will be explained from the perspective of process design and code analysis. The overall flow chart is shown in Figure 2.1.

Since industrial level communication requires high real-time and accuracy, it is necessary to ensure the accuracy and real-time performance of the message before analyzing the message, and it is necessary to determine whether the problem of packet loss occurs and whether the communication is normal at the present stage. Therefore, a large part of the overall communication process is to determine the authenticity of the message obtained and whether it is the information intended to be expressed in communication transmission. In this section, we only consider the solution of the communication packet loss problem, and do not consider the signal distortion and error caused by noise. After judging whether the communication information is lost, the message is interpreted in detail to complete the design of the whole communication module.

3.2. Interpretation of Detailed Steps

3.2.1. Communication stability detection

The system needs to delay a period of time after initialization to prevent data flows in the channel from misjudging the received packets. The delay time does not need to be too long. In this paper, a delay of 2000ms is selected to completely clear the data flow in the channel. Then enter the judgment of receiving and sending wait time and communication delay time. In this paper, the receiving and sending wait time is determined by using STM32's own TIM timer. When the timer reaches the set time, the interrupt service function automatically increases the receiving and sending wait time (m_udUsart1WaitUs). Only when the sending and receiving waiting time is greater than the

communication delay time (m_udUsart1DelayUs), the transmission mode will be entered. The preparation time before communication is shown in Figure 2.2.

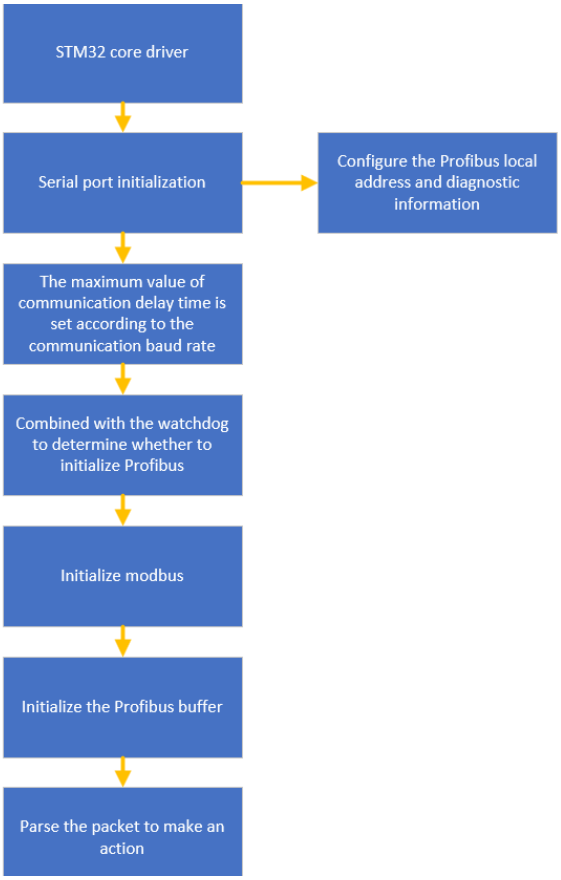

Figure 2.1. Overall flow chart of Profibus communication

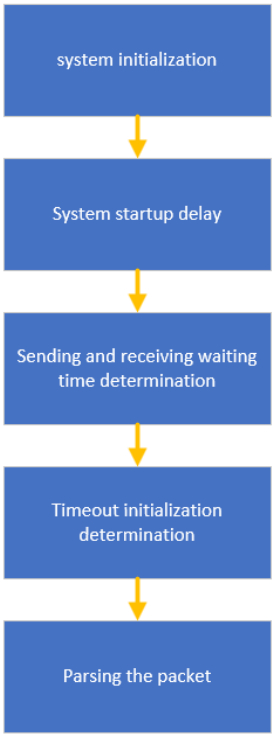

Figure 2.2. Preparation before Profibus communication

3.2.2. Packet parsing

After the communication stability test is passed, the 485 communication module is adjusted to the receiving state, and the receiving counter is set. When a byte is received, the timer is automatically increased by one. The timer is used to judge the validity of subsequent Profibus-DP messages. Before the data exchange between the master station and the slave station, it is also necessary to carry out configuration, diagnosis and parameterization and other related configurations. In the whole Profibus communication network, it is necessary to make clear which master station needs to communicate with which slave station first, which is equivalent to making a call before it is clear who is calling whom. The master station sends connection request message SD1 to the slave station. This kind of transmission is sent through the form of broadcast, and the content contains the address information of the master station. The address information and function code of the slave station can be received by all the slave stations. When receiving a complete frame of data beginning with 10 and ending with 16, the slave station will start to analyze it. If the received address does not match its own address, it will not take any action. Answer the master station The slave station is ready to receive the message. Then the master station will also send configuration packets and parameterization packets. Only when the three types of packets pass at the same time, the sent request data packets will be responded to. The specific flow chart is shown in Figure 2.3.

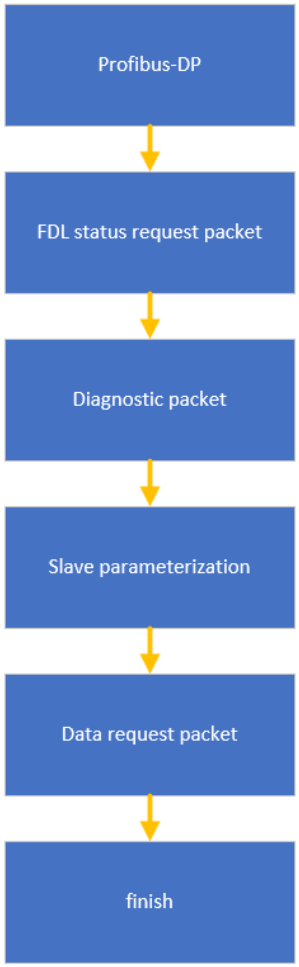

Figure 2.3. Profibus communication flow

Note that in the communication process, FDL status request messages, diagnostic messages and parameterized messages are equivalent to keys, unlocking the communication lock in order. When no FDL status request messages are carried out, diagnostic messages are directly sent, and the slave station does not carry out any operation, which is reflected in the code as FDL request message flag bit, diagnostic message flag bit, etc. Therefore, When the communication address of the slave station

is changed or the watchdog is triggered by the device failure, FDL request and configuration parameterization request need to be re-performed, which is also a reflection of the stability and efficiency of Profibus. In this paper, communication is used to control and detect remote signal, telemetry and remote control of motor protection controller. Telemetry and remote signal data are collected by Modbus and stored in STM32 internal resources. Profibus-DP performs a forwarding function, which is equivalent to realizing a Modbus-Profibus gateway function. This chapter only analyzes how Profibus collects and sends data. The main functions used in this paper and their specific descriptions are shown in the following table. Function definition:

Table 2.1. function definition

Function name	Description
System_Init	System initialization
m_ucUsartClk	Usart Clock Judgment
m_ucProfibusBufOutUpdate	From station action flag
ProfibusBufOutDispose	Execute action functions
Usart1Main	Core serial function
Usart1ProfibusDP_Dispose	Parse message function
m_ucRXBuf_0	Determine the header type
ucDat_chack	Checksum diagnostics
m_ucUsartDiag	Configuration configuration

The main variables are defined as shown in the table below

Table 2.2. Variable definition

Variable names	Description
m_udUsart1WaitUs	Send and receive wait time
m_udUsart1DelayUs	Communicatio n delay time
m_ucUsart1Diag1	Diagnostic information
ucDataByteLen	Receive length
m_uwUsart1WatchDogTime	Watchdogtime
m_ucUsart1MinDelay	Minimum delay response time
ucDA	Master station address
ucSA	Slave station address
m_ucUsart1InConfigCnt	Enter the number of configurations
m_ucUsart1OutConfigCnt	Output the number of configurations
ucPowerOn	Power-on Stability flag
ucSlaveDiag	Diagnostic Markers
ucSetPrm	Parameterized flags
ucConfig	Configuration flags
udUsart1Addr	Local mailing address 3
udId	Native identifier
udUsart1BaudRate	Baud rate of local communication

3.2.3. Data feedback

In the previous article, the relevant process of PROFIBUS-DP has been roughly described. This section will describe how to send Modbus data collected through Profibus communication protocol. The relevant flow of Modbus communication is not introduced. Generally speaking, all collection communications send packets through time polling, collect telemetry data and remote communication data through data packets, and then the host computer analyzes the packets to get user data. The method used in this paper is also time polling, but for the direct application of Modbus communication,

the difference is that Modbus is used as the communication bottom layer. The telemetry and telemetry data are stored in STM32 internal resources, and the telemetry and telemetry data are refreshed after each recall. However, this approach in this paper also has drawbacks. For Siremote, there will be a slight delay time. The delay time lies in the fact that the data after storage is not the real-time data that is fully forwarded during each forwarding. The forwarding process is shown in Figure 2.4.

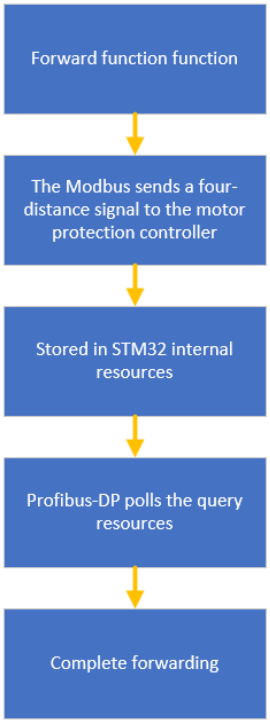

Figure 2.4. Profibus-modbus gateway process

When designing the forwarding flow, this paper finds that all the data collected by the motor protection controller is uint8_t. Therefore, in the forwarding process, this paper uses the query point table to convert all the data collected by modbus into floating-point data for forwarding, and the Profibus forwarding data are floating-point data for convenient calculation.

The main function definition of the forwarding module:

Table 2.3. function definition

mbh_send	Send frame command
mbh_exec	Parse frame command
mbh_timer3T5Isr	3.5T timing judgment
mbh_hook_rec02	Telexin data analysis
mbh_hook_rec03	Telemetry data parsing
Struct_init	Storage structure definition
hexToDecimal	Convert hexadecimal to decimal
convertValues	Splicing data

Main variable definitions:

Table 2.4. variable definition

hex_telemetry	Telemetry Array
remote_signaling	Remote_signaling array
FloatToUint8_t	Telemetry storage unit
state	modbus host status
txLen	The length of the frame you need to send
txCounter	bytes count has been sent
rxCounter	Receive count

4. RESULTS DISCUSSED

The collection and forwarding functions of modbus and Profibus-DP are completed through the above two methods. The following is a serial debugging assistant to simulate the master station of Profibus-DP for data collection. For Profibus-DP, the order of sending packets is crucial, and it needs to be sent in full accordance with the order. In this communication, the address of the master station is set to 02, the address of the slave station is 04, and the connection, configuration, parameterization and diagnosis messages are sent. The sending order and messages are as follows:

Send :10 02 04 49 4F 16 // View slave station status

Send :68 05 05 68 82 84 6D 3C 3E ED 16 // Diagnostic message

Send :68 0C 0C 68 82 84 5D 3D 3E B8 15 17 0B 00 08 00 D5 16 // Parameterized message

Send :68 07 07 68 82 84 7D 3E 3E 11 27 37 16// Configures the message

Send :68 05 05 68 02 04 5D 00 00 63 16 // Telexin data

Send: 68 05 05 68 02 04 5D 00 01 64 16 // Telemetry data

The returned data is shown in Figure 3.1

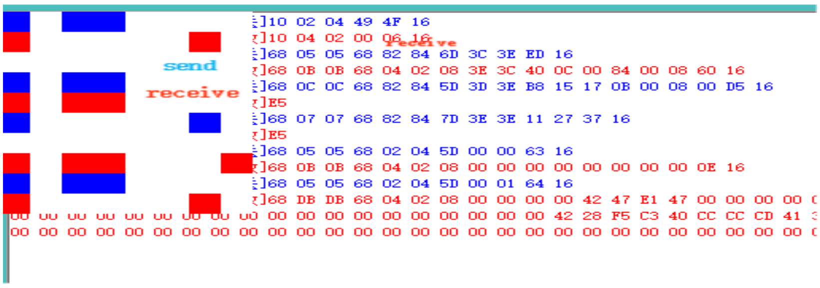

Figure 3.1. Profibus communication example

REFERENCES

[1] Yang Haodong. Design and Implementation of Electrical Information Acquisition Subsystem based on Modbus [D]. University of Electronic Science and Technology of China, 2019:6-9.

[2] HAO Z J, ASADULLAH A, WAWALE S. Application of MODBUS double-layer communication network technology in intelligent management of urban traffic equipment [J]. International Journal of System Assurance Engineering and Management, 2021, 13(Suppl 1): 25-28.

[3] WAN Y, FENG X N, CHEN Y X. A Dual Detection Method for Siemens Inverter Motor Modbus RTU Attack [J]. Journal of Computer and Communications, 2021, 09(07): 44-48.

[4] PALLAVI D. Design and Implementation of Circuit Analysis System for Industrial Watt-hour Meter based on MODBUS Protocol [J]. International Journal of Power and Energy Engineering, 2020, 2(1): 15-28.

[5] WENQIAN F, YINGXU L, ZENGHUI L. Vulnerability mining for Modbus TCP based on exception field positioning [J]. Simulation Modelling Practice and Theory, 2020: 15- 18.

[6] CHRISTOPHER P, TERRY G, SAJAL B. Fooling the Master: Exploiting Weaknesses in the Modbus Protocol [J]. Procedia Computer Science, 2020, 171(C): 35-46.

[7] Zong Zhenyan. Design of Fault Automatic Diagnosis System for Electric control Board of Variable frequency Air Conditioner [D]. Shandong University of Science and Technology, 2020:13-28.

[8] WANG Chao. Research on Modbus Communication Protocol and its Application in Oilfield Control System [J]. Instrument User, 2014, 21(02): 51-53.

[9] Lv Guohua, Cheng Guanghe, Fangli Zhen. Implementation of Modbus Communication Based on ARM7 microprocessor [J]. Information Technology and Informatization, 2010(05): 45-47.

[10] Zhu Jing, Qi Xiangdong. Communication between IFIX and PLC Based on OPC, Modbus and ModbusTCP/IP [J]. Electronic Devices, 2013, 36(2): 260-264.

[11] Dou Yan-nan, Meng Qing-Yao, Ding Qi. Analysis of Modbus Protocol and Security Based on Wireshark [J]. Network Security Technology and Application, 2021(06):4-6.]

[12] Wang Zhebei, Li Zhuo, Lu Haisong, et al. Overview of Typical Fieldbus protocols for Communication networks [J]. Industrial Control Computer, 2021, 34(11):5-8+11.

[13] Wang P, Zhang Y F, Guo H. et al. Design of Profibus-DP Wireless Communication Module [J]. 2nd International Conference on Signal Image Processing and Communication, 2022, 12246:156-160.