

ICS 25.040

CCS N 10



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 19582.3-2008

**Modbus industrial automation network specification -- Part 3:
Modbus protocol implementation guide over TCP/IP
(English Translation)**

Issued on: February 27, 2008

Implemented on: September 1, 2008

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China**

Table of Contents

Foreword...	3
Introduction...	5
1 Scope...	6
2 Client/Server Model...	6
3 Normative References...	7
4 Abbreviations...	7
5 Background Overview...	8
5.1 Protocol Description...	8
5.2 Modbus Function Code Description...	11
6 Functional Description...	11
6.1 Modbus Component Structure Model...	11
6.2 TCP Connection Management...	15
6.3 Use of TCP/IP Stack...	22
6.4 Communication Application Layer...	27
7 Implementation Guidelines...	41
7.1 Object Model Diagram...	41
7.2 Implementation Class Diagram...	46
7.3 Sequence Diagrams...	47
7.4 Class and Method Description...	50

1 Scope

This Part describes the Modbus message transmission service over TCP/IP and provides reference information to assist software developers in implementing this service. This Part does not include the encoding of Modbus function codes; for this information, please refer to GB/T

19582.1-2008.

This Part provides a comprehensive and accurate description of the implementation of the Modbus message transmission service. Its purpose is to facilitate interoperability between devices using the Modbus message transmission service.

This Part consists of three main parts.

---An overview of the Modbus protocol over TCP/IP;

- A functional description of the Modbus client, server and gateway implementations;
- Suggested implementation guidelines for an object model of a Modbus implementation example.

2 Client/Server Model

The Modbus message transmission service provides client/server communication between devices connected to TCP/IP Ethernet (see Figure 1).

This client/server model is based on 4 message types.

- Modbus request;
- Modbus confirmation;
- Modbus instruction;
- Modbus response.

Figure 1 -- Modbus Client/Server Model

Modbus request is a message sent by the client over the network to initiate transaction processing;

Modbus instruction is a request message received by the server;

Modbus response is a response message sent by the server;

Modbus confirmation is a response message received by the client.

The Modbus message transmission service (client/server model) is used for real-time information exchange.

- Between two device application programs;
- Between a device application and other devices;
- Between an HMI/SCADA application program and a device;
- Between a PC and a device program providing online services.

3 Normative References

The clauses in the following documents become clauses of this Part through the reference in this Part of GB/T 19582. For dated references, subsequent amendments (excluding errata) or revisions do not apply to this Part; however, parties agreeing to this Part are encouraged to investigate whether to use the latest versions of these documents. For undated references, the latest version applies to this Part.

GB/T 19582.1-2008 Modbus Industrial Automation Network Specification - Part 1. Modbus

Application Protocol

RFC1122 Requirements for Internet Hosts - Communication Layers

4 Abbreviations

ADU (Application Data Unit)

IETF (Internet Engineering Task Force)

IP (Internet Protocol)

MAC (Medium Access Control)

MB (Modbus)

MBAP (Modbus Application Protocol)

PDU (Protocol Data Unit)

PLC (Programmable Logic Controller)

TCP (Transport Control Protocol)

BSD (Berkeley Software Distribution)

MSL (Maximum Segment Lifetime)

SCADA (Supervisory Control and Data Acquisition)

5.1.1 Overall communication structure

See Figure 2 ~ Figure 3.

The Modbus TCP/IP communication system may include different types of devices.

---Modbus TCP/IP client and server devices connected to the TCP/IP network;

---Interconnection devices, such as bridges, routers or gateways that interconnect the TCP/IP network and a serial link subnet, which allows Modbus serial link client and server terminal devices to be connected.

Figure 3 -- General Modbus Frame

Modbus protocol defines a simple protocol data unit (PDU) independent of the fundamental communication layer. Modbus protocol mappings on a specific bus or network can introduce some additional fields into the application data unit (ADU).

The client initiating Modbus transaction processing establishes a Modbus application data unit.

This function code instructs the server what operation to perform.

5.1.2 Modbus application data unit over TCP/IP

See Figure 4.

This clause describes the encapsulation of Modbus request or response over a Modbus TCP/IP network.

Figure 4 -- Modbus Request/Response over TCP/IP

A special header is used on TCP/IP to identify Modbus application data unit. This message header is called MBAP header (Modbus Application Protocol header).

This message header differs from the Modbus RTU application data unit used over serial links in several ways.

---The Modbus "slave station address" field, typically used on Modbus serial links, is replaced by a single-byte "unit identifier" in the MBAP message header. This "unit identifier" is used for communication via devices such as bridges, routers and gateways, which use a single IP address to support multiple independent Modbus terminal units.

---All Modbus requests and responses are designed in a way that allows the receiver to verify the end of the message. For Modbus PDU with a fixed-length function code, the function code alone is sufficient. For function codes transmitting a variable amount of data in a request or response, the data field includes the number of bytes.

---When transmitting Modbus protocol via TCP, even if the message has been divided into multiple information packets for transmission, additional length information must be transmitted in the MBAP header, so that the receiver can identify message boundaries.

The existence of explicit and implicit length rules, and the use of CRC-32 error checking codes (on Ethernet), reduce undetected request or response message errors to an extremely low level.

5.1.3 MBAP header description

The MBAP header includes the following fields, as shown in Table 1.

Table 1 -- Fields of MBAP Header

The message header is 7 bytes long.

Transaction processing identifier. used for transaction processing pairing. In the response, the

Modbus server replicates the transaction processing identifier from the request.

Protocol identifier. used for multiplexing within the system. A value of 0 is used to identify the