



# 中华人民共和国国家标准化指导性技术文件

GB/Z 19582.3—2004

---

## 基于 Modbus 协议的工业自动化网络规范 第 3 部分: Modbus 协议在 TCP/IP 上的 实现指南

Modbus industrial automation network specification—  
Part 3: Modbus protocol implementation guide over TCP/IP

2004-09-21 发布

2005-03-01 实施

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

## 目 次

|                         |    |
|-------------------------|----|
| 前言 .....                | Ⅲ  |
| 1 范围 .....              | 1  |
| 2 客户机/服务器模型 .....       | 1  |
| 3 规范性引用文件 .....         | 2  |
| 4 缩略语 .....             | 2  |
| 5 背景概要 .....            | 2  |
| 5.1 协议描述 .....          | 2  |
| 5.2 Modbus 功能码描述 .....  | 4  |
| 6 功能描述 .....            | 4  |
| 6.1 Modbus 组件结构模型 ..... | 4  |
| 6.2 TCP 连接管理 .....      | 6  |
| 6.3 TCP/IP 栈的使用 .....   | 10 |
| 6.4 通信应用层 .....         | 13 |
| 7 实现指南 .....            | 22 |
| 7.1 对象模型图 .....         | 22 |
| 7.2 实现类的图 .....         | 26 |
| 7.3 序列图 .....           | 27 |
| 7.4 类和方法的描述 .....       | 30 |

## 前 言

本指导性技术文件包括两个通信规程中使用的 Modbus 应用层协议和服务规范：

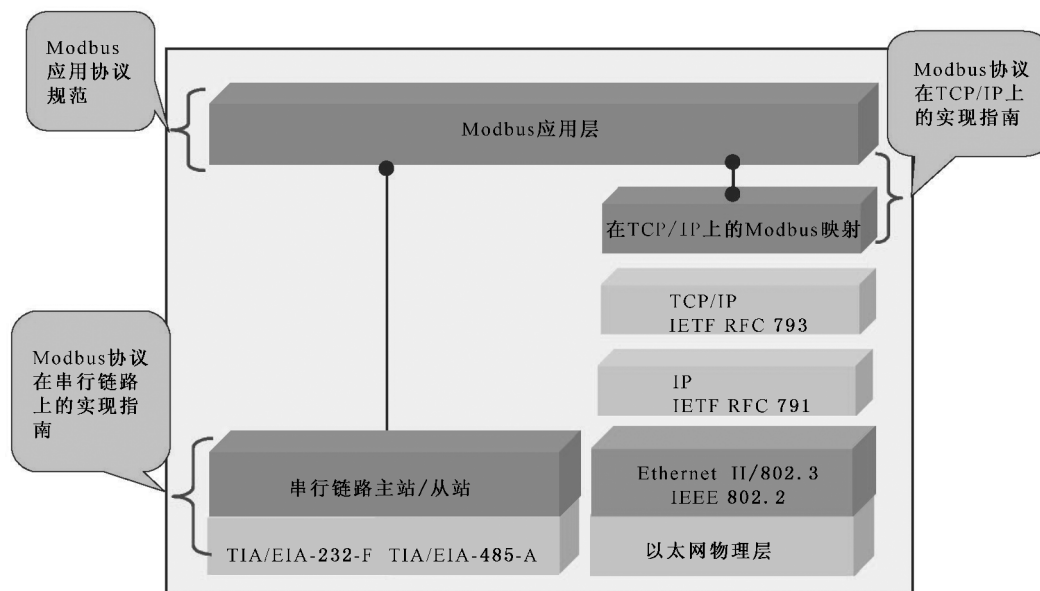
——串行链路上的 Modbus

Modbus 串行链路基于 TIA/EIA 标准：232-F 和 485-A。

——TCP/IP 上的 Modbus

Modbus TCP/IP 基于 IETF 文件：RFC793 和 RFC791。

串行链路和 TCP/IP 上的 Modbus 是根据相应 ISO 分层模型说明的两个通信规程。下图强调指出了本指导性技术文件的主要部分。深色方框表示规范，浅色方框表示已有的国际标准（TIA/EIA 和 IETF 标准）。



基于 Modbus 协议的工业自动化网络规范分为三部分。

——第 1 部分：Modbus 应用协议

——第 2 部分：Modbus 协议在串行链路上的实现指南

——第 3 部分：Modbus 协议在 TCP/IP 上的实现指南

第 1 部分描述了 Modbus 事务处理；第 2 部分提供了一个有助于开发者实现串行链路上的 Modbus 应用层的参考信息；第 3 部分提供了一个有助于开发者实现 TCP/IP 上的 Modbus 应用层的参考信息。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京交通大学现代通信研究所、上海自动化仪表股份有限公司、施耐德电气（中国）投资有限公司、冶金工业钢铁研究总院、宝钢集团上海宝信软件股份有限公司。

本部分主要起草人：欧阳劲松、孙昕、刘铁椎、冯晓升、王勇、张荣生、丛力群、段永康。

# 基于 Modbus 协议的工业自动化网络规范

## 第 3 部分: Modbus 协议在 TCP/IP 上的实现指南

### 1 范围

本部分叙述了 TCP/IP 上的 Modbus 报文传输服务,提供参考信息以帮助软件开发者使用这种服务。本标准不包括 Modbus 功能码的编码内容,有关这些内容见 GB/Z 19582.1—2004《基于 Modbus 协议的工业自动化网络规范 第 1 部分: Modbus 应用协议》。

本部分描述了 Modbus 报文传输服务的实现。其目的是促进在使用 Modbus 报文传输服务的设备之间的互操作。

本部分主要由三部分组成:

- 在 TCP/IP 上的 Modbus 协议概述;
- Modbus 客户机和服务器实现的功能描述;
- 针对一个 Modbus 实现实例的对象模型建议的实现准则。

### 2 客户机/服务器模型

Modbus 报文传输服务提供设备之间的客户机/服务器通信,这些设备联接在一个 Ethernet(以太网)TCP/IP 网络上(见图 1)。

这个客户机/服务器模型基于 4 种报文类型:

- Modbus 请求
- Modbus 证实
- Modbus 指示
- Modbus 响应

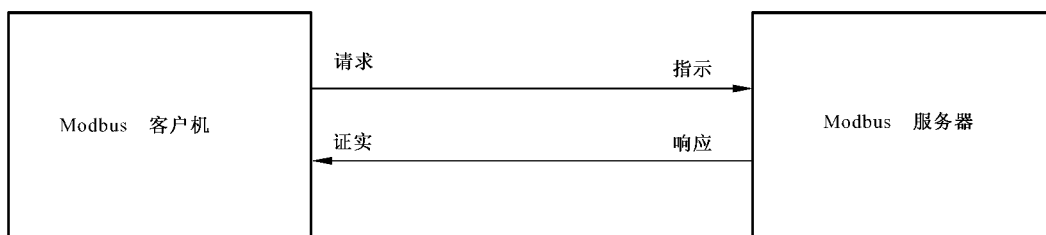


图 1 Modbus 客户机/服务器模型

Modbus 请求是客户机在网络上发送用来启动事务处理的报文;

Modbus 指示是服务器侧接收的请求报文;

Modbus 响应是服务器发送的响应报文;

Modbus 证实是在客户机侧接收的响应报文。

Modbus 报文传输服务(客户机/服务器模型)用于实时信息交换:

- 在两个设备应用程序之间;
- 在设备应用和其他设备之间;
- 在 HMI/SCADA 应用程序和设备之间;
- 在一个 PC 和一个提供在线服务的设备程序之间。