



中华人民共和国国家标准

GB/T 19582.1—2008
代替 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

Modbus industrial automation network specification—
Part 1: Modbus application protocol

2008-02-27 发布

2008-09-01 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
引言	IV
1 范围	1
2 规范性引用文件	1
3 缩略语	2
4 背景概要	2
5 总体描述	3
5.1 协议描述	3
5.2 数据编码	4
5.3 Modbus 数据模型	5
5.4 Modbus 寻址模型	6
5.5 Modbus 事务处理的定义	7
6 功能码分类	8
6.1 公共功能码定义	8
7 功能码描述	9
7.1 01(0x01)读线圈	9
7.2 02(0x02)读离散量输入	11
7.3 03(0x03)读保持寄存器	12
7.4 04(0x04)读输入寄存器	14
7.5 05(0x05)写单个线圈	15
7.6 06(0x06)写单个寄存器	17
7.7 07(0x07)读异常状态(仅用于串行链路)	18
7.8 08(0x08)诊断(仅用于串行链路)	19
7.9 11(0x0B)获得通信事件计数器(仅用于串行链路)	23
7.10 12(0x0C)获得通信事件记录(仅用于串行链路)	24
7.11 15(0x0F)写多个线圈	27
7.12 16(0x10)写多个寄存器	29
7.13 17(0x11)报告从站 ID(仅用于串行链路)	30
7.14 20(0x14)读文件记录	31
7.15 21(0x15)写文件记录	33
7.16 22(0x16)屏蔽写寄存器	35
7.17 23(0x17)读/写多个寄存器	37
7.18 24(0x18)读 FIFO 队列	39
7.19 43(0x2B)封装接口传输	40
7.20 43/13(0x2B/0x0D)CANopen 通用引用请求和响应 PDU	42
7.21 43/14(0x2B/0x0E)读设备标识	42
8 Modbus 异常响应	46
附录 A(资料性附录) Modbus 保留的功能码、子码及 MEI 类型	48
附录 B(资料性附录) CANopen 通用引用命令	48
参考文献	49

前 言

GB/T 19582—2008《基于 Modbus 协议的工业自动化网络规范》分为三部分：

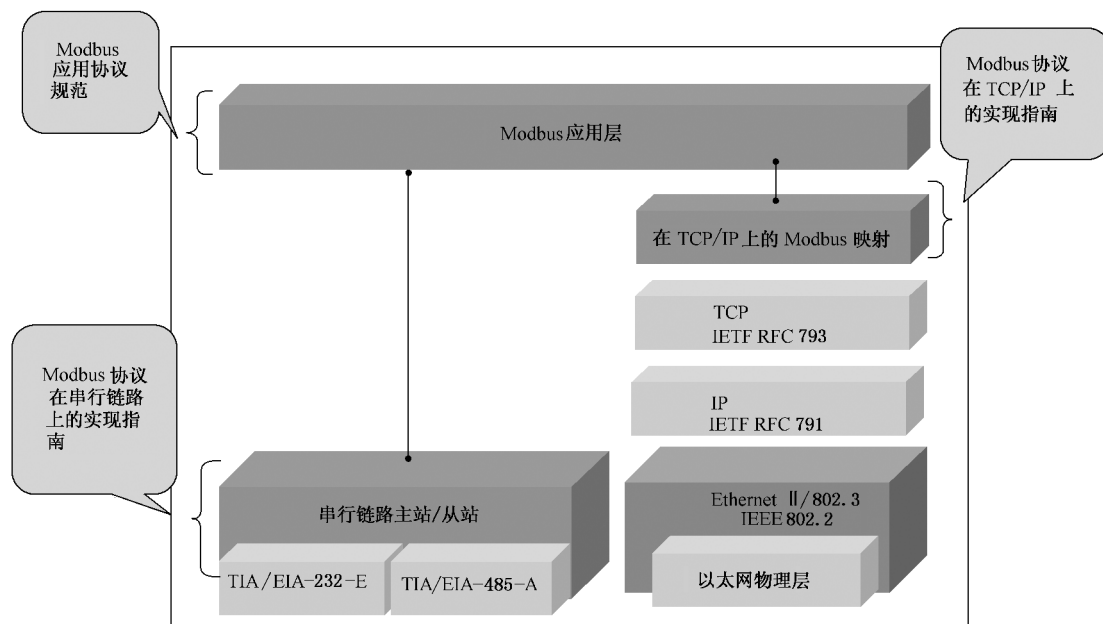
- 第 1 部分：Modbus 应用协议；
- 第 2 部分：Modbus 协议在串行链路上的实现指南；
- 第 3 部分：Modbus 协议在 TCP/IP 上的实现指南。

第 1 部分描述了 Modbus 事务处理；第 2 部分提供了有助于开发者在串行链路上实现 Modbus 应用层的参考信息；第 3 部分提供了有助于开发者在 TCP/IP 上实现 Modbus 应用层的参考信息。

GB/T 19582—2008 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-E 和 485-A。
- TCP/IP 上的 Modbus
Modbus TCP/IP 基于 IETF 标准：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 GB/T 19582—2008 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）。



本部分从实施之日起代替 GB/Z 19582.1—2004；GB/Z 19582.1—2004 并于该日起予以废止。

本部分的附录 A、附录 B 为资料性附录。

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第四分技术委员会归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、西南大学、上海自动化仪表股份有限公司、北京交通大学现代通信研究所、北京机械工业自动化研究所、国家继电器质量监督检验中心、中国四联仪器仪表集团有限公司、中海石油研究中心、西北工业大学、施耐德电气(中国)投资有限公司。

本部分主要起草人：王玉敏、柳晓菁、刘枫、包伟华、孙昕、刘云男、唐济扬、贺春、刘渝新、徐伟华、欧阳劲松、何军红、华镛、王勇。

GB/Z 19582.1 首次发布时间为 2004 年 9 月 21 日，本部分第一次修订。

引 言

GB/T 19582—2008 是对 GB/Z 19582—2004《基于 Modbus 协议的工业自动化网络规范》的修订,修订的依据是 IEC 61158 CPF15(FDIS):2006 实时以太网 Modbus-RTPS。本部分的结构与 GB/Z 19582.1—2004 基本一致,但在技术内容上对 GB/Z 19582.1—2004 进行了补充和完善。

基于 Modbus 协议的工业自动化网络规范

第 1 部分: Modbus 应用协议

1 范围

Modbus 是 OSI 模型第 7 层上的应用层报文传输协议,它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信,见图 1。

从 1979 年开始,Modbus 作为工业串行链路的事实标准,Modbus 使成千上万的自动化设备能够通信。目前,对简单而精致的 Modbus 结构的支持仍在增长。互联网用户能够使用 TCP/IP 栈上的保留系统端口 502 访问 Modbus。

Modbus 是一个请求/应答协议,并且提供功能码规定的服务。Modbus 功能码是 Modbus 请求/应答 PDU 的元素。本部分描述了 Modbus 事务处理框架内使用的功能码。

Modbus 应用层报文传输协议用于在通过不同类型的总线或网络连接的设备之间的客户机/服务器通信。

目前,通过下列方式实现 Modbus 通信:

- 以太网上的 TCP/IP,见 GB/T 19582.3。
- 各种介质(有线:EIA/TIA-232-E、EIA-422、EIA/TIA-485-A;光纤、无线等等)上的异步串行传输。
- Modbus+,一种高速令牌传递网络。

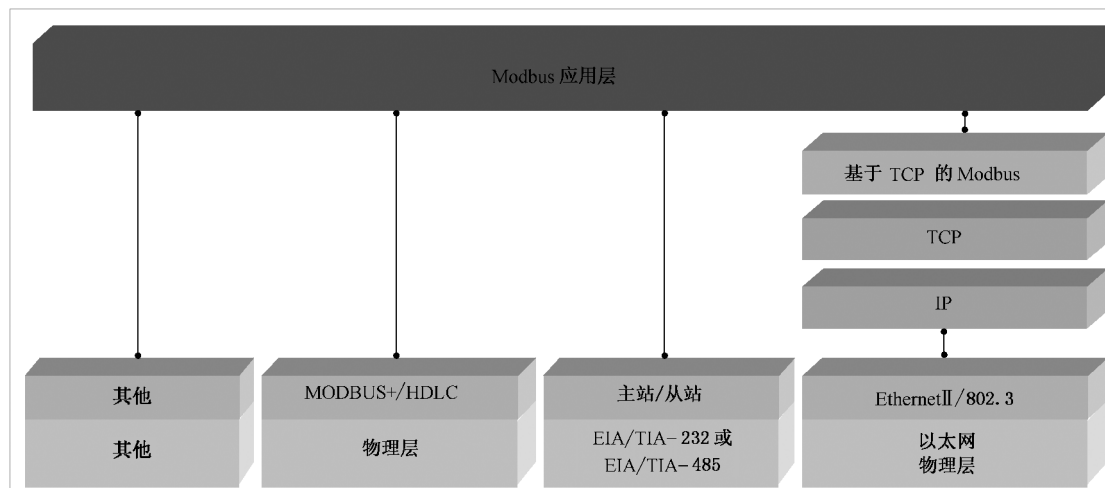


图 1 Modbus 通信栈

2 规范性引用文件

下列文件中的条款通过 GB/T 19582 的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 15969 可编程序控制器

RFC 791 Internet Protocol, Sep81 DARPA