

## 一文快速认识Modbus协议

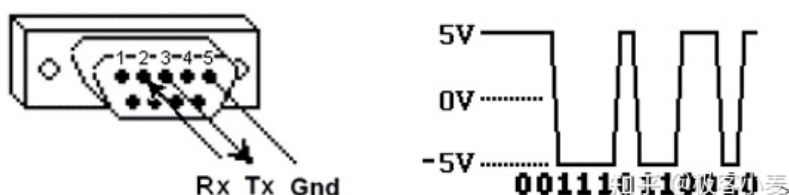
- [1 什么是Modbus?](#)
- [2 主从模式](#)
- [3 协议的分类](#)
  - [3.1 Modbus ASCII](#)
  - [3.2 Modbus RTU](#)
  - [3.3 Modbus TCP](#)
  - [3.4 Modbus Plus](#)
- [4 libmodbus](#)
- [5 freemodbus](#)

## 1 什么是Modbus?

Modbus 是 Modicon（施耐德）公司于1979年开发的**串行通信协议**。它最初设计用于公司的可编程逻辑控制器（PLC）。Modbus是一种开放式协议，支持使用**RS232/RS485/RS422**协议的串行设备，同时还支持调制解调器。它的简单性以及制造商可以免费将其纳入其产品的事实使其成为连接工业电子设备的最流行的方法。Modbus 比其他通信协议使用的更广泛的主要原因有以下几点：

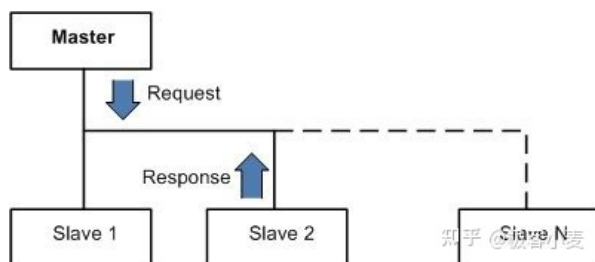
- 公开发表并且无著作权要求；
- 易于部署和维护；
- 对供应商来说，修改移动本地的比特或字节没有很多限制；

Modbus 通过设备之间的串行线进行**数据传输**。最简单的设置是使用一根串行电缆连接两个设备（主设备和从设备）上的串行端口。数据以称为**比特的 1 和 0**的序列发送。每个位都作为电压发送。0 被发送为正电压，1 被发送为负电压。如下图所示；



## 2 主从模式

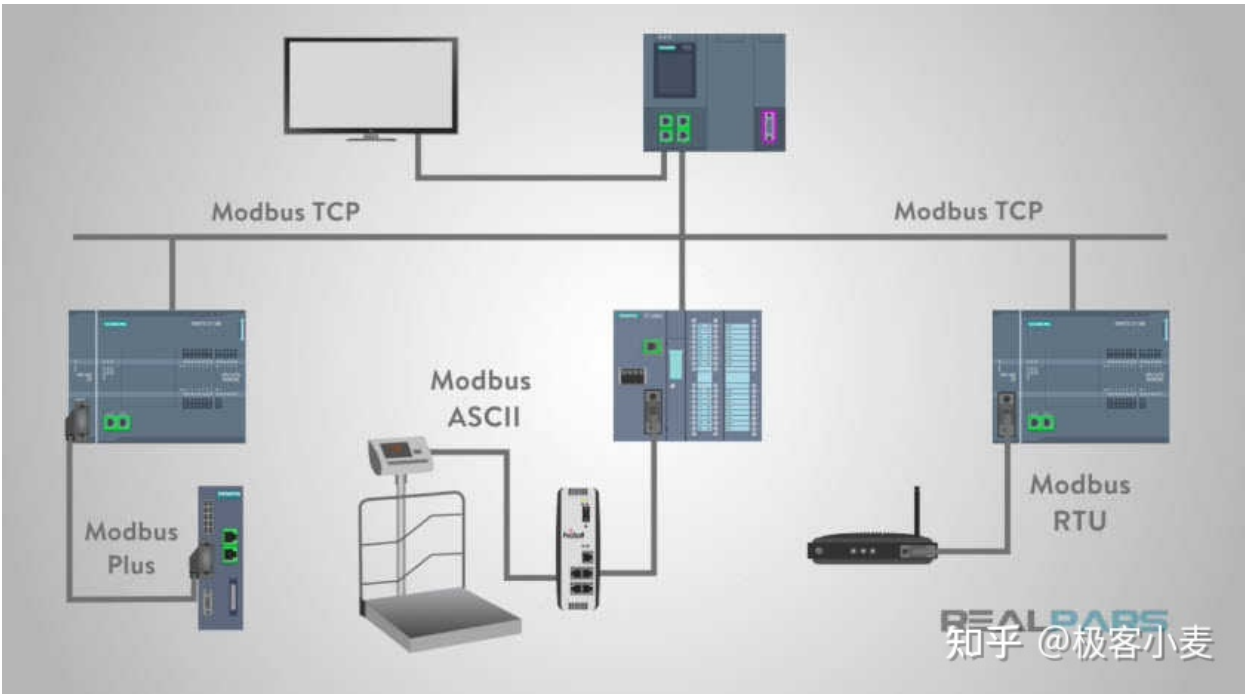
Modbus 解决了通过**串行线路**在电子设备之间发送信息的问题。该协议在遵循该协议的体系结构中实现**主/从模型**。Modbus主站（Master）负责从其他设备（Slave）请求信息。标准Modbus网络中有一个Modbus主站。具体如下图所示；



主设备向从设备请求信息，最多大约可达到240个。每个从设备都有自己**唯一的从设备地址标识**（Slave Address）。除了从从设备请求信息之外，主设备还可以写入从设备的**内部寄存器**。

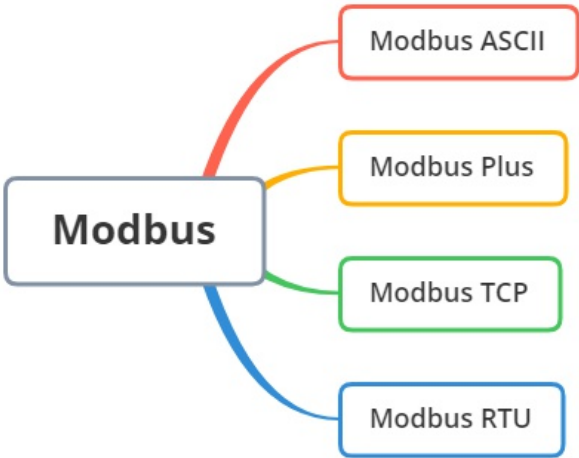
## 3 协议的分类

Modbus 的应用十分广泛，特别是在工业控制领域，具体如下图所示；



我们可以看到最常用 Modbus 协议总共有以下四种：**Modbus ASCII**，**Modbus RTU**，**Modbus Plus**，**Modbus TCP**；

具体如下图所示；



知乎 @极客小麦

3.1 Modbus ASCII

当设备设置为使用 ASCII（美国信息交换标准代码）模式在 MODBUS 串行线上进行通信时，消息中的每个8位字节将作为两个ASCII 4位字符发送。当物理通信链路或设备的功能不允许符合RTU计时器管理要求时，使用此模式。所以此模式的效率不如RTU，因为每个字节需要两个字符。示例：字节0x7D编码为两个字符： 0x35 和 0x42（在 ASCII 表中为 0x37 = '7'，而 0x44 = 'D'）。

3.2 Modbus RTU

Modbus RTU 是一种紧凑的，采用二进制表示数据的方式；因为使用二进制编码和CRC错误检查的结合使得Modbus RTU适用于工业应用，因为它比ASCII字符的替代方案更有效地传输。在Modbus RTU与ASCII之间进行选择时，如果考虑性能，则RTU是首选。

### 3.3 Modbus TCP

Modbus TCP 是在 TCP/IP 网络上运行的Modbus的实现，旨在允许Modbus ASCII / RTU协议在基于TCP / IP的网络上传输。Modbus / TCP将Modbus消息嵌入TCP / IP帧内。尽管实现起来非常简单，但是与网络相关的特性增加了一些挑战。例如，由于Modbus主机期望并要求在一定时间范围内对其轮询做出响应，因此必须考虑TCP / IP网络的不确定性（和其他方面）。Modbus ASCII和Modbus TCP之间的主要区别在于，Modbus ASCII所需的LRC错误检查由IP层执行。

“对于以上 TCP / RTU / ASCII 的这三种通信协议在数据模型和功能调用上都是相同的，只有封装方式是不同的。

### 3.4 Modbus Plus

Modbus有一个扩展版本Modbus Plus（Modbus+或者MB+），不过此协议是Modicon专有的，和Modbus不同。它需要一个**专门的协处理器来处理类似HDLC的高速令牌旋转**。它使用 1Mbit/s 的双绞线，并且每个节点都有转换隔离设备，是一种采用转换 / 边缘触发而不是电压 / 水平触发的设备。连接Modbus Plus到计算机需要特别的接口，通常是支持ISA（SA85），PCI或者PCMCIA总线的板卡。[^1]

## 4 libmodbus

libmodbus是一个多平台的 modbus 开源库，适用于Linux，Mac OS X，FreeBSD，QNX和Win32等操作系统；可以根据Modbus协议发送和接收数据。支持RTU（串行）和TCP（以太网）通信。官网：[libmodbus.org](http://libmodbus.org) Github：[github.com/stephane/libmodbus/](https://github.com/stephane/libmodbus/)

## 5 freemodbus

FreeModbus 是嵌入式系统的Modbus ASCII / RTU和Modbus TCP实现。它提供了Modbus应用协议v1.1a的实现，并支持Modbus over Serial Line Specification 1.0中定义的RTU / ASCII传输模式。从版本0.7开始，FreeModbus也支持Modbus / TCP。0.9版为使用lwIP TCP / IP堆栈的嵌入式系统添加了第一个Modbus / TCP端口。官网：<https://www.embedded-experts.at> Github：<https://github.com/cwagner-at/freemodbus>

FreeModbus 是一款开源的Modbus协议栈，但是只有从机开源，主机源码是需要收费的。同时网上也没有发现比较好的开源的Modbus主机协议栈，所以才开发这款支持主机模式的FreeModbus协议栈。本版FreeModbus版本号更改为V1.6，特性如下：

- 新增加的主机源码与原有从机的风格及接口保持一致；
- 支持主机与从机在同一协议栈运行；
- 支持实时操作系统及裸机移植；
- 为应用提供多种请求模式，用户可以选择阻塞还是非阻塞模式，自定义超时时间等，方便应用层灵活调用；
- 支持所有常用的Modbus方法。

Github: [https://github.com/armink/FreeModbus\\_Slave-Master-RTT-STM32](https://github.com/armink/FreeModbus_Slave-Master-RTT-STM32)