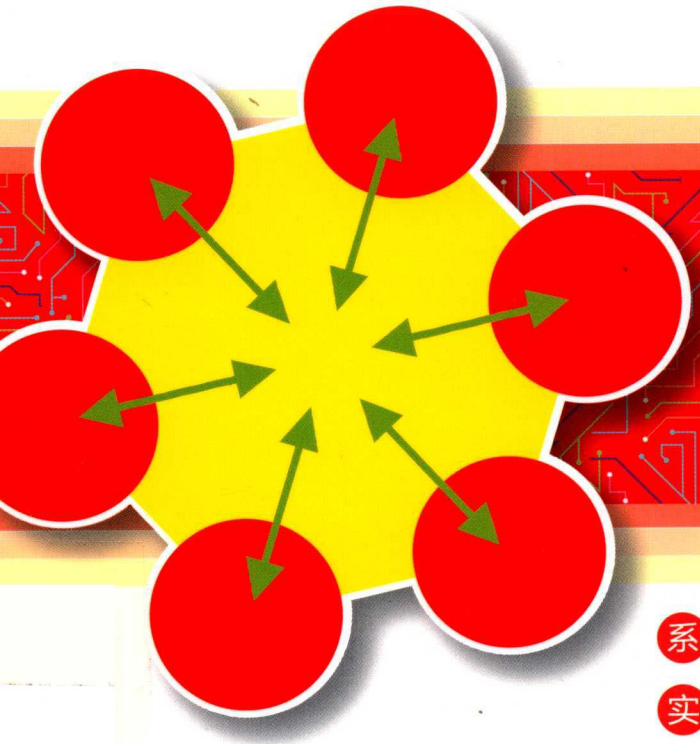
The Practical Developing Guide for Modbus

Modbus 软件开发实战指南

杨更更 著



系统 ⟷ 全面汇集Modbus软件开发经验

实战 ⟷ 借助一书一电脑完成实战训练

实用 ⟷ 内容精炼，图文并茂

实效 ⟷ 快速上手，学以致用

清华大学出版社

The Practical Developing Guide for Modbus

Modbus
软件开发实战指南

杨更更 著

清华大学出版社
北京

内 容 简 介

Modbus是工业自动化领域使用最广泛的通信协议之一，随着电子、计算机和通信技术的不断发展，特别是物联网以及“互联网＋”等概念的兴起，Modbus通信技术也从串行总线发展到了Modbus TCP，方兴未艾。为了让广大在校学生、工业控制和自动化工程师及技术人员了解Modbus协议的内涵，特别是彻底掌握Modbus通信技术的软件开发方法，作者从初学者的角度，由浅入深，循循善诱，以文字和画面相结合的方式撰写了本书。

本书分为11章，首先介绍了Modbus协议，特别是功能码消息帧的定义，然后从软件开发的角度，详细介绍了辅助调试工具、软件开发环境的构筑，重点介绍和解析了libmodbus开发库的源代码，以及使用libmodbus在不同语言环境下的开发技巧。阅读本书，可快速入门并精通Modbus软件开发技术。作为软件技术开发指南的书籍，本书不仅仅局限于Modbus通信协议，对其他通信协议的软件开发也有很强的参考价值。

本书可作为各大中专院校、工程设计院、系统集成商和工厂企业的Modbus通信协议开发人员的软件设计和开发的入门指导书籍，也可作为工业自动化领域及物联网开发的参考资料，还可供广大自动化及通信专业的教师、学生及物联网开发爱好者阅读。

图书在版编目(CIP)数据

Modbus软件开发实战指南/杨更更著. —北京：清华大学出版社，2017(2017.4重印)
ISBN 978-7-302-46475-4

Ⅰ. ①M…　Ⅱ. ①杨…　Ⅲ. ①工业企业－以太网络－通信协议－软件开发－指南　Ⅳ. ①TP393.11-62 ②TN915.04-62

中国版本图书馆CIP数据核字(2017)第024649号

责任编辑：焦　虹
封面设计：常雪影
责任校对：徐俊伟
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　张**：18.75　　**字　数**：281千字
版　　次：2017年4月第1版　　**印　次**：2017年4月第2次印刷
印　　数：1501～3000
定　　价：59.00元

产品编号：073799-01

前 言

如果时间能够倒退回到五六年之前，也许人生将会是另外一番际遇。

当时的我初次接触到 Modbus 通信协议，并且需要基于 Modbus 完成一个质量高度稳定的工业控制程序，怎么办呢？一开始，面对浩如烟海的资料和设计要求确实显得一筹莫展。不过现在想想，如果那时遇到了像这样的一本书，我一定会毫不犹豫地买下来。呵呵☺，听到这样的话，你心里一定在想："嘿，王婆卖瓜，自卖自夸。"好吧，我承认有一些自夸了，人嘛，都是有那么一点点虚荣心的。

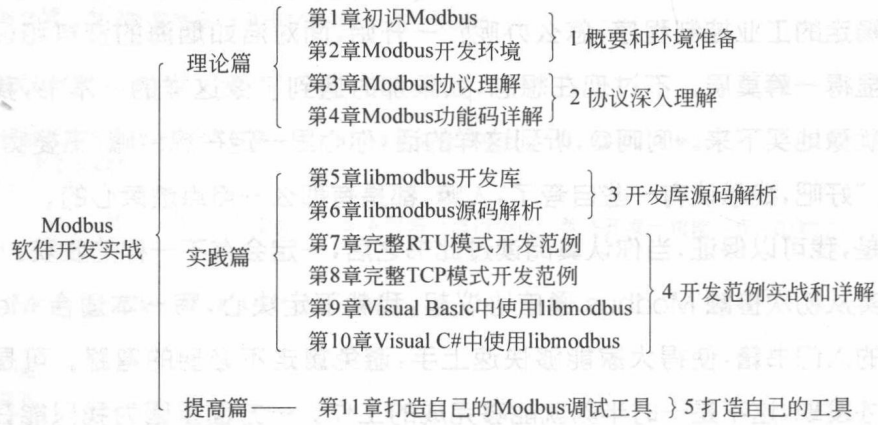
但是，我可以保证，当你认真阅读过此书之后，一定会有不一样的收获。

其实从初次接触 Modbus 通信协议起，我就下定决心，写一本适合 Modbus 初学者的入门书籍，使得大家能够快速上手，避免重走不必要的弯路。可是真正写起来才发现，这不是一时半刻就能够完成的工作。一方面是因为我只能在工作的闲暇时间写作；另外一方面是软件开发技术上牵扯的方方面面太多，如何有条理地组织各种材料也是一个大难题。就这样，写写停停，甚至写作提纲也是几易其稿。好在没有什么压力，在坚持之下最后竟然"凑成"了这一本看似不错的 Modbus 开发入门资料。提供给周围的一些人阅读，都觉得不错值得出版，这也给了我信心。

正所谓"闻道有先后，术业有专攻"。我曾经咨询过很多资深的开发人员，他们平日里大多会去研究和学习各种新奇的开发技术，不会有太多的时间去总结和归纳。据我所知，目前市场上关于 Modbus 开发的书籍并不太多，以至于至今还没有一本专门介绍 Modbus 软件开发的书。机缘巧合，我做了第一个吃螃蟹的

人。 我希望能够通过这本书把我所学习和掌握的一些 Modbus 软件开发工具和技能介绍给大家，让大家体会到软件开发的乐趣，减轻 Modbus 开发入门时的迷茫和无助。 如果能够实现这个目的，善莫大焉。 不仅如此，这本书不仅仅局限于 Modbus 本身，书中提到的开发技巧和经验对其他的开发工作也有借鉴意义。

本书大体可划分为三大部分：理论篇、实践篇和提高篇，篇章结构如下所示：



理论篇主要介绍 Modbus 协议本身，便于初学者体会 Modbus 协议的精髓所在，打好基础。 实践篇通过对 libmodbus 开发库源码的分析以及各种范例程序的演示，便于读者快速入门和上手，掌握各种模式下的开发方法和技巧。 提高篇则进一步带领读者开发自己的 Modbus 调试工具。 按照各章节的内容，读者可以循序渐进地阅读本书，逐步完成从入门到精通的过程。

作为软件开发者，很多人都没有付费购买书籍的习惯。 我觉得吧，该付费的时候就别省，也许还不到一顿饭钱，就可以系统地提升自己，让你在同事中脱颖而出，不到一顿饭的投资换来的是成千上百倍的回报。

很多人又会说，不用买你的书，我也可以自己通过 Google 或百度来解决问题啊。 是的，的确没错，现在互联网这么发达，没有解决不了的问题，但是这

要花费你大量的时间和精力，与其这样，还不如去学更多的东西，做些更有意义的事情。 在互联网时代，最重要的是懂得如何站在别人的肩膀上。

本书定位

本书是循序渐进地学习 Modbus 软件开发的书籍，需要你有针对性地去阅读。 当然，遇到问题或者想了解某个知识点时，可以直接定位到相关的章节，查看内容。

本书以通俗易懂的语言和画面描述 Modbus 软件的开发技巧，基本上每个操作都会有画面或者实际程序代码演示，便于读者自学。

本书以解决 Modbus 软件开发中的问题为目的，围绕这一点着重讲述如何快速入门并精通 Modbus 软件开发技术。 对于 Modbus 开发来说必要的硬件不可缺少，但是为了能迅速入门，减少硬件依赖，本书尽可能使用各种软件工具模拟硬件环境，阅读本书一台电脑足矣，这也是本书的一大特色。

目标读者

- 如果你初学 Modbus 通信协议；
- 如果你想用 C/C++ 语言开发 Modbus 通信库；
- 如果你想用其他语言（如 Visual Basic、Visual C# ）开发 Modbus 应用程序；
- 如果你想从事物联网或 Modbus 测试开发；
- 如果你英语不好；
- 如果你想节省搜索的时间；
- 如果你想提高工作效率。

那么这本书简直就是为你量身订做的。

尽管本人已尽力确保本书的准确性和完整性，但因知识和能力有限，书中难

免存在纰漏之处，恳请各位读者不吝批评指正，争取将来进一步完善本书，以此来回报大家对本书的支持和厚爱。

致谢

在本书的写作和出版过程中，得到了很多人的热情帮助和支持，在此一并致谢！

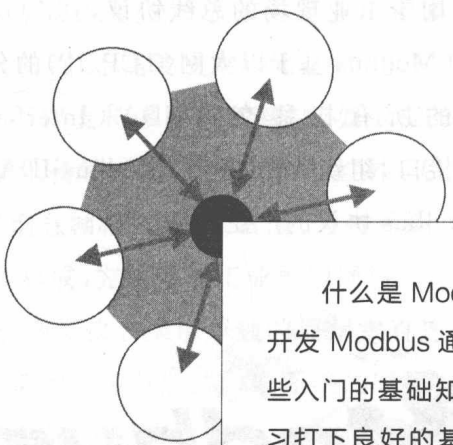
首先要感谢创造和发明 Modbus 通信协议的那些人，正是因为他们创造性的工作才有了如此简洁、优雅并应用广泛的通信协议供大家使用。 可以毫不夸张地说，Modbus 协议的出现推动了人类工业自动化生产的进步。

其次要感谢清华大学的杨开明教授、北京交通大学的杨莉副教授，在本书的写作和出版过程中各位老师都给出了详细的意见和建议。

最后，感谢家人的支持和所有阅读本书的读者。 如果能够给各位读者带来哪怕一点收获或体会，那将是对我极大的鼓舞。 谢谢！

杨更更

目 录



第 1 章

初识 Modbus

什么是 Modbus 通信协议？ 在学习和开发 Modbus 通信协议之前，需要学习一些入门的基础知识，以便为后续章节的学习打下良好的基础。 简而言之，Modbus 通信协议是工业领域通信协议的业界标准，并且是当前工业电子设备之间相当常用的连接方式之一，特别是在物联网蓬勃发展的当下，了解并掌握广泛应用的 Modbus 通信协议意义重大。

本章主要介绍 Modbus 相关的背景知识和一些基本概念。

1.1 背景

Modbus 协议是由 MODICON(现为施耐德电气公司的一个品牌)在 1979 年开发的,是全球第一个真正用于工业现场的总线协议,其 LOGO 如图 1-1 所示。之后为了更好地普及和推动 Modbus 基于以太网(TCP/IP)的分布式应用,施耐德公司已将 Modbus 协议的所有权移交给 IDA(Interface for Distributed Automation,分布式自动化接口)组织,并成立了 Modbus-IDA 组织,此组织的成立和发展,进一步推动了 Modbus 协议的广泛应用。

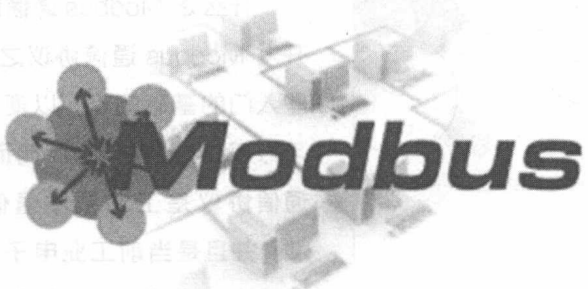


图 1-1 Modbus LOGO

访问 Modbus 官方网址(http://www.modbus.org)可以获取完整的协议文本。

Modbus 协议是应用于电子控制器上的一种通用语言。通过此协议,可以实现控制器相互之间、控制器经由网络和其他设备之间的通信。它已经成为一种通用的工业标准,有了它,不同厂商生产的控制设备可以连接成工业网络,进行集中监控。此协议定义了一个控制器能够认识使用的消息结构,而不管它们是经过何种网络进行通信的;而且描述了控制器请求访问其他设备的过程,如何应答来自其他设备的请求,以及怎样侦测错误并记录;并制定了统一的消息域的结构和内容。

当在 Modbus 网络上通信时，此协议决定了每个控制器必须要知道它们的设备地址，识别按地址发来的消息，决定要产生何种行为。如果需要回应，控制器将生成反馈信息并通过 Modbus 协议发送。

Modbus 通信协议具有以下几个特点：

- Modbus 协议标准开放、公开发表并且无版税要求。用户可以免费获取并使用 Modbus 协议，不需要交纳许可证费，也不会侵犯知识产权。
- Modbus 协议可以支持多种电气接口，如 RS232、RS485、TCP/IP 等；还可以在各种介质上传输，如双绞线、光纤、红外、无线等。
- Modbus 协议消息帧格式简单、紧凑、通俗易懂。用户理解和使用简单，厂商容易开发和集成，方便形成工业控制网络。

在大多数工厂里，现场仪表采用单独的控制室直连对绞线电缆连接到控制系统。当仪表设备被连接到一种分散式 I/O 系统的时候，在 Modbus 协议的帮助下，可以增加更多的现场设备，但是仅仅需要一根对绞线电缆就可以把所有数据传送到 Modbus 主站设备。以 Modbus 网络的方式组网连接的时候，可以把现场设备连接到一个 DCS 过程控制系统、PLC 设备或工业计算机系统，整个工厂的连接都能够从对绞线电缆控制室直连的方式转变成为 Modbus 网络连接方式。

现代工业控制领域持续不断产生和应用诸如现场总线和网状网络等先进的概念，而 Modbus 协议的简单性以及它的便于在许多通信媒介上实施应用的特点一直使它受到最广泛的支持，并且成为全球应用最广泛的工业协议。当使用现有老式控制系统的用户发现自己需要扩充现场仪表或者增加远程控制器的时候，基本上都会采用 Modbus 作为一个能够解决复杂问题的简单方案。当用户试图把一个外来设备连接到既存控制系统里面时，使用设备的 Modbus 接口被证明是最容易、最可靠的办法。

虽然 Modbus 已经发展到了极为成熟的阶段，但仍然是最普及的通信方式之一。Modbus 便于学习、使用，非常可靠，价格低廉，并且可以连接到工业控制领域几乎所有的传感器和控制设备上。学会并掌握 Modbus 开发将会成为一项具有广泛意义和实际应用价值的技能。