运用 ModBus 通信协议，实现电子秤与 PLC 的实时通信

上海彩信电子科技有限公司　陈东富

【摘　要】　本文介绍了在工业控制系统中广泛使用的 ModBus 通信协议。以 ModBus 的 ASCII 方式为例，剖析了 ModBus 的指令结构，着重说明基于 ModBus 通信协议的设备之间如何进行数据通信、如何使用 ModBus 通信协议把衡器接入 PLC 系统，并简单介绍了 PLC 系统与局域网的互联。
【关键词】　ModBus 通信协议；PLC 可编程控制器；衡器

在衡器行业中，但凡涉及串行通信时，工程师们都会有一种无奈，就是通信协议问题。由于我国衡器厂众多，各自采用自己的通信协议，使得通信协议五花八门，互不兼容。由于是自成一体，也为后续与其他系统联网、维修、仪表配件互换等留有后遗问题。若采用一种工业控制领域的主流协议，各衡器厂的通信协议都与这个主流协议兼容，那么上述问题自然迎刃而解。这个主流协议首推 ModBus。

一、什么是 ModBus

ModBus 是一种通信协议，是由 Modicon 公司发表于 1979 年，主要用于 PLC（可编程逻辑控制器）系统。目前，在工业自动化设备通信连接中，ModBus 已是相当常见的一种连接方式。

二、ModBus 与其他通信协议比较

1、物理层简单、价廉：ModBus 可以在常用且廉价的 RS232、RS485 等物理媒介上运行，不像 CanBus、ProfiBus、BitBus 等需昂贵的专用芯片支持。

2、免费：ModBus 是一种公开的，可以无偿使用的协议。而使用 ProfiBus 则需要向有关国际组织登记缴费。

3、使用普及：ModBus 是当前工业控制中使用最广的一种通信协议，基于这点，具有 ModBus 的设备接入工控系统相对容易。

4、维护方便：由于接入 ModBus 总线相对其他工控总线而言，比较简单。一般具有 RS232、RS485 等串行口的 PC 机都可以接入，使用 PC 机自带的超级终端软件或其他串行控制软件，就能观察 ModBus 通信过程，可以很方便地查出故障站点。

三、ModBus 的主要型式

ModBus 主要有四种型式：ASCII、RTU、TCP/IP 和 Plus。

1、ASCII 型式：采用 ASCII 码进行数据交换，使用纵向冗余校验的校验和（LRC）进行数据校验。

2、RTU 型式：采用二进制码进行数据交换，使用循环冗余校验的校验和（CRC）进行数据校验。

3、TCP/IP 型式：主要用于以太网，不使用校验和进行数据校验。

4、Plus 型式：该型式为 Modicon 公司专有，采用专门的协处理器进行数据处理。

目前，使用最广泛的型式是 ASCII 和 RTU，主要采用 RS232、RS422、RS485 进行物理连接，其中 RS485 使用最多。

四、ModBus 的结构

ModBus 协议是一个 master（主）/slave（从）架构的协议。有一个节点是 master 节点，其他使用 Modbus 协议参与通信的节点是 slave 节点。每一个 slave 设备都有一个唯一的地址。ModBus 的通信比较简单，由 master 发通信指令，指令中含有欲于之通信的 slave 站号。当 master 发指令时，所有 slave 都处于收听状态，一旦 slave 收听到与自己地址相同的站号时，立刻执行指令的内容，并回传执行的结果。

五、ASCII 型式的 ModBus 通信协议的格式

在 ModBus 上通信时，各站点的通信参数必须一致，如：波特率、奇偶校验。

通信时，一个信息字节中的每 8 位分为两个 ASCII 字符进行传输，允许字符传输间隔在 1 秒之内。

1、ASCII 型式每一字节的格式

16 进制编码，ASCII 字符（0-9、A-F），即：0x30-0x39、0x41-0x46。

1 位开始位、7 位数据位（先低后高）、1 位奇偶校验（无奇偶校验时为 0）、1 位停止位。

2、数据错误校验采用纵向冗余校验（LRC）

3、通信帧格式（ModBus 命令格式）

开始	地址（站号）	功能	数据	校验（LRC）	结束
：(0x3a)	xx	xx	x...	xx	CR、LF(0x0d、0x0a)
1 字符	2 字符	2 字符	N 字符	2 字符	2 字符

一个基本的 ModBus 命令，除了开始、校验、结束字符外，还必须有地址项及功能项。地址——也就是站号，想要被操作的对象（slave 站号）；功能——想要被操作的对象完成的任务。ModBus 命令可以没有数据项。

被操作的对象，在完成所要求的操作后，必须回传一帧信息，传递操作结果。回传信息的格式

与命令格式相同，只是数据内容为操作的结果。

六、利用 ModBus，实现 PLC 与电子称重设备的通信

为了使大家对 Modbus 有更进一步的了解，下面用例子方式说明如何把电子称重设备接入 PLC 控制系统的 Modbus 总线网络。例子中的称重仪表为上海彩信电子科技有限公司生产的 XK315A1 增强型仪表。本例中，1 台 PLC 作为主机（master），10 台电子秤作为从机（slave），使用 XK315A1 增强型仪表作为电子秤显示仪表，从机地址为 70、71、72、....79。通过 RS485 连接 PLC 和各仪表，采用 ModBus ASCII 通信协议。PLC 可以对各台仪表进行置零、去皮、读取重量等多项操作。称重系统示意图如图 1 所示，图中的计算机是在系统调试时接入 RS485 总线的，用以观察 RS485 中传输的数据，正常工作时是移除的。

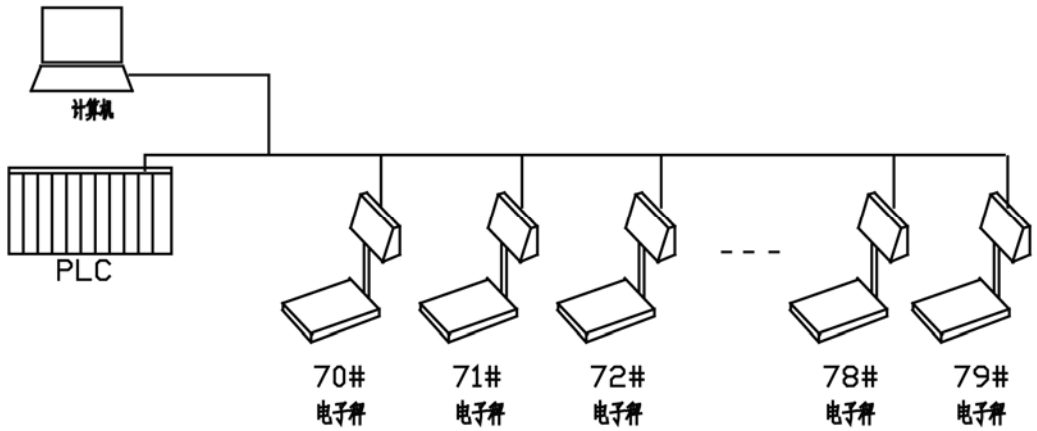

图 1　称重系统示意图

上述系统可实现以下功能：

1、正常工作时，PLC 每隔 10 秒轮询一次，获取每台秤的重量。

2、当秤台上重量异常时，PLC 会发出警告信息，提示控制室人员注意。

3、控制人员可以通过 PLC，对某台秤发出置零、去皮等操作指令。

4、PLC 可对各台秤的称量，进行各项统计，生成必要的统计报表。

七、ModBus 与局域网互连

现在，很多 PLC 都具有局域网接口，通过该接口，就可以远程控制称重系统了。当然，也可以通过接在 Modbus 总线上的 PC 机，利用 PC 机的软、硬件资源，编制相应的软件，将重量信号传送到局域网上。若局域网通过路由器接入因特网，很显然重量数据就可以在因特网上传输了。本系统是通过 PLC 的 DH+网络接入局域网的。当然，网络部分使用的协议，首推 TCP/IP、NetBEUI。Modbus 也有相关的 TCP/IP 型式，这里就不再赘述了，大家可以参考相关的书籍。

上述的称重系统只是 PLC 的一个子系统，是后期改造的一个项目。其整个 PLC 系统（见图 2）是采用美国 ROCKWELL 公司的 PLC，共有 5 台 PLC 机箱（采用 PLC5 系列）、4 台工控机和 2 台服务器、若干台 PC 组成的。PLC 采用 ROCKWELL 公司的 DH+网络连接，使用 DF1 协议；其中 1

台 PLC 与称重系统采用 RS485 连接，使用 Modbus 协议；DH+网络通过 1 台作为连接桥的工控机，连入局域网。工控机上的监控软件是 RSVIEW32，操作人员通过该软件的人机界面，观察各项数据，发出各项指令，当然也包括称重数据及指令。另外，局域网上的 PC 机也安装了 RSVIEW32 软件，只不过取消了操作指令，但可以通过该软件观察各项数据，便于其他相关人员关注设备运行情况。

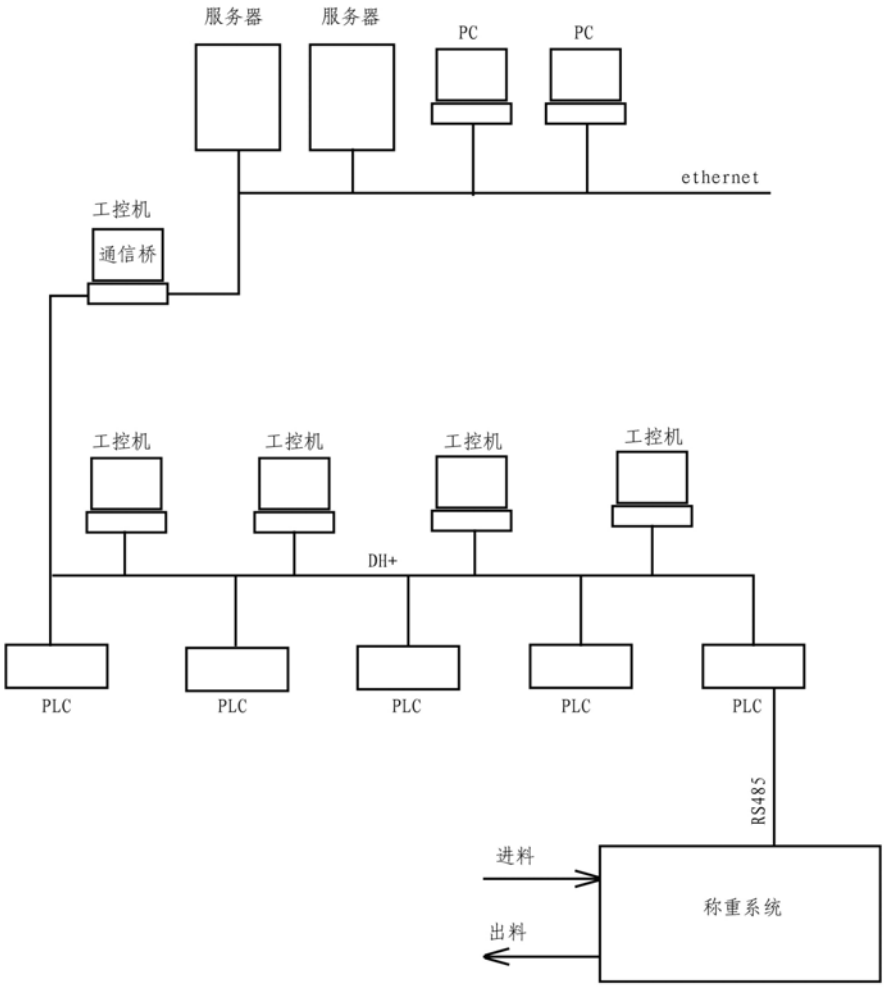

图 2　PLC 系统图

八、结束语

本文简单介绍了 ModBus 通信协议，例举了电子秤采用 RS485 串行接口接入 PLC 系统，用 ModBus 通信协议，实现与 PLC 的实时通信。由于水平有限，如有错误的地方，望谅解。

PLC 程序采用的是梯形图，其中有对串行口进行操作的梯形图，设置图中的相关属性，如波特率、奇偶校验，把相关的 Modbus 操作命令写入其中即可。有关 PLC 的编程请参阅 ROCKWELL 公司的《PLC5 指令系统与使用说明》。

关于 XK315A1 增强型仪表的 ModBus 协议及指令举例，请看附录。

附录：

XK315A1 增强型仪表的 ModBus 协议格式

说明	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	xx	xx	xxxx	xxxx	xxxx	LRC	\CR\ LF
回传	：	xx	xx		xx	xxxx	LRC	\CR \ LF
出错回传	：	xx	xx 最高位置 1			xx 错误码	LRC	\CR \ LF

报头、报尾：所有指令均以冒号（：）开始，以回车符、换行符结束。

站号：2 个 ASCII 码，范围为 01-90（16 进制：0x01-0x5A）。

功能码：2 个 ASCII 码。

02：读继电器输出状态；

04：读称量状态（显示值、皮重等）；

05：置零操作；

06：皮重操作；

07：通信测试；

08：读定值；

09：写定值。

首址：4 个 ASCII 码，读写数据的位置。

数据量：4 个 ASCII 码，读写数据的数量。

数据值：读写的数据。

校验码：2 个 ASCII 码，采用 LRC 校验。

LRC 校验码运算：报头（：）不参与运算，LRC 在数据之后，在\CR\LF 之前。参加运算的是报头之后，LRC 之前的所有数据。LRC 为参加运算的数据之和的补码，舍去进位。

当仪表执行指令出错时，会回传错误码，并将功能码的最高位置 1。

错误码：

00--接收到的功能码出错；

01--数据地址错；

02--数据数量错；

03--数据值错，如：预置皮重大于最大称量 FS；

04--称量为负时去皮；

05--不在称重状态时置零；

06--称量不稳定时置零；

07--称量>2%FS 时置零；

08--称量<-2%FS 时置零。

接下来以地址为 78（16 进制为 4E）号的仪表为例，详述每条指令。PLC 作为 master，发送指令；电子秤仪表作为 slave，接收指令，并回传执行结果。

读取重量数据（功能码：04）

说明	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	04	0000	0007		A7	\CR\ LF
回传	：	4E	04		07	120003E70000CA	E1	\CR\ LF

例中：站号 4E，即 78 号；功能码 04 表示要读取重量数据；仪表的重量数据专门放置在重量数据单元，其地址从 0000 到 0006，共 7 个字节。其中 0000：状态数据；0001-0003：显示值；0004-0006：皮重值。读取重量数据时，可以单独读，也可以 2 个一起读或全部读。首址 0000 表示从重量数据的 0000 地址开始读取；数据量 0007 表示共要读取 7 字节数据；校验码 A7 表示校验和 LRC=A7。

当 PC 发出指令后，每个从站仪表都会接收，只有与指令中指定的站号相同的仪表，才会响应，回传所需信息。

78 号地址的仪表，收到上述指令后，会回传“：4E0407120003E70000CAE1\CR\LF”

其中“120003E70000CA”是 PC 想得到的 78 号站的重量信息。

12--状态数据，表示当前显示为正、重量稳定、显示值是净重，当前数据包含 2 位小数；

0003E7--显示值，同状态数据结合考虑，即：当前的显示是净重 9.99kg；

0000CA--皮重值，即：当前的皮重是 2.02kg。

数据校验：所有被参与校验的数据+校验码=0（舍去进位）。

0x4E+0x04+0x00+0x00+0x00+0x07+0xA7=0x100，舍去进位 1 后，等于 0，表示数据检验正确。

状态数据：

D7	D6	D5	D4	D3	D2	D1	D0
0：正 1：负	0：不在零位 1：在零位	0：稳定 1：动态	0：毛重 1：净重	恒为 0	000：无小数；001：1 位小数; 010：2 位小数；011：3 位小数		

如要单独读显示值，可发指令“：4E0400030003A8\CR\LF”

78 号仪表回传“：4E04030003E7C1\CR\LF”

如要同时读显示值及皮重，可发指令“：4E0400030006A5\CR\LF”

78 号仪表回传“：4E04060003E70000CAF4\CR\LF”

置零操作（功能码：05）

	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	05				AD	\CR\LF
回传	：	4E	05				AD	\CR\LF
说明	置零成功							
回传	：	4E	85			07	26	\CR\LF
说明	置零失败，重量>2%FS							

去皮操作（功能码：06）

	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	06	0004	0003	000064	41	\CR\LF
回传	：	4E	06		03	000064	45	\CR\LF
说明	设置皮重=100，显示净重							
指令	：	4E	06	0004	0000		A8	\CR\LF
回传	：	4E	06		03	0000C9	E0	\CR\LF
说明	操作前为毛重状态，操作后，把毛量作为皮重，皮重=201，显示净重为 0							
指令	：	4E	06	0004	0000		A8	\CR\LF
回传	：	4E	06		03	000000	A9	\CR\LF
说明	操作前为净重状态，操作后，恢复毛量显示，皮重=0							

去皮操作正确执行后，回传的数据为去皮操作后的皮重值。

读取定值（功能码：08）

	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	08	0001	0004		A5	\CR\LF
回传	：	4E	08		04	00006400	45	\CR\LF
说明	首址：0001--1#定值、0005--2#定值、0009--3#定值、000D--4#定值、0011--5#、0015--6#定值； 数据中，前 3 字节表示定值，例中：000064 表示 1#定值=100 后 1 字节厂家保留，这里不用。							
指令	：	4E	08	0005	0004		A1	\CR\LF
回传	：	4E	08		04	00012C00	79	\CR\LF
说明	2#定值=300							
指令	：	4E	08	000D	0004		99	\CR\LF
回传	：	4E	08		04	0003E800	BB	\CR\LF
说明	4#定值=1000							

设置定值（功能码：09）

	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	09	0001	0004	0001F400	AF	\CR\LF
回传	：	4E	09		04	0001F400	B0	\CR\LF
说明	首址：0001--1#定值、0005--2#定值、0009--3#定值、000D--4#定值、0011--5#、0015--6#定值；数据中，前 3 字节表示定值，例中：0001F4 表示设置 1#定值=500 后 1 字节厂家保留，这里恒为 0。							
指令	：	4E	09	0009	0004	00038400	15	\CR\LF
回传	：	4E	09		04	00038400	1E	\CR\LF
说明	设置 3#定值=900							
指令	：	4E	09	000D	0004	00044C00	48	\CR\LF
回传	：	4E	09		04	00044C00	55	\CR\LF
说明	设置 4#定值=1100							

仪表的回传数据值为设定后的定值。

读取输出继电器状态（功能码：02）

	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	02				B0	\CR\LF
回传	：	4E	02		01	0C	A3	\CR\LF
说明	数据为 1 字节，低四位从低位到高位分别代表 1#-4#继电器输出状态。 0：断开　1：吸合　　上述数据 0C（0000 1100）表示：3#、4#继电器吸合，1#、2#继电器断开。							

通信测试（功能码：07）

	报头	站号	功能码	首址	数据量	数据值	校验码	报尾
指令	：	4E	07				AB	\CR\LF
回传	：	4E					B2	\CR\LF
说明	通信正常，返回站号							

作者简介

陈东富，男，上海交通大学毕业，所学专业：电子工程，工作单位：上海彩信电子科技有限公司技术部，任副总经理