原创文章，转载请注明出处。

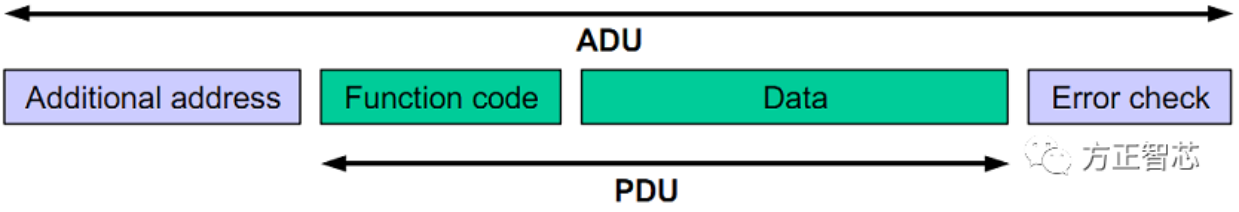
更多实用资料请登录方正智芯官网：www.founderchip.com

作者：北岛李工

在易维通的匠说上有网友留言S7-1200与S7-200的Modbus通信问题，我做了简单的回答。由于通信涉及很多方面，回答者只能根据提问者反馈的情况，猜测可能的问题原因。而当通信出现故障时，不同的情况遇到的问题可能不一样，无法一概而论。因此，我想最好的办法是做一个通信连载的教程，把整个流程梳理一遍。当你有了基本概念，再根据自己的实际情况，有针对性的查找原因会更简单些。

本章我们先简单介绍下Modbus的通信原理，然后介绍下例程中需要用的硬件及网络的拓扑结构。

Modbus RTU是一种主从通信协议，其物理层采用RS485网络。RS485的串行通信规程中规定应用数据单元（Application Data Unit，ADU）的最大长度为256个字节。在Modbus RTU协议中，从站地址占用1个字节，校验位占用2个字节，因此协议数据单元PDU（Protocol Data Unit）的最大长度为256-1-2=253字节。



在协议数据单元PDU中，功能代码占用1个字节，因此数据长度为0~252个字节。如下图：

方正智芯(founder chip)——Modbus RTU ADU				
从站地址	功能代码	数据	校验段	
			CRC1	CRC2
1 字节	1 字节	0~252个字节	1 字节	1字节
方正智芯				

Modbus通信协议的PDU包括三种：

1）Modbus请求PDU（Modbus Request PDU）；

2）Modbus应答PDU（Modbus Response PDU）；

3）Modbus异常应答PDU（Modbus Exception Response PDU）；

以功能代码“0x01”为例，其请求PDU的格式如下表：

方正智芯——Modbus 请求PDU格式			
名称	长度	描述	值
功能码	1字节	Modbus功能代码	1
起始地址	2字节	Modbus参数地址	0x0000~0xFFFF
线圈数量	2字节	读取线圈的数量	0x01~0x7D0
方正智芯			

其应答PDU的格式如下表：

方正智芯——Modbus 应答PDU格式			
名称	长度	描述	值
功能码	1字节	Modbus功能代码	1
数据长度	1字节	应答数据的长度	N
线圈状态	n字节	线圈的值	n=N 或n=N+1
N=输出点的数量/8，若余数不为0，则N=N+1			
方正智芯			

不同的功能码其数据长度的单位不同。位（bits）操作的功能码，其请求数据的长度以“位”为单位；字（WORD）操作的功能码，其请求数据的长度以“字”为单位；

比如：功能码0x01（读取线圈），其请求数据（线圈数量）是以“位（bits）”为单位的；而功能码0x03（读取保持寄存器），其请求数据（保持寄

存器）是以“字（WORD）”为单位的；

Modbus通信协议规定了不同的参数地址，与PLC的CPU地址有一种对应关系。以S7-200 Smart为例，Modbus参数地址与CPU的地址的对应关系见下面的表格：

方正智芯——S7-200 Smart存储区与Modbus地址参数对照表		
Modbus参数地址	**PLC存储区**	**S7-200 Smart CPU地址**
00001~00256	输出存储区Q	Q0.0 ~ Q31.7
10001~10256	输入存储区I	I0.0 ~ I31.7
30001~30056	模拟量存储区AI	AIW0 ~ AIW110
40001~4xxxx	保持存储区	T ~ T+2*(xxxx-1)
T为设置的V存储区的起始地址，若已知V存储区地址，推算Modbus地址公式如下：Modbus参数地址=40000+（T/2+1），T为偶数		
方正智芯		

本例程主站采用S7-1200的PLC，从站采用S7-200 Smart的PLC。

1、硬件配置：

1.1 主站：

S7-1200 CPU1215C；

CM1241-RS485；

1.2 从站：

S7-200 Smart CPU ST40；

2、通信任务：

2.1 Modbus主站读取从站Modbus参数地址40001开始的10个字长的数据；

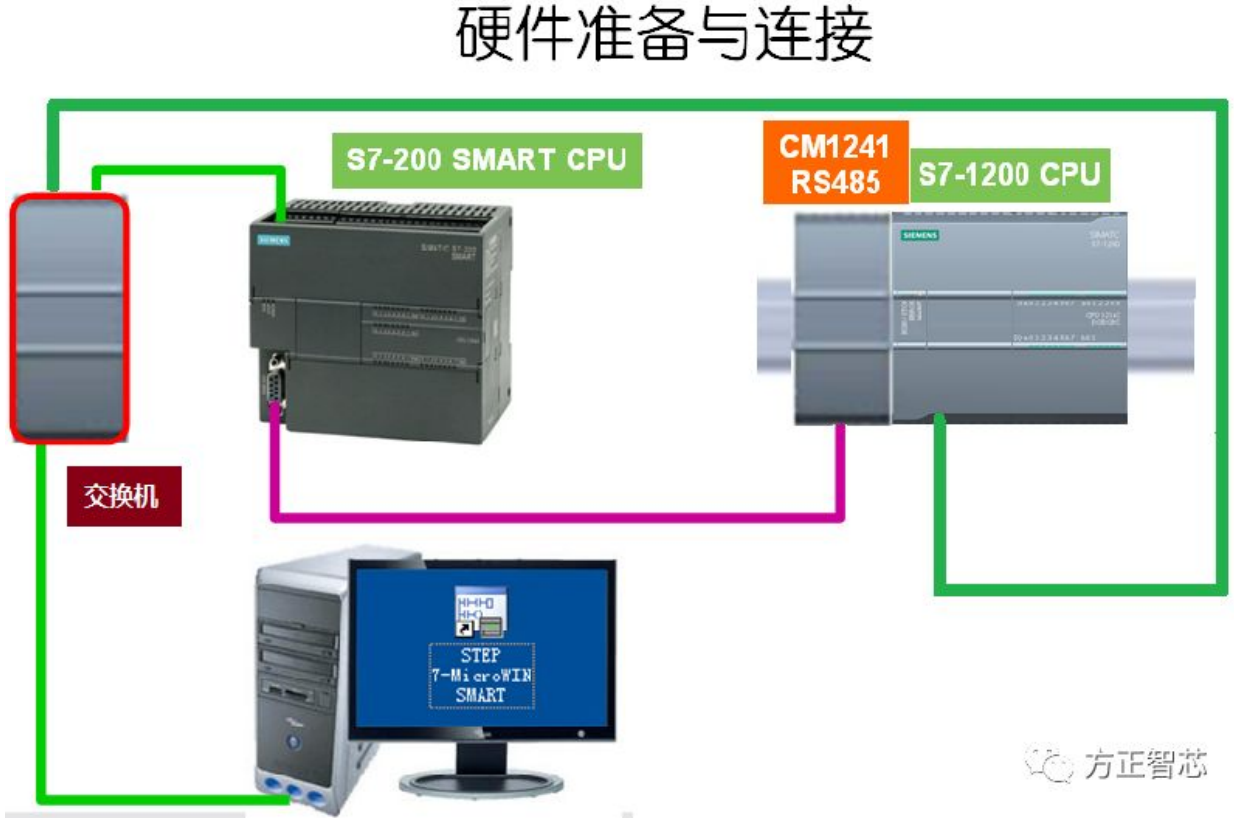
2.2 Modbus主站将6个字长的数据写入到从站起始Modbus参数地址40011；

2.3 Modbus主站读取从站Modbus参数地址10001开始的8个位的数据；

2.4 Modbus主站将8个位写入到从站Modbus参数地址00001；

3、网络连接：

主站的CM1241-RS485模块通过Profibus电缆连接到从站CPU ST40本体的RS485端口；为了监控和下载程序方便，可以用交换机将CPU ST40、CPU1215C和编程电脑PG/PC连接起来。整个网络拓扑图如下：



关于Modbus的通信原理及本例程的网络拓扑结构就介绍到这里，下一篇文章我们介绍Modbus主站CPU1215C的配置。

如果你喜欢这篇文章，可以去官网（www.founderchip.com）下载本文PDF版本。

小程序【李工谈工控】提供方便的文章检索功能，欢迎体验：