江西省西门子授权总代理---景德镇市西门子电机维修授权合作伙伴

产品名称	江西省西门子授权总代理---景德镇市西门子电机维修授权合作伙伴
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子PLC:西门子伺服电机 西门子触摸屏:西门子电缆 西门子变频器:西门子模块
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房（仅限办公）
联系电话	13510737515 13185520415

产品详情

S7协议之PDU读取

大部分人都知道S7协议一次性读取有限制，但是具体是多少？怎么计算出来的？

S7协议的一次性读取长度是根据PDU计算出来的，这个PDU的值是来自于PLC本身，不同型号的CPU，它的PDU是不一样的，可以参考下面两张图：

西门子PLC的PDU大小是和CPU息息相关的，一般会有240、480、960三个档次，知道PDU之后，那么一次性读取的字节长度，就是在PDU的基础上减去18，这个18是指包头包尾会有18个字节，这样我们就知道了一般的PLC，一次性能读取222个字节（240-18=222），但是对于S7-1516这样的PLC，我们一次性是可以读取942个字节的（960-18=942），这个一次性能读取的字节越长，越能提高上位机的通信效率。

刚刚的方式是通过KepServer测试的，实际开发过程中，该怎么获取CPU的PDU呢，实际上在建立连接的第二次握手时，返回的报文中就包含PDU的值。

第二次握手返回的报文长度是27个字节，最后两个字节就是PDU的值，上图展示的是S7-1200PLC返回的报文，0和240的组合即为240。

对于S7-1500，我这里也做了一下测试，结果如下，返回结果为3和192，3和192的组合恰好是960（960=3*256+192）。

虽然PDU是由硬件做了限制，但是我们可以通过软件的方式，实现大量数据的读取，只需要在底层做一些封装即可。做了一下测试，针对S7-1200和S7-1500同时读取M区的8000个字节的耗时比较，S7-1200耗时800多ms，S7-1500耗时仅需200ms，由此可见，硬件对通信的重要性。

S7协议之多组读取

对于很多其他的通信协议，当我们遇到数据变量比较零散，同时读取多个存储区或者一个存储区多个不同部分的时候，我们只能针对每个存储区或者每块区域做一个数据请求，但是西门子S7协议可以解决这样的问题。

西门子S7协议有一个非常强大的一个地方，可以同时读取很多个不同的存储区，最大支持19种，总共读取长度仍然受PDU的限制。

这里我们仍然以实验测试为例，体验多组读取带来的美妙体验。

假设我们的通信组配置如下：

通信组01：读取I区从0开始的1个字节

通信组02：读取Q区从0开始的1个字节

通信组03：读取M区从0开始的200个字节

通信组04：读取M区从500开始的50个字节

通信组05：读取M区从1000开始的60个字节

通信组06：读取DB100从0开始的20个字节

通信组07：读取DB100从20开始的20个字节

通信组08：读取DB100从40开始的20个字节

通信组09：读取DB100从60开始的20个字节

我们采用常用S7-1200PLC，通过配置软件实现配置以上9个通信组，开始通信测试，首先我们选择的是单组读取的方式，就是针对每个组，依次进行读取，结果如下，耗时大约200ms，这个时间应该相对来说还是比较正常的。

接着，将读取方式改成了多组读取，再进行测试发现结果如下：

通过结果发现，多组读取对于存储区较为零散的项目来说，有着非常重要的作用，可以大大提高通信效率。

总结

通过上面一系列的分享，相信大家对西门子PLC通信有了更加深入的了解，希望大家可以多多实践。

每种通信方式都有自己的优缺点，对各种通信方式和协议了解之后，你才能够在不同的场合选择适合的通信方式，给出最合理的解决方案。

写在后面