保密等级
公开

Q/DX

青岛鼎信通讯股份有限公司技术文档

Q/DX D121.088-2022

西门子.net S7 协议通信传输规范

V1.0

2022－06－21 发布　　2022－06－21

青岛鼎信通讯股份有限公司　　发布

目　　次

前　言

为保证电控软件工程师与上位机软件工程在公司项目中正常交互，顺利对接公司上位机系统，方便后期设备维护，对与西门子PLC通过S7通讯协议进行交互提出规范。

本规范定义了青岛鼎信通讯股份有限公司、青岛鼎信通讯消防安全有限公司、青岛鼎信通讯科技有限公司及相关公司通过S7协议与西门子PLC进行通讯交互时的基本规范。

本标准由青岛鼎信通讯股份有限公司工程技术本部自动化部软件组起草。

西门子.net S7 协议通信传输规范

1 范围

本规范定义了青岛鼎信通讯股份有限公司、青岛鼎信通讯消防安全有限公司、青岛鼎信通讯科技有限公司及相关公司通过S7协议与西门子PLC进行通讯交互时的基本规范。

本规范简要介绍了上位机软件对当前模块的设计，方便后续开发者对代码进行快速了解和熟悉。

2 规范性引用文件

本标准根据工作实际情况进行整理，并进行规范要求，无其他参考整理。

3 规范概述

规范主要包含以下几方面：

1）西门子S7通讯协议基础说明

2）西门子PLC配置说明

3）.net S7上位机设计规范

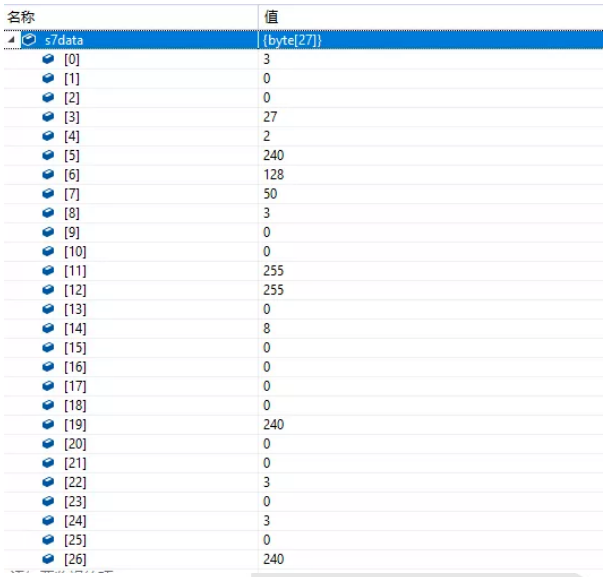
4 西门子 PLC 基础设置说明

西门子PLC支持很多种通信协议，主要分为两种，一种是串口通信，一种是以太网通信，同时也可以通过OPC实现数据通信。西门子PLC通信还是以太网通信为主，我们常说的西门子通信协议分别是S7协议和Profinet协议，但是Profinet是一种总线协议，目前，C#是无法直接与西门子PLC走Profinet通信的。因此，西门子PLC常用的以太网通信方案为S7通信：基本上从S7-200到S7-1500均可以实现，这里有很多可以选择的开源或商业库，包括http://s7.net、pronodave、libnodave、sharp7、Hslcomm，也可以自己封装通信库。本规范中使用的是HslCommunication组件库。

S7通信协议优势在于不需要编写PLC程序，而且S7协议在底层做了很强的封装，在上位机通信应用中相比其他通信协议来说，也有很大的优势。虽然不需要编写PLC程序，但仍然需要做一些简单的配置。

4.1 西门子 PLC 读取 PDU 限制

S7协议一次性读取有限制，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，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。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，下图展示的是S7-1200PLC返回的报文，0和240的组合即为240。



名称	值
s7data	{byte[27]}
[0]	3
[1]	0
[2]	0
[3]	27
[4]	2
[5]	240
[6]	128
[7]	50
[8]	3
[9]	0
[10]	0
[11]	255
[12]	255
[13]	0
[14]	8
[15]	0
[16]	0
[17]	0
[18]	0
[19]	240
[20]	0
[21]	0
[22]	3
[23]	0
[24]	3
[25]	0
[26]	240

图1　S7-1200 二次握手返回报文

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），一次性能读取的字节越长，越能提高上位机的通信效率。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。测试发现针对S7-1200取M区的8000个字节的耗时约800ms。

4.2　西门子 PLC 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，再进行测试发现耗时约为50ms。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。

5 西门子 PLC 配置说明

5.1 西门子 PLC 端配置说明

1）开启Put/Get。PLC侧需要设置勾选允许来自远程对象的Put/Get通信访问 对于西门子1200/1500系列，必须要勾选允许Put/Get访问，对于200Smart/300/400，则不需要。

2）DB块去除优化访问。对于基于博图开发S7-1200/1500的项目，如果要与DB块数据通信，需要要去除DB的优化的块访问，对于200Smart/300/400，则不需要。如果希望通过标签通信，可以采用OPCUA。

3）务必保证通信地址是有效地址。因为PLC大多数是基于存储区的，每个地址肯定是隶属于某个存储区，西门子PLC自带的存储区有I区、Q区、M区、T区、C区，但是对于常用的DB存储区是没有的，需要自行创建，也就意味着，如果需要读取DB地址，必须要提前创建好DB存储区，除此以外，DB存储区创建之后，默认是没有字节的，需要自己一个个添加变量，才能形成有效存储区，因此一个DB存储区的范围是有限并且可见的（可以通过偏移量看出来）。

5.2 西门子 PLC 交互节点创建说明。

1）电控软件工程师在设计与上位机软件交互通讯的变量时，应尽量将节点创建在DB储存区，并在汇总后导出变量储存地址（地址偏移量）。

2）电控软件工程师在设计与上位机软件交互通讯的变量时，应当尽量避免与自身程序运行变量重叠的现象，避免在进行程序修改时出现交互变量地址整体偏移的情况。

3）电控软件工程师在更新程序时，应当尽量避免对交互变量区进行变量的删除和涉及变量类型的修改，避免出现交互变量地址整体偏移的情况。程序修改时，应该对当前变量区后端进行添加操作，保留原本的变量地址。当出现大面积颠覆性修改时。可与上位机软件工程师沟通进行整体更新和修改。

4）电控软件工程师在设计与上位机软件交互通讯的变量时，应当将相同功能模块变量节点设计成结构体的形式，相同功能进行在连续的数据分区，构成连续的地址字节。方便后期上位机软件工程师进行批量配置、批量采集和批量写入。提高交互效率。

6 .net S7 读取上位机设计规范

本上位机通讯采集模块由青岛鼎信通讯股份有限公司工程技术本部自动化部软件组基于HslCommunication组件库，以保持与已有OPC UA 通讯框架相似保证其他模块的快速切换，自行设计、开发。本章将会对.Net S7 读取和采集模块的设计模式进行说明，以供后续开发着对模块架构、类、方法等快速熟悉了解。

6.1 重点类简介

1） HslcommS7ItemServiceImpl。西门子S7通讯协议服务实现。管理本工站所有西门子PLCS7通讯客户端管理实例（HslcommS7ClientItem），方法主要包括连接/断开Server、创建断开变量节点订阅、读取指定节点数据等功能，通过HslDataChanged事件将客户端管理实例中的变量数值变化进行汇总时间上报。

2)HslcommS7ClientItem ：西门子PLCS7通讯客户端管理实例,管理具体PLC的HslS7 Server(HslSiemens)信息、具体读写客户端实例(HslSiemensClient)、HslS7 操作变量（HslSiemensOperatedata）列表、HslS7监视变量(HslSiemensMonitordata)列表，负责进行具体的连接/断开Server、创建断开变量节点订阅、读取指定节点数据等功能。将客户端返回的监视变量变化值转化为操作变量变化值，通过HslDataChanged事件上报。

3）HslSiemensClient ： 西门子PLCS7通讯客户端,包含HslConnOpera、HslReadOpera、HslWriteOpera、HslMonitoredItemsOpera、HslSubscriptionOpera 等具体操作类，具体方法包括HslSubscriptionOpera创建对监视变量的监视订阅器（HslSubscription）。在HslConnOpera中进行断开/连接，HslReadOpera中读取节点数据，HslWriteOpera中写入节点数据，并通过DataChangedEventHandler事件上报至上一层。

4）HslSubscription ：监视变量监视订阅器，通过管理并循环读取监视变量列表中的所有变量，将值发生变化的节点值和具体变化量通过DataChangedEventHandler事件上报至HslSiemensClient。

5）HslSiemensOperatedata ：HslS7 操作变量，是我们在其他任务模块中配置的变量，是解析后最终使用的数值。包含bool，short，int，float， double 等类型。支持单个读取和写入，是监控模块与外界交互的具体实例数据类型。

6）HslSiemensMonitordata ：HslS7 监视变量，是我们为了提高交互效率、加快数据采集频率对数据采集监控模块而设计的数据类型，其支持单个标量请求和原始字节请求。通过一次性采集多个操作变量的地址内容。通过解析后可映射为一个或多个操作变量。从而提高效率。

版本记录

版本编号/修改状态	拟制人/修改人	审核人	批准人	备注
V1.0	刘春松	张路	周利民	