

SMART PLC 之间 Get/Put 网络通讯的实现

陕西航泰电气有限公司 秦建军

摘要：公司一主要产品控制系统涉及到 S7200CN 之间 PPI 网络通讯，西门子新推出的 SMART PLC 不支持 PPI 网络，增加了以太网，本文旨在验证 Get/Put 网络应用在公司产品控制系统中的可行性，为公司将来选用 SMART 替代 CN 做好前期准备。

关键词：以太网； Get/Put 指令； Get/Put 向导

1 引言

实现 2 台 CPU SR30 AC/DC/RLY（6ES7 288-1SR30-0AA0）之间以太网连接通讯，验证 SMART PLC 之间组成以太网的可行性以及便捷性。

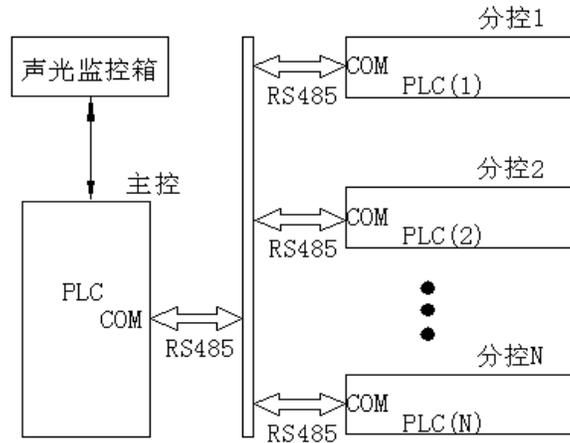
2 工艺要求

煤矿井下运输安全是煤矿安全生产的重要一环，一条斜井运输巷道每隔一定距离分布有一套安全辅助设备。在矿井上水平面设有绞车房，作为整个运输系统控制中枢，控制绞车（滚筒）收卷释放钢丝绳牵引矿车在一定倾角范围内的斜坡上下运行达到运输物料的目的。

工艺要求矿车失控（例如钢丝绳断裂）时，设置在斜坡运输轨道上的安全辅助设备（挡车栏）必须可靠关闭，缓冲拦截失控矿车，避免矿车失控后强大的动能冲击对矿井内人员、设备造成伤害。

分散布置在 1 千米左右斜井轨道上的安全设备（挡车栏）如果要集中控制显然不是经济的选择。目前业界井下运输安全防护系统——跑车防护装置普遍采用 PLC 之间联网分散控制，集中管理的方案。上车场平台（操控点）布置主站，与散布在一条斜井轨道上的众多分站联网，主站主动收发信息，分站就地控制设备，连接于主站的监控设备显示主站收集的各个分站信息，便于绞车操作员做出判断处理。

系统控制原理框图如下图：



声光监控箱作为人机交互界面显示联网的所有分站控制的设备状态。对于以上介绍的系统，联网设备一模一样，每套设备我们只关心提起、落下到位情况、运行情况，所以每套联网设备设计“报警”、“上限位”、“运行”、“下限位”四个状态显示。同时还可以作为指令开关的载体。

主控（主站）收集矿车位置和指令开关信号，实时通讯提供给分站（分控）作为就地控制电机运转提升下放挡车栏的信号，同时接收各个分站的设备状态信息。

分站（分控）接收主站（主控）信号分析判断提升下放挡车栏。

3 自动化平台选型

矿井下设备众多、环境恶劣、情况复杂，对设备安全性（防爆、本安）、可靠性有很高要求。PLC 在控制系统中可靠性、抗干扰性表现优秀，成为井下设备控制系统控制器的首选。

以上介绍的系统，无论主站还是分站，输入输出点数不多，属于小型控制系统。

- 每套装置输入输出点数合计在 20~30 点以内
- 需要具有良好的 PLC 之间简单组网功能（一般不会考虑扩展网络接口）
- 良好的可靠性、抗干扰能力（对速度要求不是很高，但是对可靠性要求很高）

以上三点，目前市面上见到的小型 PLC 基本都能提供满足要求的 CPU 模块。我曾经使用了 5 台西门子 CPU224CN 控制器组网，利用 V4.0 STEP 7 MicroWIN SP9 提供的 NETR/NETW 向导功能编写控制逻辑，在 800 米距离的井下跑车防护控制系统中成功使用，目前运行良好。

本次设计主要目的是实现 SMART PLC 之间 Get/Put 网络连接，验证将来同样工况条件下能否使用 SMART PLC 之间以太网实现跑车防护装置的逻辑控制要求，至于通讯距离与速率问题不在本次测试范围内。

硬件环境：

2 台 CPU SR30 AC/DC/RLY（6ES7 288-1SR30-0AA0）

一台 TP-LINK（TL-R402）路由器

软件环境：

STEP 7-MicroWIN SMART 编辑软件

Microsoft Windows XP Professional Service Pack 3（2002 版本）

4 PLC 程序设计

2 台 SR30，一台做主机（192.168.2.200），一台做从机（192.168.2.201）

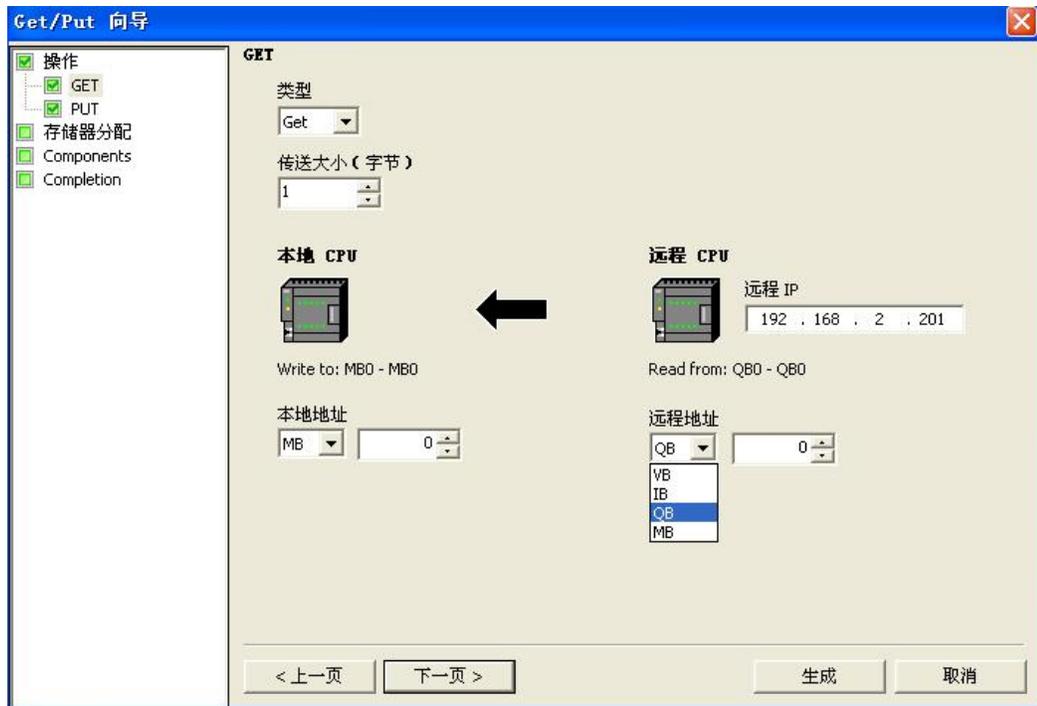
主站 PLC 输入输出点定义：

序号	符号	地址	注释
1	传感器 1	I0.0	1#挡车栏位置传感器（只对 1#地址设备有效）
2	控制按钮	I0.1	对所有联网分站设备有效
3	复位	I0.2	报警后复位，对所有联网分站设备有效
4	报警 1	Q0.0	1#挡车栏故障
5	开到位 1	Q0.1	1#挡车栏开到位
6	运行 1	Q0.2	1#挡车栏正在运行（上提、下放）
7	关到位 1	Q0.3	1#挡车栏关到位

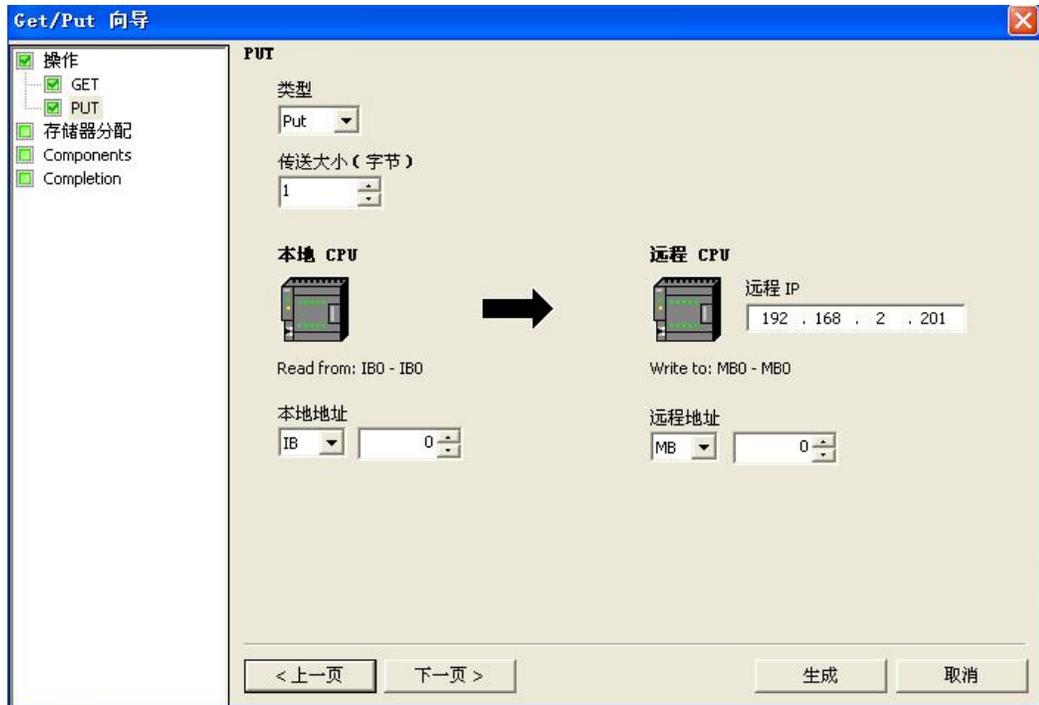
四个输出量 Q0.0~Q0.3 点亮声光监控箱指示灯，指示远方设备运行情况；三个输入量 I0.0~I0.2 信号通讯传送给分站，传感器 1 信号一对一传送控制对应的远方挡车栏运行，只对应分站有效，控制按钮、复位指令对所有联网分站均有效。

对于主站来说只需要将三个输入信号 PUT 给分站，同时 GET 来自联网分站的状态信息输出 Q 位驱动点亮状态指示灯即可。

使用 STEP 7-MicroWIN SMART 提供的 GET/PUT 向导工具进行以太网连接编程。
如下图所示：主要完成主站分站交换数据地址的对应设置，系统就会自动生成一个供使用者调用的子程序。



GET 操作将远程分站中的一个字节 QB0 中的状态量传送（映射）到本地主站中一个字节 MB0。



PUT 操作将本地主站中的一个字节 IB0 中的传感器信息传送（映射）到远程分站中的一个字节 MB0 中。

主站控制器 STL 程序如下：

Network 1

// 将收集到的输入量 IB0 信号通过以太网 PUT 到分站作为就地控制信号 MB0，同时 GET 分站输出的状态信号 QB0 作为显示信号 MB0 输出

LD SM0.0

LPS

CALL SBR1, +0, M1.0, M1.1

A M0.0

= Q0.0

LRD

A M0.1

= Q0.1

LRD

A M0.2

= Q0.2

LPP

A M0.3

= Q0.3

由于 GET/PUT 向导工具的强大功能，以上逻辑只需简单的一个网络就可实现。

分站 PLC 输入输出点定义：

序号	符号	地址	注释
1	上提按钮	I0.0	提升挡车栏
2	下放按钮	I0.1	下放挡车栏
3	复位	I0.2	报警后复位
4	上提到位	I0.3	上限位停止提升
5	下放到位	I0.4	下限位停止下放
6	故障报警	Q0.0	运行时故障报警停止电机
7	上限位置	Q0.1	上限位置停止电机正转提升挡车栏
8	电机运行	Q0.2	电机运行状态（包括正转、反转）
9	下限位置	Q0.3	下限位置停止电机反转下放挡车栏
10	提升	Q0.4	挡车栏电机正转
11	下放	Q0.5	挡车栏电机反转

对于分站不需要再次进行 GET/PUT 向导设置，由于主站中已经设置 PUT: IB0-MB0 的映射，所以在分站直接使用 MB0 就行。其 M0.0 实质就是主控中定义的传感器 1(I0.0) 信号。

分站控制器 STL 程序如下：

Network 1

// 挡车栏运行过程中出现故障（长时间不到位或者短时间不能离开原位置）后输出报警同时停止电机运行，按下复位（有主站复位信号和分站复位信号）报警消除

```
LD    T210
O     T211
O     T220
O     T222
O     Q0.0
AN    M0.2
AN    I0.2
=     Q0.0
```

Network 2

// 分站就地按钮控制提升以及主站通讯过来的提升信号（位置传感器信号、主站人为指令信号）控制提升

```
LD    I0.0
O     M0.0
O     M0.1
EU
LPS
AN    Q0.0
AN    I0.3
AN    M0.2
AN    I0.2
S     M10.0, 1
LPP
R     M11.0, 1
```

Network 3

// 分站就地按钮控制下放以及主站通讯过来的下放信号（位置传感器信号和主站人为指令信号消失）控制下放，来自主站复位信号以及分站复位信号在消除报警输出的同时下放挡车栏

LD M0.2

O I0.2

AN M0.0

AN M0.1

O I0.1

EU

LD M0.0

O M0.1

ED

OLD

LPS

AN Q0.0

AN I0.4

S M11.0, 1

LPP

R M10.0, 1

Network 4

// 到位或者故障后停止电机运转，同时正反向闭锁

LD M10.0

O I0.4

O Q0.0

EU

R M11.0, 1

Network 5

// 到位或者故障后停止电机运转，同时正反向闭锁

LD M11.0

O I0.3

O Q0.0

EU

R M10.0, 1

Network 6

// 正反向切换运转延时 1s 执行

LD M10.0

TON T201, 10

Network 7

LD T201

AN Q0.5

= Q0.4

Network 8

LD M11.0

TON T202, 10

Network 9

LD T202

AN Q0.4

= Q0.5

Network 10

// 提升故障判断

LD Q0.4

LPS

AN I0.3

TON T210, 100

LPP

A I0.4

TON T211, 30

Network 11

// 下放故障判断

LD Q0.5

LPS

AN I0.4

TON T220, 100

LPP

A I0.3

TON T222, 30

Network 12

// 电机双向运行信号合成后提供给主站作为信息显示用

LD Q0.4

O Q0.5

= Q0.2

Network 13

// 到位信号输出到 Q 位上传

LD I0.3

= Q0.1

Network 14

// 到位信号输出到 Q 位上传

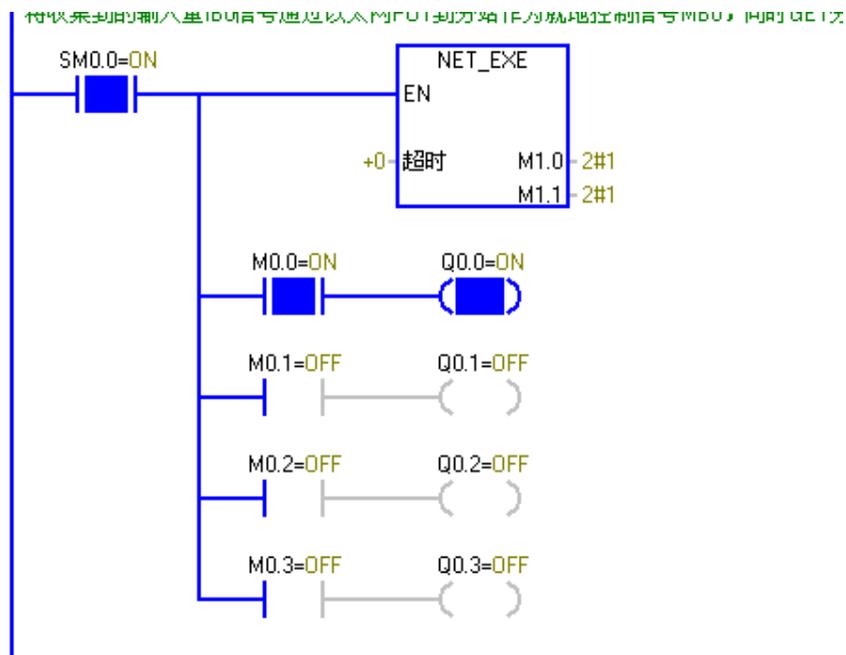
LD I0.4

= Q0.3

5 结束语

由于矿井下特殊性，不能迅速直接进行多台 SMART PLC 以太网连接的实际应用。本报告仅仅只是用 2 台 CPU SR30 AC/DC/RLY（6ES7 288-1SR30-0AA0）进行的实际项目模拟测试。测试过程中感觉相较于目前大量使用的 CN，SMART 确实在很多方面做了改进，但毕竟是刚刚推出的一款新的产品，软硬件肯定还有需要完善的地方。期待西门子大量测试调研后下一版本更加优秀。

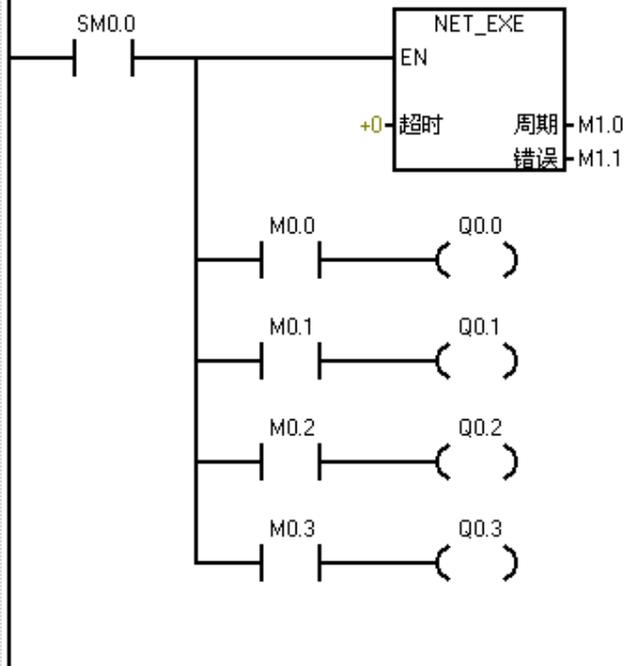
SMART 增加了以太网通讯口，但是又砍掉了 RS485 口的编程连接功能。这样导致有以太网连接功能的逻辑不能监控。



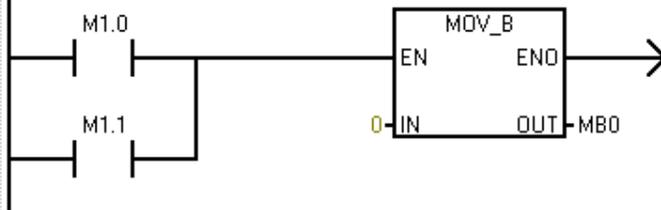
以上主控逻辑在与分控中断以太网连接后随机监控发现：周期(M1.0)/错误(M1.0)，会出现 M1.0=0/M1.1=0；M1.0=0/M1.1=1；M1.0=1/M1.1=0；M1.0=1/M1.1=1；超时一直为 0 的不同情况，感觉好像不大合理。既然断网了，有故障了，分站映射的 M0.0 应该自动复位，不应该保持原来的状态。

主控程序增加逻辑，如下图：

1 将收集到的输入量IB0信号通过以太网PUT到分站作为就地控制信号M0，同时



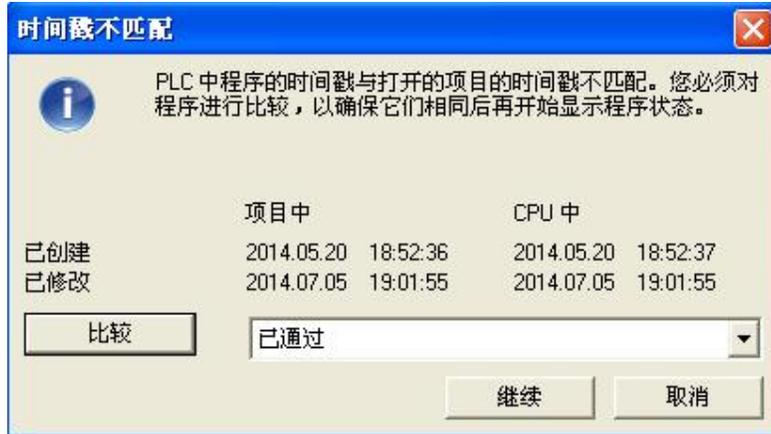
2 输入注释



将以上程序下载进主控 PLC，正常联网运行时，如果 Q0.0~Q0.3 中有输出就会出现输出抖动的情况。

所以感觉还是硬件中做成断网后软件自动复位为好。

另外即使是刚刚下载完程序，点击“程序状态监视”进行梯形图监控时也会弹出如下对话框要求比较，这个很是烦人（即使 PLC 与 PC 核对时间后问题依旧）。



作者简介：

秦建军：（1974—），陕西宝鸡人，电气自动化专业专科，目前供职于陕西航泰电气有限公司，从事煤矿井下安全辅助设备控制系统设计研发工作。

参考文献：

[1] S7-200 SMART PLUS

[2] s7-200_SMART_system_manual_zh-301310CHS