Siemens PPI协议分析

大家好：由于前段时间的疯狂的研究西门子PPI协议解密之故，所以无心插柳的研究出了较实用的西门子S7-200 PPI协议，今天奉献大家。我们经常要用于上位机、现场设备与S7-200CPU之间的通讯，但是西门子公司没有公布PPI协议的格式，用户如果想使用PPI协议监控，必须购买其监控产品或第三方厂家的组态软件。大家要知道国内的组态王、紫金桥、力控等等组态公司是花了多少钱才得到的PPI的深层协议吗？其实西门子工控产品的超高价垄断掠夺行为已经引起了我们国家及业内人士的抵制和抗议，他们的什么软件都需要授权且对于系统的霸道性是有目共睹的。
这样给用户自主开发就带来了一定的困难，特别是想用VB、VC等语言自行开发，根本没办法接入PLC，要么你大把掏钱给他们。我是通过一个串口监视软件的数据监视与分析，找出了PPI协议的关键报文格式所在。
其实西门子S7-200 PLC之间或者PLC与PC之间通信有很多种方式:自由口，PPI方式，MPI方式，Profibus方式。使用自由口方式进行编程时，在上位机和PLC中都要编写数据通信程序。使用PPI协议进行通信时，PLC可以不用编程，而且可读写所有数据区，快捷方便。这也是我们之所以要研究、找出PPI协议的源动力！
下面我们就要说说分析的方法了！
西门子的STEP 7 MicroWIN 是用于S7-200系列PLC的开发工具，它使用PC机上的COM口通过一条PC/PPI编程电缆连到PLC的编程口上。这说明，PC实际上是可以通过串口同S7-200 CPU通讯。只是我们不知道通讯协议而已。通过截获PC机串口上的收发数据，对照Step 7软件发出的指令，我们就有可能分析出有关指令的报文和通讯方式；然后，直接通过串口向PLC发送报文，以验证这些指令报文是否正确。本着这一思想，我们采用以下步骤获得这些报文。
你首先下载上面那个英文的串口监控软件，英文不好的网友可以使用我们为你汉化的汉化包，替换原文件即可，你必须使用这个软件，因为我先前使用过很多的监控软件，在收发数据很多的情况下都有死机现象，造成数据丢失，容易给我们错误分析。接下来你先打开这个软件，新建、选择端口COM1,然后再将PC/PPI编程电缆接在COM1上，这样，Step7 Micro/Win发给PLC的报文就可以在监视软件上完全裸露的展现在你的面前了。我们按S7-200系统手册设置好串口参数：9600，8，E偶校验，1位停止位。然后设置好Step7软件，使之能与S7-200 CPU正常通讯。从Step7软件中发出一个明确指令，监视软件就能显示这条报文了（用16进制显示，ASCII码的只能看到几个版本号之类的，其他都没有意义）。
我们的破解策略就是通过软件监视的方法，分析PLC内部固有的PPI通讯协议，然后上位机采用VB编程，遵循PPI通讯协议，读写PLC数据，实现人机操作任务。这种通讯方法，与一般的自由通讯协议相比，省略了PLC的通讯程序编写，只需编写上位机的通讯程序资源。S7-200的编程口物理层为RS-485结构，SIEMENS提供MicroWin软件，采用的是PPI(Point to Point)协议，关于232串口转485你可以采用我们网站开发研制的自制PPI电缆，效果倍好哦!请点击下载!还是自己动手，丰衣足食啊！

不能光说不练啊！下面我们就说说西门子PLC到底是怎么通讯的。

PC与PLC采用主从方式通讯，PC按如下文的格式发读写指令，PLC作出接收正确的响应（返回应答数据E5H或F9H见下文分析），上位机接到此响应则发出确认命令（10 02 00 5C 5E 16），PLC再返回给上位机相应数据。一般上位机要连接PLC就要先发送如下寻呼数据 10 02 00 49 4B 16 同志们呐！我们可都是有血、有肉、有思想、有灵感的高级动物啊，面对这么多枯燥、无味、复杂、混乱的机器数字你怎么记呢？反正我是记不住啊！（^_^ 开始洗脑）这时你可以闭上眼睛，安静、静、再静。。。。。。想一想战争时期的战地对讲机通话模式，那么这个初始的寻呼指令（10 02 00 49 4B 16）就可以理解为：“洞两洞两（02），我是洞洞（00），听到请回答，听到请回答！over！”。

现在我们来简单地分析一下这个指令的具体含义： 10起始符，咳嗽一声要开始讲话的意思。02是上位机要联系的下位机PLC的地址站号，就是要找的人。 00就是上位机电脑本身自己的站号。49寻呼指令，呼叫寻找的意思。16终止符，over、完毕、结束的意思。 其中4B为校验码，防止数据传输出错而设计的，它是这样得来的：02+00+49和的最后两位就是校验码，这就是所说的偶校验或称和校验也称余校验，因为取的是除以100后的余数。计算器在16进制计算时公式（02+00+49）mod 100得出的数就是校验码，你计算一下是不是等于4B啊！其他的所有PPI协议校验都是如此。假如02站号的PLC收到寻呼信号那么会回答： 10 00 02 00 02 16 意思是：“报告洞洞（00），洞两（02）收到，请指示，over！” 这样的解释是不是很好理解啊！你有更好的解释吗？既然找到了要找的人，接下来PC上位机电脑，就是司令啦！就可以发号施令了。这时上位机发出一条指令，这个指令下面详细解说，发号施令后如果PLC正确接收就会返回 E5 字符，意思是：“明白！”。其实啊，说到这里PLC只说他明白，他已经明白了上位机PC的指示，但并没有执行命令，那么要怎么他才执行命令呢？就是上位机PC发出确认命令后才执行。这时上位机会发出确认指令（10 02 00 5C 5E 16），这里的5C是执行指令，意思是：“请洞两立即执行，over！”。然后PLC就干他该干的工作了！原来PLC也不容易啊，怪不得叫下位机呢！就是下人的意思！

说了这么多乱不乱呐？目的就是要理清上下级关系、主从关系，指令的顺序，用一个好的记忆方法记住枯燥无味的机器码。

下面我们列表分析读取PLC密码的指令：68 1B 1B 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 08 00 00 03 00 05 E0 D2 16

读命令分析：一次读一条数据
1.开始定界符(68H)
2.报文数据长度
3.重复数据长度
4.开始定界符(68H)
5.远程目标地址，指该地址的值，就是PLC的地址
6.本地地址，指该地址的指针，就是上位机自己的地址
7.功能码，5CH为交替周期触发，6CH为首次信息周期触发，7CH为交替周期触发。
8-17.目的服务存取点

18-22.源服务存取点 18位分析：01:位排列 02:字节排列 04:字排列 06:双字排列
23-31.数据单元
32.校验码
33.结束分界符（16H）
报文数据长度和重复数据长度为自DA至DU的数据长度，校验码为DA至DU数据的和校验，只取其中的末字节值关于这个校验码的计算方法同上面说明。
在读写PLC的变量数据中，读数据的功能码为 6CH，写数据的功能码为 7CH。
对于一次读取一个数据，读命令都是33个字节。前面的1—22字节是相同的，为

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
起始符	长度		起始符	远程	本地	功能码			通讯编号				参数长度				04读05写	排列格式			
68	1B	1B	68	02	00	6C	32	01	00	00	00	88	00	0E	00	00	04	01	12	0A	10

读取PLC密码的指令：68 1B 1B 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 08 00 00 03 00 05 E0 D2 16

23	24	25	26	27	28	29	30	31	32	33
读取长度		数据个数		存储器类型		偏移量			校验码	终止符
02	00	08	00	00	03	00	05	E0	D2	16

因为是PC上发的读PLC数据的命令，SA=00，DA=02，如果有多个站，DA要改成相应的站号。读命令中从DA到DU的长度为1B即27个字节。从23字节开始根据读取数据的类型、位置不同而不同。上表是读不同存储器命令的Byte23—33。

字节	23	24	25	26	27	28	29	30	31	32	33
功能	读取长度		数据个数		存储器类型		偏移量			校验码	终止符
读Q0.1	01	00	01	00	00	82	00	00	00	64	16
读M0.0	01	00	01	00	00	83	00	00	00	65	16
读M0.1	01	00	01	00	00	83	00	00	01	66	16
读SMB34	02	00	01	00	00	05	00	00	01	F9	16
读VB100	02	00	01	00	01	84	00	03	20	8B	16
读VW100	04	00	01	00	01	84	00	03	20	8D	16
读VD100	06	00	01	00	01	84	00	03	20	8F	16
读I0.5	01	00	01	00	00	81	00	00	05	68	16
读I0.7	01	00	01	00	00	81	00	00	07	6A	16

上表读命令的Byte23-33从表中我们可以得出以下结果：
Byte 23 读取数据的长度
01：1 Bit 02：1 Byte
04：1 Word 06：Double Word
Byte 25数据个数,这里是01 ，一次读多个数据时见下面的说明。
Byte 27 存储器类型，01：V存储器 00：其它
Byte 28 存储器类型
04：S 05：SM 06：AI 07：AQ 1E: C
81：I 82：Q 83：M 84：V 1F: T
Byte 29,30,31存储器偏移量指针（存储器地址*8），如：VB100，存储器地址为100，偏移量指针为800,转换成16进制就是320H,则Byte 29—31这三个字节就是：00 03 20。
Byte 32 校验和，前面已说到这是从(DA+SA+DSAP+SSAP+DU) Mod 256 。
一次读多条数据
对于一次读多个数据的情况，前21Byte与上面相似只是长度LD，LDr及Byte 15不同：
Byte 15 数据块占位字节，它指明数据块占用的字节数。与数据块数量有关，长度=4+数据块数*10,如：一条数据时为4+10=0E(H)；同时读M,V,Q三个不同的数据块时为4+3*10=22(H)。
Byte 23 总是02 即以Byte为单位。
Byte 25 以字节为单位，连续读取的字节数。如读2个VD则Byte25=8
Byte 19---30 按上述一次读一个数据的格式依次列出，
Byte 31---42 另一类型的数据，也是按上述格式给出。
以此类推，一次最多读取222个字节的数据。

写命令分析：

一次写一个Double Word类型的数据，写命令是40个字节，其余为38个字节。写一个Double Word类型的数据，前面的1—22字节为：

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	15	17	18	19	20	21	22
起始符	长度		起始符	远程	本地	功能码															
68	21	21	68	02	00	7C	32	01	00	00	00	00	00	0E	00	00	04	01	12	0A	10

68 23 23 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10
写一个其它类型的数据，前面的0—21字节为：（与上面比较，只是长度字节发生变化）
68 21 21 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10

23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38

数据长度		数据个数		存储类型		偏移量			数据形式		数据位数		写入值	校验码	终止符
01	00	01	00	00	82	00	00	00	00	03	00	01	01	79	16

从22字节开始根据写入数据的值和位置不同而变化。上表是几个写命令的Byte22—40。
字 节 23 24 25 26 276 28 298 30 31 32 33 34 35 36 37 387 39 40 41
写入位置及值长度 个数 类型 偏移量 位数 值、校验码、 结束符
M0.0=1 01 00 01 00 00 82 00 00 00 00 03 00 01 01 00 71 16
M0.0=0 01 00 01 00 00 83 00 00 00 00 03 00 01 00 00 70 16
M0.1=1 01 00 01 00 00 83 00 00 01 00 03 00 01 01 00 72 16
vb100=10 02 00 01 00 01 84 00 03 20 00 04 00 08 10 00 AE 16
vb100=FF 02 00 01 00 01 84 00 03 20 00 04 00 08 FF 00 9D 16
VW100=FFFF 04 00 01 00 01 84 00 03 20 00 04 00 10 FF FF A6 16
VD100=FFFFFFFF 06 00 01 00 01 84 00 03 20 00 04 00 20 FF FF FF FF B8 1

写命令的Byte22—最后， 经分析我们可以得出以下结果：
Byte 23-- Byte 31 写入数据的长度、存储器类型、存储器偏移量与读命令相同。T，C等不能用写命令写入。
Byte 33 如果写入的是位数据这一字节为03，其它则为04
Byte 35 写入数据的位数
01: 1 Bit 08: 1 Byte 10H: 1 Word 20H: 1 Double Word
Byte 36--41值、校验码、结束符
如果写入的是位、字节数据，Byte35就是写入的值，Byte36=00，Byte37=检验码，Byte38=16H，结束。如果写个的是字数据（双字节），Byte35,Byte36就是写入的值， Byte37=检验码，Byte38=16H，结束。如果写个的是双字数据（四字节），Byte35—38就是写入的值，Byte39=检验码，Byte40=16H，结束。

看完上面的指令分析我们现在就举例几个常用的PPI协议来分析一下：
PC寻呼：10 02 00 49 4B 16
PLC返回：10 00 02 02 04 16
PC发送:10 02 00 5C 5E 16
PLC返回: E5
我们先来看看西门子S7 - 200PLC的读取密码指令：
请用串口软件以16进制发送，端口设置9600；e；8；1
发送:68 1B 1B 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 08 00 00 03 00 05 E0 D2 16 意思：要求传送（03区）系统存储区05E0位开始的8个字符（这就是8个密码数值）。
如果通讯无误，PLC会返回 E5，意思：已经收到
那么这时上位机再次发送确认执行指令 10 02 00 5C 5E 16 意思：请执行命令。（说到这里打住一下，PLC返回E5指令后上位机PC要在很短的时间内发送确认指令，晚了刚才的指令就无效了具体多长时间我也没测准，反正1、2秒时间是没有问题的。这也是很多网友问我通讯失败的原因所在）那么这时PLC还就真的乖乖的执行命令，返回如下字符：68 1D 1D 68 00 02 08 32 03 00 00 00 00 00 02 00 0C 00 00 04 01 FF 04 00 40 9B 98 02 06 9D 9A 00 76 7D 16
好了，说到这里就此停止，大家看看密码是多少啊！你如果真正明白了PPI协议就不难找出出密码了，但是这个密码是经过二次加密的，并不是真正的密码，还需要破译，至于密码算法在此不便公开，不过你多做实验一定能得出结果的。
下面再看一个读取PLC版本号的指令：
我们在解密中首先要确定的是PLC的版本号。就是要看看是老版本还是02版的，也好做出加解密方案。他的通讯源码是这样的：
68 1B 1B 68 02 00 7C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 14 00 00 03 00 00 00 09 16
发送完上面数据PLC返回E5.
再次发送确认指令：10 02 00 5C 5E 16
这时plc的版本号就返回来了。看下面：
68 29 29 68 00 02 08 32 03 00 00 00 00 00 02 00 18 00 00 04 01 FF 04 00 A0 43 50 55 20 32 32 36 20 43 4E 20 20 20 20 20 20 30 32 30 31 D7 16
你看这一段：43 50 55 20 32 32 36 20 43 4E 20 20 20 20 20 20 30 32 30 31 就是plc版本号的ASCII码。用ASC方式显示就会看的更明白上面数据是：C P U SP 2 2 6 SP C N 0 2 0 1 （sp就是空格）0201是版本号。
再一个就是读TD200密码指令：
68 1B 1B 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 02 00 01 84 00 00 50 B9 16 （VW10）
写M0指令：
68 20 20 68 02 00 7C 32 01 00 00 00 00 00 0E 00 05 05 01 12 0A 10 01 00 01 00 00 83 00 00 00 00 03 00 01 01 80 16
读222位3区（系统区）数据指令：
68 1B 1B 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 DE 00 00 03 00 00 00 C3 16
读取密码保护位指令：
68 1B 1B 68 02 00 6C 32 01 00 00 00 00 00 0E 00 00 04 01 12 0A 10 02 00 01 00 00 03 00 05 D8 C3 16
改写密码保护位指令：（你来验证是否可行）
68 20 20 68 02 00 7C 32 01 00 00 00 00 00 0E 00 05 05 01 12 0A 10 08 00 01 00 00 03 00 05 D8 00 04 00 08 04 EF 16
68 20 20 68 02 00 7C 32 01 00 00 00 00 00 0E 00 05 05 01 12 0A 10 02 00 01 00 00 03 00 05 D8 00 03 00 08 04 E8 16
全部清除指令：
68 21 21 68 02 00 7C 32 07 00 00 00 24 00 08 00 0C 00 01 12 04 11 45 01 00 FF 09 00 08 16 19 06 0D 01 08 18 1E EE 16

关于此PPI协议我也是初步研究难免有失误之处，希望众网友有更好的见解与发现能够到我们论坛发表，也可以给我QQ留言！

微信号: plcjiemi 电话: 13969908936 E-Mail: plcjiemi@qq.com
在线咨询 京ICP备14025225号-2