组态王通过以太网与西门子 S7-200 smartPLC 通讯

说明文档

北京亚控科技发展有限公司

2021 年 3 月

1.驱动通讯配置步骤：

1.在亚控公司网站或通过组态王技术部下载最新的驱动程序，版本为60.3.24.30；

2.改写下载的驱动中的初始化文件：

该文件夹中的初始化文件“kvS7200.ini”原文为

[192.168.31.12:0]

LocalTSAP=4D57

RemoteTSAP=4D57

TpduTSAP=000A

SourceTSAP=0001

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0001

……

将它改写为：

[192.168.2.1:0]　//实际的 PLC IP 地址

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0001

其中的“192.168.2.1”是 CPU 的 IP 地址。如果有多台 PLC，应列出它们的 IP 地址，例如

[192.168.2.1:0]

[192.168.2.2:0]

3．安装驱动程序

单击 Windows 的“开始”按钮，执行菜单命令“\所有程序\组态王 6.60 SP1\工具\安装新驱动”，打开驱动安装工具（见图 1）。单击“…”按钮，打开保存驱动的文件夹，双击其中的驱动文件“S7_TCP.dll”，单击“安装驱动”按钮，安装成功后显示“安装完成！”（如图 2）。

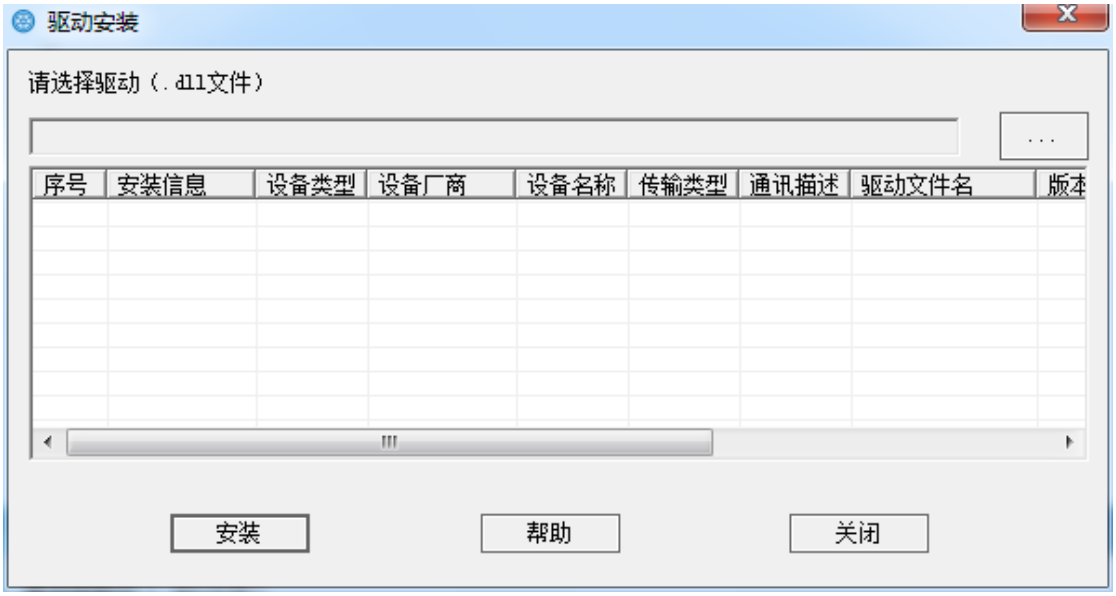


图 1　驱动安装界面

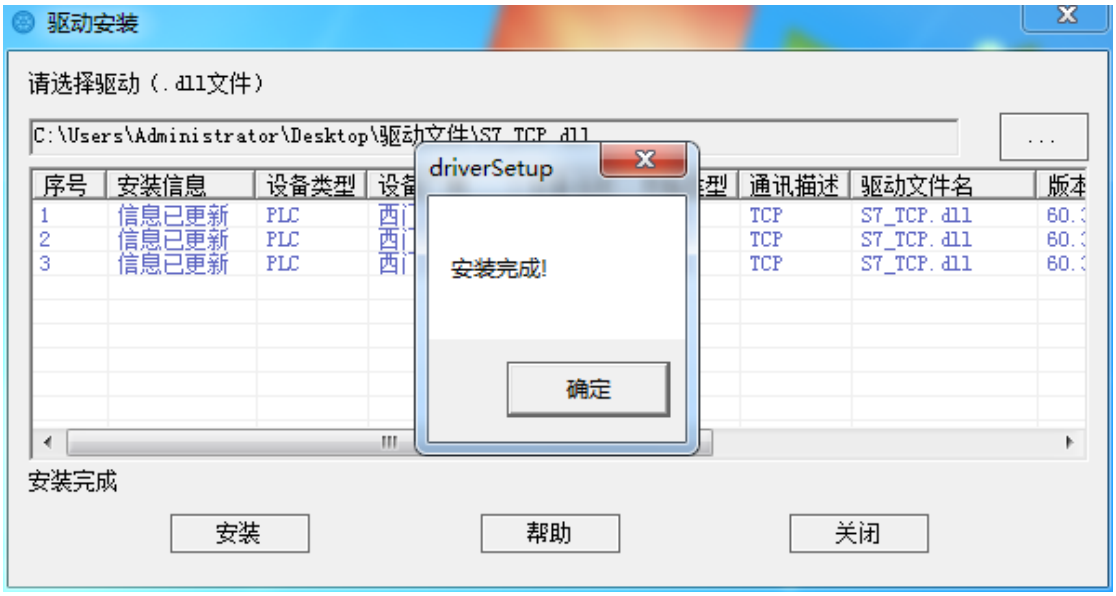


图 2　驱动安装完成提示界面

4．组态通信中的接口

选中工程浏览器中的“设备”，双击右边窗口中的“新建”，弹出设备配置向导界面。选中设备驱动列表中的“PLC”- “西门子”-“S7-200（TCP）”-“TCP”。单击“下一步”按钮，填写设备逻辑名称，点击“下一步”按钮，选择所连接的串行设备的串口号，点击“下一步”按钮，设定安装设备的地址为“192.168.2.1:0”，采用默认的恢复间隔和最长恢复时间。

5．通信实验

略。

2.配置说明：

对于新增的 S7200_Smart 设备配置文件做如下说明：

首先以下是配置文件的格式范例：\Program Files\kingview\Driver 文件夹中的 kvS7200.ini。

[192.168.31.12:0]

LocalTSAP=4D57

RemoteTSAP=4D57

TpduTSAP=000A

SourceTSAP=0001

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0001

红色标记是用来区分 Smart 设备的。

蓝色标记对应设备的 IP 地址。

对应字段：

LocalTSAP 和 RemoteTSAP，原 S7 设备默认值为 4D57，Smart 默认值是 0101

对应字段：

TpduTSAP 和 SourceTSAP 是为 Smart 设备新增的两个字段，这两个值是初始化时与原 S7 设备不同的地方（可能会因 Smart 设备型号不同而值发生变化导致无法连接，这种情况需要截取现场数据帧来确认这两个值，确认方法见附录）

对于多上位的配置依然是修改 LocalTSAP 和 RemoteTSAP 字段，配置操作应与原驱动说明文档中类似，此二值由西门子软件配置。

```
[192.168.2.1:0]
/SMART
LocalTSAP=0201
RemoteTSAP=0201
TpduTSAP=000A
SourceTSAP=0000
```

如上图 LocalTSAP 和 RemoteTSAP 改为 0201 即可支持两个上位连接。此二值可选 0101、0201、0301 三个值。

【SR60】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=000A

【SR30】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0001

【CR40】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0001

【CR60】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0001

【1SA00】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=031C

【ST40】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0009

【SR20】 【SR40】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0009

【ST60】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=00DD

【ST40】【ST30】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0009（【ST40】:0001、0152）

【SR20】【SR30】【SR40】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=0009（SR30 还可以设置为 0001，SR40 还可以设置为 0006）

【ST60】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

SourceTSAP=00DD　(也可以是 0003、0329、000F、005A、004F)

【ST20】

[192.168.2.1:0]

/SMART

LocalTSAP=0101

RemoteTSAP=0101

TpduTSAP=000A

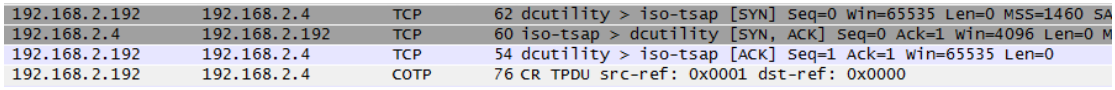
SourceTSAP=0011

如果应用的 smart 的型号此上没有，可以使用一下方法获取：

附录：

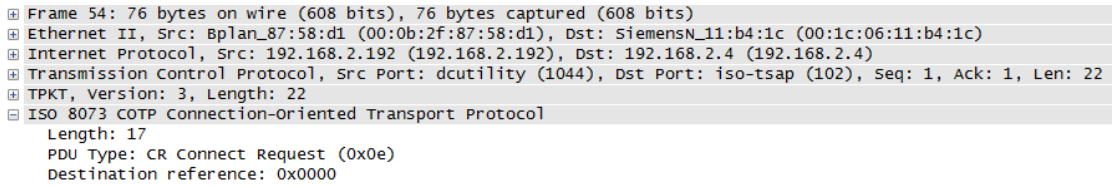
应用 wireshark 软件：

确认方法如下：



在西门子软件与设备三次握手成功后的第一帧中包含配置文件中的所有的需要的数据。

选择第一条数据后下面会有对应的数据如图：

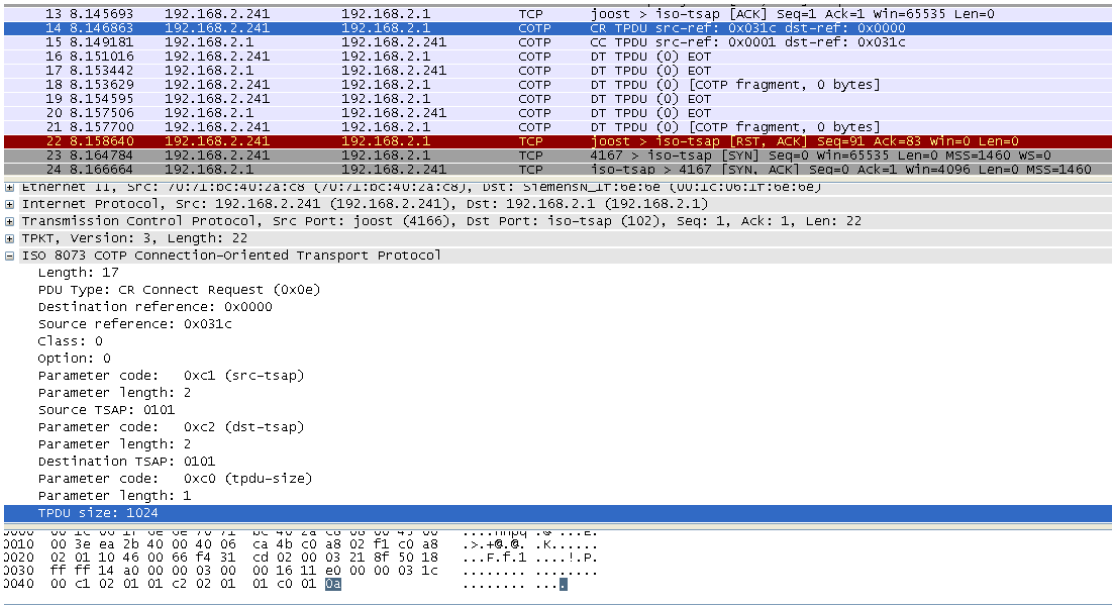


点开 ISO 8073 包含的内容，其中：

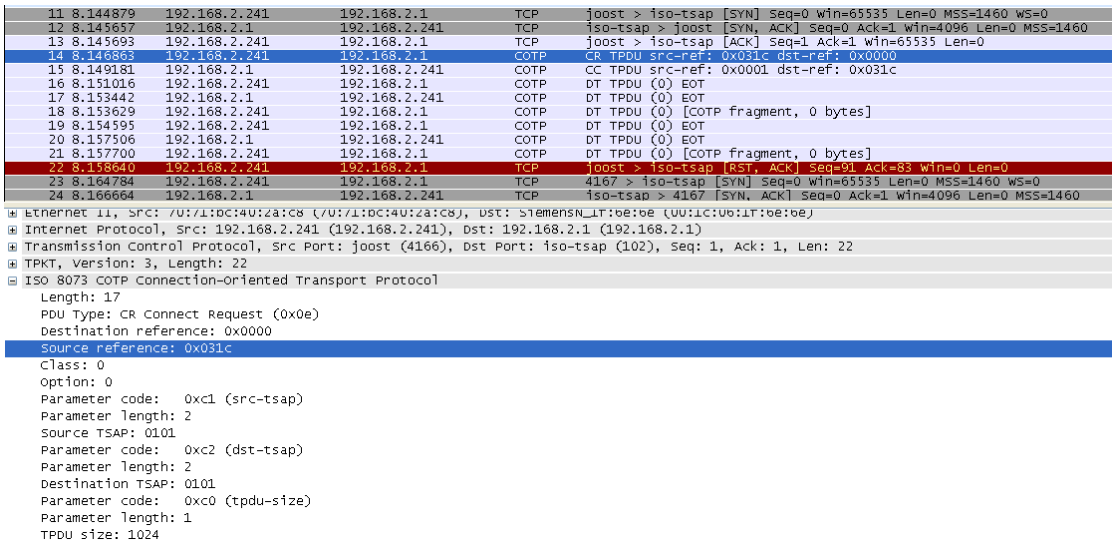
内容 TPDU size 对应字段 TpduTSAP 的值；

内容 Source reference 对应字段 SourceTSAP 的值；

TPDU 为单字节数据，高位补零，例如 TPDU size 对应数据为 0x0A，对应到配置文件为 0x000A。如下图所示：

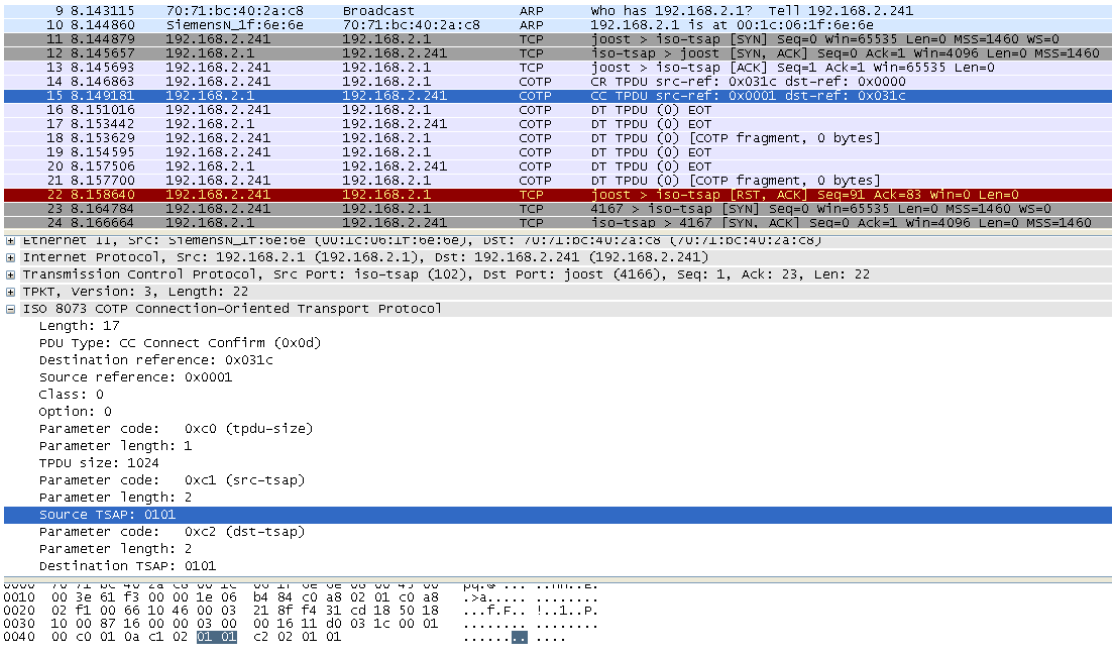


内容 Source reference 对应字段 SourceTSAP 的值；如下图示 031C



对应修改即可。

（注：配置文件中涉及到数据的字母均大写）



3.TSAP 参数的设置：

TSAP,传输服务访问点，Transport Service Access Point 的缩写，表示的是连接资源的地址。ISO-on-TCP 协议允许至单个 IP 地址的多个连接。TSAP 可唯一标识连接到同一个 IP 地址的这些通信端点连接。端口 102 为 ISO-on-TCP 协议所专用。不能为此协议设置端口号,不过,可以为本地或远程伙伴设置 TSAP。

TSAP 参数的设置通过 PC_Access_SMART 进行。

TSAP 规则如下：

- TSAP 须为 S7-200 SMART 字符串数据类型（长度字节，后接字符串）；
- TSAP 长度必须至少为 2 个字符，但不得超过 16 个 ASCII 字符；
- 本地 TSAP 不能以字符串“SIMATIC-”开头；
- 如果本地 TSAP 恰好为 2 个字符，则必须以十六进制字符“0xE0”开头。例如：TSAP“$E0$01”是合法的，而 TSAP“$01$01”则是不合法的。（“$”字符表示后续值为十六进制字符。）