组态王通过以太网与西门子 S7-200 smartPLC 通讯

说明文档

亚控科技 WellinTech

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.dl1",单击"安装驱动"按钮, 安装成功后显示"安装完成!"(如图 2)。

⑧ 驱动:9	3 驱动安装									
请选择	请选择驱动(. 出1文件)									
序号	安装信息	设备类型	设备厂商	设备名称	传输类型	通讯描述	驱动文件名	版本		

图1 驱动安装界面

⑧ 驱动ਤ	安装					line.		X	
请选择驱动(. 出1文件)									
C:\Use	C:\Users\Administrator\Desktop\驱动文件\S7_TCP_d]]								
序号	安装信息	设备类型	设备	driverSetup	型	通讯描述	驱动文件名	版本	
1	信息已更新 信息已更新	PLC PLC	船			TCP TCP	S7_TCP. dl1 S7_TCP. dl1	60.1 60.1	
3	信息已更新	PLC	面门	安装完成!	_	TCP	S7_TCP. dl1	60.1	
				确定					
•									
安装完成									
安装 帮助 关闭									

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 Loca1TSAP=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:

192.168.2.192	192.168.2.4	ТСР	62 dcutility > iso-tsap [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SA
192.168.2.4	192.168.2.192	TCP	60 iso-tsap > dcutility [SYN, ACK] Seq=0 Ack=1 win=4096 Len=0 M
192.168.2.192	192.168.2.4	тср	54 dcutility > iso-tsap [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.2.192	192.168.2.4	COTP	76 CR TPDU src-ref: 0x0001 dst-ref: 0x0000

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:

 Frame 54: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
Ethernet II, Src: Bplan_87:58:d1 (00:0b:2f:87:58:d1), Dst: SiemensN_11:b4:1c (00:1c:06:11:b4:1c)
Internet Protocol, Src: 192.168.2.192 (192.168.2.192), Dst: 192.168.2.4 (192.168.2.4)
Transmission Control Protocol, Src Port: dcutility (1044), Dst Port: iso-tsap (102), Seq: 1, Ack: 1, Len: 22
ISO 8073 COTP Connection-Oriented Transport Protocol Length: 17 PDU Type: CR Connect Request (0x0e) Destination reference: 0x0000

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:

13 8.145693	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap [ACK] Seq=1 Ack=1 Win=65535 Len=0
14 8.146863	192.168.2.241	192.168.2.1	COTP	CR TPDU src-ref: 0x031c dst-ref: 0x0000
15 8.149181	192.168.2.1	192.168.2.241	COTP	CC TPDU src-ref: 0x0001 dst-ref: 0x031c
16 8.151016	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) EOT
17 8.153442	192.168.2.1	192.168.2.241	COTP	DT TPDU (0) EOT
18 8.153629	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) [COTP fragment, 0 bytes]
19 8.154595	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) EOT
20 8.157506	192.168.2.1	192.168.2.241	COTP	DT TPDU (0) EOT
21 8.157700	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) [COTP fragment, 0 bytes]
22 8.158640	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap [RST, ACK] Seq=91 Ack=83 win=0 Len=0
23 8.164784	192.168.2.241	192.168.2.1	TCP	4167 > iso-tsap [SYN] Seq=0 win=65535 Len=0 MSS=1460 wS=0
D4 0 166664	100 160 0 1	100 160 0 041	TCD	100 topp > 4167 [SYN ACK] 500-0 Ack-1 Win-4006 Lon-0 MSS-1460

24 8.166664 192.168.2.1 192.168.2.41 TCP iso-tsab > 4167 [Svn. AcK] Seque A W Etnernet II, SrC: /U/I/EC/4U/24/26 (U/I/I/EC/4U/24/26), DST: StemensN_IT:Seise (UU/IC/US/IT:Seise) # Internet Protocol, SrC: 192.168.2.241 (192.168.2.241), DST: 192.168.2.1 (192.168.2.1) # Transmission Control Protocol, SrC Port: joost (4166), DST Port: iso-tsap (102), Seq: 1, Ack: 1, Len: 22 # TFKT, Version: 3, Length: 22 B ISO 8073 COTP Connection-oriented Transport Protocol Length: 17 PDU Type: CR Connect Request (0x0e) Destination reference: 0x0000 Source reference: 0x031c Class: 0 Option: 0 option: 0 Parameter code: 0xcl (src-tsap) Parameter length: 2 Source TSAP: 0101 Parameter code: 0xc2 (dst-tsap) Parameter length: 2 Destination TSAP: 0101 Parameter code: 0xc0 (tpdu-size) Parameter length: 1 size: 1024

00 3e ea 2b 40 00 40 06 ca 4b co 38 02 01 co 40 00 3e ea 2b 40 00 40 06 ca 4b co 38 02 11 co 38 02 01 10 46 00 66 f4 31 cd 02 00 03 21 8f 50 18 ff ff f1 4a 00 00 00 03 00 00 16 11 e0 00 00 00 31 c 00 16 cd 02 01 01 cc 02 01 00 00 00 03 1c 0010 0020 0030 0040

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

11 8.144879	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap [SYN] Seq=0 win=65535 Len=0 MSS=1460 wS=0
12 8.145657	192.168.2.1	192.168.2.241	TCP	iso-tsap > joost [SYN, ACK] Seq=0 Ack=1 win=4096 Len=0 MSS=1460
13 8.145693	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap [ACK] seq=1 Ack=1 win=65535 Len=0
14 8.146863	192.168.2.241	192.168.2.1	COTP	CR TPDU src-ref: 0x031c dst-ref: 0x0000
15 8.149181	192.168.2.1	192.168.2.241	COTP	CC TPDU src-ref: 0x0001 dst-ref: 0x031c
16 8.151016	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) EOT
17 8.153442	192.168.2.1	192.168.2.241	COTP	DT TPDU (0) EOT
18 8.153629	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) [COTP fragment, 0 bytes]
19 8.154595	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) EOT
20 8.157506	192.168.2.1	192.168.2.241	COTP	DT TPDU (0) EOT
21 8.157700	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) [COTP fragment, 0 bytes]
22 8.158640	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap [RST, ACK] Seq=91 Ack=83 win=0 Len=0
23 8.164784	192.168.2.241	192.168.2.1	TCP	4167 > iso-tsap [SYN] seq=0 win=65535 Len=0 MSS=1460 WS=0
24 8.166664	192.168.2.1	192.168.2.241	TCP	iso-tsap > 4167 [SYN. ACK] Seg=0 Ack=1 win=4096 Len=0 MSS=1460

24 8.100004 192.106.2.1 192.108.2.241 (10) 150-T505 2410 [SNN. ACK] Seque A # Etnernet II, SrC: /U:/L:0Ci4U:Zaics (/U:/L:0Ci4U:Zaics), UST: StemensN_LT:0e:be (UU:L:U0:LT:0e:be) # Internet Protocol, SrC: 192.168.2.241 (192.168.2.241), DST: 192.168.2.1 (192.168.2.1) # Transmission Control Protocol, SrC Port: joost (4166), DST Port: iso-tsap (102), Seq: 1, Ack: 1, Len: 22

TPKT, Version: 3, Length: 22

IFKI, Version: 3, Length: 22
ISO 8073 COTP Connection-oriented Transport Protocol Length: 17
PDU Type: CR Connect Request (0x0e) Destination reference: 0x0000 Source reference: 0x031c

Class: 0 Option: 0 option: 0 Parameter code: 0xcl (src-tsap) Parameter length: 2 Source TSAP: 0101 Parameter code: 0xc2 (dst-tsap) Parameter length: 2 Destination TSAP: 0101 Parameter code: 0xc0 (tpdu-size) Parameter length: 1 TPDU size: 1024

对应修改即可。

(注: 配置文件中涉及到数据的字母均大写)

9 8.143115	70:71:bc:40:2a:c8	Broadcast	ARP	who has 192.168.2.	1? Tell 192.168.2.241				
10 8.144860	SiemensN_1f:6e:6e	70:71:bc:40:2a:c8	ARP	192.168.2.1 is at	00:1c:06:1f:6e:6e				
11 8.144879	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap	[SYN] Seq=0 Win=65535 Len=(0 MSS=1460 WS=0			
12 8.145657	192.168.2.1	192.168.2.241	TCP	iso-tsap > joost	[SYN, ACK] Seq=0 Ack=1 Win=	=4096 Len=0 MSS=1460			
13 8.145693	192.168.2.241	192.168.2.1	TCP	joost > iso-tsap	[ACK] Seq=1 Ack=1 Win=65535	5 Len=0			
14 8.146863	192.168.2.241	192.168.2.1	COTP	CR TPDU src-ret: (0x031c dst-ref: 0x0000				
15 8.149181	192.168.2.1	192.168.2.241	COTP	CC TPDU src-ref: ()x0001 dst-ref: 0x031c				
16 8.151016	192.168.2.241	192.168.2.1	COTP	DT TPDU (0) EOT					
17 8.153442	192.168.2.1	192.168.2.241	COTP	DT TPDU (U) EOT	farming Alexan				
18 8.103629	192.168.2.241	192.108.2.1	COTP	DT TPDU (0) [COTP	tragment, u bytesj				
19 8.154595	102.108.2.241	102.168.2.1	COTP	DT TPDU (0) EOT					
20 8.157500	102.108.2.1	102 168 2 1	COTP	DT TPDU (0) ECT	fragmont 0 bitos]				
21 8.137700	192.108.2.241	192.108.2.1	TCP	Joost N Jso-tsap	PST ACKI Sec-01 Ack-82 W	n-0 Lan-0			
22 8.158040	192.168 2 241	192.168.2.1	TCP	$4167 \times iso tsan [9]$	XN] Sed-0 Win-65535 Len-0	MSS-1460 WS-0			
23 8.104784	192.100.2.241	192.108.2.1	TCP	iso_tsan \ /167 [9	STNJ SEG-0 WHI-05555 LEH-0	1096 Len-0 MSS-1460			
24 0.100004	1)2.100.2.1	172.100.2.241			STALL ACK DEG-0 ACK-I WIII-	4050 ECHI-0 MBB-1400			
Ethernet II, Sr	C: STEMENSN_11.00.00 (00.IC.00.II.00.00),	DSU: 70:71:0	(102 100 2 241)	(C.40.2a.C6)				
incernet Protoc	UI, SEC: 192.108.2.1 (.	192.108.2.1), DSU: 1	92.108.2.241	(192.108.2.241)					
Transmission Co Transmission Co	ntrol protocol, src Po	rt: 1so-tsap (102),	Dst Port: jo	iost (4166), seq: 1,	ACK: 23, Len: 22				
⊞ TPKT, Version:	3, Length: 22								
⊟ ISO 8073 COTP C	onnection-Oriented Tra	nsport Protocol							
Length: 17									
PDIL Type: CC	Connect Confirm (0x0d)								
Destination r	eference: 0x031c								
Course apfend	ererence. 0x0510								
Source refere	nce: 0x0001								
Class: 0									
Option: O									
Parameter cod	e: 0xc0 (tpdu-size)								
Parameter len	ath: 1								
TEDU size: 10	24								
Depember cod	a: Oxel (end tean)								
Parameter Cou	eth. 2								
Parameter Ten	gun: z								
Source TSAP: 0101									
Parameter code: 0xc2 (dst-tsap)									
Parameter len	gth: 2								
Destination T	SAP: 0101								
				-					
0010 00 3e 61 f3	00 00 1e 06 b4 84 c0	a8 02 01 c0 a8 .>a	a						
0020 02 f1 00 66	10 46 00 03 21 8f f4	31 cd 18 50 18	f.F. !1.	.P.					
0030 10 00 87 16	00 00 03 00 00 16 11	d0 03 1c 00 01	<u></u>						
0040 00 c0 01 0a	c1 02 01 01 c2 02 01	01							

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。)