S7-PN/ModbusTCP 协议转换器

用户手册

版本: V2.01 发布日期: 11/2020 大连德嘉工控设备有限公司

目录

1.	产品概述	. 3
2.	参数设置	. 5
3.	实例演示	10

S7-PN/ModbusTCP 协议转换器

Apply to Honeywell FTE(Fault Tolerant Ethernet), Emerson OHI(Ovation Highway Interface), Network Isloation

1 产品概述

S7-PN/ModbusTCP 协议转换器,它能将西门子 S7-300、S7-1200、S7-1500、S7-200 Smart、 S7-200 CP243 等产品转换成 Modbus TCP 协议(服务端) 为电脑或其它系统提供 Modbus TCP 协议,通过网线读写西门子 PLC 中 DB 块(或是 V 区)数据,以及 Q 区、I 区状态值。

【网络隔离型】: 西门子 PLC 与其它系统(ModbusTCP 侧)分处于两个独立的网络中, 而该 S7-PN/ModbusTCP 转换器跨接这两个网络,是中间的网关,它具有隔离 PLC 与其它网 络的功能,使 PLC 的网络与 ModbusTCP 侧的网络可运行在不同网段中,实现两个网络的彻 底隔离,彼此独立。

PLC 是重要的生产控制设备,它的网络是不能随意与 DCS、MIS、或办公网络等其它 系统网络直接相连的,这就需要该 S7-PN/ModbusTCP 做为网关隔离,将内网与外网实现硬 件分割,同时能够进行数据安全交换,实现网络安全防护,不给工业病毒、互联网远程恶意 攻击留有任何可乘之机。

同时也彻底切断网络攻击病毒在不同网络中的蔓延,另外网关型 S7-PN/ModbusTCP 转换器还具有连接霍尼韦尔的 FTE (Fault Tolerant Ethernet)、艾默生的 OHI(Ovation Highway Interface)的特殊网络功能。



Modbus TCP 功能码与西门子 PLC 数据的对应关系:

01 功能码:读取线圈、05 写单个线圈、15 写多个线圈(0xxxx)

地址 [0,1,2,..10...] 对应西门子 PLC Q 区: [Q0.0, Q0.1, Q0.2, .. Q1.2....] 02 功能码: 读取输入状态(1xxxx) 地址 [0,1,2,..10...] 对应西门子 PLC I 区: [I0.0, I0.1, I0.2, ..I1.2.....]

04 功能码:功能取消

03 功能码:读取保持寄存器、06 写单个寄存器、16 写多个寄存器(4xxx)

地址 [0,1,2,..10...] 对应: DB 块中的 DBW0, DBW2, DBW4, ...DBW20....

或 V 区的 VW0, VW2, VW4, ... VW20...

注:如果对应的数据地址超出 DB 块的实际长度,将会出现全部或部分 DB 块数据不能被读 写,例如:DB1 的长度为 100 字节,用 03 功能码读取,起始地址为 0,长度为 52,这就是要读取 DB1 从 0 开始的 104 个字节,它超过了实际 DB1 块数据长度,就会出现读数 据失败,并不是超出地址的数据读不到,而是整个 DB 块的数据都读不到!切记! 支持最大通讯数据为 1024 个字节。

产品外观: (网络隔离型)



2 参数设置

下边重点介绍网关型 S7-PN/ModbusTCP 转换器:

它有两个网口(LAN1和LAN3)。LAN1用于连接西门子PLC;LAN3用于连接电脑或 DCS、MIS、霍尼韦尔的FTE、艾默生的OHI等具有ModbusTCP协议的其它系统。 请注意这两个网口都要分别设置(出于安全考虑)

一、连接西门子 PLC 侧的网口(LAN1)设置:

1、首先用电脑通过网线连接 LAN1 的网口(或经过交换机与 LAN1 连接),如果不知 道转换器的实际 IP 地址(或忘记了),你可以使用后门 IP 地址(192.168.1.222)来进入转换 器设置页面,但该地址并不是真实地址,只能用来查看或修改实际 IP。

电脑本地网卡的 IP 地址请不要使用自动获取方式,而是将 IPV4 设成固定 IP 地址:如 192.168.1.100,如果是笔记本电脑请将无线网卡禁用(通过软件选择);然后打开电脑中的 微软 IE 浏览器(请不要使用其他公司的浏览器,比如 360、谷歌、搜狗等),在地址栏中直接键入 192.168.1.222(当然也可以使用它实际的 IP 地址,如 192.168.1.10),之后你就进入了 S7-PN/ModbusTCP 转换器(PLC 侧)的设置页面主菜单,如下图:



2、转换器的 IP 地址(PLC 侧)要与西门子 PLC 的 IP 地址处于同一段址中,即 IP 地址的前 3 段完全一样,第 4 段不一样(切记!千万不能一样),用鼠标点击"转换器 IP (PLC 侧)",就进入了下面的 IP 设置页面,只需修改 IP,而 MAC 则无需改变。

	_ 🗆 🗙
🚱 🗢 🖉 http://1. 🌏 💌 🗟 🍫 🗙 🔎 Bing	P -
文件 (E) 编辑 (E) 查看 (Y) 收藏夹 (A) 工具 (E) 帮助 (H)	
😋 收藏夹 🛛 🍰 🤌 诊断调试 🤌 ETH-MPI (smartIE)使用	»
🏉 IP/MAC设置 🔰 🔹 🕤 🔹 🖶 🔹 页面 (2) 🔹	, »
转换器IP (PLC侧)	~
转换器IP: 255 255 255 255 (0255) 转换器MAC: 00 02 99 1B 00 39 不用改变	
提交 取消 大连德嘉工控设备有限公司 Tel:0411-82810696 返回主菜单	
完美 (100)	<u>▼</u> 0% ▼ %0

💽 🗢 🖉 http://192.168.1.222/set_dbnd	o. htm 📀 💌 🚱 🆘 🗙 🔎 Bing	P
🏉 设置	🏠 • 🔂 - 🖃 📾 • 页面 健) • 安全 ଓ) • 工具 @) •	?
PL	.C类型、块号、IP	A
西门子PLC IP地址: 255 255 255	255 (0255)	
PLC类型: 0S7-1200 S7-1500 S7-200 [S7-300\1200\1500] DB块号 ⁶⁵⁵³⁵ (0 smart ◎S7-300 ◎SIEMENS CP243-1-ISO 注: s7-200或smart 对应的是V区,DB块号必须填 '1',切试	31)
大连德嘉工	提交 取消 控设备有限公司 Tel:0411-82810696 2019年09月12日 返回主菜单	
完成		

3、再次回到主菜单,用鼠标点击 "PLC 类型/块号及 IP", 就进入了 DB 块设置页面:

在该设置页面中选择所连的 PLC 的 IP 地址以及 PLC 类型,如果是 S7-300\1200\1500,还要填 写用于通讯的 DB 块号,而 S7-200 或 smart 使用 V 区, DB 块号填'1'

4、 再次回到主菜单, 用鼠标点击"读写 PLC 速度/禁写", 就进入了速度设置页面:

➢速度和写允许 - Tindows Intern	et Explorer					
📀 🗢 🖉 http://192.168.1.22	2/set_spd.htm	🕀 🛨 (🗟 🍫 🗙 🔎	Bing	\$	-
🏉 速度和写允许			💁 • 📾 • 🖃 d	• 页面(2)•	安全(5) • 工具 🔞 •	. »
调整	读写PLC	的速度	及写入允	许/禁止		
转换器对PLC的读写间隔时间:	© 20MS	• 30MS	© 50MS	© 100MS	© 200MS	
写入控制: C 允许Q区、DB区	写入 ◎禁」	LQ区写入但	允许DB区写入	○全面禁止	Q区、DB区写入	
+	、 连德嘉工控记	提交 设备有限公司 2019年09月 返回主菜	取消 引 Tel:0411-82 引2日 译	810696		
,] Internet	100%	-

该页面用于控制读写 PLC 速度(准确说是频率)及写保护,如果通讯数据量小,请选 [100MS];如果不对 PLC 进行写操作,请选 【全面禁止 Q 区、DB 区写入】

5、 如果想查看本产品的通讯状态,请回到主菜单,用鼠标点击"通讯检测故障诊断", 见下图:

②诊断 - Windows Internet Explorer	
🚱 😔 🗢 🙋 http://1. 📀 💌 🔄 🍫 🗶 🔎 Bing	P -
後诊断 日本 (1) → (2)) • *
故障诊断及调试	
本转换器是否与西门子PLC建立连接:NO	
地址类型区域[功能码]问题地址 0XXXX Q 区: [01功能码] No error 1XXXX I 区: [02功能码] No error 4XXXX DB/V: [03功能码] No error	
过10秒再刷新一下,会给你更准确的信息 如果发现之前有不需要或不正确的modbus TCP取数地址出现,请按下键	
清空命令循环池	
返回主菜单	Ŧ
記成 🛛 📄 👘 🤤 Internet 🕅 🔩 🕫 🔍 100%	• //.

二、连接 Modbus TCP 侧(如电脑或 DCS、MIS、霍尼韦尔的 FTE、艾默生的 OHI 等具有 Modbus TCP 协议的其它系统)的网口(LAN3)设置:

首先用电脑通过网线连接 LAN3 的网口(或经过交换机与 LAN3 连接),如果不知道转换器的实际 IP 地址(或忘记了),你可以使用后门 IP 地址(192.168.1.222)来进入转换器设置页面,但该地址并不是真实地址,只能用来查看或修改实际 IP。

电脑本地网卡的 IP 地址请不要使用自动获取方式,而是将 IPV4 设成固定 IP 地址:如 192.168.1.100,如果是笔记本电脑请将无线网卡禁用(通过软件选择);然后打开电脑中的 微软 IE 浏览器(请不要使用其他公司的浏览器,比如 360、谷歌、搜狗等),在地址栏中直接键入 192.168.1.222(当然你也可以使用它实际的 IP 地址,如 192.168.1.10),之后就进入了 S7-PN/ModbusTCP 转换器(ModbusTCP 侧)的设置页面主菜单,如下图:



转换器的 IP 地址(ModbusTCP 侧)要与电脑或 DCS、MIS、霍尼韦尔的 FTE、艾默生的 OHI 等具有 Modbus TCP 协议的设备 IP 地址处于同一段址中,既 IP 地址的前 3 段完全一样,第4段不一样(切记!千万不能一样),用鼠标点击"FTE/OHI/DCS 侧 IP 地址设置",就进入了下面的 IP 设置页面:

SET - Tindows Internet Explorer	
S → Image: Attp://1. Image: Attr: Attp://1. Image: Attr:	P -
🏉 SET 👘 🖓 🔹 📾 🔹 页面 @) 🔹 安全 (S) 🔹 工具 @) 🔹 🧔	∂ •
modbusTCP接口侧	
通讯转换器IP: 255 255 255 255 (0255) 通讯转换器MAC: 00 FF FF FF FF FF (两位十六进制数)不用改变	
提交 取消 大连德嘉 Tel:0411-82810696 Fax:0411-82813210 2019年09月26日	
Version 2.0 返回主菜单	
完成 🛛 📄 👘 🚱 Internet 🖓 🔫 🔩 100	× • //.

3 实例演示

1、首先用电脑通过网线连接 LAN1 的网口(或经过交换机与 LAN1 连接),如果不知 道转换器的实际 IP 地址(或忘记了),你可以使用后门 IP 地址(192.168.1.222)来进入转换 器设置页面,但该地址并不是真实地址,只能用来查看或修改实际 IP。



2、转换器的 IP 地址(PLC 侧)要与西门子 PLC 的 IP 地址处于同一段址中,如: 192.168.1.10,这里使用的是 CPU315-2 PN/DP,其 IP 地址为 192.168.1.30。

後 IP/MAC设置 - Windows Internet Explorer		x
Image: Comparison of the product of the pr	۶	-
🚖 收藏夹 👍 🙋 百度 🙋 京东 🙋 苏宁易购 🖉 淘宝 🥏 天猫		
<i>⊘</i> IP/MAC设置 ¹	工具(0) 🕶 🧕) -
转换器IP(PLC侧)		*
转换器IP:192 168 001 010 (0255)		
转换器MAC: 00 02 99 3B 00 2B 不用改变		
提交取消		
大连德嘉工控设备有限公司		
Tel:0411-82810696		
返回主菜单		
完成	a 100%	-

3、再次回到主菜单,用鼠标点击 "PLC 类型/块号及 IP",就进入了 DB 块设置页面,填入实际 S7-300PLC 的 IP 地址: 192.168.1.30, DB 块号填入 00011,代表 DB11



4、如果想查看本产品的通讯状态,请回到主菜单,用鼠标点击"通讯检测故障诊断"

🍘 诊断 - Windows Internet Explorer	
Image: Second	+ م
🚖 收藏夹 👍 🙋 百度 🙋 京东 🙋 苏宁易购 🙋 淘宝 🙋 天猫	
	▼ @ ▼
故障诊断及调试	ſ.
本转换器是否与西门子PLC建立连接: Yes	, ,
过10秒再刷新一下,会给你更准确的信息	
如果发现之前有不需要或不正确的modbus TCP取数地址出现, 请按下键	
清空命令循环池	
返回主菜单	
See Internet 保护模式: 禁用 《 🖌	r 🔍 100% 🔻

5、连接 Modbus TCP 侧设置,用电脑通过网线连接 LAN3 的网口(或经过交换机与 LAN3 连接),如果不知道转换器的实际 IP 地址(或忘记了),你可以使用后门 IP 地址 (192.168.1.222)来进入转换器设置页面,但该地址并不是真实地址,只能用来查看或修改 实际 IP。



6、转换器的 IP 地址(ModbusTCP 侧)设置,如: 192.168.1.20(当然可以使用其他网段)



7、使用 Modbus Poll 调试软件测试如下,连接时, IP 填: 192.168.1.20,端口号: 502,选择 03 功能码(4xxxx), Modbus 寄存器地址从 0 开始读 10 个,可见通讯成功。

<u></u>	地址 名称	类型	初始值	实际值	注释	(
	0.0 STATO[0]	WORD	¥#16#0	¥#16#007B		To Modbus Poll - Mbpoli1
10	2.0 STAT0[1]	WORD	¥#16#0	¥#16#01C8		File Edit Connection Setup Functions Display View Window Help
	4.0 STAT0[2]	WORD	¥#16#0	V#16#029A		D 🚅 🖬 📇 🗶 🗂 🗏 🖨 🔟 05 06 15 16 17 22 23 TC 🗵 🤶 🛠
10	6.0 STATO[3]	WORD	¥#16#0	V#16#0037		
11	8.0 STAT0[4]	WORD	V#16#0	V#16#007B		Mbpoll1
11	10.0 STAT0[5]	MORD	V#16#0	V#16#0021		Tx = 296: Err = 24: ID = 1: F = 03: SR = 1000ms
	12.0 STATO[6]	WORD	¥#16#0	¥#16#0042		
	14.0 STAT0[7]	WORD	¥#16#0	¥#10#0000		Read/Write Definition
I.	16.0 STATO[8]	WORD	¥#16#0	V#16#0000	-	Allas 00000
I.	18.0 STATO[9]	WORD	¥#16#0	V#16#0000		0 0x007B Slave ID:
1	20.0 STATO[10]	WORD	¥#16#0	V#16#0000	_	1 0x01C8
	22.0 STATO[11]	WORD	¥#16#0	V#16#0000	_	Function Us head holding hegisters (ex)
	24.0 STATO[12]	WORD	¥#16#0	¥#16#0000		Address 0 Protocol address. E.g. 4001
	26.0 STATO [13]	WORD	9#16#0	V#16#0000		3 0x0037
1.	28.0 STAT0[14]	WORD	¥#16#0	¥\$16#0000		4 0x007B Quantity 10
1.	30.0 STAT0[15]	WORD	9#16#0	V#16#0000		- S 0x0021 Scan Rate: 1000 [ms]
-	32.0 STAT0[16]	WORD	V#16#0	V#16#0000	-	Disable
1	34.0 STATO[17]	WORD	V#16#0	V#16#0000	-	6 0X0042 Read/Write Disabled
	36.0 STATO [18]	WORD	V#16#0	V#16#0000		7 0 Disable on error Read/
	38.0 STATO [19]	WORD	¥#16#0	V#16#0000		0 1
	40.0 STAT0[20]	WORD	¥#16#0	¥#16#0000		- O Bows
-	42.0 STATO[21.	WORD	¥#16#0	V#16#0000	_	● 10 ○ 20 ○ 50 ○ 100 ○ Fit to Quantity
1.	44.0 STAT0[22]	WORD	¥#16#0	V#16#0000		
1.	46.0 STATO[23]	MORD	V#16#0	V#16#0000	-	Hide Alias Columns
1.	48.0 STATO [24.	WORD	V#16#0	V#16#0000	_	Address in Cel Enror/Daniel Mod
	50.0 STATO [25]	WORD	¥#16#0	V#16#0000	_	
	52.0 STATO 126.	WOKD	¥#16#0	9#16#0000	_	
	54.0 STATO [27.	WORD .	9#16#0	9216#0000	_	
	56.0 STATO [28]	WORD .	9#16#0	¥#16#0000	_	-
	58.0 STATO [29]	WORD	9#16#0	¥#16#0000	_	
	60.0 STATO [30]	WORD	9#16#0	V#16#0000	_	
	62.0 STAT0[31]	WORD	9#16#0	V#16#0000	-	-
	64.0 STAT0[32]	WORD	9#16#0	V#16#0000		-
	66.0ISTAT0133	INORD	14#16#0	9716#0000		