# 如何使用 S7-1500 冗余 PLC 建立 Modbus TCP 通信

S7-1500 Redundant PLC Modbus TCP getting started

**Getting Started** 

Edition (2020年6月)

**摘 要**本文介绍了 S7-1500 冗余 PLC S7-1500H 的 Modbus TCP 通信的基本组态和编程。 关键词 冗余 PLC, S7-1500R/H, 1513R, 1515R, 1517H, Modbus TCP

Key Words Redundant PLC,S7-1500R/H, 1513R, 1515R, 1517H, Modbus TCP

目 录

如何使用 S7-1500 冗余 PLC 建立 Mod	lbus TCP 通信	
1 S7-1500 R/H 冗余系统		
1.1 网络结构		
1.2 系统 IP 介绍		
1.3 Modbus TCP 通讯编程		5
1.3.1 CPU 做服务器		5
1.3.2 CPU 做客户端		
1.3.3 CPU 切换时的通讯状态		
2 相关手册链接		

#### 1 S7-1500 R/H 冗余系统

#### 1.1 网络结构

以 CPU1517H 为例,网络结构示意如下图所示:



图 1 S7-1500H 网络结构示意图

CPU 1517H 冗余 PLC 有 PROFINET X1 接口和 X2 接口, Modbus TCP 通讯可以将设备 (例如 Standard PLC)通过交换机接入到任何网络接口中。如果接入 X1 接口,需要通过交换机 接入到 MRP 环网中,但是并不需要支持 H-sync 转发。如果接入 X2 接口,只需要使用交换机将 设备(例如 Standard PLC)接入就可以,不需要组成 MRP 环网,同时交换机也不需要选择支持 MRP 和 H-sync 转发。

#### 1.2 系统 IP 介绍

对于 S7-1500R/H 冗余系统除了各 CPU 的设备 IP 地址之外, S7-1500R/H 冗余系统还可以 分配以下系统 IP 地址:

● 两个 CPU 上 PROFINET 接口 X1 的系统 IP 地址

● 两个 CPU 上 PROFINET 接口 X2 的系统 IP 地址

通过系统 IP 地址,可与其它设备(如,HMI 设备、CPU、PG/PC)进行通信。这些设备通常通过系统 IP 地址与冗余系统的主 CPU 进行数据通信。这样,可确保在冗余操作中原来的主 CPU 发生故障后,通信伙伴可在 RUN-Solo 系统状态下与新的主 CPU(之前的备用 CPU)进行

数据通信。每个系统 IP 地址都有一个虚拟 MAC 地址,用户可在 STEP 7 中启用该系统 IP 地址。

与设备 IP 地址相比,系统 IP 地址的优势:

- 通信伙伴专与主 CPU 进行通信。
- 即使主 CPU 故障,仍可通过系统 IP 地址与 S7-1500R/H 冗余系统进行数据通信。

以下介绍 Modbus TCP 通讯的连接的建立与编程。

#### 1.3 Modbus TCP 通讯编程

#### 1.3.1 CPU 做服务器

本节以 CPU 1517H 作为服务器端与 ModScan32 进行 Modbus TCP 通讯

组态步骤如下:

序号	描述	图示
1	项目中添加 CPU1517H	A device name:         R.C.3         Controllers         O U SISHA PROPORCI         O U SISHA PROPORCI



Unrestricted IA&DT Service & Support

Page 6-19

		PROFINET interface_2 [Module]
		General IO tags System constants Texts General Fthermet addresses
		Ethernetaddresses Time synchronization Interface networked with
		Subnet: PN/IE_2
		IP protocol
		IP address: 192 . 168 . 1 11
		Subnet mask: 255 . 255 . 0     Use router
		C Router address: 0 . 0 . 0
		System IP address for switched communication
		IP address: 192.168.1 .10
		Subhet mask: 255 . 255 . 255 . 0 Virtual MAC address: 00-00-5E-00-01- 2
		注意:设置虚拟 MAC 地址时,需确保以太网广播域中存储的所有 MAC 地址
		唯一。特别是在包含由 VRRP 组成的第三方设备以及由多个 STEP 7 项目所
		组态的冗余系统组成的系统中。
4	冗余 PLC	PROFINET interface_1 [Module]
	MRP 设置: 冗	General IO tags System constants Texts
	余 PLC 的	Ethernet addresses Time synchronization
	MRP 默认设置	Advanced options     MRP domain     Interface options
	为:管理员	Media redundancy         Ring port 1:         PROFINET interface_1 [X1]Port_1 [X1 P1 R]
	(自动),不	Port [X1 P1 R]     Ring port 2: PROFINET interface_1 [X1]Port_2 [X1 P2 R]
	雪雨修改	Diagnostics interrupts Domain settings
5	而安修 <u>以</u> 。 打开冗余	Project tree
	PIC 1的	Devices
	Flogiani	S7-1500RH
	DIUCKS 文件 夹、双击 Main	
	九 进行 TCD	Device configuration     Q. Online & diagnostics
	埃,近们 TCF	
	"痈性。 八 」 儿	☑ Online & diagnostics     ■       ▶  Software units     ■
	本 PIC 1 中讲	Program blocks     Add new block
	[·····] / / / / / / / / / / / / / / / / /	Main [OB1]      Technology objects      External course files
		► Decision of the second s
	ショム何住川	
	FLU_2 屮。 	



				SI	EMENS	•
8	建立寄存器区	Data_DB		<i></i>		-
	域的 DB. 分别	Name	Data type	Retain	Accessible f	Writa
		1 🔄 🔻 Static	Array(0, 99) of Int			
	给服务器和客	3 📶 = 🕨 Client_Data	Array[099] of Int	ă		
	户端建立100					
	个字的空间					
9	填写服务器块	▼ Network 1:				
	的其它引脚	Comment				
		1.0	%DB4			
		-MB.	SERVER_DB			
		EN	ENO			
		"Data DB".	DR - false			
		Sever_Data MB_HOLD_RE	G ERROR → false	2		
		"Server_ Connect DB".	STATUS - 16#000	0		
		ConnectCONNECT				
		│ ┃ISCONNECT使用默认的	参数 False。			
		然后编译下载到 PLC。				

设定 ModScan32 步骤

序	描述	图示
号		
1	在 ModScan32 中	■ ModScan32 - [ModSca1] - □ ×
	在 Connection 菜 单中,选择 Connect 设置连接 的参数	File Connection Setup View Window Help - 5 × Connect Disconnect Auto-Start > QuickConnect Length: 100 03: HOLDING REGISTER ▼ ** Device NOT CONNECTED1 **

2	在 Connect 中选	Connection Details X
	择 Remote	Connect 5
	TCP/IP Server,	Remote TCP/IP Server
	IP Address 填写冗	Service 502
	余 PLC 的系统	
	IP:	Word 8 T Delay 5 ms after RTS before
	192,168,0,10,	Parit NONE  Wait for CTS from sla
	Service 中填写冗	Stop 1 Delay 8 ms after last character before
	金 PLC 开放的端	rotocol Selection
	口号: 502. 设置	OK Cancel
	完成后点击OK按	
	钮,此时	
	ModScan32 会去	
	主动连接冗余	
	PIC	
3	此时可以看到连接	■ ModScan32 - [ModSca1]
	计数已经开始计数	File Connection Setup View Window Help
	了,可以判断	
	Modbus TCP 的链	Device Id: 1
	接已经建立。	Address: 0001 MODBUS Point Type Valid Slave Responses: 4
		Length: 100 03: HOLDING REGISTER   Reset Ctrs
		40001:        0>       40026:       >       40051:       >       0>       40076:       >       0>         40002:       >       40027:       >       40052:       >       40076:       >       >         40003:       >       40028:       >       40053:       >       40078:       >       >         40004:       >       40029:       >       40054:       >       40079:       >         40005:       >       40030:       >       40055:       >       40080:       >         40006:       >       40031:       >       40056:       >       40081:       >         40007:       >       40032:       >       40057:       >       40082:       >         40008:       >       40033:       >       40058:       >       40083:       >

同时可以在 TIA Portal 中的网络视图(图 1)中也可看到链接已经建立完成, ID 为 1 的 OUC 连接的状态已经变成绿色了。

				Topology V	view 🔒 Network view	Device view
Network Connect	ions HMI connection			₹ ŧ		
S7-1500R/H-Sys S7-1500R/H-Sta						1
<	PN/IE_1				> 100%	·
<	PN/IE_1	I/O communication	VPN	TeleControl	> 100%	<u></u> ş <u></u> (
M     Network overview	PN/IE_1	I/O communication	VPN	TeleControl	100% Connection type	
M     Network overview     Local connection p     Programmed open	PN/IE_1	I/O communication	VPN Local ID	TeleControl Partner 192.168.0.221	100%      Connection type      Programmed open user co	v
M     Network overview     Local connection n     Programmed open     Programmed open	PN/IE_1	I/O communication	VPN Local ID 1 2	TeleControl           Partner           192.168.0.221           192.168.0.221	I00%      Connection type      Programmed open user co      Programmed open user co	ommunication
	PN/IE_1     Connections     user communication,     user communication,     ce connection_192.16	I/O communication	VPN Local ID 1 2	TeleControl           Partner           192.168.0.221           192.168.0.221           192.168.0.221	Connection type     Programmed open user co     Programmed open user co     Programming device conn	ommunication nection

图 1

下面可以通过 ModScan32 向寄存器中写入数据进行测试,从图 2 中可以看到向 40001 中写入数据 55,然后在 PLC 侧的 DB 块中可以看到第一个数据变成了 55。或者将 PLC 侧 Sever\_Data[9]的数值修改成 105,同时可以看到 ModScan32 这侧的 40010 的数值变成了 105。

	Nan	me		Data type		Monitor value	Retain	essible f Writa Visible in Setpoint Si	upervis Comment	
-	•	Sta	tic							
-		•	Sever_Data	Array[0						
-00			Sever_Data[0]	Int	0	55	Mod	2 - [ModSca1]		— П X
-			Sever_Data[1]	Int	0	0				
-		•	Sever_Data[2]	Int	0	0	E File	ection Setup View Window Help		- 6
-	5		Sever_Data[3]	Int	0	0	0 🛋 🛛	IEI R		
-			Sever_Data[4]	Int	0	0				
-			Sever_Data[5]	Int	0	0	<u> </u>	<u>23</u> <u>26</u> <u>64</u> <u>68</u>		
-			Sever_Data[6]	Int	0	0		Device Id: 1		
			Sever_Data[7]	Int	0	0	Address	001 MODBUS Point Type	Number of Pol	s: 427
-			Sever_Data[8]	Int	0	0			Valid Slave Re	sponses: 427
-			Sever_Data[9]	Int	0	105	Length:	00 03: HOLDING REGISTER	<u> </u>	Reset Ctrs
			Sever_Data[10]	Int	0	0				<u>.</u>
			Sever_Data[11]	Int	0	0				
-			Sever_Data[12]	Int	0	0	40001:	55> 40026: < 0> 40051: <	0> 40076: <	0>
			Sever_Data[13]	Int	0	0	40002	0> 40027. < 0> 40052. < 0> 40053. <	0> 40077: <	0>
-			Sever Data[14]	Int	0	0	40004:	0> 40029: < 0> 40054: <	0> 40079: <	0>
3 -00			Sever Data[15]	Int	0	0	40005:	0> 40030: < 0> 40055: < 0> 40031: < 0> 40056: <	0> 40080: <	0>
-			Sever Data[16]	Int	0	0	40007:	0> 40032: < 0> 40057: <	0> 40082: <	0>
			Sever Data[17]	Int	0	0	40008:	U> 40033: < U> 40058: < 0> 40034: < 0> 40059: <	U> 40083: < 0> 40084 <	U> 0>
-			Sever Data[18]	Int	0	0	40010:	05> 40035: < 0> 40060: <	0> 40085: <	0>
			Sever Data[19]	Int	0	0	40011:	0> 40036: < 0> 40061: < 0> 40037: < 0> 40062: <	0> 40086: <	0>
			Sever Data[20]	Int	0	0	40013:	0> 40038: < 0> 40063: <	0> 40088: <	0>
			Sever Data[21]	Int	0	0	40014:	0> 40039: < 0> 40064: <	0> 40089: <	0>
			Sever_Data[22]	Int	0	0	40016:	0> 40041: < 0> 40066: <	0> 40091: <	0>
			Sever Data[23]	Int	0	0	40017:	0> 40042: < 0> 40067: <	0> 40092: <	0>
-			Sever Data[24]	Int	0	0	40018:	0> 40043: < 0> 40068: < 0> 40044: < 0> 40069: <	0> 40093: <	0>
			Sever Data[25]	Int	0	0	40020:	0> 40045: < 0> 40070: <	0> 40095: <	0>
-			Sever Data[26]	Int	0	0	40021:	0> 40045: < 0> 40071: < 0> 40047: < 0> 40072. <	0> 40096: < 0> 40097: <	0>
			Sever Data[27]	Int	0	0	40023:	0> 40048: < 0> 40073: <	0> 40098: <	0>
			Sever Data[28]	Int	0	0	40024:	U> 40049: < D> 40074: < D> 40050: < D> 40075. <	U> 40099: <	U> 0>
-			Sever Data[29]	Int	0	0	13023.	0/ 10000. ( 0/ 400/0. (	o, 10100. (	
			Sever Data[30]	Int	0	0	For Help,	F1		Polls: 427 Re

图 2



#### 1.3.2 CPU 做客户端

本节以 CPU 1517H 作为客户端与 Modbus TCP Client Tester 软件进行 Modbus TCP 通讯

组态步骤如下:

序号	描述	图示
1	打开右侧指令 中通讯的栏, 在 Others- >Modbus TCP 文件夹中拖出 程序块 MB_CLIENT ,到 Main 程 序。	Network 1:
2	建立 Connect 参数 DB	Client_Connect_DB         Name       Data type       Start value       Comment         1<1       •       × Static       •       •         2<1       •       Connect       TCON_IP_v4       •       •         3<1       •       InterfaceId       HW_NY       257       HW-identifier of IE-interface submodule         4<1       •       ID       CONN_OUC       2       connection reference / identifier         5<1       •       ConnectionType       Byte       16#08       type of connection: 11=TCPIP, 19=UDP (17=TCP         6<1       •       ActiveEstablished       Bool       true       active[Passive connection establishment         7<1       •       × RemoteAddress       IP_V4       remote IP address       IPv4         8<1       •       × ADDR       Array[1.4] of Byte       IPv4 address       IPv4 address         9<1       •       ADDR[2]       Byte       168       IPv4 address       IPv4 address         10<1       •       ADDR[3]       Byte       0       IPv4 address       IE         11<1       •       ADDR[4]       Byte       21       IPv4 address       IE         12<1       •       ADDR[4]
3	建立寄存器区 域的 DB,客户 端建立 100 个 字的空间	Data_DB         Name       Data type        Retain       Accessible f       Writa          1       Image: Static       Image:

Page 12-19



#### 设定 Modbus TCP Client Tester 步骤

序号	描述	图示
1	打开 Modbus	Modbus-TCP Client Tester - X
	TCP Client	
	Tester 软件点	14:49:55:372         Modbus Server started on DESKTOP-65KN66U <192.168.227.1>           14:50:00.900         Connection accepted on socket 964 from 192.168.0.10:50968           14:58:47.375         Socket 964 closed
	击左上角的	14:58:47.390         Modbus Server stopped           14:58:33:488         Modbus Server started on DESKTOP-65KN66U <192.168.227.1>           14:59:02.293         Connection accepted on socket 1384 from 192.168.0.10:56672
	Start Server 激	Client Connections
	活服务器。	Societ     Producess     View     Accepted     requests     Connect     Interme       1>     Image: Second     Time (min.)     (sec.)       2>     Bytes Received:     Avg. Bytes / Sec.:       3>     Image: Second     Avg. Bytes / Sec.:
		View VO Buffers
		Data Areas           Registers         Colis           0         1         2         3         4         5         6         7         8         9
		Edit Values Configure Areas Go to

Page 13-19

2	激活后,如果	Modbus-TCP Client Tester - 🗆 🗙
	PLC 程序已经	
	运行可以看到	Event Log           14:58:53.498         Modbus Server started on DESKTOP-65KN66U <192.168.227.1>           14:59:02.293         Connection accepted on socket 1384 from 192.168.0.10:56672
	客户端列表中	17:37:11.212         Socket 1384 closed           17:37:11.228         Modbus Server stopped           17:39:13.496         Modbus Server started on DESKTOP-65KN66U <192.168.227.1>
	已经显示了连	17:39:17:307 Connection accepted on socket 1096 from 192.168.0.10:50007
	接 IP,同时可	Socket         IP Address         View         Accepted         Rejected         Requests         Connect         Idle Time           1096         192.168.0.10:50007         1>         1         Requests         / Second         Time (min.)         (sec.)
	以看到已经有	8 0 1 0 1 Bytes Received: 1704 Avg. Bytes / Sec.: 213
	请求信号。	3>         74 BB 00 00 00 CF FF 10 00 00 00 64 C8 00 02 00 05 00 C           4>         Bvtes Transmitted:         96         Ava. Bvtes / Sec.:         12
		View VO Buffers 74 BB 00 00 00 06 FF 10 00 00 06 4

通过 TIA Portal 中的网络视图(图 3)中也可看到链接已经建立完成, ID 为 2 的 OUC 连接的状

#### 态已经变成绿色



图 3

通过修改 MB\_CLIENT 的参数可以进行数据的写入操作,图 4 中可以看到对 40001 起始地址 100 个字的数据进行写操作,可以看到 Modbus TCP Client Tester 软件的寄存器的数据发生了变化。



图 4

以上是使用冗余 PLC 进行 Modbus TCP 通讯建立的演示过程,每套冗余系统都可以进行 Modbus TCP 的通讯,同时既可以做服务器也可以做客户端。对于冗余,需要注意的是连接参数的 InterfaceID,这个需要使用系统 IP 的硬件标志符,这样可以保证通讯设备一直连接的是主 PLC。1.3.3 CPU 切换时的通讯状态

在 CPU1517H 做为客户端的时候,进行数据写入的时候,主备 CPU 进行切换时,Modbus TCP 通讯会断开,然后自动连接上,通讯的切换的时间大约为 100ms 左右。



从上图中可以看到在 CPU 切换时通讯块 ERROR 引脚输出为 True (在图中②位置),同时 STATUS 引脚输出错误代码 16#80C5 (在图中①位置),大概在 100ms 后通讯恢复,可以正常 写入数据。

当 CPU1517 备份 CPU 启动进行同步的时候,ModbusTCP 通讯也会断开后再自动连接,这个通讯断开的时间在 130ms 左右。



图 6

从上图中可以看到在 CPU 切换时通讯块 ERROR 引脚输出为 True (在图中2位置),同时 STATUS 引脚输出错误代码 16#80C5 (在图中①位置),大概在 130ms 后通讯恢复,可以正常 写入数据。

以上测试是在 TIA V16 下使用 CPU1517H 其固件为 V2.8 下进行测试,测试结果仅供参考。

## 2 相关手册链接

有关 S7-1500 冗余 PLC 的更多技术信息请参考手册:

- S7-1500R/H 冗余系统 <u>https://support.industry.siemens.com/cs/cn/zh/view/109754833</u>
- CPU1517H 设备手册 <u>https://support.industry.siemens.com/cs/cn/zh/view/109754836</u>
- CPU 1513R-1 PN 设备手册
   <a href="https://support.industry.siemens.com/cs/cn/zh/view/109754834">https://support.industry.siemens.com/cs/cn/zh/view/109754834</a>
- CPU 1515R-2 PN 设备手册
   <a href="https://support.industry.siemens.com/cs/cn/zh/view/109754835">https://support.industry.siemens.com/cs/cn/zh/view/109754835</a>

#### 附录-推荐网址

#### 自动化系统

西门子(中国)有限公司 工业自动化与驱动技术集团 客户服务与支持中心 网站首页:<u>www.4008104288.com.cn</u> 自动化系统 下载中心: <u>http://www.ad.siemens.com.cn/download/DocList.aspx?TypeId=0&CatFirst=1</u> 自动化系统 全球技术资源: <u>http://support.automation.siemens.com/CN/view/zh/10805045/130000</u> "找答案"自动化系统版区:

http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1027

#### 通信/网络

西门子(中国)有限公司

工业自动化与驱动技术集团 客户服务与支持中心

网站首页: <u>www.4008104288.com.cn</u>

通信/网络 下载中心:

http://www.ad.siemens.com.cn/download/DocList.aspx?TypeId=0&CatFirst=12

通信/网络 全球技术资源:

http://support.automation.siemens.com/CN/view/zh/10805868/130000

"找答案" Net 版区:

http://www.ad.siemens.com.cn/service/answer/category.asp?cid=1031

#### 注意事项

应用示例与所示电路、设备及任何可能结果没有必然联系,并不完全相关。应用示例不表示 客户的具体解决方案。它们仅对典型应用提供支持。用户负责确保所述产品的正确使用。这 些应用示例不能免除用户在确保安全、专业使用、安装、操作和维护设备方面的责任。当使 用这些应用示例时,应意识到西门子不对在所述责任条款范围之外的任何损坏/索赔承担责 任。我们保留随时修改这些应用示例的权利,恕不另行通知。如果这些应用示例与其它西门 子出版物(例如,目录)给出的建议不同,则以其它文档的内容为准。

#### 声明

我们已核对过本手册的内容与所描述的硬件和软件相符。由于差错难以完全避免,我们不能 保证完全一致。我们会经常对手册中的数据进行检查,并在后续的版本中进行必要的更正。 欢迎您提出宝贵意见。

#### 版权©西门子(中国)有限公司 2001-2008 版权保留

复制、传播或者使用该文件或文件内容必须经过权利人书面明确同意。侵权者将承担权利人的全部损失。权利人保留一切权利,包括复制、发行,以及改编、汇编的权利。

西门子(中国)有限公司