

应用与工具•10月/2014年

S7-400 PN-H 冗余系统集成 PN 口使用 ModbusTCP PN RED 软件 包的 Modbus TCP 快速入门

PN-H, MODBUS/TC P, MODBUS/TCP PN RED 软件包

http://support.automation.siemens.com/CN/view/zh/81715142

目录

1	Modbus TCP 通讯概述	3
	1.1 通讯所使用的以太网参考模型	3
	1.2 Modbus TCP 数据帧	3
	1.3 Modbus TCP 使用的通讯资源端口号	3
	1.4 Modbus TCP 使用的功能代码	3
	1.5 Modbus TCP 通讯应用举例	4
2	? SIMATIC S7-400H 冗余系统 Modbus/TCP 通讯概述	4
	2.1 S7-400 PN-H 冗余系统 CPU 集成 PN □ Modbus/TCP 通讯机理概述	4
	2.2 软件包" Modbus/TCP PN CPU Redundant V1.0"使用说明 2.2.1 软件包" Modbus/TCP PN CPU Redundant V1.0"软硬件需求 2.2.2 软件包" Modbus/TCP PN CPU Redundant V1.0"软硬件需求	6 6 7
3	; 配置 S7-400 PN-H 冗余系统通过 CPU 集成 PN □作为 Server 进行 Modbus TCP 通讯	8
	3.1 例子中使用的硬件设备及软件	9
	3.2 S7-400 PN-H 冗余系统及 Modscan32 软件组态	10
	3.3 通讯测试	14
4	↓ 配置 S7-400 PN-H 冗余系统通过 CPU 集成 PN 口作为 Client 进行 Modbus TCP 通讯	23
	4.1 例子中使用的硬件设备及软件	23
	4.2 S7-400 PN-H 冗余系统及 Modbus slave 软件组态	24
	4.3 通讯测试	28
5	,软件包" Modbus/TCP PN CPU Redundant V1.0"授权	35
	5.1 读取 IDENT_CODE	35
	5.2 通过拨打西门子授权服务中心申请注册码 REG_KEY	36
	5.3 通过网站申请注册码 REG_KEY	37
	5.4 使用注册码 REG_KEY	40

1 Modbus TCP 通讯概述

MODBUS/TCP 是简单的、中立厂商的用于管理和控制自动化设备的 MODBUS 系列通讯 协议的派生产品,显而易见,它覆盖了使用 TCP/IP 协议的"Intranet"和"Internet"环境中 MODBUS 报文的用途。协议的最通用用途是为诸如 PLC's, I/O 模块,以及连接其它简单域 总线或 I/O 模块的网关服务的。

1.1 通讯所使用的以太网参考模型

Modbus TCP 传输过程中使用了 TCP/IP 以太网参考模型的 5 层: 第一层:物理层,提供设备物理接口,与市售介质/网络适配器相兼容 第二层:数据链路层,格式化信号到源/目硬件址数据帧 第三层:网络层,实现带有 32 位 IP 址 IP 报文包 第四层:传输层,实现可靠性连接、传输、查错、重发、端口服务、传输调度 第五层:应用层,Modbus 协议报文

1.2 Modbus TCP 数据帧

Modbus 数据在 TCP/IP 以太网上传输,支持 Ethernet II 和 802.3 两种帧格式,Modbus TCP 数据帧包含报文头、功能代码和数据 3 部分,MBAP 报文头(MBAP、Modbus Application Protocol、Modbus 应用协议)分 4 个域,共7 个字节。

1.3 Modbus TCP 使用的通讯资源端口号

在 Moodbus 服务器中按缺省协议使用 Port 502 通信端口,在 Modus 客户器程序中设置任意 通信端口,为避免与其他通讯协议的冲突一般建议 2000 开始可以使用。

1.4 Modbus TCP 使用的功能代码

按照使用的通途区分,共有3种类型分别为:

1) 公共功能代码: 已定义好功能码,保证其唯一性,由 Modbus.org 认可;

2) 用户自定义功能代码有两组,分别为65~72和100~110,无需认可,但不保证代码使用唯一性,如变为公共代码,需交 RFC 认可;

3) 保留功能代码,由某些公司使用某些传统设备代码,不可作为公共用途。 按照应用深浅,可分为**3**个类别:

1) 类别 0, 客户机/服务器最小可用子集: 读多个保持寄存器(fc.3); 写多个保持寄存器 (fc.16);

2) 类别 1,可实现基本互易操作常用代码:读线圈(fc.1);读开关量输入(fc.2);读输入寄存器(fc.4);写线圈(fc.5);写单一寄存器(fc.6);

3) 类别 2,用于人机界面、监控系统例行操作和数据传送功能:强制多个线圈(fc.15);读通用寄存器(fc.20);写通用寄存器(fc.21);屏蔽写寄存器(fc.22);读写寄存器(fc.23)。

1.5 Modbus TCP 通讯应用举例

在读寄存器的过程中,以 Modbus TCP 请求报文为例,具体的数据传输过程如下:

1) Modbus TCP 客户端实况,用 Connect()命令建立目标设备 TCP 502 端口连接数据通信 过程;

2) 准备 Modbus 报文,包括 7 个字节 MBAP 内请求;

3) 使用 send()命令发送;

4) 同一连接等待应答;

5) 同 recv()读报文,完成一次数据交换过程;

6) 当通信任务结束时,关闭 TCP 连接,使服务器可以为其他服务。

2 SIMATIC S7-400H 冗余系统 Modbus/TCP 通讯概述

2.1 S7-400 PN-H 冗余系统 CPU 集成 PN 口 Modbus/TCP 通讯机理概述

S7-400 PN-H 冗余系统控制器是西门子推出的基于 Profinet 系统冗余的解决方案,其中 每个 CPU 上集成了两个 Profinet 接口,如下图 1 所示:



Picture 1: 集成 PN 接口的 S7-400 PN-H 冗余系统

2013 年 11 月西门子推出了基于 S7-400PN-H 冗余系统 CPU 集成 PROFINET 接口的 Modbus/TCP 冗余通信软件包" Modbus/TCP PN CPU Redundant V1.0",其通信网络架构 和程序块版本如下图 2、3 所示:



Picture 2: S7-400 PN-H 冗余系统 CPU 集成 PN 口的 Modbus/TCP 网络架构

5

Product	Identification number	From version
Modbus/TCP PN CPU redundant	6AV6676-6MB10-0AX0	1.0
FB 913 "TCP_COMM"		3.2
FB 914 "MOD_CLI"		1.6
FB 915 "MB_PNHCL"		1.0
FB 916 "MOD_SERV"		1.5
FB 917 "MB_PNHSV"		1.0

Picture 3:软件包" Modbus/TCP PN CPU Redundant V1.0"程序版本

软件包" Modbus/TCP PN CPU Redundant V1.0"的通信机理及特点如下:

- 如果 S7-400 PN-H CPU 做 Modbus/TCP Server,该解决方案能够允许通信伙伴通过 任意一个机架 CPU 的 PN 口通信链路(图 2 中单边的链路为 0A、1A;双边链路为 0A、 1A/0B、1B)建立通信及数据的一致性,链路的选择完全由客户端自行根据链路的通信 状况决定,当任一链路中断、PN-H CPU 冗余模式的切换均不会对通信造成任何影响
- 2)如果 S7-400 PN-H CPU 做 Modbus/TCP client,解决方案能够保证通过任意一个机架 CPU 的 PN 口通信链路(图 2 中单边的链路为 0A、1A;双边链路为 0A、1A/0B、1B)与 通信伙伴建立通信及数据的一致性,当任一链路中断、PN-H CPU 冗余模式的切换均不 会对通信造成任何影响
- 3) 解决方案中提供了完整的 TCP 层及 Modbus 应用层的诊断

2.2 软件包" Modbus/TCP PN CPU Redundant V1.0" 使用说明

2.2.1 软件包" Modbus/TCP PN CPU Redundant V1.0" 软硬件需求

该软件包需要的软件需求如下图 4、5 所示:

400 PN-H-CPU (only Modbus/TCP PN and Modbus/TCP PN Red)

6ES7 412-5HK06-0AB0	V6.0.1
6ES7 414-5HM06-0AB0	V6.0.1
6ES7 416-5HS06-0AB0	V6.0.1
6ES7 417-5HT06-0AB0	V6.0.1
6ES7 410-5HX08-0AB0	V8.0

Picture 4: 软件包" Modbus/TCP PN CPU Redundant V1.0"所需要的硬件需求

Software requirements

· SIMATIC STEP 7 version 5.5 SP2 HF1 or higher for the PN Red PLC version of the MODBUS blocks

Picture 5: 软件包" Modbus/TCP PN CPU Redundant V1.0" 所需要的软件需求

2.2.2 软件包" Modbus/TCP PN CPU Redundant V1.0" 软硬件需求

当将软件选项包安装完集成到 Step7 时可以在 Step7 安装文件的相应目录中找到块库、例 程、英文手册,如下图 6-8 所示,在实际的项目调试过程中由于例子程序的各项功能比较完 善,因此可以直接使用例子程序根据项目的实际情况修改相应的参数即可,可以节省大量的 参数设置时间。

- The libraries under \Program Files\Siemens\Step7\S7libs,
- The example projects under \Program Files\Siemens\Step7\Examples,
- The manual under \Program Files\Siemens\Step7\S7manual\S7Comm.
- The software registration form under \Program Files\Siemens\Step7\S7libs\ Modbus_PN_CPU_Red.

Picture 6: 块库、例程、英文手册和软件注册的文件夹位置

Jserprojects Libraries Sample pro	ijects Multiprojects	
	Language Engl	ish 💌
Name	Storage path	
MB_TCP_PN_RED_400	C:\Program Files\Siemens\Step7\EXAMPLES\MB_TCP_PN_RED_400 C:\Program Files\Siemens\Step7\Examples\MB_TCP_PN_RED_CFC)
	C:\Program Files\Siemens\Step7\Examples\exie	
ZEn01_01_STEP7STL_1-9	C:\Program Files\Siemens\Step7\Examples\zen01_01	
ZEn01_02_STEP7STL_1-10	C:\Program Files\Siemens\Step7\Examples\zen01_02 C:\Program Files\Siemens\Step7\Examples\zen01_03	
ZEn01_04_STEP7FBD_1-10	C:\Program Files\Siemens\Step7\Examples\zen01_04	-
Selected		
er projects: raries:		
mple projects:		<u>_</u>
Itiprojects:	<u></u>	Browse
OK	Cancel	Help

Picture 7: 例程(注: 当找不到例程时可以通过"Browse.."按钮来进行查找)

Name	Storage path			
SRAPH7	C:\Program Files\Siemens\Step7\S7libs\graphlib	L		
📚 Modbus PN CPU Red	C:\Program Files\Siemens\Step7\S7LIBS\Modbus_PN_CPU_Red	L		
📚 PNIODiag	C:\Program Files\Siemens\Step7\S7libs\PNI0Diag	L		
📚 Redundant IO CGP V40	C:\Program Files\Siemens\Step7\S7libs\red_io_1	L		
📚 Redundant IO CGP V52	C:\Program Files\Siemens\Step7\S7libs\red_io52	L		
📚 Redundant IO MGP V32	C:\Program Files\Siemens\Step7\S7libs\red_io_0 C:\Program Files\Siemens\Step7\S7libs\simation			
SIMATIC_NET_CP				
Standard Library	C:\Program Files\Siemens\Step7\S7libs\stdlib30	1		
Selected				
ser projects:				
braries:				
ample projects:				
ultiprojects:	Browse			

Picture 8: 功能块库(注: 当找不到块库时可以通过"Browse.."按钮来进行查找)

3 配置 S7-400 PN-H 冗余系统通过 CPU 集成 PN 口作为 Server 进行 Modbus TCP 通讯

下面以 S7-400 PN-H 冗余系统及 Modscan32 软件为例,详细介绍如何将 S7-400 PN-H 冗余系统通过 CPU 集成 PN 口配置为 Server, Modscan32 为 Client 进行 Modbus TCP 通讯,下图 9 为服务器功能块库的程序结构及各功能块完成的功能:



Picture 9:软件包"Modbus/TCP PN CPU Redundant V1.0"服务器程序架构 注:Modscan32软件可以从网上免费下载得到,本例中使用的版本为 V7.0版,由于各 版本的功能不尽相同,因此需要注意版本问题。

3.1 例子中使用的硬件设备及软件

本例中所用的硬件设备如下表:

名称	数量	订货号

S7-400 电源模块 PS 407 10A	2	6ES7407-0KA02-0AA0
S7-400 CPU412-5H PN/DP	2	6ES7412-5HK06-0AB0(V6.0)
S7-400 机架	1	6ES7400-2JA00-0AA0
网线	若干	
笔记本电脑	1	

Table 1:服务器硬件清单

所用到软件如下表:

名称	订货号
STEP7 V5.5 SP3 组态编程软件 英文版	
" Modbus/TCP PN CPU Redundant V1.0" 软件选项包	6AV6676-6MB10-0AX0
Modscan32 V7.0	

Table 2:服务器软件清单

3.2 S7-400 PN-H 冗余系统及 Modscan32 软件组态

打开 STEP7 软件,新建一个项目文件,插入一个"SIMATIC H 站",在硬件组态中分 别插入 PS407 电源,CPU412-5H PN/DP 等并设置 Rack 0、1 CPU 的集成 PN 接口的 IP 地 址,如下图 10 所示:

Station Edit Insert PLC View Options V	indow Help			
D 😅 🐎 🖩 🕵 🎒 🖨 🖪 🛍 🏜	🗈 🖿 🐮 K?			
	074A Properties - Etherne 1412-5 H PN/DP Media Redun Seneral	tRack0 (R0/52.5) dancy Time-of-Day Synchronization 0 Addresses PD0EINET Synchronization	Iptions Ein	d.
X7 000 X7 000 IF1 HS IF2 HS X5 000 X5 0000 X5 000 X5 00	DP Content mc module Short description: mcmdule Device name: 7 V	PN-IO PN-IO Ethemotifiest0 replacement without exchangeable medium		Isindard Image: PROFIBUS PA PROFIBUS PA Image: Property Part of the Property Part of th
IDR/2014 1 PS 2 DP X2 DP X1 MR IF1 HS IF2 HS X6 EH X5 P1 R Pace X5 P2 R IFac 4 5	07 4A Interface 1412-5 H PN/DP(1) Device number: 0/P Device number: 0/B Networked: 0/P Device number: 0/B Device number: <td>Ethernet 0 192.158.2.10 Yes Properties</td> <td>X</td> <td></td>	Ethernet 0 192.158.2.10 Yes Properties	X	
	DK	Cancel	Help	CPU 4122PN CPU 4131 CPU 4132DP CPU 4132DP CPU 4142DP CPU 4142DP CPU 4142DP
Slot Module Order number 1 PS 407 4A 6ES7 407-002 2 CPU 412-5 H PN/DP 6ES7 412-50	Firmware M I Q Com 02-0AA0 V6.0 2	ment		CPU 414-3 PN/DP CPU 414-3 PN/DP CPU 414-5 PN/DP CPU 416-1 CPU 416-2 DP CPU 416-3 DP
X2 DP X1 MPI/DP	8191 2 8130			CPU 416-3 PN/DP DPU 416F-2

Picture 10: 硬件组态

硬件组态完成后,编译保存,并将例程站点"H Single-sided (Server)"中的程序 (System data 不需要拷贝)拷贝到该项目中。

由于需要在 SIMATIC 站与其他通讯伙伴之间建立 TCP 连接用于 Modbus 通讯,而对于 CPU 的集成 PN 口来说须通过 Open IE(开放式以太网通讯)的方式来建立 TCP 连接,通过 S7-CPU 的 PROFINET 接口 进行 Modbus TCP 通信时,需要使用通信块 FB65 "TCON"、 FB66 "TDISCON"、FB63 "TSEND" 和 FB64 "TRCV",要进行 Modbus TCP 通信,必须在 数据块中为 Rack0 及 Rack1 冗余 CPU 指定相应的参数,相应得参数在程序中主要由 DB2 " MODBUS_HPARAM_PN_2" 来完成初始化(注意:参数设置必须在"Data View"视图下 的"Actual value" 列中设置),其中各参数的含义如下图 11、12 所示:

Address	Name	Туре	Initial value	Connent					
0.0		STRUCT							
+0.0	double_sided_red	BOOL	FALSE						
+2.0	connection_OA	STRUCT			+66.0	connection_1A	STRUCT		
+0.0	block_length	WORD	W#16#40	#!Verbindung_0001!#	+0.0	block_length	WORD	W#16#40	#!Verbindung_0002!#
+2.0	id	WORD	W#16#1		+2.0	id	WORD	W#16#2	
+4.0	connection_type	BYTE	B#16#11		+4.0	connection_type	BYTE	B#16#11	
+5.0	active_est	BOOL	FALSE		+5.0	active_est	BOOL	FALSE	
+6.0	local_device_id	BYTE	B#16#5		+6.0	local_device_id	BYTE	B#16#15	
+7.0	local_tsap_id_len	BYTE	B#16#2		+7.0	local_tsap_id_len	BYTE	B#16#2	
+8.0	rem_subnet_id_len	BYTE	B#16#0		+8.0	rem_subnet_id_len	BYTE	B#16#0	
+9.0	rem_staddr_len	BYTE	B#16#0		+9.0	rem_staddr_len	BYTE	B#16#0	
+10.0	rem_tsap_id_len	BYTE	B#16#0		+10.0	rem_tsap_id_len	BYTE	B#16#0	
+11.0	next_staddr_len	BYTE	B#16#0		+11.0	next_staddr_len	BYTE	B#16#0	
+12.0	local_tsap_id	ARRAY[116]	B#16#1, B#16#F6		+12.0	local_tsap_id	ARRAY[116]	B#16#1, B#16#F6	
*1.0		BYTE			*1.0		BYTE		
+28.0	rem_subnet_id	ARRAY[16]	B#16#0, B#16#0, 3		+28.0	rem_subnet_id	ARRAY[16]	B#16#0, B#16#0, 3	
*1.0		BYTE			*1.0		BYTE		
+34.0	rem_staddr	ARRAY[16]	B#16#0, B#16#0, 3		+34.0	rem_staddr	ARRAY[16]	B#16#0, B#16#0, 3	
*1.0		BYTE			*1.0		BYTE		
+40.0	rem_tsap_id	ARRAY[116]	B#16#0, B#16#0, 3		+40.0	rem_tsap_id	ARRAY[116]	B#16#0, B#16#0, 3	
*1.0		BYTE			*1.0		BYTE		
+56.0	next_staddr	ARRAY[16]	B#16#0, B#16#0, 3		+56.0	next_staddr	ARRAY[16]	B#16#0, B#16#0, 3	
*1.0		BYTE			*1.0		BYTE		
+62.0	spare	WORD	W#16#0	#!Verbindung_0001!#	+62.0	spare	WORD	W#16#0	#!Verbindung_0002!#
=64.0		END_STRUCT			=64.0		END_STRUCT		

Copyright © Siemens AG Copyright year All rights reserved

Rack0 CPU集成PN的OPEN IE TCP连接参数

Rack1 CPU集成PN的OPEN IE TCP连接参数

Picture11: DB2 " MODBUS_HPARAM_PN_2" 的 TCP 连接参数设置部分

关于 DB2 " MODBUS_HPARAM_PN_2" 的 Rack0 及 Rack1 冗余 CPU TCP 连接参数含义 如下表 3 所示:

类型	参数	含义
	double_sided_red	通信伙伴是否为冗余系统,1=冗余,0=单站
	block_length	固定值W#16#40
OPEN IE	ld	连接ID,用于FB63/64/65/66,Rack0和Rack1CPU必须唯一
	connection_type	取决于CPU类型,用于FB65(TCON)

	TCP(兼容模式): CPU315、317<= FWV2.3			
	W#16#01;			
	TCP:CPU315,317>= FW V2.4、IM151-8PN/DP CPU、			
	CPU314C、CPU319、CPU412、CPU414与CPU416			
	W#16#11			
	主动或被动连接:			
active_est	S7作Client时为主动 TRUE			
	S7作Server时为被动 FALSE			
	取决于CPU类型:			
	IM151-8PN/DP B#16#1			
local device id	CPU314C、315、317 B#16#2			
	CPU319 B#16#3			
	CPU412(H)、414(H)、416(H) B#16#5			
	Rack1中的CPU B#16#15			
	local_device_id的长度:			
local_tsap_id_len	主动连接时 W#16#0			
	被动连接时 W#16#2			
rem_subnet_id_len	未使用			
	参数rem_staddr的长度:			
rem_staddr_len	未具体定义连接 B#16#0			
	有具体连接 B#16#4			
	rem_tsap_id的长度:			
rem_tsap_id_len	主动连接时 W#16#2			
	被动连接时 W#16#0			
	通讯接口类型选择:			
next_staddr_len	通过外部CP模块: 非0的其它值			
	通过CPU的集成PN 口: W#16#0			
	本地连接TSAP号,与参数connection_type有关:			
	1)connection_type= B#16#01时			
local tsan id	local_tsap_id[1] 本地连接端口号的低字节[16进制]			
	local_tsap_id[2] 本地连接端口号的高字节[16进制]			
	local_tsap_id[3-16] B#16#00			
	2)connection_type= B#16#11时			

	local_tsap_id[1] 本地连接端口号的高字节[16进制]
	local_tsap_id[2] 本地连接端口号的低字节[16进制]
	local_tsap_id[3-16] B#16#00
rem_subnet_id	未使用
	通信伙伴的IP地址,与参数connection_type有关,以
	192.168.0.1为例:
	1)connection_type= B#16#01时
	rem_staddr[1]= B#16#01(1),
	rem_staddr[2]= B#16#00(0)
	rem_staddr[3]= B#16#A8(168)
rom staddr	rem_staddr[4]= B#16#C0(192)
rem_staddi	rem_staddr[5-6]=B#16#00(为IPV6预留)
	2)connection_type= B#16#11时
	rem_staddr[1]= B#16#C0(192)
	rem_staddr[2]= B#16#A8(168)
	rem_staddr[3]= B#16#00(0)
	rem_staddr[4]= B#16#01(1)
	rem_staddr[5-6]=B#16#00(为IPV6预留)
	远程连接TSAP号,与参数connection_type有关:
	1)connection_type= B#16#01时
	local_tsap_id[1] 本地连接端口号的低字节[16进制]
	local_tsap_id[2] 本地连接端口号的高字节[16进制]
rem_tsap_id	local_tsap_id[3-16] B#16#00
	2)connection_type= B#16#11时
	local_tsap_id[1] 本地连接端口号的高字节[16进制]
	local_tsap_id[2] 本地连接端口号的低字节[16进制]
	local_tsap_id[3-16] B#16#00
next_staddr	CP的机架号和槽号,当使用CPU的PN口时为 B#16#00
L	

Table 3: DB2 " MODBUS_HPARAM_PN_2" 的 TCP 连接参数含义

					- 客户端	/服备器选择		
+130.0	server_client	BOOL	TRUE					
+130.1	single_write	BOOL	FALSE		- 与功能	码相关,单写模式	4	
+130.2	connect_at_startup	BOOL	FALSE					
+131.0	reserved	BYTE	B#16#0		744			
+132.0	data_type_1	BYTE	B#16#3	.	建立过	E按楔式(ENQ_E	NR/PLC 尼	日初后)选择
+134.0	db_1	WORD	₩#16#B					
+136.0	start_1	WORD	¥#16#0					
+138.0	end_1	WORD	W#16#1F3					
+140.0	data_type_2	BYTE	B#16#3					
+142.0	db_2	WORD	W#16#C					
+144.0	start_2	WORD	W#16#2D0		可定 ♥8个	数据区, 支持功	能码1 2	3 4 5 6
+146.0	end_2	WORD	¥#16#384					
+148.0	data_type_3	BYTE	B#16#4		15、16			
+150.0	db_3	WORD	W#16#D					
+152.0	start_3	WORD	W#16#2D0		IN:含义如	如下		
+154.0	end_3	WORD	W#16#3E8				u skr. um st	6 mil
+156.0	data_type_4	BYTE	B#16#0		<u>Data type</u>	X:加定 X FKT MOD	bus av ne z	至型
+158.0	db_4	WORD	¥#16#0		Identifier	Data type	Size	
+160.0	start_4	WORD	W#16#0		0	Area not used		•
+162.0	end_4	WORD	W#16#0		0	Area not used		
+164.0	data_type_5	BYTE	B#16#1	<u> </u>	1	Coils	Bit	
+166.0	db_5	WORD	₩#16#E		2	Inpute	Dit.	•
+168.0	start_5	WORD	¥#16#280		2	inputs	ы	
+170.0	end_5	WORD	₩#16#4E2		3	Holding Register	Word	
+172.0	data_type_6	BYTE	B#16#2		4	Input Pogiator	Word	•
+174.0	db_6	WORD	¥#16#F		4	Input Register	word	
+176.0	start_6	WORD	W#16#6A4					
+178.0	end_6	WORD	W#16#8FC					
+180.0	data_type_7	BYTE	B#16#1		db v· 粉垢	地中		
+182.0	db_7	WORD	¥#16#10			「大う		
+184.0	start_7	WORD	W#16#6A4		start x [.] m	odbus寄存器或H	特值起始	洲北 对应DB从0字
+186.0	end_7	WORD	W#16#8FC					
+188.0	data_type_8	BYTE	B#16#0		节廾始			
+190.0	db_8	WORD	¥#16#0			dbuc安方思武山	快估法市	
+192.0	start_8	WORD	W#16#0		End_X. Ind	JUDUS可什品以L	、可但知不	मलमा
+194.0	end_8	WORD	W#16#0					
+196.0	conn_OA_send_buffer	ARRAY [1	260 (B#16#0)		消息内剖	3存储区		
*1.0		BYTE			- 1 - الماد - 1 ال مخط			
+456.0	conn_OA_recv_buffer	ARRAY [1	260 (B#16#0)		一按収致視	行储区		

Picture 12: DB2 " MODBUS_HPARAM_PN_2" 的 Modbus 参数设置部分

3.3 通讯测试

由于" Modbus/TCP PN CPU Redundant V1.0"选项包支持功能码FC1, 2, 3, 4, 5, 6, 15, 16, 不同的功能码测试过程中类似,因此下面以FC03(读写保持寄存器)为例来说明 通讯测试的整个过程,对于其他功能码的测试将不再重复描述,对于Modbus的数据类型可 参考下表4:

基本表	对象类型	访问类型	注释
离散量输入	单个位	只读	1/0系统可提供这种类型数据
线圈	单个位	读写	通过应用程序可改变这种类型数据
输入寄存器	16位字	只读	1/0系统可提供这种类型数据
保持寄存器	16位字	读写	通过应用程序可改变这种类型数据

Table 4: Modbus 数据类型

在测试过程中我们将重点关注通讯连接的建立和当一个链路中断时自动切换到另一个链 路的过程。

由于服务器主功能块 FB917" MB_PNHSV"的参数需要初始化,因此分别在 OB100 及 OB1 中调用 FB917,在 OB100 中调用 FB917 完成相关参数的初始化,FB917 的管脚分布 如下图 13 所示:

🗆 🛛 et	work 3: cycl	ic call of FB MB_PNHSV - S7 is	server
	CALL MB PNE	HSV″. ″IDB MODBUS″	FB917 / DB917
	∕id O a	:= "CONTROL DAT".id 0 a	DB1.DBWO
	id_1_a	:="CONTROL_DAT".id_1_a	DB1.DBW2
	id_0_b	:=	
	id_1_b	:=	
	db_param	:="MODBUS_HPARAM_PN_2"	DB2
IN 🔨	RECV_TIMEOU	<pre>F:= CONTROL_DAT . RECV_TIMEOUT</pre>	DB1.DBD4
	CONN_TIMEOU	I:="CONTROL_DAT".CONN_TIMEOUT	DB1.DBD8
	DISCONNECT	:="CONTROL_DAT".DISCONNECT	DB1.DBX12.0
	REG_KEY_DB	:="License DB"	DB3
	Init	:="CONTROL_DAT".Init	DB1.DBX12.1
	ENR	:="CONTROL_DAT".ENR	DB1.DBX12.2
	LICENSED	:="CONTROL_DAT".LICENSED	DB1.DBX20.0
	BUSY	:="CONTROL_DAT".BUSY	DB1.DBX20.1
	ESTAB_OA	:="CONTROL_DAT".ESTAB_OA	DB1.DBX20.2
	NDR_OA	:="CONTROL_DAT".NDR_OA	DB1.DBX20.3
	ERROR_OA	:="CONTROL_DAT".ERROR_OA	DB1.DBX20.4
	STATUS_OA	:="CONTROL_DAT".STATUS_OA	DB1.DBW22
	ESTAB_1A	:="CONTROL_DAT".ESTAB_1A	DB1.DBX24.0
	NDR_1A	:= "CONTROL_DAT".NDR_1A	DB1.DBX24.1
	ERROR_1A	:= "CONTROL_DAT". ERROR_1A	DB1.DBX24.2
	STATUS_1A	:="CONTROL_DAT".STATUS_1A	DB1.DBW26
	ESTAB_OB	:=	
	NDR_OB	:=	
OUT 🄇	ERROR_OB	:=	
	STATUS_OB	:=	
	ESTAB_1B	:=	
	NDR_1B	:=	
	ERROR_1B	:=	
	STATUS_1B	:=	
	IDENT_CODE		
	RedErrSY	:= CONTROL_DAT .RedErrSY	DB1.DBX28.0
	KedErrDev	= CONTROL_DAT .RedErrDev	DB1.DBX28.1
	lotComErr Tudt D	= CONIROL_DAT . TotComErr	DB1.DBX28.2
	Init_Error	= CONIROL_DAI .Init_Error	DB1.DBX28.3
	Init_Status	:= CONTROL_DAT .Init_Status	DB1.DB#30

Picture 13: 功能块 FB917" MB_PNHSV" 管脚分布

FB917"	MB	PNHSV"	的各参数含义如	下表 5:
--------	----	--------	---------	-------

类型	参数	格式		含义	初始
					化
IN	id 0 a	WORD	假定两个 Rack	CPU0 与 UP0 的连接	是
	IU_U_A		CPU 简称为	ID	
	id 1 a	WORD	CPU0、	CPU1 与 UP0 的连接	是
	IU_1_a		CPU1(下同),	ID	
	id 0 b	WORD	如通讯伙伴也	CPU0 与 UP1 的连接	是
	IQ_0_0			ID	

Copyright © Siemens AG Copyright year All rights reserved

			$\lambda \mapsto \lambda / \lambda \times k + k$		
		WORD	为冗余的话简	CPU1 与 UP1 的连接	是
	id_1_b		称为 UP0、	ID	
			UP1		
	dh naram	BLOCK	会粉化 DB 由		是
	ub_param	_DB	多 级化 DD 八		
	RECV_TIME	TIME	监视应用层接收数据的超时时间,最少		否
	OUT		20ms		
	CONN_TIME	TIME	TCP 连接建立超时	时监控时间,最短	否
	OUT		100ms		
	DISCONNEC	BOOL	在 ENR=FALSE '	情况下为 TRUE 时断开	否
	Т		远程伙伴的连接		
	REG_KEY_D	BLOCK	授权 DB 块		否
	В	_DB			
	Init	BOOL	手动初始化		否
	ENR	BOOL	接收使能		否
OUT	LICENSED	BOOL	功能块是否授权		否
	BUSY	BOOL	作业正在处理		否
	NDR_0A	BOOL	CPU0 与 UP0 的	的连接请求成功响应和处	否
			理		
	ERROR_0A	BOOL	CPU0与UP0的	连接错误	否
	STATUS_0A	WORD	CPU0与UP0的	连接状态	否
	NDR_1A	BOOL	CPU1 与 UP0 的	的连接请求成功响应和处	否
			理		
	ERROR_1A	BOOL	CPU1与UP0的	连接错误	否
	STATUS_1A	WORD	CPU1与UP0的	连接状态	否
	NDR_0B	BOOL	CPU0 与 UP1 的	的连接请求成功响应和处	否
			理		
	ERROR_0B	BOOL	CPU0与UP1的	连接错误	否
	STATUS_0B	WORD	CPU0与UP1的	连接状态	否
	NDR_1B	BOOL	CPU1 与 UP1 的	的连接请求成功响应和处	否
			理		
	ERROR_1B	BOOL	CPU1与UP1的	连接错误	否
	STATUS_1B	WORD	CPU1与UP1的	连接状态	否
	-				

Copyright © Siemens AG Copyright year All rights reserved

IDENT_	STRIN	预授权解码输出,将此码连同软件序列	否
CODE	G	号发给西门子 IT 部门后可得到授权	
	[18]		
RedErrS7	BOOL	S7 冗余丢失	否
RedErrDev	BOOL	通信伙伴冗余丢失	否
TotComErr	BOOL	通信完全丢失	否
Init_Error	BOOL	初始化错误	否
Init_Status	WORD	初始化状态	否

Table 5: FB917" MB_PNHSV" 管脚参数定义

下载网络组态及程序到 CPU 中,使能参数 ENR=1,在新建打开的两个 Modscan32 窗口的的"Set up->Data Definition"中设置数据扫描周期、寄存器连接类型、起始地址、长度等,如下图 14 所示:

ModScan32 - [ModSca1]	
File Connection Setup View Window Help	
Display Definition	
Address: 0001 Scan Rate: 1000 (msecs)	5: 0
Slave Address: Point Type: 03 HOLDING REGISTER Point Address: 1 Length: 10	Ctrs
** Device NOT CONNECT OK Cancel 40001: 0> 40002: 0> 40003: 0> 40004: 0> 40005: 0> 40006: 0> 40007:<	

Picture14: Modscan32 中 Modbus 数据参数定义

由于 Modbus 的内部地址编排时基于数据链路层和应用层有一定的映射关系,因此 Modbus 的地址与 SIMATIC 中的 DB 块的地址时按照一定的地址映射关系来相对应,这样造 成了 DB 块中有一定的地址偏移量,在本例中假设数据区的定义如下图 15 所示,其 DB 偏移

量、	Modbus 物理编址、	应用层编址如一	下图 16 月	斤亓
_				_

Copyright © Siemens AG Copyright year All rights reserved

data_type_1	B#16#3	Holding register
db 1	W#16#B	DB 11
start_1	W#16#0	Start address: 0
end 1	W#16#1F3	End address: 499
data type 2	B#16#3	Holding register
db 2	W#16#C	DB 12
start 2	W#16#2D0	Start address: 720
end 2	W#16#384	End address: 900
data type 3	B#16#4	Input register
db 3	W#16#D	DB 13
start 3	W#16#2D0	Start address: 720
end 3	W#16#3E8	End address: 1000
data type 4	B#16#0	Not used
db 4	0	0
start_4	0	0
end_4	0	0
data_type_5	B#16#1	Coils
db_5	W#16#E	DB 14
start 5	W#16#280	Start address: 640
end 5	W#16#4E2	End address: 1250
data type 6	B#16#2	Inputs
db 6	W#16#F	DB 15
start 6	W#16#6A4	Start address:1700
end 6	W#16#8FC	End address: 2300
data type 7	B#16#1	Coils
db 7	W#16#10	DB 16
start 7	W#16#6A4	Start address: 1700
end 7	W#16#8FC	End address: 2300
data type 8	B#16#0	Not used
db 8	0	0
start 8	0	0
end 8	0	0

Picture15: 本例中的数据区定义



Picture16: DB 偏移量、Modbus 物理编址、应用层编址对应关系

在 Step7 的项目程序中新建一个变量监控表,插入需要监控的参数和数据区变量,可以看到 Modscan32 软件与 S7-400 的数据通讯已经建立起来了,双方可以进行正常的保持寄存器数据读写操作,如下图 17 所示:

Copyright © Siemens AG Copyright year All rights reserved

1	末(T) (約48	an a	500 BST TOTA H (BOODUS_ICF_ 5入(I) FIC 支張(A) 視問(V) 決議(D)	BELVEL KO	00	a ray or (51 Flogram (1) ORLINE)
-		6		0 6 w	66° 47 11.00	
4	轮射		(7 9	夏示格武	状态值	修改教位
1	DB1.DBX	12.2	"CONTROL_DAT". ENR	BOOL	true	
	DB1.DBX	20.1	"CONTROL_DAT". BUSY	BOOL	true	
	DB1.DBX	20.0	"CONTROL_DAT".LICENSED	BOOL	false	
					_	OA链路状态
	DB1.DBX	20.2	"CONTROL DAT".ESTAB OA	BOOL	true	
	DB1.DBX	20.3	"CONTROL_DAT".NDR_0A	BOOL	false	Company of the second se
	DB1.DBX	20.4	"CONTROL_DAT". ERROR_OA	BOOL	false	LodScan32 - [LodSca1]
	DB1.DBW	22	"CONTROL_DAT". STATUS_OA	HEX	¥#16#A090	Eile Connection Setup View Mindow Help
0	DB1.DBW	40	"CONTROL_DAT". Save_STATUS_OA	HEX	W#16#A100	
	DB1.DBD	32	"CONTROL DAT". Count NDR 0A	DEC	L#51	
2	DB1.DBD	36	"CONTROL_DAT". Count_ERROR_OA	DEC	L#3	
3			1 0 42	中国本		Device Id: 1
4	DB1.DBX	24.0	"CONTROL DAT". ESTAB 1A	BOOL	false	Address: 0001 MODBUS Point To
5	DB1.DBX	24.1	"CONTROL_DAT". NDR_1A	BOOL	false	
5	DB1.DBX	24.2	"CONTROL DAT". ERROR 1A	BOOL	false	Length: 10 U3: HOLDING REGIST
7	DB1.DBW	26	"CONTROL_DAT". STATUS_1A	HEX	W#16#A0FF	
B	DB1.DBW	50	"CONTROL_DAT". Save_STATUS_1A	HEX	W#16#A100	40001: < 94>
9	DB1.DBD	42	"CONTROL DAT". Count_NDR_1A	DEC	L#0	40003: < 33>
0	DB1.DBD	46	"CONTROL_DAT". Count_ERROR_1A	DEC	L#14	40004: < 44>
1						40006: < 0>
2	DB1.DBX	28.0	"CONTROL DAT", RedErrS7	BOOL	true	40007: < 0>
3	DB1.DBX	28.1	"CONTROL_DAT". RedErrDev	BOOL	true	40009: < 0>
4	DB1.DBX	28.2	"CONTROL_DAT". TotComErr	BOOL	false	40010: < 0>
5	//Data		1	1303.000		1
6	DB11.DBW	0	"Holding Register Area".DB_VAR[0]	DEC	94	
7	DB11.DBW	2	"Holding Register Area".DB_VAR[1]	DEC	22	
8	DB11.DBW	4	"Holding Register Area".DB_VAR[2]	DEC	33	通信新提
9	DB11.DBW	6	"Holding Register Area".DB_VAR[3]	DEC	44	
5	DB11.DBW	8	"Holding Register Area".DB VAR[4]	DEC	55	
	DB11.DBW	10	"Holding Register Area".DB VAR[5]	DEC	0	
	DB11.DBW	12	"Holding Register Area".DB VAR[6]	DEC	0	
3	DB11.DBW	14	"Holding Register Area".DB VAR[7]	DEC	0	
	DB11.DBW	16	"Holding Register Area".DB VAR[8]	DEC	0	
5	DRII DRW	1.9	"Holding Register Ares" DB VAR[9]	DEC	0	

Picture17: 通讯连接建立

下面来看一下链路冗余使用的过程,正常情况下通过任何的一个 Modscan32 窗口(对应 IP192.168.2.10 和 192.168.2.11)均可以与 S7-400H 系统建立通讯,如下图 18 所示,当断开 其的一个链路(比如可以拔掉网线或将 CPU 转到 Stop 状态,本例将 IP 为 192.168.2.10 断 开),可以看到 IP 为 192.168.2.11 链路仍保持正常通讯,从而不影响 S7-400H 系统与对方的 通讯,另外通过观察各链路连接参数也可监控其连接状态,如下图 18、19 所示:

3	变量 — [Se	rver_	Job @S7_400PH-H\Modbus_ICP_	Server_RG	CPU 412-5	H PH/DP\S7 Program(1) OHLINE]
<u>الا</u>	表格 (I) 编辑	(E) Å	插入(L) PLC 变量(A) 视图(V) 选项(Q)	窗口(图) 帮助	Ð	
4		6	× BRO X 2 1 K?	Cy 60 42	60° 42 11.00	1
1	绝址		符号	显示格式	状态值	
1	DB1.DBX	12.2	"CONTROL_DAT". ENR	BOOL	true	Tooscan32 - [Rodscal]
2	DB1.DBX	20.1	"CONTROL_DAT". BUSY	BOOL	true	E Eile Connection Setup Yiew Mindow Help -
3						□☞■ ● € \$ \$ \$ \$ \$ \$ \$
4	DB1.DBX	20.0	"CONTROL_DAT".LICENSED	BOOL	false	
5						
6	DB1.DBX	20.2	"CONTROL_DAT".ESTAB_OA	BOOL	true	Device Id: 1
7	DB1.DBX	20.3	"CONTROL_DAT". NDR_OA	BOOL	false	Address: MODBUS Point Type
8	DB1.DBX	20.4	"CONTROL_DAT". ERROR_0A	BOOL	false	Length: 10 03: HOLDING BEGISTER
9	DB1.DBW	22	"CONTROL_DAT". STATUS_OA	HEX	W#16#A090	
10	DB1.DBW	40	"CONTROL_DAT". Save_STATUS_OA	HEX	W#16#A100	40001. 4 125.
11	DB1.DBD	32	"CONTROL_DAT". Count_NDR_0A	DEC	L#1082	40002: < 22>
12	DB1.DBD	36	"CONTROL_DAT". Count_ERROR_OA	DEC	L#3	40003: < 33>
13			0A、1A	连路状态		40005: < 55>
14	DB1.DBX	24.0	"CONTROL_DAT".ESTAB_1A	BOOL	true	40006: < 0>
15	DB1.DBX	24.1	"CONTROL_DAT". NDR_1A	BOOL	false	40008: < 0>
16	DB1.DBX	24.2	"CONTROL_DAT". ERROR_1A	BOOL	false	40009: < 0>
17	DB1.DBW	26	"CONTROL_DAT". STATUS_1A	HEX	W#16#A090	
18	DB1.DBW	50	"CONTROL_DAT". Save_STATUS_1A	HEX	W#16#A100	- IodScan32 - [IodScal]
19	DB1.DBD	42	"CONTROL_DAT".Count_NDR_1A	DEC	L#272	The Connection Saturn View Vindor Holn
20	DB1.DBD	46	"CONTROL_DAT". Count_ERROR_1A	DEC	L#165	
21						Ÿ☞⊌ ◎€! \$\$\$₩↓ € \$`K!
22	DB1.DBX	28.0	"CONTROL_DAT".RedErrS7	BOOL	false	
23	DB1.DBX	28.1	"CONTROL_DAT". RedErrDev	BOOL	false	· · · · · · · · · · · · · · · · · · ·
24	DB1.DBX	28.2	"CONTROL_DAT". TotComErr	BOOL	false	世 信 数 / 作 Device Id: 「
25	//Data			1		MODBUS Point Type
26	DB11.DBW	0	"Holding Register Area".DB_VAR[0]	DEC	126	Length: 10 03: HOLDING REGISTER 💽
27	DB11.DBW	2	"Holding Register Area".DB_VAR[1]	DEC	22	
28	DB11.DBW	4	"Holding Register Area".DB_VAR[2]	DEC	33	40001: < 126>
29	DB11.DBW	6	"Holding Register Area".DB_VAR[3]	DEC	44	40002: < 22>
30	DB11.DBW	8	"Holding Register Area".DB_VAR[4]	DEC	55	40004: < 44>
31	DB11.DBW	10	"Holding Register Area".DB_VAR[5]	DEC	0	40005: < 55>
32	DB11.DBW	12	"Holding Register Area".DB_VAR[6]	DEC	0	40007: < 0>
33	DB11.DBW	14	"Holding Register Area".DB_VAR[7]	DEC	0	40008: < 0>
34	DB11.DBW	16	"Holding Register Area".DB_VAR[8]	DEC	0	40010: < 0>
35	DB11.DBW	18	"Holding Register Area".DB_VAR[9]	DEC	0	

Picture 18: IP 192.168.2.10 及 192.168.2.11 链路连接监控表

쐡	变量 - [Se	rver_	Job @S7_400PH-H\Modbus_TCP_	Server_R	G\CPU 412-5	H PN/DP\S7 Program(1) ONLINE]
8	表格(江) 编辑	(匠) 当	新入(I) PLC 安量(A) 视图(Y) 选项(D)	留口(2) 帮助	防田	
-		6		Of er w	* 60° 42° 110	
	🏠 絶離		R9	显示格式	秋恭值	■ ModScap32 - [ModScal]
1	DB1.DBX	12.2	"CONTROL_DAT". ENR	BOOL	true	Louscansz (Louscar)
2	DB1.DBX	20.1	"CONTROL_DAT". BUSY	BOOL	true	Tile Lonnection Setup Fiew Eindow Halp
3						
4	DB1.DBX	20.0	"CONTROL_DAT".LICENSED	BOOL	false	
5						
6	DB1.DBX	20.2	"CONTROL_DAT".ESTAB_OA	BOOL	false	Device Id: 1
7	DB1.DBX	20.3	"CONTROL_DAT". NDR_0A	BOOL	false	Address: MODBUS Point Type
8	DB1.DBX	20.4	"CONTROL_DAT". ERROR_OA	BOOL	false	Length: 10 03: HOLDING REGISTER •
9	DB1.DBW	22	"CONTROL_DAT". STATUS_0A	HEX	W#16#A0FF	
10	DB1.DBW	40	"CONTROL_DAT". Save_STATUS_0A	HEX	W#16#80C4	** MODBUS Write Failure-DATA NOT UPDATED! **
11	DB1.DBD	32	"CONTROL_DAT".Count_NDR_0A	DEC	L#12	40002: (0)
12	DB1.DBD	36	"CONTROL_DAT". Count_ERROR_0A	DEC	L#3	40003: 〈 0〉 UA进信仪牌
13			0A、1A	连路状态		40005: < 0>
14	DB1.DBX	24.0	"CONTROL_DAT".ESTAB_1A	BOOL	true	40006: < 0>
15	DB1.DBX	24.1	"CONTROL_DAT". NDR_1A	BOOL	false	40008: < 0>
16	DB1.DBX	24.2	"CONTROL_DAT". ERROR_1A	BOOL	false	40009: < 0>
17	DB1.DBW	26	"CONTROL_DAT". STATUS_1A	HEX	W#16#A090	
18	DB1.DBW	50	"CONTROL_DAT". Save_STATUS_1A	HEX	W#16#A100	- IodScan32 - [IodSca1]
19	DB1.DBD	42	"CONTROL_DAT".Count_NDR_1A	DEC	L#49	File Connection Satur View Window Help
20	DB1.DBD	46	"CONTROL_DAT". Count_ERROR_1A	DEC	L#2	
21						
22	DB1.DBX	28.0	"CONTROL_DAT". RedErrS7	BOOL	true	
23	DB1.DBX	28.1	"CONTROL_DAT".RedErrDev	BOOL	true	
24	DB1.DBX	28.2	"CONTROL_DAT". TotComErr	BOOL	false	Address: 0001 Device Id: 1
25	//Data					MODBUS Point Type
26	DB11.DBW	0	"Holding Register Area".DB_VAR[0]	DEC	84	Length: 10 03: HOLDING REGISTER 👱
27	DB11.DBW	2	"Holding Register Area".DB_VAR[1]	DEC	0	
28	DB11.DBW	4	"Holding Register Area".DB_VAR[2]	DEC	0	40001: < 84>
29	DB11.DBW	6	"Holding Register Area".DB_VAR[3]	DEC	0	40002: 〈 0〉 1A通信止滞
30	DB11.DBW	8	"Holding Register Area".DB_VAR[4]	DEC	0	40004: < 0>
31	DB11.DBW	10	"Holding Register Area".DB_VAR[5]	DEC	0	40005: < 0>
32	DB11.DBW	12	"Holding Register Area".DB_VAR[6]	DEC	0	40007: < 0>
33	DB11.DBW	14	"Holding Register Area".DB_VAR[7]	DEC	0	40008: < 0>
34	DB11.DBW	16	"Holding Register Area".DB_VAR[8]	DEC	0	40010: < 0>
35	DB11.DBW	18	"Holding Register Area".DB_VAR[9]	DEC	0	

Picture 19: 将 IP 192.168.2.10 链路中断后监控表

4 配置 S7-400 PN-H 冗余系统通过 CPU 集成 PN 口作为 Client 进行 Modbus

TCP 通讯

下面以 S7-400 PN-H 冗余系统及 Modbus slave 软件为例,详细介绍如何将 S7-400 PN-H 冗余系统通过 CPU 集成 PN 口配置为 Client, Modbus slave 为 Server 进行 Modbus TCP 通讯,下图 20 为服务器功能块库的程序结构及各功能块完成的功能:



Picture 20: 软件包" Modbus/TCP PN CPU Redundant V1.0" 客户端程序架构

注: Modslave 软件可以从网上免费下载得到,本例中使用的版本为 V4.3 版,由于各版本的功能不尽相同,因此需要注意版本问题。

4.1 例子中使用的硬件设备及软件

本例中所用的硬件设备如下表:

名称	数量	订货号
S7-400 电源模块 PS 407 10A	2	6ES7407-0KA02-0AA0
S7-400 CPU412-5H PN/DP	2	6ES7412-5HK06-0AB0(V6.0)
S7-400 机架	1	6ES7400-2JA00-0AA0
网线	若干	
笔记本电脑	1	

Table 6: 客户端硬件清单

所用到软件如下表:

名称	订货号
STEP7 V5.5 SP3 组态编程软件 英文版	
" Modbus/TCP PN CPU Redundant V1.0" 软件选项包	6AV6676-6MB10-0AX0
Modbus slave V4.3	

Table7: 客户端软件清单

4.2 S7-400 PN-H 冗余系统及 Modbus slave 软件组态

打开 STEP7 软件,新建一个项目文件,插入一个"SIMATIC H 站",在硬件组态中分别插入 PS407 电源,CPU412-5H PN/DP 等并设置 Rack 0、1 CPU 的集成 PN 接口的 IP 地址,如下 21 所示:

Station Edit Insert PLC View Opt	tions Window Help	ocuto_obtoacc_s]
D 🚅 🔓 🖉 🙀 🎒 🕒 🕞 🗌	🛍 🋍 👔 🗖 🚼 🕅	
1 2	PS 407 4A	Properties - EthernetRack0 (R0/S2.5)
λ2 λ7 F1 F2 λ5 λ5 <i>P2R</i> <u>λ5<i>P2R</i></u> 4	DP MP/DP H Sync module Etheme@ack0 Pail 1 Poil 2	General Addresses PROFINET Synchronization Profile Standard Short description: PN-I0 Image: Standard Image: Standard Image: Standard Device name: Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: Standard Image: St
1 1 1 2 2 2 2 2 2 2 2 2 2 2 2 2	PS 407 4A PS 407 4A PS 407 4A DP MP/UP 412-5 H PN/DP(1) DP MP/UP H Sync module H Sync module Ethemet/Fack 7 Pot 7 Pot 7 Pot 2	Interface CPU 400 Type: Ethernet Device number: 0 Videes: 192 168 2.10 Networked Yes Properties Comment Comment CPU 412-41 Comment CPU 412-54 Comment CPU 412-54 Comment CPU 412-54 Contract CPU 412-54
< (0) UR2ALU-H		OK Cancel Help B::::::::::::::::::::::::::::::::::::
Slot Module Order 1 PS 407 4A 6ES7 2 ICPU 412-5 H PN/DP 6ES7 2/2 ICPU 412-5 H PN/DP 6ES7	r number Firmware 407-0DA02-0AA0 412-5HK06-0AB0 V6.0	M I Q Comment B::: CPU 4143 PN/DP 2
X1 MP//DP		2 2730 CPU 416F 2

Picture 21: 硬件组态

硬件组态完成后,编译保存,并将例程站点"H Single-sided (Client)"中的程序 (System data 不需要拷贝)拷贝到该项目中。

由于需要在 SIMATIC 站与其他通讯伙伴之间建立 TCP 连接用于 Modbus 通讯,而对于 CPU 的集成 PN 口来说须通过 Open IE(开放式以太网通讯)的方式来建立 TCP 连接,通过 S7-CPU 的 PROFINET 接口 进行 Modbus TCP 通信时,需要使用通信块 FB65 "TCON"、 FB66 "TDISCON"、FB63 "TSEND" 和 FB64 "TRCV",要进行 Modbus TCP 通信,必须在 数据块中为 Rack0 及 Rack1 冗余 CPU 指定相应的参数,相应得参数在程序中主要由 DB2 "MODBUS_HPARAM_PN_2"来完成初始化(注意:参数设置必须在"Data View"视图下的"Actual value"列中设置),其中各参数的含义如下图 22、23 所示:

Addres:	Name	Туре	Initial value	Comment					
0.0		STRUCT							
+0.0	double_sided_red	BOOL	FALSE						
+2.0	connection_OA	STRUCT			+66.0	connection_1A	STRUCT		
+0.0	block_length	WORD	¥#16#40	#!Verbindung_0001!#	+0.0	block_length	WORD	¥#16#40	#!Verbindung_0002!#
+2.0	id	WORD	¥#16#1		+2.0	id	WORD	¥#16#2	
+4.0	connection_type	BYTE	B#16#11		+4.0	connection_type	BYTE	B#16#11	
+5.0	active_est	BOOL	TRUE		+5.0	active_est	BOOL	TRUE	
+6.0	local_device_id	BYTE	B#16#5		+6.0	local_device_id	BYTE	B#16#15	
+7.0	local_tsap_id_len	BYTE	B#16#0		+7.0	local_tsap_id_len	BYTE	B#16#0	
+8.0	rem_subnet_id_len	BYTE	B#16#0		+8.0	rem_subnet_id_len	BYTE	B#16#0	
+9.0	rem_staddr_len	BYTE	B#16#4		+9.0	rem_staddr_len	BYTE	B#16#4	
+10.0	rem_tsap_id_len	BYTE	B#16#2		+10.0	rem_tsap_id_len	BYTE	B#16#2	
+11.0	next_staddr_len	BYTE	B#16#0		+11.0	next_staddr_len	BYTE	B#16#0	
+12.0	local_tsap_id	ARRAY[116]	16 (B#16#0)		+12.0	local_tsap_id	ARRAY[116]	16 (B#16#0)	
*1.0		BYTE			*1.0		BYTE		
+28.0	rem_subnet_id	ARRAY[16]	B#16#0, B#16#0,		+28.0	rem_subnet_id	ARRAY[16]	B#16#0, B#16#0,	
*1.0		BYTE			*1.0		BYTE		
+34.0	rem_staddr	ARRAY[16]	B#16#A, B#16#0,		+34.0	rem_staddr	ARRAY[16]	B#16#A, B#16#0,	
*1.0		BYTE			*1.0		BYTE		
+40.0	rem_tsap_id	ARRAY[116]	B#16#1, B#16#F6		+40.0	rem_tsap_id	ARRAY[116]	B#16#1, B#16#F6	
*1.0		BYTE			*1.0		BYTE		
+56.0	next_staddr	ARRAY[16]	B#16#0, B#16#0,		+56.0	next_staddr	ARRAY[16]	B#16#0, B#16#0,	
*1.0		BYTE			*1.0		BYTE		
+62.0	spare	WORD	¥#16#0	#!Verbindung_0001!#	+62.0	spare	WORD	¥#16#0	#!Verbindung_0002!#
=64.0		END_STRUCT			=64.0		END_STRUCT		
									· · · · · · · · · · · · · · · · · · ·

Rack0 CPU集成PN口Open IE TCP连接参数

Rack1 CPU集成PN口Open IE TCP连接参数

Picture22: DB2 " MODBUS_HPARAM_PN_2" 的 TCP 连接参数设置部分

关于 DB2 " MODBUS_HPARAM_PN_2" 的 Rack0 及 Rack1 冗余 CPU TCP 连接参数含义 如下表 8 所示:

类型	参数	含义			
	double_sided_red	通信伙伴是否为冗余系统,1=冗	余, 0= 单站		
	block_length	固定值W#16#40			
	ld	连接ID,用于FB63/64/65/66 ,Rac	k0和Rack1CPU必须唯一		
		取决于CPU类型,用于FB65(TC	ON)		
		TCP(兼容模式): CPU315、317<	= FWV2.3		
	connection_type	W#16#01;			
		TCP:CPU315,317>= FW V2.4、IM151-8PN/DP CPU、			
		CPU314C、CPU319、CPU	l412、CPU414与CPU416		
OPEN IE		W#16#11			
通讯参数		主动或被动连接:			
	active_est	S7作Client时为主动 TRUE			
		S7作Server时为被动 FALSE			
		取决于CPU类型:			
	less device id	IM151-8PN/DP	B#16#1		
		CPU314C、315、317	B#16#2		
		CPU319	B#16#3		

	CPU412(H)、414(H)、416(H)	B#16#5
	Rack1中的CPU	B#16#15
	local_device_id的长度:	
local_tsap_id_len	主动连接时 W#16#0	
	被动连接时 W#16#2	
rem_subnet_id_len	未使用	
	参数rem_staddr的长度:	
rem_staddr_len	未具体定义连接 B#16#0	
	有具体连接 B#16#4	
	rem_tsap_id的长度:	
rem_tsap_id_len	主动连接时 W#16#2	
	被动连接时 W#16#0	
	通讯接口类型选择:	
next_staddr_len	通过外部CP模块: 非0的其	它值
	通过CPU的集成PN 口: W#16#	0
	本地连接TSAP号,与参数connecti	on_type有关:
	1)connection_type= B#16#01时	
	local_tsap_id[1] 本地连接端口号	·的低字节[16进制]
	local_tsap_id[2] 本地连接端口号	·的高字节[16进制]
local_tsap_id	local_tsap_id[3-16] B#16#00	
	2)connection_type= B#16#11时	
	local_tsap_id[1] 本地连接端口号	·的高字节[16进制]
	local_tsap_id[2] 本地连接端口号	·的低字节[16进制]
	local_tsap_id[3-16] B#16#00	
rem_subnet_id	未使用	
	通信伙伴的IP地址,与参数conne	ction_type有关,以
	192.168.0.1为例:	
	1)connection_type= B#16#01时	
rem staddr	rem_staddr[1]= B#16#01(1),	
—	rem_staddr[2]= B#16#00(0)	
	rem_staddr[3]= B#16#A8(168)	
	rem_staddr[4]= B#16#C0(192)	
	rem_staddr[5-6]=B#16#00(为IPV	6预留)

		2)connection_type= B#16#11时			
		rem_staddr[1]= B#16#C0(192)			
		rem_staddr[2]= B#16#A8(168)			
		rem_staddr[3]= B#16#00(0)			
		rem_staddr[4]= B#16#01(1)			
		rem_staddr[5-6]=B#16#00(为IPV6预留)			
		远程连接TSAP号,与参数connection_type有关:			
		1)connection_type= B#16#01时			
		local_tsap_id[1] 本地连接端口号的低字节[16进制]			
		local_tsap_id[2] 本地连接端口号的高字节[16进制]			
	rem_tsap_id	local_tsap_id[3-16] B#16#00			
		2)connection_type= B#16#11时			
		local_tsap_id[1] 本地连接端口号的高字节[16进制]			
		local_tsap_id[2] 本地连接端口号的低字节[16进制]			
		local_tsap_id[3-16] B#16#00			
	next_staddr	CP的机架号和槽号,当使用CPU的PN口时为 B#16#00			
т					

Table 8: DB2 " MODBUS_HPARAM_PN_2" 的 TCP 连接参数含义 客户端/服务器选择

1100.0				1	- 合广圳	们以分布也引手		
+130.0	server_client	BOOL	TRUE		L			
+130.1	single_write	BOOL	FALSE		- 与功能	妈相夫, 甲与模式	ũ –	
+130.2	connect_at_startup	BOOL	FALSE					
+131.0	reserved	BYTE	B#16#0					
+132.0	data_type_1	BYTE	B#16#3		建业组	送按惧式(ENQ_E	NR/PLC 尼	i 功后)选择
+134.0	db_1	WORD	W#16#B					
+136.0	start_1	WORD	W#16#0					
+138.0	end_1	WORD	W#16#1F3					
+140.0	data_type_2	BYTE	B#16#3					
+142.0	db_2	WORD	¥#16#C					
+144.0	start_2	WORD	¥#16#2D0	1	可定义8个	数据区,支持功	能码1、2、	3, 4, 5,
+146.0	end_2	WORD	¥#16#384					
+148.0	data_type_3	BYTE	B#16#4	1	5, 16			
+150.0	db_3	WORD	W#16#D					
+152.0	start_3	WORD	¥#16#2D0		N:含义如	如下		
+154.0	end_3	WORD	¥#16#3E8				n skt. Let st	A 101
+156.0	data_type_4	BYTE	B#16#0		<u>)ata type</u>	X:拉克大支 KI MOC	10US WIEZ	<u>5</u> 型
+158.0	db_4	WORD	¥#16#0		Identifier	Data type	Size	
+160.0	start_4	WORD	¥#16#0		0	Area not used		1
+162.0	end_4	WORD	¥#16#0		0	Area not used		
+164.0	data_type_5	BYTE	B#16#1		1	Coils	Bit	
+166.0	db_5	WORD	¥#16#E		2	Innuto	Dit	
+168.0	start_5	WORD	¥#16#280		2	inputs	ы	
+170.0	end_5	WORD	¥#16#4E2		3	Holding Register	Word	
+172.0	data_type_6	BYTE	B#16#2		4	law of Deviators	Manual .	
+174.0	db_6	WORD	¥#16#F		4	Input Register	vvora	I
+176.0	start_6	WORD	W#16#6A4					
+178.0	end_6	WORD	¥#16#8FC					
+180.0	data_type_7	BYTE	B#16#1		lb v %/ 15	中日		
+182.0	db_7	WORD	¥#16#10		ID_X: 实灯程	沃万		
+184.0	start_7	WORD	W#16#6A4		tart v m	odbus客左哭武上	1/ 時信記始	·#바바 장하
+186.0	end_7	WORD	W#16#8FC					
+188.0	data_type_8	BYTE	B#16#0		节开始			
+190.0	db_8	WORD	W#16#0	1.				DI-LT
+192.0	start_8	WORD	¥#16#0		-na_x: ma	DODUS命仔器以比	5符但结果:	地址
+194.0	end_8	WORD	W#16#0					
+196.0	conn_OA_send_buffer	ARRAY [1	260 (B#16#0)	—	-消息内部	3存储区		
*1.0		BYTE						
+456.0	conn_0A_recv_buffer	ARRAY [1	260 (B#16#0)	←	-接收数据	存储区		

2, 3, 4, 5, 6,

Identifier	Data type	Size
0	Area not used	
1	Coils	Bit
2	Inputs	Bit
3	Holding Register	Word
4	Input Register	Word

起始地址,对应DB从0字 吉束地址

Picture 23: DB2 " MODBUS_HPARAM_PN_2" 的 Modbus 参数设置部分 由于有 S7-400H 系统有 2 条链路(对应两个 CPU)与 Modbus Slave 软件服务器端模拟通 讯,打开 Modbus Slave 软件,在 Connection-connect 中打开连接属性对话框,连接接口选 择"TCP/IP",TCP/IP Server Port 为分别为本地服务器的端口 502,并可以勾选"Ignore Unit ID"选项,如下图 24 所示:

🕮 Modbus S	ilave - [Mbslav1]	
File Edit	Connection Setup Displa	y View Window Help
0 🚅 🔒	Connect F3	?
ID = 1: F = 0	Disconnect F4	
No connecti	Auto Connect	Connection Setup 🔀
A		Connection
0	0	Serial Port OTCP/IP UDP/IP
1	0	Cancel
2	0	Port 1 Mode
3	0	I OKT O ASCII
4	0	9600 Baud V Flow Control
5	0	
6	0	8 Data bits V BTS Togole 1 [ms] BTS disable delay
7	0	From Davids and
8	0	ТСРИР
9	0	1 Stop Bit 👽 Port 502 🔲 Ignore Unit ID
	- 13	

Picture 24: Modbus Slave 连接窗口

(说明-"Ignore Unit ID"选项的含义如下:

Ignore Unit ID-在一些厂商的 PLC 的程序或网关中可能会用到 Unit ID 以指定处理类型)

4.3 通讯测试

由于" Modbus/TCP PN CPU Redundant V1.0"选项包支持功能码FC1,2,3,4,5, 6,15,16,不同的功能码测试过程中类似,因此下面以FC03(读写保持寄存器)为例来说明 通讯测试的整个过程,对于其他功能码的测试将不再重复描述。

需要说明的是由于客户端功能块需要定义具体的功能码,而主功能块

FB915"MB_PNHCL"并没有直接的管脚来定义功能码,而是由其中的两个参数"DATA_TYPE" 和"single-write"共同决定(参见后面的管脚参数说明),详细情况如下图 25 所示:

Data type	DATA_ TYPE	Function	Length	single_ write	Function code
Coils	1	Read	Any	Irrelevant	1
Coils	1	Write	1	TRUE	5
Coils	1	Write	1	FALSE	15
Coils	1	Write	>1	Irrelevant	15
Inputs	2	Read	Any	Irrelevant	2
Holding register	3	Read	Any	Irrelevant	3
Holding register	3	Write	1	TRUE	6
Holding register	3	Write	1	FALSE	16
Holding register	3	Write	>1	Irrelevant	16
Input register	4	Read	Any	Irrelevant	4

Copyright © Siemens AG Copyright year All rights reserved

Picture 25: S7-400 PN-H 做客户端时不同的功能码的参数定义

在测试过程中我们同样将重点关注通讯连接的建立和当一个链路中断时自动切换到另一 个链路的过程。

由于客户端主功能块 FB915" MB_PNHCL"的参数需要初始化,因此分别在 OB100 及 OB1 中调用 FB915,在 OB100 中调用 FB915 完成相关参数的初始化,FB915 的管脚分布 如下图 26 所示:

		" "TTD MODDIG"	WR015 / DR015
	CALL MD_IMAUL	, IDD_MODDOS ·-"CONTROL DAT" : J O .	DB1 DBWO
	14_0_a	- CONTROL_DAT .14_0_4	DB1 DBW2
	10_1_8 :10.1	- COMINOL_DAI .1d_1_a	DDI. DDWZ
	14_0_0 ; 4 1 %	·	
	10_1_D		DB2
	do_param	MODDOS_AFARAM_FM_2	DDZ DB1 DBD4
	reuse_conn_tim	e COMINUL_DAI .reuse_conn_time "CONTROL DAT"	DB1 DBV8 O
	USE_ALL_CONN	- CONTROL_DAT . USE_ALL_CORN	DB1 DBN0.0
	CONN TIMEOUT	- CONINUL_DAI . NECV_IIMEOUI	DB1. DBD10
	DISCONDECT	- CONTROL_DAT COMM_TIMEOUT	DDI. DDDI4 DDI DDV19 O
1N 🤇	DISCOMMECT	- CONTROL_DAT DISCONNECT	DDI. DDAIO. O
	T_:+	- LICENSE DD "CONTROL DAT" T-:-	DDJ DB1 DBV18 1
	Init RNO	- CONTROL_DAT . INIT	DD1. DDA10. 1 DD1 DDV19 2
	ENŲ DATA TVDV	CUMINUL_DAI . ENQ "CONTROL DAT" DATA TYPE	DDI. DDAIO. 2 DBI DBBIO
	DAIA_IIFE	- COMINUL_DAI .DAIA_IIIE "CONTROL DAI" START ADDRESS	DB1 DBW20
	JIANI_ADDAESS	- COMINUL_DAI SIANI_ADDAESS	DB1 DBW22
	LENGIA WDITE DEAD	- CONINOL_DAI LENGIA "CONTROL DAT" WRITTE READ	DD1. DD022
	INTT	- COMINUL_DAI . HALLE_AEAD	DB1 DBR24.0
	T TORNERD	- COMINOL_DAI . UMII "CONTROL DAT" LICENSED	DB1 DB25
- I - I	BIRY	- CONTROL_DAT . LICENSED	DB1 DBX26 1
	DONE	- CONTROL_DAT DOST	DB1 DBX26 2
	REBUE	- CONTROL_DAT DOME	DB1 DBX26 3
	ERROR ESTAB OA	- CONTROL_DAT . ERROR	DB1 DBX26 4
	STAL OA	- CONTROL_DAT .ESTAD_OA	DB1 DBW28
	VCTAD 1A	- CONTROL_DAT STATUS_OA	DB1 DB120
	STATUS 1A	- CONTROL_DAT STAD_IA	DB1 DBW32
	STATUS_TA ESTAR OR	- COMINDE_DRI .SIRIOS_IR	DD1. DD002
	STATIS OF	·	
durr(FSTAR 1R	. -	
101	STATUS 1B	·-	
	TURNT CODR	·-	
	RodReeS7		DB1 DBY34 O
	RedErrDow	= CONTROL_DAT RedErron	DB1 DBX34 1
	TotComFrr	= CONTROL_DAT . Redribev	DB1 DBX34 2
	Toit Frror	- CONTROL_DAT Trit Error	DB1 DBX34 3
	Trit Statur	- CONTROL DAT . INIC_NTON	DB1 DBW36
	ZTULC SCALOS	CONTROL_DAT . INIC_Status	DD1. DD000

Picture 26: 功能块 FB915" MB_PNHCL" 管脚分布

FB915" MB_PNHCL" 的各参数含义如下表 9:

类型	参数	格式		含义	初始
					化
IN	id 0 a	WORD	假定两个 Rack	CPU0 与 UP0 的连接	是
	10_0_a		CPU 简称为	ID	
	id 1 a	WORD	CPU0、	CPU1 与 UP0 的连接	是
	ια_1_α		CPU1(下同),	ID	
	id 0 b	WORD	如通讯伙伴也	CPU0 与 UP1 的连接	是
	Id_0_0		为冗余的话简	ID	
		WORD	称为 UP0、	CPU1 与 UP1 的连接	是
	IQ_1_D		UP1	ID	
	db_param	BLOCK _DB	参数化 DB 块		是

Copyright ⊚ Siemens AG Copyright year All rights reserved

	reuse_conn_	TIME	一个链路故障后尝试重新建立连接的间	是
	time		層	
	Use_all_con	Bool	0=客户端通过一个链路发送报文	是
	n		1=客户端通过所有组态链路发送报文	
	RECV_TIME	TIME	监视应用层接收数据的超时时间,最少	否
	OUT		20ms	
	CONN_TIME	TIME	TCP 连接建立超时监控时间,最短	否
	OUT		100ms	
	DISCONNEC	BOOL	TRUE时断开远程伙伴的连接	否
	Т			
	REG_KEY_D	BLOCK	授权 DB 块	否
	В	_DB		
	Init	BOOL	手动初始化	否
	ENQ	BOOL	发送报文使能	否
	DATA_TYPE	BYTE	请求的数据类型	否
	START_ADD	WORD	请求的 Modbus 偏移量	否
	RESS			
	LENGTH	WORD	请求的 modbus 长度	否
	WRITE_REA	BOOL	0=读数据请求	否
	D		1=写数据请求	
	UNIT	BYTE	modbus 单元从站地址	
OUT	LICENSED	BOOL	功能块是否授权	否
	BUSY	BOOL	作业正在处理	否
	DONE	BOOL	至少一个连接的报文正常处理	否
	ERROR	BOOL	所有组态的连接通信故障	否
	ESTAB_0A	BOOL	连接 OA 建立	否
	STATUS_0A	WORD	连接 0A 状态	否
	ESTAB_0A	BOOL	连接 1A 建立	否
	STATUS_0A	WORD	连接 1A 状态	否
	ESTAB_0B	BOOL	连接 OB 建立	否
	STATUS_0B	WORD	连接 OB 状态	否
	ESTAB_0B	BOOL	连接 1B 建立	否
	STATUS_0B	WORD	连接 1B 状态	否

Copyright © Siemens AG Copyright year All rights reserved

IDENT_	STRIN	预授权解码输出,将此码连同软件序列	否
CODE	G	号发给西门子 IT 部门后可得到授权	
	[18]		
RedErrS7	BOOL	S7 冗余丢失	否
RedErrDev	BOOL	通信伙伴冗余丢失	否
TotComErr	BOOL	通信完全丢失	否
Init_Error	BOOL	初始化错误	否
Init_Status	WORD	初始化状态	否

Table 9: FB915" MB_PNHCL" 管脚参数定义

下载网络组态及程序到 CPU 中,给参数 ENQ 发送脉冲信号,在打开的 Modbus Slave 软件窗口的"Set up->Slave Definition"中设置、寄存器连接类型、起始地址、长度、显示的列数、数据显示格式及响应时间等,并可勾选"Hide Alias Columns"、"PLC Adresses(Base1)"、"Insert CRC/LRC error"、"Skip response",如下图 27 所示:

😂 Modbus Slave - [Mbslav1]	
🕎 File Edit Connection Setup	Display View Window Help 🗕 🗗 🗙
🗋 🗃 🔚 🎒 📑 🔮	ve Definition F8
ID = 1: F = 03 Use	e as Default
No connection	
Alias 00000	Slave Definition
00	
1 0	Slave ID: OK
2 0	Current and D3 Holding Begister (4x)
3 0	Function: Cancel
4 0	Address: U
5 0	Quantity: 10
6 0	View
7 0	Bows
8 0	
9 0	
	Display: Signed
	Liter Simulation
	Skip response Insert CRC/LRC error
	0 [ms] Response Delay
J	
Setup slave definition	TCP/IP Connection: 502

Picture 27: Modbus Slave 中 Modbus 数据参数定义

⁽说明-各勾选选项的含义如下:

Hide Alias Columns - 隐藏注释选项

PLC Addresses(Base1) - 选择寄存器地址是基于 PLC 地址编排(1..65535)还是基于协议 编排(0-65535)

Insert CRC/LRC error - 选择是否进行 CRC/LRC 错误校验

Skip response – 选择是否忽略报文丢失响应)

关于 SIMATIC 中 DB 偏移量、Modbus 物理编址、应用层编址对应关系请参考本文中 V3.3 章节说明

在 Step7 的项目程序中新建一个变量监控表,插入需要监控的参数和数据区变量,可以 看到 Modsbus Slave 软件与 S7-400H 的数据通讯已经建立起来了,双方可以进行正常的保 持寄存器数据读写操作,如下图 28 所示:

Ľ	Var - [Cli	ient_	Job @S7_400PN-H\Modbus_TCP_0	lient_RG\CPU	412-5 H PM/	DP\S7	Progr	am (1) 0	NLINE]
酱	Inble Edit	Insert	PLC Variable View Options Mindow	Selp					
-14		8		00 66° 40° 66°	MA Iller				
	åddress 📩		Symbol	Display format	Status value	Nodify	value		
1	DB1.DBX	18.2	"CONTROL_DAT". ENQ	BOOL	false	读写	(·诗·晋	
2	DB1.DBB	19	"CONTROL_DAT". DATA_TYPE	HEX	B#16#03	-12-	122 XA	- KLE	
3	DB1.DBW	20	"CONTROL_DAT". START_ADDRESS	DEC	0				
4	DB1.DBW	22	"CONTROL_DAT". LENGTH	DEC	5				
5	DB1.DBX	24.0	"CONTROL_DAT". WRITE_READ	BOOL	false	fals	s		
6	DB1.DBB	25	"CONTROL_DAT". UNIT	DEC	1				
7	DB1.DBX	26.0	"CONTROL_DAT". LICENSED	BOOL	false				
8									
9	DB1.DBX	26.1	"CONTROL_DAT". BUSY	BOOL	false	6			
10	DB1.DBX	26.2	"CONTROL_DAT". DONE	BOOL	false	al Hod	bus S		[bslav1]
11	DB1.DBX	26.3	"CONTROL_DAT". ERROR	BOOL	false	💭 201	e <u>E</u> dit	Connectio	m Setup
12			0A.	1A链路状态	1			5 7 9	08
13	DB1.DBX	26.4	"CONTROL_DAT". ESTAB_OA	BOOL	true	ID = 1:	F = 03		CANNEL COM
14	DB1.DBW	28	"CONTROL_DAT". STATUS_OA	HEX	W#16#A090				
15	DB1.DBW	38	"CONTROL_DAT". Save_STATUS_OA	HEX	¥#16#0000			111000000	
16	DB1.DBX	30.0	"CONTROL_DAT". ESTAB_1A	BOOL	true	A	lias	4x0000	
17	DB1.DBW	32	"CONTROL_DAT". STATUS_1A	HEX	W#16#A090			5001	
18	DB1.DBW	40	"CONTROL_DAT". Save_STATUS_1A	HEX	¥#16#0000	1		5001	
19					1	2		22	
20	DB1.DBD	42	"CONTROL_DAT". Count_Done	DEC	L#436	3		33	
21	DB1.DBD	46	"CONTROL_DAT". Count_Error	DEC	L#0	4	-	44	
22							-		
23	DB1.DBX	34.0	"CONTROL_DAT". RedErrS7	BOOL	false	5	_	55	
24	DB1.DBX	34.1	"CONTROL_DAT". RedErrDev	BOOL	false	6	1	0	
25	DB1.DBX	34.2	"CONTROL_DAT". TotComErr	BOOL	false	7		0	
26	//data			1.000	Contraction of the		1-11 -22	set am	
27	DB11.DBW	0	"Holding Register Area".DB_VAR[0]	DEC	5001	8	通信	数据 ⁰	
28	DB11.DBW	2	"Holding Register Area".DB_VAR[1]	DEC	22	9		0	
29	DB11.DBW	4	"Holding Register Area".DB_VAR[2]	DEC	33	10		0	
30	DB11.DBW	6	"Holding Register Area".DB_VAR[3]	DEC	44				
31	DB11.DBW	8	"Holding Register Area".DB_VAR[4]	DEC	55	For Hel	p, pres	s F1.	

Picture 28: S7-400PN-H 作为客户端与 Modbus Slave 软件通讯

下面看一下链路冗余使用及中断后自动切换的过程,在 Mosbus Slave 软件窗口中,假 设其中的一个 Mosbus Slave 通过端口号为 502 与作为 IP 地址为 192.168.2.10 的 CPU 集成 PN 接口通讯,当断开该链路(比如可以拔掉网线、将正在通讯的 CPU 转到 Stop)可以看到功 能块将自动切换到另一个链路(Modbus Slave 和 IP 地址为 192.168.2.11 的 CPU 集成 PN 接 口)进行通讯,通过观察各链路连接状态参数也可观察得到,如下图 29、30 所示:

ď	¥a	r - [Cli	ent_	Job @S7_400PN-H\Modbus_TCP_(Client_RG\CPU	412-5 H PW/	DP\S7	rogr	am (1)	OWLINE]
4	I al	D 🚅 🖬	G	Main Options Tindow X X Yes Yes </th <th>Selp Selp</th> <th>Ma Her</th> <th></th> <th></th> <th></th> <th></th>	Selp Selp	Ma Her				
	1	Address		Symbol	Display format	Status value	Modify 1	alue		
1		DB1.DBX	18.2	"CONTROL_DAT". ENQ	BOOL	false				
2		DB1.DBB	19	"CONTROL_DAT". DATA_TYPE	HEX	B#16#03				
3		DB1.DBW	20	"CONTROL_DAT". START_ADDRESS	DEC	0				
4		DB1.DBW	22	"CONTROL_DAT". LENGTH	DEC	5				
5		DB1.DBX	24.0	"CONTROL_DAT". WRITE_READ	BOOL	false	false			
6		DB1.DBB	25	"CONTROL_DAT". UNIT	DEC	1				
7		DB1.DBX	26.0	"CONTROL_DAT". LICENSED	BOOL	false				
8										
9		DB1.DBX	26.1	"CONTROL_DAT". BUSY	BOOL	false	-	_	_	
10		DB1.DBX	26.2	"CONTROL_DAT". DONE	BOOL	false	I Lod	ous S	ilave -	[Ibslav]
11		DB1.DBX	26.3	"CONTROL_DAT". ERROR	BOOL	false	D Eile	Edit	t <u>C</u> onnecti	ion Setup
12				0A, 1A	链路正常				5 T 4	2 6 8
13		DB1.DBX	26.4	"CONTROL_DAT". ESTAB_OA	BOOL	true	ID = 1:	F = 0.	3	
14		DB1.DBW	28	"CONTROL_DAT". STATUS_OA	HEX	W#16#A090	10 - 1.	- 0.		
15		DB1.DBW	38	"CONTROL_DAT". Save_STATUS_OA	HEX	W#16#0000			1010000	1
16		DB1.DBX	30.0	"CONTROL_DAT". ESTAB_1A	BOOL	true	LA LA	ias	4x0000	1
17		DB1.DBW	32	"CONTROL_DAT". STATUS_1A	HEX	W#16#A090				
18		DB1.DBW	40	"CONTROL_DAT". Save_STATUS_1A	HEX	W#16#0000			500	4
19					1		2		22	1
20		DB1.DBD	42	"CONTROL_DAT".Count_Done	DEC	L#437	3		33	3
21		DB1.DBD	46	"CONTROL_DAT". Count_Error	DEC	L#0	4		44	
22										
23		DB1.DBX	34.0	"CONTROL_DAT". RedErrS7	BOOL	false	5		55	i.
24		DB1.DBX	34.1	"CONTROL_DAT". RedErrDev	BOOL	false	6	1	0)
25		DB1.DBX	34.2	"CONTROL_DAT". TotComErr	BOOL	false	7 /		n	1
26		//data			10020000				skit ten a	
27		DB11.DBW	0	"Holding Register Area".DB_VAR[0]	DEC	500	8	通信	一数据 •	<u>+</u>
28		DB11.DBW	2	"Holding Register Area".DB_VAR[1]	DEC	22	19		0	E .
29		DB11.DBW	4	"Holding Register Area".DB_VAR[2]	DEC	33	10		C	
30		DB11.DBW	6	"Holding Register Area".DB_VAR[3]	DEC	44		_		3
31		DB11.DBW	8	"Holding Register Area".DB_VAR[4]	DEC	55	For Help	, pres	ss F1.	-

Picture29: 两个链路均正常情况下按照缺省链路取值

1	ar - [Cli	ent_	Job @S7_400PN-H\Modbus_ICP_C	lient_RG\CPU	412-5 H PM	DP\S	7 Prog	ram (1) 0M	INE]
8	able Edit	Insert	PLC Variable View Options Mindow]	felp					
4		6		9 6 w 66	142 //cz				
8	Address		Symbol	Display format	Status value	Nodis	7 value		
1	DB1.DBX	18.2	"CONTROL_DAT". ENQ	BOOL	false				
2	DB1.DBB	19	"CONTROL_DAT". DATA_TYPE	HEX	B#16#03	1			
3	DB1.DBW	20	"CONTROL_DAT". START_ADDRESS	DEC	0				
4	DB1.DBW	22	"CONTROL_DAT". LENGTH	DEC	5				
5	DB1.DBX	24.0	"CONTROL_DAT". WRITE_READ	BOOL	false	fa	lse		
6	DB1.DBB	25	"CONTROL_DAT". UNIT	DEC	1				
7	DB1.DBX	26.0	"CONTROL_DAT".LICENSED	BOOL	false				
8									
9	DB1.DBX	26.1	"CONTROL_DAT". BUSY	BOOL	false	-			
10	DB1.DBX	26.2	"CONTROL_DAT". DONE	BOOL	false	- 16	odbus	Slave - 🔲	oslavi]
11	DB1.DBX	26.3	"CONTROL_DAT". ERROR	BOOL	false		ile <u>E</u> di	t <u>Connection</u>	Setup
12					-	D	📽 🖬		ė ?
13	DB1.DBX	26.4	"CONTROL_DAT".ESTAB_0A	BOOL()A故障	false	ID =	1: F = 0	3	
14	DB1.DBW	28	"CONTROL_DAT". STATUS_0A	HEX	W#16#A0FF				
15	DB1.DBW	38	"CONTROL_DAT". Save_STATUS_OA	HEX	W#16#A0FF			4	
16	DB1.DBX	30.0	"CONTROL_DAT".ESTAB_1A	B00L1A正常	true		Alias	4x0000	
17	DB1.DBW	32	"CONTROL_DAT". STATUS_1A	HEX	W#16#A090	1		505	
18	DB1.DBW	40	"CONTROL_DAT". Save_STATUS_1A	HEX	W#16#80C4	-			
19						2		22	
20	DB1.DBD	42	"CONTROL_DAT".Count_Done	DEC	L#470	3		33	
21	DB1.DBD	46	"CONTROL_DAT".Count_Error	DEC	L#1	4		44	
22				1					
23	DB1.DBX	34.0	"CONTROL_DAT".RedErrS7	BOOL	true	5		55	
24	DB1.DBX	34.1	"CONTROL_DAT".RedErrDev	BOOL	true	6	1	0	
25	DB1.DBX	34.2	"CONTROL_DAT". TotComErr	BOOL	false	7	/	0	
26	//data					0	28 /2	快快雨带	
27	DB11.DBW	0	"Holding Register Area".DB_VAR[0]	DEC	505	7	胆信	和然世币	
28	DB11.DBW	2	"Holding Register Area".DB_VAR[1]	DEC	22	9		0	
29	DB11.DBW	4	"Holding Register Area".DB_VAR[2]	DEC	33	10		0	
30	DB11.DBW	6	"Holding Register Area".DB_VAR[3]	DEC	44		9		
31	DB11.DBV	8	"Holding Register Area".DB_VAR[4]	DEC	55	For }	elp, pre	ss F1.	

Picture30::链路中断后切换到另一个链路通讯

5 软件包" Modbus/TCP PN CPU Redundant V1.0" 授权

每个 CPU 都需要对功能块进行授权,对于 PN-H 冗余系统 CPU 来说,将只对 Rack0 的 CPU 进行授权验证,授权有两个步骤:读取 IDENT_CODE 和申请注册码 REG_KEY, 且在 CPU 中必须调用 OB121,下面以客户端程序块为例来说明授权步骤。

5.1 读取 IDENT_CODE

1、下载程序并将 CPU 切换到 RUN 模式;

2、打开功能块 FB915" MB_PNHCL" 背景块 DB915,确认 IDENT_CODE 的偏移地址为 52; 如图 31 所示:

SIMATIC	Manager - MB_TCP_P	N_RED_4	00					
ie Edt Ir	sert PLC Vew Optio	rs Wind	low - Help					
	2 . K BR	die O	2 2		👬 💽 < No Filter	>	+ 7	2 32 00 5 E T N2
	MB_TCP_PN_RED	_400 (Co	mponent	view)	C:\Program Files\StE	MENSI,ST	IP7\example	WILTER PRARED HILLONLINE
	B MB_TCP_PN_RE	D_400	Ob	ject name	Symbolic nan	nei	KNOV	/HOW protec Load memory C
	🖹 🛄 H Double-side	d (Client)		· · ·				
	E CPU 414	DB P	Param - [I	D8915-	MB_TCP_PN_RED_400	H Doub	e-sided (Clie	nt)\CPU 414-5 H PN/DP_ONLINE]
B	S7-P	Data	block Ec	It BLC	Debug View Window	Help		
ē	E	🗳 🔓		00	↓ 糸 略 ඬ !<>!	1 mil 1	60° N?	
1	H Double-sid	1	Address	Declar	Name	Type	Initial valu	Actual value
	🗈 💼 H Single-side	16	32.0	in	LENGTH	WORD	W#16#0	W#16#0
	E III H Single-side	17	34.0	in	WRITE_READ	BOOL	FALSE	FALSE
		18	35.0	in	UNIT	BYTE	B#16#0	B#16#0
		19	36.0	out	LICENSED	BOOL	FALSE	FALSE
		20	36.1	out	BUSY	BOOL	FALSE	FALSE
	E	21	36.2	out	DONE	BOOL	FALSE	FALSE
		22	36.3	out	ERROR	BOOL	FALSE	FALSE
		23	36.4	out	ESTAB_QA	BOOL	FALSE	FALSE
		24	38.0	out	STATUS_DA	WORD	W#16#0	W#16#A0FF
		25	40.0	out	ESTAB_1A	BOOL	FALSE	FALSE
		26	42.0	out	STATUS_1A	WORD	W#16#0	W#16#FFFF
		27	44.0	out	ESTAB 08	BOOL	FALSE	FALSE
		28	46.0	out	STATUS OB	WORD	W#16#0	W#16#FFFF
		29	48.0	out	ESTAB_18	BOOL	FALSE	FALSE
		30	50.0	out	STATUS 18	WORD	W#16#0	W#16#FFFF
		31	52.0	out	IDENT_CODE	STRI		CACAIMBDBHFEEDMAM2'
	<u> </u>	32	72.0	out	RedErrS7	BOOL	FALSE	TRUE
		33	72.1	out	RedErrDev	BOOL	FALSE	TRUE
		34	72.2	out	TotComErr	BOOL	FALSE	TRUE
	() () () () () () () () () ()	35	72.3	out	Init Error	BOOL	FALSE	FALSE
		36	74.0	out	Init Status	WORD	W#16#0	W#16#0
		37	76.0	stat	CONNECTION[WORD	W#16#0	W#16#1

Picture 31: 确认 IDENT_CODE 的偏移地址

3、监视 DB915.DBB52 开始的 20 个字节,偏移地址 52 开始的 18 个字符即为 IDENT_CODE,监控如图 32 所示:



图 34: 确认 IDENT_CODE

4、按上图方式,获取 IDENT_CODE 和软件包装上的 License-No,并按照章节 5.2 和 5.3 的描述步骤申请注册码。

5.2 通过拨打西门子授权服务中心申请注册码 REG_KEY

授权中心联系方式: 010-64757575

Copyright © Siemens AG Copyright year All rights reserved 通过西门子授权服务中心申请注册码时,需要您提供所购买的软件订货号、IDENT_CODE 和软件包装上的 License-No,如图 34 所示。

5.3 通过网站申请注册码 REG_KEY

1、通过西门子技术支持网站申请,打开如下网址,点击"技术问题提交":

http://support.automation.siemens.com/CN/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=zh

SIEMENS	→ sie	mens.com	→ 工业自动化与驱动技术
西门子中国 Intranet		English	联系
首 页 产品支持 应用与工具 技术服务 综合信:	急 论坛 my Support		
	登寻	表1注册 🗊	[搜索设置] Search
支持网站的新闻	→圓现在清订资	我们的快讯!	全球范围的支持
 → 在最青電记本上安装WINCC flexible 2008 SP3 或 WINCC V1 → SIMATIC 过程控制系统 PCS 7 入门指南 - 第1部分(V8.1) → SIMATIC 过程控制系统 PCS 7 入门指南 - 第2部分(V8.1) 	SP2 时希要考虑那些? 反本,含 APL) 反本,含 APL)	RSS	请选择国家 🗸
→ 怎样将更改名字后的 PLC 变量从 Excel 导入到符号表中, 实 自助支持	现 STEP 7 (TIA Portal) 中自动更新使用的变量?		mySupport i
文档搜索	技术资源		全部个人数据、信息及功能之 概览 – 比如:
输入指定产品信息,快速搜索全球技术资源库中的相关 技术文档,获取最新产品信息:	进入全球技术资源库,浏览产品常问问题,手 认证件可等	册,下载及	→ My Documentation Manager
产品订货号	→ 产品支持	6.用定例。	→ 新闻专递
60	系统演示,实用工具等	迎用关例,	CAx-Download-Manager
	→ 应用与工具		→ 技术需求
	查询关键主题一览		τ
	→ 王월		(二) 全球联系人
全球范围的专家支持	点击此处		←□ 全球商务协作
技术论坛	技术问题提交		→ 现场服务
在技术论坛您能够与其他用户交流心得探讨经验分享案 例。	您的技术问题可以直接提交至技术支持与服务 西门子专家的帮助:	热线,获得	→ 备件
✿ 现在与其他用户讨论	→⊠ 技术问题提交		←□ 进入VIP邮箱

图 35: 技术支持网站

2、请按如下示例的步骤进行操作(注意:由于步骤3搜索出来的参考信息无法解决授权问

题,请直接点击"继续"进入步骤 4),如图 36~40 所示。

图 37: 步骤 2

图 39: 步骤 5

5.4 使用注册码 REG_KEY

1、西门子授权中心收到技术支持申请后,将会尽快给您回复邮件;

2、当获取到注册码后,在项目中打开 LICENSE_DB(DB3);

3、通过菜单"View--->Data View"将 DB 块切换到数据视图模式,将获取的 17 位注册码填 写到"Actual value"中,如图 41 所示。

Address Nam	me Ty	7ре	Initial value	Actual	value	Comment
0.0 REG	G_KEY ST.	TRING [17] '	'insert REG_KEY	'insert	REG_KEY'	Registration Key

Address Name	Туре	Initial value	Actual value	Comment
0.0 REG_KEY	STRING[17]	'insert REG_KEY'	°QODGHNBVWSFJZXNHN'	Registration Key

图 41: 输入注册码

4、将 LICENSE_DB(DB3)下载到 CPU 中,并可通过查看 FB915" MB_PNHCL"的输出 引脚 LICENSED 为 true 则注册码激活成功。

Copyright © Siemens AG Copyright year All rights reserved