

常问问题 • 10/2014

基于 S7-300,400 以太网通讯模 块 CP343-1&CP443-1 Modbus TCP 通讯快速入门(更新版本 V4.3) ^{关键字: CP343-1, CP443-1, Modbus TCP, MobusTCP CP V4.3 软件包</sub>}

http://support.automation.siemens.com/CN/view/zh/90276761

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	4
1.4 Modbus TCP 使用的功能代码	4
1.5 Modbus TCP 通讯应用举例	5
2 SIMATIC S7-300/400 系统 Modbus/TCP 通讯概述	6
2.1 S7-300/400 系统 Modbus/TCP 通讯产品概述	6
2.2 "ModbusTCP CP V4.3" 软件选项包使用概述	7
2.2.1 "ModbusTCP CP V4.3" 块库使用说明	7
2.2.2 MiddbusicPCP V4.3 选项包硬件和软件需求	8
2.3 ModbusicPCPV4.3 软件远项包与 step7 集成概况	·····································
3 配直 S7-400 单站系统通过 CP443-1 作为 Server 进行 Modbus ICF	2.通讯12
3.1 例于中使用的硬件设备及软件	12
3.2 S7-400 系统及 Modscan32 软件组态	13
33 通讯测试	17
4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯	24
 4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯 4.1 例子中使用的硬件设备及软件 	24 24
 4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯 4.1 例子中使用的硬件设备及软件 4.2 S7-400 单站系统与 ModSim32 软件组态 	24 24 24
 4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯 4.1 例子中使用的硬件设备及软件 4.2 S7-400 单站系统与 ModSim32 软件组态	24 24 24 24
 4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯 4.1 例子中使用的硬件设备及软件	24 24 24 28 28
 4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯	24 24 24 28 31 32
 4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯	24 24 24 28 31 32 32

1 Modbus TCP 通讯概述

Copyright © Siemens AG Copyright year All rights reserved

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。

MODBUS/TCP 使 MODBUS_RTU 协议运行于以太网, MODBUS TCP 使用 TCP/IP 和 以太网在站点间传送 MODBUS 报文, MODBUS TCP 结合了以太网物理网络和网络标准 TCP/IP 以及以 MODBUS 作为应用协议标准的数据表示方法。MODBUS TCP 通信报文被封 装于以太网 TCP/IP 数据包中。与传统的串口方式, MODBUS TCP 插入一个标准的 MODBUS 报文到 TCP 报文中,不再带有数据校验和地址。

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,如图 1 所示:

3



图 1: MODBUS TCP 报文

由于使用以太网 TCP/IP 数据链路层的校验机制而保证了数据的完整性,MODBUS TCP 报文中不再带有数据校验"CHECKSUM",原有报文中的"ADDRESS"也被"UNIT ID"替代而加 在 MODBUS 应用协议报文头中。

1.3 Modbus TCP 使用的通讯资源端口号

Copyright © Siemens AG Copyright year All rights reserved

> 在 Modbus 服务器中按缺省协议使用 Port 502 通信端口,在 Modbus 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 S7-300/400 系统 Modbus/TCP 通讯概述

Copyright © Siemens AG Copyright year All rights reserved

2.1 S7-300/400 系统 Modbus/TCP 通讯产品概述

通过 SIMATIC S7 和第三方设备的建立 MODBUS/TCP 通信时按照产品使用分单站和冗 余系统,分为通过以太网通讯模块 CP 和 CPU 的集成 PN 口两种情况。

1) 通过以太网通讯模块 CP343-1 或 CP443-1:

在 S7 控制器通过外部 CP343-1 或 CP443-1 和第三方设备间建立 Modbus/TCP 连接时 需要软件选项包"ModbusTCP CP", 订货号为 2XV9450-1MB00,单授权(仅对一个 CPU 有 效),最新的版本为 V4.3,支持功能代码 1、2、3、4、5、6、15 和 16,功能块库及订货号 如下图 2 所示:

Product	Identification number	From version
OPEN MODBUS / TCP	2XV9 450-1MB00	4.3
FB 108 "MODBUSCP"		1.3 / 2.2
FB 106 "MB_CPCLI"		1.2 / 2.2
FB 107 "MB_CPSRV"		1.2 / 2.1

图 2:软件包"ModbusTCP CP V4.3"

2) 通过 CPU 集成的 PN 接口:

在 S7 控制器通过 CPU 集成 PN 接口和第三方设备间建立 Modbus/TCP 连接时需要产品 软件选项包"ModbusTCP PN ",订货号为 2XV9450-1MB02,最新版本 V2.6,单授权(仅对 一个 CPU 有效),支持功能代码 1、2、3、4、5、6、15 和 16,对 S7-300 和 S7-400 集成 PN 接口的 CPU 都适用,功能块库及订货号如下图 3 所示:

Product	Identification number	From version
Modbus/TCP PN CPU	2XV9 450-1MB02	2.6
FB 102 "MODBUSPN"		3.7
FB 103 "TCP_COMM"		3.2
FB 104 "MOD_CLI"		1.6
FB 105 "MOD_SERV"		1.5

图 3:软件包"ModbusTCP PN-CPU V2.6"

3) 通过 S7-400H 冗余系统的 CP443-1 接口:

通过 S7-400H 冗余系统的 CP443-1 建立第三方设备的 MODBUS/TCP 通信时需要产品软件选项包"Modbus/TCP Redundant ",订货号为 2XV9450-1MB11,最新版本 V2.1,可用于

S7-400H 或者 S7-400 单 CPU 带两个 CP443-1,支持功能代码 1、2、3、4、5、6、15 和

16,功能块库及订货号如下图 4 所示:

Product	Identification number	From version
MODBUS/TCP Redundant	2XV9 450-1MB11	2.1
FB 909 "MB_REDCL"		2.4
FB 908 "MB_CPCLI"		2.3
FB 907 "MB_REDSV"		2.3
FB 906 "MB_CPSRV"		2.2

图 4: 软件包" Modbus/TCP Redundant"

4) 通过 S7-400H 集成的 PN 接口:

通过 S7-400H 集成的 PN 接口建立第三方设备的 MODBUS/TCP 通信时需要产品软件选项包"Modbus/TCP PN CPU Redundant",订货号为 6AV6 676-6MB10-0AX0,最新版本 V1.0,可用于 S7-400H 或者 S7-400 单 CPU,支持功能代码 1、2、3、4、5、6、15 和 16,功能块库及订货号如下图 5 所示:

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

图 5: 软件包" Modbus/TCP PN CPU Redundant"

2.2 "ModbusTCP CP V4.3"软件选项包使用概述

2.2.1 " ModbusTCP CP V4.3" 块库使用说明

1) 该功能块库可以用于 S7-300 单站通过 CP343-1 或 S7-400 单站通过 CP443-1 进行 ModbusTCP 通讯。

2) 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,因此
 需要调用 SIMATIC S7 标准功能块,对于 S7-300/400 的 CP 来说,需要调用
 FC5(AG_SEND), FC6(AG_RECV)功能块。

3) 对于主要功能块 FB106、107 和 108 来说,包含了 V1.x 和 V2.x,它们管脚参数并没有 更改,只是在 V2.x 中增加了 FC10"AG_CNTRL"功能块用于管理 TCP 连接,是否支持功能 块与 CP 的型号和固件版本有关,如下图 6 所示:

Product	Identification number	From version
OPEN MODBUS / TCP	2XV9 450-1MB00	4.3
FB 108 "MODBUSCP"		1.3 / 2.2
FB 106 "MB_CPCLI"		1.2 / 2.2
FB 107 "MB_CPSRV"		1.2 / 2.1

图 6:功能块 V1.x 和 V2.x 版本区别

2.2.2 " ModbusTCP CP V4.3" 选项包硬件和软件需求

所支持硬件和软件需求如下图7和图8所示:

opyright © Siemens AG Copyright year All rights reserved
--

|--|

Product Hardware requirements and belonging order numbers

Modbus/TCP CP (2XV9 450-1MB00)

CP343-1	Block with	Block without
 	AG_CNTRL	AG_CNTRL
6GK7 343-1CX00-0XE0	No	Yes
6GK7 343-1CX10-0XE0 (*)	Yes (from FW V2.1)	Yes (up to FW 2.0)
6GK7 343-1EX11-0XE0	No	Yes
 6GK7 343-1EX20-0XE0	No	Yes
6GK7 343-1EX21-0XE0	Yes (from FW V1.0.17)	Yes
6GK7 343-1EX30-0XE0 (*)	Yes (from FW V2.0.16)	Yes
6GK7 343-1GX11-0XE0	No	Yes
6GK7 343-1GX20-0XE0	No	Yes
6GK7 343-1GX21-0XE0	Yes (from FW V1.0.24)	Yes
6GK7 343-1GX30-0XE0	Yes (from FW V1.0.23)	Yes
6GK7 343-1GX31-0XE0	Yes	Yes
CP443-1	Block with	Block without
	AG_CNTRL	AG_CNTRL
6GK7 443-1EX10-0XE0	No	Yes (V2.6)
 6GK7 443-1EX11-0XE0	No	Yes
6GK7 443-1EX20-0XE0	Yes (from FW V1.0.26,	Yes
	not V2.1.12)	(not V2.1.12)
 6GK7 443-1EX30-0XE0 (*)	Yes (from FW V3.0)	No
 6GK7 443-1EX40-0XE0	Yes (from FW V2.2)	Yes
 6GK7 443-1EX41-0XE0	Yes (from FW V1.0.24)	Yes
 6GK7 443-1GX11-0XE0	No	Yes
6GK7 443-1GX20-0XE0	Yes (from FW V2.0, not V2.1.12)	Yes
6GK7 443-1GX30-0XE0 (*)	Yes (from FW V3.0)	No
(*) These CPs support the multiple port 502. In this	case the block with AG_CNTRL must	be used.
 CPU:		

.

The Modbus blocks can be used from hardware release 2 of CPU315 and CPU317.

Modbus/TCP CP is released for standard CPUs, for F-CPUs and for PN-(H)-CPUs.

图 7:"ModbusTCP CP V4.3"软件包硬件需求

更多支持硬件信息请查看如下连接:

http://www.industry.siemens.com/services/global/en/IT4Industry/products/simatic_add_ons/ s7_open_modbus_tcp/Pages/default_tab.aspx?tabcardname=technical%20data

Software Versions The usage of the modbus blocks is possible with **STEP7 Version 5.4** or higher. Withal the use of the blocks AG_LSEND/AG_LRECV V3.1 of the update of SIMATIC NET library (http://support.automation.siemens.com/WW/view/en/22172239) is required.

图 8:"ModbusTCP CP V4.3"软件包软件需求

2.3 "ModbusTCP CP V4.3"软件选项包与 step7 集成概况

下面章节将介绍如何使用软件选项包" ModbusTCP CP V4.3 "的功能块库配置 S7-300/400 单站系统通过 CP343-1/CP443-1 与第三方模拟软件进行 Modbus/TCP 进行通讯的 详细步骤,实际上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,另外还可找到用 CFC 语言编程的功能快库,供读者选 用,如下图 9~11 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,以下主要描述了使用软件选项包" ModbusTCP CP V4.3 "配置 S7-300/400 站的详细配 置和编程步骤。

- the library in \Program Files\Siemens\Step7\S7libs,
- 2 example projects in \Program Files\Siemens\Step7\Examples,
- the manual in \Program Files\Siemens\Step7\S7manual\S7Comm,
- the software registration form in \Program Files\Siemens\Step7\S7libs\Modbus_TCP_CP.

图 9: 块库、例程、英文手册和软件注册的文件夹位置

Open Project		
User projects Libraries Sample project	ts Multiprojects	
	Language English	-
Name	Storage path	
MODBUS_TCP_CP_CFC+CFC+ MODBUS_TCP_CP_EXAMPLE+CF MODBUS_TCP_CP_Redundant PROJECT-ETHERNET_en PROJECT-PROFIBUS_en	列程 C:\Program Files\Sie P例程 \Program Files\Sie C:\Program Files\Sie C:\Program Files\Sie C:\Program Files\Sie	eme eme eme eme eme eme
Selected User projects: Libraries: Sample projects: Multiprojects:	Brows	e

图 10: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
SModbus_PN_CPU	C:\Program Files\Siemens\Step7\S7libs
♦Modbus_TCP_CP	能块库 'rogram Files\Siemens\Step7\S7libs
Modbus_TCP_CP_Red300_4	00 C:\Program Files\Siemens\Step7\S7libs
Nodbus_TCP_CP_Redundan	it C:\Program Files\Siemens\Step7\S7libs
NIODiag 😔	C:\Program Files\Siemens\Step7\S7libs
📚 Redundant IO CGP V40	C:\Program Files\Siemens\Step7\S7libs
Redundant IO CGP V51	C:\Program Files\Siemens\Step7\S7libs
Selected	
ser projects:	
braries:	
ample projects:	
ampio projecto.	

图 11: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 单站系统通过 CP443-1 作为 Server 进行 Modbus TCP 通讯

下面以 S7-400 单站系统及 Modscan32 软件为例,详细介绍如何将 S7-400 单站系统通过 CP443-1 配置为 Server, Modscan32 为 Client 进行 Modbus TCP 通讯,在本例中讲使用带 FC10"AG_CNTRL"版本的功能块,下图 12 为服务器功能块库的程序结构及各功能块完成的 功能:



图 12:服务器功能块库程序结构

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:

	r	1	
名称	数量	订货号	
S7-400 电源模块 PS 407 10A	1	6ES7407-0KA01-0AA0	
S7-400 CPU414-3PN/DP	1	6ES7414-3EM05-	
		0AB0(V5.2)	
S7 400 CP443 1	4	6GK7443-1EX41-	
37-400 CF 443-1	1	0XE0(V1.0)	
S7-400 机架	1	6ES7400-1JA00-0AA0	
网线	若干		
笔记本电脑	1		

表 1:服务器硬件清单

所用到软件如下表:

名称	订货号
STEP7 V5.5 组态编程软件 英文版	
" ModbusTCP CP V4.3" 软件选项包	2XV9450-1MB00
Modscan32 V7.0	

表 2:服务器软件清单

3.2 S7-400 系统及 Modscan32 软件组态

打开 **Step7** 软件,新建一个工程项目文件,命名为"**M_TCP_CP_V43(Server)**",在项目下 插入一个 **S7-400** 站,如下图 **13** 所示:

File Edit Insert PLC	View Options Window Help		
▲ 100 CP CP V43 (Server)	Image: Description of the sector of the s	No Filter > Y Y K Type S MPI 2	
	Copy Ctrl+C Paste Ctrl+V		
	Delete Del	SIMATIC 400 Station	
	PLC +	SIMATIC 300 Station	
	Rename F2 Object Properties Alt+Return	SIMATIC PC Station Other Station SIMATIC S5 PG/PC SIMATIC 200 Station	
		MPI PROFIBUS Industrial Ethernet PTP Foundation Fieldbus	
		S7 Program	

图 13:新建 S7-400 Station

双击插入的 SIMATIC 400 Station 的"Hardware",打开硬件组态,在硬件组态界面下分 别插入机架,电源 PS407、CPU414-3PN/DP、CP443-1,本例中将 CP 的 IP 地址设为 192.168.70.2,如下图 14 所示:

			Lana.
(0) UR2			Profil Standard
1	PS 407 10A	*	
3	CPU 414-3 PN/DP		PROFIBUS-PA
-			PROFINET IO
IF1			E SIMATIC 300
Z1	MPI/DP	E	SIMATIC 400
25	PN-IO	N	
25 F1 25 P2	Port 2		
5	CP 443-1 Advanced		E CP 443-1 Advanced-IT
6			😟 📄 6GK7 443-1EX40-0X1
7		-	E 66K7 443-1EX41-0X
perties - CP 443-1	Advanced - (B0/S5)		3 V1.0
	interes - (no/ss/		E 66K7 443-16X00-0X1
IP Access Protec	tion IP Configuration	Users Symbols	E 66K7 443-16X10-0X1
DNS Parameters	FTP PROFINE	T Diagnostics	₩ ₩ 66K7 443-16X20-0X
eneral Addresse	s Port Parameters Options 1	Time-of-Day Synchronization	DE PROFIBUS
Land	CP 442-1 Adversed	1	🛨 🦲 Point-to-Point
nort	CT CD C T L L 1 L DEL I DE	OPTIMET TO C	CPU-400
	PROFINET CBA, ISO and TCP/IP with	SEND-RECEIVE and	☐ СРУ 400-Н
	FETCH-WRITE interface, long data,	UDP, TCP, ISO, S7	EPU 412-1
	communication, Fouting, module Fe	epracement without ro, +	
rder No./	6GK7 443-1EX41-0XE0 / V1.0		EPU 413-1
lame:	CP 443-1 Advanced		E CPU 413-2 DP
Interface			CPU 414-1
There is a construction of the second			(III) (IIII) (III) (III) (III) (III) (III) (IIII) (IIIII) (IIII) (IIII) (IIII) (IIII) (IIII) (IIIII) (IIII) (IIIII) (IIIIII) (IIIIII) (IIIIIIII
lype. Etr	ernet		CPU 414-3 DP
Address: 192	. 168. 70. 2		EVEN 414-3 PN/DP
Networked: Yes	Properties		
ommefit;			
		^	😟 🛛 🚺 V5. 3
			€ 6ES7 414-3EM06-0AB0
		•	CPU 414F-3 PN/DP
			E CFU 416-1
OK		Cancel Help	

图 14:硬件组态并设置 CP443-1 的 IP 地址

打开 Netpro 网络组态,选中 CPU414-3PN/DP,插入一个新连接,连接伙伴为 Unspecified,连接类型为 TCP Connection,如下图 15 所示:

MPI(1) MPI	Lthernet	
Local ID	TIC 400(1) STUE RATE State Partner ID Partner ID Partner ID Partner ID Download selected connections Show/Hide Columns Optimize Column Width Display Columns	Ctrl+N
		Project: Station: (Unspecified) Module:
		Connection Type: TCP connection Type: Display properties before inserting
		OK Apply Cancel Help

图 15:网络组态-新建 TCP connection

打开连接属性对话框中的"General Information",由于 CP443-1 做 Server 被动连接,因此不勾选"Active connection establishment"选项,ID 保持缺省即可,在"Address"栏中同样由于 CP443-1 做 Server,因此填入连接的 Port 号设置为 502,组态完成后,编译保存,将例程站点" SIMATIC 400(Server)"中的程序(System data 不需要拷贝)拷贝到该项目中并下载(注意:OB100 中调用的 FB108 的 id 和 laddr 需根据组态确认)。对于通讯伙伴 Remote 的 IP 地址可以不填,即允许任意 IP 地址的客户端发起连接,如下图 16 所示:

operties - TCP connection	Properties - TCP connection
Options Overviee Status Information General Information Addresses Local Endpoint ID Chex):	Options Overview Status Information General Information Addresses Ports from 1025 through 65535 are available. General 1025 through 65535 are available. Of or further ports, refer to online help) IP (dec): Local IS2.168.70.2 FORT (dec): Status Information
的FB108输入端 	OK Cancel Help

图 16:S7-400 为服务器的 TCP connection 参数设置

对于服务器和客户端的端口号(下述中以 Port 代替)的选择需要注意以下几点:

1)一般情况下服务器端的 Port 号 modbus TCP 规范缺省为 502,客户端的 Port 号设 置为客户端允许的号即可,另外各厂商产品也有一些限制,对于 SIMATIC 产品一般从 2000 之后开始。

2)对于一个系统来说,当创建多个 TCP 连接时,要保证 IP 地址和 Port 号不重合,即同一个 IP 地址下创建多个 TCP 连接时 Port 号必须不同,而不同的系统因 IP 地址不同可以使用相同的 Port 号,例如本例中如果需要创建多个 TCP 连接作为 Server 时因只有一个IP,因此 Port 号必须不同。

3.3 通讯测试

由于"ModbusTCP CP V4.3"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 3:

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

表 3:Modbus 数据类型

由于服务器主功能块 FB108"MODBUSCP"的参数需要初始化,因此分别在 OB100 及 OB1 中调用 FB108,在 OB100 中调用 FB108 完成相关参数的初始化,FB108 的管脚分布 如下图 17 所示:







注意: 在图 17 中已经填写的参数不需要初始化,在 OB1 调用赋值; 而未填写的参数需要 初始化,在 OB100 中调用完成。

打开 Modscan32 软件,在"Connection--->connect"中打开连接属性对话框,连接接口选择"Remote TCP/IP Server", IP Address 分别填入 CPU 的 IP 地址 192.168.70.2, Service 为远程服务器的端口 502,在协议的选择对话框中可以定义传输模式、通讯超时响应时间, 报文发送间隔及允许写多个保持寄存器等,这里分别保持缺省设置即可,如下图 18 所示:

ModScan32 - ModSca	al		
File Connection Setu	p View Window Help		- 19 <u>-</u>
	onnection Details	23	
	Connect		
	Remote TCP/IP Server		
ModSca1	IP Address: 192.168.70.2		
Address: 0001	Configuration 502	Modbus Protocol Selections	X
Length: 100	Baud 9600 T Hardware F Word 8 T Delay	fd CASCII CRTU	DANIEL/ENRON/OMNI CASCII CRTU
	Parit NOME Vait Dela	Slave Response Time	out (msecs)
** Data Uninit 00001: <0> 00 00002: <0> 00 00003: <0> 00	rotocol Selectio OK Can	Delay Between Polls	(msecs)
00004: <0> 00 00005: <0> 0001 00006: <0> 00019 00007: <0> 0002 00008: <0> 0002 00009: <0> 0002 00009: <0> 0002	3: <u> UUU31: <u> UUU44: <u> UUU55: 5: <o> 00032: <o< td=""> 00045: <o< td=""> 00055: 0: <o> 00033: <o< td=""> 00045: <o< td=""> 00055: 1: <o> 00034: <o< td=""> 00046: <o< td=""> 00066: 1: <o> 00034: <o< td=""> 00047: <o< td=""> 00066: 2: <o> 00035: <o> 00048: <o> 00066: 2: <o> 00035: <o> 000448: <o> 00066:</o></o></o></o></o></o></o<></o<></o></o<></o<></o></o<></o<></o></o<></o<></o></u></u></u>	V Force modbus command (10 be used in cases of support the singlerpor and OF) OK	15 and 16 for singlerpoin where the slave does not int write functions 05

图 18:对应 TCP 通讯的 Modscan32 连接窗口

下载网络组态及程序到 CPU 中,使能参数 ENQ_ENR=1,在 Modscan32 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 19 所示:

🚥 ModScan32 - ModSca1							
File Connection Setup V	/iew Window Help						
	I III						
🖶 ModSca1							
Address: 0001 Length: 100	Display Definition						
** Device NOT CONNE	Point Type: 03 HOLDING REGISTER Point Address: 2 Length: 10						
00001: <0> 00014: 00002: <0> 00015: 00003: <0> 00016:	OK Cancel						

图 19:Modscan32 中 Modbus 数据参数定义

之后在 ModScan32 中就可以建立和远程 CP443-1 Server 的连接了,在 Netpro 中可以 看到连接已经建立起来,如下图 20 所示:

NetPro - [M_TCP_CP_V43(Server) (Connection s Paraget Network Edit Insert PLC View Options	status) G:\modbus TCP test\M_TCP_2_ONLINE]
🚰 🖣 🎒 🗃 🛍 🏜 🏜 🔗 🔗	
Palanna (1)	1
Industrial Ethernet	ModScan32 - ModSca1
NDT (1)	File Connection Setup View Window Help
MPI(1) MPI	
SIMATIC 400(1) CFU SF-IC SF-	ModScal Address: 0002 MODBUS Point Type Length: 10 03: HOLDING REGISTER •
Connection stat Local ID Partner ID ▶ established 0001 A050	Part TCP 40002: < 11> 40003: < 2> 40004: < 3> 40005: < 4> 40006: < 5> 40007: < 6> 40008: < 7> 40009: < 8> 40009: < 8> 40010: < 9> 40010: < 10>

图 20: Modscan32 激活与 S7-400 的连接

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 21 所示,其 DB 偏移量、Modbus 物理编址、应用层编址如下图 22 所示:

data_type_1	B#16#3	Holding Register
db_1	W#16#B	DB 11
start_1	W#16#1	Start address: 1
end 1	W#16#1F4	End address: 500
data type 2	B#16#3	Holding Register
db $\overline{2}$	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

图 21:本例中的数据区定义



图 22: 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 CP443-1 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 23 所示:

N	Ta	ble Edit	Insert	PLC Variable View Options Wi	indow Help	2			
-14	1	0 🛋 🖬	8	x 🖻 🖻 🗠 🗙 🔽 😫 🕅	2	00 60° 40° 60°	1 ² //45=		
	1	Address		Symbol	Display	Status value		Modify value	
1	1	//连接控制	l]	5-		05			
2		DB1.DBX	4.0	"CONTROL DAT". ENQ_ENR	BOOL	true			
3	1	DB1.DBX	4.1	"CONTROL DAT". LICENSED	BOOL	false	i.		
4		DB1.DBX	4.2	"CONTROL DAT". BUSY	BOOL	true			
5		DB1.DBW	6	"CONTROL DAT". STATUS	HEX	W#16#A090	D		
6		DB1.DBW	48	"CONTROL DAT". COUNT_ERROR	DEC	8			
7		DB1.DBW	50	"CONTROL DAT". COUNT_DONE	DEC	1080			
8		DB1.DBW	52	"CONTROL DAT". Save_STATUS	HEX	W#16#8304	1		
9									
10		// "CONTR	OL_DAT	". Save_STATUS_FUNC					
11		DB1.DBD	56		CHARACTER	'AG_R'	M	dScan32 - ModSca1	
12		DB1.DBD	60		CHARACTER	'ECV '	File	Connection Coture View	Window Hala
13							rie	connection setup view	window help
14		// output	: tele	gram parameters		and service and service and			
15		DB1.DBB	65	"CONTROL DAT". Save_UNIT	HEX	B#16#01	- Eul		
16		DB1.DBB	68	"CONTROL DAT". Save_DATA_TYPE	HEX	B#16#03			
17		DB1.DBW	70	"CONTROL DAT". Save_START_ADDRE	DEC	1		MedSca1	
18		DB1.DBW	72	"CONTROL DAT". Save_LENGTH	DEC	10			Device Id: 1
19		DB1.DBW	66	"CONTROL DAT". Save_TI	DEC	0	Ad	dress: 0002	
20		DB1.DBX	74.0	"CONTROL DAT". Save_WRITE_READ	BOOL	false			MODBOS Point Type
21		//data					Le	ngth: 10 03: H	IOLDING REGISTER
22		DB11.DBW	0	"DATA_AREA_1".DB_VAR[1]	DEC	11			
23		DB11.DBW	2	"DATA_AREA_1".DB_VAR[2]	DEC	2			
24		DB11.DBW	4	"DATA_AREA_1".DB_VAR[3]	DEC	3	400		
25		DB11.DBW	6	"DATA_AREA_1".DB_VAR[4]	DEC	4	400	04: < 3>	
26		DB11.DBW	8	"DATA_AREA_1".DB_VAR[5]	DEC	5	400	05: < 4>	
27		DB11.DBW	10	"DATA_AREA_1".DB_VAR[6]	DEC	6	400	07: < 6>	
28		DB11.DBW	12	"DATA_AREA_1".DB_VAR[7]	DEC	7	400	09: < 8>	
29		DB11.DBW	14	"DATA_AREA_1".DB_VAR[8]	DEC	8	400	10: < 9>	
30		DB11.DBW	16	"DATA_AREA_1".DB_VAR[9]	DEC	9	400	11, (10)	
31		DB11.DBW	18	"DATA_AREA_1".DB_VAR[10]	DEC	10			

图 23:通讯连接建立

4 配置 S7-400 单站系统作为 Client 进行 Modbus TCP 通讯

下面以 S7-400 单站系统及 ModSim32 软件为例,详细介绍如何将 S7-400 单站系统配置为 Client, ModSim32 为 Server 进行 Modbus TCP 通讯,在本例中同样使用 FC10 "AG_CNTRL"版本的功能块,由于客户端和服务器模式均使用相同的功能块,因此客户端功能块库的程序结构及各功能块完成的功能可以参考图 12。

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	1	6ES7407-0KA01-0AA0
S7-400 CPU414-3PN/DP	1	6ES7414-3EM05-
		0AB0(V5.2)
S7-400 CP443-1	1	6GK7443-1EX41-
		0XE0(V1.0)
S7-400 机架	1	6ES7400-1JA00-0AA0
网线	若干	
笔记本电脑	1	

表 4:客户端硬件清单

所用到软件如下表:

名称	订货号
STEP7 V5.5 组态编程软件 英文版	
" ModbusTCP CP V4.3" 软件选项包	2XV9450-1MB00
ModSim32 免授权版本	可从网上免费获取

表 5:客户端软件清单

4.2 S7-400 单站系统与 ModSim32 软件组态

打开 Step7 软件,新建一个工程项目文件,命名为"M_TCP_CP_V43(Client)",在项目下 插入一个 S7-400 站,如下图 24 所示:

File Edit Insert PLC	View Options Window Help	
] 🗅 🛩 🎛 🛲 X 🖻 🖻		< No Filter > 🔄 🏹 📲
M_TCP_CP_V43(Client)	Cut Ctrl+X Copy Ctrl+C Paste Ctrl+V	Type S MPI 2
6	Delete Del Insert New Object	SIMATIC 400 Station
	PLC F2 Rename F2 Object Properties Alt+Return	SIMATIC 300 Station SIMATIC H Station SIMATIC PC Station Other Station SIMATIC S5 PG/PC SIMATIC 200 Station
		MPI PROFIBUS Industrial Ethernet PTP Foundation Fieldbus S7 Program

图 24:新建 S7-400 Station

双击插入的 SIMATIC 400 Station 的"Hardware",打开硬件组态,在硬件组态界面下分别插入机架,电源 PS407、CPU414-3PN/DP、CP443-1,本例中将 CP 的 IP 地址设为 192.168.70.2,如下图 25 所示:

			E-mail 1
(0) UR2			Profil Standard
1	PS 407 10A	·	= PROFIBIIS DP
3	CPU 414-3 PN/DP	-	PROFIBUS-PA
U U			PROFINET IO
IF1			E INATIC 300
II I	MPI/DP		I I I SIMATIC 400
#5	PN-IO	_ N	□ □ □ CP-400
15 Pi	Port 1	- IN	Industrial Ethernet
<u>25 P2</u>	Fort 2		E CP 443-1 Advanced-TT
6			€ 6GK7 443-1EX40-0XE
7			E GK7 443-1EX41-0XE
			2 V1.0
erties - CP 443-17	Advanced - (RU/SS)		
TP Access Protec	tion TP Configuration	lisers Sumbols	€ 6GK7 443-1GX10-0XE
DNS Parameters	FTP PROFINET	Diamostics	€ 66K7 443-16X11-0XE
eneral Addresse	s Port Parameters Options Tim	e-of-Day Synchronization	
1	1 1 1 1	· · · · · · · · · · · · · · · · · · ·	Thornbos
nort	CP 443-1 Advanced	\	E- CPV-400
	S7 CP for Industrial Ethernet, PROF.	INET IO Controller,	庄 🧰 СРУ 400-Н
	FETCH-WRITE interface, long data, U	DP, TCP, ISO, S7	E CPU 412-1
	communication, routing, module repl	acement without PG, 🔫	⊕ <u></u> CPU 412-2 DP
der No./	6GK7 443-1EX41-0XE0 / V1.0		E CPU 412-2 PN
me:	CP 443-1 Advanced		
	1		E CPU 414-1
Interface			E CPU 414-2 DP
Type: Eth	ernet		EPU 414-3 DP
Address: 192	. 168. 70. 2		CPU 414-3 PN/DP
Networked: Yes	Properties		6ES7 414-3EM05-0AB0
			₩ V5.0
omment:			t = ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹ ₹
		*	
		*	E CPU 414F-3 PN/DP
			E CPU 416-1
			□ □ □ CPU 416-2 DP
OK		Cancel Help	E CPU 416-3 DP

图 25: 硬件组态并设置 CP443-1 的 IP 地址

打开 Netpro 网络组态,选中 CPU414-3PN/DP,插入一个新连接,连接伙伴为 Unspecified,连接类型为 TCP Connection,如下图 26 所示:

MPI(1) MPI	SINATIC 400(1)	Insert New Connection	nt project V43(Client) ecified) roadcast stations ulticast stations
.ocal ID	2 Partner ID Partner Insert New Connection Ctr Download selected connections Show/Hide Columns Optimize Column Width Display Columns	+N Project: Station: (Unspe Module:	roject <u>t</u> <u>c</u> ified)
		Connection Type: TCP co	nnection

图 26: 网络组态-新建 TCP connection

打开连接属性对话框中的"General Information",由于 CP443-1 做 Client 主动发起连接,因此需要勾选"Active connection establishment"选项,ID 保持缺省即可,在"Address" 栏中同样由于 CP443-1 做 Client,对于本地的端口号设置为 2000(一般从 2000 以外开始以 避免与别的协议资源冲突),对于通讯伙伴 Remote 的 IP 地址设置为测试 PC 机的 IP 地 址,本例中 PC 机的 IP 设置为 192.168.70.245,而 Port 号设置为 502,如下图 27 所示:

operties - TCP connection	Properties - TCP connection
Options Overview Status Information General Information Addresses Local Endpoint IB Onex): 00001 A050 V Name: TCP connection1 Via CP: CP 443-1 Advanced CEO/SS) Route V Active connection establishment Use FTF protocol 填写到OB100调用 的FB108输入端	Options Overviee Status Information General Information Ports from 1025 through 65535 are available (Por further ports, refer to online help) IP (dec): PORT (dec): Server 端口号: 502
OK Cancel Melp	OK Cancel Melp

图 27: S7-400 为客户端的 TCP connection 参数设置

组态完成后,编译保存,将例程站点"SIMATIC 400(Client)"中的程序(System data 不需要拷贝)拷贝到该项目中并下载(注意:OB100中调用的 FB108 的 id 和 laddr 需根据 组态确认)。

关于服务器和端口号的设置请参考本文中 3.2 章节说明。

4.3 通讯测试

由于"ModbusTCP CP V4.3"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,因此下面同样以 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 FB108 "MODBUSCP"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 28 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

图 28:S7-400 单站系统做客户端时不同的功能码的参数定义

由于客户端和服务器均使用相同的功能块 FB108"MODBUSCP"的参数需要初始化,因此分别在 OB100 及 OB1 中调用 FB108,在 OB100 中调用 FB108 完成相关参数的初始化,FB108 的管脚分布参见 3.3 章节中的图 17 说明。

打开 ModSim32 软件,在"Connection--->connect"中打开连接属性对话框,连接接口选择"Modbus/TCP svr",TCP/IP Server Port 为本地服务器的端口 502,如下图 29 所示:

rile connection Disp	nay window Help		
ModSim1			
Address: 0100	Device Id: MODBUS Po 03: HOLDING RE	1 Jint Type GISTER 🝷	Select Service Port
*** NOT CONNEC	 TED! * * *		502
40100: <00000>	40116: <00000>	40132: <00	
40102: <00000>	40118: <00000>	40134: <00	

图 29:ModSim32 中设置端口号

下载硬件组态及程序到 CPU 中,给参数 ENQ_ENR 发送脉冲信号;在打开的 ModSim32 软件窗口设置寄存器连接类型、起始地址、长度等,如下图 30 所示:

vice ld: 1 DBUS Point Type DING REGISTER -

图 30: ModSim32 中 Modbus 数据参数定义

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 3.3 章节图 22 的说明

之后在 CP443-1 Client 就可以建立和远程 ModSim32 Server 的连接了,在 Netpro 中可 以看到连接已经建立起来,如下图 31 所示:

29

Transfer Edit Insert	PLC View C	Detions Window 7 🖉 🕕 🖻	w Help
Ethernet(1) Industrial Ethernet		Professional U.I.	
MPI(1) MPI			
SIMATIC 400(:	1)		
CFU DP MPI/DF CP 414-3 DF Adv	GBII PN+IC -1 anc		
2 2			
	12.5	T	10

图 31: Modscan32 激活与 S7-400 的连接

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 ModSim32 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 32 所示:

5	Table Edit	Insert	PLC Variable View Option	ns Window He	p			
-14		0		R	96.	an 6	ti 47 ller	
	Address		Symbol	Display format	Status 1	value	Modify value	
1	DB1.DBX	4.0	"CONTROL DAT". ENQ_ENR	BOOL	false	r.	true	
2	DB1.DBX	4.1	"CONTROL DAT". LICENSED	BOOL	false			
3	DB1.DBX	4.2	"CONTROL DAT". BUSY	BOOL	false			
4	DB1.DBW	6	"CONTROL DAT". STATUS	HEX	¥#16#	A090		
5	DB1.DBW	48	"CONTROL DAT". COUNT_ERROR	DEC	2			
6	DB1.DBW	50	"CONTROL DAT". COUNT_DONE	DEC	8			
7	DB1.DBW	52	"CONTROL DAT". Save_STATUS	HEX	V#16#	0000		
8								
9	//"CONTRO	L_DAT'	". Save_STATUS_FUNC					
10	DB1.DBD	56		CHARACTER	' MODE	3'	ModSim32	- [ModSim1]
11	DB1.DBD	60		CHARACTER	' USCF	, ,	File Cor	nection Display Window Help
12								
13	// input:	teles	gram parameters					Device Id:
14	DB1.DBB	38	"CONTROL DAT". UNIT	HEX	B#16#	01	Address	0002 MODBUS Point Type
15	DB1.DBB	39	"CONTROL DAT".DATA_TYPE	HEX	B#16#	03		► 03: HOLDING REGISTER
16	DB1.DBW	40	"CONTROL DAT". START_ADDRE	DEC	1		Length:	10
17	DB1.DBW	42	"CONTROL DAT". LENGTH	DEC	10	1		
18	DB1.DBW	44	"CONTROL DAT". TI	DEC	0		2	
19	DB1.DBX	46.0	"CONTROL DAT". WRITE_READ	BOOL	false		40002: <000	11>
20	//data				_	1	40003. (000	33>
21	DB11.DBW	0	"DATA_AREA_1".DB_VAR[1]	DEC	11	4	40005: <000	44>
22	DB11.DBW	2	"DATA_AREA_1".DB_VAR[2]	DEC	22		40006: <000	55>
23	DB11.DBW	4	"DATA_AREA_1".DB_VAR[3]	DEC	33		40007: <000	66>
24	DB11.DBW	6	"DATA_AREA_1".DB_VAR[4]	DEC	44		40008: <000	88>
25	DB11.DBW	8	"DATA_AREA_1".DB_VAR[5]	DEC	55	1	40010: <000	99>
26	DB11.DBW	10	"DATA_AREA_1".DB_VAR[6]	DEC	66		40011: <000	10>
27	DB11.DBW	12	"DATA_AREA_1".DB_VAR[7]	DEC	77			
28	DB11.DBW	14	"DATA_AREA_1".DB_VAR[8]	DEC	88			
29	DB11.DBW	16	"DATA_AREA_1".DB_VAR[9]	DEC	99			
30	DB11.DBW	18	"DATA_AREA_1".DB_VAR[10]	DEC	10			

图 32:S7-400 单站系统作为客户端与 ModSim32 软件通讯

5 "ModbusTCP CP V4.3" 选项包通讯使用总结及相关注意事项

由于是通过 PC 测试软件模拟第三方设备与 SIMATIC CPU 的集成 PN 口进行 Modbus TCP 通讯,因此在实际的第三方设备与 CPU 的集成 PN 口进行通讯时需要注意以下几点:

1) 由于订货号 2XV9450-1MB02 程序中会占用 CPU 较大的装载和工作存储区,因此对于 性能比较低特别是 S7-300 的低端 CPU 进行通讯时必须考虑一定的富余量。

2) 对于 SIMATIC S7,参数 DB_x 的数据区建议使用不同的 DB 块,使用同一个 DB 的不同地址区会造成地址编排混乱,另外参数 Start_x 与 END_x 参数不能出现地址叠加情况。

3) 第三方设备的数据区与 SIMATIC S7 的数据 DB 块的地址对应关系可以先按照第三方的数据区域 Modbus 地址的偏移关系之后计算相应的偏移量。

4)建议使用项目中的样例程序,只须修改连接 ID,定义通讯双方的 IP 地址、端口号及相应的数据存储区等,能减少编程量,只须把样例程序放到一个单独的 FC 块中即可,样例程序中定义了足够的数据区,连接成功及错误次数指示等。

5) Modbus TCP 每一包的数据最多只能发送 125 个寄存器或 2000 个比特位,超过该范围 必须进行分包处理。

6) S7-300/400 作为 Client 能与多少个 Server 建立通讯或者作为 Server 时能与多少个 Client 通讯取决于产品所支持的 TCP 连接数, Modbus/TCP 协议并没有对此进行约束和限制。

更多关于 S7 Open Modbus/TCP 通讯的详细信息请参考西门子 Industrial IT 部门的以下连接:

http://www.industry.siemens.com/services/global/en/IT4Industry/products/simatic add ons/s7 o pen modbus tcp/Pages/default tab.aspx

更多关于 Modbus TCP 的相关信息请参考 FAQ:

"如何从 SIMATIC 建立 OPEN MODBUS /TCP 通信,以及在哪可以找到更多信息?" http://support.automation.siemens.com//CN/view/zh/22660304

在用户程序中,当功能块的块号已经被使用时,哪些 Modbus TCP 块可以重命名或重新 布线?

http://support.automation.siemens.com/CN/view/zh/58378237

6 "ModbusTCP CP V4.3" 软件包授权

未经授权的 Modbus TCP 软件可用于测试和学习,不允许用于商业行为;未经授权的软件测试时 CPU 的 INTF 指示灯红色闪烁,并在 CPU 故障缓冲区生成错误信息;同时, Modbus TCP 功能块报错,如图 33、34 所示:

tus:	😵 Error	•		Not a	force job	1	
Per	formance	e Data Disenost	Communi ic Buffer	cation	Stacks	Identifi	cation
vent:	s:	🗖 Fil	ter settings	activ [] Ti	me including C	?V/local time	differer
No.	Time o	f day	Date	Event			^
1	12:09:	23.987 PM	03/25/2014	Event ID:	16# A090		
2	12:09:	23.987 PM	03/25/2014	Area lengt	h error when re	ading	
3	12:09:	19.987 PM	03/25/2014	Event ID:	16# A090		
4	12:09:	19.987 PM	03/25/2014	Area lengt	h error when re	ading	
5	12:09:	15.986 PM	03/25/2014	Event ID:	16# A090		
6	12:09:	15.986 PM	03/25/2014	Area lenzt	h error when re	ading	
etai:	ls on	1 of 1	.20		Even	t ID: 16# A09	0
No e Even OB: PK:	ntry in at ID:	text data 16# A09 16# 01 16# 01	base. Hexadec 90	imal values	will be display	red.	, 11
50	vo åe	5.	ttings	Open Blo	ck	Help o	n Event

图 33: CPU 诊断缓冲区报错

	Т	able Edit	Insert	PLC Variable View Options	Window Help	
-14	4		6		<u>N?</u>	<u>) 67 m 66 m</u>
	1	Address		Symbol .	Display	Status value
1		//连接控制	l			
2		DB1.DBX	4.0	"CONTROL DAT".ENQ_ENR	BOOL	false
3	Γ	DB1.DBX	4.1	"CONTROL DAT".LICENSED	BOOL	false
4		DB1.DBX	4.2	"CONTROL DAT".BUSY	BOOL	false
5		DB1.DBW	6	"CONTROL DAT". STATUS	HEX	W#16#A090

图 34: Modbus TCP 功能块报错 A090

每个 CPU 都需要对功能块 MODBUSCP 进行授权。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。

6.1 读取 IDENT_CODE

1、下载程序并将 CPU 切换到 RUN 模式;

2、打开 MODBUSCP(FB108)的背景块 DB108,确认 IDENT_CODE 的偏移地址为 108;如图 35 所示:

	B Data block Edit PLC Debug View Window Help B B B B P P P B B B B I I ≪ ≫! M M 60' N?						
	Address	Declaration	Name	Туре	Initial valu	Actual valu	
39	92.0	in	ENQ_ENR	BOOL	FALSE	FALSE	
40	94.0	out	LICENSED	BOOL	FALSE	FALSE	
41	94.1	out	BUSY	BOOL	FALSE	FALSE	
42	94.2	out	DONE_NDR	BOOL	FALSE	FALSE	
43	94.3	out	ERROR	BOOL	FALSE	FALSE	
44	96.0	out	STATUS	WORD	W#16#0	W#16#0	
45	98.0	out	STATUS_FUNC	STRING [8]	,,	, ,	
46	108.0	out	IDENT_CODE	STRING [18]	,,	.,	
47	128.0	in_out	UNIT	BYIE	B#16#U	B#16#U	
48	129.0	in_out	DATA_TYPE	BYTE	B#16#0	B#16#0	

图 35: 确认 IDENT_CODE 的偏移地址

3、打开变量监视表,输入 DB108.DBB108 开始的 20 个字节,偏移地址 110 开始的 18 个字 符即为 IDENT_CODE,监控如图 36 所示:

i Va	ar - [VAT_1	@M_1	PLC N	43(Server)\SIMA	TIC 400(1)\CPU	
a i		AB	X Bali	anable view alliplical XI	De g	▶2	
		9	00				
6	Address	109	Symbol	Display format	Status	value	
	DBIOS DBB	100	-	DEC	10	_	
	DD100.DDD	110	TOP N	CUARACTER	10	-	
12	DB100, DDB	111	TDB W	CHARACTER			
	DB108 DBB	112	TDB W	CHARACTER	' H'		
	DB108, DBB	113	TDB M	CHARACTER	'H'		
	DB108, DBB	114	TDB M	CHARACTER	'A'		
	DB108, DBB	115	TDB M	CHARACTER	'B'	-	
	DB108, DBB	116	TDB M	CHARACTER	'F'		
	DB108, DBB	117	TDB M	CHARACTER	· T'	-	
	DB108, DBB	118	TDB M	CHARACTER	'C'	-	
	DB108.DBB	119	"IDB M	CHARACTER	'F'		
	DB108.DBB	120	"IDB M	CHARACTER	· A'		
	DB108.DBB	121	"IDB M	CHARACTER	. J.		
	DB108.DBB	122	"IDB M	CHARACTER	'K'		
	DB108.DBB	123	"IDB_M	CHARACTER	' M'		
	DB108.DBB	124	"IDB_M	CHARACTER	'B'		
	DB108.DBB	125	"IDB_M	CHARACTER	'J'		
	DB108.DBB	126	"IDB_M	CHARACTER	.1.		
	DB108.DBB	127	"IDB_M	CHARACTER	'2'		
	Bitte trage Das Handt	n Sie der ouch enti ENT_	a informata iDENT-C salt Informa _CODE	on how to find out it ODE hier ein tionen, wie Sie den I	DENT-COD	E ermitte	n S7-OpenMedbur //109
	Please inse You find ti Bitte trage	ert the Li he Licen n Sie die	cense-No. h se-No. on t2 Lizenz-Nr	ere. .ee package of the p hier ein.	A LANGE LANGE		37 - Operation Control States F41C32,1577 c Type of Software I Software photoes (your of Bonney Lineary): 5 - Soft Conce Type of Dec Ant dec Not any 200 No. 7 Anabit 1 Software Cass 1 Software Cass Reference have and 72 Software Concern
	Sie finden	die Lizer	nz-Nr. auf d	er Verpackung der			Sectors For Filmer Content of Sectors and Sectors
	>>> Li	cense	No / Li	zenz-Nr <<<			PLEASE CALIFORNIA CALIFORNIA CALIFORNIA
				<	1 (The		Remark / Availablerg Software and electronic documentarias or CD
	<u>.</u>						Order Bis / Browt Nr. 2009412-150002
				E	Item		John Ste Weild Elevents for a 2009th C101-000C044
					sir	na	atic add o

图 36: 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 6.2 和 6.3 的描述步骤申请注册码。

6.2 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

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 36 所示。

6.3 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

SI	E	M	E	NS
-			Real Property lies	

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!	<mark>急 论坛 mySupport</mark> 登录 注册 🗊	·搜索设置] Search
 支持网站的新闻 	→ 回现在请订阅我们的快讯! I SP2 时需要考虑那些?	全球范围的支持 请选择国家
自助支持 文档搜索 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: 产品订货号	技术资源 进入全球技术资源库,浏览产品常问问题,手册,下载及 认证件可等 → 产品支持 关于自动化系统产品综合应用,可以在此获得应用实例,系统演示,实用工具等 → 应用与工具	mysupport [1] 全部个人数据、信息及功能之 概览 – 比如: → My Documentation Manager → 新闻专递 〇 CAx-Download-Manager [1] → 技术需求
全球范围的专家支持 技术论坛 技术论坛您能够与其他用户交流心得探讨经验分享案例。 叠 现在与其他用户讨论	查询关键主题一览 → 主题 点击此处 技术问题提交 您的技术问题可以直接提交至技术支持与服务热线,获得 西门子专家的帮助: → 四 技术问题提交	联系 ←□ 全球联系人 ←□ 全球商务协作 → 现场服务 → 各件 ←□ 进入VIP邮箱

图 37: 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 38~42 所示。



图 39: 步骤 2



图 41:步骤 5



6.4 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 43 所示。

Address Name	Туре	Initial value	Actual value	Comment
0.0 REG_KEY	STRING [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 43: 输入注册码

4、将 LICENSE_DB(DB3)下载到 CPU 中, CPU 的 INTF 指示灯熄灭;并可通过查看 MODBUSPN(FB102)的输出引脚 LICENSED 为 true 且不再报 A090 错误代码,确认注册 码激活成功,如图 44 所示。

	T I	able Edit	Insert	PLC Var	riable Viev	v Options	Window	Help		
-0	-		6	x 🖻 🖻	200	K 📲 🖁	▶?	9	66" 47	66° 47
	1	Address		Symbol			Displa	ау	Status	value
1		//连接控制	J							
2		DB1.DBX	4.0	"CONTROL	DAT".ENQ_	ENR	BOOL		fals 📕	e
3	Γ	DB1.DBX	4.1	"CONTROL	DAT".LICE	NSED	BOOL		📕 true)
4		DB1.DBX	4.2	"CONTROL	DAT". BUSY		BOOL		fals	e
5		DB1.DBW	6	"CONTROL	DAT". STAT	US	HEX		W#16	\$#0000

图 44: 注册码激活成功

附表一 CP 进行 Modbus TCP 通讯 FB 输出常见故障代码及处理

STATUS(Hex)	故障原因	处理措施
	FB MODBUS	故障
A002	Modbus 起始地址 Start_x 错误	由通讯伙伴确认起始地址
A003	Modbus 地址映射的 DB 块的数据	扩展 DB 区域
	区长度太短,最低长度:	当 CP 为 Client 时,修改参数 START-
	-寄存器:	ADDRESS 或者 LENGTH
	(START_ADDRESS – start_x +	当 CP 为 Server 时,修改客户端的请求
	LENGTH) * 2	
	-位	
	(START_ADDRESS – start_x +	
LENGTH) / 8		
	其他可能的原因:	
	·参数初始化错误(CP为 Client 时)	
	·客户端请求报文时错误的地址区	
	域(CP 为 Server)	
A004	仅在 CP 为 Client 时才有此故	修改此两个参数
	障:	
	参数DATA_TYPE及	
	WRITE_READ设置不匹配,不可	
	能对输入寄存器或离散输入进行	
	写操作	

A005 CP 为 Client 时: CP 为 Client 时: 参数 LENGTH 设置无效 修改参数 LENGTH CP 为 Server 时: CP为Server时: Client 请求的寄存器号无效,合法 修改 Client 请求的数据类型范围 的数据类型范围如下: 读线圈/离散输入:1 to 2000 写线圈:1 to 1968 读寄存器:1 to 125 写保持寄存器: 1 to 123 A006 CP为客户端时: CP 为 Client 时: 数据区1-8中对应的Modbus地址 修改参数 范围(DATA TYPE, DATA TYPE,START ADDRESS和 LENGTH START_ADDRESS和 LENGTH CP为Server时:)不存在 修改Client 请求或修改数据类型 CP 为服务器时: data_type_x. 客户端请求的报文不正确 A007 CP 为 Client 时: 修改参数 MONITOR 参数MONITOR监控时间设置无 效, 值必须>20ms A008 接收监控超时,可能的原因: 检查通讯伙伴的参数设置,如单元标识 对于 MODBUSCP V2.x: 符等 所有通过 502 端口的连接激将中 断并重新建立 对于 MODBUSCP V1.x: 同步错误,报文丢失 A009 当 CP 为 Client 时,接收标识符 TI 通过抓包工具来分析和修正通讯伙伴的 与发送不一致,连接将终止和重新 报文 建立 对于 MODBUSCP V2.x: 所有通过 502 端口的连接激将中 断并重新建立 A00A CP 为 Client 时,接收参数 UNIT

	与发送的不一致,连接将终止和	
	重新建立	
	对于 MODBUSCP V2.x:	
	所有通过 502 端口的连接激将中	
	断并重新建立	
A00B	CP 为 Client 时:	CP为Client时:
	接收与发送功能码不一致	通过抓包工具来分析和修正通讯伙伴的
	CP 为 Server 时:	数据报文格式
	无效的功能码被接收	CP 为 Server 时:
	对于 MODBUSCP V2.x:	注意 FB MODBUS 仅支持功能码
	所有通过 502 端口的连接激将中	FC1、2、3、4、5、6、15、16
	断并重新建立	
	对于 MODBUSCP V1.x:	
	同步错误,报文丢失	
A00C	接收到的字节长度与寄存器/位不	通过抓包工具来分析和修正通讯伙伴的
	匹配	报文
	CP 为服务器时, CP 将发一个响	
	应异常给客户端	
	对于 MODBUSCP V2.x:	
	所有通过 502 端口的连接激将中	
	断并重新建立	
A00D	仅在 CP 为 Client 时发生:	
	响应的 MODBUS 寄存器/位地址	
	或长度与客户端请求的不一致	
A00E	MODBUS 报文报头的长度与寄存	
	器/位 不匹配, FB 将忽略	
	对于 MODBUSCP V2.x:	
	所有通过 502 端口的连接激将中	
	断并重新建立	
	对于 MODBUSCP V1.x:	
	同步错误, 报文丢失	
A00F	非0的协议标识符报文被接收	

	对于 MODBUSCP V2.x:	
	所有通过 502 端口的连接激将中	
	断并重新建立	
	对于 MODBUSCP V1.x:	
	同步错误,报文丢失	
A010	数据区 1-8 DB 块号重复使用	确保每个 Db 块号只使用一次
A011	DATA_TYPE 参数设置(范围为 1-	修改 DATA_TYPE 参数
	4)	
A012	数据区参数data_type_1和	数据区不能有重叠的 modbus 地址区域
	data_type_2设置重叠	
A013	数据区参数 data_type_1 和	修改此参数
	data_type_3 设置重叠	
A014	数据区参数 data_type_1 和	
	data_type_4 设置重叠	
A015	数据区参数 data_type_1 和	
	data_type_5 设置重叠	
A016	数据区参数 data_type_1 和	
	data_type_6 设置重叠	
A017	数据区参数 data_type_1 和	
	data_type_7 设置重叠	
A018	数据区参数 data_type_1 和	
	data_type_8 设置重叠	
A019	当参数 data_type_x 设置不为 0	db_x 不能为 0
	时,db_x 被赋值 0	
A01A	报头中长度错误:	通过抓包工具来分析和修正通讯伙伴的
	范围 3-253 字节	报文
	对于 MODBUSCP V2.x:	
	所有通过 502 端口的连接激将中	
	断并重新建立	
A01B	CP 为 Server 及使用功能码 FC05	
	时:	

	接收的线圈值无效	
	CP 将发送异常报文	
A01E	CP 接收到无法识别的数据,	分析错误信息,通过抓包工具来分析和
	对于 MODBUSCP V2.x:	修正通讯伙伴的报文
	所有通过 502 端口的连接激将中	
	断并重新建立	
	对于 MODBUSCP V1.x:	
	同步错误,报文丢失	
A01F	功能块FB MBBUSCP返回一个无	联系产品供货商
	效的状态	
A020	参数Check_conn_cycle设置<1s	当为Client模式时,参数
	时,对于功能块AG_CNTRL过短	Check_conn_cycle=TRUE下
		Check_conn_cycle设置需要>1s;
		当为 Server 模式时,
		Check_conn_cycle 设置需要>1s;
A023	数据区参数data_type_2和	数据区不能有重叠的 modbus 地址区域
	data_type_3设置重叠	
A024	数据区参数data_type_2和	
	data_type_4设置重叠	
A025	数据区参数data_type_2和	
	data_type_5设置重叠	
A026	数据区参数data_type_2和	
	data_type_6设置重叠	
A027	数据区参数data_type_2和	
	data_type_7设置重叠	
A028	数据区参数data_type_2和	
	data_type_8设置重叠	
A034	数据区参数data_type_3和	
	data_type_4设置重叠	
A035	数据区参数data_type_3和	
	data_type_5设置重叠	

right © Siemens	Copyright year	rights reserved
opyr	AG 0	All

A036	数据区参数data_type_3和	
	data_type_6设置重叠	
A037	数据区参数data_type_3和	
	data_type_7设置重叠	
A038	数据区参数data_type_3和	
	data_type_8设置重叠	
A045	数据区参数data_type_4和	
	data_type_5设置重叠	
A046	数据区参数data_type_4和	
	data_type_6设置重叠	
A047	数据区参数data_type_4和	
	data_type_7设置重叠	
A048	数据区参数data_type_4和	
	data_type_8设置重叠	
A056	数据区参数data_type_5和	
	data_type_6设置重叠	
A057	数据区参数data_type_5和	
	data_type_7设置重叠	
A058	数据区参数data_type_5和	
	data_type_8设置重叠	
A067	数据区参数data_type_6和	
	data_type_7设置重叠	
A068	数据区参数data_type_6和	
	data_type_8设置重叠	
A068	数据区参数data_type_7和	
	data_type_8设置重叠	
A07A	参数 id 设置无效:范围 1-64	修改参数 id
A07C	参数data_type_1设置无效:范围	修改参数data_type_x
	0-4	
A07D	参数data_type_1未定义,	修改参数data_type_1
	data_type_1为缺省的使用数据	
	区, 需要定义	

A07E	参数db_x值与背景DB中的值不一	修改参数db_x
	致	
A080	在 OB1 和 OB100 调用 FB	需要使用相同的背景 DB
	MODBUS 功能块时使用了不同的	
	背景 DB	
A081	CP 为 Client 且使用 FC05 功能码	通过抓包工具来分析和修正通讯伙伴的
	时:	报文
	接收的线圈状态与发送不一致	
A082	CP 为 Client 且使用 FC06 功能码	通过抓包工具来分析和修正通讯伙伴的
	时:	报文
	接收的寄存器值与发送不一致	
A083	仅在 CP 为 Client 时:在上一个请	等待DONE =TRUE 或 ERROR =
	求还没有处理完成时又发送新的	TRUE后再发送新请求
	请求	
A085	在授权期间由于无效的写权限导	对于授权DB,确认参数REG_KEY的结
	致发生错误	构是否正确
A090	功能块未授权,此为一状态信	针对CPU读出预授权解码,之后按照授
	息,参数 ERROR 并不会置 1,	权操作向IT4industry.部门索取授权码
	功能块在未授权情况仍然可以运	
	行而不影响通讯	
A091	收到异常响应码 1(仅在 Client 模	通讯伙伴不支持请求的报文
	式),连接将终止和重新建立	
A092	收到异常响应码 2(仅在 Client 模	确认参数LENGTH 或
	式),无效的或不存在的地址请求	START_ADDRESS
		是否正确
A093	收到异常响应码 3(仅在 Client 模	通讯伙伴无法执行报文接收(例如请求长
	式)	度不支持等)
A094	收到异常响应码 4(仅在 Client 模	通讯伙伴无法执行报文接收
	式)	
A095	收到未知的异常响应码(仅在	通过抓包工具来分析和修正通讯伙伴的
	Client 模式)	报文
FC/SFC 故障		

7xxx	请参考 SIMATIC 的在线帮助	通过在线帮助 SIMATIC manager ->
		mark block -> key F1 -> Ethernet ->
		see also -> code evaluation 可以查到
		相关帮助信息
8xxx	请参考 SIMATIC 的在线帮助	通过在线帮助 SIMATIC manager ->
		mark block -> key F1 -> Ethernet ->
		see also -> code evaluation 可以查到
		相关帮助信息
SFC24 故障		
80A1	DB=0 或超出了 CPU 允许的范围	选择有效的 DB
80B2	DB 块在 CPU 中不存在	DB_x 参数中的 DB 块必须创建并下载
		到 CPU 中
80B3	DB 块被创建为"Unlinked"类型	DB 块不能创建为"Unlinked"类型