CPU H05 可编程逻辑控制器

用户手册

版本: V2.01 发布日期: 08/2017 大连德嘉工控设备有限公司

目录

1.	产品概述3
2.	Modbus 通讯(填表方式)4
3.	参数设置8
4.	MicroWIN 连接设置9
5.	WinCC 连接设置16
6.	组态王连接设置
7.	力控连接设置
8.	连接 SMART LINE 参数设置 32
9.	Modbus 通讯(梯形图方式)33
10.	PLC 之间通讯设置 40
11.	PLC 之间通讯实例 44
12.	C# Modbus TCP 通讯实例 48
13.	与 Modbus 数码管通讯设置 55

1 产品概述

首先,H05型 PLC 与西门子 S7-200 完全兼容,可以用西门子 STEP7-MicroWin 或 STEP7-MicroWin SMART 编程软件,内嵌 Modbus RTU 模式(非编程),连接 Modbus 变频器、仪器仪表等,通过软件内填表方式,实现 Modbus 的通讯。

H05型 PLC——2018.9.1 最新升级(两项内容如下)

(注:其他类型的德嘉 PLC 目前还不具有此功能)

升级内容 A: 不仅可以用原来 S7-200 的编程软件也可用西门子 SMART PLC 的 STEP7-Micro/Win SMART 编程、调试、上传、下载。 但在 smart 方式下: 1.密码只能使用最高级别"不允许上传",其余级别都无效,等同于"完全权限"。 2.主 CPU 和 I/O 模块的输出在从 RUN(运行)转换为 STOP(停止)时,是否将输出冻结在 最后的状态,将继承原 S7-200 时的系统块设置,不受 smart 编程软件的影响,如想修改, 请用 S7-200 的编程软件。 设置好后,将系统块下载到 PLC 中,然后再重新用 smart 编程软件下载全部程序,但它 是无法覆盖冻结输出这一部分的内容

注:如果使用 smart 软件编程,当它下载完程序后, S7-200 的编程软件就无法上传出 PLC 中的程序;反之亦然。

如果想切换编程软件,就要在微软的 IE 浏览器地址栏中键入 192.168.1.222(PLC 的后门 地址,并不是真实地址),进入 PLC 设置菜单,先完成"STOP PLC",然后再选择 "PLC 清空", 之后就可使用你所喜欢的编程软件了!

升级内容 B: 增加 modbus 主从站非编程,以填表方式实现(简单实用) 使用填表方式时,有 modbus 主站和 modbus 从站两种选项 1.modbus 从站方式:

只需填写波特率,校验方式,从站地址即可完成

modbus 地址与 S7-200PLC 的数据对应关系如下:

00001-00128	Q0.0、	Q0.1 、	Q0.2	. Q15	.7
10001-10128	10.0 、	10.1	、 10.2	I	15.7
30001-30032	AIW0、	AIW2、	AIW4	AIW62	

4000n-4xxxx VW(n)、VW(n+2)、VW(n+4)

例 1: modbus 起始地址 8 、个数 3 对应 PLC 的 V 区为 VW8 、VW10、VW12

例 2: modbus 起始地址 19、个数 4 对应 PLC 的 V 区为 VW19、VW21、VW23、VW25 2.modbus 主站方式:

首先填写波特率、校验方式、等待从站应答时间、命令重发次数(是指 modbus 命令发送后,如果没有收到从站的正确应答,是发送下一条 modbus 命令,还是再次或多次发送本条命令)

主站方式可以有最多 64 条 modbus 命令,它通过在表中双击鼠标来添加或修改 modbus 命令行来轻松实现编程,这些命令从上致下按顺序不断循环发送执行。

每条 modbus 命令中唯一要说明的是"命令执行前延时 ms",它是指该命令执行前要延时一段时间,主要用于给从站一个缓冲时间,一般情况下是无需延时的,填写"0"即可。

2 Modbus 通讯(填表方式)

Modbus RTU 通讯设置软件下载: modbus_edit(右键点击下载)

http://www.dl-winbest.com/download/modbus_edit.rar

下面为 Modbus 命令从上往下循环执行的方式示意图:

	按序号从上往下循环执行modbus命令
序号	modbus命令
0	01读取线圈 0xxxx; 从站1; 起始地址0; 个数1; Ⅴ区地址0; 位:0; 命令执行前延时ms:0
1	02读取输入状态 1xxxx: 从站1;起始地址3;个数1; V区地址1;位:1;命令执行前延时ms:0
2	03读保持寄存器 4xxxx; 从站1; 起始地址6; 个数10; Ⅴ区地址100; 命令执行前延时ms:0
3	04读输入寄存器 3xxxx: 从站1:起始地址12: 个数5: V区地址200: 命令执行前延时ms:0
4	05写单个线圈 0xxxx:从站2;起始地址18; 个数1; Ⅴ区地址300;位:5;循环写; 命令执行前延时ms:0
5	06写单个寄存器 4xxxx:从站3;起始地址77:个数1: Ⅴ区地址500; 变化写:命令执行前延时ms:0
6	15写多个线圈 Oxxxx: 从站5: 起始地址33: 个数16: Ⅴ区地址600: 位:5: 循环写: 命令执行前延时ms:0
7	16与多个寄存器 4xxxx: 从站6:起始地址88: 个数6: Ⅴ区地址700: 循环与: 命令执行前延时ms:0
8	DoubleClick here
9	DoubleClick here
10	DoubleClick here
11	DoubleClick here
12	DoubleClick here
13	
15	
16	DubleClick here
17	DoubleClick here
18	DoubleClick here
19	DoubleClick here
20	DoubleClick here
<	>
	Д Х

下图是 Modbus 作为从站功能的相关设置参数:

᠃ 大连德売 Modbus RTU 通讯设置软件 File Ⅱ 上传modbus组态到电脑	≠ v1.2 下载modbus组态到硬件	⊧ ∥ 徳嘉	硬件设置 帮助	
德嘉设备或 PLC 的 IP地址:	192 168 1	10	自动获取(网络中只有	一个设备)
◎ 无效	© modbus主站功	伯告	[®] modbus∦	站功能
波特率: 9600 -		校验:	8位无校验1停止位 No Parity	•
Modbus从站方式:				
从站地址: 1				
Modbus地址 S7-200数据区				
00001-00128 Q0.0-Q15.7 mod	lbus对应地址为: O、1、2、	• • • 128		
10001-10128 IO.0-I15.7 mod	lbus对应地址为: 0、1、2、	。 。 。 128		
30001-30032 AIW0-AIW62 mod	lbus对应地址为: 0、2、4、	。。。62		
40001-4xxxx VW(n)、VW(n+2)	、VW(n+4) modbus对引 shhite 众歌的 动动网络	亚地址为:n 为VWO VWO	、n+1、n+2	
例2: modbus 起始	池址19、个数4 对应的Ⅴ区	/ງ0₩8 、0₩1 为VW19、VW2	0、 0w12 1、 VW23、 VW25	

下图是 Modbus 作为主站(读)功能的相关设置参数:

惠设备或 PLC 的	IP地址: 192	168 1	11	自动获取(网络中只有	有一个设备)
◎ 无效		◎ modbus主站功能	2	🔘 modbush	人站功能
波特率: 9600	*		校验: 8位	立无校验1停止位 No Parity	
命令重发次数:	从站无响应,直接发送	下一条命令	-	等待从站回答时间:	30ms
反 modburg会会					1
 O2读取输入状; DoubleClick 	态 1xxxx: 从站1: 起始 here here here here here here here her	t地址0; 个数123; VE bus 命令行編編 行前延时 ms: 0 号: 100歳は計算研究 地: 1 地: 1 地: 20	≤地址0; 位:0; □ □ 注:通常为□ 4::::::::::::::::::::::::::::::::::::	命令执行前延时ms:0	

下图是 Modbus 作为主站(写)功能的相关设置参数:

ile 上传modl	pus组态到电脑	下載modbus组态到硬件	德嘉硬件设置	帮助	
惠嘉设备或 PLC 的	IP地址:	192 168 1	11	自动获取(网络中只有	有一个设备)
◎ 无效		◎ modbus主站功能		🔘 modbus	山站功能
波特率: 9600	-	杉		佥1停止位 No Parity	
命令重发次数:	从站无响应,直接	发送下一条命令	 ▼ ₹ 	穿待从站回答时间:	30m <i>s</i>
 1 05与単个线圈 2 05写単个线圈 3 05写単个线圈 	Uxxxx; 从站1; 起 Oxxxx; 从站1; 起	29 17 11: 12 17 20 11: 12 12 11: 12 12 12: 12:	位:1; 循环与; 俞 位:2; 循环写; 俞	F安矾行前延时ms:O お令执行前延时ms:O	

以两个 PLC 之间的 Modbus 通讯为例, 一个 PLC 做从站, 保持寄存器 4xxxx、从站地址 1、 Modbus 起始地址 0; 一个 PLC 做主站(读)的方式, 功能码为 03 读保持寄存器 4xxxx、从 站地址 1、计数个数 20、V 区起始地址 1000, 监控数据如下:

查看(V) PLC(P) 调试(D)	工具(T) 窗口(W)	帮助(H)		
1 X 🖻 🖻 🗠 🗹 🖸	r 📥 💻 🛛 🕸 🖈		~ ~] 찌 ఐ 찌 태 ศ	12 12 12 12 12 12 12 12 12 12 12 12 12 1
a 🔺 🛠 🛠 📰 🖭] → + + →	-++-() -[]		
圖 项目1	2			. 5 6 7 .
	地址	格式	当前值	新值
	1 VW0	有符号	+1234	
	2 VW2	有符号	+5678	
	3 VW4	有符号	+66	
也"" <u>山</u> 朳心表	4 VW6	有符号	+88	
古 100 安然地	5 VW8	有符号	+123	从站数据
「「「」「「」「「」」「「」」「「」」「」」「「」」「」」「」」「」「」」「」	6 VW10	有符号	+456	77.24 32.10
	7 VW12	有符号	+789	
「「「」」の通信	8 VW14	有符号	+0	
砂 通信 副 沿罢 PG/PC 按口	9	有符号		
	10	有符号		
	11	有符号		
	12	有符号		
			4	. 5 6
	地址	: 格式	当前值	新值
	1 VW1000	有符号	+1234	
日 🛄 柱序状	2 VW1002	有符号	+5678	
	3 VW1004	有符号	+66	
南高 新堀中	4 VW1006		+88	
	5 VW1008		+123	主站读过来的数据
中国 示规风	6 VW1010		+456	
	7 VW1012	有符号	+789	
	8 VW1014	有符号	+0	
·····································	9	有符号		
	10	有符号		
	11	有符号		
山雪工具	12	有付号		

可见已经完成了 Modbus 的通讯。

大连德嘉工控设备有限公司最新出品的 H05 高档型 PLC,该产品具有以下特点:

- 对比 M02 型 CPU 增加了与西门子 S7-300、S7-1200 通讯的功能。
- 该产品具有 6 个 DI 通道和 6 个 DO 通道(输入输出通道与主板光电隔离)。
- 可以外接7个扩展模块(DI 128 路; D0 128 路; AI 32 路; AQ 32 路, 扩展模块可以使用 大连德嘉的 I0 模块,也可以使用西门子原装的 I0 模块,甚至还可以使用其他品牌的西门 子 200 兼容型模块)。
- 可以使用西门子 S7-200 STEP7-MicroWin 编程软件,与西门子 S7-200 完全兼容;它可以使用 MicroWin 英文环境,即在其他语言环境下也可以在线编程、下载调试,解决了 S7-200 CN 型 PLC 只能使用中文的限制,这样当出口到其他国家时可以使用英文、德文、西班牙文、法文、意大利语,而且在我们的网口设置页面中,设置了中英文俩种界面供选择,这样外国朋友也可以使用了。

- 具有 Modbus TCP, S7-200 TCP, S7-300 TCP 协议,可以与 99.9%的上位机相连接
- 可以实现 PLC 之间的通讯(包括 S7-200 SMART、 CP243-1、CP243i、CP243-ibus、
 S7-300、S7-1200、S7-1500,使用的是 S7 PUT/GET 命令)
- 具有自由口通讯功能,如 Modbus RTU 主站、从站,USS 变频器通讯等
- 适用于 C++、delphi、C#、VB 等高级语言编程通讯(使用 Modbus TCP 协议)
- 可以连接西门子精彩系列 SMART LINE 触摸屏(Smart 1000IE 和 Smart 700IE)
- 具有 PID 功能(但暂不支持参数自整定)。

目前它取消了2个命令:

- (1) PLS: 脉冲输出和脉冲计数输出
- (2) HSC: 高速脉冲计数指令

它带有以太网口,可以通过网口进行编程下载、上传程序,也可以在线监控调试,可以通过网口 连接组态王、力控、直连 Wincc(可以不通过 PC Access)。也可以通过 PLC 上的 PPI 口进行 编程、下载、上传程序,也可以通过 PPI 口连接组态王、力控、的 PLC 运行速度经过实际测量 是西门子的 3 倍

断电保持寄存器的有效范围对 V 区做了缩减,只可以对 VB0-VB2499 具有断电保持功能,而大于 VB2499 部分则没有断电保持功能。西门子目前正推 S7-200 SMART,其实就是带网口的 200PLC,你还要重新熟悉它的编程界面,和新的知识点,而如果您使用我们的 PLC 就不浪费时间了,一切都是如此的熟悉,没有一丝的不同。

3 参数设置

I/0 接线





4 MicroWin 连接设置

1. 打开 MicroWin,双击[设置 PG/PC 接口],选择如下图驱动(网卡名.TCPIP.1),选好后点 击确定.



2. 在下图中双击[通信],在"远程:"框中填入该 CPU 的 IP 地址,如 192.168.1.10,然后 点击确认

也址 ————		Dealert DOL: ODE Family Converter T
主机:	TJI-20140101SPKI	■ Featter PCIe GBE Family Controller. It
远程:	192 . 168 . 1 . 10	CPU 226 CN REL 02.01
PLC 类型:	CPU 226 CN REL 02.01	
☑ 随项目保存设置		Perch.
网络参数		
接口:	Realtek PCIe GBE Family Controller.TCPIP.2	
协议:	TCP/IP	
车接超时		
输入接收数据超时8 时数值。	时间。通信负荷大的连接可能需要较大的超	
超时时间:	3 秒	
	1	

MicroWin 设置完毕,现在就可以用 MicroWin 对大连德嘉该 PLC 进行编程了!

	2 3 1 4 1 5 1 1	6 7 8	9 10	11 • • • 12 • • • 13 • • • 14 • • •	·15·
2 新時性	符号		数据类型	i i i i i i i i i i i i i i i i i i i	主释
- CPU 224 REL 01.2	2	TEMP			
		TEMP			
		TEMP			
田 田 状态表 取 新	FIX FIX A	TEMP			
日日 数据块 早为	02 01				
	程序注释				
⊡ 🔗 通信	DT C SEAM				
	PLC 英奎				
■■「工具	选择 CPH 类型和版本:	加果您希望软件检查	PIC 的存储区	范围参数,请选	
日 日 指令		NONCOMPACT OF THE	A THO HOLD HERE		
	↓ 「				
▲ 13、	择从 PLC 读取。				
● 通 收藏夹 ● ● ● 位逻辑	择从卫士读取。		1.2		
□ • · · · · · · · · · · · · · · · · · ·	择从 PLL 读取。	11. 224		ŧприс	
 □ □	择从 PLL 读取。 PLL 类型	V 224	Ji	卖取 PLC	
□ 18 w	择从 PLL 读取。 PLC 类型 CPV 版本 01	V 224 .22	<u>ם</u>	卖取 PLC	
□ 18 w 收藏夹 □ ① 位逻辑 □ ③ 时钟 □ 2 通信 □ 3 比较 □ ④ 转换	择从 PLL 读取。 PLC 类型 CPV 版本 01	U 224 . 22	• •	卖取 PLC	
 □ 18、 收藏夹 □ 位逻辑 □ 回 时钟 □ 2 通信 □ 3 比较 □ 1 較 □ 1 較 □ 1 較 □ 1 較 	择从 PLL 读取。 PLC 类型 CPV 版本 01	U 224 . 22	 ↓ ↓	卖取 PLC 通信	
 ● 18 w 成 表 平 ● 10 w 成 表 平 ● 10 回 时 中 ● 2 通信 ● 2 通信	择从 PLL 读取。 PLC 类型 CPV 版本 01	V 224 . 22	 ↓ ↓	卖取 PLC 通信 」取消	
 ● 18 收藏夹 ● 10 位逻辑 ● 10 时钟 ● 2 通信 ● 3 括換 ● 1 计数器 ● 1 计数器 ● 1 評素 	择从 PLL 读取。 PLC 类型 CPV 版本 01	U 224 . 22	▼i ▼ 确认	奏取 PLC	
 ● 18 w 收藏夹 ● 10 位逻辑 ● 10 0 时钟 ● 2 通信 ● 3 比较 ● 3 转换 ● 1 计数器 ● 1 计数器 ● 1 整数计算 ● 1 型 数计算 	择从 PLL 读取。 PLC 类型 CPV 版本 OI	U 224 .22 所版版太号头	▼ ■ → → → → → → → → → → → → →	奏取 PLC 通信	
 ▲ 18 收藏夹 ● 位逻辑 ● 位逻辑 ● 位 逻辑 ● ④ 时钟 ● 2 通信 ● ④ 比较 ● ● 计数器 ● ● 计数器 ● ● 注 建数计算 ● ● 整数计算 ● ● 整数计算 ● ● 2 逻辑运算 	FLC 类型 CPU 版本 CPU 版本	^{U 224} .22 所版版本号头	・ ・ · · · · · · · · · · · · · · · · · ·	奏取 PLC 通信	
 ▲ 18 × 收藏夹 ● 位逻辑 ● 位逻辑 ● 回 时钟 ● 2 通信 ● 3 转换 ● 1 计数器 ● 1 计数器 ● 1 建数计算 	择从 PLL 读取。 PLC 类型 CPV 版本 01	^{U 224} .22 所版版本号头	・ ・ · · · · · · · · · · · · · · · · · ·	奏取 PLC 通信	
 ▲ 18× 收藏夹 ● 位逻辑 ● 位逻辑 ● 回 时钟 ● 2 通信 ● 3 送比较 ● 1 计数器 ● 1 计数器 ● 1 評 2 認数计算 ● 1 整数计算 ● 1 建基式算 ● 1 逻辑运算 ● 1 建序控制 	择从 PLL 读取。 PLC 类型 CPV 版本 O1 最新	U 224 .22 所版版本号头	▼ → → → → → → → → → → → → →	奏取 PLC 通信	

注意事项:下载项目时,一定要注意 PLC 的型号,如图:

1. 这个型号必须是 CPU 224REL 01.22,如果不是请右键 PLC 型号选择类型改成如图型号。如 果型号不符时点击下载会出现如图提示:

		符号	· 变量类型	数据类型		注释
CPU 224 REL 0	2.01		TEMP			
1 程序块			TEMP	1		
3 符号表	-1:40					
	L. JEY					Ľ
▋ 叙绪获 副 系統地	与四十回酒也	的出于固许接				
≝ ਨਾਸ਼ਨ ਙੇ ਨੇ⊽ਟੀਬ	信用"法顶"	拉切选择雪面了 <u>新</u> 有	ዕቶቱ			
2 通信	DC/T3 (22-90)	12011201年市3211年6月	94 7 .0			
1 向导						
算工具	远程 II	P 地址: 192.168.1.	12			CPU 224 REL 01.22
皆令	-					
🗑 收藏夹	1 項目中	的 PLC 类型 (CPU :	224 REL 02.01) 按钮、设置项目	与远程 PLC 类	² 型(CPU 224 REL 01.22) 文字記録 PLC 相対	
🖬 位逻辑	••••••••••••••••••••••••••••••••••••••	半山 以4000日 :		Th 天空,使	C-J/241 ILC (TAN):	
回 时钟						
☑ 通信						
		14				
■ \$154 (四)		1			2	
11 11 叙喆 词 沒占数计質	洗顶 ♠	おから	18 I		下載	取消
· 敷粉计管					1 +4	
前中新						
。 逻辑运算	一 把床抽			— — —	200	
▲ 传送	▶ 柱序块				rLL NG	
〒 程序控制	▼ 数据块			<u>王</u> 、[云、ī		
副移位/循环	▶ 秋玩妖			±.1	:ш.	
💼 字符串	「私保はみ	28				
画 表	T SKIN DR. SK	aue.				
<u>る</u> 定时器						
四月 二月				区成	叻后关闭对话框	
🖬 调用于程序	0	and the second second	1.	▼ 提注	示从 RUN 到 STOP 模式转	换
	自主な	取帮助和支:	择	☑ 提:	示从 STOP 到 RIN 模式转	拉
	U M			14 1/6/	2 Obt prov 303 more 1965r045	

这里请选择改动项目, 然后再点击下载即可。如果没有点击改动项目直接下载则可能出现如图情况:

	¥0,80,4×		
就请求的命令而言,PLI	· · · · · · · · · · · · · · · · · · ·		
	5G9 「	确认 取消	取消
左项 ▼ 程序快 ▼ 数据快 ▼ 系统快 ■ 配方 ■ 数据记录配置		至 : FLC 至 : FLC 至 : FLC 至 : FLC	
■ HC/J ■ 数据记录配置 ● ★ ★ ★ HE M RL 40-		▼ 成功后关闭对话框 ▼ 提示从 RUM 到 STOP 模:	式转换

此时我们需要清除 PLC 如图:

使用"选项"按钮选择需要清除	的块和/或存储卡项目。		
远程 IP 地址: 192.168.1	. 12		
悠无法撤销清除操作。若同 会清除密码信息、M 存储 合	同时选择程序块、数据块和系 ≤、断电保持存储区和强制数	统块,则除清除这三者 据。	
选项 ★		2 	取消
选项 ✓ 程序块 ✓ 数据块 ✓ 系统块 「 配方	目# 日# 日#	示 : PLC 示 : PLC 示 : PLC 示 : PLC	

先选择 PLC 中的清除选项,出现如图界面点击清除即可。

当然,我们也可以使用 ie 浏览器中的网页来清除 PLC

首先我们在 IE 浏览器地址栏中输入 192.168.1.222 (这个是后门地址,并不是实际地址,仅用于设置参数)进入设置界面:



这里是语言选项,我们选择 Chinese,进入下一界面:



请按照这三步操作: 首先, 如果 PLC 没有停止, 则先选择 STOP PLC:

	STOP PLC
请先输入验证码: 000 (888) 然后再按==> 确定 取消 取消	
	返回
	Release:20160612

输入验证码 888 后点击确定即可。之后在上一界面选择清空 PLC:

	清空PLC
只有当PLC处于STOP状态时,才可以清空PLC,该操作可影响IO输出,请慎重! 注:PLC一旦清空,PLC的程序块、数据块、系统块就回到初始值,即出厂状态	
请先输入验证码: 000 (777) 然后再按==> 确定 取消	
	返回

输入 777 后点击确定即可。清空后可能会使 PLC 的 IP 清零,我们需要重新进入设置页面设置 IP 地址:

PLC IP SET			
请输入PLC 的IP: 000 000 000 000 每一项[000-255]			
确定取消			
返回			
International Electronic Version			
Release:20160612			

这里它的段址一定要与相连的计算机相同即前三项相同第四相不同。

- 例一: 计算机 IP(192.168.1.100), 掩码(255.255.255.0), 网关(192.168.1.1), PLC
 - 的 IP(192.168.1.10)。
- 注:参数设置提交后,最好在 cmd 窗口键入 arp -d (删除计算机中已保留的 IP/MAC 表),以便 PLC 新改动的 IP/MAC 与老地址无冲突 。

5 WinCC 连接设置(以 WinCC7.3 为例)

1. 打开 Wincc,双击变量管理,打开变量管理器,添加驱动:





2. 填右键单击变量管理,在弹出的菜单中选择添加驱动,SIMATIC S7 Protocol Suite,如下 图所示



3. 添加好驱动之后,右键单击 SIMATIC S7 Protocol Suite 下的 TCP/IP,在弹出的菜单中选择系统参数



4. 在弹出的对话框中点击单位选项卡

IMATIC S7 月期管理 「通过 PLC	✓ 更改驱动的传输	
📝 激活 (A)	60 间隙(I)	30 超时间隙(I)
- ─CPV 停机监控		
📝 激活 (E)		
在 AS 中通道使	用了周期读服务。	
785	五 [m涨]	 ≢¤8h

5. 在逻辑设备名称选框中选择驱动为: 网卡名. TCPIP. 1

SIMALIC SI TIX	
选择逻辑设备名称	
였 类型/总线配置文	TCP/IP
逻辑设备名称 (2):	amily Controller TCPIP 1 👻
☑ 自主前设常(A) 作业处理	
TETTAGE	
🗐 写 (带优先权) 🕊)	
🔤 写 (带优先权) 🕊)	

如何查看网卡名:点击屏幕右下角的电脑图标,选择打开网络和共享中心



在网络共享中心中点击本地连接

查看基本网络信息并设置连接		
in an	🍥	查看完整映射
🐝 TJ-20140101SPKI 网络 (此计算机)	2 Internet	
查看活动网络		
网络 2 家庭网络	访问类型: Internet 家庭组: 已加入 连接: ♀ 本地连接 2	
更改网络设置		
设置新的连接或网络 设置无线、宽带、拨号、临时或 VPN 连	接;或设置路由器或访问点。	
连接到网络 连接到或重新连接到无线、有线、拨号或	t VPN 网络连接。	
送择家庭组和共享选项 访问位于其他网络计算机上的文件和打印	7机,或更改共享设置。	
疑难解答 诊断并修复网络问题,或获得故障排除信	息。	

在弹出的对话框中点击详细信息

规	
连接 一	
IPv4 连接:	Internet
IPv6 连接:	无 Internet 访问权限
媒体状态:	已启用
持续时间:	05:36:24
· · · · · · · · · · · · · · · · · · ·	
▲300. 详细信息	(E)
正 ¹ 夏: 详细信息 舌动	(8) (8) 已发送 — 【算》 — 已接收
	BOD. 0 maps BOD. 0 maps BOD. 0 maps BOD. 0 maps CE CE CE CE CE CE CE CE CE CE

下图中的描述内容就是你的网卡名

届时	值
	IA
	P LAI DOT OPP P
加速	Realter file OBL Family Controll
初理地址	60-45-CB-89-21-14
已启用 DHCP	8
IPv4 地址	
IPv4 子网掩码	
IPv4 默认网关	
IPv4 DNS 服务器	
IPv4 WINS 服务器	
已启用 NetBIOS ove	문
连接-本地 IPv6 地址	
TPv6 野社网关	
TPv6 DNS 服务哭	
1110 Date (1007) 68	
x [

6. 再回到变量管理器中,右键点击 TCP/IP,选择新建连接,在 TCP/IP 选项下会生成一个名为 NewConnection_1 的新连接选项。





7. 右键单击 NewConnection_1, 在弹出的菜单中选择



8. 在弹出的对话框中填写 MO2 的 IP 地址, 192.168.1.10

S(网络地址 IP 地址(I):	192.168.1.10	
机架号(B):	0	
插槽号(E):	0	
🔲 发送/接收原始数	刘据块 创)	
连接资源 (C):	02	

现在连接已经建立成功,已经可以建立变量和画面了。

6 组态王连接设置

1. 打开组态王开发软件,选择设备→COM1



2. 双击"新建",选择 S7-200 系列(TCP)→TCP

亩 S5系列	
⊕ S7-1200	
⊕ ST-200 (MF1) ⊕ ST-200 (ST)	
E- 57-200 (TCP)	
TCP	1
由. S7-200系列 由. S7-200系列(0P)	-
由 S7-200系列(USB)	
⊕ S7-300 (MPI)	
i i (#)- \$7=300 (\$7.)	
\$所达的设备 - 会广宏, 再门了	
:广」外: 四日子 いるな好。 c7_000 (707)	
(首名称: S1-200(UCF)	
	 B. S5条列 B. S7-1200 B. S7-200 (MPI) B. S7-200 (S7) C. S7-200 (CP) C. S7-200系列 B. S7-200系列 (USB) B. S7-200系列 (USB) B. S7-300 (MPI) H. S7-300 (S7)

3. 选择 com 口号,此处选择默认值 com2

设备配置向导—	—选择串口号		×
		你所选择的为串行设备,请选择与 设备所连接的串口。 COM2 使用虚拟串口(GPRS设备) KVCOM1 使用哪个虚拟串口没有限制,但是每 个虚拟串口只能定义同一类型的设备。	
6		〈上一步(8)下一步(8)〉 耳	则消

4. 单击"下一步",输入要安装的设备的逻辑名称

-		请给要安装的设备指定唯-	的逻辑名称
	B	┏ 指定冗余设备	

5. 再单击"下一步",输入设备的 IP 地址及相对于 PLC 的位置

设备配置向导——设备地划	设置指南	X
	在这一步,请为要安装的设备指定地址。 使用默认值或技地址帮助按钮取得设备地 业帮助信息。 192.168.1.10:0 地址帮助 你所指定的设备地址必 须在32个字节以内。	
	< 上一步 (B) 下一步 (B) > 取消	肖 <u></u>

6. 再单击"下一步",保持默认值,直接单击"下一步"

 尝试恢复间隔:	
最长恢复时间:	
24 小时	
▶ 使用动态优化	

7. 单击"完成",就配置了一个"TCP"设备。

	你朋友女装的设备信息:
	└ 设备信息
	新设备为 西门子 生产的 S7-200(TCP)
	、
	反审逻辑-石: 利10 反笛
and the second s	设备地址:192.168.1.10:0
	通讯万式: TCP
	▶ 自动建变里

至此,就完成了 PLC 与组态王的连接。

7 力控连接设置

1. 打开组态软件,进入开发系统,打开"I0设备组态"->"PLC"->"SIEMENS"->"S7-200 TCP 协议",画面如下:



 第一步:基本参数配置,定义设备名称,修改更新周期。(更新周期一定要修改为250毫 秒以上!)

	设备名称: DO1	
	设备描述:	
S.	更新周期: 250	臺秒 ▼
	超时时间: 3	秒 🔻
	设备地址: 通信方式: TCP/IP网络	•
	故障后恢复查询 周期:300 秒 🗌 最大时都	限: ⁶⁰ 分钟
	☑ 独占通道	高级

3. 第二步:通讯参数。设备 IP 地址: 192.168.1.10,端口号: 102

	设备IP地址: 192.16	68.1.10 端口: 102
IR	□ 启用备用通道 备用III地址:	
	□ 王逋迴恢复后自动回 □ 本机网卡冗余 本机网卡IP地址:	
	备用网卡IP地址:	端口: 0 次后重新初始化链接

4. 点击完成,现在你的 PLC 可以与力控软件连接了。

 TSAP (PLC):	10.00	
TSAP (PC):	10.11	

8 连接 SMART LINE 参数设置

1、在触摸屏上设置好触摸屏的 IP 地址,如 192.168.1.200

2、在 SIMATIC WinCC flexible 2008, 给触摸屏编程, 如下图所示

称	通讯驱动程序	在线	注释	
[接_1	SIMATIC S7 200	▼ 开	-	
9 区域指	针			
数 区域指 Smart 10	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			Station
B 区域推 Smart 10	(計) 00 IE 援口 以太网			Station
Smart 10) (00 IE () (以太网) () () () () () () () () () () () () ()	▼		Station 「」」 PLC 设备
& 区域指 Smart 10	除計 00 IE 接口 以太网 ₩₩	▼		Station 加加 PLC 设备 地址
数 区域指 Smart 10 受型 ⊙ IP ○ ISO	将 00 IE 接口 以太网 ₩1 192, 168, 001, 200	▼ I 设备		Station 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章
数 区域指 Smart 10 ● IP ● ISO	特 00 IE 接口 以太网 以太网 192、168、001、200 只能在设备上组态地址	▼		Station 「「」」 「」」 「」」 「」」 「」」 「」」 「」」 「

9 Modbus 通讯(梯形图方式)

想要进行 modbus 通讯必须安装 modbus 指令库,指令库大家可以网上下载一个,这里就不提供了。

接线:本例是在两个 **S7-200 CPU** 的 **PORT 0** 口进行的 **modbus** 通讯,两个 **CPU** 的 **PORT 0** 口 通过 PPI 电缆进行连接(电缆的针脚连接为 3, 5, 8)。

这个例子能实现的功能是读取从站 40001 地址开始的 10 个字,存到主站 VB400 开始的 10 个字。

主站程序如下:

网络 1	网络标题
初始化	Modbus 主站通信,
EN	使能:必须保证每一扫描周期都被使能(使用SM0.0)
Mode	模式:常为1,使能 Modbus 协议功能;为0 时恢复为系统 PPI 协议
Baud	波特率:设为9600,要与从站波特率对应
Parity	校验:校验方式选择 0= 无校验
Timeou	t 超时:主站等待从站响应的时间,以毫秒为单位,典型的设置值为1000毫秒(1秒), 允许设置的范围为1-32767。 注意: 这个值必须设置足够大以保证从站有时间响应。
Done	完成位:初始化完成,此位会自动置1。可以用该位启动 MBUS_MSG 读写操作
Error	初始化错误代码(只有在 Done 位为1时有效):0= 无错误 1= 校验选择非法 2= 波特率选择非法 3= 模式选择非法
SN 	40.0 MBUS_CTRL EN 40.0
	Mode
	9600- Baud Done - V0.0 0- Parity Error - VB1 +1000- Timeout

读取从站	保持寄存器的数据
EN	使能:同一时刻只能有一个读写功能(即 MBUS_MSG)使能 注意:建议每一个读写功能(即 MBUS_MSG)都用上一个 MBUS_MSG 指令的 Done 完成位来激 活,以保证所有读写指令循环进行(见程序)。
First	读写请求位:每一个新的读写请求必须使用脉冲触发
Slave	从站地址:可选择的范围 1-247
RW	读写操作: 0=读, 1=写 注意:1.开关量输出和保持寄存器支持读和写功能 2.开关量输入和模拟量输入只支持读功能
Addr	读写从站的数据地址:选择读写的数据类型 00001至0xxxx- 开关量输出 10001至1xxxx- 开关量输入 30001至3xxxx- 模拟量输入 40001至4xxxx- 保持寄存器
Count	通讯的数据个数(位或字的个数) 注意: Modbus主站可读/写的最大数据量为120个字(是指每一个 MBUS_MSG 指令)
DataPtr	数据指针:1.如果是读指令,读回的数据放到这个数据区中 2.如果是写指令,要写出的数据放到这个数据区中
Done	读写功能完成位
	 3= 接收超时(从站无响应) 4= 请求参数错误(slave address,Modbus address,count,RW) 5= Modbus/自由口未使能 6= Modbus正在忙于其它请求 7= 响应错误(响应不是请求的操作) 8= 响应CRC校验和错误 101= 从站不支持诸求的功能 102= 从站不支持散据地址 103= 从站不支持此种数据类型 104= 从站设备故障 105= 从站接受了信息,但是响应被延迟 106= 从站忙,拒绝了信息 108= 从站存储器奇偶错误
常见的错	误及其错误代码:
1. 如果多	个 MBUS_MSG 指令同时使能会造成6号错误
2. 从站 d	elay参数设的时间过长会造成3号错误
3. 从站挡	电或不运行,网络故障都会造成3号错误
SMO	.5MBUS_MSG
	EN
зма —	1.5 First
	3-Slave Done-V0.1
	0- RW Error-VB2
	40001 - Addr
	510 Control

我们要注意的是需要分配库存储区地址,如下图:



这段寄存器地址不能再被程序中的任何指令使用,包括 MBUS_INIT 和 MBUS_SLAVE 指令在内。

从站程序如下:

网络 1 网络标题 在第一个循环周期内初始化Modbus从站协议
 Mode:
 模式选择,启动/停止MODBUS,1=启动;0=停止

 Address:
 从站地址,MODBUS从站地址,取值1~247

 Baud:
 波特率,可选1200,2400,4800,9600,19200,38400,57600,115200

 Parity:
 奇偶校验,0=无校验;1=奇校验;2=偶校验

 Delay:
 延时,附加字符间延时,缺省值为0

 MaxIQ:
 最大I/Q位,参与通信的最大I/0点数,S7-200的I/0映像区为128/128,缺省值为128

 MaxAI:
 最大AF字数,参与通信的最大AI通道数,可为16或32

 MaxHold:
 最大保持寄存器区,参与通信的V存储区字(VW)

 HoldStart:
 保持寄存器区起始地址,以&VBx指定(间接寻址方式)
 初始化完成标志,成功初始化后置1 初始化错误代码 Done: Error: 在本例子中,设置从站地址为3 Port0 通讯波特率为9600 无校验 口以使用的S7-200最大数字量输入输出点数为128 可以使用的S7-200最大模拟量输入寄存器字数为32 可以使用的V区寄存器地址字数为100,起始地址为VB1000 注意:本例子中,Modbus RTU 从站指令使用的库存储为VB0---VB779,这段寄存器地址不能再被程序中的任何指 令使用,包括MBUS_INIT 和 MBUS_SLAVE 指令在内 First_Scan~:SM0.1 MBUS_INIT EN 1-Mode Done - M10.1 3-Addr Error MB11 9600 - Baud 0-Parity 0-Delay 128 - MaxIQ 16-MaxAl 100-MaxHold &VB1000-HoldSt~ 网络 2 在每个循环周期内执行 Modbus 从站协议 Done: MODBUS执行,通信中时置1,无 MODBUS 通信活动时为0 Error: 错误代码: 0=无错误 MBUS_SLAVE Always_On:SM0.0 EN Done M10.2 Error - MB12

同样,从站也需要分配库存储区。之后把程序编译下载运行,这里我们给从站 VB1000 开始的 20 个字节赋值如下:

1	地址	格式	当前值
1	VB1000	无符号	1
2	VB1001	无符号	2
3	VB1002	无符号	3
4	VB1003	无符号	4
5	VB1004	无符号	5
6	VB1005	无符号	6
7	VB1006	无符号	7
8	VB1007	无符号	8
9	VB1008	无符号	9
10	VB1009	无符号	10
11	VB1010	无符号	11
12	VB1011	无符号	12
13	VB1012	无符号	13
14	VB1013	无符号	14
15	VB1014	无符号	15
16	VB1015	无符号	16
17	VB1016	无符号	17
18	VB1017	无符号	18
19	VB1018	无符号	19
20	VB1019	无符号	20
21	1	有符号	
_		The second se	

然后可以观察到主站 VB400 开始的 20 个字节如下:

	地址	格式	当前值	
1	VB400	无符号	1	
2	VB401	无符号	2	
3	VB402	无符号	3	- II
4	VB403	无符号	4	
5	VB404	无符号	5	
6	VB405	无符号	6	
7	VB406	无符号	7	
8	VB407	无符号	8	
9	VB408	无符号	9	
10	VB409	无符号	10	
11	VB410	无符号	11	
12	VB411	无符号	12	1
13	VB412	无符号	13	1
14	VB413	无符号	14	
15	VB414	无符号	15	
16	VB415	无符号	16	
17	VB416	无符号	17	
18	VB417	无符号	18	1
19	VB418	无符号	19	
20	VB419	无符号	20	
21		有符号		
22		有符号		

这就是一个简单的 200 之间的 modbus 通讯。下面我们在两台 PLC 中间加一个 USB 转 485 串口监 视器,然后我们用串口调试助手可以看到例子执行时的请求码和响应码。

🔤 友善串口调试助手																							E	.][
文件(2) 編辑(2) 祝田(2) :	T具0		帮助	00	1	e e	+	1	2																
申口设置 申□Prolifi(COM3)♥ 波特率 9600 ♥ 数据位 8 ♥ 校验位 Fone ♥ 停止位 1 ♥ 流 控 Wone ♥	03 03 05 05 05 05 05	03 03 10 03 10 03 10	00 14 00 11 00 11 00 11	00 01 00 12 00 12 00 12	00 02 00 13 00 13 00 13	0A 03 0A 14 0A 14 0A 14	C4 04 C4 CE C4 CE C4 CE	2F 05 2F 6E 2F 6E 2F 6E	06 03 03	07 03 03 03	08 14 14 14	89 81 81 81	0A 02 02	0B 03 03	0C 04 04	00 05 05	0E 06 06	0F 07 07	10 08 08	11 09 09	12 0A 0A	13 08 08 08	14 0C 0C	CE OD OD	6E 0E 0E
接收设置 ASCII ③ Hex 9 自动换行 显示发送 显示时间 发送设置 ④ ASCII ③ Hex																								发送	
□ 重复双达 1000 ♥ ms COM3 OPENED, 9500, 8, NONE, 1,	OFF	1	Rx :	132	Byte	es			T	x: 0	Byt	e 5			1										~

图中第一行为请求码,下面讲一下这个码是怎么来的。 我们例子中使用的是 03 功能码(读保持寄存器):

请求

功能码	1个字节	0x03	
起始地址	2 个字节	0x0000 至 0xFFFF	
寄存器数量	2 个字节	1至125 (0x7D)	

响应

功能码	1个字节	0x03	
字节数	1个字节	2×N*	
寄存器值	N*×2个字节		

*N=寄存器的数量

首先是请求: 03 03 00 00 00 0A C4 2F

03 为串口号, 接的是 COM 3 03 为功能码 00 00 为起始地址即 40001 00 0A 为寄存器数量, 读 10 个字 C4 2F 为 CRC 校验码

响应: 03 03 14 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0F 10 11 12 13 14 CE 6E 03 为串口号 03 为功能码 14 为字节数,一共 20 个字节 01~14 为寄存器中的值 CE 6E 为 CRC 校验码

10 PLC 之间通讯设置

此产品可以实现西门子 CP243-1,大连德嘉的 CP243i, CP243-ibus, ETH-PPI, ETH-ibus, 还有西门子 S7-200 SMART、S7-300、S7-1200、S7-1500 之间的通讯。

注: 在 S7-1200/S7-1500 的编程软件 Portal 中,初始定义 DB 块时, 【仅符号访问】的选项不 要打对号"v"

项	目(P) 编辑(E) 视图(V) 插入() 在约	銭(O) 选项(N X の生で	り 工具(1) ト ± □□		•	Totally I	ntegra	ted Automation PORT	AL
	项目树		C AC/DC/	Rly] > 程序	央 → Data_bl	ock_1 [DB1]	_ 7	=×	任务 🔳 🗉	
	设备								选件	1
	B 0 0	<u>ل</u>	ý 🖗 🔩							日田
			Data_b	lock_1					∨ 查找和替换	AD.
	PLC_1 [CPU 1214C A	C/DC/Rly]	名称		数据:	类型	偏移量	启动		
等			1 🕣 🕶 S	tatic		5				臣
PL	◎ 任我和诊断		2	data_time	DIL	Ľ	0.0	DIG		
	■ 添加新块									
	💶 Main [OB1]									
	Data_block_1			1					在子结构中查排	
	▶ 📷 糸鏡块	1177	7701	-					在隐藏文本中到	
	▶ 扁 外部源文件	血1%1直印状		_					一使用通配符	
	▶ 📮 PLC 变量	将快照111	习起馆值●						使用正则表达;	
	▶ 📠 PLC 数据类型	10日間(1)	Ctrl+X Ctrl+C						○ 整个文档	=
	▶ ■ 监控与强制表 Traces	■ 复酌(P)	Ctrl+V					-	⊙ 从当前位置开	
	■ Haces ■ 程序信息	1 复制为文本	格式 (X)						○ 选择	
	▶ 🖀 设备代理数据	★ 删除(D)	Del	_						
	国 文本列表	重命名(N)	F2	- pro- 100-100-100				>		
	▶ 1 本地模块	编译	,	<u>③</u> 属	生」信息	1 2 诊断				
	□■ 公共叙述 前 文档设置	下载到设备	(L)	连接信	息报警	显示				
	▲ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	● 转到在线(N ● 転到南线(R ● 転到南线(R ● 転到南线(R ● 転回南銭)(R ● 転回気気気気気気気気気気気気気気気気気気気気気気気気気気気気気気気気	I) Ctrl+K	均离线					替换为:	
	,在线访问			■操作 设·	备/模块	报警		详		
	<	「「「「「「「「「」」」 「「」」 「」 「」 「」 「」 「」 」 」 」	((G)	_						<u> </u>
	∨ 详细视图	父父51用信 ★ 交叉引用	l思 Sniπ+F11 F11						∨ 语言和资源	-
		圓 调用结构(C	.)							^
	名称	📃 分配列表(A)						编辑语言:	=
	💷 🕨 data_time		信 ・						中文(中华人民共	
		专有技术保	(护(W)				1			~
		📑 打印(P)	Ctrl+P					>		6 20 - 76
	 Portal 祝图 	▲ 打印预览(\	/)	ita_block_1		✓ 坝目 sī	/-1200 已非	1卅。		
4		风属性	Alt+Enter							

Data_block_1 [DB1] 常規	<
常规 信息 时间戳 编译 保护	属性
了题题了下载但不重新初…	■优化的块访问
< <u> </u>	· · · · · · · · · · · · · · · · · · ·

注: 在博图 V13 中的设备组态---->属性---->连接机制----->允许从远程伙伴(PLC、HMI、OPC、...) 使用 PUT/GET 通讯访问打上勾。如下图所示:



Select Language
Chinese
English
International Electronic Version
ID:H05-20160612-001

1. 首先在 IE 浏览器中输入后门地址 192.168.1.222 进入 H05 PLC 的设置界面。

这里可以选择中英文,我们点击中文进入

2. 选择 PLC 通讯,进入下一界面



H05 高档型 PLC 提供了 6 个通道。

3. 数据通讯设置界面,这里可以选择取数/送数,不进行通讯时选择无效即可。我们只需要填入取/送数的长度,本方地址,对方 PLC 的 IP 以及起始地址,设置起来十分简单。

注意下方说明的地址对应关系。



注意: 传送数据时 H05 高档型 PLC 需要保持运行状态。

11 PLC 之间通讯实例

这是一个 3 个 PLC 之间的通讯,我们从 S7-300 中 DB1.DBW0 数据取出来,存在我们的 H05 的 VW100 中,并将数据送到 S7-1200 的 MW0 中,送到 S7-200 SMART 的 MW0 中。

S7-300的 IP 地址设置为 192.168.1.20 S7-1200的 IP 地址设置为 192.168.1.21 S7-200 SMART 的 IP 地址设置为 192.168.1.22

1. H05 通过网页设置 PLC 之间通讯参数

PLC STATUS : RUN
RUN PLC
STOP PLC
IP 设 置
MAC 设置
PLC 清空
PLC 诊断
PLC 通讯
返回
International Electronic Version Release:20160612

从 S7-300 中取数设置:



将数据送到 S7-1200 的 MW0



C () () http://192.168.1.222/PG1_SET.htm	合 🕁 戀
通道:1 取数或送数	^
·	
○无效 ●送数 ○取数	
取数/送数长度: 002 子节 本万起始地址00100	
対方 PLC IP: 192 168 001 022 [000-255] 記始地地100000	
对方数据区: ○I区 ○Q区 ●M区 ○V区 ○DB块 DB块号[00000]	
对方PLC类型: ●S7-1200 S7-200 smart CP243(remote) OS7-300 OSIEMENS CP243-1-ISO	
返回	
说明. 太古地州 0-10000代書V区(0-10000)	
)光田 中子作用10000-733331(生地区(0-3333))	
况明: 本方地址30000-399991(表1区(0-9999)	
说明:本方地址40000-49999代表Q区(0-9999)	
Release:20160612	· · · · · · · · · · · · · · · · · · ·
	≤ 100% ▼

将数据送到 S7-200SMART 的 MW0 中,与上图 1200 设置(除更改 IP 地址)其它一样

2. 我们首先观察一下 S7-300 中的数据,我们将数据值定义为 FFFF

😅 (edb	1 可访问的节点\pr	-io ONLINE		
地址	名称	类型	初始值	实际值
	0.0 STATO	WORD	W#16#FFFF	V#16#FFFF
<				

3. 再观察一下 S7-1200 的 MW0 的数据值

(T) i	窗口(W) 帮助(H)	「转到在线 💋 转	到离线 🏭 🖪 🚺	* =			
1 🕴	PLC_1 [CPU 1214	IC AC/DC/Rly] 🔸	监控与强制表 🕨	监控表_1			_ # = ×
*	1 10 9, 90 2						
1	名称	地址	显示格式	监视值	修改值	9	注释
	1	96MW0	十六进制 💽	16#FFFF			
		≪忝加>					
	(n) 1 1→	(1) 窗口(W) 帮助(H) 1 PLC_1 [CPU 1214 ● IP IS 月 名 名 1 名称 11 图	 (1) 窗口(W) 帮助(H) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	 (7) 窗口(W) 帮助(H) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	(1) 窗口(W) 帮助(H) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	(1) 窗口(W) 帮助(H) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ 1 > PLC_1 [CPU 1214C AC/DC/Rly] > 监控与强制表 > 监控与强制表 > 监控表_1 ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	(1) 窗口(W) 帮助(H) □ □ □ □ □ □ □ □ □ □ □ PLC_1 [CPU 1214C AC/DC/Rly] > 监控与强制表 > 监控与强制表 > 监控表_1 ジ □ □ ジ □ □ ○ □ □ □ ○ □ □ ジ □ □ ○ □ □ ○ □ □ ○ □ □ ○ □ </td

4. 最后看一下 S7-200 SMART 的 MW0 数据值

态力	图表 - 🎦 - 🔽 🔟	i 🧀 🧷 🔒 📆 🕅 i	<u>a</u> -		
	地址~	格式	当前值	新值	
1	MW0	十六进制	▼ 16#FFFF		
2		有符号			
3		有符号			
1		有符号			
5		有符号	7	11. 	

实现数据的传送就这么简单。

注意:

如果你的 S7-300 有网口,你可以直接使用 PLC 的网口,如果你的 S7-300 没有网口,可以用我们的 ETH-MPI(Smart IE) 增加一个网口 。

12 C# Modbus TCP 通讯实例

这里我只是简单的理解一下 Modbus TCP/IP 协议的内容,就是去掉了 modbus 协议本身的 CRC 校验,增加了 MBAP 报文头。

这里只是简单的理解,深入之后可能会有更多的东西需要学习,但为了可以快速入门,我们先按 照这个思路往下走。

我们首先来看一下, MBAP 报文头都包括了哪些信息和内容

域	长度	描述	客户机	服务器
事务元标识符	2个字节	MODBUS 请求/响 应事务处理的识别 码	客户机启动	服务器从接收的请求中重 新复制
协议标识符	2个字节	0=MODBUS 协议 http://blog.csd	客户机启动 n.net/	服务器从接收的请求中重 新复制
长度	2个字节	以下字节的数量	客户机启动(请 求)	服务器(响应)启动
单元标识符	1个字节	串行链路或其它总 线上连接的远程从 站的识别码	客户机启动	服务器从接收的请求中重 新复制

MBAP 报文头包括下列域:

下面我们再来介绍一下针对我们 PLC 的功能码

1、0x01功能码: 按位读取Q区(线圈)

例:我们来读取从 Q0.0 到 Q0.5 这 6 个线圈

发送码分析:

请求 PDU

功能码	1个字节	0x01
起始地址	2个字节	0x0000 至 0xFFFF
线圈数量	2个字节	1至2000 (0x7D0)

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x01, 0x00, 0x00, 0x00, 0x00, 0x06

接收码分析:

响应 PDU

功能码	1个字节	0x01
字节数	1个字节	N*
线圈状态	N个字节	n=N 或 N+1

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x04, 0x01, 0x01, 0x01, 0x2A

modbus 数据中从左数, 0x01 表示功能码, 0x01 表示 1 个字节数据, 0x2A 表示数据值

把 0x2A 转换为 2 进制为 0010 1010 , 从左数起,前 2 位是补充数据 00,剩下的 101010 表示我 们读取的 Q0.5 到 Q0.0 的状态。

QO. 5----- ON,

- Q0.4 ----- OFF,
- QO. 3-----ON,
- Q0.2----OFF,
- QO. 1-----ON,
- Q0. 0-----OFF.

注意数据的顺序, 左侧是高位, 右侧是低位。

注意:上述发送及接收数据中,红色数码是 MBAP 报文头,黑色码是 modbus 数据, 下同

2、0x02功能码:按位读取 I 区 (离散输入)

例:我们来读取从10.0到10.5这6个离散输入点

发送码分析:

请求 PDU

功能码	1 个字节	0x02
起始地址	2个字节	0x0000至 0xFFFF
输入数量	2 个字节	1至2000 (0x7D0)

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x02, 0x00, 0x00, 0x00, 0x00, 0x06

接收码分析:

响应 PDU

功能码	1个字节	0x82
字节数	1个字节	N*
输入状态	N*×1个字节	

*N=输出数量/8,如果余数不等于0,那么N=N+1

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x04, 0x01, 0x02, 0x01, 0x00

modbus 数据中从左数, 0x02 表示功能码, 0x01 表示 1 个字节数据, 0x00 表示数据值

把 0x0 转换为 2 进制为 0000 0000 , 从左数起,前 2 位是补充数据 00,剩下的 000000 表示我 们读取的 10.5 到 10.0 的状态。

3、0x03功能码: 按双字节(VW)读取 V 区或者读 MW

Modbus 寄存器 0-----19999 是读取 WW

Modbus 寄存器 20000-----20031 是读取 MW

例:我们来读取从 VWO 到 VW2 这个数据

发送码分析:

请求

功能码	1个字节	0x03
起始地址	2 个字节	0x0000 至 0xFFFF
寄存器数量	2 个字节	1至125 (0x7D)

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x03, 0x00, 0x00, 0x00, 0x03

接收码分析:

响应

功能码	1 个 <mark>字节</mark>	0x03
字节数	1 个字节	2×N*
寄存器值	N*×2个字节	

*N=寄存器的数量

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x09, 0x01, 0x03, 0x06, 0x04, 0x00, 0x03, 0x01, 0x02, 0x05

modbus 数据中从左数, 0x03 表示功能码, 0x06 表示 6 个字节数据, 0x04, 0x00, 0x03, 0x01, 0x02, 0x05 表示数据值

VW0 为 0x0400, VW2 为 0x0301, VW4 为 0x0205

4、0x05功能码:按位写Q区

例:我们来把 Q0.0 置 1,请注意,置位数据为 0xFF00,清零数据为 0x0000

发送码分析:

请求

功能码	1 个字节	0x05
输出地址	2个字节	0x0000 至 0xFFFF
输出值	2 个字节	0x0000 至 0x00

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x05, 0x00, 0x00, 0xFF, 0x00

接收码分析:

响应

功能码	1 个字节	0x05
输出地址	2个字节	0x0000至 0xFFFF
输出值	2个字节	0x0000 至 0xFF00

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x05, 0x00, 0x00, 0xFF, 0x00,

5、0x06功能码: 按双字节(VW)写V区或者写MW

Modbus 寄存器 0-----19999 是写 WW

Modbus 寄存器 20000-----20031 是写 MW

例: 我们将数据 0x2636 写入 VW0

发送码分析:

请求

功能码	1 个字节	0x06
寄存器地址	2个字节	0x0000至 0xFFFF
寄存器值	2 个字节	0x0000至 0xFFFF

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x06, 0x00, 0x00, 0x26, 0x36

接收码分析:

响应

功能码	1 个 <mark>字节</mark>	0x06
寄存器地址	2 个字节	0x0000至0xFFFF
寄存器值	2个字节	0x0000至 0xFFFF

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x06, 0x00, 0x00, 0x26, 0x36

6、0x0F功能码: 按多个位写Q区

例: 我们将 Q0.0 到 Q0.5 共 6 个线圈全部置位 1

发送码分析:

请求 PDU

功能码	1个字节	0x0F
起始地址	2个字节	0x0000 至 0xFFFF
输出数量	2 个字节	0x0001至0x07B0
字节数	1个字节	N*
输出值	N *×1个字节	

*N=输出数量/8,如果余数不等于0,那么N=N+1

我们要将 Q0.0 到 Q0.5 输出 1,要发送的值应该为二进制 0011 1111,转换为 16 进制为 0x3F

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x08, 0x01, 0x0F, 0x00, 0x00, 0x00, 0x06, 0x01, 0x3F

接收码分析:

响应 PDU

功能码	1 个字节	0x0F
起始地址	2 个字节	0x0000 至 0xFFFF
输出数量	2 个字节	0x0001至 0x07B0

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x0F, 0x00, 0x00, 0x00, 0x06

7、0x10功能码: 写 2N 个 VW 或者 MW

Modbus 寄存器 0-----19999 是写 WW

Modbus 寄存器 20000-----20031 是写 MW

例: 我们将数据 0x01, 0x05, 0x0A, 0x09 写入 VW0 和 VW2

发送码分析:

请求 PDU

功能码	1个字节	0x10	
起始地址	2个字节	0x0000 至 0xFFFF	
寄存器数量	2个字节	0x0001 至 0x0078	
字节数	1个字节	2×N*	
寄存器值	N*×2个字节	值	

*N=寄存器数量

根据上面的分析,我们需要发送 0x00, 0x01, 0x00, 0x00, 0x00, 0x0B, 0x01, 0x10, 0x00, 0x00, 0x00, 0x00, 0x01, 0x01, 0x05, 0x0A, 0x09

接收码分析:

响应 PDU

功能码	1个字节	0x10
起始地址	2 个字节	0x0000 至 0xFFFF
寄存器数量	2个字节	1至123 (0x7B)

我们收到的数据为 0x00, 0x01, 0x00, 0x00, 0x00, 0x06, 0x01, 0x10, 0x00, 0x00, 0x00, 0x02

好的,至此,我们关于 Modbus TCP 命令连接我们 PLC 的分析就结束了,后面我上传了我做好 的 C#程序供大家参考,

这里要注意一个问题,此程序中缺少断线重连机制,请大家自己添加一下吧

13 与数码管 Modbus 通讯实例

1. 首先,将 PLC 与数码管显示器接好,然后在 PLC 中建立 modbus 主站,如图:



其中的参数要根据数码管的说明来填写,数码管手册如下图:

功能	指令
	10H 功能码
显示 10 进 制数(帯正 负号和小 数点)	 PLC 发送:01 10 00 90 00 02 04 00 02 01 EA DB 1C 01:数码管屏的站号(RS485 地址) 10:功能码,表示写多个寄存器 00 90:数码管屏的显示寄存器(带小数点和正负号的整数) 00 02:寄存器个数 04:数据个数(字节数) 00 02: 00表示正负号(00=正数:01=负数,数字前显示-) 02表示小数点位数,0表示无小数点。2表示小数点后有2位数字 01 EA:2位整数,高字节在前。01 EA表示十进制 490
	 DB 1C: 二个字节 CRC 码 此命令将显示 "4.90" 数码管屏返回 : 01 10 00 90 00 02 41 E5 例子: (1) 01 10 00 90 00 02 04 01 01 00 0A 2A F8 将显示 "-1.0" (2) 01 10 00 90 00 02 04 00 01 00 02 2A C2 将显示 "0.2"

可以看到这个例子为 PLC 发送: 01 10 00 90 00 02 04 00 02 01 EA DB 1C

其中 01 为数码管地址,即 Slave 填入 1 ,因为需要向数码管写入,所以 RW 填 1

00 09 为数码管屏的显示寄存器,转换成 10 进制为 144,因为起始地址为 40001,所以我们这里 要填入 40001+144 = 40145

04 为数据字节数,即 2 个字,所以 Count 填入 2 最后数据指针自己选择即可,注意不要与分配的库存储区冲突,这里我们用的是 VB400

	地址	格式	当前值
1	VB400	十六进制	16#00
2	VB401	十六进制	16#02
3	VB402	十六进制	16#01
4	VB403	十六进制	16#EA

如图,我们要向 VB400~VB403 写入 00 02 01 EA。

这里接一个 USB 转 485 串口监视器,然后我们用串口调试助手可以对通信进行监视,如下图:

🔤 友善串口调试助手		_ 🗆 🗙
文件(E) 编辑(E) 视图(Y)]	工具(II) 帮助(H)	
- 📔 🔚 🚥 🕂 -	- 🕨 🔳 🖉 🍾 🖃 🌣	
串口设置 串□ Prolifi(COM3 ♥ 波特率 9600 ♥	01 10 00 90 00 02 04 00 02 01 EA DB 1C 01 10 02 41 E5 01 10 00 90 00 02 04 00 02 01 EA DB 1C 01 10 02 41 E5 01 10 00 90 00 02 04 00 02 01 EA DB 00 90 00 02 04 00 02 01 EA DB	00 90 00 1C 01 10
数据位 8		
校验位 None		
流控 None		
接收设置 ASCII ③ Hex 自动换行 显示发送 显示发送 		
★送设置 ASCII ● Hex	01 10 00 90 00 02 04 00 02 01 EA DB 1C	发送
□ 重复发送 1000	01 10 00 90 00 02 04 00 02 01 EA DB 1C OFF Rx: 42 Bytes Tx: 0 Bytes 1	×

我们可以看到 01~1C 为 PLC 发送的码, 01~E5 为返回的码, 和手册完全一样, 同时你的数码管 也会显示 4.90 如下图:

