CPU CT61AT 可编程逻辑控制器

用户手册

版本: V2.01 发布日期: 4/2024 大连德嘉工控设备有限公司

目录

1	产品概述	3
2	参数设置	5
3	STEP 7-MicroWIN SMART 连接设置	6
4	WinCC 连接设置	9
5	组态王连接设置	. 18
6	力控连接设置	. 22
7	连接 SMART LINE 参数设置	. 24
8	ModbusRTU 通讯(填表方式)	. 25
9	ModbusTCP 通讯(填表方式)	29
10	PLC 之间通讯设置(填表方式)	. 32
11	PLC 之间通讯实例	. 35
12	C# Modbus TCP 通讯实例	39

1 产品概述

本产品为兼容 S7-200Smart PLC,集成以太网口,支持 STEP 7 MicroWIN SMART 编程, 上下载程序,在线监控,可与西门子 PLC 通讯,可使用(S7-300) TCP 协议直连 WinCC。 1、集成1个 RS485 口(支持 PPI 协议或 Modbus 协议),1个以太网口,集成 ModbusRTU、 ModbusTCP、西门子 PUT/GET 三大协议(注:提供更人性化的填表式通讯编程,对初学者可 以立即完成,本产品的卖点之一)

2、具有 12DI/12DQ 晶体管(地址: I0.0-1.3/Q0.0-1.3)、4AI、4AQ、4 AI(TC),不支持扩展,10K 程序空间,4K 数据空间。

3、24V DC 电源, 兼容西门子 S7-200Smart。

4、12DI 为漏型接法(即1M 接负极)

实现功能

● 可 Modbus RTU/TCP 以及 S7 PUT/GET 通讯,可网口编程、监控。

● 最多可以连接 12 个触摸屏或者上位机, 12 个 ModbusTCP 客户端。

● 可通过以太网与 S7-200 SMART/S7-200/S7-300/S7-1200/S7-1500 通讯。

● 可以连接西门子精彩系列 SMART LINE 触摸屏 (Smart 1000IE 和 Smart 700IE),以 及昆仑通态、步科、威伦通等诸多触摸屏。

● 具有 PID 功能,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

接线图如下:



断电保持寄存器的有效范围对 V 区做了缩减,只可以对 VBO-VB3966 具有断电保持功能,而 大于 VB3966 部分则没有断电保持功能(此存储区总数为 3967,还可用 VB1000-VB4966 或 VB1000-VB2000+VB3000-VB5966 这类使用)。

需要注意的是强制输出在断电以后没有保存功能,重新上电以后取消强制。

技术参数: 供电电源:标准工业24VDC 安装方式:DIN35mm标准导轨安装 尺寸W x H x D (mm):175x100x81 防护等级:IP20 网口通讯速率:100Mbps



2 参数设置

CT61AT PLC 可以登录网页进行查看型号以及参数配置,具体操作方法: 电脑 IP 地 址设置成 192.168.1.xxx(如: 192.168.1.100),浏览器地址栏里输入 192.168.1.222 (回 车),即可配置以及查看参数。

主菜单
欢迎使用大连德嘉工控产品
192 168 001 010
Select Language Chinese English
International Electronic Version
ID:CT61AT-20231226A

点击"Chinese"进入子菜单,可设置 PLC 的 IP 地址,运行/停止,清空



3 STEP 7-MicroWIN SMART 连接设置

打开 STEP 7-MicroWIN SMART,点击"通信",查找 CPU,就能找到 CT61AT CPU,其默 认 IP 地址为 192.168.1.10,可通过后门网页【IP 设置】或者直接点击当前界面"编辑"修改 IP 地址。

通信接口	
Realtek PCIe GBE Family Controller.TCPIP.1	按下 *编辑* 按钮以更改所选 CPU 的 IP 数据和站名称。按下 *闪 烁指示灯* 按钮使 CPU 的 LED 持续闪烁,以便目测找到连接的 CPU. MAC 地址 00:CB:EE:40:00:2E 闪烁指示灯 IP 地址 192 . 168 . 1 . 10 编辑 子 阿掩码 255 . 255 . 255 . 0 默认网关 192 . 168 . 1 . 1 站名称(ASCII 字符 a-z、0-9、-和.) plc200smart
查找 CPU 添加 CPU 编辑 CPU 删除 CPU	
	72

系统块中配置的 CPU 类型为 CPU SR20 (AC/DC/Relay), 版本号: V02.04.00, 该 CPU 不支持 扩展模块功能。

相快	_	版木	输入	输出	订货号
PU CPU SR20 (AC/E)C/Relay)	V02.04.00_00.00	. 10.0	Q0.0	6ES7 288-1SR20-0AA0
0					
1					
13					91
14					
15					
通信 数字單输入		➡➡ • 地址数据固定为下面	的值,不能	通过其它方式	式更改
10.0 - 10.7	1000				
 □ 10.0 - I0.7 □ I1.0 - I1.7 劫 文 單 输出 		IP 地址:		4 4	
 □ I0.0 - I0.7 □ I1.0 - I1.7 数字里输出 保持范围 安全 		IP 地址: 子网掩码:	·	4 4 4 4	
 □ 10.0 - 10.7 □ 11.0 - 11.7 動字里輸出 保持范围 安全 启动 		IP 地址: 子网掩码: 默认网关:	• • •	· ·	

其中使用 4AI、4AQ、4AI(TC)定义如下模块类型即可,使用对应相同 IO 地址

	模块	版本	输入	输出	订货号
CPU	CPU SR20 (AC/DC/Relay)	V02.05.01_00.00	10.0	Q0.0	6ES7 288-1SR20-0AA0
SB					
ЕМ О	EM AQ04 (4AQ)			AQW16	6ES7 288-3AQ04-0AA0
EM 1	EM AE04 (4AI)		AIW32		6ES7 288-3AE04-0AA0
EM 2	EM AT04 (4ALTC)		AlW48		6ES7 288-3AT04-0AA0
ЕМ З					
EM 4	田	th 细太顺 c 拉	召这捕	(立))(市(支4)	太
EM 5	侯	大组心顺力权	RIXIE	世间则于生	tier

4AI 电流或电压类型在系统块中选择,4AQ 电压或电流类型通过接线端子选择

	模块	版本	输入	输出	订货号
CPU	CPU SR20 (AC/DC/Relay)	V02.05.01_00.00.01.00	10.0	Q0.0	6ES7 288-1SR20-0AA0
SB					
EM O	EM AQ04 (4AQ)			AQW16	6ES7 288-3AQ04-0AA0
EM 1	EM AE04 (4AI)		AlW32		6ES7 288-3AE04-0AA0
EM 2	EM AT04 (4AI TC)		AlW48		6ES7 288-3AT04-0AA0
ЕМ З					
EM 4					
EM 5					

■ 模組参数 ■ 模拟里输入	<u>一</u> 通道 0 (和1327
<u>回 通道 0</u> <u>同</u> 通道 1	电压
── 回 通道 2 ── 回 通道 3	范围 +/- 10v 💌

4AI(TC)热电偶类型在系统块中选择

1

系统	央				>
	模块	版本	输入	输出	订货号
CPU	CPU SR20 (AC/DC/Relay)	V02.05.01_00.00.01.00	10.0	Q0.0	6ES7 288-1SR20-0AA0
SB		100			
EM 0	EM AQ04 (4AQ)			AQW16	6ES7 288-3AQ04-0AA0
EM 1	EM AE04 (4AI)		AIW32		6ES7 288-3AE04-0AA0
EM 2	EM AT04 (4ALTC)		AlW48		6ES7 288-3AT04-0AA0
EM 3					
EM 4					
EM 5					

偶 \$`关。	类型	
1月10日 1月11日 - 1月11日 - 1月111日 - 1月11日 - 1月111日 - 1月1110日 - 1月1110日 - 1月1110日 - 1月1110日 - 1月1110日 - 1月111000 - 1月111000000000000000000000	热电偶	
道 2	热电偶	
道3	类型K (NiCr-Ni) ▼	
	类型 B (PtRh-PtRh)	
	突型 N (NiCrSi-NiSi) 类型 E (NiCr-CuNi)	
	类型R (PtRh-Pt)	
	奕型 S (PtRh-Pt)	
	类型 T (Cu-CuNi)	
	类型 K (NiCr-Ni)	

注意: 以下功能无法使用

系统块			on Belacter Bandarias e		×
模块	版本	输入	输出	订货号	
CPU CPU SR20 (AC/DC/Relay)	V02.04.00_00.00.00.00	10.0	Q0.0	6ES7 288-1SR	20-0440
SB					
EM 1					
EM 2				<u> </u>	
EM 3					
EM 4					
EM 5					
 □通信 □数字里输入 □ 10.0 - 10.7 □ 11.0 - 11.7 □ 数字里輸出 □ 保持范围 □ 定会 □ 启动 ☑ 次 允i ☑ 次 允i ☑ 该功能无法使用, 默认CE 	PU 启动后的模式	र्ट,			
	调试 工具 帮助 大 大 大 示 Get/Put 数据日志 PROFINE	□ 运动控制团	▲ PID 短板 PID 板 PID 和 PID	SMART 5 驱动器组态 * PRC	查找 ETK 设备
同寺			116.200	上具	
			▼ 協力 個人	- 「※ 慧彦 - 39	
□ ① ① ○ 新增功能 □ <td>1 程序注释 1 程序没注释 2 输入注释</td> <td></td> <td></td> <td></td> <td></td>	1 程序注释 1 程序没注释 2 输入注释				
	 ○ 定时器 PROFINET ● @ Modbus RTU ● @ Modbus RTU ● @ Modbus RTU ● @ Modbus RTU ● @ Modbus TCP (● @ Modbus TCP (● @ Open User Co ● @ Open User Co ● @ PN Read Write 	Master (v2.0 Master2 (v2. Slave (v3.1) Client (v1.4) Server (v1.0) mmunication e Record (v1.1))) .0)) h (∨1.0) 1.0)		

4 WinCC 连接设置

1. 打开 WinCC(以 WinCC7.3 为例),双击变量管理,打开变量管理器,添加驱动:



2. 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

文件(E) 编	辑(E) 视图	图(V) 帮助(H)		
变量管理	«	查找	♀ - 属性	\$
□- 变量管	雪理	名称	▲ □ 选择	
🕀 💝 🖻	┃, 添加弱	新的驱动程序 🔸	SIMATIC S7 Protocol Suite	
	国复制		SIMATIC S7-1200, S7-1500 Channel	
	13 粘贴		SIMATIC S5 Serial 3964R	
			SIMATIC S5 Programmers Port AS511	
		7 @Redunda	SIMATIC S5 Profibus FDL	
		8 @SCRIPT_	SIMATIC S5 Ethernet Layer 4	
		9 @SCRIPT_	SIMATIC TI Serial	
		11 @ServerN	SIMATIC TI Ethernet Layer 4	
		12 @ServerVe	SIMATIC 505 TCPIP	
		13 @TLGRT_/	Allen Bradlay, Ethernat ID	
		14 @TLGRT_S	Miteubichi Ethernet	
		16 @TLGRT_	Medbur TCDD	
		17 💥		
		18	Drafibure DD	
		19	Profibus DP	
支量管	理	21		
	and a second	22	Simotion	
✓ 报警记	录	23	System Info	
夜量记	录	24		
 # #	11 🔹 🔹	26 26	-	

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

设备状态监控 ☑ 激活 (A) 60 间隙 (E) 30 超时间隙 (E) CPU 停机监控 ☑ 激活 (E)
 ☑ 激活 (A) 60 间隙 (I) 30 超时间隙 (I) CPU 停机监控 ☑ 激活 (I)
- CPV 停机监控 ☑ 激活 @)
☑ 激活 ⑫)
在 AS 中通道使用了周期读服务。

5. 在逻辑设备名称选框中选择驱动为:网卡名.TCPIP.1

SIMATIC S7 单位	
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 👻
📝 自动设置 (A)	
作业处理	
□写(带优先权)(@)	
输入新的设备名称或从列表	中选择被请求的设备。

6. 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

当前连接到:	47
M络 2 Internet 访问	
拨号和 VPN	^
宽带连接	•
2	
打开网络和共享中心]
	13:59

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		
I	- 🔷 -	🜔	查看完整映射
ペ TJ-20140101SPKI (此计算机)	网络 2	Internet	
查看活动网络			连接或断开连接
阿络 2 家庭网络	び 落 道	i问类型: Internet :庭组: 已加入 :接: ♀ 本地连接 2	
更改网络设置			120 22
设置新的连接或网络 设置无线、宽带、拨号、M	新式 VPN 连接;或设置	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 VPN 网络	各连接。	
选择家庭组和共享选项 访问位于其他网络计算机」	_的文件和打印机,或更	改共享设置。	
吴 疑难解答			
·····································	茨得故障排除信息。		

在弹出的对话框中点击详细信息

(规	
连接 —	
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
速度	100.0 Mbp:
£÷h	
舌动 ——	
活动	已发送 —

下图中的描述内容就是你的网卡名

同時	(8
	Ц
YE接持定的 INS E%	
抽还	Realtek PUle GBE Family Controll
初理观址	60-45-CB-89-21-14
已启用 DHCP	台
IPv4 地址	
IPv4 子网摘码	
IPv4 默认网关	
IPv4 DNS 服务器	
IPv4 WINS 服务器	
已启用 NetBIOS ove	是
连接-本地 IPv6 地址	
TPv6 野山网关	
IPv6 DNS 服务器	
•	

7. 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。





8. 右键单击 NewConnection_1, 在弹出的菜单中选择



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

S7 网络地址		
IP 地址(I):	192. 168. 1. 10	
机架号(B):	0	
插槽号(I):	0	
🔤 发送/接收原始数	如据块 (22)	
连接资源 (C):	02	
腧入自动化系统的 I	P thatilto	
列如: 142.11.0.123		

现在连接已经建立成功,已经可以建立变量和画面了。

5 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

-	P-S5 Series	
	由 SS系列	
	<u>⊕</u> - \$7−1200	
	⊕-S7-200 (MPI)	
	〒-S7-200条列	H
	由-S7-200系列(DP)	100
(\land)	亩 S7-200系列(USB)	
	(±-51-300 (MF1)	-
	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
	「恐則処則反軍」 たって完。 悪门ス	
古40本+H	设备名称: S7-200(UCP)	
高級重換	通信描述: TCP	

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		X
		你所选择的为串行设备,请选择与 设备所连接的串口。 一使用虚拟串口(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) 〉 1	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一的逻辑名称
	新工口设备
	□ 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

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 址帮助信息。	
[192.168.1.10:0	
< 上一步 @) 下一步 @) > 取	消

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。

	你所要安装的设备信息:
	- 设备信息
	新设备为 西门子 生产的 S7-200(TCP)
	・
	·汉田赵福伯·利10汉田
a para a subsection of the second s	设备地址:192.168.1.10:0
	通讯方式• 100
	▶ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

至此,就完成了 PLC 与组态王的连接。

6 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:	
SK.	更新周期: 250	壹秒 、
	超时时间: 3	秒、
, and the second s	设备地址:	li,
	通信方式: TCP/IP网络	
	故障后恢复查询	
	周期: 300 秒 🗌 最大时	· 40 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: 192.168.1.	10 端口: 102
□ 启用备用通道 备用IP地址:	
□ 主通道恢复后自动回切	
□本机网卡冗余 本机网卡IP地址:	端口: 0
备用网卡IP地址:	端口: 0
□ 连续采集失败 3	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	
ISAP (PC):	10.11	

23

7 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 WinCC flexible SMART, 给触摸屏编程, PLC 设备 IP 地址为 CT61AT IP 地址即可, 如下图所示

			and second			
ናቁ	通讯驱动程序	在线	注 释	1		
崔接_1	SIMATIC S7 200	▼ 开	•			
Smart 1	000 IE				Station	
Smart 1	000 IE 接口 以太网	×			Station	
Smart 1	000 IE 接口 以太网	✓ 41 设备			Station	PLC 设备
Smart 1	000 IE 接口 以太网 HM 地址	▼ 41 设备				PLC 设备
Smart 1 『 』 受 IP	000 IE 接口 以太网 地址 192, 168, 001, 200	✓ 41 设备			Station	PLC 设备 001.010
Smart 1 【】 【】 ● IP ● ISO	000 IE 接口 以太网 地址 192、158、001、200	✓ AI 设备			Station 上 地址 192、168、 扩展插槽	PLC 设备 001, 010
Smart 1 第二 ● IP ● ISO	000 IE 接口 以太网 地址 192、168、001、200 只能在设备上组态地址	✓			5tation 単址 192、168、 扩展插槽 机架	PLC 设备 001, 010 0
Smart 1 上 受 IP ○ ISO	000 IE 接口 以太网 地址 192、168、001、200 只能在设备上组态地址 访问点 S70NLLIN	▼ 4I 设备 E			Station 「192、168、 が展插槽 机梁 図 循环操作	PLC 设备 001, 010 0

8 ModbusRTU 通讯(填表方式)

下载 PLC 通讯组态插件:点击下载

http://www.dl-winbest.com/download/PLC_Config.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
席号	modbus命令 ^
0	□读取线圈 Dyxxy、从头1、起始他业D。个数1、V区地址D。位·D、命令执行前证时merD
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 0xxxx: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	DoubleClack here
9	DoubleClick here
11	
12	
13	DoubleClick here
14	DoubleClick here
15	DoubleClick here
16	DoubleClick here
17	DoubleClick here
18	DoubleClick here
19	DoubleClick here
20	DoubleClick have
Part of the local division of the local divi	7
	41
	X

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 S7-200P	LC 的数据对应关系如下:	
00001-00128	Q0.0、Q0.1、Q0.2Q1	5.7
10001-10128	10.0 、10.1 、10.2 115	.7
30001-30032	AIW0、AIW2、AIW4AIW62	2

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。

以两个 CT61AT 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 5、V 区起始地址 500,RS485 接线方式为 A--A, B--B,方法如 下:

		态 V1.0		
ne 上传祖念到 嘉设备 PLC 的 IP地址	F数組念到PLC 192 168 1 10		■ 報助 英取(网络中只有一个设备 Slave S7 PUT/CFT)
RS485 @ 无效	● modbus主站功)能	© modbus从站功能	
波特率: 9600 命令重发次数: 2	▼ 从站无响应,直接发送下一条命令	校验: ? ▼	8位无校验1停止位 No Pa 等待从站回答时间:	arity • 30ms •
序号 modbus命令 0 03读保持寄存 1 DoubleC 2 DoubleC 3 DoubleC 4 DoubleC 5 DoubleC 6 DoubleC 7 DoubleC 8 DoubleC 9 DoubleC 10 DoubleC 11 DoubleC 12 DoubleC 13 DoubleC 14 DoubleC	F器 4xxxx:从站1:起始地址0: modbus 命令行编辑 命令执行前延时 ms: 功 能 号: D3读保持寄存器 4x 从站地址: 1 起始地址: 0 计数个数: 5 PLC内部V区起始地址: 500	个数5; V区 □ □ 注:通常为0	地址500; 命令执行前延时 , ▶ ▶	LS: 0

(1) 其中一个 CT61AT PLC,编辑 Modbus 主站命令,下载到 PLC 中

如需上传组态命令到电脑功能,先把 PLC 切换到 STOP 状态,再上传即可。

(+) ② [++ Ø http://192.168.1.222/cn_ma そ 、
👍 🕨 建议网站 (2) ▼ 🦻 搜狗搜索 🤗 系统重装 🥙 影视大全 🕨 建议网站
PLC STATUS : RUN
内嵌Modbus : 主站
RUN PLC
STOP PLC
IP 设 置
MAC 设置
PLC 清空
PLC 诊断
PLC 通讯

下载成功后,可以网页通过后门地址查看 Modbus 主从站方式

(2) 另一个 CT61ATPLC,编辑 Modbus 从站命令,下载到 PLC 中

📴 S06 PLC modbusRTU/TCP &S7 PUT/GET 填表式通讯组态 V1.0
File 上传组态到电脑 下载组态到PLC 德嘉硬件设置 帮助
德嘉设备 PLC 的 IP地址: 192 168 1 11 自动获取(网络中只有一个设备)
RS485 modbusRTU 以太网 modbusTCP Poll 以太网 modbusTCP Slave S7 PUT/GET
RS485 ◎ 无效 ◎ modbus主站功能 ◎ modbus从站功能
波特率: 9600 ▼ 校验: 8位无校验1停止位 No Parity ▼
Wedbus从站方式·
从站地址: 1
Modbus地址 S7-200数据区
00001-00128 Q0.0-Q15.7 modbus对应地址为: 0、1、2、。。。128
10001-10128 IO.0-I15.7 modbus对应地址为: 0、1、2、。。。128
30001-30032 AIWO-AIW62 modbus对应地址为: 0、2、4、。。。62
40001-4xxxx VW(n)、VW(n+2)、VW(n+4) modbus对应地址为: n、n+1、n+2
例1: modbus 起始地址8 、个数3 对应的V区为VW8 、VW10、VW12
/y/2: modbus 延宕中地址19、「字数4 X1/2日)V区/JV₩19、V₩21、V₩23、V₩25

(← ⊖)	/cn_ma 😌 🝷 🖒 搜索	ター 🕆 🛪
👍 🐌 建议网站 (2) 🔻 🙆 搜狗搜索 餐 系	统重装 🛃 影视大全 🐌 建议网站	
Р	LC STATUS : RUN	^
内	嵌Modbus : 从站	
	RUN PLC	
	STOP PLC	
	IP 设 置	
	MAC 设罟	
	PLC 清空	
	PLC 诊断	
	PLC 通讯	

下载成功后,也可网页通过后门地址查看 Modbus 主从站方式

最后同时监控两个 PLC 的状态数据,如下:

地址	格式	当前值	田 🔤 转换	Linkle	4-94	±± 25 /#
1 VW0	无符号	11	田田田 计数器	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	行政	
2 VW2	无符号	22	中国 密料法官	1 VW500		22
3 VW4	无符号	33		2 VW502	大行ち	- 22
VW6	无符号	44	田 🔤 逻辑运算	3 VW304	- 元付ち	
VW8	无符号	55	由 🙆 传送	4 VW306	工行ち	44
	有符号		田 22 程序控制	5 VW308	尤付ち	00
	有符号		田田 移位/循环	0	月付ち	
	有符号		田圃 美格			
9	有符号		田 🙆 定时器			
	485从站数据		 ● PROFINET ● @ 库 ● @ 调用子例程 		485主站数据	

提供 485 通讯断线诊断功能,通过 CPU 状态位监控可以判断出通讯异常情况,断线响应时 长为 16s,下面为 Modbus64 条命令具体对应 CPU 状态位关系:

命令 (序号)	状态位地址
0	SM200.0
1	SM200.1
	•••••
63	SM207.6
64	SM207.7
485 通讯正堂时状态位地址值为1	. 异常(新线或者诵讯参数等

485 通讯正常时状态位地址值为 1,异常(断线或者通讯参数错误)状态位地址值为 0。

9 ModbusTCP 通讯(填表方式)

下载 PLC 通讯组态插件: 点击下载

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

(1) 以 ModbusTCP 作为主站(客户端)为例,编辑如下几种命令,下载到 PLC 中

著设备 5485	PLC 的 IP地址: 192 168 1 10 自动获取(网络中只有一个设备) modbusRTU 以太网 modbusTCP Poll 以太网 modbusTCP Slave S7 PUT/GET
序号	modbusTCP 命令
0	
1	02读取输入状态 1xxxx 从站IP: 192.168.1.165; slaveID=1; 起始地址0; 个数5; V区地址200
2	03读保持寄存器 4xxxx 从站IP: 192.168.1.165; slaveID=1; 起始地址0; 个数5; V区地址300
3	04读输入寄存器 3xxxx 从站IP: 192.168.1.165; slaveID=1; 起始地址0; 个数5; V区地址400
4	DoubleClick here
5	DoubleClick here
6	DoubleClick here
7	DoubleClick here
В	DoubleClick here
9	DoubleClick here
10	DoubleClick here
11	DoubleClick here
12	DoubleClick here
13	DoubleClick here
14	DoubleClick here
15	DoubleClick here

通过电脑端使用 Modbus Slave 模拟从站(服务器),该电脑 IP 地址为: 192.168.1.165,建 立对应功能码和连接,最终监控如下:



(2) 再以 ModbusTCP 作为从站(服务器)为例,下载到 PLC 中

💀 S06 PLC modbusRTU/TCP &S7 PUT/GET 埴表式通讯组态 V1.0	9 <u>—</u> 9		×
File 上传组态到电脑 下载组态到PLC 德嘉硬件设置 帮助			
德嘉设备 PLC 的 IP地址: 192 168 1 10 自动获取(网络中只有一个	∖设备)		
RS485 modbusRTU 以太网 modbusTCP Poll 以太网 modbusTCP Slave S7 PUT/G	ET	10	
PLC始终开启 modbusTCP Slave 功能,并且不能被关闭: 允许被访问的功能研	她下:		
01功能码: 读 Q区 [addr/8].[addr%8] 注: (/) 整除 (%) 余数			
02功能码: 读 I⊠ [addr/8].[addr%8] 注: (/) 整除 (%)余数			
03功能码:读 V区(0-10000)对应VB 0-10000 读 M区(20000-20031)对应	MB 0-3	1	
05功能码:写一位 Q区 [addr/8].[addr%8] 注: (/) 整除 (%) 余	数		
06功能码:写单个 V区(0-10000)对应VB 0-10000 写 M区(20000-20031)ス	<u> MB</u>	0-31	
15功能码:写多位 Q区 [addr/8].[addr%8] 注:(/)整除 (%)余	数		
16功能码:写多个 V区(0-10000)对应VB 0-10000 写 M区(20000-20031)ス	拉略	0-31	

通过电脑端使用 Modbus Poll 模拟主站(客户端)来读取或写入,建立对应功能码和连接,最终监控如下:



10 PLC 之间通讯设置(填表方式)

下载 PLC 通讯组态插件: 点击下载

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

该方式也可以在网页中【PLC 通讯】功能中进行设置,数据是同步的,通过通讯组态插件或 者是在网页中设置,两种方式选一种即可。

(1)以"取数"方式为例,编辑该命令如下,其中对方 PLC 类型为 S7-200SMART,下载到
 PLC

🖳 SO6 PLC r	nodbusRTU/TCP & S7 PUT/GET 填表式通讯组态 V1.0		23
File	上传组态到电脑 下载组态到PLC 德嘉硬件设置 帮助		
德嘉设备 PL	C 的 IP地址: 192 168 1 10 自动获取(网络中只有一个	设备)	
RS485 mo	dbusRTU 以太网 modbusTCP Poll 以太网 modbusTCP Slave S7 PUT/GET	7	
	Y PUT/GET 命令	_	
0 取	数 长度:2 本方起始地址:20 对方PLC IP:192.168.1.25 对方起始地均	t:20 V⊠	对方:
1 Do 2 Do	🖳 S7 PUT/GET命令		
3 Do 4 Do 5 Do	◎ 无效 ◎ 送数 ◎ 取数		
	取数/送数长度:2 字节 本方起始地址:20		
	对方PLC IP: 192 168 1 25 对方起始地址: 20		
	对方数据区:		
	◎ I区 ◎ Q区 ◎ M区 ◎ V区 ◎ DB块 DB块号: 65535		
	对方PLC类型		
	● S7-1200 1500 S7-200 smart ◎ S7-300 ◎ CP243-1-IS0		
	确定 取消		-
	说明:本方地址 0-19999代表V区(0-19999)		
	说明: 本方地址 20000-29999代表M区(0- 9999)		
	说明:本方地址 30000-39999代表I区(0-9999)		
	说明:本方地址 40000-49999代表Q区(0- 9999)		

监控数据如下:

首	- 🛅 - 🔽 🔟 🖓 🌽	2 🔒 🚡 📆 🕅 🛛	📶 🖸 🔹			68 / 🔒 🚡 🖏	M 🖸 🔹
	地址	格式	当前值		地址~	格式	当前值
1	VB20	无符号	66		VB20	无符号	66
2	VB21	无符号	88	2	2 VB21	无符号	88
3		有符号		3	3	有符号	
4		有符号		2		有符号	
5		有符号		5	ī	有符号	
6	0	有符号		6	6	有符号	
2							
	 	7		•	()) 图表1 /		

(2) 再以"送数"方式为例,编辑该命令如下,其中对方 PLC 类型为 S7-200SMART,下载 到 PLC 中

ne S06 PLC modbusRTU/TCP & S7 PUT/GET 填表式通讯组态 V1.0	23
File 上传组态到电脑 下载组态到PLC 德嘉硬件设置 帮助	
德嘉设备 PLC 的 IP地址: 192 168 1 10 自动获取(网络中只有一个设备)	
RS485 modbusRTU 以太网 modbusTCP Poll 以太网 modbusTCP Slave S7 PUT/GET	
序号 S7 PUIT/CFT 命令	
0 取数 长度:2 本方起始地址:20 对方PLC IP:192.168.1.25 对方起始地址:20 V区	对方
1 送数 长度:2 本方起始地址:40 对方PLC IP:192.168.1.25 对方起始地址:40 V区 2 Doub	对方:
3 Doub PS7 PUT/GET命令	
4 Doub 5 Doub ◎ 无效 ◎ 送数 ◎ 取数	
取数/送数长度:2 字节 本方起始地址:40	
对方PLC IP: 192 168 1 25 对方起始地址: 40	
□ 对方数据区:	
◎ I区 ◎ Q区 ◎ M区 ◎ V区 ◎ DB块 DB块号: 65535	
对方PLC类型	
• S7-1200 1500 S7-200 smart © S7-300 © CP243-1-IS0	Þ
说明:本方地址 0-19999代表V区(0-19999)	
说明:本方地址 20000-29999代表M区(0-9999)	
说明:本方地址 30000-39999代表I区(0- 9999) 道明:本方地址 40000-49999代表I区(0- 9999)	
MCHJ. 47.11671 40000 433331 (46.407 (0 3333)	

监控数据如下:

++h+u+	校士	当前值		titut 🔺	格式	当前值
1 VR20	1月15、		1	VB20	无符号	66
2 VP21		00	2	VB21		88
2 VD21	九付ち	00	3		有符号	
4 VB40		111	4	VB40	无符号	111
5 VB41	无符号	222	5	VB41	无符号	222
6	有符号		6		有符号	
7	有符号		7		有符号	

可见,通讯成功,这种方式要比指令编程方式更快捷,更方便。

11 PLC 之间通讯实例

此例为网页中设置方式,也可通过通讯组态插件完成设置,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 CT61AT 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. CT61AT 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:







C Image: C <thimage: c<="" th=""> <thimage: c<="" th=""> <thimag< th=""><th>⊕ ☆ @</th></thimag<></thimage:></thimage:>	⊕ ☆ @
通道:1 取数或送数	^
· · · · · · · · · · · · · · · · · · ·	
取数/送数长度: 002 字节 本方起始地址 00100	
对方PLC类型: のS7-1200 S7-200 smart CP243 (remote) のS7-300 のSIEMENS CP243-1-ISO	
提交 取消	
遊回	
况明:本万地址 0-19999代表Ⅵ兰(0-19999)	
说明:本方地址20000-29999代表M区(0-9999)	
说明:本方地址30000-39999代表I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	⊐ (@DB1 可访问的节点\pn-io_ONLINE)						
地址	名称		初始值	实际值			
	0.0 STATO	WORD	W#16#FFFF	W#16#FFFF			
<							

3. 再观察一下 S7-1200 的 MW0 的数据值

I I	具(T) i	窗口(W) 帮助(H)	『转到在线 💋 转	到离线 🎝 🖪 🖪	≭ ∃ ∐			
项	目1)	PLC_1 [CPU 1214	IC AC/DC/Rly] 🔸	监控与强制表 →	监控表_1			_ # = X
1	× 💉 🛛	1 10 9, 90 2						
	i	名称	地址	显示格式	监视值	修改值	9	注释
1		*1*	96MW0	十六进制 💽	16#FFFF			
2			<添加>					
								_
	-							
-								
-								

4. 最后看一下 S7-200 SMART 的 MW0 数据值

	- 🎦 - 🕞 🔳	Gi 🥒 🔒 🚡 🐯 🛙	<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			
4		有符号			
5		有符号		43.	

实现数据的传送就这么简单。

12 C# Modbus TCP 通讯实例

这里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 VW

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

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

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 VWO 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