S7-1500/1200 系列与 H3u 的 Modbus TCP 通讯

张长兴(18606277674)

说明:在TIA软件中,"MB_CLIENT"指令作为 Modbus TCP 客户端通过 PROFINET 连接进行通信。通过"MB_CLIENT"指令,可以在客户端和服务器之间建立连接、发送 Modbus 请求、接收响应并控制 Modbus TCP 客户端的连接终端。

S7-1200 固件版本 V4.0 支持"MB_CLIENT"指令和最高 V3.1 版本的库。S7-1200 固件版本 V4.1 及更高版本和 S7-1500,支持"MB_CLIENT"指令的所有库版本。

可通过 CPU 或 CM/CP 的本地接口建立连接。

1. 硬件连接



图 2.1.0 TCP 组网接线图

- ▶ 网线要求:网线采用标准超7类,带屏蔽层,水晶头必须带屏蔽层。
- > 交换机要求:工业级交换机(建议使用字泰工业交换机)。
- 2. 西门子 TIA 软件设置
- (1)建立工程,根据实际所连设备添加 CPU 类型,比如 SIMATIC S7-15001511T-1 PN,6ES7 511-1TK01-0AB0。

V Siemens - C:\Users\Administrator\Desktop\Simen	TCP/S71200 TCP/S7	71200_TCP		l rec
项目(P) 编辑(E) 视图(V) 插入(I) 在线(O) 诜项(N)	漆加新设备			×
	设备名称:			
			_	
项目例 □ □ □	PLC_3			
设备				
		▼ 1 控制器	设备:	
		SIMATIC \$7-1200		
		▼ III SIMATIC \$7-1500		
₩ ▼	控制器	T CPU		
· · · · · · · · · · · · · · · · · · ·	12.9366	CPU 1511-1 PN		
▲ ^{设备和网络} 第一步		CPU 1511C-1 PN		CPU 1511T-1 PN
▼ PLC_1 [CPU 1215C DC/DC/Rly]		CPU 1512C-1 PN		
		CPU 1513-1 PN		CECT E11 17/01 0400
№ 在线和诊断		CPU 1515-2 PN	10英写·	6ES7 STI-TIKUT-0ABU
▼ 🛃 程序块	HMI	CPU 1516-3 PN/DP =	版本:	V2.5
· · · · · · · · · · · · · · · ·		CPU 1517-3 PN/DP		
Hain [OB1]		CPU 1518-4 PN/DP	说明:	
MB_date [DB2]		CPU 1518-4 PN/DP ODK	带显示屏的	T-CPU:工作存储器可存储 225 KB 代
MB_date1 [DB3]		CPU 1518-4 PN/DP MFP	伯和1 MB 刻 拍和制 丁香	()据:位指令执行时间 60 ns:4 级防 艺功能:扩展法动控制、闭环控制、计
MB_date2 [DB4]	DC Tilt	CPU 1511F-1 PN	数与测量:	限踪功能:PROFINETIO 控制器. 支持
MB_date3 [DB6]	PC系统	CPU 1513F-1 PN	RT/IRT. 性能	升级 PROFINET V2.3. 双端口. 智能设
MB_date4 [DB7]		CPU 1515F-2 PN	首: 支持 MH 户安全诵信.	S7 诵信, Web 服务哭, DNS 容白端
▶ 110 系统块		CPU 1516F-3 PN/DP	. OPC UA 服	务器数据访问,等时同步模式,路由
▶ 【录 工艺对象		CPU 1517F-3 PN/DP	功能:运行系	系统选件. 固件版本 V2.5
▶ 圖 外部源文件		CPU 1518F-4 PN/DP		
▶ A PLC 变望		CPU 1518F-4 PN/DP ODK		
▶ L@ PLC 数据类型 ~		CPU 1518F-4 PN/DP MFP		
✔ 详细视图		▼ Im CPU 1511T-1 PN		
		6ES7 511-1TK01-0AB0		
		▶ 🛄 CPU 1515T-2 PN 第三步	ŧ.	
to The		CPU 1516T-3 PN/DP		
		◆ CPU 1515T-2 PN 第三步	Þ	

图 2.2.0 TIA 工程建立

(2) 添加通讯功能块,"MB_CLIENT"。

转至离线 品? 📭		▲ <在项目中搜	索>	-		Totally Integrat	ed Autor	nation PORTAI	
DC/DC/Rly] ▶ 程序	序块 ▶ Main [0	B1] 🗕 🖬 🖬	iХ	指令	第一步				Γ
				选项					
<u> 영</u> + 요 + 명 + E	- 1 to 1 to 1	a (m 125) i	4		tes Les	va 🤻			
			•	1					- ~
数据类型	默认值	注释							
	auto tiza	1-2-1-		▶ 基本指令		100 10	aler"		18
			^	名称		抽还	版本		
								^	ľ
			_				V1.0		
			^	 ⑤ 定时器操作 			V1.0		
)R				▶ <u>+1</u> 计数器操作			V1.0	~	H
				> 扩展指令					1
1				> 工艺					Ъ
				✔ 通信	第二步				Ŧ
				名称		描述	版本		1
				▶ 🛅 S7 通信			V1.3		Π
				▶] 开放式用户	通信		V6.0		L
			- 11	▶ 🗀 WEB 服务器	-		V1.1		L
				▼ □ 其它	第二十	⇒			
				- MODBU	S TCP		<u>V5.0</u>		
				= MB_	CLIENT 第四:	·通过 PROFINET进行…	V5.0		
				= MB_	SERVER	通过 PROFINET进行	V5.0		
			≡	=- MB_	RED_CLIENT	Redundant communic	V1.0		
				=- MB_	RED_SERVER	Redundant communic	V1.0		
				▶ 🛅 通信处理器					
			~	▶ 🛅 远程服务			V1.9		
> 100%	-	Y							

图 2.2.1 MODBUS-TCP 主站功能块添加

.



图 2.2.2 MODBUS-TCP 主站功能块示意

(3) "MB_CLIENT" 实例化,引脚配置。



图 2.2.3 MODBUS-TCP 主站功能块设置

注意事项:西门子软件中,需要建立数据块进行变量声明与定义。按照功能块引 脚要求,定义准确的变量数据类型。 如下图所示。

5							
页目(P) 编辑(E) 视图(V) 插入(I) 在线(O) 选项(N)	工具(1)	窗口(W)	帮助(H)				
🦉 📑 🔚 保存项目 🎒 🐰 🗉 値 🗙 🎝 🛨 (ぞう			1 N 铸车	在紙 🔊	转至离线 🤽		3山坦宏、
项目树 🛛 🗸	冷加羽	「吠					
辺久	名称	:					
	- 数据	块_1					
E							
		_	类型	:	🥃 全局 DB	-	
▼ S71200_TCP			语言	-	DB	T	
		-OB					
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	-	组织块	编号	-	9	÷	
→ FLC_T [CF0 1215C DQDQMy]					○ 手动		
			1		(3) 自动		
▼ 🛃 程序块			400.4				
◎ 添加新块 第一步		FB	加过				
- Main [OB1]		函数块	数据	块 (DB) 保存	字程序数据。		
MB_date [DB2]							
MB_date1 [DB3]			1				
MB_date2 [DB4]							
MB_date3 (DB6)		FC					
■ MB_date4 [DB/]		函数					
▶ 📮 PLC 变量							
▶ 💽 PLC 数据类型 🗸		DB	第一步				
✓ 详细视图		粉堆中	20-02				
		2X10PVC	百久	信自			
		- 1- 4	£9	In Alares			
	> 耳	1日見 -					

图 2.2.5 添加数据块



图 2.2.5 数据块中变量定义

(4) 数据传送。

功能块"MB_CLIENT",引脚MB_MODE、MB_DATA_ADDR 和 MB_DATA_LEN 参数对 应关系及地址说明。

MB_MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus 功能	功能和数据类型
0	1到9999	1 到 2000	01	在远程地址 0 到 9998 处,读取 1 到 2000 个输出位
0	10001 到 19999	1 到 2000	02	在远程地址 0 到 9998 处,读取 1 到 2000 个输入位
0	 40001 到 49999 400001 到 465535 	1 到 125	03	 在远程地址 0 到 9998 处,读取 1 到 125 个保持性寄存器 在远程地址 0 到 65534 处,读取 1 到 125 个保持性寄存器
0	30001 到 39999	1到125	04	在远程地址 0 到 9998 处,读取 1 到 125 个输入字
1	1 到 9999	1	05	在远程地址 0 到 9998 处,写入 1 个输出位
1	 40001 到 49999 400001 到 465535 	1	06	 在远程地址 0 到 9998 处,写入 1 个保持性寄存器 在远程地址 0 到 65534 处,写入 1 个保持性寄存器
1	1 到 9999	2 到 1968	15	在远程地址 0 到 9998 处,写入 2 到 1968 个输出位
1	 40001 到 49999 400001 到 465535 	2 到 123	16	 在远程地址 0 到 9998 处,写入 2 到 123 个保持性寄存器 在远程地址 0 到 65534 处,写入 2 到 123 个保持性寄存器
2	1 到 9999	1到1968	15	在远程地址 0 到 9998 处,写入 1 到 1968 个输出位
2	 40001 到 49999 400001 到 465535 	1 到 123	16	 在远程地址 0 到 9998 处,写入 1 到 123 个保持性寄存器 在远程地址 0 到 65534 处,写入 1 到 123 个保持性寄存器
11	在该指令的执行过程中,不会 MB_DATA_ADDR 和 MB_D/	≥评估 ATA_LEN 参数的值。	11	 读取服务器的状态字和專件计数器: 状态字反映了处理的状态(0 - 未处理,0xFFFF - 正在处理) Modbus请求成功执行时,事件计数器将递增。如果执行 Modbus 功能时出错,则服务器将发送消息,但不会递增事件计数器。
80	-	1	08	通过诊断代码 0x0000 检查服务器状态(返回循环测试 -服务器发回请求): ● 每次调用 1 个 WORD
81	-	1	08	通过诊断代码 0x000A复位服务器的事件计数器: ● 每次调用 1 个 WORD
101	0到 65535	1 到 2000	01	在远程地址 0 到 65535 处,读取 1 到 2000 个输出位
102	0到65535	1 到 2000	02	在远程地址 0 到 65535 处,读取 1 到 2000 个输入位
103	0到 65535	1 到 125	03	在远程地址 0 到 65535 处,读取 1 到 125 个保持性寄存器
104	0到 65535	1 到 125	04	在远程地址 0 到 65535 处,读取 1 到 125 个输入字
105	0到65535	1	05	在远程地址 0 到 65535 处,写入 1 个输出位
106	0到65535	1	06	在远程地址 0 到 65535 处,写入 1 个保持性寄存器
115	0到65535	1 到 1968	15	在远程地址 0 到 65535 处,写入 1 到 1968 个输出位
116	0到 65535	1 到 123	16	在远程地址 0 到 65535 处,写入 1 到 123 个保持性寄存器

(5) 根据功能块说明, MODBUS-TCP 从站, 建立 IP 地址关联, 按照(4) 中地址 对应关系, 实现数据交互。

	🛅 🛄 🛍 🗒 💋 转至在线 🖉	转至离线	<u>ů</u> ? [X		中搜索>	-111				
•	\$7-1500_TCP_H3u → PLC_1 [CP	U 1516-3 PN	/DP]								_ = = >	×
								拓扑视图	上 网络	见图 11 说	备视图	٦
	+ PLC 1 [CPU 1516-3 PN/DP]			-	(+) +		四名旗些					
-					- ~		× 181 194, 542					
~							₩… 模址	决		机架插	槽 1	
										0 10	.0	^
							-	PLC 1		0 0		-
=			_					▼ PROFINE	「接口 1	0 1:	K1 _	
								14 12	1	0 1	/1 P1	~
	< III > 100	%	_	•	<u></u> Y		<		_		>	
	PROFINET 接口_1 [Module]							属性	」信息	2 诊断	CLEK	M
	常规 10 变量 系统常	数 文本										
	常规	이	L								5	^
	以太网地址	以太阳地	L								[≡
	时间同步	接口连接	到									
	操作模式				75	· +====						
	▲ 品级选项 按口选面				-T-P	1 木联网						
~						添加	加新子网					
	 ▶ 实时设定 	10.44.321										
	▶ 端口 [X1 P1 R] •	IP ID IX										
_	▶ 端口 [X1 P2 R]					在项目中i	设罢 IP 地址					
	Web 服务器访问						o Jublic - T	100 100				
							่⊓ม⊎มา	192 . 168	. 0 . 1			
						9 1	≫1預6月· [255 . 255	255.0			
						□ 使用路田書	÷					
						路由書	器地址: [0.0	0.0			
						○ 在设备中]	直接设定 IP	地址				
~												1
ĥ	の日初		\$71	200_	ГСР 🕨	PLC_1 [CPU 12	15C DC/D	C/Rly] ▶ ≵	É序块 ▶ MB	_date [DB2]		
	设备											
E		🔲 📑			h 🛃	主 ° 保持实	际值 🔒	快照 🐴	🦳 将快照值	夏制到起始值中	B- B-	
			1	MB_da	te							
•	571200_TCP	^		名和	尔		数据类型	<u>u</u>	起始值	保持	可从HMI	
	📑 添加新设备		1	•	Static							
	品 设备和网络		2 .	•	▼ Slav	er_IP	TCON_IP	_v4				
	▼ [1] PLC_1 [CPU 1215C DC/DC/Rly]	=	3 .	•	• 1	rterfaceId	HW_ANY	1	64			
	□ 女性和心#5		4 .	•			CONN_O	DUQ	1			
	▼ 14线和序制		5	<u>ല</u> ഞ		onnection type	Bool 笛	=	false			
	▲ 经10000 ● 添加新块		7 .			emoteAddress	IP V4 1	·罟本	ions c	第四步		
	Main [OB1]		8 -	■	コル	ADDR	Array[1	4始的/te		设置社	7 🖉	
	J MB_date [DB2] 第→分	ŧ	9 -			ADDR[1]	Byte	大王	192	始值		
	MB_date1 [DB3]		10	• ^{里~}		ADDR[2]	Byte	4	168			
	MB_date2 [DB4]		11	•	1	ADDR[3]	Byte		0			
	MB_date3 [DB6]		12 •	•	/	ADDR[4]	Byte		88			
	MB_date4 [DB7]		13 •	•	- 1	emotePort	UInt	/	0			
	▶ □□ 系税状		14 .	- E	•	ocalPort	UInt		502 false			
	 ▶ □ ▶ □ ↓ ↓ 小部頂文件 		15 .	-	DEC	1	Bool		false			
	▶ 📮 PLC 变量		17	 -	disc	onect 1	Bool		false			
	▶ <a>Image: PLC 数据类型	~	18	•	MO	DE1	Int		0	Ä		
~	/ 详细视图										_	



🛉 🎦 🔒 保存项目 💄 🐰 🗎 🛍 🗶	う ± (2l ±				😭 🖉 सं至在	线 💋 转至离线 👗? 🛄	I ×		宝项目中搜索>	-ini		
项目树		\$7				1 [CPU 1516-3 PN/DP]	・程序坊	{ → DB2 [DB				
设备												
- 19		1	ې تۇ <u>نا</u> ئ		▶ 🚬 🙄 保	持实际值 🔒 快照 🛰	吗. 将快	999月11日	始值中 🔜 🛃 将	起始值加载为实际(ā 🔜 🖦	
			DB2									
▼ S7-1500_TCP_H3u	2 0 ^		1	呂称		数据类型	偏移重	起始值	监视值	保持	可从 HMI/	<u> </u>
📑 添加新设备		1	-00	- Sta	tic							
晶 设备和网络		2		-	date	Array[0100] of UInt	0.0					
PLC_1 [CPU 1516-3 PN/DP]	2 • 1	3	-		date[0]	UInt	0.0	0	23			
■】 设备组态		4	-00		date[1]	UInt	2.0	0	3			V
Q 在线和诊断		5	-		date[2]	UInt	4.0	0	1066		 Image: A start of the start of	
▼ 🔜 程序块	•	6	-00		date[3]	UInt	6.0	0	3141		v	
📑 添加新块		7	-00		date[4]	UInt	8.0	0	4141			 Image: A start of the start of
📲 Main [OB1]	•	8	-00		date[5]	UInt	10.0	0	13		V	
🥃 DB1 [DB2]		9	-		date[6]	UInt	12.0	0	0			 Image: A start of the start of
🥃 DB2 [DB3]		10	-		date[7]	UInt	14.0	0	14			
▶ 🐷 系统块	•	11	-00		date[8]	UInt	16.0	0	0		V	
▶ 🙀 工艺对象		12	-00		date[9]	UInt	18.0	0	1313		 Image: A start of the start of	Image: A start of the start
▶ 词 外部源文件		13	-		date[10]	UInt	20.0	0	0			
▶ 浸 PLC 变量		14	-00		date[11]	UInt	22.0	0	0		 Image: A start of the start of	Image: A start and a start
▶ 📴 PLC 数据类型	• •	15	-		date[12]	UInt	24.0	0	0		V	
∨ 详细视图		16	-		date[13]	UInt	26.0	0	0			 Image: A start of the start of
		17	-00		date[14]	UInt	28.0	0	0			 Image: A start of the start of
		18			date[15]	UInt	30.0	0	0		Image: A start of the start	 Image: A start of the start of
		19	-00		date[16]	UInt	32.0	0	0		Image: A start of the start	 Image: A start of the start of
名称	数据类型	20	-00		date[17]	UInt	34.0	0	0			

₩ Siemens - C:\Users\Administrator\Desktop\Simen_TCP\S7-1500_TCP\S7-1500_TCP_H3u\S7-1500_TCP_H3u



A Siemens - C:\Users\Administrator\Desk 项目(P) 編辑(E) 视图(V) 插入(I) 在线(O	top\Simen_TCP\S7-150) 选项(N) 工具(T)	00_TCP\S7-1500_TCP_ 窗口(W) 帮助(H)	H3u\S7-1500_TCP_H	Bu		
P C R R R R R R R R R R R R R R R R R R	う ± (# ± 量 🗓 [🖸 🖳 📮 🔊 转至在	线 💋 转至离线 🛔	a 🖪 🖪 🗶 🗏 🛄 [<在项目中搜索>	- Wi
项目树	■ ◀ \$7-150	0_TCP_H3u → PLC_	1 [CPU 1516-3 PN/I	DP] + 程序块 + DB2 [i		
设备			- 1	!	1	
E		🔍 🛃 🗮 🙄 保	特实际值 🔒 快照	🐴 🧠 将快照值复制到;	起始值中 🔍 🕵 🕴	船站始值加载为实际值 🛃
	DB2	名称	数据类型	偏移童 起始值	监视值	保持 可从
晶 设备和网络	1 🕣	 Static 				
▼ Li PLC_1 [CPU 1516-3 PN/DP]		date	Array[0200	0.0	424	
№ 在线和诊断	4 📶	date[1]	Int	2.0 0	5	
	5 🕣	date[2]	Int	4.0 0	35	
	0 7 -	date[4]	Int	8.0 0	11	
DB1 [DB2]	8 🕣	date[5]	Int	10.0 0	0	
▼ → 系统块	9 4 10 4	<pre>date[6] date[7]</pre>	Int	12.0 0	-12	
▶ 🔤 程序资源	9 11 🕣	date[8]	Int	16.0 0	-14	
 ▶ ▲ 上之对象 ▶ ➡ 小部源文件 	12 -	date[9]	Int	18.0 0	56	
▶ 📮 PLC 变重	 14 	 date[11] 	Int	22.0 0	0	
▶ <u>■ PLC 数据类型</u>	0 🞽 15 🕣	date[12]	Int	24.0 0	0	
AutoShop V2.93.01 C	\Users\Admi	nistrator\Des	ktop\Simen	_TCP\\$7-1500	- [MAIN]	
文件(F) 编辑(E) 查看(V) 梯形图(L)	PLC(P) 调	试(D) 工具(T) 向导(Z) 远	程设备 窗[](W) 帮助(H)
	▲	o e x				
	L L ++	+ + + _				Ter Tur T
	VITT H	+++	· ↓ *		+	101 101 1 1.
	4		网络1	网络注释		
□	1. 2	H	网络2	网络注释		
日 一日 元件监控衣		+				
↓ III	- F		MAIN			
信息輸出窗口						
元件名称	数据类型	显示格式	当前值		注释	
1 DO	16位整数	十进制	424			
2 D1	16位整数	十进制	5			
3 D2	16位整新	十进制	35			
4 D3	16位整新	十进制	0			
5 D4	16(合來來表	上进制	11			
e DE	10125230	上进制	0			
T DC	10129230	丁进利	0			
ра ра	16位金数	十进制	-12			
זע א	16位整数	十进制	0			
9 D8	16位整数	十进制	-14			
10 D9	16位整数	十进制	56		-	
11 D10	16位整数	十进制	0		2	
12 D11	16位整数	十进制	0			
13 D12	16位整数	十进制	0			
14 D13	16位整数	十进制	0			
15 D14	16位邀称	十讲制	0			

3. 汇川 H3u AutoShop3.0 设置

H3u 做从站,服务器。只需要在以太网配置中,设置好 IP 地址即可。

□	以太网配置
	retatu
I I I MAIN	123000 注: 勾诜自完义诜
	IP地址 192,168,0,88 ▼自定火 项,可设置印最后
·····································	子网摘码 255 . 255 . 0 第二步 开关控制,取值范
□	围1-254
MAIN	网关地址 192 . 168 . 1 . 1
	端口
	侦听端口 502
一 模块配置	
□■ 通讯配置	
COM1	
	主站配置请右键添加,不添加默认从站
	1土线映取

图 2.3.0 H3u 以太网设置