## **ProgrammerSought**

_	
_	

search	

## [Industrial control old horse] Detailed explanation of Siemen s PLC TCP protocol

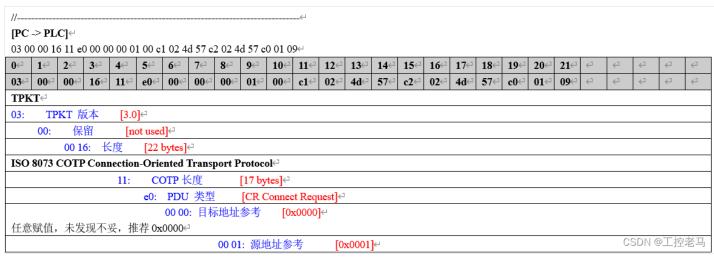
tags: Miscellaneous Notes on Industrial Control Technology Microcontroller embedde d hardware manufacture

## Detailed explanation of Siemens PLC TCP protocol

Note: Blue text indicates the cracked part, [red text] indicates the numerical description of the cracked part, black text indicates further explanation of the cracked part, black italic bold text indicates the uncracked part, and the highlighted text indicates the driver needs to process For parts that are not highlighted, just keep the default driver processing.

1.Initialize the connection

1.1 S7-200





#### [PLC -> PC]

03 00 00 16 11 d0 00 01 53 38 00 c0 01 09 c1 02 4d 57 c2 02 4d 57

0←	1←	2←	3←	4←	5∹	6←	7←	8←	9↩	10←	11←	12←	13↩	14←	15⊖	16⊖	17⊡	18←	19←	20←	21←	4	4	4	4	4
03⊡	00€	00←	16	11←	d0∈	00€	01←	53⊖	38∈	00←	<b>C</b> 0∈	01←	09↩	c1←	02←	4d∈	57⊖	c2←	02←	4 <b>d</b> ←	57⊖	↩	↩	↩	↩	↩
TPK	T←																									
03:	TP	KT 覑	反本	[3.0	)]↩																					
	00:	保	留	[n	ot used	<b>l]</b> ←																				
		00 1	6:	长度	[22]	bytes]	₽																			
ISO	8073 (	COTP	Cor	nectio	n-Orie	nted [	Transp	ort P	rotoco	ol€																
				11:	CC	отр 🕆	度	[17 b	ytes]←	1																
					d0:		类型				t Conf	irm]←														
						00 0	1: 目	标地址	参考		[0x0]	001]←														
								53 5	8: 源:	地址》	多考	[	0x535	8]←												
53 58	8 or 53	50	目前	监视到	此两種	中情况	,←																			
										00:	选	项设置	₽													
											c0:	参	数码	[Tpg	lu Size	-]←										
												01:	长度	[1	byte]	$\leftarrow$										
													09:	TPDU	」大小		[5121	oytes]	딛							
														c1:	参数			Tsap]	F							
															02:	参	数长周	更		[2 byt	es]⊖					
																4d 5	7: 源	TSAF	• [	0x4D5	7]↩					
																		c2:	参	数码		et-Ts	ap]←			
																			02:	参数	女长度	[2	2 bytes	] <del>\</del>		10.77
																				4d 5	7: 目	标 TS	SAP C	0x4D	57]ः	石当

1.2 S7-300

//-----

[PC -> PLC]

03 00 00 16 11 e0 00 00 00 00 00 c1 02 01 00 c2 02 01 02 c0 01 09

					_																		_			
0←	1←		← 4	← 5	-	6←	7←	8∈	9←	10←	11←	12←	13⊡	14←	15⊖	16⊖	17⊱	18∈	19←	20←	21←	4	4	←	4	4
03←	00←	00← 1	.6← 1	1← e(	)←	00↩	00←	00€	00€	00€	c1←	02←	01←	00←	<b>c2</b> ←	02←	01←	02←	c0←	01←	09∈	4	↩	4	Ţ	←
TPK	T←																									
03:	TP	KT 版z	k	[3.0]←																						
	00:	保留		[not u	sed	₽																				
		00 16:	长度	[1	22 b	ytes]	-																			
ISO	8073 (	COTPC	onnec	tion-C	riei	nted 7	[rans]	ort P	rotoco	ol←																
			1	1:	СО	тр К	:度		[17 by	tes]←																
							类型		[CR C		t Req	uest]←	ı													
								地址	_		k0000															
任意	赋值,	未发现	不妥,	推荐						-		•														
								00 00	): 源均	址参	考	[0	x0000	↵												
任意	赋值,	未发现	不妥,	推荐	0x0	0000€						-		-												
										00:	选巧	设置	H													
该值	为 0↩																									
											c1:	参	数码	[Src	-Tsap]	↩										
												02:	长				tes]←									
													01 00:	源	ГSAР		x4D5′	7]←								
默认	为01	00,不	故改变	Ę												_		-								
															c2:	参	数码	Ds	t-Tsap	) <del>(</del>						
																02:	参	数长周			[2 byt	es]←				
																	01 02	2:	目标:	ΓSAP		x0102	2]←			
默认	为01	02, 02	表示(	CPU 於	槽号	号↩																	-			
																			c0:	参	数码	[ <u>T</u> 1	gdu Si	ze]←		
																					参数			BBÿte∳	正控:	老马

09: TPDU 吳中 《玉遊廣電》

//-----

[PLC -> PC]

03 00 00 16 11 d0 00 00 44 31 00 c0 01 09 c1 02 01 00 c2 02 01 02

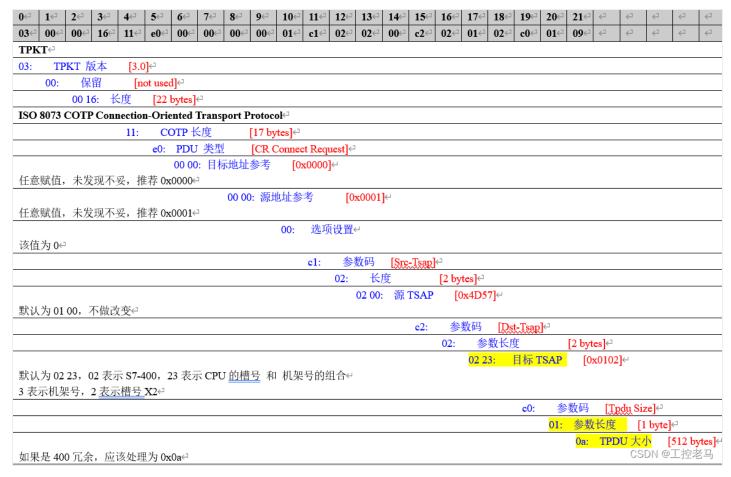
0←	1←	2←	3∈ੋ	4←	5⊖	6∈	7←	8∈	9ċ	10←	11←	12←	13⊖	14←	15⊖	16⊡	17⊖	18∈	19⊖	20←	21←	↩	←	←	←	←
03←	00€	00←	16←	11←	d0←	00←	00←	44←	31←	00←	C0←	01←	09∈	c1←	02←	01←	00€	<b>c2</b> ←	02←	01←	02←	4	4	4	4	4
TPK	T←																									
03:	TP	KT 版		[3.0	)]←																					
	00:	保			ot used	<b>l]</b> ←																				
		00 10		度		bytes]																				
ISO	8073	COTP	Con	aectio				port P	rotoco	ol←																
				11:		OTP ‡			[17 by																	
					d0:		类型				et Con															
						00 0	0: 目	标地址				001]←														
								44 3	1: 源:	地址参	多考	[	0x443	1]←												
目前	监视到	<b>到此一</b>	种情	况↩																						
\.\.\.\.\.\.\.\.\.\.\.\.\.\.\.\.\.\.\.										00:	选	<b>项设置</b>	.←													
该值	为 0↩											4- 1	det arm													
											c0:		数码		Size]											
												01:	参数			yte] <b></b>			_							
													09:		J 大小		[512 b									
-														c1:		数码		-Tsap		. 1						
-															02:		数长度			rtes]←						
																01 0	U: {	原 TSA		_	100]←		-			
																		c2:			Dst-					
																			02:		数长			ytes]←		岁旦
																				01 0	2: 目	标 TS	AP C	0x016	2 <b>j</b> ej 11.	2-1

1.3 S7-400

//-----

[PC -> PLC]

03 00 00 16 11 e0 00 00 00 01 00 c1 02 02 00 c2 02 02 23 c0 01 09



//-----

## 03 00 00 16 11 d0 00 00 44 31 00 c0 01 0ac1 02 01 00 c2 02 01 02

0←	1←	2←	3←	4←	5⊖	6∈	7∈	8∈	9←	10←	11←	12←	13∈	14□	15⊖	16∈	17∈	18∈	19⊖	20∈	21∈	4	←	4	4	4
03←	00←	00←	16←	11←	d0←	00←	00€	44←	31←	00←	<b>C</b> 0←	01←	0a←	c1←	02←ੋ	02←	00←	c2←	02←	02←	23←	4	←	4	4	4
TPK	T←																									
03:	TP	KT 版	本	[3.0	<b>]</b> ←																					
	00:	保留			ot used	l]←																				
		00 16		度		bytes]																				
ISO	8073	COTP	Coni	1ection				port P	rotoc	ol€																
				11:		OTP †			[17 by	tes]←																
					d0:		类型			Connec																
						00 0	00: 目	标地址				001]←														
				_				44 3	1: 源	地址参	考	[	0x443	1]←												
目前	监视到	刘此一和	沖情:	兄↩																						
) de 64e	vI									00:	选	项设置	$\leftarrow$													
13/1	为 0↩											4-1	det area													
											c0:				[Size]											
												01:	参数			yte]←			_							
													0a:	TPDU			[512 t									
														cl:		数码		-Tsap		1.1						
															02:		数长原			ytes]←						
																02 0	U: i	原 TSA		_	100]←		.7			
																		c2:			[Dst-]			4 1/2		
																			02:		数长			ytes]← ເລເນ ຜ		艺马
																				02.2	は: 日	你 TS	SAP <sup>CS</sup>	UXUIT	Zjem	

2 Initialize communication

//-----

[PC -> PLC]

03 00 00 19 02 f0 80 32 01 00 00 cc c1 00 08 00 00 f0 00 00 01 00 01 03 c0

0←	1←	2←	3∈	4←	5∹	6←	7ċ	8∈	9←	10←	11←	12€	13€	14∈	15€	16€	17∈	18⊖	19∈	20€	21←	22€	23∈	24←	4	←	←	↩	↩	↵
03∈	00€	00∈	19∈	02←	<b>f</b> 0←	80€	32€	01←	00€	00€	cc∈	<b>c1</b> ←	00€	08∈	00€	00€	<b>f</b> 0←	00€	00€	01←	00€	01€	03∈	<b>c</b> 0∈	↩	↩	↩	↩	↩	↩
TPF	∵T																													
03:	T	PKT	版本	:	[3.0]	Ę																								
	00:		保留		[not	used	₽																							
		00	19:	长度	Ę	[25 b	ytes]	$\leftarrow$																						
ISO	8073	CO	TPC	onnec	ction-	Orie	nted	Trans	port	Prot	col∈																			
				02:		COT	P K	度	[	2 byte	es]←																			
					f0:	PD	U 类	型	[[	T DA	ATA]€																			
						80:	目标	地址	参考		[0:	<b>c</b> 0000	<b>)</b> (																	
												.000	0000	= TP	DU n	umbe	r [0x0	⊃[00												
												1	= L	ast da	ata un	nit [Ye	s]←													
							32 (	01: PC	$\leftarrow$																					
									00 (	00:	↩																			
											CC (	:1:	时间	戳↩																
													00 0	8:	内线	容长月	度(从:	f0 开	始)	[8 b	ytes]	Ę								
															00	00 f0	00 00	01 0	0 01	03 c0	: ←									
在测	试中	一直	[未变	化,	猜测	为固氮	宇長	及↩																			CSDI	/ @I	控老	;⊒j

[PLC -> PC]

03 00 00 1b 02 f0 80 32 03 00 00 cc c1 00 08 00 00 00 f0 01 00 01 00 01 00 f0

00 10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200 210 220 230 240 250 260 0 0 0
034 004 004 1b4 024 f04 804 324 034 004 004 ccc c14 004 084 004 004 004 f04 014 004 014 004 014 004 f04 44 44
TPKT₽
03: TPKT 版本 [3.0]←
00: 保留 [not used]←
00 1b: 长度 [27 bytes]↩
ISO 8073 COTP Connection-Oriented Transport Protocol <sup>□</sup>
02: COTP 长度 [2 bytes]↩
f0: PDU 类型 [DT DATA]←
80: 目标地址参考 [0x0000←
.000 0000 = TPDU number [0x00]←
1 = Last data unit [Yes]←
32 03: PLC←
00 00: ←
cc c1: 时间戳←
00 08: 内容长度(从 f0 开始) [8 bytes]←
00 00 00 00 f0 01 00 01 00 01 00 f0:←
在测试中一直未变化,猜测为固定字段中 CSDN @工控老

3. Read data

3.1 Typical example [Mo]

//-----

[PC -> PLC]

03 00 00 1f 02 f0 80 32 01 00 00 00 00 00 00 00 04 01 12 0a 10 02 00 01 00 00 83 00 00 00

0/24/23, 8:21 PM	[Indus	strial co	ntrol o	old ho	orse] De	etaile	d expla	natior	of Sie	emen	ns PLC	CTC	P pro	otoco	ıl - Pı	rogra	amme	er Sou	ught	
0  1  2  3  4  5  6  7  8	94 104	11← 1	2← 13←	146	15← 16←	174	18 19	€ 20€	21 2	2← 23	3∈ 24∈	25€	264	27€ :	28€ 2	29← 3	30← ←	4 4	ے د	2 2
03 00 00 1f 02 f0 80 32 01			0 00 €			_	-	-			0∈ 01∈	-	-		_	_	00€ €	41 4	1 41	4 4
TPKT←	000	000	00	06	00 00	04	01 12	Ua.	10 0	25 00	01	00	00	03	000	000	000	- 7		
03: TPKT 版本 [3.0]←																				
00: 保留 [not used]↩																				
00 1f: 长度 [31 byte																				
ISO 8073 COTP Connection-Oriente		ort Prot	tocol⊬																	
02: COTP 长度	[2	bytes]	Ę																	
f0: PDU 类型	[DT	DATA	₽																	
80: 🗏	标地址参	考	[0x0	0000€	1															
			.0	000 0	000 = TP	DU 1	number	[0 <b>x</b> 00]	$\leftarrow$											
			1		= Last d	ata uı	nit [Yes]	$\leftarrow$												
32 01:	PC←																			
	00 00:	2																		
		00 00	: B	时间覆	<b>V</b> ←															
		00 00		) 0e:		<del>长</del> 度	(从 04 升	干地)	Γ14 h	artes l	4									
根据内容长度确定↩			00	, oc.	ring	人人又	(/)( 04 )	1 74)	[140	ytesj	`									
<b>松州内存以及州足</b> 、					00 00:	米行	据长度	诗粉	(相理)	00.0	004									
读数据不做改变↩					00 00:	奴	加 以及:	) 厌爱	加利力	( 00 (	000									
写数据 s7-300: ←																				
Bit, Byte: 05←																				
Short, <u>Ushort</u> : 06←																				
Long, Float: 08←																				
4																				
写数据 s7-200←																				
Bit, Byte, Short, <u>Ushort</u> : 06←																				
Long, Float: 08←																				
						04	: 读操											0011		5-F/T/
							01:	包数目	[1	Pac]	$\leftarrow$						C	2DIV (	⊕j:	空老马
根据包数目确定,推荐01℃																				
							12	0a 10	02: 3	变量数	数据排	列格	式	$\leftarrow$						
推荐 12 0a 10 02↩																				
12 0a 10 01:位排列←																				
12 0a 10 02:字节排列←																				
12 0a 10 04: 字排列←																				
12 0a 10 06: 双字排列↩																				
										00	01:	变量	数目	[1x	c1=11	byte]	$\forall$			
根据变量数据排列格式和变量字节数	[确定数目	$\leftarrow$																		
											0	0 00:	F	PLC 存	字储 [≥	区地均	<mark>L</mark> ←			
根据具体存储区确定↩																				
DB Section Adr/256 Adr%256 ←																				
V Section 00 01←																				
other Sections 00 00€																				
													83:	PLC	存储	<mark>X</mark> ←				
根据具体存储区确定↩																				
I Section 81€																				
Q Section 82←																				
M Section 83←																				
DB Section 84																				
V Section 84€																				
Takeskiikii o+														0,00,0	00. *	5/01	(2 July 1-	L.		
根据目休 <u>德</u> 教斯·杜· <b>·</b> ·································													g	000	υ <b>υ:</b> [	四個社	罗坦耳	L		
根据具体偏移地址确定←																				
Offset Address*8/0x10000←																				
(Offset Address*8/0x10000) /256←																	-	000	-T-1-	カナア
(Offset Address*8/0x <u>10000)%</u> 256←																	C	2DM (	<b>₽</b> ⊥∄	空老马

10/24/23, 8:21 PM

//-----

[PLC -> PC]

03 00 00 1a 02 fo 80 32 03 00 00 00 00 02 00 05 00 00 04 01 ff 04 00 08 ec

0← 1	<i>←</i> 2	3←	-	5⊖	6∈	7ċ		9ċ	10∈	11€	12€	13€	14€	15€	16∈	17∈	18∈	19∈	20€	21€	22€	23€	24€	25€	↵	←	↩	↵	↩	$\leftarrow$
03∈ 0	0 ⊖0	00← 1a←	02∈	f0∈	80€	32€	03€	00€	00€	00€	00€	00€	02€	00€	05€	00€	00€	04←	01	ff⊍	04€	00	08€	ec≓	7	↩	↩	4	₹	$\leftarrow$
TPKT	`←																													
03 00	00 1a	ı←																												
03:	TP	KT 版	<b>*</b>	[3.0]	↩																									
	00:	保留		[no	t use	<b>d]</b> ←																								
		00 1a:	长度	Ę	[26]	bytes	₽																							
ISO 8	073 C	COTP	Connec	ction	-Orie	ented	Tran	spoi	t Pro	otoco	$\leftarrow$																			
			02:	С	OTP	长度		[2	byte	:s]←																				
				f0:	PD	U 类	텣	[D	T DA	ATA]€	2																			
					80:	目标	地址	参考		[0x	0000	$\leftarrow$																		
											.000	0000	= TP	DU n	umbe	r [0x	00]←													
											1	= L	ast d	ata ur	nit [Ye	es]←														
						32	03: PI	LC←																						
								00	00:	$\leftarrow$																				
										00 (	00:	时	间戳	딛																
												00	02:←	1																
														00	05:	内	容长	度(从	, ff ₹	F始)	[5	bytes	j⇔							
																00	00:€	3												
																		04:	读技	操作←	3									
																			01:	包	数目	[1]	Pac]	-						
																				ff (	)4: -	包起	始标	志↩						
																						00 (	08:	变量	量长/	度 [8	bits]	_		
按位さ	<u>⊦</u> ←																													
																								ec:	变	を量値	@SD	N @_	□控≉	;프

3.2 Reference example [VB0 VB254 VB255]

//-----

```
03 00 00 2b 02 f0 80 32 01 00 00 00 00 00 01 a 00 00 4 02 12 0a 10 02 00 01 00 01 84 00 00 01 20 a 10 02 00 02 00 01 84 00 07 f0
TPKT \leftarrow
03:
     TPKT 版本
                  [3.0]←
  00:
        保留
                 [not used]←
    00 2b:
          长度
                 [43 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
             COTP 长度
                           [2 bytes]←
              PDU 类型
                           [DT DATA]←
            80: 目标地址参考
                           [0x0000↔
                              .000\ 0000 = TPDU\ number\ [0x00] \leftarrow
                              1... .... = Last data unit [Yes]←
                32 01: PC←
                   00 00:
                       00 00:
                               时间戳 ↩
                            00 1a: 内容长度(从 04 开始) [26 bytes]←
根据内容长度确定↩
                                                 00 00:
                                                        数据长度,读数据默认 00 00€
读数据不做改变↩
写数据 s7-300: ←
Bit, Byte: 05←
Short, Ushort: 06←
Long, Float: 08←
写数据 s7-200←
Bit, Byte, Short, Ushort: 06€
Long, Float: 08€
                                                                                                     CSDN @工控老马
                                          读操作↩
                                        02: 包数目 [2 Pac]←
根据包数目确定,推荐01↩
                                          12 0a 10 02: 变量数据排列格式 ↔
推荐 12 0a 10 02←
12 0a 10 01: 位排列←
12 0a 10 02: 字节排列←
12 0a 10 04: 字排列↩
12 0a 10 06: 双字排列↩
                                                     00 01: 变量数目 [1x1=1byte]←
根据变量数据排列格式和变量字节数确定数目↩
                                                        00 01: PLC 存储区地址↔
根据具体存储区确定↩
DB Section
           Adr/256 Adr%256 ←
V Section
                  01←
                  00↩
other Sections 00
                                                            84: PLC 存储区←
根据具体存储区确定↩
I Section
           82←
Q_Section
M. Section
           83←
           84←
DB_Section
Y Section
           84←
                                                               00,00,00: 包偏移地址↔
根据具体偏移地址确定↩
Offset Address*8/0x10000←
(Offset Address*8/0x10000) /256←
(Offset Address*8/0x10000) %256
                                                                      12 0a 10 02: 变量数据排列格式 ↔
推荐 12 0a 10 02←
                                                                                                     CSDN @工控老马
12 0a 10 01: 位排列←
```

```
12 0a 10 02: 字节排列←
12 0a 10 04: 字排列←
12 0a 10 06: 双字排列↩
                                                                               00 02: 变量数目 [2x1=2byte]←
根据变量数据排列格式和变量字节数确定数目↩
                                                                                   00 01: PLC 存储区地址↔
根据具体存储区确定↓
          Adr/256 Adr%256 ←
DB Section
Y Section
           00
                  01←
other Sections
                  00←
                                                                                       84 PLC 存储区←
根据具体存储区确定↩
           81←
I Section
Q Section
           82←
M_Section
           83←
DB Section
           84←
           84←
V_Section
                                                                                         00 07 f0: 包偏移地址↔
根据具体偏移地址确定↩
Offset Address*8/0x10000←
(Offset Address*8/0x10000) /256←
                                                                                                     CSDN @工控老马
(Offset Address*8/0x10000)%256←
```

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
03 00 00 21 02 f0 80 32 03 00 00 00 00 00 02 00 0c 00 00 04 02 ff 04 00 08 43 00 ff 04 00 10 00 00
TPKT←
03:
      TPKT 版本
                     [3.0]
          保留
   00:
                    [not used]←
     00 21: 长度
                    [23 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
                 COTP 长度
          02:
                                  [2 bytes]←
                 PDU 类型
                               [DT DATA]←
               80: 目标地址参考 [0x0000↩
                                    .000\ 0000 = TPDU\ number\ [0x00] \leftarrow
                                    1... .... = Last data unit [Yes]←
                  32 03: PLC←
                       00 00:
                               \leftarrow
                             00 00:
                                      时间戳 ↩
                                 00 02: ←
                                                 内容长度(从 ff 开始)
                                       00 0c:
                                                                     [12 bytes]←
                                           00 00:←
                                                04: 读操作↩
                                                       包数目 [2 Pac]←
                                                          包起始标志↩
                                                     ff 04:
                                                                 变量长度 [8 bits]←
                                                         00 08:
按位计↩
                                                            43 00:
                                                                    变量值↩
                                                                 ff 04: 包起始标志₽
                                                                              变量长度[16 bits]←
                                                                     00 10:
按位计↩
                                                                                   变量值↩
                                                                          00 00:
                                                                                                                       CSDN @工控老马
```

4 Write data

4.1 S7-200

4.1.1 Typical example [MBo]

//-----

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
TPKT←
     TPKT 版本
                 [3.0]←
03:
  00:
        保留
                [not used]←
    00 25: 长度
                 [37 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol<sup>™</sup>
              COTP 长度
                            [2 bytes]←
          f0: PDU 类型
                         [DT DATA]←
            80: 目标地址参考 [0x0000←
                             .000 0000 = TPDU number [0x00]←
                             1... .... = Last data unit [Yes]←
               32 01: PC←
                        00 00:
                               时间戳↩
                                                                                                  CSDN @王控老马
                            00 0e: 内容长度 [14 bytes]←
```

```
从 05 开始计数↩
                                                     数据长度,读数据默认 00 00€
读数据不做改变↩
写数据 s7-300: ←
Bit, Byte: 05←
Short, Ushort: 06←
Long, Float: 08←
写数据 s7-200←
Bit, Byte, Short, Ushort: 06←
Long, Float: 08€
                                   05: 写操作↩
                                     01: 包数目 [1 Pac]←
根据包数目确定,推荐01↩
                                       12 0a 10 02: 变量数据排列格式 ↔
推荐 12 0a 10 02←
12 0a 10 01: 位排列↩
12 0a 10 02: 字节排列←
12 0a 10 04: 字排列↩
12 0a 10 06: 双字排列↩
                                               00 01: 变量数目
                                                               [1x1=1byte]←
根据变量数据排列格式和变量字节数确定数目↩
                                                          PLC 存储区地址↩
                                                   00 00:
根据具体存储区确定↩
DB Section
         Adr/256 Adr%256 ←
Y Section
                 01←
                00↩
          00
other Sections
                                                       83: PLC 存储区 ←
                                                                                               CSDN @工控老马
根据具体存储区确定↩
```

```
I Section
Q_Section
          82←
          83←
M_Section
DB Section
          84←
          84←
V Section
                                                         00.00.00: 包偏移地址 + 位偏移地址↔
根据具体偏移地址确定↩
(包偏移地址 + 位偏移地址)*8/0x10000₽
((包偏移地址 + 位偏移地址)*8%0x10000)/256↩
(包偏移地址 + 位偏移地址)*8%0x10000%256₽
                                                                00 04: 位标志↔
00 03: - 位操作←
00 04: - 非位操作↩
                                                                     00 08: 变量长度
                                                                                     [8 Bit]←
按位计↩
                                                                             变量值 ↩
                                                                                              CSDN @工控老马
                                                                        0a 00:
```

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 \,\circlearrowleft
03 00 00 16 02 f0 80 32 03 00 00 00 00 02 00 01 00 00 05 01 ff
TPKT \leftarrow
       TPKT 版本
                      [3.0]←
          保留
                    [not used]←
     00 16: 长度
                     [22 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
                 COTP 长度
                                 [2 bytes]←
              f0: PDU 类型
                                 [DT DATA]←
                80: 目标地址参考
                                   [0x0000←
                                      .000 0000 = TPDU number [0x00]←
                                      1... .... = Last data unit [Yes]←
                   32 03: PLC←
                        00 00:
                              00 00:
                                       时间戳 ↩
                                  00 02: ←
                                                  内容长度(从 ff 开始)
                                        00 01:
                                                                        [1 byte]←
                                             00 00:←
                                                  05: 写操作↩
                                                     01: 包数目 [1 Pac]←
                                                                                                                          CSDN @工控老马
                                                       ff: 停止符↩
```

4.1.2 Reference example [Q0.0]		
//	 	
[PC -> PLC]		

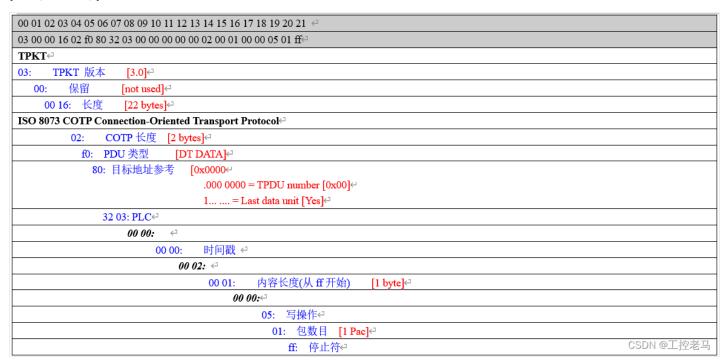
```
10/24/23. 8:21 PM
                                      [Industrial control old horse] Detailed explanation of Siemens PLC TCP protocol - Programmer Sought
  00\ 01\ 02\ 03\ 04\ 05\ 06\ 07\ 08\ 09\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30\ 31\ 32\ 33\ 34\ 35\ 36 e^{-1}
  03 00 00 25 02 f0 80 32 01 00 00 00 00 00 0e 00 06 05 01 12 0a 10 01 00 01 00 08 30 00 00 00 00 03 00 10 10 00
  TPKT←
  03:
         TPKT 版本
                        [3.0]
     00:
            保留
                       [not used]←
        00 25:
               长度
                       [37 bytes]←
  ISO 8073 COTP Connection-Oriented Transport Protocol
                    COTP 长度
                               [2 bytes]←
                    PDU 类型
                                  [DT DATA]←
               f0:
                 80: 目标地址参考[0x0000~
                                    .000 0000 = TPDU number [0x00]←
                                   1... .... = Last data unit [Yes]←
                   32 01: PC←
                        00 00:
                                \leftarrow
                             00 00:
                                      时间戳↩
                                  00 0e:
                                            内容长度 [14 bytes]←
   从 05 开始计数↩
                                                                     数据长度,读数据默认0000℃
                                                            00 00:
  读数据不做改变↩
  写数据 s7-300: ←
  Bit, Byte: 05←
  Short, Ushort: 06←
  Long, Float: 08←
  写数据 s7-200←
  Bit, Byte, Short, Ushort: 064
  Long, Float: 08€
                                                                                                                          CSDN @工控老马
                                                写操作↩
                                               01: 包数目
                                                              [1 Pac]←
                                                  12 0a 10 01: 变量数据排列格式 ↔
   12 0a 10 01: 位排列←
   12 0a 10 02: 字节排列↩
   12 0a 10 04: 字排列↩
   12 0a 10 06: 双字排列↩
                                                           00 01: 变量数目
                                                                              [1x1=1byte]←
   根据变量数据排列格式和变量字节数确定数目↩
```

```
00 00:
                                                          PLC 存储区地址←
DB Section
           Adr/256 Adr%256 ←
           00
                 01←
V_Section
other Sections 00
                 00€
                                                        83: PLC 存储区←
I Section
           81←
Q Section
          82←
           83←
M Section
           84←
DB Section
           84←
V_Section
                                                         00 00 00: 包偏移地址 + 位偏移地址↔
(包偏移地址 + 位偏移地址)*8/0x10000~
((包偏移地址 + 位偏移地址)*8%0x10000)/256↔
(包偏移地址 + 位偏移地址)*8%0x10000%256₽
                                                               00 03: 位标志↩
00 03:- 位操作↔
00 04:- 非位操作↩
                                                                    00 01: 变量长度 [1 Bit]←
按位计↩
                                                                        01 00: 变量值↩
                                                                                                    CSDN @工控老马
```

[PLC -> PC]

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
03 00 00 16 02 f0 80 32 03 00 00 00 00 02 00 01 00 00 05 01 ff
TPKT←
03:
      TPKT 版本
                    [3.0]←
  00:
         保留
                   [not used]←
     00 16: 长度
                   [22 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
               COTP 长度
                               [2 bytes]←
           f0: PDU 类型
                             [DT DATA]←
             80: 目标地址参考 [0x0000←
                                 .000 0000 = TPDU number [0x00]←
                                 1... .... = Last data unit [Yes]←
               32 03: PLC←
                    00 00:
                         00 00:
                                  时间戳↩
                             00 02: ←
                                            内容长度(从ff开始)
                                   00 01:
                                                                [1 byte]←
                                        00 00:↩
                                             05: 写操作↩
                                               01: 包数目 [1 Pac]←
                                                                                                                 CSDN @工控老马
                                                  ff: 停止符↩
```

```
00\ 01\ 02\ 03\ 04\ 05\ 06\ 07\ 08\ 09\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30\ 31\ 32\ 33\ 34\ 35\ \hookleftarrow
TPKT←
      TPKT 版本
                   [3.0]
   00:
         保留
                  [not used]←
     00 24: 长度
                  [36 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
               COTP 长度
                         [2 bytes]←
           f0: PDU 类型
                           [DT DATA]←
             80: 目标地址参考
                             [0x0000←
                                .000 0000 = TPDU number [0x00]←
                                1... .... = Last data unit [Yes]←
              32 01: PC←
                   00 00:
                        00 00:
                                时间戳←
                            00 0e: 内容长度 [14 bytes]←
从 05 开始计数↩
                                                   00 00:
                                                          数据长度,读数据默认 00 00€
读数据不做改变↩
写数据 s7-300: ←
Bit, Byte: 05←
Short, Ushort: 06←
Long, Float: 08←
写数据 s7-200←
Bit, Byte, Short, Ushort: 064
Long, Float: 08€
                                    05: 写操作↩
                                       01: 包数目 [1 Pac]←
                                                                                                        CSDN @工控老马
                                        12 0a 10 02: 变量数据排列格式↔
12 0a 10 01: 位排列↩
12 0a 10 02: 字节排列←
12 0a 10 04: 字排列←
12 0a 10 06: 双字排列↩
                                                 00 01: 变量数目 [1x1=1byte]←
根据变量数据排列格式和变量字节数确定数目↩
                                                            PLC 存储区地址↔
                                                     00 00:
DB Section
           Adr/256 Adr%256 ←
V. Section
                  01←
                  00←
other Sections
            00
                                                          83: PLC 存储区←
I_Section
           81←
Q Section
           82←
M. Section
           83←
DB Section
           84←
V. Section
           84←
                                                           00.00 00: 包偏移地址 ←
包偏移地址*8/0x10000↩
(包偏移地址*8%0x10000)/256↩
(包偏移地址*8%0x10000)%256₽
                                                                  00 04: 位标志↔
00 03:- 位操作↔
00 04:- 非位操作←
                                                                      00 08: 变量长度 [8 Bit]←
按位计↩
                                                                                                        CSDN @工控老马
                                                                           09: 变量值←
```

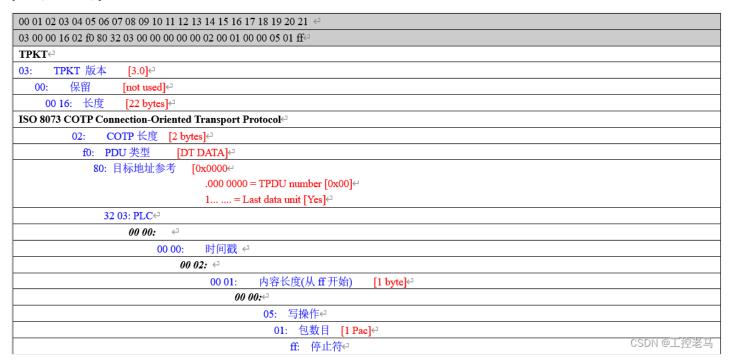




```
00\ 01\ 02\ 03\ 04\ 05\ 06\ 07\ 08\ 09\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30\ 31\ 32\ 33\ 34\ 35\ \hookleftarrow
 TPKT←
      TPKT 版本
 03:
                   [3.0]←
   00:
          保留
                  [not used]←
     00 24: 长度
                   [36 bytes]←
 ISO 8073 COTP Connection-Oriented Transport Protocol
                COTP 长度
                          [2 bytes]←
           f0: PDU 类型
                            [DT DATA]←
             80: 目标地址参考
                              [0x0000←
                                 .000 0000 = TPDU number [0x00]←
                                1... .... = Last data unit [Yes]←
               32 01: PC←
                   00 00:
                         00 00:
                                时间戳←
                             00 0e: 内容长度 [14 bytes]←
 从 05 开始计数↩
                                                           数据长度,读数据默认 00 00€
                                                    00 00:
 读数据不做改变↩
 写数据 s7-300: ←
 Bit, Byte: 05←
 Short, Ushort: 06←
 Long, Float: 08←
 写数据 s7-200←
 Bit, Byte, Short, Ushort: 064
Long, Float: 08€
                                         写操作↩
                                        <mark>01: 包数目</mark> [1 Pac]←
                                                                                                          CSDN @工控老马
                                         12 0a 10 02: 变量数据排列格式↔
12 0a 10 01: 位排列←
12 0a 10 02: 字节排列←
12 0a 10 04: 字排列←
12 0a 10 06: 双字排列↩
                                                 00 01: 变量数目
                                                                   [1x1=1byte]←
根据变量数据排列格式和变量字节数确定数目↩
                                                      00 00:
                                                             PLC 存储区地址←
           Adr/256 Adr%256 ←
DB Section
V_Section
            00
                  01←
other Sections
            00
                  00←
                                                           83: PLC 存储区←
I Section
           81←
           82←
Q Section
           83←
M_Section
           84←
DB_Section
V_Section
           84€
                                                             00,00,00: 包偏移地址 ←
包偏移地址*8/0x10000↩
(包偏移地址*8%0x10000)/256↩
(包偏移地址*8%0x10000)%256₽
                                                                   00 04: 位标志
00 03:- 位操作←
00 04: - 非位操作↩
                                                                       00 08: 变量长度
                                                                                         [8 Bit]←
按位计↩
```

CSDN @工控老马

09: 变量值←





```
10/24/23. 8:21 PM
                           [Industrial control old horse] Detailed explanation of Siemens PLC TCP protocol - Programmer Sought
  TPKT←
       TPKT 版本
  03:
                 [3.0]←
    00:
         保留
                [not used]←
     00 25:
           长度
                 [37 bytes]←
  ISO 8073 COTP Connection-Oriented Transport Protocok
                       [2 bytes]←
              COTP 长度
           f0: PDU 类型
                        [DT DATA]←
            80: 目标地址参考
                          [0x0000←
                            .000 0000 = TPDU number [0x00]←
                            1... .... = Last data unit [Yes]←
              32 01: PC←
                 00 00:
                     00 00:
                            时间戳 ↩
                         00 Of:
                               内容长度 [15 bytes]←
  与读操作从 04 开始计数不同,该内容长度表示 000d 加上写入数据的长度的和₽
                                                  数据长度,读数据默认0000℃
                                            00 00:
  读数据不做改变↩
  写数据 s7-300: ←
  Bit, Byte: 05←
  Short, Ushort: 06←
  Long, Float: 08←
  写数据 s7-200←
  Bit, Byte, Short, Ushort: 06←
  Long, Float: 08€
                                05: 写操作←
                                                                                         CSDN @工控老马
                                  01: 包数目
                                             [1 Pac]←
                                    12 0a 10 02: 变量数据排列格式↔
  12 0a 10 01: 位排列←
  12 0a 10 02: 字节排列←
  12 0a 10 04: 字排列↩
  12 0a 10 06: 双字排列↩
                                           00 02: 变量数目 [2x1=2byte]←
  根据变量数据排列格式和变量字节数确定数目↩
```

```
PLC 存储区地址↔
                                                     00 00:
DB Section
           Adr/256 Adr%256 ←
            00
                  01←
V. Section
other Sections
                  00€
                                                          83: PLC 存储区←
I Section
           81←
           82←
Q Section
M Section
           83←
DB_Section
           84←
V Section
           84←
                                                            00.00 00: 包偏移地址 ←
包偏移地址*8/0x10000↩
(包偏移地址*8%0x10000)/256↩
(包偏移地址*8%0x10000)%256₽
                                                                  00 04: 位标志↔
00 03:- 位操作←
00 04:- 非位操作↩
                                                                      00 10: 变量长度
                                                                                       [16 Bit]←
按位计↩
                                                                           03 03: 变量值←
                                                                                                        CSDN @工控老马
```

#### [PLC -> PC]

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
03 00 00 16 02 f0 80 32 03 00 00 00 00 02 00 01 00 00 05 01 ff€
TPKT \leftarrow
       TPKT 版本
                     [3.0]
   00:
          保留
                    [not used]←
     00 16: 长度
                    [22 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
                 COTP 长度 [2 bytes]←
            f0: PDU 类型
                               [DT DATA]←
               80: 目标地址参考
                                  [0x0000←
                                     .000\ 0000 = \text{TPDU number } [0x00] \leftarrow
                                     1... .... = Last data unit [Yes]←
                 32 03: PLC←
                      00 00:
                                     时间戳 ↩
                           00 00:
                                00 02: ←
                                      00 01:
                                               内容长度(从 ff 开始)
                                           00 00:←
                                                05: 写操作↩
                                                  01: 包数目 [1 Pac]←
                                                     ff: 停止符↩
                                                                                                                         CSDN @工控老马
```

4.2.4 Typical Example [MW0] Another protocol frame, the difference lies in the variable data arrangement format and the number of variables

//-----

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
TPKT←
03:
     TPKT 版本
                 [3.0]←
  00:
        保留
                [not used]←
    00 25: 长度
                 [37 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
              COTP 长度
                       [2 bytes]←
             PDU 类型
                         [DT DATA]←
            80: 目标地址参考
                           [0x0000←
                              .000 0000 = TPDU number [0x00]←
                             1... .... = Last data unit [Yes]←
              32 01: PC←
                 00 00:
                      00 00:
                             时间戳 ↩
                          00 Of:
                                内容长度 [15 bytes]←
与读操作从 04 开始计数不同,该内容长度表示 000d 加上写入数据的长度的和□
                                                      数据长度,读数据默认0000←
                                               00 00:
读数据不做改变↩
写数据 s7-300: ←
Bit, Byte: 05←
Short, Ushort: 06←
Long, Float: 08←
写数据 s7-200←
Bit, Byte, Short, Ushort: 064
Long, Float: 08€
                                  05: 写操作↩
                                    01: 包数目
                                                [1 Pac]←
                                                                                                 CSDN @工控老马
                                      12 0a 10 04: 变量数据排列格式↔
12 0a 10 01: 位排列←
12 0a 10 02: 字节排列←
12 0a 10 04: 字排列←
12 0a 10 06: 双字排列↩
                                             00 01: 变量数目 [2x1=2byte]←
根据变量数据排列格式和变量字节数确定数目↩
                                                        PLC 存储区地址←
DB Section
          Adr/256 Adr%256 ←
V. Section
                 01←
          00
                 00€
other Sections
                                                      83: PLC 存储区←
          81←
I Section
          82←
O Section
M Section
          83←
DB Section
          84€
V_Section
                                                        00.00 00: 包偏移地址 ←
包偏移地址*8/0x10000↩
(包偏移地址*8%0x10000)/256↩
(包偏移地址*8%0x10000)%256₽
                                                              00 04: 位标志←
00 03:- 位操作←
00 04:- 非位操作←
                                                                  00 10: 变量长度
                                                                               [16 Bit]←
按位计↩
                                                                      03 03: 变量值↩
                                                                                                 CSDN @工控老马
```

[PLC -> PC]

```
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 \,\circlearrowleft
03 00 00 16 02 f0 80 32 03 00 00 00 00 02 00 01 00 00 05 01 ff\!\!\!\!/
TPKT←
03:
      TPKT 版本 [3.0]←
         保留
                   [not used]←
     00 16: 长度
                  [22 bytes]←
ISO 8073 COTP Connection-Oriented Transport Protocol
                COTP 长度 [2 bytes]←
            f0: PDU 类型
                             [DT DATA]←
              80: 目标地址参考 [0x0000←
                                   .000 0000 = TPDU number [0x00]←
                                   1... .... = Last data unit [Yes]←
                32 03: PLC←
                    00 00: ←
                                   时间戳 ↩
                          00 00:
                              00 02: ←
                                    00 01:
                                             内容长度(从 ff 开始) [1 byte]₽
                                         00 00:←
                                              05: 写操作↩
                                                01: 包数目 [1 Pac]←
                                                                                                                    CSDN @工控老马
                                                   ff: 停止符↩
```

Copyright Complaint Spam Report

8

Powered By **VDO.AI** 

Golang tcp forwarding remoteAddr error

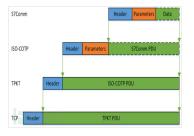
## **Intelligent Recommendation**

[Industrial control old horse] Detailed explanation of Siemens PLC TCP protocol - Programmer Sought

# URG urgent data (generally not used) ACK ACK # source port # dest port # by bytes of data wild # bytes wild # bytes wild # bytes # by

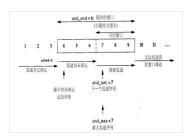
## TCP protocol detailed explanation

Articles directory Foreword 1. Overview of the TCP protocol 1. Protocol features 2.TCP message segment Second, TCP reliable data transmission 1 Overview 2. Re -timeout time selection 3. Quick re -tran...



## Siemens PLC protocol-S7COMM-extended

Siemens PLC protocol-S7COMM-extended Article Directory Siemens PLC protocol-S7COMM-extended S7 Communication structure TPKT protocol structure For example COTP protocol Introduction COTP connection pa...



## LwIP protocol stack-TCP control block (tcp\_pcb) detailed explanation

The source code of the tcp\_pcb structure of the TCP part of the LWIP protocol is as follows: struct tcp\_pcb { IP\_PCB;//This is a macro that describes the IP related information of the

connection, incl...



## Use QT to give Siemens PLC to Siemens PLC through the Modbusrtu protocol

demand Use the host computer software to control the qo.o indicator of the lower computer through the ModbusRTU protocol material computer1 USB turn 485 device1 PLC(s7-

200)\*1 Next machine PLC program:...

10/24/23. 8:21 PM

0 7.8 15.16 · 31
8位类型 8位代码 16位检验和
(不同类型和代码有不同的内容) 
(不同类型和代码有不同的内容)

[Industrial control old horse] Detailed explanation of Siemens PLC TCP protocol - Programmer Sought

## #TCP/IP# Detailed Explanation of TCP IP Volume 1: Protocol-Chapter 6 ICMP: Internet Control Message Protocol

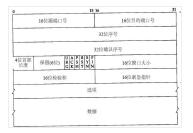
6.1 Introduction I C M P is often considered as an integral part of the I P layer. It transmits error messages and other information

that needs attention. I C M P messages are usually used by IP layer...

Credit Card Rates in Khu Pho Luong Binh May Shock You

Credit Cards | Search Ads

## **More Recommendation**



"TCP/IP Detailed Explanation Volume 1: Prot ocol" Reading Notes Chapter 17 TCP: Transmission Control Protocol

Source http://blog.csdn.net/jiange\_zh code> Chapter 17 TCP: Transmission Control Protocol 1. TCP services TCP provides a

connection-oriented, reliable byte stream service. Connection-oriented means...



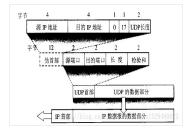
How to quickly implement Siemens S7-200/ 300 PLC to Modbus-TCP protocol and third-p arty data docking

How to quickly implement Siemens S7-200/300 PLC to Modbus-TCP protocol and third-party data docking introduction

Siemens SIMATIC automation control system is widely used in the industrial control mark...

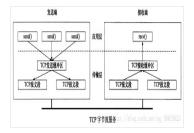
## C # with Mitsubishi PLC communication detailed use (FX5U i ndustrial control equipment)

The last article talks about any communication with Mitsubishi PLC device, this detailed introduction to the use of the project. Reading writes including 32-bit data registers. 1. Data registers (such...



## Detailed explanation of TCP / UDP protocol

Both TCP and UDP protocols are transport layer protocols, a specification used to transmit data. TCP data packet format The sequence number is seq, the acknowledgment number corresponds to ack, and FI...



## Detailed explanation of TCP/UDP protocol

Detailed TCP protocol The TCP connection is full-duplex, that is, both sides can read and write data through one connection. The TCP protocol connection is one-to-one, so applications based on broadca...

### **Related Posts**

- [Industrial control old horse] Siemens PLC s7-300SCL programming detailed explanation
- [Industrial Control Old Horse] Modbus TCP Detailed Explanation

- [Industrial control old horse] Detailed design plan of marquee control system based on Siemens S7-200PLC
- Industrial control old horse Detailed design of washing machine PLC program control system
- [Industrial Control Old Horse] ASCII communication guide for ABB AC500 series
   PLC and West 8100+ series instrument
- [Industrial control old horse] Mitsubishi Q series PLC debugging and Mitsubishi touch screen alarm instructions
- [Industrial Control Old Malays] Omron PLC Socket Send FINS / TCP Command Analysis
- Siemens PLC protocol-S7COMM
- Detailed explanation of TCP protocol (5)-TCP congestion control
- TCP flow control and congestion control-detailed explanation of sliding window protocol

## Xem thử bạn có nhận ra ai trong số những người nổi tiếng không tran...

**BestFamilyMag** 

Changarad Links by Tabasla

## **Popular Posts**

- Keywords: packet
- idea integrates tomcat and solves the console garbled problem
- [SOJ 639] trees
- Xiaobaixue front-end ------CSS basic grammar

- MYSQL date and time type format (detailed introduction)
- Network stream (template transfer)
- Layui jq finds the elements of the first element
- Python Algorithm Learning: Competitive Code Programming-Lanqiao Cup School Trial (Preliminary) Replay
- Freeswitch startup service script
- RISCV's cache

### **Recommended Posts**

Data Structures and Algorithms basis

- Front End Knowledge Sharing SHEETJS Usage Experience
- Solve Endnote's reference to the problem without GBT7714 format
- Day04 (array)
- Mac installation git
- Image and large array types
- Convert grayscale image to pseudo-color image-pseudo-color processing
- GHOST blog build
- Android application component Service
- Krpano tutorial view tag Chinese description

## Tham gia chương trình bằng cấp trực tuyến có thể thú vị hơn bạn...

Bằng cấp trực tuyến | Quảng cáo tìm kiếm

## **Related Tags**

Miscellaneous Notes on Industrial Control Technology

C++

Development language

embedded hardware

single chip microcomputer

manufacture

Industrial Control Technology Miscellaneous Records

tcp

ci

hardware engineering

Copyright DMCA 2018-2023 - All Rights Reserved - www.programmersought.com User Notice