

# WPF上位机应用开发VIP课程

开发进阶, 蜕变架构, 升职加薪, 只争朝夕!

Jovan

# 朝夕教育 WPF上位机VIP课程



20:00开始上课

#### WPF上位机应用开发西门子S7协议:

- ① 仿真环境搭建
- ② Modbus通信测试
- ③ 了解S7系列PLC数据存储
- ④ S7报文结构与报文解析
- ⑤ S7通信库封装



## 欢迎来到朝夕教育WPF上位机VIP课程

同学们晚上好!!!!

今天课程继续来学习S7协议的主要报文结构,是后续进行抓包分析以及代码通信的基础

不公开 报文结构复杂

## 开发环境

- 1、Visual Studio 2019 16.9
- 2、.NET5







#### 了解西门子PLC

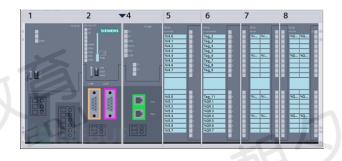
#### 1、PLC

Modbus并不确定什么设备。特定的设备可编程逻辑控制器(计算单元、存储单元、通信单元)分品牌,关注:通信协议、有现成的库、

2、西门子PLC: LOGO、S7-200、S7-200Smart、S7-300、S7-400、S7-1200、S7-1500 S7协议通信







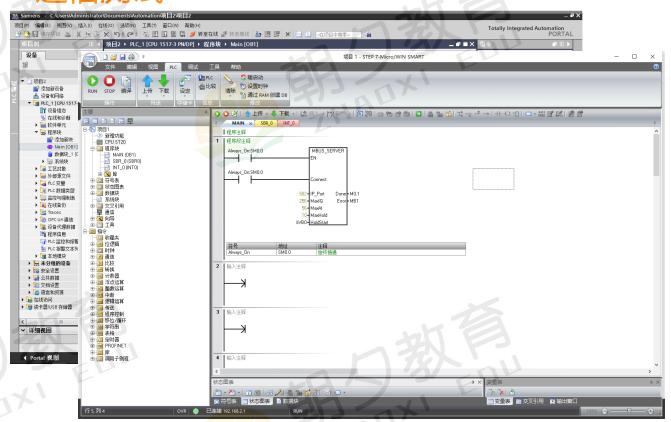


#### 仿真环境与Modbus通信测试

1、200Smart / STEP 7 仿真工具,只针对PLC编程

> 是<mark>否正常读取数据</mark> 测试网络断线

2、PLCSIM Advanced /博途



#### 西门子PLC存储区

1、存储区分类,需要用S7协议

I: 数字量输入(DI)

Q: 数字量输出

Al: 模拟量输入

AQ: 模拟量输出

V: 变量存储区

M: 位存储区

T: 定时器存储区

C: 计数器存储区

HC: 高速计数器

AC: 累加器

SM: 特殊存储器

L: 局部存储区

S: 顺序控制继电器

2、访问规则: bit、B、W、D

B: byte W:word ->2byte D:double->4byte

Bit: 10.0

DB块

#### **\$7**协议

1、私有协议,非公开,OPC、S7.NET Snap7(Sharp7)

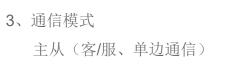
2、第7层协议:数据格式-》电平信号-》在通信介质

PDU: Protocol Data Unit

TPKT: Transport service ontop of the TCP(报文连接剂)

COTP: Connection-Orirented Transport Protocol

WireShark (保证通信正常,读写功能)



伙伴(双边通信)PLC-》PLC

4、协议层次结构与请求流程 大体的层次结构(TPKT、COTP、S7) 请求流程

Application Layer						FMS	DP	PA
			col	col				
Presentation Layer			protocol	protocol	protocol			
Session Layer			S7	S7	S7 prot			
Transport Layer	UDP	RF TCF	C1006	ISO	3	3		
Network Layer		IP	97					
Data Link Layer Physical Layer	) li	ndustrial E	Etherne	et	MPI	FDL PROFIE	BUS	PROFIBUS PA

#### \$7协议

- 1、私有协议, 非公开, OPC、S7.NET Snap7(Sharp7)
- 2、第7层协议:数据格式-》电平信号-》在通信介质
- 3、通信模式
- 4、协议层次结构与请求流程 大体的层次结构(TPKT、COTP、S7) 请求流程
  - 建立Socket连接: 进行TCP三次握手
  - COTP的握手请求(请求建立通信)
  - 整个S7的握手请求(请求建立操作通信)
  - 进行读写操作(S7协议报文)

WireShark (保证通信正常,读写功能)



Application Layer						FMS	DP	PA
Application Layer			00	col				
Presentation Layer			protocol	protocol	protocol			
Session Layer			S7	S7	S7 prot			
Transport Layer	UDP	RF TCF	C1006	ISO		3		
Network Layer		IP	45	Z				
Data Link Layer		ndustrial E	therne	at		FDL		PROFIBUS
Physical Layer		radotifui L	oriic		MPI PROFIBUS			PA

## ► **\$7**协议-**COTP**

- 1、第一次交互
- 2、请求与响应

				COTP通信请求		
		长度(bit)	发送	说明	响应	说明
0		8	0x03	Version,版本默认3	0x03	Version,版本默认3
1	TPKT	8	0x00	Reserved,保留默认0	0x00	Reserved,保留默认0
2	IPKI	16	0x00(Hi)	整个请求字节数	0x00	整个请求字节数
3		10	0x16(Lo)		0x16	笠   阴水子   以
4		8	0x11	当前字节以后的字节数	0x11	当前字节以后的字节数
5		8	0xe0	PDU Type,连接请求[附录一]	0xd0	PDU Type,确认连接
6		16	0x00	DST reference	0x00	DST reference
7		10	0x00	D31 Telefence	0x00	D31 Teleferice
8		16	0x00	SRC reference	0x00	SRC reference
9		10	0x01	site relatified	0x01	Site reference
			0000	Class	0000	Class
10		8	0-	Extended formats	0-	
			0	No explilcit flow control	0	No explilcit flow control
11		8	0xc1	Parameter-Code: src-tsap 上位机	0xc0	Parameter code:tpdu-size
12	COTP	8	0x02	Parameter-Len	0x01	Parameter length
13			0x10	Source TSAP:01->PG;02->OP;03->S7单边(服务器模式);0x10->S7双边通	0x0a	TPDU size
14		16	0x00	信机架与插槽号为0	0xc1	Parameter-Code: src-tsap
15		8	0xc2	Parameter-code: dst-tsap PLC	0x02	Parameter-Len
16		8	0x02	Parameter len	0x10	Source TSAP
17		16	0x03	Destination TSAP	0x00	Source 13AF
18		10	0x <b>0</b> 1	机架与插槽号: 0, 1->200Smart/1200/1500;0,2->300/400	0xc2	Parameter-code:dst-tsap
19		8	0xc0	Parameter code:tpdu-size	0x02	Parameter len
20		8	0x01	Parameter length	0x01	Destination TSAP
21	AI	8	0x0a	TPDU size	0x02	Destination 13A

# **S7**协议-S7COMM

- 1、第二次交互
- 2、请求与响应

PDU Len

1、PLC型号

2、240、480、960

				S7通信请求				
		长度(bit)	发送			长度(bit)	响应	
0		8	0x03	Version,版本默认3		8	0x03	Version,版本默认3
1	TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved,保留默认0
2 3	IPKL	16	0x00 0x19	整个请求字节数	IPKI	16	0x00 0x19	整个请求字节数
4		8	0x02	当前字节以后的字节数	111	8	0x02	当前字节以后的字节数
5	СОТР	8	0xf0	PDU Type,数据传输[附录一]	СОТР	8	0xf0	PDU Type,数据传输
6	COIF	8	-000 0000	TPDU number	COTF	8	-000 0000	TPDU number
U		O	1	Last data unit:Yes		O	1	Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x01	ROSCTR: JOB [附录二]		8	0x03	ROSCTR:Ack_Data
9			0x00	Redundancy Identification			0x00	Redundancy Identification
10		16	0x00	(Reserved)		16	0x00	(Reserved)
11 12	S7- Header	16	0x00 0x00	Protocol Data Unit Reference	S7-	16	0x00 0x00	Protocol Data Unit Reference
13 14		16	0x00 0x08	Parameter length	Header	16	0x00 0x08	Parameter length
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length
17		8	0xf0	Function:Setup communication[附录五]		8	0x00	Error class: No error (0x00)[附录三]
18		8	0x00	Reserved		8	0x00	Error code: 0x00
19		10	0x00	Max AmQ(parallel jobs with ack)		8	0xf0	Function:Setup communication
20		16	0x03	calling		8	0x00	Reserved
21	S7-Parameter		0x00	Max AmQ(parallel jobs with ack)			0x00	Max AmQ(parallel jobs with ack)
22		16	0x03	called	S7- Parame	16	0x01	calling
23			0x03	100	ter		0x00	Max AmQ(parallel jobs with ack)
24		16	0xc0	PDU length	$A \rightarrow$	16	0x01	called
25 26	AAD			7	13.0	16	0x00 0xf0	PDU length 240

► \$7协议-\$7COMM\_:==

1、数据请求

I				\$70	omm-读			
		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version,版本默认3		8	0x03	Version, 版本默认3
1	TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved,保留默认0
2	IFKI	_ 16	0x00	整个请求字节数	ITKI	16	0x00	整个请求字节数
3		10	0x1f			10	0x1a	
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5	COTP	COTP 8 0xf0 PDU Type,数据传输附录—] CO	СОТР	8	0xf0	PDU Type,数据传输		
6		8	-000 0000	TPDU number		8	-000 0000	TPDU number
-		Ü	1	Last data unit:Yes			1	Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x01	ROSCTR:JOB[附录二		8	0x03	ROSCTR:Ack_Data
9		16	0x00	Redundancy Identification (Reserved)		16	0x00	Redundancy Identification (Reserved)
10			0x00	,,			0x00	,
11	S7-Header	16	0x00	Protocol Data Unit Reference		16	0x00	Protocol Data Unit Reference
12			0x00		S7-Header		0x00	
13		16	0x00	Parameter length	37-Headel	16	0x00	Parameter length
14			0x0e				0x02	<b>.</b>
15		16	0x00	Data length		16	0x00	Data length
16			0x00	3			0x05	
17	S7-Parameter	8	0x04	Function: Read Var (0x04)[附录五]		8	0x00	Error class: No error (0x00) )[附录三]
18	57 1 41 4111 10101	8	0x01	Item count: 1		8	0x00	Error code: 0x00
19		8	0x12	结构标识,一般默认0x12	S7-Parameter	8	0x04	Function: Read Var (0x04)
20		8	0x0a	此字节往后的字节长度	37-rarameter	8	0x01	Item count: 1
21		8	0x10	Syntax Id: S7ANY (0x10)[附录六]		8	0xff	Return code: Success (0xff)[附录九]
22		8	0x02	Transport size: BYTE (2)[附录七]		8	0x04	Transport size: BYTE/WORD/DWORD (0x04)
23		16	0x00	数据长度	Data Item[1]	16	0x00	数据响应长度
24	Item[1]	10	0x01	<b></b>		10	0x01	<b>数插闸)型区</b> 及
25	itelli[i]	16	0x00	数据块编号 DB1.DBX100.0		n	0x00	数据 (不定长度)
26	0x01							
27		8	0x84	Area[附录八]				
28 29	24 18-3位 Byte Address:100		361		1			
30			2-0位	Bit Address:0				

# **S7**协议-S7COMM-写

1、数据请求

					S7Comn	m-写			
			长度(bit)	发送			长度(bit)	响应	
0			8	0x03	Version, 版本默认3		8	0x03	Version, 版本默认3
1			8	0x00	Reserved,保留默认0		8	0x00	Reserved, 保留默认0
2	TPKT	1		0x00		TPKT		0x00	
3			16	0x24	整个请求字节数		16	0x1a	整个请求字节数
4			8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5			8	0xf0	PDU Type, 数据传输[附录一]		8	0xf0	PDU Type,数据传输
	COTP			-000 0000	TPDU number	COTP		-000 0000	TPDU number
6			8	1	Last data unit:Yes		8	1	Last data unit:Yes
7			8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8			8	0x01	ROSCTR:JOB[附录二]		8	0x03	ROSCTR:Ack Data
9				0x00				0x00	-
10			16	0x00	Redundancy Identification (Reserved)		16	0x00	Redundancy Identification (Reserved)
11	67.11		4.0	0x00	D		4.0	0x00	D + 1D + 11 i D (
12	S7-Head	ier	16	0x00	Protocol Data Unit Reference		16	0x00	Protocol Data Unit Reference
13			4.0	0x00	5	S7-Header	4.0	0x00	D
14			16	0x0e	Parameter length		16	0x02	Parameter length
15		16		0x00	Data lawath		10	0x00	Data lawath
16			16	0x05	Data length		16	0x01	Data length
17	Paramet	or	8	0x04	Function: Write Var (0x05) [附录五]		8	0x00	Error class: No error (0x00)[附录三]
18	raiaillet	.eı	8	0x01	Item count: 1		8	0x00	Error code: 0x00
19			8	0x12	结构标识,一般默认0x12	Parameter	8	0x04	Function: Write Var (0x05)
20			8	0x0a	此字节往后的字节长度	Parameter	8	0x01	Item count: 1
21			8	0x10	Syntax Id: S7ANY (0x10)	Data Item[1]	8	0xff	Return code: Success (0xff)[附录九]
22			8	0x02	Transport size: BYTE (2)				
23			16	0x00	数据长度				
24		Item	10	0x01	<b>双插</b> 区度				
25		[1]	16	0x00	数据块编号				
26				0x02	4				
27			8	0x84	Area[附录八]				
28				18-3	<b>_</b>				
29			24	位	Byte Address:0				
30				2-0位	Bit Address:0				
31	Data I	tem[1]	8	0x00	Return code: Reserved (0x00) 附录九				
32	Duta	centil	8	0x02	Transport size:[附录七]				
33				0x02		20 0			
34			16	0x00	数据响应长度				
35			n	0x01	数据 (不定长度)				
33			- "	0,00	XVID (TALKIX)				

#### S7协议-S7COMM-SZL

- 1、系统状态列表(德语: System-ZustandsListen, 英语: System-Status-Lists)
- 2、系统数据、CPU中的模块状态数据、模拟的诊断数据、诊断缓冲区

消息服务

诊断信息

告警信息

					m-读取订货号			
		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version, 版本默认3		8	0x03	Version,版本默认3
1	TPKT	8	0x00	Reserved, 保留默认0	TPKT	8	0x00	Reserved, 保留默认0
2	IPKI	16	0x00	整个请求字节数	IPKI	16	0x00	整个请求字节数
3			0x21				0x45	
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5	COTP	8	0xf0	PDU Type, 数据传输	COTP	8	0xf0	PDU Type, 数据传输
6		8		TPDU number		8	-000 0000	TPDU number
-			1	Last data unit:Yes			1	Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x07	ROSCTR:Userdata		8	0x07	ROSCTR:Userdata
9 10		16	0x00 0x00	Redundancy Identification (Reserved)		16	0x00 0x00	Redundancy Identification (Reserved)
11 12	S7- Header	16	0x00 0x00	Protocol Data Unit Reference	S7-Header	16	0x00 0x00	Protocol Data Unit Reference
13 14		16	0x00 0x08	Parameter length		16	0x00 0x08	Parameter length
15 16		16	0x00 0x08	Data length		16	0x00 0x08	Data length:8
17 18 19		24	0x00 0x01 0x12	Parameter head: 0x000112		24	0x00 0x01 0x12	Parameter head: 0x000112
20		8	0x04	Parameter length: 4	Parameter	8	0x04	Parameter length: 4
21	Paramete	8	0x11	Method (Request/Response): Reg (0x11)		8	0x11	Method (Request/Response): Resp (0x12)
	r		0100	Type:Request(4)			0100	Type:Requet(4)
22		8	0100	Function group:CPU functions(4)		8	0100	Function group:CPU functions(4)
23		8	0x01	Subfunction: Read SZL (1)		8	0x01	Subfunction: Read SZL (1)
24		8	0x01	Sequence number: 1		8	0x00	Sequence number: 0
25		8	0xff	Return code: Success (0xff)		8	0xff	Return code: Success (0xff)
26		8	0x09	Transport size: OCTET STRING (0x09)		8	0x09	Transport size: OCTET STRING (0x09)
27		-	0x00				0x00	
28		16	0x04	Length: 4		16	0x24	Length: 36
29	Data	16	0x01 0x11	SZL-ID:取的值的地址 0000 0000 0000 0000		16	0x01 0x11	SZL-ID
31 32		16	0x00 0x01	SZL-Index: 0x0001 [Identification of the module]		16	0x00 0x01	SZL-Index: 0x0001 [Identification of the module]
33 34					Data	16	0x00 0x1c	SZL partial list length in bytes: 28
35 36					Data	16	0x00 0x01	SZL partial list count: 1
37 38						16	0x00 0x01	Index: Identification of the module (0x0001)
39						n	xxxx	MlfB (Order number of the module): 6ES7 151-8AB01-0AB0
40 41						16	0x00 0xc0	BGTyp (Module type ID): 0x00c0
42						16	0x00 0x03	Ausbg (Version of the module or release of the operating system): 3
44 45						16	0x00 0x01	Ausbe (Release of the PG description file): 1

## · S7协议-S7COMM-Run

1、数据请求

				S7Comm-l	Run			
4		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version, 版本默认3		8	0x03	Version, 版本默认3
1	TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved,保留默认0
2	ITKI	16	0x00 0x25	整个请求字节数		16	0x00 0x14	整个请求字节数
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5	COTP	8	0xf0	PDU Type,数据传输	COTP	8	0xf0	PDU Type,数据传输
_	COTP	8	-000 0000	TPDU number	COIP	8	-000 0000	TPDU number
6		8	1	Last data unit:Yes		8	1	Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x01	ROSCTR:JOB		8	0x03	ROSCTR:Ack Data
9 10		16	0x00 0x00	Redundancy Identification (Reserved)		16	0x00 0x00	Redundancy Identification (Reserved)
11 12	S7- Header	16	0x00 0x00	Protocol Data Unit Reference	S7-	16	0x00 0x00	Protocol Data Unit Reference
13 14		16	0x00 0x20	Parameter length	Header	16	0x00 0x01	Parameter length
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length
17		8	0x28	Function:PI-Service		8	0x00	Error class: No error (0x00)
18			0x00			8	0x00	Error code: 0x00
19			0x00		Parameter	8	0x28	Function: PI-Service (0x28)
20			0x00					
21		56	0x00	Unknown bytes				
22			0x00					
23			0x00					
24			0xfd					
25		16	0x00	Parameter block length				
26	Parameter		0x50	Parameter block length				
27	Parameter	8	0x09	String length				
28			0x50					
29			0x5f					
30			0x50					
31			0x52	PI (program invocation) Service:				
32		72	0x4f	P PROGRAM [PI-Service P PROGRAM				
33		13"	0x47	(PLC Start / Stop)]				
34			0x52					
35			0x41					
36			0x4d					

# S7协议-S7COMM-Stop

1、数据请求

				S7Comm-S	top			
		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version, 版本默认3		8	0x03	Version, 版本默认3
1 .	TPKT	8	0x00	Reserved, 保留默认0	TPKT	8	0x00	Reserved, 保留默认0
2 3	IPKI	16	0x00 0x21	整个请求字节数	IPKI	16	0x00 0x14	整个请求字节数
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5	COTP	8	0xf0	PDU Type,数据传输	COTP	8	0xf0	PDU Type,数据传输
6	COTF	8	-000 0000 1	TPDU number Last data unit:Yes	COTP	8	-000 0000 1	TPDU number Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x01	ROSCTR:JOB		8	0x03	ROSCTR:Ack_Data
9 10		16	0x00 0x00	Redundancy Identification (Reserved)		16	0x00 0x00	Redundancy Identification (Reserved)
11 12	S7-Header	16	0x00 0x00	Protocol Data Unit Reference	S7-Header	16	0x00 0x00	Protocol Data Unit Reference
13 14		16 0x00 0x10		Parameter length	57-Header	16	0x00 0x01	Parameter length
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length
17		8	0x29	Function:PLC Stop		8	0x00	Error class: No error (0x00)
18			0x00			8	0x00	Error code: 0x00
19			0x00		Parameter	8	0x29	Function: PLC Stop (0x29)
20		40	0x00	Unknown bytes				
21			0x00					
22			0x00					
23		8	0x09	Length				
24	Parameter		0x50					
25			0x5f					
26 27			0x50 0x52					
28		72	0x32 0x4f	PI(program invocation)				
29		2/12	0x47	Service:P_PROGRAM				
30			0x47 0x52					
31			0x41					
32			0x4d					

# ▶ **\$7**协议-**\$7COMM**-时间

1、数据请求

					S7Comm-	获取时间									
			长度(bit)	发送	说明		长度(bit)	响应			<b></b>				
0			8	0x03	Version,版本默认3		8	0x03	Version,版本						
1	TPKT	T	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved, (5	留默认0					
2			16	0x00 0x1d	整个请求字节数				长度(bit)	发送	S7Comm 说明	1-设置时间	长度(bit)	响应	说明
4			8	0x02	当前字节以后的字节数		0		8	0x03	Version,版本默认3		8	0x03	Version,版本默认3
5	СОТР	p	8	0xf0	PDU Type, 数据传输	COTP	1		8	0x00	Reserved,保留默认0		8	0x03	Reserved,保留默认0
6			8	-000 0000	TPDU number		2	TPKT		0x00		TPKT		0x00	
V			8		Last data unit:Yes		3		16	0x27	整个请求字节数		16	0x21	整个请求字节数
8			8	0x32 0x07	Protocol Id, 默认 ROSCTR:Userdata		4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
9				0x07			5		8	0xf0	PDU Type, 数据传输		8	0x62	PDU Type,数据传输
11			16	0x00	Redundancy Identification (Reserved)			COTP			O TPDU number	COTP			TPDU number
1	1			0x00			6		8		Last data unit:Yes		8		Last data unit:Yes
1.	S7-Hea	ider	16	0x00	Protocol Data Unit Reference	S7-Header	7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
1.			16	0x00	Parameter length		8		8	0x07	ROSCTR:Userdata		8	0x07	ROSCTR:Userdata
1-			10	0x08	raiameter length		9			0x00				0x00	
1:			16	0x00 0x04	Data length		10		16	0x00	Redundancy Identification (Reserved)		16	0x00	Redundancy Identification (Reserved)
11			24	0x00 0x01	Parameter head		11 12	S7-Heade	r 16	0x00 0x00	Protocol Data Unit Reference	S7-Header	16	0x00 0x00	Protocol Data Unit Reference
19				0x12	Tarameter nead		13			0x00				0x00	
21			8	0x04	Parameter length		14		16	0x08	Parameter length		16	0x0c	Parameter length
2	1 Parame	eter	8	0x11	Method (Request/Response): Reg (0x11)		17		16	0x00	Data length		16	0x00	Data length
2	2			0100	Type:Requet(4)			10	0x14	Data length		16	0x0e	Data length	
			0	0111	0111 Function group:Time functions(7)	Parameter				0x00				0x00	
2			8	0x01	Subfunction: Read clock (1)		18		24	0x01	Parameter head		24	0x01	Parameter head
2-			8	0x00	Sequence number:0		19			0x12				0x12	
2:			8	0x0a 0X00	Return code: Object does not exist (0x0a) Transport size: NULL (0x00)		20		8	0x04	Parameter length		8	0x08	Parameter Length
2		a	0	0X00	Transport size. NOLL (0x00)		21	Paramete	r 8	0x11	Method (Request/Response): Req (0x11)		8	0x12	Method (Request/Response): Res (0x12)
2			16	0000	Length		22		8	0100	Type:Requet(4)		8		Type: Response (8)
2				07.00		Data	22		8	0111	Function group:Time functions(7)	Parameter	8	0111	Function group: Time functions (7)
31	0						23		8	0x02	Subfunction: Set clock (1)		8	0x01	Subfunction: Read clock (1)
3							24		8	0x00	Sequence number:0		8	0x01	Sequence number:1
3.							25		8	0xff	Return code: Success (0xff)		8	0x00	Data unit reference number: 0
3:							26		8	0X09	Transport size: OCTET STRING (0x09)		8	0x00	Last data unit: Yes (0x00)
3							27		16	0X00	Length		16	0x00	Error code: No error (0x0000)
31							28			0X0a	•		10	0x00	, ,
3							29		8	0x00	S7 Timestamp - Reserved: 0x00		8	0xff	Return code: Success (0xff)
31							30		8	20	S7 Timestamp - Year 1:19	Data	8	0x09	Transport size: OCTET STRING (0x09)
3!	9						31	Data	8	21	S7 Timestamp - Year 2: 21	Data	16	0x00	Length: 0
41	0						32	Data	8	5	S7 Timestamp - Month: 5		10	0x00	Length. 0
4:	1						33		8	8	S7 Timestamp - Day: 8				
4:	2						34		8	20	S7 Timestamp - Hour: 11				
							35		8	0	S7 Timestamp - Minute: 59				
							36		8	0	S7 Timestamp - Second: 33				
							37		16	0x04	0000 0000 0100 Milliseconds				
					UX		38		10	0x45	' 0111 Weekday:Saturday(7)				

# S7协议-S7COMM-Userdata-获取系统块

- 1、数据请求
- 2、模块信息列出为

列举一<mark>下</mark>块的类型 读取块的信息

24   8   0x01   Subfunction: List blocks(1)   Parameter   8   0x01   Subfunction: Read SZL (1)   16   0x00   0x0												
TPKT   1						S7Comm-获取Block信息						
TPKT			长度(bit)	发送	说明		长度(bit)	响应	i	<b></b>		
TPCT   8	0		8	0x03	Version,版本默认3		8	0x03	Version, 版本默认3			
16	1		8	0x00	Reserved, 保留默认0	TOUT	8	0x00	Reserved, 保留默认0			
A	2	IPKI	16		整个请求字节数	IPKI	16		整个请求字节数			
S	4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数			
6	5		8	0xf0	PDU Type, 数据传输		8	0xf0				
1		COTP				COTP						
8	6		8				8					
8	7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认			
9	8		8				8					
11			16	0x00	Redundancy Identification (Reserved)		16	0x00	Redundancy Identification (Reserv	ved)		
13	11	S7-Header	16	0x00	gv	S7-Header	16	0x00	Protocol Data Unit Reference			
14												
15			16		Parameter length		16		Parameter length			
16										Item[2]	16	F
17			16		Data length		16		Data length			
18											16	F
19										h (2)		
8			24		Parameter nead		24		Parameter nead	item[3]	16	F
Parameter   8												
Rem			-								16	F
8	21	Parameter	8				8			Itom[4]		
Subfunction List blocks(1)   Parameter   8	22		8		71		8			item[4]	16	D
24						Parameter						
Sequence number: 0   Sequen			-								16	D
27   8							-			Item[5]		
Rem[1]			8	0xff						rem[5]	16	SD
Barrier   Bar	27		8	0x00	Transport size: NULL (0x00)		8	0x00	Last data unit: Yes (0x00)			
16	28	Data		000				0×00			16	S
Data   B			16		Length		16		Error code: No error (0x0000)	Item[6]		
Data   8   Oxff   Return code; Success (Oxff)   0x00   S     31   8   0x09   Transport size; OCTET STRING (0: 16   0x47     32   0x00   16   0x00   S     33   16   0x00   16   0x00   S     34   18   16   0x00   Oxfe   16   0x00   S     35   36   16   0x00   Oxfe   S     36   0x00   Oxfe   Oxf	29			0x00				0x00		icin[0]	16	S
S	30					Date	8	0xff	Return code: Success (0xff)			
32   16   0x00   0x30   Length: 剩余字节长度   kem[7]   16   0x00   Si   0x30   Cength: 剩余字节长度   kem[7]   16   0x00   Si   0x00   0x00   Si   0x00   0x00   Si   0x00   0x00   Si   0x00   0x0	31					Data	8	0x09	Transport size: OCTET STRING (0:		16	SF
33   0	32						16	0x00	Length: MASHK#	Item[7]		
Rem[1]   0x00   Ob表型   16 0x00   S	33						10	0x30	Length: 料水子口区设		16	SF
35 0x08 0x0e 16 0x0e 5	34					Item[1]	10	0x00	ODWE			Н
36 0x00 ORthatyle	35			V			16	0x08	UB央空		16	S
37 OXO1 CHAMPSONIN	36						16	0x00	ORITH WITH			
	37						16	0x01	OBJEST			

#### S7协议-S7COMM-StartUpload

- 1、数据请求 PLC-》PC 请求开始上传/下载 上传/下载 数据量大于PDU长度240 结束上传/下载
- 2、文件标识
  - \_: Complete Module
  - \$: Module header for up-loading
- 3、Status
  - ---- 1 More data following:True
  - ---- --0- Error:False

					N 1 /4			
		14-4-41.5	11227	S7Comm-请	<b>水上</b> 专	Le state (		Was
		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version, 版本默认3		8	0x03	Version, 版本默认3
1	TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved,保留默认0
2		16	0x00 0x23	整个请求字节数	X	16	0x00 0x23	整个请求字节数
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5	COTP	8	0xf0	PDU Type, 数据传输	COTP	8	0xf0	PDU Type,数据传输
6	COTT	8	-000 0000		COTI	8		TPDU number
U		O	1	Last data unit:Yes		U	1	Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x01	ROSCTR:JOB		8	0x03	ROSCTR:Ack_Data
9 10		16	0x00 0x00	Redundancy Identification (Reserved)		16	0x00 0x00	Redundancy Identification (Reserved)
11 12	S7-Header	16	0x00 0x00	Protocol Data Unit Reference	S7-Header	16	0x00 0x00	Protocol Data Unit Reference
13 14		16	0x00 0x12	Parameter length	37-neader	16	0x00 0x10	Parameter length
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length
17		8	0x1d	Function: Start upload (0x1d)		8	0x00	Error class: No error (0x00)
18		8	0x00	Function Status		8	0x00	Error code: 0x00
19		16	0x00			8	0x1d	Function: Start upload (0x1d)
20		16	0x00	Unknown byte(s) in blockcontrol: 0000		8	0x00	Function Status
21 22		32	0x00 0x00	UploadID: 0x00000000		16	0x00 0x00	Unknown byte(s) in blockcontrol: 0000
23 24		52	0x00 0x00	орюась. Охоооооо		32	0x00 0x00	UploadID: 0x00000007
25	Parameter	8	0x09	Filename Length		32	0x00	Opioadib. 0x00000007
26		8	_	File identifier:_			0x07	
27		16	0x00	Block type: 08 (OB)	Parameter	8	0x07	Blocklengthstring length
28		10	0x08	Block type. 08 (OB)			0	
29			0x00				0	
30			0x00				0	
31		40	0x00	Block number		56	0	Blocklength: 0000216
32			0x00			30	2	Diockiength, 0000210
33			0x01				1	
34	8 A	Destination filesystem: A (Active embedded module)	led		6			

# ▶ S7†办议-S7COMM-Upload

1、数据请求

			S7C	omm-上传			
	长度(bit)	发送	说明		长度(bit)	响应	说明
	8	0x03	Version,版本默认3		8	0x03	Version,版本默认3
TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved,保留默认0
2	16	0x00 0x19	整个请求字节数	IPKI	16	0x00 0xf1	整个请求字节数
1	8	0x13	当前字节以后的字节数		8	0x11	当前字节以后的字节数
	8	0x62	PDU Type, 数据传输		8	0x62	PDU Type,数据传输
COTP	U		TPDU number	СОТР		-000 0000	TPDU number
	8	1	Last data unit:Yes		8	1	Last data unit:Yes
	8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
	8	0x01	ROSCTR:JOB		8	0x03	ROSCTR:Ack Data
	16	0x00	Redundancy Identification		16	0x00	Redundancy Identification (Reserved)
)	10	0x00	(Reserved)		10	0x00	Reduitedity identification (Reserved)
S7-Header	16	0x00	Protocol Data Unit Reference	S7-Header	16	0x00	Protocol Data Unit Reference
37-Headel	10	0x00	Plotocol Data Offic Reference		10	0x00	Protocor Data Offic Reference
3 1	$ \begin{array}{ccc} 0x00 \\ 0x08 \\ 16 & 0x00 \\ 0x00 & 0x00 \end{array} $ Parameter length  Data length		Parameter length		16	0x00 0x02	Parameter length
		Data length		16	0x00 0xdc	Data length:220	
	8	0x1e	Function: Upload (0x1e)		8	0x00	Error class: No error (0x00)
	8	0x00	Function Status		8	0x00	Error code: 0x00
)		0x00	Unknown byte(s) in blockcontrol:		8	0x1e	Function: Upload (0x1e)
)	16	0x00	0000	Parameter	8	0x00	Function Status
Parameter	1	0x00		Data	16	0x00	Length:216
	32 0x00 UploadID: 0x00000007		10	0xd8	Length. 210		
-a1	32	0x00 0x07	opioadib. 0x00000001		16	0x00 0xfb	Unknown byte(s) in blockcontrol: 00fb
		OAO1			n	OXID	Data

# > \$7协议-\$7COMM-EndUpload

1、数据请求

				S7Comm-约	吉束上传			
		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version,版本默认3		8	0x03	Version,版本默认3
1	TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved,保留默认0
2 3	7	16	0x00 0x19	整个请求字节数	IFKI	16	0x00 0x14	整个请求字节数
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
5	COTP	8	0xf0	PDU Type,数据传输	COTP	8	0xf0	PDU Type,数据传输
c	COIP	0	-000 0000	TPDU number	COIP	0	-000 0000	TPDU number
6		8	1	Last data unit:Yes		8	1	Last data unit:Yes
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
8		8	0x01	ROSCTR:JOB		8	0x03	ROSCTR:Ack_Data
9 10		16	0x00 0x00	Redundancy Identification (Reserved)		16	0x00 0x00	Redundancy Identification (Reserved)
11 12	S7-Header	16	0x00 0x00	Protocol Data Unit Reference	S7-	16	0x00 0x00	Protocol Data Unit Reference
13 14		16	0x00 0x08	Parameter length	Header	16	0x00 0x01	Parameter length
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length
17		8	0x1f	Function: end upload (0x1f)		8	0x00	Error class: No error (0x00)
18		8	0x00	Function Status		8	0x00	Error code: 0x00
19	Parameter	16	0x00	Errorcode: 0x0000 (No error)	Parameter	8	0x1f	Function: end upload (0x1f)
20		0x00	Ellorcode. Oxodoo (No ellor)					
21								
22		32	0x00	UploadID: 0x00000007				
23		J.L	0x00	opioudio. oxoooooo				
24			0x07					

# S7协议-S7COMM-Start Download

1、数据请求

2、

				0 1 TPk 2 T	长度(bit) 8 8		ersion,版本默认 eserved,保留默		说明 Version, 版本默认3 Reserved, 保留默认0
				S7Comm-请	求下载				整个请求字节数 当前字节以后的字节数
		长度(bit)	发送	说明		长度(bit)	响应	说明	ョルチャル后的チャ数 PDU Type,数据传输 TPDU number
0	TPKT	8 8	0x03 0x00	Version,版本默认3 Reserved,保留默认0	TPKT	8	0x00	Version,版本默认3 Reserved,保留默认0	Last data unit:Yes Protocol Id,默认 ROSCTR:Ack Data
2 3		16	0x00 0x31	整个请求字节数		16	0x00 0x14	整个请求字节数	Redundancy Identification (Reserved)
4 5	СОТР	8 8	0x02 0xf0	当前字节以后的字节数 PDU Type,数据传输	СОТР	8 8		当前字节以后的字节数 PDU Type,数据传输	Protocol Data Unit Reference
6	COIP	8	-000 0000 1	TPDU number Last data unit:Yes	COIP	8		TPDU number Last data unit:Yes	Parameter length
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认	Data length
8		8	0x01	ROSCTR:JOB		8		ROSCTR:Ack_Data	Error class: No error (0x00) Error code: 0x00
9	S7-	16	0x00 0x00	Redundancy Identification (Reserved)		16	0x00 0x00	Redundancy Identification (Reserved)	Function: Start download (0x1a)
11 12	Heade r	16	0x00 0x00	Protocol Data Unit Reference	S7-	16	0x00 0x00	Protocol Data Unit Reference	
13 14		16 0x00 F	Parameter length	Heade r	16	0x00 0x01	Parameter length		
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length	
17	Paramete r	8	0xfa	Function: Start download (0xfa)		8	0x00	Error class: No error (0x00)	
18		n	XXXX	Parameter data		8	0x00	Error code: 0x00	
19					Paramete r	8	0xfa	Function: Start download (0xfa)	
				36 37	. 8	0x01 U 0x00	nknown char be	tore load mem:1	
			11/	36 37 38 39 40 41	48	0x00 0x00 0x05 0x00 0x00	Length of load	memory	
	1			43 44 45 46 47 48	24	0x00 0x00 0x00 0x00 0x04 0x00 0x00	Length of MC7	code:000212	

S7Comm-请求下载

## S7协议-S7COMM-Download

1、数据请求

							长度(bit)	发送		说明		长度(bit)	响应	说明
					0		8		/ersion,版本默记			8	0x03	Version, 版本默认3
					1	TPKT	8		Reserved, 保留黑	<b></b>	TPKT	8	0x00	Reserved, 保留默认0
					2		16	0x00	8个请求字节数			16	0x00	整个请求字节数
						S7Co	mm-下载							前字节以后的字节数
		长度(bit)	发送		说明				长度(bit)	响应	说即	3		IU Type,数据传输
0		8	0x03	Version, 版本默	:i.k.3				8	0x03	Version,版本默认3			DU number
1		8	0x00	Reserved, 保留					8	0x00	Reserved,保留默认0			st data unit:Yes
	TPKT	0		neserveu, 沐田	表 い			TPKT	0		Reserved,未由款以U			otocol ld,默认 DSCTR:Ack Data
2		16	0x00	整个请求字节数	Þ				16	0x00	整个请求字节数			-
3			0xf7							0xf7				dundancy Identification (Reserv
4		8	0x02	当前字节以后的?	字节数				8	0x02	当前字节以后的字节数			
5	COTD	8	0xf0	PDU Type,数据	传输			COTE	8	0xf0	PDU Type,数据传输			otocol Data Unit Reference
	COTP		-000 0000	TPDU number				COTP		-000 000	0 TPDU number			
6		8	1	Last data unit:Y	es				8	1				rameter length
7		8	0x32	Protocol Id, 默					8	0x32	Protocol Id, 默认			ita length:226
8		8	0x01	ROSCTR:JOB					8	0x03	ROSCTR:Ack Data			ror class: No error (0x00)
9			0x00							0x00	_			ror code: 0x00
10		16	0x00	Redundancy I	dentification	n (Reserve	d)		16	0x00	Redundancy Identific	ation (Res	served)	inction: Download (0x1b)
														nction Status
11	S7- Header	16	0x00	Protocol Data	Protocol Data Unit Reference			16	0x00	Protocol Data Unit Reference		ngth:222		
12	пеацег		0x00					S7-		0x00				gcrzzz
13		16	0x00	Parameter ler	ath			Header	16	0x00	Parameter length			nknown byte(s) in blockcontrol: (
14		10	0x12	raiailletei lei	igtii				10	0x01	raiameter length			* **
15		4.0	0x00	- N.					4.0	0x00	5 . 1 .1 .005			ıta
16		16	0xd4	Data length					16	0x00	Data length:226			
17	Parameter	8	0x1b	Function: down	load (0xfb)				8	0x00	Error class: No error (0)	(00)		
18		n	xxxx	Parameter Data					8	0x00	Error code: 0x00			
19	Data	n	xxxx	Data				Paramete	r 8	0xfb	Function: Download (0	xfb)		
					32			0x00						
					33			0x01						
					34		8		Destination filesy	stem: P				

# ► **\$7**协议-**\$7COMM-End Download**1、数据请求

				1 8		ved 佐田野汁U		8 0x00 R	eserved 保留默认0
				S7Con	nm-结束下载				数
		长度(bit)	发送	说明		长度(bit)	响应	说明	的字节数
0		8	0x03	Version,版本默认3		8	0x03	Version, 版本默认3	女据传输
1	TPKT	8	0x00	Reserved,保留默认0	TPKT	8	0x00	Reserved, 保留默认0	t:Yes
2	II KI	16	0x00 0x23	整个请求字节数	II KI	16	0x00 0x14	整个请求字节数	默认 _Data
4		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数	Identification (Reserve
5	СОТР	8	0xf0	PDU Type,数据传输	СОТР	8	0xf0	PDU Type,数据传输	a Unit Reference
6	COIP		-000 0000	TPDU number	COIP	8	-000 0000	TPDU number	a Unit Reference
O		0	1	Last data unit:Yes		0	1	Last data unit:Yes	ngth
7		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认	,
8		8	0x01	ROSCTR:JOB		8	0x03	ROSCTR:Ack_Data	,
9		16	16 0x00 Redundancy Identification (Reserved)			16	0x00 0x00	Redundancy Identification (Reserved)	lo error (0x00) x00 wnload (0x1c)
1 2	S7- Head er	Head 16	0x00 0x00	Protocol Data Unit Reference	S7-	16	0x00 0x00	Protocol Data Unit Reference	
3		16	0x00 0x12	Parameter length	Head er	16	0x00 0x01	Parameter length	
15 16		16	0x00 0x00	Data length		16	0x00 0x00	Data length:0	
17	Para	8	0xfc	Function: download ended (0xfc)		8	0x00	Error class: No error (0x00)	
18	meter	n	xxx	Parameter data		8	0x00	Error code: 0x00	
19					Paramete	8	0xfc	Function: Download (0xfc)	

# \$7协议-\$7COMM-激活程序块

1、数据请求

				S7Comm-激活	5块			
		长度(bit)	发送	说明		长度(bit)	响应	说明
0		8	0x03	Version,版本默认3		8	0x03	Version,版本默认3
	TPK	8	0x00	Reserved,保留默认0	TPK	8	0x00	Reserved, 保留默认0
	T		0x00	The A. W. B. A. L. L. Co.	T		0x00	THE A 19TH A 19TH
		16	0x2b	整个请求字节数		16	0x14	整个请求字节数
		8	0x02	当前字节以后的字节数		8	0x02	当前字节以后的字节数
	СОТ	8	0xf0	PDU Type, 数据传输	COT	8	0xf0	PDU Type,数据传输
	Р	8	-000 0000	TPDU number	P	8	-000 0000	TPDU number
		8	1	Last data unit:Yes			1	Last data unit:Yes
		8	0x32	Protocol Id, 默认		8	0x32	Protocol Id, 默认
		8	0x01	ROSCTRJOB		8	0x03	ROSCTR:Ack_Data
		16	0x00	Redundancy Identification (Reserved)		16	0x00	Redundancy Identification (Reserved)
		10	0x00	neumoancy identification (keserved)		16	0x00	neutricality identification (Reserved)
	S7- Hea	16	0x00	Protocol Data Unit Reference	67	16	0x00	Protocol Data Unit Reference
	der	10	0x00	TOLOCOL Data Offic Reference	S7- Hea	10	0x00	
		16	0x00	Parameter length	der	16	0x00	Parameter length
		10	0x1a	raiameter length		10	0x01	ratameter length
		16	0x00	Data length		16	0x00	Data length:0
			0x00	Datalength		10	0x00	Data length.o
		8	0x28	Function: PI-Service (0x28)		8	0x00	Error class: No error (0x00)
			0x00			8	0x00	Error code: 0x00
			0x00		Parameter	8	0x28	Function: PI-Service (0x28)
			0x00					
		56	0x00	Unknown bytes: 000000000000fd				
			0x00					
			0x00					
			0xfd					
		16	0x00	Parameter block length: 10				
			0x0a					
		8	0x01	Number of blocks: 1				
		8	0x00	Unknown byte: 0x00				
	Par	16	0x00	Block type: 0A (DB)				
	ame ter		0x0a					
	tel		0x00					
			0x00					
		40	0x00	Block number: 00001				
			0x00					
			0x01					
		8	0x50	Destination filesystem: P (Passive (copied,	but not chaine	d) module)		
		8	0x05	String length: 5				
			0x5f					
			0x49	PI (program invocation) Service: _INSE				
		40	0x4e	[PI-Service _INSE (Activates a PLC module)]				
			0x53	module)j				
			0x45					

### \$7通信测试程序

- 1、S7.NET通信库的使用
- 2、通信与WireShark抓包







## \$7通信库封装

1.









#### 附录一

#### 1、CTOP->PDU type已知枚举值

0xe0	连接请求
0xd0	连接确认
0x08	断开请求
0x0c	断开确认
0x05	拒绝访问
0x01	加急数据
0x02	加急数据确认
0x04	用户数据
0x07	TPDU错误
0xf0	数据传输



#### 附录二

#### 1、S7Header->ROSCTR已知枚举值

0x01	Job request。主站发送请求	
0x02	Ack。从站响应请求不带数据	
0x03	Ack_Data。从站响应请求并带有数据	
0x07	Userdata。原始协议的扩展。读取编程/调试、SZL读取、安全功能、时间设置等	

#### 附录三

#### 1、S7Header->Error class已知枚举值

0x00	无错误
0x81	应用程序关系错误
0x82	对象定义错误
0x83	无资源可用错误
0x84	服务处理错误
0x85	请求错误(如果有错,此码较多)
0x87	访问错误

#### 附录四

#### 1、S7Parameter->Error code已知枚举值

0x0000	无错误	0x8500	L7PDU大小错误
0x0110	无效块类型编号	0xD401	L7无效SZL ID
0x <mark>0112</mark>	无效参数	0xD402	L7无效索引
0x011A	PG资源错误	0xD403	L7 DGS连接已宣布
0x011B	PLC重新外包错误	0xD404	L7 最大用户NB
0x011C	协议错误	0xD405	L7 DGS功能参数语法错误
0x011F	用户缓冲区太短	0xD406	L7无信息
0x0141	请求错误	0xD601	L7 PRT 函数参数语法错误
0x01C0	版本不匹配	0xD801	L7 无效变量地址
0x01F0	未实施	0xD802	L7 未知请求
0x8001	L7无效CPU状态	0xD803	L7 无效请求状态

#### 附录五

#### 1、S7Parameter->Function已知枚举值

0x00	CPU服务	
0xF0	设置通信	
0x04	读取变量	
0x05	写变量	
0x1A	请求下载	
0x1B	下载块	
0x1C	下载结束	
0x1D	开始上传	
0x1E	上传	
0x1F	结束上传	
0x28	PLC 控制	
0x29	PLC 停止	



## 附录六

#### 1、S7Parameter->Item->Syntax Id已知枚举值

0x10	S7ANY: Address data S7-Any pointer-like DB1.DBX10.2
0x13	PBC-R_ID: R_ID for PBC
0x15	ALARM_LOCKFREE: Alarm lock/free dataset
0x16	ALARM_IND: Alarm indication dataset
0x19	ALARM_ACK: Alarm acknowledge message dataset
0x1a	ALARM_QUERYREQ: Alarm query request dataset
0x1c	NOTIFY_IND: Notify indication dataset
0xa2	DRIVEESANY: seen on Drive ES Starter with routing over S7
0xb2	1200SYM: Symbolic address mode of S7-1200
0xb0	DBREAD: Kind of DB block read, seen only at an S7-400
0x82	NCK: Sinumerik NCK HMI access

### 附录七

#### 1、S7Parameter->Item->Transport size常见值

		ITEM	
0×01	BIT	0x0A	TOD(Time of day 32位)
0x02	Byte	0x0B	TIME(IEC时间32位)
0x03	CHAR	0x0C	S5TIME (Simatic时间16位)
0x04	WORD	0x0F	DATE AND TIME
0x05	INT	0x1C	COUNTER
0x06	DWORD	0x1D	TIMER
0x07	DINT	0x1E	IEC TIMER
80x0	REAL	0x1F	IEC COUNTER
0x09	DATE	0x20	HS COUNTER

	DATA
0×00	NULL
0x03	BIT
0x04	BYTE/WORD/DWORD
0x05	INTEGER
0x07	REAL
0x09	OCTET STRING

## 附录八

#### 1、S7Parameter->Item->Area常见值

0x03	System info of 200 family   200系列系统信息
0x05	System flags of 200 family   200系列系统标志
0x06	Analog inputs of 200 family   200系列模拟量输入
0x07	Analog outputs of 200 family   200系列模拟量输出
0x80	Direct peripheral access (P)   直接访问外设
0x81	Inputs (I)   輸入(I)
0x82	Outputs (Q)   输出(Q)
0x83	М
0x84	Data blocks (DB)   数据块(DB) V
0x85	Instance data blocks (DI)   背景数据块 (DI)
0x86	Local data (L)   局部变量(L)
0x87	Unknown yet (V)   全局变量(V)
0x1c	S7 counters (C)   S7计数器(C)
0x1d	S7 timers (T)   S7定时器(T)
0x1e	IEC counters (200 family)   IEC计数器(200系列)
0x1f	IEC timers (200 family)   IEC定时器(200系列)



### 附录九

#### 1、S7Data->Item->Return code已知枚举值

0xff	成功
0x00	Reserved   未定义,预留
0x01	硬件错误
0x03	对象不允许访问
0x05	地址越界,无效地址,所需的地址超出此PLC的极限
0x06	请求的数据类型与存储类型不一致
0x07	日期类型不一致
0x0a	对象不存在



### 附录十

#### 1、Userdata已知枚举值

0x0	转换工作模式(Mode-transition)
0x1	工程师命令调度(Programmer commands)
0x2	循环读取(Cyclic data)
0x3	块功能 (Block functions)
0x4	CPU功能 (CPU functions)
0x5	安全功能(Security)
0x6	PBC BSEND/BRECV
0x7	时间功能(Time functions)
0xf	NC编程 (NC programming)

#### 附录十一

#### 1、PI service names已知枚举值

_INSE	PI-Service_INSE(Activates a PLC module)。激活设备上下载的块,参数是块的名称
_DELE	工程师命令调度(Programmer commands)。从设备的文件系统中删除一个块,该参 <mark>数是块的名称</mark>
P_P <mark>ROGR</mark> AM	循环读取(Cyclic data)。设置设备的运行状态(启动、停止、复位)
_MODU	块功能(Block functions)。压缩PLC内存
_GARB	CPU功能(CPU functions)。将RAM复制到ROM,参数包含文件系统标识符(A/E/P)

## 附录十二

#### 1、文件系统

Р	被动模块。Passive (copied,but not chained) module
А	有源嵌入式模块。Active embedded module
В	有源和无源模块。Active as well as passive module



## 附录十三

#### 1、文件系统

Р	被动模块。Passive (copied,but not chained) module
А	有源嵌入式模块。Active embedded module
В	有源和无源模块。Active as well as passive module



### \$7协议-\$7COMM-控制支持情况

1、数据请求

			CPU				CP	DRIVE
	300	400	WinAC	Snap7S	1200	1500	343/443/IE	SINAMICS
DB Read/Write	0	0	0	0	0	O(3)	-	0
EB Read/Write	0	0	0	0	0	0	-	0
AB Read/Write	0	0	0	0	0	0	-	0
MK Read/Write	0	0	0	0	0	0	-	-
TM Read/Write	0	0	0	0	-	-	-	-
CT Read/Write	0	0	O <sub>bloo</sub>	0	-	-	-	-
Read SZL	0	0	0	0	0	0	0	0
Multi Read/Write	0	0	0	0	0	0	-	0
Directory	0	0	0	0	-	-	0	(2)
Date and Time	0	0	0	0	-			0
Control Run/Stop	0	0	0	0	-		(1)	0
Security	0	0	0	0	-		-11	-
Block Upload/Down/Delete	0	0	0		/		0	0



# THANKYOU

开发进阶, 蜕变架构, 升职加薪, 只争朝夕!

Jovan





