朝夕教育
ZHAOXI EDU

# 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

朝夕教育
ZHAOXI EDU

**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

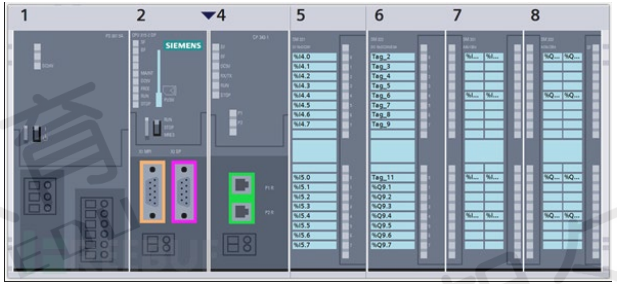
1、PLC

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

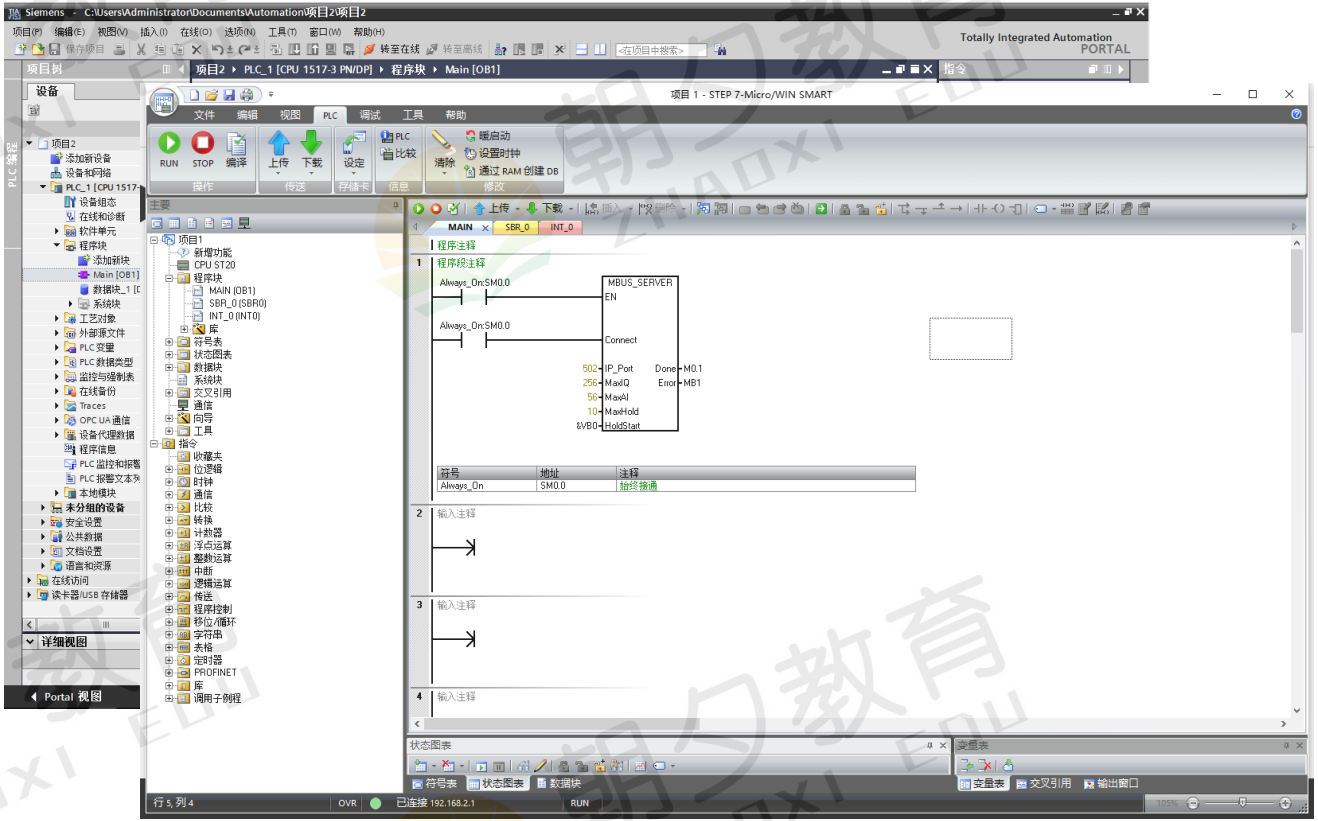
1、200Smart / STEP 7

仿真工具，只针对PLC编程

是否正常读取数据

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

AI：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

DB块

2、访问规则：bit、B、W、D

B：byte　W:word　->2byte　D:double->4byte

Bit: I0.0

# S7协议

1、私有协议，非公开，OPC、S7.NET　Snap7(Sharp7)　　WireShark（保证通信正常，读写功能）

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

3、通信模式

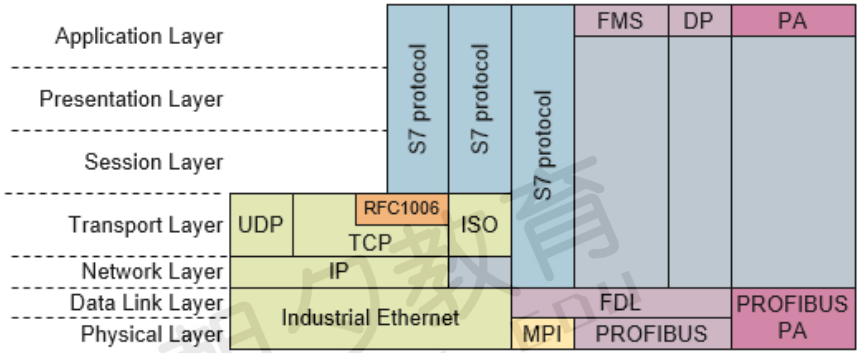
主从（客/服、单边通信）

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



# S7协议

1、私有协议，非公开，OPC、S7.NET　Snap7(Sharp7)　　WireShark（保证通信正常，读写功能）

2、第 7 层协议：数据格式-》电平信号-》在通信介质

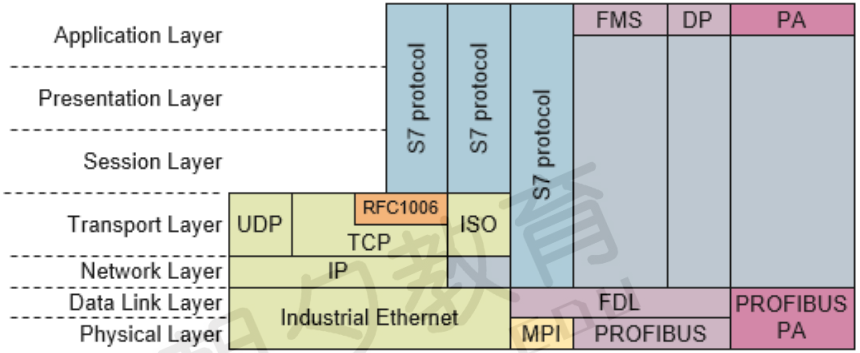
3、通信模式

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）



# S7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 | TPKT | 8 | 0x03 | Version，版本默认3 | 0x03 | Version，版本默认3 |
| 1 | | 8 | 0x00 | Reserved，保留默认0 | 0x00 | Reserved，保留默认0 |
| 2 | | 16 | 0x00(Hi) | 整个请求字节数 | 0x00 | 整个请求字节数 |
| 3 | | | 0x16(Lo) | | 0x16 | |
| 4 | COTP | 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 | | | 0x00 | | 0x00 | |
| 8 | | 16 | 0x00 | SRC reference | 0x00 | SRC reference |
| 9 | | | 0x01 | | 0x01 | |
| 10 | | 8 | 0000 ---- | Class | 0000 ---- | Class |
| | | | ---- --0- | Extended formats | ---- --0- | Extended formats |
| | | | ---- ---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 | | 8 | 0x02 | Parameter-Len | 0x01 | Parameter length |
| 13 | | 16 | 0x10 | Source TSAP:01->PG;02->OP;03->S7单边（服务器模式）;0x10->S7双边通信<br>机架与插槽号为0 | 0x0a | TPDU size |
| 14 | | | 0x00 | | 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<br>机架与插槽号：0，1->200Smart/1200/1500;0,2->300/400 | 0x00 | |
| 18 | | | 0x01 | | 0xc2 | Parameter-code:dst-tsap |
| 19 | | 8 | 0xc0 | Parameter code:tpdu-size | 0x02 | Parameter len |
| 20 | | 8 | 0x01 | Parameter length | 0x01 | Destination TSAP |
| 21 | | 8 | 0x0a | TPDU size | 0x02 | |

# 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 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x19 | | | | 0x19 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 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 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 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 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x08 | | | | 0x08 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length |
| 16 | | | 0x00 | | | | 0x00 | |
| 17 | S7-Parameter | 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 | | 16 | 0x00 | Max AmQ(parallel jobs with ack) calling | S7-Parameter | 8 | 0xf0 | Function:Setup communication |
| 20 | | | 0x03 | | | 8 | 0x00 | Reserved |
| 21 | | 16 | 0x00 | Max AmQ(parallel jobs with ack) called | | 16 | 0x00 | Max AmQ(parallel jobs with ack) calling |
| 22 | | | 0x03 | | | | 0x01 | |
| 23 | | 16 | 0x03 | PDU length | | 16 | 0x00 | Max AmQ(parallel jobs with ack) called |
| 24 | | | 0xc0 | | | | 0x01 | |
| 25 | | | | | | 16 | 0x00 | PDU length 240 |
| 26 | | | | | | | 0xf0 | |

# S7协议-S7COMM-读

1、数据请求

2、

S7Comm-读

| | | | 长度(bit) | 发送 | 说明 | | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | | 8 | 0x03 | Version，版本默认3 | TPKT | | 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 | | | 16 | 0x00 | 整个请求字节数 | | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | | 0x1f | | | | | 0x1a | |
| 4 | COTP | | 8 | 0x02 | 当前字节以后的字节数 | COTP | | 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 |
| 6 | | | 8 | -000 0000 | TPDU number | | | 8 | -000 0000 | TPDU number |
| | | | | 1--- ---- | Last data unit:Yes | | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | | 8 | 0x32 | Protocol Id，默认 | S7-Header | | 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 | | | 16 | 0x00 | Protocol Data Unit Reference | | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | | 0x00 | | | | | 0x00 | |
| 13 | | | 16 | 0x00 | Parameter length | | | 16 | 0x00 | Parameter length |
| 14 | | | | 0x0e | | | | | 0x02 | |
| 15 | | | 16 | 0x00 | Data length | | | 16 | 0x00 | Data length |
| 16 | | | | 0x00 | | | | | 0x05 | |
| 17 | S7-Parameter | | 8 | 0x04 | Function: Read Var (0x04)[附录五] | | | 8 | 0x00 | Error class: No error (0x00) )[附录三] |
| 18 | | | 8 | 0x01 | Item count: 1 | | | 8 | 0x00 | Error code: 0x00 |
| 19 | Item[1] | | 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 | | | 8 | 0x01 | Item count: 1 |
| 21 | | | 8 | 0x10 | Syntax Id: S7ANY (0x10)[附录六] | Data | Item[1] | 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 | | | 16 | 0x00 | 数据响应长度 |
| 24 | | | | 0x01 | | | | | 0x01 | |
| 25 | | | 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 | | | 24 | 18-3位 | Byte Address:100 | | | | | |
| 29 | | | | | | | | | | |
| 30 | | | | 2-0位 | Bit Address:0 | | | | | |

# S7协议-S7COMM-写

1、数据请求

2、

S7Comm-写

| | | | 长度(bit) | 发送 | | | | 长度(bit) | 响应 | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | | 8 | 0x03 | Version，版本默认3 | TPKT | | 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 | | | 16 | 0x00 | 整个请求字节数 | | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | | 0x24 | | | | | 0x1a | |
| 4 | COTP | | 8 | 0x02 | 当前字节以后的字节数 | COTP | | 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 |
| 6 | | | 8 | -000 0000 | TPDU number | | | 8 | -000 0000 | TPDU number |
| | | | | 1--- ---- | Last data unit:Yes | | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | | 8 | 0x32 | Protocol Id，默认 | S7-Header | | 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 | | | 16 | 0x00 | Protocol Data Unit Reference | | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | | 0x00 | | | | | 0x00 | |
| 13 | | | 16 | 0x00 | Parameter length | | | 16 | 0x00 | Parameter length |
| 14 | | | | 0x0e | | | | | 0x02 | |
| 15 | | | 16 | 0x00 | Data length | | | 16 | 0x00 | Data length |
| 16 | | | | 0x05 | | | | | 0x01 | |
| 17 | Parameter | | 8 | 0x04 | Function: Write Var (0x05) [附录五] | | | 8 | 0x00 | Error class: No error (0x00)[附录三] |
| 18 | | | 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 | | | 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 | | Item [1] | 16 | 0x00 | 数据长度 | | | | | |
| 24 | | | | 0x01 | | | | | | |
| 25 | | | 16 | 0x00 | 数据块编号 | | | | | |
| 26 | | | | 0x02 | | | | | | |
| 27 | | | 8 | 0x84 | Area[附录八] | | | | | |
| 28 | | | 24 | 18-3位 | Byte Address:0 | | | | | |
| 29 | | | | | | | | | | |
| 30 | | | | 2-0位 | Bit Address:0 | | | | | |
| 31 | Data | Item[1] | 8 | 0x00 | Return code: Reserved (0x00) [附录九] | | | | | |
| 32 | | | 8 | 0x02 | Transport size:[附录七] | | | | | |
| 33 | | | 16 | 0x00 | 数据响应长度 | | | | | |
| 34 | | | | 0x01 | | | | | | |
| 35 | | | n | 0x00 | 数据（不定长度） | | | | | |

# 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

S7Comm-读取订货号

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x21 | | | | 0x45 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x07 | ROSCTR:Userdata | | 8 | 0x07 | ROSCTR:Userdata |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x08 | | | | 0x08 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length:8 |
| 16 | | | 0x08 | | | | 0x08 | |
| 17 | Parameter | | 0x00 | | Parameter | | 0x00 | |
| 18 | | 24 | 0x01 | Parameter head: 0x000112 | | 24 | 0x01 | Parameter head: 0x000112 |
| 19 | | | 0x12 | | | | 0x12 | |
| 20 | | 8 | 0x04 | Parameter length: 4 | | 8 | 0x04 | Parameter length: 4 |
| 21 | | 8 | 0x11 | Method (Request/Response): Req (0x11) | | 8 | 0x11 | Method (Request/Response): Resp (0x12) |
| 22 | | 8 | 0100 ---- | Type:Request(4) | | 8 | 0100 ---- | Type:Requet(4) |
| | | | ---- 0100 | Function group:CPU functions(4) | | | ---- 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 | Data | 8 | 0xff | Return code: Success (0xff) | Data | 8 | 0xff | Return code: Success (0xff) |
| 26 | | 8 | 0x09 | Transport size: OCTET STRING (0x09) | | 8 | 0x09 | Transport size: OCTET STRING (0x09) |
| 27 | | 16 | 0x00 | Length: 4 | | 16 | 0x00 | Length: 36 |
| 28 | | | 0x04 | | | | 0x24 | |
| 29 | | 16 | 0x01 | SZL-ID:取的值的地址 0000 0000 0000 0000 | | 16 | 0x01 | SZL-ID |
| 30 | | | 0x11 | | | | 0x11 | |
| 31 | | 16 | 0x00 | SZL-Index: 0x0001 [Identification of the module] | | 16 | 0x00 | SZL-Index: 0x0001 [Identification of the module] |
| 32 | | | 0x01 | | | | 0x01 | |
| 33 | | | | | | 16 | 0x00 | SZL partial list length in bytes: 28 |
| 34 | | | | | | | 0x1c | |
| 35 | | | | | | 16 | 0x00 | SZL partial list count: 1 |
| 36 | | | | | | | 0x01 | |
| 37 | | | | | | 16 | 0x00 | Index: Identification of the module (0x0001) |
| 38 | | | | | | | 0x01 | |
| 39 | | | | | | n | xxxx | MlfB (Order number of the module): 6ES7 151-8AB01-0AB0 |
| 40 | | | | | | 16 | 0x00 | BGTyp (Module type ID): 0x00c0 |
| 41 | | | | | | | 0xc0 | |
| 42 | | | | | | 16 | 0x00 | Ausbg (Version of the module or release of the operating system): 3 |
| 43 | | | | | | | 0x03 | |
| 44 | | | | | | 16 | 0x00 | Ausbe (Release of the PG description file): 1 |
| 45 | | | | | | | 0x01 | |

# S7协议-S7COMM-Run

1、数据请求

2、

S7Comm-Run

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

# S7协议-S7COMM-Stop

1、数据请求

2、

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

# S7协议-S7COMM-时间

1、数据请求

2、

S7Comm-获取时间

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | | | |
| 3 | | | 0x1d | | | | | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | | | |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | | | |
| 6 | | 8 | -000 0000 | TPDU number | | | | |
| | | | 1--- ---- | Last data unit:Yes | | | | |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | | | |
| 8 | | 8 | 0x07 | ROSCTR:Userdata | | | | |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | | | |
| 10 | | | 0x00 | | | | | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | | | |
| 12 | | | 0x00 | | | | | |
| 13 | | 16 | 0x00 | Parameter length | | | | |
| 14 | | | 0x08 | | | | | |
| 15 | | 16 | 0x00 | Data length | | | | |
| 16 | | | 0x04 | | | | | |
| 17 | Parameter | 24 | 0x00 | Parameter head | Parameter | | | |
| 18 | | | 0x01 | | | | | |
| 19 | | | 0x12 | | | | | |
| 20 | | 8 | 0x04 | Parameter length | | | | |
| 21 | | 8 | 0x11 | Method (Request/Response): Req (0x11) | | | | |
| 22 | | 8 | 0100 ---- | Type:Requet(4) | | | | |
| | | | ---- 0111 | Function group:Time functions(7) | | | | |
| 23 | | 8 | 0x01 | Subfunction: Read clock (1) | | | | |
| 24 | | 8 | 0x00 | Sequence number:0 | | | | |
| 25 | Data | 8 | 0x0a | Return code: Object does not exist (0x0a) | | | | |
| 26 | | 8 | 0X00 | Transport size: NULL (0x00) | | | | |
| 27 | | 16 | 0X00 | Length | | | | |
| 28 | | | 0X00 | | | | | |
| 29 | | | | | Data | | | |
| 30 | | | | | | | | |
| 31 | | | | | | | | |
| 32 | | | | | | | | |
| 33 | | | | | | | | |
| 34 | | | | | | | | |
| 35 | | | | | | | | |
| 36 | | | | | | | | |
| 37 | | | | | | | | |
| 38 | | | | | | | | |
| 39 | | | | | | | | |
| 40 | | | | | | | | |
| 41 | | | | | | | | |
| 42 | | | | | | | | |

S7Comm-设置时间

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x27 | | | | 0x21 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x07 | ROSCTR:Userdata | | 8 | 0x07 | ROSCTR:Userdata |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x08 | | | | 0x0c | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length |
| 16 | | | 0x14 | | | | 0x0e | |
| 17 | Parameter | 24 | 0x00 | Parameter head | Parameter | 24 | 0x00 | Parameter head |
| 18 | | | 0x01 | | | | 0x01 | |
| 19 | | | 0x12 | | | | 0x12 | |
| 20 | | 8 | 0x04 | Parameter length | | 8 | 0x08 | Parameter Length |
| 21 | | 8 | 0x11 | Method (Request/Response): Req (0x11) | | 8 | 0x12 | Method (Request/Response): Res (0x12) |
| 22 | | 8 | 0100 ---- | Type:Requet(4) | | 8 | 1000 ---- | Type: Response (8) |
| | | | ---- 0111 | Function group:Time functions(7) | | | ---- 0111 | Function group: Time functions (7) |
| 23 | | 8 | 0x02 | Subfunction: Set clock (1) | | 8 | 0x01 | Subfunction: Read clock (1) |
| 24 | | 8 | 0x00 | Sequence number:0 | | 8 | 0x01 | Sequence number:1 |
| 25 | Data | 8 | 0xff | Return code: Success (0xff) | | 8 | 0x00 | Data unit reference number: 0 |
| 26 | | 8 | 0X09 | Transport size: OCTET STRING (0x09) | | 8 | 0x00 | Last data unit: Yes (0x00) |
| 27 | | 16 | 0X00 | Length | | 16 | 0x00 | Error code: No error (0x0000) |
| 28 | | | 0X0a | | | | 0x00 | |
| 29 | | 8 | 0x00 | S7 Timestamp - Reserved: 0x00 | Data | 8 | 0xff | Return code: Success (0xff) |
| 30 | | 8 | 20 | S7 Timestamp - Year 1: 19 | | 8 | 0x09 | Transport size: OCTET STRING (0x09) |
| 31 | | 8 | 21 | S7 Timestamp - Year 2: 21 | | 16 | 0x00 | Length: 0 |
| 32 | | 8 | 5 | S7 Timestamp - Month: 5 | | | 0x00 | |
| 33 | | 8 | 8 | S7 Timestamp - Day: 8 | | | | |
| 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 | | | | |
| 38 | | | 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

列举一下块的类型

读取块的信息

S7Comm-获取Block信息

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x24 | | | | 0x51 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x07 | ROSCTR:Userdata | | 8 | 0x07 | ROSCTR:Userdata |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | gv | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x08 | | | | 0x0c | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length |
| 16 | | | 0x04 | | | | 0x34 | |
| 17 | Parameter | | 0x00 | | Parameter | | 0x00 | |
| 18 | | 24 | 0x01 | Parameter head | | 24 | 0x01 | Parameter head |
| 19 | | | 0x12 | | | | 0x12 | |
| 20 | | 8 | 0x04 | Parameter length: 4 | | 8 | 0x08 | Parameter length: 4 |
| 21 | | 8 | 0x11 | Method (Request/Response): Req (0x11) | | 8 | 0x12 | Method (Request/Response): Res |
| 22 | | 8 | 0100 ---- | Type:Request(4) | | 8 | 1000 ---- | Type:Response(8) |
| | | | ---- 0100 | Function group:CPU functions(4) | | | ---- 0100 | Function group:CPU functions(4) |
| 24 | | 8 | 0x01 | Subfunction: List blocks(1) | | 8 | 0x01 | Subfunction: Read SZL (1) |
| 25 | | 8 | 0x00 | Sequence number: 0 | | 8 | 0x01 | Sequence number: 1 |
| 26 | Data | 8 | 0xff | Return code: Success (0xff) | | 8 | 0x00 | Data unit reference number: 0 |
| 27 | | 8 | 0x00 | Transport size: NULL (0x00) | | 8 | 0x00 | Last data unit: Yes (0x00) |
| 28 | | 16 | 0x00 | Length | | 16 | 0x00 | Error code: No error (0x0000) |
| 29 | | | 0x00 | | | | 0x00 | |
| 30 | | | | | Data | 8 | 0xff | Return code: Success (0xff) |
| 31 | | | | | | 8 | 0x09 | Transport size: OCTET STRING (0 |
| 32 | | | | | | 16 | 0x00 | Length: 剩余字节长度 |
| 33 | | | | | | | 0x30 | |
| 34 | | | | | Item[1] | 16 | 0x00 | OB类型 |
| 35 | | | | | | | 0x08 | |
| 36 | | | | | | 16 | 0x00 | OB块数量 |
| 37 | | | | | | | 0x01 | |

| | | | | |
|---|---|---|---|---|
| Item[2] | 16 | 0x00 | 0x0E | FB类型 |
| | 16 | 0x00 | 0x00 | FB块数量 |
| Item[3] | 16 | 0x00 | 0x0C | FC类型 |
| | 16 | 0x00 | 0x00 | FC块数量 |
| Item[4] | 16 | 0x00 | 0x0A | DB类型 |
| | 16 | 0x00 | 0x00 | DB块数量 |
| Item[5] | 16 | 0x00 | 0x0B | SDB类型 |
| | 16 | 0x00 | 0x0C | SDB块数量 |
| Item[6] | 16 | 0x00 | 0x0D | SFC类型 |
| | 16 | 0x00 | 0x47 | SFC块数量 |
| Item[7] | 16 | 0x00 | 0x0F | SFB类型 |
| | 16 | 0x00 | 0x0e | SFB块数量 |

# 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

S7Comm-请求上传

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x23 | | | | 0x23 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x12 | | | | 0x10 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length |
| 16 | | | 0x00 | | | | 0x00 | |
| 17 | Parameter | 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 | Unknown byte(s) in blockcontrol: 0000 | Parameter | 8 | 0x1d | Function: Start upload (0x1d) |
| 20 | | | 0x00 | | | 8 | 0x00 | Function Status |
| 21 | | 32 | 0x00 | UploadID: 0x00000000 | | 16 | 0x00 | Unknown byte(s) in blockcontrol: 0000 |
| 22 | | | 0x00 | | | | 0x00 | |
| 23 | | | 0x00 | | | | 0x00 | UploadID: 0x00000007 |
| 24 | | | 0x00 | | | 32 | 0x00 | |
| 25 | | 8 | 0x09 | Filename Length | | | 0x00 | |
| 26 | | 8 | _ | File identifier:_ | | | 0x07 | |
| 27 | | 16 | 0x00 | Block type: 08 (OB) | | 8 | 0x07 | Blocklengthstring length |
| 28 | | | 0x08 | | | | 0 | |
| 29 | | 40 | 0x00 | Block number | | 56 | 0 | Blocklength: 0000216 |
| 30 | | | 0x00 | | | | 0 | |
| 31 | | | 0x00 | | | | 0 | |
| 32 | | | 0x00 | | | | 2 | |
| 33 | | | 0x01 | | | | 1 | |
| 34 | | 8 | A | Destination filesystem: A (Active embedded module) | | | 6 | |

# S7协议-S7COMM-Upload

1、数据请求

2、

| S7Comm-上传 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x19 | | | | 0xf1 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x08 | | | | 0x02 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length:220 |
| 16 | | | 0x00 | | | | 0xdc | |
| 17 | Parameter | 8 | 0x1e | Function: Upload (0x1e) | | 8 | 0x00 | Error class: No error (0x00) |
| 18 | | 8 | 0x00 | Function Status | | 8 | 0x00 | Error code: 0x00 |
| 19 | | 16 | 0x00 | Unknown byte(s) in blockcontrol: 0000 | Parameter | 8 | 0x1e | Function: Upload (0x1e) |
| 20 | | | 0x00 | | | 8 | 0x00 | Function Status |
| 21 | | 32 | 0x00 | UploadID: 0x00000007 | Data | 16 | 0x00 | Length:216 |
| 22 | | | 0x00 | | | | 0xd8 | |
| 23 | | | 0x00 | | | 16 | 0x00 | Unknown byte(s) in blockcontrol: 00fb |
| 24 | | | 0x07 | | | | 0xfb | |
| 25 | | | | | | n | ..... | Data |

# S7协议-S7COMM-EndUpload

1、数据请求

2、

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

# S7协议-S7COMM-Start Download

1、数据请求

2、

S7Comm-请求下载

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x31 | | | | 0x14 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x20 | | | | 0x01 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length |
| 16 | | | 0x00 | | | | 0x00 | |
| 17 | Parameter | 8 | 0xfa | Function: Start download (0xfa) | | 8 | 0x00 | Error class: No error (0x00) |
| 18 | | n | xxxx | Parameter data | | 8 | 0x00 | Error code: 0x00 |
| 19 | | | | | Parameter | 8 | 0xfa | Function: Start download (0xfa) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 36 | | 8 | 0x01 | Unknown char before load mem:1 | | | | |
| 37 | | | 0x00 | | | | | |
| 38 | | | 0x00 | | | | | |
| 39 | | 48 | 0x00 | Length of load memory | | | | |
| 40 | | | 0x05 | | | | | |
| 41 | | | 0x00 | | | | | |
| 42 | | | 0x00 | | | | | |
| 43 | | | 0x00 | | | | | |
| 44 | | | 0x00 | | | | | |
| 45 | | 24 | 0x00 | Length of MC7 code:000212 | | | | |
| 46 | | | 0x04 | | | | | |
| 47 | | | 0x00 | | | | | |
| 48 | | | 0x00 | | | | | |

| 说明 |
|---|
| 整个请求字节数 |
| 当前字节以后的字节数 |
| PDU Type，数据传输 |
| TPDU number |
| Last data unit:Yes |
| Protocol Id，默认 |
| ROSCTR:Ack_Data |
| Redundancy Identification (Reserved) |
| Protocol Data Unit Reference |
| Parameter length |
| Data length |
| Error class: No error (0x00) |
| Error code: 0x00 |
| Function: Start download (0x1a) |

# S7协议-S7COMM-Download

1、数据请求

2、

S7Comm-下载

| | | 长度(bit) | 发送 | 说明 |
|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 |
| 1 | | 8 | 0x00 | Reserved，保留默认0 |
| 2 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0xf7 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length |
| 14 | | | 0x12 | |
| 15 | | 16 | 0x00 | Data length |
| 16 | | | 0xd4 | |
| 17 | Parameter | 8 | 0x1b | Function: download (0xfb) |
| 18 | | n | xxxx | Parameter Data |
| 19 | Data | n | xxxx | Data |

S7Comm-下载

| | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 |
| 1 | | 8 | 0x00 | Reserved，保留默认0 |
| 2 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0xf7 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length |
| 14 | | | 0x01 | |
| 15 | | 16 | 0x00 | Data length:226 |
| 16 | | | 0x00 | |
| 17 | | 8 | 0x00 | Error class: No error (0x00) |
| 18 | | 8 | 0x00 | Error code: 0x00 |
| 19 | Parameter | 8 | 0xfb | Function: Download (0xfb) |
| 32 | | | 0x00 | |
| 33 | | | 0x01 | |
| 34 | | 8 | P | Destination filesystem: P |

S7Comm-下载

| | | 长度(bit) | 发送 | 说明 |
|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 |
| 1 | | 8 | 0x00 | Reserved，保留默认0 |
| 2 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0xf7 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length |
| 14 | | | 0x12 | |
| 15 | | 16 | 0x00 | Data length |
| 16 | | | 0xd4 | |
| 17 | Parameter | 8 | 0x1b | Function: download (0xfb) |
| 18 | | n | xxxx | Parameter Data |
| 19 | Data | n | xxxx | Data |

S7Comm-下载

| | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 |
| 1 | | 8 | 0x00 | Reserved，保留默认0 |
| 2 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0xf7 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length |
| 14 | | | 0x01 | |
| 15 | | 16 | 0x00 | Data length:226 |
| 16 | | | 0x00 | |
| 17 | | 8 | 0x00 | Error class: No error (0x00) |
| 18 | | 8 | 0x00 | Error code: 0x00 |
| 19 | Parameter | 8 | 0xfb | Function: Download (0xfb) |
| 32 | | | 0x00 | |
| 33 | | | 0x01 | |
| 34 | | 8 | P | Destination filesystem: P |

# S7协议-S7COMM-End Download

1、数据请求

2、

S7Comm-结束下载

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x23 | | | | 0x14 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x12 | | | | 0x01 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length:0 |
| 16 | | | 0x00 | | | | 0x00 | |
| 17 | Parameter | 8 | 0xfc | Function: download ended (0xfc) | | 8 | 0x00 | Error class: No error (0x00) |
| 18 | | n | xxx | Parameter data | | 8 | 0x00 | Error code: 0x00 |
| 19 | | | | | Parameter | 8 | 0xfc | Function: Download (0xfc) |

S7Comm-结束下载

| | | 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 | | 8 | 0x00 | Reserved，保留默认0 | | 8 | 0x00 | Reserved，保留默认0 |
| 34 | | 8 | P | Destination filesystem: P | | | | |

# S7协议-S7COMM-激活程序块

1、数据请求

2、

S7Comm-激活块

| | | 长度(bit) | 发送 | 说明 | | 长度(bit) | 响应 | 说明 |
|---|---|---|---|---|---|---|---|---|
| 0 | TPKT | 8 | 0x03 | Version，版本默认3 | TPKT | 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 | | 16 | 0x00 | 整个请求字节数 | | 16 | 0x00 | 整个请求字节数 |
| 3 | | | 0x2b | | | | 0x14 | |
| 4 | COTP | 8 | 0x02 | 当前字节以后的字节数 | COTP | 8 | 0x02 | 当前字节以后的字节数 |
| 5 | | 8 | 0xf0 | PDU Type，数据传输 | | 8 | 0xf0 | PDU Type，数据传输 |
| 6 | | 8 | -000 0000 | TPDU number | | 8 | -000 0000 | TPDU number |
| | | | 1--- ---- | Last data unit:Yes | | | 1--- ---- | Last data unit:Yes |
| 7 | S7-Header | 8 | 0x32 | Protocol Id，默认 | S7-Header | 8 | 0x32 | Protocol Id，默认 |
| 8 | | 8 | 0x01 | ROSCTR:JOB | | 8 | 0x03 | ROSCTR:Ack_Data |
| 9 | | 16 | 0x00 | Redundancy Identification (Reserved) | | 16 | 0x00 | Redundancy Identification (Reserved) |
| 10 | | | 0x00 | | | | 0x00 | |
| 11 | | 16 | 0x00 | Protocol Data Unit Reference | | 16 | 0x00 | Protocol Data Unit Reference |
| 12 | | | 0x00 | | | | 0x00 | |
| 13 | | 16 | 0x00 | Parameter length | | 16 | 0x00 | Parameter length |
| 14 | | | 0x1a | | | | 0x01 | |
| 15 | | 16 | 0x00 | Data length | | 16 | 0x00 | Data length:0 |
| 16 | | | 0x00 | | | | 0x00 | |
| 17 | Parameter | 8 | 0x28 | Function: PI-Service (0x28) | | 8 | 0x00 | Error class: No error (0x00) |
| 18 | | 56 | 0x00 | Unknown bytes: 000000000000fd | | 8 | 0x00 | Error code: 0x00 |
| 19 | | | 0x00 | | Parameter | 8 | 0x28 | Function: PI-Service (0x28) |
| 20 | | | 0x00 | | | | | |
| 21 | | | 0x00 | | | | | |
| 22 | | | 0x00 | | | | | |
| 23 | | | 0x00 | | | | | |
| 24 | | | 0xfd | | | | | |
| 25 | | 16 | 0x00 | Parameter block length: 10 | | | | |
| 26 | | | 0x0a | | | | | |
| 27 | | 8 | 0x01 | Number of blocks: 1 | | | | |
| 28 | | 8 | 0x00 | Unknown byte: 0x00 | | | | |
| 29 | | 16 | 0x00 | Block type: 0A (DB) | | | | |
| 30 | | | 0x0a | | | | | |
| 31 | | 40 | 0x00 | Block number: 00001 | | | | |
| 32 | | | 0x00 | | | | | |
| 33 | | | 0x00 | | | | | |
| 34 | | | 0x00 | | | | | |
| 35 | | | 0x01 | | | | | |
| 36 | | 8 | 0x50 | Destination filesystem: P (Passive (copied, but not chained) module) | | | | |
| 37 | | 8 | 0x05 | String length: 5 | | | | |
| 38 | | 40 | 0x5f | PI (program invocation) Service: _INSE [PI-Service _INSE (Activates a PLC module)] | | | | |
| 39 | | | 0x49 | | | | | |
| 40 | | | 0x4e | | | | | |
| 41 | | | 0x53 | | | | | |
| 42 | | | 0x45 | | | | | |

# S7通信测试程序

1、S7.NET通信库的使用

2、通信与WireShark抓包

# S7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 |
| 0x0112 | 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 | | | |
|---|---|---|---|
| 0x01 | 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 |
| 0x08 | REAL | 0x1F | IEC COUNTER |
| 0x09 | DATE | 0x20 | HS COUNTER |

| DATA | |
|---|---|
| 0x00 | 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) \| 输入（I） |
| 0x82 | Outputs (Q) \| 输出（Q） |
| 0x83 | M |
| 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，该参数是块的名称 |
| P_PROGRAM | 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

| | |
|---|---|
| P | 被动模块。Passive (copied,but not chained) module |
| A | 有源嵌入式模块。Active embedded module |
| B | 有源和无源模块。Active as well as passive module |

# 附录十三

## 1、文件系统

| | |
|---|---|
| P | 被动模块。Passive (copied,but not chained) module |
| A | 有源嵌入式模块。Active embedded module |
| B | 有源和无源模块。Active as well as passive module |

# S7协议-S7COMM-控制支持情况

1、数据请求

2、

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

朝夕教育
ZHAOXI EDU

# THANK YOU

开发进阶，蜕变架构，升职加薪，只争朝夕！

Jovan

# 获取更多资源，对话微软MVP，微信扫一扫！

微信公众号

助教小姐姐

助教小仙女