


OMRON-FINS(TCP)协议详细解析和攻击

原创 Chary Liu 2020-07-23 09:41:27 7764 收藏 19 版权

分类专栏: 漏洞挖掘 文章标签: 工业控制 网络协议

 漏洞挖掘 专栏收录该内容

1 订阅 8 篇文章 订阅专栏

OMRON FINS协议解析&攻击项目链接

1. FINS协议简介

欧姆龙(Omron)是来自日本的全球制造公司，产品是工业和制造业的机器。其中、小型PLC在国内市场有较高的占有率，有CJ、CM等系列。PLC可以支持Fins、Host link等协议进行通信。支持以太网的欧姆龙PLC CPU、以太网通信模块根据型号的不同，一般都会支持FINS(Factory Interface Network Service)协议，一些模块也会支持EtherNet/IP协议。

FINS协议使用的TCP/UDP端口：9600

FINS协议使用的编码格式为：ASCII

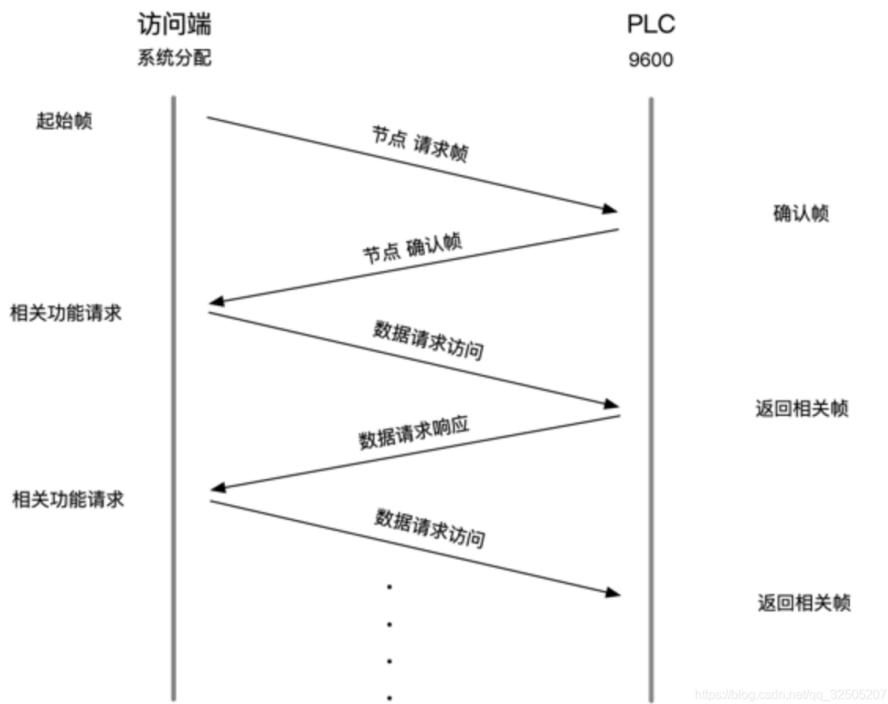
Fins协议封装在TCP/UDP之上，FINS以太网协议基于OSI模型如下。

OSI layer	Protocol
7 Application Layer	FINS
6 Presentation Layer	
5 Session Layer	
4 Transport Layer	ISO-on-TCP (RFC 1006)
3 Network Layer	IP
2 Data Link Layer	Ethernet
1 Physical Layer	Ethernet

2. FINS协议解析

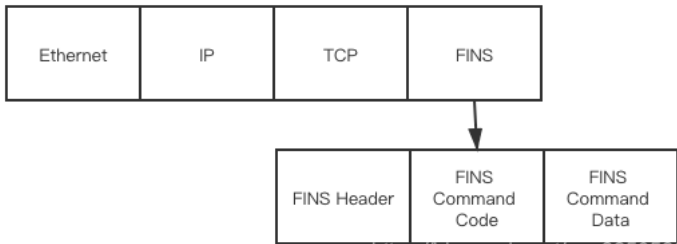
2.1 FINS会话流程

FINS会话流程是基于TCP/IP协议，下图表述了FINS会话开始几个数据帧的作用。FINS协议的会话有一次请求帧，请求帧中附着着发起方的节点参数。PLC端（Server端）会确认并将自己的节点参数放回给请求方。



2.2 FINS帧结构

FINS帧结构包含三部分组成，分别由FINS Header、FINS Command Code和FINS Command Data组成。



2.3 FINS Header

2.3.1 FINS/TCP Header

Magic Bytes(4 bytes): 0x46494e53(Protocol ID, 协议ID, FINS的16进制ASCII码)

Length(4 bytes): 数据长度, 指后续跟着的字符长度

Reserved(3 bytes):保留, 通常为0x000000

Command Type(1 byte):数据帧类型, 值如下:

- 0x00: connect request 连接请求数据帧
- 0x01: connect Response, 连接请求确认数据;
- 0x02: data, 数据传输;



Chary Liu

关注

4

Error Code(4 bytes): 保留, 通常为0x00000000

▼ OMRON FINS Protocol

▼ FINS/TCP Header

Magic Bytes: 0x46494e53

Length: 21 (0x00000015)

Command: Frame Send (0x00000002)

Error Code: Normal (0x00000000)

► FINS Header

► Command Data

0000	00 00 0a 98 86 e2 00 0c	29 98 18 da 08 00 45 00).....E.
0010	00 45 00 bb 40 00 80 06	00 00 c0 a8 14 e6 c0 a8	.E..@.....
0020	14 7a 04 08 25 80 1b f2	a0 d2 5b 5a 3b 19 50 18	.z..%... ..[Z;.P.
0030	fb e8 aa e8 00 00 46 49	4e 53 00 00 00 15 00 00FI NS.....
0040	00 02 00 00 00 80 00	02 00 7a 00 00 00 ef 05z.....
0050	05 01 00		.. https://blog.csdn.net/qq_32505207

2.3.2 FINS Header

0: ICF(1 byte): (Information Control Field) 信息控制码:

- 由4个子字段组成, 分述如下:
- 1.... = Gateway bit, 是否使用网关, 0x01表示使用;
- .1... = Data Type bit, 数据类型比特位, 0x01表示为响应, 0x00表示命令;
- ...0. = Reserved bit, 第一个保留比特位, 默认置0;
- ...0 = Reserved bit, 第二个保留比特位, 默认置0;
-0.. = Reserved bit, 第三个保留比特位, 默认置0;
-0... = Reserved bit, 第四个保留比特位, 默认置0;
-0. = Reserved bit, 第五个保留比特位, 默认置0;
-1 = Response setting bit, 第一个保留比特位响应标志为, 0x01表示非必需回应, 0x00表示必须进行回应。

1: Rev(1 byte): (Reserved) 预留 一般为0x00。

2: GCT(1 byte): (Gateway count) 网关数量, 一般为0x02。

3: DNA(1 byte): (Destination network address) 目标网络地址。

- 00: 本地网络
- 01 to 7F: 远程网络

4: DA1(1 byte): (Destination node number) 目标节点号。

- 01 to 7E: SYSMAC NET 网络节点号
- 01 to 3E: SYSMAC LINK 网络节点号
- FF: 广播节点号

5: DA2(1 byte): (Source unit number) 源单元号。

- 00: PC (CPU)
- FE: SYSMAC NET连接单元或者SYSMAC LINK单元连接网络
- 10 to 1F: CPU 总线单元

6: SNA(1 byte): (Source network address) 源网络地址。

- 00: 本地网络
- 01 to 7F: 远程网络

7: SA1(1 byte): (Source node number) 源节点号



Chary Liu

关注

 4

- 01 to 7E: SYSMAC NET 网络节点号
 - 01 to 3E: SYSMAC LINK 网络节点号
 - FF: 广播节点号
- 8: SA2(1 byte): (Source Unit address) 源单元地址
- 00: PC (CPU)
 - FE: SYSMAC NET连接单元或者SYSMAC LINK单元连接网络
 - 10 to 1F: CPU 总线单元
- 9: SID(1 byte): (Service ID) 序列号 范围00-FF
- 10 ~ 11: Commands code(2 byte): 命令码, 分为一级命令码和二级命令码。详细的命令码可参考 FINS Commands code。

FINS Header

OMRON ICF Field: 0x80, Gateway bit: Use Gateway, Data Type bit: Command, Response setting bit: Response Required

Reserved: 0x00

Gateway Count: 0x02

Destination network address: Local network (0x00)

Destination node number: SYSMAC NET (0x7a)

Destination unit address: PC (CPU) (0x00)

Source network address: Local network (0x00)

Source node number: SYSMAC NET / LINK (0x00)

Source unit address: Unknown (0xef)

Service ID: 0x05

Command CODE: Controller Data Read (0x0501)

Command Data

00000000000a9886e2000c299818da08004500.....).....E·

0000004500bb400080060000c0a814e6c0a8E·@·.....

000000147a040825801bf2a0d25b5a3b195018·z·%·...[Z;·P·

000000fbee8aae800046494e53000000150000.....FINS.....

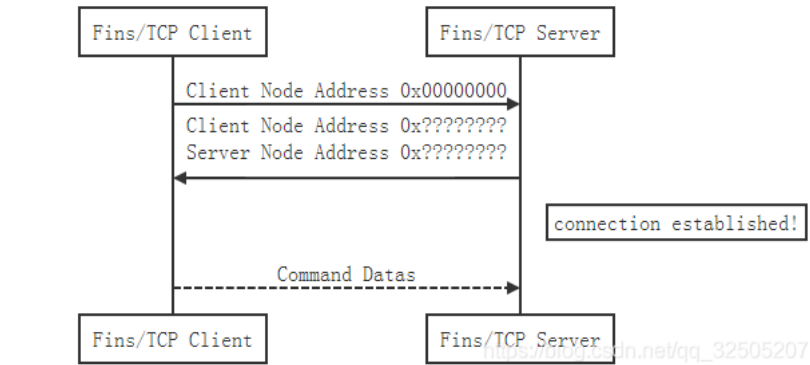
0000000002000000800002007a000000ef05.....·z·.....

000000050100.....·..

3. Command

3.1 Client/Server Node Address 建立连接

这两个字段是Fins/TCP的客户端/服务器建立连接的时候的类似DHCP协议客户端获取IP地址的时候才会出现的，如下所示：



Fins/TCP协议的客户端/服务器在传输有效的命令数据之前，由客户端先向服务器发送一个包含 Client Node Address字段的报文申请节点地址,类似DHCP协议，由于客户端申请的时候还没有节点地址，因此该字段被置为0x00000000，如下图所示：

▼ OMRON FINS Protocol

▼ FINS/TCP Header

Magic Bytes: 0x46494e53

Length: 12 (0x0000000c)

Command: Node Address Data Send (Client to Server) (0x00000000)

Error Code: Normal (0x00000000)

Client Node Address: 0 (0x00000000)

0000	00 00 0a 98 86 e2 00 0c	29 98 18 da 08 00 45 00).....E.
0010	00 3c 00 00 ba 40 00 80 06	00 00 c0 a8 14 e6 c0 a8	·<·@·.....
0020	14 7a 04 08 25 80 1b f2	a0 be 5b 5a 3b 01 50 18	·z·%·... [Z;·P·
0030	fc 00 aa df 00 00 46 49	4e 53 00 00 00 0c 00 00FI NS.....
0040	00 00 00 00 00 00 00 00	00 00

https://blog.csdn.net/qq_32505207

服务器收到客户端请求后，给客户端分配相应的节点地址并通告给客户端，同时在报文中包含服务器自己的节点地址信息，如下所示：

OMRON FINS Protocol

▼ FINS/TCP Header

Magic Bytes: 0x46494e53

Length: 16 (0x00000010)

Command: Node Address Data Send (Server to Client) (0x00000001)

Error Code: Normal (0x00000000)

Client Node Address: 239 (0x000000ef)

Server Node Address: 122 (0x0000007a)

000	00 0c 29 98 18 da 00 00	0a 98 86 e2 08 00 45 00	..).....E.
010	00 40 ee 7d 00 00 1e 06	03 8a c0 a8 14 7a c0 a8	·@·}.....z..
020	14 e6 25 80 04 08 5b 5a	3b 01 1b f2 a0 d2 50 18	·%·... [Z ;.....P.
030	10 00 e2 44 00 00 46 49	4e 53 00 00 00 10 00 00	...D·FI NS.....
040	00 01 00 00 00 00 00 00	00 ef 00 00 00 7az.....

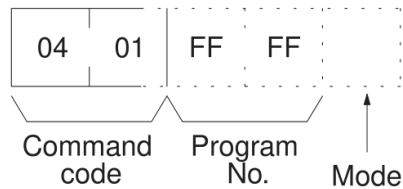
https://blog.csdn.net/qq_32505207

客户端收到服务器的响应报文后，即使用分配的节点地址与服务器进行通信，由此客户端/服务器之间就建立起了有效的长连接。

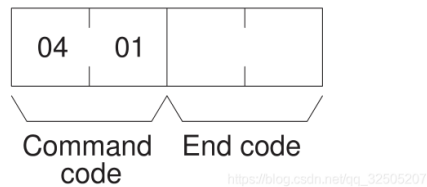
3.2 操作模式切换：RUN/MONITOR/STOP/RESET

PLC模式切换

Command Format



Response Format




Commands Code:
功能码，0x0401

Program No.:
程序码，一般为0xFFFF

Mode:
模式

- Monitor模式 0x02
- Run模式 0x04

 Chary Liu

关注

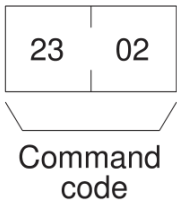
Memory Area Code: 存储区域代码，需要根据PLC型号而定

Bit/Flags: 位/状态设置

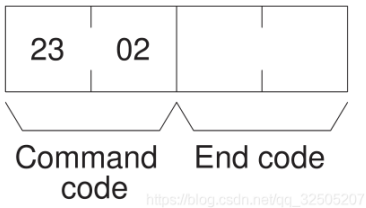
3.3.2 取消强制设置

Command Code:0x2302

Command Format



Response Format



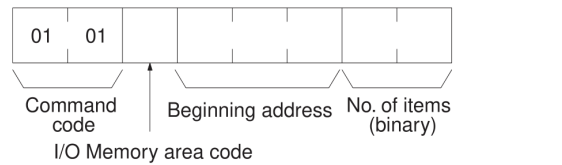
3.4 读取/写入 IO Memory Area

I/O Memory Area Codes

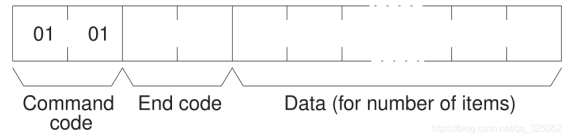
Area		Data type	CS/CJ mode memory area code (Hex)	CV mode memory area code (Hex)	Bytes per element
CIO Area	CIO	Bit	30	00	1
Work Area	WR		31	---	
Holding Bit Area	HR		32	---	
Auxiliary Bit Area	AR		33	00	
CIO Area	CIO	Word	B0	80	2
Work Area	WR		B1	---	
Holding Bit Area	HR		B2	---	
Auxiliary Bit Area	AR		B3	80	
Timer Area	TIM	Completion Flag	09	01	1
Counter Area	CNT				
Timer Area	TIM	PV	89	81	2
Counter Area	CNT				
DM Area	DM	Bit	02	---	1
	DM	Word	82	82	2
EM Area	EM bank 0 to bank C	Bit	20 to 2C	---	1
	EM bank 0 to bank C	Word	A0 to AC	90 to 97	2
	EM current bank	Word	98	98	2
	EM current bank No.	EM current bank No.	BC	9C	2
Task Flag	TK	Bit	06	---	1
	TK	Status	46	---	1
Index Register	IR	PV	DC	---	4
Data Register	DR	PV	BC	9C	2
Clock Pulses		Bit	07	---	1
Condition Flags		Bit			1

3.4.1 读取 IO Memory Area

Command Format



Response Format



Command Code: 0x0101

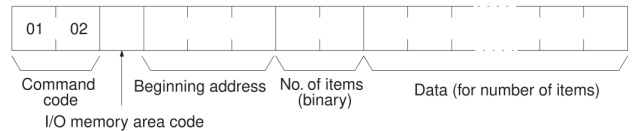
IO Memory area code: IO存储区代码

Beginning address: 起始地址

No of items (二进制) : 0 ~ 15

3.4.2 写入 IO Memory Area

Command Format



Response Format



Command Code: 0x0102

IO Memory area code: IO存储区代码

Beginning address: 起始地址

No of items (二进制) : 0 ~ 15

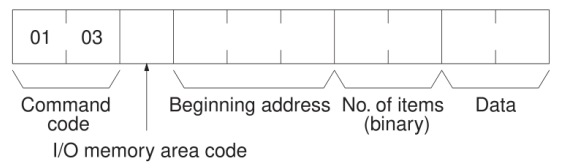
Data: 要写入的数据

记得根据data长度改fins/tcp header里的包长度

3.4.3 填充 IO Memory Area

使用相同数据填充IO Memory Area

Command Format



Response Format



Command Code: 0x0103



IO Memory area code: IO存储区代码

Beginning address: 起始地址

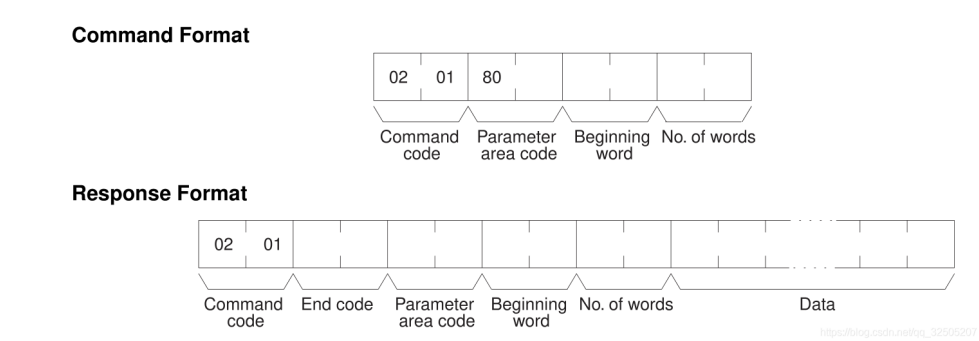
No of items (二进制) : 0 ~ 15

Data: 要填充的数据

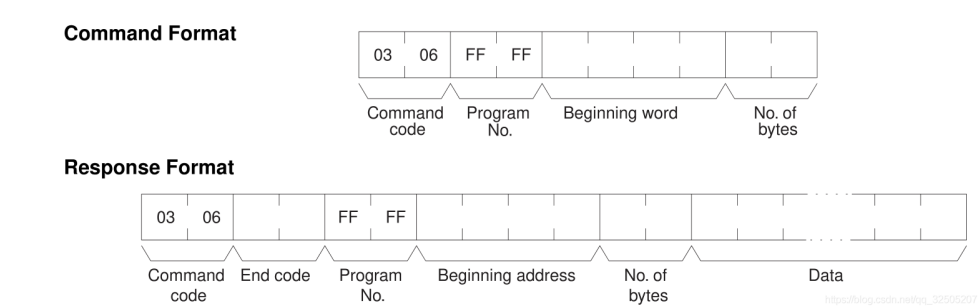
3.5 非专用IO存储区

非专用IO存储区: Parameter Area、Program Area

3.5.1 读取 Parameter Area

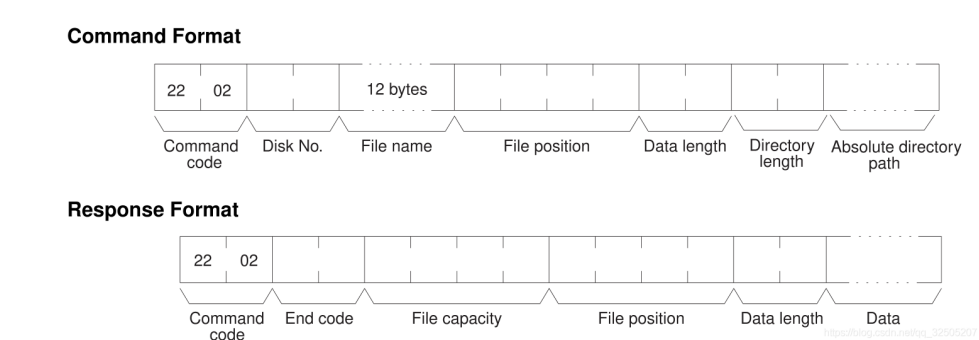


3.5.1 读取 Program Area



3.6 读取/写入/删除单个文件

3.6.1 读取单个文件



Command Code: 0x2202

Disk No: 磁盘号

- 0x8000: Memory Card
- 0x8001: EM flie memory

File name: 最大长度12bytes, 值为16进制的ascii码, 缺的

File position: 起始的byte adress, 文件开始于0x00000000

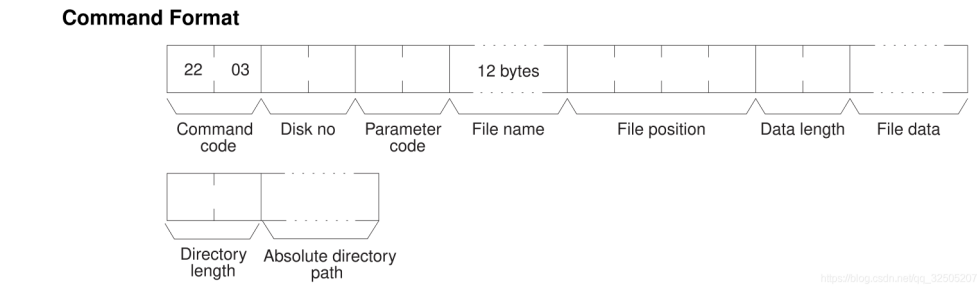
Data length: 要读的数据长度

Directory length: 文件所在目录名称长度包括\, 0x0000为默认根目录

Absolute Directory path: 最长65个字, 开始于\ (0x5c)

记得根据data长度改fins/tcp header里的包长度

3.6.2 写入单个文件



Command Code: 0x2203

Disk No: 磁盘号

- 0x8000: Memory Card
- 0x8001: EM flie memory

File name: 最大长度12bytes, 值为16进制的ascii码, 缺的后面补0x00

File position: 起始的byte adress, 文件开始于0x00000000

Data length: 要读的数据长度

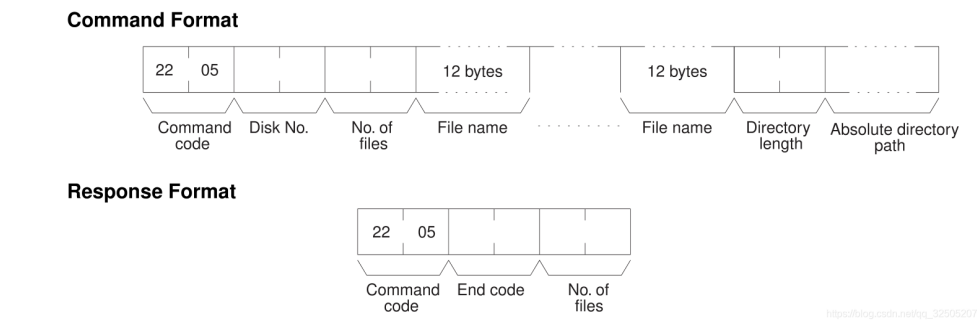
File data: 要写入的文件数据, 值为16进制的ascii码

Directory length: 文件所在目录名称长度包括\, 0x0000为默认根目录

Absolute Directory path: 最长65个字, 开始于\ (0x5c)

记得根据data长度改fins/tcp header里的包长度

3.6.3 删除文件



Command Code: 0x2202

Disk No: 磁盘号

- 0x8000: Memory Card
- 0x8001: EM flie memory

Chary Liu

关注

No of files:	指定要删除的文件数量，单个写0x0001即可
File name:	最大长度12bytes，值为16进制的ascii码，缺的后面补0x00
Directory length:	文件所在目录名称长度包括\，0x0000为默认根目录
Absolute Directory path:	最长65个字，开始于\（0x5c）

4. 攻击

由于fins协议的设计缺陷，攻击者可以通过以下步骤对其进行攻击：

1. 与plc建立tcp连接
2. 发送fins协议会话初始包
3. 根据协议解析的fins协议的对应功能的报文结构组包
4. 发送恶意报文：如启停plc、篡改指定内存、读写文件等。

Omron-Fins通讯协议04-24

根据别人的完档加自己的测试完成的Omron-Fins通讯协议，亲测有用，不是官方文档，如有纰漏，欢迎大家指...

基于 FINS 协议的OMRON PLC 与上位机通信08-29

基于 FINS 协议的OMRON PLC 与上位机通信

评论 5

请先[登录](#)后发表评论~

评论

weixin_58404086

您好，我问下，cxp软件能用这个协议跟plc通信吗

回复 5 月前 ...

撸BUG

QT能使用这个协议与plc通信吗

回复 7 月前 ...

Chary Liu 作者

回复 撸BUG

和编程工具没关系，只要是能建立tcp连接就行

回复 7 月前 ...

glow_worm

没有PLC可以模拟FINS tcp 通信吗

回复 1 年前 ...

Chary Liu 作者

回复 glow_worm

不能，我这个是对一个plc的一些功能写的

回复 1 年前 ...

欧姆龙PLC的FINS协议解释(实测通过) - CSDN博客11-1

欧姆龙PLC的FINS协议解释 UDP访问方式: 读取示例:读取DM区20个字, 从DM100H开始 命令:80 00 02 00 41 ...

Socket编程之聊天程序 - 模拟Fins/ModBus协议通信过程...11-1

目前工业控制中的温控主流采用串口通信,使用数据通信协议为ModBus协议,而与底层PLC通信则多采用Fins协...

串口与欧姆龙通信Fins协议07-21

详细介绍串口与欧姆龙通信Fins指令 CPU单元: CJ2M-CPU35 RS232串口选件板: CP1W-CIF01 USB转232...

FINS通讯手册07-10

欧姆龙官方手册, 详细的介绍了fins协议的格式规则, 很实用

欧姆龙以太网FINS协议通讯测试11-16

用C#写的通讯测试工具, 基于以太网FINS协议. 实现了CS/CJ/NJ系列, DM、WR、CIO区的位和字的读写功...

欧姆龙fins通讯协议

Chary Liu

关注

4

https://blog.csdn.net/qq_32505207/article/details/107484766

11/14