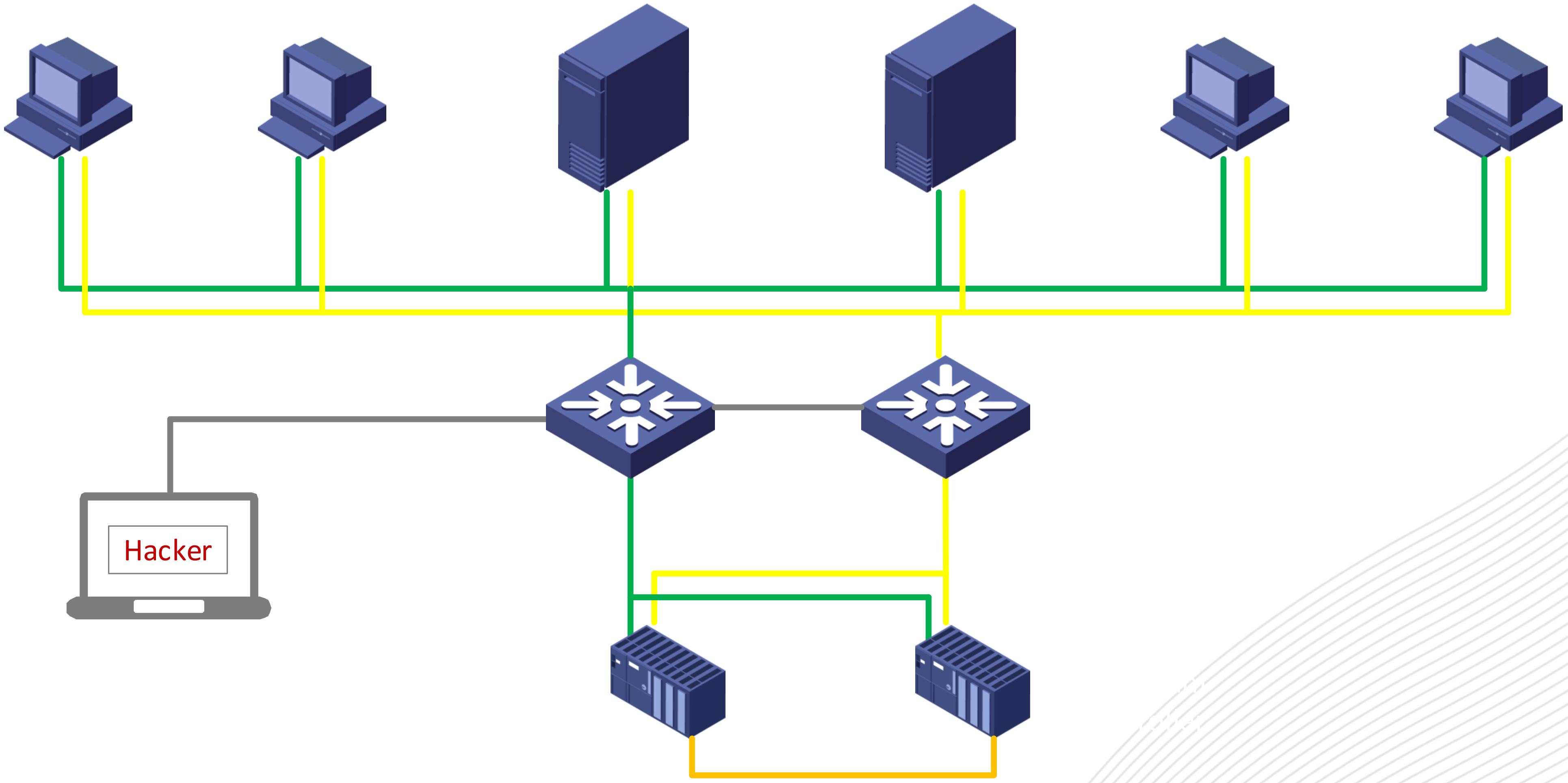
Industrial Red Team

工业集散控制系统（DCS）脆弱性分析

工控安全红队IRTeam

INDUSTRIAL RED TEAM

DCS网络架构图



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

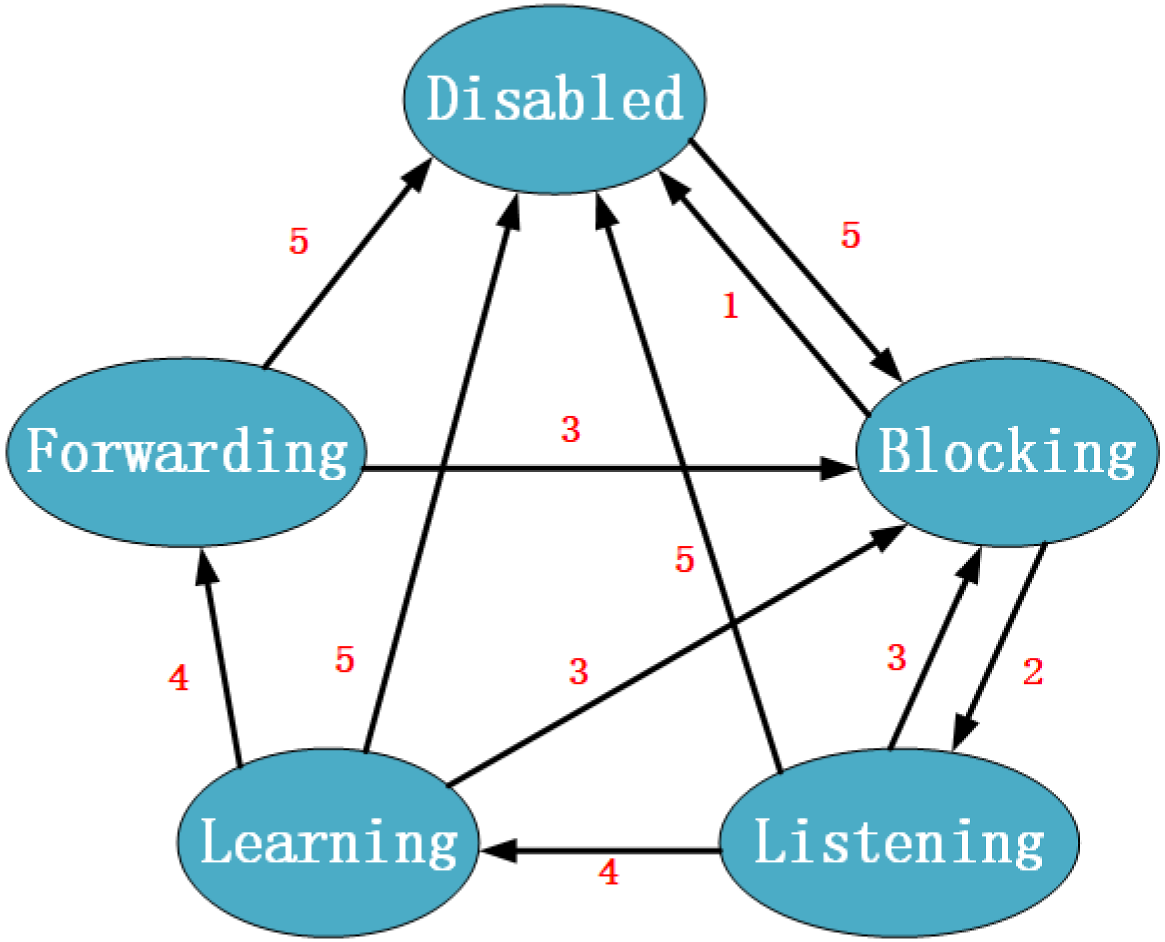
3、2台Server（windows Server 2003）

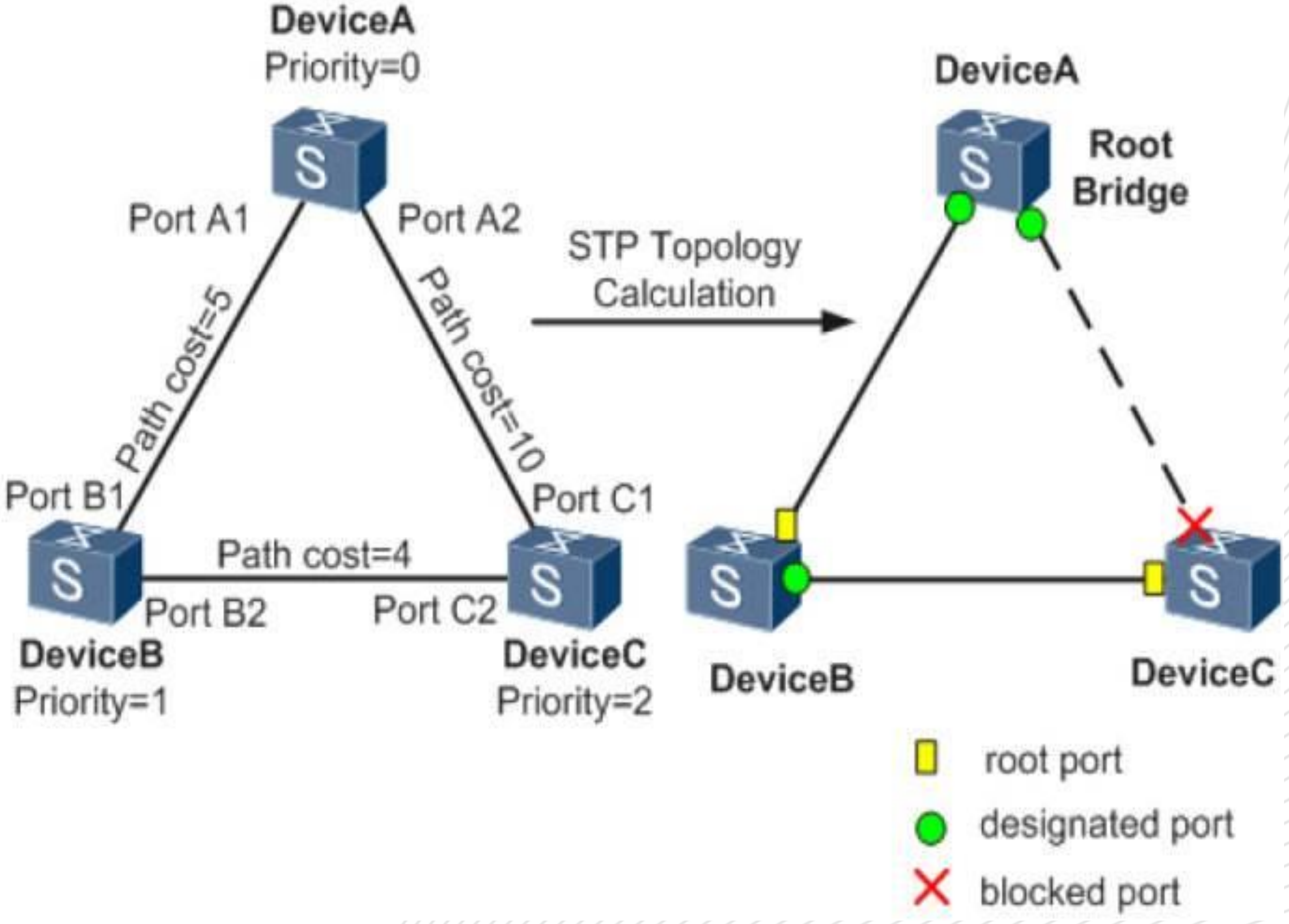
4、4台Client（Windows XP SP3）

5、1台Kali 2008

DCS系统的脆弱性-网络层

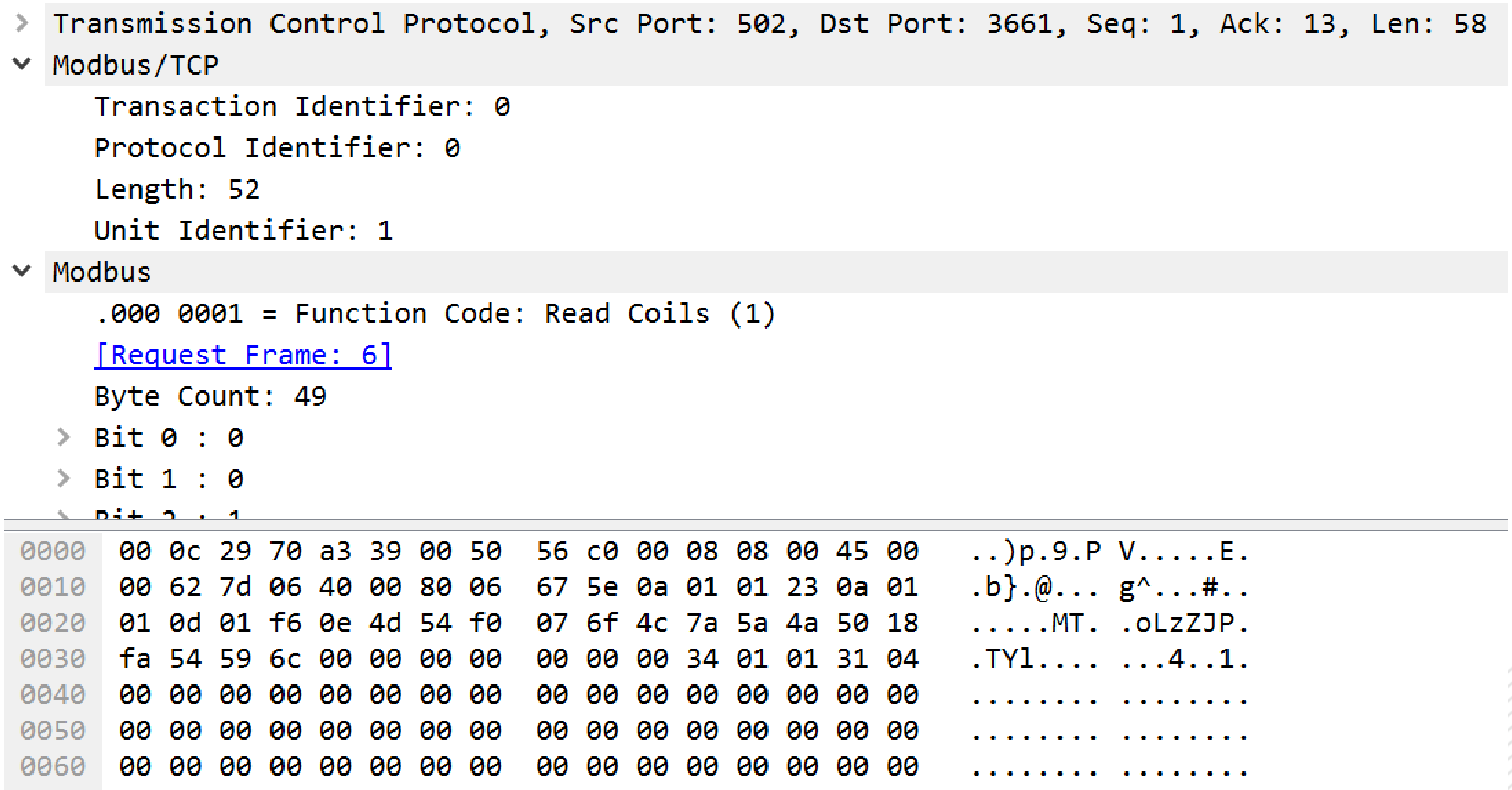
可以采用STP的BPDU的攻击方式产生网络的震荡





DCS系统的脆弱性-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
  > Bit 2 : 1

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

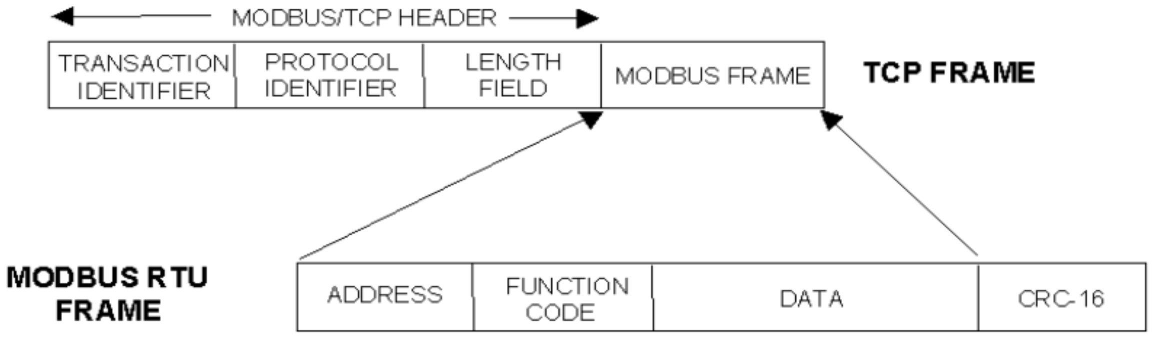


Figure 1-1 Modbus RTU Protocol within a TCP/IP Frame

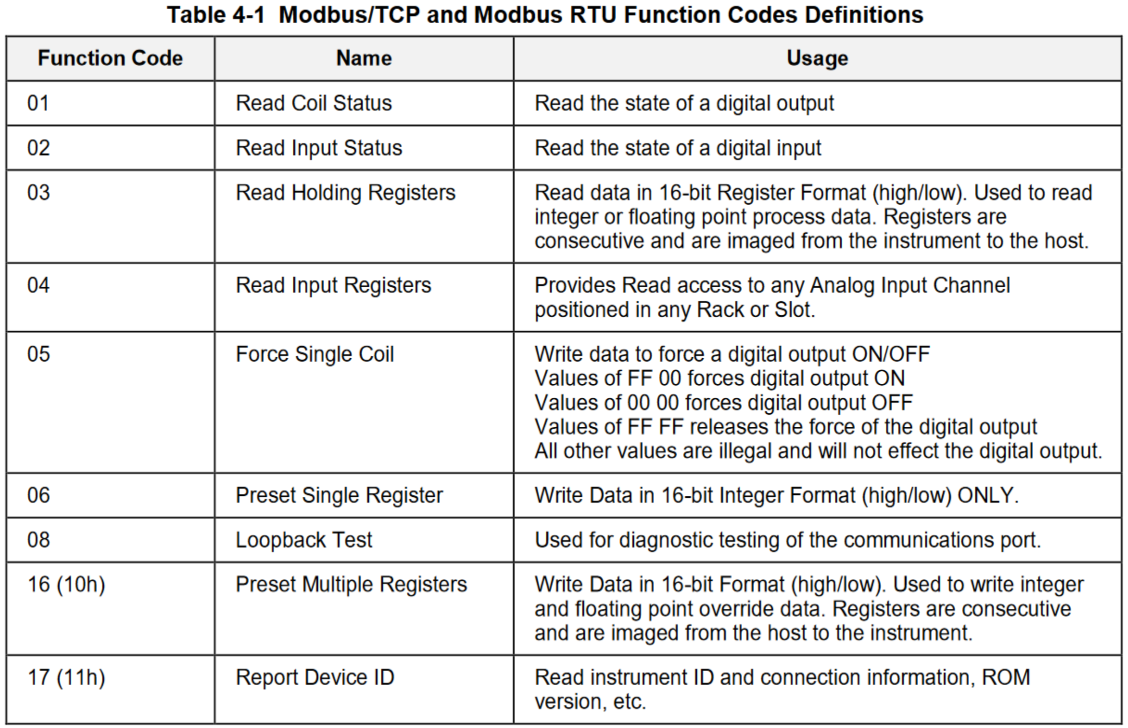


Table 4-1 Modbus/TCP and Modbus RTU Function Codes Definitions

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）

工控安全红队IRTeam率先开发国内首款基于工控安全的测试平台KALI ICS，平台内集成多数工控测试工具和一款软PLC的模拟器。

IRT 工控安全红队

微信扫描二维码，关注我的公众号

INDUSTRIAL RED TEAM