# 2017年威努特
# 工控安全公开培训

北京威努特技术有限公司

# 课程表

1、工控系统基础知识与工控网络架构介绍

2、传统信息安全与工控安全的区别

3、工控安全风险及隐患介绍

4、典型工控安全事件深度分析

5、工控网络渗透技术介绍

6、典型行业案例分享

7、主流工控安全产品及解决方案介绍

# 工控系统基础知识与网络架构介绍

北京威努特技术有限公司

# 目录

# 基础知识

## 自动化基本技能

- **自动化(Automation)：**是指机器或装置在无人干预的情况下按规定的程序或指令自动地进行操作或运行；
- **自动化装置：**是指无需人的参与就可以自动进行工作，完成特定任务的机器；
- **工业自动化系统：**是运用控制理论、仪器仪表、计算机和其它信息技术，对工业生产过程实现检测、控制、优化、调度、管理和决策，以达到增加产量、提高质量、降低消耗、确保安全为目标的集成系统。

# 基础知识

## 自动化基本技能

- **自动控制：**指在无人直接参与的情况下，利用控制装置使被控对象（机器、设备）的某一个物理量自动地按照预定的规律运行运行；
- **控制系统：**为实现某一控制目标所需要的物理部件（及软件）的有机组合，通常由控制器和被控对象组成；
- **自动控制理论：**是研究自动控制共同规律的科学，它包括以反馈控制理论为基础的古典控制理论（单输入、单输出），以状态空间为基础的现代控制理论（多输入、多输出）以及以模糊控制和神经网络为代表的智能控制（不需精确数学模型）。

# 基础知识

## 工业控制系统定义

- **工业控制:**主要是指使用计算机技术，微电子技术，电气手段，使工厂的生产和制造过程更加自动化、效率化、精确化，并具有可控性及可视性；
- **工业控制系统（简称：ICS）:**由几种不同类型的控制系统组成，包括监控数据采集系统（SCADA），分布式控制系统（DCS），可编程逻辑控制器（PLC）和远程测控单元（RTU）等，广泛运用于石油、石化、冶金、电力、燃气、煤矿、烟草以及市政等领域。

# 基础知识

- **工业自动控制系统基本类型：**
  - **顺序控制系统：**顺序控制是按照预先规定的时间顺序（或逻辑关系），逐步对各设备或对象进行控制到方法。如电梯等；
  - **过程控制系统：**对工业生产过程中的各物理量（如温度、压力、液位等）进行闭环控制，使其按照要求的规律变化；
  - **运动控制系统：**控制运动物体的转速或位置，使其按照要求的规律变化。如调速系统，位置随动系统等；
  - 监控系统：对生产过程中的大量运行参数进行采集、显示、记录或报警。

# 目录

# 系统基本组成

一个自动化系统无论结构多么复杂都有下面几个主要组成部分：

**检测器：**主要是获得反馈信息，计算目标值与实际值之间的差值-△e；

**控制器：**相当于大脑在分析决策上的作用，适时地决定系统应该实施怎样的调节控制；

**执行器：**完成控制器下达的决定；

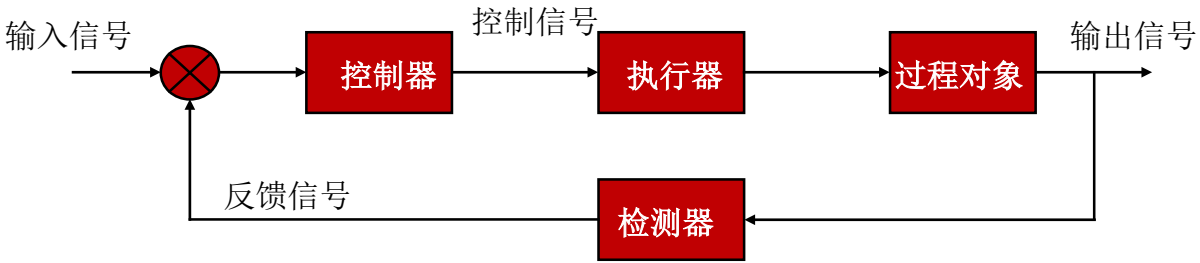
**对象：**　被控制的客观实体；

**其它：**输入值（设定值、扰动变量等）。

# 系统结构

**自动化系统结构：**

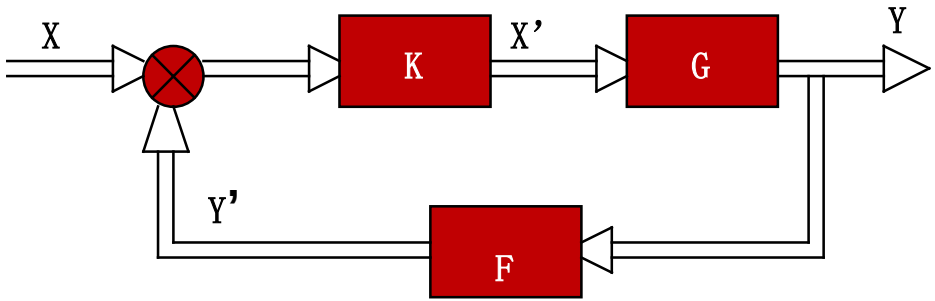
一个简单自动控制系统结构图




自动控制是基于反馈的技术。反馈理论的要素包括三个部分：测量、比较和执行。测量关心的变量，与期望值相比较，用两者之间的偏差来纠正调节系统的响应。因此，自动化技术的核心思想是反馈，通过反馈建立起输入（原因）和输出（结果）之间的联系。使控制器可以根据输入与输出的实际情况来决定控制策略，以便达到预定的系统功能。
系统构成前向通道和反馈通道两个通道，前向通道是任务执行的功能主体。

# 系统结构

复杂自动化系统往往是多变量，多回路，多类型的系统。




$$X = \{ x_0, x_1, x_2, \ldots x_n \}$$

$$Y = \{ y_0, y_1, y_2, \ldots y_n \}$$

# 主要组成部分及其作用

**控制器 - 系统的大脑**　自动控制系统中控制器在整个系统中起着重要的作用，扮演着系统管理和组织核心的角色。系统性能的优劣很大程度上取决于控制器的好坏。

AB-1769

欧姆龙cj1

施耐德140

三菱Q系列

ABB

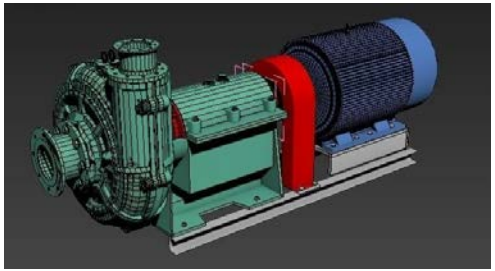
B&R

Deltav

S7-400、400H

# 主要组成部分及其作用

**执行器 - 系统的手脚**　执行器在自动控制系统中的作用就是相当于人的四肢，它接受调节器的控制信号，改变操纵变量，使生产过程按预定要求正常运行。在生产现场，执行器直接控制工艺介质，若选型或使用不当，往往会给生产过程的自动控制带来困难。因此执行器的选择、使用和安装调试是个重要的环节。


# 主要组成部分及其作用

**传感器 - 系统的耳目**　传感器被用来测量各种物理量，种类有温度传感器、流量传感器、压力传感器等等。传感器要满足可靠性的要求，从传感器的输出信号中得到被测量的原始信息，如果传感器不稳定，那么对同样的输入信号，其输出信号就不一样，则传感器会给出错误的输出信号，也就失去了传感器应有的作用。

# 计算组件-传统控制与现代控制

**PID控制——比例、积分、微分**

PID控制器作为最早实用化的控制器已有50多年历史，现在仍然是应用最广泛的工业控制器。PID控制器简单易懂，使用中不需精确的系统模型等先决条件，因而成为应用最为广泛的控制器。

现代控制——最优控制、自适应控制、预测控制、
自学习控制……

智能控制——模糊控制、专家系统、神经网络

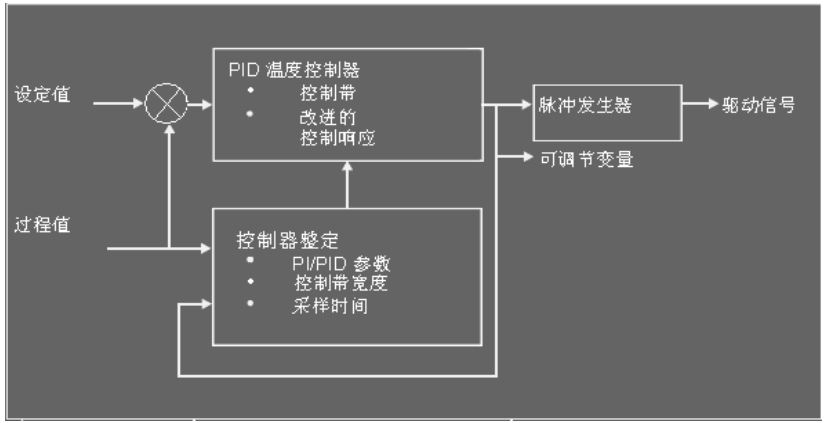
# 专用软件-策略组态与人机界面

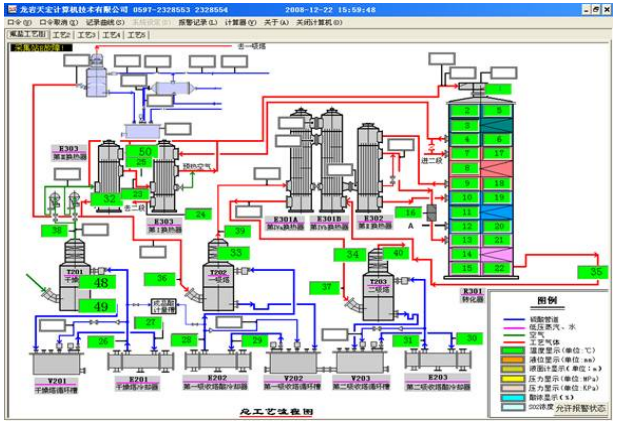
**顺序控制开关逻辑控制**

如：继电器矩阵控制、可编程序控制器 I/O模块输入输出控制。

**回路控制连续调节控制**

如： FM 458-1 DP 应用模块专为自由组态的高性能闭环控制和技术应用（如运动控制）而设计。



# 自动控制系统专用软件

| PLC + HMI部分 | | | | |
|---|---|---|---|---|
| 厂商 | 硬件型号 | 下位编程 | 上位监控 | |
| 西门子 | S5 | Step5 | | |
| | S7-200 | MicroWin | | |
| | S7-300/400 | Step7 | WinCC | |
| | S7-300/400 S7-1200/1500 | TIA Step7 | TIA WinCC | |
| ABB | AC500 | Automation Builer | | |
| 施耐德 | 小型PLC M2X8 | SoMache | Vijeo Citect<br>Intouch | |
| | 中大型PLC | Unity Pro | | |
| GE | PAC RX3i PAC RX7i | Proficy ME | Cimplicity iFix | |
| | PAC 8000 | PAC8000 Workbench | | |
| Rockwell | MicroLogix | RSLogix500 | RSView32<br>RSView SE | |
| | 1769/1756 | RSLogix5000 | | |
| Omron | | CX-One | | |
| Mitisubishi | FX | FX Win | | |
| | Q | GX-Developer | | |

# 自动控制系统专用软件

| Scada部分 | | | | |
|---|---|---|---|---|
| 厂商 | 硬件型号 | 下位编程 | 上位监控 | |
| 西门子 | | | PVSS | 跨平台 |
| 施耐德 | | Wonderware子公司 | IAS Scada | |
| | | Foxboro子公司 | I/A Scada | Unix环境 |
| | | Foxboro子公司 | Evo Scada | |
| | | Telvent子公司 | OA Sys | Unix环境 |
| | | ScadaPack子公司 | Clear Scada | |
| ABB | | PP-LV | MicroScada | |
| | | PA-OGP | Scada Vantadge | |

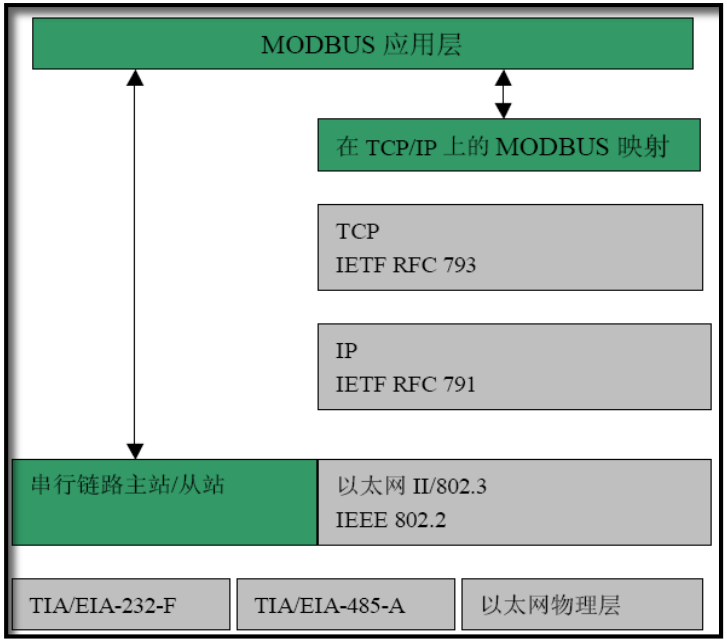
# 自动控制系统专用软件

| DCS部分 | | | | |
|---|---|---|---|---|
| 厂商 | 硬件型号 | 下位编程 | 上位监控 | |
| ABB | Freelance 700F/800F/900F | CBF | DigiVis | |
| | Symphony | Composer | PGP | |
| | Symphony Plus | S+ Engineer | S+ Operation | |
| | 800xA | 800xA | | |
| 施耐德-Foxboro | | I/A DCS | | |
| | | Evo FCS DCS | | |
| 西门子 | PCS7 | PCS7 | | |
| 西门子SPPA | T-3000 | T-3000 | | |
| Emerson PSS | DeltaV | DeltaV | | 石化专用 |
| Emerson PWS | Ovation | Ovation | | 电力专用 |
| GE-Xinhua | XDPS-400+/600 | XDPS | | |
| | OC-4000E | OC-6000E | | |
| | OC-6000E | OC-6000E | | |
| 上海新华 | XDC800 | On XDC | | |
| 中控 | JX-300XP | Advant Trol Pro | | |
| | ECS-100 | | | |
| | ECS-700 | Visual Field | | |
| 和利时 | FM/SM | Smartpro MACS II/MACS4/MACS5 | | |
| | KM | MACS6 | | |
| | NM | MACS5/6 专用版 | | 核电专用 |

# 自动控制系统专用软件

| 触摸屏部分 | | | | |
|---|---|---|---|---|
| 厂商 | 硬件型号 | 下位编程 | 上位编程 | |
| 西门子 | | | WinCC Flexible | |
| AB | 老触摸屏 | | Panel Builer | |
| | 新触摸屏 | | RSView ME | |
| ABB | CP400 | | CP400Soft | |
| | PP800 | | Panel Buile 800 | |
| Omron | | | NS-System | |
| 施耐德 | | | Vijeo Designer | |
| 施耐德-Proface | | | GP-Pro EX | |

# MODBUS 协议-标 准 分 类




MODBUS分为两种：

- 串行链路上的MODBUS
- (MODBUS on Serial Line)
- TCP/IP上的MODBUS
- (MODBUS on TCP/IP)

串行链路上的MODBUS

- TIA/EIA-232-F
- TIA/EIA-485-A

TCP/IP 上的 MODBUS

- RFC793和RFC791

# MODBUS on Serial与OSI层次对应关系

| Layer | ISO/OSI Model | |
|---|---|---|
| 7 | Application | MODBUS Application Protocol |
| 6 | Presentation | Empty |
| 5 | Session | Empty |
| 4 | Transport | Empty |
| 3 | Network | Empty |
| 2 | Data Link | MODBUS Serial Line Protocol |
| 1 | Physical | EIA/TIA-485 (or EIA/TIA-232) |

MODBUS协议的各个层次只采用了OSI层次模型中的三层：物理层，数据链路层和应用层。各层都有各层相应的标准规范。

物理层标准：EIA/TIA-485(或EIA/TIA-232)

数据链路层标准：MODBUS Serial Line Protocol MODBUS串行线协议

应用层标准：MODBUS Application Protocol MODBUS应用协议

# MODBUS on Serial与OSI层次对应关系

MODBUS协议的各个层次只采用了OSI层次模型中的三层：物理层，数据链路层和应用层。各层都有各层相应的标准规范。

物理层：在多种物理媒体上以多种速率采用 CSMA/CD 访问方式

10Base2,10Base5,10BaseTX,10BaseFX

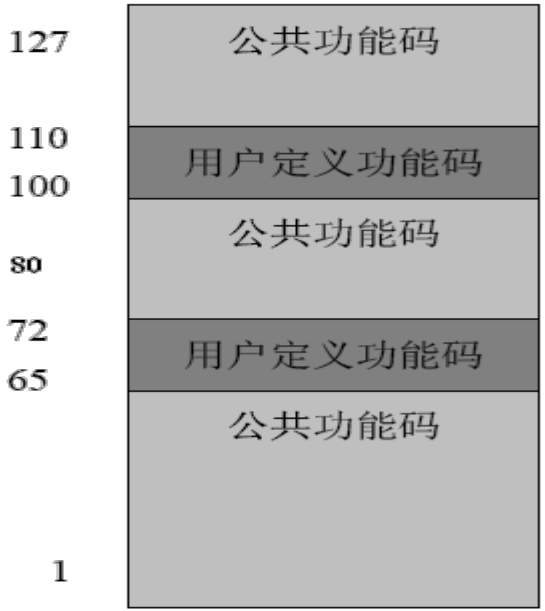
数据链路层：IEEE 802.3

逻辑链路控制 LLC (Logical Link Control)子层

媒体接入控制 MAC (Medium Access Control)子层

应用层标准：MODBUS Application Protocol MODBUS应用协议

# 功能码(FUNCTION CODE)




功能码——定义某一个PDU的功能

分为公共功能码和用户功能码

公共功能码——唯一的被较好定义的MODBUS组织认可的功能码

用户功能码——不保证唯一的，各用户不同的。只能定义65～72和100～110范围内的功能码。

# 功能码(FUNCTION CODE)

| | | | | 功能码 | | | |
|---|---|---|---|---|---|---|---|
| | | | | 码 | 子码 | （十六进制） | 页 |
| 数据访问 | 比特访问 | 物理离散量输入 | 读输入离散量 | 02 | | 02 | 11 |
| | | 内部比特或物理线圈 | 读线圈 | 01 | | 01 | 10 |
| | | | 写单个线圈 | 05 | | 05 | 16 |
| | | | 写多个线圈 | 15 | | 0F | 37 |
| | | | | | | | |
| | 16 比特访问 | 输入存储器 | 读输入寄存器 | 04 | | 04 | 14 |
| | | 内部存储器或物理输出存储器 | 读多个寄存器 | 03 | | 03 | 13 |
| | | | 写单个寄存器 | 06 | | 06 | 17 |
| | | | 写多个寄存器 | 16 | | 10 | 39 |
| | | | 读/写多个寄存器 | 23 | | 17 | 47 |
| | | | 屏蔽写寄存器 | 22 | | 16 | 46 |
| | | | | | | | |
| | 文件记录访问 | | 读文件记录 | 20 | 6 | 14 | 42 |
| | | | 写文件记录 | 21 | 6 | 15 | 44 |
| 封装接口 | | | 读设备识别码 | 43 | 14 | 2B | |

**常用的功能码——01H,02H,03H,04H,05H,06H,16H,23H等**

# 常用数据类型(Data Type)

| 基本表格 | 对象类型 | 访问类型 | 内容 |
| --- | --- | --- | --- |
| 离散量输入 | 单个比特 | 只读 | I/O 系统提供这种类型数据 |
| 线圈 | 单个比特 | 读写 | 通过应用程序改变这种类型数据 |
| 输入寄存器 | 16-比特字 | 只读 | I/O 系统提供这种类型数据 |
| 保持寄存器 | 16-比特字 | 读写 | 通过应用程序改变这种类型数据 |

bit——比特类型，通常用于表示开关量状态。

WORD——字类型，通常表示一个数。

浮点数可以采用IEEE754格式，其长度为32bits。占2个字长。在显示时，注意高低位是否需要交换。

# 其它工业通讯协议

**美系厂家：**

Rockwell ABRockwell的PLC主要是包括：PLC2、PLC3、PLC5、SLC500、ControlLogix等型号，PLC2和PLC3是早期型号，现在用的比较多的小型PLC是SLC500，中型的一般是ControlLogix，大型的用PLC5系列。DF1协议是Rockwell各PLC都支持的通讯协议，DF1协议可以通过232或422等串口介质进行数据传输，也可以通过DH、DH+、DH485、ControlNet等网络介质来传输。DF1协议的具体内容可以在AB的资料库中下载。

AB的PLC也提供了OPC和DDE，其集成的软件中RSLogix中就包含DDE和OPC SERVER，可以通过上述软件来进行数据通讯。AB的中高档的PLC还提供了高级语言编程功能，用户还可以通过编程实现自己的通讯协议。

# 其它工业通讯协议

GE现在在国内用的比较多的主要是90-70和90-30，Rx3i及Rx7i系列PLC，这两款PLC都支持SNP协议，SNP协议在其PLC手册中有协议的具体内容。现在GE的PLC也可以通过以太网链接，GE的以太网协议内容不对外公开，但GE提供了一个SDK开发包，可以基于该开发包通讯。

S7-200是西门子小型PLC，因为其低廉的价格在国内得到了大规模的应用，支持MPI、PPI和自由通讯口协议。西门子300的PLC支持MPI，还可以通过Profibus 和工业以太网总线系统和计算机进行通讯。如果要完成点对点通讯，可以使用CP340/341。

S7400作为西门子的大型PLC，提供了相当完备的通讯功能。可以通过S7标准的MPI进行通讯，同时可以通过C-总线，Profibus和工业以太网进行通讯。如果要使用点对点通讯，S7-400需要通过CP441通讯模块。西门子的通讯协议没有公开，许多组态软件都支持MPI、PPI等通讯方式，Profibus和工业以太网一般通过西门子的软件进行数据通讯。

# 其它工业通讯协议

**施耐德:**（莫迪康）施耐德的PLC型号比较多，在国内应用也比较多。其通讯方式主要是支持Modbus和MODBUS PLUS两种通讯协议。Modbus协议在工控行业得到了广泛的应用，已不仅仅是一个PLC的通讯协议，在智能仪表，变频器等许多智能设备都有相当广泛的应用。

MODBUS经过进一步发展，现在又有了MODBUS TCP方式，通过以太网方式进行传输，通讯速度更快。

Modbus PLUS相对于MODBUS传送速度更快，距离更远，该通讯方式需要在计算机上安装MODCON提供的SA85卡并需安装该卡的驱动才可以进行通讯。除了上述两种方式之外，莫迪康的PLC还支持如TCP/IP以太网，Unitelway， FIPWAY，FIPIO，AS-I，Interbus-s等多种通讯方式。

# 其它工业通讯协议

欧姆龙系列PLC在中国推广的也比较多。在通讯方式上，OMRON现在主要采用两种通讯方式：

- Host Link协议是基于串口方式进行数据传输的通讯方式。当PLC进入MONITOR方式时，上位机可以和欧姆龙PLC通讯。在和欧姆龙通讯时要注意，两次通讯之间要留一定时间，如果通讯速度过快容易造成PLC通讯异常。
- ControlLink是欧姆龙PLC的一种快速通讯方式。Control Link通过板卡进行数据通讯，板卡之间有数据交换区，由板卡实现数据的交换从而完成数据采集功能。使用该方式通讯需配置欧姆龙的驱动。

# 其它工业通讯协议

三菱PLC的小型PLC在国内的应用非常广泛。三菱的PLC型号也比较多，主要包括FX系列，A系列和Q系列。三菱系列PLC通讯协议是比较多的，各系列都有自己的通讯协议。如FX系列中就包括通过编程口或232BD通讯，也可以通过485BD等方式通讯。其A系列和Q系列可以通过以太网通讯。当然，三菱的PLC还可以通过CC-LINK协议通讯。

松下PLC和计算机之间可以通过串口和以太网进行通讯。其采用的通讯协议是MEWTOCOL协议。如大多数日系PLC一样，MEWTOCOL协议比较简单。许多软件都可以从PLC中直接读取数据。

# 通用工业通讯协议端口

## Protocols

| Service | Records | Port |
| --- | --- | --- |
| Siemens S7 | port:102 | TCP 102 |
| Modbus | port:502 | TCP 502 |
| IEC 60870-5-104 | port:2404 | TCP 2404 |
| DNP3 | port:20000 | TCP 20000 |
| EtherNet/IP | port:44818 | TCP 44818 |
| BACnet | port:47808 | TCP 47808 |
| Tridium Niagara Fox | port:1911 | TCP 1911 |
| OMRON FINS | port:9600 | TCP 9600 |
| PCWorx | port:1962 | TCP 1962 |
| ProConOs | port:20547 | TCP 20547 |
| MELSEC-Q | port:5007 | TCP 5007 |
| Crimson V3 | port:789 | TCP 789 |

# 工业通讯协议列表

| 类别 | 工业通讯协定 | | | |
|---|---|---|---|---|
| 程序自动化 | ▪ BSAP | ▪ CC-Link | ▪ CIP | ▪ CAN |
| | ▪ CANopen | ▪ ControlNet | ▪ DeviceNet | ▪ DF-1 |
| | ▪ DirectNET | ▪ EtherCAT | ▪ Ethernet Global Data (EGD) | ▪ Ethernet Powerlink |
| | ▪ EtherNet/IP | ▪ FINS | ▪ FOUNDATION fieldbus | ▪ GE SRTP |
| | ▪ HART Protocol | ▪ Honeywell SDS | ▪ HostLink | ▪ INTERBUS |
| | ▪ MECHATROLINK | ▪ MelsecNet | ▪ Modbus | ▪ Optomux |
| | ▪ PieP | ▪ Profibus | ▪ PROFINET IO | ▪ SERCOS interface |
| | ▪ SERCOS III | ▪ Sinec H1 | ▪ SynqNet | ▪ TTEthernet |
| | ▪ RAPIEnet | | | |
| 工业控制系统 | ▪ OPC DA | ▪ OPC HAD | ▪ OPC UA | ▪ MTConnect |
| 智能建筑 | ▪ 1-Wire | ▪ BACnet | ▪ C-Bus | ▪ DALI |
| | ▪ DSI | ▪ KNX | ▪ LonTalk | ▪ Modbus |
| | ▪ oBIX | ▪ VSCP | ▪ X10 | ▪ xAP |
| | ▪ ZigBee | | | |
| 输配电通讯协定 | ▪ IEC 60870-5 | ▪ DNP3 | ▪ IEC 60870-6 | ▪ IEC 61850 |
| | ▪ IEC 62351 | ▪ Modbus | ▪ Profibus | |
| 智能电表 | ▪ ANSI C12.18 | ▪ IEC 61107 | ▪ DLMS/IEC 62056 | ▪ M-Bus |
| | ▪ Modbus | ▪ ZigBee Smart Energy 2.0 | | |
| 车用通讯 | ▪ CAN | ▪ FMS | ▪ FlexRay | ▪ IEBus |
| | ▪ J1587 | ▪ J1708 | ▪ J1939 | ▪ Keyword Protocol 2000 |
| | ▪ LIN | ▪ MOST | ▪ NMEA 2000 | ▪ VAN |

# 目录

# 现代工业自动化系统

现代工业自动化系统是在现代工业企业大型化、连续化、高速化、快节奏生产的必然产物。

基础自动化L1（控制层）：现场设备控制系统
过程自动化L2（运行层）：生产过程监控系统
工厂自动化L3（管理层）：MES制造执行系统
企业自动化L4（经营层）：ERP企业资源规划

工业自动化最新技术：工业计算机网络控制系统

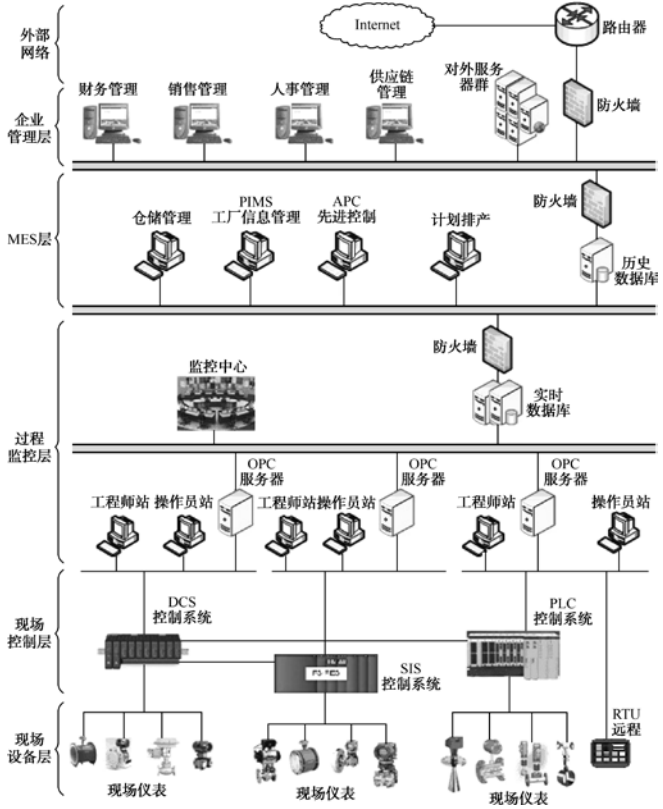
GB/T33009.1-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第1部分：防护要求》
GB/T33009.2-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第2部分：管理要求》
GB/T33009.3-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第3部分：评估指南》
GB/T33009.4-2016 《工业自动化和控制系统网络安全 集散控制系统(DCS)第4部分：风险与脆弱性检测要求》

# 工业控制系统典型架构

- 企业典型分层架构；

典型的企业生产或制造系统包括现场设备层、现场控制层、过程监控层、制造执行系统（MES）层、企业管理层和外部网络。

由图可以看出，以制造执行系统（MES）层分界，向上为通用IT领域，向下为工业控制系统领域。



# 制造执行系统（MES）层

制造执行系统（MES）层包括工厂信息管理系统（PIMS）、先进控制系统（APC）、历史数据库、计划排产、仓储管等。

1．工厂信息管理系统（PIMS）

工厂信息管理系统（PIMS）是根据企业在信息化时代生产过程中的实际需求而推出的一款管理软件。工厂信息管理系统（PIMS）以“生产管理实用化”作为生产信息管理系统建设的出发点和最终目标，提供了一套先进的现代企业生产管理模式，帮助企业在激烈的市场竞争中全方位地迅速了解自己、对市场的快速变化做出符合自身实际情况的物流调整和决策，提升企业在同行业中的竞争能力。

# 制造执行系统（MES）层

2．先进控制系统（APC）

先进控制系统就是以先进过程控制（Advanced Process Control，APC）技术为核心的上位机监控系统。

先进过程控制技术是具有比常规单回路PID控制更好控制效果的控制策略统称，专门用来处理那些采用常规控制效果不好，甚至无法控制的复杂工业过程控制问题。

先进过程控制技术可分为3大类：

（1）经典的先进控制技术：变增益控制、时滞补偿控制、解耦控制、选择性控制等。

（2）现今流行的先进控制技术：模型预测控制（MPC）、统计质量控制（SQC）、内模控制（IMC）、自适控制、专家控制、神经控制器、模糊控制、最优控制等。

（3）发展中的先进控制：非线性控制及鲁棒控制等。

# 过程监控层

过程监控层包括数据采集与监控系统（SCADA），分散型控制系统（DCS），安全仪表控制系统（SIS），可编程逻辑控制系统（PLC）的工程师站、操作站、OPC服务器、实时数据库、监控中心等。

1．数据采集与监控系统（SCADA）

数据采集与监控系统（Supervisory Control And Data Acquisition，SCADA）是以计算机为基础的生产过程控制与调度自动化系统。

SCADA系统涉及到组态软件、数据传输链路（如数传电台、GPRS等）、工业隔离安全网关，其中工业隔离安全网关是保证工业信息网络的安全，工业上大多数都要用到这种安全防护性的网关，防止病毒入侵，以保证工业数据、信息的安全。

SCADA的应用领域很广，可以应用于电力、冶金、安防、水利、污水处理、石油天然气、化工、交通运输、制药，以及大型制造等领域的数据采集与监视控制及过程控制等诸多领域。

# 过程监控层

2．分散型控制系统（DCS）

分散型控制系统（Distributed Control System，DCS）是由过程控制级和过程监控级组成的以通信网络为纽带的多级计算机系统，综合了计算机（Computer）、通信（Communication）、显示（CRT）和控制（Control）等4C技术，其基本设计思路是分散控制、集中操作、分级管理、配置灵活、组态方便。

系统组成主要由现场控制站（I/O站）、数据通信系统、人机接口单元、操作员站、工程师站、机柜、电源等。系统具备开放的体系结构，可以提供多层开放数据接口。

# 过程监控层

3．安全仪表系统（SIS）

安全仪表系统（Safety Instrumented System，SIS），有时称为安全联锁系统（Safety Interlocking System，SIS），主要是为了实现工厂控制系统中报警和安全联锁，对控制系统中检测的结果实施报警动作或调节或停机控制，是工厂企业自动控制中的重要组成部分。

安全仪表系统（SIS）主要特点（7点）

- 安全联锁的预报警功能;
- 安全联锁延时;
- 第一事故原因区别;
- 安全联锁系统的投入和切换;
- 分级安全联锁;
- 手动紧急停车;
- 安全联锁复位;

安全仪表系统（SIS）主流系统结构：有三重化（TMR）和四重化（2004D）两种。

# 过程监控层

4. 可编程控制器（PLC）

可编程逻辑控制器（Programmable Logic Controller，PLC），是一种采用一类可编程的存储器，用于其内部存储程序，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的控制设备。

从实质上来看，可编程逻辑控制器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，其外形典型图如图所示。

1）PLC基本构成

2）PLC的工作原理

# 过程监控层

5．OPC服务器

OPC全称是Object Linking and Embeding（OLE）for Process Control，它的出现为基于Windows的应用程序和现场过程控制应用建立了桥梁。

OPC标准以微软公司的OLE技术为基础，它的制定是通过提供一套标准的OLE/COM接口完成的，在OPC技术中使用的是OLE 2技术，OLE标准允许多台微机之间交换文档、图形等对象。

通过DCOM技术和OPC标准，完全可以创建一个开放的、可互操作的控制系统软件。OPC采用客户/服务器模式，把开发访问接口的任务放在硬件生产厂家或第三方厂家，以OPC服务器的形式提供给用户，解决了软、硬件厂商的矛盾，完成了系统的集成，提高了系统的开放性和可互操作性。

# 现场控制层

现场控制层包括数据采集与监控系统（SCADA）、分散型控制系统（DCS）、安全仪表控制系统（SIS）、可编程逻辑控制系统（PLC）的控制器或控制站。

这些控制器或控制站已在上一节中详细介绍，在此不做介绍。

# 现场设备层

现场设备层包括现场仪表和其他控制设备。

现场仪表通常包括温度、压力、流量、液位、电量、位移等仪表，特种检测仪表如成分分析仪，以及控制阀、电动阀等执行机构。

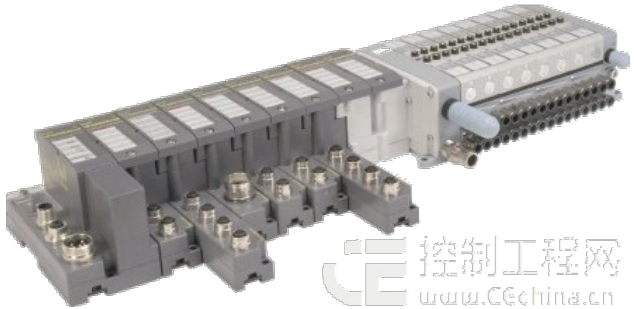
1．远程终端终端（RTU）

远程终端装置（Remote Terminal Unit，RTU）是用于监视、控制与数据采集的应用控制设备，具有遥测、遥信、遥调、遥控等功能。

目前，远程终端装置尚无统一行业标准，一般来说符合下列技术特征的控制设备，均称为RTU。

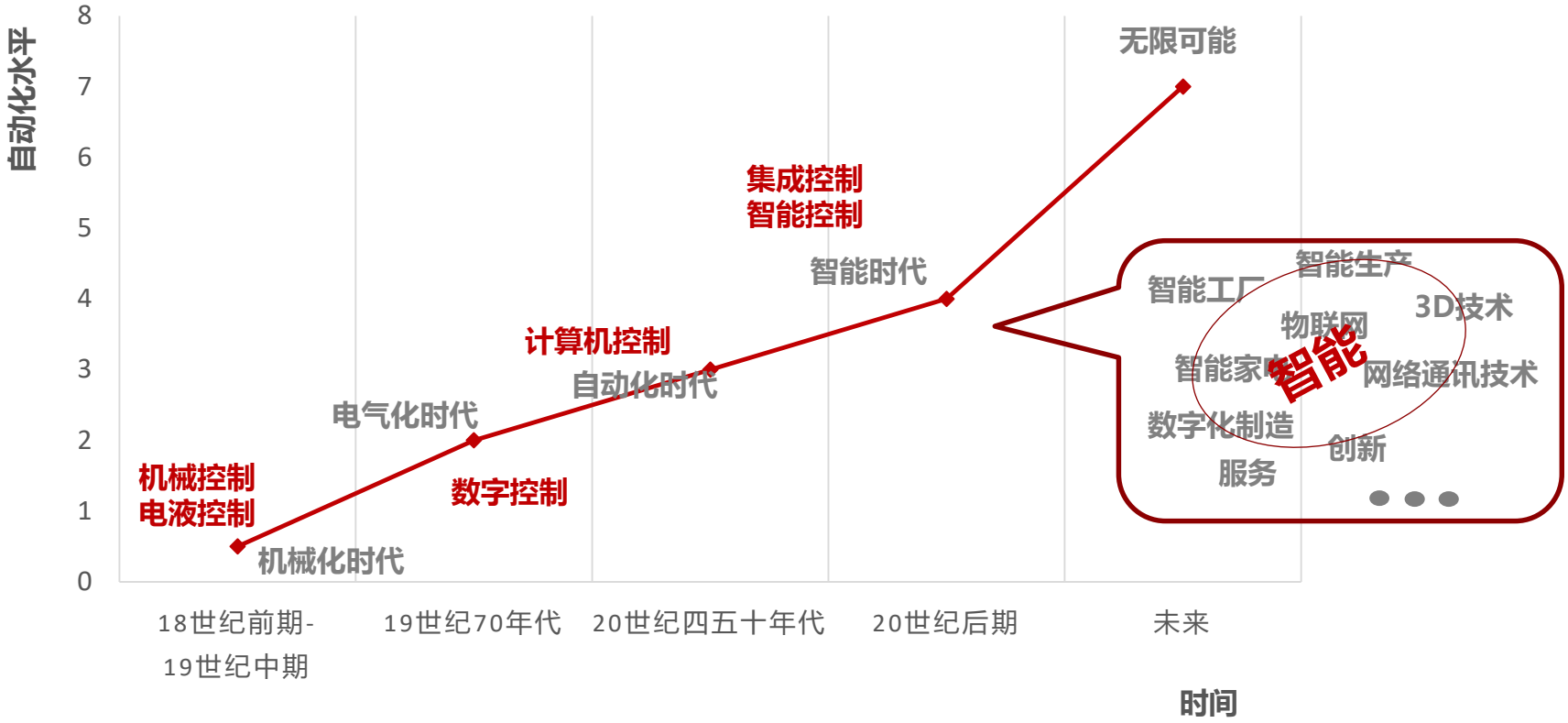
RTU主要特点

RTU主要功能



# 目录

# 控制系统发展


自动化水平
8
7
6
5
4
3
2
1
0
机械控制
电液控制
机械化时代
电气化时代
数字控制
计算机控制
自动化时代
集成控制
智能控制
智能时代
无限可能
智能
智能工厂
智能生产
3D技术
物联网
智能家电
网络通讯技术
数字化制造
创新
服务
18世纪前期-
19世纪中期
19世纪70年代
20世纪四五十年代
20世纪后期
未来
时间

# 控制系统技术转变


趋势
以前与现在
现在与将来
▪ 封闭、专有系统
▪ 开放系统，并大规模采用IT技术
▪ 通信是以独立的解决方案提供给用户
▪ 集成化网络系统，并与IT基础设备充分互联，以实现远程控制和互操作性能
▪ 只有生产部门负责工业通信的运营
▪ IT部门与生产部门共同负责自动化网络运营
▪ 很少用到安全机制
▪ 综合全面的安全防范解决方案
▪ 面向产品的服务
▪ 面向解决方案的服务

# 单一产品功能不断更新

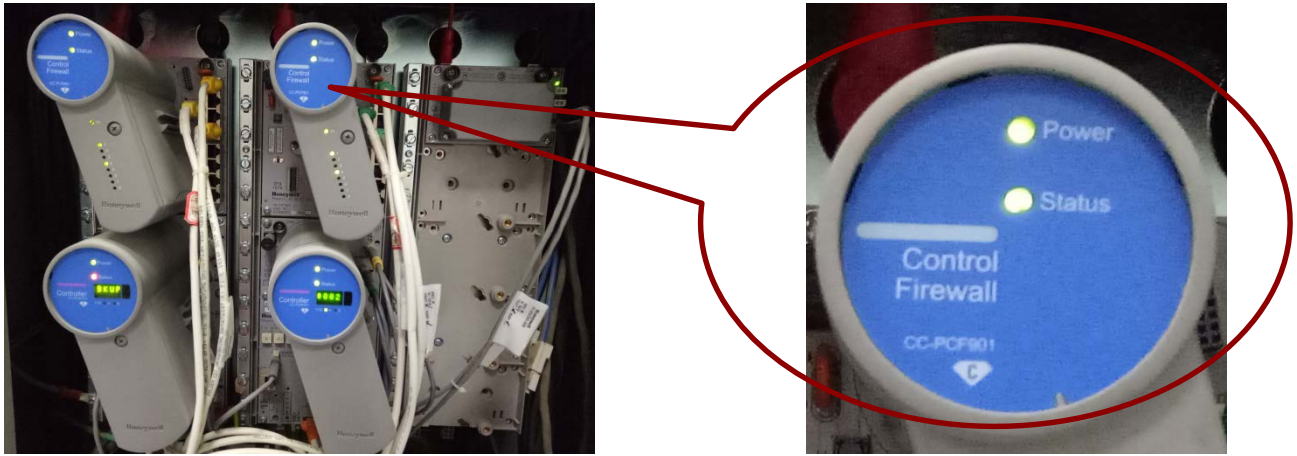
- **功能繁杂、多样化**
  - **DCS、PLC、RTU、远程I/O单元**以往都具备各自应用优势，应用于不同场合，但随着硬件、软件技术的进步，控制系统开始出现融合现象；
  - **专用控制软件功能多样化：**国外DCS、PLC等系统专用软件，以往都为专用，因此价格昂贵。但随着市场需求的变化，部分专用软件开始大量集成IO驱动，使得在不同厂商间通用成为现实，如intouch、kingview、wincc、iFiX、FC7.0等；
  - 接口更丰富，计算功能更强大。

# 单一产品功能不断更新

- **设备高度集成、智能化**
  - 底层采集设备如变送器，其无论集成度、智能化都越来越成熟，在满足客户基本需求的同时，也为智能制造提供了良好的应用基础；
  - **高端控制器越来越专业化：**在一些重要领域，如大铁、冶金、船舶、汽轮机、压缩机、核电等控制领域，专业性强、具有一定保密性，专用控制设备应运而生。如压缩机ESD的CCC、HMIA等厂家；
  - 一次仪表与二次仪表趋于一体化，控制与显示、记录一体化发展，直至虚拟仪表。即采集与变送、控制与输出高度集成、计算机模拟。

# 单一产品功能不断更新

- **控制与安全兼顾、安全集成**
  - 随着工业的发展、两化融合、工控系统面临越来越大的安全压力，部分新兴或老牌DCS企业开始研发自己的安全产品；



# 目录

# 电力系统网络架构-火电

**主控系统**

机组控制系统-DCS

数据采集系统-DAS

炉膛安全保护监控系统-BMS系统

顺序控制系统—SCS

电液调节系统—DEH

**公用辅助系统**

输煤系统

化学水处理系统

除灰、除渣、电除尘系统

吹灰、定排系统

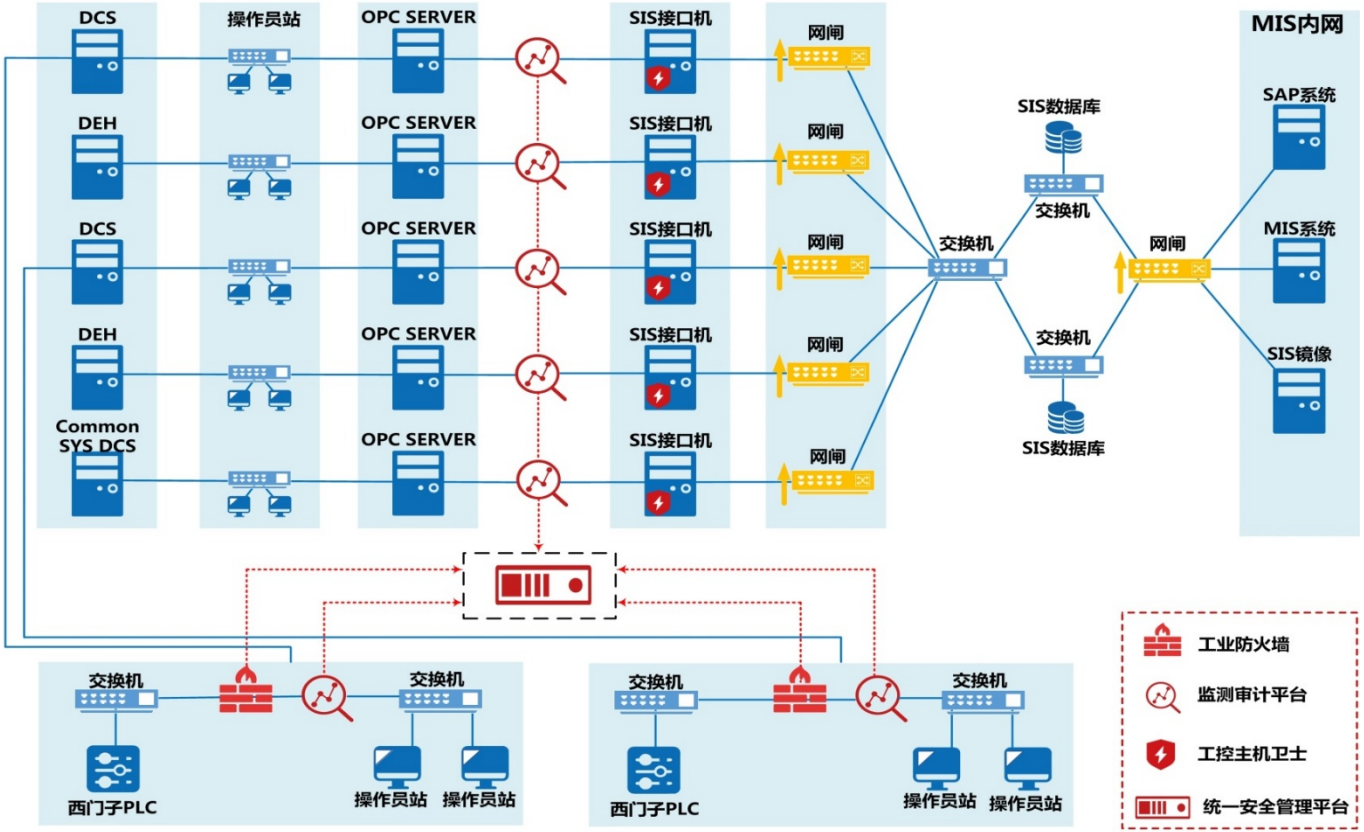
**管理系统**

管理系统信息系统-MIS

厂级监控信息系统-SIS

能源管控系统-EMS

# 电力系统网络架构-火电

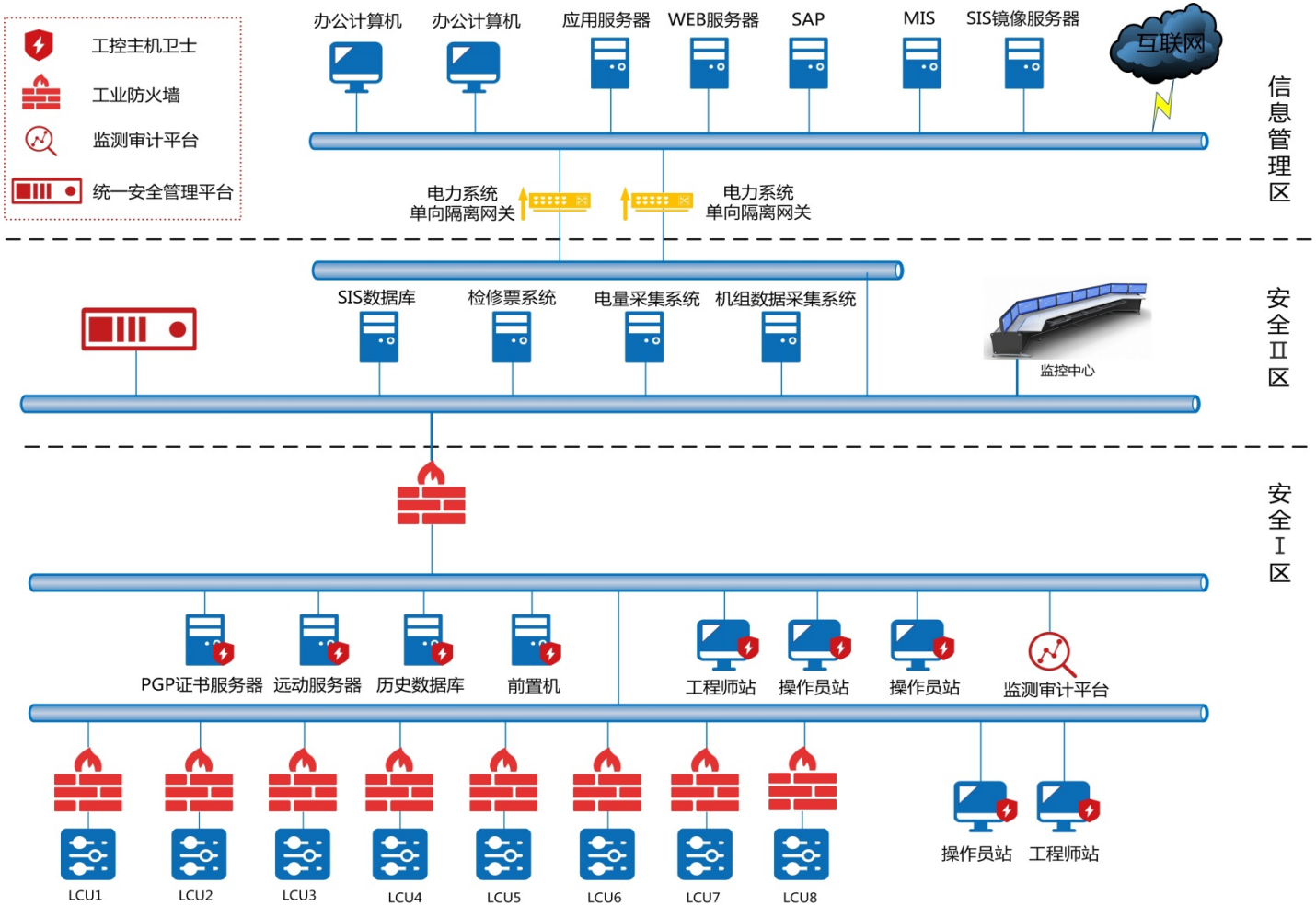

DCS
操作员站
OPC SERVER
SIS接口机
网闸
DEH
DCS
DEH
Common SYS DCS
交换机
SIS数据库
MIS内网
SAP系统
MIS系统
SIS镜像
西门子PLC
操作员站
工业防火墙
监测审计平台
工控主机卫士
统一安全管理平台

# 电力系统网络架构-水电

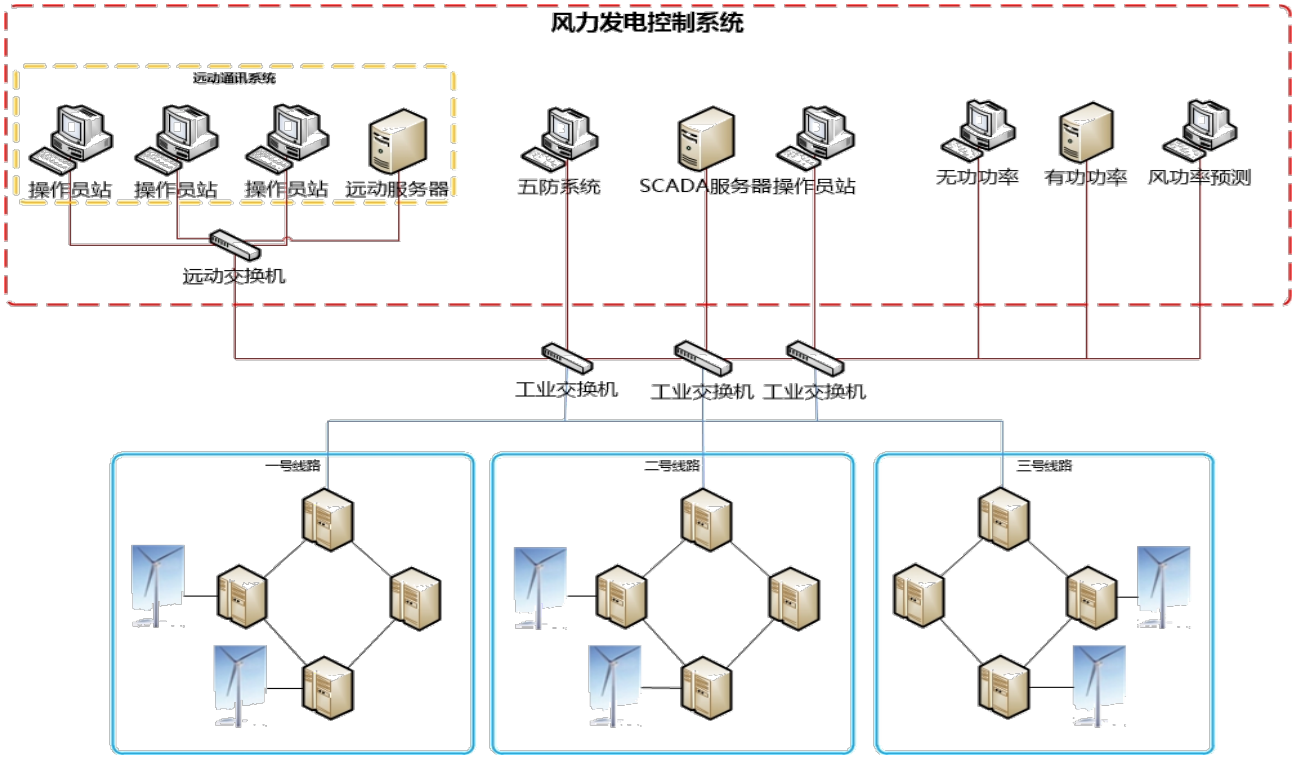
## 功能描述

- **操作终端：**操作员工作站（冗余）、工程师站（兼仿真培训）、通信处理计算机、厂长终端等设备。监控系统的功能可在监控室内全部实现；
- **现地控制单元：**包括水轮发电机组、开关站、公用设备、主变、闸门等设备的控制装置。现地各LCU在主控层和网络全部失效情况下也应能独立运行操作；

# 电力系统网络架构-水电


工控主机卫士
工业防火墙
监测审计平台
统一安全管理平台
办公计算机
办公计算机
应用服务器
WEB服务器
SAP
MIS
SIS镜像服务器
互联网
信息管理区
电力系统
单向隔离网关
电力系统
单向隔离网关
SIS数据库
检修票系统
电量采集系统
机组数据采集系统
监控中心
安全II区
安全I区
PGP证书服务器
远动服务器
历史数据库
前置机
工程师站
操作员站
操作员站
监测审计平台
操作员站
工程师站
LCU1
LCU2
LCU3
LCU4
LCU5
LCU6
LCU7
LCU8

# 电力系统网络架构-风力发电



# 精密制造

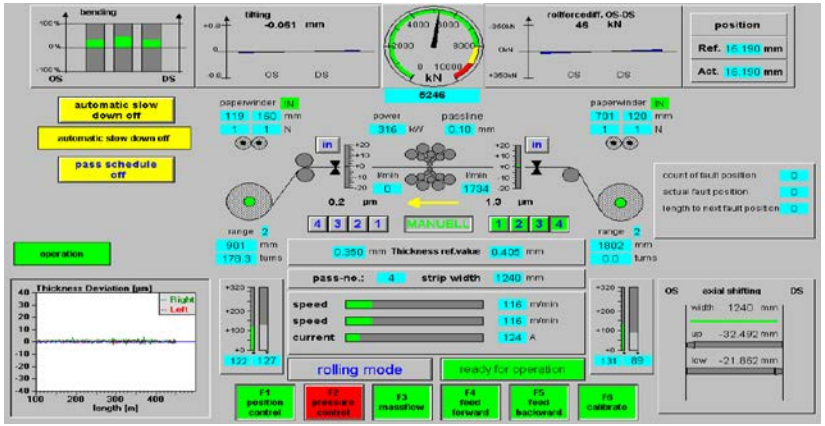
钛金板带轧机二级自动化系统

典型工业计算机网络控制系统：L1+L2

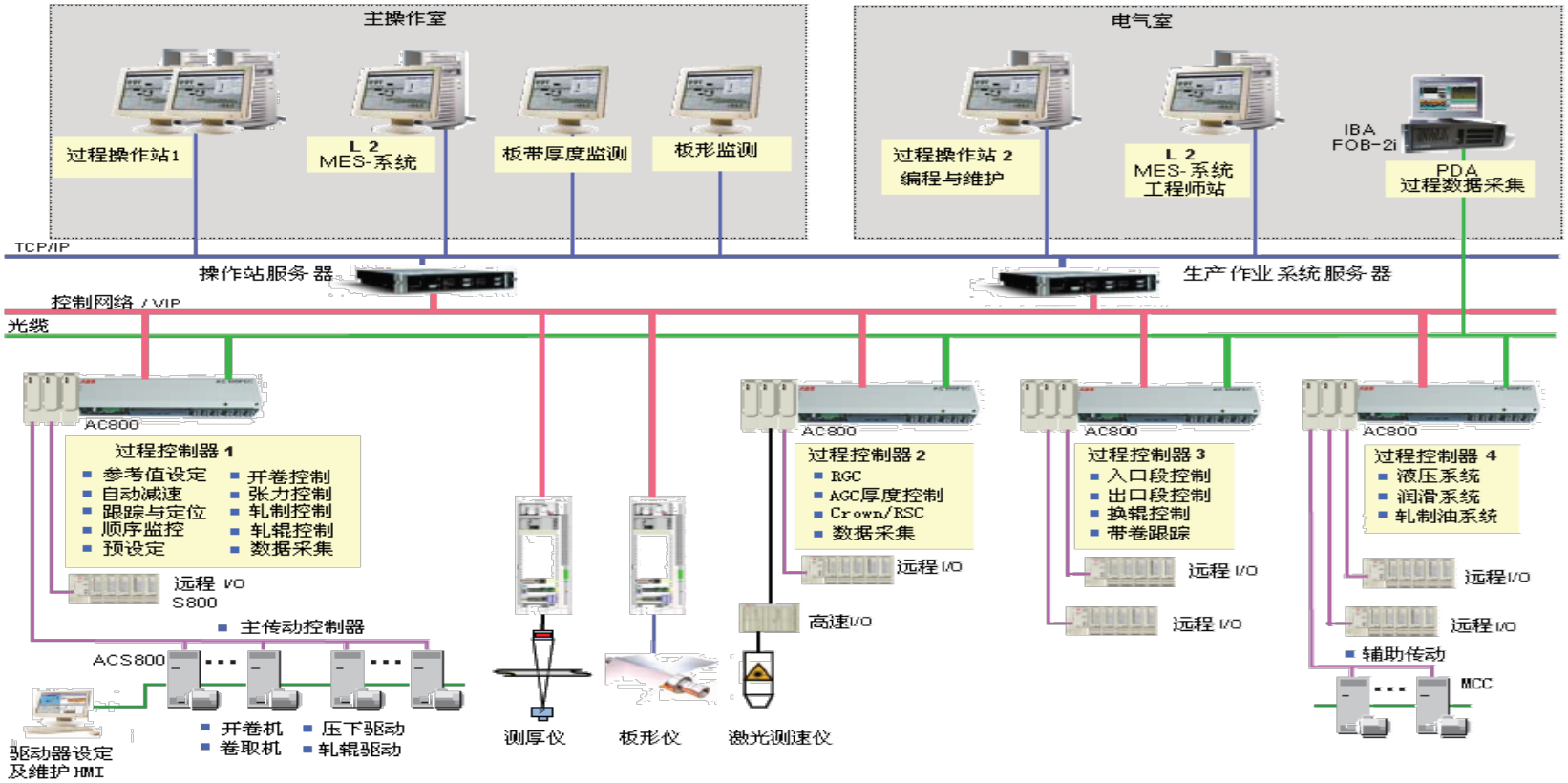
机电系统 + 计算机系统 + 网络拓扑 → 生产过程控制

集成的三电一体化系统：

电气设备、电子仪表、电子计算机 + 联网。



# 钛金板带轧机二级自动化系统配置图



# 系 统 配 置

1、电气驱动系统

设备运行控制、电机调速控制、机械运动控制、流体介质控制。包括：

可回馈交/直整流逆变器+公共直流母线+可回馈逆变器（TDC控制）、ACS800系列驱动控制器 、电机控制中心MCC等。

2、仪表检测系统

过程参数传感器、信号变换、采集、处理、传输。包括：

板形仪、X射线测厚仪、激光测速仪、张力计、辊缝位置传感器、轧辊压力传感器、线性绝对值编码器，旋转多圈绝对值编码器，接近开关，温度传感器，压力传感器等。

3、计算机控制系统

控制模型、实时过程数据采集、状况分析、决策指令、系统管理、生产管理。包括：

硬件配置：L1基础控制器 AC800 PEC，L2服务器/工作站/工程师站、PDA远程数据采集机(IBA FOB-2i采集卡)；

软件配置：Windons XP, Windows Server2003、Control IT基础开发软件、上位组态软件自动化扩展系统800XA、IBA-PDA软件包、数据库管理软件等 。

4、网络通信系统

总线拓扑、系统集成、通信协议、信息交换。包括：

工业以太网+DP网、以太网交换器等。

# 系统功能

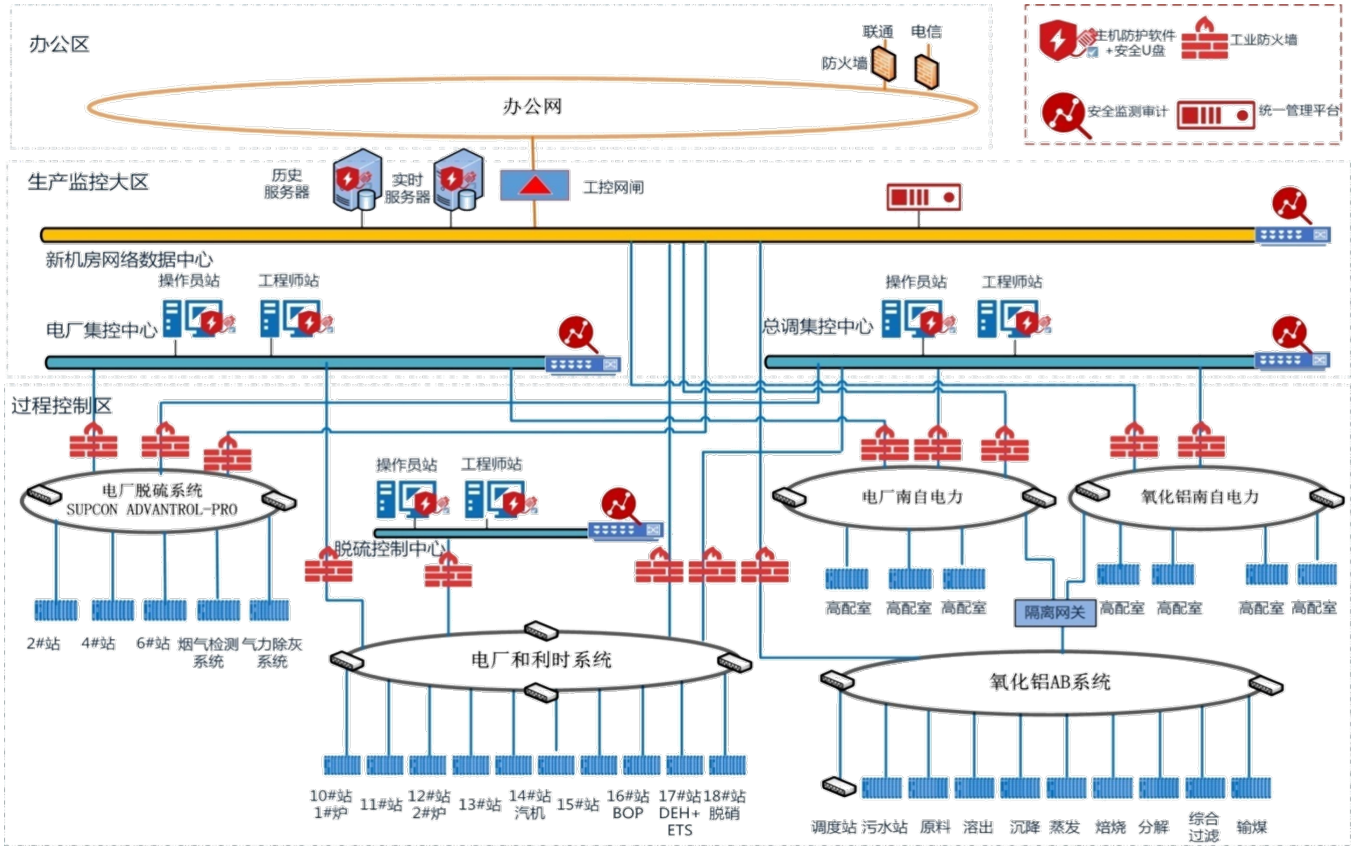
## 系统控制功能

- 辊缝和轧制力控制；
- 自动厚度控制；
- 凸度调整；
- 中间辊窜辊；
- 平直度控制；
- 轧机顺序控制；
- 辅助系统顺序控制；
- 诊断系统具有在线诊断、故障报警、报警分析、事故记录。

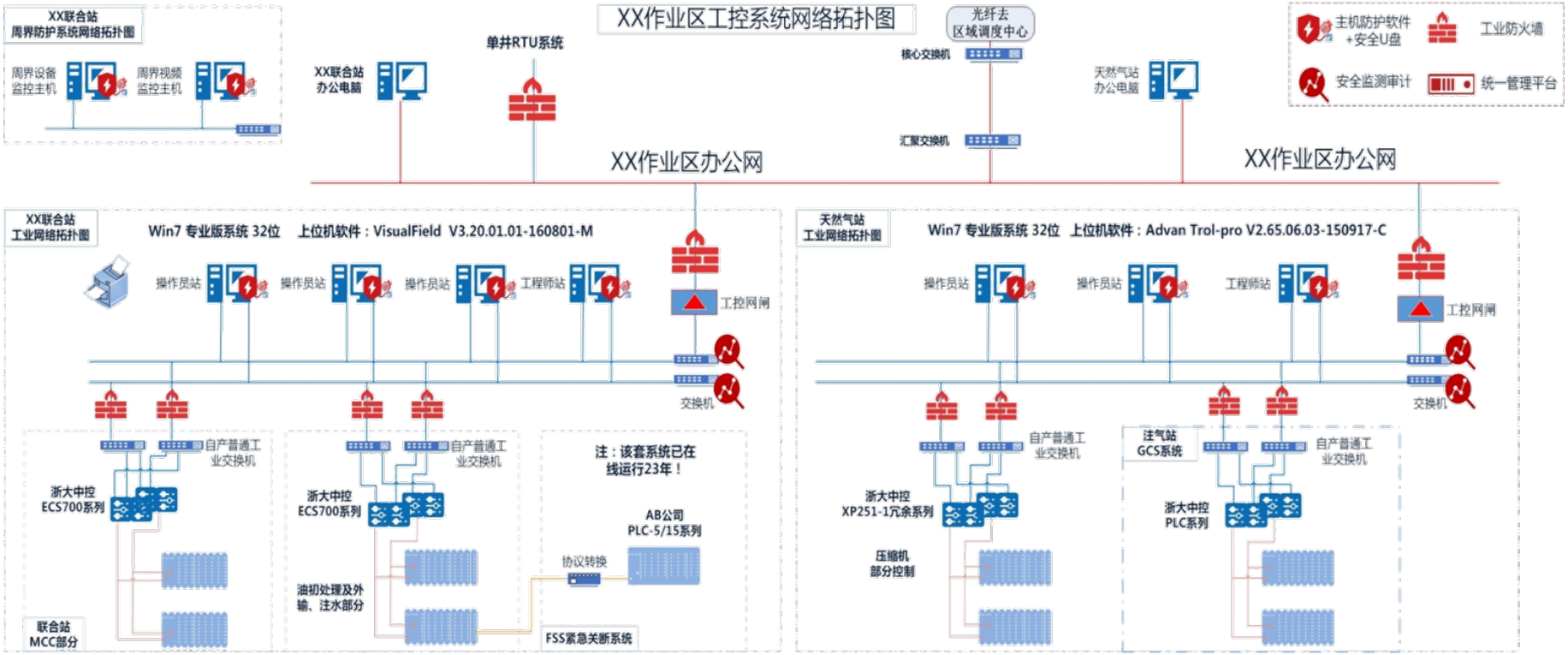
## 系统控制功能

- 输入数据和预设值；
- 轧制表模型；
- 张力模型；
- 速度模型；
- 机座辊缝模型；
- 屈服应力模型；
- 摩擦模型；
- 平直度模型；
- 位置模型；
- 反馈参数模型；
- 自适应模型

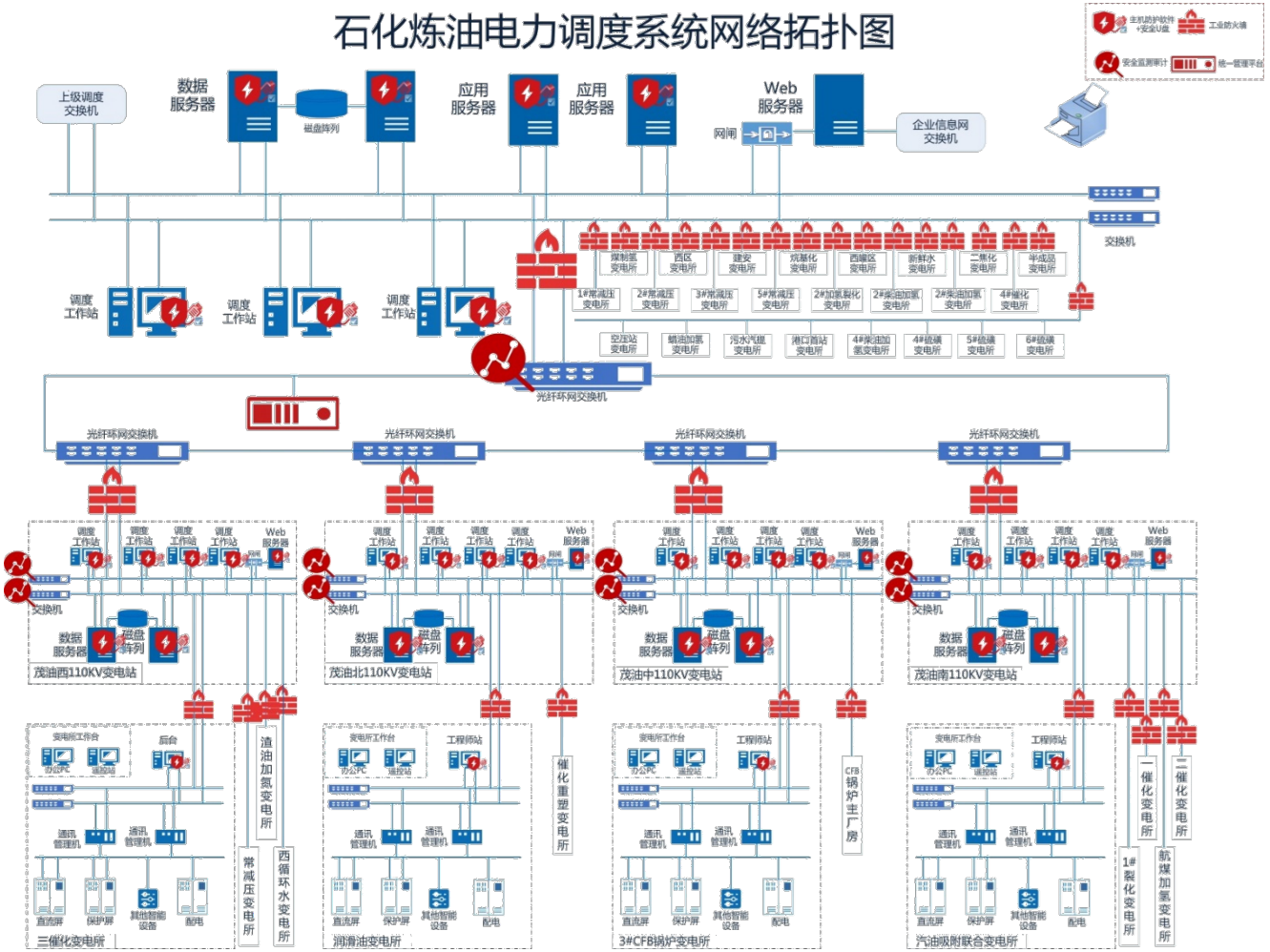
# 冶炼控制系统网络架构


办公区
联通
电信
防火墙
办公网
主机防护软件
+安全U盘
工业防火墙
安全监测审计
统一管理平台
生产监控大区
历史
服务器
实时
服务器
工控网闸
新机房网络数据中心
操作员站
工程师站
电厂集控中心
总调集控中心
过程控制区
电厂脱硫系统
SUPCON ADVANTROL-PRO
脱硫控制中心
电厂南自电力
氧化铝南自电力
高配室
隔离网关
2#站
4#站
6#站
烟气检测
系统
气力除灰
系统
电厂和利时系统
氧化铝AB系统
10#站
1#炉
11#站
12#站
2#炉
13#站
14#站
汽机
15#站
16#站
BOP
17#站
DEH+
ETS
18#站
脱硝
调度站
污水站
原料
溶出
沉降
蒸发
焙烧
分解
综合
过滤
输煤

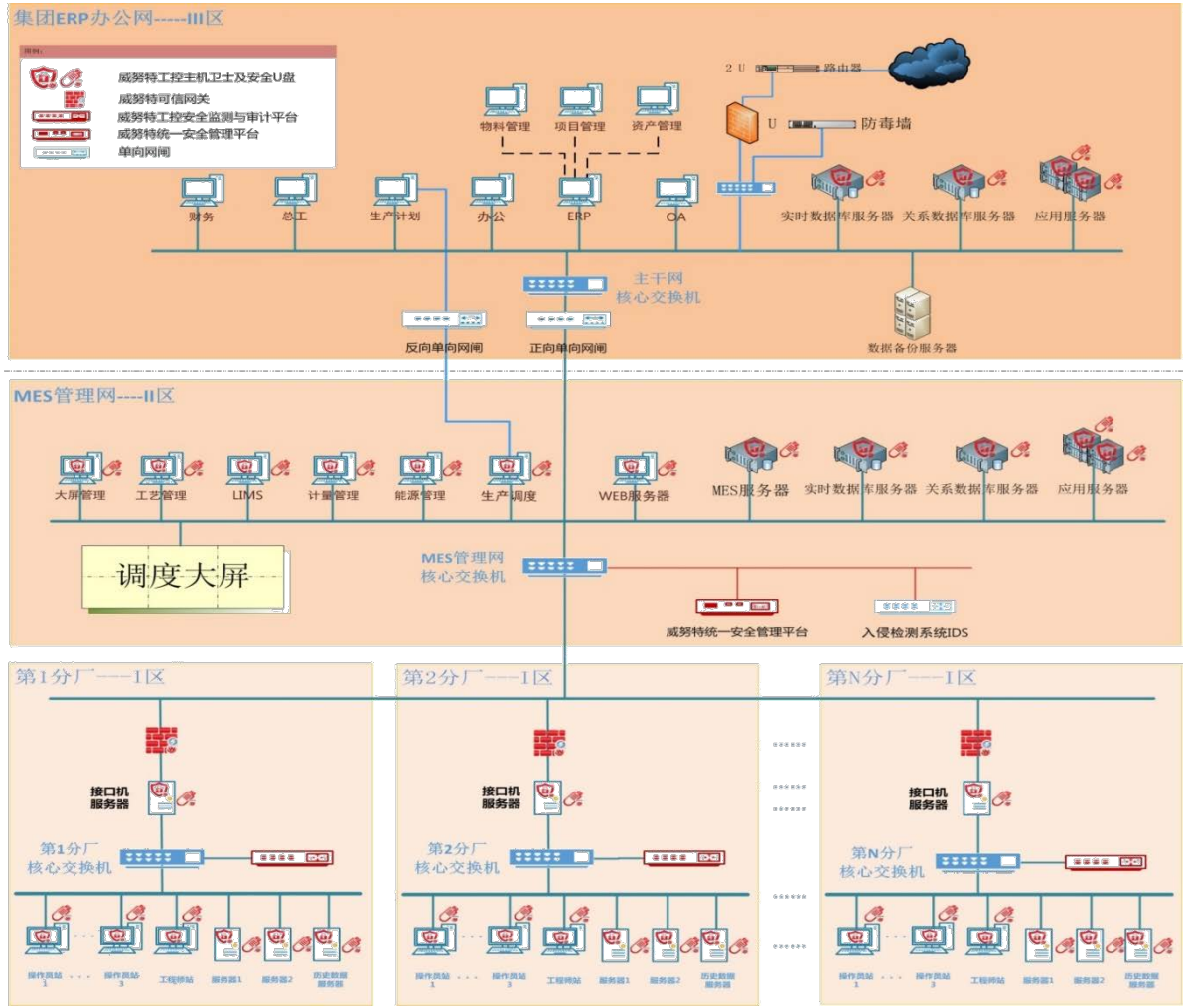
# 石油控制系统网络架构


XX联合站
周界防护系统网络拓扑图
周界设备
监控主机
周界视频
监控主机
XX作业区工控系统网络拓扑图
光纤去
区域调度中心
单井RTU系统
核心交换机
汇聚交换机
XX联合站
办公电脑
天然气站
办公电脑
主机防护软件
+安全U盘
工业防火墙
安全监测审计
统一管理平台
XX作业区办公网
XX作业区办公网
XX联合站
工业网络拓扑图
Win7 专业版系统 32位 上位机软件：VisualField V3.20.01.01-160801-M
操作员站
操作员站
操作员站
工程师站
工控网闸
交换机
自产普通工
业交换机
浙大中控
ECS700系列
浙大中控
ECS700系列
自产普通工
业交换机
注：该套系统已在
线运行23年！
AB公司
PLC-5/15系列
协议转换
油初处理及外
输、注水部分
FSS紧急关断系统
联合站
MCC部分
天然气站
工业网络拓扑图
Win7 专业版系统 32位 上位机软件：Advan Trol-pro V2.65.06.03-150917-C
操作员站
操作员站
工程师站
工控网闸
交换机
自产普通工
业交换机
浙大中控
XP251-1冗余系列
压缩机
部分控制
注气站
GCS系统
自产普通工
业交换机
浙大中控
PLC系列

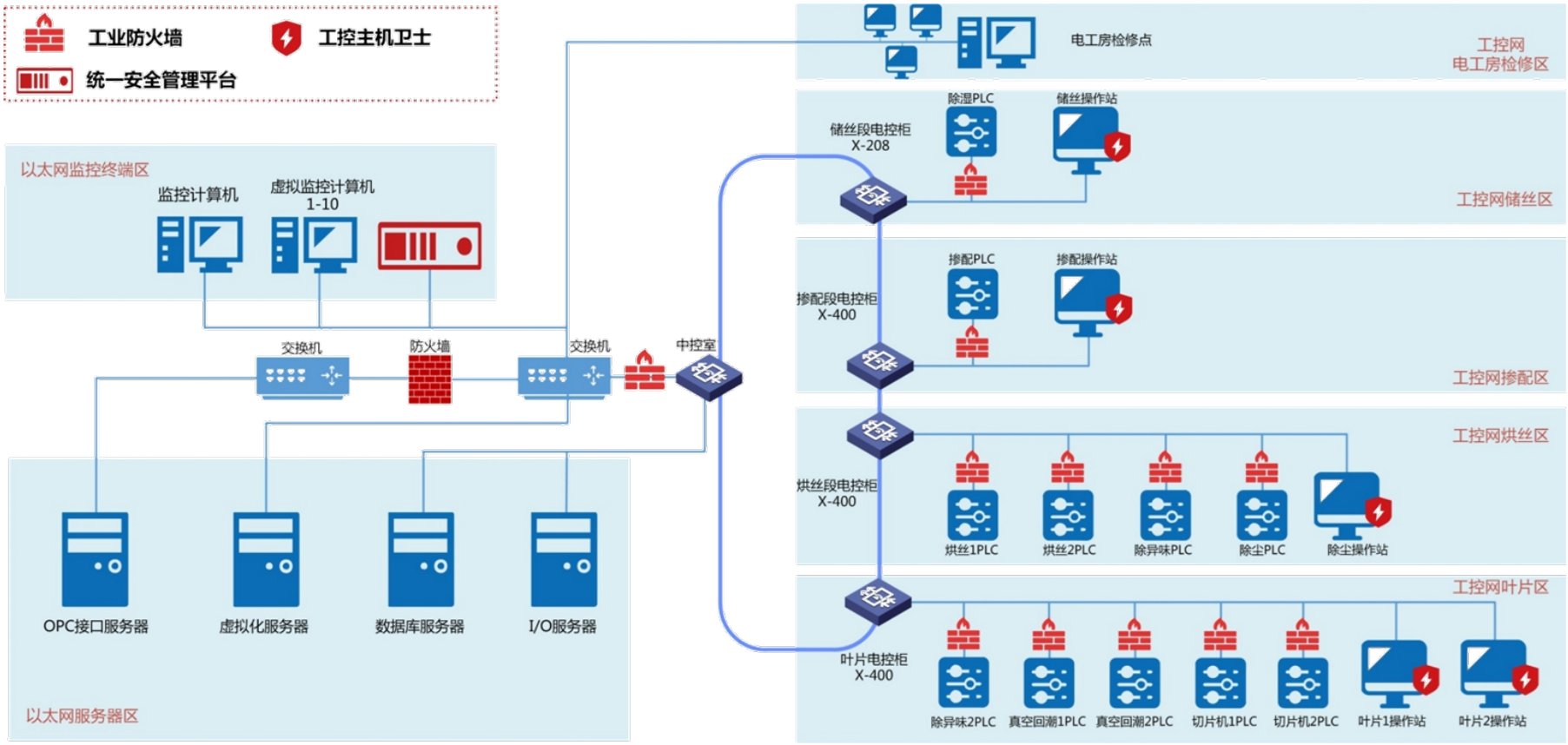
# 炼化电力控制系统网络架构



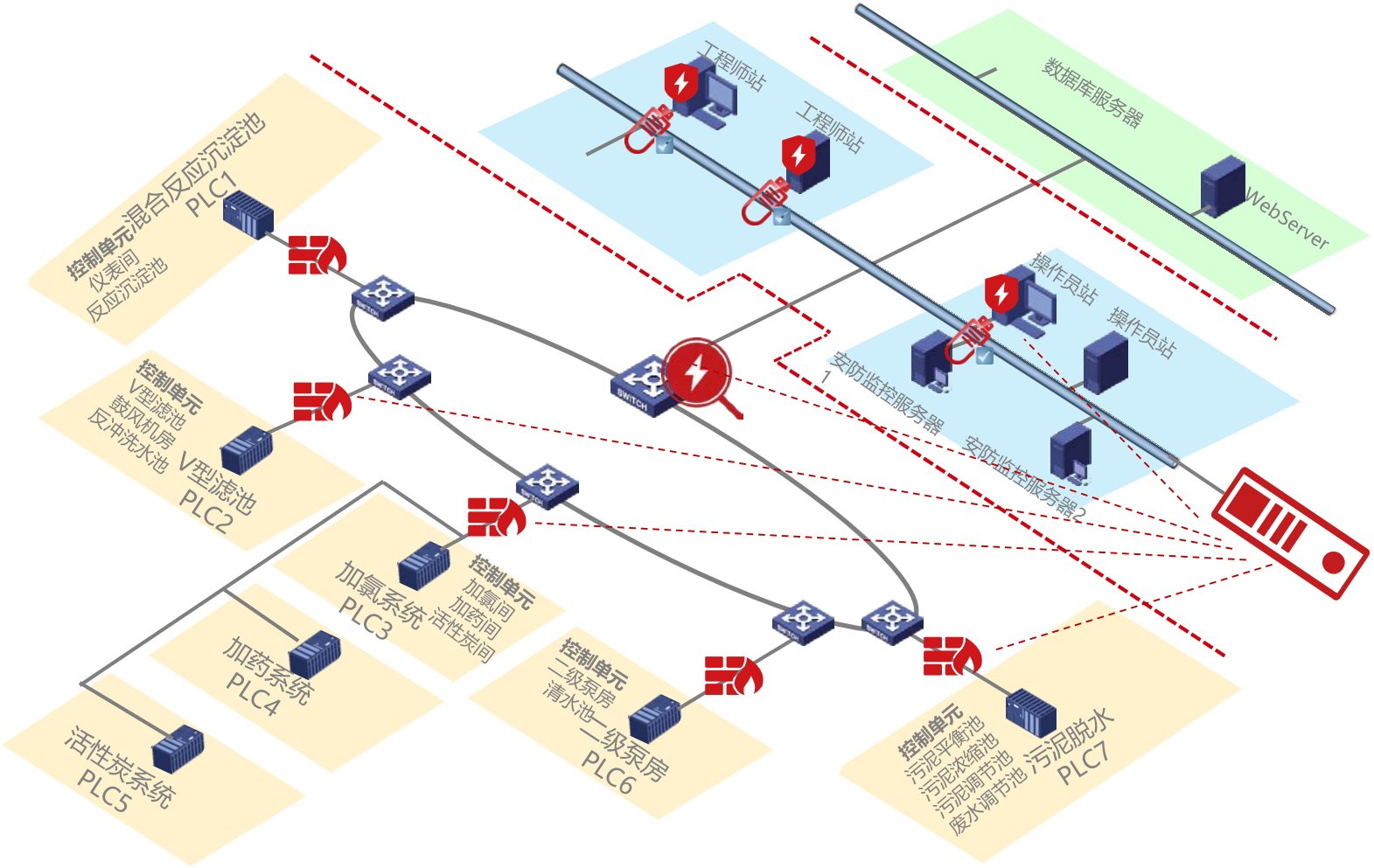
# 制造业控制系统网络架构



# 烟草控制系统网络架构


工业防火墙
工控主机卫士
统一安全管理平台
以太网监控终端区
监控计算机
虚拟监控计算机
1-10
交换机
防火墙
交换机
中控室
OPC接口服务器
虚拟化服务器
数据库服务器
I/O服务器
以太网服务器区
电工房检修点
工控网
电工房检修区
除湿PLC
储丝操作站
储丝段电控柜
X-208
工控网储丝区
掺配PLC
掺配操作站
掺配段电控柜
X-400
工控网掺配区
工控网烘丝区
烘丝段电控柜
X-400
烘丝1PLC
烘丝2PLC
除异味PLC
除尘PLC
除尘操作站
工控网叶片区
叶片电控柜
X-400
除异味2PLC
真空回潮1PLC
真空回潮2PLC
切片机1PLC
切片机2PLC
叶片1操作站
叶片2操作站

# 水处理控制系统网络架构



# 工控安全与传统安全的区别

北京威努特技术有限公司

# 工控安全定义

国际标准《工业过程测量、控制和自动化网络与系统信息安全》（IEC62443）中，针对工控安全的定义包括以下几个方面：

- 保护系统所采取的措施
- 由建立和维护保护系统的措施所得到的系统状态
- 能够免于对系统资源的非授权访问和非授权或意外的变更、破坏或者损失
- 基于计算机系统的能力，能够保证非授权人员和系统既无法修改软件及其数据也无法访问系统功能，却保证授权人员和系统不被阻止
- 防止对工控系统的非法或有害入侵，或者干扰其正确和计划的操作

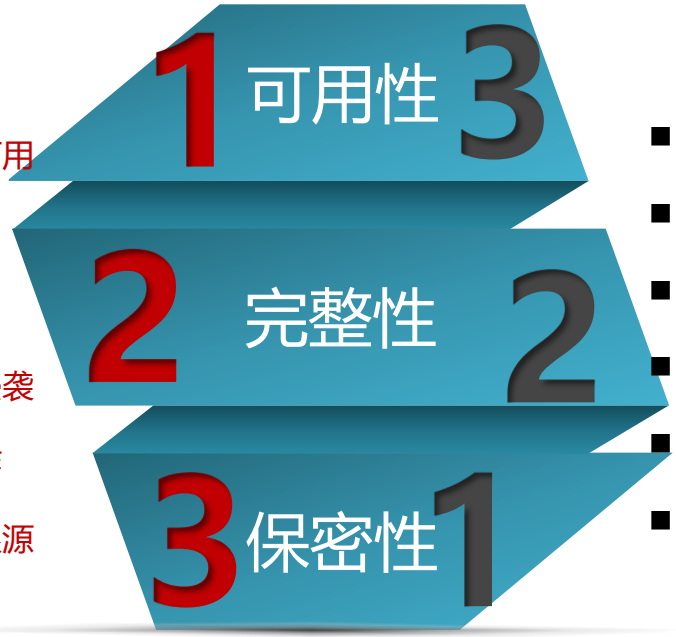
# 工控安全特殊性

- 网络通讯协议不同：大量的工控系统采用私有协议
- 系统稳定性要求高：网络安全造成误报等同于攻击
- 系统运行环境不同：工控系统运行环境相对落后
- 网络结构和行为相对稳定：不能频繁变动调整
- 安全防护要求高：无法通过补丁来解决安全问题

# 防护目标区别

## 工控安全

- 在不利条件下维护生产系统功能正常可用
- 确保信息实时下发传递
- 防范外部、内部的网络攻击
- 保护工控系统免受病毒等恶意代码的侵袭
- 避免工控系统遭受有意无意的违规操作
- 安全事件发生后能迅速定位找出问题根源




- 在不利条件下保证不出现信息泄露
- 保护信息资产的完整性
- 基本不考虑信息传递实时性
- 防范外部、内部的网络攻击
- 保护信息系统免受病毒等恶意代码的侵袭
- 安全事件发生后能迅速定位找出问题根源

## 传统安全

# 防护手段区别


VS

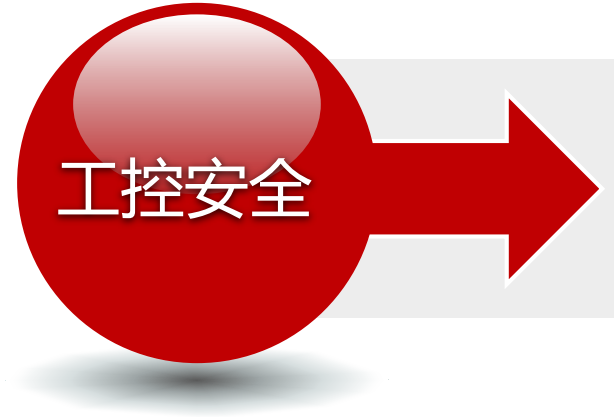

## 主动防护

白名单机制
旁路机制保证网络畅通
抵御已知未知病毒
学习建立防护策略
五元组+协议解析

## 被动防御

黑名单机制
冗余热备保证网络畅通
识别清除已知病毒
预先设置防护策略
五元组

# 网络架构区别




- 网络复杂，多种网络混合，包含有线、无线、卫星通信、无线电通信、移动通讯等
- 通信协议复杂，包含很多专用通讯协议及私有协议
- 设备复杂，网络设备、主机设备、防护设备、控制设备、现场设备种类繁多


- 网络相对简单，多为有线、无线
- 标准TCP/IP通信协议
- 设备类型相对简单，网络设备、主机设备、防护设备为主

# 数据传输区别

实时性要求高，不允许延迟
基本无加密认证机制
指令、组态、采集数据为主
流向明确基本无交叉


VS

实时性要求不高，允许延迟
加密认证防护
文件、邮件、即时消息为主
数据交叉传输

# 运行环境区别

## 工控安全

- 网络相对隔离，不联互联网
- 操作系统老旧，很少更新补丁
- 基本不安装杀毒软件
- 专用软件为主，类型数量不多
- 信息交互通过多通过U盘实现
- 安全漏洞较多，易受攻击

## 传统安全

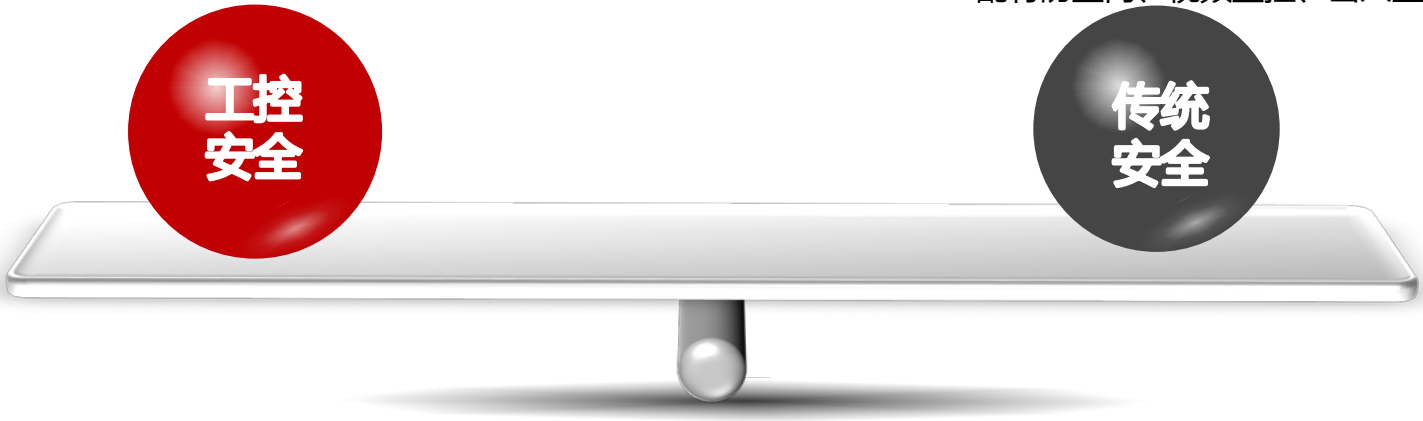
- 网络与互联网相通
- 操作系统新，频繁更新补丁
- 杀毒软件是标配
- 办公软件为主，类型数量繁多
- 信息交互多通过网络实现
- 安全漏洞较少，防护措施完善

# 物理环境区别

- 一般无机房，直接部署在生产环境
- 无专用散热装备
- 环境条件恶劣，高温、高湿、粉尘大、振动、酸碱腐蚀等
- 基本无监控、登记管理措施

VS

- 配有专用机房，统一放置设备
- 配有空调
- 环境条件优良，温湿度基本恒定，灰尘小，无振动，无腐蚀性
- 配有防盗门、视频监控、出入登记等



# 防护硬件区别

## 工控安全

- 工业级设计，全密封
- RISC架构，功耗低
- 自身散热，宽温工作
- 时延100us以下
- 标配Bypass机制
- 深度识别工业协议
- 使用寿命15—20年

## 传统安全

- 基本无三防设计
- X86架构，功耗高
- 风扇散热，温度范围有限
- 时延毫秒级以上
- Bypass机制非标配
- 基本不支持工业协议
- 使用寿命5—8年

# 防护软件区别

## 工控安全

- 白名单机制
- 不需要升级库和补丁
- 操作系统加固
- 抵御已知未知病毒
- 具备自我保护能力
- 运行占用资源少
- 支持老旧系统

VS

## 传统安全

- 黑名单机制
- 需频繁升级库和补丁
- 不加固操作系统
- 防范已知病毒
- 缺少自我保护
- 支持新版系统
- 运行比较耗资源

# 管理维护区别

## 工控安全

- 管理制度不完善甚至缺失
- 缺乏专业技术人员
- 设备维护依赖提供商
- 政策标准文件不完善

VS

## 传统安全

- 管理制度比较完善
- 配备专业维护技术人员
- 能够实现自我维护
- 标准政策文件完整

# 工控安全VS传统安全

| 分类 | 传统安全 | 工控安全 |
| --- | --- | --- |
| 性能需求 | 非实时<br>响应必须是一致的<br>要求高吞吐量<br>高延迟和抖动是可以接受的 | 实时<br>响应是时间紧迫的<br>适度的吞吐量是可以接受的<br>高延迟和/或抖动是不能接受的 |
| 可用性需求 | 重新启动之类的响应是可以接受的<br>可用性的缺陷往往可以容忍的，当然要取决于系统的操作要求 | 重新启动之类的响应可能是不能接受的<br>中断必须有 计划和前预定时间<br>高可用性需要详尽的部署前测试 |
| 管理需求 | 数据保密性和完整性是最重要的容错是不太重要的-临时停机不是一个主要的风险<br>主要的风险影响是业务操作的延迟 | 人身安全是最重要的，其次是过程保护<br>容错是必不可少的，即使是瞬间的停机也可能无法接受<br>主要的风险影响是不合规，环境影响 ，生命、设备或生产损失 |
| 体系架构安全焦点 | 首要集点是保护IT资产，以及在这些资产上存储和相互之间传输的信息。<br>中央服务器可能需要更多的保护 | 首要目标是保护边缘客户端（例如，现场设备，如过程控制器）<br>中央服务器的保护也很重要 |
| 未预期的后果 | 安全解决方案围绕典型的IT系统进行设计 | 安全工具必须先测试（例如，在参考ICS上的离线），以确保它们不佳影响ICS的正常运作 |

# 工控安全VS传统安全

| 分类 | 传统安全 | 工控安全 |
| --- | --- | --- |
| 时间紧迫的交互 | 紧急交互不太重要<br>可以根据必要的安全程度实施限制的访问控制 | 对人和其他紧急交互的响应是关键应严格控制对ICS的访问，但不应妨碍或干扰人机交互 |
| 系统操作 | 系统被设计为使用典型的操作系统采用自动部署工具使得升级非常简单 | 与众不同且可能是专有的操作系统，往往没有内置的安全功能；软件变更必须小心进行； |
| 资源限制 | 系统被指定足够的资源来支持附加的第三方应用程序如安全解决方案 | 系统被设计为支持预期的工业过程，可能没有足够的内存和计算资源以支持附加的安全功能； |
| 通信 | 标准通信协议<br>主要是无线网络，附带无线功能的<br>典型IT网络实践 | 许多专有的和标准的通讯协议<br>使用多种类型的传播媒介，包括专有用的有线和无线（无线电和卫星）；网络复杂 ； |
| 变更管理（升级） | 软件变更是及时应用的，往往是自动化的程序； | 必须进行彻底的测试，以递增方式部署到整个系统；中断必须有计划； |
| 管理支持 | 允许多元化的支持模式 | 服务支持通常是依赖单一供应商 |
| 组件生命周期 | 3-5年的生存期 | 15-20年的生存期 |
| 组件访问 | 组件通常在本地，可方便地访问 | 组件可以是隔离的，远程的，需要大量的物力才能获得对其的访问 |

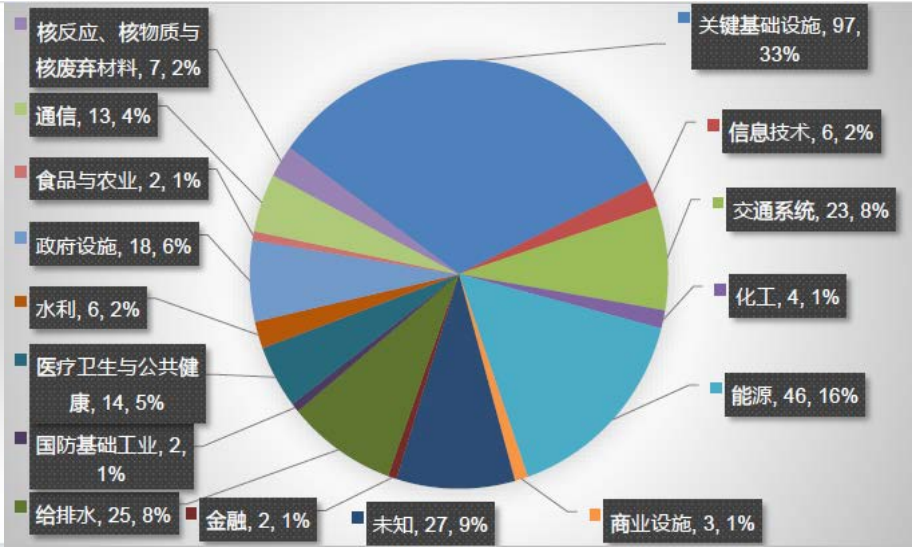
# 工控安全风险分析及对策

北京威努特技术有限公司

# 目录

# 工控信息安全发展趋势

- 公开的ICS漏洞数的年度变化趋势，逐年递增
- 美国ICS-CERT报告，工控安全事件高发，2014年245起，2015年295起，2016年278起


**与2015年报告相比，上升了24%**

# 工控信息安全发展趋势

- 公开的ICS漏洞数的年度变化趋势，逐年递增
- 美国ICS-CERT报告，工控安全事件高发，2014年245起，2015年295起，2016年278起

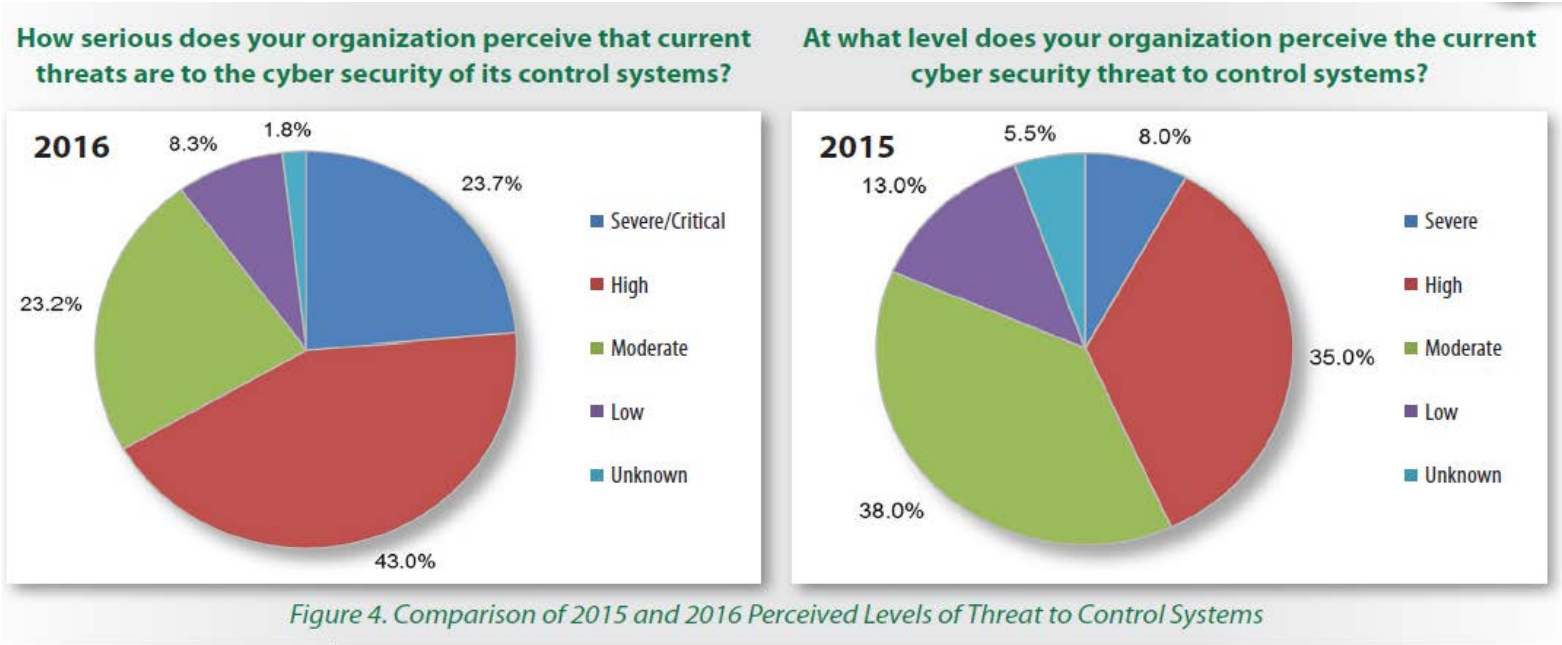
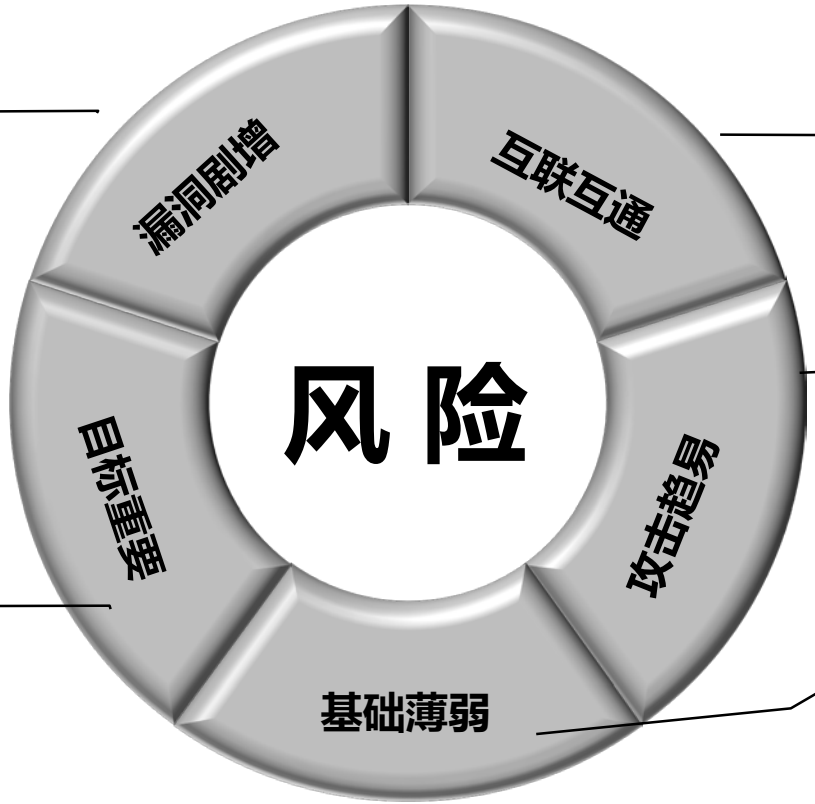



*Figure 4. Comparison of 2015 and 2016 Perceived Levels of Threat to Control Systems*

# 工控信息安全现状分析

工控软硬件产品在设计之初就很少考虑安全问题，导致安全漏洞不断涌现。迄今已发现1000多个工业控制软硬件设备漏洞，涉及123家工控厂商，33%没有被修复，90%的漏洞披露于“震网”事件后，465个漏洞为易利用的HMI漏洞。




工业控制系统正从封闭走向开放和互联，工控系统的网络安全边界明显扩大。

由于黑客大会、开源社区、白帽社区的出现，导致获取工控系统的攻击方法越来越容易。

我国工控安全防护处于起步阶段，存在不少问题，难以有效应对国家级的、有组织的、高强度的网络攻击。

工控系统作为国家关键基础设施的重要组成部分，已经成为网络部队、黑客、极端势力攻击的重要目标。

# 工业协议风险

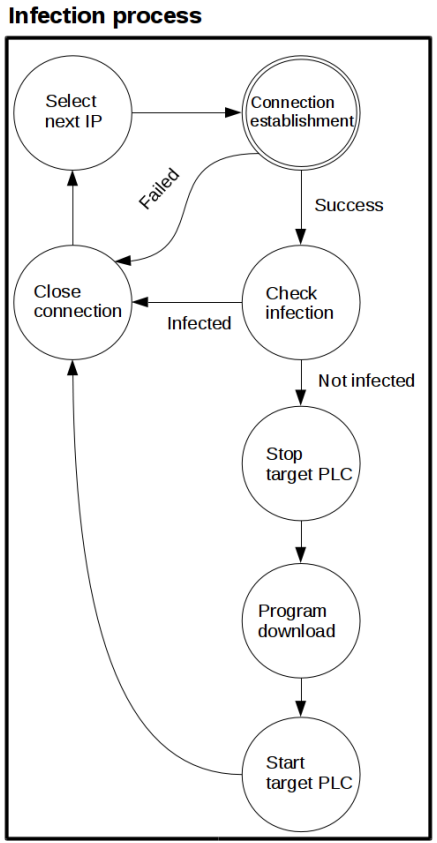
常用的工业协议有Modbus、S7、OPC、IEC104、DNP3、Profibus等，这些协议在设计初期主要是为了保证生产的连续性与稳定性，所以协议设计上在安全性与可用性之间进行取舍，进而牺牲了安全性。

**西门子S7协议**

| 严重等级 | 威胁行为描述 | 潜在危害 |
| --- | --- | --- |
| 高 | 主站下发STOP/RUN命令 | 导致设备进入停机状态/导致设备被启机初始化 |
| 高 | 主站下发download block命令 | PLC的内部程序可能正在被替换程 |
| 高 | 主站下发delet block命令 | PLC的内部程序块可能正在被删除 |
| 中 | 主站下发错误的密码请求 | 正在未授权访问 |
| 低 | 主站下发read szl请求 | 正在尝试获取设备模块信息、固件信息 |

| 漏洞标题 | 危害级别 | 点击数 |
| --- | --- | --- |
| Siemens SIMATIC S7-300/1200/15... | 高 | 1071 |
| Siemens SIMATIC S7-300 CPU拒绝... | 高 | 1004 |
| SIMATIC S7-300和S7-400 CPU信息... | 中 | 747 |
| SIMATIC S7-300和S7-400 CPU拒绝... | 中 | 705 |
| HMI/SCADA软件webaccess7.2/8.0/... | 低 | 737 |
| SIMATIC S7-300/S7-400 CPU fami... | 中 | 577 |
| IBHsoftec S7-SoftPLC CPX43堆缓... | 高 | 523 |
| Siemens S7300/400 PLC存在权限绕... | 高 | 607 |
| Siemens SIMATIC S7-300 CPU拒绝... | 高 | 1903 |
| Siemens SIMATIC S7-1200 CPU权限... | 中 | 2436 |
| Siemens SIMATIC S7-1500绕过机制... | 低 | 1987 |
| Siemens SIMATIC S7-1500拒绝服务... | 高 | 2072 |
| Siemens SIMATIC S7-1200 CPU设备... | 中 | 1857 |
| Siemens SIMATIC S7-1200打开重定... | 中 | 1674 |
| Siemens SIMATIC S7-1500拒绝服务... | 高 | 1060 |

# PLC蠕虫病毒—危机即将来临



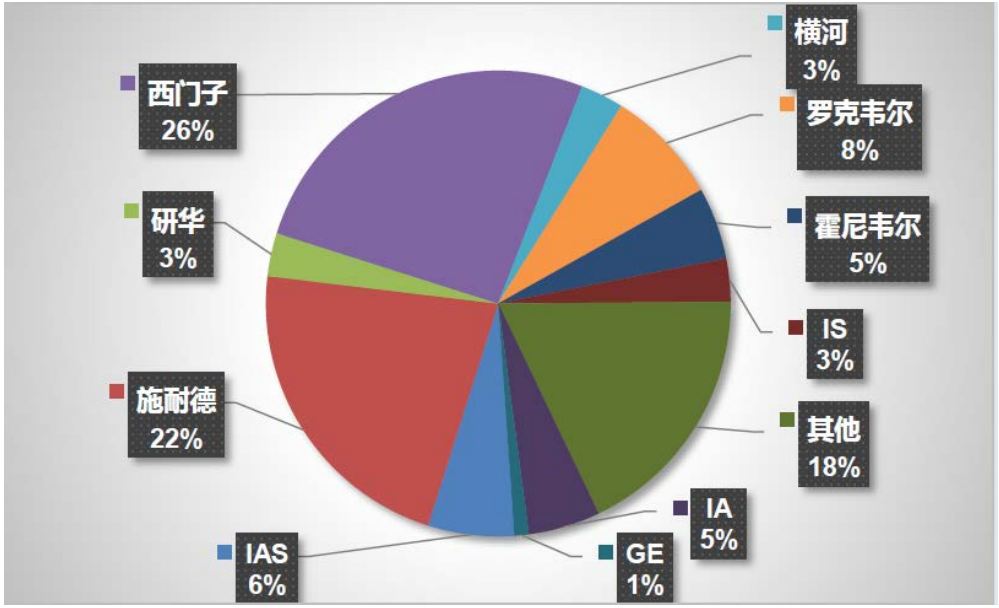

2015年，国外某实验室技术人员利用PLC的通信机制设计了一种蠕虫病毒，病毒通过利用西门子S7的权限缺失漏洞来远程操作PLC，进而在PLC之间传播和复制。

这种蠕虫病毒不需要借助PC机，仅仅基于PLC设备就能实现扩散，攻击目标并将自身进行复制。病毒代码在目标机复制后不会发生变化，从而可以重复进行目标扫描，进一步扩散。

该病毒的实现思路，适用于多个厂家的PLC设备，并且可以在一定规则范围内相互进行传播。

# 控制设备风险

工业产线通常采用的工业控制设备基本上都是来自国外厂商，如艾默生、霍尼韦尔、AB、西门子、施耐德等，这些控制设备设计的时候更多是为了实现功能，安全性考虑不足，存在很多高危安全漏洞，有的甚至存在后门，一旦被攻击利用会导致严重后果。




| 漏洞标题 | 危害级别 | 点击数 | 评论 | 关注 | 时间 |
|---|---|---|---|---|---|
| Honeywell Experion PKS拒绝服务... | 中 | 391 | | | |
| 多个Emerson产品安全绕过漏洞 | 中 | 508 | 0 | 0 | 2016-12-06 |
| 多款Schneider Electric产品资源... | 中 | 373 | | | |
| 多款Schneider Electric产品拒绝... | 高 | 278 | | | |
| Schneider Electric TSXP572634M... | 高 | 482 | | | |
| Schneider Electric Unity PRO远... | 高 | 411 | | | |
| Schneider Electric Modicon M34... | 高 | 1852 | | | |
| Schneider Electric InduSoft We... | 高 | 1082 | | | |
| Schneider Electric InduSoft We... | 高 | 1089 | | | |

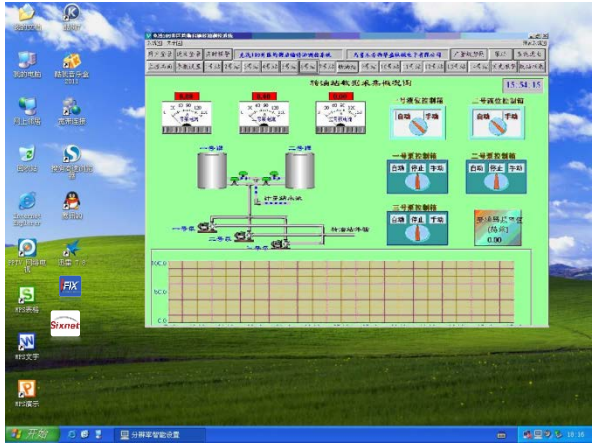
# WannaCry—老旧系统之殇

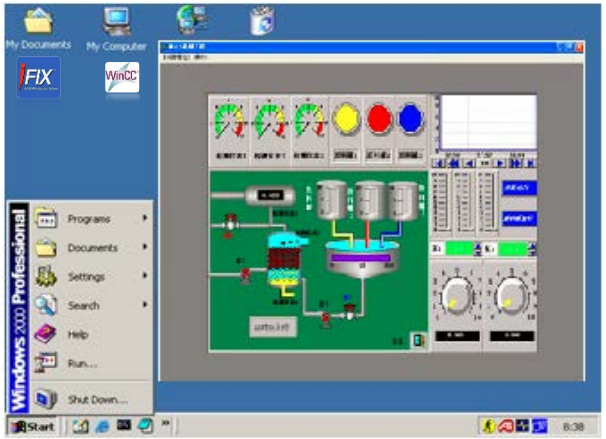

病毒利用微软今年3月份修补的MS17-010 SMB协议远程代码执行漏洞，通过扫描445端口进行传播，对主机文件进行加密。

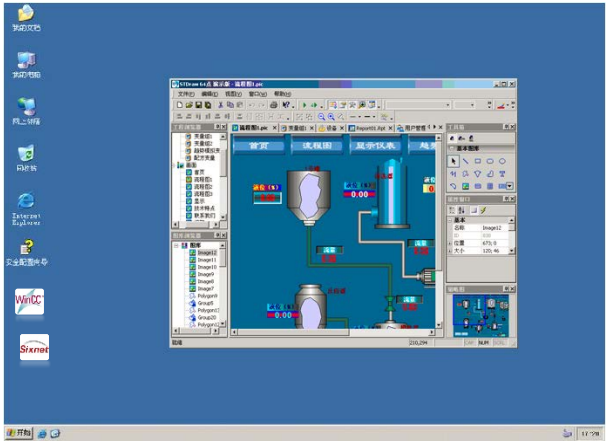
Win7及以上操作系统只要及时安装补丁，就不会受到影响，而WindowsXP/2000/2003等老旧操作系统没有补丁可打，几乎全部沦陷。

# 操作系统风险

操作员站、工程师站、工业服务器大量使用微软Windows系列操作系统，存在大量安全漏洞且很少打补丁，尤其是目前常用的老旧Windows系统，如Windows XP、Win2000、Win2003等，微软已经停止技术支持，面临无补丁可打的困境，容易遭受APT攻击。





# 控制系统频被攻破

01

- 2000年：一个工程师在应聘澳大利亚的一家污水处理厂被多次拒绝后，远程侵入该厂的污水处理控制系统，恶意造成污水处理泵站的故障。

02

- 2007年：攻击者入侵加拿大一水利SCADA控制系统，破坏了取水调度的控制计算机。

03

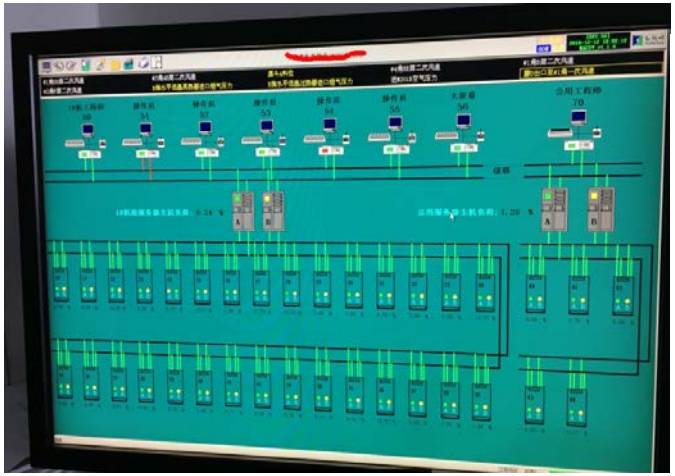
- 2011 年， 黑客通过入侵数据采集与监控系统SCADA，使得美国伊利诺伊州城市供水系统的供水泵遭到破坏。

04

- 2014年河南省某污水处理厂SCADA系统遭到网络黑客的攻击，加氯间的计量泵全部运行，导致消毒池出水余氯值居高不下。

# 应用软件风险

工业网络中使用的各种组态软件存在着大量的安全漏洞，如Sixnet 、iFIX、SIMATIC、HollySys等，这些组态软件都已经曝出大量高危、中危等安全漏洞，严重影响安全生产。任何黑客或别有用心人员都可以通过这些漏洞发起对工业控制系统有针对性的攻击行为。



Sixnet Universal Protocol Undocumented函数代码远程安全绕过漏洞

报送者:北京天融信网络安全技术有限公司

| | |
|---|---|
| CNVD-ID | CNVD-2013-12528 |
| 发布时间 | 2013-08-23 |
| 危害级别 | 高 (AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| 影响产品 | Sixnet RTU firmware < 4.8<br>Sixnet Sixnet UDR < 2.0 |
| BUGTRAQ ID | 61837 |
| CVE ID | CVE-2013-2802 |
| 漏洞描述 | 美国SIXNET公司是一家历史悠久的工业自动化和工厂商，自1976年起向世界各地用户提供高品质的控通讯产品。<br><br>Sixnet Universal Protocol存在远程安全绕过漏洞。漏洞绕过安全限制，获取文件描述和文件大小，读建新文件和执行任意代码。 |
| 漏洞类型 | 通用软硬件漏洞 |

GE Proficy HMI/SCADA-iFIX 'TCPTASK.exe'远程缓冲区溢出漏洞

报送者:北京神州绿盟科技有限公司 ★关注(0)

| | |
|---|---|
| CNVD-ID | CNVD-2013-14823 |
| 发布时间 | 2013-12-03 |
| 危害级别 | 高 (AV:N/AC:L/Au:N/C:P/I:P/A:P) |
| 影响产品 | General Electric Company Proficy HMI/SCADA – iFIX 5.1<br>General Electric Company Proficy HMI/SCADA – iFIX 5.0<br>General Electric Company Proficy HMI/SCADA – iFIX 4.5 |
| BUGTRAQ ID | 63948 |
| 漏洞描述 | GE 智能平台的Proficy HMI/SCADA–iFIX 是世界领先的工业自动化软件解决方案，提供了生产操作的过程可视化、数据采集和数据监控。<br><br>GE Proficy HMI/SCADA-iFIX 4.5, 5.0, 5.1在TCP/IP任务进程(TCPTASK.exe)的实现上存在远程缓冲区溢出漏洞。成功利用后可使攻击者在受影响应用上下文中执行任意代码。 |
| 漏洞类型 | 通用软硬件漏洞 |

# 病毒入侵—挥之不去的阴影

**Zotob病毒**
2005年：Zotob蠕虫事件对全球制造行业造成巨大经济损失超过$1,400,000。

**震网病毒**
2010年：震网病毒席卷全球，伊朗核设施遭受攻击，全球感染超过六百万台。

**Conficke病毒**
2011年：我国某石化企业某装置控制系统分别感染Conficker病毒，造成控制系统服务器与控制器通讯不同程度地中断。

**火焰病毒**
2012年：火焰病毒在中东大范围传播，侵入个人电脑、窃取私密数据。

**Havex病毒**
2014年：Havex病毒席卷欧美，劫持电力工控设备，阻断电力供应，在中国也发现有病毒样本传播。

**WannaCry病毒**
2017年：WannaCry病毒大范围爆发，影响遍布各行各业，至今尚未消除。

# 病毒传播风险

经过大量的实际项目建设，发现大部分工业控制网络中工控主机、服务器均存在大量的病毒，这些病毒有的已经影响到企业的正常生产工作。通过对这些病毒的入侵途径进行分析，发现这些病毒的传入途径多为移动存储介质的滥用造成的。



# 误操作风险

工业产线内上位机操作工程师权限过大，通过上位机直接发布操作指令、组态变更、程序下装等关键行为，误操作或恶意操作必然会导致错误生产，从而造成生产损失。

01

- 2011年5月1日，华能XX电厂恶性电气误操作事件，导致1人死亡、1人重伤。

02

- 2014年10月17日，云南电网XX供电局变电站误操作事故，导致1人触电死亡。

03

- 2016年10月25日，国家核安全局通报16起安全事件，若干核电厂在运行期间发生由于人员误操作等行为导致的运行异常或运行事件，甚至触发反应堆停堆。

# 管理缺失风险

**Process（流程）**：工控安全的各项管理制度、规范、标准，将人和技术结合在一起，以确保技术防护手段能够真正发挥作用。

01

- 龙泉、政平、鹅城换流站计算机系统发现病毒，经调查确认是技术人员在系统调试中用笔记本电脑上网所致。

02

- 上海某电厂工程师站感染病毒，导致监控数据采集异常，经调查确认是技术人员使用U盘拷贝数据造成。

03

- 四川某燃气公司操作员站感染病毒，造成SCADA运行异常，经调查发现操作员站系统安装在管理网进行，导致病毒通过网络入侵。

# 人员意识风险

**People（人）：**是最关键的一个因素。不管是技术的实施和维护，流程的遵从、改善和管理，都离不开经过培训、有专业素质的人的参与。

工业用户**安全意识不足**是很多安全事件产生的根本原因。

01

- 伊朗震网病毒事件：维护工程师遭受社会工程学攻击，U盘被植入病毒，导致1000多台离心机损坏。

02

- 乌克兰电网停电事件：员工打开钓鱼邮件附件，导致病毒侵入电网控制系统，引发大范围停电。

03

- 华东石化内鬼事件：内部人员在SCADA服务器上种病毒，骗取高额维护费，造成国有资产流失。

# 目录

# 认知误区一：网络隔离就安全

## 工控网络的入侵途径：

| | | |
|---|---|---|
| 便携电脑和<br>手机等智能终端 | USB移动存储介质 | 通过远程维护通道入侵 |
| 心怀不满或<br>被利用的员工 | WLAN无线连接 | 通过企业办公网入侵 |

……

# 认知误区二：传统IT安全产品能够解决问题

01

- 工业控制系统“可用性”第一，而IT信息系统以“机密性”第一
  - ✓ 从而要求安全产品的软硬件重新设计。例如：硬件无风扇设计，系统Fail-to-open

02

- 工业控制系统不能接受频繁的升级更新操作
  - ✓ 依赖黑名单库的信息安全产品（例如：反病毒软件，IDS/IPS）不适用。

03

- 工业控制系统对报文时延很敏感，而IT信息系统通常强调高吞吐量
  - ✓ 安全产品，必须从CPU选型、软件架构设计上保证低时延。

04

- 工业控制系统基于工业控制协议（例如，OPC、Modbus、DNP3、S7）
  - ✓ 传统安全产品支持IT通信协议（例如，HTTP、FTP），不支持工业控制协议。

05

- 工业控制系统的工业现场环境恶劣（如，野外零下几十度的低温、潮湿）
  - ✓ 按照工业现场环境要求专门设计硬件，全密闭、无风扇，支持 - 40℃～70℃等。

# 认知误区三：仅靠技术就能解决工控安全问题

- **在工控信息安全中，People, Process和Technology三个要素互相作用，缺一不可：**

**People（人）**：是最关键的一个因素。不管是技术的实施和维护，流程的遵从、改善和管理，都离不开经过培训、有专业素质的人的参与。

**Process（流程）**：工控安全的各项管理制度、规范。将人和技术结合在一起。

**Technology（技术）**：是工控安全的技术支持和保证。是为人和流程服务的。

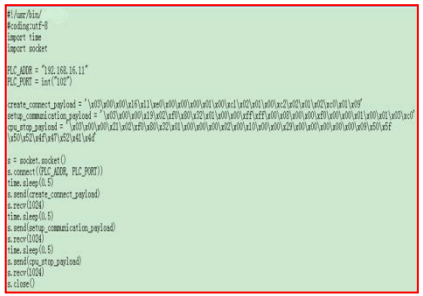
# 认知误区四：控制设备存在漏洞不会影响生产

- 部分PLC被爆大量漏洞存在：但不会影响生产运行！


**控制设备运行参数篡改攻击：**

S7编程软件是官方与西门子S7-300进行通信的软件，通信协议是S7协议，通过抓取S7数据包，绕过权限，发送数据包给西门子S7-300.可通过修改数据包字段达到修改西门子S7-300运行状态值。

方法：首先用S7编程软件建立与西门子S7-300建立通信的程序，用专用抓包软件（例如wireshark抓包，该抓包软件存在一定缺陷！），通过一些攻击方式以及协议格式分析，得出没有认证字段，然后通过下载程序获得其通信流程，通过构造错误的状态值下置数据包，发送数据包给西门子S7-300。



# 认知误区五：黑客不懂工业协议

01

- 工业环境中已广泛使用商业标准件(COTS)和IT技术，操作系统也多以Microsoft和Linux为主。

02

- 特殊环境采用的内部协议其实也有公开的文档可查，公开协议内容也早被黑客圈子熟知。

03

- 大部分的工业协议都不具备安全防护特征，详细资料能够轻易获取，很容易被黑客攻击。

04

- 由于ICS设备功能简单、设计规范，只需少许计算机知识和耐心就可以完成其逆向工程，即使经过加密处理的协议也可以实施逆向工程。

# 认知误区六：供应商会保证产品的安全性

人们能够理解ICS系统核心组件(如数据库、应用软件、服务器等)安全性的重要，但常常会忽视ICS系统外围组件(如传感器、传动器、智能电子设备、可编程逻辑控制器、智能仪表、远程终端设备等)的安全防护。其实这些外围设备很多都内置有与局域网相联的网络接口，采用的也是TCP/IP协议。这些设备运行时可能还有一些调试命令，如telnet和FTP等，未及时屏蔽。这种情况在网络服务器上也很常见。网络服务器一般隐含有一项特殊功能，即允许用户通过定位某个网址重新启动远程终端设备(RTU)。

用户通常以为供应商会对他们产品的缺陷和安全性了如指掌，实际上供应商对他们产品的认识仅限于产品所能提供的功能方面，而且对出现的安全问题也做不到快速响应。2008年研究人员发现ICS特有的数据通讯协议(WonderwareSuitlink)存在漏洞后，立即联系了供应商Wonderware，但是Wonderware1个月后才开始回应；等到Wonderware认识到产品缺陷，并知会Suitlink用户相关补救措施时，已是三个月以后的事了。这件事让很多供应商开始关注自己产品的安全性，但对大部分供应商来说，还是任重道远。

# 认知误区七：单向通信100%安全

某些情况下，极重要的ICS系统允许以单向通讯方式与其他安全区域联接。但是，这种联接方式是很不严密的，其安全程度高低取决于单向通信的实现方式。

方式一为限制发起方方式，即通信只能由某一方发起，然后双方可以互相通信；

方式二为限制负载流方式，即在方式一基础上，对方只能发送控制信号，不能发送数据或应用信息；

方式三最严格，仅允许一方发送信息，不允许另一方发送任何信息。

方式一采用基本防火墙就能实现，方式二需要进行信息包检测，方式三需要采用特殊设备实现。

通常认为，将前两种方式结合起来将是最安全的防护措施。但是，即使它们可以提供很强的安全保护，网络攻击还是有可能发生。因为控制和信号信息允许进入受保护区域，经过设备编译后，恶意代码就有可能得到运行。所以，单向通信并不能提供100%的安全保护。

# 工控信息安全正确认知

## 先前错误认知

- 我们的设备高度专业化，其安全得益于“冷门”，而工业控制系统不容易获取，所以针对它们制造的有效攻击是不可能实现的。
- 我们的工业控制系统可以与其他网络有效隔离，能够消除网络事故风险。
- 防火墙以及入侵检测与防御系统已经足够用来保护控制系统网络不受攻击。
- PLC与RTU不是运行在通用操作系统上，没有漏洞，从而缺乏必要的攻击平面。

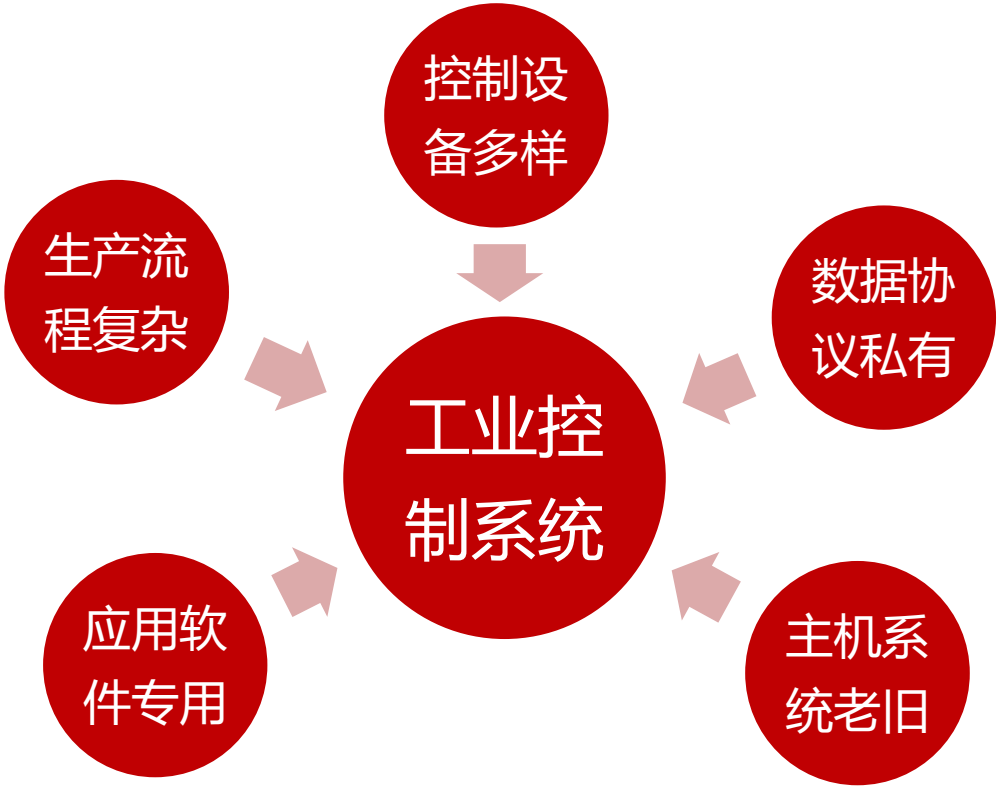
## 校正后的认识

- 高度针对工业控制系统的攻击动机、意图以及资源都是存在的。
- 控制系统依然依附于人的天性：严格的边界防御可能被一个好奇的操作员、USB驱动器以及糟糕的安全意识所绕过
- 使用多重零日漏洞来部署针对性攻击，意味着“黑名单”点防御不再够用，要考虑将“白名单”防御作为全面防御未知攻击的手段。
- PLC可以并且已经成为恶意软件感染的目标。

通过现象看本质，去伪存真！

# 目录

# 工业控制系统特点



# “白环境”安全理念

- 基于工控系统相对固化的特点，安全问题及安全防护措施有别于传统IT系统。威努特创新性的提出了建立工控系统的可信任网络白环境和工控软件白名单理念，为客户构筑工控系统“安全白环境”整体防护体系，保护工业基础设施安全。

  - 只有可信任的**设备**，才能接入控制网络
  - 只有可信任的**消息**，才能在网络上传输
  - 只有可信任的**软件**，才允许被执行

✓ 从“**黑**”到“**白**”

✓ 从 “被动防御”到“主动防护”

# 白名单VS黑名单


主动防护

设置允许规则

数量可控

抵御未知风险

效率更高

适用固化环境

VS


被动防御

设置不允许规则

难以穷举

防范已知威胁

效率较低

适用灵活环境

# “白名单”防护策略解读

## 白名单主动防御技术

通过提前计划好的协议规则来限制网络数据的交换，在工业控制网络内进行动态行为判断。通过对约定协议的特征分析和端口限制的方法，从根源上节制未知恶意行为的发生和传播。

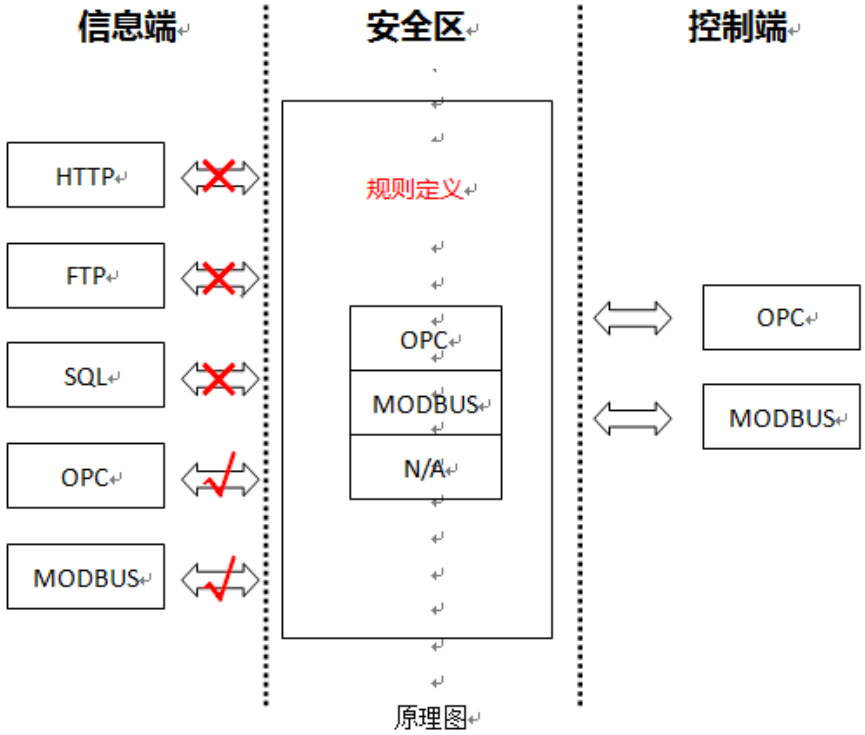
## 白名单安全机制

一种安全管理规范，不仅应用于安全防护技术的设置规则，也是在实际管理中要遵循的原则，例如在对设备和计算机进行实际操作时，需要使用指定的笔记本、U盘；管理人员只信任可识别的身份，未经授权的行为将被拒绝；设备安全检测明确安全风险等。

# 协议白名单

通过安全防护设备（如工业防火墙、安全审计设备等）深度识别网络协议，阻断无关的协议，过滤非法的工业协议数据，仅允许正常的协议数据通过，建立协议白名单：

- 协议只读控制（如OPC只读）
- 协议功能码识别
- 正常操作指令学习
- 异常报警及阻断



# 设备白名单

## 安全检测机制

按照国家安全测评标准，配合主管检测部门，建立工控设备安全检测机制

## 安全检测手段

利用工控安全检测装备（漏洞挖掘、漏洞扫描）检测发现设备存在的已知、未知漏洞及后门，全面掌握设备的健壮性和安全性

## 建立准入白名单

形成设备准入白名单列表，谨慎选用存在漏洞和风险的系统及设备，对已经投入使用的设备进行安全整改，加强设备安全防护

# 指令白名单

通过学习识别现场操作流程及操作指令，建立适合现场实际生产情况的指令白名单，阻断误操作或恶意操作指令，确保生产产线稳定运行。

# 主机白名单

通过技术手段对操作系统进行加固，扫描建立主机白名单，识别、阻止任何白名单外的程序运行，防范已知未知病毒、木马、恶意程序运行和传播及针对0day漏洞的脚本攻击

## 白名单管理

自动扫描、跟踪软件安装及升级、自定义添加、手工导入等方式管理白名单

## 阻止恶意程序执行

识别、阻止任何白名单外的程序运行，阻止病毒、木马、恶意程序运行和传播

## 主机安全加固

操作系统完整性监控、进程的内存空间保护、配置文件和注册表完整性保护

## 基线管理

账户策略、审核策略、安全选项、IP安全、进程审计、系统日志等

## 移动存储介质管理

灵活控制安全U盘和普通U盘的“禁用、只读、可读写”权限，杜绝U盘“串染”病毒

## 告警及日志管理

对日志、告警记录进行丰富、全面的记录

# 软件白名单


## 防护原则

只允许经过工业企业自身授权和安全评估的软件运行

# 移动介质白名单

**防护原则：**拆除或封闭工业主机上不必要的USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

**技术手段：**通过控制软件实现移动介质合法性注册，建立介质白名单，实现移动介质的合法识别和读写控制

# 制度白名单

通过建立工控安全管理机制、成立信息安全协调小组等方式，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。

## 一级文档

- 安全防护总体基本要求
- 安全防护总体实施方案
- 人员安全管理规定
- 安全建设规定
- 安全运维规定
- 安全防护应急预案

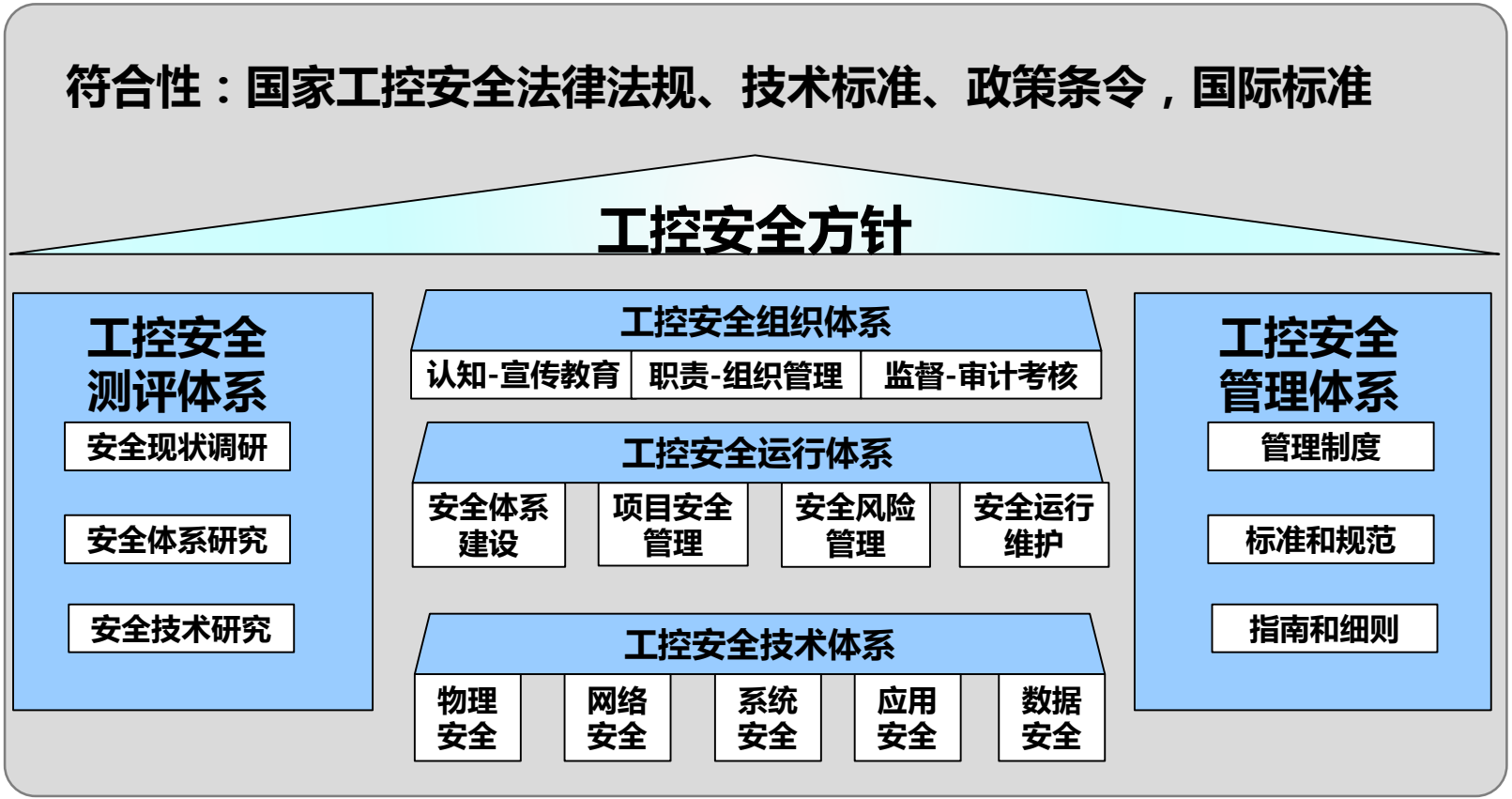
## 二级文档

- 机房管理制度
- 网络接入制度
- 主机管理制度
- 安全介质管理制度
- 系统安全配置策略
- 操作系统安全配置基线
- 网络设备安全配置基线
- 防火墙安全配置基线

## 三级文档

- 系统网络安全接入流程
- 操作系统安全配置基手册
- 网络设备安全配置作业指导书
- 各类记录表单

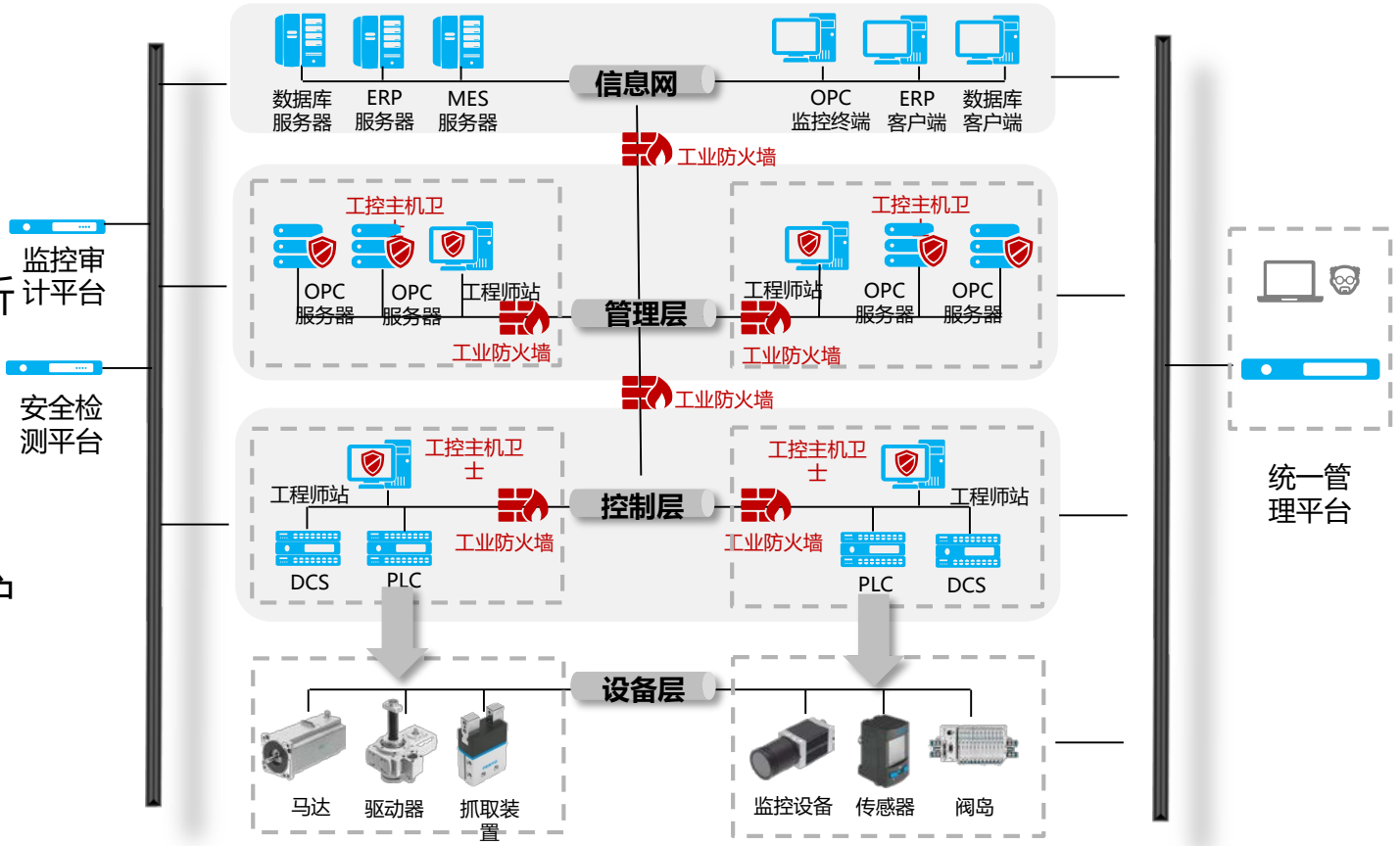
# 工控安全防护总体规划


符合性：国家工控安全法律法规、技术标准、政策条令，国际标准
工控安全方针
工控安全
测评体系
安全现状调研
安全体系研究
安全技术研究
工控安全组织体系
认知-宣传教育
职责-组织管理
监督-审计考核
工控安全运行体系
安全体系
建设
项目安全
管理
安全风险
管理
安全运行
维护
工控安全技术体系
物理
安全
网络
安全
系统
安全
应用
安全
数据
安全
工控安全
管理体系
管理制度
标准和规范
指南和细则

# “白环境”防护整体解决方案

**核心技术理念：**

- 白名单机制
- 工业协议深度解析
- 纵深防御
- 实时监控审计
- 集中管理统一维护
- 安全准入检测



# 典型工控安全事件深度分析

北京威努特技术有限公司

# 目录

# 工控系统典型安全事件

**Conficker (Warm)**
Target: French Navy
Impact: Failure to download flight plans.

2009

**Stuxnet (Warm)**
Target: Iran's nuclear facility
Impact: Destroyed multiple centrifuges

2010

**Night Dragon (Trojan)**
Target: Exxon, BP, Shell and others
Impact: Collect data from SCADA system

2011

**DUQO (Malware)**
Target: Western countries and others
Impact: Conduct reconnaissance on ICS\SCADA

2011

**Flame (Malware)**
Target: Iranian Oil Ministry, Iranian National Oil co.
Impact: Steal and delete information from ICS\SCADA systems

2012

**Havex (Malware)**
Target: General Electric and others
Impact: Scan for ICS\SCADA devices\servers and send data to C&C servers

2014

**Black Energy (Malware)**
Target: Ukrainian Power Grid
Impact: Massive data deletion and power shutdown to more than 225,000 people

2015

**IRONGATE (Malware)**
Target: Siemens S7-315 PLCSIM
Impact: Process manipulation, sending false data to HMI and malicious traffic to PLC

2016

**Who Will Be Hit Next?**

Based on Checkpoint article - 2016

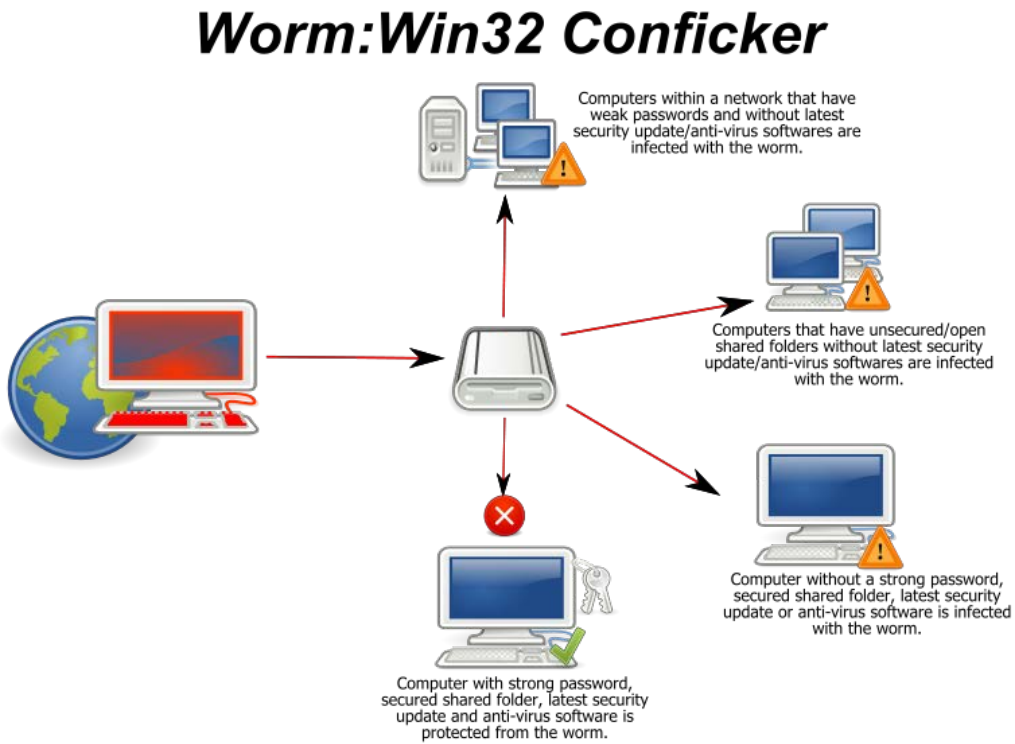
# 国内工控领域典型安全事件

- 2015年3月，国内某石化 3#酮苯装置 Honeywell TPS工控网络中的DCS系统中感染了“Conficker”蠕虫。
- 2015年6月，国内某电力企业的网管设备频繁掉线告警，最终定位其业务网络感染了“Welchia”蠕虫。
- 2015年12月，国内某冶金企业工控网络中感染了“Fanny”木马病毒。
- 2016年1月，国内某钢铁企业CSP工控网络中的DCS系统感染了“Conficker”蠕虫。
- 2016年8月，国内某石油企业的Telvent Oasys的工程师站发现了“Conficker”蠕虫。
- 2017年2月，国内某石油管道系统的工控网络中发现了“Havex”木马病毒。
- 2017年5月，国内多个加油站的工控网络感染了“WannaCry”蠕虫。
- 2015年~2017年，国内多个行业的工控网络多次发现“lpk.dll”U盘木马病毒。

# 目录

# Conficker蠕虫攻击案例分析（一）

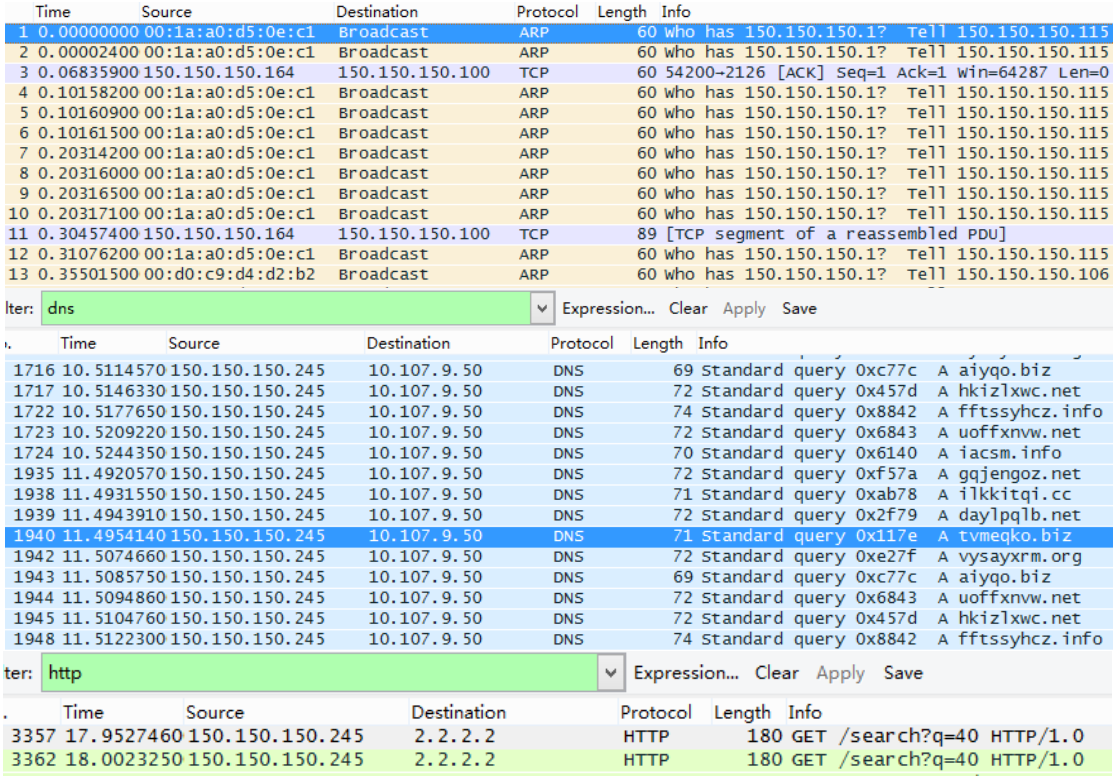
- Conficker蠕虫
  - Conficker蠕虫于2008年爆发，当时全球超过1500万台电脑感染。
  - Conficker利用Windows操作系统的MS08-067漏洞传播，也可以通过USB接口和内网密码爆破来传播。
  - 影响Windows XP、Vista、Server2003、Server2008等系统。



# Conficker蠕虫攻击案例分析（二）

- 工控网络被感染后的异常

  - 发现异常的大量ARP请求，请求网关地址。（工控局域网一般不配置网关地址）
  - 用虚拟机模拟网关，配置网关地址，支持返回DNS请求和TCP的SYN包后发现了异常流量。
  - 工控网络发现大量的DNS请求，目标域名为*.info，*.cc，*.biz。
  - 工控网络发现HTTP异常流量，命中Conficker黑名单签名。



| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.00000000 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 2 | 0.00002400 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 3 | 0.06835900 | 150.150.150.164 | 150.150.150.100 | TCP | 60 | 54200→2126 [ACK] Seq=1 Ack=1 Win=64287 Len=0 |
| 4 | 0.10158200 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 5 | 0.10160900 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 6 | 0.10161500 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 7 | 0.20314200 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 8 | 0.20316000 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 9 | 0.20316500 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 10 | 0.20317100 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 11 | 0.30457400 | 150.150.150.164 | 150.150.150.100 | TCP | 89 | [TCP segment of a reassembled PDU] |
| 12 | 0.31076200 | 00:1a:a0:d5:0e:c1 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.115 |
| 13 | 0.35501500 | 00:d0:c9:d4:d2:b2 | Broadcast | ARP | 60 | who has 150.150.150.1? Tell 150.150.150.106 |

lter: dns Expression... Clear Apply Save

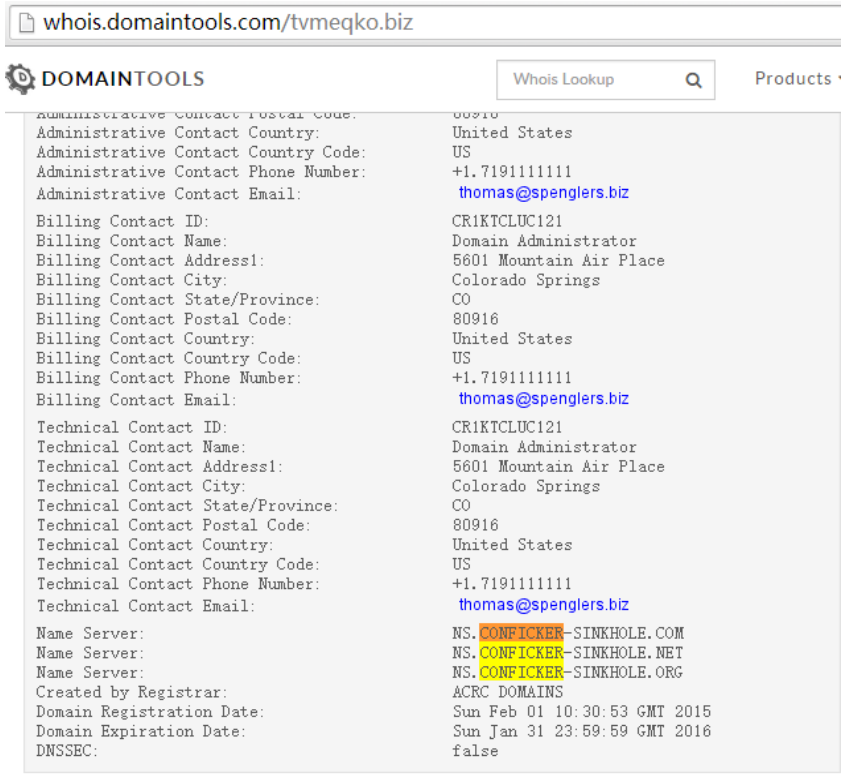
| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1716 | 10.5114570 | 150.150.150.245 | 10.107.9.50 | DNS | 69 | Standard query 0xc77c A aiyqo.biz |
| 1717 | 10.5146330 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0x457d A hkizlxwc.net |
| 1722 | 10.5177650 | 150.150.150.245 | 10.107.9.50 | DNS | 74 | Standard query 0x8842 A fftssyhcz.info |
| 1723 | 10.5209220 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0x6843 A uoffxnvw.net |
| 1724 | 10.5244350 | 150.150.150.245 | 10.107.9.50 | DNS | 70 | Standard query 0x6140 A iacsm.info |
| 1935 | 11.4920570 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0xf57a A gqjengoz.net |
| 1938 | 11.4931550 | 150.150.150.245 | 10.107.9.50 | DNS | 71 | Standard query 0xab78 A ilkkitqi.cc |
| 1939 | 11.4943910 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0x2f79 A daylpqlb.net |
| 1940 | 11.4954140 | 150.150.150.245 | 10.107.9.50 | DNS | 71 | Standard query 0x117e A tvmeqko.biz |
| 1942 | 11.5074660 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0xe27f A vysayxrm.org |
| 1943 | 11.5085750 | 150.150.150.245 | 10.107.9.50 | DNS | 69 | Standard query 0xc77c A aiyqo.biz |
| 1944 | 11.5094860 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0x6843 A uoffxnvw.net |
| 1945 | 11.5104760 | 150.150.150.245 | 10.107.9.50 | DNS | 72 | Standard query 0x457d A hkizlxwc.net |
| 1948 | 11.5122300 | 150.150.150.245 | 10.107.9.50 | DNS | 74 | Standard query 0x8842 A fftssyhcz.info |

ter: http Expression... Clear Apply Save

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 3357 | 17.9527460 | 150.150.150.245 | 2.2.2.2 | HTTP | 180 | GET /search?q=40 HTTP/1.0 |
| 3362 | 18.0023250 | 150.150.150.245 | 2.2.2.2 | HTTP | 180 | GET /search?q=40 HTTP/1.0 |

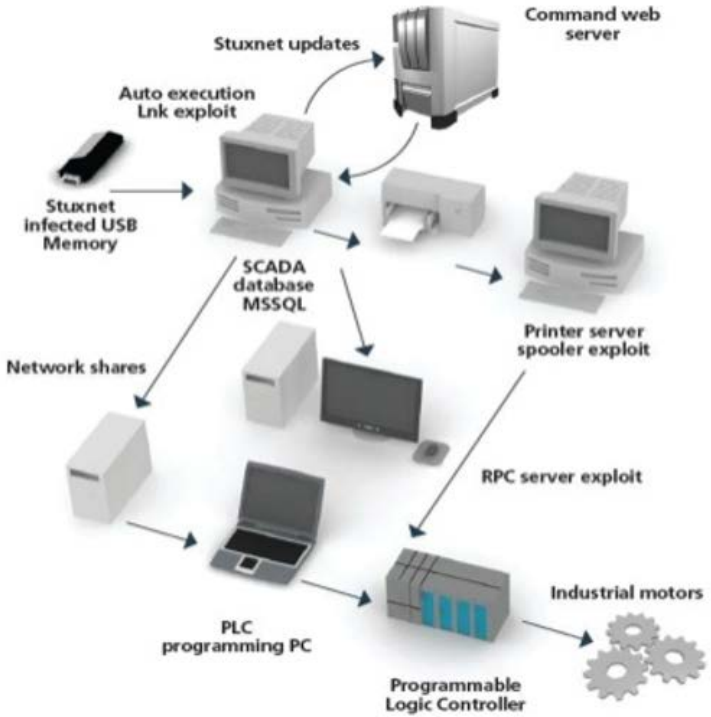
# Conficker蠕虫攻击案例分析（三）

- 域名分析
  - 微步在线 x.threatbook.cn
  - whois.domaintools.com
- 流量分析
  - Wireshark 抓包；
  - Suricata 异常流量分析。



# Stuxnet病毒攻击案例分析（一）

- Stuxnet病毒
  - Stuxnet蠕虫病毒是世界上首个专门针对工业控制系统编写的破坏性病毒。
  - Stuxnet利用对Windows系统和西门子SIMATIC WinCC系统的7个漏洞进行攻击。
  - Stuxnet主要通过U盘和局域网进行传播。



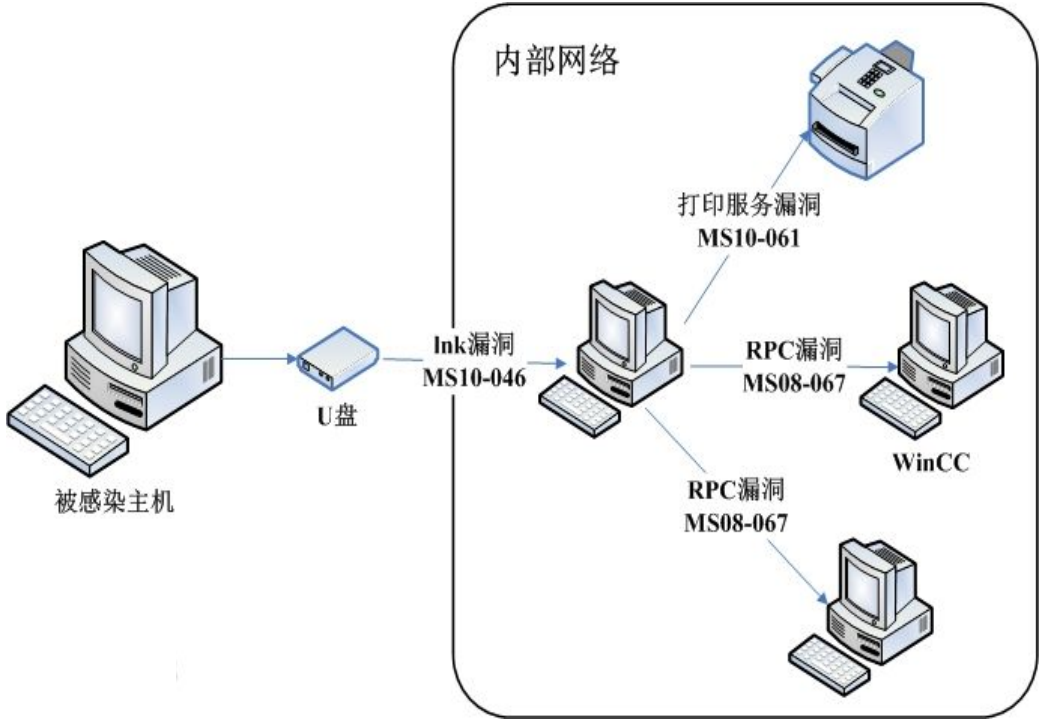
# Stuxnet病毒攻击案例分析（二）

## Stuxnet利用的7个漏洞

- MS08-067（RPC远程执行漏洞）
- MS10-046（快捷方式文件解析漏洞）
- MS10-061（打印机后台程序服务漏洞）
- MS10-073（内核键盘布局程序的本地提权漏洞）
- MS10-092（任务计划程序的本地提权漏洞）

- WINCC 数据库口令硬编码漏洞，Stuxnet利用该漏洞控制SQL数据库。

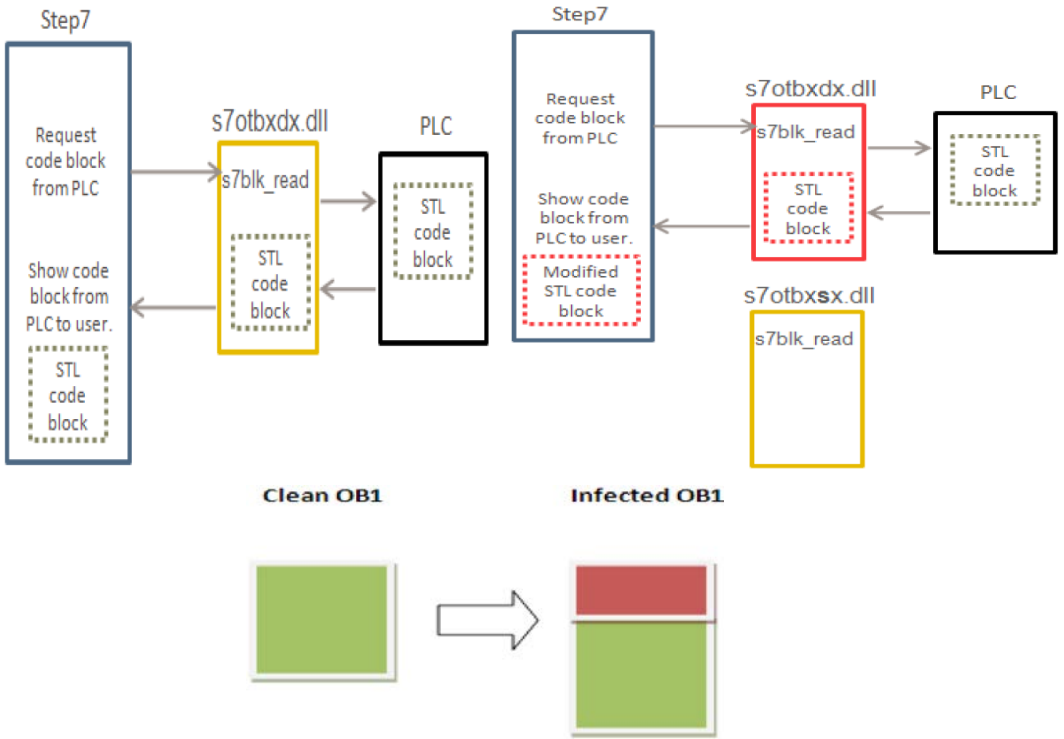
- WINCC 打开Step7工程时的DLL预加载漏洞 ，Stuxnet利用该漏洞替换恶意的Step7 DLL文件，达到攻击PLC的目的。



# Stuxnet病毒攻击案例分析（三）

## Stuxnet攻击PLC的方法

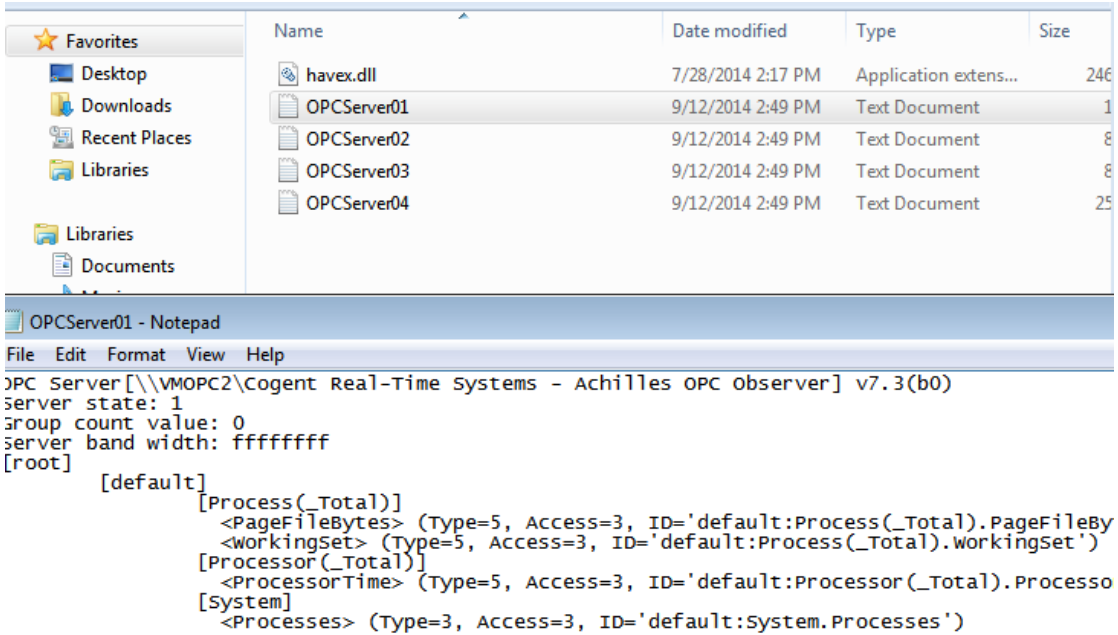
- Step 7 软件使用库文件s7otbxdx.dll 来和PLC通信。
- Stuxnet会将原始的s7otbxdx.dll文件重命名为s7otbxsx.dll，然后用自身取代原始的DLL文件。
- 被Stuxnet修改后的s7otbxdx.dll 文件保留了原来的导出表，导出函数为109个，其中16个被改动后的DLL拦截了，被拦截的导出函数为在PLC中读、写、定位代码块的功能。
- 通过拦截这些请求，Stuxnet 可以在PLC 管理员没有察觉的情况下，修改发送至PLC或从PLC返回的数据。同时，通过利用这些功能，Stuxnet 可以将恶意代码隐藏在PLC中。



# Havex木马攻击案例分析（一）

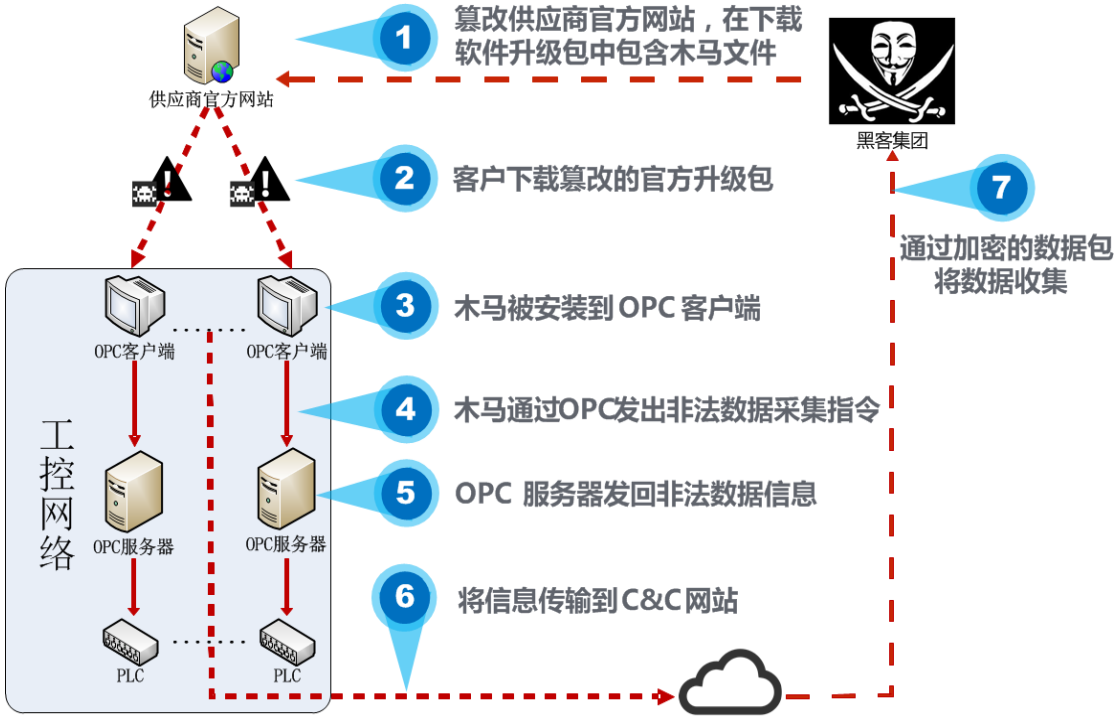
- Havex木马

  - Havex木马于2014年爆发，它被用于工业间谍活动。
  - Havex的主要构成为通用的远程木马（Remote Access Trojan，RAT）和用PHP编写的服务器程序。
  - Havex RAT存在超过88个变种，通信C&C服务器超过164个。



# Havex木马攻击案例分析（二）

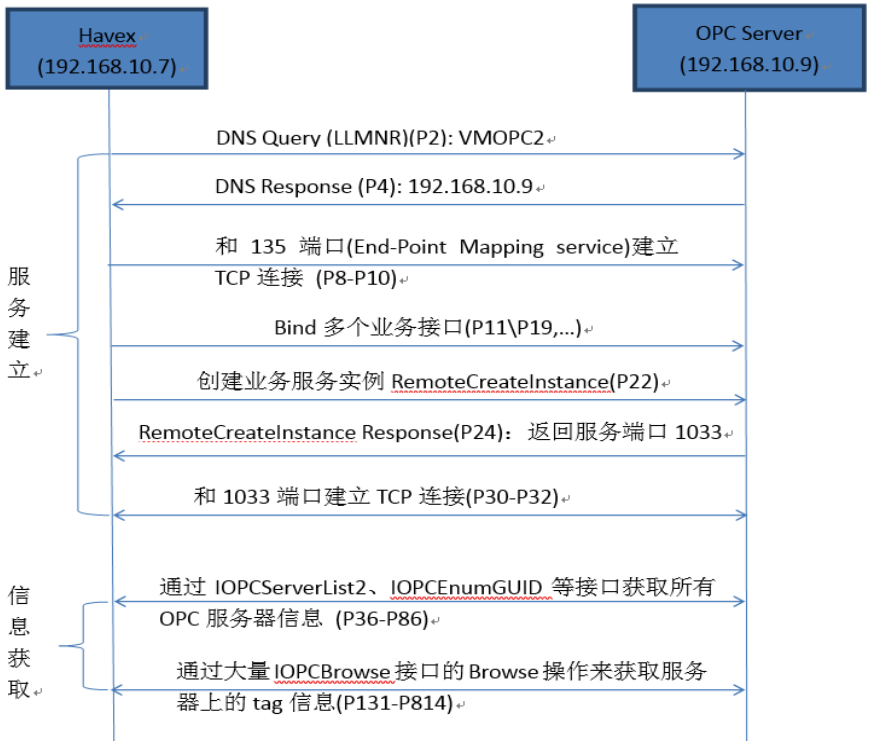
- Havex木马传播途径
  - 钓鱼邮件、垃圾邮件。
  - 漏洞利用工具。
  - 在被入侵的厂商主站为用户提供的软件安装包中包含该木马。



# Havex木马攻击案例分析（三）

- Havex木马通讯过程

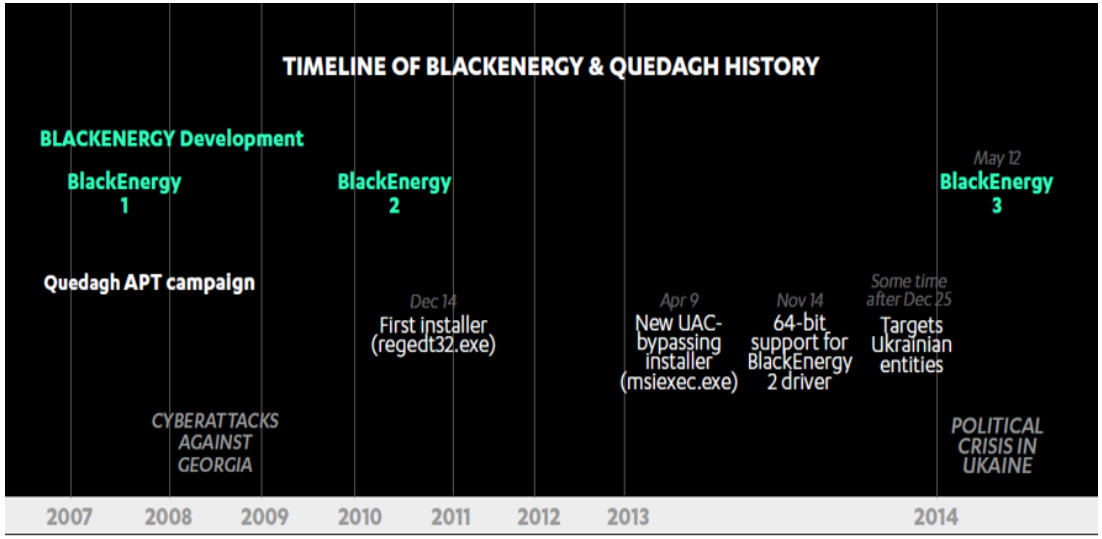
  - Havex利用OPC DCOM协议来收集工控设备的信息，然后将这些信息反馈到C&C服务器。
  - Havex通过IOPCServerList2、IOPCEnumGUID等接口获取OPC服务器信息。
  - Havex通过IOPCBrowse接口的Browse操作来获取服务器上的tag信息。



# BlackEnergy恶意软件攻击案例分析（一）

## BlackEnergy恶意软件

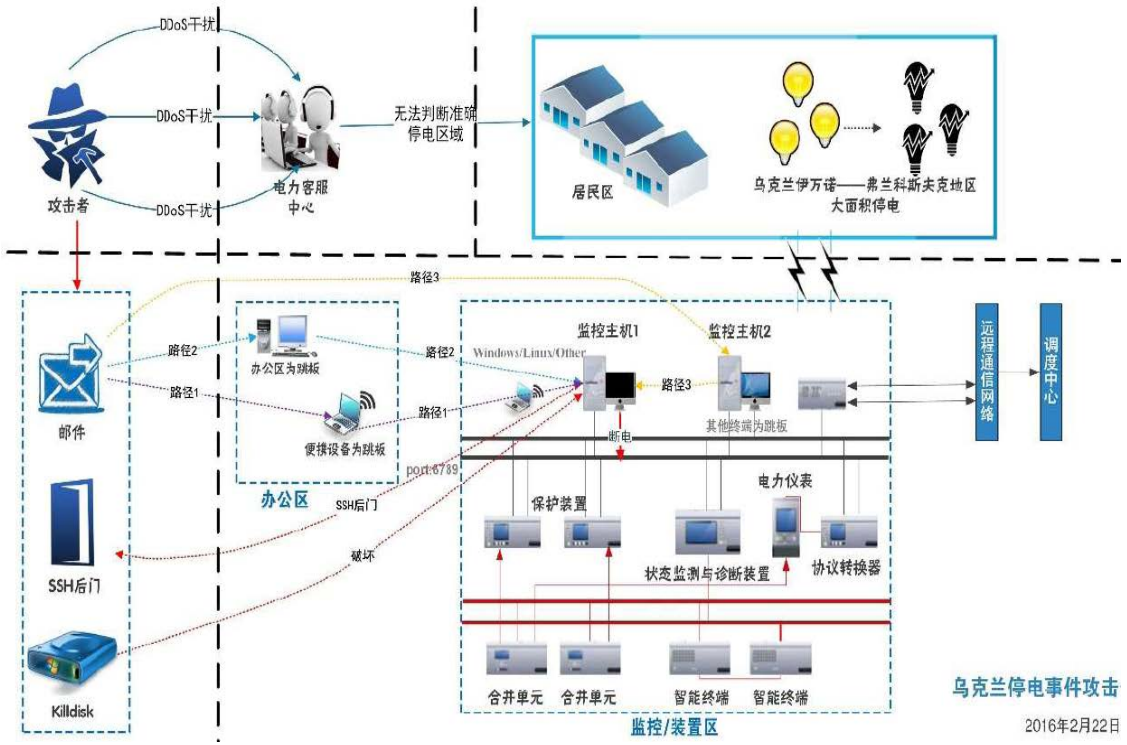
- 2007年，Arbor公司首次公布了BlackEnergy的分析报告，它是一个DDOS木马。
- 2008年，俄格冲突期间，BlackEnergy被用来对格鲁吉亚实施网络攻击。
- 2010年，BlackEnergy第二个版发布，集成了rootkit技术。
- 2014年，美国CERT发布公告，美国工控系统在三年前已经被BlackEnergy攻击，它攻击的HMI包括，GE Cimlicity、WebAccess和WinCC。
- 2014年，SandWorm组织被iSIGHT发现利用MS14-060传播BlackEnergy。
- 2015年，乌克兰电网被BlackEnergy攻击导致140万人口断电几小时。



# BlackEnergy恶意软件攻击案例分析（二）

## 乌克兰电网被攻击事件回顾

- 以BlackEnergy 等相关恶意代码为主要攻击工具；
- 通过BOTNET 体系进行前期的资料采集和环境预置；
- 以邮件发送恶意代码载荷为最终攻击的直接突破入口；
- 通过远程控制SCADA 节点下达指令为断电手段；
- 以摧毁破坏SCADA 系统实现迟滞恢复和状态致盲；
- 以DDoS 电话作为干扰，最后达成长时间停电并制造整个社会混乱的具有信息战水准的网络攻击事件。



# BlackEnergy恶意软件攻击案例分析（三）

## BlackEnergy攻击组件介绍

- BlackEnergy 组件是DLL 库文件，一般通过加密方式发送到僵尸程序，一旦组件DLL 被接收和解密，将被置于分配的内存中，然后等待相应的命令。
- 例如：可以通过组件发送垃圾邮件、窃取用户机密信息、建立代理服务器、伺机发动DDoS 攻击等。
- 乌克兰电网攻击事件中主要用到了KillDisk组件，该组件会使用随机数据覆盖文件，删除MBR，导致系统无法启动。

| 组件名称 | 功能 |
| --- | --- |
| SYN | SYN攻击 |
| HTTP | http攻击 |
| DDOS | DDoS攻击 |
| spm_v1 | 垃圾邮件 |
| Ps | 密码偷窃 |
| ibank.dll | 窃取银行证书 |
| VSNET | 传播和发射有效载荷 |
| weap_hwi | 编译ARM系统上运行的DDoS工具 |
| FS | 搜索特定的文件类型 |
| DSTR | 这通过用随机数据重写它破坏 |
| RD | 远程桌面 |
| Ciscoapi.tcl | 针对思科路由器 |
| KillDisk | 删除MBR，导致系统无法启动 |

# Stuxnet VS BlackEnergy 攻击案例

| | 震网事件 | 乌克兰变电站遭受攻击事件 |
|---|---|---|
| 主要攻击目标 | 伊朗核工业设施 | 乌克兰电力系统 |
| 关联被攻击目标 | Foolad Technic Engineering Co<br>（该公司为伊朗工业设施生产自动化系统）<br>Behpajooh Co.Elec & Comp.Engineering<br>（开发工业自动化系统）<br>Neda Industrial Group<br>（该公司为工控领域提供自动化服务）<br>Control-Gostar Jahed Company（工业自动化公司）<br>Kala Electric（该公司是铀浓缩离心机设备主要供应商） | 乌克兰最大机场基辅鲍里斯波尔机场<br>乌克兰矿业公司<br>乌克兰铁路运营商<br>乌克兰国有电力公司UKrenergo<br>乌克兰TBS电视台 |
| 作用目标 | 上位机（Windows、WinCC）、PLC控制系统、PLC | 办公机（Windows）、上位机（Windows） |
| 造成后果 | 大大延迟了伊朗的核计划 | 乌克兰伊万诺-弗兰科夫斯克地区大面积停电 |
| 核心攻击原理 | 修改离心机压力参数、修改离心机转子转速参数 | 通过控制SCADA系统直接下达断电指令 |
| 使用漏洞 | MS08-067（RPC远程执行漏洞）<br>MS10-046（快捷方式文件解析漏洞）<br>MS10-061（打印机后台程序服务漏洞）<br>MS10-073（内核键盘布局程序本地提权漏洞）<br>MS10-092（任务计划程序本地提权漏洞）<br>WINCC数据库口令硬编码<br>WINCC 打开Step7工程时DLL预加载漏洞 | MS14-060（Windows OLE远程代码执行漏洞） |
| 攻击入口 | USB摆渡、人员植入（猜测） | 邮件发送带有恶意代码宏的文档 |
| 前置信息采集和环境预置 | 可能与DUQU、FLAME 相关 | 采集打击一体 |
| 通讯与控制 | 高度严密的加密通讯、控制体系 | 相对比较简单 |
| 恶意代码模块情况 | 庞大严密的模块体系，具有高度的复用性 | 模块体系，具有复用性 |
| 抗分析能力 | 高强度的本地加密，复杂的调用机制 | 相对比较简单，易于分析 |
| 数字签名 | 盗用三个主流厂商数字签名 | 未使用数字签名 |
| 攻击成本 | 超高开发成本 、超高维护成本 | 相对较低 |

# WannaCry蠕虫攻击案例分析（一）

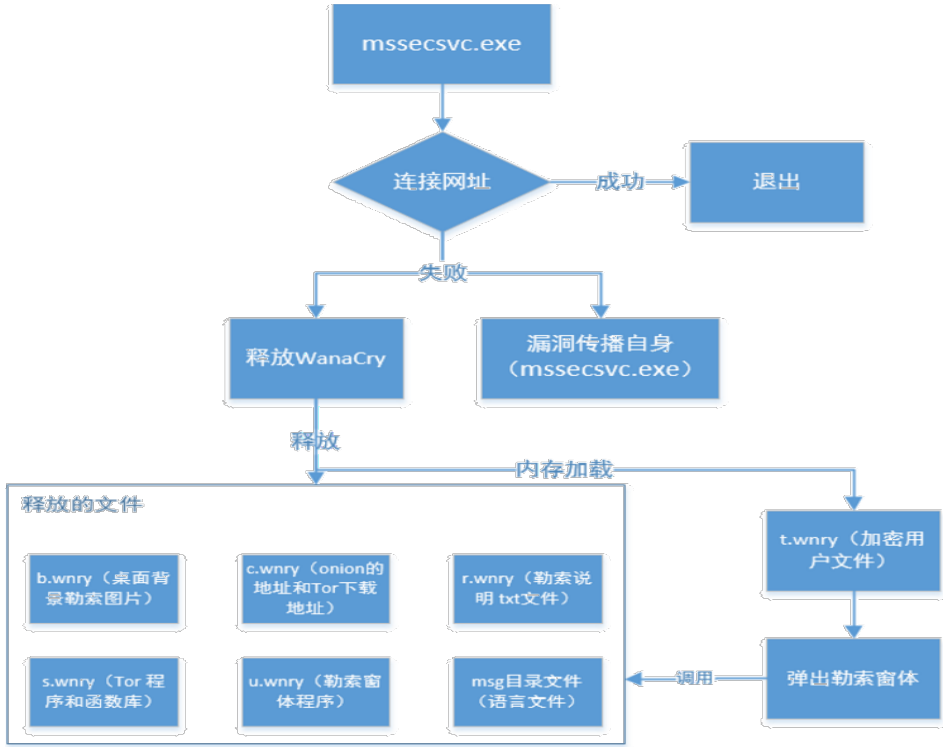
## WannaCry蠕虫

- WannaCry，一种“蠕虫式”的勒索病毒软件，大小3.3MB，由不法分子利用此前披露的Windows SMB服务漏洞（MS17-010）攻击手段，向终端用户进行渗透传播。
- 该恶意软件会扫描电脑上的TCP 445端口(SMB)，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。勒索金额为300至600美元。
- 2017年4月14日，黑客组织Shadow Brokers公布的Equation Group（方程式组织，隶属于美国国家安全局）使用的“网络军火”中包含了该漏洞的利用程序。

# WannaCry蠕虫攻击案例分析（二）

## WannaCry蠕虫行为分析

- 蠕虫主程序，带有域名开关，负责利用漏洞进行传播、释放WannaCry勒索软件执行。
- WannaCry勒索软件程序，释放Tor程序连接暗网、加密自动后缀名文件、弹出勒索窗体。
- WannaCry勒索软件会加密系统中的照片、图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件，被加密的文件后缀名被统一修改为“.WNCRY”。
- 勒索软件窗体文件，显示勒索敲诈内容、倒计时信息、比特币购买地址、攻击者比特币钱包等信息。



# WannaCry蠕虫攻击案例分析（三）

## WannaCry蠕虫文件加密分析

- WannaCry蠕虫加密的基本操作均在内部加载的DLL中完成，加密文件的算法是128位AES，而AES密钥被RSA加密，RSA为随机生成的密钥对，公钥在本地系统保存，私钥提交到攻击者服务器。
- 勒索者秘密生成一个2048位的RSA私钥，并将对应公钥硬编码置于病毒体内。
- 受害者感染病毒后，会生成一对自己的公钥私钥，私钥被勒索者的公钥加密并保存为PKY文件，受害者的每一个文件都被128位的AES加密，其AES密钥被加密后置于文件头的地方。
- 这个设计的目的在于，勒索者可以为每个受害者单独提供解密服务，任何一台主机的解密数据服务，不会对其它主机的解密造成影响，从而保证勒索者可以按主机收取费用。

```
10003B12   5B              pop     ebx
10003B13   C2 0800         retn    8
10003B16   53              push    ebx
10003B17   8BCE            mov     ecx, esi
10003B19   E8 E2000000     call    10003C00
10003B1E   85C0            test    eax, eax
10003B20   75 73           jnz     short 10003B95
10003B22   8D56 0C         lea     edx, dword ptr [esi+C]
10003B25   52              push    edx
10003B26   50              push    eax
10003B27   50              push    eax
10003B28   8B46 04         mov     eax, dword ptr [esi+4]
10003B2B   68 14010000     push    114
10003B30   68 40CF0010     push    1000CF40
10003B35   50              push    eax
10003B36   FF15 40D90010   call    dword ptr [1000D940]        ADVAPI32.CryptImportKey
10003B3C   85C0            test    eax, eax
10003B3E   74 46           je      short 10003B86
10003B40   8B4E 04         mov     ecx, dword ptr [esi+4]
10003B43   8D7E 08         lea     edi, dword ptr [esi+8]
10003B46   57              push    edi
10003B47   51              push    ecx
```



图表 1 导入密钥

# 方程式组织的病毒木马武器库

## 方程式组织

- 方程式组织（Equation Group）是一个由卡巴斯基实验室发现的尖端网络犯罪组织，后者将其称为世界上最尖端的网络攻击组织之一，同震网（Stuxnet）和火焰（Flame）病毒的制造者紧密合作且在幕后操作。
- 在方程式组织使用的恶意软件中，发现了诸如“STRAITACID”和“STRAITSHOOTER”之类的美国国家安全局代号。

| | | |
|---|---|---|
| EquationLaser | Equation 组织早期使用的植入程序，大约在 2001 至 2004 年间被使用。兼容 Windows 95/98 系统。 | 2001-2003 |
| EquationDrug | 该组织使用的一个非常复杂的攻击组件，用于支持能够被攻击者动态上传和卸载的模块插件系统。怀疑是 EquationLaser 的升级版。 | 2003-2013 |
| DoubleFantasy | 一个验证式的木马，旨在确定目标为预期目标。如果目标被确认，那么已植入恶意代码会升级到一个更为复杂的平台，如 EQUATIONDRUG 或 GRAYFISH。 | 2004-2012 |
| TripleFantasy | 全功能的后门程序，有时用于配合 GRAYFISH 使用。看起来像是 DOUBLEFANTASY 的升级版，可能是更新的验证式插件。 | 2012-至今 |
| Fanny | 创建于 2008 年的利用 USB 设备进行传播的蠕虫，可攻击物理隔离网络并回传收集到的信息。Fanny 被用于收集位于中东和亚洲的目标的信息。一些受害主机似乎已被升级到 DoubleFantasy，然后又升级为 EQUATIONDRUG。Fanny 利用了两个后来被应用到 Stuxnet 中的 0day 漏洞。 | 2008-2011 |
| GrayFish | Equation 组织中最复杂的攻击组件，完全驻留在注册表中，依靠 bootkit 在操作系统启动时执行。 | 2008-至今 |

# 目录

# 高级持续威胁攻击

- APT：Advanced Persistent Threat（高级持续性威胁）
  - 当前最具威胁的攻击形式
  - 针对高价值目标，有组织、目的非常明确的高级攻击行为
  - 世界各国网络部队发起攻击的核心手段，破坏性之高难以衡量
  - 采用长期潜伏、反复试探、不断渗透的方式发起攻击
  - 通常利用未知的漏洞、未知的攻击手段发起攻击
  - 检测难度非常大，传统安全产品、检测技术无法与之对抗
  - 从2011年开始，连续三年在世界最著名的安全盛会（RSA）中成为最热点、最核心的安全问题

# APT攻击的典型案例

2011：窃取RSA令牌种子

2012：火焰攻击中东

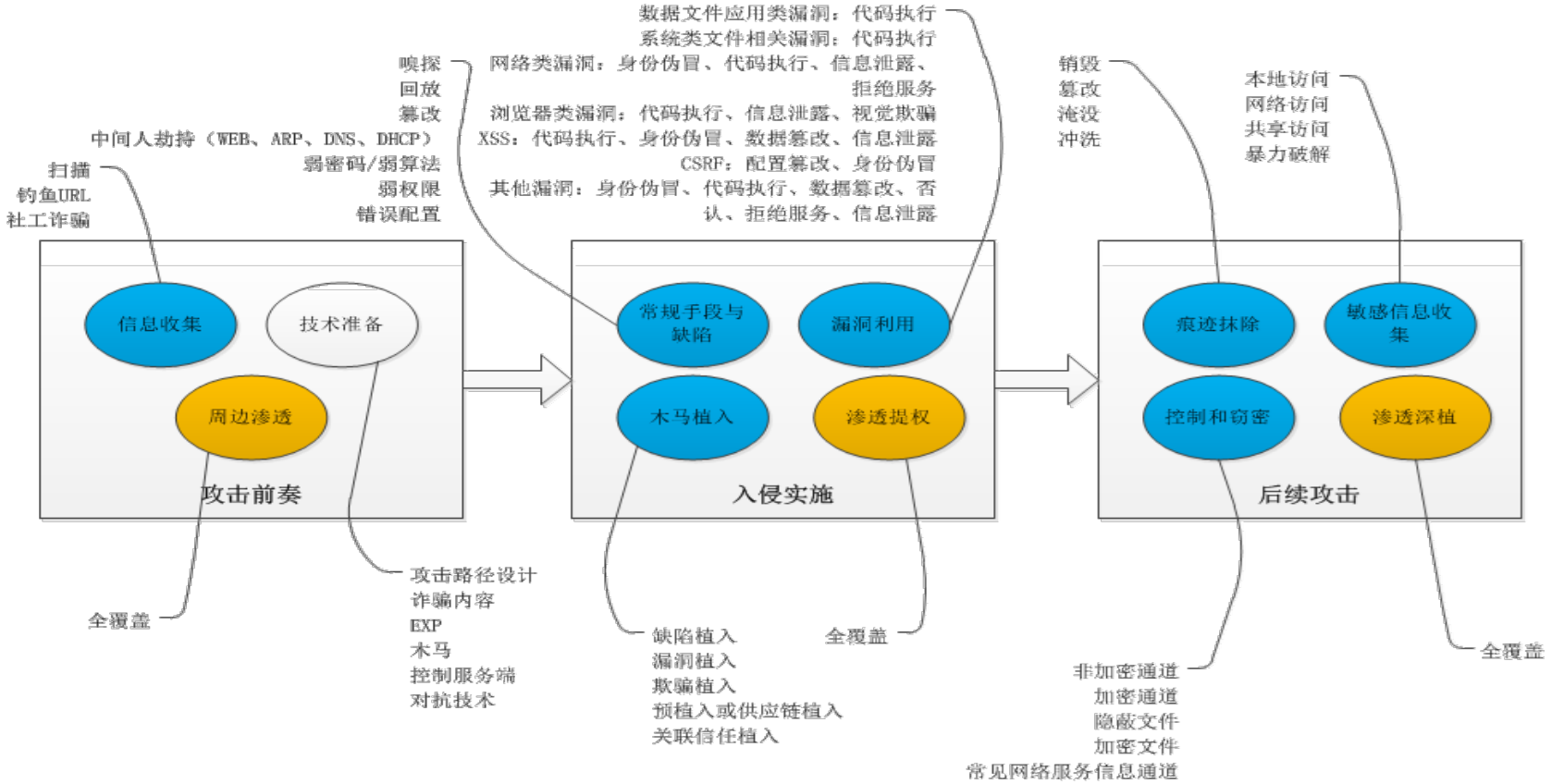
2012：窃取NASA资料

2010：震网攻击伊朗核电站

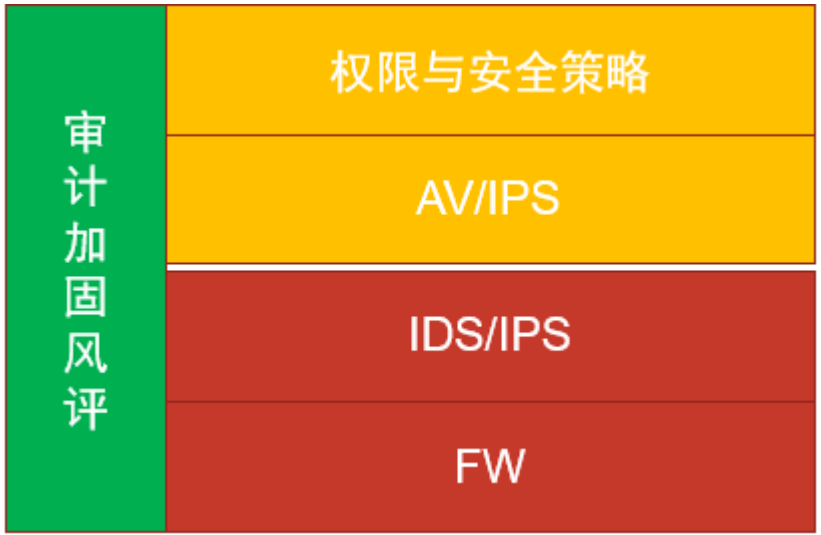
为什么我们的安全防护体系在专业黑客攻击下不堪一击？

2015：乌克兰电网被攻击

# APT攻击生命周期


数据文件应用类漏洞：代码执行
系统类文件相关漏洞：代码执行
嗅探
回放
篡改
网络类漏洞：身份伪冒、代码执行、信息泄露、拒绝服务
浏览器类漏洞：代码执行、信息泄露、视觉欺骗
XSS：代码执行、身份伪冒、数据篡改、信息泄露
CSRF：配置篡改、身份伪冒
其他漏洞：身份伪冒、代码执行、数据篡改、否认、拒绝服务、信息泄露
中间人劫持（WEB、ARP、DNS、DHCP）
弱密码/弱算法
弱权限
错误配置
扫描
钓鱼URL
社工诈骗
销毁
篡改
淹没
冲洗
本地访问
网络访问
共享访问
暴力破解
信息收集
技术准备
周边渗透
攻击前奏
常规手段与缺陷
漏洞利用
木马植入
渗透提权
入侵实施
痕迹抹除
敏感信息收集
控制和窃密
渗透深植
后续攻击
全覆盖
攻击路径设计
诈骗内容
EXP
木马
控制服务端
对抗技术
缺陷植入
漏洞植入
欺骗植入
预植入或供应链植入
关联信任植入
全覆盖
非加密通道
加密通道
隐蔽文件
加密文件
常见网络服务信息通道
全覆盖

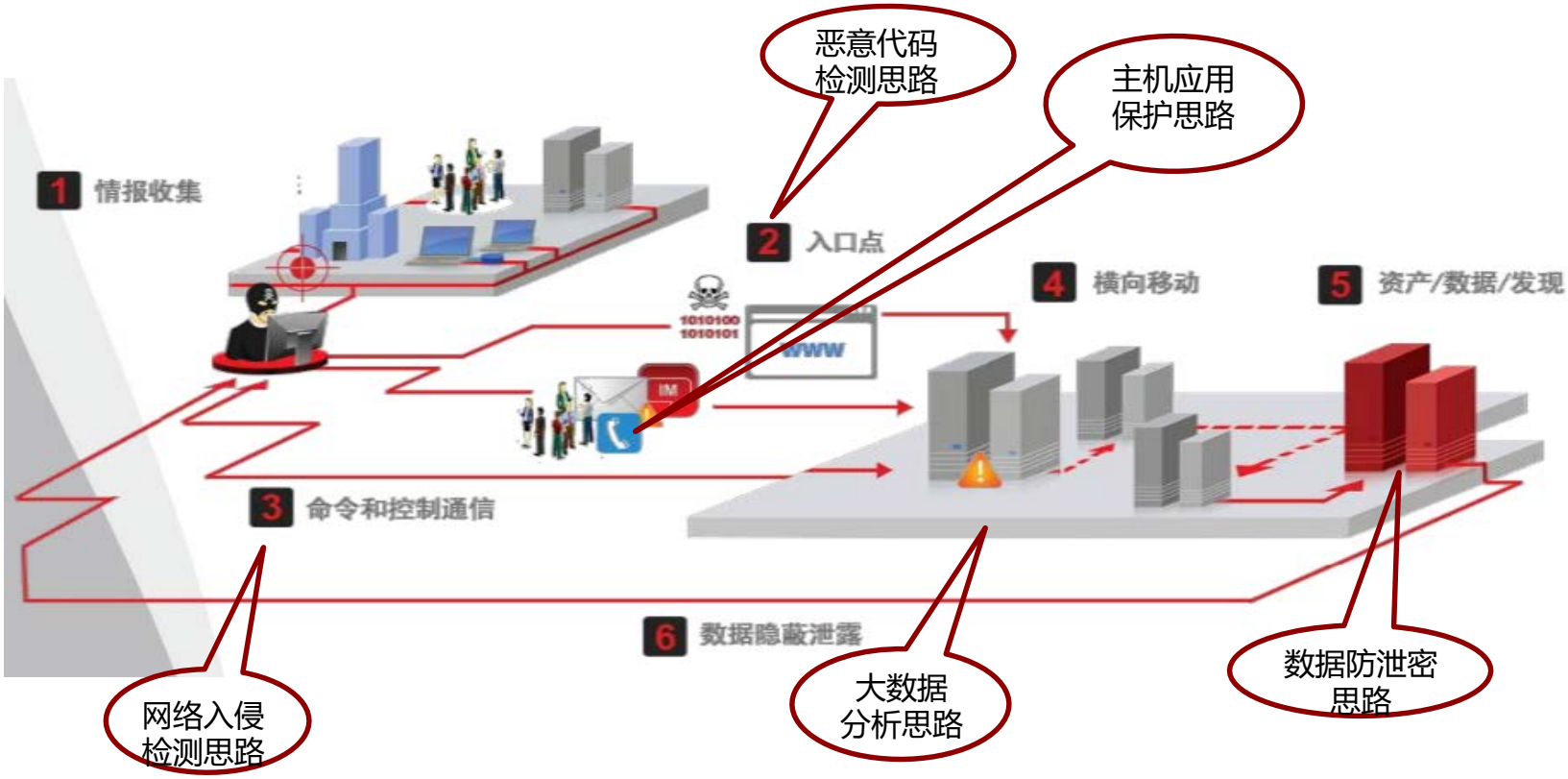
# 面对APT攻击，传统防护的短板




基于已知知识：
已知安全漏洞与缺陷
已知木马行为与特征
已知攻击行为
明文内容
限定的权限

难以应对：
未知安全漏洞与缺陷
未知木马行为与特征
未知攻击行为
加密内容
社会工程

# APT检测防御思路

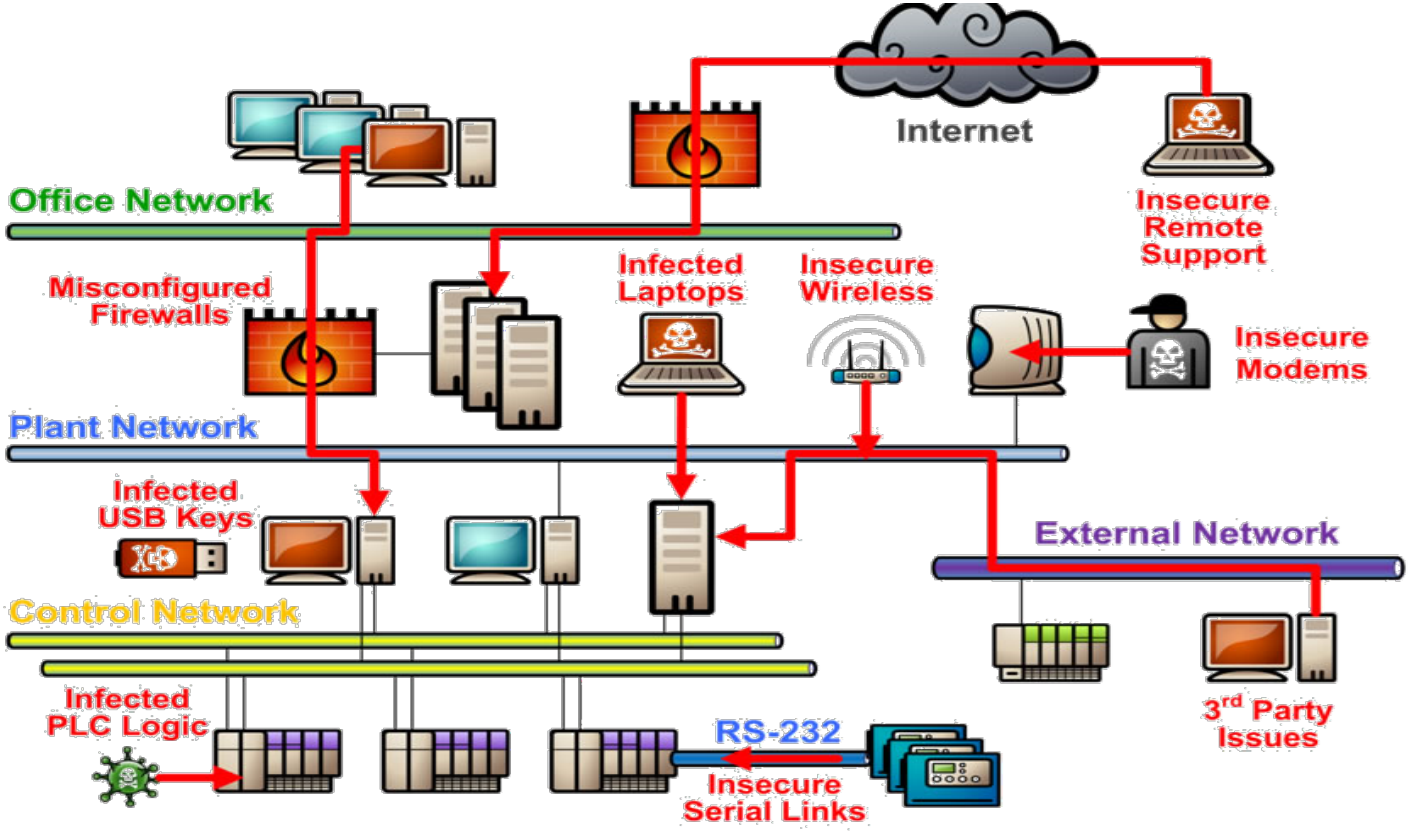

恶意代码
检测思路
主机应用
保护思路
1 情报收集
2 入口点
4 横向移动
5 资产/数据/发现
3 命令和控制通信
6 数据隐蔽泄露
网络入侵
检测思路
大数据
分析思路
数据防泄密
思路

# 工控网络渗透技术交流

北京威努特技术有限公司

# 目录

# 网络攻击路径


Internet
Office Network
Insecure
Remote
Support
Misconfigured
Firewalls
Infected
Laptops
Insecure
Wireless
Insecure
Modems
Plant Network
Infected
USB Keys
External Network
Control Network
Infected
PLC Logic
RS-232
Insecure
Serial Links
3rd Party
Issues

# 目录

# 工控漏洞分类

## 按攻击类型分类

- 检验篡改组态数据
- 伪造控制指令
- 实时欺骗
- 获取超级权限
- 导致拒绝服务
- … …

## 按攻击目标分类

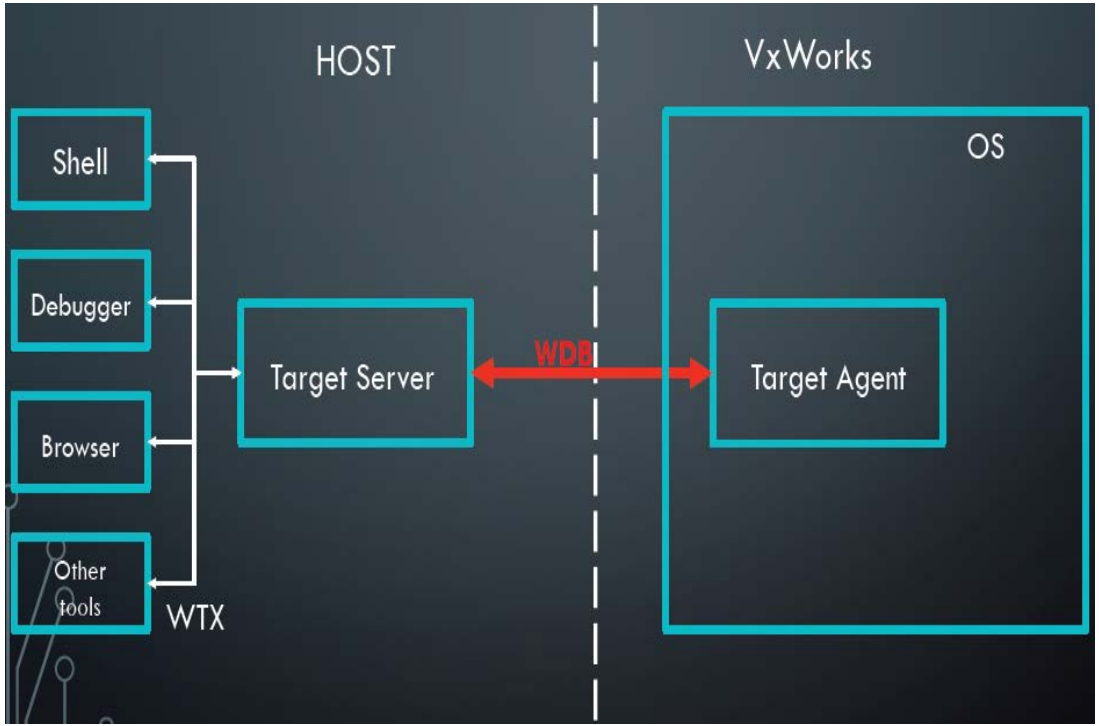
- 实时操作系统（VxWorks）
- 组态软件（WinCC、KingView）
- DCS（ABB Symphony、Emerson DeltaV）
- PLC（Siemens SIMATIC S7、Schneider Modicon Quantum）
- 工业交换机（Hirschmann PowerMICE）
- 数控机床（Fanuc CNC）
- … …

# 工控漏洞案例（一）

- 实时操作系统 & 获取超级权限

  - VxWorks tPortMapd RPC 远程整数溢出漏洞

  - 该漏洞属于整型溢出漏洞，成功的利用该漏洞可在VxWorks 5.x、VxWorks 6.x上添加新用户并控制目标机，在漏洞利用过程中使用了堆喷射技术来传递Shellcode。

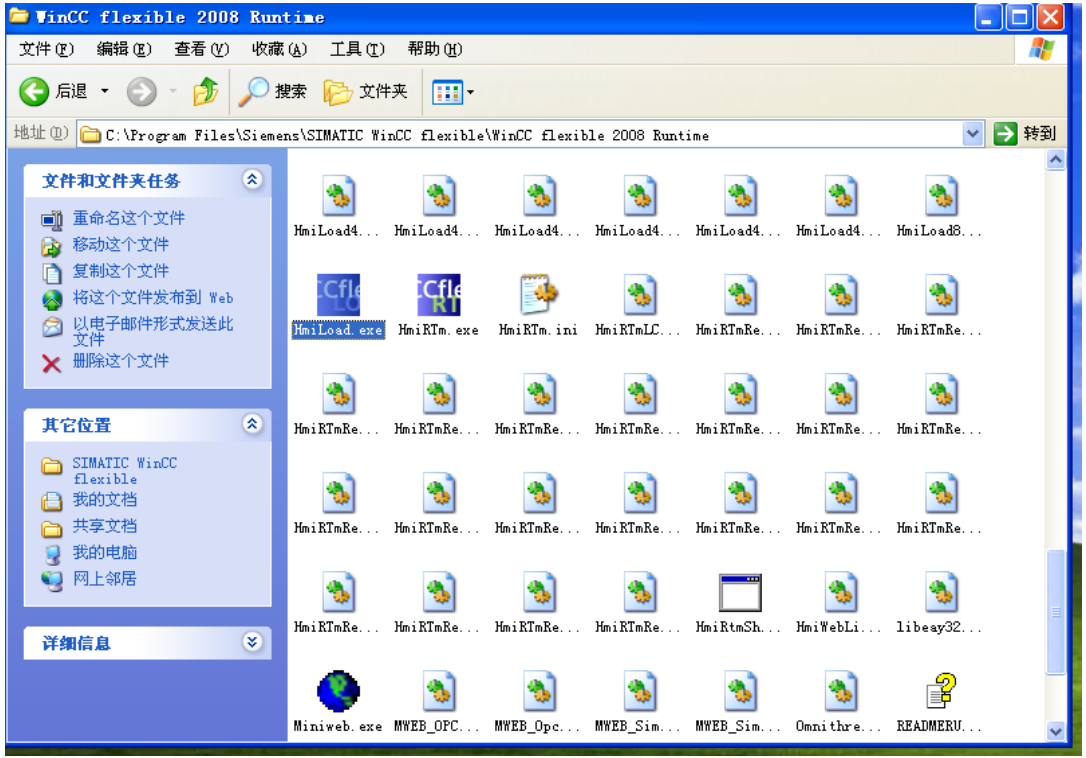


# 工控漏洞案例（二）

- 组态软件 & 获取超级权限

  - Siemens SIMATIC WinCC 目录遍历、文件上传漏洞

  - WinCC多个版本中的运行加载器中的HmiLoad存在目录遍历漏洞。远程攻击者可利用该漏洞借助字符串中的..（点 点）执行、读取、创建、修改或删除任意文件。

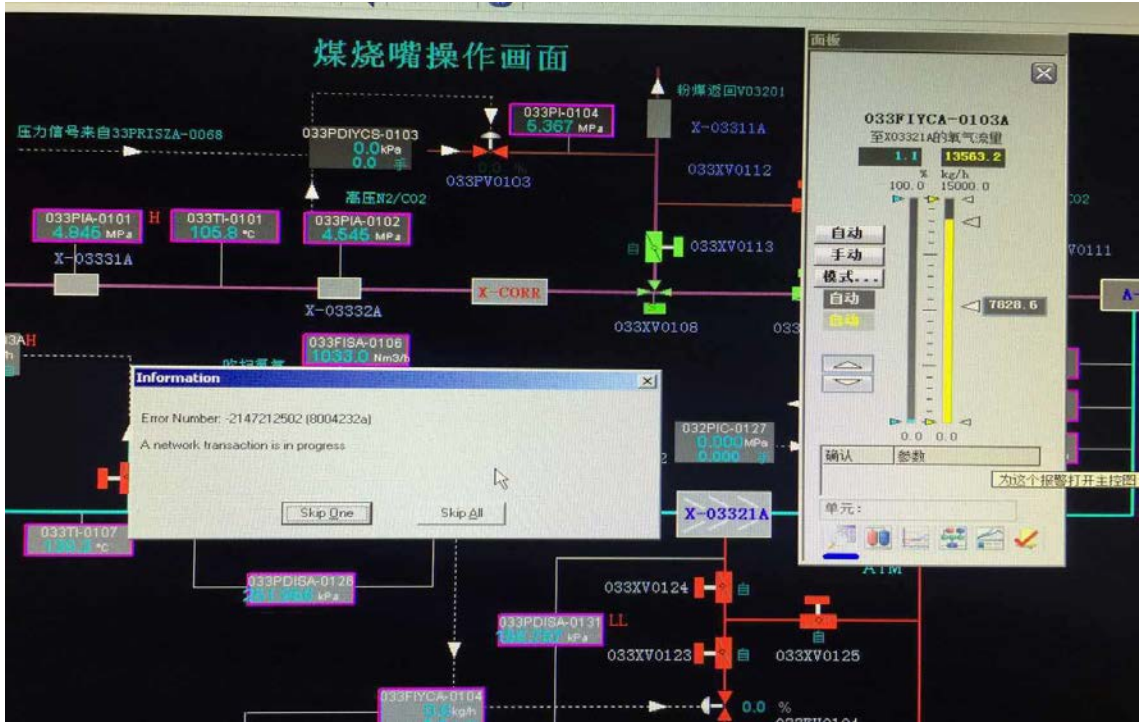


# 工控漏洞案例（三）

- DCS & 导致拒绝服务

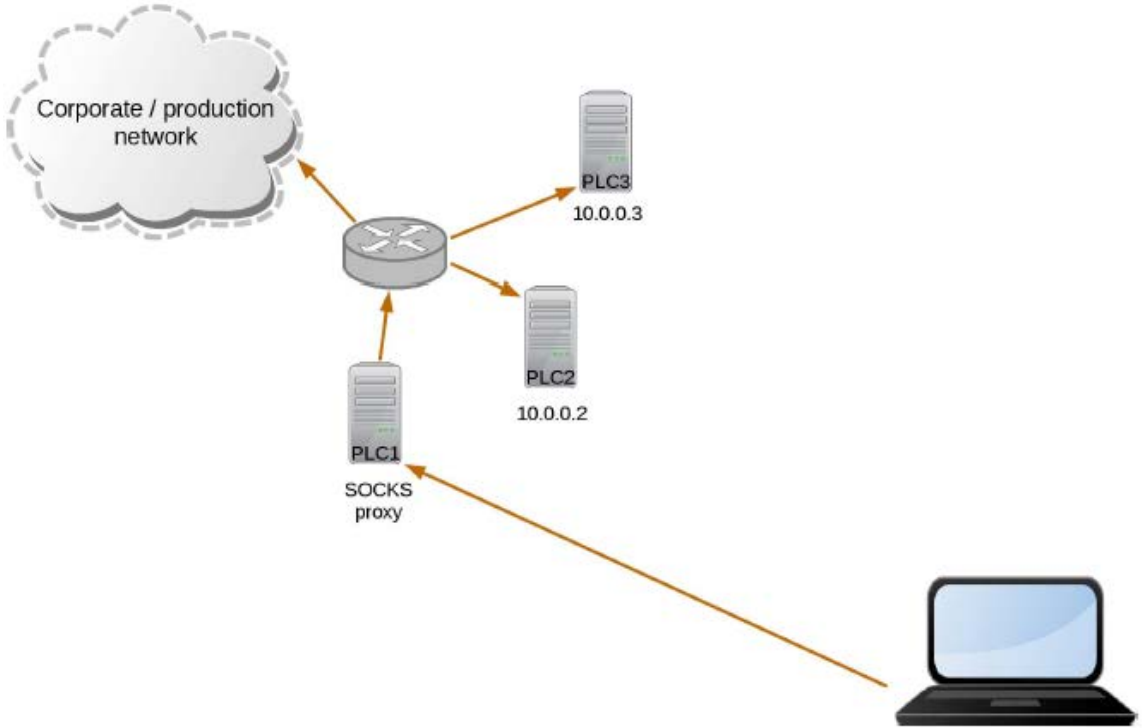
  - Emerson DeltaV DCS工作站拒绝服务漏洞

  - 将DeltaV控制包的特定偏移位置处数据修改为某个固定值后，艾默生监控工作站在处理该通信数据包时，由于缺乏正确的安全校验逻辑，导致工作站持续弹出错误窗口，无法进行正常的监控画面操作，造成工作站拒绝服务。



# 工控漏洞案例（四）

- PLC & 检验篡改组态数据
  - Blackhat2015，来自德国SCADACS的团队演示了针对西门子PLC的代码植入，可以在西门子PLC中植入特定的逻辑代码使PLC变为代理服务器，并通过该代理服务器作为跳板攻击其他控制设备。

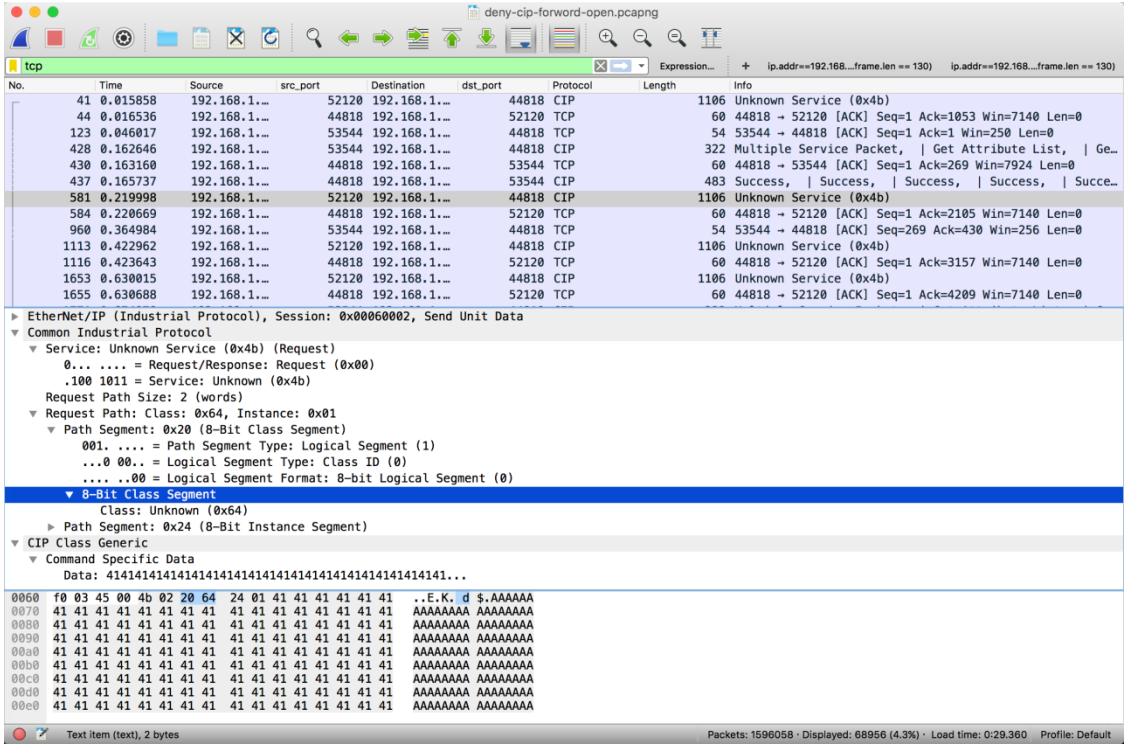


# 工控漏洞案例（五）

- PLC & 导致拒绝服务

  - AB CompactLogix 5000系列控制器CIP协议拒绝服务漏洞

  - AB CompactLogix 5000系列控制器的CIP通讯协议存在漏洞，漏洞被成功利用后将导致目标设备无法正常响应部分CIP功能码的请求，所有依赖这些功能码的以太网监控数据采集或控制指令下发将无法正常工作从而严重影响现场生产。



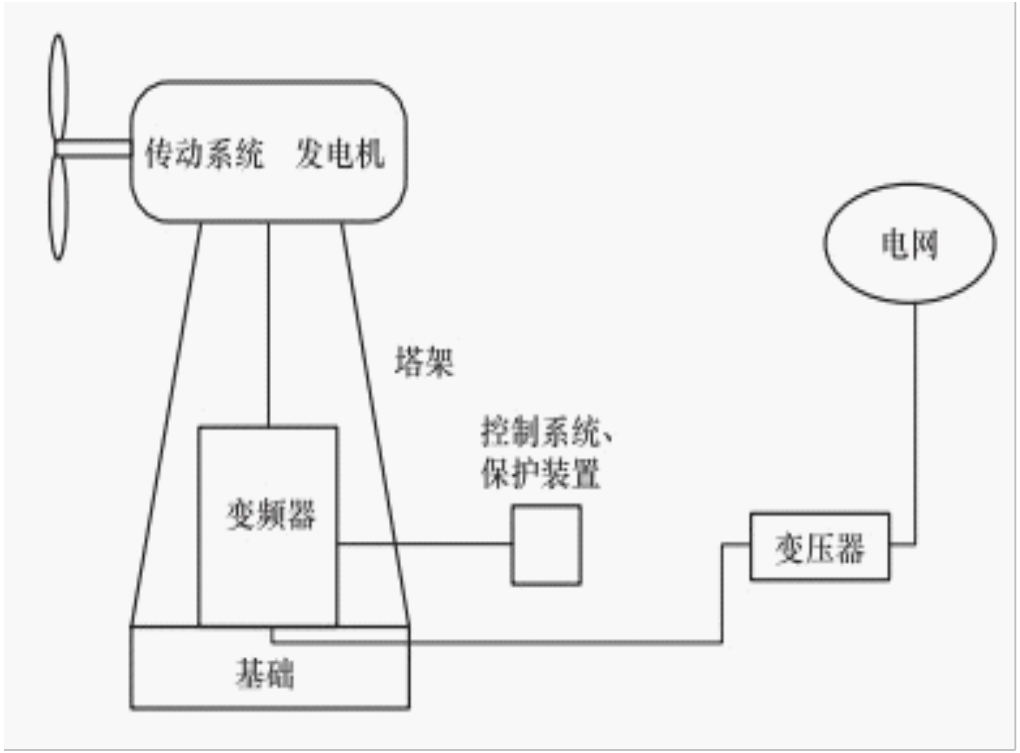
# 工控漏洞案例（六）

- CNC & 伪造控制指令
  - 西门子数控系统 SINUMERIK 840D sl系统的PCU ，具有用于 Ethernet、 MPI 和 PROFIBUS DP 通讯的接口。
  - 840D sl系统中PCU与NCU之间通信时数据进行分析，得知该系统加工G代码的传输是采用的是明文传输，可以被攻击者篡改控制代码，伪造控制指令。


# 目录

# 风力发电系统架构

- 风力发电系统一般包括风电机组、线路、变压器等。
- 风电机组，一般包括传动系统、偏航系统、液压与制动系统、发电机、控制和安全系统等。



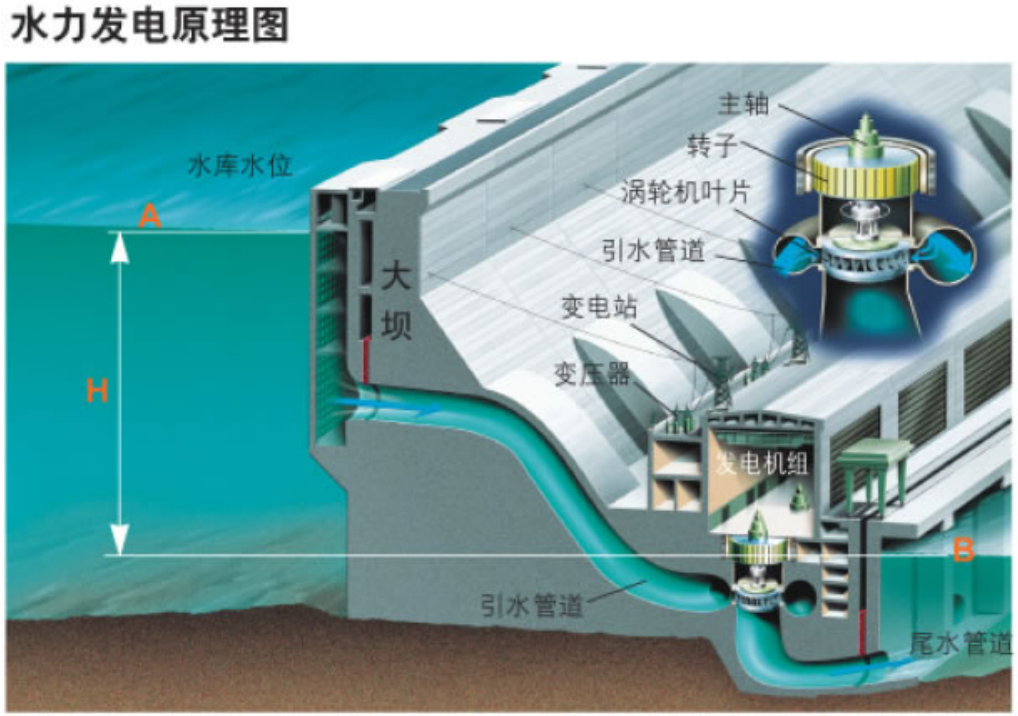
# 风力发电系统案例

- Bachmann MX213 PLC安全漏洞
  - 该PLC开启了Telnet、FTP、HTTP以及RPC服务，这些服务均存在严重的安全漏洞。
  - 利用FTP漏洞登录后甚至能够获取该PLC内部的任意文件包括Vxworks的内核文件。
- 研华-TPC-651H HMI安全漏洞
  - 该HMI开启了Telnet、RDP远程桌面服务（3389）、windows共享等服务，且部分服务存在严重的安全漏洞。
  - 通过利用这些漏洞可以成功的获取具有系统管理员权限的命令行权限甚至完全控制该设备。

# 水力发电系统架构

- 水力发电系统一般包括水轮发电机组、变压器、高压配电装置、互感器等。

- 水轮发电机组，一般包括水轮机、发电机、调速器等。

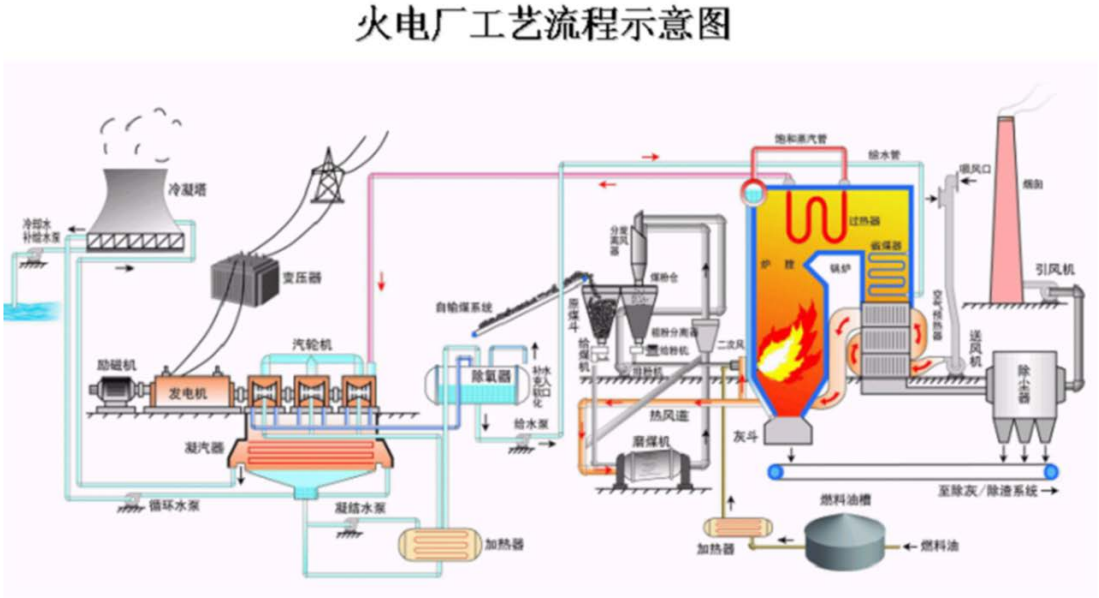


# 水力发电系统案例

- 梯调系统中的安全问题
  - 某纵向认证设备，用户名、密码明文存储在数据库中。
  - 某纵向认证设备，登陆界面存在格式化字符串溢出漏洞，导致设备重启。
- 船闸系统中的安全问题
  - 西门子S7-400 PLC存在安全认证问题，黑客可绕过上位机直接控制该PLC，恶意的CPU-STOP命令可关闭该PLC，导致船闸失控。
  - 西门子OSM交换机，snmp服务采用默认的口令admin/admin，web管理员界面的默认口令admin/admin、user/user、登陆可绕过。

# 火力发电系统架构

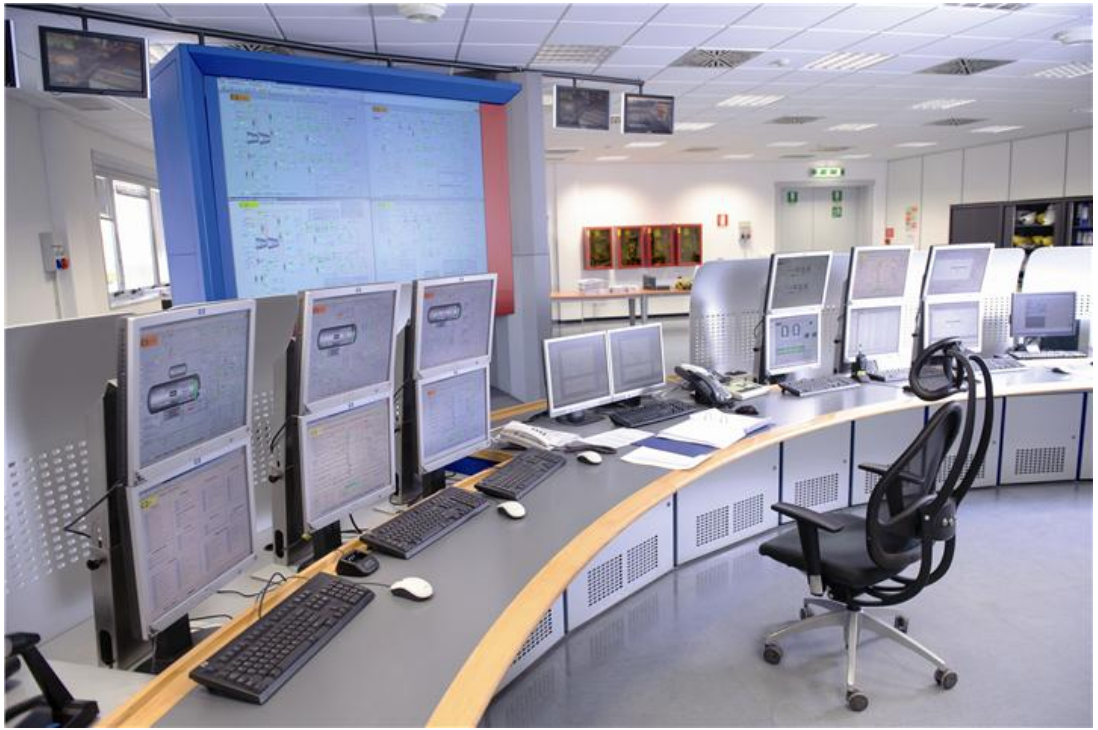
- 火力发电系统主要由燃烧系统（以锅炉为核心）、汽水系统（主要由各类泵、给水加热器、凝汽器、管道、水冷壁等组成）、电气系统（以汽轮发电机、主变压器等为主）、控制系统等组成。



# 火力发电系统案例

- ABB Symphony系列DCS通讯协议存在设计缺陷
  - 攻击者也能够进行重放攻击改变DCS的工作模式，从而影响工艺的正常运行造成非常严重的后果。

- ABB Symphony系列DCS拒绝服务漏洞
  - 该漏洞被利用将导致IET 800卡件瘫痪并自动重启。在重启过程中所有的以太网数据交互都将受到影响。



# 行业典型案例分享

北京威努特技术有限公司

# 目录

现场案例部分由于涉及客户敏感信息
不在公开文档发布，请谅解

# 目录

# 典型问题分享：从“拒绝服务”到“安全稳定”

## 项目背景

XX油田作为国内名列前茅的油田公司，其已探明的油气储量和每年的油气产量在国内具有举足轻重的战略地位。一直以来，该公司在工业控制系统的安全方面也高度重视，力求打造油田行业的工控安全标杆项目。

在完成整体的工控系统纵深防御之后，系统也一直稳定运行。

## 问题描述

油田公司某分厂有一个控制器需要增加读取点数，信息中心的工程师进行加点操作，此时更改控制逻辑可以正常进行，但采集数据的动作却没有成功，通过工程师站查看数据存在坏点。工程师又通过ping控制器的方式发现控制器没有响应，对应的通道已坏死，无论如何操作都无法恢复，只能冷重启控制器。

# 典型问题分享：从“拒绝服务”到“安全稳定”

## 问题分析

XX油田所使用的控制器（国外品牌）安全系数较低，在 没有安全防护的情况下，且不说存在数据非法采集的问题，单就增加数据采集的点数而言，用正常速率建立会话连接，当连接数增加到2500左右时，必然导致拒绝服务，最后只能通过冷重启来释放连接，如果遭遇Pingflood之类的攻击更是毫无抵抗之力。

## 补充说明

从我们做实际项目的经验和漏洞挖掘的实验情况来看，工业控制设备的自身安全性问题比较多，涉及到处理能力、漏洞、后门等，工控安全中对控制设备的安全防护是一个非常重要的方面。

# 典型问题分享：从“拒绝服务”到“安全稳定”

## ■现场问题解决：

通过开启防火墙的并发连接数控制的方式来提高控制器的安全系数，并且在防火墙上配置会话老化时间，在白名单防护的同时，给原通信双方发送reset报文，在合理阻断非法的采集请求的同时，保证控制器的正常服务能力。

## ■问题根源解决：

这个问题是一个典型的工控设备通信健壮性不足的问题，而这恰恰也是当前工控设备普遍存在的现象。使用专门针对工控设备进行通信健壮性测试的漏洞挖掘类工具，去挖掘设备未知的漏洞，进而促使工控设备厂商去修补漏洞，这样能从根源上杜绝类似问题发生，防患于未然。越早发现问题，安全的代价就越低。

# 典型问题分享：工业现场“扫毒”记

## 项目背景

除了电力、石化等国家基础工业领域，与民生密切相关的市政系统也分布了大量的工业控制系统，做好这部分的安全防护工作，同样意义重大。

某燃气公司经过长时间技术交流和对比测试后，最终选择了成熟的工控安全解决方案来保障生产的安全与稳定。

## 问题描述

现场所有的操作员站和工程师站平时通过网络共享或U盘拷贝文件，但没有安装任何安全软件，在查毒过程中都发现有病毒感染，其中部分病毒（马吉斯病毒）还非常顽固。由于控制软件授权昂贵，任何情况下遭到破坏，都需要重新采购，这也给杀毒工作也带来风险。

# 典型问题分享：工业现场“扫毒”记

## 根源分析

工业现场的相对封闭性，使得补丁升级、病毒库升级变成一件很复杂的事情，在这种情况下，只要没出大问题，能用的东西就会一直用下去，因此从工业现场找到一个很原始的操作系统版本或者找到一个很古老的病毒样本都是一件很简单的事情。

工业控制相关的软件都是专业软件，和传统防病毒软件在兼容性方面测试不够充分，因此这也是造成工业主机爱“裸奔”的一个重要原因，甚至有部分工业控制系统生产商明确告诉客户：“如果因为安装了某某防病毒软件导致系统异常，我们概不负责。”

# 典型问题分享：工业现场“扫毒”记

**杀毒过程**

技术专家在实验室内反复试验，最终通过如下过程中能彻底清除马吉斯病毒：

- 下载如下四个软件：360顽固木马专杀工具、超级巡警、SRENG、瑞星专杀MagistrKiller。
- 重启按F8进入安全模式，安装MagistrKiller后运行查杀。
- 360顽固木马专杀工具查杀。
- 手动删除C盘\WINDOWS\AppPatch目录下的AcLua.dll和AcSpecfc.dll文件，\WINDOWS\system32\drivers下的eth8023.dll文件。
- 打开SRENG,安装运行,然后删除LINKINFO.DLL驱动。
- 重启后，打开360安全卫士，结束explorer.exe进程。用360安全卫士查杀恶意软件，这时linkinfo已经可以杀掉了。
- 用超级巡警和360安全卫士再次查杀。

# 典型问题分享：工业现场“扫毒”记

**解决方案**

- 基于“白名单”思想的主机防护软件是解决上述问题一剂良药，具有**低开销、全兼容、无需升级病毒库文件**等优势。
- 移动存储设备的管控功能、配套安全U盘等技术手段也能解决客户现场数据交换的需求。

长期以来，病毒问题是困扰工业控制系统主机的一个棘手问题，从大名鼎鼎的震网病毒到2015年岁末的BlackEnergy，这些如鬼魅般游荡在工业控制系统网络中的杀手总是伺机而动。

# 现场常见工控安全问题分享

01

工业控制
网络安全问题

02

工业控制
设备安全问题

03

工业控制
主机安全问题

04

安全管理制度
与安全意识问题

# 工业控制网络安全问题

## 1 生产网与办公网互通

- 生产网络与办公网络没有有效的隔离手段，在一些业务分散、站点较多的行业比较普遍。

## 2 链路共享、数据混合

- 视频监控和数据采集共用通信链路，数据流量混合，行业特点同上。

## 3 保留远程维护通道

- 技术人员为了方便，保留远程维护的通道；管理人员为了移动办公，远程访问重要数据。

## 4 专业审计系统缺失

- 普遍缺少专业针对工控系统的审计工具，传统审计工具无法解决工控系统的审计需求。

# 网络安全--案例 I

**案例描述**

- 某民营电厂为方便领导实时掌握生产信息，将重要的生产管理服务器违规接入互联网，而同时该服务器又和生产控制系统、办公网络互连。在现场安全检查时，发现该服务器有活跃的境外IP访问，并且有数据的交互。

**问题思考**

- 领导实时掌握生产信息的初衷是好的，但是在没有做好有效的安全防护之前，这样的设计就无形中将内部的生产系统完全暴露在公网之上，为恶意的访问和网络攻击提供了便利，工业数据上网是发展的趋势，但是前提是要做好合理的规划和全方位的安全防护。

**解决方案**

- 在互联网出口处部署安全设备，做好访问控制策略。
- 在生产网边界部署安全设备，防止工业数据的泄露。

# 网络安全--案例II

**案例描述**

- 某油田公司由于采油井数量众多并且地理分布较广，为了方便管理同时降低人工成本，在重要场站和油井现场部署视频监控系统，由此产生的视频流量和工控系统的数据流量共用链路。

**问题思考**

- 视频流量较大，而工控系统的数据流量相对较小但是最为关键。链路共享的情况下，一方面容易造成关键数据流量丢失，另一方面长距离、分布式的数据采集存在数据泄露和被篡改的安全隐患。

**解决方案**

- 网络改造，将视频和工控系统的数据流量通过不同的物理网络传输。
- 部署安全防护设备，防止数据被篡改和泄露。

# 网络安全--案例Ⅲ

**案例描述**

- 某新能源企业由于生产现场地理位置比较偏远，设备维护的工程技术人员了方便操作，违规保留远程维护通道，有安全检查时，就将通道临时关闭，打游击战。

**问题思考**

- 从降低成本、及时响应的角度来说，远程维护通道的保留也无可厚非，但是从安全管理的角度来说，这就是非常大的安全风险。

**解决方案**

- 在工控系统部署审计设备，记录相关的访问操作、网络会话、数据流量等。
- 在生产网边界部署防护设备，防止非法访问工控系统及工业数据的泄露。

# 工业控制设备安全问题

## 1 控制器处理能力弱

- 通常来讲，很多工业控制设备的性能一般，处理能力较弱。现场典型案例分享中的控制器“拒绝服务”就是这个问题的有力证明。

## 2 控制器漏洞和后门

- 由于设计和实现上的不足，绝大部分工业控制设备存在不同程度的漏洞；由于人为的因素，部分设备甚至预留后门。

## 3 关键控制设备无防护

- 由于前期规划设计不够全面且重视不足，工业现场普遍缺少对控制设备的安全防护。

# 工控设备安全--案例

**案例描述**

- 在某电网研究机构进行的电网设备漏洞挖掘测试时，所有被测试设备均发现了漏洞，包括有协议栈设计缺陷、操作系统层面的漏洞、协议本身的设计缺陷等。在其他现场进行工控设备漏洞挖掘时，不论是电网中的控制设备还是自控领域的PLC设备，不论是国产设备还是国外设备，都能或多或少发现不同程度的漏洞。

**问题思考**

- 工业控制设备和工业控制协议从设计之初就对安全考虑不足，同时自身的脆弱性，各种漏洞和后门的存在，让安全隐患如同一把悬在头上的利剑。

**解决方案**

- 设备入网前要进行通信健壮性测试，即做漏洞挖掘的工作，让问题提前暴露。
- 部署防护设备，通过对工业协议的深度解析和指令级控制，对关键控制设备进行防护。
- 部署防护设备，对工业数据传输进行防护和控制，避免数据的泄露。

# 工业控制主机的安全问题

## 1 主机病毒感染

- 移动存储设备无序使用，生产/办公网隔离不到位，都会造成工控主机病毒感染。

## 2 非法软件安装

- 操作人员违规安装非工作必备软件，如游戏软件、即时会话软件等。

## 3 操作系统老旧

- 工业现场一方面是操作系统普遍落后于当前主流，另一方面是不会及时打补丁。

## 4 安全防护失位

- 无任何防护软件，安装但是病毒库升级不及时，或者由于软件冲突，防护功能关闭。

# 主机安全--案例

**案例描述**

- 某国有电厂操作员工作站上一方面有病毒感染，另一方面部分安装了游戏娱乐软件。
- 主机USB接口贴有封条，但是形同虚设，需要时就会揭开使用。

**问题思考**

- 非法软件的安装从某种意义上来说和感染病毒是一样的，都会对工控主机造成巨大的潜在威胁。
- 为了寻求工作的方便性，移动存储设备的管控是防不胜防。

**解决方案**

- 部署基于白名单思想的主机防护软件，只允许合法的、必要的程序运行。
- 对U盘进行管控，同时配合专用的安全U盘，实现数据交换的需求。

# 安全管理制度与安全意识问题

## 1 安全管理制度缺失

- 很多工业企业没有完善的安全管理制度和安全应急制度。
- 管理制度名严实松，从指导思想上对信息安全管理产生松懈。
- 责任落实不到人， 缺少相应岗位支撑安全管理。
- 安全管理者存在“制度快递员”的问题，将文件转发了事。

## 2 人员安全意识不足

- 对工控安全的认识不够导致大多数人对工控安全是什么还比较模糊。
- “无过便是功”的思想长期主导，导致企业没有出问题便认为没有问题。
- 信息安全会导致生产安全的思想还浮于表面，未深入心智。
- “我是管生产的”信息化的那点事情与我无关的思想还根深蒂固。

# 制度&意识--案例

**案例描述**

- 在配合执法部门进行安全检查时，在多个行业的现场发现：工控系统的安全管理制度不完善是个普遍问题，人员的安全意识也亟待提升。
- 曾经在不同的工业现场发现重要的密码贴在桌面或者电脑机箱上。

**问题思考**

- 首先就是对工控安全的紧迫性和重要性认识不足。
- 其次技术人员在工控安全方面的技术水平需要加强。

**解决方案**

**工控安全培训**

- 提高工控安全意识
- 掌握工控安全防护方法

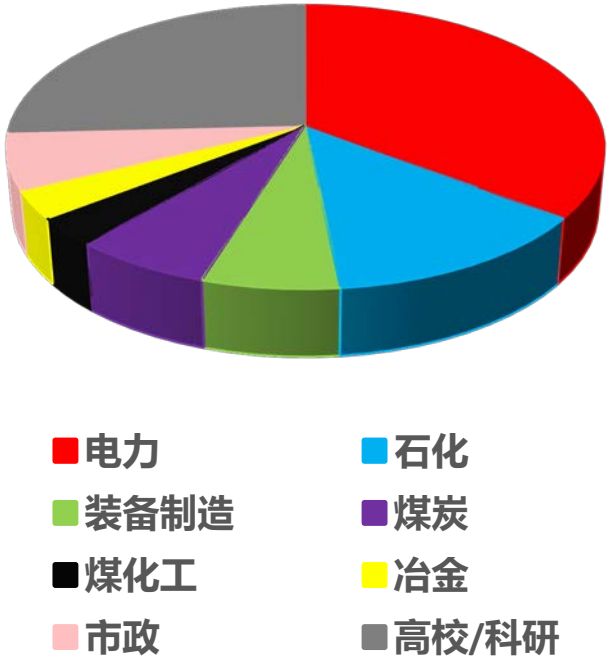
**工控安全评估**

- 识别工控安全风险
- 制定标准/制度/流程

# 目录

# 威努特工控安全项目实施总结

- 截至目前，威努特已经完成近百个工控安全项目实施。
- 国家关键基础工业领域：电力（含发电、电网）、石化（含采油、炼化、输油）、煤炭、煤化工、装备制造、冶金等行业，部署产品主要包括统一安全管理、工业防火墙、监测与审计系统、工控主机卫士等。
- 市政民生领域：包括天然气、污水处理等行业，部署产品主要包括统一安全管理平台、工业防火墙、监测与审计系统、工控主机卫士等。
- 高校、科研机构、测评机构：部署产品主要包括工控安全攻防实验平台、谛听、天鉴、天睛等。



# 专注工控 捍卫安全

- 无论是落地案例的数量，还是工业行业的覆盖率，威努特都处于工控安全领域的领先地位。

- 在项目实施的过程中，广泛听取工业客户和合作伙伴的意见和建议，在不断提升产品和解决方案水平的同时，力求打造工控安全的全生命周期解决方案。

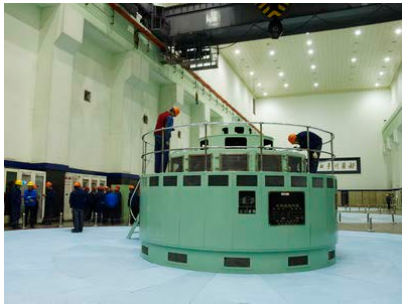
- 做好项目实施，更要做好客户服务，让工控安全真正从“被动防御” 走向“主动防护”。

# 主流工控安全产品及解决方案介绍

北京威努特技术有限公司

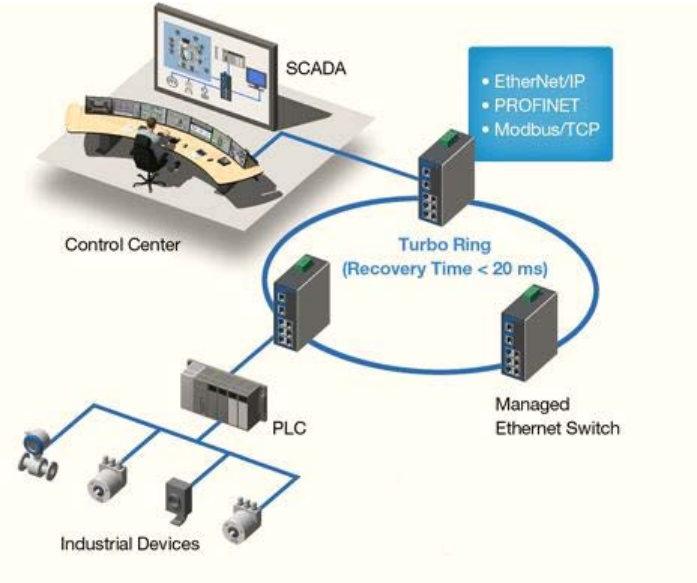
# 目录

# 应用场景分析



- 工业控制系统的工业现场环境更加恶劣（如低温、潮湿），这就要求工业控制系统中的信息安全硬件产品必须按照工业现场环境的要求专门设计,而不能与传统IT安全产品一概而论；
- 工业控制系统对报文时延很敏感，这就要求工业控制系统中的信息安全产品，必须从CPU选型、软硬件架构上做到低时延，这对当前一些基于X86 CPU及开源软件架构的传统IT安全产品是一个严峻挑战；
- 工业控制系统对网络的可用性要求高，这就要求工业控制系统中的信息安全产品必须满足一旦安全产品自身出现问题，不能影响网络畅通的要求。这与传统信息安全产品的“故障关闭”原则有很大区别。

# 产品技术分析

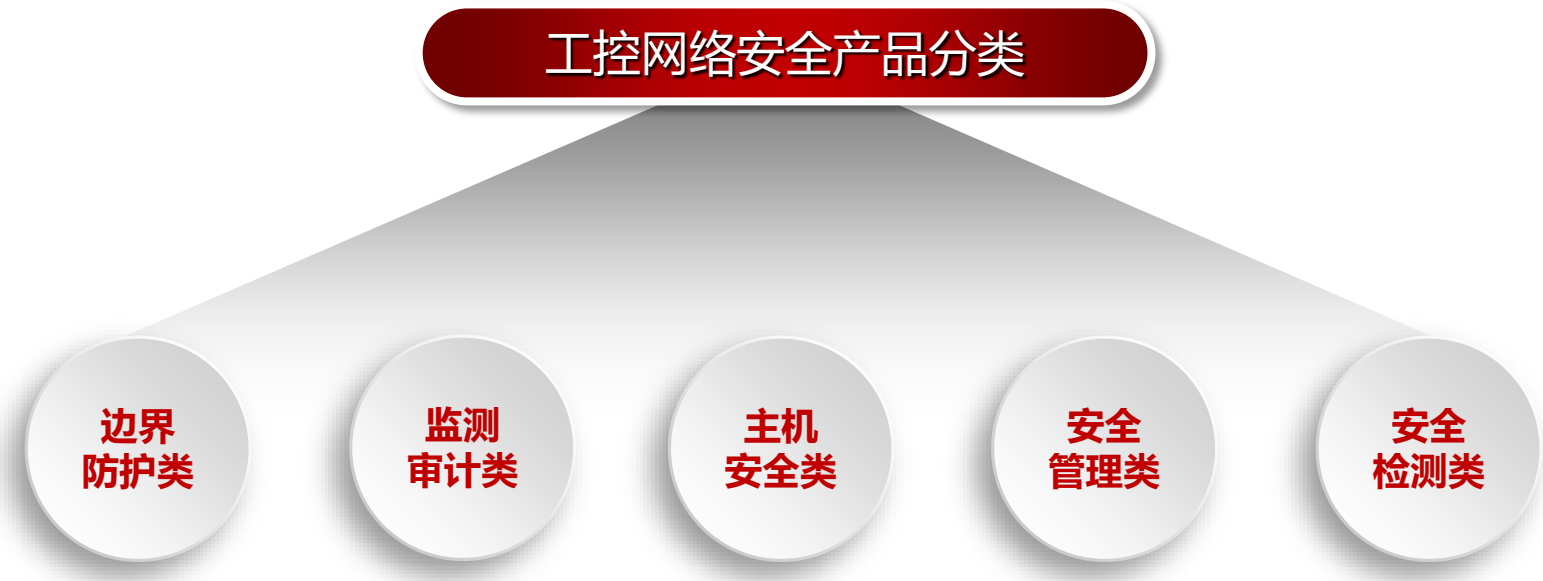



- 工业控制系统中更多是基于工业控制专有协议进行通信，这就要求工业控制系统信息安全产品必须支持工业控制通信协议（如OPC，MODBUS，DNP3，S7）；

- 传统的IT信息安全产品更多的需要通过不断的升级“库”来满足当前安全的需要（如反病毒软件、IDS入侵检测系统等），而工业控制系统不能接受频繁的升级，这就要求工业控制系统安全产品既不能频繁升级，还要能满足安全要求。

# 目录

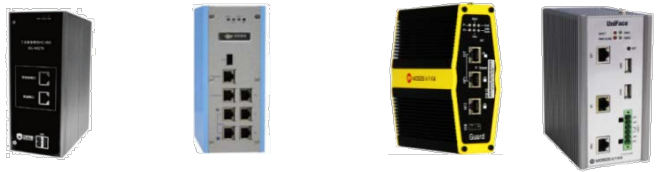
# 工控信息安全专用产品总述



# 边界防护类-工业防火墙

## 导轨式工业防火墙

威努特



## 机架式工业防火墙

威努特

- 此类产品多采用工业级的架构，采用低功耗、无风扇设计，来满足工业现场特殊的环境需求；
- 部署方式通常以串接方式工作，部署在工控以太网与企业管理网络之间、厂区不同区域之间，控制层与现场设备层之间。通过一定的访问控制策略，对工控系统边界、工控系统内部区域进行边界保护；
- 工控防火墙、工控隔离产品均属于边界防护类。

# 工业防火墙功能特点

## 传统防火墙基础功能

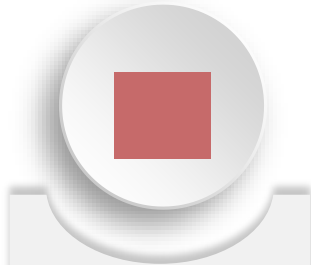
继承传统防火墙的基本访问控制功能，具备对源、目的IP，源、目的端口，协议类型5元组的控制能力

## 支持工业协议

能够对工业通信协议进行解析，如主流 的 OPC 、Siemens S7 、Modbus等协议的深度报文解析，弥补传统IT防火墙对于工业协议解析的空白

## 白名单机制

大多采用“白名单”机制对边界进行安全防护，即将信任的数据、协议放入到可信列表中，拒绝一切非可信任流量



## 更符合工业现场特点

一般支持学习、告警、阻断三种工作模式，符合工业用户对边界防护产品的心理需求

# 对工业防火墙功能认识误区

**对于工业防火墙，普遍存在下面2个误区：**

**1 工业防火墙就是传统防火墙换上工业外壳**

一部分用户会认为工业防火墙就是传统防火墙换了工业的外壳，功能没啥区别，换汤不换药，但实际上工业防火墙与传统防火墙在设计原则、工作机制、功能配置等方面有巨大差异，对工业协议的深度解析，对工业网络流量自学习建模的工作机制是工业防火墙独有的特点。

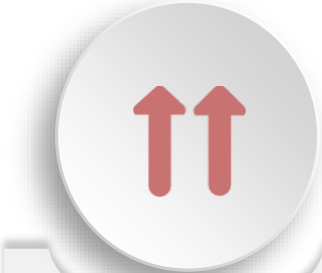
**2 过分依赖自学习，缺乏人工配置**

自学习确实是形成白名单的一种很好的方式，但却容易受到不固定因素的影响，如学习时间不足、部分业务数据只有在特殊的情况下才能产生，这些因素都直接影响白名单策略的完整性，所以自学习+人工配置形成的白名单策略才能更好的应用于工业现场。

# 边界防护类-隔离产品

- 隔离产品一般泛指网闸,目前在电力行业、石油行业应用较多，从功能角度可划分双向隔离网闸和单向隔离网闸；
- 部署方式通常以串接方式工作，部署在生产控制网与管理网之间。如部署在电厂的I,II区与III,IV区之间。满足通用工业控制系统由管理网与办公网之间单项传输的技术要求；
- 目前网闸产品因其功能的特殊性，仅适用于传统网络和工业网络的一些特殊场景。

# 网闸设备产品特点



## 架构特殊

网闸设备内部设置两套独立主机，每个主机运行独立的安全操作系统和应用系统，这两套主机分别通过网络连接生产控制区网络和管理信息大区网络

## 协议隔离

隔离装置的内外网主机之间不提供反向数据通道通信，可以阻断管理信息大区到生产控制大区通信途径，同时支持1bit返回模式，以进行数据验证

## 关键操作检测

隔离装置通过数据代理的方式来禁止生产控制区网络应用程序与管理信息大区应用程序之间进行直接连接，从而在一定程度上杜绝了病毒及木马携带传输的可能性

# 网闸VS工业防火墙

## 网闸产品

- 以安全为主，在保证安全的前提下，支持尽可能多的应用；
- 在安全方面，虽然对数据包进行了拆包处理，但对于数据的载荷部分未做深度解析，形成安全空白区；
- 对于数据的转发延迟性高，不适用于对数据传输低延迟性要求高的场景。

## 工业防火墙产品

- 防火墙是以应用为主、安全为辅，在支持尽可能多的应用的前提下，来保证使用的安全；
- 在安全方面，能够对数据包进行深度解析，甚至做到指令集解析；
- 对数据转发延迟性小，更适合工业网络环境。

网闸产品与防火墙产品无法衡量其好与坏，更多的区别在于应用场景的不同，防火墙适用于多种业务场景，而网闸产品只适用于对数据延迟性要求不高的业务场景。

# 监测审计类

## 导轨式监测审计系统

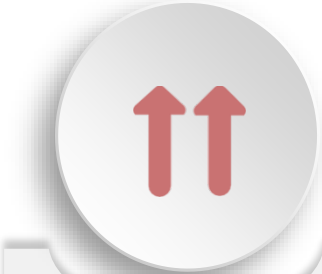
威努特

## 机架式监测审计系统

威努特

- 此类产品多采用工业级的硬件架构，采用低功耗、无风扇设计，来满足工业现场特殊的环境需求，如低温、高湿等；
- 此类产品通过镜像接口分析网络流量，及时发现网络流量或设备的异常情况并告警，通常不会主动去阻断通信；
- 旁路的部署方式，也使得这类产品不会因为自身的故障而影响工控系统的正常运行，这样的部署方式更容易让工业用户接受。

# 监测审计系统功能特点



## 自学习建立通信模型

利用白名单的方式，建立可信任的业务数据流模型，通过该模型来判断通信的合法性。部分工控协议的解析为指令级,对于工业现场来说，意义较大，可以脱离于系统原有厂商的监控系统，作为第三方监控手段对事后追溯提供依据

## 无需更新特征库

利用白名单的方式，摆脱原有IT系统中涉及的IDS，IPS需要不断升级“库”来满足安全需求的束缚

## 关键操作检测

由白名单机制衍生出来的对工业现场业务中的关键操作（如对工程师站组态变更、操控指令变更、PLC下装、负载变更等）违规报警、无流量，异常流量报警等更加符合工业现场需求

# 对监测审计系统的认识误区

**对于监测审计系统，普遍存在下面2个误区：**

**1 仅是换了一个工业外壳**

与工业防火墙面临同样问题，一部分用户会认为监测换了工业的外壳，功能没啥区别，换汤不换药，但实际上其设计原则、工作机制、功能配置等方面有巨大差异，对工业协议的深度解析，对工业网络流量自学习建模的工作机制是工控监测审计独有的特点。

**2 监测审计平台需要额外的监测管理平台管理**

在很多业务场景中，如管道、市政燃气等很多部署设备的位置都属于无人站，难以采用人工的方式进行配置，通过统一的管理平台能够管理所有安全设备，同时避免重复性的投资。

# 主机安全类

**工控系统中的主机设备，如工程师站、操作员站等是工控系统的风险点，病毒的入侵、人为的误操作等威胁主要都是通过主机类设备进入工控系统。**

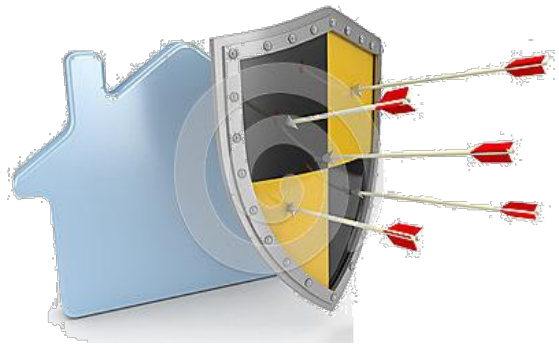
## 主流主机安全防护产品

**白名单防护类**

通过在主机上安装客户端程序，确保只有可信的程序、进程才允许运行，防止恶意程序的侵入；

**主机加固类**

结合等级保护合规性要求，对主机操作系统进行策略性安全加固，增强主机安全防护能力。



# 主机安全产品功能特点

## 白名单产品

- 采用「白名单」技术，为工作站即电脑主机创造一个安全可控的环境，主要功能是对可执行文件保护、U盘的使用控制等。因工业现场业务环境相对”确定”，所以白名单产品容易被工业用户接受，既防止了恶意程序的入侵，也避免的传统主机安全防护产品（杀毒软件）误差、漏杀的问题；
- 利用动态跟踪安装包安装技术自动将安装过程中的可执行文件或临时释放的临时可执行文件识别并添加到白名单库中，满足工业现场软件升级的需求。

## 加固式产品

- 加固式产品主要是对主机的内核级安全加固防护，通过对文件、目录、进程、注册表和服务进行的强制访问控制，制约和分散原有系统管理员的权限，把普通的操作系统从体系上升级，从而满足等级保护标准中对于主机安全的要求。

# 对主机安全产品的认识误区

**对于主机安全防护产品，普遍存在下面2个误区：**

**1 白名单软件或主机加固软件会不会也如杀毒软件一般，不适用于工业现场**

从原理的角度白名单软件是工作在操作系统层面的，是完全没有可能影响系统的运行；而主机加固软件是工作在驱动层面的，那么是否影响系统的运行，还要取决于硬件、软件的驱动。如出现驱动问题，也会出现影响系统运行的情况。

**2 也会存在扫描、查杀等动作，影响系统运行**

从工作方式、工作原理的角度，白名单软件和主机加固软件采用主动防御的方式，均不存在扫描、查、杀的动作，故不会出现影响系统运行的情况。

# 监测审计类-堡垒机

威努特

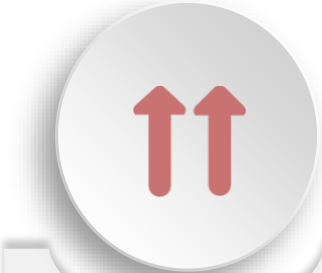
- 堡垒机一般部署在工业网络中管理大区，主要的作用是对运维人员维护过程的全面跟踪、控制、记录、回放，同时对自然人的身份进行统一授权；
- 在工业现场移动设备的交叉使用，把病毒、木马引入到原本脆弱的工控系统；运维人员的不当操作，引起生产事故，以及工控设备配置文件无备份。都给工控系统带来很大的风险，所以在此背景下，为有效解决工业控制系统现场运维风险，堡垒机应运而生。

# 安全管理类-管理平台

威努特 

- 安全管理类产品主要的用途是对部署在工业网络中的安全设备进行集中监测、统一管理，在工业网络中有诸多无人场景，如市政燃气、油田等行业现场均有无人值守站；
- 安全管理类产品一般部署在中心级测，如生产区的机房、管理区的机房，是非高温、非高湿的工作环境，所以安全管理类产品在设计时大多采用传统X86架构。

# 管理平台的功能特点



## 安全设备集中管理

集中管理工控网络中的安全设备，包括设备状态监控、拓扑管理、系统配置管理、日志管理等

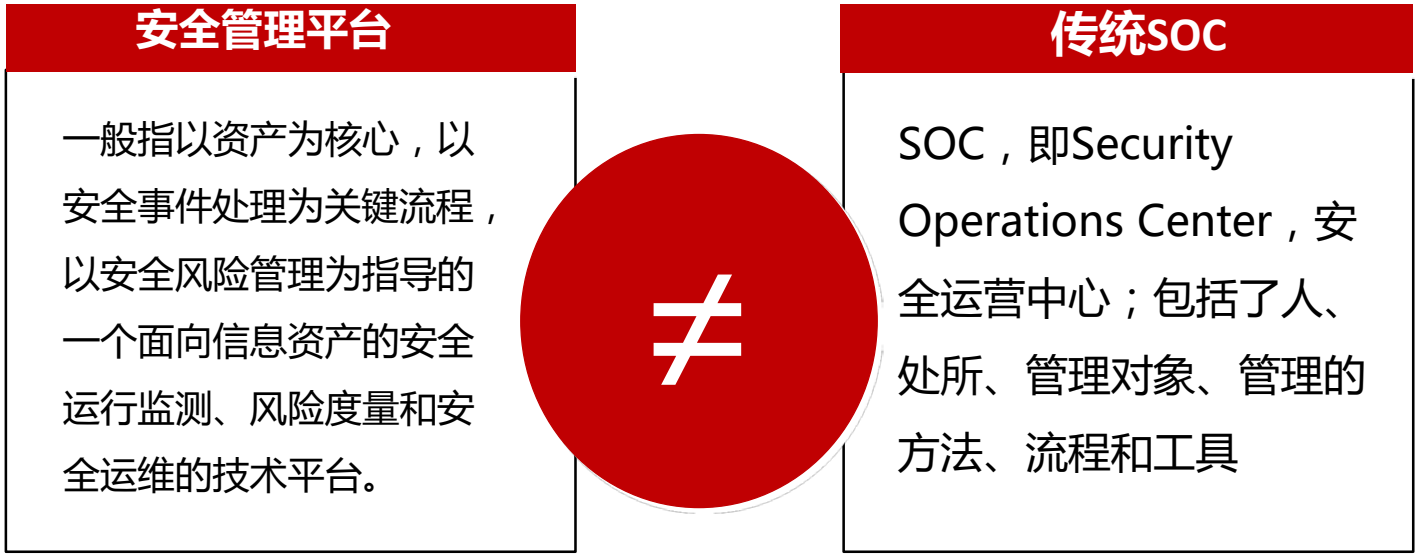
## 主机安全统一管理

统一管理工控网络中的主机安全软件，包括模板配置、策略下发、主机状态监测、日志管理等

## 日志管理分析

对工控网络中的安全日志（如：攻击日志、流量日志、访问日志、主机日志、系统日志）进行汇总、关联分析并形成报告，为工控网络安全事件分析和调查取证提供依据

# 安全管理平台VS传统SOC




总而言之，眼下安管平台不等于SOC，你可以将安全管理平台理解为SOC的一个部分，SOC的技术支撑平台。

# 安全检测类-漏洞挖掘&漏洞扫描

## 漏洞挖掘平台

威努特

## 漏洞扫描平台

威努特

- 漏洞挖掘和漏洞扫描产品均属于安全检测类产品，一些厂家将两者合一，以一个产品形态出现；
- 漏洞挖掘其存在的价值在于解决在工业控制系统潜在的未知漏洞，对SCADA系统、DCS系统、PLC控制器等工业控制系统、设备进行漏洞挖掘；
- 漏洞扫描其存在的价值在于检测工业控制系统的已知漏洞，可以支持对西门子、施耐德、GE等工控厂商的SCADA/HMI软件、DCS系统、PLC控制器进行扫描、识别，检测工业控制系统存在漏洞并生成相应的报告，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而在漏洞全面评估的基础上实现安全自主掌控。

# 应用场景

## 直连部署


## 桥接部署

# 漏洞挖掘VS漏洞扫描

**漏洞扫描产品**

基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算系统（主机、控制器等）的安全脆弱性进行检测，发现可利用的已知漏洞的一种安全检测（渗透攻击）产品。

≠

**漏洞挖掘产品**

基于模糊测试技术，通过向目标系统提供非预期的输入并监控输出中的异常来发现目标系统的未知漏洞的一种安全检测产品。

# 安全检测类-工控态势感知

习主席在419会议上提出要对关键信息基础设施进行通报预警，监管单位如经信委是有这方面的需求的。整体行业来看，工业和信息化部部长苗圩2017年2月在“2017工业互联网峰会”表示，工信部正在研究制定工业互联网发展路径，将进一步形成我国工业互联网发展的顶层设计。这也更加促进了“工控态势感知”的发展。

# 工控态势感知功能特点

## 工控网络资产在线探测

支持全球工控设备、网络设备、物联网设备、工控网络协议及常规服务的探测与定位

## 工控系统漏洞感知

实时发现全球互联网上暴露的工业网络漏洞数量，及其严重程度

## 全网威胁态势可视化

多维度展示扫描分析结果，并以地域图、柱状图、饼状图、雷达图等形式展现

## 工控网络安全态势感知

全面诊断工控系统协议、服务、漏洞及威胁分布，智能分析工控系统资产，客观评估网络安全态势

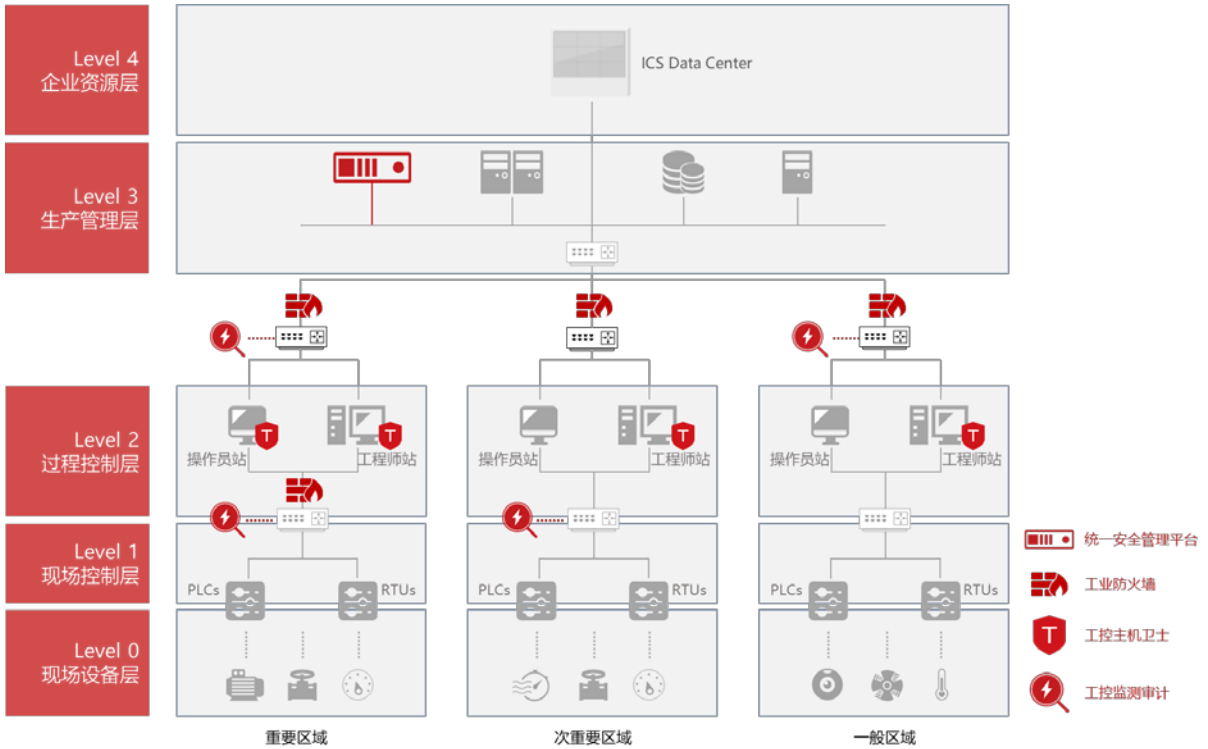
# 目录

# 工控安全解决方案模型

国内首家提出工业网络安全“**白环境**”解决方案体系的工控安全厂商，迄今已为上百家关键行业客户建立自主可控、安全可靠的工控安全整体防护体系

## 核心技术理念：

- 纵深防御
- 白名单机制
- 工业协议深度解析
- 实时监控审计
- 统一平台管理



# 工业控制系统“白环境”解决方案理念

**方案核心安全理念**

创新性提出了建立工控系统的**可信任网络白环境**和**工控软件白名单**的理念为客户构筑工控系统“安全白环境”整体防护体系，保护国家基础设施安全。

- 只有可信任的**设备**，才能接入控制网络
- 只有可信任的**消息**，才能在网络上传输
- 只有可信任的**软件**，才允许被执行

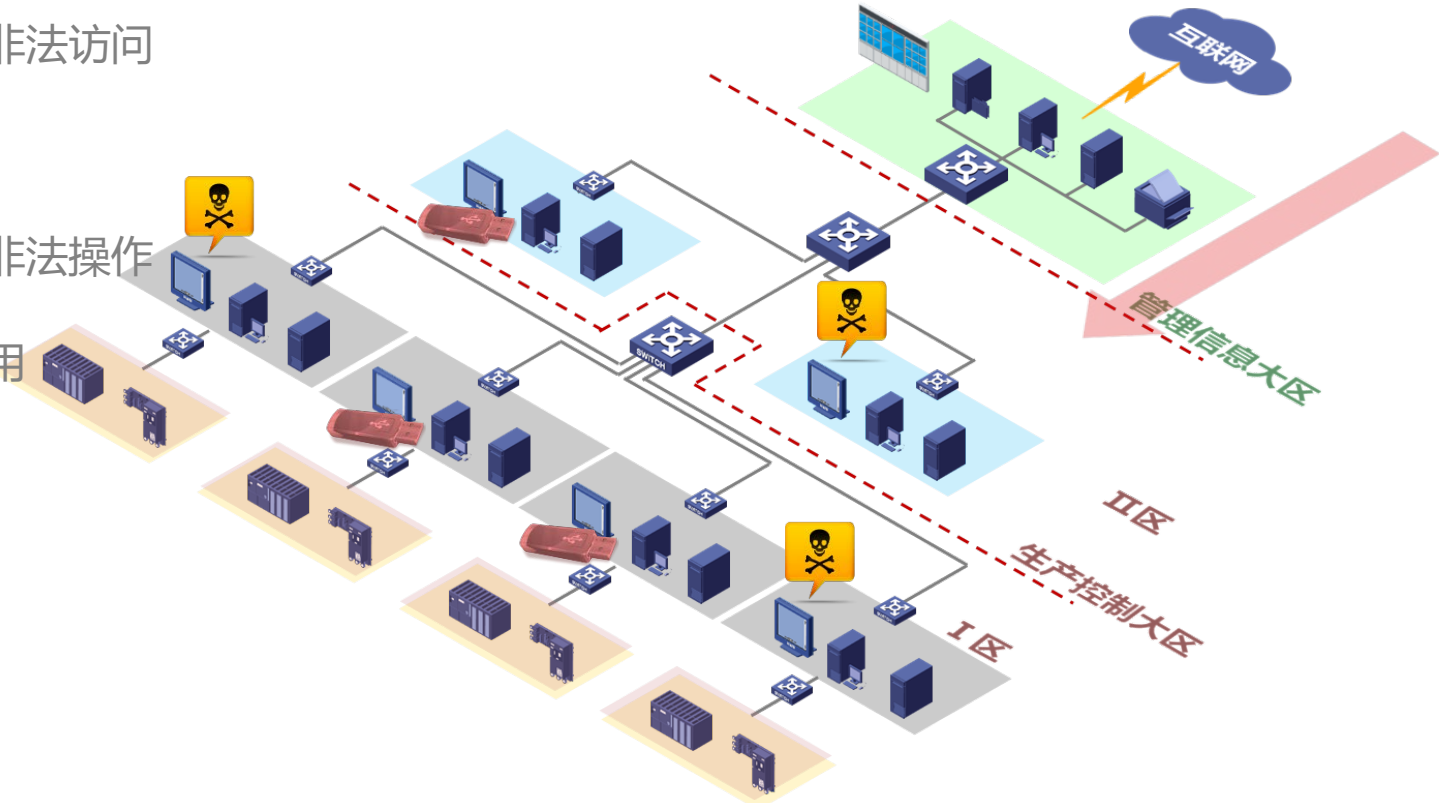
**技术亮点及创新点**

- 从“黑”到“白”
- 从“被动防御”到“主动防护”

# 浅谈电力行业网络安全解决方案

# 发电厂常见安全威胁

- 从互联网而来的非法访问
- 远程维护通道
- 用户有意无意的非法操作
- 移动存储介质滥用
- 针对漏洞的攻击
- ……



# 发电厂常见工控安全问题

- **我们的网络运行时间不短了，也没发生什么事情，不需要……，但从现场检查来看**
  - 生产控制区的传统防火墙策略基本为空
  - 现场存在远程维护端口或远程后门（如：TeamViewer软件）
  - 操作员站或工程师站能上互联网
  - 只有28%的主机安装了杀毒软件
  - 90%的杀毒软件未及时升级病毒库
  - 不少的上位机安装了与工作无关的软件（如：游戏、视频等）
  - U盘使用的控制，采用易碎贴封堵的算是情况好的
  - 部分发电厂已经发现如乌克兰电网事件的病毒样本，但用户全然不知
  - 不少电厂采用了已经明确报出漏洞的PLC等设备
  - ……

# 发电厂工控安全问题（一）

## 安全问题（一）

- **现场设备**：存在多种接入方式、基础和核心设备严重依赖国外产品和技术。
- **控制系统**：组成部件多、协议复杂，工业协议缺乏加密认证、运行环境存在大量漏洞和隐患并缺乏防护、缺少针对工业控制设备的信息安全检测手段、标准和方法。
- **监控信息系统**：体系架构缺乏基本的安全保障、控制人员缺乏网络安全意识。
- **网络边界**：边界隔离采用传统物理隔离，缺乏相应的访问控制策略，系统直接暴露在互联网上的风险较大。

# 发电厂工控安全问题（二）

- **安全问题（二）**
  - **嵌入式操作系统**：存在系统内核的漏洞、误操作或内部的破坏、数据窃取、数据篡改、假冒攻击、重播攻击、“拒绝服务”攻击和病毒攻击等问题 。
  - **HMI站操作系统**：操作系统不易更新、漏洞难打补丁。存在0day漏洞、系统提权漏洞、缓冲区溢出漏洞、UPNP漏洞、RDP漏洞等。
  - **实时数据库服务**：黑客通过B/S应用、基于Web窃取工控系统数据库中数据，数据泄露发生在内部，运维人员直接接触敏感数据。
  - **杀毒软件**：病毒库需要不定期经常更新，不适合于工业控制环境，且它对新病毒处理滞后。
  - **控制器** ：存在硬件和软件代码设计错误，如逻辑错误漏洞、副本安装、未使用的块及隐藏跳转等软件设计错误漏洞。

# 发电厂工控安全问题（三）

## 安全问题（三）

- **SCADA系统监控软件，仿真软件，OPC软件，网络管理软件以及在数据服务器、操作员站，工程师站上安装的应用软件：**软件种类多、漏洞多，存在SQL注入漏洞、跨站脚本漏洞、本地提权漏洞、缓冲区溢出漏洞和逻辑错误漏洞等软件安全问题。
- **安全管理策略和管理流程：**存在管理和技术障碍，安全策略和管理流程欠缺、有待完善。
- **通信协议：**协议存在拒绝服务漏洞、栈缓冲区溢出漏洞、缺乏有效认证，无授权等漏洞。
- **网络审计：**系统对网络安全性、可靠性有较大依赖，对实时性要求较高，实时控制网络缺少审计。
- **传输控制：**工控系统的数据和指令传输为明文传输、传统加解密算法复杂、执行时间长。

# 发电厂工控安全重点需求

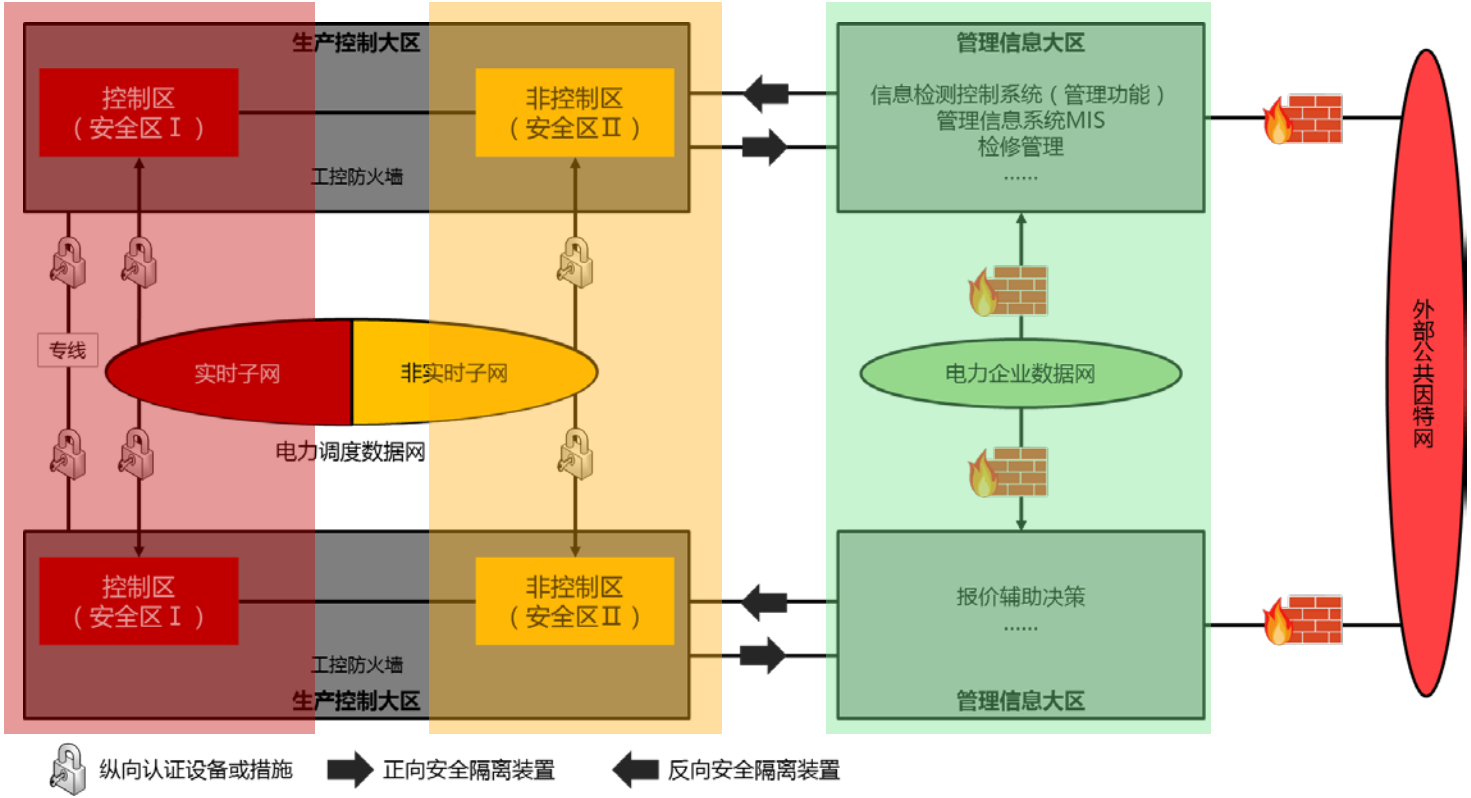
- 符合国能安全[2015]36号 发电厂监控系统安全防护方案要求
- 安全措施的引入不能影响工业生产的业务持续性
- 重点解决生产控制大区内部不同区域之间的隔离问题
- 重点解决上位机及服务器主机加固和防病毒问题
- 要有技术手段支撑用户了解工控网络整体安全状态，如日志、告警等
- 针对已经投产并存在漏洞的PLC等设备要采取有效的防护手段

# 发电厂常见安全措施

## 常见安全措施

- 生产控制大区和管理信息大区采用单向网闸隔离
- 与第三方接入（如：环保、安全等部门）采用单向隔离装置
- 部分主机安装了杀毒软件，但未及时更新病毒库
- 部分电厂针对生产控制大区采用了传统防火墙进行逻辑隔离，但效果平平
- 安全措施不完善，没有基于等保“一个中心、三重防护”进行建设
- 采用的安全产品不适应工业控制网络
- 安全建设核心思想依然沿用传统IT网络“黑名单”的方式

# 安全分区、网络专用、横向隔离、纵向认证



# 边界安全防护

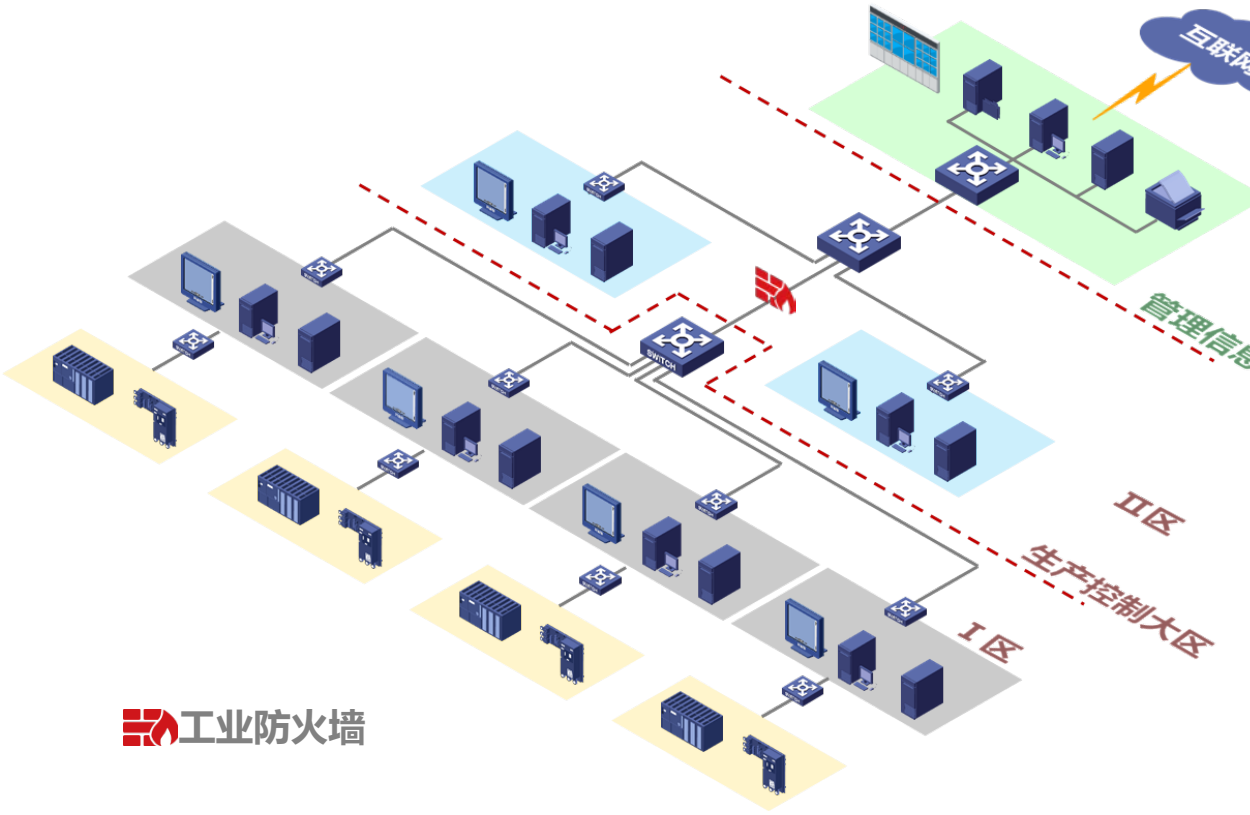
| 分类 | | 基本要求 |
| --- | --- | --- |
| 国能安全[2015]36号发电厂监控系统安全防护方案 **-4边界安全防护** | 4.1横向边界防护 | 4.1.1 生产控制大区与管理信息大区边界安全防护； |
| | | 4.1.2 控制区（安全区I）与非控制区（安全区II）边界安全防护； |
| | | 41.3 系统间安全防护<br>火电厂内同属于控制区的各机组监控系统之间、机组监控系统与控制系统之间、统一机组的不同监控系统之间，同属于非控制区的各系统之间，各不同位置的场站网络之间，采用一定强度的逻辑访问控制措施； |
| | 4.2纵向边界防护 | a）电厂控制大区系统与调度系统通过电力调度数据网进行远程通信时，采用认证、加密访问控制、加密等技术措施实现数据的远方安全传输以及纵向边界的安全防护；<br>b）参与系统AGC、AVC调节的电厂应当在电力调度数据网的边界配置纵向加密认证装置进行安全防护；<br>c）对于不具备建立调度数据网的小型火电厂可以通过远程拨号、无线等方式接入相应调度机构的安全接入区 |
| | 4.3第三方边界安全防护 | a） 火电厂控制大区中的业务系统与环保、安全等政府部门进行数据通信时，其边界应采用与生产控制大区与管理信息大区之间的防护方式进行隔离；<br>b） 信息管理大区与外部网络之间采用防火墙、VPN等保证边界数据传输的安全;<br>c） 禁止外部系统直接与生产控制大区的业务系统或设置采用远程拨号等方式直接访问，而不经过安全隔离 |

# 边界隔离（ Ⅰ区和Ⅱ区之间）

从Ⅱ区而来的非法访问，可能引起Ⅰ区实时网络的异常

部署对工业协议深度解析的隔离阻断装置实现网络分层分区，边界访问控制，避免无授权设备对区域的访问

部署对工业协议深度解析的隔离阻断装置实现基于通信“白环境”边界攻击防御和过滤



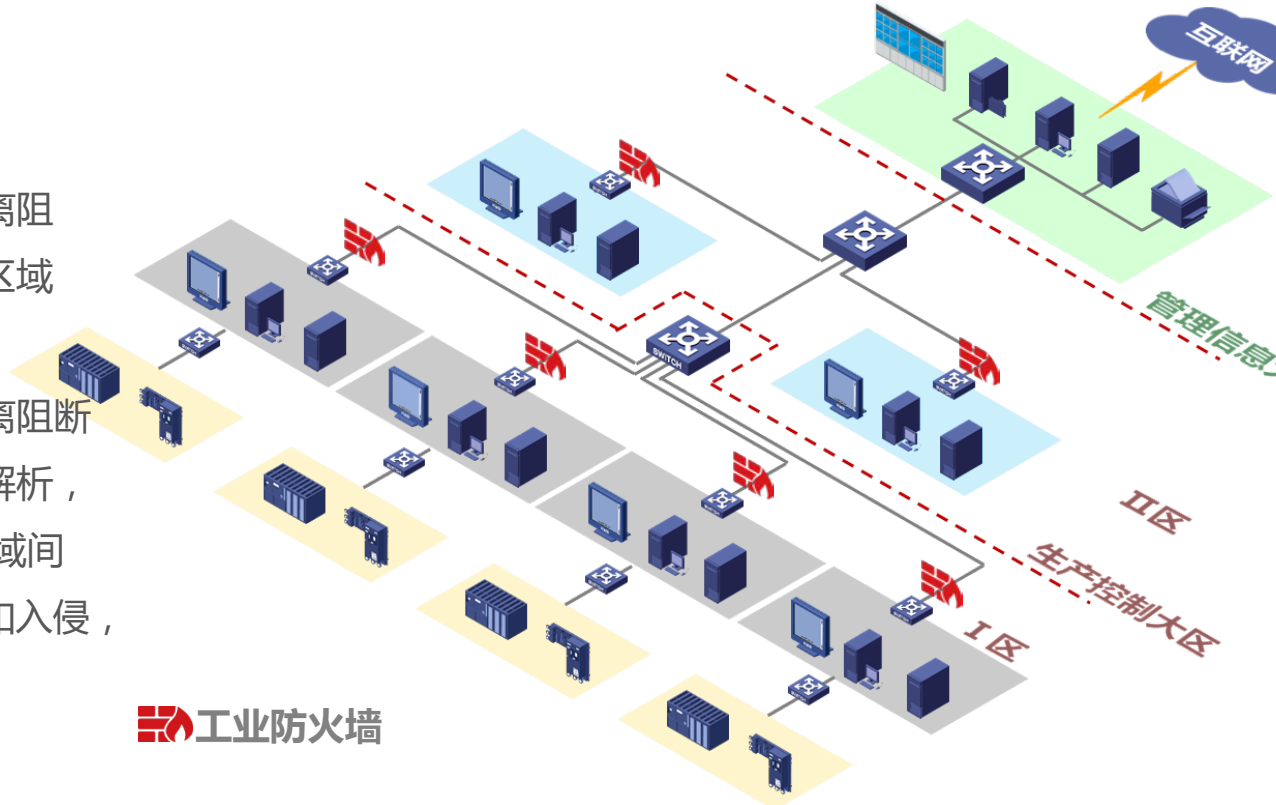
# 区域隔离（ 生产控制大区内部）

针对某个区域指定的非法攻击

区域内部问题影响至其他区域

部署对工业协议深度解析的隔离阻断装置实现基于区域和功能的区域网络划分及隔离

部署对工业协议深度解析的隔离阻断装置实现对工业专有协议深度解析，建立通讯“白环境“，阻止区域间的越权访问，病毒、蠕虫扩散和入侵，将危险源控制在有限范围内



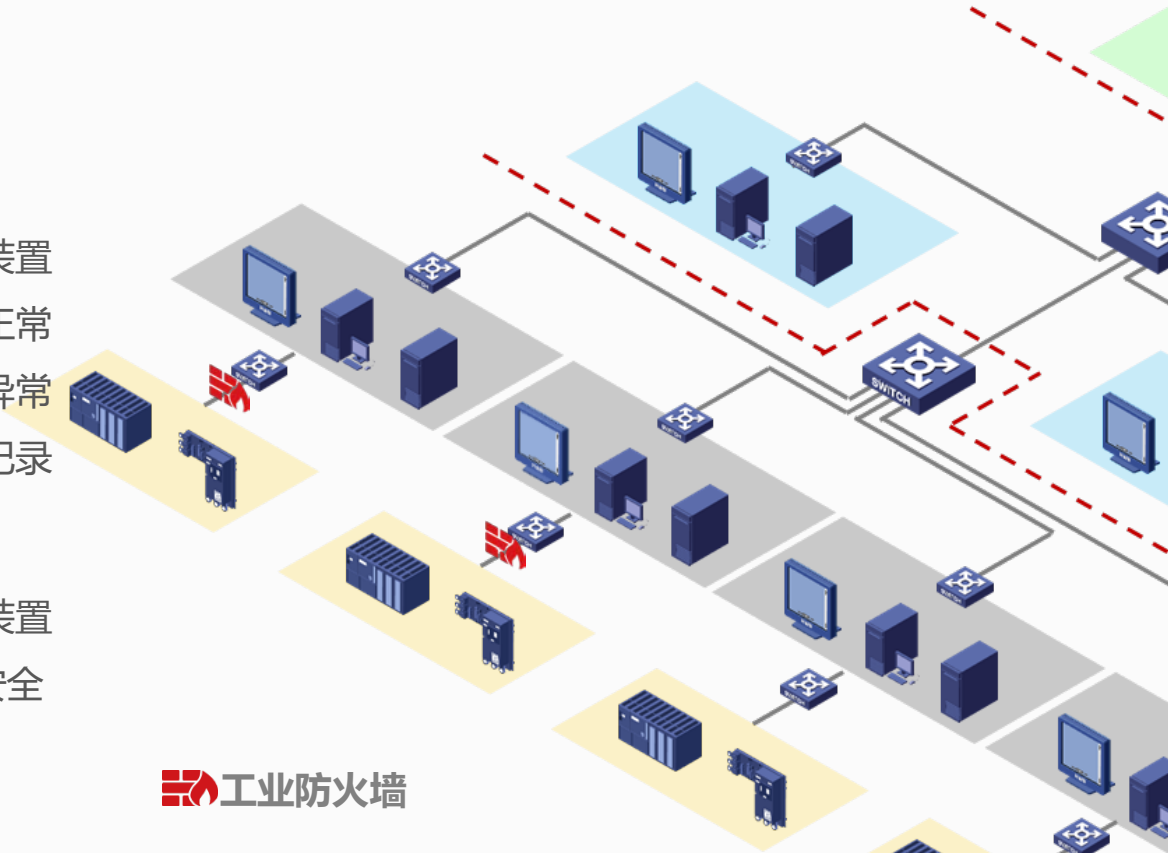
# 重要系统隔离

从上位机而来，针对重要PLC的攻击

操作员或工程师有意无意的非法操作

部署对工业协议深度解析的隔离阻断装置实现对工业专有协议深度解析，学习正常操作流量，建立通讯“白环境”，对异常流量和非法行为进行告警及阻断，并记录日志

部署对工业协议深度解析的隔离阻断装置实现针对PLC、DCS等工控设备已知安全漏洞利用等行为的阻断



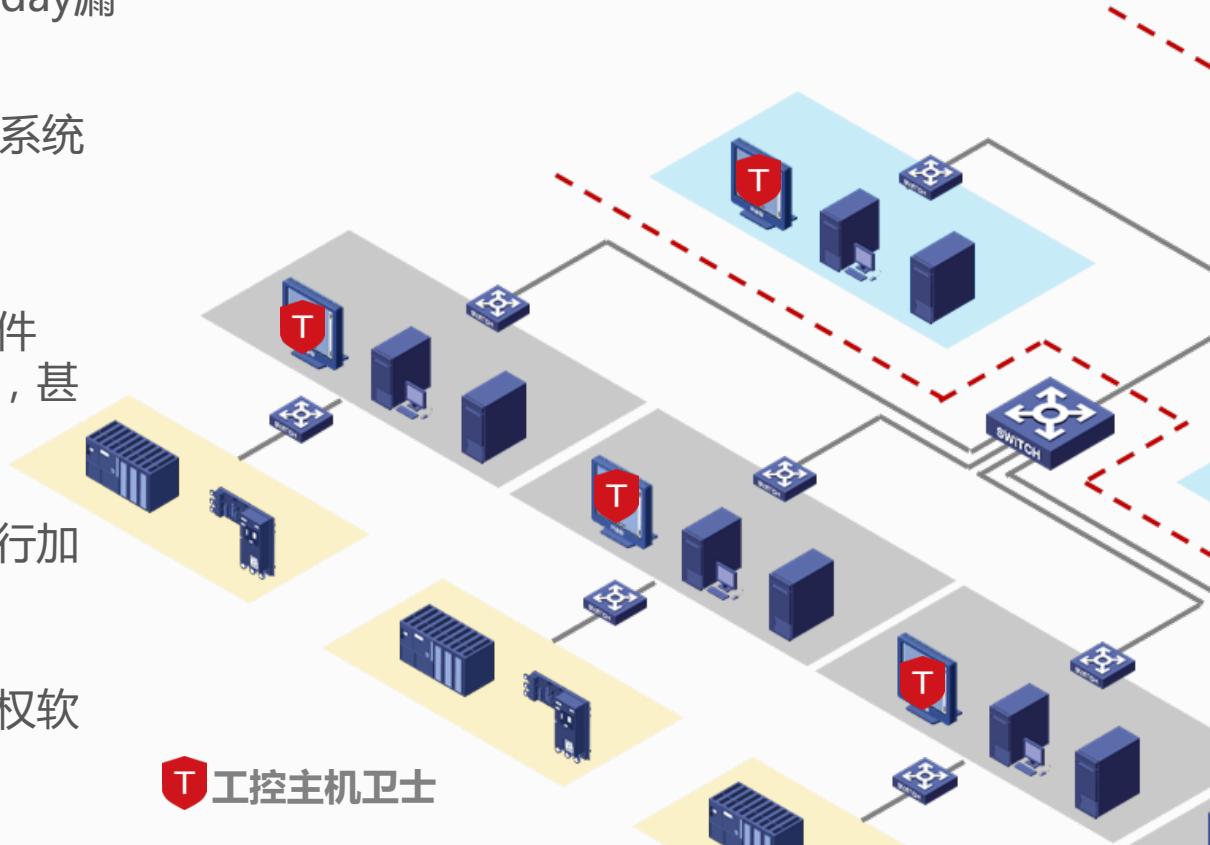
# 主机与设备安全防护

| 分类 | | 基本要求 |
| --- | --- | --- |
| 国能安全[2015]36号发电厂监控系统安全防护方案 **-5.2主机与网络设备加固** | 主机加固 | 发电厂厂级信息监控系统等关键应用系统的主服务器，以及网络边界处的通信网关机、web服务器等，应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专用软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当经过测试。 |
| | 网络设备加固 | a）非控制区的网络设备与安全设备应当进行身份鉴别、访问权限控制、会话控制等安全配置加固。可以应用电力调度数字证书，在网络设备和安全设备实现支持HTTPS的纵向安全web服务，能够对浏b）览器客户端访问进行身份认证及加密传输。<br>生产控制大区中除安全接入区外，应当禁止具有无线通信功能的设备；管理信息大区业务系统使用无线网络传输业务信息时，应当具备接入认证、加密等安全机制。 |
| | 外设管控 | 应当对外部存储器、打印机等外设的使用进行严格管理。 |

# 主机安全防护

- 病毒、木马感染上位机，甚至0-day漏洞的利用导致系统不可用
- 上位机系统安全策略缺失，引起系统或用户行为失当，导致安全风险

- 部署工控主机卫士建立可执行文件“白名单”，阻止恶意软件执行，甚至是0-day漏洞的利用
- 部署工控主机卫士对操作系统进行加固，如注册表、配置文件等
- 部署工控主机卫士实现阻止未授权软件的安装



# 综合安全防护

| 分类 | | 基本要求 |
| --- | --- | --- |
| 国能安全[2015]36号发电厂监控系统安全防护方案 **-5综合安全防护** | 5.1 入侵检测 | 生产控制大区可以统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计； |
| | 5.3应用安全控制 | 发电厂厂级信息监控系统等业务系统应当逐步采用用户数字证书技术，对用户登录失败处理功能，根据身份与权限进行访问控制，并且对操作系统行为进行安全审计。对于发电厂内部远程访问业务系统的情况，应当进行会话控制，并采用会话认证、加密与抗抵赖等安全机制。 |
| | 5.4 安全审计 | 生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为以及病毒和黑客的攻击行为。对于远程用户登录到本地系统中的操作行为，应该进行严格的安全审计。 |
| | 5.5 专用安全产品的管理 | 安全防护工作中涉及使用横向单向安全隔离装置、纵向加密认证装置、防火墙、入侵检测系统等专用安全产品的，应当按照国家有关要求做好保密工作，禁止关键技术和设备的扩散。 |
| | 5.7 恶意代码防范 | 应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应当经过测试。禁止生产控制大区与管理信息大区公用一套防恶意代码管理服务器； |
| | 5.8 设备选型与漏洞整改 | 发电厂电力监控系统在设备选型及配置时，应当禁止选用经国家相关管理部门检测认定并经国家能源局通报存在漏洞的风险的系统及设备；对于应经投入运行的系统及设备，应当按照国家能源局及其派出机构的要求及时进行整改，同时应当加强相关系统与设备的运行管理和安全防护。 |

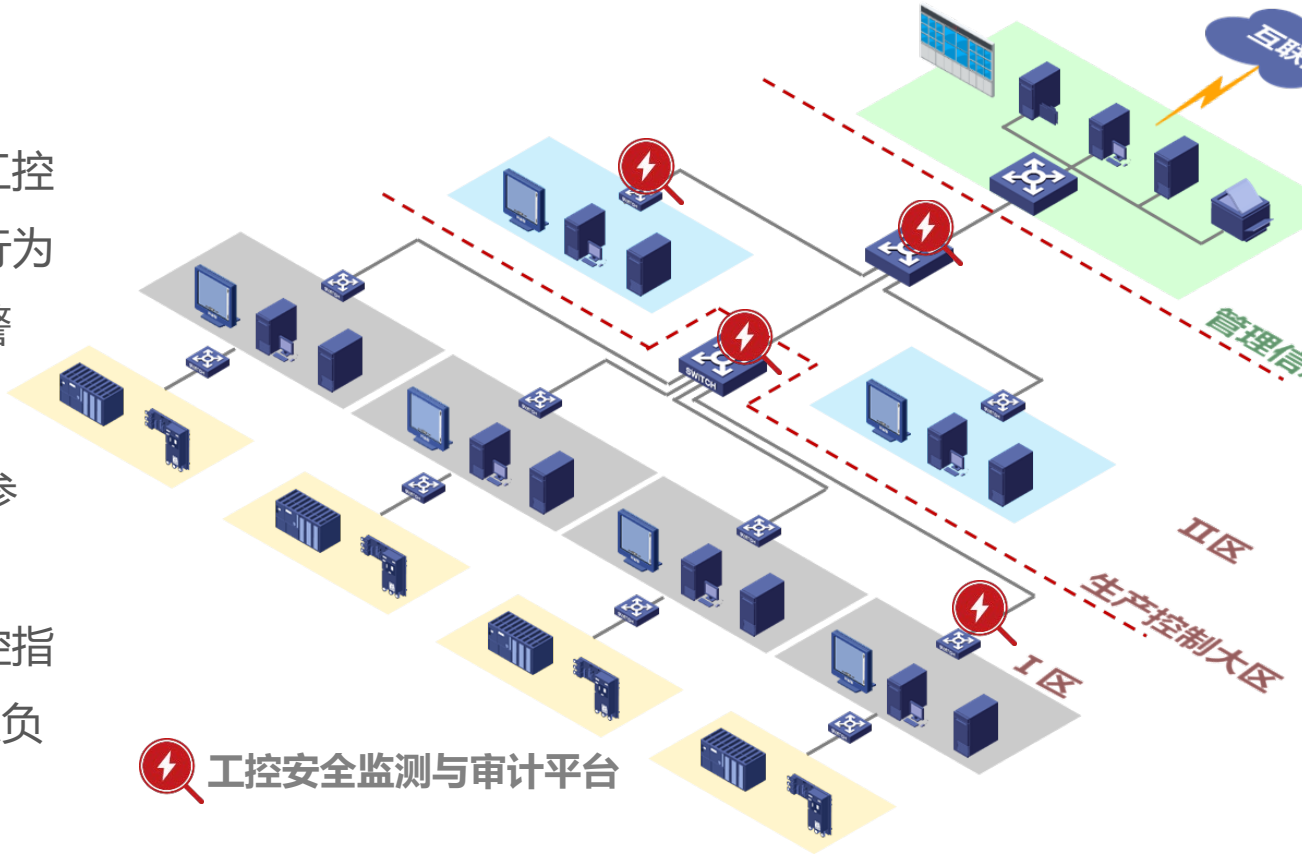
# 工控网络监测与审计

隐蔽不可知的恶意流量

部署监测与审计系统记录工控协议通信，建立正常通信行为模型，对异常操作进行告警

识别并检测工控协议攻击、TCP/IP攻击、网络风暴、参数阈值检测

对工程师站组态并更、操控指令变更、PLC程序下装以及负载变更等关键事件告警



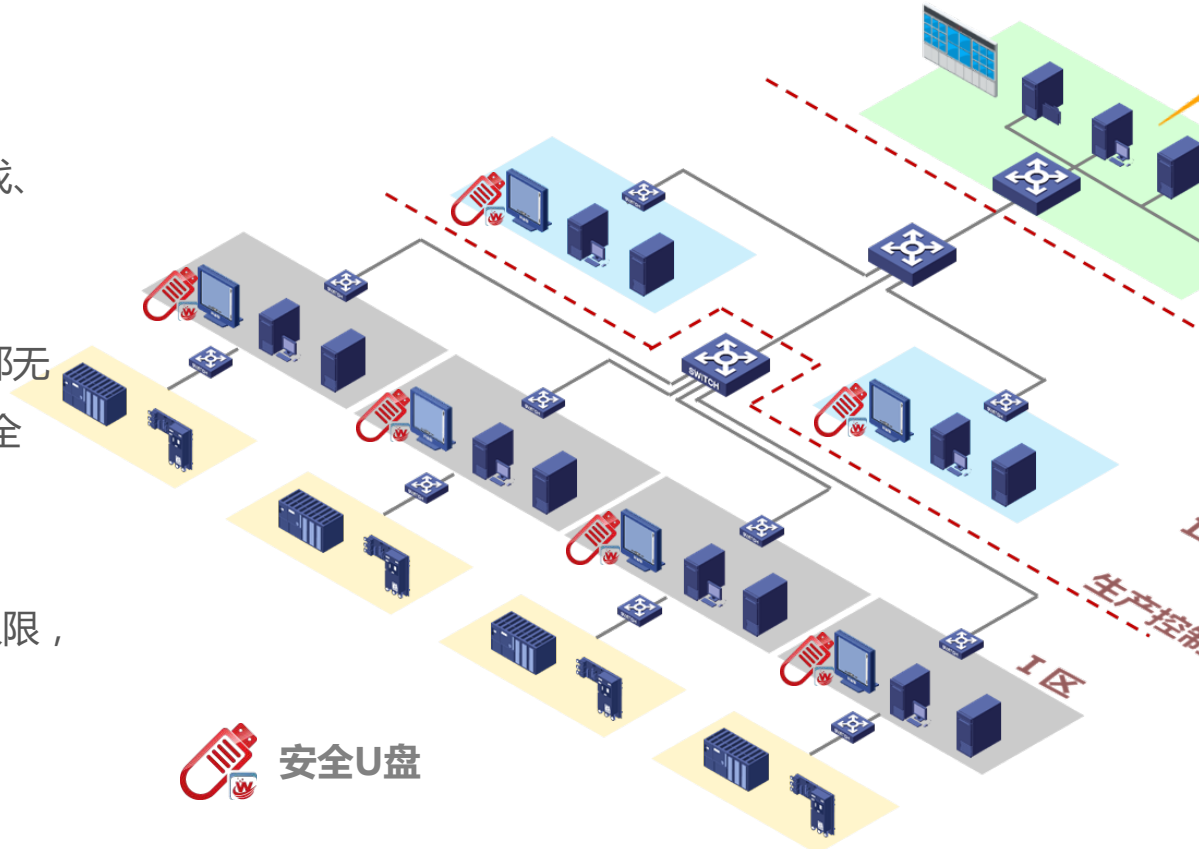
# 文件安全传递

普通U盘随意插拔，带来未知病毒等

通过U盘带入与工作无关数据，如游戏、视频、程序等，导致系统不可用

采用安全U盘，仅能在内部使用，外部无法使用，自带硬件安全芯片，数据安全存储

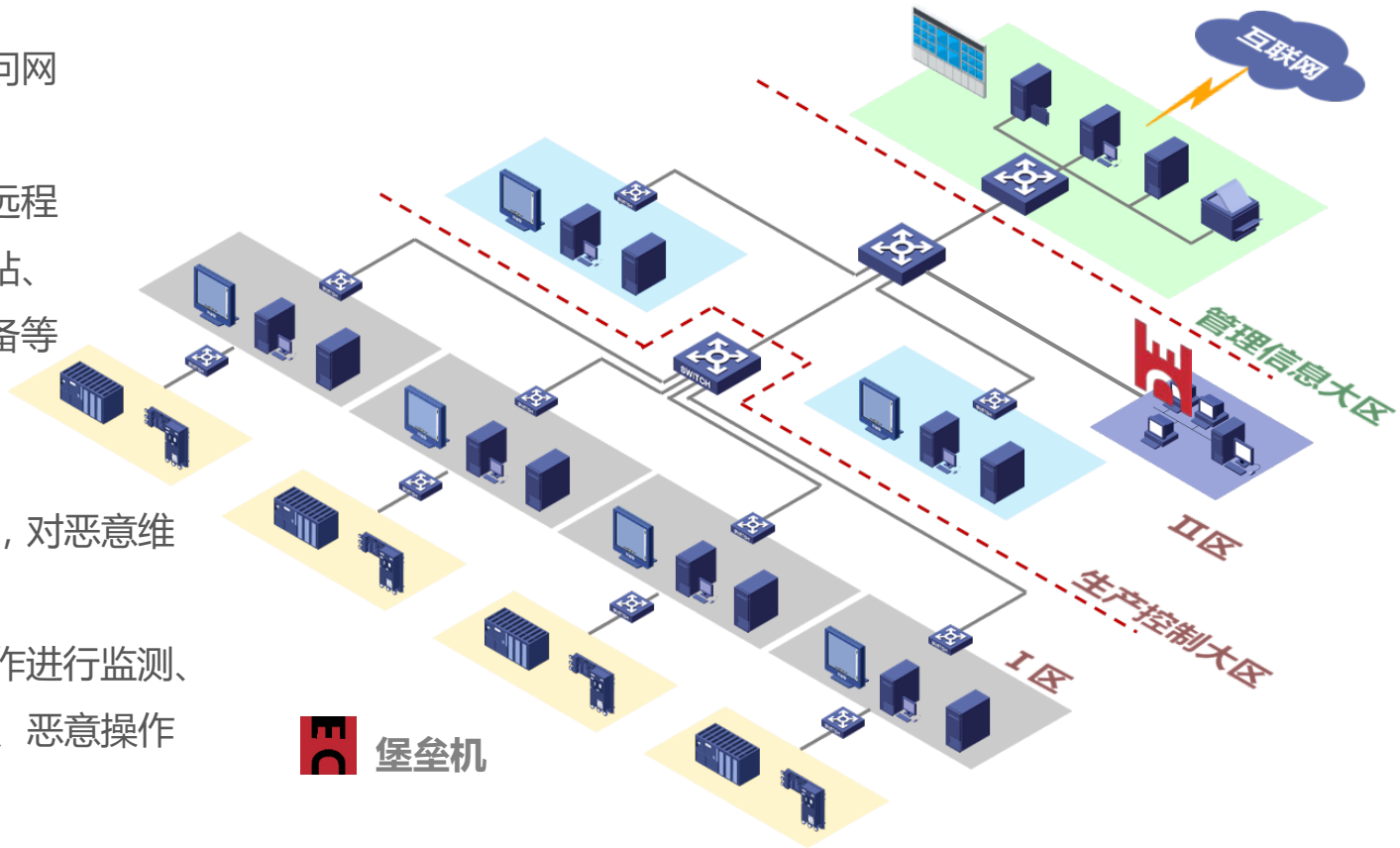
针对普通U盘，控制普通U盘的使用权限，包括禁止使用、只读使用、不控制



# 应用数据安全之网络设备防护&审计&身份鉴别

- 阻止非授权用户访问网络、安全设备
- 阻止非授权的用户远程维护服务器、工作站、网络设备、安全设备等

- 全程记录维护行为，对恶意维护行为进行取证
- 对远程维护行为操作进行监测、审计，阻止误操作、恶意操作



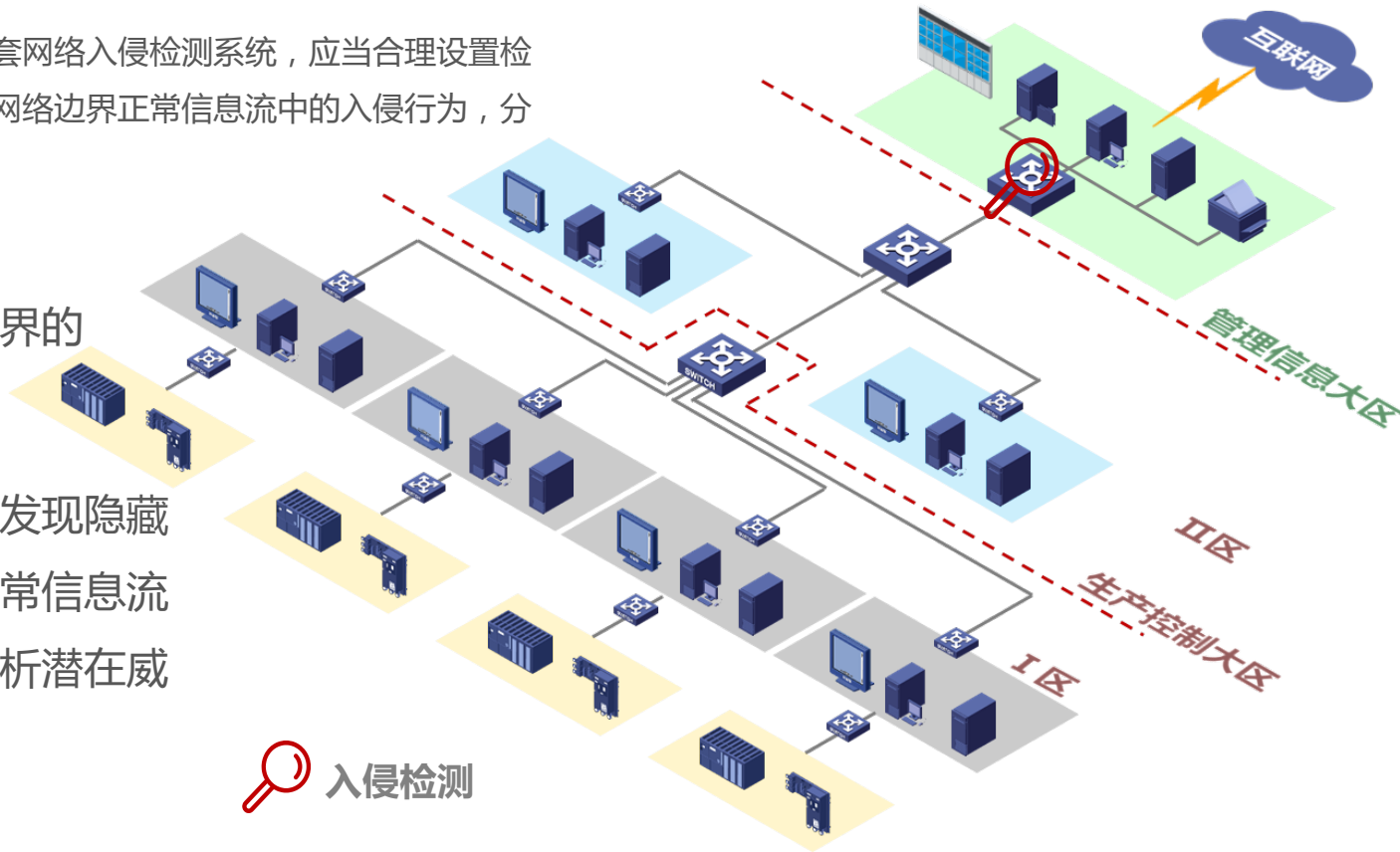
# 入侵检测

国能安全[2015]36号：

生产控制大区**可以**统一部署一套网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计

隐藏于流经网络边界的入侵行为

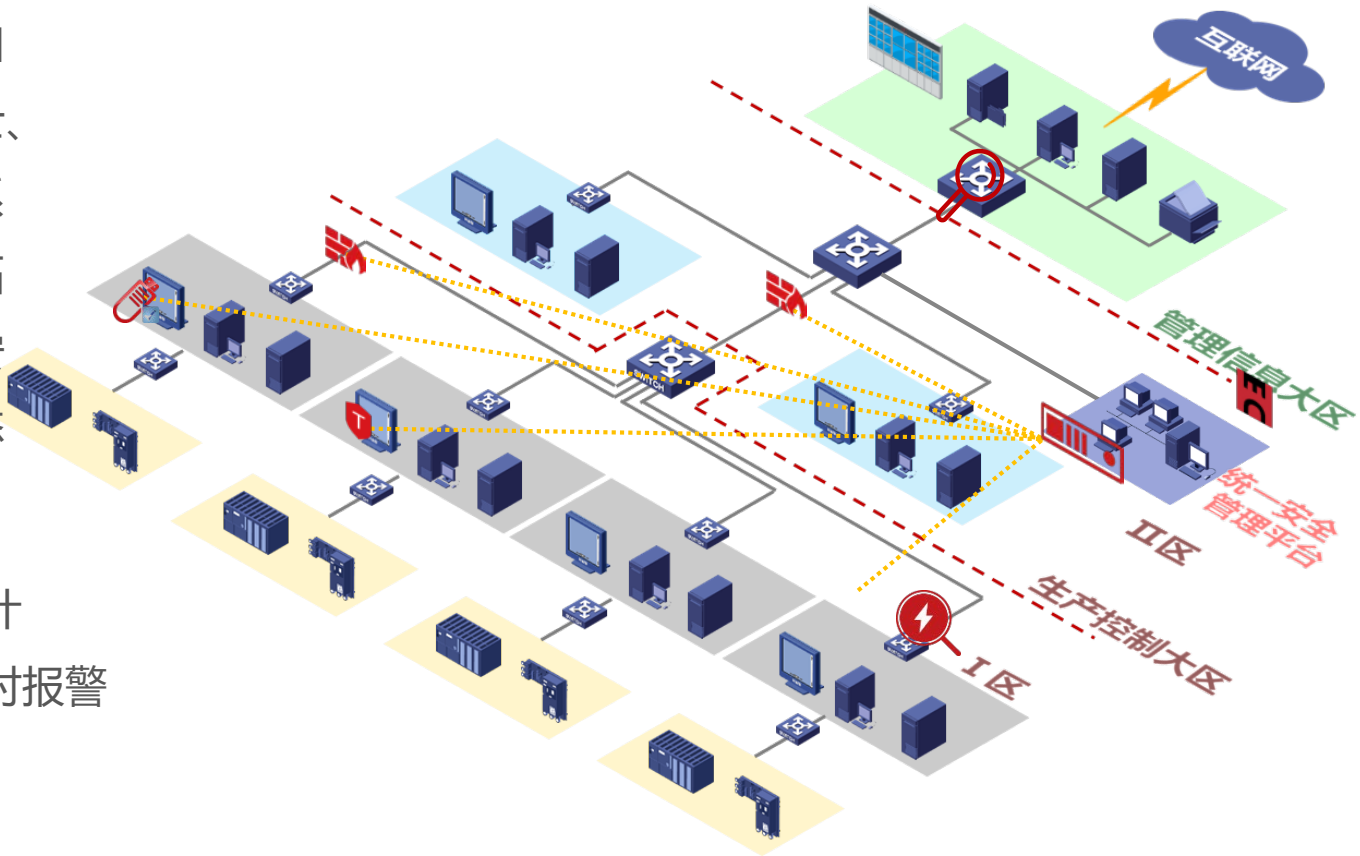
部署入侵检测检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计



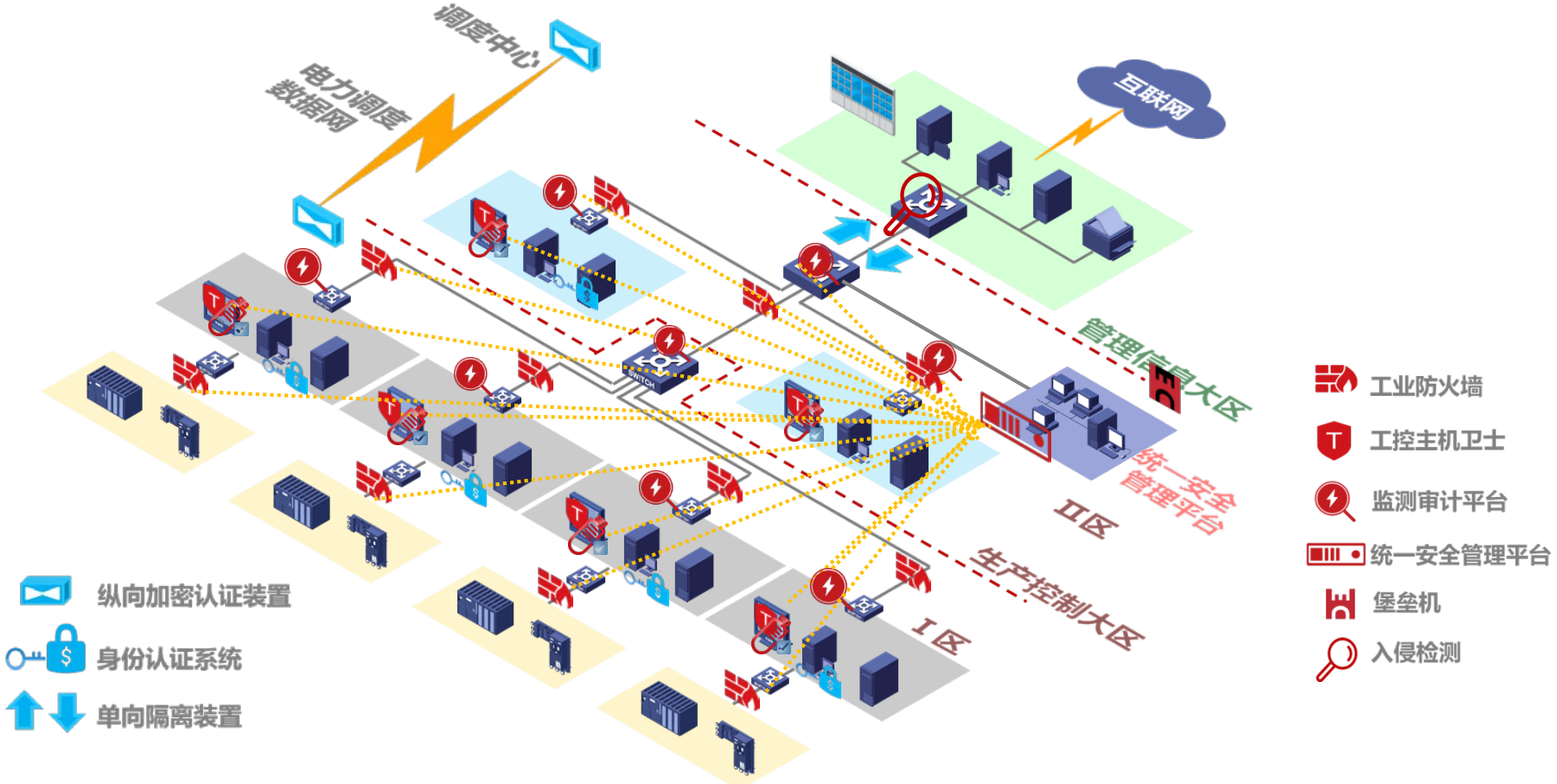
# 统一安全管理

集中管理安全设备：如工业防火墙、可信卫士、工控安全检测与审计系统，实现工控网络的拓扑管理、安全配置及安全策略管理、设备状态监控、告警日志等

- 集中的安全日志审计
- 工作站终端异常实时报警
- 分级分权限管理



# 网络安全总体防护方案部署示意图



# 浅谈市政燃气行业SCADA系统网络安全解决方案

# 安全问题—网络安全方面

- 中心控制系统和站控系统之间进行业务通信时，缺乏相应的安全机制保证业务信息的完整性，保密性；
- 缺乏记录和发现内部非授权访问的工具和手段，对重要业务系统维护人员缺少技术监控手段，无法有效记录维护人员的操作；
- 两化融合、TCP/IP网络通讯技术广泛应用，使工业控制系统面临更多传统信息网络面临的病毒、黑客，木马等信息安全问题；
- 通信协议自身存在漏洞，攻击者可利用漏洞对SCADA系统发送非法控制命令；
- 控制中心与站控系统之间主要采用MODBUS TCP协议和CIP协议进行通信，但这两个协议存在被窃听、分析、替换的风险；
- 一些不具备光纤通信的厂站采用GPRS、CDMA通信，直接通过APN虚拟专网进行采集数据、下发控制指令，缺乏加密措施；

# 安全问题—主机安全方面

- 大量的终端和现场设备如PLC，RTU和IED采用国外设备，如成都燃气SCADA系统采用SIXNET，重庆燃气采用AB、BB、艾默生；
- 中心控制系统和站控系统中的工程师站、操作员站、部分服务器均采用windows系统，其中包括微软不进行漏洞和补丁更新的WIN XP系统,WIN 2000系统,WIN 2003系统，对于系统的漏洞束手无策；
- 因担心杀毒软件误差业务程序（如oasys软件），多数业务现场主机类设备未找到合适防病毒方法，少量主机类设备虽安装了传统网络防病毒软件，但一直处于无法更新病毒库的困境中；
- 缺乏有效的审计能力，对发生的事件没有记录；
- 对外联的接口如USB接口，仍采用物理安全的方式解决；

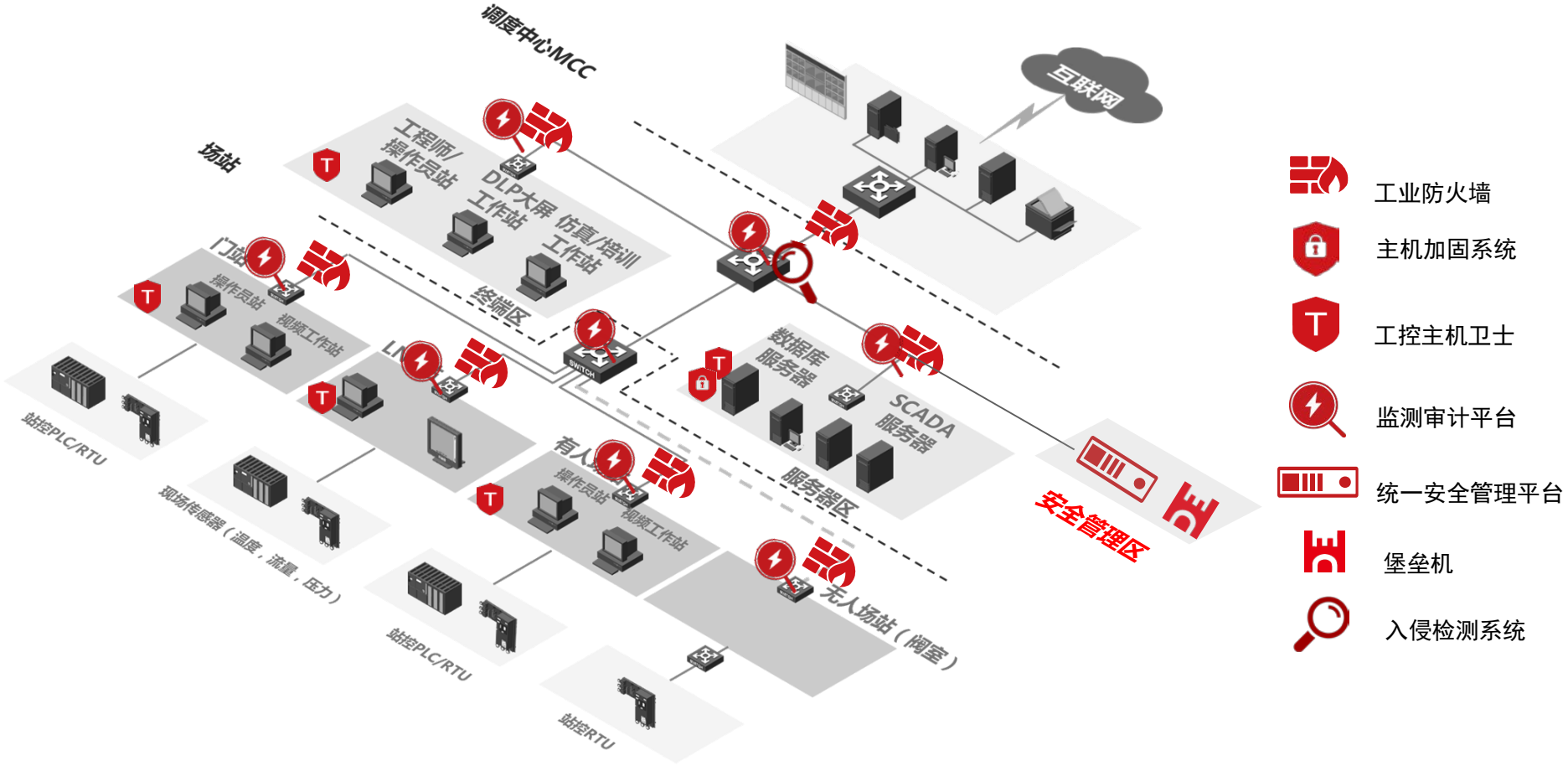
# 安全问题—应用和数据安全方面

- 工业控制系统使用的通信协议在设计初期未考虑安全环节，尤其目前在城市燃气中用的较多的 MODBUS TCP，CIP，OPC等协议；
- 很多工业控制系统设备制造商、集成商为了减低成本，尽可能的使用通用技术标准，如TCP/IP或使用自我研发、修改的MODBUS TCP协议；
- 工业控制系统使用的通信协议逐渐公开，甚至出版发行；
- OPC协议使得工业控制系统可以直接与PC上的应用程序交互，使工业控制系统更容易被攻击；

# 安全问题—管理方面

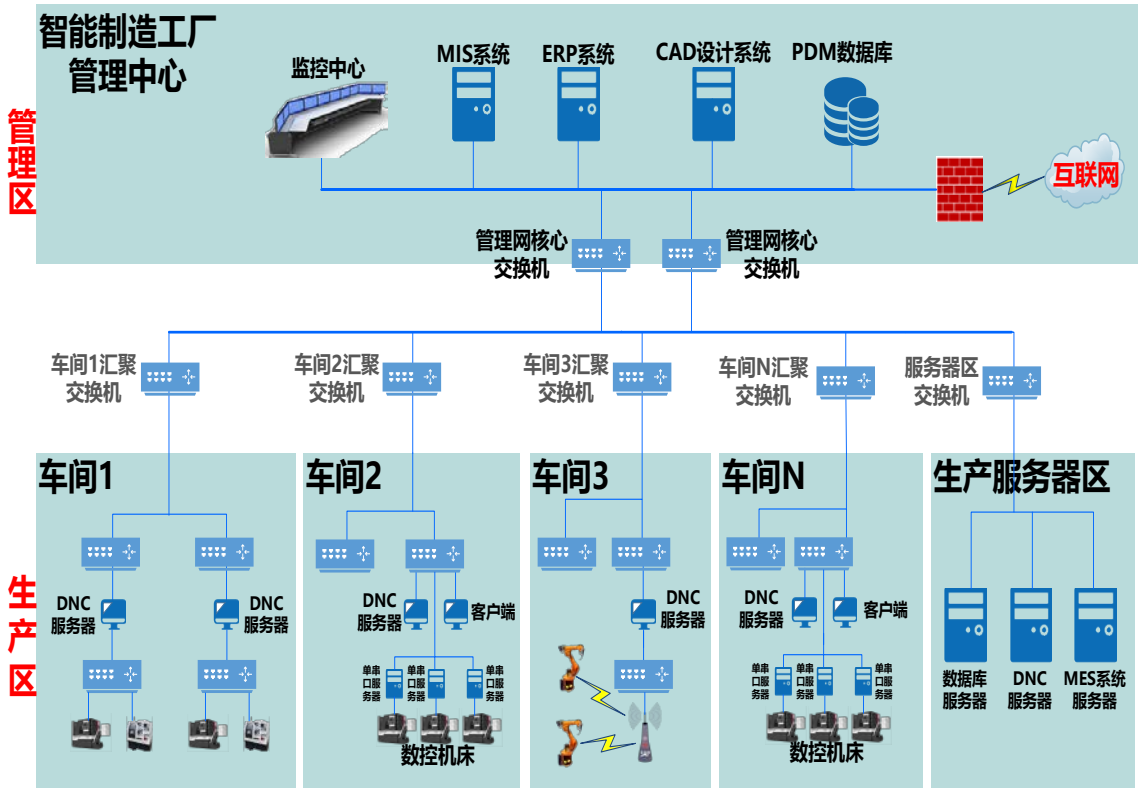
- 没有专门为工业控制系统设计信息安全方面的管理部门和工作流程；
- 缺少工业控制系统信息安全培训和意识培训工作；
- 缺少仿真实验平台辅助开展安全培训工作；
- 对内部信息的保护缺乏有效的管理手段及办法，如在公开渠道就可以获得一些基础的工业控制系统技术细节；

# 网络安全总体防护方案部署示意图



# 浅谈智能制造行业网络安全解决方案

# DNC系统网络架构




## DNC系统网络架构介绍

系统层级自下而上共五层，分别为设备层、控制层、车间层、企业层和协同层。具体包括：

- 设备层级包括传感器、仪器仪表、条码、射频识别、机器、机械和装置等，是企业进行生产活动的物质技术基础；
- 控制层级包括可编程逻辑控制器（PLC）、数据采集与监视控制系统（SCADA）、分布式控制系统（DCS）和现场总线控制系统（FCS）等；
- 车间层级实现面向工厂/车间的生产管理，包括制造执行系统（MES）等；
- 企业层级实现面向企业的经营管理，包括企业资源计划系统（ERP）、产品生命周期管理（PLM）、供应链管理系统（SCM）和客户关系管理系统（CRM）等；
- 协同层级由产业链上不同企业通过互联网络共享信息实现协同研发、智能生产、精准物流和智能服务等。

# DNC工控网络的安全现状

- 高精尖数控设备绝大多数依赖进口，无法进行自主维护，依赖国外厂商；
- DNC工控控制网络防护建设不够完善，仅通过传统防火墙、防病毒软件等进行防护；


- 缺乏对信息安全问题的高度重视，对企业核心技术知识和国家机密的信息安全风险并未有足够的认识；
- 国务院、工信部、国家保密局、国防科工局、总装备部对数控系统与管理网络的链接进行了严格规定。

# 智能制造工控网络入侵途径分析

WIFI无线连接

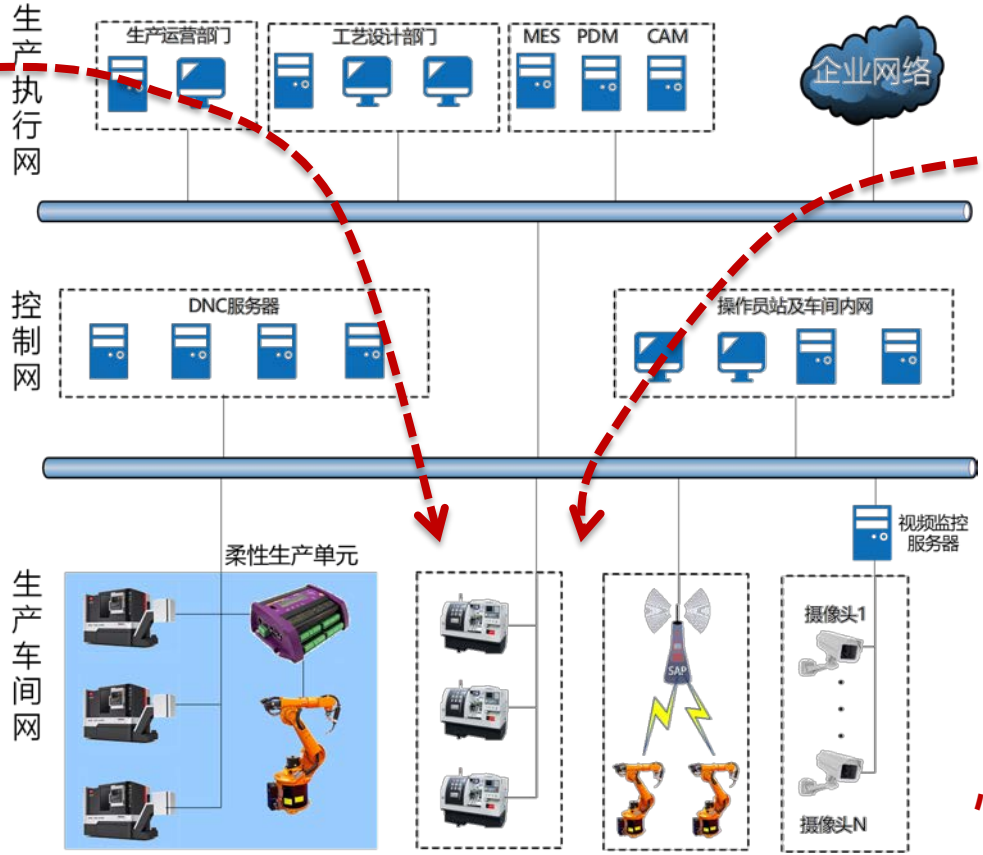
远程维护通道

手机等智能终端

企业办公网

USB移动存储介质

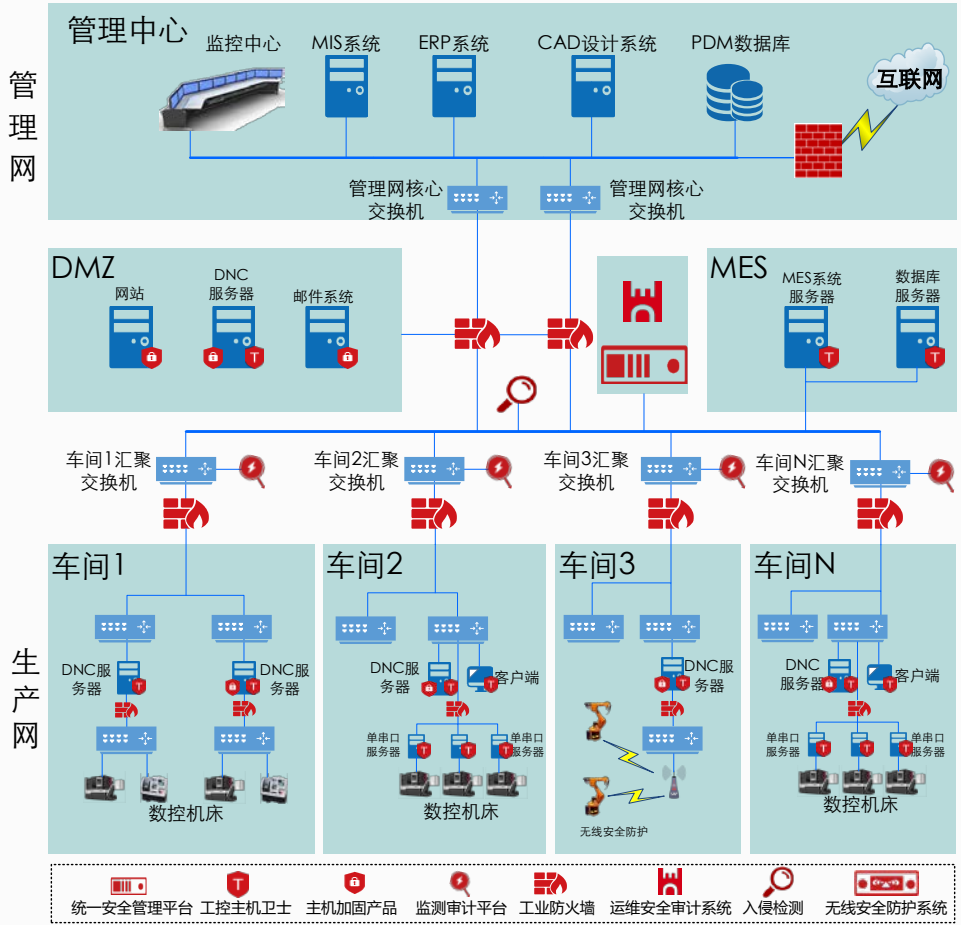
心怀不满的恶意员工



# 智能制造工控网络的安全风险分析

- DNC服务器、客户端等大部分是Windows系统，使用传统的数据库，系统老旧且不更新补丁，存在很大安全隐患；
- 数控机床所使用通讯协议存在安全上的设计缺陷，漏洞较多；
- 数控专用工控操作系统无适配的杀毒软件；
- 使用外来数据传输介质进行NC程序传输，无技术监控手段，管理难度大，危及设备安全；
- 数控设备或系统在业务指令发生异常时无法及时发现；
- 维修用数字设备在无安全监督或未经安全监测的情况下接入数控设备，带来潜在安全隐患；
- 来自管理网的病毒和攻击行为影响DNC系统；
- DNC系统大量使用无线网络进行生产活动，无线非法接入、篡改、伪造等行为可能会造成生产中断、效率降低、良品率下降等。

# 网络安全总体防护方案部署示意图



威努特 WINICSSEC

专注工控·捍卫安全