目录

工业控制系统信息安全

纲要

1. 工控系统安全介绍
2. 工控系统安全威胁
3. 工控系统安全理念
4. 工控系统安全策略

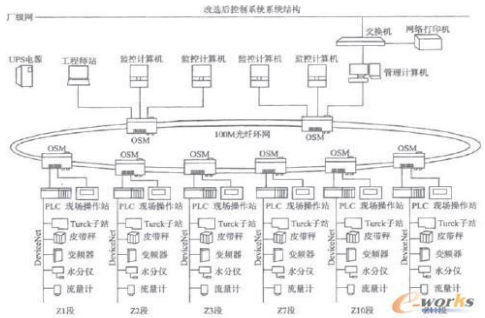
基本概念

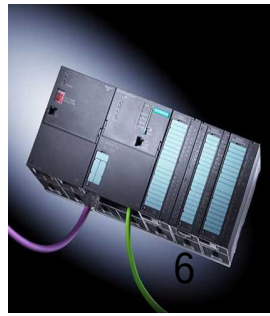
- **工业控制系统(ICS)是综合集成了计算机、网络、现代通信，微电子以及自动化技术，是对多种控制系统的总称，包括：**
  - 可编程逻辑控制器(PLC)；
  - 监控和数据采集(SCADA)系统；
  - 分布式控制系统（DCS)；

ICS普遍应用于电力、水处理、石油、天然气、化工、交通运输、制造业（烟草、汽车、食品等）。

基本概念

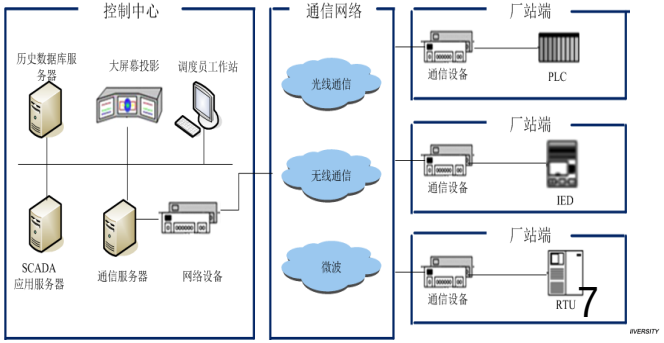
- **可编程逻辑控制器(PLC)；**
  - PLC单纯的实现逻辑功能和控制，不提供人机界面，实现操作需借助与按钮指示灯、HMI以及SCADA系统，PLC实现单机及简单控制。





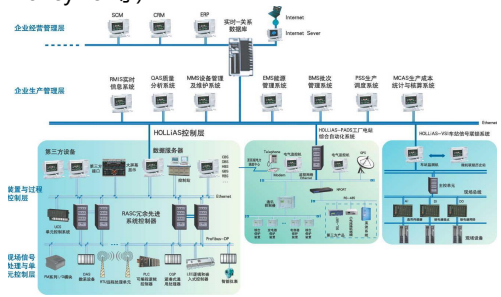
基本概念

- **监控和数据采集(SCADA)系统**
  - SCADA是对分布距离远，生产单位分散的生产系统的一种数据采集、监视和控制系统，SCADA作为生产管理级上位监控



基本概念

- **分布式控制系统（DCS)**
  - DCS兼具PLC和SCADA二者功能，但是基本上用在比较大的系统中和一些控制要求高的系统中，实现复杂控制；（Honeywell等）

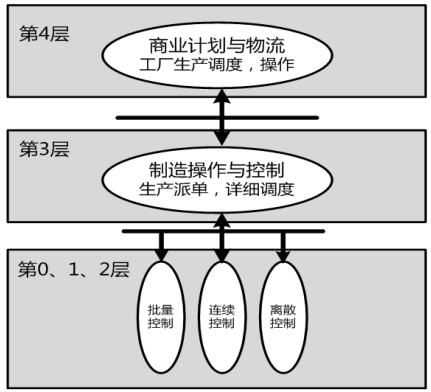


工业控制系统特点

- 实时性要求高，强调实时I/O能力；
- 可用性要求高，系统一旦上线，不能接受重新启动之类的响应，中断停机必须有计划（例检修）；
- 工控硬件要求寿命长、可靠性高，防电磁干扰，防爆，防尘等要求非常严格；
- 特有的工业控制协议通讯协议，不同厂商控制设备采用不同通信协议，很多协议不公开；
- 工控系统上线生产后，一般不会调整；
- 工控系统要求封闭性比较强。

工业控制系统功能层次

工业控制系统功能层次



纲要

Stuxnet震网病毒

- **2010年7月震惊全球工业界——世界上首个专门针对ICS编写的病毒；**

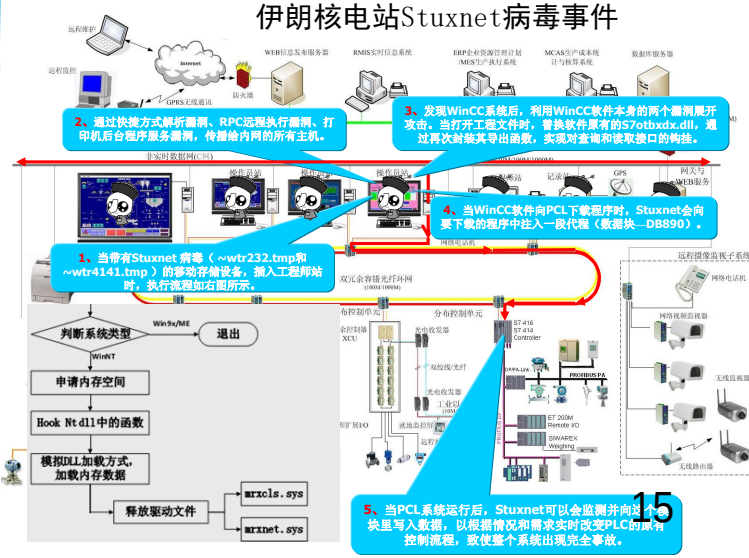
伊朗核电站Stuxnet病毒事件

来自安天实验室《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》

- 目标：伊朗核电站提炼浓缩铀的设施
- 目的：干扰浓缩铀提取过程，降低成品浓度
- 方法：渗透至工业内网，利用工业控制系统的安全漏洞，改变相关设施的运行参数
- 结果：成功！使伊朗核工业陷入停滞

攻击目标为DCS中的西门子WinCC HMI / 组态软件、STEP7组态软件以及S7-300 / 400系列PLC（某些型号），采用与攻击渗透民用以太网相似的方法。

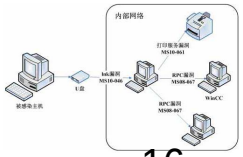
伊朗核电站Stuxnet病毒事件



伊朗核电站Stuxnet病毒事件

病毒特点：

- 针对特定场景
- 结构复杂，隐藏、掩饰手段高明
- 多种伪装，盗用数字签名，逃避查杀，同时利用多个0day漏洞，不惜代价；
- 7个已知和未知漏洞，其中至少4个0day漏洞（其中五个windows系统漏洞和2个西门子SIMATIC WinCC漏洞）；
- 修改PLC的程序逻辑，造成物理过程的故障；
- 传播途径：U盘、共享网络、打印机，目标明确，



伊朗核电站Stuxnet病毒事件

- 危害
  - 使得伊朗核计划拖后两年，60%的个人电脑感染病毒；
  - 全球超过45000个网络遭受攻击；
  - 多个行业的领军企业的工控系统受此感染。
- 时间表
  - 2010年6月，震网病毒首次发现，并且攻击伊朗核设备成功；
  - 2010年12月，微软推出针对Stuxnet所利用的漏洞修复补丁；
  - 2012年7月，西门子公司宣布修复Stuxnet利用的软件漏洞。

从发现病毒，到发布修复补丁，一共两年多时间

伊朗核电站Stuxnet病毒事件

- 美国《纽约时报》称，美国和以色列情报机构合作制造出“震网”病毒。
- “震网”病毒结构非常复杂，计算机安全专家在对软件进行反编译后发现，它不可能是黑客所为，应该是一个“受国家资助的高级团队研发的结晶”。

工业控制系统安全事件-能源

- 2000年，俄罗斯政府声称黑客成功控制了世界上最大的天然气输送管道网络
- 2001年，黑客入侵了监管美国加州多数电力传输系统的独立运营商
- 2003年，美国俄亥俄州Davis-Besse的核电厂控制网络内的一台计算机被微软的SQL Server蠕虫病毒所感染，导致其安全监控系统停机近5小时
- 2003年，中国龙泉、政平、鹅城换流站控制系统发现病毒，后发现是由外国工程师在系统调试中使用笔记本电脑所致
- 2010年，“震网(Stuxnet)”病毒在伊朗出现
- 2011年，沙特国家石油公司受到攻击，超过三万台电脑瘫痪
- 2012年，美国国土安全局下属的ICS-CERT组织称，自2011年12月以来，已发现多起试图入侵大型输气公司的黑客活动
- 2012年4月22号，伊朗石油部和国家石油公司内部电脑网络遭受病毒攻击，为安全起见，伊朗方面暂时切断海湾附近哈尔克岛石油设施的网络连接

工业控制系统安全事件-水处理

- 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，恶意造成污水处理站的故障，导致超过1000立方米的污水被直接排入河流，导致严重的环境灾难
- 2006年，黑客从互联网上攻破了美国哈里斯堡的一家污水处理厂的安全措施，在其系统内植入了能够影响污水处理的恶意程序，导致了严重的事故
- 2007年，攻击者侵入加拿大的一个水利SCADA控制系统，通过安装恶意软件破坏了用于从Sacrmento河调水的控制计算机
- 2010.1.31 12岁男孩侵入亚利桑那州的罗斯福大坝，150万英亩的水域，可把整个凤凰城淹掉
- 2011年，黑客通过Internet操纵了美国伊利诺伊州城市供水系统SCADA，使得其控制的供水泵遭到破坏

工业控制系统安全事件-交通

- 1997年，一个十几岁的少年侵入纽约NYNES系统，干扰了航空与地面通信，导致马萨诸塞州的Worcester机场关机6小时
- 2003年，SCX运输公司的计算机系统被病毒感染，导致华盛顿特区的客货运输中断
- 2003年，19岁的Aaron Caffery 侵入Houston渡口的计算机系统，导致该系统停机
- 2008年，一少年攻击了波兰Lodz的城铁系统，用一个电视遥控器改变轨道扳道器，导致4节车厢出轨
- 2011年，上海地铁因信号系统故障发生追尾事件，原因查明是系统升级过程中发生信息阻塞导致信号灯故障

工业控制系统安全事件-交通

2011年，温州动车追尾事件

工业控制系统安全事件-能源

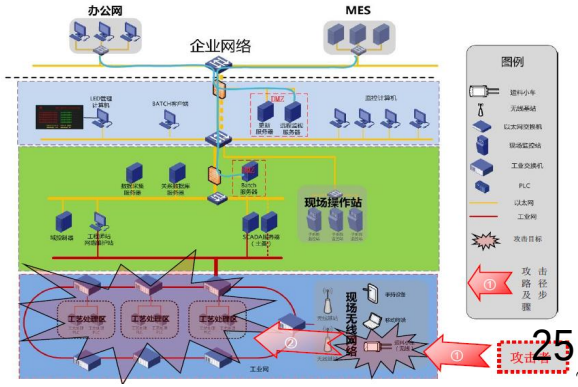
- 2000年6月5号，江苏省某县供电局某220KV变电所发生了一起带地线合闸的恶性误操作事故，造成全所停电。当时负荷达70000KW，给该县造成了很大的经济损失
- 2006年，清华同方环境有限公司在中国华能集团公司德州电厂二期3号机组脱硫装置运行过程中，旁路门突然非受控性关闭，致使工作间内7人被埋，其中4人抢救无线死亡
- 2007年，法国电力公司全资企业广西来宾B电厂（2台36万千瓦燃煤机组）因江边水泵房设备的控制和通讯完全中断，造成两台机组停运，全厂对外停电
- 2008年，华中（河南）电网因续电保护误动作、安全稳定控制装置拒动等原因引发一起重大电网事故，导致华中东部电网与川渝电网解列，华中电网与西北电网直流闭锁、与华北电网解列
- 2012年，亚马逊等网站上出现了智能电表破解装置，声称可以通过无线网更改智能电表读数

工业控制系统安全事件-制造

- 1992年，一前雇员关闭了雪佛兰位于22个州的应急报警系统，直到一次紧急事件发生以后发被发现
- 2005年，在Zotob蠕虫安全事件中，尽管在Internet与企业网、控制网之间都部署了防火墙，但还有13个美国汽车厂由于被蠕虫病毒感染而被迫关闭，50,000 生产线工人被迫停止工作，预计经济损失超过1,400,000美元
- 2011年，美国某大型药厂被黑客侵入并悄悄更改了生产物料配比，导致几个批次的药品出现不良反应，给药厂造成巨大损失

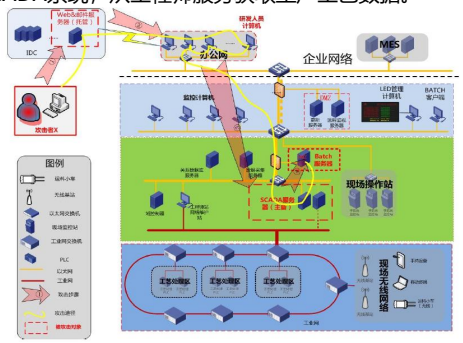
工业控制系统安全事件

- 入侵者通过现场无线网络，入侵工控生产过程控制系统，控制产品生产温度，改变产品生产质量。



工业控制系统安全事件

- 入侵者在邮件中植入木马，控制办公终端，进一步渗透到SCADA系统，从工程师服务获取生产工艺数据。



某制造行业工控安全事件

- 移动存储设备的随意接入，把病毒带入工控系统。
- 移动笔记本在没有准入控制和身份认证的情况下接入工控网络，把病毒带入到工控系统。
- 维护工控系统疏忽导致网线插错，造成工控网形成网络风暴，造成生产停车。
- 固定IP地址与DHCP共存造成的IP地址冲突，影响生产作业。
- 硬件设备丢失问题。

某石化行业工控安全事件

- 2009.6. 储控中心电脑感染蠕虫死机；
- 2009.10.芳烃装置控制系统感染病毒运行异常；
- 2010.5. 上层网络感染病毒故障；
- 2009-2010.操作站频繁死机；

虽未发生严重事故，但还是耗费了大量的人力、物力和精力去处理安全事件，给安全生产带来很大隐患!

工控系统的脆弱性

- **工业控制应用系统几乎是传统IT信息系统的拷贝，但安全防护远远落后于传统IT系统的安全防护。**
  - 工控系统大量采用IT通用软硬件，如PC服务器和终端产品、操作系统和数据库系统；
  - 由于工控系统兼容性的问题，系统补丁和杀毒软件的安全措施不到位，使系统的脆弱性得以放大!

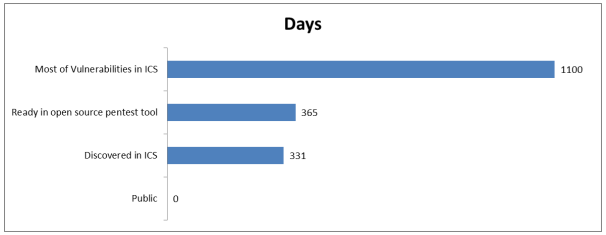
工控系统的脆弱性

- **工控软件与通信协议不健壮**
  - 相对于传统IT软件，工业控制系统组态软件、PLC嵌入式系统等在设计过程中主要考虑可用性，实时性、对安全性考虑不足；
  - 工控系统通信协议缺乏授权和加密、缺乏对用户身份的鉴别和认证等安全机制。

工控系统的脆弱性

- 工业控制系统安全不仅使用一个技术问题，更是一个管理问题，需要完善的工业控制系统安全政策、标准、制度和安全意识来支撑。
- 相对信息系统用户来说，工控系统用户安全意识更加薄弱！

工控系统的脆弱性



大多数的漏洞在工控系统上存在的时间超过3年
一年左右，这些漏洞就已经存在于开源的黑客入侵工具

网络安全风险急速增加

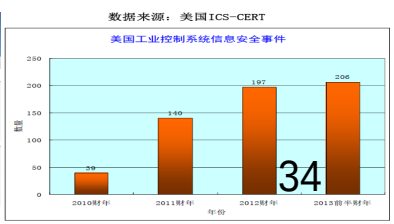
- **2012年美国ICS 蜜罐实验**
  - 模拟了一个连接在Internet 上的 ICS
  - 18 小时内发生第一次深度攻击
  - 28 天内发生39次深度攻击
- **美国DHS的统计，41% 记录在案的针对关键基础设施的攻击是针对能源相关行业**
  - 石油及天然气行业
  - 电力基础设施
- **攻击已经蔓延到关键基础设施的各个部门**

针对关键基础设施的网络攻击常常成为新闻头条

Sources – Wall Street journal, Wired Magazine

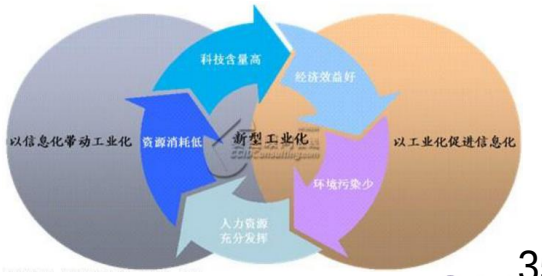
工控系统面临的威胁

- 台湾ICST在几个月时间，通过检测31厂家的67个产品，挖掘出50个可以被利用的漏洞。
- 从2007年起，每年的黑客大会都有关于工控系统安全的报告。
- 美国ICS-CERT报告，2012年工控安全事件197起，2013上半年工控安全事件206起。排在前三位的行业分别是：能源、关键制造业、交通。



工控系统面临的威胁分析

- **来自于经营管理网与互联网的威胁**
  - “两化”融合，信息化带动了工业化，工业化促进了信息化。产生了新型工业化，同时是也把传统IT风险延伸到了工控系统
  - 使工控系统面临来自经营管理网和互联网的威胁；



工控系统面临的威胁分析

- **来自于工控系统内网的威胁：**
  - 操作系统漏洞已知与无法修复的尴尬！
  - 病毒木马横行与无法杀毒的尴尬！
  - 非工控应用软件的存在，带来的未知风险！
  - 移动介质的随意使用带来的风险！
  - 移动笔记本随意接入带来的风险！
  - 工业无线网络边界的不可见与非法接入的不可控风险！

安全标准与动态

- 2014.1.12美国白宫发布《网络安全框架》
- 2013.5美国商务部NIST更新《工业控制系统安全指南》版本r1，2014年第一季度将推出第二版本
- 国际电工委员会制定IEC 62443(ISA99)工控安全标准。

安全标准与动态

- 2011-2013连续三年被发改委纳入国家信息安全专项
- 2013.12.26国家标准批准公布《工业以太网交换机技术规范》
- 2012年6月，《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号）中明确：保障工业控制系统安全。
- 2011年9月，工业和信息化部发布《 关于加强工业控制系统信息安全管理的通知》（451号文）

工控安全动态

- 工信部安全协调司赵泽良司长在RSA中国2011大会上强调“工业控制系统安全工作也到了非加强不可的时候了！”
- 2014年02月27日 中央网络安全和信息化领导小组成立；
- 2014年3月6日上海市正式发布了《上海市网络与信息安全事件专项应急预案》。

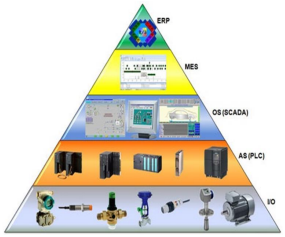
纲要

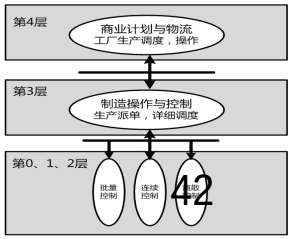
工控系统安全-白名单

- **工控PC、服务器的进程、服务**
  - 操作员站、工程师站、HMI、WEB服务器、数据库服务器；
- **工控系统访问控制列表**
  - IT防火墙、工业交换机、工业防火墙等；
- **工控系统资产**
  - 能够实时识别非法设备进入工控系统。

工控系统安全-层次化

- **“层次化”**
  - 根据工控系统功能的不同，对工控系统进行纵向分层、横向分域，域分等级，目的是进行安全隔离防护。
  - 针对工控系统的特点，我们提出了“三层架构，二层发防护”的方案。





工控系统安全-边缘化

- **“边缘化”**
  - 从工控系统演变过程可以看到，工控系统最初是独立的自动控制系统，但随着信息化的发展，以及智能控制的要求，不断的引入IT技术、互联网技术，从而使工控系统不再独立。
  - 工控系统安全，需要加强工控系统周边信息化系统的安全。例如：SCADA、MES、ERP安全。

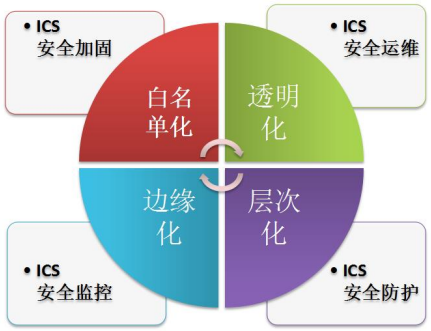
工控系统安全-透明化

- **“透明化”**
  - 工控系统安全采取的技术措施、管理措施，不能够降低系统使用者的易用性，安全措施对使用者来说是透明的；
  - 工控系统安全解决方案，不能够降低系统的可用性、尽可能避免系统的延时（如果有延时，必须在可接受的范围之内）。

纲要

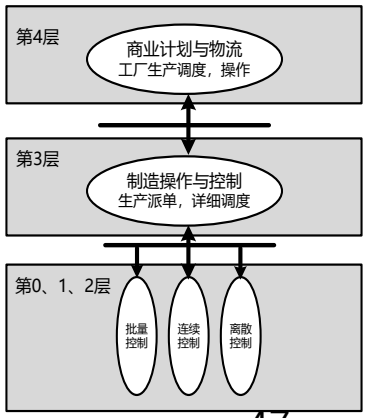
工控系统安全解决方案思路

- 基于工控系统安全防护理念，从四个维度，解决工控系统安全问题。



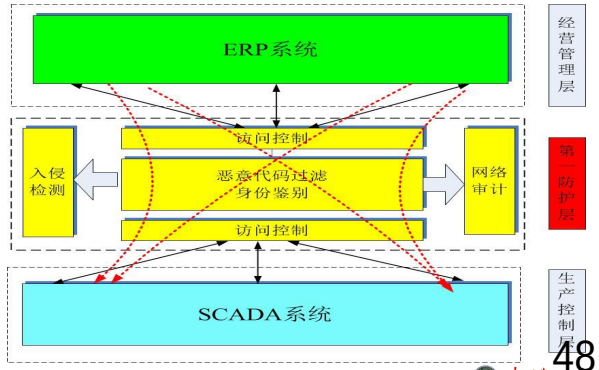
工控系统安全防护

- 纵向分层：三层架构，二层防护。经营管理层、生产控制层、过程控制层。
- 横向分域：不同的车间、不同的生产线进行逻辑隔离。
- 分层分域的目的就是进行安全隔离防护。



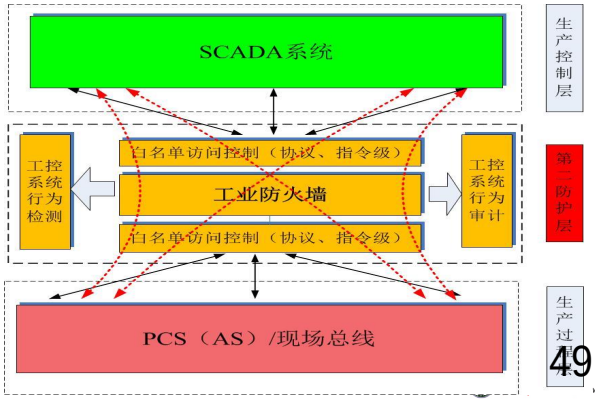
工控系统安全防护

- 经营管理层与生产控制层之间的防护



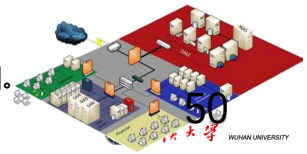
工控系统安全防护

- 生产控制层与生产过程层之间的防护



工控系统安全加固

- **经营管理层-系统安全加固**
  - 对ERP、MIS等与生产控制层交互的终端、服务器以及交换设备进行安全加固。
- **生产控制层-系统安全加固**
  - 对SCADA、MES系统中工控计算机（IPC）、服务器进行白名单式安全加固，同时对工业交换机进行加固
- **生产过程层-系统安全加固**
  - 对PLC、RTU等进行安全加固。

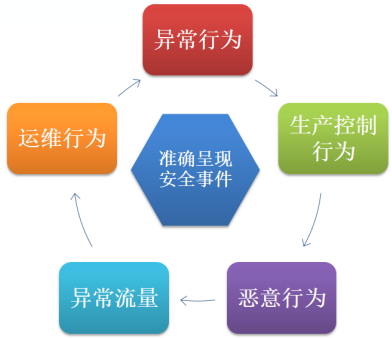


工控系统安全监控

- 工控系统的可用性监控

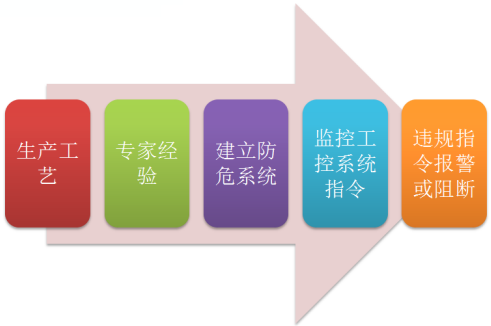
工控系统安全监控

- 工控系统网络行为监控

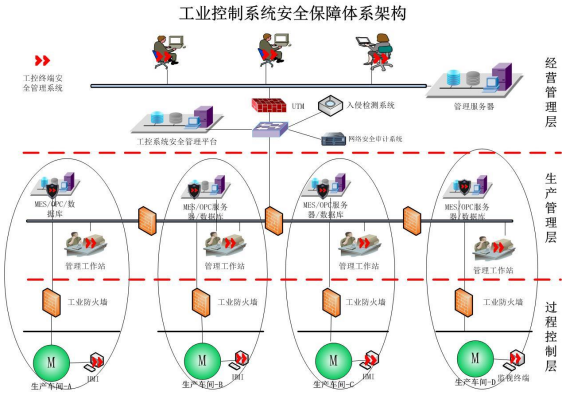


工控系统安全监控

- 工控系统指令监控



工控系统安全解决方案整体框架



解决方案解决的主要问题

- 工控机（IPC）操作系统的加固（进程、服务白名单）
- 工控机（IPC）外设管理，如USB接口，光驱，网卡，串口。
- 工控机（IPC）强口令认证。
- 工控系统与管理系统的安全隔离控制。
- 工控系统的无线安全接入。
- 工控系统远程安全接入。
- 工控系统的设备准入控制。
- 工控系统的可用性、异常事件以及流量监控。
- 工控系统病毒的查杀。

国外工控系统安全解决方案

- 国际上有两种不同的工控系统信息安全解决方案:
- 主动隔离式解决方案
- 被动检测式解决方案

国外工控系统安全解决方案

- 主动隔离式解决方案
- 即相同功能和安全要求的设备放在同一区域内，区域间通信靠专有管道执行，通过对管道的管理来阻挡非法通信，保护网络区域及其中的设备。其典型代表是加拿大 Byres Security 公司推出的 Tofino 工控系统信息安全解决方案。

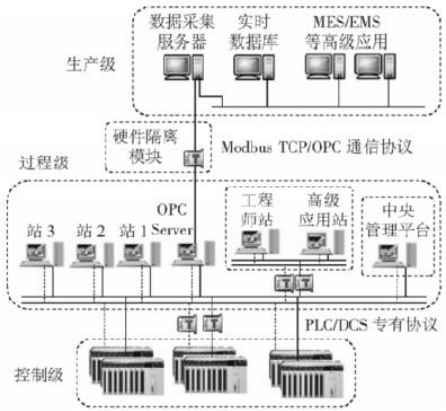
国外工控系统安全解决方案

Tofino 工控系统信息安全解决方案

硬件隔离模块	应用于受保护区域或设备的边界
功能软插件	对经过硬件模块的通信进行合法性过滤
中央管理平台	对安全模块的配置和组态，并提供报警的显示、存储和分析
特点	是基于白名单原理，能够深入到协议和控制器模型的层次对网络进行交通管制。

国外工控系统安全解决方案

- Tofino 工控系统信息安全解决方案



国外工控系统安全解决方案

- Tofino 工控系统信息安全解决方案
- 因为所有的网络威胁最后都要经由通信来实现，而工控系统具有物理结构和通信模式相对固定的特点，所以主动隔离式是一种比较有效的解决方案，可以根据实际要求对工控系统进行灵活的信息安全防护。应用这种方案的关键是防护等级和安全区域的确定，需要寻求一个防护深度和成本的折中。

国外工控系统安全解决方案

- 被动隔离式解决方案
- 被动检测式解决方案延续了 IT 系统的网络安全防护策略。由于 IT 系统具有结构、程序、通信多变的特点，所以除了身份认证、数据加密等技术以外，多采用病毒查杀、入侵检测等黑名单匹配的方式确定非法身份，通过多层次的部署来加强网络信息安全。其典型代表是美国 Industrial De-fender 公司的工控系统信息安全解决方案。

国外工控系统安全解决方案

- Industrial De-fender 解决方案
- Industrial Defender 解决方案主要面向安全要求较高的电力行业推出，包括统一威胁管理(UTM) 、主机入侵防护、网络入侵检测、访问管理、IP 网关和安全事件管理等部分。

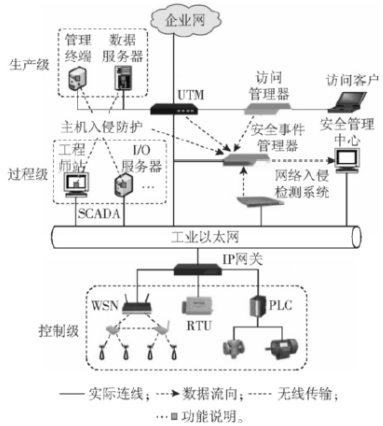
国外工控系统安全解决方案

Industrial De-fender 解决方案

统一威胁管理	构成了安全防御的第 1 道防线，集成了防火墙、防毒墙入侵防御、远程访问身份验证和虚拟专用网络(VPN) 技术
主机入侵防护	自动拦截所有未经授权的应用程序
网络入侵检测	被动检测控制网络安全边界内所有的网络流量，能够检测到来自内部或外部的可疑活动
访问管理和IP网管	保证了授权的远程访问和设备子站的安全接入
安全事件管理	对网络中的安全事件进行集中监视和管理

国外工控系统安全解决方案

- Industrial De-fender 解决方案



国外工控系统安全解决方案

- 被动隔离式解决方案
- 被动检测式解决方案的主要硬件设备均部署于原有系统之外，且主机入侵防护功能通过代理终端以白名单技术实现，这些措施大大减少了对原有系统性能的影响，满足了工控系统可用性的要求。然而，由于网络威胁特征库的更新总存在滞后，所以基于黑名单技术的安全组件对于新出现的入侵行为不能及时做出响应。因此，一些新型病毒或黑客行为仍可能对工控系统造成危害。

国外工控系统安全解决方案

- 主动隔离与被动隔离式解决方案比较
- 相比较而言，主动隔离式方案主要对网络交通进行管理，而被动检测式方案更侧重于对应用程序的监控。二者都可以达到较好的安全防御效果，需要根据不同的行业领域或应用场景来选择应用。

国内工控系统信息安全解决方案

- Stuxnet 事件发生以后，国内工业领域相关科研机构针对控制系统信息安全这一新课题开展了研究工作，例如工控系统隔离装置以及基于工业模型的入侵检测系统等。工控系统信息安全已经成为国内工业领域关注的热点之一，但尚未形成统一的标准和成熟的产品。为了应对日益严峻的工业信息安全形势，各行业都在提出符合自身网络特点的解决方案。以我国冶金行业的工控系统信息安全综合解决方案为例。

国内工控系统信息安全解决方案

- 我国冶金行业的工控系统信息安全解决方案
- 解决方案主要从区域隔离、入侵检测、外设管理、安全运维 4方面出发。建立如下 3
- 个层次的纵深防御体系:

第 3层，主机防御

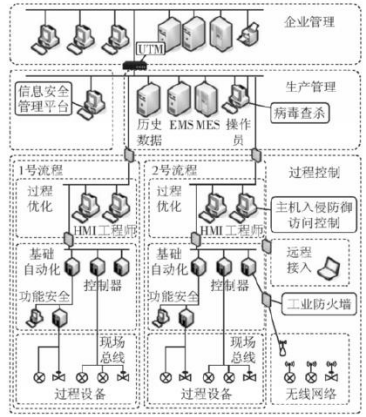
第 2层，通信管理

第 1层，边界隔离

最后，由统一的信息安全管理平台对所述防御体系进行实时监管。该平台支持网络安全设备的在线配置和组态，可视化地监督网络资产运行状况，能够及时发现和弥补安全漏洞。同时，可以提供详细的信息安全审计功能，通过对安全事件的跟踪和预警，为网络故障的及时排查和分析提供可靠依

国内工控系统信息安全解决方案

- 我国冶金行业的工控系统信息安全解决方案



国内工控系统信息安全解决方案

- 我国冶金行业的工控系统信息安全解决方案
- 方案通过边界隔离、通信管理和主机防御 3个层次的深度防御，确保只有绝对必要的人员、设备和程序才能访问关键控制系统，符合工控系统信息安全定义的描述，同时也满足我国冶金行业控制系统的特点对信息安全防护的要求，具有一定的参考应用价值。

国内工控系统信息安全解决方案

- 要充分应对目前面临的安全形势，这些还远远不够，需要从以下几方面作更多的努力:
- (1) 发展具有自主知识产权的安全产品。我国的工业信息安全产业还处于起步阶段，基础薄弱，水平不高，防护能力低于很多西方国家，关键技术和产品还受制于人。
- (2) 加快安全规范和技术标准的制定。工控系统信息安全标准将为政府和企业建立多层防御策略架构、进行风险评估提供指南和方向。
- (3) 加强管理。最有效的信息安全防护并非仅仅依赖技术解决方案就能完成，其中 80% 要靠渗透到工控系统管理者、操作员日常工作中的安全管理制度。

国内工控系统信息安全解决方案

- 总之，21 世纪工业文明的特征是数字化、网络化和信息化，网络的快速发展为各种信息安全威胁打开了方便之门。面对越来越频繁发生的工业信息安全事件，当前首要的任务是充分认识到问题的迫切性和后果的严重性。同时，更要认识到工控系统信息安全不是一个单纯的技术问题，而是涉及到多方面的动态系统工程，需要在整个工业基础设施生命周期的各个阶段中持续实施，即所谓“安全不是一个结果，而是一个过程”。