2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

工控安全：瓷器店里捉老鼠
——浅谈工控网络攻与防

谢 丰

博士，研究员
中国信息安全测评中心
fengxie@126.com

目录

一、工控安全：从功能安全到信息安全

二、工控入侵：新特点，新变化

三、工控防护：旧瓶新酒，理念革新

一、工控安全：从功能安全到信息安全

工业控制系统

- 离散控制系统DCS、可编程逻辑控制器PLC、远程终端单元RTU、智能电子设备IED、数据采集系统SCADA…
- 超过80%的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业，是关键基础设施的“大脑”和“中枢神经”

石化

电力

水利

交通

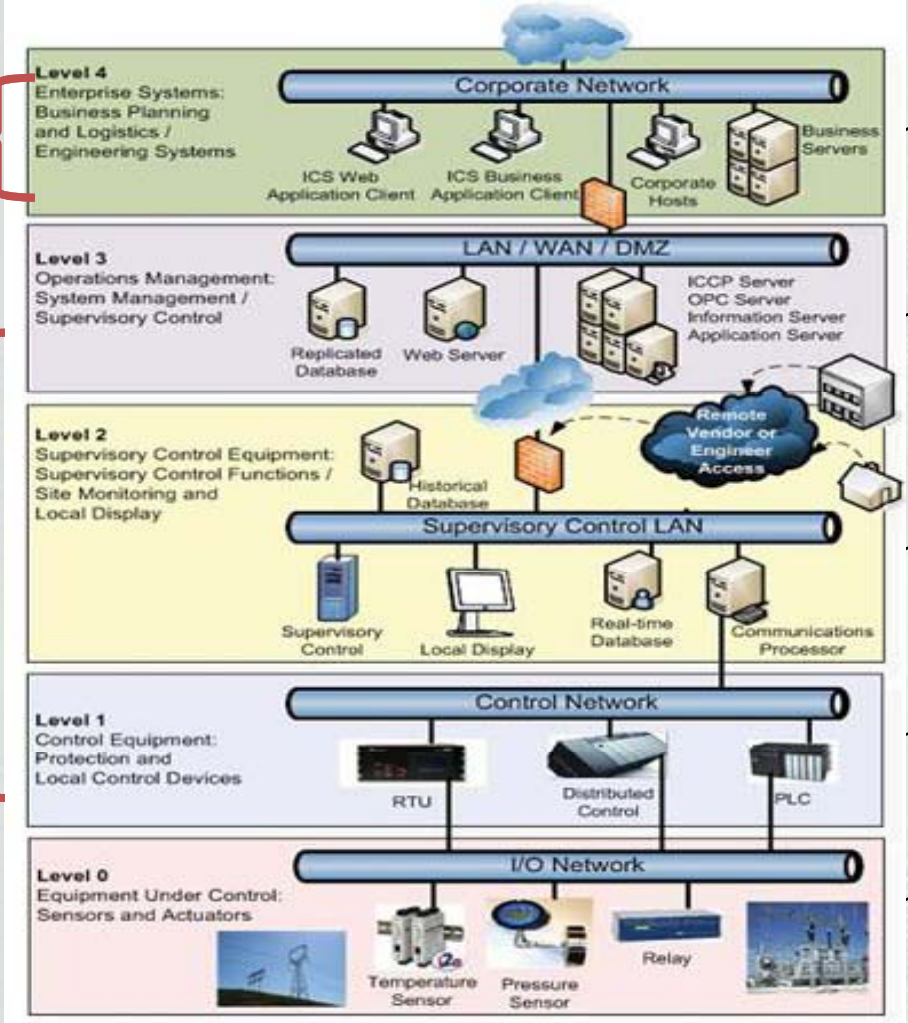
核能

制造

典型工控网络架构

IT网络

工业控制网络



4:企业系统层—IT系统ERP

3:运行管理层—生产调度MES

2:监视控制层—上位机HMI

1:本地控制层—PLC等

0:过程层—现场仪器仪表

从功能安全到信息安全

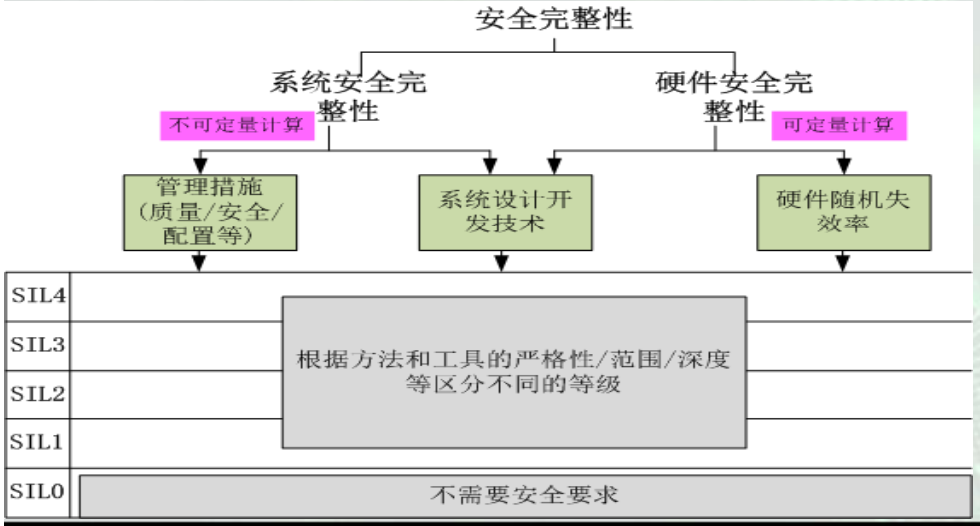
二者有交集，但有本质上的差别

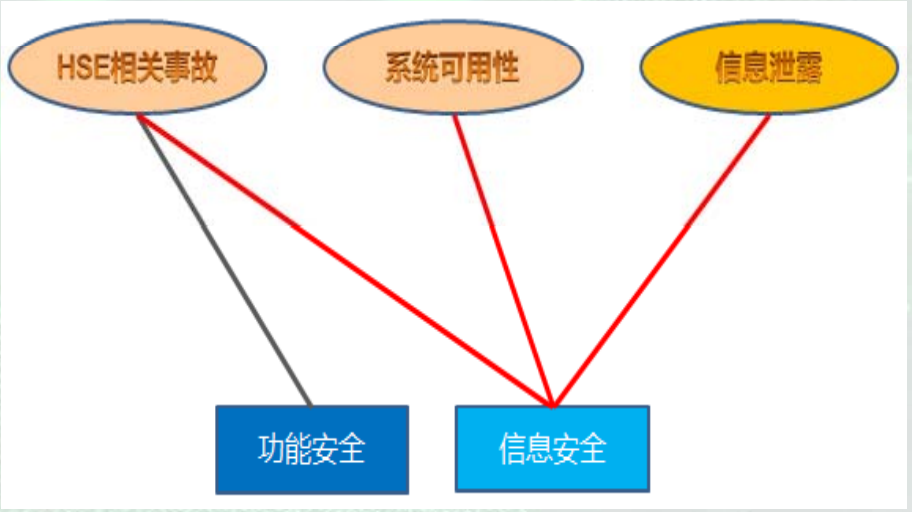
功能安全Safety

- 威胁源：系统自身的、偶然的威胁，比如硬件随机失效
- 威胁后果：人身伤亡、系统损失、环境破坏（HSE）
- 故障导致安全原则
- 安全完整性等级

信息安全Security

- 威胁主体：人（黑客、恐怖组织、国家政府）
- 威胁后果：不仅是HSE，还考虑系统可用性、信息泄露、公司声誉等
- 漏洞是核心环节





三、工控入侵：新特点，新变化

工控入侵技术不断变化

两化深度融合，以及中国制造2025、工业4.0提出，网络威胁开始蔓延至工控、领域，直接影响工业安全、国家安全

2010年震网病毒利用0-day漏洞，绕过物理隔离防护，篡改工艺参数破坏离心机

2010-2011 齐鲁石化、大庆石化等多地感染 Conficker 蠕虫，导致控制器通信中断

2014年利用水坑攻击感染Havex病毒，通过OPC Server获取生产数据，影响上千家能源企业，8000个能源系统

2014年通过钓鱼攻击，从互联网渗透到德国某钢厂的工控网，直接影响炼钢炉

2015年黑色能量病毒攻击乌克兰电力系统，远程关闭断路器并删除系统以迟滞恢复，导致大停电

2015年 美国官方宣布ISIS恐怖组织试图攻击美国一处电力网络公司，未成功。

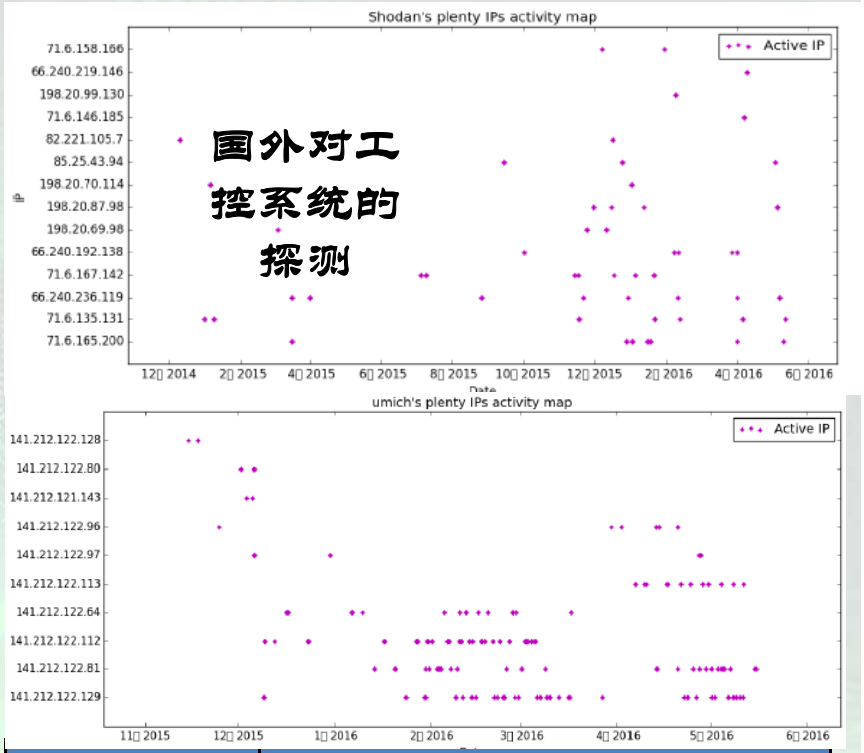
2016 年 PLC Blaster工控蠕虫（未来的病毒？）

变化与特点

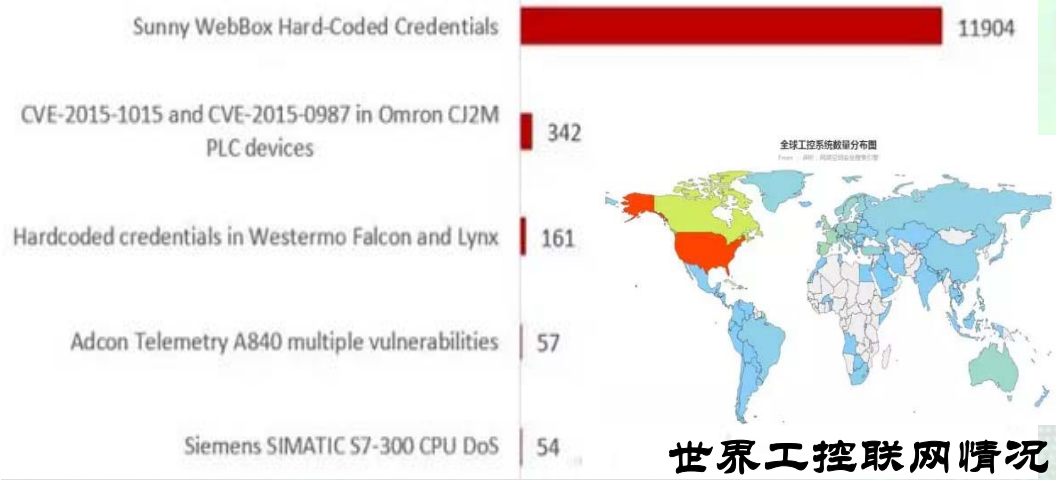
- 网络攻击已经从影响虚拟资产演变到破坏物理世界。
- 通用化、软硬结合、互联互通的技术变化直接带来基础设施攻击面的增大，通过互联网渗透到工控已成为一种重要途径。任何工控系统都可能成为目标。
- 传统病毒与工控病毒相互交织。
- 以计算机为跳板的攻击在未来可能发展到直接攻击控制系统。
- 从利用未公开漏洞高难度攻击方式延伸到常规手段组合式攻击，甚至绕过工控底层知识的壁垒。

工控探测活动日渐增多

2016年7月，卡巴斯基声称通过全网扫描，全球170个国家有188,019工控主机与ICS设备相连，92%存在脆弱性容易被利用



卡巴斯基公布的联网工控设备漏洞



世界工控联网情况

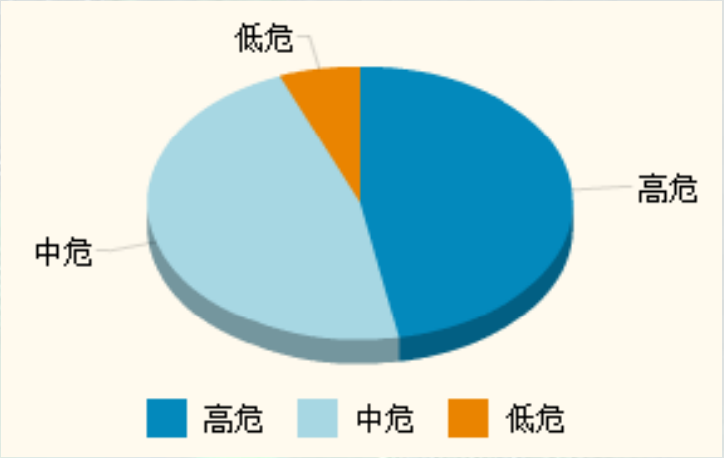
端口	工控
102	Siemens
502	Modbus
789	Red Lion
1911	Tridum Fox
2404	IEC 104
44818	EtherNet/IP

常见工控探测端口

工控安全漏洞有了新的特点

工控漏洞是网络入侵的首选突破点

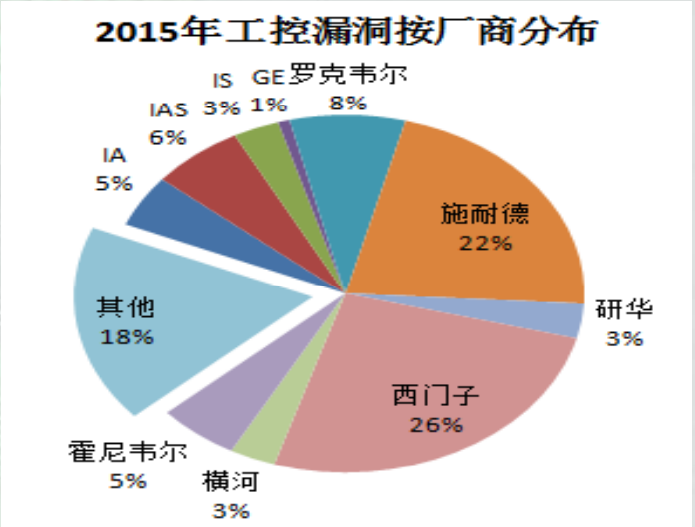
- 危害影响
  - 从信息网络的影响扩大到物理过程
  - 几乎都为中高危，且高危占工控漏洞总数近一半



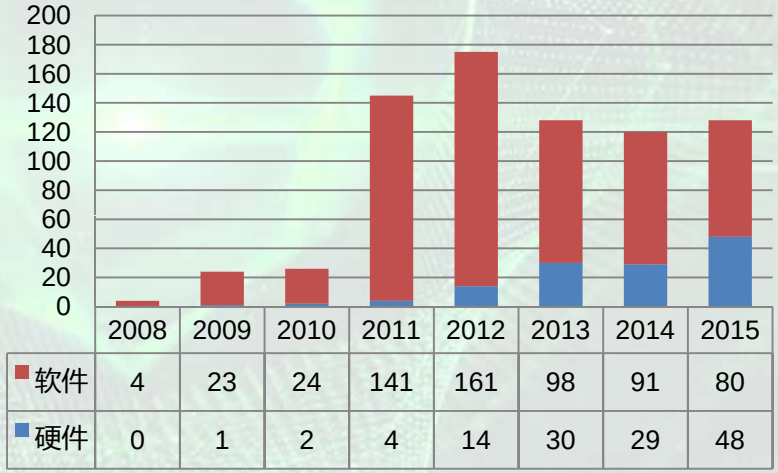
- 漏洞价值评价
  - 拒绝服务型漏洞不再是“鸡肋”，可利用性不再是漏洞挖掘与利用的唯一目标

危害级别	高 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	SIEMENS SIMATIC S7-300 CPUs with Profinet support < V3.2.12 SIEMENS SIMATIC S7-300 CPUs without Profinet support < V3.3.12
CVE ID	CVE-2016-3949
漏洞描述	Siemens SIMATIC S7-300 CPU是西门子（Siemens）公司的一款用于制造行业的模块化通用控制器。 Siemens SIMATIC S7-300 CPU系列设备存在拒绝服务漏洞。攻击者利用漏洞在一定条件下可发起拒绝服务攻击，即通过发送精心编制的数据包到102/ TCP（ISO-TSAP）端口或现场总线Profibus，导致设备进入故障模式，冷启动可恢复系统。

- 漏洞发现
  - 图形组态软件、编程软件、下位机、工控协议...
  - 硬件设备漏洞占比逐年增大
  - 发现预警难度大：硬件获取难（价格昂贵、购买困难）、故障调试难（嵌入式）、设备类型多、私有协议多、软件公开资料少
- 漏洞修补
  - 先天不足，不易修补
  - 实时修补难



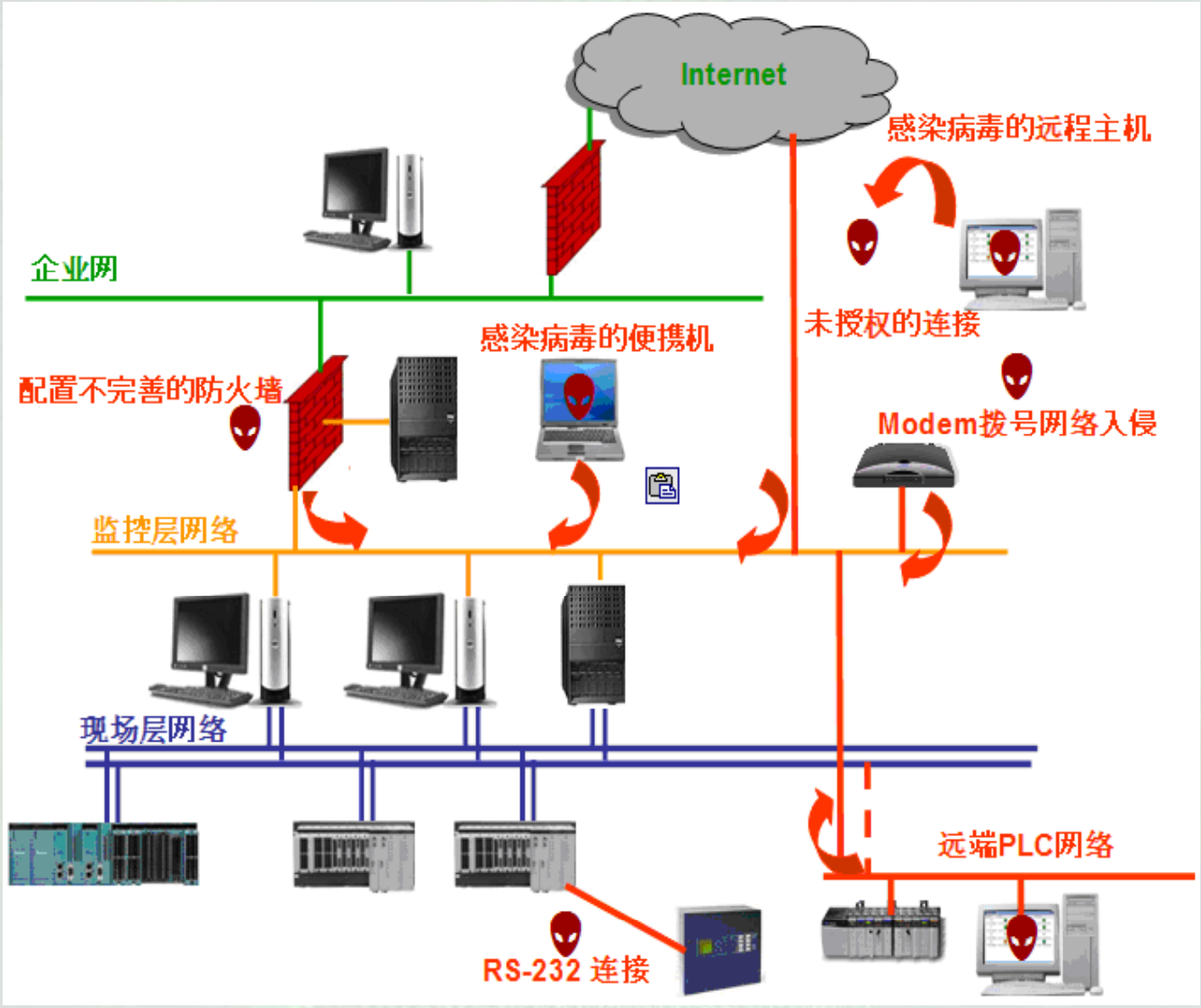
2008-2015年工控软硬件漏洞数量对比



	2008	2009	2010	2011	2012	2013	2014	2015
软件	4	23	24	141	161	98	91	80
硬件	0	1	2	4	14	30	29	48

攻击无孔不入

- 互联网
- 企业办公网络
- 虚拟专网
- 拨号连接
- “可信”的第三方连接(远程诊断和维护)
- 无线网络
- 现场设备
- U盘摆渡



三、工控防护：旧瓶新酒，理念革新

由于信息安全从来都不是工控系统的设计目标，因此工控系统基本上没有任何防护

产品设计

- 几乎所有工控产品都没有安全机制，无鉴别、无加密、无审计

运行管理

- 职责不清晰，人员安全意识薄弱，security经常属于“三不管地带”，未纳入生产安全范畴
- 上线前未检测，上线后未评估

技术措施

- 工控系统没有防护措施，系统处于“裸奔”状态，其最重要的防护就是封闭，一旦能够接触，就能很轻易的攻击

主要技术风险

- 恶意代码无防护
- 网络连接无隔离
- 系统漏洞难修补
- 工控网络无监控
- 远程通信无保护

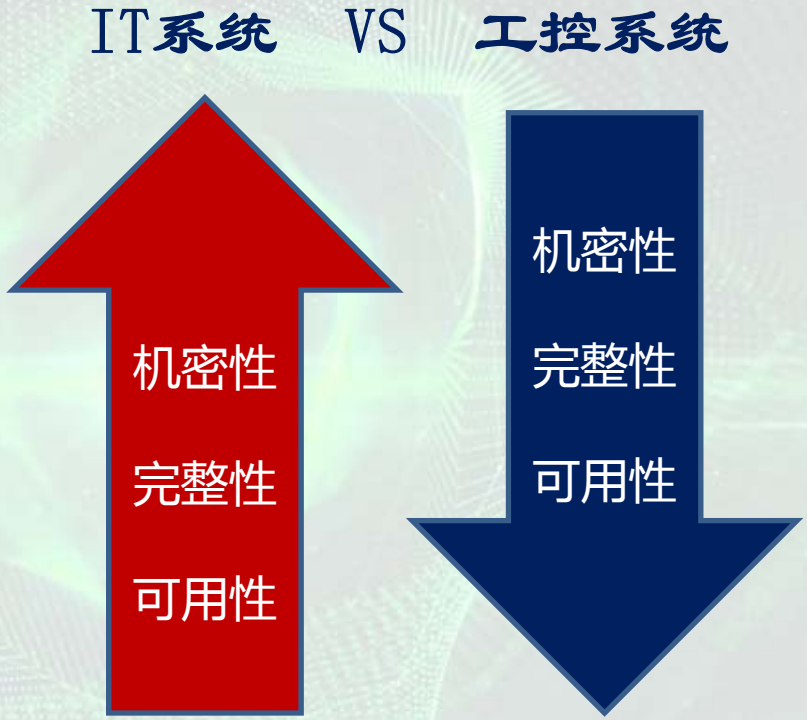
工控系统的特殊性导致大量现有信息安全措施无法直接应用，绝不能简单地将已有技术照搬到工控系统中

IT系统需求

- 高吞吐量
- 标准统一的通信协议
- 设备部署在本地，易于访问
- 设备生命周期为3~5年

工控系统需求

- 高实时性
- 高可靠性，系统不允许重启
- 人和控制过程安全
- 通信协议多种多样
- 设备不易访问
- 设备生命周期为15~20年



工控安全防护的困难

- 实时性高，可靠性高，绝不能影响工控生产运行（雷区）
- 核心设备极其脆弱
- 基本属于“交钥匙”工程，毫无安全意识，不懂安全技术
- 研究测试环境投入大，研发难度大

研发不易开展

用户不敢尝试

措施难以执行

工控系统信息安全如同瓷器店里捉老鼠。瓷器很脆弱，我们既要能抓住老鼠，又不能毁坏瓷器。

工控安全需要理念革新

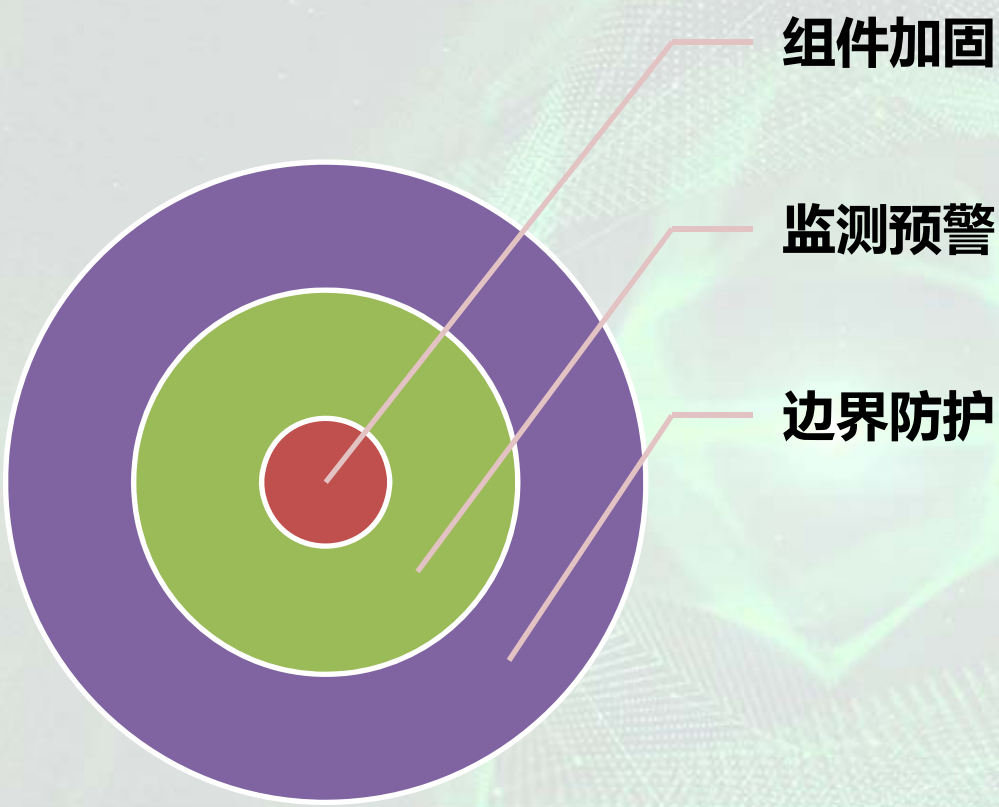
- 依据工控系统特点，形成工控安全技术
  - 工控网络通信行为固定、流量规律性强、联网设备变动小，容易建立工控网络安全基线
  - 整体封闭，系统难以升级，杀毒也难以升级
  - 应用程序单一
  - 运维人员不懂安全

坚持管理+技术的信息安全传统套路

- 管理上，形成工控信息安全管理体系
  - 建立工控安全组织管理机构
    - 明确“由谁管”
  - 制定并落实工控安全管理制度
    - U盘管控、运维管控…
  - 开展工控安全意识与技能培训
    - 跨领域培训

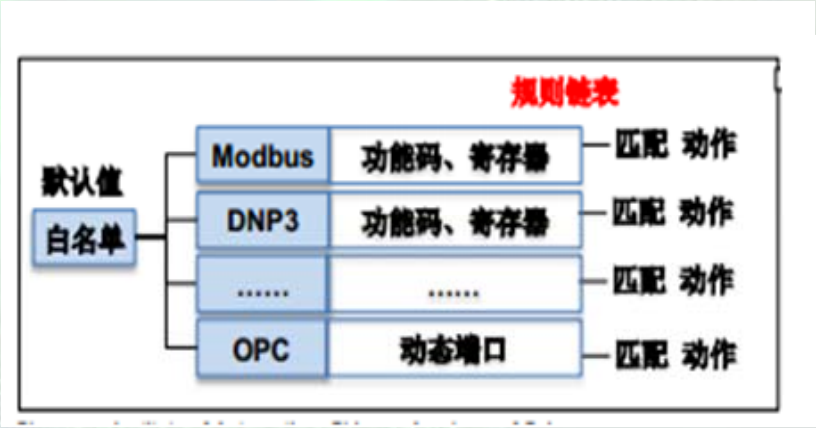
可借鉴大量已有标准规范、最佳实践，如IEC 62443、GB/T 30976、美国管道SCADA安全、21步提高工控安全最佳实践等等

- 技术上，“旧瓶新酒”，形成“纵深防御”安全防护体系



边界防护

- 识别网络连接
  - 统计表明89%的系统是联网的，平均高达有11个网络连接
  - 无线接入（Wifi、GPRS/3G/4G、数传电台)、拨号调制解调
  - 精细化管理、智能制造、工业大数据加速促进网络互联
- 划分安全区域
  - DMZ、监控区…
- 边界隔离保护
  - 指令级过滤
    - Modbus、OPC、DNP3…
  - 单向数据传输
    - 控制区→非控制区

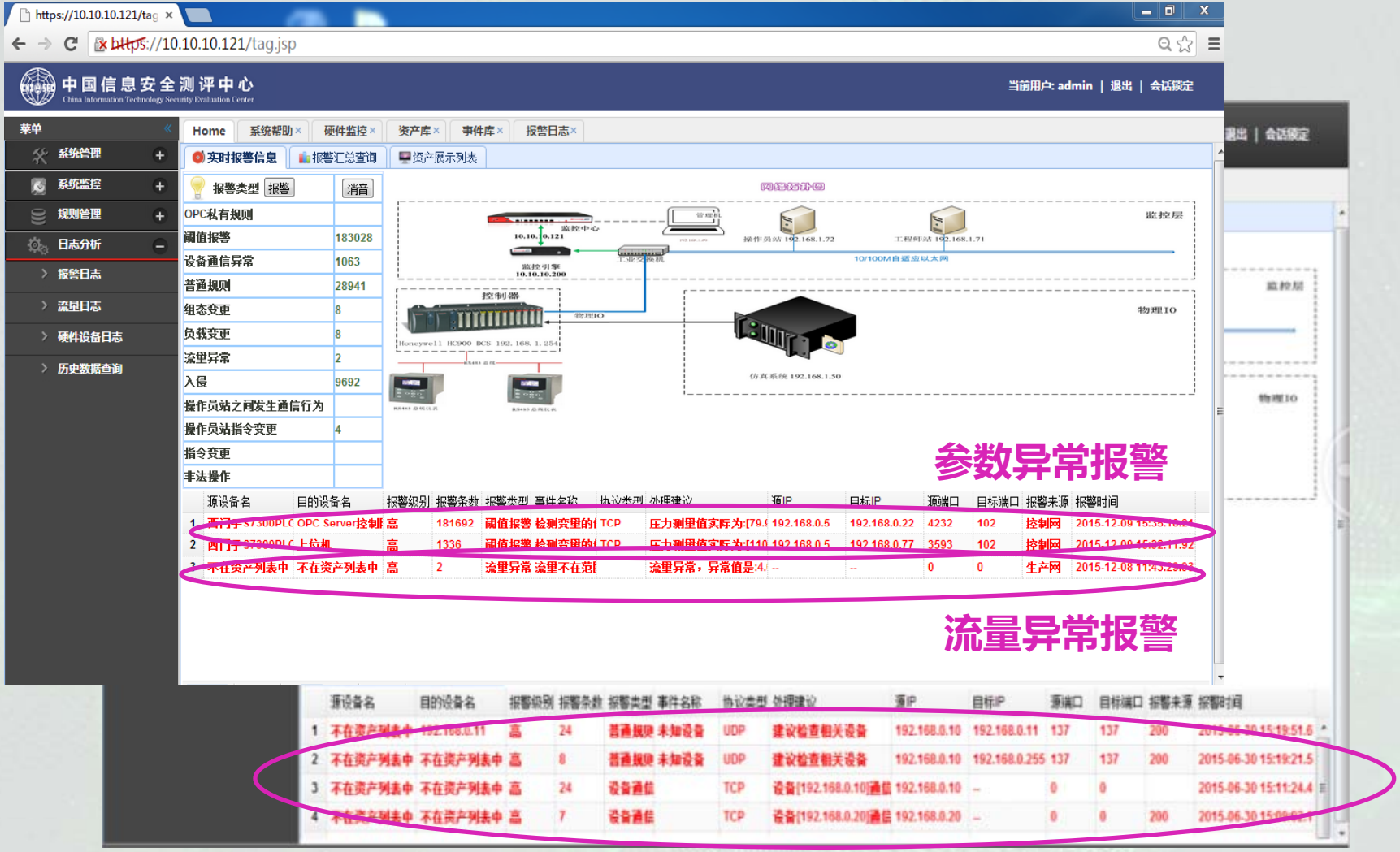


监测预警

- 由于缺少手段，我们对工控网络情况“一无所知”，直接造成“谁进来了不知道，是敌是友不知道，干了什么不知道”
- 旁路部署在工控网络中，避免影响生产运行
- 分析工控网络数据，发现渗透、病毒等威胁，感知安全态势

聪者听于无声

明者见于未行


https://10.10.10.121/tag.jsp
中国信息安全测评中心
China Information Technology Security Evaluation Center
当前用户: admin | 退出 | 会话锁定
菜单
系统管理
系统监控
规则管理
日志分析
报警日志
流量日志
硬件设备日志
历史数据查询
Home
系统帮助
硬件监控
资产库
事件库
报警日志
实时报警信息
报警汇总查询
资产展示列表
报警类型 报警 消音
OPC私有规则
阈值报警 183028
设备通信异常 1063
普通规则 28941
组态变更 8
负载变更 8
流量异常 2
入侵 9692
操作员站之间发生通信行为
操作员站指令变更 4
指令变更
非法操作
监控层
物理IO
参数异常报警
流量异常报警
非授权接入报警

组件加固

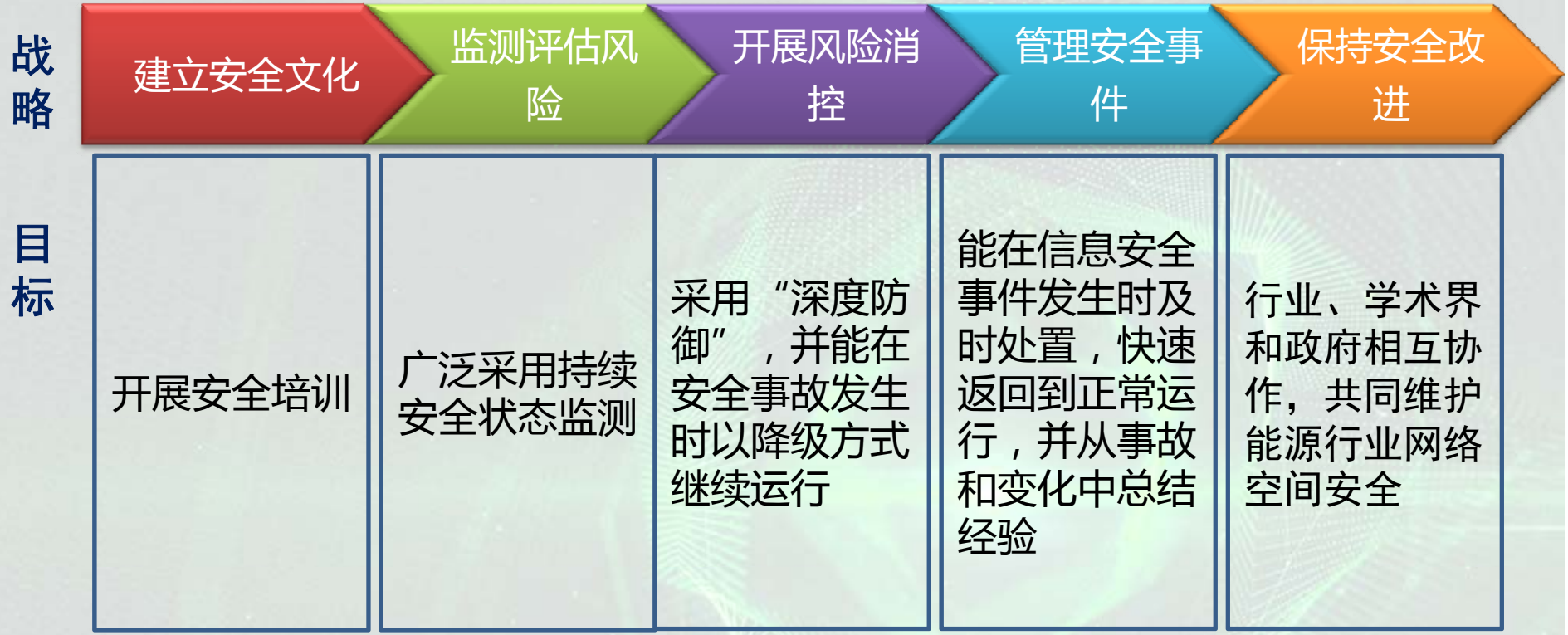
- 安全配置
  - 端口限制、地址限制、口令设置...
- U盘管控
  - 堵住U盘摆渡攻击的入口
- 应用白名单
  - 工控环境下的“杀毒”
  - 回避了“升级”困境
- 启用自带安全机制
  - 本质安全

各方协同，构建命运共同体

美国能源系统工控安全路线图对我们的启发

愿景：到2020年，实现韧性的能源供应系统的设计、安装、运行和维护，保持在信息安全攻击下维持关键功能的可生存性。

- 障碍：
  - 信息安全威胁是不可预期的
  - 老系统升级受限于设备和体系结构的固有局限性
  - 新解决方案难以在不中断运行情况下进行
  - 不充分的威胁、漏洞、事故和消控信息共享
  - 网络安全投资不足
  - 能源行业网络安全法规不确定性


战略
建立安全文化
监测评估风险
开展风险消控
管理安全事件
保持安全改进
目标
开展安全培训
广泛采用持续安全状态监测
采用“深度防御”，并能在安全事故发生时以降级方式继续运行
能在信息安全事件发生时及时处置，快速返回到正常运行，并从事故和变化中总结经验
行业、学术界和政府相互协作，共同维护能源行业网络空间安全

总结

- 工控系统的价值必然会吸引越来越多的外在攻击与渗透
- 工控网络的特点决定了工控信息安全技术必须重构
- 建立工控安全文化、形成工控安全生态是一场持久战

谢　谢