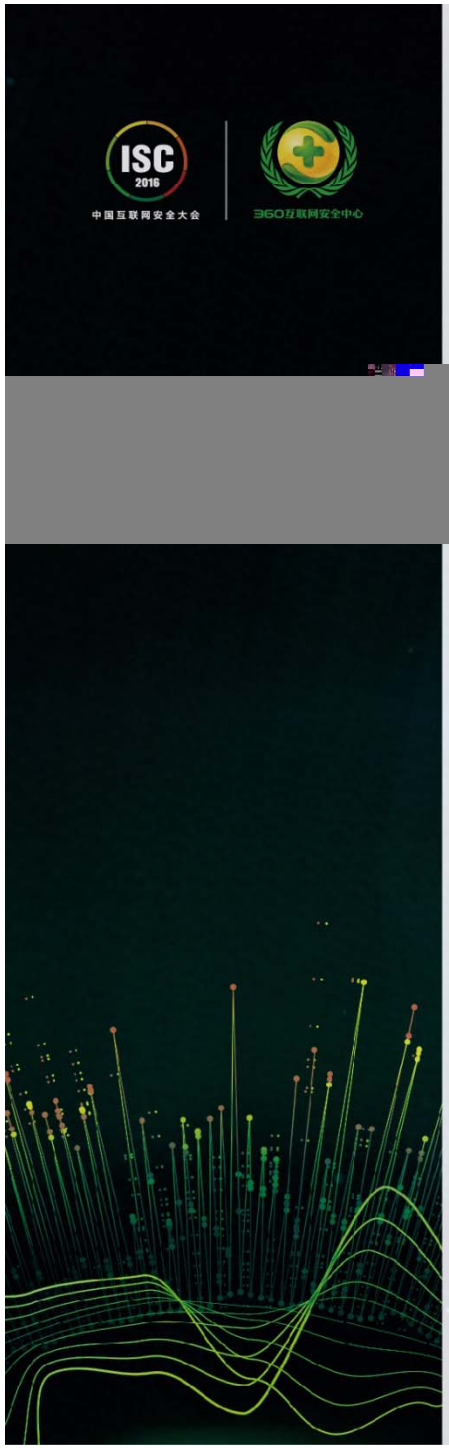
2016 中国互联网安全大会
China Internet Security Conference

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


ISC
2016
中国互联网安全大会
360互联网安全中心


ISC
2015
中国互联网安全大会
360互联网安全中心

- 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”

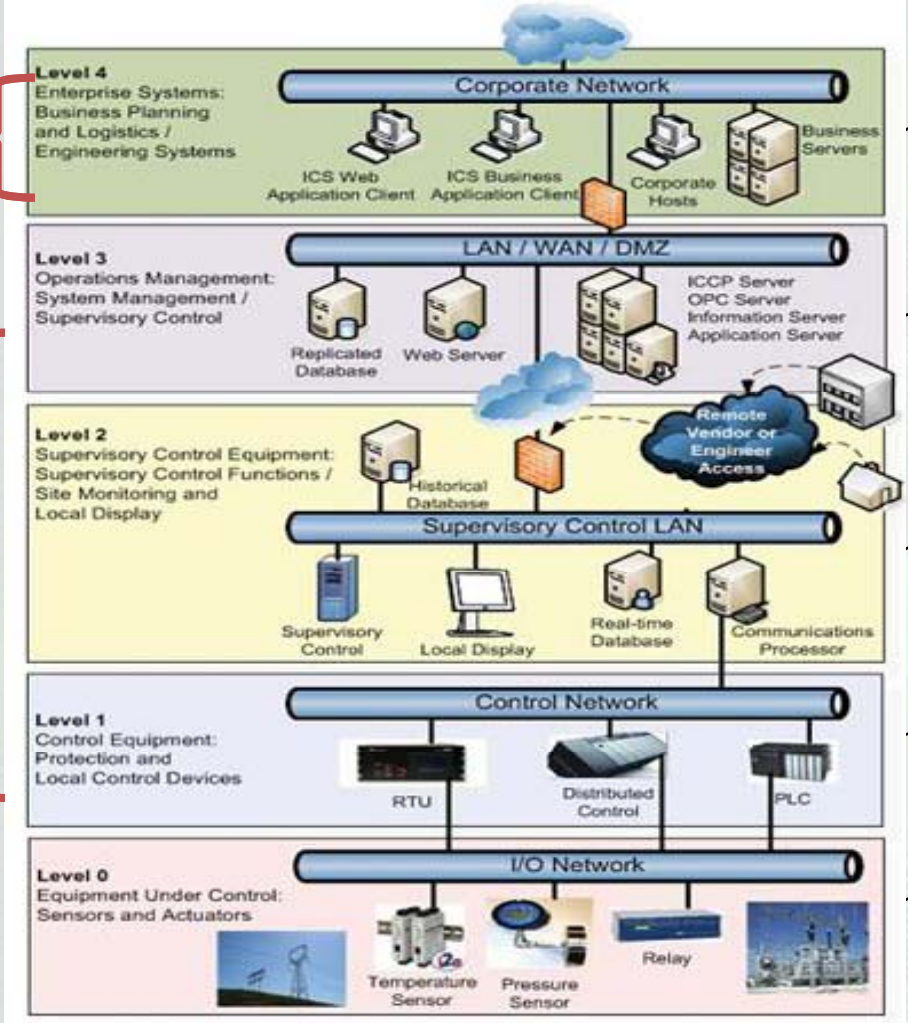





典型工控网络架构

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

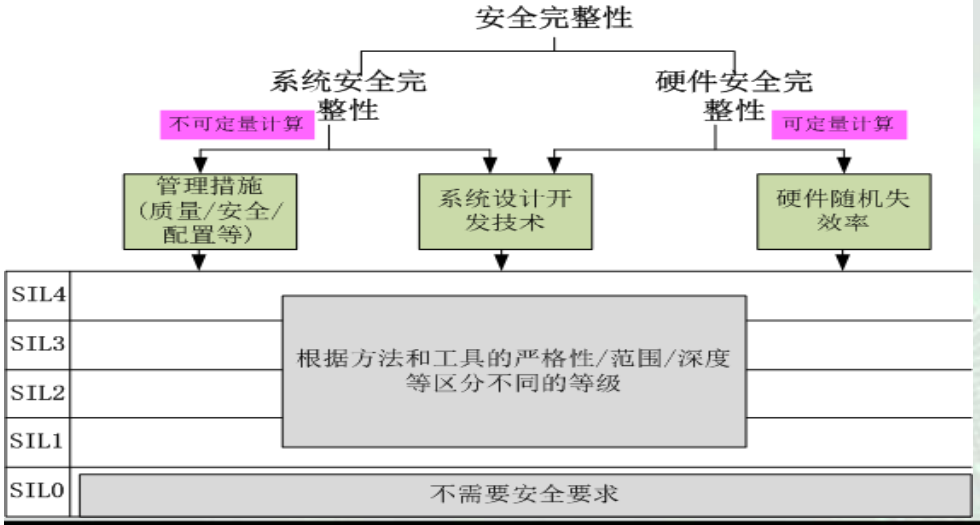
二者有交集，但有本质上的差别

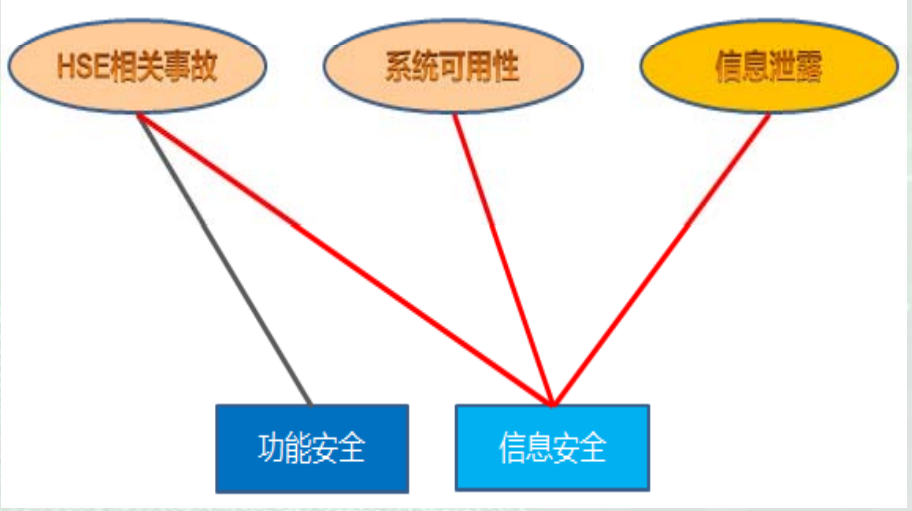
Safety

- 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

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






ISC
2015
中国互联网安全大会
360互联网安全中心

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
0-day

2014
Havex
OPC Server

2015

2016 PLC
Blaster

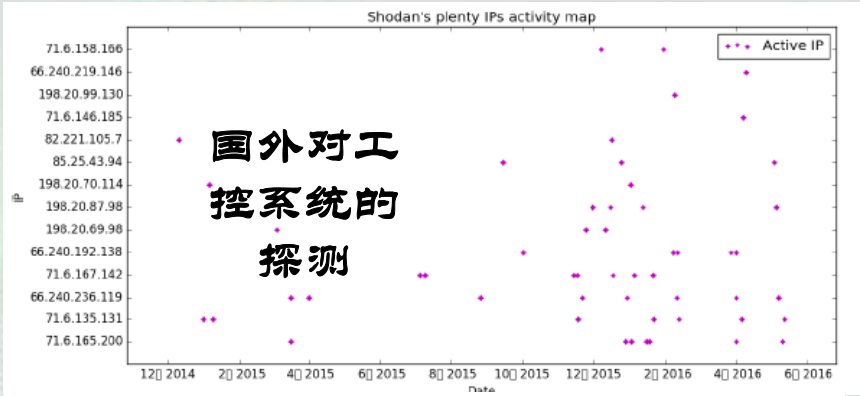
8000

2010-2011
Conficker

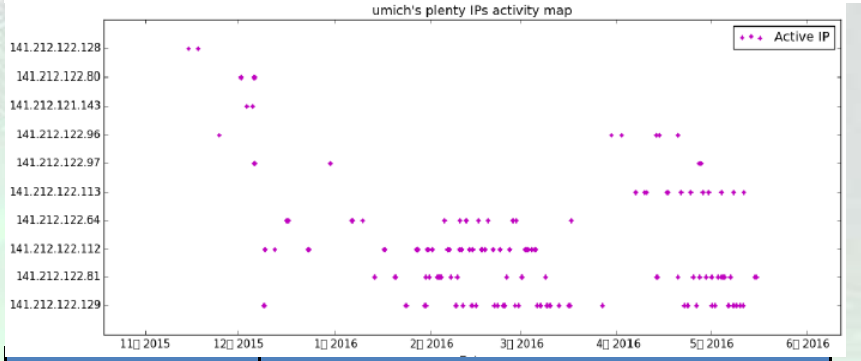
2014

2015
ISIS

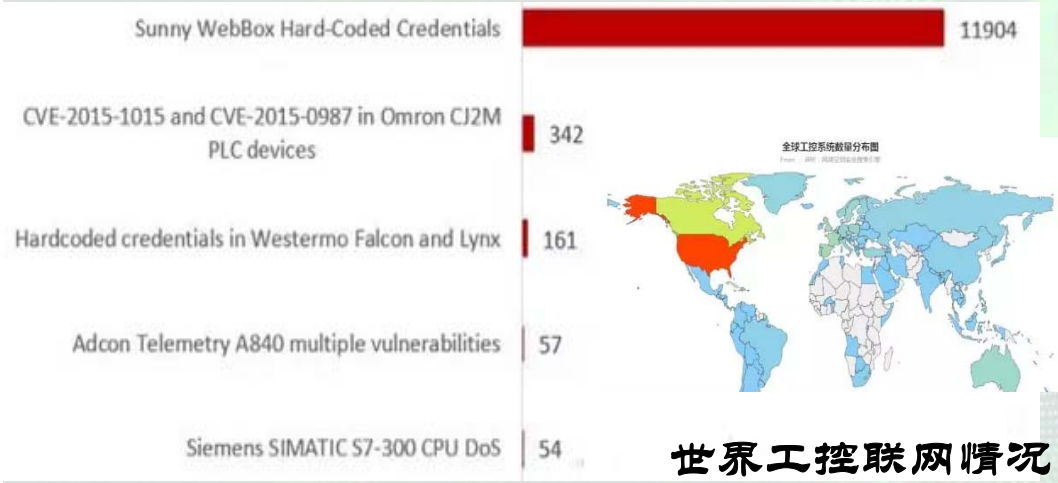
-
-
-
-
-



国外对工控系统的探测



卡巴斯基公布的联网工控设备漏洞

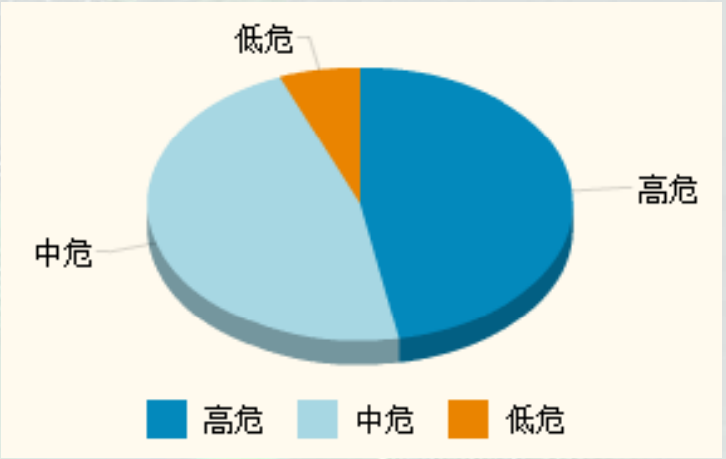


世界工控联网情况

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

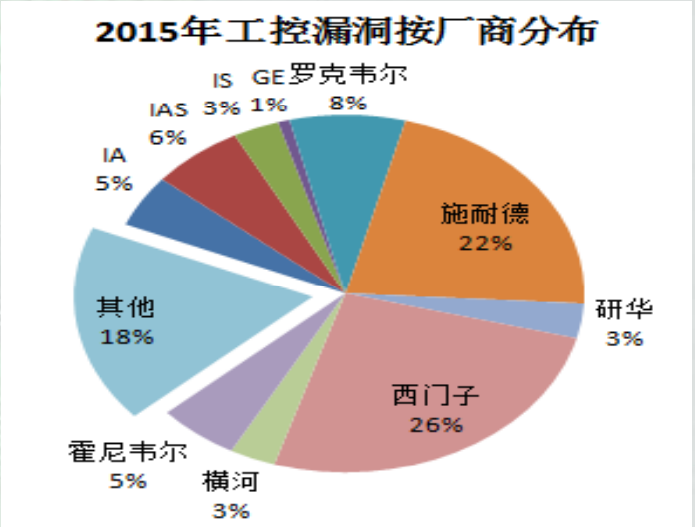
常见工控探测端口

-
  -
  -
-
  -

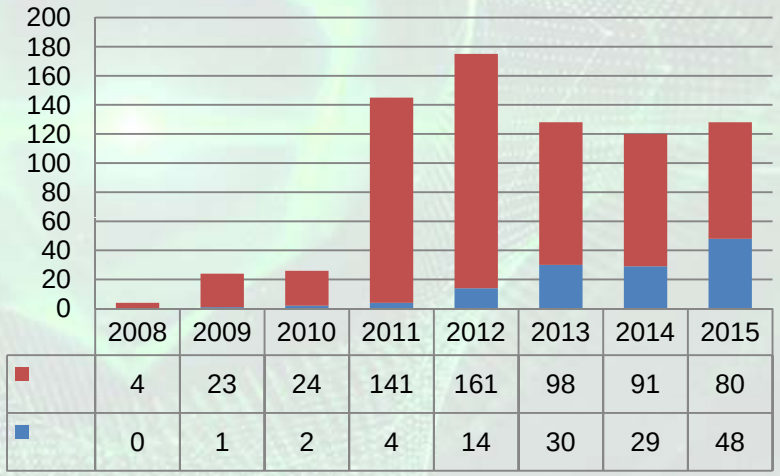


危害级别	高 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
影响产品	SIEMENS SIMATIC S7-300 CPUs with Profinet support < V3.2.12 SIEMENS SIMATIC S7-300 CPUs without Profinet support < V3.3.12
CVE ID	CVE-2016-3949
漏洞描述	Siemens SIMATIC S7-300 CPU是西门子（Siemens）公司的一款用于制造行业的模块化通用控制器。 Siemens SIMATIC S7-300 CPU系列设备存在拒绝服务漏洞。攻击者利用漏洞在一定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。

-
  -
  -
  -
-
  -
  -

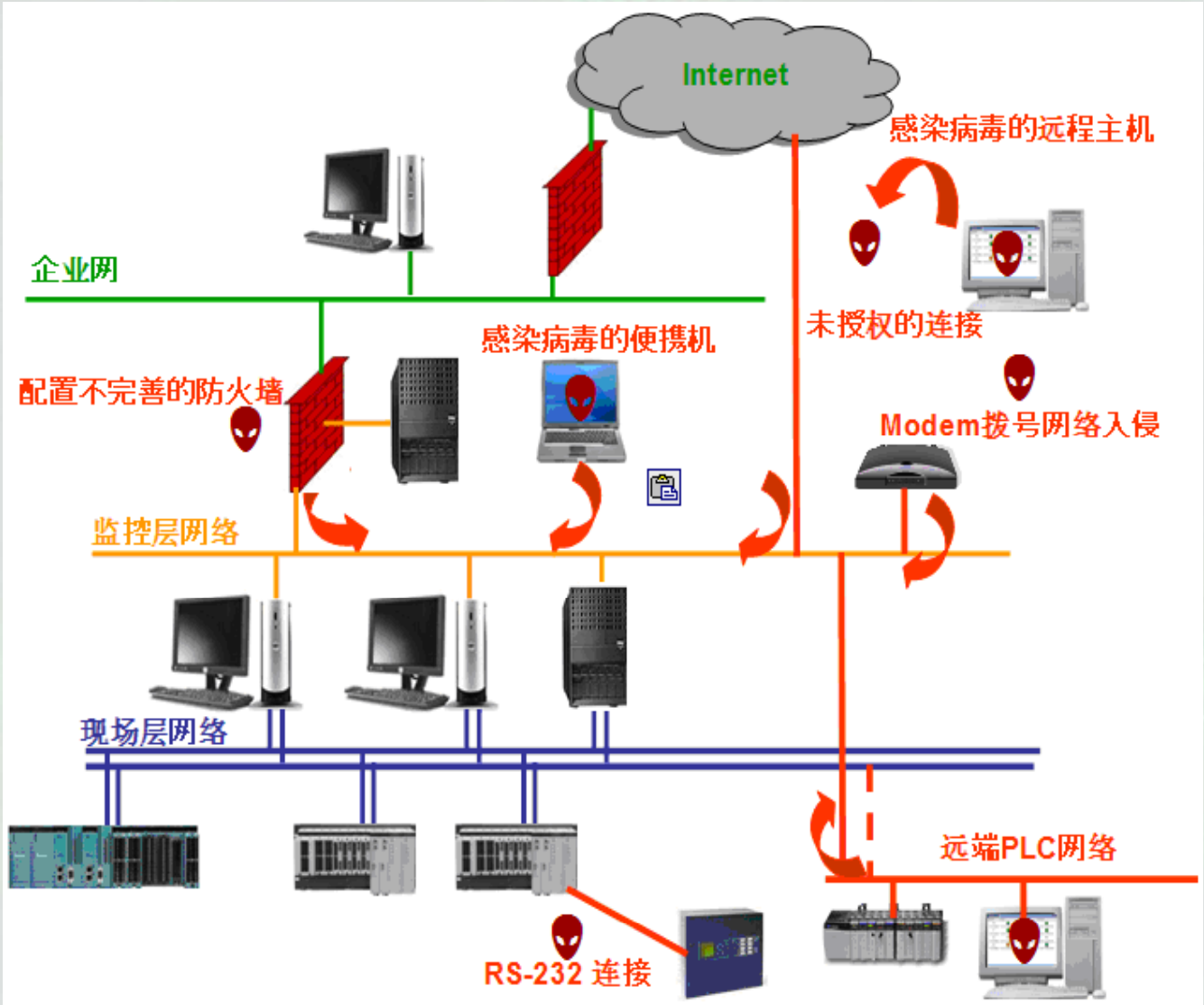


2008-2015年工控软硬件漏洞数量对比



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

- 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




ISC
2015
中国互联网安全大会
360互联网安全中心

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

- security
-

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

- 研发不易开展
- 用户不敢尝试
- 措施难以执行

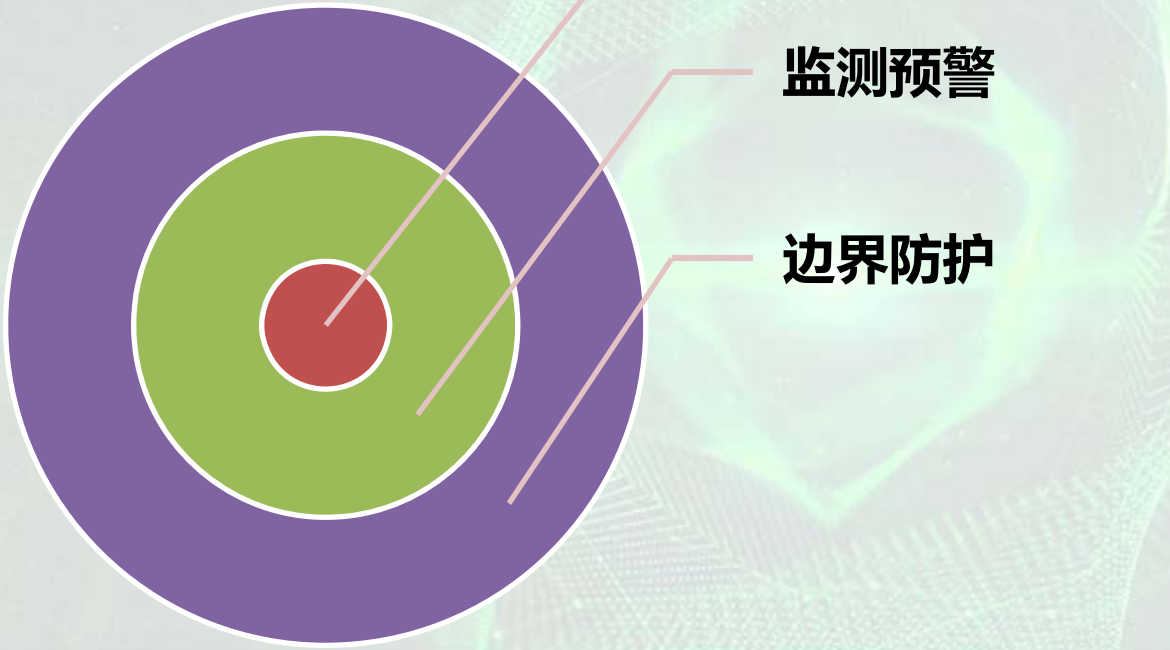
工控系统信息安全如同瓷器店里捉老鼠。瓷器很脆弱，我们既要能抓住老鼠，又不能毁坏瓷器。

-
  -
  -
  -
  -

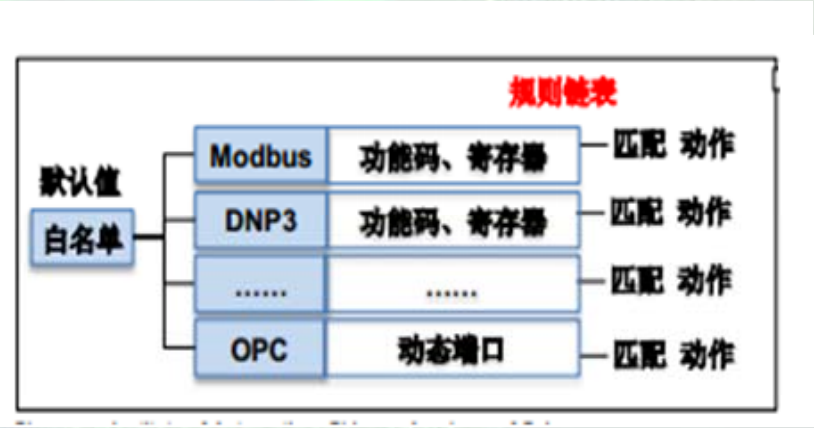
坚持管理+技术的信息安全传统套路

-
  -
    - 明确“由谁管”
  -
    - U盘管控、运维管控…
  -
    - 跨领域培训

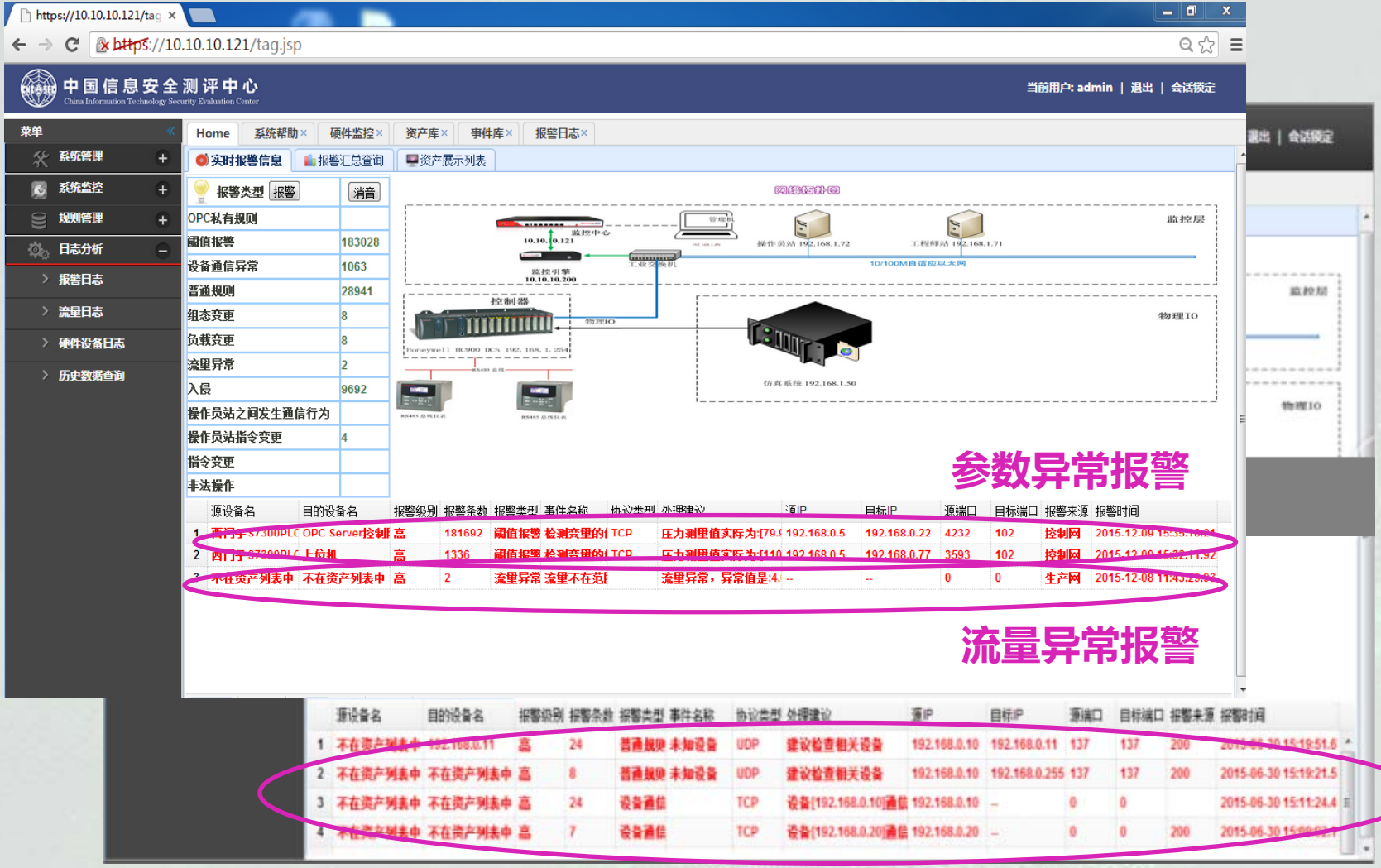
可借鉴大量已有标准规范、最佳实践，如IEC 62443、GB/T 30976、美国管道SCADA安全、21步提高工控安全最佳实践等等


组件加固
监测预警
边界防护

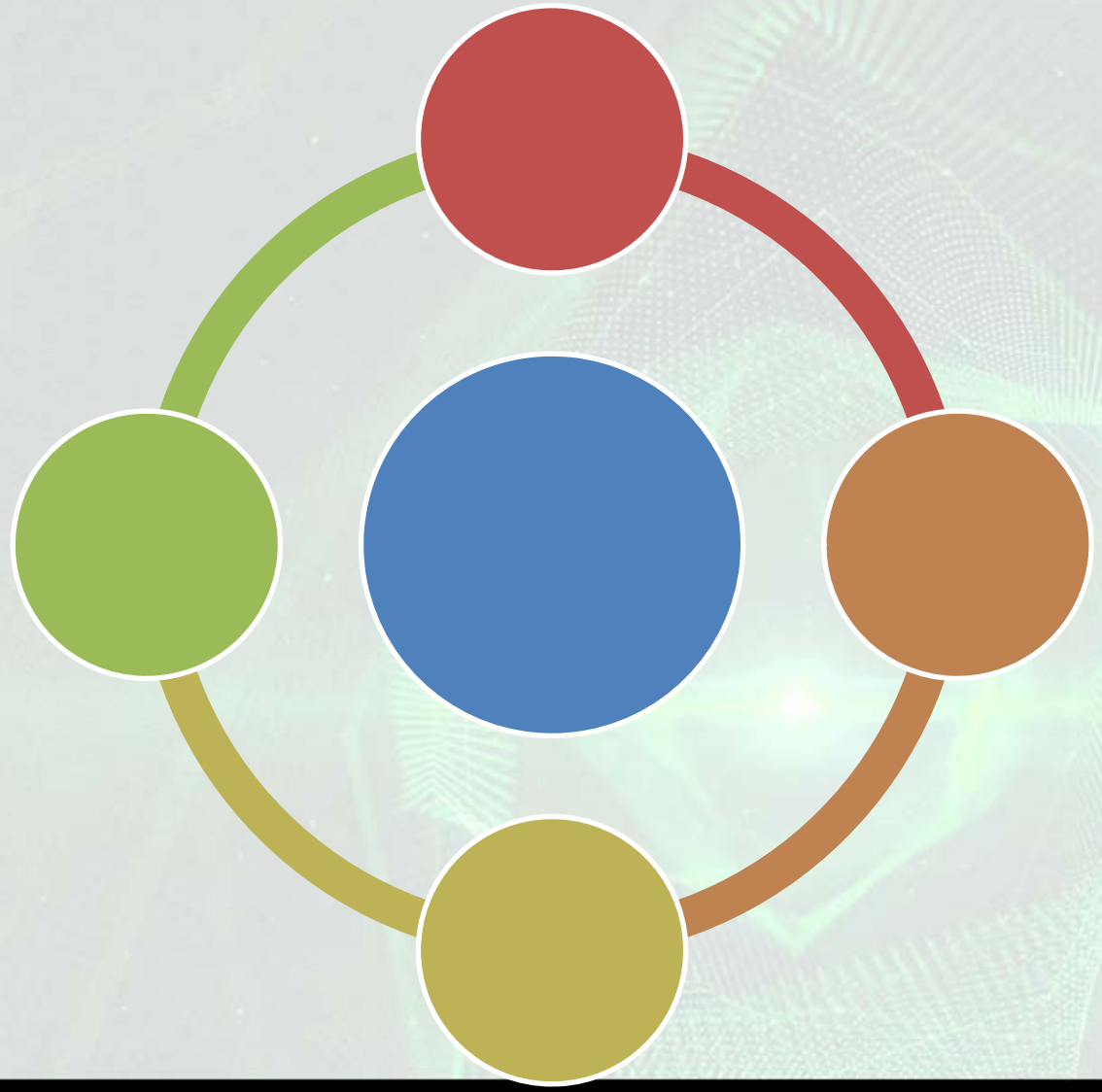
-
  -
  -
  -
-
  -
-
  -
    - Modbus、OPC、DNP3…
  -
    - 控制区→非控制区



- 谁进来了不知道，是敌是友不知道，干了什么不知道
- **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

-
  -
-
  -
-
  -
  -
-
  -



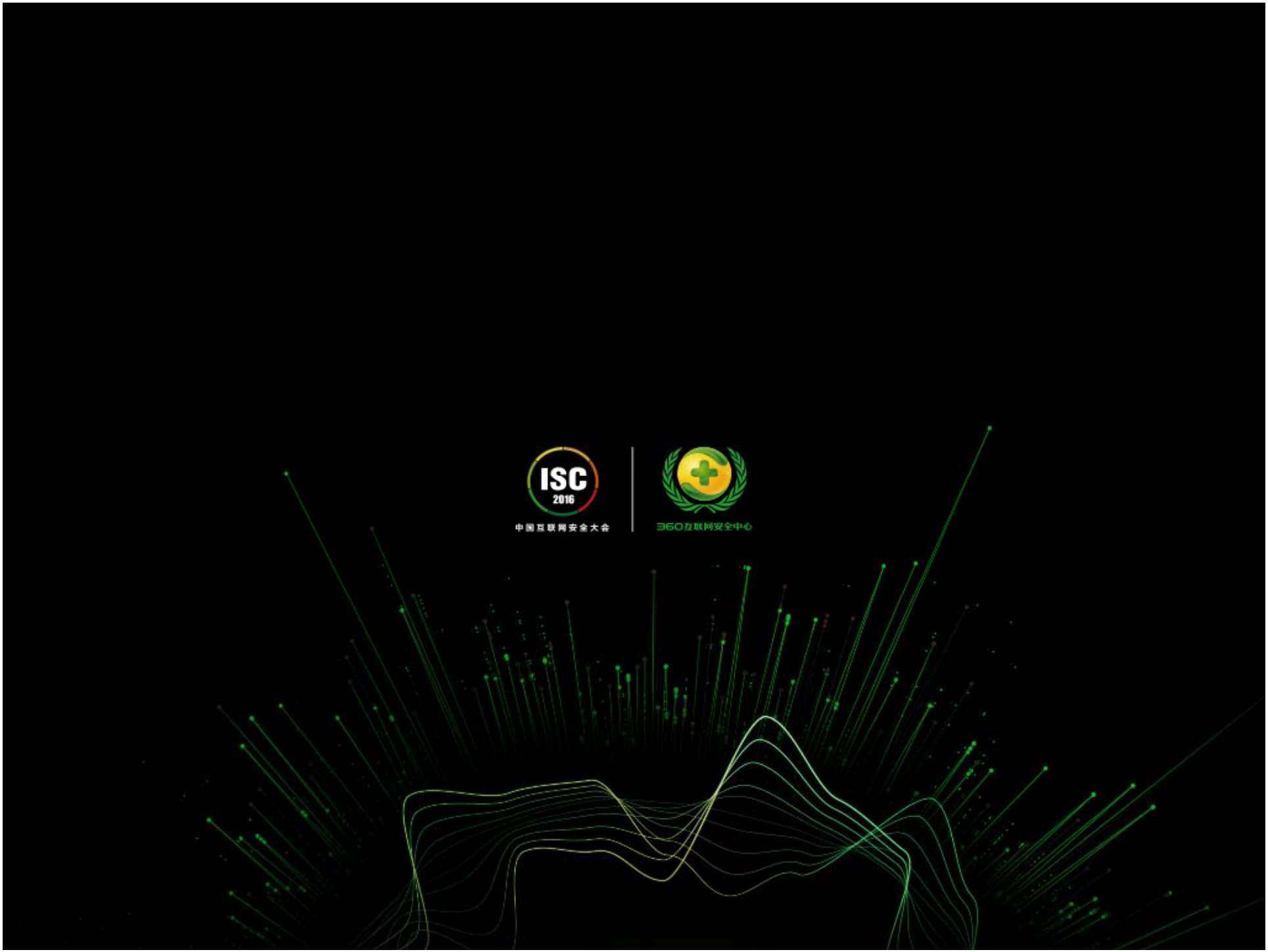
美国能源系统工控安全路线图对我们的启发

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。

-
  -
  -
  -
  -
  -
  -


战略
目标
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

-
-
-


ISC
2016
中国互联网安全大会
360互联网安全中心