C3安全峰会
CYBER | CLOUD | COMMUNICATION

我国工控系统安全技术研究的思考

孙利民
中国科学院信息工程研究所 研究员

C3

目录

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Speaker Topic 01

我国工控系统安全面临的挑战

工业控制系统

- 工业控制系统(Industrial Control Systems, ICS),是由各种自动化控制组件和实时数据采集、监测的过程控制组件共同构成，用于监测和控制工业生产过程，确保工业设备正常运行。（NIST SP800-82）
  - 其核心组件包括数据采集与监控系统(Supervisory Control and Data Acquisition, SCADA)、分布式控制系统(Distributed Control Systems, DCS)、可编程控制器(Programmable Logic Controller, PLC)、远程终端(Remote Terminal Unit, RTU)、人机交互界面设备(Human Machine Interface, HMI),以及确保各组件通信的接口技术。
  - 工业控制系统广泛应用于石化、水利、电力、冶金、生产制造等行业领域。

工业控制系统是国家基础设施的核心

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 2013年2月12日，美国总统奥巴马签发总统政策指令< Presidential Policy Directive --Critical Infrastructure Security and Resilience>（PPD-21），指出国家重大基础设施所包含的16个工业部门。


信息处理


通信系统


金融系统


政府部门


关键制


水利设


公共卫生


供水系统


核电系统


应急处理


能源系统


国防军业


交通运输


食品系统


化工系统


商业设施

The White House
Office of the Press Secretary

For Immediate Release February 12, 201

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

工业控制系统是国家基础设施的核心

- 2016年12月27日，《国家网络空间安全战略》明确界定关键信息基础设施的保护范畴，**国家关键信息基础设施是**指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。

工控系统遭受前所未有的安全威胁

C3安全峰会
CYBER | CLOUD | COMMUNICATION

2011年美国伊利诺伊州供水系统

2014年Havex病毒威胁基础设施

2008年波兰城市轨道交通脱轨

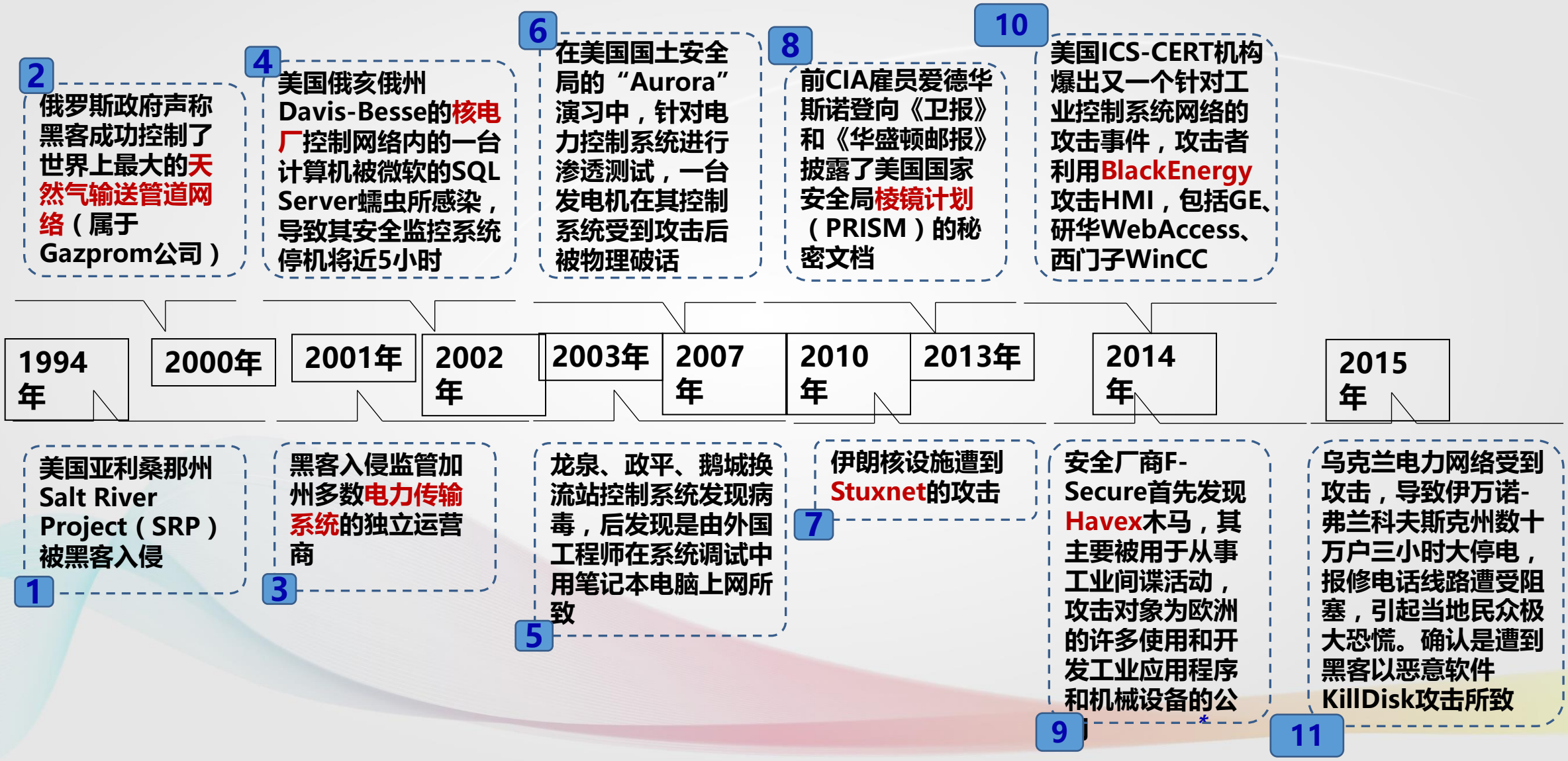
2014年英国的石油管道被引

2015年12月乌克兰电网停电

2010年震网破坏伊朗核设施

2001年澳大利亚污水泄露

工控安全的典型事件


1994年
2000年
2001年
2002年
2003年
2007年
2010年
2013年
2014年
2015年
1 美国亚利桑那州Salt River Project（SRP）被黑客入侵
2 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（属于Gazprom公司）
3 黑客入侵监管加州多数电力传输系统的独立运营商
4 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蠕虫所感染，导致其安全监控系统停机将近5小时
5 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用笔记本电脑上网所致
6 在美国国土安全局的“Aurora”演习中，针对电力控制系统进行渗透测试，一台发电机在其控制系统受到攻击后被物理破话
7 伊朗核设施遭到Stuxnet的攻击
8 前CIA雇员爱德华斯诺登向《卫报》和《华盛顿邮报》披露了美国国家安全局棱镜计划（PRISM）的秘密文档
9 安全厂商F-Secure首先发现Havex木马，其主要被用于从事工业间谍活动，攻击对象为欧洲的许多使用和开发工业应用程序和机械设备的公
10 美国ICS-CERT机构爆出又一个针对工业控制系统网络的攻击事件，攻击者利用BlackEnergy攻击HMI，包括GE、研华WebAccess、西门子WinCC
11 乌克兰电力网络受到攻击，导致伊万诺-弗兰科夫斯克州数十万户三小时大停电，报修电话线路遭受阻塞，引起当地民众极大恐慌。确认是遭到黑客以恶意软件KillDisk攻击所致

2016年工控安全事件

- **美国**
  - 2016年2月黑客组织AnonSec公开约250G的NASA数据
  - 2016年3月美国水处理和流控制操作系统遭黑客入侵
  - 2016年8月达美航空公司飞机因网络攻击停飞
- **以色列**
  - 2016 年 01 月 28 日，能源与水力基础设施部称
  - 该国电力供应系统受到重大网络攻击侵袭
- **德国**
  - 2016年4月，德国Gundremmingen核电站遭到攻击
- **澳大利亚**
  - 2016年10月，外国间谍入侵澳大利亚关键基础设施网络
- **乌克兰**
  - 2016年二月，Black Energy被曝再次攻击乌克兰矿业和铁路系统
- ……

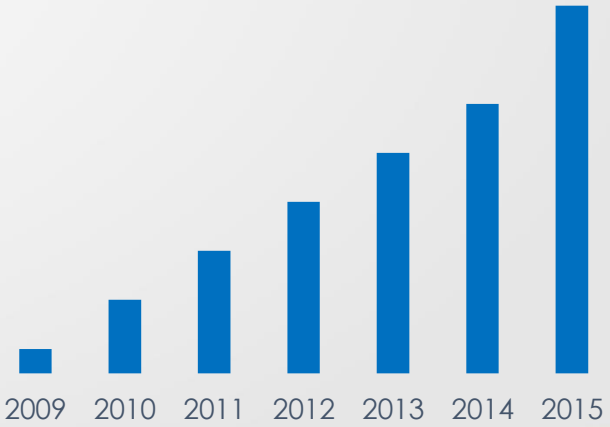
中国是全球网络攻击最大受害国

C3安全峰会
CYBER | CLOUD | COMMUNICATION

CN ERT/CC
国家互联网应急中心

国家互联网应急中心发布《2016年中国互联网网络安全报告》：2016年互联网应急中心发现网络安全事件超过**12万起**，我国网络空间安全形势不容乐观。

- 自2009年以来网络攻击增长15倍
- 其中30%是针对国家基础设施
- 近期案例：wannacry病毒



工控系统的特点

IT 信息传输的通用平台

ICS 与物理世界进行实时交互

对比点	工业控制系统	IT信息系统
安全目标	可信的物理世界的感知 可靠的物理世界的反馈控制	可信信息获取、处理与存储
体系架构安全焦点	首要是边缘客户端，其次是中央服务器	服务器以及其上的信息
未预期后果	安全工具必须进行充足离线测试，确保系统正常运行	安全方案可以参考典型IT系统设计
实时性	自治决策型系统，对控制事件需实时响应	允许一定程度上的网络延迟和阻塞
生命周期	部署和开发周期长，更新换代慢15~20年	系统发展更迭速度快，3~5年
连续性	一旦上线，不允许中断	允许重启和宕机。补丁可随时、自动完成
通信协议	大量专用和私有协议，适用于多种应用	采用统一的TCP/IP协议
系统操作	专有操作系统，软件变更比较复杂	经典操作系统，升级简单
资源限制	前端设备嵌入物理环境，资源有限	有足够的资源进行安全策略的部署

工控系统安全漏洞-数量

- **国内外网站工控漏洞数量统计**
  - ICS-CERt的数据表明，虽然工控安全越来越被关注，但工控漏洞的数量并没有减少，相反还有逐年增加的趋势
  - CNVD的数据显示，2010年之后工控漏洞数量显著增长，出现此趋势的主要原因可能是2010年震网病毒出现后，攻击者和安全人士对工业控制系统的关注显著增加

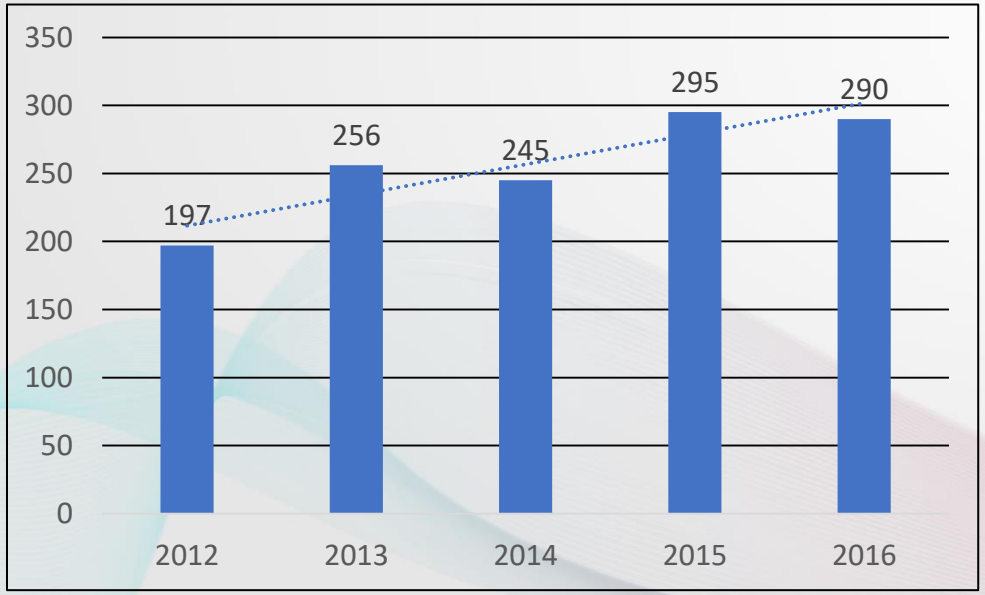


图1.ICS-CERT上2012-2016年工控漏洞走势图

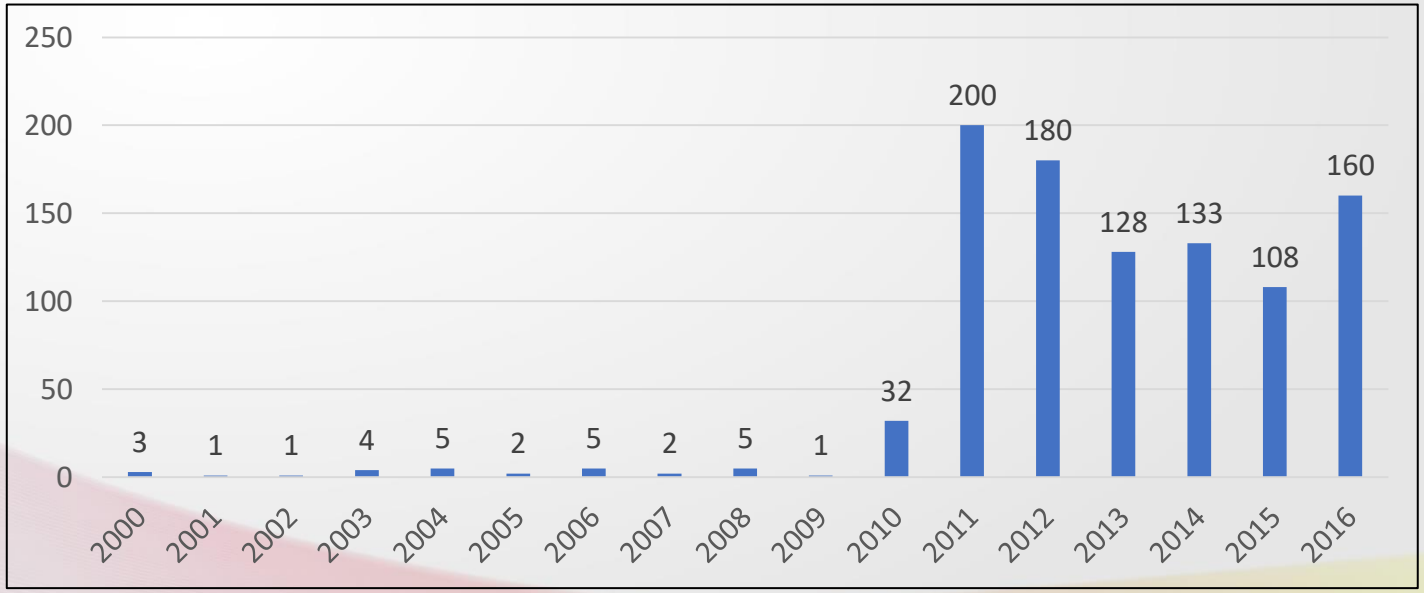
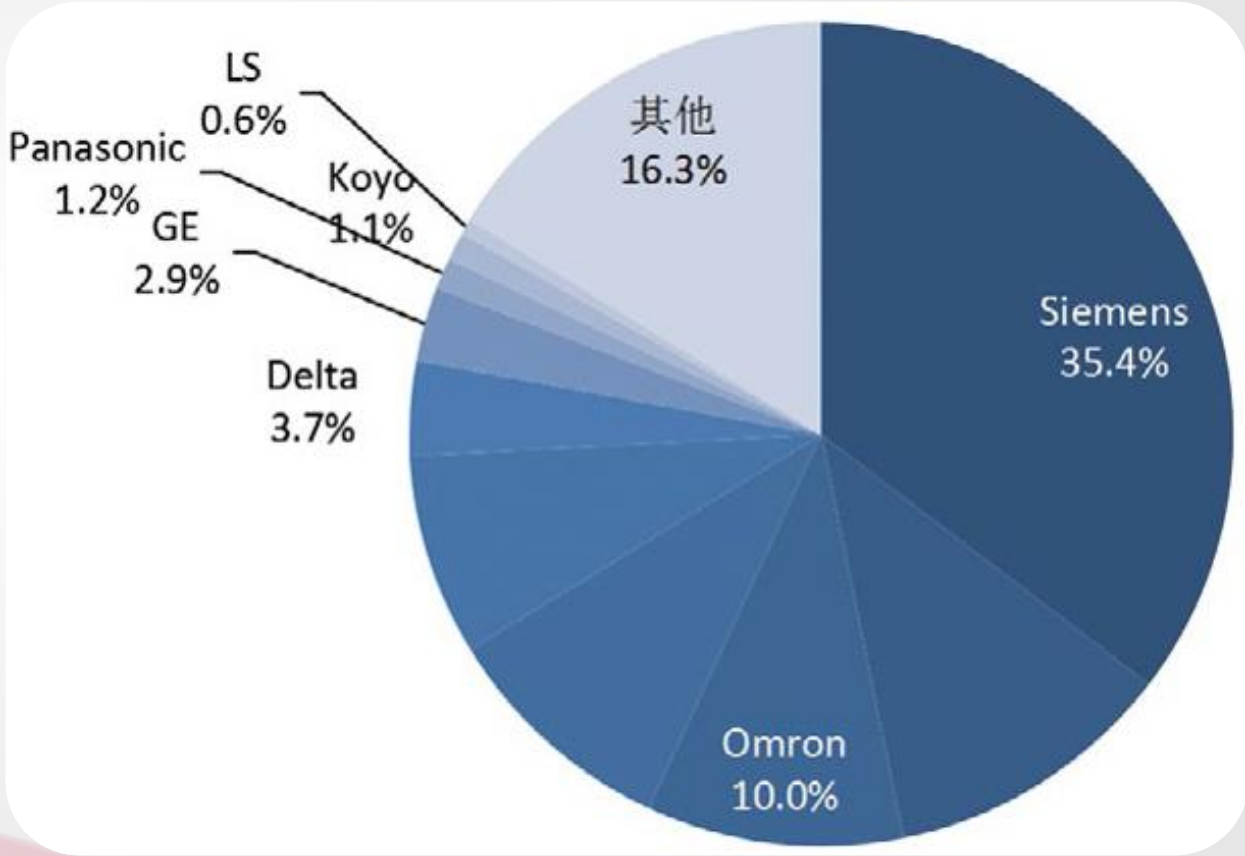


图2.CVND上2000-2016年工控漏洞走势图

国内工控安全现状

- 高端PLC依赖国外，超过80% PLC设备、65%的操作员站为国外的
- 主流/大型工控设备依赖国外，DNC设备基本是国外的
- 2016年工控系统安全检查
  - 5.5万家单位自查，2.6万家单位现场检查
  - 共发现漏洞46万余个，高危漏洞9.8万个。



国内工控系统安全-面临更大的挑战

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- **工控系统更新换代慢**
  - 遗留系统 + 在建系统 + 研发系统
  - ***遗留系统存在众多漏洞、后门***
- **主流/大型工控设备*国外厂商为主***
  - 应急处理、备份处理
  - 远程维护问题
- **工控设备与信息安全产品是分离的**
  - 工控设备厂商与信息安全公司两类企业
  - 工控设备与安全产品没有很好结合
- **工控系统应用区域广、涉及面多**
  - 石油、天然气、水利等管道数千公里
  - ***攻击面大***

如何统一规划和考虑？

如何进行安全监测与应急处置？

如何实现系统的内生安全？

如何部署全方位的安全防护？

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Speaker Topic 02

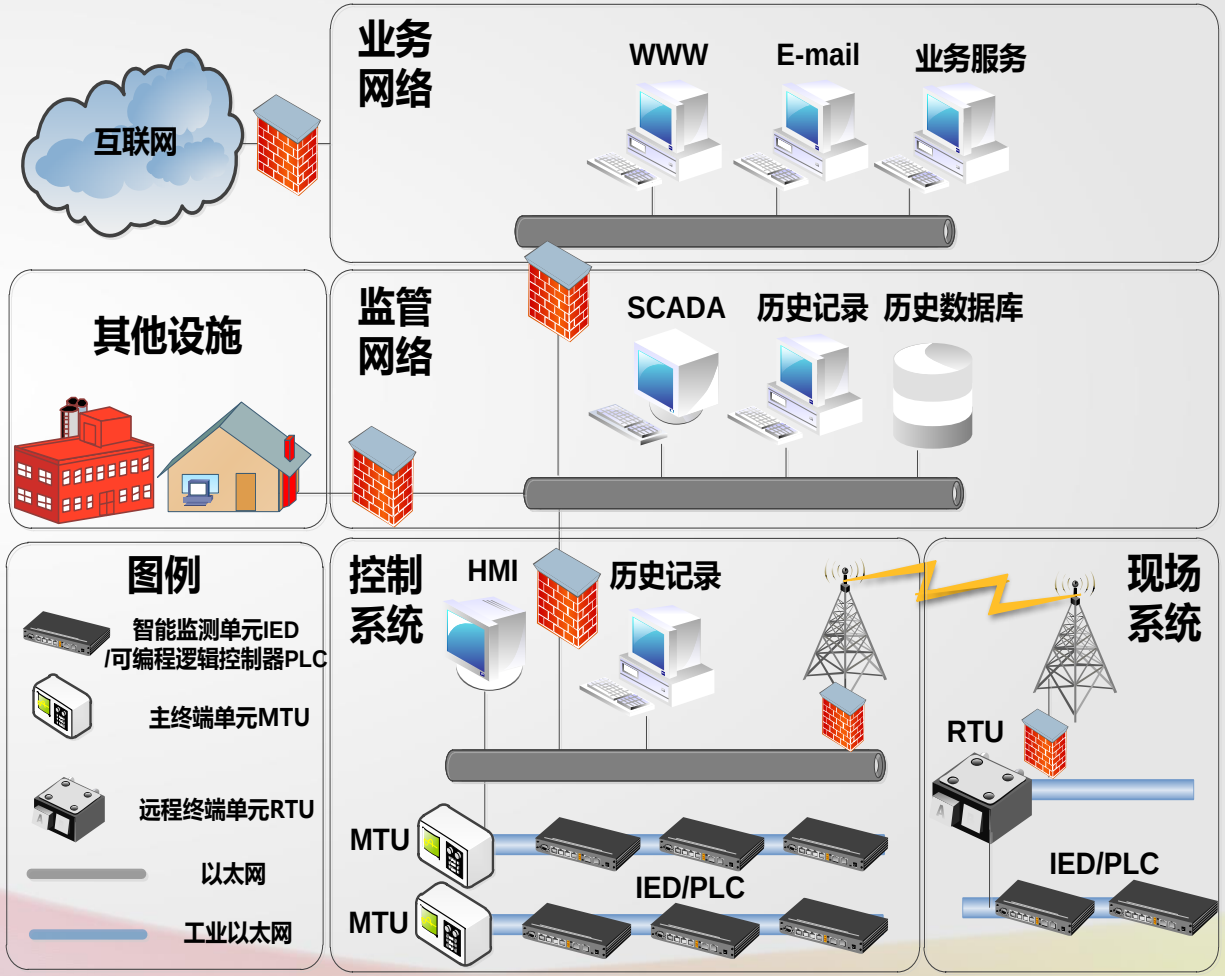
工控系统安全防护方案的思考

工控系统-目前常规安全防护策略

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- **常规-防护策略**
  - 建立安全区域：不同安全区域、DMZ区域
  - 边界防护设备：防火墙、网闸、IDS/IPS
  - 主机防护设备：主机加固、U盘监管
  - 监管预警：配置检查、安全检测/审计

- **漏洞挖掘、漏洞扫描、漏洞补丁管理**



常用安全防护策略的分析？

- **工业防火墙**
  - 是一种基于预先确定的安全规则来监视和控制网络进出流量的网络安全设备
  - 典型防火墙是建立在可信任、安全的内部网络和不安全或不被信任的外部网之间的一个屏障
- **工控系统**
  - 很多工控设备是国外产品，生成年代比较久，没有详细的资料
  - 工控系统的运行过程是在本质上是联系的，实时性强，安全要求高
- **工业防火墙效果不好**
- **国家电网：十六字安全防护策略**
  - **安全分区、网络专用，横向隔离、纵向认证**

常用安全防护策略的分析？

- **白名单机制？**
  - 白名单是一个列表或者实体的注册表，在列表上的实体是可以节搜、获准和/或认可的
  - 常见的白名单有用户白名单、资产白名单、应用程序白名单等
  - 体现工控贴点：特定操作人员、在特定设备上、在特定时间、按照设定的操作规范、操作规定的设备，达到设定的状态或结果
- **工控系统现状**
  - 工控私有协议很多，往往不公开
  - 不同工控系统的用户，操作流程也多种多样；一个用户厂家也是动态变化
- **白名单机制实现困难，不能完全掌握工控系统知识**

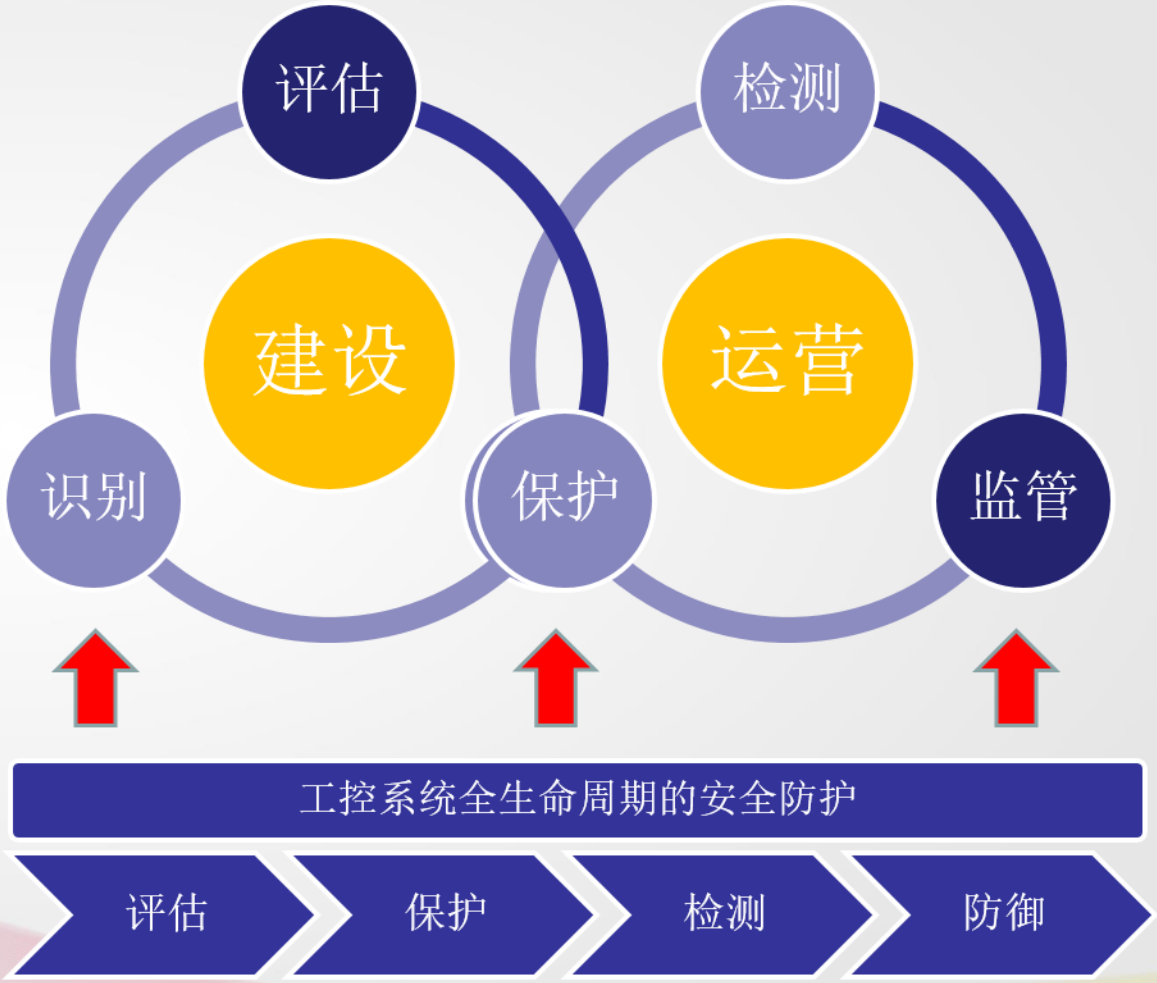
我国工控系统安全面临的挑战？

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- **国内工控系统的安全现状- Security issues of ICS in China**
  - 主流/大型工控设备还是国外厂家为主 – most of the ICS devices are not made in China
  - 工控系统的更新换代慢 – it’s hard to upgrade the industrial control systems
  - 现有工控系统的漏洞多 – there are a lot of vulnerabilities in current industrial systems
  - 被后门被漏洞 – it’s easy to be hacked through backdoors and vulnerabilities
- **现实情况下如何保证工控系统的安全？How to secure ICS?**
  - **相当长时间内存在“被漏洞、被后门”，在现实环境下如何办？**
  - **如何实现工控系统的短、中、长期安全？**
  - **工控私有协议多，工控用户操作不规范的情况下，如何办？**

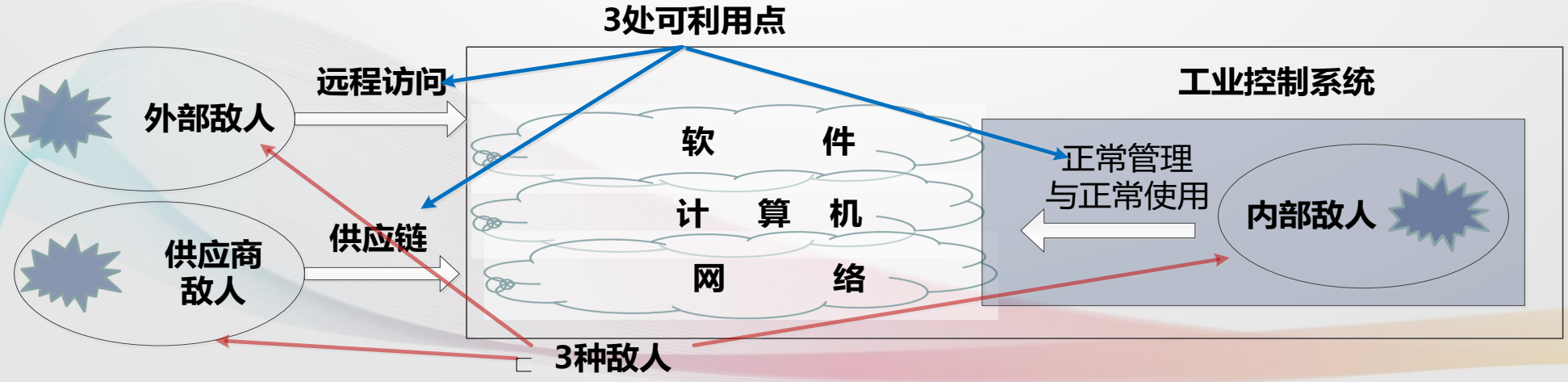
长远考虑1：工控系统-全生命周期的安全防御体系

- **建设期**
  - 识别：设备识别与安全脆弱性分析
  - 评估：系统安全风险的自动推演
  - 保护：依据评估结果，制定保护方案
- **运营期**
  - 保护：部署保护设施
  - 检测：实时主动发现未知安全攻击
  - 监管：全局的安全态势感知和响应



长远考虑2：工控系统-全链条的安全监管体系

- **对工控系统的的攻击点**
  - 设备生产商、供应商、建设集成商、操作人员、管理人员等 + 外部敌人
- **工控系统全链条的安全监管**
  - 设备生产→供应链→建设→使用→维护→应急
  - 软硬件备份 + 安全检查/监测 + 安全管理



C3安全峰会
CYBER | CLOUD | COMMUNICATION

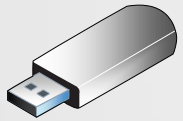
Speaker Topic 03

工控系统安全技术的思考

工控系统攻击路径

从外部网络，通过黑客技术或钓鱼渗透到企业网络

从外部网路，通过无线连接，入侵感染工控网络

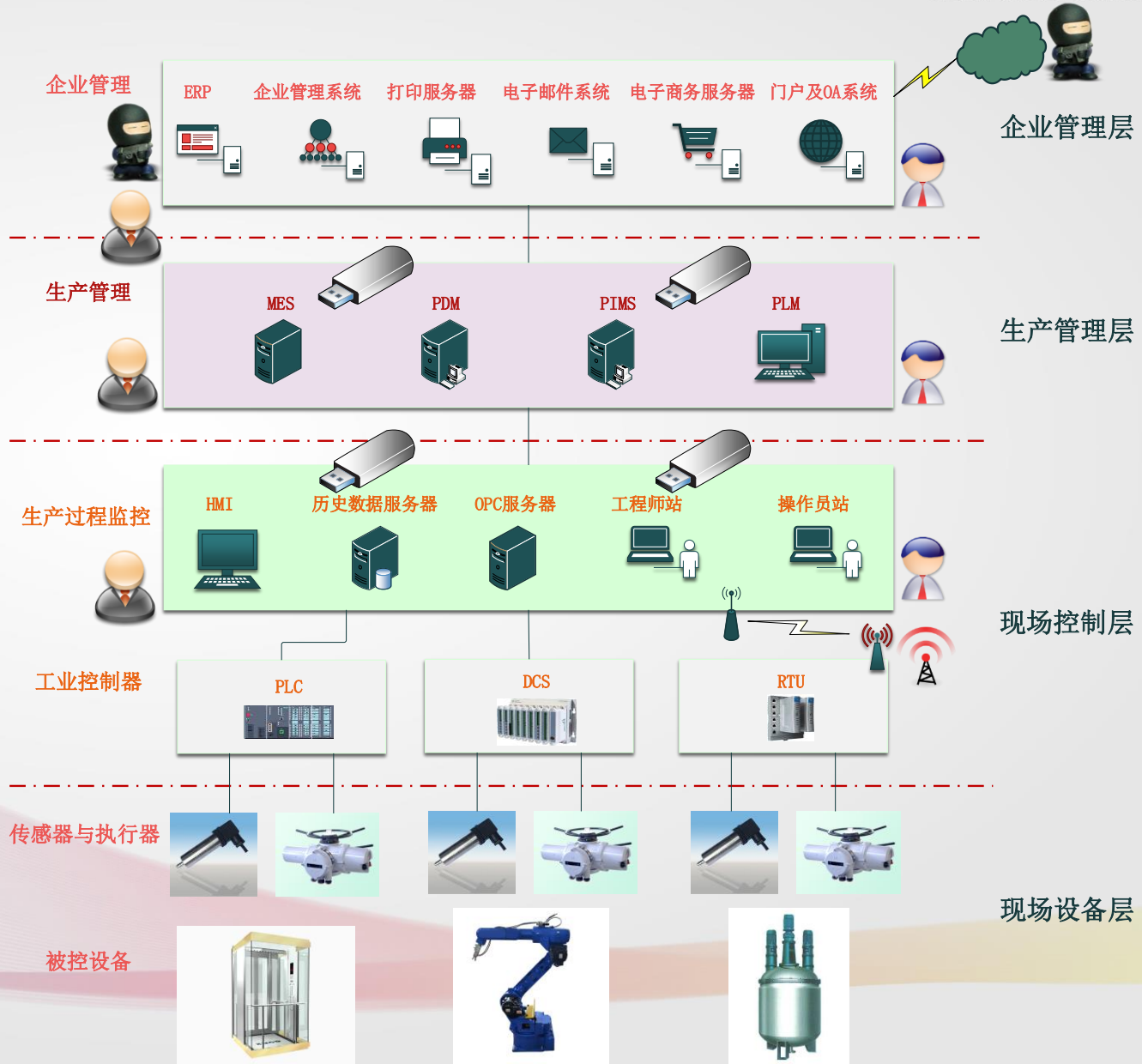


移动介质，通过USB移动存储介质，将病毒、蠕虫传播到工控网络中

从内部网络，恶意员工主动或误操作等

从内部网络，利用被感染的设备，破坏和攻击

环境设备如摄像头，被渗透后用来攻击工控网络

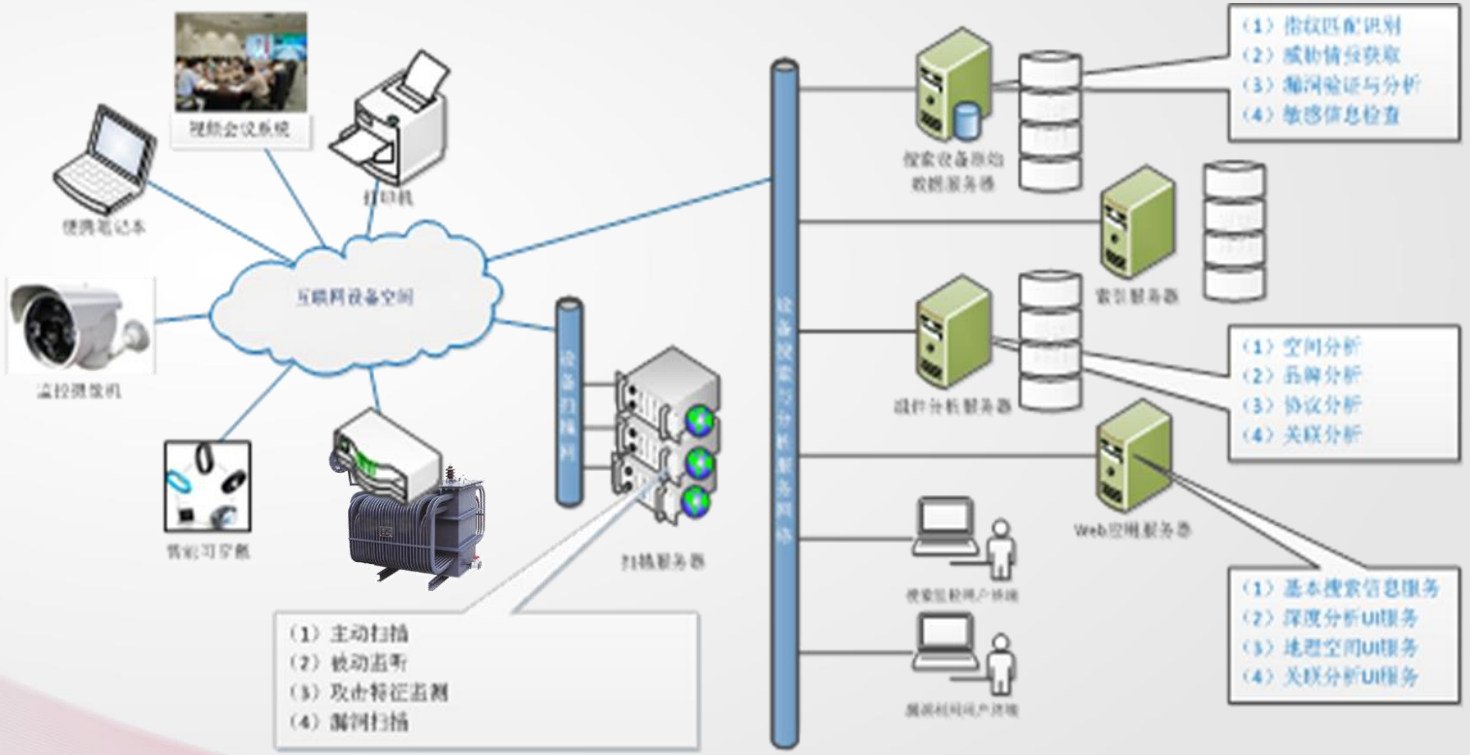


近期考虑：渐进式主动安全监管防护策略

- **渐进式主动安全监管防护的策略**
  - **原则：不改动-少改动-整合设计**
  - 【外】非法外联
  - 【内】资产清点与非法接入与服务、内部攻击发现
  - 【表】基于旁路的流量深度安全感知、物联网环境安全感知
  - 【里】MTD、内生安全、主动防御
- **渐进式主动安全监管防护的实践**
  - 法器1. “网络雷达” - 网络设备搜索与定位发现非法外联
  - 法器2. “企业纠察” - 内网设备清点与安全评估
  - 法器3. “神秘之船” - 工控系统安全防护的基础-内外网的攻击发现
  - 法器4. “隐形监管” - 基于旁路的流量深度感知、物理环境感知
  - 法器5. “内生安全” - 控制与安全的融合形成自身免疫

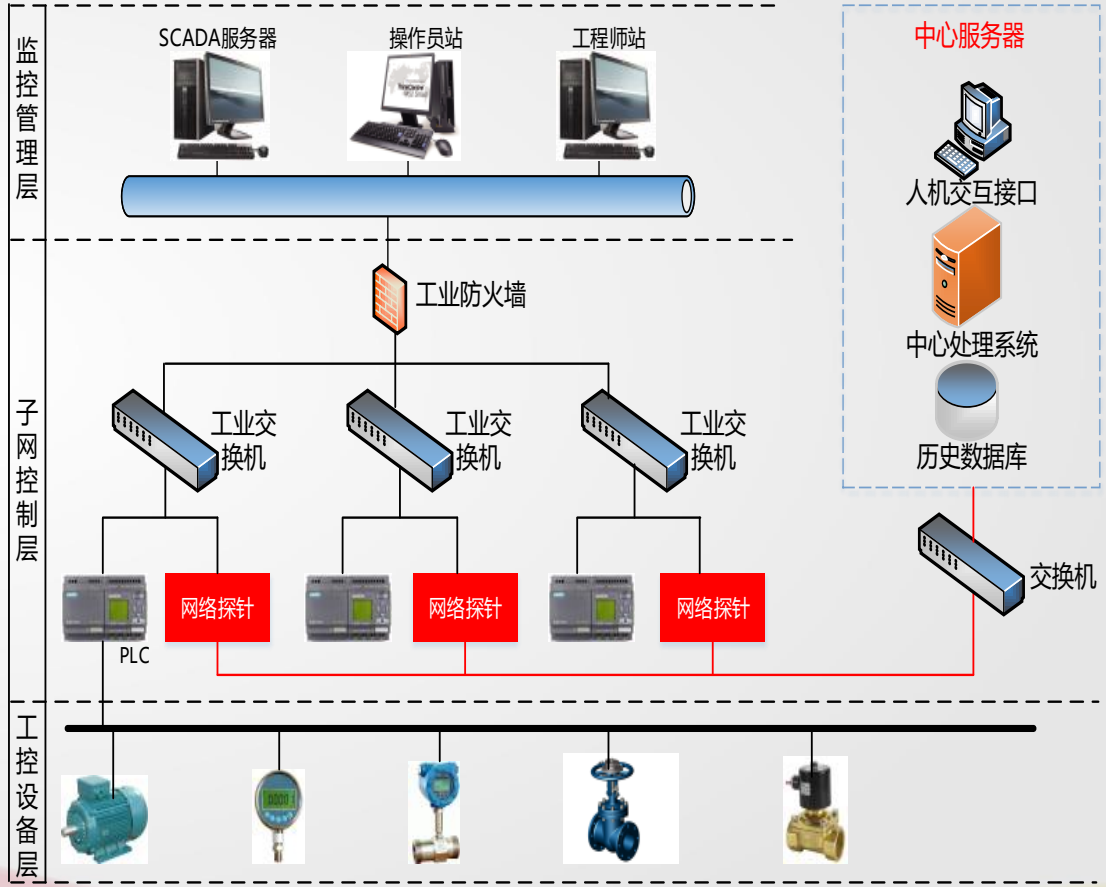
1. “网络雷达”- 工控设备搜索与定位-违规外联

- **大量安全事件原因：非法外联**
- **工控设备搜索与安全检测系统**
  - 构建指纹库
  - 构建漏洞库
  - 位置信息库
- **关键技术**
  - 自动化特征提取与指纹生成技术
  - 快速精细化探测扫描技术
  - 漏洞挖掘与脆弱性分析技术
- **工控设备发现**



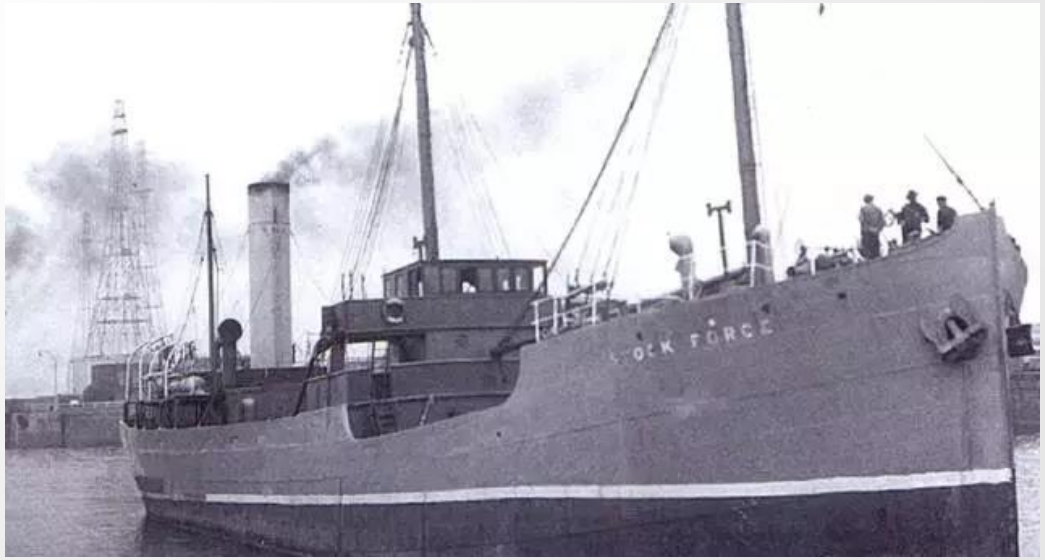
2. “隐形监管”-基于旁路的入侵检测

- **基于旁路的入侵检测**
  - 准确判断入侵检测困难，工控是高可用实时系统
  - 流量的深度解析，无线通信的深度检测
- **关键技术**
  - 工控协议深度解析
  - 流量特征的分析与进度获取
  - 业务操作流程与重要操作的关联关系
  - 攻击行为与特征击分析，检测规则库构建
  - 面向白名单的检测策略自学习机制
    - 程序自学习
    - 现场自学习

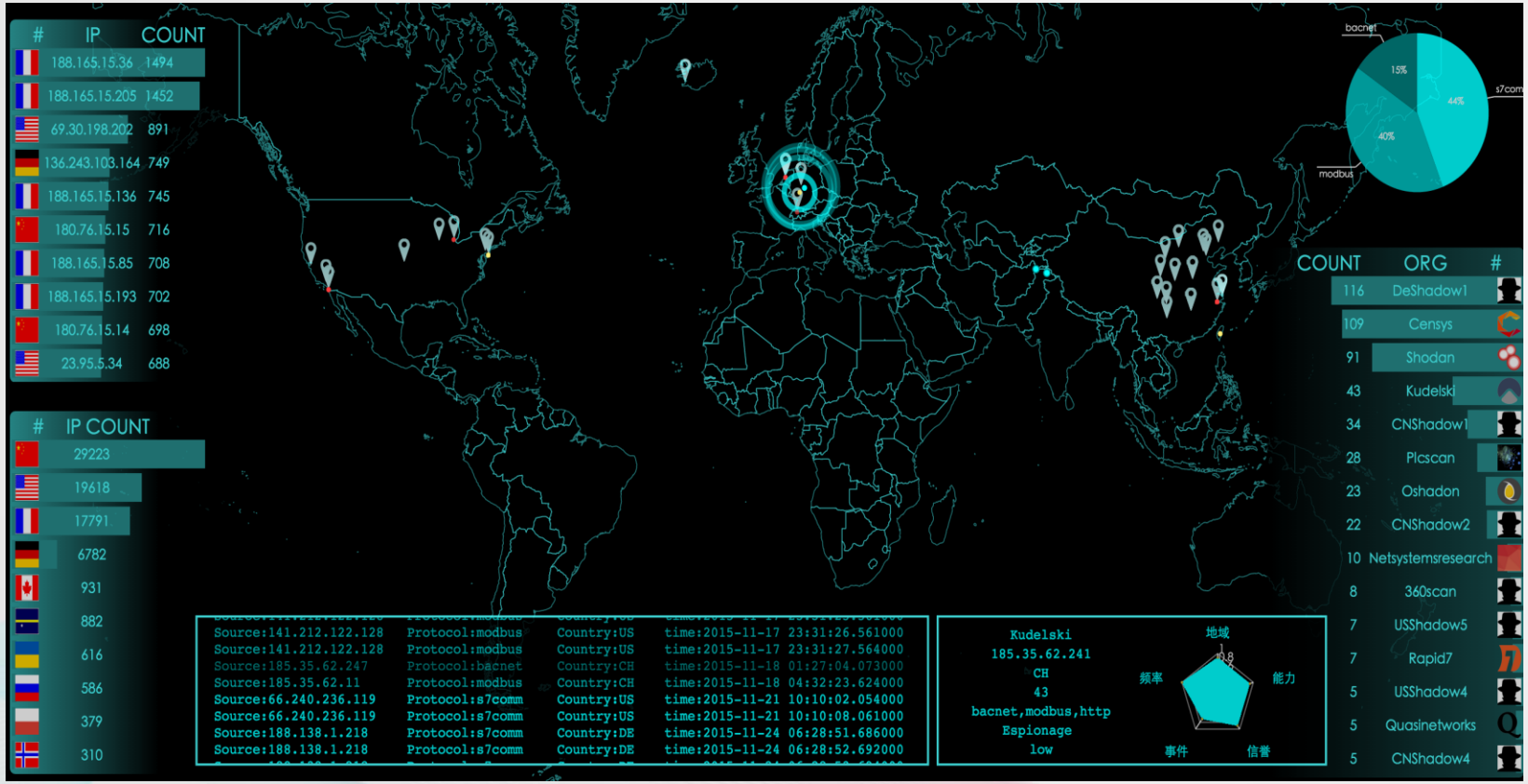


3. “神秘之船“-工控系统安全防护的基础-攻击发现

- **“神秘之船”**
  - 一战：德军利用潜艇大肆攻击协约国船只，英国海军发现不了水下活动的潜艇，于是提出了“神秘之船”方案，即建造外型酷似商船的猎潜艇，诱使德军潜艇攻击...
- **入侵诱捕-诱捕入侵**
  - 了解谁- 在入侵？
  - 入侵者- 做什么？ - **及时掌握入侵态势**
  - **获取** **- 攻击样本**
- **核心关键技术**
  - “诱惑” - 仿真真实环境
  - “捕获” - 捕获威胁数据
  - **分析** **- 攻击行为。**



3. “神秘之船“-神秘战队



- 统计分析
- 探测模式分析
- 利用能力分析
- 入侵能力分析

结束语

- **统筹考虑，渐进式、正对性的安全防护策略**
  - 统一规划，整体安全策略
  - 遗留系统、在建系统、设计系统
- **建立生态：多方协同，集智攻关，共建工控安全生态圈**
  - 自动化厂商：内嵌安全机制
  - 信息安全厂商：安全防护技术
  - 系统集成厂商：系统安全建设
  - 行业用户：安全运行管理

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You