打破工控系统“潜规则”，赢得安全新动力

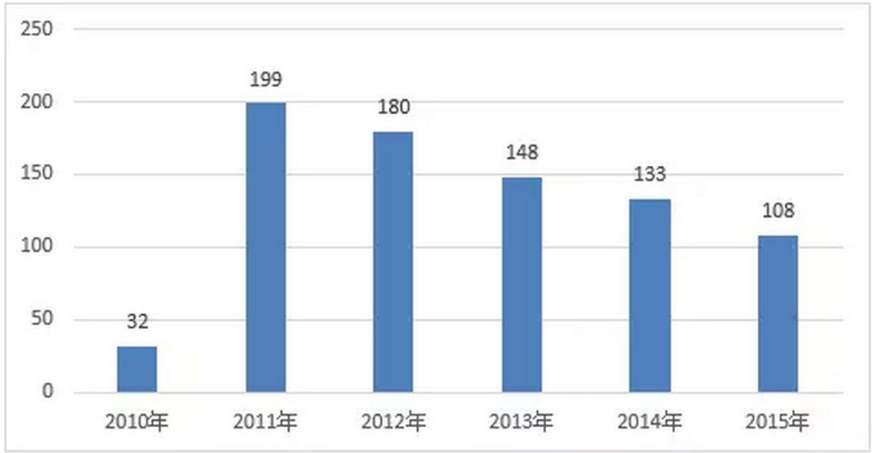
孟雅辉
启明星辰集团公司
2016年5月21日

工控安全“外热内温（冷）”

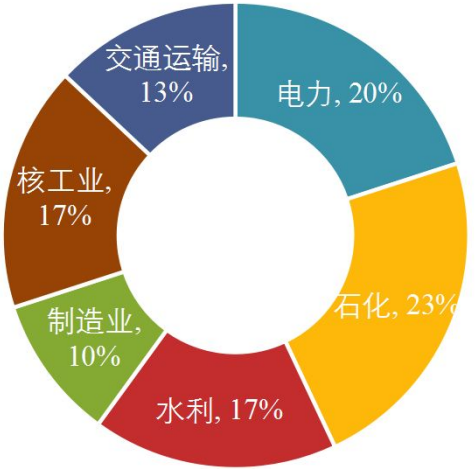
工控系统信息安全背景

数　据

- 公开的ICS漏洞数的年度变化趋势
- 据权威工业安全事件信息库RISI统计，截止到2016年初，全球已发生300余起针对工业控制系统的攻击事件。



各行业发生的工控信息安全事件占比

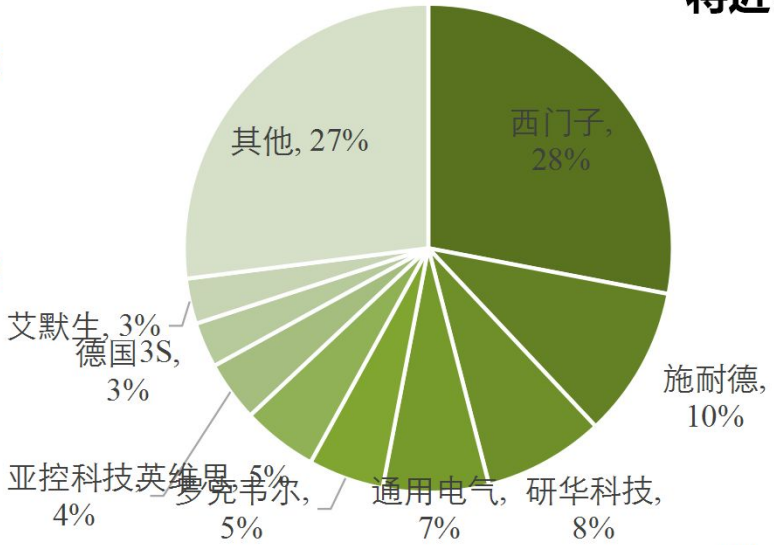


数据来源工控网

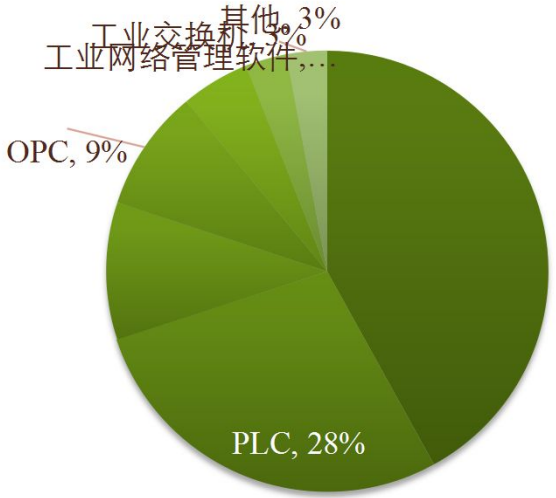
工业控制系统信息安全形势

数　据

- 公开漏洞涉及的主要工业控制系统厂商



- SCADA/HMI系统漏洞占比超过40%，PLC漏洞接近30%，DCS及OPC漏洞占到将近10%。



数据来源工控网

国内外工业控制系统信息安全现状

事件

- 2015年底，BlackEnergy攻击致乌克兰停电事件。
- 2014年12月22日，韩国负责运营23个核反应堆的水力原子力学公司透露，其电脑系统遭到黑客入侵，韩总统关注，并邀请美国协助调查此次核电系统黑客入侵事件。
- 2015年，发现国内著名网络摄像头生产制造企业海康威视的监控设备存在严重安全隐患，部分设备已被境外IP地址控制。

国内外工业控制系统信息安全现状

事件

- 2015年，某集团“内鬼”事件，产品提供商的员工为中石化华东公司的SCADA系统（油管监控系统），“私人订制”了一套病毒程序，病毒爆发导致系统无法运行。
- 2014年12月，德国联邦信息安全办公室公布了德国一家钢铁厂因网络攻击造成停产的事件。
  - 攻击者使用鱼叉式钓鱼邮件和社会工程学手段，获得钢铁厂办公网络的访问权，然后利用网络进入生产网络。攻击行为导致工控系统的控制组件和整个生产线被迫停止运转，由于是不正常的关闭炼钢炉，给钢铁厂带来了重大的破坏。

国外工控信息安全政策和标准

国外政策

- 2014年12月，欧洲网络与信息安全局(ENISA)针对工业控制系统发布了《Certification of Cyber Security skills of ICS/SCADA professionals》。 该报告探讨了现有信息安全技术及举措如何引申应用到工业控制系统，明确了工业控制系统信息安全面临的挑战并提出了一系列发展建议。
- 2015年1月，美国总统奥巴马拜访了美国国土安全部国家网络安全与通信集成中心(NCCIC)，提出了一项针对网络安全信息共享的立法提案以加强网络安全的信息共享，对抗网络犯罪。
- 2015年4月，美国国防部发布第二版网络战略报告(第一版于2011年发布)，指导美国网络力量的发展，加强网络防御建设与网络威慑力量。
- 2015年5月，日本在首相官邸举行网络安全战略本部会议，制定了新的《网络安全战略》，提出了“信息自由流通”、“对使用者的开放性”等五项原则。

国外工控信息安全政策和标准

国际标准
NIST
SP800-82

- **目的**：为保障ICS系统安全，美国国家标准与技术研究院（NIST）制定的关于工业控制网络安全的工作指南。
- **对象**：ICS定义主要包括SCADA、DCS、PLC三个控制系统，为其提供系统安全实施指南。
- **网络架构**：概括ICS典型系统拓扑结构，指出工控系统面临的典型威网络架构胁和可能的脆弱点，为降低相关风险提供相关对策。
- **漏洞威胁**：分析ICS发展现状，提出ICS面临的安全威胁和主要漏洞，并对这些威胁和漏洞，提出缓解威胁、弥补漏洞的建议和方法。

国外工控信息安全政策和标准

国际标准
IEC 62443

目的

为了应对工业自动化和控制系统通信网络中的信息安全挑战，IEC/TC65/ WG 10（工业过程测量、控制与自动化/网络与系统信息安全工作组）与国际自动化协会ISA99成立联合工作组，共同制定IEC62443《工业过程测量、控制和自动化网络与系统信息安全》系列标准。

内容

IEC 62443 系列标准目前分为通用、信息安全程序、系统技术和部件技术4 个部分，共包含12 个文档，每个文档描述了工业控制系统信息安全的不同方面。

影响

IEC 62443 系列标准通过四个部分，涵盖了所有的利益相关方，即资产所有者、系统集成商、组件供应商，以尽可能地影响 实现全方位的安全防护。

国内工控信息安全政策和标准

国内政策

- 习总书记任中央网络安全和信息化领导小组组长
  - 网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题
  - 没有网络安全就没有国家安全，没有信息化就没有现代化
- 2016年4月19日，习主席在网络安全和信息化工作座谈会上再强调加快信息基础设施安全保障体系。
- 2015年4月，中央机构编制委员会办公室颁布《中央编办关于工业和信息化部有关职责和机构调整的通知》，明确工业和信息化部负责网络强国建设相关工作。

国内工控信息安全政策和标准

国内政策

- 2015年5月，国务院印发《中国制造2025》的通知，专门提到“加强智能制造工业控制系统网络安全保障能力建设，健全综合保障体系”。
- 从2011年开始，国家发改委开展工业控制系统信息安全专项，涉及面向现场设备环境的边界安全专用网关产品、面向集散控制系统（DCS）的异常监测产品、安全采集远程终端单元（RTU）产品、工业应用软件漏洞扫描产品等工控安全产业化项目。以及覆盖石油化工、电网、电厂、先进制造等在内的工控安全试点。

国内工控信息安全政策和标准

GB30976.1-2014

工业控制系统信息安全第1部分：评估规范

国内工控信息安全政策和标准

GB/T 30976.2-2014

工业控制系统信息安全 第2部分：验收规范；

国内工控信息安全政策和标准

国内其他标准

- 《工业控制系统信息安全等级保护设计技术指南(草稿)》、《工业控制系统信息安全等级保护基本要求(草稿）》正在编写过程中。
- TC260在研标准：工业控制系统安全管理基本要求、安全检查指南、应用指南等系列标准。
- 集散控制系统（DCS）信息安全系列标准、可编程逻辑控制器（PLC）系统信息安全要求等标准正在征求意见中。
- 在工控安全建设方面走在前列的电力行业早些年已经在生产系统中建立了相关规范，如《电力二次系统安防护规定》（电监会5号令）、《电力二次系统安全防护总体方案》（电监会全34号文）等，发改委14号令 《电力监控系统安全防护规定》。

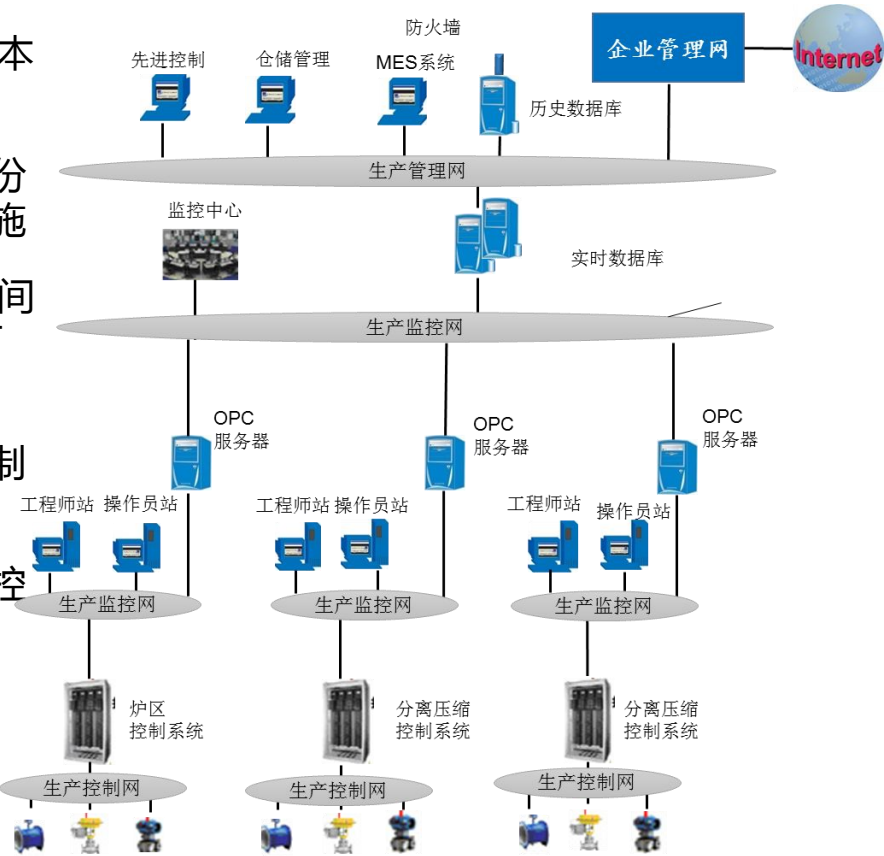
各行业工控信息安全动态

工控相关行业动态

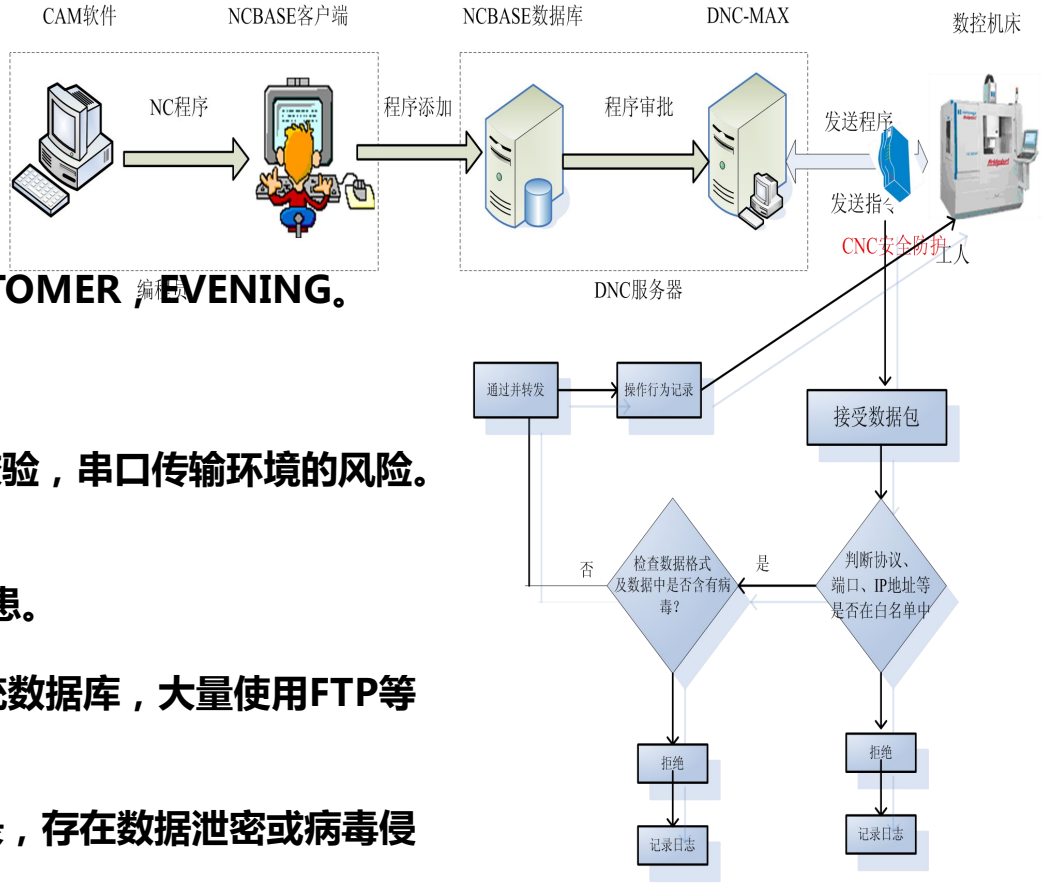
- 能源局多次强调工控系统信息安全的重要性，要求电力行业贯彻14号令和36号文，并进行检查。
- 电力、石化、煤炭、冶金、烟草、轨道交通、市政、军工等行业在尝试做工控信息安全试点，有的在编写行业工控安全标准。

工控系统面临的信息安全问题-石化行业

- 操作站、工程师站、服务器采用通用windows系统，基本不更新补丁；
- DCS控制器与操作站、工程师站系统通信基本不使用身份认证、规则检查、加密传输、完整性检查等信息安全措施
- 生产执行层的MES服务器和监督控制层的OPC服务器之间缺少对OPC端口的动态识别，OPC服务器可以允许任何OPC客户端连接获取任何数据；
- 工程师站权限非常大，只要接入生产网络，就可以对控制系统进行运维。
- 多余的网络端口未封闭，工控网络互连时缺乏安全边界控制；
- 外部运维操作无审计监管措施。



工控系统面临的信息安全风险-先进制造

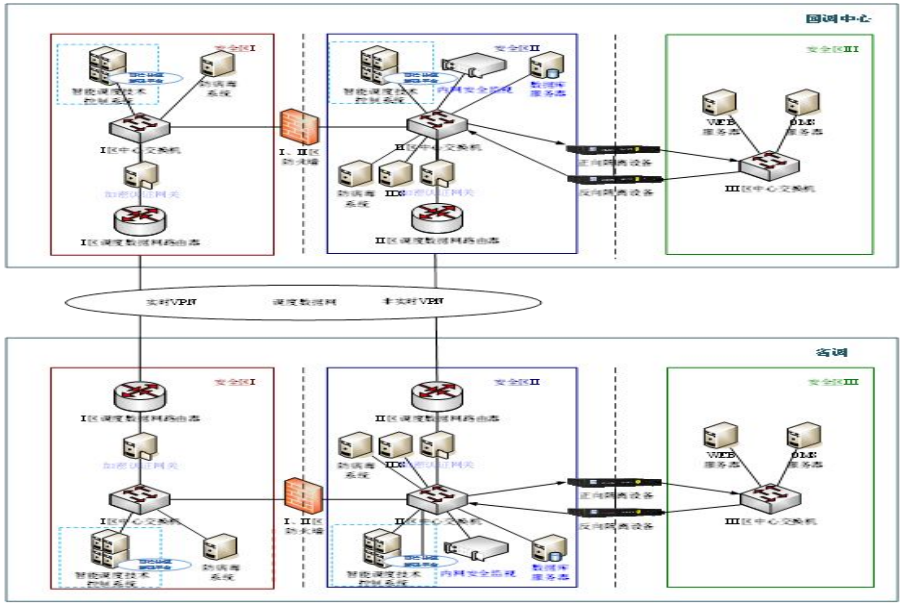


- 工控系统默认口令问题，SUNRISE。CUSTOMER，EVENING。
- 通过操作站感染病毒。
- 串口网口转换，定制协议过于简单，缺乏校验，串口传输环境的风险。业务指令异常无法发现。
- 数据传输，NC代码等文件传输存在安全隐患。
- DNC服务器等都是Windows系统安装传统数据库，大量使用FTP等传统，操作有被渗透的可能。
- 第三方运维人员在运维设备时缺乏审计记录，存在数据泄密或病毒侵入的威胁。

工控系统面临的信息安全风险-电网和发电

安全建设现状

1. 探索智能变电站的信息安全防护
2. 建立可信计算密码平台，更新调度数字证书、纵向加密认证、横向隔离装置、防火墙、入侵检测系统，搭建安全仿真平台。
3. 智能变电站技术、分布式能源智能大电网，不仅有监视，还有控制。用电信息在互联网上传输，需要加密；用户的智能电器暴露在电力系统中，可能受到攻击。
4. 安全区II的电厂和省调之间采用IEC104规约，框架确定，但是格式混乱



发电（水火）面临的风险：

1、所有发电控制系统连接在一区，无任何安全防护措施。

2、随着发电全厂一体化建设的推进，因联通导致的风险越来越大。

3、操作站采用通用操作系统，未安装补丁，感染病毒。

4、OPC问题一样突出。

5、远程运维依然存在，安全运维审计装置缺失。

工控安全产品市场

工控安全产品各行业分布情况（2014年）

行业	市场规模，百万元	市场份额
电力	118.8	53.8%
石化（油气）&化工	43.7	19.8%
冶金	20.5	9.3%
烟草	11.0	5.0%
煤矿	5.0	2.3%
其它	22.0	9.9%
合计	220.8	100%

注：其它主要包括市政、交通、军工等行业。

数据来源：gongkong

仅为IT安全市场份额的1%左右，存在巨大的差距

是什么拖住了工控安全前进的步伐？

何为“潜规则”？

它是指看不见的、明文没有规定的，约定俗成的，无局限性，却又是广泛认同、实际起作用的，人们都“遵循”的一种规则。

工控系统的“潜规则”在哪？

“潜规则”

- 生产系统关系重大，我不能进行信息安全检查。
- 虽然目前也有设备响应速度慢，甚至网络偶尔中断的情况，基本也没造成大的影响，生产为重，我们不要做改动了。
- 运维服务有厂商或集成商支持，有问题直接找他们，不需要对我们的系统太了解。
- 我们都清楚子系统之间应该做访问控制，我担心串接设备影响控制系统，从而影响生产，还是不做了吧。

“潜规则”怎么破？

OR

打破“潜规则”

- 生产系统关系重大，我可以进行信息安全检查。

  a.设备检修时
  b.生产系统仿真环境
  c.采用不影响生产的被动检查工具，手工检查

- 虽然目前也有设备响应速度慢，甚至网络偶尔中断的情况，基本也没造成大的影响，生产为重，我们还是可以做改动

  a.设备检修时
  b.生产系统仿真环境
  c.采用不影响生产的旁路检测设备

打破“潜规则”

- 运维服务有厂商或集成商支持，有问题直接找他们，不需要对我们的系统太了解。
- 我们都清楚子系统之间应该做访问控制，我担心串接设备影响控制系统，从而影响生产，还是不做了吧。

给自己三种选择，如何破？

他山之石，可以攻玉

从2016年RSA大会看工控安全

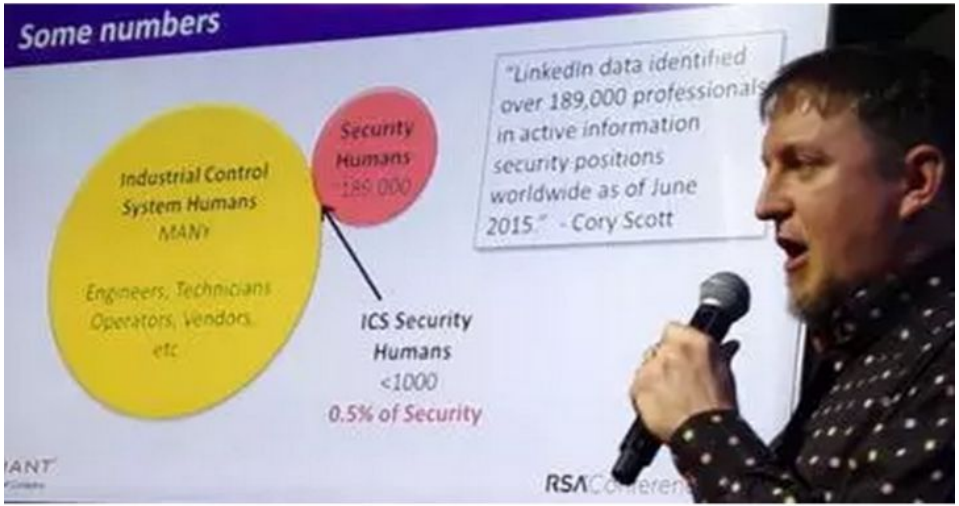
1、国外工控安全虽受重视去却是稳中求静

- 很多大牌厂商如Checkpoint、Palo Alto、Fortinet均有工业防火墙以及实际应用，但在展会上都非常低调，没有单独陈设
- 厂商分类中没有工控安全（ICS），大会却安排了两整天的ICS专题SANDBOX。诸多信息安全专家讲解了包括工控安全IOT与ICS(When World collide : IoT Meets ICS)、如何进入工控安全领域(How to Get into ICS Security)、ICS/SCADA网络态势感知(Cyber-Situational Awareness in ICS/SCADA)等多个主题。

从2016年RSA大会看工控安全

2、在IT与OT融合过程中，目前ICS专家人才异常缺乏

目前全球的工业控制系统人才很多，信息安全人才大约有18万9千人，但其中只有5%是工控信息安全人才，这些人才要保障全球那么多的关键基础设施是远远不够的。



从2016年RSA大会看工控安全

- 3、国外的工业用户仍然有诸多管理不规范、技术措施不完善导致的ICS安全问题。
  - 我们在现场通过与专家沟通，类似通过U盘导致的震网病毒时间、通过Email导致的乌克兰电网事件等在美国诸多工业用户中也常有出现，但因多数未直接导致诸如震网病毒事件的严重后果，部分客户也会在考虑功能时放弃安全考量，导致工业控制网络仍处在一个不可控的状态中。

从2016年RSA大会看工控安全

- 4、工控安全防护监测并重，安全培训仍是重中之重。
  - 国外工控安全建设参考的是著名的NIST SP800-82 REVISION 2、IEC62443、NERC/CIP、CFATS等标准
  - 技术措施上，展会和沙箱演示里不仅有工业防火墙，同时也有支持工业环境的监测系统，如卡巴斯基实验室的工控网络监测系统等。
  - 仍然强调客户对安全的认知，安全措施取代不了安全认知，所以培训教育仍是老生常谈，但又不得不谈的重要项。

从2016年RSA大会看工控安全

- 5、首次在ICS/SCADA里提出了网络空间的态势感知，并且落地务实
  - 专家表示，ICS中的态势感知能够对网络中的每个元素和资产状况及相互关联关系做到心中有数并直观呈现，这样就能够及时发现和解决问题，从被动安全到主动安全。

启明星辰工控安全在路上

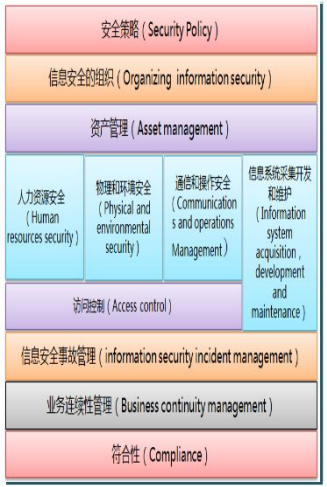
工控系统信息安全防护建设参考标准

工控安全防护建设参考标准

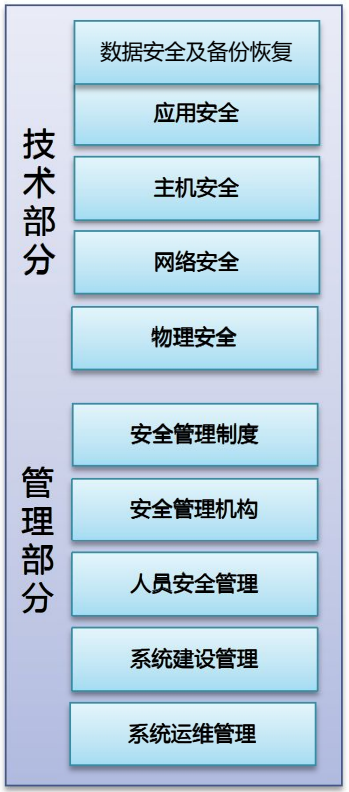
- 以451号文为基准
- 参考国际国内标准
- 结合行业生产特点

IEC62443

《工业控制系统安全指南》
NIST SP800-82



ISO27001

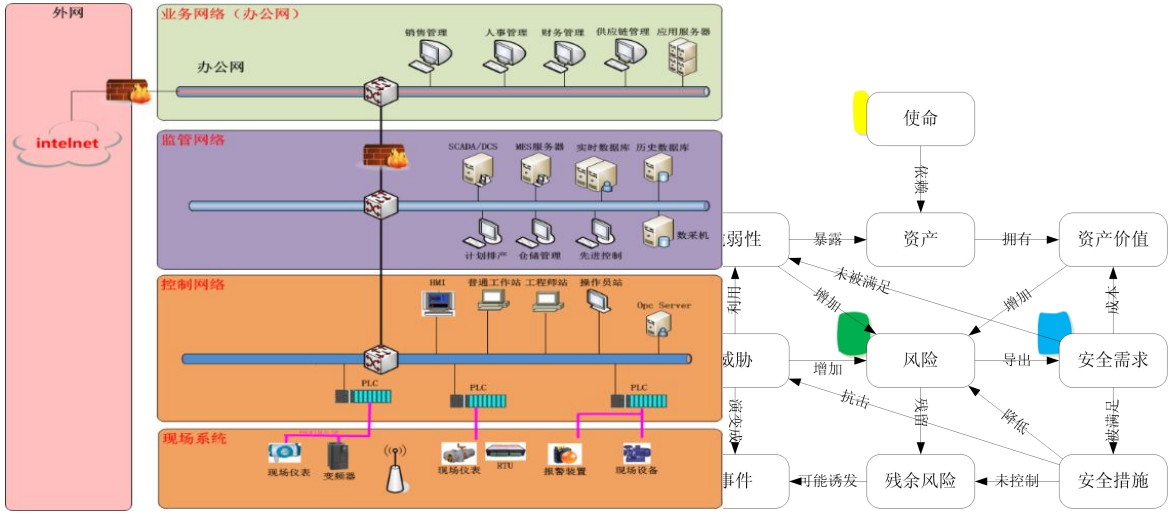


等级保护

防护体系建设思路

工控安全建设思路

依据 “垂直分层、横向分区、边界防护 、内部监测 ” 总体策略



融合秩序的工控系统信息安全产品体系

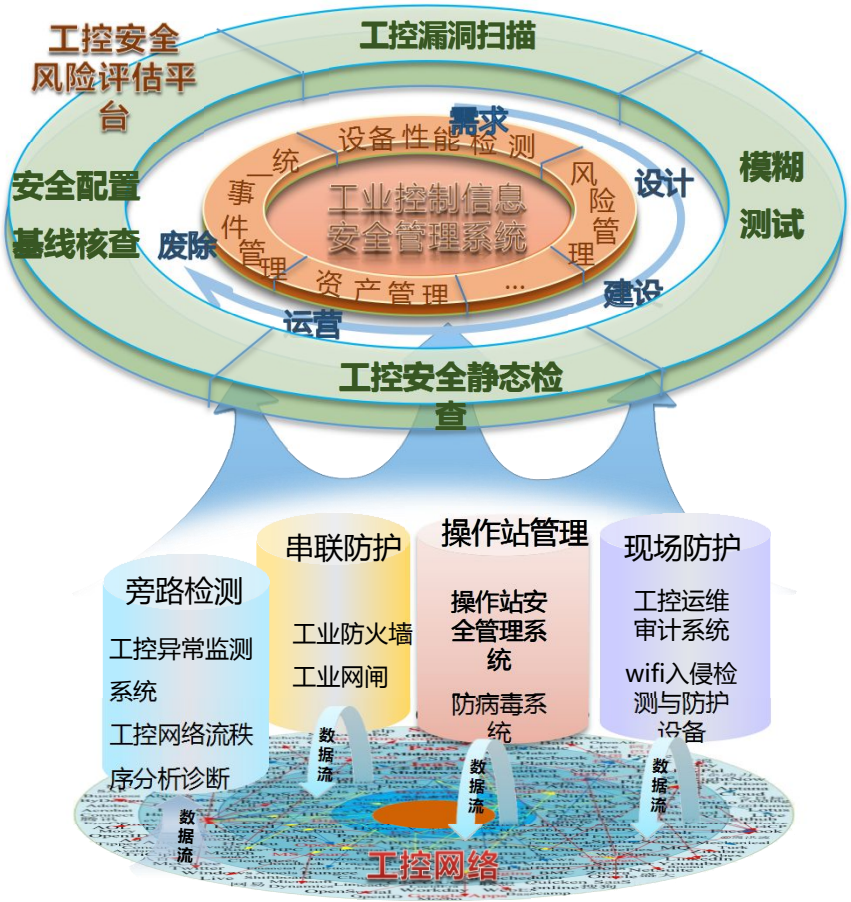
- 基于全生命周期（事前、事中、事后）
- 覆盖三层（过程控制、生产控制、现场控制）
- 集防护监测的统一体系

通过操作站带来的风险

“两网连接“带来的风险

现场与远程运维带来的风险

工业无线带来的风险



工业控制系统防护体系

- 边界隔离防护
- 网内异常监测
- 现场审计与防护
- 统一安全管理

安全贵在未雨绸缪，信赖源自风雨同舟

工控安全风险评估平台


工控安全风险评估平台
漏洞扫描
发现已知漏洞
模糊测试
挖掘未知漏洞
静态检查
挖掘未知漏洞
基线核查
挖掘未知漏洞
可知
可防
可预测
我的任务
待办任务
创建任务
录入
操作
删除
删除
完成
安全贵在未雨绸缪

携手共赴工控安全之路

从争论中找机遇找核心

互联网+工业

工业+互联网

TESLA MOTORS

互联网基础设施

互联网思维

机遇

安全贵在未雨绸缪，信赖源自风雨同舟

共建威胁情报监测平台

监管机构

自动化集成厂商

信息安全厂商

用户

高校大学

威胁情报监测平台

舆情监测

沙箱技术

虚拟执行

漏洞扫描

配置核查

网络安全威胁情报交换服务

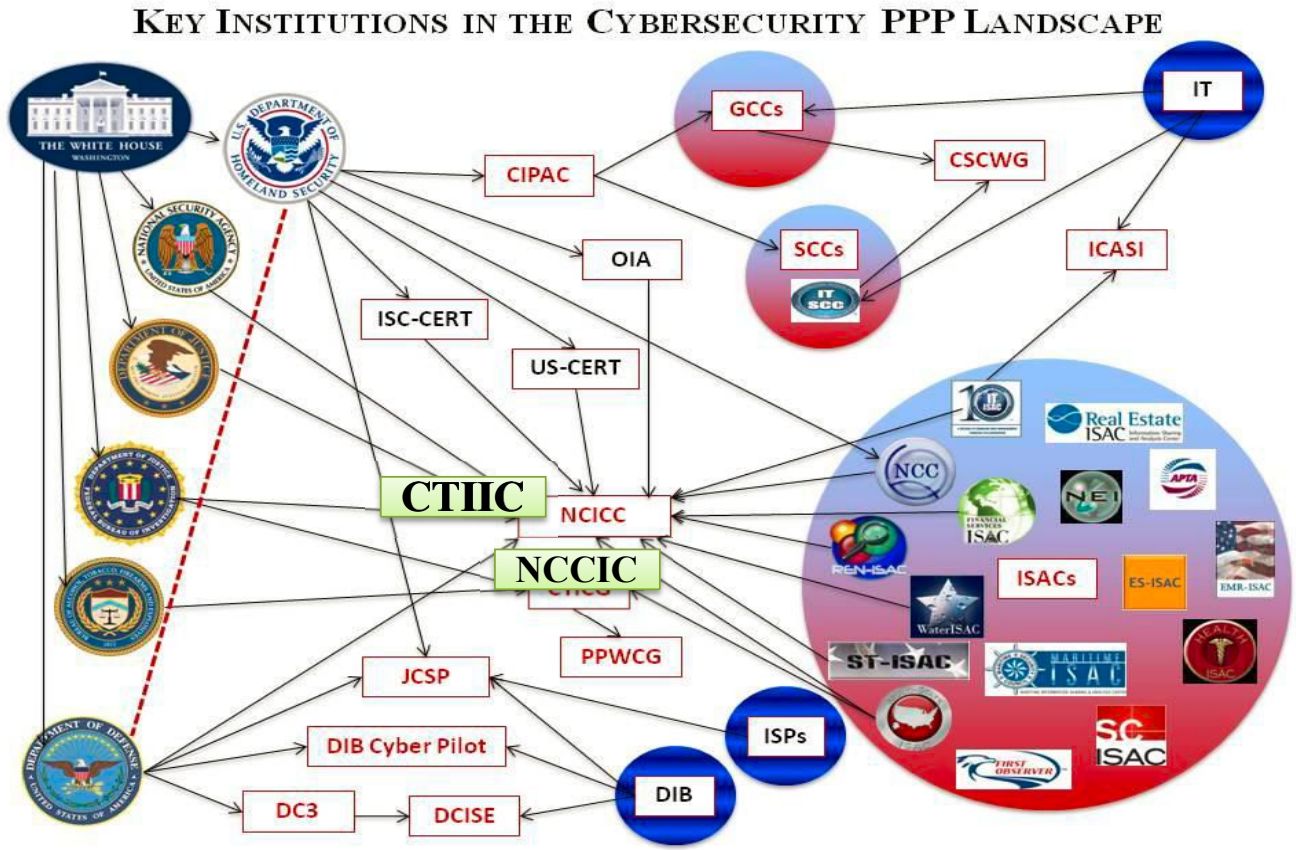
- **Consortiums-情报组合形式，类似市场，提供多种源可选**
  - OSINT 中情局 公开资源情报计划 Open source intelligence
  - Check Point Software Technologies' ThreatCloud IntelliStore integrating feeds from CrowdStrike, IID, iSIGHT Partners, NetClean, PhishLabs, SenseCy, ThreatGRID
  - Cyveillance
- **Threat Intelligence Alliances-（厂家间的）威胁情报联盟形式**
  - Cyber Threat Alliance: Fortinet, Palo Alto, McAfee and Symantec
  - Microsoft Interflow: Members of the Microsoft Active Protections Program (MAPP)
  - CSIS Security Group, Fox-IT and Group-IB
  - Norse and HP
- **Circle of Trust Exchange Platforms-（组织间）互信交换平台形式**
  - ActiveTrust Platform: IID
  - Threat Central: HP
- **Intelligence Exchange Services Platforms- 威胁交换服务平台形式(多源汇聚)**
  - AlienVault, ThreatConnect, ThreatStream and Vorstack

企业外部的安全威胁情报源（含开源及商业）

- OSINT
- ISACs / US-CERT
- SANS
- CVEs, CWEs, OSVDB (Vulns)
- Dell SecureWorks
- iSight Partners
- Norse IPViking/Darklist
- Cyveillance
- Fox-IT/Group-IB/IID
- OpenDNS
- MAPP

- IBM QRadar
- Palo Alto Wildfire
- FireEye/Mandiant
- RSA NetWitness Live/Verisign iDefense
- Symantec Deepsight
- McAfee Threat Intelligence
- AlienVault OTX

美国的信息安全及信息共享组织结构



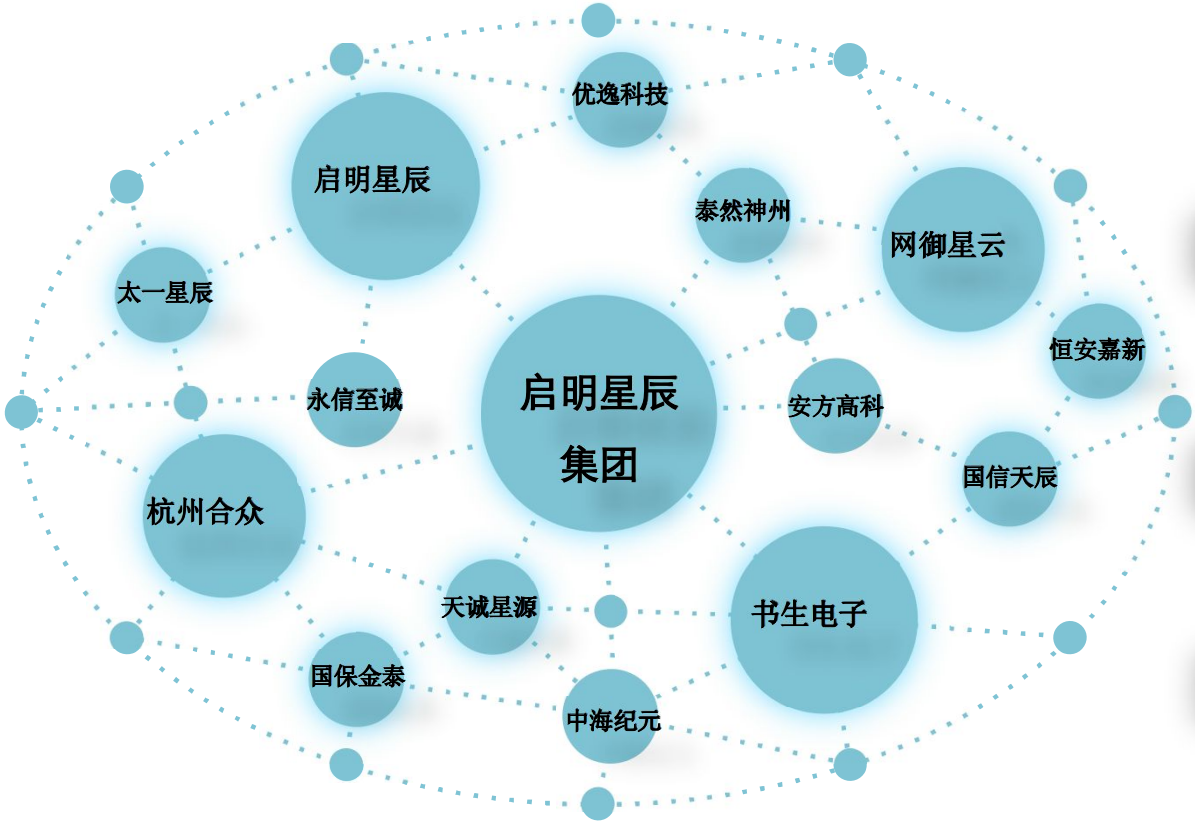
NCCIC 网络安全和通信整合中心，是国土安全部下属，是负责推动政府与企业共享网络威胁信息的主要机构。

新成立的CTIIC 网络威胁与情报整合中心，直接归国家情报总监办公室管辖，负责分析和整合国土安全部、联邦调查局、中央情报局、国家安全局等部门收集到的网络威胁信息。该机构将拥有**50**名左右员工，划拨的预算约为每年**3500**万美元，但并不会展开任何监督工作。

启明星辰
领航信息安全

启明星辰集团历程

启明星辰集团战略布局



安全贵在未雨绸缪，信赖源自风雨同舟