ISC 2017

2017 中国互联网安全大会 China Internet Security Conference

工控安全应急工作的探索与实践

张洪

国家工业信息安全发展研究中心
高级工程师

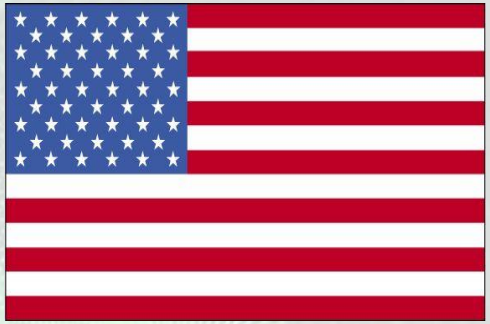
目录

- 工控安全应急的挑战
- 国家工控应急管理工作
- 我们的工作

工控发展

工业4.0

中国制造2025



工业互联网

云计算

大数据

人工智能

工控安全事件层出不穷

重大工控安全事件（2010-2017）

2010

2011

美国伊利诺伊州城市供水SCADA系统遭黑客入侵，毁掉了一个向数千户家庭供水的水泵

“震网”病毒攻击伊朗布什尔核电站

2012

“Flame”病毒感染中东能源行业。被认为是迄今为止发现的最大规模的和最为复杂的网络攻击病毒

“Duqu”病毒袭击中东和欧洲能源行业

2013

以色列交通控制系统被黑客攻击

黑客大会上，研究人员展示了对民航客机、智能汽车、医疗设备的入侵

2014

黑客组织“Dragonfly”利用Havex恶意软件入侵欧美能源控制系统

OpenSSL“心脏出血”漏洞影响西门子、ABB等公司工业产品

2015

俄罗斯黑客利用“Black Energy”攻击乌克兰电网系统

俄罗斯某工控安全研究团队公布了名为“SCADAPass”的工业控制设备默认密码清单

2016

美国网络服务商Dynamic Network Service公司遭受大规模物联网DDoS攻击，导致大规模网络服务中断

首例可在PLC之间传播的蠕虫病毒被测试证实

美国旧金山地铁系统感染勒索事件，被索要七万余美金赎金

工控安全应急的挑战

攻防
不对称

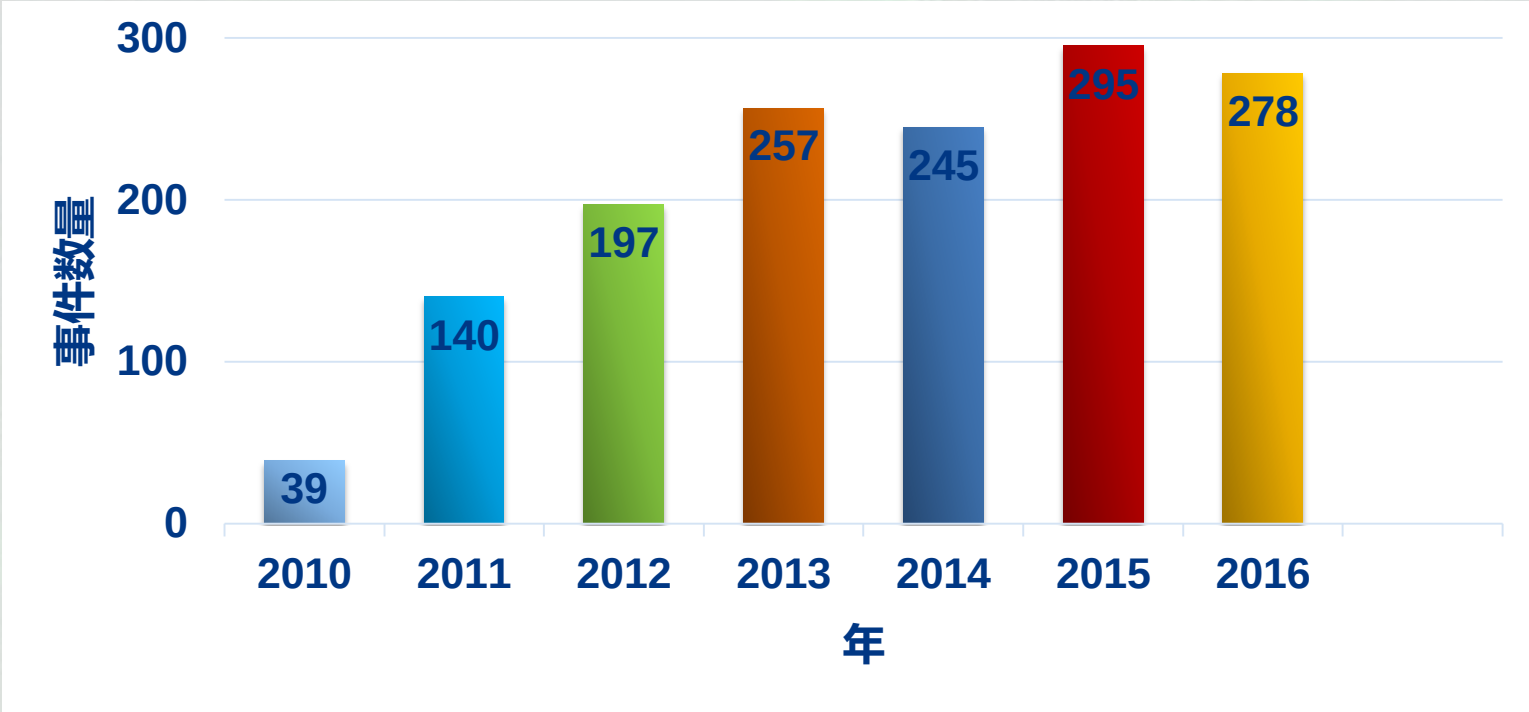
技术
不对称

人员
不对称

投入
不对称

工控安全应急的挑战

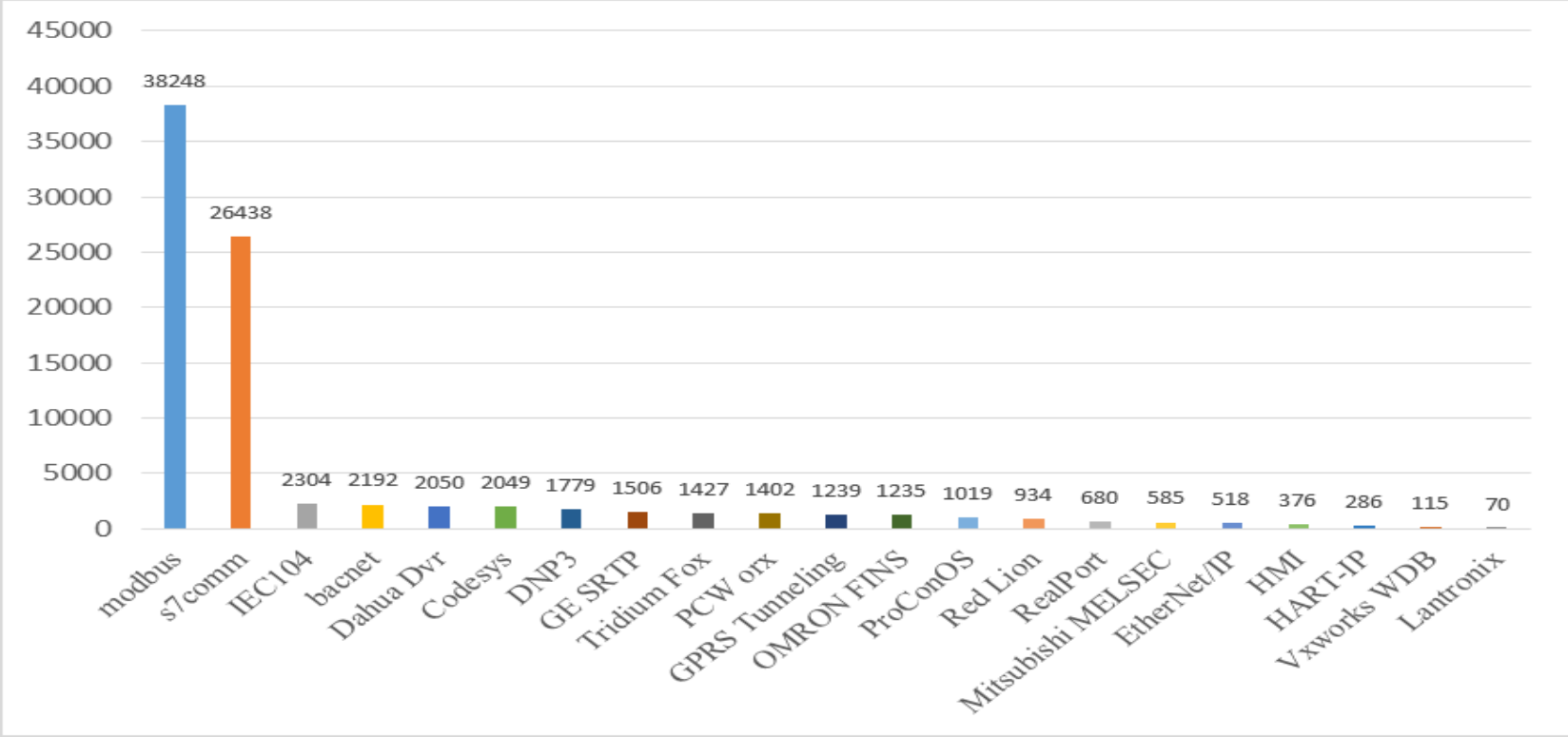
一、形势不对称—攻



工控安全事件数量（ ICS-CERT ）

工控安全应急的挑战

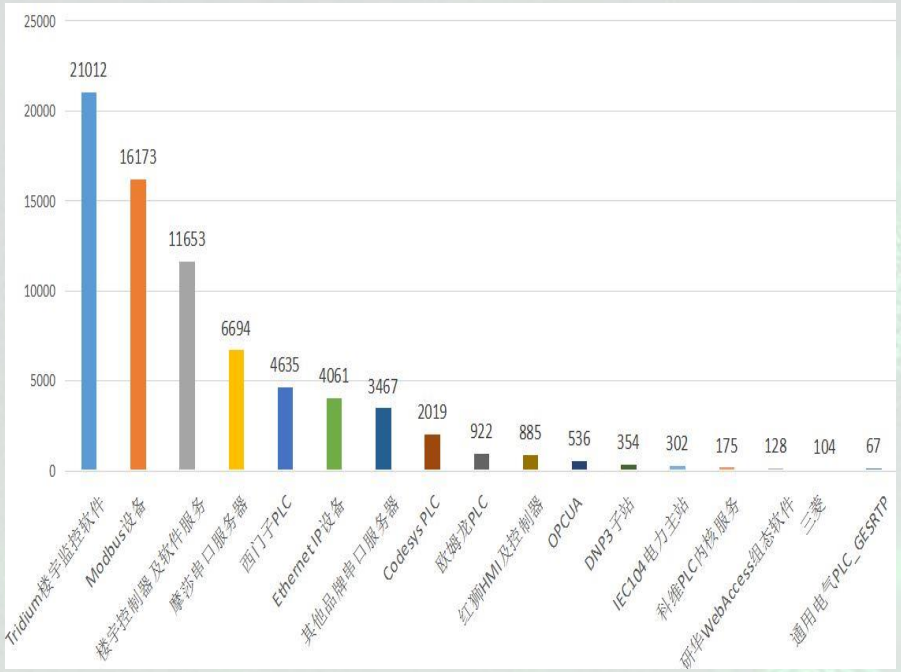
一、形势不对称—攻

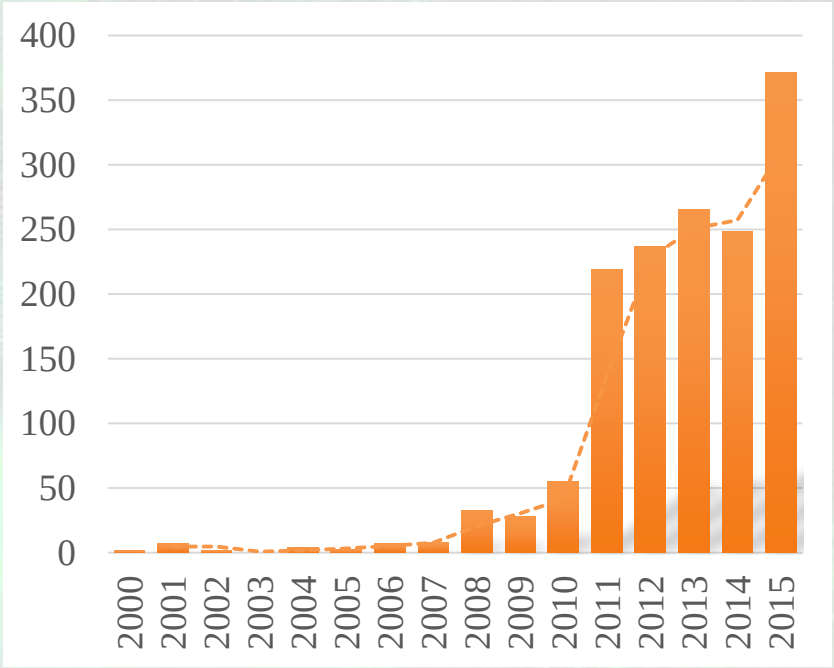


2015年11月至今，针对工控系统的网络攻击高达17万+次。

工控安全应急的挑战

一、形势不对称—防





据中心监测发现，暴露在互联网上的主流工控系统数量高达72,000+个，系统类型有近20种。

FireEye统计2000-2015年全球共发现1490个工业控制系统漏洞

工控安全应急的挑战

二、技术不对称—攻

政治化

网络空间安全

军事化

网络部队

黑客组织

工业控制系统

极端势力

工业控制系统作为国家关键基础设施的重要组成部分，成为国家之间网络对抗和有组织黑客的攻击目标。

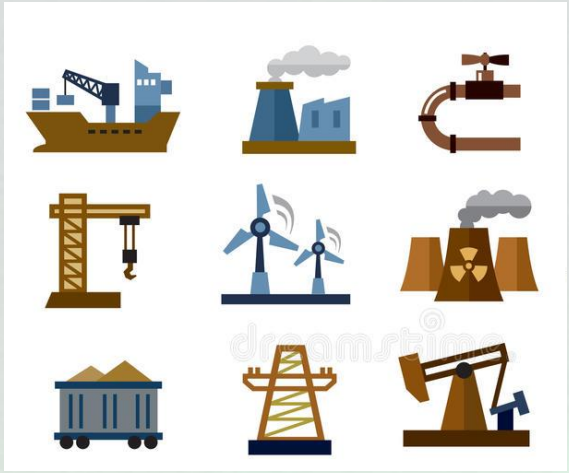
工控安全应急的挑战

二、技术不对称—攻

- 2017年3月7日，维基解密以“穹顶7”（Vault7）为代号，公开了美国大量网络攻击工具。
- 攻击对象包括Windows，OS X，Linux等操作系统，以及网络平台、智能手机、车载系统、智能设备等。
- 工业控制系统的攻击工具“武器化”，成为国家安全新“威慑”。

工控安全应急的挑战

二、技术不对称—防



- 种类众多
- 数量巨大
- 行业分布广
- 专业性强

7x24
hours

- 7 * 24 小 时
  不间断运行

- 通用协议、组件
- IT+OT

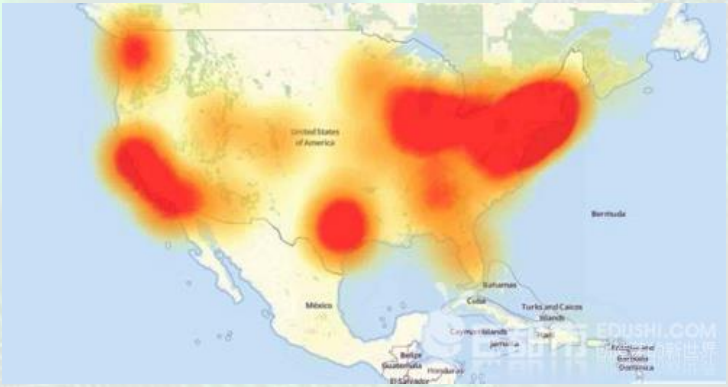
工控安全应急的挑战

二、技术不对称—防

工业辅助系统安全隐患日益突出，严重威胁工业信息安全

2015年2月，国内在互联网上的视频设备因弱口令问题被黑客攻击。

2016年10月，攻击者利用网络摄像机等大量视频设备发起DDoS攻击，使得半个美国网络瘫痪。

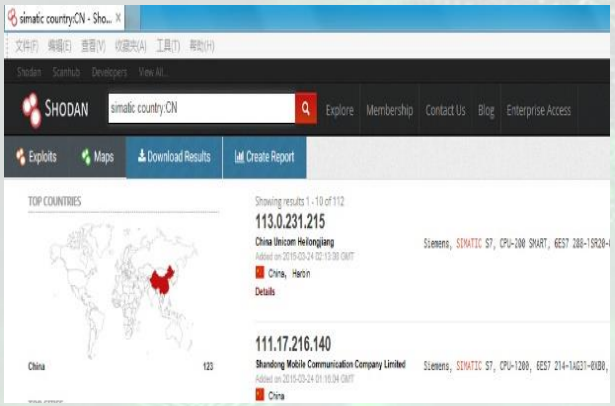


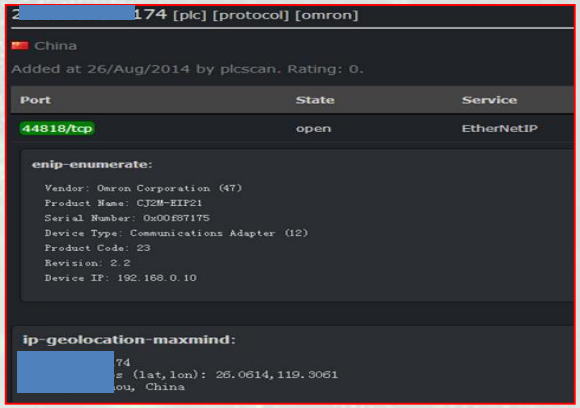
三、人员不对称—攻

- 大量工控系统软硬件设备的安全漏洞及利用方式可通过公开或半公开的渠道获得。
- 在国内外很多白帽社区中，大量SCADA系统的漏洞细节和利用方式被公布。
- 在github等开源社区中，可以获得很多关于工控设备的弱口令信息以及工控系统的扫描、探测、渗透工具。

工控安全应急的挑战

三、人员不对称—攻





1.通过google等网页搜索引擎检索

2. 通过Shodan等主机搜索引擎检索

3. 通过在线监测平台匹配工控通信协议指纹特征

工控安全应急的挑战

三、人员不对称—防

工控安全应急的挑战

四、投入不对称

四两拨千斤 Vs 小马拉大车

工控安全应急挑战的解决思路

形势不对称	• 梳理全国工控系统清单 • 按重要性、影响范围确定防护对象
技术不对称	• 加强工控应急技术手段研发 • 研究工控系统应急整体解决方案
人员不对称	• 开展跨领域合作，培养复合型工控安全人才。 • 加强人员安全培训，开展攻防实战对抗。
投入不对称	• 明确政府、企业的主体责任和边界，确保资源投入。 • 开展工控安全应急专业服务

目录

国家工控安全管理工作

《关于加强工业控制系统信息安全管理的通知》（工信部[2011]451号）

中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China

关于加强工业控制系统信息安全管理的通知

发布日期：2011-10-27　　来源：信息安全协调司

工信部协[2011]451号

- 制定工控系统信息安全应急预案，明确应急处置流程和临机处置权限，建立应急技术支撑队伍。

国家工控安全管理工作

《中华人民共和国网络安全法》

- 2017年6月1日起施行
- 建立健全网络安全风险评估和应急工作机制
- 制定网络安全事件应急预案
- 组织应急演练

国家工控安全管理工作

《国家网络安全事件应急预案》（中网办发文[2017]4号）

中共中央网络安全和信息化领导小组办公室

Office of the Central Leading Group for Cyberspace Affairs

中央网信办关于印发《国家网络安全事件应急预案》的通知

2017年06月27日 16:20:53　来源：中国网信网　【打印】【纠错】

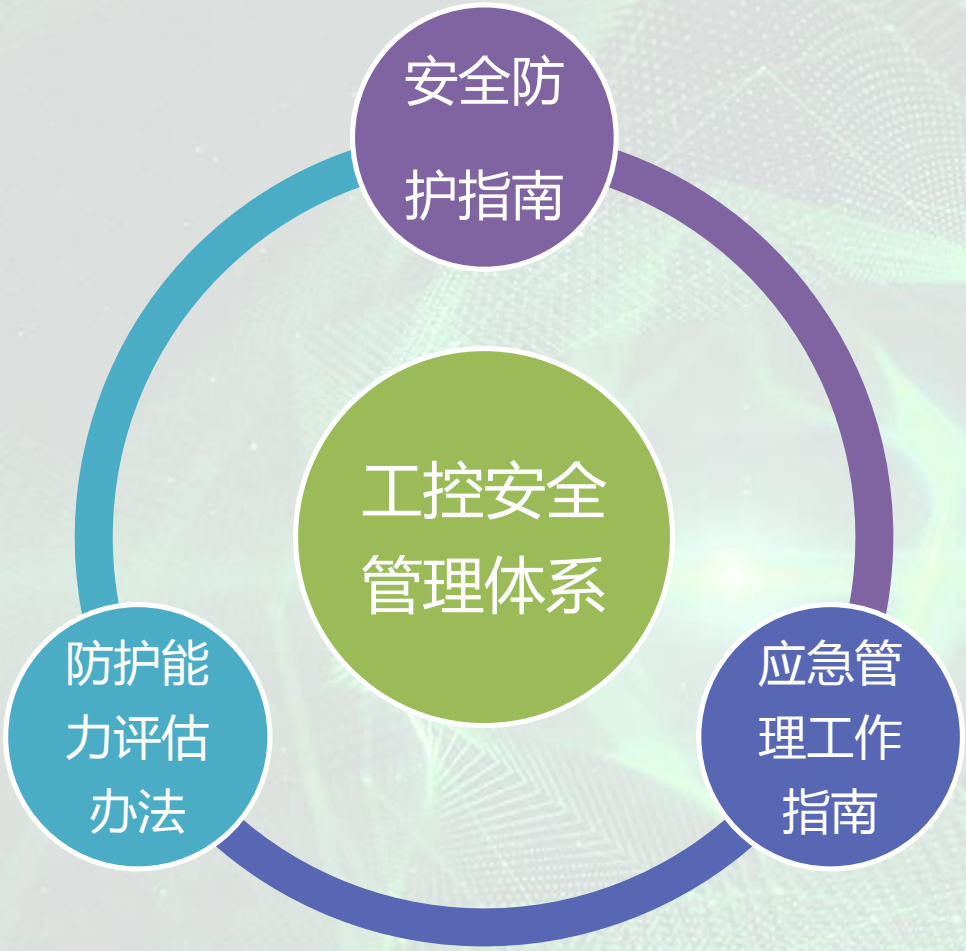
中央网信办关于印发《国家网络安全事件应急预案》的通知

中网办发文〔2017〕4号

- 中央网信办统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制。
- 中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

国家工控安全管理工作

工信部 — 建设工控安全管理体系



国家工控安全管理工作

《工业控制系统信息安全防护指南》（工信部信软[2016]338号）

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部关于印发《工业控制系统信息安全防护指南》的通知

工信软函〔2016〕338号

为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号），保障工业企业工业控制系统信息安全，制定《工业控制系统信息安全防护指南》，现印发你们。

工业和信息化部指导和管理全国工业企业工控安全防护和保障工作，并根据实际情况对指南进行修订。地方工业和信息化主管部门根据工业和信息化部统筹安排，指导本行政区域内的工业企业制定工控安全防护实施方案，推动企业分期分批达到本指南相关要求。

工业和信息化部
2016年10月17日

- 制定工控安全事件应急响应预案，当遭受安全威胁导致工控系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大。

国家工控安全管理工作

《工业控制系统信息安全事件应急管理工作指南》（工信部信软[2017]122号）

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部关于印发《工业控制系统信息安全事件应急管理工作指南》的通知

发布时间：2017-06-15 来源：信息化和软件服务业司

工信部信软[2017]122号

- 建立健全工控安全事件应急工作机制。
- 提升工控安全事件应急处置能力。

国家工控安全管理工作

《工业控制系统信息安全防护能力评估工作管理办法》（工信部信软〔2017〕188号）

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部关于印发《工业控制系统信息安全防护能力评估工作管理办法》的通知

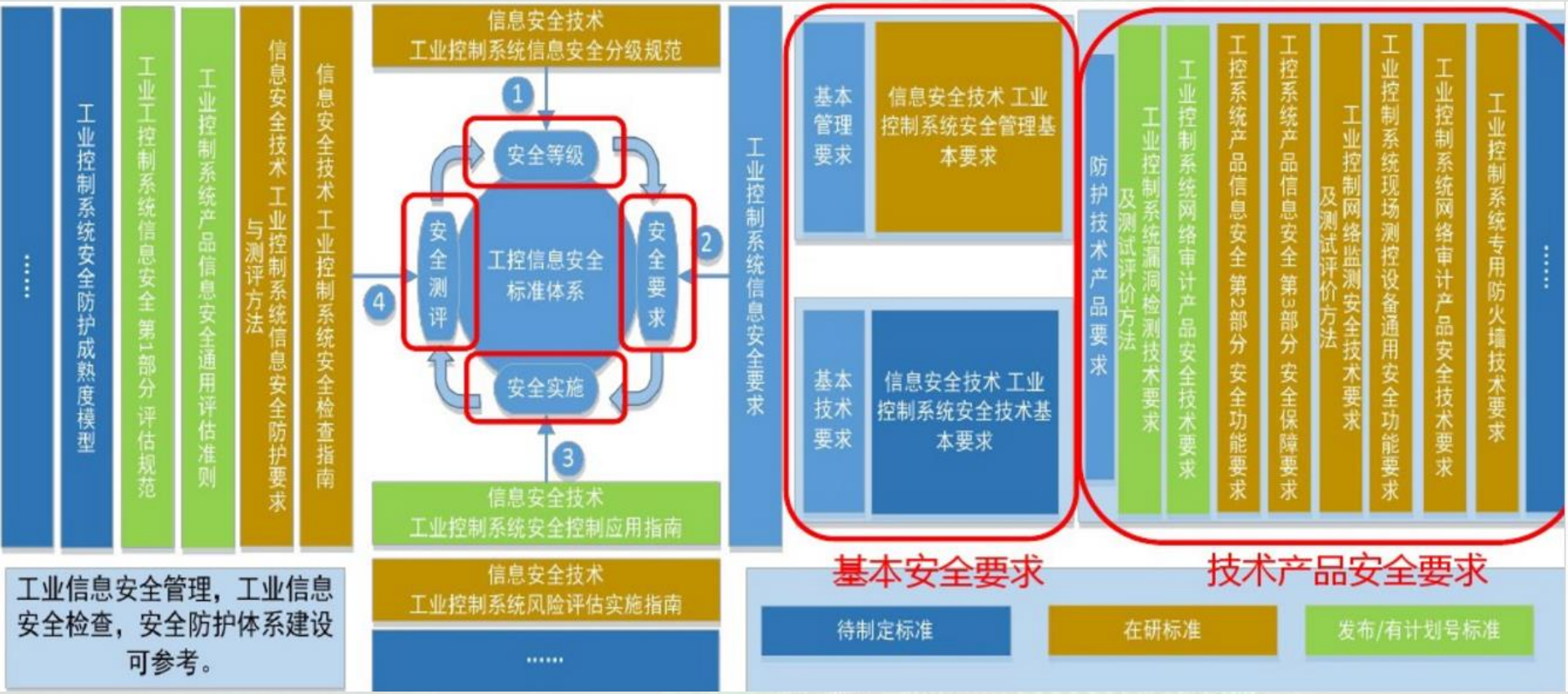
发布时间：2017-08-11

工信部信软〔2017〕188号

- 重点评估企业是否制定工控安全事件应急响应预案，并定期开展应急演练。

国家工控安全管理工作

工控安全标准体系



目录

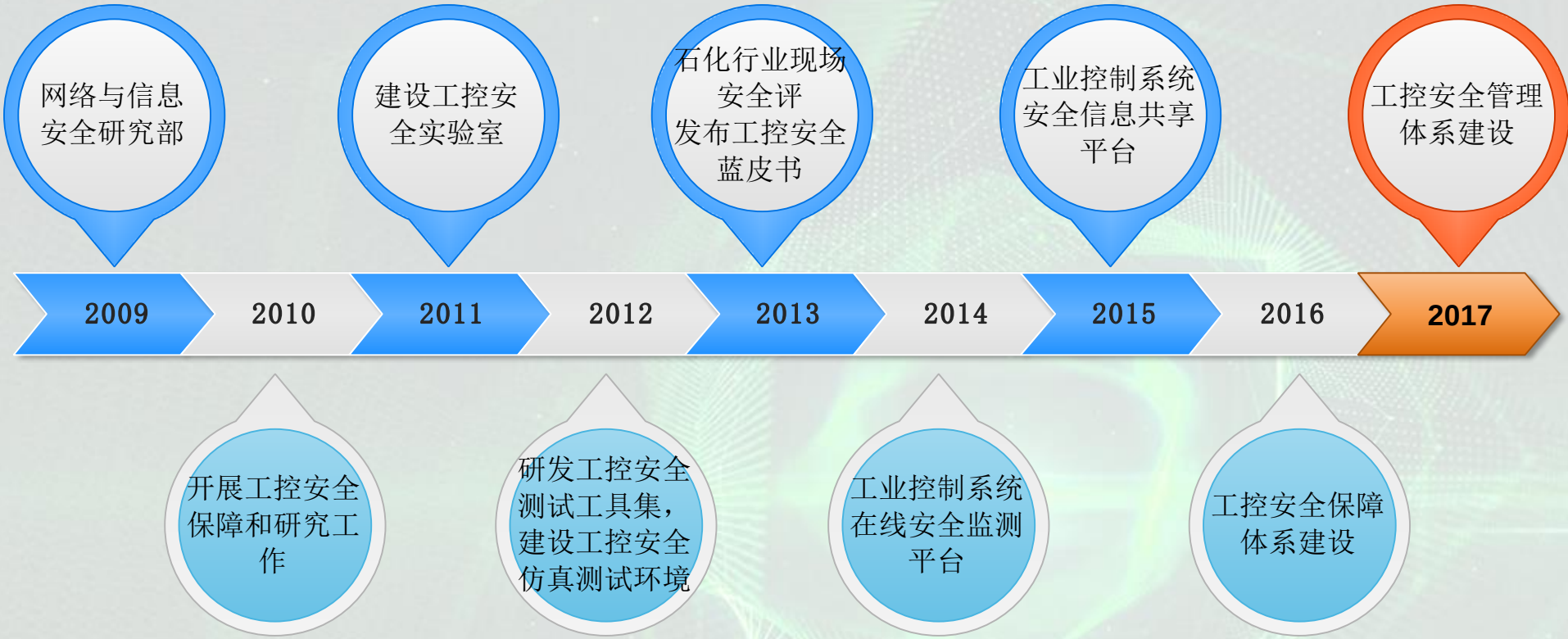
国家信息安全发展研究中心介绍

工业和信息化部电子科学技术情报研究所

2017.1.22

国家工业信息安全发展研究中心

国家信息安全发展研究中心介绍



国家信息安全发展研究中心介绍

ICS-CERT	国家工业信息安全发展研究中心
态势感知	监测预警
漏洞通报	风险通报与信息共享
技术分析	测试验证
事件响应	风险核查
检查评估	检查评估
安全培训	宣传培训
工作协调	产学研桥梁
	政策制度研究
	解决方案推进……

我们的工作

监测技术能力

- 重要工控系统在线安全监测平台
- 工控网络安全威胁捕获分析系统
- 国家工控系统安全信息共享平台
- 工业控制系统与产品安全漏洞库

我们的工作

安全检查

- 2016年工控网络安全检查：共检查8家工业企业的78个核心工业控制系统、688个工业信息系统，发现了400多项安全风险隐患。
- 自2013年8月，利用国家网络安全检查信息共享平台平台，累计处置风险漏洞7900多个。

我们的工作

工业信息安全通报

9

北京、辽宁、江苏、浙江、江西
山东、广东、四川、陕西

技术机构：电子四院、电子五所、中国软件评测中心等
科研院所：中国信息安全研究院、电子六所、电子十五所等
安全企业：启明星辰、绿盟、天融信、安天网络、威努特、烽台科技等
工控厂商：和利时、浙江中控、大华、海康威视等
社会团体：中国有色金属工业协会、中国石油和化学工业联合会、中国钢铁工业协会、中国机械工业联合会

31

我们的工作

应急处置

- 利用国家工业控制系统网络安全信息共享平台，累计通报和处置各类工控安全风险信息1425起。

- 2017年3月6日，Struts2重大漏洞披露后，迅速开展研判和应急，24小时内核查出我国9100个受影响的网站或系统，其中工业信息系统453个，紧急向地方和行业主管部门、受影响的工业企业发送通报87次。

我们的工作

国家工业信息安全产业联盟

- 原则
  - 自愿、平等、互利、合作、共享
- 目标
  - 整合资源，推动工业信息安全技术创新。
  - 促进产、学、研、用结合及成果共享
- 作用
  - 政府和产业界协同联动的平台
  - 自动化、信息化与信息安全领域的跨界融合平台
  - 行业资源整合、对接、推广平台

我们的工作

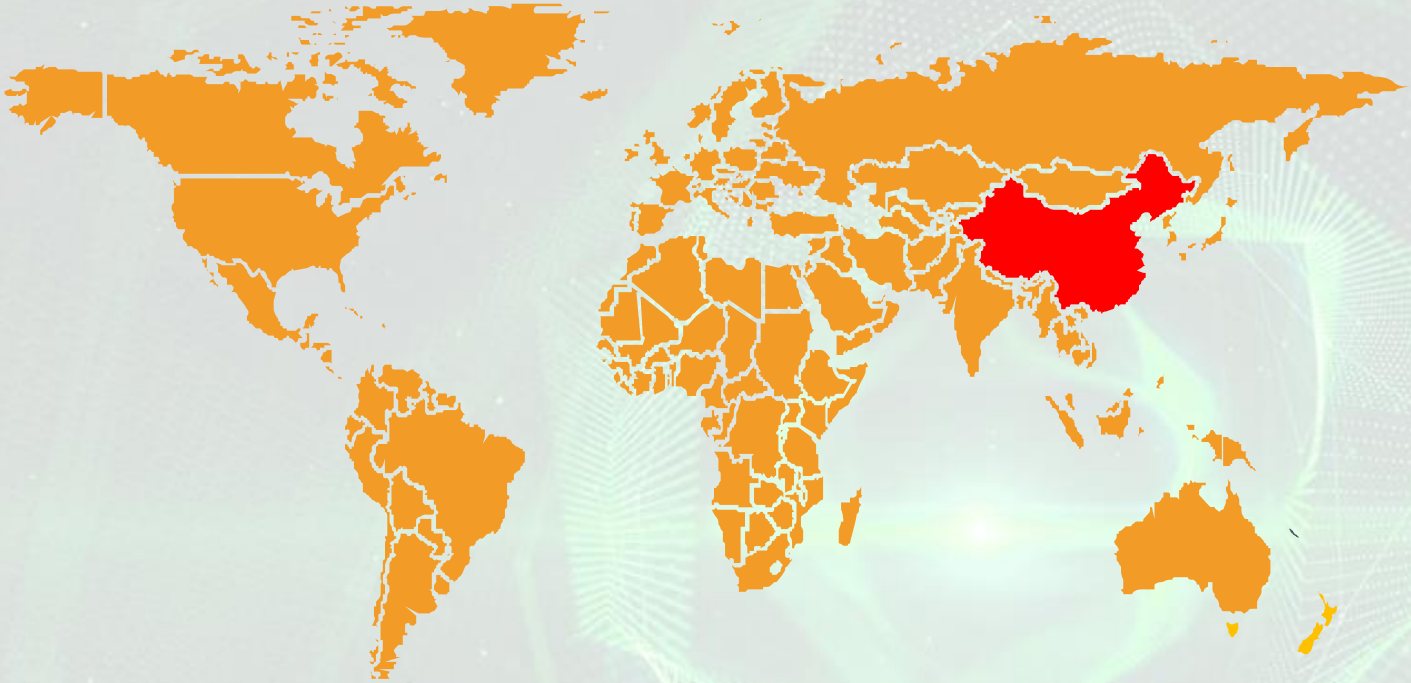
国家工业信息安全产业联盟

我们的工作

安全防护能力评估试点

我们的工作

应急体系建设



上下协同、政企联动、国际协作

谢　谢