工业信息安全态势白皮书

（2017 年）

国家工业信息安全产业发展联盟（NISIA）

二〇一七年十二月

前 言

工业自动化和信息化系统是工业设备的核心组成部分，是支撑国民经济的重要设施，是工业各行业、各企业的神经中枢。因此，工业信息安全越来越受到世界各国的高度重视，成为网络空间安全的重要组成部分。当前，国际上工业信息安全形势仍然十分严峻。作为网络攻击的高价值战略目标，暴露在互联网上的工业控制系统及设备数量不断增加，对其实施攻击的技术门槛不断降低，工控系统相关高危漏洞不断出现，重大工业信息安全事件不断发生，全球工业信息安全总体风险处于持续攀升的高危状态。

我国工业信息安全形势亦不容乐观。随着我国工业由传统产业向数字化、网络化和智能化转型升级，网络安全威胁日益向工业领域蔓延。与此同时，我国工业领域仍存在信息安全防护水平偏低、管理力度稍显不足、防护措施不到位、从业人员安全意识不强和高端技术人才匮乏等问题。这无疑加剧了我国工业领域面临的信息安全风险。

为应对当前工业信息安全领域的严峻形势和挑战，党中央和国家站在国家安全的高度，对保障工业信息安全作出战略性、前瞻性部署，2017年，在国务院主管部门的领导组织下，我国工业信息安全工作取得显著进展，积极开展了系列文件宣贯、工控安全检查、防护能力评估等一系列工作，政策体系、管理体系、

标准体系初步构建，国家级技术支撑体系初具规模，工业信息安全共享平台运行顺畅，工业信息安全领域产学研用强强联合，工业信息安全产业呈现健康发展的喜人势头。

新时期，加强工业信息安全建设、加快构建全方位工业信息安全保障体系，是推进我国由制造大国向制造强国、网络大国向网络强国历史性转变的重要前提和基础支撑。国务院颁布《关于深化“互联网+先进制造业” 发展工业互联网的指导意见》，作为工业领域建设和发展的又一个重要指导性文件，为今后一个时期我国工业信息安全工作提出了新课题，提供了新机遇，赋予了新动能。我们要深刻理解、认真贯彻，紧密联系我国工业信息安全的现实情况，切实做好各项工作。

本书由国家工业信息安全发展研究中心会同中国电子技术标准化研究院、工业和信息化部电子第五研究所、中国信息安全研究院、中国科学院信息工程研究所、和利时、奇虎360、绿盟科技、威努特、启明星辰、杭州安恒信息、树根互联等机构和企业联合完成。由于时间关系，报告尚有许多不足之处，敬请指正。

工业信息安全态势白皮书编写组

2017 年 12 月

目 录

一、工业信息安全总体态势 1
（一）全球工业信息安全整体风险突出 1
1.暴露在互联网的工控系统及设备有增无减 1
2.工控系统网络攻击难度逐渐降低 3
3.工业信息安全高危漏洞层出不穷 5
4.重大工业信息安全事件频繁发生 9
（二）我国工业信息安全形势依然严峻 12
1.工业领域信息安全意识仍显薄弱 12
2.工控系统安全防护水平相对落后 13
3.核心技术产品自主可控程度偏低 14
（三）国内外重大工业信息安全事件剖析 15
1.Struts2 再曝远程代码执行高危漏洞 16
2.“WannaCry”勒索病毒爆发并威胁工业信息安全 17
3.新型恶意软件“工业破坏者”直指电力领域工控设备 21
二、我国工业信息安全工作取得的进展 23
（一）工业信息安全法规政策逐步健全 23
（二）工业信息安全标准体系取得进展 25
（三）工业信息安全检查评估有序开展 27
（四）工业信息安全保障能力全面提升 29
（五）工业信息安全宣传教育不断深入 31

（六）工业信息安全产业发展起势蓄能 33
三、未来我国工业信息安全面临的主要挑战 34
（一）工控系统日益成为黑客攻击和网络战的重要目标 34
（二）大批网络武器泄露显著降低工业领域的攻击门槛 35
（三）针对工业领域的勒索软件、定向攻击将愈发普遍 37
（四）工业互联网的应用普及给工控安全带来更大挑战 39
（五）工业数据作为企业核心资源面临严峻的安全风险 40
四、下一步工业信息安全工作的建议 41
（一）加强政策引导 41
（二）健全标准体系 42
（三）推动技术产品研发 42
（四）优化产业生态环境 43
（五）加快专业人才培养 43

一、工业信息安全总体态势

（一）全球工业信息安全整体风险突出

当前全球范围内工业信息安全整体形势不容乐观，监测发现，全球暴露在互联网上的工业控制系统及设备数量不断增多，工控安全高危漏洞频现，针对工业控制系统实施网络攻击的门槛进一步降低，重大工业信息安全事件仍处高发态势，波及能源、制造、医疗、通信、交通、市政等重要领域的关键信息基础设施。随着工业互联网、智能制造、物联网等各种创新应用不断发展和深入，作为工业领域的“神经中枢”，工业控制系统互联互通的趋势愈加明显，与此同时也面临着前所未有的、复杂严峻的网络安全威胁，全球工业信息安全总体风险持续攀升。

1.暴露在互联网的工控系统及设备有增无减

随着工业生产对管理和控制一体化需求的不断升级，以及网络、通讯等信息技术的广泛深入应用，越来越多的工业控制系统（以下简称“工控系统”）与企业网中运行的管理信息系统（如 MES、ERP）之间实现了互联、互通、互操作，甚至可以通过互联网、移动互联网等直接或间接地访问，这就导致了从研发端、管理端、消费端、生产端任意一端都有可能实现对工控系统的网络攻击或病毒传播，工控系统面临的安全风险进一步加大。根据对有关工控系统在线监测平台

数据的统计发现，截至 2017 年 11 月，全球范围内暴露在互联网上的工控系统及设备数量已超 10 万个（如图 1 所示），相比 2016 年年底上升了 43%。全球越来越多的工控系统及设备与互联网连接，极易暴露更多的安全风险隐患。

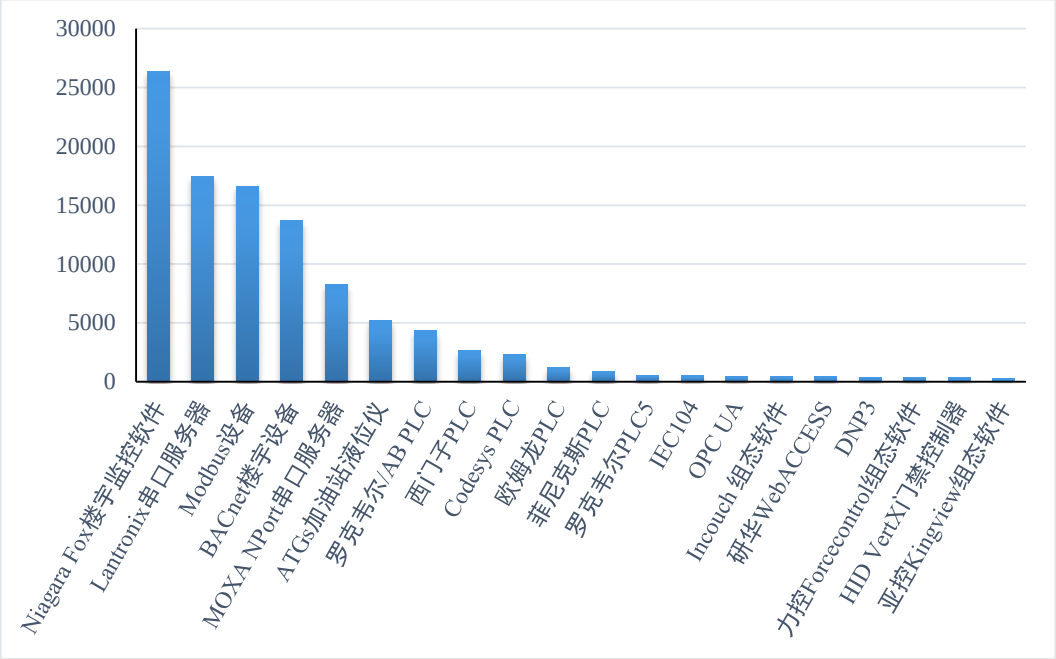


图 1 联网工控系统设备数量统计

数据来源：国家工业信息安全产业发展联盟整理分析

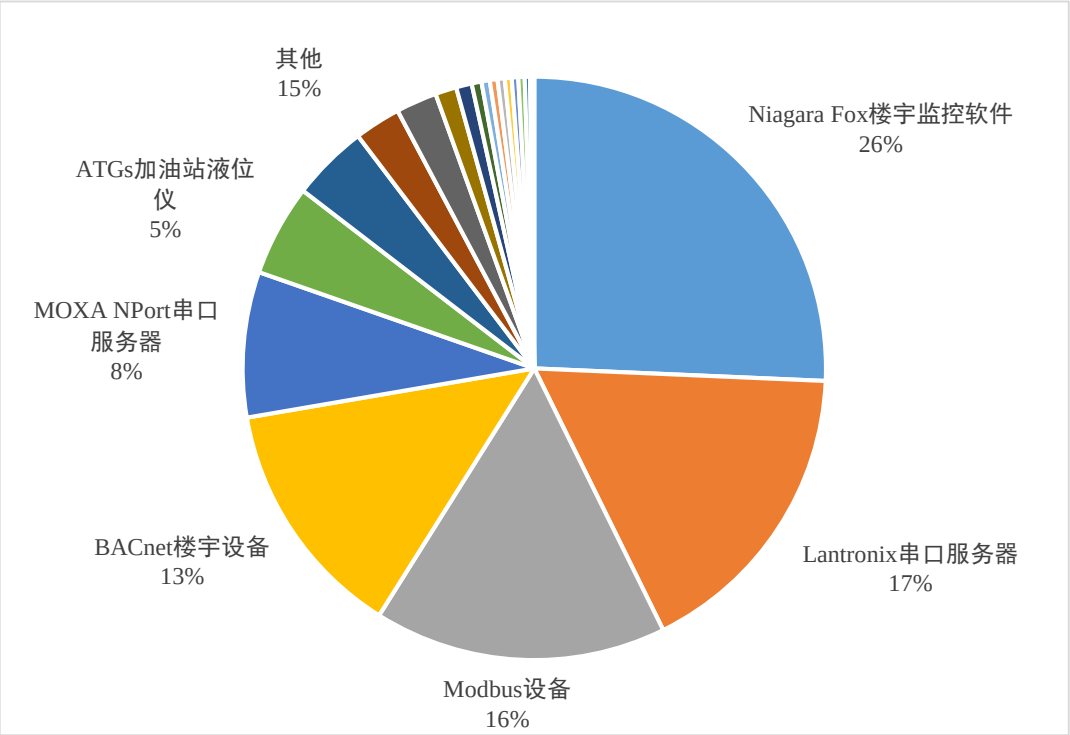


图 2 联网工控系统设备分类占比统计

数据来源：国家工业信息安全产业发展联盟整理分析

据统计，排名前十的工控系统及设备类型是 Niagara Fox 楼宇监控软件、Lantronix 串口服务器、Modbus 设备、BACnet 楼宇设备、MOXA NPort 串口服务器、ATGs 加油站液位仪、罗克韦尔/AB PLC（Ethernet/IP）、西门子 PLC、Codesys PLC、欧姆龙 PLC，前三种类型的联网工控系统数量占比依次为 26%、17%和 16%，合计占比高达 59%（如图 2 所示）。这些工控系统及设备广泛应用于制造、能源、市政等重要领域。

2.工控系统网络攻击难度逐渐降低

随着越来越多的工控系统暴露在互联网上，工控系统日

益成为“众矢之的”，黑客有目的地探测并锁定攻击目标变得更加容易。加上针对工控系统的漏洞挖掘和发布与日俱增，大量工控系统安全漏洞、攻击方法可以通过互联网等多种公开或半公开渠道扩散，极易被黑客等不法分子获取利用。如今，对工控系统的入侵攻击已不再神秘，进一步加剧了工控系统的安全风险。

一是大量工控系统软硬件设备漏洞及利用方式可通过公开或半公开的渠道获得。2015 年 12 月，俄罗斯著名工控安全研究团队在第 32 届混沌通讯大会上发布了名为“SCADAPass”的工控软硬件设备组件的默认密码清单及其更新版本，该清单涉及了 48 家工控厂商的 134 个工控设备型号，详细描述了各工控设备的设备类型、默认用户名及密码、网络端口、通讯协议与服务等敏感信息。由于工控系统运维的复杂性，大量关键信息基础设施运营单位在安装工控系统时使用产品自带的默认密码，甚至关闭密码功能。攻击者可能利用该清单获取的默认密码拿到工控设备的操作权限。2017 年 11 月 14 日，安全服务咨询公司 SEC Consult 研究人员发现西门子产品“SICAM”的远程终端单元（Remote Terminal Unit ，RTU）存在严重安全漏洞，并发布概念验证代码。

二是诸多黑客大会、开源论坛和白帽社区公开大量工控系统入侵案例细节。如今年 4 月初举办的亚洲黑帽大会上，

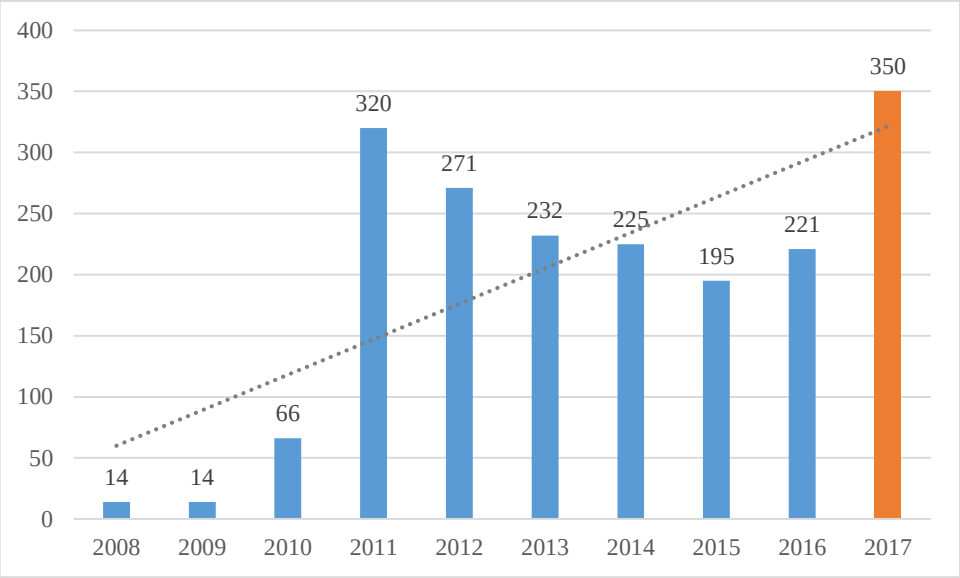
研究人员展示了世界上第一款可以在可编程逻辑控制器（PLC）之间进行传播的蠕虫病毒，发布了技术思路和概念验证程序。我国知名白帽子技术社区乌云上也有相当多SCADA 系统风险案例，详细描述了 SCADA 系统的漏洞细节和利用方式。众多开发者社区发布的工控系统安全事件技术分析报告不断增多，其中许多技术分析报告给出了网络攻击步骤、详细攻击代码甚至攻击工具等详细信息，易被黑客获取、复现以实施网络攻击。

三是美国网络武器库遭泄埋下重大工业信息安全隐患。维基解密、影子经纪人等黑客组织公开披露了大批网络攻击工具和安全漏洞，与木马病毒相结合，可被用于入侵感染工控系统，引发高频次、大规模的网络攻击，造成严重后果。例如，震惊全球的”WannaCry”勒索病毒就利用了黑客组织“影子经纪人”披露的美国国安局的“永恒之蓝”漏洞进行传播，给工控系统造成巨大危害。截至 2017 年 9 月 8 日，维基解密已经泄露 23 批美国中央情报局（CIA） Vault7 文件，这些文件中包含了大量网络攻击工具，可被直接或修改后用来对工控系统发动网络攻击，潜在的安全隐患极大。

3.工业信息安全高危漏洞层出不穷

一是工业信息安全漏洞数量连年呈现高发态势。白皮书在综合参考美国 CVE、NVD、CNVD 和 CNNVD 收录的工控漏洞信息的基础上统计发现，近年来全球漏洞数量居高不

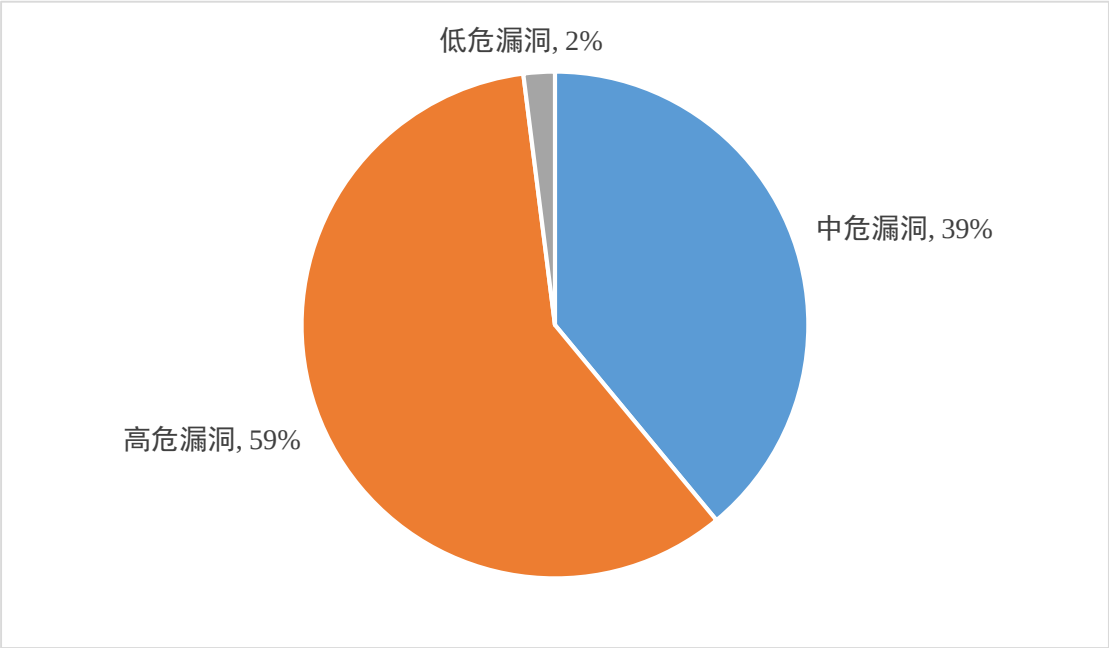
下，尤其在 2011 年漏洞数量发生急剧增长，比上一年几乎翻了 4 倍(见图 3),2016 年到 2017 年的增长率也超过了 50%，工控安全漏洞威胁十分严重。



数据来源：工控系统行业漏洞库平台
http://ivd.winicssec.com/index.php/Home/Index/index/p/12.html

图 3　工控漏洞数量变化趋势

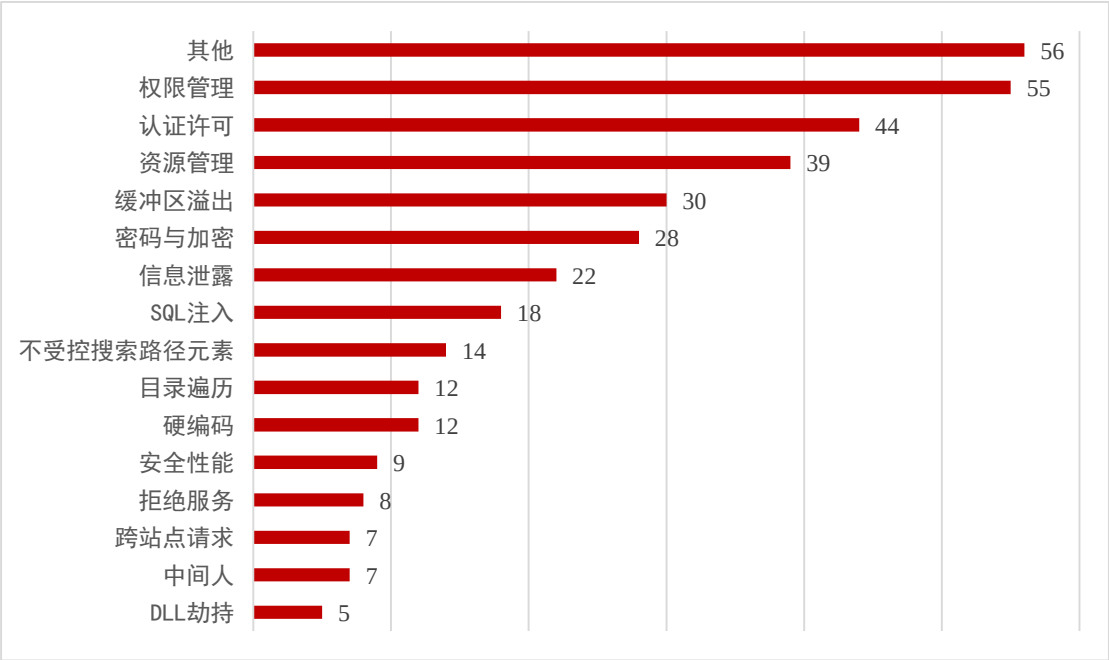
二是半数以上的工控安全漏洞均为高危漏洞。截至 2017 年 11 月，在国家工业信息安全发展研究中心跟踪研判的所有 366 个工控相关漏洞（涉及工业控制、智能设备、物联网等领域）中，高危漏洞数量占比最高，达到 59%，其次是中危漏洞，占比也达到 39%，低危漏洞占比为 2%。由于披露的工控相关漏洞大多重要程度高，危险性大，一旦被利用，极易造成破坏性的后果。



数据来源：国家工业信息安全发展研究中心统计

图 4　2017 年全球工控相关漏洞的威胁等级分布

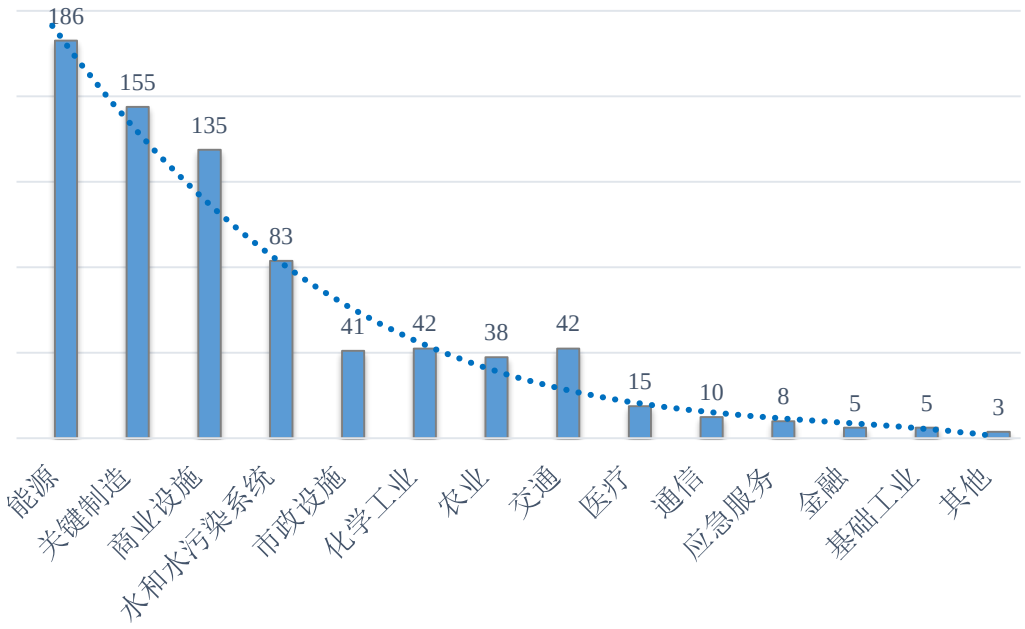
三是披露的漏洞类型呈现多样化特征。具体包括权限管理、认证许可、资源管理、缓冲区溢出、密码与加密问题、信息泄露、不受控搜索路径元素、SQL 注入、目录遍历、硬编码 、安全性能、拒绝服务、跨站点请求、中间人、DLL 劫持等，共有 33 种以上。其中权限管理、认证许可、资源管理、缓冲区溢出、密码与加密、信息泄露等漏洞类型数量最多（见图 5）。对业务连续性、实时性要求高的工控系统来说，无论是利用这些漏洞造成业务中断、获得控制权限还是窃取敏感生产数据，都将对工控系统造成极大的安全威胁。



数据来源：国家工业信息安全发展研究中心统计

图 5　2017 年全球工控漏洞类型的分布情况

四是工控漏洞广泛分布在能源、制造、商业设施、水务、市政等重点领域。根据美国工业控制系统网络安全应急响应小组（ICS-CERT）统计，在其 2016 年跟踪发布的 392 个关键基础设施相关行业安全漏洞中，多数分布在能源、制造、商业设施、水务、市政等密切关系国计民生的关键基础设施领域。其中，能源行业稳居第一位，相关漏洞共计 186 个，关键制造业紧随其后，相关漏洞共计 155 个（如图 5 所示）。



数据来源：US ICS-CERT，国家工业信息安全产业发展联盟整理

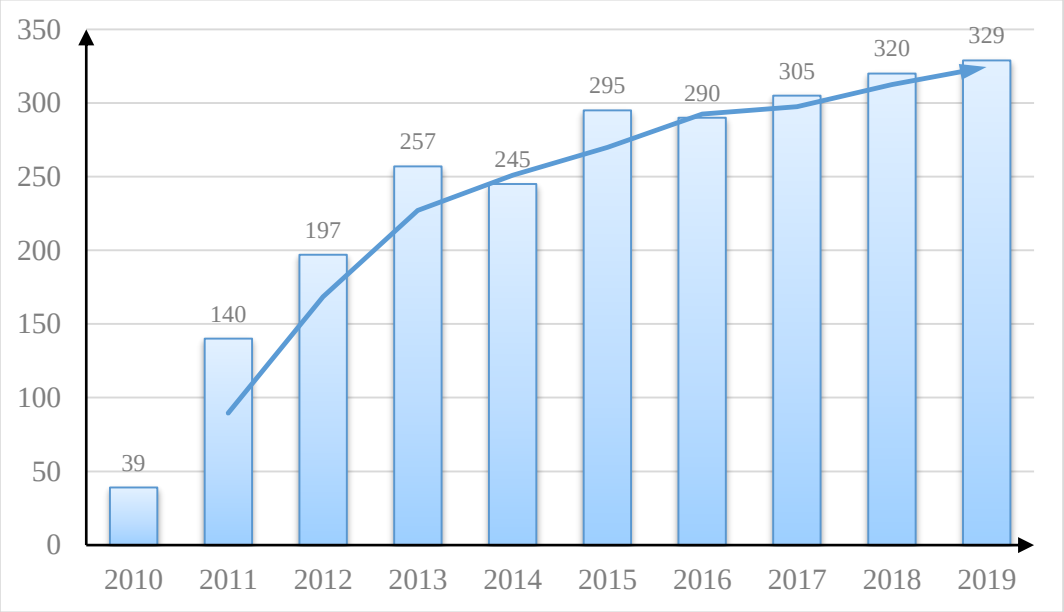
图 6　2016 年关键基础设施相关行业工控漏洞分布情况

五是工控漏洞的修复进度较为迟缓。卡巴斯基实验室工控系统网络应急响应小组（Kaspersky Lab ICS CERT）在其发布的《2017 上半年工业自动化系统的威胁景观》报告中指出，2017 年上半年全球新增的工控漏洞数量要明显高于修复的漏洞数量，漏洞处置进度迟缓。究其原因在于，一方面供应商漏洞修复工作的优先级别较低，还要受到软件开发迭代周期的限制；另一方面工业企业出于维持业务连续性的考虑，及时更新和安装补丁的积极性不高。

4.重大工业信息安全事件频繁发生

近年来，全球工业领域发生的信息安全事件愈发频繁，事件数量高居不下，遍及各个工业领域，事件波及范围不断扩大，造成的后果也愈加严重。根据美国 ICS-CERT 发布

《ICS-CERT 年度回顾》，自 2010 年以来，工业领域网络安全事件呈现逐年上升的趋势，特别是 2015 年以来，每年发生的安全事件数量接近 300 起（见图 7）。

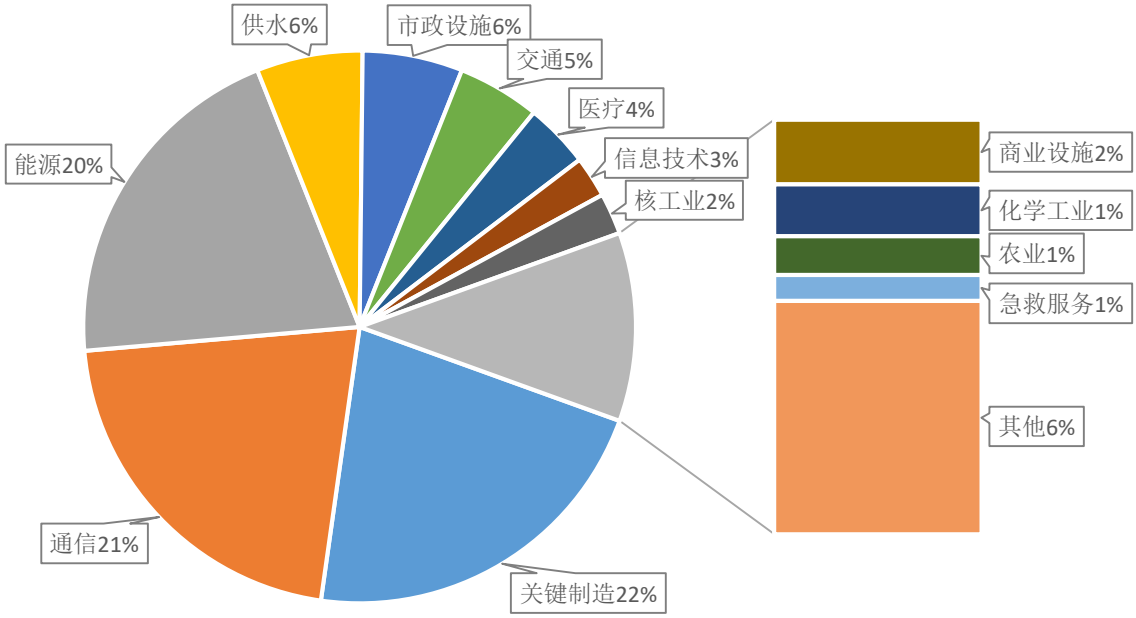


数据来源：美国 ICS-CERT，国家工业信息安全产业发展联盟整理

图 7 美国 ICS-CERT 历年安全事件报告数量[1]

从被攻击事件发生所在行业的分布来看，关键制造、通信、能源、供水和市政设施是安全事件发生较多的前五个行业（如图 8 所示）。

[1]注：2017 年数据统计截止至 11 月 10 日，2018 年、2019 年为预测数据。



数据来源：美国 ICS-CERT，国家工业信息安全产业发展联盟整理

图 8 工控安全事件发生所在行业分布情况

同时，近年来重大工业信息安全事件时有发生，对工业生产和国家安全造成严重影响。2015 年 12 月，乌克兰电力系统遭受黑客攻击，将可远程访问并控制工控系统的 BlackEnergy（黑暗力量）恶意软件植入乌克兰电力部门，造成电网数据采集和监控系统崩溃，导致伊万诺—弗兰科夫斯克地区大约一半家庭停电数小时。2016 年 3 月，Verizon 公司发布的安全事件报告中称一家名为 Kemuri 的水务公司自来水控制系统被黑客攻击，导致正常供水受到影响。2016 年 10 月，美国、德国、利比亚遭受大规模 DDoS 攻击，造成大面积网络瘫痪。2017 年 2 月，一种几乎无法被检测到的极为复杂的恶意程序感染了全球超过 140 家机构的计算机系统，

包括美国、南美、欧洲和非洲的银行、通信、市政等多种关键信息基础设施系统。2017 年 5 月，“蠕虫式”勒索软件“WannaCry”勒索病毒入侵了全球 150 多个国家的信息系统，雷诺、日产等汽车制造厂商被迫停产，多国能源、通信等重要行业损失惨重。这些攻击通常都是经过精心策划的，并且可对现实世界造成严重后果。

（二）我国工业信息安全形势依然严峻

随着《中国制造 2025》的全面推进，我国工业领域的数字化、网络化、智能化水平加快提升，各类新技术、新产品、新模式不断涌现，信息安全风险隐患交织联动。与此同时，我国工业企业工控安全防护水平偏低，仍存在管理力度不足、防护措施不到位、人员意识不强和技术人才匮乏等一系列问题，无疑加剧了工控系统面临的安全风险。

1.工业领域信息安全意识仍显薄弱

目前我国在工控安全管理工作中仍存在不少问题，各地区、各部门、各工业企业对工控系统信息安全问题重视仍不够，大量工业企业责任人对网络安全工作认识还不到位，重发展轻安全，安全投入严重不足，导致工业企业存在较多安全隐患，对工业生产安全和社会正常运转造成威胁。主要体现在：**一是**网络安全宣传培训教育工作不足，员工的信息安全意识相对欠缺，无法帮助企业及时发现存在的安全隐患；

二是拥有网络安全专业背景和技术能力的人员匮乏，一旦企业出现工业信息安全问题无法及时采取措施应对；**三是**大量业务系统、数据库使用弱口令，大大降低了黑客等不法分子突破企业边界的难度，使企业被攻击的安全风险急剧上升；**四是**网络安全管理制度不完善，且部分现行制度未能有效执行，例如我国工业主管部门指导企业开展工业信息安全工作的相关文件未能有效执行，或企业员工未按管理规定开展相关工作，致使企业出现工业信息安全管理混乱、工业信息安全责任不明晰、生产数据等敏感信息外泄等问题。

2.工控系统安全防护水平相对落后

工控系统作为工业领域的神经中枢，在设计之初基本处于与外网隔离的状态，因此多数未考虑信息安全防护问题。随着近年来工业互联逐步深入发展，传统工控系统安全所依赖的封闭假设被网络化甚至是互联网化彻底打破，这使得原本脆弱的工控系统要同时面临来自内外网的、更为复杂多变的安全风险。

通过我国今年开展的工控系统防护能力评估工作发现，多数企业缺乏针对工控系统的有效防护措施，我国工业企业整体防护水平相对落后，仍存在工业主机安全管理和防护不到位、工控系统网络边界防护措施不足、工控系统未建立安全配置、工控系统未使用身份认证、部分无效服务默认开启等问题。国家工业信息安全发展研究中心通过工控系统在线

安全监测平台发现的暴露于互联网的重要工控系统中，约 20%的系统可被远程入侵并完全接管。同时，工业企业的信息安全应急灾备手段不足，约 70%的被查工业企业缺少完善的应急灾备体系，一旦发生信息安全事件导致数据损坏或丢失，将无法进行恢复。再者，安全管理制度落实不到位，U 盘、WiFi、手机的违规使用，系统源代码等敏感信息在开源平台泄露公开，均为企业安全带来极大风险隐患。从总体上看，相比于发达国家，我国工业信息安全防护技术能力仍显薄弱，手段相对落后，事件应急较为迟缓，工业企业的信息安全防护水平亟待提高。

3.核心技术产品自主可控程度偏低

当前，我国各个行业、各个领域的重要工控系统大量采购国外技术和设备，受制于人的局面尚未得到根本改变。针对国内数据库市场统计发现，Oracle、IBM、SAP 占据国内结构化数据库 70%以上的市场份额，达梦、神舟、人大金仓等国产数据库仅占据 7%的低端市场份额；在非结构化数据库市场，IBM、EMC、Oracle 占据了一半以上市场份额。根据我国近几年重点领域信息安全检查工作统计，数千个工控系统由国外厂商提供运行维护，大量工业企业不具备自主维护能力，系统运行的可控能力较低，同时缺乏对国外产品和服务的监管，缺少必要的技术检测措施和安全可控方案，风险难以掌握。

我国 CPU、服务器、操作系统等核心产品和技术发展滞后，国产化率低，核心竞争力不足，是推动工控领域实现自主可控过程中亟待突破的关键症结。部分国产工业控制基础软件仍然缺乏基础编码、软件开发、接口集成、运行维护等接口的标准与规范，导致软件的可扩展性、可配置性、可重构性和互操作性较差，应用效果不佳。部分涉及国家基础设施建设的关键行业，在精密采集、精准时钟、智能算法、故障定位、中断调度等方面的核心设备、产品和技术仍然受制于国外公司，本土企业自主创新能力仍然不强。

此外，我国现有工业信息安全产业规模有待进一步扩大，产业核心基础能力相对不足，产业生态体系尚未健全。目前我国工业信息安全产业包括产品、技术、服务等占整个 IT 业比重不足 2%，远低于欧美发达国家近 10%的水平。我国工业领域有庞大的信息化投入和广泛的应用市场，但在安全方面的投入与西方国家差距过大，很难支撑我国加速推进智能制造、工业互联网过程中的安全需求。

（三）国内外重大工业信息安全事件剖析

2017 年以来，在全球范围内先后发生了 Struts2 高危漏洞危及多个重要领域关键信息基础设施、”WannaCry”勒索病毒席卷全球等多起重大工业信息安全事件，波及范围十分广泛，影响程度极为严重。此外更是出现了专门瞄准工控系统的新型恶意软件“工业破坏者”（Industroyer），能够通过入侵

系统引发大规模停电，甚至造成电力设备损坏和级联故障。国内外工业信息安全事件频发，亟须引起高度重视。

1.Struts2 再曝远程代码执行高危漏洞

2017 年 3 月 6 日，Apache 基金会公布了一个针对 J2EE 框架 Struts2 的远程代码执行漏洞（漏洞编号 S2-045，CVE 编号 cve-2017-5638），涉及 Struts 2.3.5—Struts 2.3.31、Struts 2.5—Struts 2.5.10 多个版本。S2-045 漏洞的危害程度超出了之前曝出的 S2-016、S2-019、S2-032 等高危漏洞，且影响范围广泛，市政、电力、航空航天、装备制造、水利等多个工业领域受到影响。

（1）漏洞背景

Struts 是美国阿帕奇（Apache）基金会 Jakarta 项目组的一个开源项目，采用 Model View Controller（MVC）模式，帮助 Java 开发者利用 J2EE 开发 Web 应用，主要提供两个版本框架产品：Struts 1 和 Struts 2。Apache Struts2 是世界上最流行的 Java Web 服务器框架之一，在金融、电力、交通、医疗等领域的关键信息基础设施中均有广泛应用。

（2）技术原理

此次曝光的 S2-045 漏洞的利用无需任何前置条件（如开启 dmi，debug 等功能）以及启用任何插件，攻击者可绕过绝大多数防护设备的通用防护策略，在使用基于 Jakarta 插件的

文件上传功能时，通过修改浏览器 HTTP 请求头中的 Content-Type 值来触发该漏洞，直接获取应用系统所在服务器的控制权限，执行系统命令，进而对受影响站点造成极为严重的危害，引发数据泄露、网页篡改、后门植入等安全事件。

（3）影响分析

S2-045 漏洞影响主要体现在以下三个方面：

一是大量重要系统面临严重安全威胁。工业企业的部分信息系统如生产运行管理系统、办公自动化系统（OA）、企业资源计划系统（ERP）中大量应用了 Struts 架构，攻击者可利用漏洞获取系统权限，进而渗透至工业生产内网，可能造成严重的生产安全事故。

二是漏洞能导致数据泄露、DDoS 攻击和远程服务器控制。S2-045 漏洞影响巨大，黑客可利用该漏洞对远程目标服务器执行系统命令，轻则窃取系统数据信息，重则可取得系统服务器控制权，构成信息泄露、运行安全等威胁。

三是漏洞潜在影响严重。攻击者可通过 S2-045 漏洞作为突破口渗透进入系统内部并长期蛰伏，持续收集各种信息，众多工业相关系统都面临严重的潜在影响。

2.“WannaCry”勒索病毒爆发并威胁工业信息安全

2017 年 5 月 12 日，“WannaCry”勒索病毒在全球范围内大规模爆发，电力、石油、通信、交通运输、医疗等众多行

业领域受到事件影响，据统计，此次勒索病毒感染了全球 150 多个国家的 30 万台主机。从我国受影响情况来看，教育、政府、能源、电力等重点领域重要系统均受到相关波及，造成系统中断、数据丢失、业务停摆等一系列严重后果。从源头上看，该勒索病毒利用了今年 4 月遭泄密的美国国家安全局（NSA）网络军火库中的“永恒之蓝”攻击程序，通过 Windows 系统漏洞实现迅速广泛传播。

（1）攻击原理

“WannaCry”勒索病毒主要利用美国国家安全局（NSA）泄露的网络武器“永恒之蓝”和 Windows 操作系统 445 端口的“MS17-010”漏洞进行传播和感染，具有自我复制、主动传播的特性，利用 RSA 和 AES 两种加密算法对文件进行加密。“WannaCry”勒索病毒攻击过程由攻击启动，传播与感染，文件加密，文件解密四个步骤组成，各个步骤的详细情况如下:

攻击启动: “WannaCry”勒索病毒勒索软件启动后，首先尝试连接到一个被称为“开关域名”的域名，如果该域名能成功连接，则退出执行，否则进入感染释放阶段。

传播与感染: 勒索软件启动传播之后，恶意代码会判断当前执行的参数个数，如果参数小于 2 个，恶意代码就会进入到感染阶段，创建服务名为“mssecsvc2.0”的服务并启动执行，然后恶意代码会加载资源数据，并通过运行“tasksche.exe”程序来加密用户文件进行勒索。如果参数大于 2 个，则通过

服务以“-m security”形式运行，进入到传播阶段，利用服务器信息模块（Server Message Block，SMB）的“MS17-010”漏洞，创建线程向局域网中的其他 IP 发送远程执行代码进行传播。

文件加密：一旦进入感染阶段，恶意代码就开始对主机进行加密勒索。首先，勒索程序会获取主机的名称，并据此名称生成一个唯一标识来标识被感染主机。然后，勒索软件会解压并释放加密程序到被感染的主机。最后，运行加密程序对被感染主机文件进行加密。勒索软件同时使用对称加密算法（AES 加密算法）和非对称加密算法（RSA 加密算法）对主机文件进行加密，其中 RSA 算法直接调用微软“CrtyptAPI”函数库中的代码，AES 算法则采用将代码静态编译到动态链接库（Dynamic Link Library，DLL）中的方式进行调用。首先勒索软件随机生成一个 128 位的 AES 密钥，然后用该密钥加密用户的文件，最后使用 RSA 公钥将生成的 AES 密钥进行加密。对于不同的文件该勒索软件使用不同的 AES 密钥。

解密原理：为了向用户展示能够成功解密文件，引导用户支付赎金，程序内置了其中一个公钥配对的私钥，可解密部分文件。解密时，程序首先会判断本地是否存在解密所需的私钥文件，如果存在，则尝试解密文件来判断密钥是否正确。如果文件不存在或者文件存在但密钥错误，勒索软件会创建服务与远程服务器进行通信，查询付款信息，若用户已

经成功缴纳赎金，则服务器返回私钥文件，然后用返回的私钥文件进行解密。

（2）影响分析

“WannaCry”勒索病毒肆虐，俨然是一场全球性互联网灾难，给广大电脑用户造成了巨大损失，影响范围十分广泛。在能源行业，西班牙电力公司 Iberdola、天然气公司 Gas Natural 因勒索病毒攻击影响正常工作。在通信行业，西班牙电信巨头 Telefonica，俄罗斯第二大电信运营商 Megafon 等均受到不同程度的影响。在交通运输行业，德国德累斯顿火车站、丹麦的航运巨头马士基集团等受到勒索病毒的攻击。在医疗行业，英国卫生保健系统受到极大影响，英格兰 48 家机构、苏格兰 13 家机构报告称医院遭受勒索病毒攻击，被迫使用纸质办公；除此之外还有美国、印尼的少数医院也受到勒索病毒攻击。于此同时，政府部门也未能幸免，俄罗斯外交部、内政部、印度安得拉邦警察局等国家的相关政府部门的计算机也感染了勒索病毒。“WannaCry”勒索病毒的大面积爆发，给全球各国的网络安全敲响了警钟。

（3）我国工业领域受影响情况

我国石油石化、通信等工业行业也遭受了“WannaCry”勒索病毒的影响。在石油行业，“WannaCry”勒索病毒攻击造成某大型石油公司的 2 万座加油站短时间内无法使用银行卡及网络支付，影响范围波及北京、上海、杭州、重庆、成都、

南京等多个城市。

3.新型恶意软件“工业破坏者”直指电力领域工控设备

2017 年 6 月，据外媒报道，美国关键基础设施安全公司 Dragos 和斯洛伐克杀毒软件公司 ESET 的研究人员发现了一款对工控系统存在安全威胁的恶意软件“工业破坏者”（Industroyer）。安全研究人员经分析认为，“工业破坏者”恶意软件与 2016 年 12 月 17 日发生在乌克兰首都基辅输电变电站的网络攻击事件有关。

（1）基本情况

“工业破坏者”主要针对电力工控系统，具有部分组件定制化、能够逃避检测等特点，可通过入侵系统引发大规模停电，甚至造成设备损坏、级联故障等严重后果，全球电力等关键行业领域的工控系统面临着被入侵的巨大威胁。

（2）技术分析

一方面，该恶意软件支持对多种广泛应用于关键信息基础设施的电力自动化协议的利用。“工业破坏者”可以支持 IEC 60870-5-101、IEC 60870-5-104、IEC 61850 以及 OLE 处理控制数据访问（简称 OPC DA）四种协议，这四种协议广泛应用于变电站、交通管理、供水系统等关键信息基础设施中。开发者可以利用该恶意软件重新设置程序攻击任何使用这些协议的工控系统，还可以通过软件定制化实施对特定对象的攻击，比如扩展支持对 DNP3 协议的利用后，就可以实

施对北美电力系统的定向打击。

另一方面，该恶意软件能利用重要工业自动化设备漏洞实施攻击。经测试，“工业破坏者”可以利用西门子 SIPROTEC 系列保护继电器的一个漏洞实行溢出攻击，从而导致其停止响应，引发大规模停电，必须手动重启设备才能恢复。

（3）事件影响

从直接危害看，“工业破坏者”可以导致变电站的继电保护和控制系统无法正常工作，通过攻击一个变电站就能导致多个变电站级联断电，从而引发大面积停电。据安全研究人员分析称，“工业破坏者”的功能足以完成导致乌克兰停电事件的网络攻击，而且恶意软件的激活时间点也恰巧是 2016 年 12 月 17 日（即停电事故发生的日期）。

从潜在影响看，“工业破坏者”是一款全新的专门针对工控系统的网络武器，在此之前，现实世界仅出现过为数不多的可以针对工控系统的恶意攻击程序，分别是 BlackEnergy、Havex 和 Stuxnet。同时，该恶意软件还是迄今为止第一款可以直接与电网硬件进行交互的公开恶意软件。

通过对该恶意软件攻击原理进行分析，可以看出“工业破坏者”恶意软件的开发者对电力行业基础设施中工控系统的工作方式有相当全面的了解，表明黑客已经具备很强的工控系统相关知识，如果进一步拓展该恶意软件的协议支持类型以及攻击方法，将会造成更加严重的影响。

二、我国工业信息安全工作取得的进展

党中央、国务院高度重视网络安全。习近平总书记提出了没有网络安全就没有国家安全的科学论断，将网络安全作为总体国家安全的重要组成部分。在党的十九大报告中，总书记强调：“坚持总体国家安全观。统筹发展和安全，增强忧患意识，做到居安思危，是我们党治国理政的一个重大原则。”工业信息安全作为网络安全的重要组成部分，是保障国家总体安全的重要内容，为实施制造强国战略和推进“互联网+”行动计划提供支撑。2017 年，我国工业信息安全工作取得显著进展，积极开展了指南文件宣贯、工控安全检查、防护能力评估等一系列工作，政策体系、管理体系、技术支撑体系初步构建，国家级技术队伍建设初具规模，工业信息安全产业呈现良好发展势头，工业信息安全保障水平有了明显提高。

（一）工业信息安全法规政策逐步健全

近年来，国家从法律法规、战略规划、标准规范等多个层面对工业信息安全做出了一系列工作部署，提出了一系列工作要求。

今年 6 月起正式实施的《中华人民共和国网络安全法》要求对包括工控系统在内的“可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”实行重点保护。去年 12 月国家互联网信息办公室发布的《国家网络空间安全战略》

提出要“采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏”。《中国制造 2025》提出要“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”。《国务院关于深化制造业与互联网融合发展的指导意见》将“提高工业信息系统安全水平”作为主要任务之一。近期刚发布的《关于深化“互联网+先进制造业”发展工业互联网的指导意见》（以下简称《指导意见》）围绕制造强国和网络强国建设的安全保障需求，以“强化安全保障”为指导思想、“安全可靠”为基本原则，提出“建立工业互联网安全保障体系、提升安全保障能力”的发展目标，部署“强化安全保障”的主要任务，为工业互联网安全保障工作制定了时间表和路线图。

作为国务院工业和信息化工作的主管部门，工业和信息化部从总体国家安全观出发，高度重视工业信息安全，对加强工控安全防护工作提出了一系列指引。2011 年 9 月，工业和信息化部印发了《关于加强工控系统信息安全管理的通知》（工信部协〔2011〕451 号）文件，有效提升了相关主管部门和工业企业的工控安全意识。为应对新时期下的工控安全新形势，2016 至 2017 年，工业和信息化部陆续发布《工业控制系统信息安全防护指南》、《工控系统信息安全事件应急管理工作指南》和《工业控制系统信息安全防护能力评估工作管理办法》等政策文件，明确工控安全防护、应急以及能

力评估等工作的要求，这三个政策文件共同构建了工控安全管理体系，进一步完善了工业信息安全顶层设计。

（二）工业信息安全标准体系取得进展

工业信息安全标准体系的建设对促进工业产业健康发展有着极其重要的规范和指导作用。全国信息安全标准化技术委员会（TC260）在国家标准委的领导下，对全国信息安全标准进行统一归口管理。除此，全国电力系统管理及信息交换标准化技术委员会（TC82）、全国工业过程测量和控制标准化技术委员会（TC124）、全国电力监管标准化技术委员会（TC296）等标准化机构也在积极推动工业信息安全相关国家标准的研制工作。截至目前，我国已发布工业信息安全相关国家标准 10 余项，在研国家标准近 20 项，已初步建立了工业信息安全系统级标准体系。

随着工业化与信息化融合步伐加快，通过深入分析新背景下工业领域面临的信息安全问题和标准化需求，借鉴联邦信息安全管理法中有关风险管理的规定和做法，以及 ISO/IEC27000 等国外标准体系中信息安全管理的先进经验，经过组织行业讨论和试验验证，我国重点围绕工控系统信息安全，目前已经形成较为清晰完整的标准体系，包括安全等级、安全要求、安全实施和安全测评四类标准。四类标准作为开展工控系统信息安全工作的四个阶段，依次形成循环，切实提高工控系统的信息安全保障能力。同时，在每类标准

的基础上，可按照标准所涉及的主要内容进行细分。考虑到新一代信息技术产业的飞速发展，为提高标准体系的延伸与可扩展性，围绕工业互联网、工业大数据、物联网等重点领域信息安全问题进行标准体系完善，总体框架如下图所示。

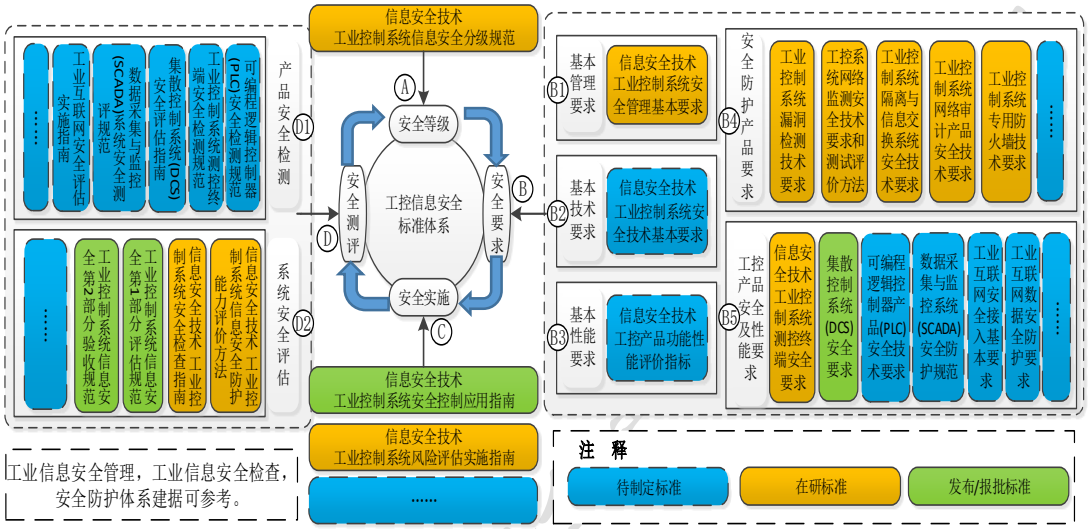


图 9　工业信息安全标准体系总体参考框架

1、安全等级

安全等级类标准旨在通过制定《工控系统信息安全分级规范》等标准，区分传统信息系统安全要素，从工业系统重要性程度、受侵害后潜在影响程度、信息安全威胁等级等方面综合评定工业控制系统信息安全等级。

2、安全要求

安全要求类标准从管理、技术和性能三方面提出系统级信息安全基本要求。同时，通过细化产品与技术分类，面向工控系统（PLC 系统、SCADA 系统、DCS 系统）、工业设备

（嵌入式终端、工业主机、工业网络通信设备）、工业安全技术（漏洞检测技术、网络监测安全技术）、工业安全防护产品（工业防火墙、安全审计产品）、工业新应用（工业互联网、工业大数据、工业云、物联网）等方面提出具体的安全要求。

3、安全实施

安全实施类标准主要为工控系统信息安全实施提出安全指导。当前，全国信息安全标准化委员会发布了《工控系统安全控制应用指南》，该标准提供了可用于工控系统的安全控制列表，规范了工控系统的安全控制选择过程，制定工控系统的安全程序，形成具体安全解决方案。

4、安全测评

安全测评类标准旨在制定工业系统相关产品安全检测认证以及安全能力评估等第三方测评与服务类标准，确保信息安全控制措施的科学性和有效性，根据测评结果和风险评估提高工业产品信息安全质量，及时调整信息安全策略，助力工业企业整体提升安全防护能力。

（三）工业信息安全检查评估有序开展

为进一步贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》等文件的要求，加强对工控安全工作的指导和督促检查，提升企业管理和技术防护水平，工业和信息化部在历年检查工作基础上，进一步扩大检查范围，扩展检查深度，组织开展了2017年度工控安全检查工作。此项工

作是推动《工业控制系统信息安全防护指南》(以下简称《防护指南》)落地实施的重要举措。国家工业信息安全发展研究中心、中国电子技术标准化研究院、工业和信息化部电子第五研究所和中国软件评测中心组织技术人员赴生产现场检查。

此次检查以“突出重点、兼顾一般”为工作原则，按照企业安全自查、检查队伍技术抽查等方式开展。其中，自查工作覆盖全国 31 个省（区、市）的工业企业，地方工业和信息化主管部门从工控系统构成、安全软件选择与管理、配置与补丁管理、边界安全防护等方面，指导工业企业开展体系化工控安全自查。抽查范围包括化工、冶金、汽车制造、烟草等典型行业的代表性工业企业，参照《防护指南》要求逐项检查其信息安全管理情况以及防护手段部署落实情况，并指导企业进行整改加固。发现的主要问题包括部分工业企业安全意识仍显不足、工控安全管理机制缺失、工控安全防护能力薄弱等。

这次年度工控安全检查工作有力地推动了《防护指南》实施，进一步摸清了贯彻落实情况，基本掌握我国工控安全现状，通过有效排查和梳理工控安全风险点，指导工业企业有针对性地部署安全防护措施等工作。

与此同时，从今年 4 月起，工业和信息化部组织技术机构面向电力、化工、装备制造、石油、有色、烟草等关系国

计民生、国家安全的重点行业，遴选具有代表性的典型企业，开展了工控安全防护能力评估工作，指导帮助工业企业深入理解《防护指南》要求，了解评估要点，明确防护工作切入点，指导企业开展针对性防护整改工作，从技术、管理、运行等方面全面提升工业信息安全防护水平。

（四）工业信息安全保障能力全面提升

一是组建国家队伍，提供专业人才支撑。2017 年，按照《国务院关于深化制造业与互联网融合发展的指导意见》文件要求，工业和信息化部依托部属单位电子一所重组建设了“国家工业信息安全发展研究中心”(以下简称“国家工信安全中心”),作为支撑我国工业领域信息安全的研究与推进机构，开展工业信息安全及相关领域的战略研究、技术研发、监测预警、检查评估、应急处置和产业推进等工作，提升工业信息安全保障支撑能力，维护工业信息安全。

二是加强监测预警，搭建技术支撑平台。工业和信息化部依托国家工信安全中心等技术机构，建设了重要工控系统在线安全监测平台、国家工控系统安全信息共享平台。搭建智能制造仿真测试平台以及可编程逻辑控制器（PLC）、分布式控制系统(DCS)、工控系统通信总线等安全仿真测试平台。组建了国家工控系统与产品安全质量监督检验中心，全面提升了漏洞发现及验证、风险监测与研判、安全防护解决方案验证等安全保障能力，为开展工业信息安全监测预警、信息

通报、质检评估等工作的提供有力技术支撑。

三是深化应急管理，提升应急响应能力。2017 年 5 月，工业和信息化部印发《工控系统信息安全事件应急管理工作指南》(简称《应急指南》), 结合工控安全事件应急工作实际，以防范重大工控安全事件为重点，厘清工业和信息化部、地方工业和信息化主管部门、技术支撑队伍和企业职责，为加强工控安全事件应急管理和组织协调，提升工控安全事件应急处置能力提供了工作指引。2017 年 9 月，工业和信息化部组织开展工控安全事件应急演练及培训，以特定工控安全事件为背景，针对工业企业快速响应、政府机构应急联动、技术支撑队伍现场应急处置等工作开展演练，达到检验《应急指南》、理顺流程、锻炼队伍的效果，同时通过应急培训活动，有力地指导了地方工信主管部门统筹加强应急预案体系、组织体系、技术手段、应急演练、资源保障等方面工作。

四是推进信息通报，建立联防联控网络。为及时掌握工业信息安全风险、威胁信息，2017 年 5 月，工业和信息化部印发了《关于开展工业信息安全信息报送与通报工作的通知》（工信软函〔2017〕517 号）并组织开展工业信息安全信息报送与通报试点工作，推动行业联防联控，初步建立覆盖 9 个省（市）工信主管部门及 36 个企业、科研院所、行业协会的工控安全风险信息报送网络。半年来，汇集工控安全风险信息 2000 多条，向国家有关部委、中央企业、各省（区、市）

通报重要风险预警100余份，有效地提高了相关部门、企业主动应对和处置安全风险的能力。

（五）工业信息安全宣传教育不断深入

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》文件要求，推动《工业控制系统信息安全防护指南》落地实施，提升地方工业和信息化主管部门及企业工业控制系统信息安全防护水平，在工业和信息化部指导下，2017 年全国工业信息安全宣贯培训、技能竞赛、论坛会议等宣传教育活动深入开展。

一是首次开展全国范围内的工控系统信息安全培训工作。今年 3 月- 6 月，工业和信息化部信息化和软件服务业司委托国家工信安全中心，分别面向华东、华南、华北、西南、西北、东北等六大片区组织开展了2017年工控系统信息安全培训工作，来自全国 31 个省区市、240 余个地市工信主管部门及350 余家工控系统用户企业的1200 余名领导同志和从业人员参加了培训。此次培训通过详细解读《工业控制系统信息安全防护指南》，普及工控系统信息安全相关知识，讲解工业控制系统信息安全防护技术，进一步强化了地方工业和信息化主管部门及企业工业信息安全意识，提升了工控系统信息安全相关技能，使得工业信息安全的理念更加深入人心。

二是工业信息安全教材编制工作取得实质性进展。由国

家工信安全中心牵头编制了《工业控制系统信息安全防护技术概论》(简称《技术概论》),作为全国工控系统信息安全培训的指定教材。《技术概论》详细介绍了我国关于工业信息安全的指导原则、方针政策和工作部署，特别强调工业企业在工控安全防护工作中的主体责任，有针对性地普及了工控安全相关基础知识，并围绕《防护指南》提出的十一项防护要求，提出可供工业企业参考的防护策略、实施建议和解决方案，为推动工业信息安全意识普及和知识技能教育发挥了积极作用。

三是工业信息安全技能竞赛、论坛会议等活动如火如荼开展。为提升社会工业信息安全意识、加大工业信息安全专业人才选拔与培养力度，2017 年 12 月，在工业信息化部指导下，由国家工业信息安全发展研究中心与浙江省经济和信息化委员会联合举办的首届工业信息安全技能大赛在浙江杭州拉开序幕，大赛模拟真实工业控制网络系统，聚焦行业安全问题，召集来自全国 24 个省（区、市）科研院所、著名高校和知名企业的 49 支战队的近 200 名选手，针对行业实际应用设备进行漏洞挖掘，并开展工业信息安全攻防实战。本次大赛是落实《网络安全法》的重要举措，在普及工业信息安全常识、培养工业信息安全人才、推动行业整体安全意识提升、促进安全防护技能提高等方面开展了积极探索。此外，国家网络安全宣传周、世界智能制造大会等活动纷纷设

置工业信息安全相关分论坛，通过工业信息安全宣传教育与意识普及，强化提升全社会工业信息安全意识。

（六）工业信息安全产业发展起势蓄能

近年来我国工业信息安全市场呈现出良好的发展势头，具体表现为:

一是我国工业信息安全企业从“布局市场”逐渐转向“深耕市场”。近年来我国工业信息安全产业领域资本战略布局方向呈现更加清晰、更有针对性的特点和趋势。在近年来的资本布局的基础上，工业信息安全主流厂商中，半数已经完成资本并购和资本洽谈。资本的引进，加速了工业信息安全厂商的发展，同时也对工控系统信息安全市场发展起到重要的促进作用。工业信息安全产业渠道布局、业务模式更加多样化，这已成为目前我国工业信息安全市场良性发展的一个突出特点，为我国工业信息安全市场的健康发展注入了生机和活力。例如，工控设备厂商/集成商、MES 厂商、设计院与用户逐渐成为紧密联系的合作对象，而在此之前，我国工业信息安全产业研发、生产和用户相互分离，工业信息安全企业对工控设备厂商/集成商的依赖性较高，限制了工业信息安全企业的产品研发和市场拓展。

二是智能化趋势有力推动和牵引工业信息安全产业发展。工业信息安全需要专门的安全产品、技术和服务，以往由于工业信息安全市场规模较小，大量的工控系统供应商

（如 ABB、霍尼韦尔、罗克韦尔、西门子、施耐德、和利时、中控、横河电机等）很少研发独立的工业信息安全产品，一般通过控制系统集成安全功能或者通过安全模块实现通信区域隔离，再配套第三方的信息安全软件来实现安全保障。随着智能制造的逐步实施，控制系统内部的信息安全防护也越来越多的被关注。智能制造为工业信息安全企业和工控系统供应商研发和创新独立的工业信息安全产品提出了市场需求，开拓了产业发展的新机遇。

三是产业联盟为工业信息安全产业跨界资源整合发挥桥梁纽带作用。为促进产业发展，形成工业信息安全“产、学、研、用”的良好生态，2017 年 6 月 8 日，在工业和信息化部的指导下，国家工信安全中心牵头发起成立了国家工业信息安全产业发展联盟，联盟首批会员单位达 187 家，聚集了工业领域的领军企业，工控系统和信息安全领域的“佼佼者”，以及科研实力雄厚的研究院所和高等院校，实现了工业信息安全领域的强强联合，合力构建科学的工业信息安全产业生态体系。

三、未来我国工业信息安全面临的主要挑战

（一）工控系统日益成为黑客攻击和网络战的重要目标

从工控系统的地位看，工控系统是我国工业生产的“神经中枢”，是电力系统、钢铁石化、轨道交通、先进制造、国防

军工、市政水务以及核设施等重点领域关键信息基础设施的核心组成，工控安全直接关系到人民生命财产安全、社会稳定甚至国家安全。

工控系统的极端重要性决定了其极易成为互联网攻击和网络战的重要目标，面临严重的安全挑战。一方面，从工控系统自身结构看，由于采用专用的通信协议、操作系统和软硬件设置，且缺乏相应的安全防御措施，系统固有的漏洞容易被攻击者利用以进行破坏性的操作。从外部网络环境看，在“互联网+”、“工业 4.0”等政策的驱动下，工控系统与传统 IT 环境的物理隔离逐渐被打破，攻击者能够使用传统的 IT 系统攻击方法深入到工控系统网络，从而发起攻击。

当前大国间军事对抗日益升级，恐怖主义活动和社会不稳定因素不断增加，未来工控系统将进一步成为国家间网络对抗的重要目标，以及黑客组织实施攻击破坏的重点对象，防护压力空前增大。据网络安全公司卡巴斯基实验室最新报告，仅 2017 年上半年就发现约 18000 种针对工控系统的恶意软件。伊朗震网病毒、乌克兰电网事件、俄罗斯输气管道爆炸、德国钢厂事故等一系列信息安全事件表明，工控系统正面临越来越多的复杂攻击，如何增强工控系统安全性，抵御内外部攻击已经成为了世界各国关注的焦点问题。

（二）大批网络武器泄露显著降低工业领域的攻击门槛

2017 年，美国中央情报局（CIA）、国家安全局（NSA）

的网络武器资料泄露，“WannaCry”和“永恒之石”（“EternalRocks”）等网络安全事件，都是不法分子利用这些泄露的网络武器工具发起的攻击。这些网络武器的攻击对象包括微软、安卓、苹果 iOS、OS X 和 Linux 等多种通用操作系统，以及车载智能系统和路由器等网络节点单元和智能设备，由于工业生产领域同样大量使用标准 IT 产品，使得不法分子可以利用这些网络武器入侵工控领域并发起网络攻击，加剧工控系统遭受恶意攻击的威胁。

一是维基解密持续公开美 CIA 文件。美国当地时间 3 月 7 日，维基解密以“穹顶 7”（Vault7）为代号，分批公开了 CIA 大规模实施网络攻击和间谍活动的秘密文件。维基解密称，此次公开的文件是相关系列文件的第一部分，名为“Year Zero”（元年）。“元年”文件共有 8761 份秘密文件，包括 7818 个网页和 943 份附件。通过研究这些曝光资料发现，美已经建立网络攻击武器库和战略资源库，具备了针对各类操作系统、智能设备等全方位、多层次的攻击能力，可发起国家级、有组织的网络攻击行动。美利用这些网络武器可持续针对全球开展大范围网络监听与攻击活动，其目标十分广泛，不仅涵盖 Windows、OS X、Linux 等主流操作系统，还包括手机、车载系统及智能电视等众多智能终端设备。

二是 NSA 网络武器工具泄露。4 月，与 NSA 存在关联的黑客组织影子经纪人（Shadow Brokers）泄露出一份震惊世

界的机密文档，其中包含了多个 Windows 远程漏洞利用工具，可以影响当前全球 70% 的 Windows 服务器。此次泄露的工具包括 23 个新的黑客工具，其中，有针对互联网信息服务（IIS）6.0、服务器信息块（SMB）、远程桌面协议（RDP）服务等的远程漏洞利用工具。大量 Windows 版本及 IBM Lotus Notes、Mdaemon、EPICHERO Avaya Call Server 和 Imail 等产品面临漏洞威胁。另外，“影子经纪人”从 2017 年 6 月开始，每月都会出售包括浏览器、路由器、手机的漏洞及相关工具，以及 SWIFT 供应商和央行入侵等数据。曝光的网络工具通过暗网等渠道进行非法交易和大量扩散，使得犯罪分子可轻易获取攻击工具，发起高强度网络攻击门槛大大降低。

（三）针对工业领域的勒索软件、定向攻击将愈发普遍

针对工控系统的勒索攻击、定向攻击等新型攻击模式逐渐成熟。一方面，传统勒索软件已对能源、交通等领域的工控系统造成了影响；另一方面，出现了定向攻击工控系统的新型恶意软件，如直击电网工控设备的网络攻击武器“Industroyer”，以及专门针对工控领域的勒索软件“必加”（Petrwrap），对工业信息安全造成极大威胁。

一是勒索软件持续呈现高发态势，重点工业领域将面临更多勒索软件威胁。勒索软件通过加密数据、操作劫持等方式，使得用户设备、数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。在匿名网络“暗网”和虚拟货币

“比特币”的加持下，相关地下黑色产业链逐渐成熟，使得勒索软件极易获取传递且复制成本低廉，我国勒索软件家族数量也从 2015 年的 30 多个暴涨至 140 多个，不法分子在商业利益驱使下，将勒索软件与最新网络武器相结合，对全球进行大范围、无差别的攻击，具备更大杀伤力。今年以来，勒索软件有进一步蔓延至工业领域的趋势。据赛门铁克数据显示，全球范围内制造业已经成为遭受勒索软件攻击最多的行业领域之一，数量占比高达 17%；去年 11 月旧金山市政地铁系统爆发勒索软件感染事件，是勒索软件深入渗透至公共基础设施控制层的全球第一例。制造、能源、市政、交通等重点工业领域密切关系到工业生产安全和社会正常运转，关键业务数据具备极高价值，一旦遭受攻击破坏影响恶劣，将日益成为勒索软件的重点攻击目标。

二是针对工业企业的定向攻击行为增多，主要集中于制造业、建筑业、交通运输业及工程行业。据卡巴斯基实验室发布的《2017 上半年工业自动化系统威胁全景》报告称，攻击者开始将注意力逐渐转移到工业控制网络，针对工业企业有目的的定向性攻击数量越来越多，如黑客可利用掌握的 0-day 漏洞开发出用于特定用途的恶意程序，透过用户常用的访问站点实施水坑式攻击，成功感染企业网终端，并借助 USB 传输、本地资源下载、远程访问等方式最终渗透至相对隔离的工控网络。从行业分布来看，受到攻击的工业企业多

集中在制造、建筑、交通运输及工程等行业，且大部分为工业设施及自动化系统的设计制造商，其中针对制造企业的攻击行为数量最多，占比高达 65%。

（四）工业互联网的应用普及给工控安全带来更大挑战

工业互联网是在制造业发展面临深刻变革这一背景下提出的，是我国扭转发展失衡局面、重构竞争优势、抢占产业制高点的重要机遇，意义十分重大。随着国务院印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，我国工业互联网发展面临难得的战略窗口期，同时也给保障工控安全带来更为严峻的挑战。

一方面，网络空间对抗博弈加剧，工业领域信息基础设施成为重点攻击目标，防护压力空前增大。另一方面，相较传统网络安全，工业互联网安全呈现新的特点，较传统网络安全进一步增加了安全防护难度。**一是互联互通导致攻击路径增多。**工业互联网实现了全系统、全产业链和全生命周期的互联互通，使传统互联网安全威胁延伸至工业生产领域，且攻击者从研发端、管理端、消费端、生产端都有可能实现对工业互联网的攻击。**二是开放化、标准化导致易攻难守。**工业互联网系统与设备供应商越来越多的使用公开协议以及标准化的 Windows 或 Unix 操作系统技术架构。这些协议与模块操作系统的安全漏洞使攻击者的攻击门槛大为降低。**三是现有安全产品和技术措施相对滞后于工业互联网发展**

普及的步伐。工业互联网架构中通信和计算资源往往有限，很多传统安全防护设备由于占用资源较大，可能不再适用，由于产业技术支撑能力严重不足，尚未出现。**四是海量设备集成和数据流动带来新的信息安全挑战。**工业互联网集成海量设备系统，导致更多安全漏洞产生，工业数据量爆炸性增加，互联互通使得工业生产网络的攻击泄密事件的数量飙升，所造成的影响也变得更为重大。

（五）工业数据作为企业核心资源面临严峻的安全风险

工业数据囊括了从客户需求到销售、订单、计划、研发、设计、工艺、制造等整个产品全生命周期的各类数据，这些数据具有的价值巨大，特别是研发、设计、工艺等数据还可能涉及知识产权，关系企业经营和生产安全，甚至关乎国家安全。当前，我国工业数据的安全防护能力较为薄弱，安全环境比较严峻：一是工业数据安全顶层设计不足。工业数据安全监管相关的政策制度、标准规范等都还不够完善，开展工作缺乏政策支持，实施防护没有专门的标准指南参考。二是工业数据安全主体责任不明。在工业数据的共享、交换、流通过程中，会出现数据拥有者与管理者不同、数据所有权和使用权分离的情况，从而带来数据滥用、权属不明确、安全主体责任不清晰等安全风险，将严重损害数据所有者的权益。三是工业数据安全技术保障能力有待提升。调研发现，当前我国工业大数据还处于推广和发展阶段，安全保障没有

跟上，没有做到“三同步”，已有的安全措施以传统安全防护手段为主，专门的工业数据安全技术手段较为缺乏。因此，加强工业数据保护，提高工业数据抵御黑客攻击窃密的能力，将是日后工业信息安全工作的重要课题。

四、下一步工业信息安全工作的建议

当前，我国工业信息安全政策体系初步形成，工作体系框架基本确立，技术支撑力量明显增强，保障体系建设有效推进，综合防范能力显著提升。与此同时，随着国务院《关于深化“互联网+先进制造业”发展工业互联网的指导意见》的出台，我国工业信息安全事业面临新的发展机遇，也将面临着更为复杂多变的挑战，下一步须在继续推进工控安全保障工作基础上，大力开展工业互联网安全建设。迫切需要政产学研各界通力协作、共同应对，从政策制度、标准体系、技术产品研发、产业发展、人才培养等方面着力，加快构建全方位工业信息安全保障体系。

（一）加强政策引导

进一步强化工业信息安全顶层设计，体系化推进政策布局。研究编制工业信息安全产业的指导性文件，为构建工业信息安全技术体系、突破关键核心产品、培育骨干企业、优化产业生态环境提供有力指引，促进我国工业信息安全产业快速发展。加强工业互联网安全、工业云安全、工业大数据

安全等新兴领域的政策制定，从顶层设计、安全要求、产业发展等方面，建立新兴领域安全管理政策体系，规范和指导新技术新应用实现安全发展。加强政策宣贯，强化工业企业安全主体责任，提升工业企业安全防护意识。

（二）健全标准体系

加强工业信息安全标准顶层设计和统筹协调，从技术、管理、测评等角度建立科学合理的工业信息安全标准体系框架。研究制定工业互联网设备、平台、控制、数据等层面的安全防护、测试、评估规范。加快制定工控安全防护能力评价方法、工控设备产品级安全测试方法、工业互联网平台系统安全要求等急需标准研制，搭建重点标准的综合测试验证平台，开展相关标准试点工作。利用 ISO/IEC JTC1/SC27 等国际标准化交流平台，推进我国自主知识产权工控安全标准成为国际标准，实质性参与工控安全国际标准化工作，提升我国影响力。充分发挥国家工业信息安全产业发展联盟等行业组织的作用，加强国家标准宣贯，建立行业标准体系，编制产品推荐目录，推广通用安全框架及解决方案。

（三）推动技术产品研发

建立以企业为主导的产学研用联合创新机制，瞄准工业信息安全基础技术、共性关键技术和前沿技术，以及重点工业行业信息安全系统解决方案和核心环节。研究制定新一代

信息技术在工业领域应用的安全架构，着力构建安全可控的工业信息安全产品、技术体系，尽快突破一批工业信息安全关键核心技术。加强协同攻关，以点带面，消除瓶颈，补齐短板，整体推进，重点发展一批高端产品，形成具有市场竞争力的产品体系。积极推动核心技术成果转化和交易，加强知识产权保护和管理，促进创新成果转化，不断提升创新链、产业链、价值链整合能力。

（四）优化产业生态环境

发挥政府管理部门、行业协会的引导与支持作用，发挥产业联盟作用，拓宽企业在技术引进、投资融资、人才引进等方面的渠道。加快落实法律法规、政策标准等对工业企业信息安全的有关要求，挖掘工业企业用户信息安全需求，激发工业信息安全市场活力。统筹基础研究、技术创新、产业发展与应用部署，加强产业链各环节协调互动，增强上游技术研发与下游推广应用的协同互动效应，打造协同发展的产业生态系统。

（五）加快专业人才培养

适应互联网与制造业深度融合趋势，加快培养既掌握工业控制知识又熟悉安全防护技术的复合型人才。加强工业互联网安全相关学科建设，鼓励工业企业加强与院校合作，联合培养工业信息安全专业人才，促进工业信息安全领域产业链、岗位链、教学链有机结合。广揽国内外人才，壮大人才

队伍，提高工业信息安全领域专业人才水平，培养一支门类齐全、技术精湛的工业信息安全专业人才队伍。发挥国家工业信息安全产业发展联盟的资源优势，打造国家级工业信息安全高端智库，为工业信息安全战略部署、规划制定、决策咨询、重大问题提供智力支持和技术支撑。