

工业互联网安全风险态势报告（2018）

工业控制系统安全国家地方联合工程实验室

2019.3

主要观点

- ✧ 暴露在外的攻击面越来越大，工业互联网安全将迎来更高的挑战。中国暴露在互联网上的工控系统联网设备达到 6223 个，排名全球第五。
- ✧ 工业互联网安全漏洞数量快速增长，类型多样化特性明显，高危漏洞占比较高，安全形式日益严峻。
- ✧ 工控漏洞技术类型多达 30 种以上，无论攻击者利用何种漏洞造成生产厂区的异常运行，均会影响工控系统组件及设备的灵敏性和可靠性，造成严重的安全问题。
- ✧ 建立工业互联网安全战略推进时间表，推进实现近期、中期、远期的工作目标；
近期：安全意识培训、资产识别、工业主机（端点）防护；
中期：建立共同的 IT/OT 安全运营模式、做好网络安全控制和实时监测、提高 OT 流程的成熟度；
远期：对工控系统进行定期渗透测试、漏洞扫描、部署新的 OT 安全工具和技术、持续评估 IT/OT 一体化带来的安全风险。

摘要

- ✧ 全球工控系统联网组件总数量为 175632 个，主要集中在美洲和欧洲国家，中国联网组件总数量为 6223 个，超出意大利 365 个，排名全球第五；
- ✧ 在所有的工控系统组件中，工控设备的暴露是最为危险的。工控设备的暴露意味着攻击者有可能直接对设备本身发动攻击；
- ✧ 工业互联网安全漏洞数量快速增长，安全形式日益严峻；
- ✧ 类型多样化特性明显，且高危漏洞占比较高；
- ✧ 漏洞涉及行业广泛，以制造业、能源行业为主；
- ✧ 漏洞涉及厂商以国际厂商为主；
- ✧ 很多工业企业的信息中心管理 OT 网络和服务器的连接性和安全性，但往往对于 OT 网络上的生产设备与控制系统的连接性没有管辖权限，安全责任模糊；
- ✧ 较多工业企业的 IT 和 OT 网络并没有进行有效的隔离；部分工业企业虽然进行了分隔，并设置了访问策略，但总有员工为方便，私自设置各类双网卡机器，应加强安全意识培训；
- ✧ 建立工业互联网安全战略推进时间表，推进实现近期、中期、远期的工作目标。

目 录

研究背景	1
第一章 工控系统互联网暴露情况	2
第二章 工业互联网安全漏洞分析	4
一、 安全漏洞数量快速增长，安全形式日益严峻	4
二、 安全漏洞类型多样化特性明显	5
三、 高危漏洞占比较高	5
四、 漏洞涉及厂商以国际厂商为主	6
五、 漏洞涉及行业广泛，以制造业、能源行业为主	6
第三章 工业互联网安全威胁	8
一、 OT 安全管理不到位	8
二、 IT 和 OT 安全责任模糊	8
三、 IT 安全控制在 OT 领域无效	8
四、 缺乏 OT 资产和漏洞的可见性	8
五、 工业主机几乎“裸奔”	8
六、 IT 和 OT 网络混杂缺防护	9
第四章 工业互联网安全推进建议	10
附录一 工业控制系统安全国家地方联合工程实验室	11

研究背景

在政策与技术的双轮驱动下，工业控制系统正在越来越多地与企业内网和互联网相连接，并与新型服务模式相结合，逐步形成了工业互联网架构。工业互联网是数字浪潮下，工业体系和互联网体系的深度融合的产物，是新一轮工业革命的关键支撑。工业互联网的发展一方面极大的促进了生产效率和服务水平的提高，另一方面也使原本封闭的系统变得越来越开放，致使系统安全风险和入侵威胁不断增加，网络安全问题日益突出。

工业互联网目前已经广泛应用于电力、交通、石油、取暖、制造业等关键信息基础设施领域，一旦发生安全事件，往往会造成巨大的损失和广泛的影响。但是，由于工业互联网环境的特殊性，传统的 IT 信息安全技术并不能完全有效的保护工业系统的安全，甚至很多常用的安全技术都不能直接应用于工业网络的安全防护。对于工业互联网安全的分析与防护，需要使用一些专门的方法和专用的技术。

工业控制系统安全国家地方联合工程实验室（以下简称“联合实验室”）于 2017 年发布《IT/OT 一体化工业信息安全态势报告》，总结分析 IT/OT 融合带来的新挑战，给出工业信息安全建议和展望。

为给政府部门、科研机构和工业企业提供参考和借鉴，工业控制系统安全国家地方联合工程实验室（以下简称联合实验室）编撰了《工业互联网安全风险态势报告（2018）》。

本报告对工业互联网安全漏洞的分析，采用了一种新型漏洞评分系统，将可见性、可控性、漏洞利用目标服役情况等体现工控安全特性的指标纳入量化评估范围。报告以联合实验室漏洞库收录的工业控制系统相关的漏洞信息为基础，综合参考 CVE、NVD、CNVD、CNNVD 四大公开漏洞平台发布的漏洞信息，分析工业互联网安全风险态势，编撰了《工业互联网安全风险态势报告（2018）》。

此外，本报告分析暴露在互联网上的工控组件和安全威胁，最后提出工业互联网安全推进建议。

《工业互联网安全风险态势报告》内容被综合收录到《IT/OT 一体化工业信息安全态势报告（2018）》年度报告中。《IT/OT 一体化工业信息安全态势报告（2018）》是续 2017 年发布《IT/OT 一体化工业信息安全态势报告（2017）》后，总结分析 2018 年工业互联网 IT/OT 融合带来的新挑战，安全现状、产业发展趋势、重大应用案例等，给出 2019 年工业信息安全建议和展望。

最后，希望本报告能够帮助读者对工业互联网安全有一个更加全面、前沿的认识。

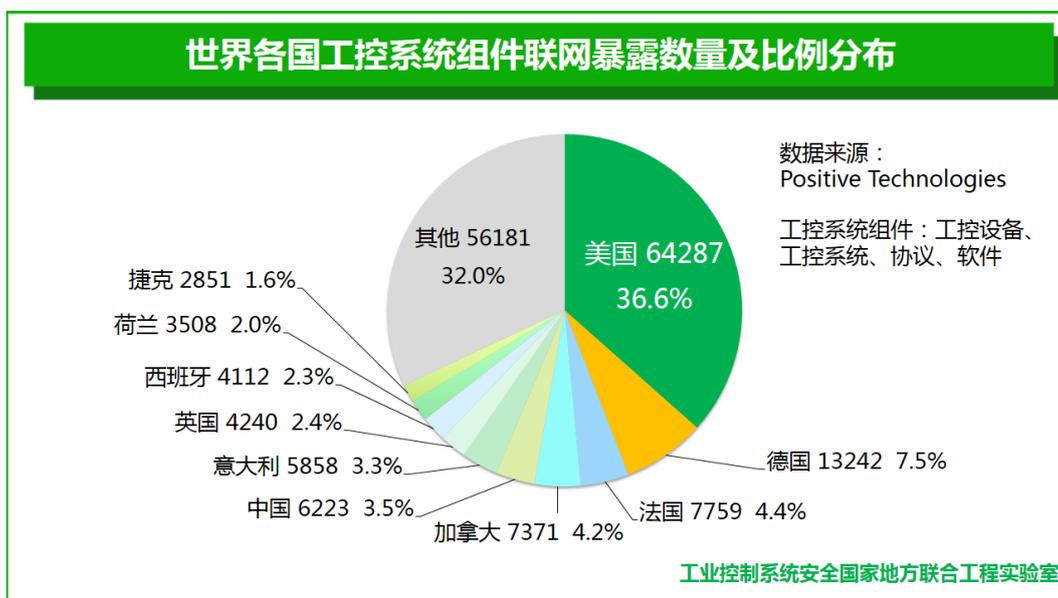
第一章 工控系统互联网暴露情况

工控系统在互联网上的暴露问题是工业互联网安全的一个基本问题。所谓“暴露，是指我们可以通过互联网直接对某些与工控系统相关的工业组件，如工控设备、协议、软件、系统等，进行远程访问或查询。

造成工控系统暴露的主要原因之一是“商业网络（IT）”与“工业网络（OT）”的不断融合。IT 与 OT 网络的连通在拓展了工业控制系统发展空间的同时，也带来了工业控制系统网络安全问题。近年来，企业为了管理与控制的一体化，实现生产和管理的高效率、高效益，普遍推进生产执行系统，实现管理信息网络与控制网络之间的数据交换，实现工业控制系统和管理信息系统的集成。如此一来，如果未能做好必要的分隔管控工作，就会导致原本封闭的 OT 系统，通过管理系统与互联网互通、互联后，面临从互联网侧传播进来的各类网络攻击风险。

工控系统的直接连接到互联网，也称为“暴露”在互联网上，这个问题要一分为二的来看待：一方面，某地区工控系统在互联网上暴露的越多，往往说明该地区工业系统的信息化程度越高，工业互联网越发达；而另一方面，因为绝大多数的工业组件其实并不需要通过互联网进行远程操作，因此，暴露的比例越大，也往往意味着工业系统在信息化的同时，没有充分的做好必要的隔离工作，系统遭遇攻击和入侵的风险也越大。

美国安全公司Positive technologies的监测数据较好的反映了全球范围内，工业组件在互联网上的暴露情况。为了收集在互联网上具有可访问性的工业控制系统站点及组件，Positive technologies采用被动方式，使用可公开访问的引擎：Google、Shodan (shodan.io)、Censys(censys.io)对全球工业系统进行了搜索。其中，Shodan 和Censys可搜索工业服务器、路由器、专用摄像头等设备的联网情况。

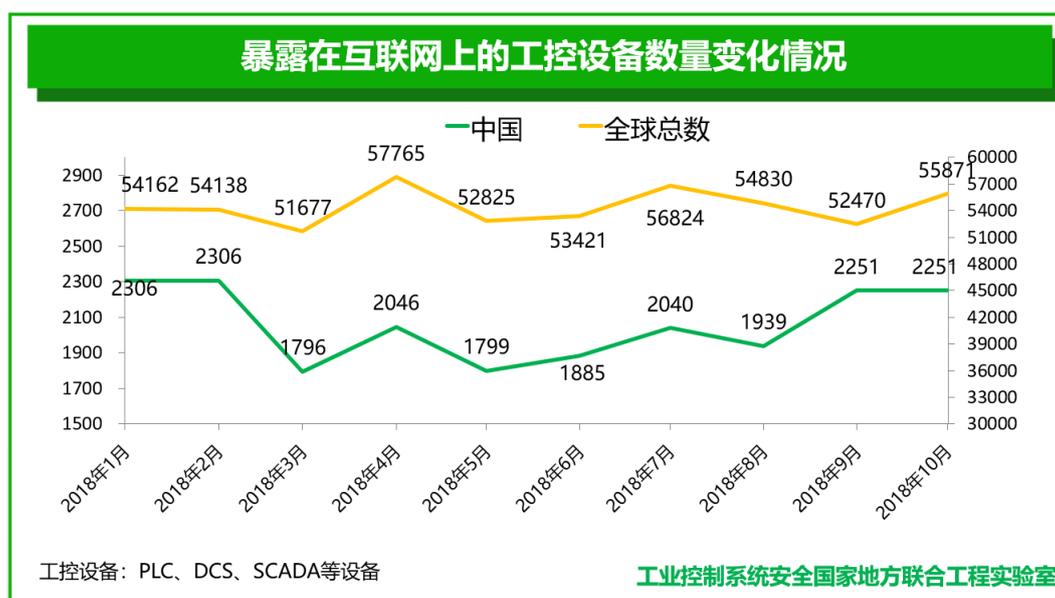


根據 Positive Technologies 2018 研究數據顯示：當前全球工控系統聯網暴露組件總數量約為 17.6 萬個。從這些工業組件的國家和地域分布來看，聯網的工控組件主要集中在美洲和歐洲國家，其中美洲占比達到 40% 以上。這也是為什麼工業互聯網安全事件多集中在歐洲和美洲等發達國家的主要原因。從具體國家來看，美國的工控系統組件聯網暴露情況最為嚴

重，达到 64287 个；其次是德国， 13242 个；法国排名第三， 7759 个。中国排名全球第五，位列加拿大之后，为 6223 个。全球各国工控系统联网组件暴露数量及分布情况如下图。

在所有的工控系统组件中，工控设备的暴露是最为危险的。工控设备的暴露意味着攻击者有可能直接对设备本身发动攻击。基于全国全球的主动探测，360 工业互联网安全大数据分析平台——哈勃平台收录了 2018 国内以及全球范围内，暴露在互联网上的工业控制系统设备数量。该平台统计的工控设备主要包括 PLC、DCS、DTU、SCADA 等设备。

统计显示，2018 年全年，中国和全球的工控设备暴露数量基本处于稳定状态，2018 年末比 2018 年初有稍微增长，在 2018 年 4 月份中国和全球的工控设备有稍微增长趋势。暴露的工控设备数量折线图如下所示。



第二章 工业互联网安全漏洞分析

安全漏洞问题是工业互联网面临的又一个顽疾。特别的，与一般的 IT 系统不同，受到生产环境的约束，很多的工业系统安全漏洞即便已知，也未必能有条件进行修复。

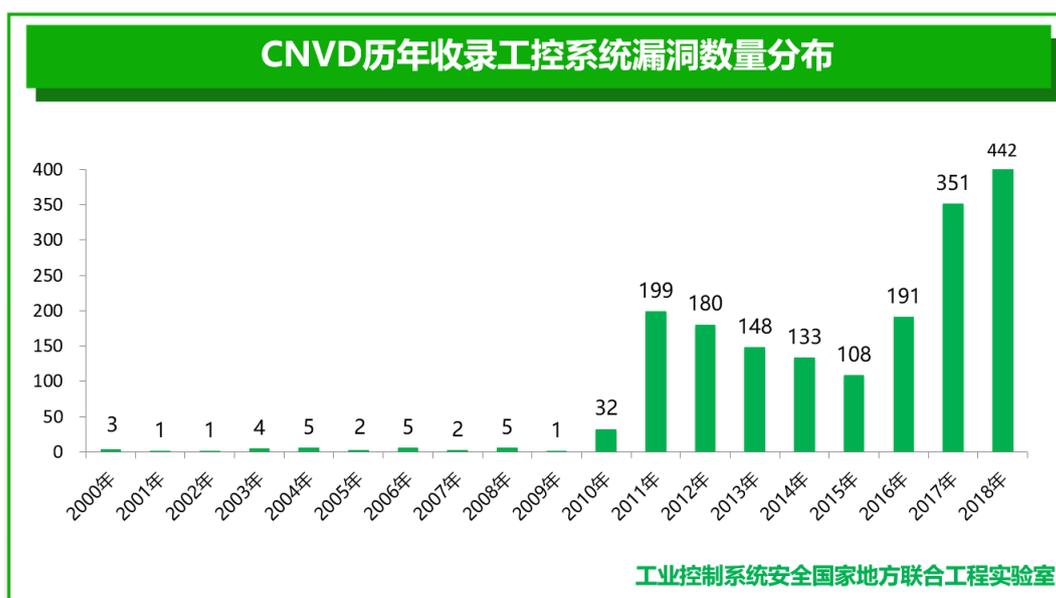
本节主要以联合实验室漏洞库收录的工业控制系统相关的漏洞信息为基础，综合参考了 Common Vulnerabilities & Exposures (CVE)、National Vulnerability Database (NVD)、中国国家信息安全漏洞共享平台 (CNVD) 及国家信息安全漏洞库 (CNNVD) 所发布的漏洞信息，从工控漏洞的年度变化趋势、等级危害、漏洞类型、漏洞涉及行业、漏洞设备类型等方面分析工业控制系统的安全威胁态势及脆弱性。

本报告中的工控漏洞风险评估方法，基于通用漏洞评分系统，将可见性、可控性、漏洞利用目标服役情况等体现工控安全特性的指标纳入量化评估范围。该方法使用改进的工控漏洞风险评估算法，既可以生成工控漏洞的基础评分、生命周期评分，也可以用于安全人员结合实际工控安全场景的具体需求以生成环境评分。

一、安全漏洞数量快速增长，安全形式日益严峻

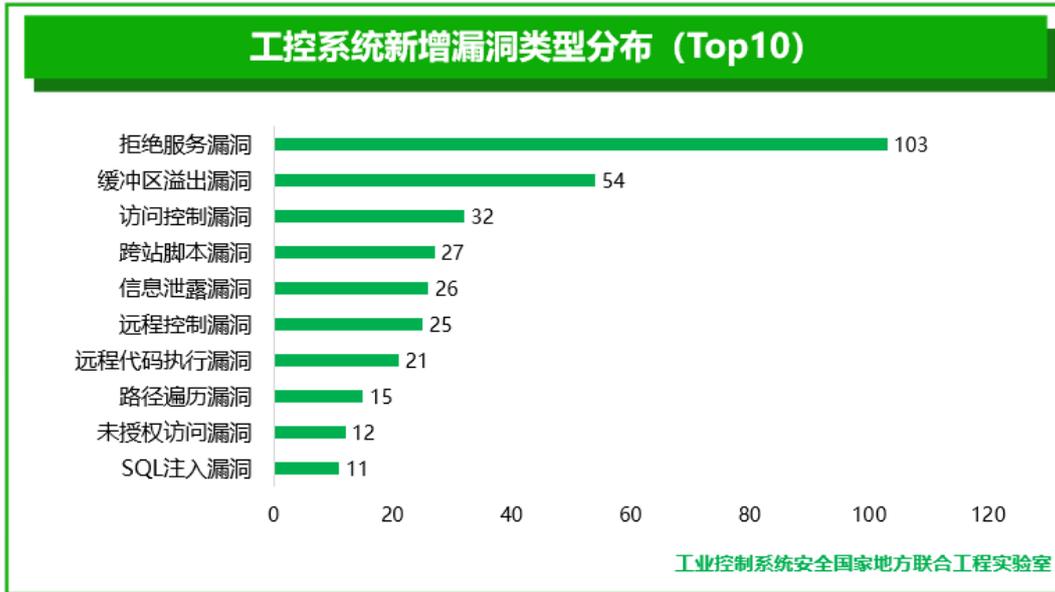
根据中国国家信息安全漏洞共享平台(CNVD)最新统计数据显示，自 2000 年-2009 年，CNVD 每年收录的工控系统漏洞数量一直保持在个位数。但到了 2010 年，该数字一下子攀升到 32 个，次年又跃升到 190 个。这和情况的发生与 2010 年发现的 Stuxnet 蠕虫病毒（震网病毒）有直接关系。Stuxnet 病毒是世界上第一个专门针对工业控制系统编写的破坏性病毒，自此业界对工业控制系统的安全性普遍关注，工业控制系统的安全漏洞数量增长迅速。

不过，从 2011 年-2015 年，CNVD 收录的工控系统漏洞数量，又呈现了一个持续的稳中有降的态势。直到 2015 年底至 2016 年初的乌克兰大停电事件之后，工控系统漏洞的发现再次进入高速增长期：2016 年 191 个；2017 年 351 个；而到了 2018 年，增长到了 442 个。



二、安全漏洞类型多样化特性明显

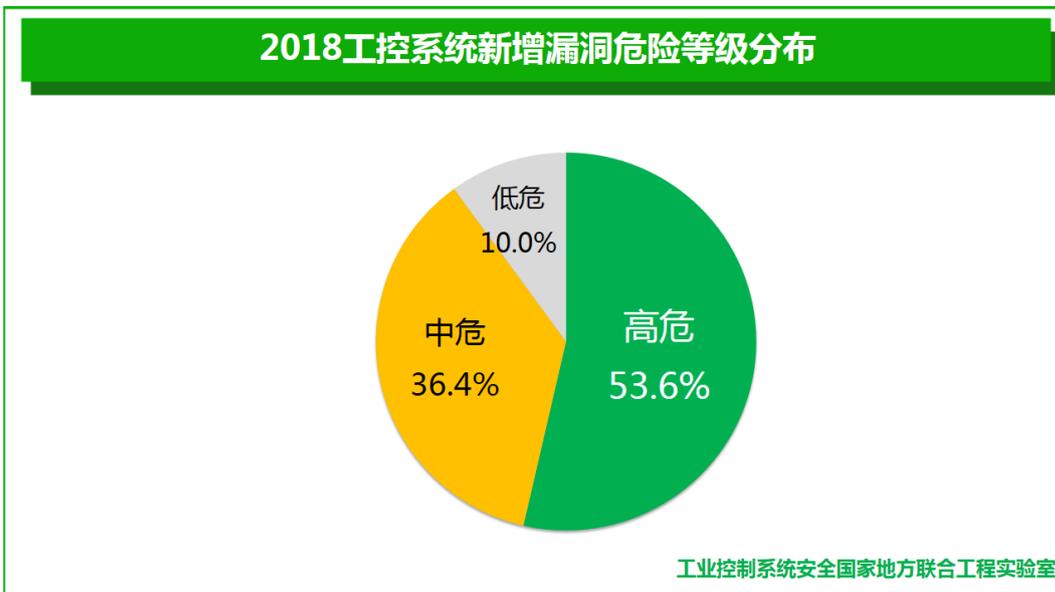
在 2018 年四大漏洞平台收录的工业控系统漏洞中，漏洞成因多样化特征明显，技术类型多达 30 种以上。其中，拒绝服务漏洞（103）、缓冲区溢出漏洞（54）和访问控制漏洞(32)数量最多，最为常见。



攻击者可以利用多样化的漏洞获取非法控制权、通过遍历的方式绕过验证机制、发送大量请求造成资源过载等安全事故。实际上，无论攻击者利用何种漏洞造成生产厂区的异常运行，均会影响工控系统组件及设备的灵敏性和可靠性，造成严重的安全问题。

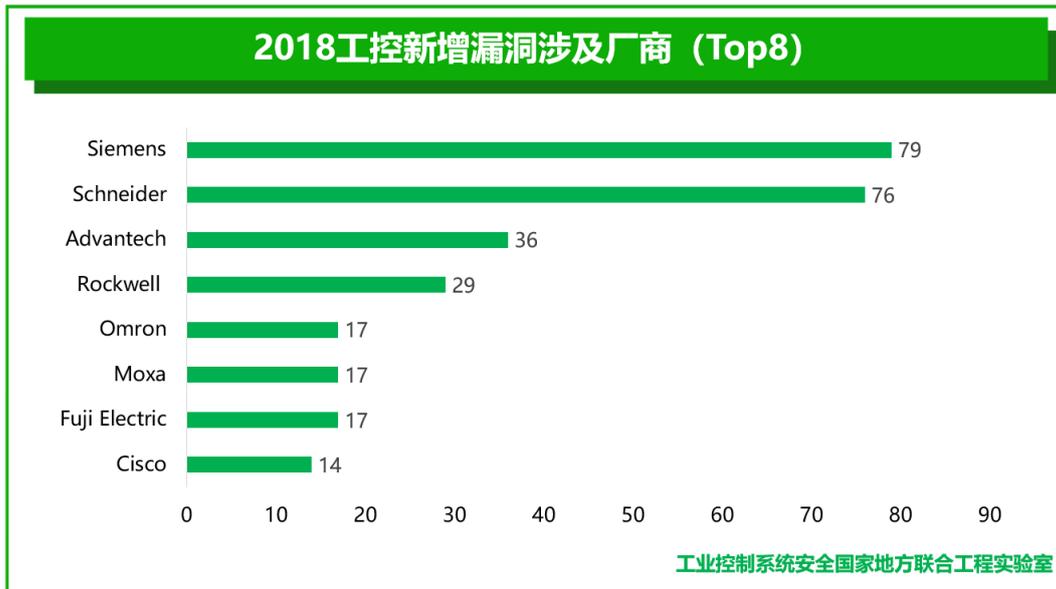
三、高危漏洞占比较高

在 2018 年四大漏洞平台收录的工业控系统漏洞中，高危漏洞占比 53.6%，中危漏洞占比为 36.4%，中高危漏洞占比达到 90%。漏洞危害等级分布如下：



四、 漏洞涉及厂商以国际厂商为主

在 2018 年四大平台新收录的工业控制系统漏洞中，涉及到的前八大工控厂商中有七个为国际厂商，一个为中国台湾厂商。这些厂商分别为西门子 (Siemens)、施耐德 (Schneider)、研华 (Advantech)、罗克韦尔 (Rockwell)、欧姆龙 (Omron)、摩莎 (Moxa)、富士电机 (Fuji Electric) 和思科 (Cisco)。漏洞涉及主要厂商情况如下图所示：

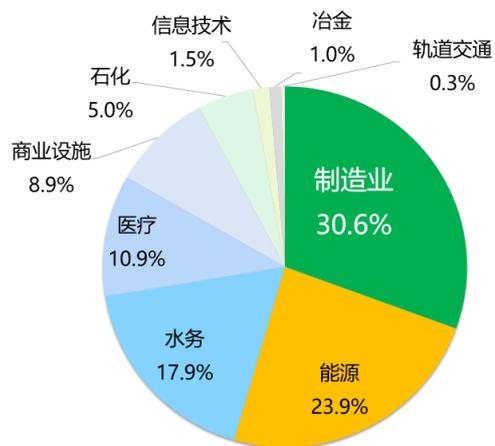


需要说明的事，虽然安全漏洞在一定程度上反映了工控系统的脆弱性，但不能仅通过被报告的厂商安全漏洞数量来片面判断比较厂商产品的安全性。因为一般来说，一个厂商的产品越是使用广泛，越会受到更多安全研究者的关注，因此被发现安全漏洞的可能性也越大。某种程度上来说，安全漏洞报告的厂商分布，更多程度上反映的是研究者的关注度。

五、 漏洞涉及行业广泛，以制造业、能源行业为主

在 2018 年四大平台新收录工业控制系统安全漏洞中，多数分布在制造业、能源、水务、医疗、食品、石化、轨道交通、冶金、市政、信息技术等关键基础设施行业。制造业占比最高，涉及的相关漏洞数量占比达到 30.6%，打破了近几年能源行业稳居第一的局面，能源行业涉及的相关洞数量为 23.9%。漏洞行业分布图如下：

工控新增漏洞行业分布



工业控制系统安全国家地方联合工程实验室

第三章 工业互联网安全威胁

联合实验室在对工业企业进行广泛、深入的研究的过程中，总结出了当前国内工业企业在工业互联网领域面临的六大主要安全威胁。

一、 OT 安全管理不到位

在很多大中型工业企业中，IT 安全管理一般措施比较到位，但 OT 安全管理措施却有显著疏失。尽管企业大小不同，但一般 IT 安全由企业的信息中心或专门团队管理。其中，制造业、石油石化、天然气，公用事业等行业的 IT 安全管理比其他行业更成熟。但一般来说，这些工业企业的安全管理和策略没有为 OT 做针对性定制，OT 网络和资产及其网络安全多年未被覆盖和管理。

二、 IT 和 OT 安全责任模糊

很多工业企业的信息中心管理 OT 网络和服务器的连接性和安全性，但往往对于 OT 网络上的生产设备与控制系统的连接性没有管辖权限；而这些设备、控制系统也是互联的，有些就是基于 IT 技术实现的，如：操作员站、工程师站等。因此，常见的 IT 威胁对 OT 系统也有影响。OT 的运维团队一般会对生产有效性负责，但往往并不对网络安全负责。对于很多工业企业来说，生产有效性通常都比网络安全性更重要。

三、 IT 安全控制在 OT 领域无效

较多工业企业在 OT 设置中使用 IT 安全控制，但没有考虑其对 OT 的影响。例如，国内某汽车企业，IT 安全团队按照 IT 安全要求主动扫描 OT 网络，结果导致汽车生产线 PLC 出现故障，引起停产。

从实践来看，较多工业企业基本不做 OT 安全评估，即使做 OT 安全评估，也是由 IT 安全服务商执行。而 IT 安全评估通常不包括 OT 网络的过程层和控制层，即使对这两层进行评估，也只能采用问卷方式而不能使用工具。执行这些评估的人员通常是 IT 安全专家，对 OT 领域也不甚了解。

四、 缺乏 OT 资产和漏洞的可见性

工业企业的 IT 团队一般不负责 OT 的资产，而是由 OT 团队负责 OT 资产。但因为生产线系统是历经多年由多个自动化集成商持续建设的，因此 OT 团队对 OT 资产的可见性十分有限，甚至没有完整的 OT 资产清单，关于 OT 资产的漏洞基本上无人负责和收集。

五、 工业主机几乎“裸奔”

工业企业的 OT 网络中存在着大量工业主机，如：操作员站、工程师站、历史数据服务器、备份服务器等。这些 PC 或服务器上运行的实时数据库、监视系统、操作编程系统等，向上对 IT 网络提供数据，向下对 OT 中的控制设备及执行器进行监视和控制，它们是连接信息世界和物理世界的“关键之门”。

但在实际系统中，这些工业主机上面基本没有任何安全防护措施，即使有一部分有防护措施，但因没有进行更新已经失效，工业主机几乎处在“裸奔”状态。近年来不断发生的各类工业安全事件中，首先遭到攻击或受影响往往都是工业主机。

六、 IT 和 OT 网络混杂缺防护

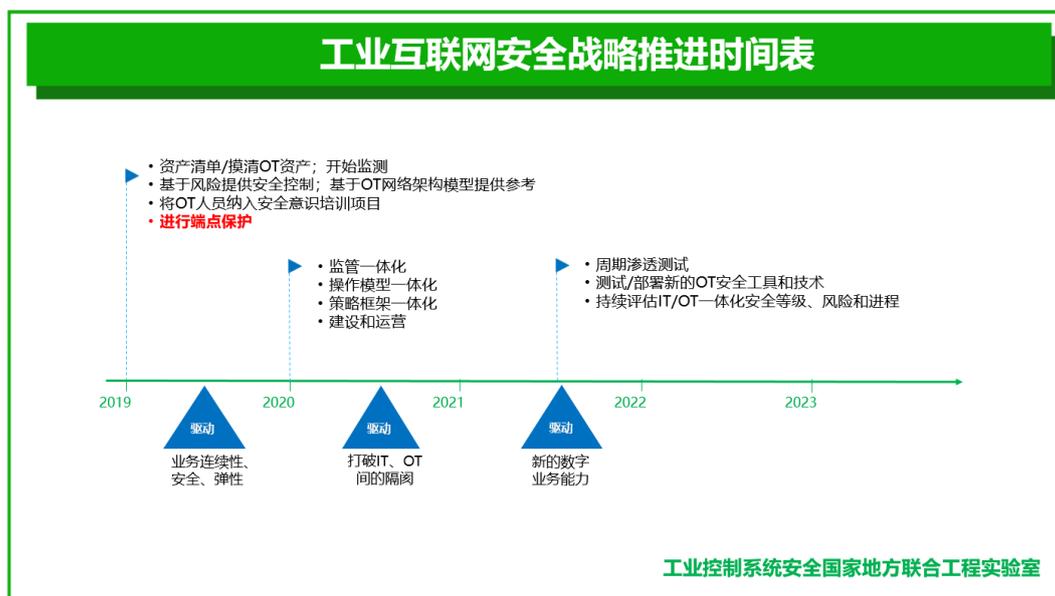
很多工业企业的 IT 和 OT 网络并没有进行有效的隔离，部分工业企业虽然进行了分隔，并设置了访问策略，但总有员工为方便，私自设置各类双网卡机器，使得 IT、OT 网络中存在许多不安全、也不被掌握的通信通道。

OT 系统往往由不同集成商在不同时间建设，使用不同的安全标准。因此，当需要集成商进行维修维护时，工作人员经常会开放远程维护端口，而且这些端口往往不采用任何安全防护措施，甚至有将常见端口打开后忘记关闭的情况发生，从而增加工业互联网的攻击剖面。

第四章 工业互联网安全推进建议

安全治理是一个长期且复杂的过程，难以一蹴而就，需要循序渐进。

结合工业互联网安全风险和威胁，总结工业互联网安全推进建议。整体来看，可以分为三个目标阶段：近期、中期、远期的工作目标。工业互联网安全战略推进时间表如下所示。



近期目标强调对团队成员的安全意识培训；同时对 OT 资产进行充分管理，包括清点、分类、跟踪记录等。OT 资产一般包括设备、过程、软件、网络资源、人员等。根据 OT 资产相对应的风险等级，制定安全应对方案，提高 OT 资产的可见性和可控性；工业主机是连接信息世界、物理世界的门户，实施工业主机（端点）防护。

中期目标是统一 IT/OT 安全治理工作正式化；建立共同的 IT/OT 安全运营模式；修订现有的安全策略框架；使用工业防火墙、流量监测实施 IT/OT 网络安全控制和实时监测；提高 OT 安全流程的成熟度。

远期目标强调对工控系统进行定期渗透测试，漏洞扫描等安全测试方式；应用新的 OT 安全工具和技术，进行概念验证、实验、测试、部署、维护；衡量和控制 OT 安全流程及其有效性；持续评估 IT/OT 安全级别；识别可能影响 OT 功能的基础设施和工控系统的潜在风险。

附录一 工业控制系统安全国家地方联合工程实验室

工业控制系统安全国家地方联合工程实验室（简称：工业安全国家联合实验室）是由国家发展与改革委员会批准授牌成立，由 360 企业安全集团承建的对外开放的工业控制安全技术方面的公共研究平台。

实验室依托 360 企业安全的安全能力和大数据优势，同时联合了公安三所、信通院、国家工业信息安全发展研究中心、中科院沈阳自动化所、东北大学等科研院所及大学。实验室以对工业控制系统安全领域有重大影响的前沿性、战略性技术作为研究目标，建立以工程实验室为主，联合高等院校、科研院所和国家需求部门、企业共同参加的，产、学、研、用相结合的合作机制，发挥高等院校、科研院所在基础理论研究方面的力量和优势，发挥国家需求部门、企业在技术创新和应用方面的主体作用，共享科研成果。

实验室积极吸纳国内外优秀的科技人才，建立高水平专业人才培养基地。目前实验室已与北京大学、西安电子科大、吉林大学、武汉大学、北京理工、信息工程大学等均建立了人才联合培养机制。

实验室拥有软件著作权 7 项，专利 16 项，创新地提出了工业互联网自适应防护架构（PC4R），推出了工业主机防护、工业防火墙/网关、工业互联网安全监测预警系统、工业安全监测等工业安全领域完整解决方案及产品，并已经在众多央企和工业企业中进行应用。未来，工业安全国家联合实验室将充分利用科技资源，发挥产学研联盟作用，打造产业链合作，与产业链企业实现互利共赢，在合作中共同壮大，努力成为工业互联网安全产业创新的龙头。