IT/OT 一体化工业信息安全态势报告（2019）

工业控制系统安全国家地方联合工程实验室

2020.3

主要观点

- ✧ 中国工控系统互联网暴露数量呈现明显增长趋势。根据 Positive Technologies 研究数据，中国暴露在互联网上的工控设备数量跃居第三。 工控设备的内生安全设计已经成为迫切任务。

- ✧ 勒索病毒仍然是工业互联网安全的最大挑战。在 2019 年工业应急响应安全事件中，病毒攻击仍然是工业企业遭受失陷的主要原因，其中，病毒多为“永恒之蓝”蠕虫变种、挖矿蠕虫。病毒攻击的主要目标是工业主机，然而工业主机基本处于裸奔状态，因此，工业企业应落实工业主机的安全防护。

- ✧ 三级协同的“工业互联网安全技术保障平台”建设将全面提升工业互联网安全保障水平。平台基于“监测-响应”的技术路线进行建设实施，有助于工业生产的长期可靠、稳定运行。

- ✧ 采购可信任第三方远程、驻场或托管式工业安全运营服务不仅可以在威胁发现、风险预测、处置响应、追踪溯源等方面大幅度提高工业企业网络安全防护能力，还可以减少人力资源投入、降低工业企业安全运营成本。

- ✧ 省级或行业级工业互联网安全技术保障平台应以服务工业用户为首要目的，为接入企业提供有价值的安全运营服务。

摘　要

- ✧ 截止到 2019 年 12 月，CNVD 收录的与工业控制系统相关的漏洞高达 2306 个，2019 年新增的工业控制系统漏洞数量达到 413 个，基本和 2018 年持平，工业控制系统漏洞数据居高不下，形式依然比较严峻。
- ✧ 漏洞成因多样化特征明显，技术类型多达 30 种以上。
- ✧ 在 CVE、NVD、CNVD、CNNVD 四大漏洞平台收录的工业控制系统漏洞中，高危漏洞占比 57.3%，中危漏洞占比为 35.5%，中高危漏洞占比高达 92.8%。
- ✧ 在收录的工业控制系统安全漏洞中，多数分布在制造业、能源、水务、商业设施、石化、医疗、交通、农业等关键基础设施行业。
- ✧ 根据 Positive Technologies 研究数据显示，当前全球工控系统联网暴露组件总数量约为 22.4 万个，同比去年增长 27%。
- ✧ 中国工控系统互联网暴露数量呈现明显增长趋势，由 6223 个增长到 16843 个，增长比例高达 2.7 倍，排名全球第三。
- ✧ 2019 年工业控制系统常见漏洞为缓冲区溢出漏洞、拒绝服务漏洞、访问控制漏洞、跨站脚本漏洞、未授权访问漏洞、远程代码执行漏洞。
- ✧ 2019 年，工业安全应急响应中心处理的工业安全事件中，勒索病毒仍然是工业互联网安全的最大挑战。

关键词：工业互联网安全漏洞；工业互联网安全威胁；安全漏洞；推进建议

目　　录

研究背景

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、2018 年已发布 《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《IT/OT 一体化工业信息安全态势报告（2019）》。本报告综合参考 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。此外，本报告分析暴露在互联网上的工控组件和安全威胁，给出应急响应典型案例，最后提出工业互联网安全推进建议。

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　　工业互联网安全现状分析

一、 工业互联网安全漏洞分析

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。

根据中国国家信息安全漏洞共享平台最新统计，截止到 2019 年 12 月，CNVD 收录的与工业控制系统相关的漏洞高达 2306 个，2019 年新增的工业控制系统漏洞数量达到 413 个，基本和 2018 年持平，工业控制系统漏洞数据居高不下，形势依然比较严峻。CNVD 工控新增漏洞年度分布如下所示：

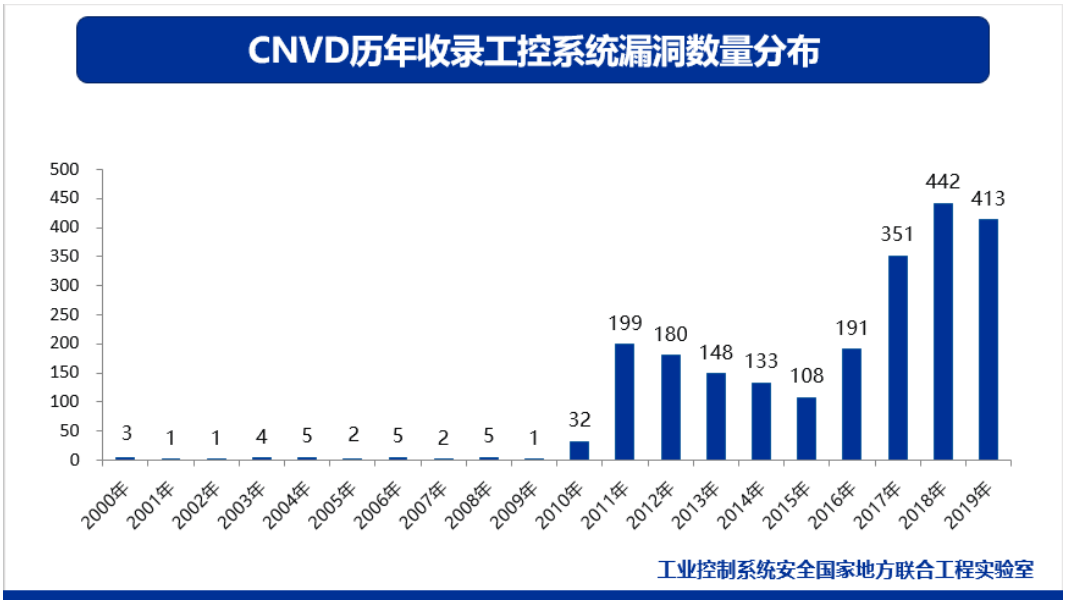

图 1: 2000-2019 年 CNVD 收录的工控系统漏数量分布图

在 2019 年，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）四大漏洞平台收录的漏洞信息共达到了 690 条漏洞，漏洞成因多样化特征明显，技术类型多达 30 种以上。其中，缓冲区溢出漏洞（105）、拒绝服务漏洞（90）和访问控制漏洞(75)数量最为常见。2019 年工控系统新增漏洞类型分布如下：

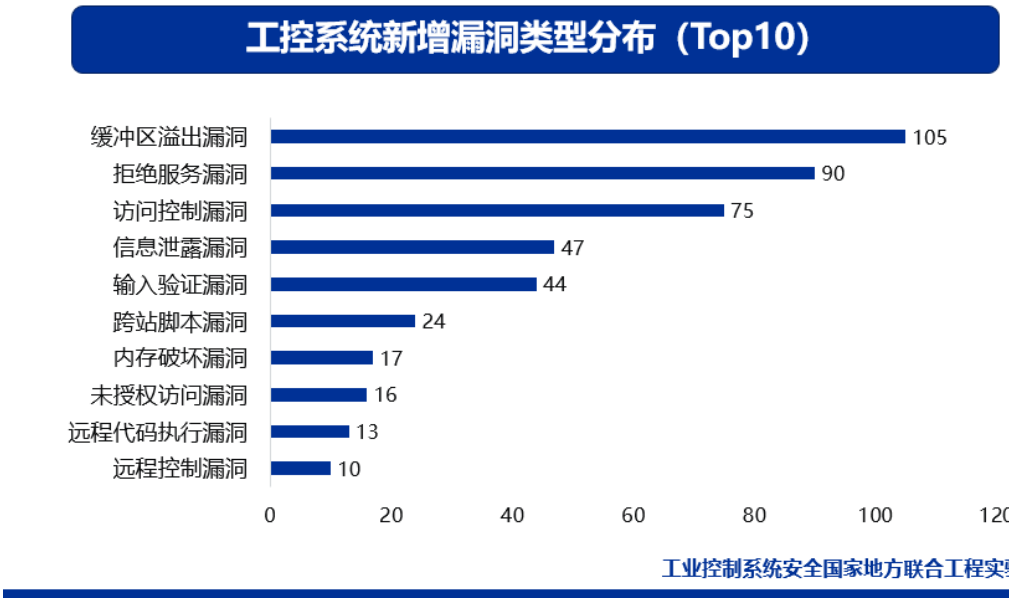

图 2: 2019 年四大漏洞库平台收录的工控系统漏洞类型分布图

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可用性和可靠性。

在四大漏洞平台收录的工业控系统漏洞中，高危漏洞占比 57.3%，中危漏洞占比为 35.5%，中高危漏洞占比高达 92.8%。在信息安全技术 标准中定义：漏洞可以容易地对目标对象造成严重后果为高危漏洞，工业控制系统又多应用于国家关键基础设施，一旦遭受网络攻击，会造成较为严重的损失。

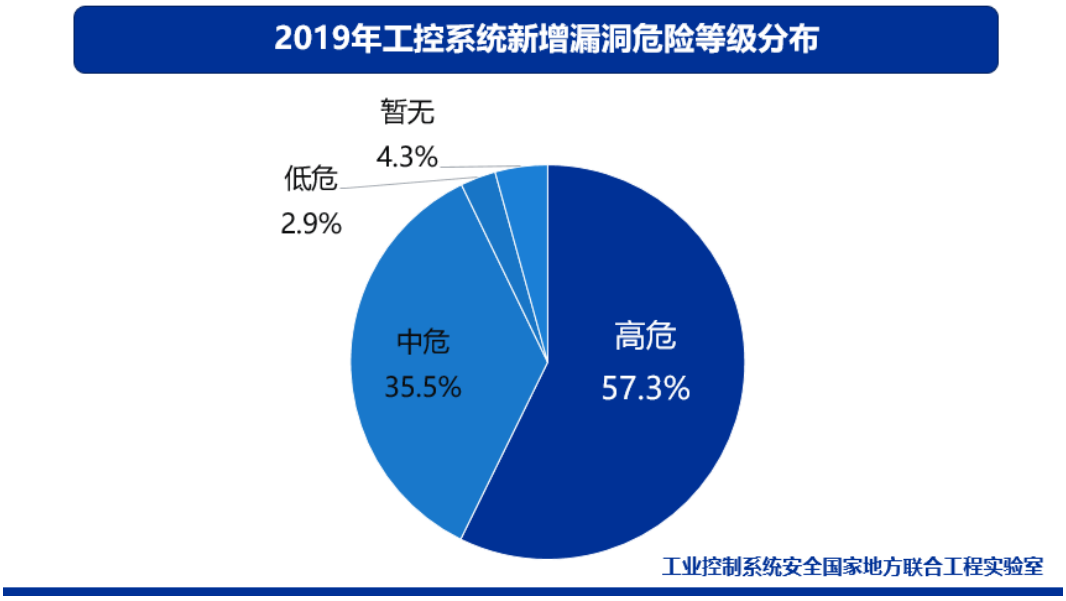

图 3: 2019 年四大漏洞库平台收录的工控系统漏洞危险等级图

在收录的工业控制系统漏洞中，涉及到的前八大工控厂商分别为西门子（Siemens）、施耐德（Schneider）、研华（Advantech）、摩莎（Moxa）、趋势科技（TRENDnet）、三菱（Mitsubishi）、欧姆龙（Omron）、和友讯（D-Link）。漏洞涉及主要厂商情况如下图所示：

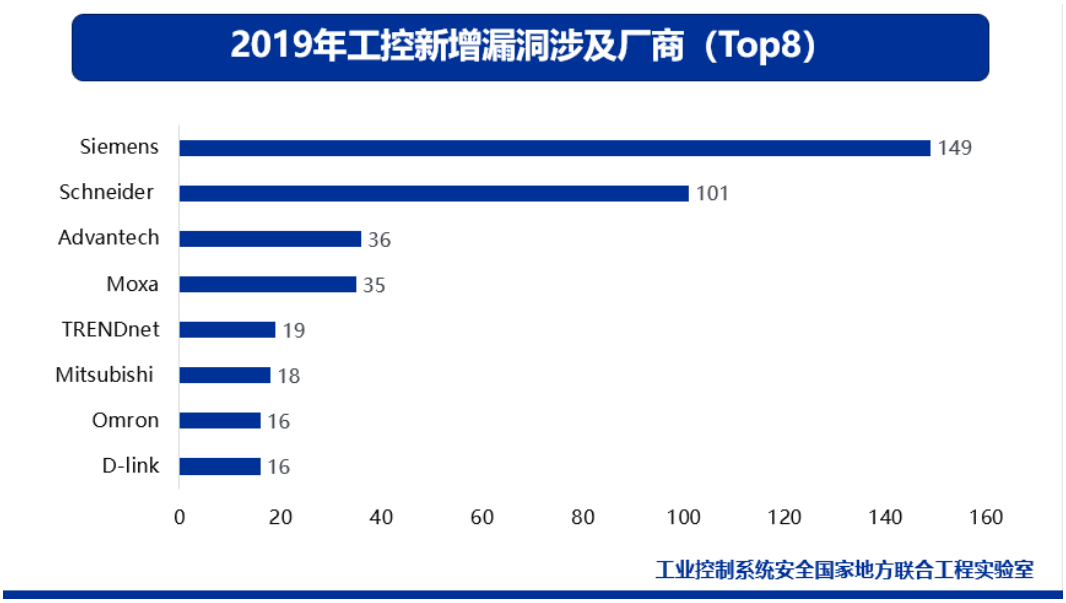

图 4: 2019 年四大漏洞库平台收录的工控设备厂商漏洞数据统计图

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。

在收录的工业控制系统安全漏洞中，多数分布在制造业、能源、水务、商业设施、石化、医疗、交通、农业、信息技术、航空等关键基础设施行业。一个漏洞可能涉及多个行业，在690 个漏洞中，有 566 个漏洞涉及到制造业，也是占比最高的行业。涉及到的能源行业漏洞数量高达 502 个。制造业和能源行业工控漏洞较多，应加强这两个行业工业安全建设。漏洞行业分布图如下：

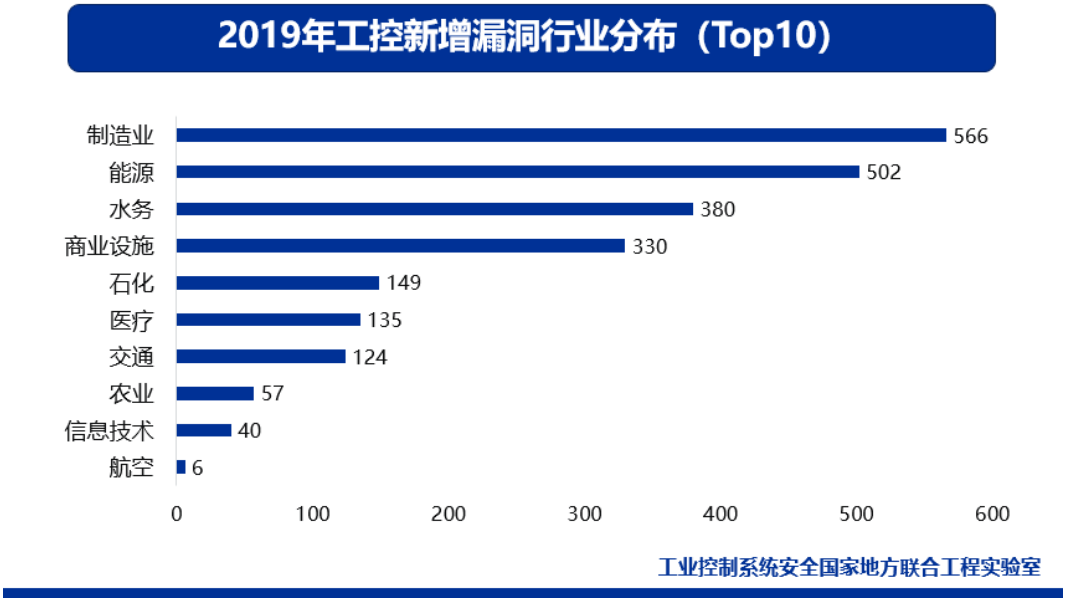

图 5: 2019 年四大漏洞库平台收录的工控漏洞涉及行业分布图

二、 工控系统互联网暴露原因

随着云计算、物联网、大数据技术的广泛应用，工控系统已渐渐从最初的封闭状态向开放状态改变，工业控制系统越来越多的采用通用硬件和通用软件，工控系统的开放性与日俱增，暴露在互联网上的工业控制系统设备越来越多，安全形式日益严峻。

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，暴露的比例越大，也往往意味着工控设备将直接面对来自互联网的威胁，在工业互联网安全建设中，工控设备的内生安全设计已经成为迫切任务。

三、 工控系统互联网暴露总数持续攀升

为了收集在互联网上具有可访问性的工业控制系统组件，美国安全公司Positive technologies采用被动方式，使用可公开访问的引擎： Shodan（shodan. io）、 Google、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。

根据 Positive Technologies 研究数据显示：当前全球工控系统联网暴露组件总数量约为 22.4 万个，同比去年增长 27%。将可通过互联网访问的工业控制系统组件（工控设备、协议、软件、工控系统等）数量按照国家进行分类，美国联网的工控设备暴露情况最为严重，达到 95661 个，其次为德国，联网工控组件达到 21449 个，相比去年而言，中国工控系统互联网暴露数量呈现明显增长趋势，由 6223 个增长到 16843 个，增长比例高达 2.7 倍，排名第三。全球各国工控系统联网组件暴露数量及分布情况如下图。

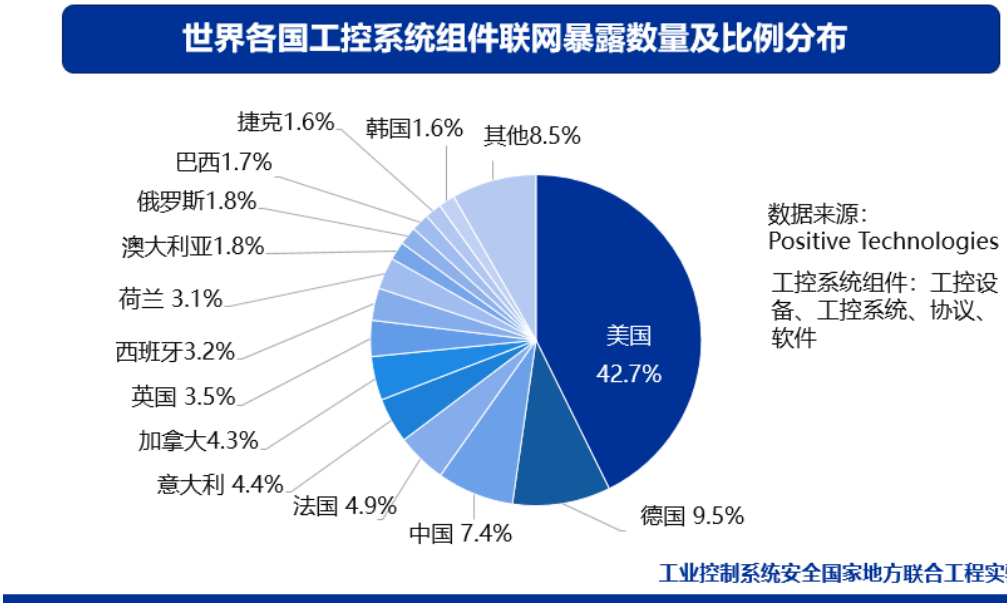

图 6: 世界各国工控系统联网组件暴露数量分布图

美国和德国联网设备在全球排名前两位，美国遥遥领先，同时也证实了美国工业突飞猛进的发展。德国联网的工控设备排名全球第二，工业发展迅速。2015 年，中国国务院颁布了印发《中国制造 2025》、《关于积极推进“互联网+”行动的指导意见》；2016 年，印发《关于深化制造业与互联网融合发展的指导意见》；推进信息化与工业化的深度融合，促进在工业互联网综合集成应用；2017 年，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》；2019 年，印发《加强工业互联网安全工作的指导意见的通知》，中国布局工业互联网，工业得到进一步发展，这也是中国工控系统组件联网暴露数量攀升到全球第三的原因。

第二章　　2019 工业互联网安全工作进展

一、 工业互联网安全重要文件

1）工业互联网综合标准化体系建设指南

2019 年 3 月，为发挥标准在工业互联网产业生态体系构建中的顶层设计和引领规范作用，推动相关产业转型升级，加快制造强国和网络强国建设步伐，工业和信息化部、国家标准化管理委员会共同组织制定《工业互联网综合标准化体系建设指南》。

该建设指南从从工业互联网产业发展实际出发， 运用综合标准化的理念和方式， 着力构建重点突出、 协调配套、 科学开放、 融合创新的工业互联网标准体系， 加快基础共性、总体性、安全、 应用等重点领域标准的制定和实施， 促进工业互联网产业持续快速健康发展。

2）网络安全漏洞管理规定（征求意见稿）

2019 年 6 月，为贯彻落实《中华人民共和国网络安全法》，加强网络安全漏洞管理，保证网络产品、服务、系统的漏洞得到及时修补，提高网络安全防护水平，工业和信息化部发布《网络安全漏洞管理规定（征求意见稿）》。中华人民共和国境内网络产品、服务提供者和网络运营者，以及开展漏洞检测、评估、收集、发布及相关竞赛等活动的组织（或个人,应当遵守本规定。

3）水利网络安全管理办法（试行）

2019 年 8 月，为确保水利信息化规划建设同步落实网络安全等级保护制度，明确运行阶段网络安全责任，强化监督检查和责任追究，有效保障水利网络安全，水利部组织编制了《水利网络安全管理办法（试行）》。

《办法》包括总则、网络安全规划建设、网络运行安全、监测预警与应急处置、监督考核与责任追究、附则共六章。《办法》指出，水利网络安全遵循“积极利用、科学发展、依法管理、确保安全”的方针，建立及时发现漏洞、及时有效处置漏洞和严格责任追究三套机制，确保水利信息化规划建设同步落实网络安全等级保护制度，明确运行阶段网络安全责任。

4）加强工业互联网安全工作的指导意见

2019 年 8 月，为加快构建工业互联网安全保障体系，提升工业互联网安全保障能力，促进工业互联网高质量发展，推动现代化经济体系建设，护航制造强国和网络强国战略实施，工信部、教育部、国家能源局等十部委联合发布《加强工业互联网安全工作的指导意见》。

《意见》中包括推动工业互联网安全责任落实、构建工业互联网安全管理体系、提升企业工业互联网安全防护水平、强化工业互联网数据安全保护能力、建设国家工业互联网安全技术手段、加强工业互联网安全公服务能力、推动工业互联网安全科技创新与产业发展七大主要任务。同时，《意见》指出，到 2025 年，制度机制健全完善，技术手段能力显著提升，安全产业形成规模，基本建立起较为完备可靠的工业互联网安全保障体系。

5）关于促进网络安全产业发展的指导意见（征求意见稿）

2019 年 9 月，为应对互联网、大数据、人工智能和实体经济深度融合伴生的新风险，积极应对 5G、工业互联网、下一代互联网、物联网等新技术新应用带来的新挑战，工信部组织编写《关于促进网络安全产业发展的指导意见》（征求意见稿）。

《意见》中强调着力突破网络安全关键技术，积极创新网络安全服务模式，合力打造网络安全产业生态，大力推广网络安全技术应用，加快构建网络安全基础设施。通过以上多个方面加强 5G、下一代互联网、工业互联网、物联网、车联网等新兴领域网络安全威胁和风险分析，大力推动相关场景下的网络安全技术产品研发。加强工业互联网、车联网、物联网安全管理，督促指导相关企业采取必要的网络安全技术措施。重点围绕工业互联网、车联网、物联网新型应用场景，建设网络安全测试验证、培训演练、设备安全检测等共性基础平台。支持构建基于商用密码、指纹识别、人脸识别等技术的网络身份认证体系。

6）工业大数据发展指导意见（征求意见稿）

2019 年 9 月，为推进工业大数据发展，逐步激活工业数据资源要素潜力，不断提升数据治理和安全保障能力，工业和信息化部发布《工业大数据发展指导意见（征求意见稿）》

《意见》中强调到 2025 年，工业大数据资源体系、融合体系、产业体系和治理体系基本建成，形成从数据集聚共享、数据技术产品、数据融合应用到数据治理的闭环发展格局，工业大数据价值潜力大幅激发，成为支持工业高质量发展的关键要素和创新引擎。

7）工业互联网企业网络安全分类分级指南（试行）（征求意见稿）

2019 年 12 月，为贯彻落实《加强工业互联网安全工作的指导意见》，推动工业互联网

安全责任落实，对工业互联网企业网络安全实施分类分级管理，提升工业互联网安全保障能力和水平，工业和信息化部发布《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）。

依据企业属性，工业互联网企业主要包括三类：1，应用工业互联网的工业企业（简称“联网工业企业"），主要涉及原材料工业、装备工业、消费品工业和电子信息制造业等行业；2.工业互联网平台企业（简称“平台企业”，主要指对外提供工业互联网平台等互联网信息服务的企业）；3.工业互联网基础设施运营企业，主要包括基础电信运营企业和标识解析系统建设运营机构。

二、 工业安全标准体系建设

建立健全工业控制系统信息安全标准体系对工业信息安全建设具有重要的指导意义。通过工业信息安全标准体系的建设，可有效提高对工业信息安全风险的管控能力，通过与等级保护等工作接续起来，使得工业信息安全管理更加科学有效。同时，信息安全标准体系的建立将使得企业安全实施水平与国际先进水平接轨，从而加快工业控制系统信息安全的落实。

为了充分发挥生产、管理、科研、应用等各方面在各个行业、产业、企业、组织、机构的标准化工作中的作用，广泛开展信息安全领域的标准化工作，2002 年，中国通信标准化协会（CCSA）成立。2016 年，经国家标准化管理委员会批准成立全国信息安全标准化技术委员会（以下简称“信安标委”，TC260）。

信安标委是在信息安全专业领域内，从事全国标准化工作的技术工作组织，负责全国信息安全标准化的技术归口工作。另有全国电力系统管理及其信息交换标准化技术委员会（TC82）、全国电力监管标准化技术委员会（TC296）、全国工业过程测量和控制标准化技术委员会（TC124）共同推动工业控制系统信息安全标准工作。

2019 年 5 月，网络安全等级保护制度 2.0 标准**《信息安全技术网络安全等级保护基本要求》**、**《信息安全技术网络安全等级保护测评要求》**、**《信息安全技术网络安全等级保护安全设计技术要求》**国家标准正式发布，2019 年 12 月 1 日实施。等保 2.0 扩展了网络安全保护的范围，提高了对关键信息基础设施进行等级保护的要求，并且针对不同保护对象的安全目标、技术特点、应用场景的差异，采用了安全通用要求与安全扩展要求结合的方式，以更好地满足安全保护共性化与个性化要求，提升了等级保护的普适性与可操作性。同时，对

工业控制系统提出了安全扩展要求，以适用工业控制的特有技术和应用场景特点。安全拓展要求主要针对物理环境安全、网络和通信安全、设备和计算安全、安全建设管理和安全运维管理提出了具体的标准。

2019 年 6 月，国家标准**《信息安全技术 工业互联网平台安全要求及评估规范》**征求意见稿发布。工业互联网平台作为工业互联网的核心，由数据采集体系、工业 PaaS 平台和应用服务体系三大核心要素构成，是实体经济全要素连接的枢纽、资源配置的中心和智能制造的大脑。本标准对工业互联网相关组织开展安全防护工作提出了安全控制措施，可为工业互联网平台建设、运维、技术研发等方面安全防护工作提供规范性指导。

2019年7月，国家标准**《电力信息系统安全等级保护实施指南》**正式实施。为规范电力信息系统安全等级保护实施的流程、内容和方法，加强电力信息系统的安全管理，防范网络攻击对电力信息系统造成的侵害，保障电力系统的安全稳定运行，依据国家和行业有关政策，制定此标准。该标准由国家能源局提出，由全国电力监管标准化技术委员会(SAC/TC296)归口。

2019 年 8 月，国家标准**《信息安全技术 工业控制系统网络审计产品安全技术要求》**发布。随着工业化与信息化的深度融合，来自信息网络的安全威胁正逐步对工业控制系统造成极大的安全威胁，通用安全审计产品在面对工业控制系统的安全防护时显得力不从心，因此急需要一种能应用于工业控制环境的安全审计产品对工业控制系统进行安全防护。

2019 年 8 月，国家标准**《信息安全技术 工业控制网络监测安全技术要求及测试评价方法》**发布。应用于工业控制环境的网络监测产品与通用网络监测产品的主要差异体现在：通用网络监测产品主要针对互联网通用协议进行分析和响应，应用于工业控制环境的网络监测产品除了能够分析部分互联网通用协议外，还具有对工业控制协议的深度解析能力，而无需对工业控制系统中不会使用的通用协议进行分析。应用于工业控制环境的网络监测产品可能有部分组件需部署在工业现场环境，因此比通用网络监测产品具有更高的环境适应能力。应用于工业控制环境的网络监测产品比通用网络监测产品具有更高的可用性、可靠性、稳定性。

2019 年 8 月，国家标准**《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》**发布。工业控制系统漏洞检测的目的是检查和分析系统的安全脆弱性，发现可能被入侵者利用的漏洞，并提出防范和补救措施，工业控制系统漏洞检测产品可以用于离线环境、工业控制系统试运行期间或工业系统维修期间，能够对工业控制系统中的工业控制设备、通信设备、安全保护设备以及工业控制软件等进行自动检测，发现存在的漏洞。

2019年8月，国家标准**《信息安全技术 工业控制系统产品信息安全通用评估准则》**发

布。该标准定义了工业控制系统产品信息安全评估的通用安全功能组件和安全保障组件集合，规定了工业控制系统产品的安全要求和评估准则。该标准适用于工业控制系统产品安全保障能力的评估、产品安全功能的设计、开发和测试。

2019年8月，国家标准**《信息安全技术 工业控制系统安全检查指南》**发布。该标准制定的目的是为了指导我国国家关键基础设施中相关工业控制系统行业用户开展工业控制系统信息安全自评工作，掌握工业控制系统信息安全总体状况，及时有效发现工业控制系统存在的问题和薄弱环节，进一步健全工业控制系统信息安全管理制度，完善工业控制系统信息安全技术措施，提高工业控制系统信息安全防护能力，为国家对重点行业工业控制系统信息安全检查等工作提供支撑，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。

2019年8月，国家标准**《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》**发布。应用于工业控制环境的网络安全隔离与信息交换系统与通用网络安全隔离与信息交换系统的主要差异体现在：通用网络安全隔离与信息交换系统除了需具备基本的五元组过滤外，还需要具备一定的应用层过滤防护能力。用于工业控制环境的网络安全隔离与信息交换系统除了具有通用网络安全隔离与信息交换系统的部分通用协议应用层过滤能力外，还需要具有对工业控制协议应用层的过滤能力；结合工业控制环境中当前的信息安全防护技术水平，以及信息安全防护不得影响系统功能的正常运行，通用网络安全隔离与信息交换系统所要求的强制访问控制要求还不能够适应于工业控制环境；工业控制环境下的网络安全隔离与信息交换系统比通用网络安全隔离与信息交换系统具有更高的可用性、可靠性、稳定性等要求。

2019年8月，国家标准**《信息安全技术 工业控制系统专用防火墙技术要求》**发布。应用于工业控制环境的防火墙与通用防火墙的主要差异体现在：通用防火墙除了需具备基本的五元组过滤外，还需要具备一定的应用层过滤防护能力，用于工业控制环境的防火墙除了具有通用防火墙的部分通用协议应用层过滤能力外，还具有对工业控制协议应用层的过滤能力；用于工业控制环境的防火墙比通用防火墙具有更高的环境适应能力；工业控制环境中，通常流量相对较小，但对控制命令的执行要求具有实时性，因此，工业控制防火墙的乔吐量性能要求可相对低一些，而对实时性要求较高；工业控制环境下的防火墙比通用防火墙具有更高的可靠性、稳定性等要求。

第三章　　工业互联网安全威胁

一、 2019 年新公开工业控制系统严重漏洞

（一） 缓冲区溢出漏洞

缓冲区溢出（buffer overflow）是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出漏洞进行攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。如 2019 年 12 月，研华（Advantech）公司发布通报称，DiagAnywhere Server 软件存在高危漏洞。

Advantech DiagAnywhere Server 缓冲区溢出漏洞 （CVE-2019-18257）

威胁预警： CVSS v3 9.8 （高危漏洞）

风险评估：成功利用该漏洞，可能允许远程执行代码。

受影响的产品：DiagAnywhere 服务器版本 3.07.11 及更低版本

漏洞解决方案：

用户可关注该链接，掌握漏洞修复方案：

https://www.advantech.com

（二） 拒绝服务漏洞

拒绝服务漏洞是指可以实现拒绝服务攻击（ Denial of Service，DOS）的漏洞。DOS 攻击的目的是使计算机或网络无法提供正常的服务。利用拒绝服务漏洞进行攻击，攻击者往往不需要具有很高的攻击带宽，有时只需要发送 1 个数据包就可以达到攻击目的。如 2019 年 7 月，西门子（Siemens）公司发布通报称，Siemens SIPROTEC 5 和 Siemens DIGISI 5 存在高危漏洞。

Siemens SIPROTEC 5 和 Siemens DIGISI 5 拒绝服务漏洞（ CVE-2019-10931）

威胁预警： CVSS v3 7.8（高危漏洞）

风险评估：攻击者可借助特制的数据包利用该漏洞造成拒绝服务。

受影响的产品：

Siemens DIGSI 5 < V7.90

Siemens SIPROTEC 5

漏洞解决方案：

用户可关注该链接，掌握漏洞修复方案：

https://cert-portal.siemens.com/productcert/pdf/ssa-899560.pdf

（三） 访问控制漏洞

访问控制指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。访问控制漏洞，就是攻击者可以绕过安全限制，执行未授权的操作。利用访问控制漏洞进行攻击，可以导致系统的信息泄露、被篡改、删除，甚至可以取得系统特权，进而进行各种非法操作。如 2019 年 11 月，西门子（Siemens）公司发布通报称，Siemens SIMATIC S7-1200 CPU 存在高危漏洞。

Siemens SIMATIC S7-1200 CPU 访问控制漏洞（CVE-2019-13945）

威胁预警： CVSS v3 10（高危漏洞）

风险评估：成功利用该漏洞，攻击者可以通过物理访问异步收发传输器接口控制进程。

受影响的产品：

Siemens SIMATIC S7-1200 CPU

漏洞解决方案：

用户可关注该链接，掌握漏洞修复方案：

https://cert-portal.siemens.com/productcert/pdf/ssa-686531.pdf

（四） 跨站脚本漏洞

跨站脚本漏洞通常存在于客户端和服务器端，是能够实现跨站脚本攻击（Cross-site scripting，通常简称为 XSS）的漏洞。，利用 XSS 漏洞可以进行广告拦截、窃取隐私、钓鱼欺骗、窃取密码、传播恶意代码等各种各样网络攻击。如 2019 年 3 月，摩莎（Moxa ）公司发布通报称，Moxa IKS 和 EDS 存在高危漏洞。

Moxa IKS 和 EDS 访问控制漏洞（CVE-2019-6565）

威胁预警： CVSS v3 10（高危漏洞）

风险评估：成功利用该漏洞，攻击者可进行跨站脚本攻击。

受影响的产品：

Moxa IKS-G6824A <=4.5

Moxa EDS-405A <=3.8

Moxa EDS-408A <=3.8

Moxa EDS-510A <=3.8

漏洞解决方案：

用户可关注该链接，掌握漏洞修复方案：

https://www.moxa.com/support/request_support.aspx

（五） 未授权访问漏洞

未授权访问漏洞可以理解为需要安全配置或权限认证的地址、授权页面等存在一定的缺陷，导致其他用户可以直接访问，从而引发重要权限可被操作、数据库、网站目录等敏感信息泄露的漏洞。如 2019 年 10 月，研华（Advantech ）公司发布通报称，Advantech WISE-PaaS/RMM 存在高危漏洞。

Advantech WISE-PaaS/RMM 未授权访问漏洞（CVE-2019-13547）

威胁预警： CVSS v3 9.8（高危漏洞）

风险评估：成功利用该漏洞，未经身份验证的攻击者可以使用工控设备。

受影响的产品：

Advantech WISE-PaaS/RMM 3.3.29 及之前版本

漏洞解决方案：

用户可关注该链接，掌握漏洞修复方案：

https://www.advantech.com

（六） 远程代码执行漏洞

远程代码执行漏洞，用户通过浏览器提交执行命令，由于服务器端没有针对执行函数做过滤，远程代码执行漏洞会导致攻击者在目标系统执行任意命令。如 2019 年 12 月，西门子（Siemens）公司发布通报称，Siemens SPPA-T3000 Application Server 存在高危漏洞。

Siemens SPPA-T3000 Application Server 远程代码执行漏洞（CVE-2019-18283）

威胁预警： CVSS v3 9.8（高危漏洞）

风险评估：成功利用该漏洞，攻击者可在服务器上执行任意代码。

受影响的产品：

Siemens SPPA-T3000 Application Server（全部版本）

漏洞解决方案：

用户可关注该链接，掌握漏洞修复方案：

https://www.siemens.com

第四章　　工业安全应急响应典型案例

2019 年奇安信工业安全应急响应中心和安全服务团队共同为全国工业企业提供应急求助 273 起，涉及医疗卫生、交通运输、制造业、能源等重要关键信息基础设施行业。遭受勒索病毒攻击仍然是工业企业面临的最大挑战，这些安全事件均不同程度地造成较为严重的社会负面影响，带来了严重损失。

一、 某工业集团入网前 Conficker、Fakefolder 病毒处置

场景回顾

2019 年 1 月，某工业集团为了便于各测试系统中测试数据的统一采集、存储和管理，各测试系统将陆续接入 TDM 系统（测试数据管理系统）中，当前仍然有部分测试设备、系统未接入。由于移动介质的交叉使用、相关使用规范的缺失，当前未入网的设备/系统中存在大量病毒，因此该工业集团请求工业安全应急响应中心进行应急响应。

问题研判

工业安全应急响应中心人员到达现场后，经对现场情况的了解及设备的检测，发现当前设备、系统、网络中存在的主要问题是由于 U 盘的不合理使用使得 TDM 系统中感染了“Conficker” 蠕虫、矢网仪感染了“FakeFolder”蠕虫病毒。

病毒可通过移动介质、网络大范围传播，由此形成恶性循环；同时，病毒感染后可进行各种恶意操作，如安装后门、窃取敏感数据、篡改数据等，数据可通过被感染的移动介质和主机传播外泄，由此造成敏感数据丢失、测试数据不准确，最终导致产品出现功能、性能问题的可能性；缺乏对 U 盘使用的基本管理制度，亦无技术管控措施；安全意识有待高，安全制度建立有待完善。

处置方案

1） 在工业终端、服务器等安装工业主机安全防护系统，建立安全基线，对 U 盘使用进行策略配置；

2） 对于 TDM 系统，可在控制主机和数据中转主机之间配置工业网关设备，保证数据的安全、单向传输，在 TDM 网络边界处部署工业防火墙。

除此之外，做好应急准备，将安全处置风险降到最低或可控。

二、 某大型制造企业遭受 WannaMine3.0 及“永恒之蓝”勒索病毒攻击

场景回顾

2019 年 2 月，某大型制造企业的卧式炉、厚度检测仪、四探针测试仪、铜区等多个车间的机台主机以及 MES（制造执行系统）客户端都不同程度的遭受蠕虫病毒攻击，出现蓝屏、重启现象。该企业内部通过处理(机台设备离线、部分 MES 服务器/客户端更新病毒库，更新主机系统补丁)暂时抑制了病毒的蔓延，但没有彻底解决安全问题，因此紧急向工业安全应急响应中心求救。

问题研判

工业安全应急响应中心人员到达现场后，经对各生产线的实地查看和网络分析可知，当前网络中存在的主要问题是工业生产网和办公网网络边界模糊不清，MES 与工控系统无明显边界，采用两个网段公用的现场，各生产线未进行安全区域划分，在工业生产网中引入了 WannaMine3.0、“永恒之蓝”勒索蠕虫变种，感染了大量主机，且勒索蠕虫变种在当前网络中未处于活跃状态（大部分机台设备已离线）。

处置方案

1） 制定 MES（制造执行系统）与工控系统的安全区域，规划制定安全区域划分；

2） 隔离感染主机：已中毒计算机关闭所有网络连接，禁用网卡，未进行查杀的且已关机的受害主机，需断网开机；

3） 切断传播途径：关闭潜在终端的网络共享端口，关闭异常的外联访问；

4） 查杀病毒：使用最新病毒库的终端杀毒软件，进行全盘查杀；

5） 修补漏洞：打上“永恒之蓝”漏洞补丁并安装工业主机安全防护系统。

三、 某钢铁企业智能工厂改造前“永恒之蓝”勒索变种病毒处置

场景回顾

2019 年 3 月，某钢铁企业为了适应发展，满足智能制造要求，对工厂进行现代化改造，新建数采网，提高信息化程度，推进数字化工厂建设。在前期规划建设中，发现部分工控主机出现蓝屏异常现象，为保证后期改造中安全升级改造符合实际需要，制定符合实际情况的

工业安全解决方案，因此该钢铁企业请求工业安全应急响应中心进行应急响应。

问题研判

工业安全应急响应中心人员到达现场后，经现场实际检查，当前网络中存在的主要问题为网络中的交换机未进行基本安全配置，各层级网络由“桥梁式”主机互通互联，边界缺乏工业防火墙保护，“永恒之蓝”勒索病毒通过办公网传入生产网，当前生产网络中存在“永恒之蓝”勒索病毒（其他 rootkit 病毒、文件型感染病毒亦存在），且病毒处于活跃状态。

处置方案

1） 通过主机临检工具扫描病毒并进行删除，安装微软补丁；

2） 对 OT 资产进行清点，分级和分类，各区域边界部署工业防火墙设备；

3） 对工业主机实施“白名单”类的工业主机安全防护软件的部署，可以在生产间隙或检修时完成；

4） 在核心交换机旁部署实施工业安全监测系统，构建全面的防御和监测体系。

四、 某化工集团遭受蠕虫病毒攻击

场景回顾

2019 年 5 月，该化工集团的乙炔产线出现 3 台操作员站重启，服务器卡顿，数据不能实时显示的问题，受病毒影响生产被迫停止 48 小时。为了尽快恢复生产，客户现场对中毒机器进行格式化，重装系统，暂时解决问题，同时紧急向奇安信工业安全应急响应中心求救。

问题研判

工业安全应急响应中心人员到达现场后，经现场实际检查，当前网络中存在的主要问题为各服务器、工业主机账号密码存在相似、未满足密码复杂度要求的现象，工业主机没有部署任何安全防护产品和措施，弱口令被攻击者利用，导致工业主机遭受病毒攻击。

处置方案

1） 对已攻陷主机排查与查杀处置，结束病毒进程并删除服务，删除下载和释放的病毒文件、注册表项，安装工业主机安全防护系统；

2） 每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长（15 位、两种组合以上）；

3）对工业网所有机器使用专杀工具检测。建立完善的工业安全防护制度和统一方案，确保生产安全、连续、稳定。

第五章　　工业互联网安全推进建议

结合工业互联网安全风险和威胁，我们发现传统的“围墙式”网络安全建设、业务和安全“两张皮”、IT 安全管理和 OT 安全管理“两张皮”式的安全防护体系已经不能满足越来越复杂的网络安全环境。因此，规划建设“工业互联网安全技术保障平台”有利于全面提高工业互联网安全建设水平。

三级协同的“工业互联网安全技术保障平台”建设将全面提升工业互联网安全保障水平。平台基于“监测-响应”的技术路线进行建设实施，有利于工业生产的长期可靠、稳定运行。因此，旁路的、非侵入式的平台建设结合关键节点串接、阻断式的安全防护是工业互联网安全建设的发展趋势。

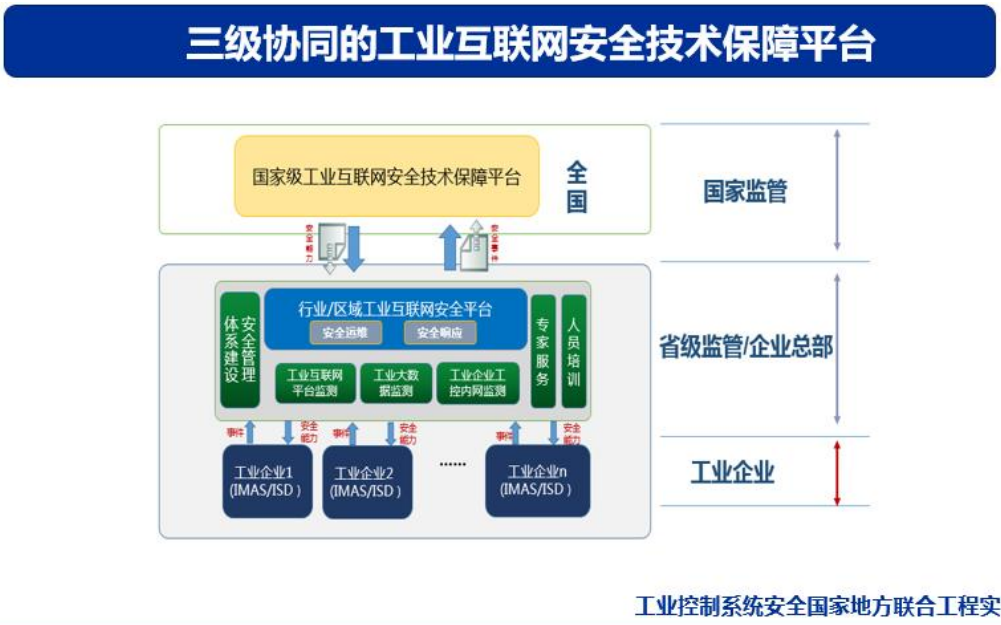

图 7：三级协同的工业互联网安全技术保障平台

通过近年来不断的宣传教育，大多数工业企业开始重视工业网络安全工作，但是很多企业存在着重建设、轻运营的问题。一方面，这些企业对安全运营的重要性缺乏必要的认识。另一方面，工业企业也普遍缺乏合格的安全人才。这些现状导致已部署的平台长期处于一种无运营或者有限运营的状态，不能充分发挥平台的安全防护能力。

我们认为工业企业可以利用外部资源，特别是安全公司提供的远程、驻场或托管式安全运营服务开展工作。工业企业也可以把安全运营工作上移到集团、行业等平台，通过委托方式用专业安全团队来提供安全保障。这些平台通常都具备本地化的应急响应团队，可以对工业安全事件进行及时响应。

采用以上方案，不仅可以在威胁发现、风险预测、处置响应、追踪溯源等方面大幅度提

高工业企业网络安全防护能力，还可以减少人力资源投入、降低工业企业安全运营成本。省级或行业级平台在和企业数据对接过程中，要重点做好数据采集、数据传输、数据存储、数据处理等方面的安全防护工作，构建全生命周期的工业大数据安全防护体系。省级或行业级工业互联网安全技术保障平台要以服务工业用户为主要目的，为接入企业提供有价值的安全运营服务。数据上报后帮助工业企业定期分析安全风险，及时发现安全威胁，第一时间应急响应，事后实现追踪溯源，减少企业安全损失，提供安全咨询，让工业企业看到数据上报后给企业所带来的价值。

目前工业互联网安全技术保障平台建设还在起步阶段，特别是企业侧平台的建设机会巨大。平台建设应处理好与等保建设之间的关系，加强平台的运营和管理，吸引更多的工业企业接入上级平台。平台的建设必将推动我国工业互联网快速、健康发展。

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，由奇安信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。

工业安全国家联合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。

工业安全国家联合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、西安电子科技大学、吉林大学、武汉大学、北京理工大学、信息工程大学等均建立了人才联合培养机制。

工业安全国家联合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），推出了工业主机安全防护系统、工业防火墙/网关、工业安全监测系统、工业安全监测控制平台、工业互联网安全监测服务平台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。

附录二 2019 工业互联网安全重大事件

一、 挪威海德鲁铝业集团多家铝生产工厂遭受病毒攻击

2019 年 3 月，世界最大的综合性铝业集团之一挪威海德鲁公司（Norsk Hydro）在全球多家铝生产工厂遭受严重网络攻击，造成多个工厂关闭和部分工厂切换为手动运营模式。

据海德鲁公司透露，此次网络攻击由一种名为“LockerGoga”的勒索软件造成，该勒索软件能够对目标计算机所有文件进行加密，然后要求受害者支付勒索赎金。

根据海德鲁公司最新披露，公司在挪威国家安全局及合作伙伴帮助下采用工厂隔离、病毒识别、恢复备份系统等方式遏制病毒传播和进行系统修复，但目前病毒传播和感染的整体情况不明，全面恢复正常生产还有很大难度。已发现的病毒主要破坏企业 IT 系统，造成 IT 系统与工控系统数据连接失效，导致生产停产。

二、 委内瑞拉电力系统遭受网络攻击再度瘫痪

2019 年 3 月，委内瑞拉开始大规模停电，从安第斯山脉到加勒比海岸地区陆续进入断电状态，停电以后委内瑞拉的主要交通系统全部瘫痪，基础设施陆续失效。

此次停电是自 2012 年以来委内瑞拉持续时间最长、影响地区最广的停电，委内瑞拉新闻部长罗德里格斯也表示，此次停电的原因是国内最重要的古里水电站遭到反对势力蓄意破坏，委内瑞拉政府称这一行为是反对势力在对委内瑞拉发动“能源战争”。持续的“高科技网络攻击”让委内瑞拉电力部门的修复工作频频受阻，全面恢复供电举步维艰。据分析，新版 Stuxnet 病毒最有可能成为此次攻击的手段。

三、 日本制造企业 Hoya 感染挖矿病毒，产线被迫停产三天

2019 年 4 月，日本领先的光学产品制造商 Hoya 公司称，公司在 2 月底遭受了一次严重的网络攻击，100 多台电脑感染了病毒，导致 Hoya 公司的用户 ID 和密码被黑客窃取。黑客还在攻击期间试图挖掘加密货币，工厂生产线因此停止了三天。

Hoya 表示，网络攻击发生后，一台控制网络的计算机服务器首先停机，工人们无法使用软件来管理订单和生产，因此工业产出比正常水平下降了大约 40%。随后，病毒也开始在其他电脑上感染，但最终在开始加密货币挖掘操作之前被成功阻止。

四、 大型飞机零部件供应商 ASCO 遭勒索病毒攻击

2019 年 6 月，世界上最大的飞机零部件供应商之一 ASCO 的一个工厂遭勒索病毒攻击，由于勒索病毒感染导致 IT 系统瘫痪，该公司目前约有 1000 名工人暂停工作。另外，ASCO 也关闭了德国、加拿大和美国的工厂。

目前还不清楚 ASCO 是否已支付赎金以恢复其系统的访问权限从备份中恢复，或从头开始购买新系统重建其计算机网络。这充分说明了，目前的飞机零件制造工厂，均是采用互联网智能化管理模式进行批量生产，智能化工厂安全以及设施设备保护将是制造商需要考虑的重要问题。此安全事件告诫我们：随着工业互联网的发展，IT 和 OT 技术逐渐融合， 在拓展了发展空间的同时也带来一系列网络安全问题。企业需要了解自身能力和系统的局限性，以形成全面的网络安全战略，从而确保设备、网络、数据、信息等得到正确的保护。

五、 德国军工巨头莱茵金属公司遭恶意软件袭击

2019 年 9 月，总部位于德国的德国莱茵金属公司（Rheinmetall）由于受到恶意软件攻击，其在美国，巴西和墨西哥的汽车工厂的生产受到了严重干扰。

攻击涉及一个未知的恶意软件，于 9 月 24 日晚上开始。导致该恶意软件进入 IT 系统的工厂受到“重大破坏”。公司认为，从攻击中恢复需要花费两到四周的时间，并且估计从第二次攻击开始，该事件将导致每周损失 300 万欧元至 400 万欧元。

六、 印度 Kudankulam 核电站内网遭受恶意软件攻击

10 月 30 日，印度核电公司（NPCIL）证实，印度 Kudankulam 核电站内网感染了恶意软件。据了解，该软件由知名朝鲜黑客组织 Lazarus 开发，属于 Dtrack 后门木马的变体。其功能包括窃取设备的键盘记录、检索浏览器历史记录，以及列出正在运行的进程等。从其功能可以明显看出，Dtrack 通常用于侦察目的，并用作其他恶意软件有效载荷的投递器。

据了解，攻击组织至少从 2018 年起开始针对印度的银行、核电站领域实施 APT 攻击，并且至今仍在进行中。推测针对银行的活动可能从 2018 年夏至 2019 年上半年，而针对核电站的攻击活动可能从 2019 年 7 月甚至更早开始。

根据公开声明，受感染的计算机属于连接到互联网的用户，目前并没有证据显示该核电站的控制系统受到攻击。APT 是一种高级持续性威胁，具有较强的隐蔽能力，需从设备、控

制、网络、数据等方面采用主被动结合的防御方式。

七、 自动化设备生产商皮尔兹遭勒索软件攻击

2019 年 10 月，总部位于德国全球最大的自动化设备生产商之一皮尔兹公司遭遇 BitPaymer 勒索病毒的攻击，使得该公司在全球范围内的所有服务器和 PC 工作站，包括通信设施，都受到了影响。

为预防起见，该公司切断了所有的网络连接，并阻止外部对公司网络的访问，同时皮尔兹员工花了三天时间才恢复电子邮件服务的访问，又花了三天才恢复其国际电子邮件服务，。在被攻击的一周内，其订单系统无法正常工作，无法提交订单和检查客户状态，导致其全球 76 个国家或地区的业务均受影响。

八、 石油巨头 Pemex 遭受勒索软件攻击

2019 年 11 月，墨西哥石油巨头 Pemex 遭受 DoppelPaymer 勒索软件攻击，攻击者索要 565 个比特币，相当于约 500 万美元，并要求在 48 小时内支付赎金。

据报道，Pemex 要求员工断开中央网络的计算机连接，并备份关键信息。由于无法访问他们的计算机或中央服务器，管理工作被迫停止。该公司的工作人员无法访问网络上的几个系统，无法访问付款和其他管理活动。