工业互联网平台安全白皮书(2020)

工业互联网安全系列研究报告

国家工业信息安全发展研究中心
CHINA INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

工业信息安全产业发展联盟
National Industrial Security Industry Alliance
NISIA

版权申明

序

国家工业信息安全发展研究中心（工业和信息化部电子第一研究所）简称国家工信安全中心，是工业和信息化部直属事业单位，是我国工业领域国家级信息安全研究与推进机构。为加快推进工业信息安全技术研发和保障能力建设，更好地推动工业信息安全事业发展，国家工信安全中心于2018年9月成立保障技术所。

自成立以来，保障技术所始终坚持贯彻落实总体国家安全观，以护航制造强国和网络强国建设为重点，围绕新一代信息技术与制造业融合带来的安全需求，以“风险可发现、可防范、可处置”为保障目标，面向工业控制系统、工业互联网、工业云、工业大数据、新一代信息技术等领域开展核心安全技术攻关，2018年以来承担40余个工控安全、工业互联网安全专项和重大课题，构建保障技术平台和专业技术力量，有力支撑主管部门完成工控安全、工业互联网安全等相关监督指导工作，帮助工业互联网企业提升安全保障能力。保障技术所建立了扎实的技术与服务能力，包括工业信息安全技术保障平台建设、工业信息安全实验室建设支撑、工业互联网安全技术服务与咨询、工业互联网数据安全监测与防护、工业数据安全交换共享、工业互联网标识解析建设与安全认证、标准研究与对标评估、安全评估评测等。

保障技术所联合业界单位，推出了《工业互联网平台安全》《工业互联网边缘计算安全》《工业互联网标识解析安全》《工业互联网数据安全》等系列白皮书，可为业界开展工业互联网安全相关工作提供参考。由于成稿仓促，加之水平有限，报告中难免有疏漏和错误之处，恳请批评指正。在此对于给予白皮书编制和发布等提供指导、支持、帮助的单位和个人一并表达感谢。

编写组

2020年12月

白皮书编写说明

工业互联网平台是面向制造业数字化、网络化、智能化需求而构建的，基于云平台的海量数据采集、汇聚、分析和服务体系，支持制造资源实现泛在连接、弹性供给、高效配置。一方面，工业互联网平台是业务交互的桥梁和数据汇聚分析的中心，连接大量工业控制系统和设备，与工业生产和企业经营密切相关。其高复杂性、开放性和异构性加剧其面临的安全风险，一旦平台遭入侵或攻击，将可能造成工业生产停滞，波及范围不仅是单个企业，更可延伸至整个产业生态，对国民经济造成重创，影响社会稳定，甚至对国家安全构成威胁。保障工业互联网平台安全，是保障制造强国与网络强国建设的主要抓手。另一方面工业互联网平台上承应用生态、下连系统设备，是设计、制造、销售、物流、服务等全生产链各环节实现协同制造的“纽带”，是海量工业数据采集、汇聚、分析和服务的“载体”，是连接设备、软件、产品、工厂、人等工业全要素的“枢纽”。因此，做好工业互联网平台安全保障工作，是确保工业互联网应用生态、工业数据、工业系统设备等安全的重要保证。工业互联网平台作为工业互联网的重要关键，面临着更具挑战的安全风险，加快提升工业互联网平台安全保障能力迫在眉睫。

在这样的背景下，国家工业信息安全发展研究中心会同工业信息安全产业发展联盟，联合相关企事业单位，共同研

究编写《工业互联网平台安全白皮书（2020）》。希望提高业界对工业互联网平台安全风险及相关防护技术的重视、达成共识，以推动工业互联网平台安全发展，为工业互联网健康发展保驾护航。

本白皮书旨在共商工业互联网平台安全，共筑产业生态，主要分为六个部分。第一部分介绍了国内外工业互联网平台发展情况。第二部分梳理了工业互联网平台安全防护现状。第三部分分析了工业互联网平台安全需求与边界。第四部分提出了包含防护对象、安全角色、安全威胁、安全措施、生命周期五大视角的工业互联网平台安全参考框架。第五部分汇编总结了保障工业互联网平台安全的关键技术。第六部分从政策标准、安全技术、产业协同三个方面对工业互联网平台安全发展进行展望。

编写组

主编: 陈雪鸿、李俊

编写单位和成员:

国家工业信息安全发展研究中心	王冲华、樊佩茹、周昊、余果、林晨、杨帅锋、张雪莹、江浩、孙岩、李耀兵、夏宜君、张莹、李红飞
北京大学	沈晴霓、方跃坚
杭州海康威视数字技术股份有限公司	王滨、王星
中国科学院信息工程研究所	郝志宇、王雅哲、崔磊、霍冬冬
北京东方国信科技股份有限公司	敖志强、孙广明
北京六方云信息技术有限公司	李江力、赵学全
广州安加互联科技有限公司	彭卓、何立林
武汉大学	赵波、赵鹏远
广州大学	殷丽华、罗熙
启明星辰信息技术集团股份有限公司	雷慧桃
海尔数字科技(上海)有限公司	莫止卿
青岛海尔工业智能研究院	陈启龙、欧阳佩佩
浪潮云信息技术有限公司	李传忠、黄先芝
腾讯云计算(北京)有限责任公司	李向前、王朋群

东南大学	黄杰
众能联合数字技术有限公司	张海港
中国联通研究院	徐雷、于城
阿里云计算有限公司	郑景鑫
中国电子科技集团公司信息科学研究院	张德、方赴洋
北京信息科技大学	张仰森、李军
华东师范大学	刘虹
陕西省网络与信息安全测评中心	杨帆
上海工业控制安全创新科技有限公司	杨昆
北京神州慧安科技有限公司	刘瑛、项立洋
恒安嘉新（北京）科技股份公司	王泽政、李鹏超
北京交通大学	陶耀东
亚信科技（成都）有限公司	吴天飞
绿盟科技集团股份有限公司	王晓鹏、张涛
长扬科技（北京）有限公司	汪义舟、张亚京
山东省电子信息产品检验院	李侠
哈尔滨安天科技集团股份有限公司	王乃青、刘佳男
用友网络科技股份有限公司	杨宝刚
杭州安恒信息技术股份有限公司	冀宗玉
北京立思辰信息安全科技集团	佟海燕

目录
CONTENTS

一、工业互联网平台发展情况 …… 1
（一）工业互联网平台概述 …… 1
（二）全球工业互联网平台 …… 2
（三）我国工业互联网平台 …… 4
二、工业互联网平台安全防护现状 …… 8
（一）工业互联网平台安全顶层设计 …… 8
（二）工业互联网平台安全建设发展多样化 …… 11
（三）我国工业互联网平台安全能力现状 …… 14
三、工业互联网平台安全需求与边界 …… 19
（一）工业互联网平台安全需求特征 …… 19
（二）工业互联网平台安全边界 …… 23
四、工业互联网平台安全参考框架 …… 25
（一）安全防护对象视角 …… 25
（二）安全角色视角 …… 28
（三）安全威胁视角 …… 31
（四）安全措施视角 …… 37
（五）生命周期视角 …… 43
五、工业互联网平台安全关键技术 …… 46
六、工业互联网平台安全发展展望 …… 53
（一）政策标准 …… 53
（二）安全技术 …… 54
（三）产业协同 …… 56

一、工业互联网平台发展情况

（一）工业互联网平台概述

国际主流工业大国都在大力推进工业互联网建设，并以工业互联网平台为引擎，探索工业制造业数字化、智能化转型发展新模式。工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台。目前，业界已基本形成智能终端（边缘）+云架构+工业APP的工业互联网平台技术架构，一方面平台承载工业知识与微服务，向上支撑工业APP和云化工业软件的开发和部署，为企业客户提供各类应用服务；另一方面工业互联网平台向下实现海量的多源设备、异构系统的数据采集、交互和传输，支持软硬件资源和开发工具的接入、控制及应用。

随着国内外对工业互联网平台变革性质和重要作用的认识不断深入，制造企业、自动化企业、通信企业、互联网企业等各类主体聚焦自身核心能力，基于公有云、私有云或混合云构建面向不同行业领域、不同技术架构、不同运行模式的工业互联网平台，旨在提升设备连接、设备管理、数据存储及处理、数据高级分析、软件应用管理、平台应用开发、整合集成等服务能力，用于满足工业领域设备产品管理、业务运营优化、社会化资源协作三个方面的需求，以实现降低成本、提高

效率、提升产品和服务品质、创造新价值四大成效。

针对工业应用场景，工业互联网平台通过各类机器设备、人、业务系统的互联，促进数据跨系统、端到云的流动，基于数据分析、建模和应用，实现数据驱动的生产、运营闭环优化，形成新的业务模式和新的业态。与传统工业IT架构相比，工业互联网平台促使流程驱动的业务系统转变为数据驱动的应用范式，为工业企业提供了基于数据的新技术、新方法、新服务和新价值。

（二）全球工业互联网平台

在国际经济开放融合的背景下，随着5G网络、人工智能、大数据等新兴技术的发展，全球工业互联网平台保持高速增长态势。据咨询机构IoT Analytics的统计，2019年全球工业互联网平台（包括物联网平台）公司数量达到620个，各类企业围绕工业互联网平台的参与热情和布局力度持续高涨。

1.制造巨头凭借已有工业积淀拓展平台市场

制造巨头凭借主机厂优势，打开工业互联网平台市场。西门子MindSphere平台和通用电器Predix平台从关键通用设备入手，借助在底层工业装置的数据采集、工业知识的封装和复用、信息资产建模等方面的优势，基于自有系统，实现工业现场设备、工业数据、企业运营数据、人员及其他资产的相互连接；库卡KUKA Connect平台、安川电机MMcloud

平台、霍尼韦尔Sentience平台等通过机器人、机床等设备优势，开展工业设备数据的深层次采集，为各家企业提供状态监控、设备维护提醒、实时故障发现等产品增值性服务。

2.工业互联网平台对不同工业场景形成适配

IT优势企业以数据算法、通信连接等为切入点，探索工业应用场景。在数据算法方面，以微软、亚马逊为代表的互联网巨头为平台提供各类大数据、人工智能通用算法框架和工具，与工业企业客户联合进行研发，形成可视化管理、质量分析优化、预测性维护等工业解决方案；在底层连接方面，**思科**等通信巨头也开始将平台连接和服务能力向工厂内渗透，从各种工业以太网和现场总线中获取实时生产数据，支撑形成工业智能应用。制造企业以行业领域深耕为基础，打造行业领域竞争力。在电气领域，ABB、菲尼克斯电气、施耐德电气以电力电气、自动化行业为主，提供端到端的工业数字化解决方案；在工程机械领域，卡特比勒、小松、日立等平台面向工程机械领域资源调配、设备运维、供应链协同方面的需求，提供设备预测性维护、备品备件管理、智慧施工、互联网金融等能力。

3.数据驱动的工业互联网平台应用更加活跃

数据成为工业互联网平台的生产资料，科技企业成为应用引领者。数据连接方面，Sieraa Wiless、Telit、Device Insight等M2M通信领域公司充分发挥在数据连接方面

的技术优势，结合工业互联网平台，帮助工业企业实现资产的远程连接和在线管理；数据分析方面，Uptake、C3IoT、Mnubo、Particle等国际工业互联网、物联网公司将工业大数据、人工智能技术与工业互联网平台进行深度结合，满足工业领域日益深入的数据分析需求；数据应用方面，日立Lumada、东芝SPINEX、富士机械NEXIM平台基于数据改善生产制造过程，优化自身价值链和降低运营成本。此外，制造企业与软件企业的战略合作促进了数据的深度应用，PTC与罗克韦尔合作推出ThingWorx，提供面向生产过程可视化的数据汇聚和高级生产分析功能，帮助管理者直观地了解工厂运行状态。

（三）我国工业互联网平台

2020年，我国工业互联网平台初步展现多元化发展态势，覆盖原材料、装备、机械、消费品、电子、交通等多种行业及场景。工业互联网平台应用与创新走深走实，在行业和区域中赋能工业数字化转型效果逐渐凸显，充满活力的产业生态体系加速形成。

1.工业互联网平台应用由政策驱动转向市场主导

随着工业互联网平台、网络、安全等配套政策趋于完善，工业互联网平台的发展与应用已经成为工业企业构建网络化协同、规模化定制、服务型制造等新模式、新业态、新动能。海尔COSMOPlat平台打造了包括大数据、供应链、协

同制造、智能维保等170多个专业解决方案，覆盖房车、建陶、纺织、模具、机床、农业等15个行业生态。阿里云通过SupET “1+N” 工业互联网平台，为100余家中小信息化服务商、大数据创新企业和信息工程服务企业提供服务，实现云端工业APP一站式开发、托管、集成、运维和交易。航天云网INDICS平台以云制造为核心，立足航空航天领域，面向电子信息、工程机械、汽车制造等行业提供应用服务。树根互联 “根云” 平台提供快速物联、设备预测性维护、配件预测管理、大数据AI等能力，与行业巨头联合打造 “机床云”、“纺织云”、“3D打印共享云”、“空压机云”、“电机云”、“注塑云”、“筑工云” 等数十个垂直行业云平台。

2.新一代信息技术为工业互联网应用落地提供新场景

大数据、人工智能、5G、区块链等新一代信息技术日趋成熟，涌现出更多 “平台+新技术” 的创新解决方案。东方国信Cloudiip平台、富士康 “工业富联” 平台、紫光云引擎 “芯云” 平台等通过 “平台+5G” 融合应用，实现高可靠、低时延、高通量的数据集成，催生数字化工业灵活组网、智能终端远程控制、全场景运营优化等模式；中国电信工业互联网开放平台、杭州汽轮工业互联网服务平台等开展 “平台+4K/8K高清视频” 融合探索，实现高精度、异构图像视频数据分析，催生智能产品检测、设备远程运维等模式；华为FusionPlant平台、中兴ThingxCloud兴云平台等通过 “平台+VR/AR” 融合

应用，实现三维动态视景快速生成与分析，催生人机协同工作、产品自动化分拣、产品设计可视化等模式。

3.面向特定行业领域的系统解决方案成为应用聚焦点

工业互联网平台在各行业领域中应用的深度和广度不断拓展，平台产业链图谱更加完善。行业龙头围绕行业痛点挖掘深度应用。在石化行业，石化盈科面向生产过程复杂、生产工序间耦合度高的流程行业，开发基于ProMACE工业互联网平台的生产计划、调度、操作全过程管控方案。在工程机械行业，徐工集团、三一重工、中联重科等国内企业和Uptake等国外企业以远程运维为切入点，日本小松以智慧施工为切入点，加速推动工程机械行业向设备维护智能化、综合解决方案“交钥匙化”方向加速转型。在汽车行业，北汽新能源打造了“北汽云”京津冀地区产业协同工业互联网平台，形成汽车个性化定制、质量大数据分析、车联网等解决方案。部分企业发挥协同优势整合产业链上下游资源。在后市场领域，众能联合整合豪士科、捷尔杰、Haulotte、临工重机等工程机械产品，构建物联网智能平台，实现物流、租赁、服务全业务链条融合。

随着工业互联网创新发展战略的深入推进，工业互联网平台赋能水平显著提升，基于平台的制造业生态体系日趋完善。工业互联网创新发展工程实施3年来，平台方向共支持了226个创新工程项目，累计带动社会资本投资近254亿元，建

设19个创新体验和推广中心，5个工业互联网实训基地和长三角工业互联网示范区。重点工业互联网平台平均工业设备连接数达到65万台、工业APP达到1950个、工业模型数突破830个，平台活跃开发者人数超过3800人，在钢铁、石化、机械、轻工、电子等领域催生了一批新模式新业态，显著带动行业转型升级。

二、工业互联网平台安全防护现状

纵观全球工业互联网平台安全态势，发达国家从工业控制系统、物联网、云平台、大数据等不同角度推动工业互联网平台安全发展，我国重点围绕工业互联网安全，出台政策文件，制定安全标准，规范企业加强工业互联网平台安全。然而，我国工业互联网平台安全保障能力建设仍处于起步阶段，亟需提升企业安全防护意识，突破相关核心技术，支撑我国工业互联网平台健康发展。

（一）工业互联网平台安全顶层设计

1.主要发达国家工业互联网平台安全顶层设计

美国、欧盟、日本及其它发达国家尚未出台专门针对工业互联网平台安全的指导性文件，当前主要围绕工业控制系统、物联网、云平台等角度出台政策与标准体系，推进工业互联网平台安全防护工作。

美国政府和行业联盟出台政策、标准与规范指南文件，积极引导工业互联网安全发展。**政府层面，**2014年，美国发布《国家网络安全保护法》，将工控系统列为网络安全重点保护对象。之后，相继发布《网络安全国家行动计划》《物联网安全战略原则》《美国国土安全部工业控制系统能力增强法案》《缓解云漏洞指南》，从工业控制系统安全、物联网安全、云安全等角度提出相应保障策略。**行业联盟层面，**2016

年以来，美国工业互联网联盟（IIC）发布《工业物联网安全框架》《端安全最佳实践》，提出工业物联网安全的六大内容。此后，相继发布《商业视角下的工业互联网安全概括》《工业互联网安全成熟度模型》《云计算关键领域安全指南V4.0》等多个指导性文件，并举办多次安全论坛，推进安全解决方案落地实施。

欧盟高度重视工业战略下的网络安全问题。2012年，发布《未来经济复苏与增长：建设一个更强的欧洲工业》，强调提升工控系统的安全防护能力。2013年，欧洲网络与信息安全局（ENISA）相继发布《工业控制系统网络安全白皮书》《智能制造背景下的物联网安全实践》《工业4.0-网络安全挑战和建议》，给出工业4.0下的网络安全建议。2019年，欧盟发布《增强欧盟未来工业的战略价值链》报告，指出增强工业互联网战略价值链需大力发展欧洲网络安全产业。**德国**加快推进“工业4.0”战略实施，同步强调安全保障工作。2013年，德国政府推出《德国工业4.0战略计划实施建议》，提出保障工业4.0安全的措施建议。随后，德国工业4.0平台发布《工业4.0安全指南》《跨企业安全通信》《安全身份标识》等指导性文件，提出以信息物理系统平台为核心的分层次安全管理思路。

日本持续推进面向制造的网络安全。2014年，发布《网络安全基本法》，强调电力等基础设施运营方的网络安全要

求。2016年，成立“工业网络安全促进机构（ICPA）”，抵御关键基础设施攻击。2017年，日本提出“互联工业”战略，强调网络安全的重要性，成立“工业网络安全卓越中心”，旨在保护工业基础设施免受网络攻击。

其他国家也将基础设施和工业控制系统安全作为网络安全的重点。2016年，新加坡发布《国家网络安全策略》，建立强健的基础设施网络；澳大利亚发布《澳大利亚网络安全战略》，重视国家重要基础设施；以色列发布“前进2.0”网络安全产业计划，重视工业系统安全。

2.我国工业互联网平台安全顶层设计

一方面，出台**政策文件**指导工业互联网平台安全保障体系建设。2017年，国务院发布《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，提出要加强安全防护能力，重点突破工业互联网平台安全等产品研发，建立与工业互联网发展相匹配的技术保障能力。2018年，工信部印发《工业互联网平台建设及推广指南》提出要完善工业互联网平台安全保障体系，制定完善工业信息安全管理等政策法规，明确安全防护要求。同年，发布《工业互联网平台评价方法》，将安全可靠作为评价工业互联网平台安全能力的一个方面，要求在平台中建立安全防护机制，确保关键零部件和软件应用安全可靠。2019年，工信部等十部门印发《加强工业互联网安全工作的指导意见》，指出要支持工业互联网安全

科技创新，加大对工业互联网安全技术研发和成果转化的支持力度，强化平台安全等相关核心技术研究。2020年3月4日，中共中央政治局常务委员会在会议中强调，要加快新型基础设施建设进度，工业互联网等七大领域被纳入“新基建”体系。3月20日，工信部发布《关于推动工业互联网加快发展的通知》，提出要加快健全安全保障体系，完善安全技术监测体系，健全安全工作机制，加强安全技术产品创新，督促指导企业提升安全水平。

另一方面，加速推进工业互联网平台安全**标准化**工作。2019年，信安标委发布《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）》，明确工业互联网平台各层次的安全管理与安全技术防护要求，并提出相应的安全评估方法。国家烟草专卖局率先召集烟草领域、安全领域专家形成《烟草行业卷烟制造工业互联网平台通用技术要求标准（草案）》，对中国烟草总公司及各下属单位卷烟制造工业互联网平台安全要求进行规定。此外，国家工业信息安全发展研究中心2019年发布《工业信息安全标准化白皮书》，对构建工业互联网平台安全标准体系等提供指导。

（二）工业互联网平台安全建设发展多样化

我国工业互联网平台已经从概念普及进入实践深耕阶段，国内各大主流平台逐步实现了用户、设备、产品和企业的全方位连接，平台安全体系建设取得初步成效。当前，国内工

业互联网平台安全处于工业企业、平台企业、安全企业、互联网企业、硬件企业多方共建状态。

1.工业企业自建工业互联网平台并实施安全加固

龙头工业企业和大型智能制造公司面向工业转型发展需求构建工业互联网平台，同步实施安全加固。从综合安全防护的角度出发，在平台各层次及数据方面部署相应安全防护措施。例如，中国航天科工集团旗下航天云网Indics工业互联网平台，构建了涵盖设备、网络、控制、应用、数据的完整安全保障体系。海尔COSMOPlat工业互联网平台自主研发海安盾安全防护系统，以工业IaaS层的虚拟化安全、主机安全为重点，形成集态势感知、业务系统安全分析、漏洞发现为一体的安全解决方案。

2.平台企业输出具备一定安全能力的工业互联网平台

大型制造企业及互联网企业依托自身特色打造工业互联网平台，孵化独立运营的平台服务，向其他企业输出具备一定安全能力的工业互联网平台。例如，寄云科技NeuSeer工业互联网平台为能源化工企业提供安全生产管控能力，降低安全管理的人工依赖，提升安全管理水平。树根互联根云平台聚焦PaaS和SaaS层安全，支持平台主机、应用的安全审计和工业APP上线前安全检测与加固。东方国信Cloudiip工业互联网平台支持海量大数据的接入、存储、分析和模型共享，并保障数据安全。阿里云工业互联网平台将安全技术

进行解构、重组，打造完整、可靠、可信的安全生态系统，提升平台服务的内生安全能力。浪潮云洲工业互联网平台发布云数据铁笼IDS，为多方安全计算场景提供第三方支持和服务，解决数据隐私泄露问题，并提供基于区块链的数据计算全流程安全审计。

3.安全企业输出平台安全解决方案

安全企业利用自身积累的安全经验为工业互联网平台提供安全解决方案，除提供资产测绘、杀毒软件、防火墙、入侵检测、流量审计、安全监测等传统安全软件外，还通过SaaS服务模式输出安全能力，为工业互联网平台提供技术支撑。例如，阿里云盾提供了DDoS防护、主机入侵防护、Web应用防火墙、态势感知等一站式安全产品及服务，助力提升工业互联网平台安全防护水平。360、启明星辰等安全厂商为航天云网Indics工业互联网平台建立病毒库、漏洞库及防护工具库，支持平台入侵检测、漏洞扫描和主动防御。长扬科技打造了工控安全评估、工控等保检查、工业防火墙、工控主机卫士、统一安全管理、安全态势感知等多种安全产品，支持工业互联网平台安全防护。

4.互联网企业输出集成安全能力的平台系统及软件

互联网企业依托系统、软件专精优势，为工业互联网平台提供安全的操作系统、虚拟化软件、数据库、大数据分析模型等。例如，东土科技发布了Intewell工业互联网操作系

统，依托国产自主、安全可靠的“道系统”，面向智能装备、智能制造等多领域提供国产设备软件基础运行平台。以阿里云关系型数据库为代表的安全数据库、以阿里云大数据计算服务为代表的安全大数据服务和安全虚拟化系统也在业界广泛使用。

5.硬件企业研发集成安全能力的硬件设备

设备安全是确保工业互联网平台上层系统及软件安全的基础，硬件企业研发集成安全能力的工业控制设备、安全路由、安全网关、安全边缘节点、可信服务器等，为工业互联网平台提供基于硬件的安全防护能力。例如，中电智科面向国家重要基础设施应用，研发了安全增强型PLC，可满足各种控制规模、不同安全要求的自动化应用场景。华为、深信服等研发了安全网关、安全路由器，增强工业网络及平台网络的通信安全性。大唐高鸿依托其自主研发的硬件平台，搭载国产可信芯片，研制了可信服务器，为用户构建从基础设施层到应用系统层的安全计算环境。

（三）我国工业互联网平台安全能力现状

工业互联网平台是业务交互的桥梁和数据汇聚分析的中心，联结全生产链各个环节实现协同制造，平台高复杂性、开放性和异构性的特点加剧了其所面临的安全风险。

1.工业互联网平台是网络攻击的重要目标

CNCERT发布的《2019年我国互联网网络安全态势综述》指出，我国根云、航天云网、OneNET、COSMOPlat、奥普云、机智云等大型工业互联网平台，持续遭受来自境外的网络攻击，平均攻击次数达90次/日，较上一年（2018年）提升了43%，攻击类型涉及远程代码执行、拒绝服务、Web漏洞利用等。

2018年工信部对20家典型工业互联网龙头企业的213个重要工业互联网平台开展安全检查评估发现，平台企业用户普遍认为业务上云的同时网络安全责任“一迁了之”，漠视安全漏洞，对已知已报漏洞尤其是弱口令、跨站攻击、恶意程序注入等常见漏洞未及时跟踪处置；对外包云服务的安全管控意识不强，对云平台、办公网及生产控制网互联互通后的整体安全态势感知能力不足。2019年工信部组织的对某典型工业互联网平台攻防演练活动中，攻击方探测到平台各类信息化系统100多个，发现高危漏洞20多个，通过利用漏洞可获得平台内网系统控制权、窃取敏感信息，以此为跳板，进而对内网其他设备、系统和网络发起渗透，最终可导致企业工业互联网平台及相关设备网络瘫痪。

2.工业互联网平台安全能力的侧重点与薄弱点

本白皮书编制组设计了工业互联网平台安全能力评价模型，对我国典型工业互联网平台现有安全能力进行调研，分析结果如表1所示。

表1. 典型工业互联网平台安全能力侧重点与薄弱点

平台对象	安全能力侧重点	安全能力薄弱点
工业数据	数据加密传输、数据加密存储等	工业数据分类分级、细粒度访问控制、敏感数据识别和保护等
工业应用层	身份认证、权限控制、安全审计等	工业应用安全加固、统一安全运维、应用日志分析等
工业云平台服务层	数据访问控制、安全服务组件、接口安全等	微服务组件安全、工业应用开发环境安全等
工业云基础设施层	抗DDOS攻击、访问控制、边界网络安全、云主机杀毒等	虚拟机流量流向可视化，云内网络威胁隔离机制，虚拟化软件安全等
边缘计算层	设备接入认证、网络安全审计、通信加密策略安全防护等	边缘设备可信验证、工业协议深度解析、对接不同厂商端侧设备等

工业数据安全能力侧重于数据加密传输、加密存储等，在数据分类分级、访问控制、敏感数据识别和保护等方面较为薄弱。

工业应用层安全能力侧重于身份认证、权限控制、安全审计等，在应用安全加固、统一安全运维等方面还有待提高。

工业云平台服务层安全能力侧重于数据访问控制、安全服务组件、接口安全等，在微服务组件安全、工业应用开发环境安全等方面较为薄弱。

工业云基础设施层安全能力侧重于抗DDoS攻击、访问控制、边界网络安全、云主机杀毒等，在虚拟机流量流向可视化、云内网络威胁隔离机制、虚拟化软件安全等方面还有待提高。

边缘计算层安全能力侧重于设备认证、网络安全审计、通信加密等，在设备可信验证、工业协议深度解析、对接不同厂商端侧设备等方面较为薄弱。

3.工业互联网平台安全管理存在不足

《加强工业互联网安全工作的指导意见》对建立安全管理制度、落实安全责任做出明确规定。但是，我国企业在工业互联网平台安全管理方面仍存在一定不足:

一是安全管理制度不完善。工业互联网企业普遍缺乏针对平台安全建设、供应商安全要求、安全运维、安全检查和培训等的安全管理制度，安全责任落实不明晰，对内部人员缺乏有效安全管控。

二是安全投入缺乏。工业互联网企业对工业互联网平台安全投入较少，专职安全防护的人员较少，普遍存在“重功能、轻安全”的现象。

三是安全配置管理不足。当前工业互联网平台安全配置

管理严重依赖人工，自动化智能化程度不足，缺乏快速有效的安全配置检测预警机制，一旦出现配置错误，无法及时发现和启动相应安全措施。

四是安全建设考虑不全面。工业互联网平台在设计、开发、测试、运行和维护各阶段缺乏相应的安全指导规范，未将安全融入平台建设的整个生命周期中。

三、工业互联网平台安全需求与边界

当前产业界和学术界已经开始认识到工业互联网平台安全的重要性和价值，并开展了积极的探索，但是目前平台安全仍处于产业发展初期，缺乏系统性研究。本白皮书就工业互联网平台安全的需求特征进行分析，对工业互联网平台安全边界进行限定，为提出工业互联网平台安全参考框架奠定基础。

（一）工业互联网平台安全需求特征

1.海量、异构工业设备接入及设备资源受限的特征

接入设备海量，爆发式增长。一方面，工业设备在设计之初一般缺乏安全考虑，自身安全防护能力薄弱，海量工业设备接入工业互联网平台后，一旦被攻击者利用向平台发起跳板攻击，影响后果将成倍放大。另一方面，工业互联网平台边缘层缺乏对海量工业设备的状态感知、安全配置自动化更新和主动管控机制，导致利用海量工业设备发起的APT攻击感染面更大、传播性更强。因此，工业互联网平台需要行之有效的工业设备接入方案，保证接入的海量终端设备可信、可管、可控、可追溯。

接入设备异构，种类类型众多。海量异构工业设备接入工业互联网平台时，连接条件和连接方式多样，存在大量不安全的接口。当前工业互联网平台边缘层缺乏对异构工业设

备接入的安全管理，接口安全防护也有所欠缺。因此需要平台边缘层能突破异构工业设备的对接限制、互操作限制和管控限制，提供统一的安全接口自动部署及安全策略自动更新等能力。

终端设备资源受限。工业终端设备通常采用轻量化设计，存在计算、存储和网络资源等限制，且基于硬件的可信执行环境在工业边缘计算场景并未被大规模采用，这使得远离平台中心的终端设备容易遭受恶意入侵。因此需要提供轻量化的身份认证、可信验证、数据加密、隐私保护等高安全等级防护手段，增强终端设备的安全防护能力。

2.不同架构工业云协调运维、快速部署的特征

不同架构工业云协调运维。传统模式下，工业企业只需运维单服务器或数据库的安全，一旦出现问题，运维人员可以立即采取措施。但工业互联网平台涉及大量云端服务器、多类型数据库、甚至不同架构的工业云平台，在多系统、多应用、多云平台协同交互过程中，需要采用节约成本、处理快速、节省时间、社会化、信息化的运维模式，部署安全防护措施，优化安全配置，突破安全隔离、数据摆渡、网络行为审计等安全管控技术，加强工业互联网平台信息及操作权限管理，避免权限失控。

跨平台快速部署。工业生产围绕企业效益和排期进行统一安排，然而对缺乏安全防护的生产线，在初次部署安全措

施时，协调时间和生产线恢复生产的时间不能完全吻合，往往面临部分安装后需等待二次安装的尴尬境地，可能造成企业生产安全防护能力的降低和缺失，对工业互联网平台安全造成影响。因此，需要提供快速、高效、智能化的跨机器、设备、系统的安全措施快速部署机制。

3.工业微服务多样化、多服务复杂协同的特征

微服务多样化。工业微服务框架是以单一功能组件为基础，通过模块化组合实现“高内聚低耦合”应用开发的软件框架。工业生产涉及多种行业与产品，微服务的原子化特征可为不同业务提供重复利用的优势，但因工业体量庞大，且每个微服务作为独立的功能需求开发，导致多种微服务构建规则并存。因此构建安全的微服务，制定多样化微服务安全接入准则，是工业互联网平台安全的一项新挑战。

多服务的复杂协同。一方面，工业互联网平台微服务数量庞大，工业应用可能同时调用多个微服务完成特定业务，此时多服务之间需要复杂协同交互，需要采用集中认证和授权、双向SSL等方式来保证微服务通信过程的安全性；另一方面，工业微服务缺乏统一的标准化的构建规则，微服务与平台、应用及用户间缺乏安全接入、安全调用设计。因此，需要创新型的微服务安全标准化机制，解决微服务与平台、应用及用户之间的相互信任问题。

4.工业应用协同工作、开放定制的特征

多应用灵活协同工作。工业互联网平台上，不同业务流程中存在多样化的工业应用。一方面，存在大量应用间数据安全共享与协同处理的场景，需要根据数据共享需求对各应用、用户进行细粒度访问控制；另一方面，为保证应用之间鉴权的合理性，防止出现跨应用的攻击，需要明确区分工业应用的功能和权限，保证平台的应用安全。

应用研发的开放化、定制化。伴随工业互联网平台开放性的提升，工业应用研发创新能力增强，呈现开放定制的特征。工业互联网平台上存在大量未知的应用发布者，可以为用户提供差异化、个性化功能的工业应用，为保证工业应用来源的安全、可靠，需要对应用开发者的身份信息进行核实与展示，对工业应用进行全生命周期的安全管理、运行时监控和安全审计。

5.工业数据多源异构、大规模访问与共享的特征

海量多源异构数据的聚合计算。工业数据包括平台运营数据、企业管理数据等，具有体量大、种类多、来源广、结构差异大、行业差异大等特征。工业数据的多源性扩大了数据的攻击面，工业数据的异构性增加了海量数据融合分析的难度。因此，需要针对工业数据来源多样、类型不统一、质量要求高等特点，突破多源异构工业数据的安全融合分析技术，实现多源异构数据汇聚利用与数据保护。

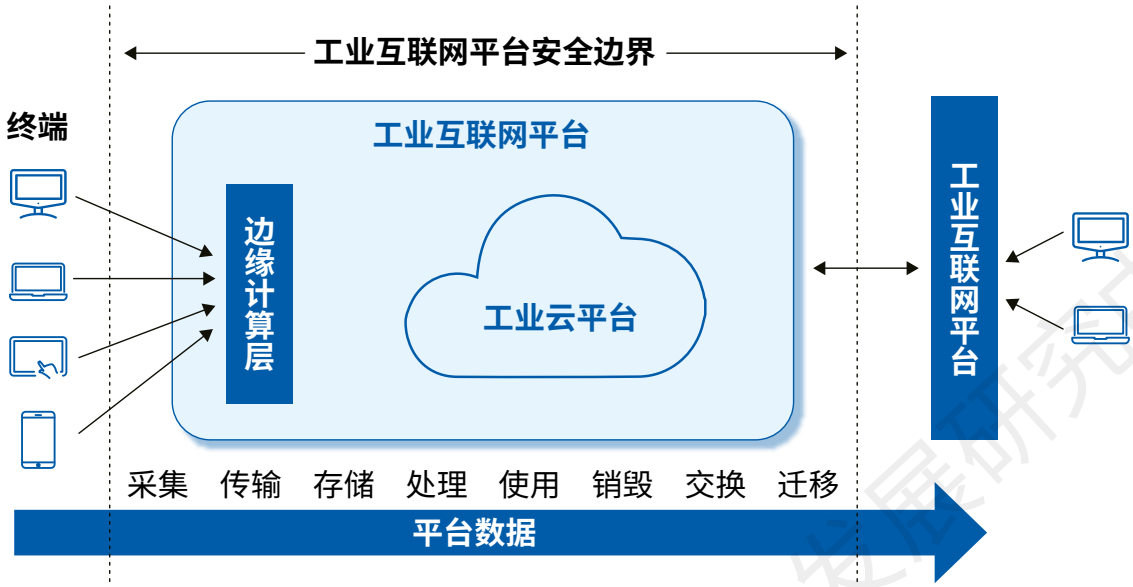
大规模数据的细粒度访问控制。工业应用场景中，由于工业生产流程、生产工艺的不同，要求不同的用户仅能访问自己所涉及工艺范围内的数据。面对海量工业数据，现有基于用户身份或角色的访问控制策略难以细粒度控制数据授权范围，亟需创新工业互联网平台大规模数据的用户访问控制策略，加强工业互联网平台数据的安全管理和审计。

共享的工业数据中包含大量敏感信息。工业数据包括研发设计、开发测试、系统设备资产信息、控制信息、工况状态、工艺参数、系统日志、物流、产品售后服务等产品全生命周期各环节所产生的各类数据，其中往往包含工业企业的商业JM。工业互联网平台上数据的流通与共享将扩大数据安全管理的范围，增加数据安全防护的难度和数据攻击事件分析的复杂度，需要针对数据滥用、隐私泄露等威胁进行安全防护。

（二）工业互联网平台安全边界

本白皮书工业互联网平台安全的范畴包括边缘计算层、工业云平台和平台数据，如图1所示。

图1. 工业互联网平台安全边界



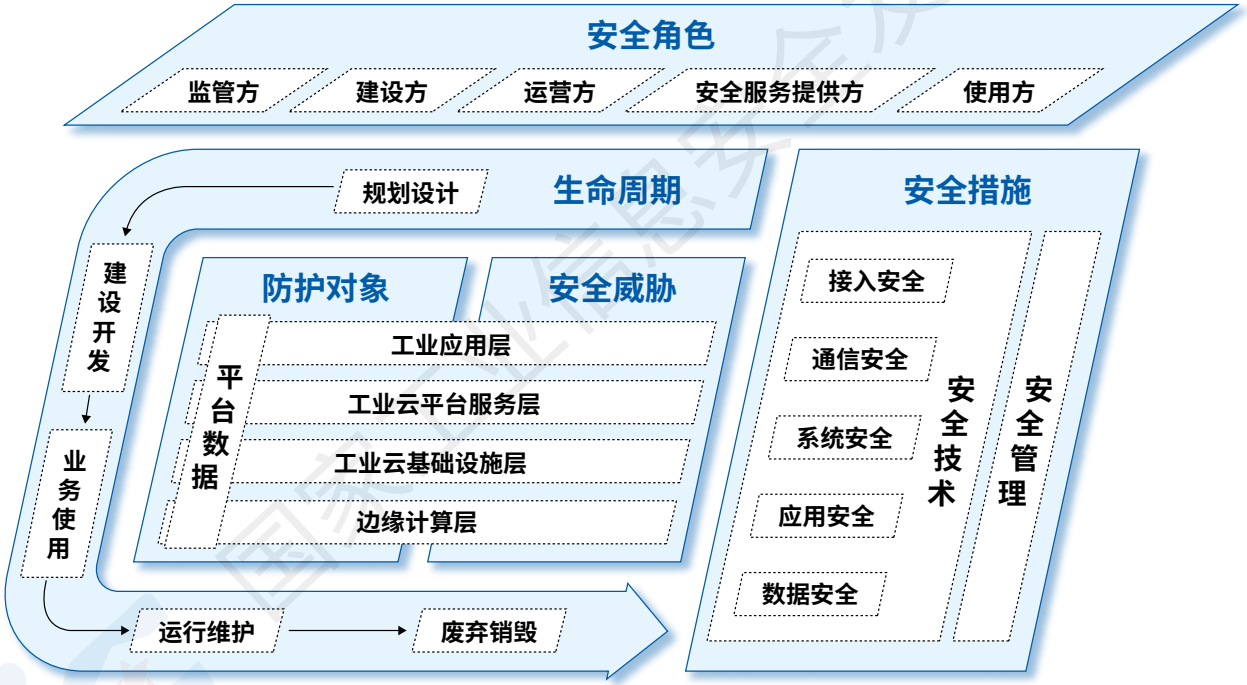
边缘计算层对多源异构终端设备、系统的数据进行实时高效采集和云端汇聚，其安全防护的范围包括终端设备安全接入、协议解析、边缘数据采集传输等过程（不包括边缘节点及边缘网络）。工业云平台是工业互联网平台提供大数据处理、工业数据分析、工业微服务、工业应用等创新功能的主体，其安全防护的范围包括工业云基础设施层、工业云平台服务层、工业应用层所涉及的设备、系统、应用、数据等。工业互联网平台促进了工业数据的分析、流动与共享，释放了数据的潜在价值，根据数据在平台上生命周期阶段的不同，平台数据安全防护的范围包括设备接入、平台运行、工业APP应用、平台迁移等过程中生成和使用的数据。

四、工业互联网平台安全参考框架

本白皮书从防护对象、安全角色、安全威胁、安全措施、生命周期五个视角提出工业互联网平台安全参考框架，明确防护对象，厘清安全角色，分析安全威胁，梳理安全措施，提出全生命周期的安全防护思路。

工业互联网平台安全参考框架如图2所示。

图2. 工业互联网平台安全参考框架



（一）安全防护对象视角

工业互联网平台包括边缘计算层、工业云基础设施层、工业云平台服务层、工业应用层和平台数据五大防护对象。

工业互联网平台安全防护对象如图3所示。

图3. 工业互联网平台安全防护对象

1.边缘计算层

边缘计算层通过现场设备、系统和产品采集海量工业数据，依托协议转换，通过边缘计算设备实现多源异构底层数据的归一化和汇聚处理，并向云端平台集成。边缘计算层安全防护对象可进一步细化包括：通信协议、数据采集与汇聚、设备接入等。

2.工业云基础设施层

工业云基础设施层主要通过虚拟化技术将计算、网络、存储等资源虚拟化为资源池，支撑上层平台服务和工业应用的运行，其安全是保障工业互联网平台安全的基础。工业云基础设施层安全防护对象可进一步细化包括：虚拟化管理软件、虚拟化应用软件、服务器、云端网络、存储设备等。

3.工业云平台服务层

工业云平台服务层利用通用PaaS调度底层软硬件资源，通过容器技术、微服务组件等提供工业领域业务系统和具体应用服务，为工业应用的设计、测试和部署提供开发环境。工业云平台服务层的安全与工业应用的安全具有非常强的相关性，是保障工业互联网平台安全的关键要点。工业云平台服务层安全防护对象可进一步细化包括：通用PaaS环境、工业大数据系统、工业应用开发环境、工业微服务组件、工业数据模型、容器镜像等。

4.工业应用层

工业应用涉及专业工业知识、特定工业场景，集成封装多个低耦合的工业微服务组件，功能复杂，缺乏安全设计规范，容易存在安全漏洞和缺陷。工业应用是工业互联网平台安全的重要防护对象，其安全水平是平台各层安全防护能力的“外在表现”。工业应用层安全防护对象可进一步细化包括：工业知识库、工业应用接口、应用配置、第三方依赖库、Web服务等。

5.工业数据

工业数据的实时利用是工业互联网平台最核心的价值之一，通过大数据分析系统解决控制和业务问题，能减少人工决策所带来的不确定性。根据《工业数据分类分级指南（试行）》，工业数据包括研发、生产、运维、管理等数据域，是工

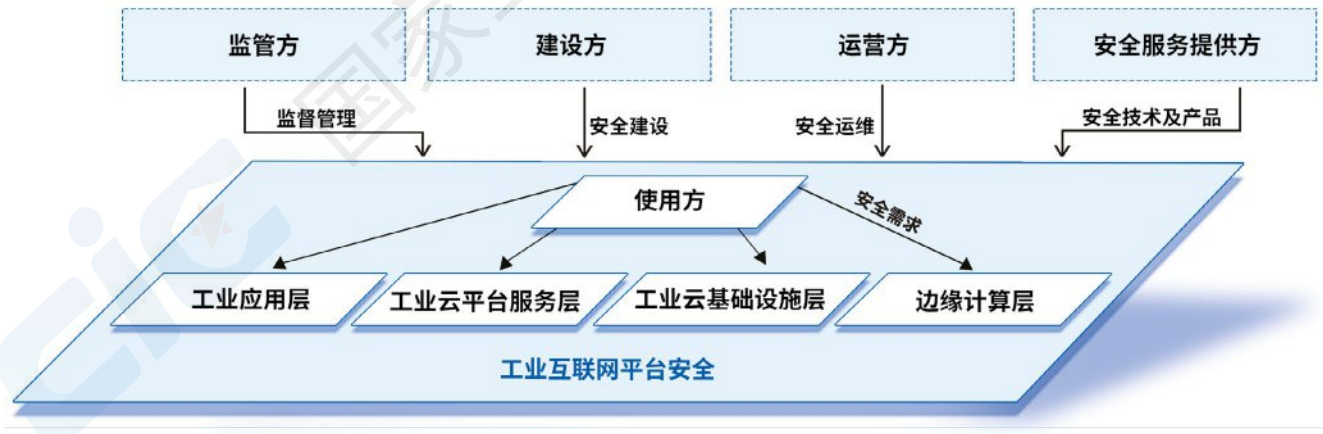
业互联网平台安全的重要防护对象。工业数据安全防护对象可进一步细化为数据生命周期的各个环节：采集、汇聚、传输、存储、迁移、分析、交互与共享、销毁等。

（二）安全角色视角

工业互联网平台安全与平台企业、工业企业、第三方开发者、用户等多个参与方息息相关，明确各方的职责是保障平台安全的前提。本安全参考框架中，将工业互联网平台安全相关参与方分为五个角色：监管方、建设方、运营方、安全服务提供方和使用方，每个角色可以由一个或多个实体（个人或机构）担任，每个实体也可能同时担任多个角色。

工业互联网平台安全角色如图4所示。

图4. 工业互联网平台安全角色



1.监管方

政府作为监管机构履行监督管理职责。工业和信息化部组织开展工业互联网平台安全相关政策制定、标准研制等工作，明确平台安全防护要求和安全评估规范，对平台安全工作开展总体指导。地方工信主管部门负责对本行政区域内工业互联网平台的安全监管工作，组织开展平台安全评估，提升平台漏洞发现、安全防护和应急处置能力，防范安全隐患。

工业互联网平台企业按照属地原则接受当地监管机构的指导和监督，强化企业安全主体责任，保障平台安全运行。

2.建设方

建设方需按照国家相关标准要求，确保所交付的工业互联网平台满足客户的安全要求。工业互联网平台建设方应围绕平台安全的总体目标和规划，根据平台安全建设开发标准和规范，通过技术和管理手段，完成工业互联网平台应用组件、产品和功能的开发，提供技术和服务支持，确保平台具备国家及行业标准规定的安全防护水平。

3.安全服务提供方

安全服务提供方是保障工业互联网平台安全运行的第三方服务者，涉及到保障平台安全正常运行的各个方面，如电力供应商、基础设施安全供应商、安全硬件供应商、安全软件供应商、网络安全解决方案提供商等，负责提供平台设

备、系统、应用安全运行所需要的安全技术、产品和服务，确保平台具备认证、加密、监测、检查、评估、响应等安全能力。各安全服务提供方需按照相关政策和标准提供符合安全要求的服务，保障工业互联网平台安全、稳定运行。

4.运营方

运营方落实工业互联网平台安全主体责任。按照“谁运营谁负责”的原则，企业依法落实平台安全的主体责任，明确工业互联网平台安全责任部门和责任人，负责平台安全运维，包括但不限于平台安全认证、检查评估、安全审计及平台安全事件的监测、预警、响应和恢复等，建立安全事件报告和问责机制，加大安全投入，部署有效的安全防护措施。

5.使用方

使用方利用工业互联网平台开展相关业务时，应按照平台安全规范正常操作。使用方是使用平台产品、应用和服务的主体，可以是工业企业、平台企业、团体机构或个人。使用方应根据业务需要对工业互联网平台提出具体的安全需求，并在使用过程中遵守平台安全规范，进行安全配置管理，避免在使用过程中为平台带来安全威胁。

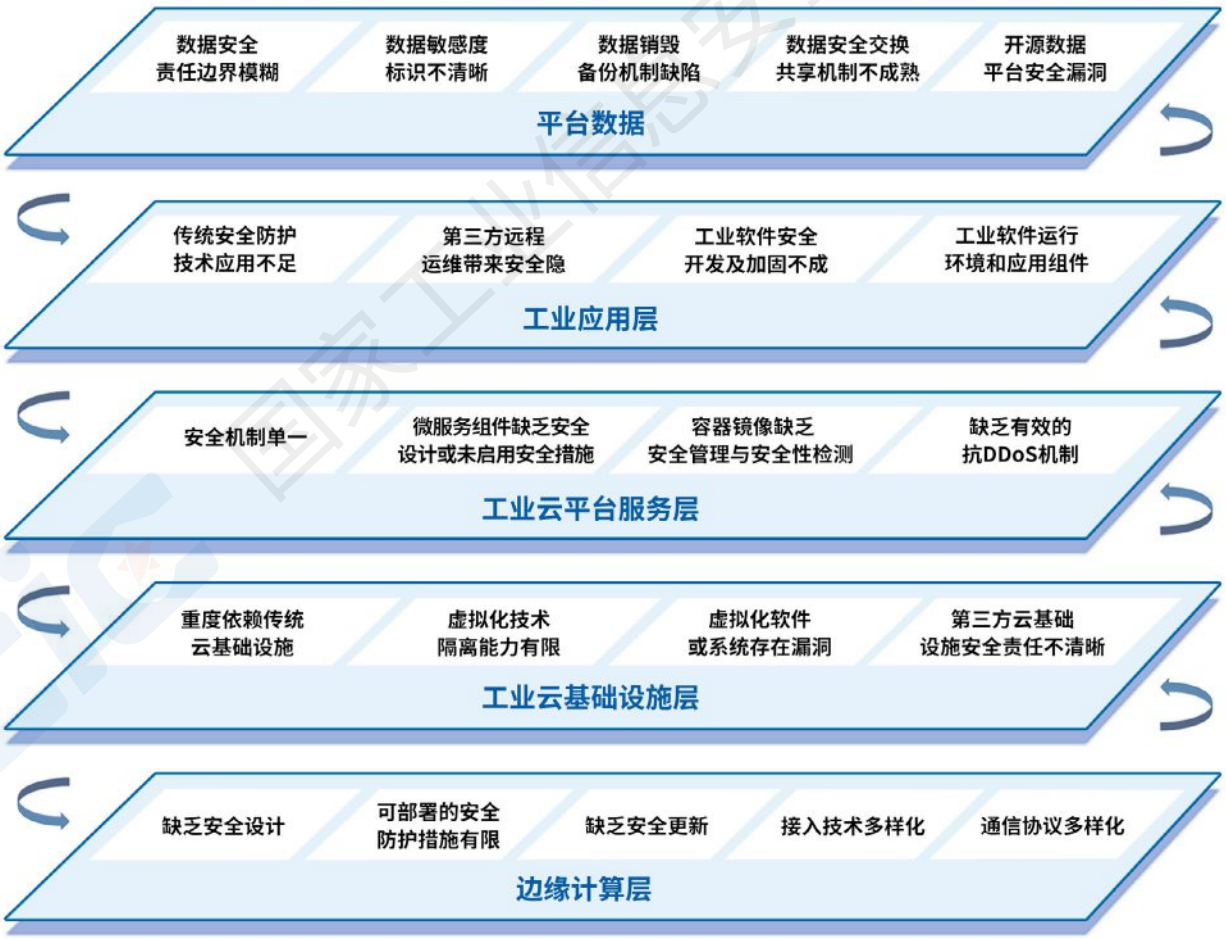
工业互联网平台的安全稳定运行离不开监管方、建设方、安全服务提供方、运营方和使用方等多个角色的协作。监管方对工业互联网平台进行监督管理，建设方按照相关标准开展安全建设，安全服务提供方为保障平台安全提供技术和

产品支持，运营方对平台进行安全维护，使用方对平台提出安全需求，并进行安全使用。工业互联网平台安全需所有相关方共同落实，在运行过程中，各方仍需加大责任意识和安全意识，共同保障工业互联网平台的安全。

（三）安全威胁视角

安全威胁视角分析了工业互联网平台五个层面面临的不同安全威胁，如图5所示。

图5. 工业互联网平台安全威胁



1.边缘计算层

一是边缘计算层设备普遍缺乏安全设计。边缘计算层设备地理位置分散、暴露，多通过物理隔离进行保障，普遍缺乏身份认证与数据加密传输能力，自身安全防护水平不足。攻击者容易对设备进行物理控制和伪造，并以此为跳板向其他设备与系统发动攻击。

二是边缘计算层设备可部署的安全防护措施有限。边缘计算层设备和软件存在低功耗、低时延等性能需求，资源受限，开发时往往只重视功能需求，导致可部署的安全防护措施有限。由于边缘设备海量，当遭到APT恶意攻击时，感染面更大、传播性更强，很容易蔓延到大量现场设备和其他边缘节点。

三是边缘计算层设备缺乏安全更新。出于稳定性和可靠性考虑，边缘计算层设备和软件部署后一般不升级，大量固件和软件开发较早，存在长期不更新、产品服务商不提供维护服务甚至已停止服务的情况，不可避免地存在安全漏洞，加剧网络攻击风险。

四是接入技术多样化增加安全防护难度。连接工业互联网平台进行维护、管理的边缘计算层设备呈指数级增长，在众多接入场景和需求的驱动下，接入技术不断更新，给平台边缘计算层接入安全防护带来新的挑战。

五是通信技术多样化成为安全防护新难点。边缘节点与海量、异构、资源受限的工业现场设备大多采用短距离无线通信技术，边缘节点与云平台采用的多是消息中间件或网络虚拟化技术，多样化的通信技术对边缘计算层消息JM性、完整性、真实性和不可否认性等的保障带来很大的挑战。

2.工业云基础设施层

一是工业互联网平台存在与传统云平台相同的脆弱性。现有工业互联网平台重度依赖底层传统云基础设施的硬件、系统和应用程序，一旦底层设备或系统受损，必然对平台上层的应用和业务造成重大影响，可能导致系统停顿、服务大范围中断等后果，使工业生产和企业经济效益遭受严重损失。

二是虚拟化技术提供的安全隔离能力有限。工业云基础设施层通过虚拟化技术为多租户架构、多客户应用程序提供物理资源共享能力，但虚拟化技术提供的隔离机制可能存在缺陷，导致多租户、多用户间隔离措施失效，造成资源未授权访问问题。

三是虚拟化软件或虚拟机操作系统存在漏洞。工业云基础设施层虚拟化软件或虚拟机操作系统一旦存在漏洞，将可能被攻击者利用，破坏隔离边界，实现虚拟机逃逸、提权、恶意代码注入、敏感数据窃取等攻击，从而对工业互联网平台上层系统与应用程序造成危害。

四是第三方云基础设施安全责任边界不清晰。多数平台企业采购第三方云基础设施服务商提供的服务建立工业互联网平台，在考虑平台安全防护时，存在工业互联网平台安全责任边界界定不清晰的问题。

3.工业云平台服务层

一是传统安全手段无法满足多样化平台服务的安全要求。工业云平台服务层包括工业应用开发测试环境、微服务组件、大数据分析平台、工业操作系统等多种软件栈，支持工业应用的远程开发、配置、部署、运行和监控，需要针对多样化的平台服务方式创新、定制安全机制。当前工业互联网平台一般采用传统信息安全手段进行防护，无法满足多样化平台服务的安全要求。

二是微服务组件缺乏安全设计或未启用安全措施。工业云平台服务层微服务组件与外部组件之间的应用接口或者缺乏安全认证、访问控制等安全设计，或者已部署接口调用认证措施但不启用，容易造成数据非法窃取、资源应用未授权访问等安全问题。

三是容器镜像缺乏安全管理以及安全性检测。容器镜像是工业互联网平台服务层中实现应用程序标准化交付、提高部署效率的关键因素。但是，一方面，若容器镜像内部存在高危漏洞或恶意代码，未经安全性检测即被分发和迭代，将造成容器脆弱性扩散、恶意代码植入等问题；另一方面，容

器镜像管理技术不完善，一旦被窃取，容易造成应用数据泄露、山寨应用问题。

四是缺乏有效的拒绝服务攻击防御机制。工业云平台服务层承载着工业数据分析与建模、业务流程决策与指导等工业互联网平台的核心工作，对服务的可靠性和可持续性有较高要求。当前工业云平台服务层仍缺乏有效的拒绝服务攻击防御机制，攻击者可轻易实现拒绝服务攻击，造成资源耗尽、网络瘫痪等后果。

4.工业应用层

一是工业应用层传统安全防护技术应用力度不足。当前工业应用层的软件重视功能、性能设计，对鉴别及访问控制等安全机制设计简单且粒度较粗，攻击者可通过IP欺骗、端口扫描、数据包嗅探等通用手段发现平台应用存在的安全缺陷，进而发起深度攻击。

二是第三方远程运维带来安全隐患。工业应用层中涉及到的大量控制系统和软件来自国外品牌，服务商通过远程运维的方式接入工业互联网平台，一旦第三方远程运维业务流程存在安全缺陷，将对工业互联网平台带来安全隐患。

三是工业应用安全开发与加固尚不成熟。当前工业应用安全开发、安全测试、安全加固等技术研究仍处于探索起步阶段，业内尚未形成成熟的安全模式和统一的安全防护体系。

四是工业应用组件存在安全风险。一般而言，工业应用基于C/C++、C#、JAVA、Python等语言进行开发，其组件多采用Weblogic等编程框架，可能由于内存结构、数据处理、环境配置及系统函数等设计原因，导致内存溢出、敏感信息泄露、隐藏缺陷、反序列化漏洞等问题，进而造成上层应用调用组件时出现强制性输入验证、信息泄露、缓冲区溢出、跨站请求伪造等威胁，甚至会造成软件运行异常和数据丢失。

5.工业数据

一是数据安全防护责任边界模糊。工业数据具有体量大、种类多、关联性强等特点，流经工业互联网平台多个层次，在采集、传输、存储、处理、使用等多个环节中涉及到的责任人众多，工业互联网平台上工业数据安全防护的主体责任边界模糊，难以界定。

二是敏感数据标识及保护技术待完善。工业数据包含研发、生产、运维、管理等数据信息，在不同应用场景下，数据的价值不同，敏感程度也不同，如果不能对数据敏感度进行准确识别和有效分类，将无法实现对敏感数据的细粒度标识。工业数据投入使用时，还需要根据业务场景对工业数据进行脱敏处理，当前平台仍缺乏完善的数据脱敏和隐私保护措施，工业数据使用过程中存在敏感信息泄露等安全问题。

三是数据销毁及备份机制存在缺陷。工业互联网平台服务商在将资源重新分配给新用户时，若对存储空间中的数据

没有进行彻底擦除，将造成用户数据泄露风险。此外，平台服务提供商若未制定数据备份策略，定期对数据进行备份，则在用户数据丢失时难以保证能及时恢复。

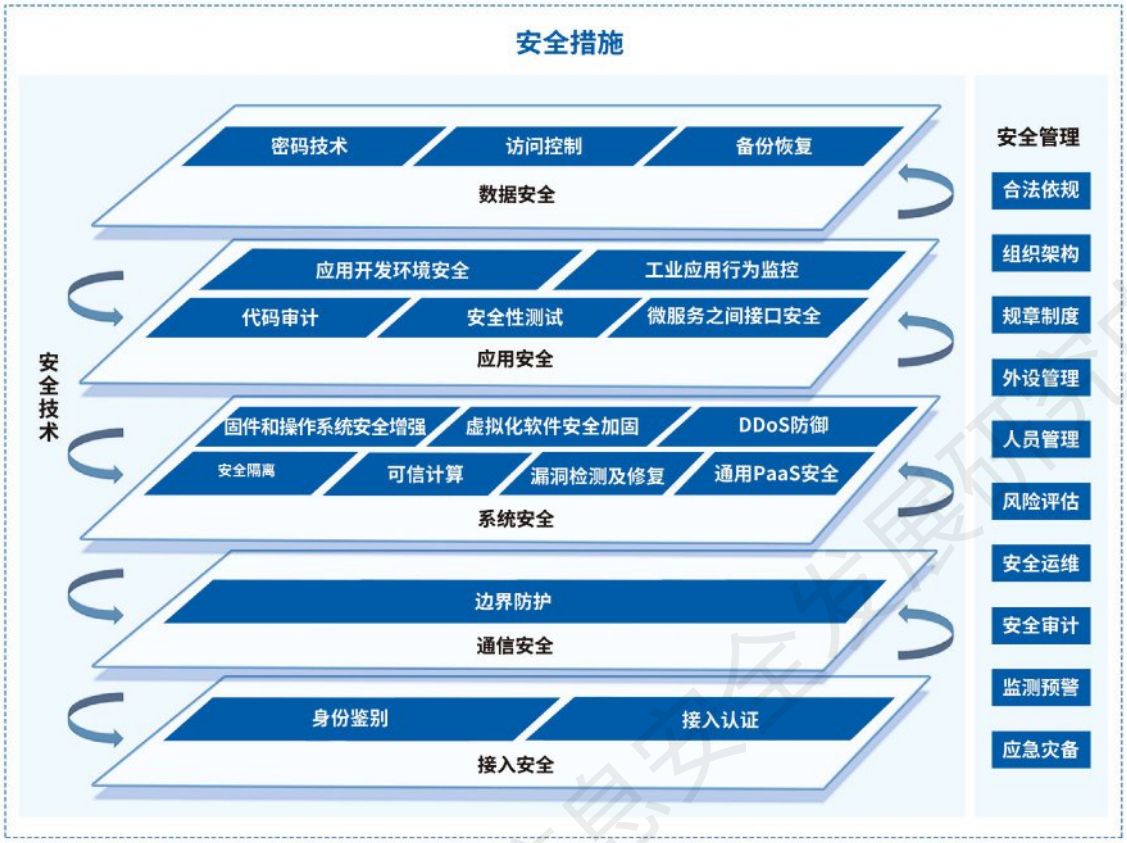
四是数据安全共享交换机制尚不成熟。在工业大数据分析决策过程中，通常需要联合多方数据进行计算或训练模型，当前工业互联网平台数据安全共享交换机制尚未成熟，平台大数据安全分析技术仍有待研究。

五是开源数据平台存在安全漏洞。工业大数据分析系统作为工业互联网平台数据汇集、分析和决策的重要工具，需要较高的安全能力。但是当前大数据分析系统主要基于开源软件（大数据存储和计算框架）进行部署，一旦存在安全漏洞，被攻击者利用，将造成分析结果被篡改、被伪造等问题。

（四）安全措施视角

针对工业互联网平台五个方面的安全威胁，防护措施视角从技术和管理的角度提出相应可落地的安全实施方案。安全技术包括通信安全、系统安全、应用安全和数据安全，安全管理通过制度和规范协同资源，保障安全技术的贯彻落实。工业互联网平台安全防护措施如图6所示。

图6. 工业互联网平台安全防护措施



1.安全技术

（1）通信安全

密码技术。采用密码技术保证通信过程中敏感数据的完整性和保密性，可支持国家商用密码算法。

身份鉴别。对登录工业互联网平台的用户进行身份鉴别，实现用户身份的真实性、合法性和唯一性校验，可支持通过多种标准协议对接客户自有第三方认证体系登录，包含但不限于OpenID Connect、OAuth 2.0、LDAP、SAML等。

接入认证。对接入工业互联网平台的设备进行认证，形成可信接入机制，保证接入设备的合法性和可信性，对非法设备的接入行为进行阻断与告警。

边界防护。在工业互联网平台内部不同网络区域之间，及平台与外部网络之间部署防火墙、软件定义边界（SDP）等边界防护产品，解析、识别、控制平台内部网络及平台与外部网络之间的数据流量，结合身份鉴别、访问控制等技术，抵御来自平台外部的攻击。

（3）系统安全

安全隔离。对工业互联网平台不同虚拟域、服务和应用都采用严格的隔离措施，防止单个虚拟域、服务或应用发生安全问题时影响其它应用甚至整个平台的安全性。

可信计算。应用可信计算技术，基于安全芯片，对工业互联网平台设备及软件进行可信加固，使之具备可信启动、可信认证、可信验证等能力。

漏洞检测及修复。工业互联网平台操作系统、数据库、应用程序在运行过程中，要定期检测漏洞，发现漏洞及补丁未及时更新的情况，并采取补救措施，对开放式Web应用程序安全项目（OWASP）发布的常见风险与漏洞能进行有效防护或缓解。

DDoS防御。在工业云平台部署DDoS防御系统，保证平台服务的可用性和可靠性。

固件和操作系统安全增强。对工业互联网平台设备固件及操作系统施加防护，提高其抗攻击能力。

虚拟化软件安全加固。对工业互联网平台虚拟化软件进

行安全性增强，确保其上虚拟域应用、服务、数据的安全性，为多租户提供满足需求的安全隔离能力。

通用PaaS资源调度安全。对工业互联网平台通用PaaS资源调度的相关服务进行安全加固，避免通用PaaS组件安全缺陷为平台引入安全威胁。

（4）应用安全

代码审计。对工业互联网平台系统及应用进行代码审计，发现代码中存在的安全缺陷，预防安全问题的发生。

安全性测试。工业应用在投入正式使用前，应进行安全性测试，尽早找到安全问题并予以修复。

微服务组件接口安全。提供API全生命周期管理，包括创建、维护、发布、运行、下线等，对平台微服务组件接口进行安全测试和安全加固，避免由于接口缺陷或漏洞为平台引入安全风险。

应用开发环境安全。确保工业云平台服务层应用开发框架、工具和第三方组件的安全，避免工业应用开发环境被恶意代码污染而造成安全隐患。

工业应用行为监控。对工业软件、服务的行为进行安全监控，通过行为规则匹配或者机器学习的方法，识别异常，进行告警或阻止高危行为，从而降低影响。

（5）数据安全

密码技术。对工业互联网平台敏感数据、用户及设备的

鉴别凭证数据（例如密钥等）、资源及应用访问控制策略等的存储和传输利用密码技术实施保护，保证平台关键数据、资源、应用的安全，能支持国家商用密码算法及各种密码应用协议，相关设计遵循《中华人民共和国密码法》等法规及标准。

访问控制。对工业互联网平台关键数据、资源及应用制定访问控制策略，并根据平台用户角色和业务流程的变更及时调整，确保平台对用户访问行为的细粒度控制和授权，可采用零信任技术保障平台身份鉴别和访问控制安全。

备份恢复。通过在线备份、离线备份或热备份等方式，对工业互联网平台系统、应用、服务、数据等进行备份，为防止平台出现安全事故导致业务中断的问题。

2.安全管理

安全管理。通过计划、组织、领导、控制等环节来协调人力、物力、财力等资源，促进保障工业互联网平台安全。

合法依规。在进行工业互联网平台安全管理时，依照国家的战略方针、各项政策、法律法规、标准规范采取措施。

组织架构。结合工业互联网平台安全防护对象的实际需要和相关规定，制定安全管理组织架构。

规章制度。根据工业互联网平台安全目标，制定安全管理策略，制定合理且可执行的规章制度，确保人员规范操作，保证安全技术正确实施。

外设管控。对工业互联网平台所涉及硬件设备接口进行严格管控，防止外部设备的非法接入。

人员管理。对工业互联网平台开发、建设、运行、维护、管理、使用的相关人员进行培训，熟悉安全标准和规范，减少由人员引入的漏洞和缺陷。

风险评估。对工业互联网平台各层次的安全性进行评价，对潜在的脆弱性和安全威胁进行研判，确定平台安全风险等级，制定针对性风险处理计划。

安全运维。对平台操作系统和应用进行定期漏洞排查，及时修复已公开漏洞和后门；对平台系统及应用进行安全性监测和审核，阻止可疑行为并及时维护；平台状态发生变更时及时进行安全性分析和测试。

安全审计。对工业互联网平台上与安全有关的信息进行有效识别、充分记录、存储和分析，对平台安全状态进行持续、动态、实时的审计，向用户提供安全审计的标准和结果。

监测预警。构建工业互联网平台安全情报共享机制，结合其它组织机构已公开的安全信息，实现平台风险研判、安全预警、加固建议等功能。

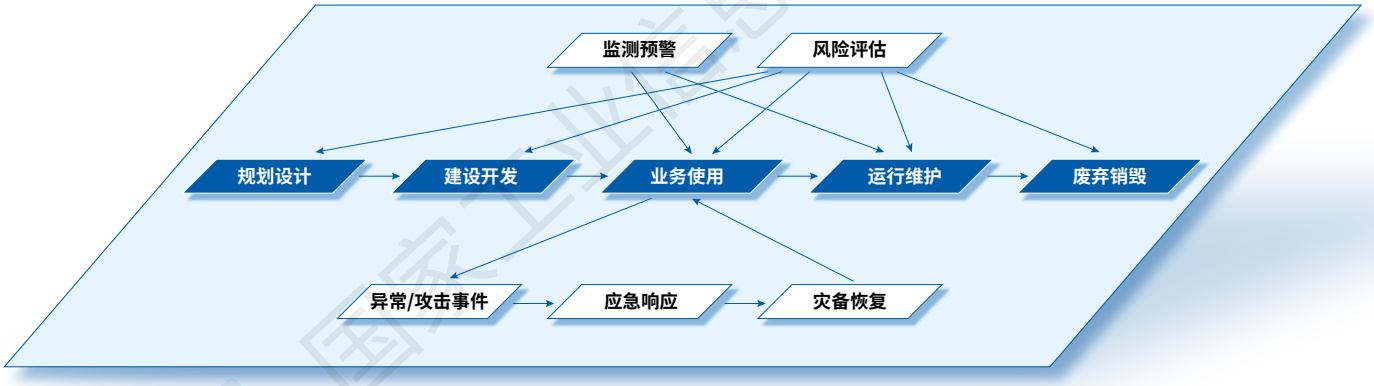
应急灾备。制定工业互联网平台安全应急预案，对平台应急相关人员提供应急响应培训，开展应急演练；制定灾备恢复指南，掌握平台安全事件发生的原因和结果，完成有效的技术处置和恢复，降低平台不可用造成的影响。

（五）生命周期视角

现有工业互联网平台建设普遍存在“重功能轻安全”的问题，未在平台开发初期引入安全设计。随着平台建设的深入，安全防护难度加大、安全风险加剧、安全建设成本超出预期，本安全参考框架从全生命周期安全防护的视角出发，将安全融入平台规划设计、建设开发、业务使用、运行维护和废弃销毁的各个阶段，提高工业互联网平台全生命周期的安全防护能力。

工业互联网平台安全生命周期如图7所示。

图7. 工业互联网平台安全生命周期



1.规划设计

工业互联网平台安全规划设计包括需求分析和方案设计两个环节。一是需求分析，要求确定平台安全的防护范围，不得随意更改，如果有确需新增或变更的需求，应组织专家评审后变更。二是方案设计，根据平台安全需求，设计工业互

联网平台安全方案；组织相关部门和安全专家对平台安全方案的合理性和正确性进行审定，经过批准后才能正式实施；建立平台安全风险衡量标准，形成平台安全定期衡量机制。

2.建设开发

工业互联网平台安全建设开发包括安全开发、安全性测试、部署实施、上线试运行四个环节。一是安全开发，应组建专业的平台安全建设开发团队，进行平台软硬件建设、开发、管理和审计等工作。二是安全性测试，平台设备、系统、软件建设开发完成后，完成完整的功能、性能和安全性测试，提交明确的测试方案、测试用例和测试报告。三是部署实施，在平台设备、系统、软件部署实施环节，应进行最小化部署，在部署方案中明确记录配置参数和配置文件，以供后期运维阶段作参考。四是上线试运行，在平台上线试运行环节，每个平台项目都要做第三方安全检测，明确并处置平台存在的安全风险。

注意，工业互联网平台须在国家相关主管部门进行备案，根据《中华人民共和国网络安全法》《GB/T22239-2019网络安全等级保护基本要求》等相关要求开展工业互联网平台安全建设，以使平台达到相应的安全防护要求。

3.业务使用

相关人员在使用工业互联网平台业务时，应确保人员操作符合平台安全规范。明确工业互联网平台使用人员的活动

目的、安全义务和安全责任，对相关人员的安全活动进行监督记录，要求关键人员签署保密协议，保证平台安全防护措施在业务使用过程中能正确发挥作用。

4.运行维护

工业互联网平台在其生命周期内，需要不断的维护和升级改进，以维护平台功能更新及安全稳定的运行。应组建专业的工业互联网平台安全运维机构及安全支撑服务团队，定期对平台设备、系统、应用进行风险评估、安全监测、安全审计、应急演练等工作，贯彻执行平台安全技术措施和安全管理制度；在平台发生安全事件时，进行应急响应和灾备恢复工作，保障平台业务的可用性和可靠性。

5.废弃销毁

工业互联网平台部分或全部设备、系统、应用、数据等发生废弃销毁时，要注意不影响平台其它业务的正常运行。废弃销毁流程符合国家、行业及企业的相关法律和流程，销毁过程中不发生敏感信息泄露问题。

在工业互联网平台生命周期中，风险评估应在平台规划设计、建设开发、运行维护、业务使用和废弃销毁全部五个环节贯彻实施，监测预警应在平台运行维护和业务使用两个环节贯彻实施。相关安全防护措施见本白皮书第四（四）节。

五、工业互联网平台安全关键技术

针对工业互联网平台的需求特征和面临的安全威胁，本白皮书汇编总结了提升工业互联网平台的关键技术，为保障工业互联网平台安全的建设方、运行方、安全服务提供方和技术研究人员等提供参考。

1.边缘设备可信接入技术

重点适用：边缘计算层

大量边缘设备采用有线或无线方式连接工业互联网平台，具有移动性、松耦合、频繁接入或退出的情况，导致边缘网络拓扑和通信条件不断变化，面临易受控制、伪造、不安全系统与组件等威胁。需研究边缘设备可信接入技术，在提供轻量级硬件或软件支持的设备身份识别、多因子安全接入认证、完整性验证与恢复等功能的同时，保障边缘设备低功耗、低时延等系性能要求。

2.通信协议安全增强技术

重点适用：边缘计算层

通信协议是设备与平台、用户与平台、平台与平台间完成通信或服务所必须遵循的规则和约定。当前，工业互联网平台存在大量数据通信，所采用的通信协议具有类型多样、明文传输等特点，需要在对现有生产环境影响最小的前提下，突破通信协议脆弱性分析、高效身份认证、细粒度授权和轻量级加密等技术，实现通信协议的安全性增强。

3.平台接入设备安全管控技术

重点适用：边缘计算层、工业云基础设施层

工业互联网平台接入设备具有种类异构、数量众多等特点，设备的策略分发、配置、性能监控等任务大多由人工完成，大量的设备监控和管理将耗费大量成本，不同类型设备的配置不统一还可能导致系统策略不一致，造成潜在的安全漏洞。需研究平台接入设备智能安全管控技术，提供平台接入设备安全管理、安全监控、安全策略自动化配置等功能，实现边缘设备自动化、智能化安全管控。

4.平台网络跨域信任技术

重点适用：工业云基础设施层

工业互联网平台中多网络安全域和多接入网络共存，攻击者利用被破坏的节点作为“跳板”，攻击平台网络中其他节点设备，可能造成威胁扩展。因此，需研究平台网络跨域信任技术，包括节点完整性验证、用户身份认证、接口安全、API调用安全、域间隔离审计等，避免单节点受损后跨域访问导致的网络威胁扩展问题，保障节点平台网络跨域访问时面临的域间相互信任和网络连接上下文安全。

5.“云网边端”协同的安全漏洞识别技术

重点适用：边缘计算层、工业云基础设施层、工业云平台服务层

漏洞识别是通过扫描、关联分析等手段，对目标系统缺

陷进行检测的行为。针对工业互联网平台接入设备海量、系统应用多样、网络协议复杂、服务交互频繁造成安全漏洞识别难度大、影响范围广的特点，需突破基于云、网、边、端协同的大数据分析、威胁信息共享、安全知识图谱等技术，实现对工业互联网平台设备、系统及应用的漏洞识别、分析、评估、检测与修补，从全局视角提升对漏洞的识别发现、理解分析、响应处置能力。

6.平台主机和虚拟机安全加固技术

重点适用：工业云平台服务层

工业互联网平台上层系统与应用安全重度依赖底层云主机及虚拟机的安全运行，针对越权、侧信道攻击、虚拟机操作系统漏洞、逃逸攻击、镜像篡改等风险，突破基于可信硬件的可信验证、白名单、基于AI的主动防御等技术，保护云主机与虚拟机系统及数据，以保证平台上层系统级服务的安全运行。

7.平台微服务安全调用与安全治理技术

重点适用：工业云平台服务层

工业互联网平台具有多样化的服务需求，一般将大型应用程序或服务分解为多个更小粒度的微服务，由各不同的团队并行独立开发和部署，在应对同一业务需求时调用多个微服务协同完成。需研究微服务安全协同调用技术，提供微服务接口安全验证、多微服务协同调用、微服务间安全通信、

微服务行为安全监控等功能，并对调用第三方微服务接口的通信进行安全审计和管控，提升工业互联网平台微服务的安全防护水平。

8.平台统一IoT态势感知技术

重点适用：工业云平台服务层

平台统一IoT态势感知是以边缘测IoT流量、关键网络节点流量、平台各系统日志等安全大数据为基础，对平台各层安全状态的实时统一监测，综合平台整体的安全监控数据，对平台潜在的安全风险及恶意攻击行为进行分析预警，并提供辅助性决策的一种技术。通过接入本地移动网、固网(采样)数据，实现工业互联网资产统一探测、全流量分析、风险识别、态势分析、预警通报、应急处置，同时实现基础数据管理功能、策略指令下发、情报库共享、信息推送等功能。

9.基于区块链的安全协作技术

重点适用：工业云平台服务层、工业应用层

区块链技术具有可信协作、隐私保护等优势，在应用到工业互联网平台时，能提升平台的安全性。基于区块链技术，为跨域集群建立业务共享通道，并利用高效共识机制协同更新分布式账本，能实现信息来源可信、数据可追溯审计和通道内部数据的传输和隐私安全。利用区块链不可篡改、分布式共治等赋能能力，对平台各节点构建联盟链，实现节点的自治性预防保障、运行时异常监测和受损状态的自愈合。

10.人工智能算法及系统安全保障技术

重点适用：工业云平台服务层

人工智能算法存在黑盒和白盒的对抗样本攻击，人工智能系统缺陷和漏洞也可能被攻击者利用，导致识别系统混乱、识别结果错误等安全问题。需从算法容错容侵、测试质量保障、安全配置、漏洞检测和修复等方面增强人工智能算法及系统的安全性，减缓攻击者针对人工智能算法及系统攻击成功的可能性。

11.工业应用安全检测技术

重点适用：工业应用层

传统软件漏洞、Web安全、API安全、第三方开发者植入恶意代码等问题威胁平台工业应用生态的安全发展。需面向特定工业行业、场景、业务的安全需求，研究工业应用安全检测技术，提供恶意代码分析、软件逆向、漏洞检测与利用、接口验证等功能，建立工业应用安全评估机制，及时发现工业应用接口、服务过程中可能存在的安全隐患，为部署针对性的工业应用安全防护措施提供依据。

12.多源异构工业数据清洗技术

重点适用：工业数据

数据作为工业互联网平台有效运行的重要基础生产资料，亟需着重攻克针对海量多源异构工业数据源的智能识别、爬取、适配、捕获、高速数据全映像等技术，实现对结构

化、半结构化、非结构化的海量工业数据的智能化识别、定位、跟踪、协议转换、分流及整合等，并针对工业互联网平台计算能力下沉到边缘侧的特点，重点突破数据有效抽取、清洗、去噪及转化技术，有效提升工业互联网平台边缘侧数据处理能力。

13.平台敏感数据识别保护技术

重点适用：工业数据

工业数据中包含工艺参数、生产运营数据等商业JM，若未根据数据分类分级结果进行敏感度标识，将可能造成数据管理混乱、敏感数据泄露的问题。针对此，亟需突破工业数据敏感度标识、细粒度访问控制、关键字段加密、轻量级加密共享等技术，结合国家商用密码算法保证敏感工业数据的JM性和用户访问的灵活性。

14.数据集可信性检测及防护技术

重点适用：工业数据

工业互联网平台安全、可靠地运行重度依赖数据集的有效性和正确性，数据在收集与标注时一旦出现错误或被注入恶意数据，将带来数据污染攻击，威胁依赖数据集训练的模型和算法的安全。需研究数据集可信性检测及可信防护技术，保障数据收集、传输阶段的真实性、完整性和可靠性，为后续数据分析的可信性奠定基础。

15.工业数据跨平台可信交换共享技术

重点适用：工业数据

随着工业互联网平台数据涉及范围的逐步扩大，业务场景对数据分析决策需求的多样化，工业数据跨平台开放共享、互联互通、协同分析等要求日益提高，进一步扩大了跨平台数据流通、交换、共享过程中的攻击面。亟需突破基于敏感度的数据安全域划分、数据跨域流动管控、动态数据安全交换共享、数据可用不可见等关键技术，对不同敏感度等级的域间数据流动、使用过程进行管控，做好数据流动过程中的审计，实现数据事件可追溯，确保数据交换共享过程的安全性。

16.数据驱动的APT攻击检测与智能防护技术

重点适用：边缘计算层、工业云基础设施层、工业应用层、工业数据

APT攻击是一种具备高度隐蔽性的、针对特定对象展开的、持续有效的攻击活动。借助工业互联网平台边缘计算层海量设备发起APT攻击，感染面更大、传播性更强，针对此，亟需突破基于数据驱动的APT攻击检测、攻击建模、智能分析、智能防护、自适应恢复等技术，以抵御APT攻击。

六、工业互联网平台安全发展展望

工业互联网作为“新基建”的重点方向之一，其发展已经进入快轨道。工业互联网平台作为工业互联网的核心，其安全是工业互联网安全的重要内容。我国工业互联网平台安全建设已经取得了一定成果，但网络空间安全形势瞬息万变，平台安全建设也应与时俱进，针对此，本白皮书提出工业互联网平台安全参考框架，为我国工业互联网平台产学研用提供参考。下一步，我们将从完善政策标准、创新技术手段、探索产业协同等多个维度着手，联合政府和行业力量，共同打造工业互联网平台安全生态，积极推动工业互联网平台健康发展。

（一）政策标准

一是完善工业互联网平台安全政策要求，指引发展。以《深化“互联网+先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》等政策文件为指引，统筹发展平台建设与安全建设。充分汇集产学研各界工业互联网平台的安全诉求，制定发布工业互联网平台安全防护相关政策文件，进一步明确平台安全主体责任、安全管理、安全防护、安全评估与安全测试等要求，指导、敦促企业做好平台安全保障工作。

二是健全工业互联网平台安全标准体系，规范发展。制

定工业互联网平台安全技术框架、评价指标体系等基础共性标准。组织推进平台边缘计算安全、设备接入安全、工业微服务与接口安全、平台数据管控、应用和数据迁移等关键技术标准制定。根据工业互联网平台在不同行业领域应用场景的不同安全需求，梳理可能影响平台安全的关键业务流程，结合本白皮书中的工业互联网平台安全参考框架，面向不同应用场景、行业，制定有行业特色的应用标准或行业标准。

（二）安全技术

一是建立工业互联网平台安全综合防御体系。围绕工业互联网平台各层次中关键硬件、软件组件的安全需求，结合本白皮书中的平台安全参考框架，需从安全防护对象、安全角色、安全威胁、安全措施、生命周期五个视角统筹规划工业互联网平台安全建设，围绕设备、网络、系统、服务、数据等重点领域，在平台各层面部署安全技术与安全管理措施，建立工业互联网平台安全综合防御体系，提升平台综合防御能力。

二是应对标识解析与工业互联网平台融合应用引发的新型安全威胁。随着标识解析技术的广泛应用，标识解析与工业互联网平台的融合是未来发展趋势，同时也给平台引入新的安全威胁。标识解析在架构、协议、数据、运营等方面均存在安全风险，需加强平台侧标识数据、标识解析流程、标识查询、标识解析、标识数据管理相关组件与接口的安全保

护设计及安全措施部署，增强工业互联网平台上标识应用过程中自身的抗攻击能力。

三是研究工业互联网平台敏感数据可信交换共享。随着工业互联网平台业务场景对数据分析决策的多样化，对平台数据资源开放共享、互联互通的要求日益提高，不同行业、领域平台间数据交互需求日益增多，数据的攻击面被进一步扩大。需结合工业数据分级分类相关标准，围绕工业互联网平台敏感数据可信交换共享的需求，研究敏感数据识别、标记、保护、跨平台流动管控、审计、用户差异化访问及相关软件和进程的安全保护等技术，确保敏感数据在不同域工业互联网平台间交换共享过程的安全可信。

四是加强边缘层设备和系统安全接入管控能力。围绕工业互联网平台边缘计算层对设备安全管控、接入认证、权限控制等安全能力的需求，突破边缘设备可信接入、快速鉴权、动态阻拦、追踪溯源等关键技术，实现边缘层设备、系统接入平台的可信、可管、可控、可审计和可追溯。

五是防范新兴技术应用带来新的安全风险。大数据、人工智能、区块链、5G、边缘计算等新一代信息技术与工业互联网平台的融合应用，以及第三方协作服务的深度介入增加了信息泄露、数据窃取的风险。新兴技术应用将对原有的工业互联网平台安全监管模式带来新的挑战，应在新技术应用的同时，加强新兴技术安全防护手段研究与创新。

（三）产业协同

一是培养工业互联网平台安全复合型人才。加大力度培养边缘计算、云计算、工业微服务组件、工业应用、大数据等方向的安全专项人才，加大对技术研发和成果转化的支持力度，鼓励高校、科研院所、安全企业、平台企业和工业企业联合开展工业互联网平台安全复合型人才，依托工业信息安全产业发展联盟推动人才资质评估认证。

二是加快工业互联网平台企业与安全企业联合协同。工业企业本身网络安全技术不高，人才储备不足，面临设备部署成本高、防御效果难评估、安全运维投入大、应急响应预案不充分等问题，而且由于生产、技术保密等各种考虑，其与网络安全企业的合作不够深入。着力推广工业互联网平台企业、工业企业、安全企业的联合协同，整合各自优势资源、采用多种合作形式，实现工业互联网平台安全建设和推广，提升平台安全服务水平。

三是推进工业互联网平台安全国际合作交流。大力推进国际合作，营造国内外协同的良好环境，促进国际交流、产业优势、技术优势互补。合理搭乘一带一路的发展模式快车，加强与国际工业互联网相关联盟、龙头平台公司的交流、研讨，大力推进和推广国际合作，开展具有全球化、前沿技术性的技术合作和应用创新，共同打造新世纪的工业互联网安全平台。

联系地址：北京市石景山区鲁谷路35号　　联系电话：010-88686237