工业互联网边缘计算安全白皮书（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

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

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

随着工业互联网的快速发展，接入网络的工业设备数量不断增加，网络规模不断扩大，海量数据的实时分析要求越来越高。作为更靠近工业数据源的计算模式，边缘计算逐渐成为工业互联网领域关注的焦点。2018年6月，工信部发布《工业互联网发展行动计划（2018—2020年）》，明确指出“开展工业互联网关键核心技术研发和产品研制，推进边缘计算、深度学习、区块链等新兴前沿技术在工业互联网的应用研究”；2020年3月，印发《关于推动工业互联网加快发展的通知》，鼓励相关单位在时间敏感网络、边缘计算、工业智能等领域加快技术攻关，打造智能传感、智能网关、协议转换、工业机理模型库、工业软件等关键软硬件产品，加快部署应用。

然而，边缘计算在助力工业互联网发展的同时，也带来了关联数据泄露、底层风险渗透等安全问题，安全用好这把“双刃剑”迫在眉睫。2019年，中国科学院沈阳自动化研究所、国家工业信息安全发展研究中心等十余家单位联合发布《边缘计算安全白皮书》。其中，边缘安全参考框架1.0中指出工业边缘计算是边缘计算典型的价值场景之一，并就边缘基础设施安全、网络安全、数据安全、应用安全、边云协同安全提出防护措施，但尚未针对边缘计算应用到工业互联网内网、工业现场提出具体的防护措施。然而，边缘计算作为工业互

联网内网智能化、实时化改造的重要手段，部署在工业互联网中的边缘设备、边缘网络、边缘应用、边缘平台等面临不同的安全风险，需要根据其不同特点有针对性地部署安全防护措施。

为了进一步明确边缘计算应用到工业互联网场景下存在的安全保护对象及风险、安全防护措施和相关安全角色，国家工业信息安全发展研究中心在《边缘计算安全白皮书》《工业信息安全标准化白皮书》等已有成果的基础上，组织十余家单位编写《工业互联网边缘计算安全白皮书》，提出了工业互联网场景下的边缘计算架构及安全框架，旨在为工业企业、工业互联网平台企业、安全企业等相关单位安全部署边缘计算提供参考。

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	孙岩、柳彩云、杨帅锋、张雪莹、毕婷、王冲华、江浩、李耀兵、张伟
和利时科技集团有限公司	胡鹏飞、何春明
上海观安信息技术股份有限公司	谢江
北京百度网讯科技有限公司	季石磊、王建奎
杭州海康威视数字技术股份有限公司	王滨、王星
中国科学院大学	张玉清、杨毅宇
长扬科技(北京)有限公司	汪义舟、张亚京
杭州安恒信息技术股份有限公司	李剑锋、叶鹏
北京东方国信科技股份有限公司	敖志强、孙广明
北京亚控科技发展有限公司	张硕、单维旺
北京科技大学	林福宏
中国电子信息产业集团有限公司第六研究所	王绍杰、衣然
中国铁道科学研究院集团有限公司电子计算技术研究所	姚洪磊、杨轶杰

上海电力大学	王勇
上海云剑信息技术有限公司	王威
北京亚鸿世纪科技发展有限公司	李侠、乔伟
工业信息安全（四川）创新中心有限公司	刘尚麟
中国电子科技网络信息安全有限公司	幸享宏
安天科技集团股份有限公司	马景辉
哈尔滨工程大学	王勇

目 录

一、工业互联网边缘计算概述

（一）工业互联网边缘计算概念与内涵

工业互联网边缘计算是一种将部分数据处理和数据存储放在工业互联网边缘节点的分布式计算方式，其通过融合工业互联网边缘侧的计算、通信和存储能力，就近提供边缘智能服务，并可通过云边协同机制为工业互联网平台提供数据支撑，从而实现工业互联网泛在互联、实时业务、可靠服务、数据优化、边缘应用智能、安全和隐私保护等多方面应用需求。工业互联网边缘计算架构如图 1 所示。

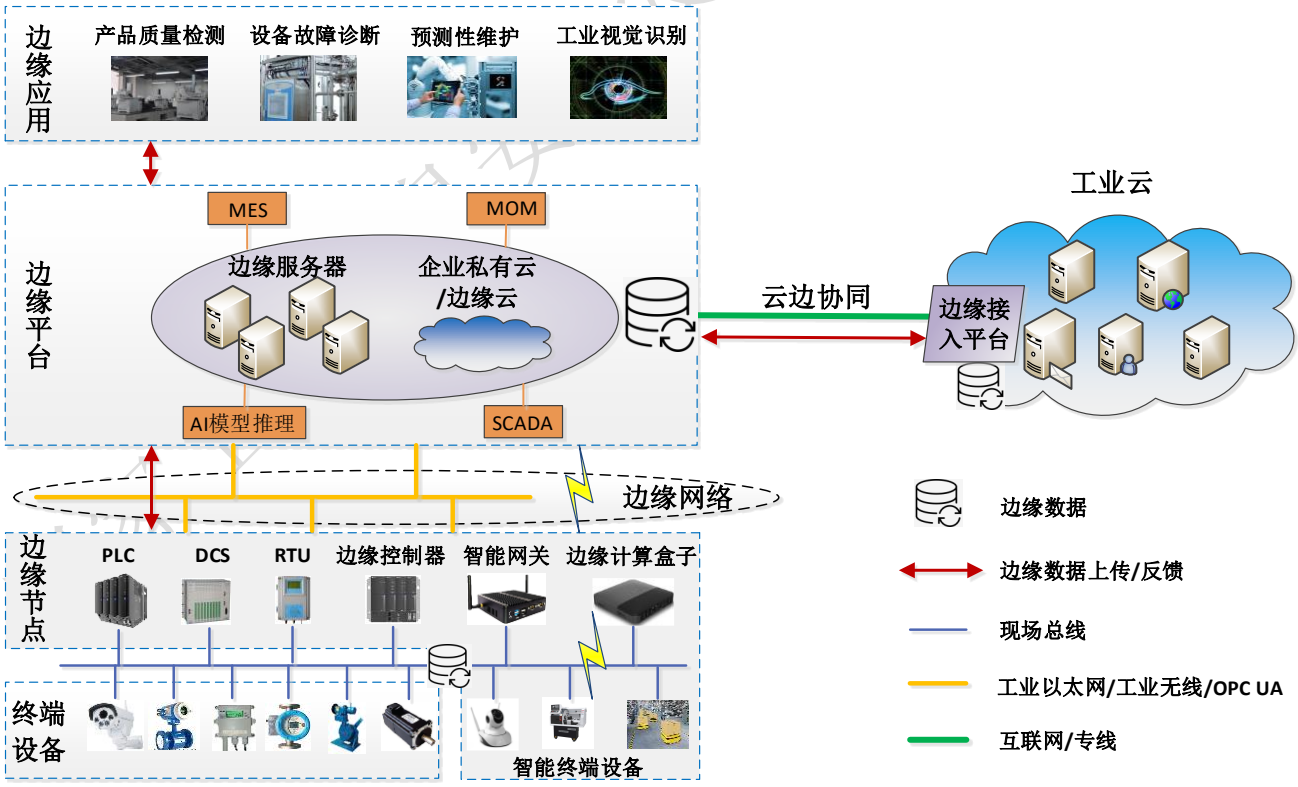

图 1 工业互联网边缘计算架构

工业互联网边缘计算架构主要包括以下内容：

a）**终端设备。**终端设备主要包括可实现工业现场数据采集

的各种传感器和仪器仪表、可执行工业控制命令的执行器和伺服电机等，终端设备可通过工业现场总线、实时以太网等通信协议与边缘节点连接，实现数据、控制命令等内容的传输；

b）**边缘节点。**边缘节点主要包括具有边缘算力的智能终端设备、工业控制设备、边缘控制器、边缘网关、边缘计算盒子等，通常部署在工业现场，实现智能感知、工业控制、实时数据处理和实时决策。其中，智能终端设备包括搭载边缘算力的智能摄像头、智能机器人、智能 AGV 小车等；工业控制设备包括 PLC、DCS、RTU 等，它们执行工业控制规则和逻辑，实现对底层终端设备的控制；边缘控制器既具有边缘计算能力，也具有实时工业控制能力；边缘网关兼具通用网关的数据转发功能和边缘侧数据处理功能；边缘计算盒子是专门用于执行边缘计算任务的算力设备。边缘节点作为边缘侧的算力硬件载体，为边缘侧的实时数据处理、AI 模型推理、实时工业控制、应用部署等提供计算能力；

c）**边缘网络。**边缘网络指在网络边缘侧负责连接各种工业设备、工业系统、工业数据，并将其接入工业互联网边缘平台的通信技术和协议。主要协议包括现场总线、工业以太网、时延敏感网（TSN）、OPC UA、5G、WiFi、NB-IoT、LoRa、MQTT 等；

d）**边缘平台。**边缘平台通常部署在企业私有云、边缘云、边缘服务器等边缘基础设施上，主要负责管理边缘侧的各种资源并提供边缘侧的基础平台能力。边缘资源管理主要是针对边缘节点资源、边缘计算资源、边缘网络资源和边缘存储资源进行调度和

协同，最大化资源的使用；边缘基础能力主要提供业务编排、统一服务接口 API 的定义和封装、轻量级容器和微服务组件等基础核心能力，支撑工业边缘智能应用和服务的开发和部署；

e）**边缘应用。**利用边缘侧的基础设施和边缘平台提供的基础能力，可以开发和部署各种边缘侧的工业应用和工业服务，包括：产品质量检测、设备故障诊断、预测性维护、工业视觉等；

f）**边缘接入平台。**边缘接入平台位于云端，主要实现工业云平台对边缘平台基础设施、边缘设备等资源的管理，提供将工业云上的应用和服务延伸到边缘的能力，实现边缘和云端的数据和能力的协同，提供完整的边缘和工业云平台一体化协同服务能力；

g）**边缘数据。**边缘数据是工业互联网的生产制造、运行服务等环节在边缘侧产生的机器数据、配置数据、决策数据、状态数据、模型数据等原始或衍生数据。这些数据呈现结构化、半结构化、非结构化等多种格式，具有分布广泛、数量巨大、时序性强等特点。

（二）工业互联网边缘计算研究现状

当前，相较于边缘计算技术在其他领域的应用，工业互联网边缘计算处于起步阶段。

1 国外研究现状

国外在工业互联网边缘计算方面的研起步较早，发展较快（如图 2 所示）。

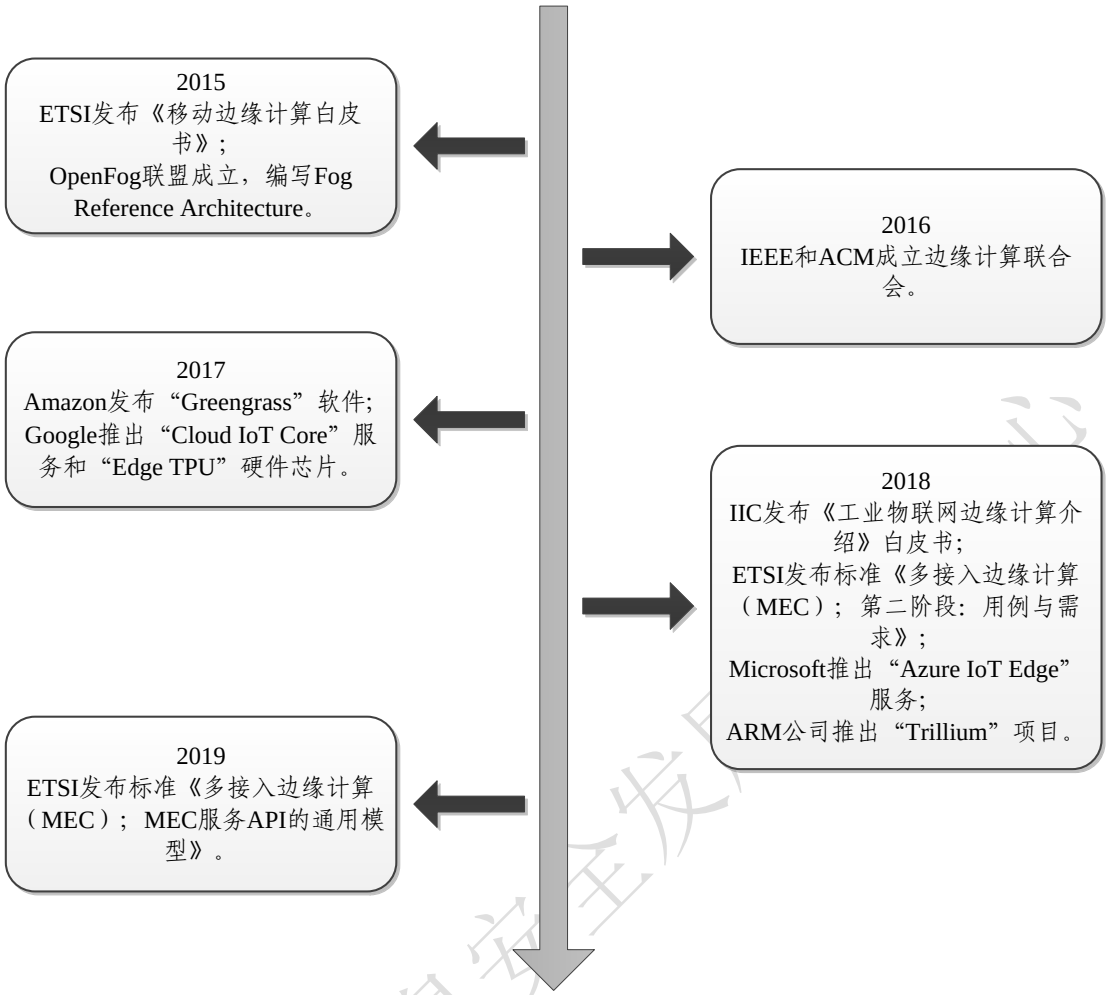

图2 国外工业互联网边缘计算发展现状概览

标准研制方面，2015 年 9 月，欧洲电信标准化协会（ETSI）发布了移动边缘计算白皮书（Mobile-Edge Computing – Introductory Technical White Paper），该白皮书给出了移动边缘计算的顶层架构设计，同时还介绍了与其他工业技术之间的接口关系。此后，该协会又分别于 2018 年 10 月和 2019 年 1 月发布了《多接入边缘计算（MEC）、第 2 阶段：用例与需求》（Multi-access Edge Computing (MEC)、Phase 2: Use Cases and Requirements）和《多接入边缘计算（MEC）；MEC 服务 API 的

通用原则》（Multi-access Edge Computing (MEC); General principles for MEC Service APIs）等多项 MEC 的相关标准，致力于更好地满足边缘计算的应用需求和相关标准制定。第三代合作伙伴计划（3GPP）也将边缘计算列入未来 5G 时代的关键技术，并且在 3GPP 系统化架构的标准化进程中，将边缘计算的需求作为重要设计因素。此外，3GPP 还将未来基于控制面和用户面分离的 5G 服务化架构写入标准，并给出了针对边缘计算的流量疏导方案和业务连续性方案。由于 3GPP 的标准化工作主要针对网络架构，因此更加注重边缘计算平台和网络架构设计相关内容，对于具体的业务场景则未做出规定。2018 年，美国工业互联网联盟（IIC）发布了《工业物联网边缘计算介绍》白皮书，阐述了边缘计算技术应用在工业物联网领域中的特性和价值，并提出了工业物联网边缘计算中的 5 条安全事项，包括：设备以及设备之上的每一层架构都应内含安全要素、计算和通信节点应被妥善监测和管理、及时应用最新的安全补丁、隔离出现的攻击、受攻击影响的组件必须及时获得处理和恢复。

组织建设方面，2015 年 11 月，思科、ARM、戴尔、英特尔、微软和普林斯顿大学联合成立了 OpenFog 联盟，主要致力于雾计算参考架构的编写；2016 年，电气和电子工程师协会（IEEE）和国际计算机学会（ACM）共同发起并成立了边缘计算联合会。

产业应用方面，亚马逊（Amazon）公司于 2017 年发布了支持边缘端机器学习的软件“Greengrass”；谷歌（Google）公司于

2017 年推出了管理边缘设备的服务“Cloud IoT Core”和运行在边缘端的硬件芯片“Edge TPU”，提升边缘设备的数据处理能力；微软（Microsoft）公司于 2018 年推出了边缘计算服务“Azure IoT Edge”，将云分析和自定义业务逻辑下移到设备端；ARM 公司于 2018 年推出“Trillium”项目，可以在边缘设备上运行机器学习算法。

2 国内研究现状

2016 年以后，我国逐步在工业互联网边缘计算领域开展研究工作。主要工作如表 1 所示。

表1　国内工业互联网边缘计算发展现状概览

范围	时间	重要事件
政策	2017 年 11 月	《深化“互联网+先进制造业”发展工业互联网的指导意见》发布
	2018 年 6 月	工信部发布《工业互联网发展行动计划（2018—2020 年）》
标准	2019 年 11 月	《边缘计算安全白皮书》发布
	2020 年 5 月	《工业互联网边缘计算总体架构与要求》等 7 项边缘计算联盟标准获得立项
	2020 年 8 月	《信息安全技术 边缘计算安全技术要求》在信安标委立项
组织	2016 年 11 月	边缘计算产业联盟（ECC）成立
	2017 年 10 月	首届中国自动化学会边缘计算专业委员会会议在沈阳举行
技术	2017 年	中国科学院沈阳自动化研究所开展“工业互联网应用协议及数据互认标准研究与试验验证”项目研究
	2018 年	工信部工业互联网创新发展工程系列项目专门设立了“工业互联网边缘计算基础标准和试验验证”等 8 个项目
	2018 年	科技部国家重点研发计划“网络协同制造和智能工厂”重点专项专门针对边缘计算设置了“工业互联网边缘计算节点设计方法与技术”等多个项目

产业	2017 年	华为公司发布边缘计算解决方案“EC-IOT”
	2018 年 3 月	阿里巴巴公司发布物联网边缘计算产品“Link Edge”
	2018 年	百度公司发布边缘计算智能解决方案“IoT Intelligence Edge”
	2018 年 10 月	中国移动成立“边缘计算开放计算实验室”

政策指导方面，2017 年 11 月，国务院发布了关于《深化“互联网+先进制造业”发展工业互联网的指导意见》，这是我国针对工业互联网发展的首个规范性意见，指明了未来发展先进制造业的方向。2018 年 6 月 7 日，工信部公布了《工业互联网发展行动计划（2018—2020 年）》，文件明确指出，开展工业互联网关键核心技术研发和产品研制，推进边缘计算、深度学习、区块链等新兴前沿技术在工业互联网的应用研究。

标准研制方面，2019 年 11 月，边缘计算产业联盟发布了《边缘计算安全白皮书》，该白皮书的目的是识别、解释和定位与边缘安全相关的体系结构、设计和技术，并提出了边缘安全的参考框架和确保处理相应安全问题的方法组合。2020 年 5 月，《工业互联网边缘计算总体架构与要求》等 7 项边缘计算联盟标准立项，8 月，国家标准《信息安全技术 边缘计算安全技术要求》在信安标委立项。

组织建设方面，2016 年 11 月，由中国科学院沈阳自动化研究所、华为技术有限公司等单位联合倡议成立了边缘计算产业联盟（Edge Computing Consortium）；中国自动化学会成立了边缘计算专业委员会，并于 2017 年 10 月举行了首届中国自动化学会

边缘计算专业委员会会议。

技术研究方面，2017 年，中国科学院沈阳自动化研究所承担“工业互联网应用协议及数据互认标准研究与实验验证”项目，对工业互联网智能制造边缘计算标准的制定进行了探索；2018 年，工信部针对工业互联网边缘计算专门设立了“工业互联网边缘计算基础标准和试验验证”等 8 个研究项目，通过软硬件等方式对边缘计算架构技术标准的可行性与科学性进行试验验证；2018 年，科技部国家重点研发计划“网络协同制造和智能工厂”中针对工业互联网边缘计算设置了“工业互联网边缘计算节点设计方法与技术”等多个项目，主要研究边缘计算技术在工业互联网场景中实现时各环节的关键技术。

产业应用方面，2017 年华为公司发布边缘计算解决方案“EC-IOT”，通过结合边缘计算和 PLC 技术为电力、交通等行业边缘智能数据处理需求提供服务；2018 年 3 月阿里巴巴公司发布物联网边缘计算产品“Link Edge”，该产品是一种可以在设备上运行本地计算、消息通信、数据缓存等功能的软件，使设备具备存储、计算、智能等能力；2018 年百度公司发布边缘计算智能解决方案“IoT Intelligence Edge”，通过在设备上安装智能边缘核心软件，将云计算的能力赋予本地；2018 年 10 月中国移动成立“边缘计算开放计算实验室”，百度、腾讯、阿里、华为、中兴等多家合作商共同参与，研究边缘计算产业生态的构建和协同发展。

（三）边缘计算助力工业互联网发展

近年来，边缘计算市场规模逐渐扩大，根据 Grand View Research 的最新报告，到 2027 年，全球边缘计算市场规模预计将达到 154 亿美元，预测期内复合年增长率为 38.6%。边缘计算通过将 ICT 基础设施“下沉”，为工业企业在边缘侧处理数据提供计算能力，有力推动工业互联网的发展。

一是边缘计算能够实现工业互联网设备、协议、数据的互联互通。工业设备的连接是 OT 和 IT 融合的基础。目前企业内网主要存在现场总线、工业以太网、时延敏感网（TSN）等多种连接方式，工业设备来自不同供应商且通信协议、接口互不兼容，导致不同的设备无法互联，设备中的工业数据无法有效采集、使用、共享，从而数据价值难以充分释放，预测性维护分析、整体设备利用率分析等面临困难。边缘计算节点通过部署协议转换功能模块，实现通信协议相互转换、异构设备互联互通。

二是边缘计算能够保证工业互联网的实时性和可靠性。相比于传统互联网，工业互联网由于涉及 OT 网络和实时控制，对系统的时延敏感度较传统互联网要高得多，工业生产线上的工业传感器、机器人、工业 AR/VR，都需要毫秒或百纳秒级的实时响应。然而，由于复杂的工业现场网络环境以及广域网数据传输过程存在的链接和路由不稳定等问题，这些因素造成的延迟过高、抖动过强等问题严重影响工业互联网服务的实时响应能力。边缘计算节点可部署在工业生产现场，通过提供不受网络传输带宽和

负载影响的“现场级”计算能力，避免断网、时延过大等因素对实时性工业生产造成影响。

三是边缘计算能够缓解云中心的带宽压力。近年来，接入工业互联网的终端设备日益增多。据 GE 预计，2020 年将有超过 500 亿台机器连入工业互联网。高档数控机床等工业生产设备、传感器等工业现场数据采集设备、PLC 等控制设备产生大量原始及衍生工业数据。随着万物互联趋势不断加深，工业数据的增长速度远远超过了网络带宽的增速，工业互联网平台面临巨大的数据处理、存储压力。边缘计算通过在本地缓存、过滤和处理数据，能够有效缓解工业互联网平台的带宽压力。

四是边缘计算能够降低企业生产成本。目前，中小企业一般倾向使用公有的中心云和私有的边缘云的方式处理工业数据。使用中心云的方式，企业的数据容易在未授权的情况下被第三方使用，存在巨大的风险成本；而使用私有的边缘云方式，可以避免或减少企业部署大型服务器带来巨大的能耗、运营成本。边缘计算在工业现场通过将异构设备互联互通，大量数据被释放，为引入大数据和机器学习等先进分析算法提供了充足的来源。搭载这些分析算法的智慧边缘节点可以有效提高生产效率，降低人工成本。据 IDC 预测，未来将有超过 50%的数据在边缘侧处理，2020 年边缘计算支出占物联网基础设施总支出的 18%，成本仅为单独使用中心云计算的 39%。

二、工业互联网边缘计算安全风险与挑战

（一）工业互联网边缘计算面临典型风险

边缘计算在助力工业互联网发展的同时，也带来了新的安全问题，安全用好这把双刃剑迫在眉睫。工业互联网边缘计算中的安全保护对象包括：工业边缘应用、工业边缘平台、工业边缘网络、工业边缘节点、工业边缘数据和边缘接入平台。其面临的安全风险如下：

1 工业边缘应用安全

工业边缘应用部署各类专业化工业软件，主要围绕设备管理、研发设计、运营管理、生产执行、产品全生命周期管理、供应链协同等工业应用场景，提供传统云化工业软件和新型轻量化工业应用及服务。工业边缘应用以工业 APP 服务的方式提供给用户，主要部署在靠近工业现场的边缘侧，由于边缘侧设备计算及存储资源有限，且工业领域可用性及可靠性要求更高，因此难以为边缘应用部署高复杂安全算法及安全防护设备，导致边缘应用面临着应用身份鉴别、应用访问控制、应用安全审计、通信保密性、应用资源控制、应用接口安全等措施不足的安全风险，极易被当做跳板攻入边缘服务器等核心基础设施中，引发重大损失。其面临的风险主要包括：

a）单一凭证身份鉴别安全风险。如单鉴别技术破解攻击；

b）边缘用户安全风险。如用户信息泄露；

c）访问控制安全风险。如未授权访问、越权访问、未经系统

运营方许可的情况下对外传输数据;

d）应用行为安全风险。如误操作、根指令删除等;

e）应用监测与审计风险。如封闭的工业应用和协议难以实时被识别，应用被篡改和入侵后难以及时发现等;

f）应用资源控制安全风险。如资源不合理利用而引发的各种攻击;

g）补丁安全风险。如虚假补丁、不可靠补丁等;

h）测试安全风险。如源代码泄露、错误和异常处理等;

i）开发安全风险。如代码漏洞、恶意后门、API 误调用、恶意入侵等;

j）边缘管理风险。如访问控制不严、管理接口破坏、资源配置不当和管理人员恶意操作等。

2 工业边缘平台安全

工业边缘平台提供边缘资源管理和边缘基础能力。工业边缘平台集成了大量边缘侧生产控制数据等重要数据，同时对部分边缘节点具有调度功能，一旦遭受攻击或渗透，将导致重要数据泄露、生产失控等安全问题。其面临的风险主要包括:

a）物理安全风险。相对于核心设施，对于部署边缘平台的边缘服务器的物理防护相对薄弱，容易导致物理损坏等风险;

b）服务操纵风险。边缘服务器通过在特定地理区域部署边缘数据中心来提供虚拟化服务和各种管理服务，攻击者可获得足够的控制权限，并滥用其特权作为合法的管理员操纵服务;

c）接口安全风险。如底层风险通过非安全接口渗透至边缘平台;

d）边界隔离安全风险。包括逻辑隔离安全风险及物理隔离安全风险等。其中，边缘平台面临自然灾害、人为破坏、窃听攻击等安全风险，边缘平台上的特定应用或者数据存在被非法调用和访问的风险;

e）边缘分析安全风险。边缘设备在实际运行中会产生大量实时动态数据，为攻击者提供了数据关联性、整合分析和隐私挖掘的可能性;

f)容器安全风险。包括虚拟机操纵、虚拟镜像泄露等。其中，虚拟机软件自身安全漏洞导致虚拟机逃逸风险，引发虚拟机之间、容器之间的非授权访问;

g）微服务组件安全风险。包括微服务组件自身漏洞导致的安全事故，微服务组件不够健壮导致的服务失败或者服务质量下降，微服务组件内部使用人员的恶意破坏等;

h）业务数据泄露。包括内部人员未遵从安全策略导致数据泄露的风险、内部人员主动泄露的风险，外部目标性攻击导致数据泄露的风险等;

i)边缘协同安全风险。如因边缘节点的自私行为导致服务失败、服务质量下降。随着网卡可编程能力的提高，自私节点可以通过控制竞争窗口大小的方式进行作弊，使自己获得更多的带宽。

3 工业边缘网络安全

工业边缘网络涉及蜂窝网络（GSM、4G、5G）、工业以太网（Modbus TCP/IP、Profinet、 Ethernet/IP、 EtherCat、PowerLink、SERCOSIII）、低功耗网络协议（Wifi、BLE、Zigbee、LoRa、NB-lot）、OPC UA 协议等多种网络通信协议，各协议安全性不一，增加了网络防护难度，此外，工业网络基础设施的多样性也导致网络安全防护困难。工业边缘网络面临的风险主要包括:

a）5G 环境下的安全风险。5G 采用公钥加密接入认证，LTE 接入到 5G 网络将带来隐私泄露风险。此外，由于边缘计算设备计算能力较弱，而联网通信具有超高可靠，低时延特性的场景，如果采用单独认证，可能会引发终端信令请求无法得到响应;

b）通信协议漏洞风险。如 Modbus、Profinet、Zigbee 等工业协议频繁爆出漏洞，极易被黑客利用，引发脆弱性攻击;

c）网络基础设施安全风险。边缘计算物联网终端设备大量使用 GSM/GPRS 物联网卡，由于 GSM 只能认证移动端的合法性，而移动端无法甄别基站的真伪，移动端用户接入伪基站后，数据信息可被伪基站截获;

d）边界安全风险：边缘设备通过各种协议采集数据、接入网关，当前常用的有 LoRa、NB-IoT。其中 LoRa 是非授权组网，NB-IoT 需要运营商授权。我国有诸多设备采用了 LoRa 协议，由于 LoRa 具有非授权组网特性，面临报文伪造、恶意拥塞、身份伪造等安全风险。

4 工业边缘节点安全

部署在工业现场的边缘节点承担着工业现场的数据采集、控制反馈、算力承载等任务。其面临的安全风险主要包括边缘设备自身安全风险和边缘设备衍生安全风险两大类，其中自身安全风险又主要包括物理安全风险、系统安全风险、设备非法接入风险、数据安全风险等。

a）设备物理安全风险。首先，部署在工业现场的缺乏物理安全控制的边缘设备可能被盗窃或破坏。其次，若边缘设备的物理接口直接暴露在设备外部，没有做安全防护，则易导致非法访问；

b）操作系统安全风险。首先，边缘算力设备可能采用通用的嵌入式 Linux、Windows、Android 等操作系统，而相关边缘设备操作系统可能存在系统漏洞、过期的组件、不恰当的配置以及不安全的更新等安全问题。一旦操作系统自身漏洞被攻击者利用，将导致大规模网络攻击等安全事件；其次，边缘设备应用层所依赖的组件若更新不及时，组件本身漏洞也可能被利用发起攻击；再次，操作系统安全配置可能存在长期不更新、不核查等问题，不恰当的系统配置也可能使攻击成功；最后，操作系统在更新过程中，更新包等应当经过验证，未经验证非官方更新包可能是被篡改过的，其中可能存在漏洞或恶意软件；

c）设备非法接入风险。为了集成或支持新的 IT 能力，工业现场的边缘设备与外界的隔离大大减少甚至提供了远程访问的能力。然而工业现场的边缘设备可能使用了默认密码、弱密码，

或采用了容易被绕过的认证机制，甚至未采用任何访问认证机制；此外，边缘设备的固件中可能保留了调试测试接口等而没有采用合适的安全保护措施，上述这些因素均可能导致攻击者远程非法接入到边缘设备；

d）边缘设备数据安全风险。边缘设备上的数据在存储、传输等环节存在涉及用户隐私或系统安全的敏感数据泄露、未授权读取或篡改等风险。此外，边缘设备与云端或移动应用端进行通信时，若控制指令或采集的数据未经加密，则攻击者可能通过监听获取敏感数据；

e）边缘设备衍生安全风险。工业现场边缘设备安全存在许多区别于传统的 IT 系统的安全风险，其中一个重要的区别体现在边缘设备的衍生安全风险上。边缘设备衍生安全指边缘设备因自身脆弱性而导致其他领域安全。工业现场边缘设备可能带来对生命安全或健康的风险，甚至对环境产生严重的破坏、造成生产损失从而导致对金融乃至国家经济正常运行带来严重影响。

5 工业边缘数据安全

工业边缘数据的安全问题贯穿整个工业系统，是创建安全边缘计算环境的基础，其根本目的在于保障数据的可用性、保密性和完整性。其面临的风险主要包括：

a）隐私泄露风险。在边缘计算网络中，数据隐私保护算法通常在资源受限的工业终端设备上失效，引发如工况状态泄露等风险；

b）工业数据被盗风险。针对黑客惯用的设备身份伪造、OTA 固件劫持、设备重放攻击、口令破解、逆向固件、设备控制、资源消耗等攻击手段，没有防护策略，导致工业数据被盗;

c）工业数据因泄露和仿冒攻击导致的数据保密性风险。边缘设备作为数据的第一入口，采集大量实时高价值数据，且安全功能有限，使得工业互联网数据泄露给未获授权的人，例如防范仿冒攻击，易引发重要生产数据泄露等安全风险;

d)数据传输安全风险。由于边缘数据的存储是动态变化的，传统的数据完整性校验方法并不能完全适用于边缘计算环境，造成传输数据被劫持，完整性被破坏等传输安全风险。此外，如果边缘设备的数据上报没有采用加密链路，也会引起数据在传输中的数据泄露风险;

e）数据使用安全风险。边缘数据中心在数据使用过程中，因内外部安全风险会导致数据越权使用，源数据污染，敏感数据泄露等数据使用安全风险。边缘数据中心自身的安全性，也会引发数据泄露等数据安全风险;

f）工业设备内存泄露风险。在工业边缘计算场景下，边缘节点远离云中心的管理，被恶意入侵的可能性大大增加，而且边缘节点更倾向于使用轻量级容器技术，但容器共享底层操作系统，隔离性更差，安全威胁更加严重。因此，仅靠软件来实现安全隔离，很容易出现内存泄露或篡改等问题;

g）APT 攻击风险。APT 攻击属于寄生形式的攻击，通过在

边缘基础设施目标基础设施中建立立足点，可以从中秘密地窃取数据，并能适应防备 APT 攻击的安全措施;

h)外包安全风险。当用户对数据的控制权交给边缘设备时，由于数据源在物理上不再拥有数据，部分需要本地数据拷贝的传统密码学算法失效;

i）交换/共享安全风险。边缘节点处于不同安全域中，不同信任域节点数据交换共享易引发重要数据泄露。

6 工业边缘接入平台安全

边缘接入平台将云端能力下发到边缘节点，提供将工业云上应用延伸到边缘的能力，实现边缘和云端的数据和能力的协同。边缘接入平台主要面临边缘-云互联 API 调用安全、边缘-云数据传输安全、边缘节点的云端安全认证等风险。具体如下:

a）边缘-云互联 API 调用安全风险。在边缘侧应用服务中，存在大量的 API 接口调用，如安防、车联网服务、智慧家居等。在第三方请求、调用 API 接口并提供服务时，存在注入、非法使用、越权、伪造身份和第三方软件自身的安全风险等多重安全问题;

b)边缘-云数据传输安全风险。在当前边缘数据应用场景下，如选择不当的通信方式或选择不安全的通信协议（如: ZigBee、蓝牙等），将存在数据侦听、篡改、伪造等安全风险;

c）边缘节点的云端安全认证风险。在边缘设备接入云平台网络中时，存在非法设备接入、伪造传感节点、节点劫持等安全

风险;

d）边缘节点对云平台的安全影响。边缘智能终端可能面临物理设计的合理性、芯片的可靠性、智能软件的安全性（漏洞与缺陷）、运行机制的可靠性等自身安全因素，可能引发云-边缘通信时边缘数据泄露风险。

（二）工业互联网边缘计算安全防护面临挑战

工业互联网边缘计算主要存在设备异构、泛在联接、分布广、高实时性、高汇聚性、资源受限、现场环境恶劣、部署场景复杂等特征。

a)设备异构导致统一管理难。工业互联网中存在生产设备、感知设备、控制设备、边缘算力设备等多种设备，设备型号不一，协议多样，统一管理难度增加，安全风险相对传统网络更大;

b）边缘云、5G 等新型基础设施的引入导致边界消失和传统的防护手段失效。IT 互联网网络中安全风险被大量引入，加大了安全能力不足的工业控制系统的攻击面;

c）高实时性导致安全防护轻量化需求增加。边缘计算在靠近工业现场数据产生的地方做数据处理，不需要通过网络请求云计算中心的响应，大大减少了系统延迟，增强了工业服务响应能力。但同时，为了确保高实时性，难以部署高复杂的加密、认证等安全措施，轻量化需求增加，但是目前轻量化算法市场化不足，部署应用困难;

d）高汇聚性导致重要工业数据保护难度增加。作为物理世

界到数字世界的桥梁，边缘计算是数据的第一入口，汇聚大量原始数据，进行数据价值创造的同时面临数据不确定性、多样性、关联分析泄露等挑战;

e）资源受限导致安全性难保障。基于工业互联网对可靠性及可用性的严格需求，资源受限节点优先保障可靠性，安全能力有限;

f）现场环境恶劣导致物理安全防护难度增加。边缘计算设备作为价值信息的运算节点和存储节点被放置在不同的工业环境中，例如工厂、矿井等，这一方面对边缘计算设备的防震、防水、防尘、防爆、防电磁、抗高低温、抗击打等环境适应性要求更高，另一方面很容易遭到人为的物理篡改和攻击，一旦遭受破坏和盗取可能造成严重后果;

g）部署场景复杂导致运维安全难度增加。由于边缘计算设备部署场景的复杂性，各边缘节点均处于分散状态，边缘计算所需的运维难度更高，对运维技术人员的能力及系统的健壮性、可视化、易管理、易维护等都提出了更高的要求。如果边缘设备和数据中心遭到破坏，系统的连续性和数据的可用性将受到影响;

h）新的研发模式带来的安全风险。如敏捷、开发即运营、快速迭代分发部署等开发模式，给追求稳定性、高效性、和持续性的工业现场带来新的网络安全和功能安全的挑战;

i）人工智能对抗的安全挑战。在人工智能场景在工业数字孪生、AR、VR、柔性制造等应用场景落地时，由于人工智能天生

的不可解释性，在遭受人工智能安全对抗攻击时，给工业生产制造引入不可控（逆）的安全风险。

三、工业互联网边缘计算安全防护

（一） 国内外工业互联网边缘计算安全防护框架

1 已有工业互联网框架

2017 年，美国工业互联网联盟（IIC）发布了工业互联网参考架构 IIRA（Industrial Internet Reference Architecture）。IIRA 参照 ISO/IEC 42010 标准，从商业、使用、功能、实现四个视角出发，探讨了功能安全、信息安全、弹性、互操作性、连接性、数据管理、高级数据分析、智能控制、动态组合九大系统特性。

2015 年，德国电工电子于信息技术标准化委员会于发布了工业 4.0 参考架构模型 RAMI4.0，该模型构建在 IEC62264、IEC62890 基础上，分别从系统集成层级、物理信息系统活动层次、生命周期与价值流三个维度形成了整体框架。

2 已有工业互联网安全框架

2016 年，美国工业互联网联盟（IIC）发布工业互联网安全框架（IISF）。该框架建立覆盖整个工业互联网的安全策略模型，以数据防护为中心，涉及安全配置和管理、安全监测和分析、通信和连接保护、终端（含边缘侧设备和云）的保护等不同维度，并从功能视图和信息系统视图的角度进行了相关维度的关联描述。

3 已有边缘计算安全参考框架

2019 年 11 月，中国科学院沈阳自动化研究所、国家工业信息安全发展研究中心等十余家单位联合发布了《边缘计算安全白皮书》，提出了国内首个边缘安全参考框架，覆盖了边缘安全类别、典型价值场景、边缘安全防护对象。其中，边缘安全防护对象覆盖边缘基础设施、边缘网络、边缘数据、边缘应用、边缘安全全生命周期管理以及边云协同安全“5+1”个层次；统筹考虑了信息安全、功能安全、隐私、可信四大安全类别以及需求特征；围绕工业边缘计算、企业与 IoT 边缘计算和电信运营商边缘计算三大典型的价值场景的特殊性，分析其安全需求，支撑典型价值场景下的安全防护能力建设。

（二）工业互联网边缘计算安全参考框架

1 基本思路

首先结合《工业信息安全标准化白皮书》对工业互联网范畴的描述和工业互联网边缘计算架构，将工业互联网边缘计算安全保护对象分为边缘节点、边缘网络、边缘平台、边缘应用、边缘接入平台、边缘数据共 6 个方面，并对这些安全保护对象的风险进行了分析。其次针对工业互联网边缘计算安全保护对象存在的安全风险，分析了对应的安全防护措施。最后将工业互联网边缘计算安全的相关责任主体分为边缘计算服务开发商、客户、边缘计算安全服务提供商、第三方评估机构四个安全角色，并对其所需承担的安全职责进行了分析，形成了集安全保护对象及风险、

安全防护措施、安全角色三维立体的工业互联网边缘计算安全框架。该框架适用于在工业互联网中规划、建设、运行边缘计算服务的相关企业，也可为科研院所、高校等进行工业互联网边缘计算安全研究提供依据和参考。

2 工业互联网边缘计算安全框架

工业互联网边缘计算安全框架是在工业互联网中部署应用边缘计算服务的基础。主要包括安全角色、安全保护对象和安全风险、安全防护措施共 3 个维度。框架图如图 3 所示。

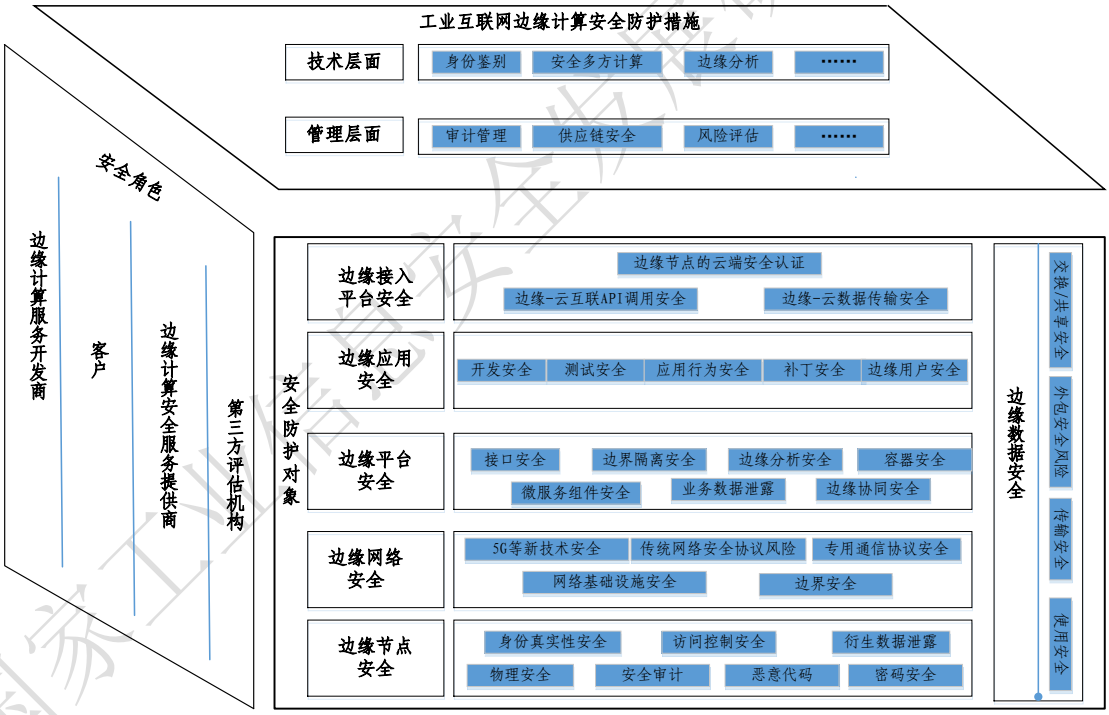

图 3 工业互联网边缘计算安全框架

（1）安全体系框架要素关系概述

明确保护对象是制定防护措施的基础。企业应梳理边缘计算部署应用的位置，在此基础上梳理可能存在风险的设备、数据等保护对象，方便针对性制定安全方案，选择防护措施。

实施安全防护是工业互联网边缘计算安全的核心。梳理相关设备、系统后，企业应结合工业设备、系统的特点，强化安全防护。如在控制系统上部署边缘计算与在工业传感器上部署边缘计算采取不同防护措施。

落实安全角色主体责任是贯穿安全全流程的关键。在系统设计之初就应梳理涉及的主体，如边缘计算服务提供商、第三方安全服务提供商，并对主体进行安全管理，如相关方如何进厂，进厂后应该遵循哪些规则等，防止人为安全风险，同时明确相关方事后责任，方便进行安全责任追溯。

综上，开展工业互联网边缘计算安全防护工作，应由相关角色根据实际保护对象的安全需求，采取技术、管理等手段加强防护。

（2）安全角色要素

工业互联网边缘计算安全角色主要分为边缘计算服务开发商、客户、边缘计算安全服务提供商、第三方评估机构四类。

边缘计算服务开发商指提供工业互联网边缘计算服务的参与方，其职责包括但不限于：设计开发安全产品与应用，并提供维护技术服务；为边缘计算安全运行提供信息安全基础服务；按照边缘计算安全管理策略部署安全技术措施，包括数据安全加密、设备认证等；协助边缘计算安全建设者进行工程建设，提供安全产品、服务和技术等。

客户指为使用工业互联网边缘计算服务而处于一定业务关

系中的参与方，其职责包括但不限于：合理安全使用边缘计算服务开发商提供的边缘计算服务；向边缘计算服务开发商反馈合理的安全需求；负责所有资产的安全管理；定期安排安全评估机构进行安全检查评估；接受安全培训和指导；负责边缘计算安全运行与维护管理；监测边缘计算安全风险，分析安全态势；发现安全事件和脆弱性，防范，阻断攻击并及时告知相关方；制定、评估并修订边缘计算安全应急预案，及时处置安全威胁并告知相关方；有效控制因边缘计算引发的安全风险渗透至工业互联网核心网络。

边缘计算安全服务提供商支撑或协助边缘计算服务开发商或客户的安全管理、技术和运维。其职责包括但不限于：通过商务合同的方式，协助或支撑边缘计算服务开发商或边缘计算服务客户开展安全管理、技术和运维，承担部分安全责任。

第三方评估机构是独立于边缘计算服务提供商的专业评估机构。其职责为：根据国家有关要求或企业自行委托对边缘计算服务开发商及其提供的边缘计算服务开展独立的安全评估。

除以上主要安全主体外，电信设备运营商、互联网厂商等相关的其他角色根据其服务内容也需承担相应的安全责任。

（3）安全防护对象要素

工业互联网边缘计算安全框架包括下面 6 个防护对象的安全：

a）边缘应用安全：边缘应用安全是满足工业边缘应用开发

及运行过程中的基本安全需求，同时防止恶意应用对边缘计算平台自身以及其他应用安全产生影响;

b）边缘数据安全：工业边缘数据的安全问题贯穿整个工业系统，是创建安全边缘计算环境的基础，其根本目的在于保障数据的可用性、保密性和完整性;

c）边缘网络安全：边缘网络安全是实现边缘计算与现有各种工业总线互联互通、满足所连接的物理对象多样性及应用场景多样性的必要条件;

d）边缘设备安全：边缘设备为整个边缘计算节点提供软硬件基础，包括边缘控制器和边缘网关等。边缘设备安全是边缘计算的基本保障，需要保证边缘设备在启动、运行、操作等过程中的安全可信，边缘设备安全涵盖从启动到运行整个过程中的设备安全、硬件安全、虚拟化安全和 OS 安全;

e）边缘平台安全：边缘平台安全是提供边缘资源管理和边缘基础能力的基础。边缘平台集成了大量生产数据、控制数据等重要数据，同时对部分边缘节点还具有调度功能，一旦遭受攻击或渗透，将导致重要数据泄露、生产失控等安全问题;

f)边缘接入平台安全：边缘接入平台安全保障边云协同的安全性。边缘接入平台将云端能力下发到边缘节点，提供将工业云上应用延伸到边缘的能力，涉及边缘节点安全管理与运维、边缘设备接入安全等内容。

（4）安全防护措施要素

工业互联网边缘计算安全防护措施主要根据安全防护对象的面临的风险，从管理、技术等角度，部署有针对性的安全防护措施。

（三）防护措施

1 工业边缘应用安全防护措施

（1）技术层面

a）用户身份认证。提供并启用用户身份标识唯一的检查功能；提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用；采用加密的方式存储用户的账号和口令信息；设置非法登陆失败的次数。针对重要的工业控制系统的访问和操作，如注册、登陆、操作、管理等，提供图形验证码等强制保护措施，对用户重要操作进行确认和验证；

b）用户授权。制定边缘应用访问授权、控制等策略，采用最小权限安全模型（例如白名单功能）管理应用访问权限，确保所使用的工业软件不在未经系统运营方许可的情况下对外传输数据；

c）安全监测。对工业边缘应用的性能、流量、用户行为等进行实时监控、分析、报警，并采用高性能白名单安全识别、机器自学习建模、智能攻击者锁定、虚拟补丁自动生成、WEB 访问流程合规防护等防护手段，主动发现包括僵尸 IP、代理 IP、扫描 IP、黑产 IP、C&C 等恶意 IP 发起的访问行为等。此外，对工

业应用软件前的漏洞和病毒扫描机制，可调用具备扫描功能的软件进行扫描；

d）资源控制。一是应限制对应用访问的最大并发会话连接数据等资源配额，并对服务水平进行监测，当服务水平降低到预先规定的阀值时进行告警；二是应在使用完毕后及时删除访问用户的个人信息数据，对留存期限有明确规定的，按相关规定执行；三是启用服务优先级设定功能，并根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源；四是应对工业互联网边界资源进行访问鉴别，只有鉴别成功的用户或系统才可以访问相应的资源。

（2）管理层面

a）访问人员管理。支持对授权管理员进行唯一身份鉴别；重点岗位的计算机使用人员应签订信息安全与保密协议，明确信息安全与保密要求和责任；人员离岗离职时应终止信息系统访问权限；应建立外部人员访问重要区域审批制度，外部人员须经审批后方可进入；对信息安全责任事故进行查处，对违反信息安全管理规定的人员给予严肃处理；

b）应用系统管理。只允许通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；提供应急的恢复目标，恢复优先级和度量指标；建立第三方组件信息备份，保证备份信息的保密性、完整性和可用性，并定期验证信息系统备份的可用性；建立网络和系统安全管理制度，对安全策略、账户管理、配

置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定;

c）应用审计管理。对业务应用系统行为进行审计，审计功能记录系统重要安全事件的日期、时间、发起者信息、类型、描述和结果等，并保护好审计结果，阻止非法删除、修改或覆盖审计记录。同时能够对记录数据进行统计、查询、分析及生成审计报表；部署相关的数据库审计措施，对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全；保护审计记录，避免受到非授权的访问、篡改、覆盖或删除等，并保留记录不少于六个月;

d）安全开发管理。具备安全开发的能力，提供需求阶段安全需求分析和风险评估；提供设计阶段进行攻击面分析与威胁建模；提供开发阶段的标准工具使用和静态分析、测试验证阶段的异常缺陷评估;

e）安全补丁与加固管理。定期进行补丁安装及更新，安装前应对补丁进行安全性测试；对边缘 APP 进行加固，并确保加固行为基本不影响应用的功能、性能和兼容性等，并实现边缘应用加固方案在主要机型上的兼容性;

f）应用软件管理。安装前对应用程序进行功能测试及安全性测试，并保留测试报告；安装时应提示终端操作系统用户对其使用的终端资源和终端数据进行确认；确保对工业生产管理的正常运行无不良影响；在运行期间，需记录用户操作行为，方便进行

行为审计;

g) 运维管理。支持可视化自动化编排与运维技术，将人、技术、流程进行深度融合，通过把人工运维经验固化成预案，构建安全事件处置的工作流，自动化触发不同安全设备执行响应动作，快速将工业边缘计算环境中复杂的事件响应过程和任务流转变为一致的、可重复的、可度量的和有效的工作流，变被动应急响应为自动化持续响应，有效提高安全运维的响应速度，降低用户的平均响应时间。

2 工业边缘平台安全防护措施

（1）技术层面

a）物理安全。对边缘平台进行外围物理加固，防止边缘平台所依托的设备遭受雷击、火灾、潮湿、盗窃等;

b）访问控制。提供并启用登录失败处理功能（包括结束会话、限制非法登录次数、自动退出等）; 严格限制用户访问权限，按照安全策略要求控制用户对业务、数据、网络资源等的访问; 对用户交互的各类信息进行必要的安全过滤;

c）边界隔离。主要包括:

虚拟化隔离：将微服务组件部署在单独的容器中运行，使得微服务组件在运行过程中，不会破坏其它运行软件，以及不被其它软件破坏;

多租户隔离：在系统、程序和数据等层面进行多租户隔离，以实现不同租户之间、同一租户的不同应用系统之间严格的访问

控制和认证授权，同时还要保护组合的应用数据免受攻击;

数据库隔离:通过隔离数据库(每个租户使用单独的数据库)、隔离存储区(多个租户使用相同的数据库，但是每个租户使用一个单独的 Schema)、合理设计库表结构来实现不同租户之间的数据隔离(多个租户使用相同的数据库，相同的 Schema，但是每个组合访问不同的表或者表的不同部分);

d)接口安全。调用平台服务时在接口处进行认证，并在接口处部署安全管控措施。接口协议操作应通过接口代码审计、黑白名单等控制措施确保交互符合接口规范;

e)数据安全。通过对网络传输的关键敏感数据进行加密，防止析出报文内容;针对不同接入方式的用户，采用不同的认证方式，检查使用数据的合理性和有效性;如需把信息共享给第三方应用，应对信息进行脱敏处理，严格保护用户隐私不被泄露;

e)容器安全。通过沙箱机制保护运行虚拟设备的进程;对边缘平台中的容器进行完整性校验和安全性检查,对容器镜像进行数字签名;严格监管对容器服务的访问,避免不必要的权限升级;提供标准的接口来访问关键敏感信息;关键敏感信息进行加密存储和传输;

f)边缘协同安全。采用 Kubernetes 等技术限定特定应用运行所需的资源。

(2)管理层面

a)人员管理。提升数据使用人员的保密意识，确保其自觉遵

循安全策略;

b）访问控制。严格数据访问权限划分，及时终止离职人员的访问、操作等相关权利，及时注销相应账号;

c）安全检查。定期进行安全检查，防止 SQL 注入等攻击;

d）安全审计。一是进行微服务组件操作安全审计，对微服务组件内部使用人员的操作进行审计，其中审计覆盖每个用户，内容应包括用户重要行为、微服务组件资源的异常使用和重要操作命令的使用等; 审计应重点关注微服务组件资源的异常使用和重要操作命令的使用等重要安全事件。二是进行边缘协同安全审计，通过对运行节点所使用的主要资源（如 CPU、内存、磁盘使用情况以及网络带宽占用情况）进行审计，对异常资源使用给出报警提示，审计记录在有效期内部允许非法访问、篡改和删除。

3 工业边缘网络安全防护措施

（1）技术层面

a）5G 新技术安全。5G 在 mMTC 大规模工业互联网领域，需要建立群组认证机制，采用专用安全芯片，选择合适的轻量化安全机制，满足工业生产的实时性需求，均衡可靠性和安全性需求之间的矛盾;

b）网络设备安全。检测 LoRa 低功耗广域网接入的虚拟化物联网设备，避免从 mMTC 对网络发起 DDoS 分布式拒绝服务攻击;

c）网络协议安全。丰富边缘计算云平台中支持的网络协议，

完善边缘技术的网络安全服务。

（2）管理层面

a）安全检测。加快边缘计算安全设备的相关产品的检测，生产单位的认证评估工作;

b）漏洞防护。边缘设备制造商需要及时更新设备驱动，避免漏洞利用攻击;

c）切片管理。运营商要加强网络切片安全管理，在 NFV 网络功能虚拟化中，保障无线网子切片、承载网子切片和核心网子切片的逻辑隔离。

4 工业边缘节点安全防护措施

（1）技术层面

a）安全芯片。对于具有高安全需求的边缘设备，可充分利用设备主控芯片的安全特性（如 TrustZone、OTP 等），结合利用高性能安全芯片，实现硬件级的高强度安全，为设备的安全启动、固件安全更新、敏感数据加密等功能提供坚实基础。其中，安全芯片主要提供密钥安全存储、芯片内的加解密、随机数生成等安全功能;

b）安全启动和可信度量。通过安全启动和可信度量确保设备启动过程中加载运行的引导程序、操作系统内核、应用程序等的完整性未遭篡改。此外，还可利用动态度量技术，验证设备运行阶段执行的应用程序的完整性;

c）操作系统加固。采取访问控制等措施对边缘设备操作系

统进行加固。系统开放的端口均应是业务必须的，禁止存在可绕过系统安全机制对系统或数据进行访问的功能；

d）安全更新。边缘设备获取固件更新数据时应采用安全通信信道，以保证固件更新包的机密性和完整性。固件更新包中应携带数字签名，用于边缘设备对固件更新包的来源和完整性进行校验，有效避免非法固件更新包；

e）非法接入检测。构建工业互联网边缘设备指纹识别库、属性信息库等，从设备开放的服务端口、设备协议标语、设备对特定请求的响应报文特征、设备 Web 主页特征等多个维度提取特征以刻画不同设备的差异，实现边缘设备的类型、厂商、属性识别，支撑基于精准设备识别的非法设备接入检测功能；

f）口令安全。边缘设备口令安全保护可从口令生成、口令使用和口令管理三方面采取措施；

g）数据安全保护。采用加密等技术手段防止边缘设备上的用户配置数据、用户隐私数据、音视频数据等关键数据泄漏，密钥可在设备首次启动时随机生成，实现一机一密；

h）终端监测分析。对边缘设备运行状态、安全状况等采取有效的安全监测及分析机制，定期或不定期地对边缘设备进行安全扫描，掌握边缘设备的系统漏洞情况、运行状况等；

i）安全审计。边缘设备上所有用户活动及引起系统变更的操作都应记录日志并定期进行审计。审计日志应能支撑事后审计需要，至少包括用户标识、时间戳、事件类型、被访问资源名称、

操作结果等信息，对于资源受限无法在本地存储日志的终端设备，应当支持日志上传功能；

g）物理安全防护。如果边缘设备支持户外部署，应当支持提供位置信息的能力；如果边缘设备采用插卡方式进行网络身份认证，应当具备防止卡片被替换或拔除的能力；如果设备被非法拆除，应能够记录并发送报警；当遭遇物理入侵时，边缘设备应能够自动复位系统，防止数据泄漏。

（2）管理层面

a）供应链安全。供应链系统具有参与主体复杂、过程环节众多、产品传递跨地域等特点，易于受到来自内外部不利因素的影响和威胁。为缓解制造安全风险，确保软件和硬件完整性，可在边缘设备生产的关键环节，如软件提供、芯片烧录/校验、软件加载、生产测试等，采取防篡改、防植入、防调包等安全管控措施，以防范未授权的硬件替换、软件植入或篡改、病毒感染等风险。其中，供应链用于生产的软件烧录、软件加载、组装和测试网络应隔离于公司的办公系统或公共互联网之外。边缘设备制造商等应参考国际通用的供应链安全管理体系，并在明确供应链运行环境、识别各环境威胁、采取风险评估和应对措施的基础上，建立全面的供应链安全管理体系，并不断更新和完善；

b）设备安全检测。边缘计算服务开发商应采用安全软硬件安全检测分析工具，对边缘设备产品进行全方位的安全检测，包括漏洞挖掘、代码审计、渗透测试等；

c）设备研发安全。边缘计算服务开发商应该参考业界最佳安全实践，将安全活动（如安全设计、安全开发、安全测试等）融入设备相关的软硬件研发流程中，制定产品研发安全管理流程，确保安全活动有效落地，从而提升边缘设备产品的机密性、完整性和可用性，增强隐私保护能力；

d）环境安全管理。边缘设备的应用企业应基于工业现场边缘设备、边缘服务器、数据库等核心软硬件明确重点物理安全防护区域；企业对于重点物理安全防护区域应采取物理隔离、访问控制、视频监控、专人职守等物理安全防护措施；

e）设备安全管理。对于边缘设备上必须开放的物理接口，应建立外接接口管理制度，并通过访问控制等技术手段防止未授权访问，避免非法接入；

f）安全监测管理。部署网络安全监测设备，及时发现、上报、处置针对边缘设备的网络攻击或异常行为；

g）备份和恢复安全。采用定期备份等措施，确保在关键数据丢失时可以及时恢复数据；应对所备份的关键业务数据定期进行恢复测试，确保备份数据的可用性。

5 工业边缘数据安全防护措施

（1）技术层面

a）数据保密性。结合属性加密、代理重加密和同态加密等应用加密理论，设计低时延、支持动态操作的分布式安全存储系统，正确处理网络边缘设备与云中心之间的协同性，保障数据保密性；

b）数据完整性。通过设计支持多源异构数据和动态数据更新的完整性审计方案加强工业互联网边缘计算数据完整性保护;

c）可搜索加密。构造安全索引使其适用于资源受限的网络边缘设备以及设计分布式可搜索加密算法解决数据密文检索问题;

d）差分隐私（Differential Privacy）技术。按照差分隐私算法在本地对数据进行处理（一般是添加随机噪声），处理之后的数据可以上传到边缘数据中心或者云端。即通过在数据中添加噪声，保护数据隐私;

e）安全多方计算技术（Secure Multi-Party Computation）。安全多方计算技术实现了在数据无需聚合的基础上，多方之间进行数据联合密文计算。使用安全多方计算技术，边缘节点之间、边缘数据中心之间、边缘数据中心与云端进行联合计算时，无需把所以数据聚合到一起，避免了数据传输中的数据泄露风险、也防止了数据传输后的数据不可控和数据确权问题;

f）联邦学习技术（Federated Learning）：联邦学习技术实现了在数据无需聚合的基础上，多方之间进行机器学习联合建模。使用联邦学习技术，可以不用把边缘设备产生的数据上传到云端，在本地就可以完成模型的训练和预测。

（2）管理层面

a）数据安全组织。制定组织的工业边缘数据安全目标、数据安全策略和规划，统一数据安全管理规范体系。结合工业数据

安全合规监管要求和业务发展要求，制定工业互联网边缘计算数据安全整体解决方案并实施。建立监控审计机制--工业互联网边缘计算数据安全工作和监督审计机制，推动并协助执行组织的建立，监督工作有效开展;

b）数据安全管理策略制度。建立工业互联网边缘计算数据全生命周期安全管理规范。明确数据采集、存储、传输、处理、使用等数据全生命周期活动的目的、用途、方式、范围、采集源、采集渠道等内容，对外部数据提供方及被采集者提供的数据进行确认，满足相关法律法规要求。在数据采集、存储、使用、加工过程的数据保护过程中，明确相关重要数据的安全控制措施，确保重要工业数据不被泄露;

c）数据分类分级。对涉及的边缘计算数据进行分类分级，组织专家评审确定数据分级。涉密信息的处理、保存、传输、利用按国家保密法规执行;

d)数据安全风险评估。建立边缘计算数据的风险评估流程。明确数据采集的风险评估方法、评估周期、评估对象，识别相关的法律法规并纳入合规评估; 定期开展边缘计算数据安全风险评估及分析工作，包括数据资产、数据威胁识别、数据脆弱性识别和边缘计算数据安全风险分析;

e）应急评估和处置。建立边缘计算数据安全应急机制、组织体系、技术支撑队伍及专家队伍等。监测预警包括监测、预警、分析研判等。应急处置包括信息报送与共享、事件处置、调查与

总结等。预防保障包括日常管理、漏洞管理、宣传培训、应急演练等；明确监测预警、应急处置、预防保障评估项，定期开展评估；

f）实时数据安全监控与分析。具备实时数据安全监测与分析技术措施，对全部业务系统进行 7*24 小时实时监测并形成监测记录。具备监测技术措施，对网络流量、日志信息、运行状态、性能状况进行监测、安全策略和系统配置、安全告警、资产漏洞、访问控制、网络异常行为、威胁信息或网络攻击事件等进行监测。

6 边缘接入平台安全防护措施

（1）技术层面

a）边缘智能产品安全。对智能产品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；

b）边缘-云网络传输信道的安全防护。加强边缘网络数据传输安全防护。采用 IPSec VPN 或者 SSL VPN 等加密隧道传输机制或 MPLS VPN 等专网进行重要数据传输，防止数据泄漏、侦听和篡改。优先采用混淆、替代等方式混合的高安全加密方法或高级安全加密标准，支持非对称加密技术，支持 IP 节点绑定加密。

（2）管理层面

a）风险管理。通过风险评估、风险管理、风险处置等流程对边缘侧的数据安全、代码安全、应用安全、数据安全、访问安全

等安全属性进行评价，识别、控制、消除、减小可能影响工业互联网平台安全的不确定事件，并对风险等级进行判定，采取相应控制措施;

b）运维管理。对运行过程中基础环境、网络、安全、主机、中间件、数据库乃至核心应用系统产生的影响其正常运行的安全事件（包括关联事件）展开监控、告警、应急响应、安全评估等，以保证接入安全。

四、工业互联网边缘计算安全未来展望

下一步应重点从体系架构构建、标准制定、技术产品研发、评测体系健全、人才建设等五个方面，提升工业互联网边缘计算安全防护能力。

一是构建统一体系架构。工业互联网边缘计算中涉及移动通信网、工业以太网、无线局域网、公共互联网等多种网络接入和承载技术，导致工业边缘计算应用的技术体系存在一定的差异性。此外，工业互联网边缘计算的系统架构需要不断整合容纳 5G、区块链、信息物理系统等新技术，以促进工业生产智能化、高效化。因此，亟需加快工业互联网边缘计算体系架构标准化、规范化建设，基于软件定义设备、虚拟化、容器隔离、微服务等关键技术，打造支撑工业互联网边缘计算的通用商用系统架构，满足不同业务需求，实现工业云业务扩展到边缘，并可部署在电信设备、工业网关或者边缘工业数据平台等不同位置，实现跨行业、跨平台的安全高效互联互通。

二是加快标准研制与落地。工业互联网边缘计算安全责任主体涉及边缘计算服务开发商、客户、边缘计算安全服务提供商、第三方评估机构等不同角色，同时边缘计算部署过程中需要跨越计算、存储、网络等方面进行长链条的技术方案整合，因此亟需制定工业互联网边缘计算安全相关标准，发挥标准的指导作用，解决行业、企业在应用工业互联网边缘计算技术过程中存在的安全管理、安全部署、安全防护等方面的标准化问题，实现互联网企业、通信设备企业、通信运营商、工业企业等多方利益在商业模式下的互利共赢。

三是开展关键核心技术研发和产品研制。推进区块链、人工智能等新兴前沿技术在工业互联网边缘计算安全中的应用研究，加大对边缘计算分布式环境下的多源异构数据传播管控和安全管理的核心技术攻关力度，研发设计适用于工业互联网环境下的多种形态边缘计算安全产品，提供差异化的工业边缘服务能力，开展在大连接、异构数据等复杂工业条件下，能够与边缘节点融合的一体化安全机制研究。

四是健全边缘计算安全应用评测体系。依据《网络安全法》《密码法》、网络安全等级保护 2.0 等相关政策标准，在工业和信息化主管部门指导下认定一批第三方边缘计算安全应用测评机构。搭建边缘计算安全应用仿真测试环境，强化边缘计算安全应用的合规性、有效性，安全技术产品的安全性、稳定性，以及与工业互联网的适应性等应用评测能力。面向智能制造、无人驾

驶等重要工业互联网应用领域，开展边缘计算安全应用评测服务，为保障边缘计算安全运行提供支撑。

五是加大人才队伍建设力度。健全多层次多类型的工业互联网与边缘计算安全复合型人才培养和服务体系，支持边缘计算安全应用实训基地建设。积极推进产学研结合，推动企业、科研机构和高等院校建立并完善工业互联网边缘计算应用安全人才联合培养模式。依托国家科技计划、示范工程和国际合作，培养高层次人才和领军人才，加快引进国际高端人才。

附件：术语

1.**工业互联网**：工业互联网是利用新一代信息技术将工业中的人、机、物、法、环等各生产要素进行全面互联，支撑工业的智能化发展，更大范围、更高效率、更加精准地优化生产和服务资源配置，实现以数字化、网络化、智能化为主要特征的新型工业发展模式。

2.**边缘计算**：边缘计算是指一种在数据源和云计算中心之间的网络边缘进行计算的新型计算模式，它利用网络边缘侧的计算、通信、存储等资源和能力来处理、分析数据，并就近提供边缘智能服务，实现低时延、高带宽、高可靠性、高安全性和隐私保护的行业应用。

3.**工业互联网边缘计算**：工业互联网边缘计算是一种将部分数据处理和数据存储放在工业互联网边缘节点的分布式计算方式，其通过融合工业互联网边缘侧计算、通信和存储能力，就近提供边缘智能服务，并可通过云边协同机制为工业互联网平台提供数据支撑，从而实现工业互联网泛在互联、实时业务、可靠服务、数据优化、边缘应用智能、安全和隐私保护等多方面应用需求。

4.**边缘算力设备**：在工业互联网中的数据源和云计算中心之间任一具有计算能力的设备。

5.**工业互联网边缘计算安全**：在工业互联网中部署和应用边缘计算所涉及的安全要素。

6.**工业互联网边缘计算安全角色**：参与工业互联网边缘计算安全活动的相关方。

7.**客户**：为使用工业互联网边缘计算服务而处于一定业务关系中的参与方。

8.**边缘计算安全服务提供商**：支撑或协助边缘计算服务开发商或客户的安全管理、技术和运维。

参考文献

[1] 工业信息安全产业发展联盟. 工业信息安全标准化白皮书，2019.12.

[2] 边缘计算产业联盟与工业互联网产业联盟. 边缘计算安全白皮书，2019. 11.

[3] 亚信安全.2019 威胁情报态势分析，2020.2.

[4] 施巍松, 张星洲, 王一帆, 等. 边缘计算: 现状与展望[J]. 计算机研究与发展, 2019, 56(1): 69-89.

[5] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.

[6] 陶耀东, 徐伟, 纪胜龙. 边缘计算安全综述与展望[J]. 计算机集成制造系统, 25(12): 3043-3051.

[7] Schneider S. The industrial internet of things (iiot) applications and taxonomy[J]. Internet of Things and Data Analytics Handbook, 2017: 41-81.

[8] Zhang J, Chen B, Zhao Y, et al. Data security and privacy-preserving in edge computing paradigm: Survey and open issues[J]. IEEE Access, 2018, 6: 18209-18237.

[9] Dai W, Nishi H, Vyatkin V, et al. Industrial Edge Computing: Enabling Embedded Intelligence[J]. IEEE Industrial Electronics Magazine, 2019, 13(4): 48-56.

[10] Zhang Y, Huang H, Yang L X, et al. Serious Challenges and Potential Solutions for the Industrial Internet of Things with Edge Intelligence[J]. IEEE Network, 2019, 33(5): 41-45.

[11] Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2018, 78: 680-698.

[12] Shirazi S N, Gouglidis A, Farshad A, et al. The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective[J]. IEEE Journal on Selected Areas in Communications, 2017, 35(11): 2586-2595.

[13] Esposito C, Castiglione A, Pop F, et al. Challenges of connecting edge and cloud computing: A security and forensic perspective[J]. IEEE Cloud Computing, 2017, 4(2): 13-17.

[14]GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[15]GB/T 35273-2020 信息安全技术 个人信息安全规范

[16] GB/T 31167-2014 信息安全技术 云计算服务安全指南