《轻工行业工业互联网企业网络安全分类分级防护要求》行业标准编制说明（征求意见稿）

一　工作简况

（一） 任务来源

根据《工业和信息化部办公厅关于印发 2023 年第一批行业标准制修订和外文版项目计划的通知》（工信厅科〔2023〕18 号）要求，由中国轻工业信息中心会同有关单位开展行业标准《轻工行业工业互联网企业网络安全分类分级防护要求》（计划号 2023-0133T-QB）编制工作。主要起草单位：中国轻工业信息中心、中国信息通信研究院、中国电子技术标准化研究院、中国轻工业企业管理协会。

该项目属于 2023 年第一批新型基础设施标准项目，计划完成时间为 2025 年 6 月。

工信部高度重视工业互联网发展，多措并举推动工业互联网网络、平台、安全三大体系建设工作，贯彻落实国务院工作部署，推动出台系列政策文件，加快工业互联网安全体系化布局，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》，工信部等主管部门发布了《工信部、市场监督管理总局等十部门关于印发加强工业互联网安全工作的指导意见的通知》《工业互联网创新发展三年行动计划（2021—2023 年）》《工业和信息化部办公厅关于开展工业互联网企业网络安全分类分级管理试点工作的通知》，提出工业互联网安全相关工作要求，不断强化工业互联网企业网络

安全分类分级管理。目前，轻工企业网络安全防护工作与主管部门的要求相距甚远，远不能适应轻工企业工业化、信息化融合发展的需要，为推动行业内工业互联网企业网络安全分级管理工作部署落地实施，制定并实施适应轻工行业的工业互联网企业网络安全防护标准是十分必要的。

（二）主要工作过程

1.起草阶段

（1）成立标准编制组，技术调研和资料收集，形成标准草案

牵头单位采用多种方式广泛征集编制单位，通过 2022 年 1 月召开的标准预研启动会，2022 年 4 月召开的轻工行业内外单位的专题调研会，2022 年 5 月面向轻工企业和有关网络安全技术厂商参加的调研活动，征集组成了既有中国信息通信研究院、中国电子技术标准化研究院、国家工业信息安全发展研究中心的专业院所，又有轻工行业内有代表性的实力企业和网络安全技术专业服务公司参加的标准编制组，为标准编制工作奠定了坚实的基础。

通过认真筹备，2023 年 8 月，正式成立标准编制组，并召开了编制组成立暨第一次工作会议。会议就标准范围和应用对象、草案主要技术内容、调研验证工作、编制组分工、工作进度计划等重要问题形成了相关决议。

标准编制组开展专题调研，对轻工行业内金牌厨柜、江苏银宝盐业集团、四川亚度家具、内蒙古金海伊利乳业有限责任公司等企

业，了解网络安全防护技术现状及公司网络安全防护采取的主要技术手段和措施，最大的网络安全隐患和采取的主要技术手段等问题，根据调研情况完善标准草案。

（2）召开标准研讨会、完善标准内容

2023 年 11 月，针对标准编制中需解决的问题，编制组面向轻工企业又开展了专题调研，根据反馈意见梳理标准框架和内容，进一步修改完善标准征求意见稿。

2023 年 12 月，编制组召开第二次工作会议，有关专家和代表对《标准》提出修改意见和建议。会议还对编写分工、上位国标协调、增强编制组广泛性做出了有关决议。

2024 年 4 月，编制组召开第三次工作会议，编制组成员和专家共同讨论了行业特色体现、进一步完善思路及具体条款修改等方面内容。会议提出：整体框架要与国标协调一致，基本要求以引用为主，在此基础上结合行业特点进行细化和丰富，并建议标准名称修改为“轻工行业应用工业互联网的工业企业网络安全分级防护要求”，编制组根据会议建议，对标准进行了修改。

2024 年 6 月，编制组赴江苏银宝盐业集团开展调研和标准验证工作。与银宝盐业有关人员座谈、研讨标准，了解企业工业互联网企业网络现状和对标准的需求，并对标准主要内容进行验证分析。

2024 年 11 月，编制组根据调研和标准验证工作的情况对标准进行了修改、完善，完成了标准征求意见稿。

（三）主要参加单位和工作组成员及其所做的工作

本标准起草单位：中国轻工业信息中心牵头，中国信息通信研究院、中国电子技术标准化研究院、国家工业信息安全发展研究中心、中国轻工业企业管理协会、圣奥科技股份有限公司、江苏省银宝盐业有限公司、北京珞安科技有限责任公司、长扬科技（北京）股份有限公司。

工作组成员：赵秀江、郭和生、李玮、李诗婧、李琳、曲海阔、王新阳、门永超、李文新、王会成、赵华、高迪、刘海涛、马亚丽、吴佳蓓等。

工作分工：赵秀江、郭和生负责该项目的总体统筹工作，确定标准主要内容框架及编制说明框架；李玮、马亚丽负责协调、组织，高迪、刘海涛负责标准主要内容和编制说明的编写；李诗婧、李琳、曲海阔参加标准部分内容的编写；门永超、王新阳主要负责网络安全防护技术内容梳理和相关内容校对；李文新、王会成、赵华参加标准附录和部分内容的编写；马亚丽、吴佳蓓负责研究分析及资料查证和编写编制说明。

二、标准编制原则和主要内容

（一）基本原则

标准编制遵循以下原则：

1. 协调统一：与工业互联网安全相关标准和法规协调统一满足工业互联网企业安全防护相关标准的基本要求和原则，与相关的国家标准和法规协调统一。

2.体现轻工行业特点：反映轻工不同企业生产和网络安全现状和未来发展，满足轻工各类企业网络安全防护工作分类施策的需求。

3.适应性和可操作性：力求标准有较好的适应性和可操作性，在满足网络安全国家标准的基础上，根据轻工行业的具体情况，细化网络安全防护要求，使标准具有良好的可操作性。

本标准起草过程中，主要按照 GBGB/TGB/T 1.1—2020《标准化工作导则 第 1 部分：标准的结构和编写》、GB/T 20000《标准化工作指南》、GB/T 20001《标准编写规则》等要求进行编写。本标准编制过程中，主要依据和参考了以下标准或文件：

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069《信息安全技术 术语》

GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南

GB/T 33008.1 工业自动化和控制系统网络安全 可编程序控制器（PLC）第 1 部分：系统要求

GB/T 33009.1 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

GB/T 44462.1-2024 工业互联网企业网络安全 第 1 部分：应用工业互联网的工业企业防护要求

GB 50016 建筑设计防火规范

GB 50057 建筑物防雷设计规范

GB 50343 建筑物电子信息系统防雷技术规范

《工业互联网企业网络安全分类分级管理指南》（试行） 工业和信息化部 2021

《工业互联网企业网络安全分类分级评估操作手册》 中国信息通信研究院、国家工业信息安全发展研究中心编制 2021（注：该手册是主管机构网络安全等级评估的具体和最具权威性依据）

（二）标准主要内容的论据

1.标准主要内容及适用范围

本标准规定了轻工企业分类和工业互联网企业网络安全防护级别，以及工业企业在设备、控制、网络、应用平台软件、管理、物理环境等方面不同级别的网络安全防护要求。

本标准适用于轻工行业应用工业互联网的工业企业网络安全分级防护工作。

2 标准主要内容的依据

（1）行业调研分析基础

轻工行业属于工业互联网中重点行业领域，随着企业设备联网、企业上云数量明显增加，控制系统联网、边界隔离不到位等大量安全隐患日益突出，工业互联网安全事件频发。

中国轻工业信息中心从 2021 年 9 月开始对若干轻工头部企业和安全服务商开展了网络安全相关调研，其中轻工行业企业包括联网企业、平台企业和标识解析企业，均为规上企业，主要涉及家具、家电、电池、食品等。受访企业在安全投入上，平均不到营收的 0.5%，最高 2%。所有受访企业均部署有网络安全设备并拥有重要数

据或核心数据，67%的受访企业建立了安全管理制度体系并采取了安全检测审计技术，50%的受访企业参加了分类分级试点工作，超过30%的受访企业遭遇过网络安全事件。在上云上平台方面，所有受访企业均已上云，其中 67%的受访企业购买公有云平台，50%拥有自建云平台。业务系统上云的企业占比 83%，设备上云企业占比 34%，主要掌握网络安全防护措施的企业占比不到 50%。

轻工行业企业数量众多，规模以上企业数量达 12.97 万家（2023年统计数据），涉及家电、家居、食品、照明等行业，随着工业互联网发展进入落地深耕阶段，企业设备联网、企业上云数量明显增加，控制系统联网、边界隔离不到位等大量安全隐患日益突出，工业互联网安全事件频发，暴露出轻工企业安全防护存在较大缺陷，影响了企业生产和营销，轻工行业企业网络安全防护技术和能力亟待提高。

（2） 标准主要内容确定的依据

1） 标准结构和内容要素依据

标准结构和安全防护要求等内容要素以国标 GB/T 44462.1-2024 为依据，标准结构和内容要素与其一致，

企业网络安全防护的初始级、基本级、增强级三个级别的网络安全防护主要从以下 7 个方面提出要求，其内容要素的结构与 GB/T 44462.1-2024 一致，具体包括：设备安全防护、工业控制安全防护、网络安全防护、数据安全防护、应用平台软件安全防护、安全管理要求、物理环境安全要求。

2） 与 GB/T 44462.1-2024 和其他行业标准比新增内容和细化内容

本标准以GB/T 44462.1-2024为主要依据，其网络安全防护要求遵循GB/T 44462.1-2024的基本规定，基本要求直接引用GB/T 44462.1-2024的条款。

本标准采用以下描述方式：XXXXX除符合GB/T 44462.1-2024中7.1.2.2的要求外，还应满足以下要求：

a) …… ;b)……;c)……。

标准中所列各条分列项内容是在 GB/T 44462.1-2024 中各相关要求的基础上，提出了细化要求或根据轻工企业的特点增加的新要求（即 GB/T 44462.1-2024 没有的内容），特别针对轻工行业智能家居产品远程运维、产品交互、互动设计、产品在线检测、产品可追溯等的网络安全以于重点关注，使本行业标准体现轻工行业特点，适应轻工企业网络安全防护的需求，以满足上级主管部门网络安全防护评估的要求。

3） 细化要求和新增要求的主要依据

在满足 GB/T 44462.1-2024 的各级安全防护要求的基础上，对其各项要求做进一步的细化要求，如明确设备、系统的对象，明确安全防护重点；在 GB/T 44462.1—2024 对各项安全防护要求的方面，结合轻工行业生产实际和安全防护需求增加进一步的要求，以确保符合相应安全防护等级的评定要求。

细化和新增要求主要依据对行业内有代表性企业和国内有关网

络安全防护公司调研和标准验证工作。

标准编制组针对 GB/T 44462.1-2024 中相关安全防护要求的细化要求和新增的安全防护要求的内容先后多次调研分析行业内有代表性的企业，并实施验证，总结企业网络安全防护管理和技术工作的实践经验。

标准编制组在立项研究和标准调研过程中通过现场参观考察、座谈沟通和调研函等多种方式开展工作，先后对金牌厨柜、四川亚度家具、内蒙古金海伊利乳业有限责任公司、新凤鸣集团股份有限公司、天能电池集团股份有限公司、四川亚度家具有限公司、上海海立（集团）股份有限公司、新海科技集团有限公司等十余家轻工行业有代表性的企业进行充分的调研。对上海派拉软件股份有限公司、北京安帝科技有限公司、北京安数云信息技术有限公司、杭州立思辰安科科技有限公司、北京六方云信息技术有限公司、瑞数信息技术（上海）有限公司、西安四叶草信息技术有限公司、北京天空卫士等 11 家网络安全厂商进行了调研。

对网络安全厂商主要调研了解以下问题：

a) 网络安全防护技术现状及公司网络安全防护采取的主要技术手段和措施。

b) 公司服务企业的类型 、提供哪些安全项目。

c) 最大的网络安全隐患和采取的主要技术手段和措施。

对轻工有关企业主要调研了解以下问题：

a) 企业工业互联网安全防护现状、企业安全防护管理和安全防

护等级评定情况。

b）企业目前主要的网络安全隐患，有无发生过重大网络安全事件。

c）企业为应对隐患可能的重大网络安全事件采取的主要技术手段和措施。

d） 企业对本标准修改完善的意见和建议。

调研和标准验证工作紧密围绕设备安全防护、工业控制安全防护、网络安全防护、数据安全防护、应用平台软件安全防护、物理环境安全要求等相关内容，各相关企业根据其网络安全防护现状和发展需求，并结合企业两化融合及网络安全管理和建设的实践经验，补充提出了许多针对性强的网络安全防护的具体细化要求，在企业实施并取得了积极成效，还对标准的主要内容进行验证（具体见三.主要试验[或验证]情况分析），这些都为标准的技术内容提供了有力的支撑，完善了标准技术内容，提高了标准的可操作性。

4） 标准主要内容的依据

“5　轻工行业工业互联网企业网络安全防护级别” 主要依据

本标准中轻工互联网企业网络安全防护等级与 GB/T 44462.1-2024 和《工业互联网企业网络安全分类分级管理指南》（试行）（简称“指南”）完全一致。GB/T 44462.1-2024 和“指南”中规定，由低到高划分为：一级、二级、三级，其分别对应安全防护级分别为：初始级防护、基本级防护、增强级防护。“指南”规定：企业定级采

用计分方式进行，计分从四个维度：企业所在行业的网络安全影响程度（20 分）、企业规模（20 分）、企业应用工业互联网的程度（30 分）和企业一旦发生工业互联网网络安全事件的影响程度（30），满分为 100 分。评分大于等于 80 分的，为三级企业； 评分大于等于 60 分，且小于 80 分的，为二级企业；评分小于 60 分的，为一级企业。企业按评分自主定级，由主管机构按 GB/T 44462.1-2024 等相关文件的要求，评估定级。

“6.1 防护对象”主要依据

这部分内容依据 GB/T 44462.1-2024 中第 6 章“6 应用工业互联网的轻工企业安全防护对象和范围”，结合轻工行业网络安全防护需要，细化企业网络安全防护的对象。

“6.2 防护范围”主要依据

轻工行业应用工业互联网的工业企业网络安全防护内容具体包括：设备安全防护、工业控制安全防护、网络安全防护、数据安全防护、应用平台软件安全防护、安全管理要求、物理环境安全要求。

这些内容与 GB/T 44462.1-2024 和“指南”一致，引用 GB/T 44462.1-2024 的第 6 章，“6 应用工业互联网的工业企业安全防护范围”，这也是保证主管部门网络安全防护等级评定时，轻工企业能够符合其网络安全防护等级评定的需要。

“7 轻工企业工业互联网初始级安全防护要求”

“7.1.1 工业主机安全” 主要依据

这部分内容主要依据 GB/T 44462.1-2024 中 7.1.1.1，参考《工业互联网企业网络安全分类分级评估操作手册》中“设备安全”相关内容，明确了轻工行业工业主机的具体对象，结合对轻工行业有关企业和其他行业调研了解的情况，提出了 ERP、MES、物料管理等业务管理系统的服务器，产品定位追踪、安全监控、能源计量、环境控制等工序的 DCS 主机、PLC 主机等主机设备作出相应要求。

“7.1.2　网络设备安全”主要依据

这部分内容主要依据 GB/T 44462.1-2024 中 7.1.2 的内容，结合对轻工行业有关企业和其他行业调研了解的情况，明确了轻工企业生产区域的现场控制网络、生产执行层网络、生产管理层网络等网络设备应符合 GB/T 44462.1-2024 中 7.1.2 的要求。

“7.2.1　应用工业互联网的工业企业控制系统安全”　主要依据

可编程逻辑控制器（PLC） 、集散控制系统（DCS）是工业企业控制系统中重要的设备，这部分内容主要依据GB/T 33008.1中“第5章PLC 系统网络安全技术要求”和GB/T 33009.1 中“4.2　DCS防护总体要求和原则”等相关内容，结合轻工企业生产控制中的安全管控、能源管控、环境管控、自动化仓储等重要系统安全防护需求。

“7.2.2　控制软件安全 ”　主要依据

这部分内容主要依据GB/T 33008.1中“第5章PLC 系统网络安全技术要求”相关内容。

“7.2.3 配置安全”“7.2.4 智能装备控制安全”和“7.3 网络安全” 主要依据

这些内容主要依据GB/T 44462.1-2024，与其中的7.1.2.3、7.1.2.4、7.1.3的内容一致。

“7.4 数据安全防护要求”主要依据

这部分内容主要依据GB/T 41479-2022和GB/T 35273-2020 ，并结合轻工行业生产、经营各相关环节中对数据的基本需求，作细致的要求。

“7.6 安全管理要求”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中“安全管理制度、安全管理机构、人员要求”等内容，手册中94～113条中相关内容，结合对行业内企业工业互联网企业安全防护管理和安全防护等级评定调研情况，总结提炼轻工企业网络安全管理的经验后形成。

“8 基本级安全防护”

“8.1.1 工业主机安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中设备安全的相关内容，结合轻工有关企业生产和网络系统运营设备企业特点和调研了解的情况，从设备唯一性标识，如品牌、型号、版本号、序列号，设备接口访问，软硬件安装和使用等方面提出进一步的要求。

“8.1.2 网络设备安全防护要求”主要依据

这部分内容主要引用《工业互联网企业网络安全分类分级评估操作手册》中 “网络设备安全”的内容 中77、78条，以对GB/T 44462.1-2024中“网络设备安全防护要求”的内容做细化要求。

“8.1.3 工业控制设备安全防护要求”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中 “控制设备安全 ”的内容中11、14、15条的内容。并根据对轻工企业和一些网络安全厂商调研、分析情况对工业控制设备身份鉴别、控制设备的软驱、光驱、USB接口、串行口或多余网口处理和监控管理以及安全配置核查审计提出要求。

“8.2.1 应用工业互联网的工业企业控制系统安全”主要依据

这部分内容主要引用《工业互联网企业网络安全分类分级评估操作手册》中 “联网控制系统安全”中27～32条的内容。结合轻工企业工业企业控制系统情况，对GB/T 44462.1-2024中“工业企业控制系统安全”的内容做细化要求，以满足轻工企业网络安全分类分级评估和管理的要求。

“8.2.2 控制软件安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中“组态软件安全”的内容中36～38条的内容，结合对轻工行业企业和其他行业调研了解的情况提出。

“8.2.3 配置安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中“组态软件安全”内容的44～47条，结合对轻工行业

企业和网络安全服务公司调研了解的情况，对企业生产和网络系统的PLC、DCS、SCADA等工控系统软件本地备份、定期数据备份，以及软件更新、补丁等提出要求。

“8.3.1 架构安全” 主要依据

这部分内容主要引用《工业互联网企业网络安全分类分级评估操作手册》中 “架构安全”的内容中59～63条的内容，对GB/T 44462.1-2024中“架构安全要求”的内容做细化要求，以满足轻工企业网络安全分类分级评估和企业网络安全管理的要求。

“8.3.2 边界安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中“组网安全”的内容中54和56条的内容。并结合轻工企业的具体情况，明确提出了产品追溯、物流追踪、装配定位等用于生产管理的无线网络和其他有线网络之间实现逻辑隔离等边界安全要求，细化了企业网络边界安全相关要求。

“8.4 数据安全防护要求”主要依据

这部分内容主要依据GB/T 41479-2022和GB/T 35273-2020，并结合轻工行业产品可追溯系统、产品在线检测系统、智能家居和智能穿戴产品远程运维系统、产品交互互动设计系统等轻工企业重要数据安全的需求，作细致的要求。

“8.5.1 平台软件安全”主要依据

这部分内容主要参考《工业互联网企业网络安全分类分级评估操作手册》中“组态软件安全”的相关内容，结合对轻工行业内部

分企业调研、分析的情况后提出。

“8.5.2　工业APP安全”主要依据

这部分内容主要按照《工业互联网平台企业安全防护规范（试行）》中的工业App安全防护要求，结合对轻工行业内部分企业调研、分析的情况后，对工业App开发、使用的重要和关键环节，如开发环境与实际运行环境、测试数据和测试结果受控、软件开发外包合同等方面提出细化要求。

“8.6　安全管理要求”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中 “安全管理制度、安全管理机构、人员要求”等内容，手册中114～119条等相关内容，结合对轻工企业网络安全防护管理和安全防护等级评定情况的调研，总结提炼了轻工企业网络安全管理的经验后形成。

“9　增强级安全防护”

“9.1.2　网络设备安全防护要求”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中 “网络设备安全”内容，手册中81和83条的相关内容，结合对轻工行业内部分企业调研、分析的情况，对轻工企业的重要的工业网络边界的安全防护设备提出采用工业专用的防火墙或安全网关等相关要求。

“9.1.3　工业控制设备安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中 “控制设备安全”18条内容，结合轻工行业企业生产实际和网络安全防护需求提出产品追溯、产品在线检测、能源和环境监控等轻工行业重点关注的重要生产、经营场景的工控系统设备的可靠性，设备操作和数据处理权限控制等各项要求。

“9.2.1 应用工业互联网的工业企业控制系统安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中 “联网控制系统安全”33、34、35条内容，结合对轻工行业企业和其他行业调研、分析的情况，对轻工行业联网控制系统安全需重点把控的关键环节和方面提出了联网控制系统安全配置、联网控制系统的开发、测试，以及系统状态监测等方面的要求。

“9.2.3 配置安全”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中 “配置安全”48条的内容，并结合对轻工行业企业和其他行业调研、分析的情况，提出轻工行业的补充要求。

“9.3.1 架构安全”主要依据

这部分内容主要引用《工业互联网企业网络安全分类分级评估操作手册》中 “架构安全”64～70条的内容，并根据轻工行业企业和其他行业调研、分析的情况，提出轻工行业的网络系统架构安全的补充要求。

“9.4 数据安全防护要求”主要依据

这部分内容主要依据GB/T 41479-2022和GB/T 35273-2020，并

结合轻工行业产品设计、与客户交互、远程运维、供应商等核心数据安全的需求作详细要求。

“9.5.1 平台软件安全”主要依据

这部分内容主要引用《工业互联网企业网络安全分类分级评估操作手册》中 “软件开发要求”的268～272条内容，结合对轻工行业平台软件安全的实际需求，提出开发人员、产品委托专业测评、审查软件等重要环节的要求。

“9.6.1 安全管理制度要求”主要依据

这部分内容主要依据《工业互联网企业网络安全分类分级评估操作手册》中“安全管理制度、安全管理机构、人员要求、安全建设、安全运维管理”等内容，手册中94～113条中相关内容，并结合轻工企业网络安全管理的经验，总结提炼。

（三）解决的主要问题

轻工产业涉及国计民生，其产品范围极为广泛，生产工艺、企业规模、生产自动化、信息化程度差异极大。目前规模以上企业数达 11.12 万家（截至 2021 年 7 月统计数据），涉及家电、家居、食品、照明、日用杂品、造纸、体育和娱乐用品、酒、饮料和精制茶制造等，随着企业信息化和工业化融合发展的推进，企业网络安全面临很大的挑战。目前企业工业互联网发展进入落地实施阶段，企业设备联网、企业上云数量明显增加，控制系统联网、边界隔离不到位等大量安全隐患日益突出，工业互联网安全事件频发，暴露出轻工企业安全防护存在较大缺陷，影响了企业生产和经营，造成难

以弥补的经济损失。

目前，轻工行业工业互联网企业网络安全防护的研究尚处于起步阶段，尚未形成完整的分级安全防护机制和要求，不能适应轻工行业工业化和信息化融合发展的需要，存在以下问题和不足：

（1）数据安全方面：轻工企业对数据全生命期保护和实时防御能力较弱，企业和行业的数据价值释放尚未充分得到安全可靠的保障。

（2）网络安全方面：Bots 自动化威胁的管理与防护较弱，安全产品和服务的兼容性、适配性，以及自主化需求未得到有效满足。

（3）工控安全方面：企业在“配置和补丁管理”“安全软件选择与管理”“安全监测和应急预案演练”等方面均处于较低水平 。工控设备资产的全面探测是企业首先要解决的问题。

（4）安全管理方面：企业存在认知度不统一、建设模式不规范、管理制度缺位、人才培养乏力，应急预案和应急演练不到位等问题。大部分企业缺少安全管理手段和措施对整体网络情况进行整体把控。

因此，制定并实施本标准推动轻工行业工业互联网安全防护工作发展，对轻工行业的网络安全防护分类施策，系统地、有针对性解决轻工行业网络安全防护问题，建立起保护轻工企业网络安全的坚固防线。

三、主要试验（或验证）情况

本标准主要起草单位具有行业领域及网络安全领域的代表性及影响力，在工业互联网安全方面具有丰富的标准制定经验。从 2021

年 9 月至今，牵头单位中国轻工业信息中心联合中国信通院开展了充分的产业调研、专家论证并广泛征求了有关轻工企业和技术服务商的意见，形成了标准草案。轻工行业领域已有 20 余家企业参与工业互联网企业网络安全分类分级管理试点工作，标准草案中相关技术内容已面向标准实施对象进行试点应用，收到了良好的效果。编制组在编制过程中，充分听取了网络安全服务机构、科研院所、测试机构、应用工业互联网的轻工企业的意见，并在工信部网安局的指导下推进开展标准条款的试点验证工作。

四、标准中涉及专利的情况

本标准不涉及专利问题。

五、预期达到的社会效益、对产业发展的作用等情况

当前轻工企业正在推进数字化转型升级，着力以数字化、网络化、智能化的生产方式，大力融合工业互联网平台技术。由于大量工业系统、生产设备和运行业务暴露在工业互联网上，很容易成为黑客攻击主要目标。而且，在工业互联网应用中，轻工业与信息技术的相互融合产生出的多样化新业态，涉及大量工业数据、程序、工业控制系统、基础网络设施和工业互联网平台等各种要素，设备种类及数量多，采集的数据种类和途径也多，导致安全防护难度大，轻工行业工业互联网企业面临日益严重的安全威胁。

面对网络安全与生产安全交织的风险和基于工业互联网的新基础设施建设、新技术创新应用、新模式业态形成带来的新型安全风险，轻工企业亟须建立一套网络安全防护体系，并持续完善，以强

有力地抵御网络攻击、最大限度降低安全风险，保障生产有序进行、业务稳定运营。目前针对轻工行业应用工业互联网的工业企业网络安全防护的研究尚处于起步阶段，尚未形成完整的分级安全防护机制和要求。通过本标准的制定实施，可以提升轻工行业应用工业互联网的工业企业网络安全防护能力，对本行业分类分级工作实现有效支撑，对企业网络安全保障工作进行有效指导，提高企业网络安全防护能力和水平。因此，本标准具有很好的产业化应用前景。

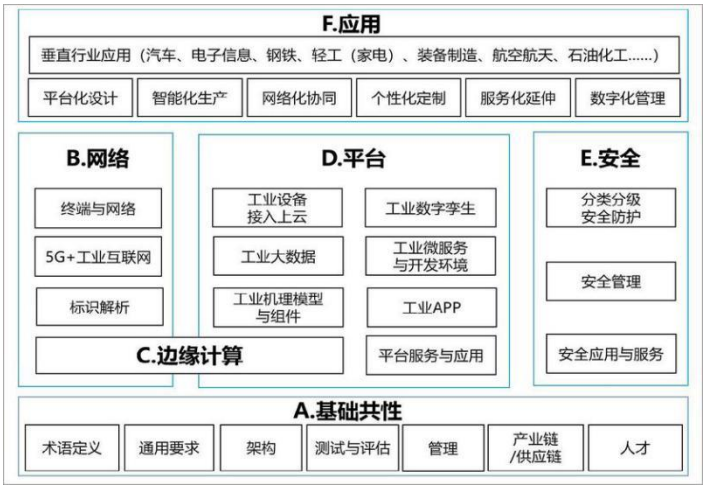
六、与国际、国外对比

本标准没有直接对应的国际标准。美国工业互联网联盟（IIC）对工业互联网安全架构及安全测试床进行了相关研究，提出了安全框架和安全检查清单，但并未制定关于工业互联网安全的相关标准；IEC TC65 制定了 IEC 62443 系列标准，从自动化角度提出了工业控制系统信息安全要求及检测规范，但并未涉及轻工行业工业互联网其他要素的安全需求。

七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准、特别是强制性标准的协调性

本标准属工信部、国标委发布《工业互联网综合标准化体系建设指南（2021 版）》，提出的面向轻工（家电）等重点行业的工业互联网应用，制定行业技术要求和管理规范。是体系中的“E 安全”部分有关标准。 面向轻工行业具体要求，结合轻工行业特点和需求的细化、丰富， 应用工业互联网工业企业网络安全分类分级标准在轻

工行业的应用落地。



工业互联网标准体系结构图

本标准符合《中华人民共和国网络安全法》等现有法律法规、规章。

本标准是《工业互联网企业网络安全：第 1 部分 应用工业互联网的工业企业网络安 全防护要求》《工业互联网平台企业安全防护要求》《工业互联网标识解析企业安全防护要求》《工业互联网企业数据安全要求》四项通信领域国家标准（在编）的配套使用标准。以上四部标准作为工信部开展工业互联网企业网络安全分类分级管理工作的支撑，规范三类企业的分类分级安全防护技术要求。本标准与有关上位标准协调一致，结合轻工行业特点，规范企业网络安全防护技术要求，是分类分级工作在行业落地实施的依据。目前在轻工行业，尚未编制过有关网络安全的标准，也不存在制定中的有关网络安全标准。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议说明

建议作为推荐性行业标准颁布实施，并建议标准颁布后半年实施。

十、贯彻标准的要求和措施建议

正式颁布后，应结合 GB/T 44462.1-2024 等相关标准、法规，对标准中的条款进行宣贯，以在利益相关方之间达成对标准条款理解上的一致性，将标准执行落到实处。

十一、废止现行有关标准的建议

无。

十二、其他应予说明的事项

标准编制组

2025 年 1 月