ICS 35.030
CCS Y01

QB

中 华 人 民 共 和 国 轻 工 行 业 标 准

QB/T XXXXX—202X

轻工行业工业互联网企业网络安全分类分级防护要求

Network security classification and grading protection requirements for industrial Internet companies in the light industry

（征求意见稿）

202X－XX－XX 发布　　202X－XX－XX 实施

中华人民共和国工业和信息化部　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国轻工业联合会提出并归口。

本文件起草单位：中国轻工业信息中心、圣奥科技股份有限公司、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、江苏省银宝盐业有限公司海精盐厂、重庆梦之想科技有限责任公司、北京珞安科技有限责任公司、北京印刷集团有限责任公司、浙江五疆科技发展有限公司、山东浪潮数字商业科技有限公司、重庆不贰科技（集团）有限公司、北京乐研科技股份有限公司等。

本文件主要起草人：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、李春江、周玲、高迪、刘海涛、马亚丽、吴佳蓓等。

轻工行业工业互联网企业网络安全分类分级防护要求

1 范围

本文件规定了轻工企业工业互联网企业网络安全防护级别、安全防护对象和范围，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。

本文件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 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2022 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 35273-2020 信息安全技术 个人信息安全规范

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

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

3 术语和定义

GB/T 22239、GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

工业互联网 industrial internet

满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。

3.2

工业互联网设备 industrial internet device

工业互联网中执行指令控制、数据采集、协议解析、数据转发等功能的设备，包括控制类设备、数据采集类设备、智能终端等。

3.3

工业控制系统 industrial control system

工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。

[来源：GB/T 32919-2016，定义3.1]

3.4

工业互联网平台 industrial internet platform

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、高效配置的载体。

3.5

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019，定义3.1]

4 缩略语

下列缩略语适用于本文件。

DCS	分布式控制系统	Distributed Control System
FTP	文件传输协议	File Transfer Protocol
HMI	人机接口	Human Machine Interface
IP	网络协议	Internet Protocol
MES	生产过程执行系统	Manufacturing Execution System
PLM	产品生命周期管理	Product Lifecycle Management
SCADA	数据采集与监视控制系统	Supervisory Control And Data Acquisition

5 轻工行业企业工业互联网企业网络安全防护级别

轻工行业企业（以下简称“轻工企业”）应依据企业所在行业的网络安全影响程度、企业规模、企业应用工业互联网的程度和企业一旦发生工业互联网网络安全事件的影响程度，按《工业互联网企业网络安全分类分级管理指南》的规定自主定级。工业互联网企业网络安全等级由低到高划分为：一级、二级、三级，其分别对应的安全防护级别为：初始级防护、基本级防护、增强级防护，具体见表1。

表1 应用工业互联网的工业企业安全防护级别的确定

企业级别	企业安全防护级别	企业安全防护要求条款
一级	初始级	6、7章
二级	基本级	6、7、8章
三级	增强级	6、7、8、9章

6 应用工业互联网的轻工企业安全防护对象和范围

6.1 防护对象

构成轻工企业工业网络的产品研发设计网络、工艺设计网络、生产管理网络、生产加工网络、仓储物流和监控网络等工业网络所涉及的网络设备、安全设备、服务器和存储等硬件设备，以及操作系统、数据库、各种中间件和其他工具软件等基础软件，以及在其网络上运行的ERP系统、MIS系统、OA系统、PLM系统、PDM系统、WMS系统等工业控制应用系统、CAD/CAM/CAE等工程软件，以及构成控制网络底层设

施的PLC控制系统、DCS系统、OPC系统（环境等监控设备）、SCADA（能源、动力等采集系统）的主机设备、控制设备、数据服务器，以及外接工业数据存储设备等。

防护对象还包括部署在企业互联网区域的云端设备及应用服务系统（标识解析管理系统、供应商管理系统、客户服务系统等），以及接入生产网络的4G/5G无线通讯网络所涉及的网络设备、安全设备、MEC端的服务器等设备，以及依托无线网络运行的轻工中间产品定位追踪系统、RFID等电子标签信息采集软件等系统。

6.2 防护范围

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：

a) 设备安全防护：包括工业主机安全、网络设备安全、工业控制设备安全，以及轻工企业典型应用场景中的联网设备网络安全防护要求；
b) 工业控制安全防护：包括应用工业互联网的工业企业控制系统安全、控制软件安全、配置安全、智能装备控制安全，以及轻工企业典型应用场景中的 OT 层网络安全防护要求。其中，联网控制系统是指应用工业互联网服务的工业控制系统；
c) 网络安全防护：包括架构安全、边界安全、通信安全等；
d) 数据安全防护：包括应用工业互联网的工业企业数据全生命周期安全等方面；
e) 应用平台软件安全防护：包括平台软件安全、工业 APP 安全等；
f) 安全管理:包括安全管理制度、安全管理机构和人员、安全建设管理、安全运维管理等安全防护要求；
g) 物理环境安全防护：包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等安全防护要求。

7 初始级安全防护要求

7.1 设备安全防护要求

7.1.1 工业主机安全

轻工企业的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，以及OPC-UA服务器等主机设备，除满足GB/T 44462.1-2024中7.1.1.1的要求外，还应满足以下要求：

a) 应定期查杀 DCS 主机、PLC 主机、OPC-UA 服务器等主机设备上的病毒；
b) DCS 主机上应部署主机防护软件（如主机安全卫士）或设备（如专用安全 U 盘）或组件（如终端准入管控模块）进行安全加固；
c) 安全、能源管控、环境监控等智能控制设备所用的 DCS 主机数据应通过光盘等安全媒介导入导出；
d) 安全、能源、环境监控等 DCS 主机与其他系统的通信连接应采用安全可靠的隔离方式。

7.1.2 网络设备安全

轻工企业生产区域的现场控制网络、生产执行层网络、生产管理层网络的交换机、LPWAN物联基站、无线路由器、SDN控制器、PLC网关、Modbus网关等网络设备，应满足GB/T 44462.1-2024中7.1.1.2的要求。

7.1.3 工业控制设备安全

轻工企业生产中PLC控制设备、DCS控制设备，能源、环境、安全控制系统的DCS控制设备等除满足GB/T 44462.1-2024中7.1.1.3要求外，还应满足以下要求：

a） 应禁止外部设备通过网络接口访问智能控制仪表等重要设备的从机等工业控制设备；
b） 应将重要的控制设备放置在密闭的控制柜内，与外部环境隔离，以防止电磁干扰、高温和粉尘等外部环境的影响。

7.2 工业控制安全防护要求

7.2.1 应用工业互联网的工业企业控制系统安全

除满足GB/T 44462.1-2024中7.1.2.1的要求外，还应满足以下要求：
a） 应建立工业控制系统的入侵防范管理机制；
b） 应对工业控制系统进行用户登录认证管理和权限控制；
c） 轻工企业生产中重要的工业控制系统，应支持关键设备和系统的硬件冗余，保证系统的可用性；
d） 轻工企业生产控制中的 PLC 系统还应符合 GB/T 33008.1 的要求；
e） 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 DCS 还应符合 GB/T 33009.1 的要求；

7.2.2 控制软件安全

除满足GB/T 44462.1-2024中7.1.2.2的要求外，还应满足以下要求：
a） 应建立安全漏洞管理机制，及时处理和跟踪漏洞信息，对存在的安全漏洞及时进行排查和整改；
b） 应定期更新 PLC 的操作系统和控制软件，修复已知的漏洞和安全问题；
c） 应定期对 PLC 的控制软件进行备份，以防止数据丢失。

7.2.3 配置安全

应满足GB/T 44462.1-2024中7.1.2.3的要求。

7.2.4 智能装备控制安全

应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。

7.3 网络安全防护要求

7.3.1 架构安全

应划分不同的网络安全域，其中企业的工业控制系统与其他系统应划分不同安全域，按照安全管理和控制的原则为各安全域分配地址。

7.3.2 边界安全

应符合GB/T 44462.1-2024中7.1.3.2的要求。

7.3.4 通信安全

应采取技术措施保证工控系统通信数据的完整性，避免各类控制指令被非法篡改和破坏。

7.4 数据安全防护要求

数据安全应符合以下要求：

a) 存储数据时，应选择合适的存储介质，并对存储介质进行安全管控；
b) 确有安全防护需求的数据可采用技术手段（如加密、数字签名、完整性校验等），实现存储数据的机密性、完整性、来源真实性；
c) 应建立数据容灾备份的规范和操作规程，明确规定数据容灾备份的周期、备份方式、备份地点等，并根据实际情况开展数据本地灾难备份与恢复；
d) 应根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施（如安全传输通道、安全传输协议等）保证数据传输安全；
e) 涉及个人信息存储、使用应符合 GB/T 35273-2020 及 GB/T 41479-2022 要求；
f) 应制定数据使用审批流程、数据使用结果发布、安全保护规则，以及相关人员岗位职责等；
g) 应对数据的使用加工进行身份鉴别和访问控制；
h) 应对数据的使用和加工进行规范管理。

7.5 应用平台软件安全防护要求

7.5.1 平台软件安全

平台软件开发和使用时应符合以下要求：

a） 应实行平台管理员的职责分离，并根据最小权限原则配置各自权限；
b） 平台软件开发、升级或更新后，应进行充分的测试，确保软件的可用性和安全性后，再进行正式部署；
c） 在使用平台软件的过程中，应定期更新平台软件，并使用正版软件补丁进行更新。

7.5.2 工业 APP 安全

应符合GB/T 44462.1-2024中7.1.4.2的要求。

7.6 安全管理要求

企业应在机构、制度、人员、防护系统建设和运维方面进行有效的安全管理，除按 GB/T 44462.1-2024 中 7.1.5 的规定外。还应符合以下要求：

a) 企业应建立基本的安全监督机构，通常由安全管理员或安全主管负责。机构的职责主要包括督

安全政策的执行、处理日常安全事务、提供基本的安全培训等；

b） 安全监督机构成员应具备基本的安全管理知识和技能，能够识别常见的安全风险并采取相应的
应对措施。此外，机构成员应了解企业安全政策和相关法规，并能够有效地传达给其他员工；

c） 应对涉及网络安全、企业和用户信息安全等重要岗位的人员的进行有效管理，确保企业信息和技术及用户信息安全。

7.7 物理环境安全要求

应满足GB/T 44462.1-2024中7.1.6的要求，进行轻工企业工业互联网物理环境安全防护工作。

8 基本级安全防护要求

8.1 设备安全防护要求

8.1.1 工业主机安全

除满足7.1.1和GB/T 44462.1-2024中7.2.1.1的要求外，还应满足以下要求：

a） 应具备唯一性标识，如品牌、型号、版本号、序列号；
b） 应只安装需要的组件和应用程序并关闭与系统业务无关的端口和服务；
c） 对外提供的接口 API 调用，应同时遵循用户访问控制，防止对设备接口的非授权访问；
d） 应规范软硬件安装和使用，不应擅自安装软件、擅自更改软硬件配置；
e） 应确保设备固件升级失败后原固件的可用性，并在升级前向用户进行确认；
f） 应对用户信息进行安全防护，保护用户信息不被泄漏；
g） 设备应用程序不包含 CNVD,CNNVD 已公布 90 天以上的漏洞，并符合以下要求，如设备应用程序升级包不允许存在恶意代码，不存在未声明的功能，不存在未声明的私有协议；
h） 应具有系统备份恢复，故障信息反馈功能，如重置设备，故障信息提示；
i） 对安全、能源、环境等重点管控系统进行控制的上位机和服务器的操作系统补丁升级应进行综合考虑，进行严格的安全评估和测试验证，在不影响生产运行的情况下进行安装；
j） 应禁止第三方或厂内维护人员的非专用笔记本电脑和 U 盘等移动设备的外部接入；
k） 产品可追溯系统、产品在线检测系统和智能家居设备等应定期进行设备漏洞扫描与及时修复，并及时更新操作系统和固件；
l） 对接入产品可追溯系统、产品在线检测、远程运维系统等的设备进行严格身份认证，并根据设备功能和需求分配最小权限；
m） 限制非法设备接入网络，仅允许经过授权的设备与系统进行通信；
n） 采用设备身份认证技术，确保设备的合法性和真实性。

8.1.2 网络设备安全防护要求

除满足 7.1.2 和 GB/T 44462.1-2024 中 7.2.1.2 的要求外，还应满足以下要求：

a） 网络关键设备和网络安全专用产品应符合相关国家标准的要求；
b） 应定期对网络设备系统进行漏洞扫描，对发现的安全漏洞进行及时处理；
c） 应对网络和安全设备的远程管理采取必要的安全措施，防止鉴别信息在传输过程中被窃取；
d） 应对网络和安全设备采取登录失败处理措施，如：结束会话、限制失败登录次数、当网络登录连接超时自动退出等。

8.1.3 工业控制设备安全防护要求

除满足7.1.3和GB/T 44462.1-2024中7.2.1.3的要求外，还应满足以下要求：

a) 控制设备应具备鉴别用户登录访问身份的安全措施；
b) 建立安全策略配置清单，确保该清单满足控制设备安全可靠运行的需要；
c) 对采用无线通信技术的控制设备，应能识别未经授权的无线设备，报告未经授权试图接入或干扰控制系统行为；
d) 如受条件限制控制设备无法采用身份鉴别措施，应由其上位控制或管理设备实现同等功能或通过管理手段控制；
e) 应封闭或拆除控制设备的软驱、光驱、USB 接口、串行口或多余网口等，如需保留应通过相关的技术措施（如物理锁或逻辑控制）实施严格的监控管理；
f) 应定期对控制设备安全配置进行核查审计。

8.2 控制安全防护要求

8.2.1 应用工业互联网的工业企业控制系统安全

除满足7.2.1和GB/T 44462.1-2024中7.2.2.1的要求外，还应满足以下要求：

a) 工业控制系统数据传输应在控制系统网络区域内进行，禁止非授权设备参与通信；
b) 对于新部署的或网络结构发生重大改变的工业控制系统，应在上线前进行安全性检测；
c) 应定期针对联网控制系统、临时接入设备以及即将上线前的设备开展查杀，并留存详细查杀记录；
d) 应确保联网控制系统相关安全配置的有效性，安全配置上线前要进行验证；
e) 应建立联网控制系统安全策略配置清单,确保该清单满足企业联网控制系统安全可靠运行的需要；
f) 禁止联网控制系统面向互联网开通 HTTP、FTP、Telnet 及邮件服务等高风险通用网络服务；
g) 应保留联网控制系统相关访问日志（包括人员账户、访问时间、操作\内容等)，并定期进行备份，以确保安全审计的有效开展；
h) 应建立联网控制系统资产清单（包括软件资产、硬件资产、数据资产等)，确保联网控制系统资产信息可查、可追溯；
i) 应能产生安全监控指令，并实时展示现场数据及设备安全状态；
j) 应对重要工业控制系统进行操作日志审计。

8.2.2 控制软件安全

除满足7.2.2和GB/T 44462.1-2024中7.2.2.2的要求外，还应满足以下要求：

a) PLC、DCS、SCADA 等工控系统软件应具备本地备份与恢复功能，定期进行数据备份；
b) 应禁止由受控计算机主动连接远程控制端的技术（如中间产品物流追踪使用的 UWB 定位控制系统等），防止泄露受控计算机的网络位置信息，从而成为攻击者进行入侵的目标；
c) 应为组态软件的登录账户设定高强度的登录密码，避免使用默认口令和弱口令，并妥善管理，定期更新口令；
d) 应跟踪组态软件的安全风险，及时更新最新补丁；
e) 应删除组态软件自带的非必要系统账户。

8.2.3 配置安全

除满足7.2.3和GB/T 44462.1-2024中7.2.2.3的要求外，还应满足以下要求：

a） 应严格口令管理，及时更改产品安装时的预设口令，杜绝弱口令、空口令，并为所有用户提供实施口令的最小和最大有效期限制；
b） 应严格账户管理，根据工作需要合理分类设置账户权限，并定期清理不必要的用户和管理员账户；
c） 应对多次登录失败的账户进行锁定的功能；
d） 安全配置中应包含禁用非必要的后台程序、账户、进程、端口和服务，并定期对账户、口令、端口、服务等进行检查并维护；
e） 应建立重要工业控制系统安全配置的备份和审计机制，审计记录应至少包含访问控制、操作系统事件、控制系统事件、备份和恢复事件、配置变更、嗅探攻击行为和审计日志事件，单条审计记录应包含时间戳、分类、来源、事件 ID 和事件结果。

8.2.4 智能装备控制安全

除满足7.2.4和GB/T 44462.1-2024中7.2.2.4的要求外，还应满足以下要求：

a) 轻工企业的工业互联网平台直接控制的现场重要设备（如AGV、工业机器人等遥控启动装置、立体库、测厚机器人），应确认设备身份的唯一性安全标识，以便对现场重要设备进行安全识别和访问控制；
b） 轻工企业生产现场的重要设备应具有识别验证控制指令来源、访问控制功能；
c） 轻工企业生产中使用的AGV控制设备应能够实现与外部安全PLC无线通信，底层通信模块应具
有底层协议解析和安全/非安全数据分离的功能，并将非安全数据传给AGV内部控制器，安全数据传给能够进行数据校验的安全板卡，以保证AGV控制安全。

8.3 网络安全防护要求

8.3.1 架构安全

除满足7.3.1和GB/T 44462.1-2024中7.2.3.1的要求外，还应满足以下要求：

a) 联网控制系统网络拓扑结构应采用纵深防御思想进行概念设计，应将全网划分为不同的安全网络层级；
b） 企业应对网络安全架构的开发和优化进行风险评估，充分考虑潜在的安全影响；
c） 系统应定义明确的网络安全边界，并采取可靠的安全技术隔离手段；
d） 联网控制系统应在不影响现有安全状态条件下实现与紧急电源之间的切换；
e） 应严禁开启双重网络接口卡（NIC）。

8.3.2 边界安全

除满足 7.3.2 和 GB/T 44462.1-2024 中 7.2.3.2 的要求外，还应满足以下要求：

a） 应采取安装防护设备或设置访问控制策略阻断不同等级安全区域之间的非授权访问；
b） 应在物流追踪、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；
c） 网络边界设备（安全网关、防火墙、路由器等）应只开放对外服务相关的端口（如设计网络只开放向生产管理网络的加工信息传输端口）或只允许数据的单向传输；
d) 应禁止将边线缓存的自动化仓库系统等重要控制网络区域部署在网络边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

8.3.3 通信安全

除满足7.3.3和GB/T 44462.1-2024中7.2. 3.3的要求外，还应符合以下要求：

a) 轻工企业现场生产设备与控制设备通信时应采用数据加密传输和访问控制等技术；
b) 对于 AGV 追踪移动终端、物资自动识别终端等无线接入设备应开启终端接入认证功能，禁止使
用不安全的 WEP 方式进行认证；采用无线接入的生产设备应采用唯一 MAC 认证方式；
c) 应能检测到非授权无线接入设备和非授权移动终端的接入行为，并进行阻断和日志记录；
d) 与外部供应商发生业务，通过公共信息网络进行通信数据传输时，应采用加密认证技术进行数
据传输、访问控制。

8.4 数据安全防护要求

8.4.1 数据存储安全

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等远程运维系统、产品交互互动设计系统等轻工企业重要数据存储应符合以下要求：

a) 应采用技术手段（如加密、数字签名、完整性校验等）和访问控制实现数据安全存储；
b) 应能够检测到数据在存储过程中机密性、完整性、可用性受到破坏，在检测到数据被破坏时，进行告警并采取必要的恢复措施；
d) 应制定数据容灾备份的规范和操作规程，开展数据容灾备份管理并制定冗余备份方案，全量数据备份至少每周一次，增量数据备份至少每天一次，必要时进行实时备份；
d) 备份数据应存放在独立的安全区域内，通过防火墙等防护措施控制备份数据的访问；
e) 应对访问频率极低的数据进行归档，建立归档数据保护机制，防止数据被篡改和删除；
f) 应定期进行数据恢复测试；
g) 应采用技术手段保证存储行为可溯源。

8.4.2 数据传输安全

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等远程运维系统、产品交互互动设计系统等轻工企业重要数据传输应符合以下要求：

a) 应采用技术手段（如加密、数字签名、完整性校验等），保证数据在传输过程中的机密性、完
整性、来源真实性；
b) 应能检测到数据在传输过程中机密性、完整性、可用性、来源真实性受到破坏，实时告警并采
取必要的措施；
c) 应采用安全传输协议进行数据传输；
d) 应在数据传输过程中，开展数据安全监测，能对网络流量行为、攻击威胁、数据泄露或篡改等
进行分析和研判；
e) 应在数据迁移前对数据开展本地备份及恢复相关工作，做好数据迁移安全评估与安全控制，防
止迁移过程中因突发状况导致数据丢失；
f) 涉及跨组织机构或者使用公共信息网络进行数据传输时，应进行内部登记、审批；
g) 应采用技术手段保证数据传输行为可溯源。
h) 核心数据传输时，应具备数据传输实时监控能力，在发现异常时第一时间进行处置。

8.4.3 数据使用安全

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等远程运维系统、产品交互互动设计系统等轻工企业重要数据使用应符合以下要求：

a) 应制定数据使用审批流程、数据使用结果发布、安全保护规则，以及相关人员岗位职责等；
c) 应对数据的使用加工进行身份鉴别和访问控制；
d) 应对数据的使用和加工进行规范管理；
e) 涉及个人信息使用应符合 GB/T 35273-2020 及 GB/T 41479-2022 要求。

8.5 应用平台软件安全防护要求

8.5.1 平台软件安全

除满足7.3.5.1和GB/T 44462.1-2024中7.2.4.1的要求外，还应符合以下要求：

a） 应使用最小权限原则对使用用户、管理用户进行权限分配；
b） 平台应能鉴别接入设备和访问用户的权限，并只开放对应权限，对非授权设备的接入行为进行告警和阻断；
e） 在巡检设备、移动物流追踪设备等通过企业工业互联网平台的虚拟化设备管理功能和平台接入时，应采取加密技术保障通信时的数据安全；
d） 平台应识别并阻断云服务用户的对云计算节点或其他用户的网络攻击行为；
e） 远程视频监控、跨企业生产设备管理等平台内部核心功能模块，应采用审核或白名单机制，只允许审核通过的用户访问核心功能模块；
f） 与外部供应商发生业务通过公共信息网络进行通信数据传输时，应采用加密认证技术进行数据传输、访问控制。

8.5.2 工业APP安全

除满足7.3.5.2和GB/T 44462.1-2024中7.2.4.2的要求外，还应符合以下要求：

a） 应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
b） 应在软件开发过程中进行安全性测试，并在软件交付前检测其中可能存在的缺陷与恶意代码等；
c） 应要求开发单位提供软件设计文档和使用指南；
d） 应在外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款；
e） 运行工业APP的服务器应采取恶意代码检测、预防攻击和备份恢复的安全措施；
f） 宜采用工业防火墙对跨企业的控制类工业APP与设备间的通信内容进行实时跟踪和深度过滤。

8.6 安全管理要求

机构管理、安全管理制度、人员管理、建设管理、运维管理等除按7.6和GB/T 44462.1-2024中7.2.5的规定外，其他安全防护要求如下：

a） 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
b） 应加强各类管理人员之间、组织内部机构之间以及安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理安全问题；
c） 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；
d） 应加强与工业互联网安全主管部门、各类供应商、业界专家及安全组织的合作与沟通；
e） 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
f） 应定期对安全管理制度的合理性和适用性进行论证和审定,对存在不足或需要改进的安全管理

制度进行修订。

8.7 物理环境安全要求

除满足 7.3.6 和 GB/T 44462.1-2024 中 7.2.6 的要求外，防雷击、防火要求还应符合以下要求:

a) 应将各类机柜、设施和设备等通过接地系统安全接地，并应满足 GB/T 22239 的有关要求；
b) 机房建筑应设置避雷装置，并应满足 GB 50057 和 GB 50343 的有关要求；
c) 机房及工业互联网平台相关设备放置场地应设置灭火设备和火灾自动报警系统；
d) 机房建筑应满足 GB 50016 的有关要求。

9 增强级安全防护要求

9.1 设备安全防护要求

9.1.1 工业主机安全

除满足 8.1.1 和 GB/T 44462.1-2024 中 7.3.1.1 的要求外，还应满足以下要求：

a) 应在设备启动时对核心应用程序进行完整性校验；
b) 不应存在绕过正常鉴别机制直接进入系统后台或控制界面的路径入口，如特定端口，特殊 URL 等；
c) 对于食品的可追溯系统、在线检测系统等安全性要求较高的设备宜使用双因子验证（2FA）；
d) 与其它设备进行通信配对时，应在双端设备上分别进行身份鉴别；
e) 具有调试功能的设备端口在出厂时应设置为默认关闭，并且开启端口时应配置用户名口令等方式进行鉴别认证；
f) 具备远程控制功能的设备在控制端发起操作和访问重要数据请求时应经过认证授权或被控端设备用户同意；
g) 应具备会话超时断开机制，用户或设备连接在指定空闲时长后自动断开连接；
h) 应提供设备连接，数据传输状态标志，在后台应用上传下载数据，远程用户连接时，给予明显的状态标志提示；
i) 联网设备应提供异常，故障时的报警信息推送功能；
j) 应对生命周期结束的设备中保存的用户敏感数据进行不可逆的销毁或抹除。

9.1.2 网络设备安全防护要求

除满足8.1.2和GB/T 44462.1-2024中7.3.1.2的要求外，还应符合以下要求：

a) 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
b) 用于轻工企业的重要的工业网络边界的安全防护设备宜采用工业专用的防火墙或安全网关；
c) 应定期对网络设备系统进行漏洞扫描，对发现的安全漏洞进行及时处理。

9.1.3 工业控制设备安全

除符合8.1.3和GB/T 44462.1-2024中7.3.1.3的要求外，还应符合以下要求：

a) 产品追溯、产品在线检测、能源和环境监控等控制设备，应禁止外来设备接入，维修、升级等操作应在专职人员陪同下使用本地专用设备进行接入操作，操作日志留存并审计；
b) 产品追溯、产品在线检测、能源和环境监控等控制系统，应采用硬件冗余技术保证工控系统设备的可靠性；
c) 应定期评审检查正在运行的设备配置，对发现潜在的风险或任何可以优化配置的改进点在不影响设备正常运行的情况下进行配置修改并留存日志；

d） 宜采用主动标识作为设备身份识别标志，并基于此标识开展设备操作和数据处理权限控制。

9.2 控制安全防护要求

9.2.1 应用工业互联网的工业企业控制系统安全

除符合8.2.1和GB/T 44462.1-2024中7.3.2.1的要求外，还应符合以下要求：

a） 联网控制系统各个区域应依据安全需求的差异设置为不同的安全要求，并根据相应的安全要求采取不同的安全防护措施；

b） 应定期自行对联网控制系统安全配置进行核查审计,避免因调试或其它操作导致配置变更后，未及时更新配置清单；

c） 应针对联网控制系统的开发、测试和生产分别提供独立环境，避免开发、测试环境中的安全风险引入生产系统；

d） 应部署具备对联网控制系统与网络进行状态监测、日志采集与事件管理、流量采集与行为分析、异常告警及关联分析等功能的网络安全监测设备，及时发现、报告并处理包括设备状态异常、恶意软件传播、异常流量、异常诊断日志、端口扫描、暴力破解等网络攻击或异常行为。

9.2.2 控制软件安全

除符合 8.2.2 和 GB/T 44462.1-2024 中 7.3.2.2 的要求外，还应对组态软件版本以及组态程序、脚本进行定期更新备份。

9.2.3 配置安全

除符合8.2.3和GB/T 44462.1-2024中7.3.2.3的要求外，还应严格管理配置管理库的访问权限及管理账号，并使边界网络设备的配置具有支持网关冗余功能。

9.2.4 智能装备控制安全

除符合8.2.4和GB/T 44462.1-2024中7.3.2.4的要求外，还应符合以下要求：

a） 轻工企业生产中重要设备应支持异常指令、状态等审计数据上报；

b） 应建立统一的智能设备管理平台，防止设备恶意控制、大规模数据泄露等问题；

c） 应建立并执行代码级的安全防护措施；

d） 应对智能设备的通信、数据进行加密技术处理。

9.3 网络安全防护要求

9.3.1 架构安全

除符合8.3.1和GB/T 44462.1-2024中7.3.3.1的要求外，还应符合以下要求：

a） 在不同网络层级之间安全防护方面，系统各个层级之间应部署访问控制设备、入侵检测与防护设备、安全隔离设备以及安全审计设备；

b） 在横向分区方面，联网控制系统不同横向分区应依据安全性需求的不同而设置不同安全等级，并根据相应的安全等级采取不同的安全防护措施；

c） 在网络组件冗余方面，联网控制系统的核心网及骨干网应建设冗余链路，确认冗余链路采用不同的网络方式构建，电力供应、现场控制站、工程师服务器、历史数据库服务器、实时数据库

服务器、HMI 服务器、核心交换机等应进行硬件冗余；

d） 在网络故障诊断与恢复方面，当网络故障时系统切换到另一路通信网络的时间应满足实际需求，当网络故障时可保证业务不中断继续运行，数据不丢失；

e） 在关键软件容错方面，联网控制系统的历史数据库、实时数据库、组态软件、监控软件等应采取容错措施；

f） 确认控制器、组态软件、数据库、监控软件、核心交换机、重要服务器等联网控制系统关键设备，或安全仪表系统、紧急停车系统、安全防护系统等联网控制系统采用国产设备，或经检测无安全漏洞的国外设备，联网控制系统运营单位应具备对联网控制系统的二次开发能力，并具备自主开展联网控制系统漏洞防护的能力。

9.3.2 边界安全

除符合8.3.2和GB/T 44462.1-2024中7.3.3.2的要求外，还应在不同区域间采取可靠的技术隔离手段形成边界防护，边界防护设备应具有识别工业协议的功能。

9.3.3 通信安全

除满足8.3.3和GB/T 44462.1-2024中7.3.3.3的要求之外，还应符合以下要求：

a） 应采用密码技术保证通信过程中数据的完整性和保密性；

b） 工业控制系统不同等级安全区域之间应部署安全防护设备；

c） 应采取虚拟专用网络（VPN）、线路冗余备份、数据加密等措施，加强对联网控制系统远程通信的保护。

9.4 数据安全防护要求

产品设计、与客户交互、远程运维、供应商等核心数据安全除满足 8.4.1、8.4.2、8.4.3 的要求之外，还应满足以下要求：

a) 应对核心数据的存储设备进行硬件冗余，保证主设备出现故障时冗余设备可以实时切换并恢复数据可用；

b) 应启用实时数据备份功能，并实施异地容灾备份；

c) 应具备数据存储行为、使用加工行为和数据传输实时监控能力，在发现异常后第一时间进行处置。

9.5 应用平台软件安全防护要求

9.5.1 平台软件安全

除满足8.4.1和GB/T 44462.1-2024中7.3.4.1的要求外，还应符合以下要求：

a） 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品；

b） 应制定代码编写安全规范，要求开发人员参照规范编写代码；

c） 应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；

d） 应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

e） 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；

f） 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

9.5.2 工业 APP 安全

除符合 8.4.2 和 GB/T 44462.1-2024 中 7.3.4.2 的要求外，还应符合以下要求：

a) 通过对轻工企业的中间产品管理软件、中间产品物流追踪、产品追溯、仓储的入出库管理终端软件等工业 APP 进行安全监测审计；
b) 重要工业 APP 应当具备容错机制，在发生单点故障时可继续提供基本功能。

9.6 安全管理

机构管理、安全管理制度、人员管理、建设管理、运维管理等除按8.6和GB/T 44462.1-2024中7.2.5的规定外，其他安全防护管理要求如下：

a) 应根据安全防护对象的安全防护需求及与其他防护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
b) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施；
c) 应预先对安全防护产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；
d) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品；
e) 系统交付时，安全测试报告应包含密码应用安全性测试相关内容；
f) 应定期评审和审核服务供应商提供的服务，并对其变更服务内容加以控制；
g) 应与选定的供应商、服务供应商签署保密协议，要求其不得泄露客户数据和业务系统的相关重要信息；
h) 应保证供应商的重要变更及时传达到客户，并评估变更带来的安全风险，采取有关措施对风险进行控制；
i) 应加强对供应链的安全审查，确保所有供应商和合作伙伴遵守相同的网络安全标准，可通过与供应商签订网络安全协议、开展安全审计等手段，确保供应链中的每个环节都不成为攻击的突破口；
j) 应定期对员工进行安全意识培训，特别是生产过程和网络操作等重要岗位人员，掌握识别网络钓鱼攻击、操作安全密码、应对数据泄露等网络安全知识，提升员工的安全防范意识。

9.7 物理环境安全要求

除满足8.3.6和GB/T 44462.1-2024中7.3.6的要求外，防雷击、防火、防水和防潮等要求还应符合以下要求:

a) 拆除或封闭工业主机上不必要的USB、光驱、无线等接口；若确需使用，通过主机外设安全管理技术手段实施严格访问控制；
b) 机房应设置交流电源地线；
c) 机房及工业设备放置场地应设置自动灭火系统；
d) 应安装对水敏感的检测仪表或元件，对机房及工业设备放置场地进行防水检测。

参 考 文 献

[1] GB/T 22239《信息安全技术 网络安全等级保护基本要求》
[2] GB/T 25069《信息安全技术 术语》
[3] GB/T 32919-2016《信息安全技术 工业控制系统安全控制应用指南》
[4] 《工业互联网企业网络安全分类分级防护系列规范（试行）》 工业和信息化部 2020
[5] 《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 2021