ICS 35.030
CCS M 10

中华人民共和国国家标准

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

Industrial internet enterprise cybersecurity—Part 1:Protection requirements of internet industrial enterprise

2024-09-29 发布　　2025-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件是GB/T 44462《工业互联网企业网络安全》的第1部分。GB/T 44462已经发布了以下部分：

——第1部分：应用工业互联网的工业企业防护要求；

——第2部分：平台企业防护要求；

——第3部分：标识解析企业防护要求。

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)和全国网络安全标准化技术委员会(SAC/TC 260)共同归口。

本文件起草单位：国家工业信息安全发展研究中心、中国信息通信研究院、南方电网科学研究院有限责任公司、国能数智科技开发(北京)有限公司、中国航天科工飞航技术研究院、北京天融信网络安全技术有限公司、交通运输部科学研究院、烽台科技(北京)有限公司、北京启明星辰信息安全技术有限公司、中国电子技术标准化研究院、北京京航计算通讯研究所、施耐德电气(中国)有限公司、正泰集团股份有限公司、杭州安恒信息技术股份有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、中国科学院信息工程研究所、郑州信大捷安信息技术股份有限公司、上海宝信软件股份有限公司、北京威努特技术有限公司、中国工业互联网研究院、国家信息技术安全研究中心、上海化工宝数字科技有限公司、上海计算机软件技术开发中心、深圳市燃气集团股份有限公司、中国南方电网有限责任公司、贵州电子信息职业技术学院。

本文件主要起草人：蒋艳、王蕊、廖剑、张哲宇、董良遇、孙军、董娜、梁志宏、匡晓云、张格、李俊、王诗蕊、章利光、于盟、马娟、杨梓涛、韩鹏军、李杨、安高峰、曹禹、原真、赵冉、杨兴城、刘志尧、李琳、王尊、张永静、毕继华、谢承运、彭华、马立祥、赵佳宁、张卫东、刘为华、王冲华、王思蕊、郭洋、查奇文、赵梓桐、曾珍珍、张瑜、刘振宇、张静、苏扬、杨祎巍、黄思齐、李景田、刘昉、王许培、裴彦纯、马霄、郝鑫、安成飞。

引　言

工业互联网企业数量众多、信息化发展程度不同且承载业务类型相异，所属行业网络安全防护规律差异化明显，为解决现有网络安全防护要求无法满足工业互联网企业发展实际需求的问题，需实施工业互联网企业网络安全分类分级管理并编制相关标准。

GB/T 44462《工业互联网企业网络安全》是指导工业互联网企业开展网络安全分类分级防护工作的基础性标准，旨在针对应用工业互联网的工业企业、工业互联网平台企业、工业互联网标识解析企业及企业数据安全，提出不同级别的网络安全管理及安全防护技术要求，用于指导企业落实与自身级别相适应的安全防护措施，由于文件的使用者需求不同，由四个部分构成。

——第1部分：应用工业互联网的工业企业防护要求。目的在于提出应用工业互联网的工业企业开展网络安全分类分级防护工作需要落实的安全要求。

——第2部分：平台企业防护要求。目的在于提出工业互联网平台企业开展网络安全分类分级防护工作需要落实的安全要求。

——第3部分：标识解析企业防护要求。目的在于提出工业互联网标识解析企业开展网络安全分类分级防护工作需要落实的安全要求。

——第4部分：数据防护要求。目的在于提出工业互联网企业开展网络安全分类分级防护工作需要落实的数据安全要求。

本文件面向应用工业互联网的工业企业，提出了初始级、基本级、增强级三个不同级别的安全要求，指导企业实施工业互联网安全分类分级管理工作，为应用工业互联网的工业企业各类信息系统安全防护水平提升奠定基础，为企业整体工业互联网安全防护能力建设提供指导。

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

1 范围

本文件规定了应用工业互联网的工业企业在设备、控制、网络、应用平台软件、管理以及物理环境等方面不同级别的网络安全防护要求。

本文件适用于指导应用工业互联网的工业企业开展网络安全分类分级防护工作。

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 25069 信息安全技术 术语

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 42021 工业互联网 总体网络架构

3 术语和定义

GB/T 25069 和 GB/T 42021 界定的以及下列术语和定义适用于本文件。

3.1

应用工业互联网的工业企业 internet industrial enterprise

运用工业互联网技术实现智能控制、运营优化和生产组织方式变革的工业企业。

4 缩略语

下列缩略语适用于本文件。

AGV:自动导引运输车(Automated Guided Vehicle)

APP:应用程序(Application)

CNC:计算机数字控制(Computer Numerical Control)

DCS:集散控制系统(Distributed Control System)

DPU:分散处理单元(Distributed Processing Unit)

ERP:企业资源计划(Enterprise Resource Planning)

HMI:人机界面(Human Machine Interface)

IED:智能电子设备(Intelligent Electronic Device)

MES:生产执行系统(Manufacturing Execution System)

PLC:可编程逻辑控制器(Programmable Logic Controller)

RTU：远程终端单元(Remote Terminal Unit)
SCADA：数据采集与监视控制系统(Supervisory Control and Data Acquisition System)
UPS：不间断电源(Uninterrupted Power Supply)
USB：通用串行总线(Universal Serial Bus)

5 应用工业互联网的工业企业安全防护级别的确定

应用工业互联网的工业企业应按照工业互联网企业网络安全定级方法确定级别，由低到高划分为一级、二级、三级，采取不同程度的安全防护，如表1所示。应用工业互联网的工业企业的安全防护要求分为初始级、基本级和增强级三个级别，其中：

——一级的应用工业互联网的工业企业按照初始级防护要求采取防护措施；
——二级的应用工业互联网的工业企业按照基本级防护要求采取防护措施；
——三级的应用工业互联网的工业企业按照增强级防护要求采取防护措施。

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	安全防护要求级别
一级	初始级
二级	基本级
三级	增强级

6 应用工业互联网的工业企业安全防护范围

安全防护从设备安全、控制安全、网络安全、应用平台安全、物理和环境安全以及安全管理要求等方面开展，应用工业互联网的工业企业典型网络层次架构示例参见附录A，安全防护范围具体包括：

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；
b) 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、智能装备控制安全等；
c) 网络安全防护：包括架构安全、边界安全、通信安全等；
d) 应用平台软件安全防护：包括平台软件安全、工业APP安全等；
e) 安全管理：包括机构管理、制度管理、人员管理、建设管理、运维管理等；
f) 物理环境安全：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。

7 应用工业互联网的工业企业安全防护要求

7.1 初始级防护要求

7.1.1 设备安全防护要求

7.1.1.1 工业主机安全

本项要求包括：

a) 应对移动存储介质的接入和使用的权限进行管理和控制；

b) 应规范工业主机系统软硬件安装和使用，禁止未授权的情况下擅自安装、卸载、升级软件及更改软硬件配置；
c) 应对工业主机外部接口进行管控，对外部接入设备，特别是有线或无线通信设备进行管理和控制。

7.1.1.2 网络设备安全

本项要求包括：
a) 应对网络设备采取登录失败处理措施，包括限制登录失败次数、结束会话等；
b) 应对网络设备的接口进行管控，关闭或封锁不使用的网络端口。

7.1.1.3 工业控制设备安全

本项要求包括：
a) 对采用无线通信技术的工业控制设备，应对无线通信采取传输加密的安全措施，保证传输报文的保密性；
b) 如受条件限制控制设备无法采用相关安全措施，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。

7.1.2 控制安全防护要求

7.1.2.1 应用工业互联网的工业企业控制系统安全

本项要求包括：
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。

7.1.2.2 控制软件安全

本项要求包括：
a) 应具备登录控制功能，对登录用户进行身份鉴别与访问权限控制；
b) 若生产控制软件自身无法实现相应功能，可以通过网络设备、安全设备或安全管理等其他设备或手段，满足相应的安全要求。

7.1.2.3 配置安全

本项要求包括：
a) 应建立针对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、配置变更操作、配置变更结果及时间戳等信息；
b) 应按照最小化原则禁用非必要的后台程序、进程、端口、服务，应定期对账户、口令、端口、服务等内容进行检查。

7.1.2.4 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。

7.1.3 网络安全防护要求

7.1.3.1 架构安全

应划分不同的网络安全域，其中工业控制系统与企业其他系统划分不同安全域，按照安全管理和控

制的原则为各安全域分配地址。

7.1.3.2 边界安全

本项要求包括：

a) 工业企业应定义明确企业网络与互联网、企业网络内部各控制系统网络和非控制系统网络、重要控制系统网络与非重要控制系统网络的安全边界；

b) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

7.1.3.3 通信安全

应采用校验技术保证通信过程中数据的完整性。

7.1.4 应用平台软件安全防护要求

7.1.4.1 平台软件安全

本项要求包括：

a) 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；

b) 在使用平台软件的过程中，应定期更新平台软件。

7.1.4.2 工业 APP 安全

本项要求包括：

c) 工业 APP 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；

d) 在使用工业 APP 过程中，应区分操作员、管理员、审计员等不同角色，并赋予不同操作权限。

7.1.5 安全管理要求

7.1.5.1 机构管理

本项要求包括：

a) 应设立网络安全管理工作的职能部门，具体承担网络安全管理工作，组织制定和落实网络安全管理制度，落实网络安全技术防护措施，开展网络安全宣传教育培训，执行网络安全监督检查等；

b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责；

c) 设立安全负责人岗位，以及系统管理员、网络管理员、安全管理员等专职人员岗位，并明确部门、各负责人和专职人员的岗位职责，明确授权审批事项、审批部门和批准人等。

7.1.5.2 制度管理

本项要求包括：

a) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；

b) 应指定或授权专门的部门或人员负责安全管理制度的制定；

c) 根据机构的安全工作总体方针和安全策略，建立适合机构安全工作实际情况的安全管理制度，覆盖机构和人员、物理和环境、安全建设和安全运维等层面的管理内容。

7.1.5.3 人员管理

本项要求包括：

a） 应指定或授权特定的部门或人员负责人员录用；

b） 应对被录用人员的身份、背景、专业资格和资质等进行审查；

c） 应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

7.1.5.4 建设管理

7.1.5.4.1 定级

本项要求包括：

a） 应明确本企业的安全等级；

b） 应以书面形式说明企业确定为某安全等级的方法和理由。

7.1.5.4.2 安全方案设计

本项要求包括：

a） 应按照企业等级情况，选择对应级别安全措施，依据风险分析的结果补充和调整安全措施；

b） 应形成能指导安全系统建设、安全产品采购和使用的详细设计方案。

7.1.5.4.3 产品采购和使用

本项要求包括：

a） 安全产品与服务的采购和使用应符合国家有关规定；

b） 网络关键设备及网络安全专用产品应通过专业机构的安全性检测后方可采购使用。

7.1.5.4.4 软件开发

应在软件交付前进行安全性测试，测试内容至少包括恶意代码检测。

7.1.5.4.5 系统交付

本项要求包括：

a） 应制定安全性测试验收方案，并依据测试验收方案实施验收，形成验收报告；

b） 应根据交付清单对所交接的设备、软件和文档等进行清点；

c） 应对负责运行维护的技术人员进行相应的技能培训；

d） 应提供建设过程中的文档和指导用户进行运行维护的文档。

7.1.5.4.6 供应链安全

本项要求包括：

a） 应选择安全合规的设备、服务、系统及软件供应商，且供应商能够为自身提供的设备、平台、系统等所承载的业务提供相应的安全防护能力；

b） 与供应商签订的协议中，应明确各方需履行的安全相关责任和义务，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；

c） 应与选定的供应商签署保密协议，要求其不应泄露客户数据和业务系统的相关重要信息。

7.1.5.5 运维管理

7.1.5.5.1 环境管理

应对机房、部署工业互联网设备区域的安全管理做出规定，指定特定的部门或人员，对出入进行管控，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。

7.1.5.5.2 资产管理

本项要求包括：

a) 应建立保护对象资产清单，包括资产责任部门、重要程度和所处位置等，工业互联网设备应包括设备型号、固件名称、固件版本及固件系统等信息；
b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。

7.1.5.5.3 密码管理

本项要求包括：

c) 使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，密码产品应经检测认证合格；
d) 根据 GB/T 39786 中密码应用基本要求等级，企业涉及的相关业务系统的管理者可根据业务实际情况选择相应级别的密码保障技术能力及管理能力。

7.1.5.5.4 配置管理

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

7.1.5.5.5 安全事件及应急处置

本项要求包括：

a) 应建立网络安全监测预警和信息通报制度，建设工业互联网安全监测技术手段；
b) 应及时向工业互联网安全主管部门报告所发现的安全弱点和可疑事件。

7.1.6 物理环境安全要求

7.1.6.1 物理位置选择

本项要求包括：

a) 室外工业互联网重要设备及控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；
b) 放置室外工业互联网重要设备及控制设备的箱体或装置应具有透风、散热、防盗、防雨和防火能力等。

7.1.6.2 物理访问控制

应在机房和工业设备放置场地出入口安排专人值守或部署电子门禁系统，控制、鉴别和记录进出的人员。

7.1.6.3 防盗窃和防破坏

应将设备或主要部件进行固定，并设置明显的不易除去的标记，如粘贴标签或铭牌、电子标签。

7.1.6.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

7.1.6.5 防火

机房应设置灭火设备。

7.1.6.6 防水和防潮

应采取措施防止雨水通过机房或场地窗户、屋顶和墙壁渗透。

7.1.6.7 温湿度控制

应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

7.1.6.8 电力供应

应在机房供电线路上配置稳压器和过电压防护设备。

7.2 基本级防护要求

7.2.1 设备安全防护要求

7.2.1.1 工业主机安全

除满足 7.1.1.1 之外，还符合以下要求：

a) 宜结合企业运检修周期开展主机安全检查，包括但不限于恶意代码查杀，对临时接入设备在接入前进行恶意代码查杀，并留存相应记录；
b) 应对工业主机的账户和口令进行管理，合理设置账户类型和权限，严禁使用空口令、弱口令，口令长度应至少 8 位，并包含数字、大写字母、小写字母、特殊字符 4 类中至少 3 类，保持口令定期更换，并定期处理多余、过期、共享、僵尸账户；
c) 应配置工业主机安全策略，并建立安全策略配置清单，定期确认相关安全策略的合规性和有效性；
d) 应采用恶意代码防范手段，对于无法及时更新恶意代码库的场景，宜安装工业主机白名单防护软件；
e) 在工业主机硬件安装使用过程中，应拆除或封闭工业主机上不必要的 USB、光驱、无线等接口，防止病毒、木马、蠕虫等恶意代码入侵，并避免数据泄露；
f) 应关闭与系统业务无关的端口和服务。

7.2.1.2 网络设备安全

除满足 7.1.1.2 之外，还符合以下要求：

a) 应对网络设备上账户、口令进行检查，严禁使用空口令、弱口令，口令长度应至少 8 位，并包含数字、大写字母、小写字母、特殊字符 4 类中至少 3 类，定期处理多余、过期、共享、僵尸账户；
b) 应对网络设备的运行日志和操作日志进行定期审计分析，发现安全风险或问题，应及时处理；
c) 应对网络设备的远程维护实行实时监管和审计，防止高危操作影响正常业务运行；

d） 应对临时接入的设备进行安全扫描，并留存安全扫描记录。

7.2.1.3 工业控制设备安全

除满足 7.1.1.3 之外，还符合以下要求：

a） 工业控制设备应具备对访问行为主体（人员、进程和设备等）进行标识与鉴别的功能；

b） 工业控制设备应具备访问控制与审计功能，支持基于角色的访问控制策略，并对重要的安全性事件和重要生产活动进行审计；

c） 工业控制设备应具备数据完整性校验功能，具备抵御数据包插入、丢失、重放、篡改的能力。

7.2.2 控制安全防护要求

7.2.2.1 应用工业互联网的工业企业控制系统安全

除满足 7.1.2.1 之外，还符合以下要求：

a） 应对重要工业控制系统部署访问控制、操作审计等安全措施；

b） 工业控制系统不应与互联网直接相连，如确需连接互联网并从工业控制系统获取数据时，应部署相应安全防护设备进行防护，以防止外部对工业控制系统进行渗透攻击和控制操作；

c） 应对工业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）保留至少 6 个月，并定期备份防止丢失或被篡改；

d） 对于新部署的工业控制系统，应在上线前进行安全检查评估。

7.2.2.2 控制软件安全

除满足 7.1.2.2 之外，还符合以下要求：

a） 应对控制软件应用层代码文件、工程文件、重要操作记录文件等进行完整性保护；

b） 应保存启动、停止、复位以及用户登录、访问、退出等关键动作的操作日志，日志记录的留存时间不少于 6 个月；

c） 生产控制软件开发、升级或更新后，应在测试环境进行充分地测试，确保软件的可用性和安全性后，再进行正式部署。

7.2.2.3 配置安全

除满足 7.1.2.3 之外，还符合以下要求：

在进行配置变更时，应先完成配置变更测试验证，验证之后方可进行正式的配置变更，应对变更操作进行记录，在出现配置变更问题时可以进行快速回退复原。

7.2.2.4 智能装备控制安全

除满足 7.1.2.4 之外，还符合以下要求：

a） 对工业互联网平台直接控制的现场重要设备（如 AGV、CNC 机床、工业机器人等），应确认设备身份的唯一性安全标识，以便针对现场重要设备进行安全识别和访问控制；

b） 现场重要设备应具有识别验证控制指令来源、访问控制功能；

c） 应采用校验技术或密码技术保证现场重要设备在进行数据交互过程中数据的完整性。

7.2.3 网络安全防护要求

7.2.3.1 架构安全

除满足 7.1.3.1 之外，还符合以下要求：

a) 应在工业企业网络安全架构的确定和更改前考虑潜在的安全风险和所承载业务的重要性，如有变更需对网络安全架构进行评审；
b) 应保证网络的带宽满足业务高峰期需求，并考虑异常生产工况、突发业务等情况下的带宽需求；
c) 应保证网络线路与设备的业务处理能力满足业务高峰期需要。

7.2.3.2 边界安全

除满足 7.1.3.2 之外，还符合以下要求：
a) 不宜将重要网络区域划分在边界处，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；
b) 应在网络边界进行安全监测，识别网络边界的入侵行为，具备入侵行为阻断能力。

7.2.3.3 通信安全

除满足 7.1.3.3 之外，还符合以下要求：
a) 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手段进行数据传输、访问控制；
b) 应对无线连接的授权、监视以及执行使用进行限制。

7.2.4 应用平台软件安全防护要求

7.2.4.1 平台软件安全

除满足 7.1.4.1 之外，还符合以下要求：
a) 应在平台内部区分不同模块的读写权限并限制读写范围；
b) 应具备虚拟化安全设备，对平台内的功能模块、虚拟机等资源进行安全防护；
c) 应监测、记录网络运行状态和网络安全事件，保存平台软件的操作日志，并定期备份，保存期限不少于 6 个月，避免受到未预期的删除、修改或覆盖等。

7.2.4.2 工业 APP 安全

除满足 7.1.4.2 之外，还符合以下要求：
a) 应在工业 APP 中集成具有网络安全防护功能的模块；
b) 在使用工业 APP 过程中，应根据工业 APP 的被控对象、功能和使用场景，细化账号权限范围，并定期检查账号权限范围，及时取消不必要的授权；
c) 应对使用工业 APP 的用户进行身份认证，严禁使用空口令、弱口令，口令长度应至少 8 位，并包含数字、大写字母、小写字母、特殊字符 4 类中至少 3 类，保持口令定期更换，并定期处理多余、过期、共享、僵尸账户。

7.2.5 安全管理要求

7.2.5.1 机构管理

除满足 7.1.5.1 之外，还符合以下要求：
a) 加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理安全问题；
b) 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；
c) 应加强与工业互联网安全主管部门、各类供应商、业界专家等合作与沟通，建立外联单位联系列表，包括外联单位名称、联系人和联系方式等信息。

7.2.5.2 制度管理

除满足 7.1.5.2 之外，还符合以下要求：

a) 安全管理制度应通过正式、有效的方式发布，并进行版本控制；

b) 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。

7.2.5.3 人员管理

除满足 7.1.5.3 之外，还符合以下要求：

a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b) 应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

c) 应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案，外部人员离场后应及时清除其所有的访问权限。

7.2.5.4 建设管理

7.2.5.4.1 定级

同 7.1.5.4.1。

7.2.5.4.2 安全方案设计

除满足 7.1.5.4.2 之外，还符合以下要求：

a) 应根据安全防护对象的安全防护需求进行安全方案设计；

b) 应组织相关部门和有关安全专家对安全方案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。

7.2.5.4.3 产品采购和使用

同 7.1.5.4.3。

7.2.5.4.4 软件开发

除满足 7.1.5.4.4 之外，还符合以下要求：

a) 应确保工业控制系统的开发、测试和生产环境保持独立，避免开发、测试环境中的安全风险引入生产系统；

b) 应要求开发单位提供软件设计文档和使用指南；

c) 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、严禁关键技术扩散和设备行业专用等方面的约束条款。

7.2.5.4.5 系统交付

同 7.1.5.4.5。

7.2.5.4.6 供应链安全

除满足 7.1.5.4.6 之外，还符合以下要求：

a) 应制定供应链安全策略(包括采购策略等)，并对安全策略的有效性进行持续监控；

b) 应在服务协议中规定服务合约到期时，完整地返还客户信息，并承诺相关信息均已清除；
c) 应确保外包运维服务商的选择符合国家的有关规定；
d) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

7.2.5.5 运维管理

7.2.5.5.1 环境管理

除满足 7.1.5.5.1 之外，还符合以下要求：
重要区域不宜接待来访人员，不应随意放置含有敏感信息的纸档文件和移动介质等。

7.2.5.5.2 资产管理

除满足 7.1.5.5.2 之外，还符合以下要求：
a) 应建立资产(包括工业互联网设备)管理制度，对资产入库、存储、部署、携带、维修、丢失和报废等过程进行管理；
b) 应建立存储介质相关资产台账(清单)，对存储介质进行标识管控；
c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
d) 应记录工业互联网设备的状态(包括外观、电量、指示灯等信息)，对工业互联网设备进行现场维护(除尘、充电、修理等)；
e) 应优先选择资质完备、经验丰富、安全可靠的运维服务商，应在合同中或以其他方式明确供应商应承担的网络安全责任和义务；
f) 应密切关注产品漏洞和补丁发布，及时进行软件升级、补丁安装管理，工业控制系统软件升级、补丁安装前应请专业技术机构进行安全评估和验证。

7.2.5.5.3 密码管理

同 7.1.5.5.3。

7.2.5.5.4 安全审计

本项要求包括：
a) 应对重要设备、平台、系统等启用安全审计功能，对重要的用户行为和重要安全事件进行审计，审计记录应包括事件的时间日期、用户、事件类型、事件简介及其他与审计相关的信息；
b) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
c) 审计记录中不宜使用明文记录敏感数据，如用户口令等；
d) 审计记录的留存时间应不少于 6 个月。

7.2.5.5.5 配置管理

除满足 7.1.5.5.4 之外，还符合以下要求：
a) 应定期对工业控制系统安全策略配置进行定期评估和优化，并建立安全策略配置清单；
b) 应定期对网络设备的业务配置和安全配置进行核查，防止网络安全风险的发生影响业务系统。

7.2.5.5.6 安全事件及应急处置

除满足 7.1.5.5.5 之外，还符合以下要求：
a) 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，留存相应

记录；

b） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

c） 应制定网络安全事件应急预案，包括应急处理流程、系统恢复流程等内容，并定期进行评估和修订。

7.2.6 物理环境安全要求

7.2.6.1 物理位置选择

除满足 7.1.6.1 之外，还符合以下要求：

a） 机房和常规工业设备放置场地应选择在具有防震、防风和防雨等能力的建筑内；

b） 机房场地不宜设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

7.2.6.2 物理访问控制

除满足 7.1.6.2 之外，还符合以下要求：

a） 应在重要服务器、数据库、工程师站等核心工业互联网软硬件所在区域或工业互联网平台采取视频监控等手段；

b） 人员进出记录应至少保存 3 个月，机房出入口应有视频监控，监控记录应至少保存 3 个月。

7.2.6.3 防盗窃和防破坏

除满足 7.1.6.3 之外，还符合以下要求：

a） 应将通信线缆铺设在隐蔽安全处，可铺设在管道或线槽、线架中；

b） 主机房或重要设备区域应安装必要的防盗报警设施或设置有专人值守的视频监控系统，监控录像记录应至少保存 3 个月。

7.2.6.4 防雷击

除满足 7.1.6.4 之外，还符合以下要求：

应对室外控制设备电源、信号线路加装浪涌保护器等避雷装置。

7.2.6.5 防火

除满足 7.1.6.5 之外，还符合以下要求：

机房及工业设备放置场地应设置灭火设备和火灾自动报警系统。

7.2.6.6 防水和防潮

除满足 7.1.6.6 之外，还符合以下要求：

应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

7.2.6.7 防静电

本项要求包括：

应采用防静电地板或地面并采用必要的接地防静电措施。

7.2.6.8 温湿度控制

除满足 7.1.6.7 之外，还符合以下要求：

应设置温湿度自动调节设施，使工业互联网平台相关设备放置场地的温湿度的变化处于设备运行所允许的范围之内。

7.2.6.9 电力供应

除满足 7.1.6.8 之外，还符合以下要求：

应提供短期的备用电力供应，保障设备在断电情况下仍正常运行。

7.2.6.10 电磁防护

本项要求包括：

电源线和通信线缆应铺设在不同的桥架或管道，避免互相干扰。

7.3 增强级防护要求

7.3.1 设备安全防护要求

7.3.1.1 工业主机安全

除满足 7.2.1.1 之外，还符合以下要求：

a) 应在不影响业务系统运行的前提下，定期对主机设备系统进行补丁更新，补丁安装前要进行完整性和可用性验证；
b) 工业主机应安装白名单软件或防恶意代码软件并定期更新病毒库，更新前应进行离线测试避免影响工业主机的可用性；
c) 应对工业主机系统内的关键系统文件、业务文件、注册表信息等进行安全防护，对文件和注册表的操作权限进行管控；
d) 应通过主机外设安全管理和技术手段对确需使用工业主机外设接口的设备实施访问控制，并对设备进行安全验证，以避免未授权的外设终端接入；
e) 应对临时接入的主机类设备采用技术和管理手段进行访问控制，在进行安全扫描保证安全的前提下接入，并对设备的行为进行审计和管控，留存相应记录；
f) 对主机采用技术手段进行防护策略配置时，应留存相应记录。

7.3.1.2 网络设备安全

除满足 7.2.1.2 之外，还符合以下要求：

a) 应对网络设备的配置文件进行定期离线备份；
b) 应及时更新网络设备系统和补丁，系统和补丁升级前进行安全性验证，并提前对重要文件进行备份；
c) 应定期对网络设备系统进行漏洞扫描，对发现的安全漏洞及时处理，并保证相应操作不影响业务运行；
d) 应对网络监控日志进行管理和审计分析，发现安全风险或问题，及时进行处理；
e) 应对网络设备的远程管理采取必要的安全措施，对远程操作进行实时审计和管控。

7.3.1.3 工业控制设备安全

除满足 7.2.1.3 之外，还符合以下要求：

a) 对于控制设备内部的关键程序和文件，应具备对其进行加密和操作授权的功能，防止关键业务逻辑被窃取和篡改；
b) 如确需远程维护，应进行实时监管和审计，防止异常操作影响正常业务运行；

c) 宜部署统一配置管理平台对 RTU、IED、DPU 等现场测控设备进行集中管理；
d) 对于直接或依靠其他工具提供备份功能的现场测控设备，应进行应用级和系统级信息（包括系统安全状态信息）的备份；
e) 对未使用的网络接口或串行通信接口，应默认为关闭状态。

7.3.2 控制安全防护要求

7.3.2.1 应用工业互联网的工业企业控制系统安全

除满足 7.2.2.1 之外，还符合以下要求：

a) 应定期对工业控制系统安全配置进行核查审计，避免因调试或其他操作导致配置变更后，未及时更新配置清单；
b) 应部署具备对工业控制系统进行状态监测、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、端口扫描、暴力破解等网络攻击或异常行为；
c) 应每半年或在系统重大变更后，对工业控制系统进行安全检查和评估，防止出现重大安全缺陷或安全漏洞；
d) 对发现的重大安全缺陷或安全漏洞，经过充分测试评估后，应及时进行修补或建立针对性的检测防护技术措施。

7.3.2.2 控制软件安全

除满足 7.2.2.2 之外，还符合以下要求：

a) 应采取措施保证控制软件的软硬件运行环境安全；
b) 应具备容错机制，在发生单点故障时，应能持续提供生产控制功能；
c) 应当在保证生产控制软件可靠、稳定运行的基础上，提高生产控制软件自身的安全防护能力；
d) 应对控制软件进行第三方代码安全审计，对发现的安全缺陷或安全漏洞及时进行修补或采取必要措施防护。

7.3.2.3 配置安全

除满足 7.2.2.3 之外，还符合以下要求：

a) 应具备恶意代码防护、服务器口令、服务器安全审计、服务器补丁更新、网络设备等口令接入控制及统一防护等方面的策略；
b) 应设立独立的配置变更管理服务器，用于存放配置信息及备份的配置，按照约定的周期备份配置，并定期开展备份恢复测试；
c) 应严格管理配置管理库的访问权限，核心配置信息要控制知悉范围，配置管理库的完整性、可用性要得到保证；
d) 应建立机制定期评审正在运行的配置，以发现潜在的风险或任何可能优化配置的改进点。

7.3.2.4 智能装备控制安全

除满足 7.2.2.4 之外，还符合以下要求：

a) 现场重要设备应支持异常指令、状态等的审计数据上报；
b) 工业互联网平台与其直接控制的现场重要设备（如 AGV、工业机器人、CNC 机床等）通信时，应通过平台侧或终端侧对流量进行限制。

7.3.3 网络安全防护要求

7.3.3.1 架构安全

除满足 7.2.3.1 之外，还符合以下要求：

a) 应能够按照业务服务的重要程度分配带宽，优先保障重要业务；
b) 应提供通信线路、关键网络设备的硬件冗余，保证网络的可用性。

7.3.3.2 边界安全

除满足 7.2.3.2 之外，还符合以下要求：

a) 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网；
b) 在控制网络和非控制网络的边界防护机制失效时，应能及时阻止边界通信；
c) 应在控制系统内安全域以及企业整体安全域之间的边界防护机制失效时，及时进行报警，并保障不影响关键设备间的通信；
d) 当使用无线设备连接控制网络和非控制网络，或连接控制网络内不同安全域时，应对无线设备采取边界防护措施，包括但不限于身份标识和鉴别、访问控制等；
e) 应在网络边界节点处对恶意代码进行检测和清除，并维护恶意代码防护主程序及特征库的升级和更新。

7.3.3.3 通信安全

除满足 7.2.3.3 之外，还符合以下要求：

a) 应采用密码技术保证通信过程中数据的保密性；
b) 在工业企业内部网络进行通信数据传输时，应在通信前对通信的双方进行身份认证。

7.3.4 应用平台软件安全防护要求

7.3.4.1 平台软件安全

除满足 7.2.4.1 之外，还符合以下要求：

a) 针对平台内部核心功能模块，应采用审核或白名单机制，只允许审核通过的设备访问核心功能模块；
b) 针对平台内部对外提供服务的功能模块，应具备注册机制，掌握设备接入情况，可以在发生异常情况时，及时拒绝异常设备接入；
c) 应采取措施保障虚拟机安全，包括虚拟机隔离，实时监控虚拟机资源使用情况等。

7.3.4.2 工业 APP 安全

除满足 7.2.4.2 之外，还符合以下要求：

a) 应在部署工业 APP 之前，检测工业 APP 的潜在安全漏洞，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
b) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
c) 应定期更换工业 APP 的认证口令；
d) 对于重点设备和重点数据的敏感访问和操作，应采用多因素认证。

7.3.5 安全管理要求

7.3.5.1 机构管理

除满足 7.2.5.1 之外，还符合以下要求：

a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
b) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

7.3.5.2 制度管理

除满足 7.2.5.2 之外，还符合以下要求：
a) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；
b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
c) 应确定安全检查内容，汇总安全检查数据，形成安全检查报告，根据安全检查结果进行整改。

7.3.5.3 人员管理

除满足 7.2.5.3 之外，还符合以下要求：
a) 应对被录用人员具备的技术技能进行考核，与被录用人员签订保密协议；
b) 应明确关键岗位，关键岗位人员上岗前应签订岗位责任协议，在调离关键岗位时，应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
c) 应配备专职安全管理员，不可兼任，关键岗位应配备多人共同管理；
d) 应针对不同岗位开展针对性网络安全相关培训，应定期对相关人员进行技能考核；
e) 接触系统的外部人员应签署保密协议，严禁非授权操作和获取敏感信息，严禁访问关键区域或系统。

7.3.5.4 建设管理

7.3.5.4.1 定级

同 7.2.5.4.1。

7.3.5.4.2 安全方案设计

除满足 7.2.5.4.2 之外，还符合以下要求：
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。

7.3.5.4.3 产品采购和使用

除满足 7.2.5.4.3 之外，还符合以下要求：
a) 应预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；
b) 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。

7.3.5.4.4 软件开发

除满足 7.2.5.4.4 之外，还符合以下要求：
a) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
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。

7.3.5.4.5 系统交付

除满足 7.2.5.4.5 之外，还符合以下要求：

安全测试报告应包含密码应用安全性测试相关内容。

7.3.5.4.6 供应链安全

除满足 7.2.5.4.6 之外，还符合以下要求：

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，如涉及重要变更，评估变更带来的安全风险，采取有关措施对风险进行控制。

7.3.5.5 运维管理

7.3.5.5.1 环境管理

除满足 7.2.5.5.1 之外，还符合以下要求：

a) 应明确重要安全区域，对进入重要安全区域的人员进行活动实时监视等；
b) 应加强对工业互联网设备部署区域设施、文件等的保密性管理，包括但不限于部署图纸、设备检查工具、设备维护记录等。

7.3.5.5.2 资产管理

除满足 7.2.5.5.2 之外，还符合以下要求：

a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
b) 应对信息分类与标识方法明确规定，并对信息的使用、传输和存储等进行规范化管理；
c) 应确保信息处理设备在带离机房、现场设备区和办公地点前已进行审批，含有存储介质的设备带出工作环境时重要数据应加密；
d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；
e) 应建立资产变更的申报和审批程序，依据程序控制所有的变更，记录变更实施过程；
f) 应建立各类工业互联网设备的主控芯片型号、软件版本、操作系统（如有）名称及版本等设备底层信息台账。

7.3.5.5.3 密码管理

同 7.2.5.5.3。

7.3.5.5.4 安全审计

除满足 7.2.5.5.4 之外，还符合以下要求：

a) 应能对远程访问企业内部网络的用户行为进行审计和数据分析；
b) 应对审计进程进行保护，防止未经授权的中断。

7.3.5.5.5 配置管理

除满足 7.2.5.5.5 之外，还符合以下要求：

应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

7.3.5.5.6 安全事件及应急处置

除满足 7.2.5.5.6 之外，还符合以下要求：

a) 应建设完善工业互联网安全监测技术手段，宜接入国家级或省级工业互联网安全监测平台；
b) 对造成业务中断和信息泄露的重大安全事件应采用不同的处理程序和报告程序；
c) 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
d) 应定期开展网络安全应急演练，检验应急预案的可操作性，并结合应急演练结果，对应急预案进行评估和适用性修订。

7.3.6 物理环境安全要求

7.3.6.1 物理位置选择

除满足 7.2.6.1 之外，还符合以下要求：

a) 机房场地不应设在建筑物用水设备的隔壁或下层，否则应加强防水和防潮措施；
b) 确保工业互联网平台服务器及运行关键业务和数据的物理设备位于中国境内；
c) 对于存在爆炸危险的生产车间(装置)，主机房、现场控制室、现场机柜室应位于爆炸危险区域外。

7.3.6.2 物理访问控制

除满足 7.2.6.2 之外，还符合以下要求：

针对重要核心工业互联网软硬件所在区域或工业互联网平台(如工程师站、数据库、服务器、工业控制设备等)应划分重点物理安全防护区域。

7.3.6.3 防盗窃和防破坏

除满足 7.2.6.3 之外，还符合以下要求：

a) 应对机房设置监控报警系统或设置有专人值守的视频监控系统，非 7×24 h 人员值守和巡查的机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵及时显示入侵部位，并驱动声光报警装置；
b) 应将室外控制设备安装在具有防盗能力的箱体或装置中；
c) 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和技术手段实施严格访问控制。

7.3.6.4 防雷击

同 7.2.6.4。

7.3.6.5 防火

除满足 7.2.6.5 之外，还符合以下要求：

a) 机房及工业设备放置场地应设置灭火设备和火灾自动报警系统，能够自动检测火情、自动报警，并自动灭火；
b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

7.3.6.6 防水和防潮

除满足 7.2.6.6 之外，还符合以下要求：

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和报警。

7.3.6.7 防静电

除满足 7.2.6.7 之外，还符合以下要求：

应采取措施防止静电的产生，例如，采用静电消除器、佩戴防静电手环等。

7.3.6.8 温湿度控制

同 7.2.6.8。

7.3.6.9 电力供应

除满足 7.2.6.9 之外，还符合以下要求：

a) 应配备 UPS，在配有发电机等后备电源的情况下，UPS 供电能力能支持到后备电源开始供电；

b) 备用电力供应的实际供电能力应满足主要设备和环境控制设备在断电情况下正常运行至少 2 h。

7.3.6.10 电磁防护

同 7.2.6.10。

附 录 A
（资料性）
应用工业互联网的工业企业典型网络层次架构示例

图 A.1 描述了应用工业互联网的工业企业的典型网络层次架构，根据图 A.1 的层次架构划分，各层具体组成及功能情况说明如下：

a） 企业资源层：以办公终端、服务器、云平台、ERP 等办公管理软件为主；

b） 生产管理层：以 MES 系统为代表的典型制造执行系统，包括各种服务器、云服务物理主机、业务应用系统、业务平台等，对生产过程进行管理，如制造数据管理、生产调度管理等；

c） 过程监控层：以生产过程的集中监控为目的构建的集中监控中心，包括工业监控主机、工业数据服务器、工业监视软件、SCADA 软件等，用于对生产过程数据进行采集与监控，并利用 HMI 系统实现人机交互；

d） 现场控制层：实现生产流程的采集、分析、计算、逻辑输出和反馈调节，包括各种 PLC、DCS 等系统及网络和主机等设备；

e） 现场设备层：包括各类数据采集传感器、无线发送接收设备、工业机器人、AGV 移动小车等就地设备，对生产过程进行感知与操作。

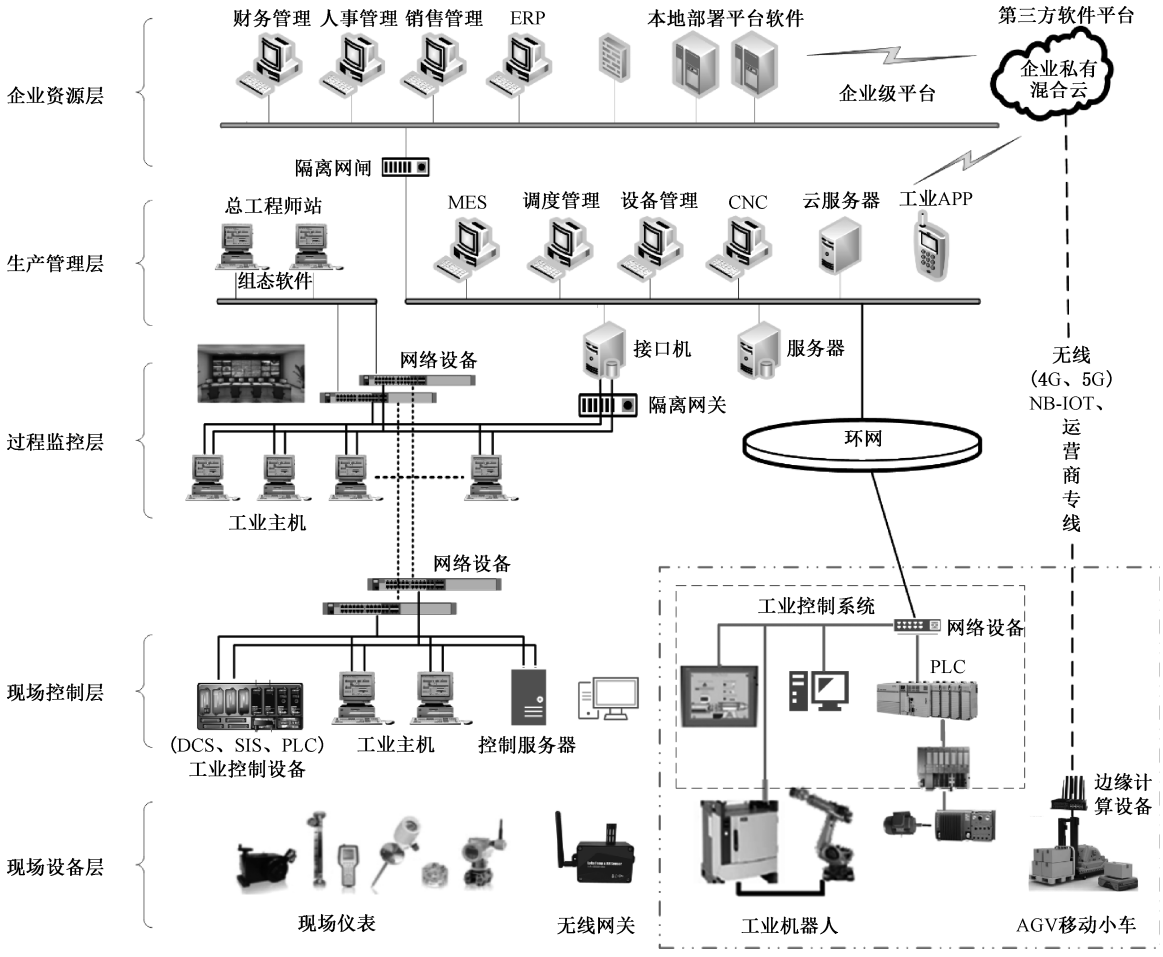

图 A.1 应用工业互联网的工业企业典型网络层次架构示意图

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 32919—2016 信息安全技术 工业控制系统安全控制应用指南
[3] GB/Z 41288—2022 信息安全技术 重要工业控制系统网络安全防护导则
[4] GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型
[5] 工业互联网安全分类分级管理办法(工信部网安〔2024〕68号)