ICS 35.030
CCS M 10

中华人民共和国国家标准

GB/T 44462.2—2024

工业互联网企业网络安全 第2部分：平台企业防护要求

Industrial internet enterprise cybersecurity—Part 2：Protection requirements of industrial internet platform 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2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：中国信息通信研究院、国家工业信息安全发展研究中心、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)、中国工业互联网研究院、中国电子技术标准化研究院、北京航空航天大学、上海宝信软件股份有限公司、卡奥斯物联科技股份有限公司、杭州安恒信息技术股份有限公司、南京中新赛克科技有限责任公司、奇安信科技集团股份有限公司、北京天融信网络安全技术有限公司、北京珞安科技有限责任公司、北京启明星辰信息安全技术有限公司、北京神州绿盟科技有限公司、国网电商科技有限公司、北京升鑫网络科技有限公司、郑州信大捷安信息技术股份有限公司、北京信安世纪科技股份有限公司、国能大渡河大数据服务有限公司、富士康工业互联网股份有限公司、腾讯(深圳)科技有限公司、国网河南省电力公司、西安热工研究院有限公司、上海电器科学研究所(集团)有限公司、北京六方云信息技术有限公司、长扬科技(北京)股份有限公司。

本文件主要起草人：魏亮、赵爽、李诗婧、张倩、柯皓仁、马娟、于广琛、李艺、秦国英、王吉、吴诗雨、王冲华、周昊、张哲宇、王斌斌、余涛、徐洪涛、李俊鹏、唐刚、张德馨、查奇文、李琳、糜靖峰、洪晟、安成飞、刘畅、寇增杰、张晓东、崔莹莹、尹雅伟、郭兴科、张福、刘为华、焦靖伟、李林、罗玮、党芳芳、李帅、杨东、苑鹏飞、李江力、汪义舟。

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。

本文件面向工业互联网平台企业，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，为工业互联网平台企业加强网络安全防护能力建设奠定基础。

工业互联网企业网络安全
第2部分:平台企业防护要求

1 范围

本文件规定了工业互联网平台企业在接入层、基础设施层、平台层、应用层、管理以及物理环境等方面不同级别的网络安全防护要求。

本文件适用于指导工业互联网平台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

GB 50174 数据中心设计规范

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

工业互联网 industrial internet

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态,通过对人、机、物、系统等的全面连接,构建起覆盖全产业链、全价值链的全新制造和服务体系。

[来源:GB/T 42021—2022,3.1]

3.2

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、高效配置的工业云平台。

3.3

工业互联网平台企业 industrial internet platform enterprise

面向制造业数字化、网络化、智能化需求,基于云平台等方式对外提供工业大数据、工业 APP 等资源和公共服务的企业。

4 缩略语

下列缩略语适用于本文件。

APP:应用程序(Application)

CPU:中央处理器(Central Processing Unit)
IP:网际互连协议(Internet Protocol)
PKI:公钥基础设施(Public Key Infrastructure)
SSL:安全套接层(Secure Socket Layer)

5 工业互联网平台企业安全防护级别的确定

工业互联网平台企业应按照工业互联网企业网络安全定级方法相关标准划分级别,由低到高划分为一级、二级、三级,采取不同程度的安全防护。工业互联网平台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,如表1所示,其中:

——一级工业互联网平台企业应按照初始级防护要求采取防护措施;
——二级工业互联网平台企业应按照基本级防护要求采取防护措施;
——三级工业互联网平台企业应按照增强级防护要求采取防护措施。

表1 工业互联网平台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 工业互联网平台企业安全防护范围

工业互联网平台企业安全防护范围从接入层安全、基础设施层安全、平台层安全、应用层安全、安全管理以及物理环境安全要求等方面展开,参见附录A。具体内容包括:

a) 接入层安全防护:主要指针对网关等接入设备提出安全防护规范,包括接入设备安全、接入层网络安全等方面;
b) 基础设施层安全防护:包括计算环境安全、网络安全、网络设备安全、虚拟化安全等方面;
c) 平台层安全防护:包括通用组件安全、通用接口安全、容器安全等方面;
d) 应用层安全防护:包括面向各类工业应用场景的业务应用安全等方面;
e) 安全管理:包括机构管理、制度管理、人员管理、安全建设管理、安全运维管理等方面;
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、电磁防护等方面。

7 工业互联网平台企业安全防护要求

7.1 初始级防护要求

7.1.1 接入层安全防护要求

7.1.1.1 接入设备安全防护要求

7.1.1.1.1 设备硬件安全

本项要求包括:

应使用物理方式移除或覆盖硬件接口、敏感引脚等关键物理接口，避免硬件调试接口直接暴露，若确需使用，应设置严格的访问控制手段。

7.1.1.1.2 设备系统安全

本项要求包括：

a) 设备应具备通过升级或更新的方式消除安全漏洞的能力；
b) 设备不应存在已公布的漏洞，或具备补救措施防范漏洞安全风险；
c) 系统设计应符合最小特权原则，用户只拥有执行其任务所需的最小权限，并禁止所有未被允许的权限；
d) 应禁用不安全的远程管理服务，如确需远程管理，应使用安全的通信协议；
e) 应对登录、调试、远程管理设备的用户进行身份标识和鉴别；
f) 身份标识应具有不易被冒用的特点，鉴别信息应具有复杂度要求并定期更换；
g) 应依法记录并留存相关访问日志，日志留存时长不少于 6 个月。

7.1.1.1.3 设备接入安全

本项要求包括：

应对接入工业互联网平台中的设备进行身份鉴别，确保接入设备为已授权的合法设备。

7.1.1.2 接入层网络安全防护要求

7.1.1.2.1 安全通信

本项要求包括：

a) 设备在通信过程中应对敏感数据、重要参数进行加密，保证传输数据内容的机密性；
b) 设备在通信过程中应具备安全机制，以确保数据传输的连续性，避免数据丢失；
c) 设备在通信过程中进行完整性校验，保证传输数据的有效性和完整性；
d) 应对接入层网络行为、安全事件等日志记录进行保护，如定期备份或配置日志访问权限等，避免记录受到未预期的删除、修改或覆盖等。

7.1.1.2.2 访问控制

本项要求包括：

应对接入设备的地址、端口、协议等进行检查，以允许/拒绝数据进出。

7.1.2 基础设施层安全防护要求

7.1.2.1 计算环境安全防护要求

7.1.2.1.1 身份鉴别

本项要求包括：

a) 应对登录计算环境的用户进行身份标识和鉴别；
b) 用户身份标识应具有不易被冒用的特点，鉴别信息应具有复杂度要求并定期更换；
c) 应对计算环境身份鉴别过程设置登录失败处理措施，防止暴力破解。

7.1.2.1.2 访问控制

本项要求包括：

a） 应及时删除或重命名默认账户，修改默认账户的默认口令，并删除多余账户；
b） 应根据用户的角色分配权限，实现用户的权限分离，仅授予用户所需的最小权限。

7.1.2.1.3 安全审计

本项要求包括：
a） 应对用户重要操作行为、安全事件等进行日志记录，日志留存时长不少于6个月；
b） 应对日志记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

7.1.2.1.4 资源控制

本项要求包括：
应对登录计算环境的并发会话数进行限制。

7.1.2.1.5 恶意代码防范

本项要求包括：
a） 应具备恶意代码检测和防范能力；
b） 应对恶意代码库进行维护和及时更新。

7.1.2.1.6 入侵防范

本项要求包括：
a） 应关闭不使用的服务或端口，防止非授权访问；
b） 计算设备应遵循最小化安装的原则，仅安装需要的组件和应用程序。

7.1.2.2 网络安全防护要求

7.1.2.2.1 架构安全

本项要求包括：
应绘制与当前运行情况相符的网络拓扑结构图。

7.1.2.2.2 访问控制

本项要求包括：
a） 应对跨越边界的访问和数据流提供访问控制措施；
b） 应对访问数据的源地址、目的地址、源端口、目的端口和协议等进行检查，以判断允许/拒绝数据进出；
c） 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力。

7.1.2.2.3 安全审计

本项要求包括：
a） 应监测、记录网络运行状态、网络安全事件，并留存相关的网络日志不少于6个月；
b） 应对日志记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

7.1.2.2.4 入侵防范

本项要求包括：
应在关键网络节点处检测和记录网络攻击行为。

7.1.2.3 网络设备安全防护要求

7.1.2.3.1 身份鉴别

本项要求包括：

a) 应对登录网络设备的用户进行身份标识和鉴别；

b) 用户身份标识应具有不易被冒用的特点，鉴别信息应具有复杂度要求并定期更换；

c) 应对网络设备身份鉴别过程设置登录失败处理措施，防止暴力破解。

7.1.2.3.2 访问控制

本项要求包括：

a) 应及时删除或重命名默认账户，修改默认账户的默认口令，并删除多余账户；

b) 应根据用户的角色分配权限，实现用户的权限分离，仅授予用户所需的最小权限。

7.1.2.3.3 资源控制

本项要求包括：

应对登录网络设备的并发会话数进行限制。

7.1.2.4 虚拟化安全防护要求

7.1.2.4.1 虚拟机安全

本项要求包括：

a) 应支持虚拟机之间、虚拟机与宿主机之间的隔离；

b) 虚拟机应能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保虚拟机崩溃后不影响虚拟机监控器及其他虚拟机；

c) 虚拟机应支持系统加固或使用经过加固的系统镜像。

7.1.2.4.2 虚拟网络安全

本项要求包括：

a) 应实现不同系统或应用虚拟网络之间的隔离；

b) 应在虚拟化网络边界部署访问控制措施，并设置访问控制规则。

7.1.2.4.3 虚拟化平台安全

本项要求包括：

平台应由授权管理员进行管理，管理员访问应具有身份鉴别机制，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换。

7.1.3 平台层安全防护要求

7.1.3.1 通用组件安全防护要求

7.1.3.1.1 身份鉴别

本项要求包括：

a) 应对管理通用组件的用户进行身份标识和鉴别；

b) 管理通用组件的用户身份标识应具有唯一性，鉴别信息应具有复杂度要求并定期更换；

c） 应启用登录失败处理功能，如采取结束会话、限制非法登录次数或自动退出等措施。

7.1.3.1.2 访问控制

本项要求包括：

a） 应在通用组件权限配置能力内，根据用户的业务需要，配置其所需的最小权限；

b） 应对配置文件配置最小的访问控制权限。

7.1.3.2 通用接口安全防护要求

7.1.3.2.1 身份鉴别

本项要求包括：

应具备对通用接口认证的能力。

7.1.3.2.2 访问控制

本项要求包括：

a） 应根据调用需求，按照最小化原则对接口调用进行控制；

b） 应对接口调用的情况进行日志记录，内容应包括日期和时间、请求主体、请求方式、请求内容、请求结果等，日志留存时长不少于6个月；

c） 应对日志记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

7.1.3.2.3 网络通信安全

本项要求包括：

应保证传输数据的机密性和完整性。

7.1.3.3 容器安全防护要求

7.1.3.3.1 构建安全

本项要求包括：

a） 容器应遵循最小化安装原则，只安装必要组件；

b） 应支持对容器镜像进行漏洞扫描，并安装必要的安全补丁。

7.1.3.3.2 分发安全

本项要求包括：

a） 应防止对不同版本的镜像重复使用；

b） 应对镜像进行管理，对于过期无用的镜像及时进行删除。

7.1.3.3.3 运行安全

本项要求包括：

a） 不宜使用管理员权限运行容器，禁止使用特权容器；

b） 宿主存储资源不应直接共享给容器，应为容器创建单独分区；

c） 应对容器资源的使用进行限制，如内存、处理器、网络、存储等。

7.1.3.3.4 维护安全

本项要求包括：

a) 应定期对容器进行漏洞扫描，并通过补丁升级的方式进行修复，保证容器不存在已公布的漏洞；
b) 应对容器内恶意代码进行检测。

7.1.4 应用层安全防护要求

7.1.4.1 身份鉴别

本项要求包括：
a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别，用户身份标识唯一；
b) 应提供登录失败处理功能，如采取结束会话、限制非法登录次数或自动退出等措施；
c) 应具备登录超时后锁定或注销功能。

7.1.4.2 访问控制

本项要求包括：
应严格限制用户的访问权限，按照用户需求控制用户对业务应用的访问。

7.1.4.3 运行安全

本项要求包括：
不应设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

7.1.4.4 资源控制

本项要求包括：
应限制对应用访问的最大并发会话连接数等资源配额。

7.1.4.5 上线前检测

本项要求包括：
应针对所有上线的应用，进行上线前的应用漏洞扫描。

7.1.4.6 安装安全

本项要求包括：
应包含可有效表征供应者或开发者身份的签名信息、软件属性信息。

7.1.4.7 升级安全

本项要求包括：
应支持软件更新机制，并且应通过安全机制保证升级的时效性和准确性。

7.1.4.8 卸载安全

本项要求包括：
应能删除安装和使用过程中产生的资源文件、配置文件和用户数据。

7.1.5 安全管理要求

7.1.5.1 机构管理

本项要求包括：

应设立安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位。

7.1.5.2 制度管理

本项要求包括：

应制定安全工作的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。

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) 外部人员离场后应清除其所有的访问权限。

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级别；

b) 应以书面形式说明企业确定为某网络安全级别的方法和理由。

7.1.5.4.2 安全方案设计

本项要求包括：

应根据安全防护对象的安全防护需求进行安全方案设计。

7.1.5.4.3 产品采购和使用

本项要求包括：

a) 网络关键设备及安全专用产品的采购和使用应符合国家有关规定；

b) 网络关键设备及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；

c) 密码产品与服务的采购和使用应符合国家密码管理主管部门的要求。

7.1.5.4.4 软件开发

本项要求包括：

a) 开发环境应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，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) 应在软件交付前进行缺陷和恶意代码等安全检测；

b) 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；

c) 应根据交付清单对所交接的设备、软件和文档等进行清点；

d) 应对负责运行维护的技术人员进行相应的技能培训。

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，其所提供的设备、平台系统等应为其所承载

的业务提供相应的安全防护能力；

b） 应在服务协议中规定具体服务内容和技术指标；

c） 应在服务协议中规定供应商的权限与责任，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；

d） 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；

e） 应与选定的供应商签订相关协议，明确供应链各方需履行的安全相关义务。

7.1.5.5 运维管理

7.1.5.5.1 环境管理

本项要求包括：

应对机房的安全管理作出规定，指定专门的部门或人员负责机房安全，对机房出入进行管理，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） 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b） 信息和资产均应指定部门和人员承担责任。

7.1.5.5.3 密码管理

本项要求包括：

a） 应根据 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；

b） 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。

7.1.5.5.4 配置管理

本项要求包括：

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） 应建立网络安全事件监测手段；

b） 应制定安全事件报告和处置管理制度，明确安全事件的报告和处置流程；

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

d） 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；

e） 在发生网络安全事件时，应立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。

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） 机房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。

7.1.6.2 物理访问控制

本项要求包括：
机房场地出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

7.1.6.3 防盗窃和防破坏

本项要求包括：
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。

7.1.6.4 防雷击

本项要求包括：
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

本项要求包括：
机房场地应设置灭火设备。

7.1.6.6 防水和防潮

本项要求包括：
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 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。

7.1.6.8 温湿度控制

本项要求包括：
应设置温湿度自动调节设施，使机房场地的温湿度的变化处于设备运行所允许的范围之内。

7.1.6.9 电力供应

本项要求包括：
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 接入层安全防护要求

7.2.1.1 接入设备安全防护要求

7.2.1.1.1 设备硬件安全

除满足 7.1.1.1.1 之外，还符合以下要求：
设备应具备独立的安全运行区域，用于密钥的全生命周期管理（包括密钥生成、存储、使用等），禁止

与非安全运行区域共享存储空间，以防止被篡改或非法获取。

7.2.1.1.2 设备系统安全

除满足 7.1.1.1.2 之外，还符合以下要求：

a) 应能针对重要用户行为和安全事件生成审计记录，内容包括日期和时间、事件主体和客体、操作类型、操作结果等信息；
b) 应支持日志导出备份功能；
c) 不应在系统或应用日志中记录用户口令等敏感信息，如确需记录，应使用脱敏或加密等措施。

7.2.1.1.3 设备接入安全

同 7.1.1.1.3。

7.2.1.2 接入层网络安全防护要求

7.2.1.2.1 安全通信

除满足 7.1.1.2.1 之外，还符合以下要求：

a) 应使用安全的通信协议，保证远程通信过程中数据传输安全；
b) 应按照设备通信服务级别的高低次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护高级别服务通信。

7.2.1.2.2 访问控制

除满足 7.1.1.2.2 之外，还符合以下要求：

a) 应遵循访问控制规则最小化原则，删除多余或无效的访问控制规则，优化访问控制列表；
b) 应具备检测访问异常行为的能力，并支持拦截或告警功能；
c) 应能够对非授权的接入设备非法连到工业互联网平台的行为进行检查或限制。

7.2.1.2.3 安全审计

本项要求包括：

a) 应对接入层网络日志进行安全审计，内容包括事件日期和时间、事件主体和客体、事件类型及其他与审计相关的信息；
b) 审计记录的时间应由系统范围内唯一确定的时钟产生，以确保时间的准确性。

7.2.2 基础设施层安全防护要求

7.2.2.1 计算环境安全防护要求

7.2.2.1.1 身份鉴别

除满足 7.1.2.1.1 之外，还符合以下要求：

当对计算环境进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取。

7.2.2.1.2 访问控制

除满足 7.1.2.1.2 之外，还符合以下要求：

a) 应由授权主体配置访问控制策略；
b) 应采用技术措施对允许远程访问的终端地址范围进行限制。

7.2.2.1.3 安全审计

除满足 7.1.2.1.3 之外，还符合以下要求：

应对日志记录进行安全审计，内容包括事件日期和时间、事件类型、事件主体和客体标识及结果等。

7.2.2.1.4 资源控制

除满足 7.1.2.1.4 之外，还符合以下要求：

a) 应具有登录计算环境的操作超时锁定或自动退出功能；

b) 应对计算环境中的资源进行监测，包括 CPU、硬盘、内存、网络等资源使用情况，发现异常及时提供告警。

7.2.2.1.5 恶意代码防范

除满足 7.1.2.1.5 之外，还符合以下要求：

当检测到恶意代码植入时，应对其进行有效阻断或隔离。

7.2.2.1.6 入侵防范

除满足 7.1.2.1.6 之外，还符合以下要求：

a) 应支持检测网络入侵行为，记录入侵的源 IP、攻击类型、攻击时间等，并在发生严重入侵事件时提供报警；

b) 应对计算环境中的安全漏洞、配置隐患等定期进行检测，保证计算环境不存在已公布的漏洞，或具备补救措施防范漏洞安全风险。

7.2.2.1.7 可信验证

本项要求包括：

应基于信任根，对系统引导程序、操作系统、应用程序等进行可信验证。

7.2.2.2 网络安全防护要求

7.2.2.2.1 架构安全

除满足 7.1.2.2.1 之外，还符合以下要求：

a) 应保证网络关键设备的业务处理能力具备冗余空间，满足业务高峰期需要；

b) 应保证网络各个部分的带宽满足业务高峰期需要；

c) 应对安全区域进行划分，根据平台服务的类型、功能及租户的不同划分不同的子网、网段或安全组；

d) 应按照用户服务级别的高低次序来指定带宽分配优先级别，保证在网络发生拥堵时优先保护高级别用户的服务通信。

7.2.2.2.2 访问控制

除满足 7.1.2.2.2 之外，还符合以下要求：

a) 应定期审查访问控制规则的有效性，删除多余或无效的访问控制规则，优化访问控制列表；

b) 不应从互联网直接访问内部系统或管理后台，如确需远程管理，应使用安全的专用通信隧道。

7.2.2.2.3 安全审计

除满足 7.1.2.2.3 之外，还符合以下要求：

a） 审计记录内容应包括事件的日期和时间、事件主体和客体、事件类型、事件结果及其他与审计相关的信息；
b） 应保证所有网络设备的系统时间由唯一确定的时钟产生，以保证时间一致性。

7.2.2.2.4 恶意代码防范

本项要求包括：
a） 应在关键网络节点处对恶意代码进行检测和清除；
b） 应周期性地维护恶意代码库的升级和检测系统的更新。

7.2.2.2.5 入侵防范

除满足 7.1.2.2.4 之外，还符合以下要求：
当检测到暴力破解、漏洞利用、拒绝服务等攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间等，并及时进行报警和阻断。

7.2.2.3 网络设备安全防护要求

7.2.2.3.1 身份鉴别

除满足 7.1.2.3.1 之外，还符合以下要求：
当对网络设备进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取。

7.2.2.3.2 访问控制

除满足 7.1.2.3.2 之外，还符合以下要求：
a） 应由授权主体配置访问控制策略；
b） 应采用技术措施对允许远程访问的终端地址范围进行限制。

7.2.2.3.3 安全审计

本项要求包括：
a） 应对网络设备的运行和操作日志进行定期审计，范围应覆盖到每个用户；
b） 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。

7.2.2.3.4 资源控制

除满足 7.1.2.3.3 之外，还符合以下要求：
a） 应具有登录网络设备的操作超时锁定或自动退出功能；
b） 应对网络设备的资源进行监测，包括 CPU、硬盘、内存、网络等资源使用情况，发现异常及时提供告警。

7.2.2.3.5 安全策略

本项要求包括：
a） 应根据网络设备的防护功能和防护需求，配置安全策略，并实现安全策略最小化；
b） 应定期审查安全策略的有效性，确保及时删除过期策略；
c） 应定期对安全策略进行备份，并具备恢复能力。

7.2.2.3.6 可信验证

本项要求包括：

应基于信任根，实现对网络设备的系统引导程序、操作系统、应用程序等进行可信验证。

7.2.2.4 虚拟化安全防护要求

7.2.2.4.1 虚拟机安全

除满足 7.1.2.4.1 之外，还符合以下要求：

a) 应通过技术手段保证虚拟机镜像文件和操作系统的完整性，确保不被篡改；
b) 应采取密码技术或其他技术手段防止虚拟机镜像中敏感资源被非法访问；
c) 应保证不同虚拟机之间的内存隔离，内存被释放或分配给其他虚拟机前得到完全释放；
d) 应定期对虚拟机操作系统进行漏洞扫描，并通过补丁升级的方式进行修复，保证虚拟机不存在已公布的漏洞；
e) 应支持虚拟机系统的备份和还原。

7.2.2.4.2 虚拟网络安全

除满足 7.1.2.4.2 之外，还符合以下要求：

a) 应支持在虚拟网络节点检测网络攻击行为，记录攻击类型、攻击时间、攻击流量等，并及时进行报警和阻断；
b) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的通信异常行为，发现异常流量情况时进行告警；
c) 应支持使用虚拟化专用的网络安全设备，如虚拟防火墙、虚拟加密设备等，以提高虚拟网络的安全性；
d) 应对虚拟机网络出口带宽进行限制。

7.2.2.4.3 虚拟化平台安全

除满足 7.1.2.4.3 之外，还符合以下要求：

a) 应对管理员运维管理时的操作行为和执行的命令进行审计，至少包括虚拟机删除、虚拟机重启等；
b) 平台应支持虚拟机热迁移能力，避免因宿主机故障导致虚拟机不可用，保证虚拟机的高可用性；
c) 平台应具备高可用性，避免因网络阻塞、硬件故障、数据丢失等导致服务不可用等情况发生；
d) 平台应支持对虚拟机的运行状态、资源占用等信息进行监控；
e) 虚拟化平台的管理命令应采用加密协议进行传输。

7.2.3 平台层安全防护要求

7.2.3.1 通用组件安全防护要求

7.2.3.1.1 身份鉴别

除满足 7.1.3.1.1 之外，还符合以下要求：

应采用安全方式防止因用户鉴别认证信息泄露而造成身份冒用。

7.2.3.1.2 访问控制

同 7.1.3.1.2。

7.2.3.1.3 安全审计

本项要求包括：

a） 审计范围应覆盖到使用组件的每个用户；

b） 审计内容应包括重要用户行为、组件资源的异常使用和重要操作命令的使用等事件；

c） 审计记录应包括事件的日期和时间、事件类型、事件主体标识、事件客体标识和结果等；

d） 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

e） 应支持按用户需求提供与其相关的审计信息及审计分析报告。

7.2.3.1.4 过载保护

本项要求包括：

应通过技术手段对组件进行过载保护，如通过流量控制、改进缓存模式、服务自动扩容、服务调用者降级服务等方式，防止服务雪崩。

7.2.3.2 通用接口安全防护要求

7.2.3.2.1 身份鉴别

除满足 7.1.3.2.1 之外，还符合以下要求：

a） 应对通用接口的调用设置安全的身份鉴别方式，如 OAuth2.0 等；

b） 通过口令进行认证时，口令应具有复杂度要求，禁止使用弱口令。

7.2.3.2.2 访问控制

除满足 7.1.3.2.2 之外，还符合以下要求：

应具备通用数据接口数据格式检查能力，对无法处理的数据提供统一处理机制。

7.2.3.2.3 网络通信安全

除满足 7.1.3.2.3 之外，还符合以下要求：

a） 应通过双向加密通信的方式保证传输数据的机密性和完整性；

b） 应根据通用接口调用需求和时间戳配置超时机制；

c） 应支持通过流量分析通用接口调用情况，发现接口异常使用、网络攻击等安全事件并进行报警。

7.2.3.3 容器安全防护要求

7.2.3.3.1 构建安全

除满足 7.1.3.3.1 之外，还符合以下要求：

a） 若使用第三方容器镜像，应保证来源可靠性，并对镜像文件进行安全性测试；

b） 不应将任何硬编码密钥嵌入容器，应通过统一的方式对密钥进行管理；

c） 容器的文件系统和挂载卷应根据需求配置最小的读写权限。

7.2.3.3.2 分发安全

除满足 7.1.3.3.2 之外，还符合以下要求：

a） 应通过镜像签名保证镜像的完整性和一致性；

b） 应支持容器的统一编排管理，并由授权管理员进行管理；

c) 镜像文件上传或下载过程应通过加密方式传输；
d) 应禁止私有镜像仓库直接暴露于互联网。

7.2.3.3.3 运行安全

除满足 7.1.3.3.3 之外，还符合以下要求：
a) 应支持对容器资源使用情况进行监测，发现资源使用异常应进行告警；
b) 应支持对容器进行安全入侵检测，发现入侵后及时报警和阻断；
c) 应确保容器之间、容器与宿主机之间实现隔离，并加强容器的安全管理和漏洞修复，防止容器逃逸造成宿主机被控制；
d) 应定期检查容器运行，对于停用或不必要的容器及时删除；
e) 容器运行应开启守护进程，并且守护进程应具有实时恢复能力。

7.2.3.3.4 维护安全

除满足 7.1.3.3.4 之外，还符合以下要求：
a) 应具有容器镜像备份与恢复能力；
b) 应支持对容器进行安全审计，内容包括不限于运行相关的文件和目录、守护进程、运维的重要操作指令等。

7.2.4 应用层安全防护要求

7.2.4.1 身份鉴别

除满足 7.1.4.1 之外，还符合以下要求：
a) 应支持口令强度检查机制，口令应具有复杂度要求并定期更换；
b) 应通过技术手段保证鉴别信息不以明文形式显示和存储；
c) 修改或找回鉴别信息时，应具备验证机制，如短信验证、邮箱验证等。

7.2.4.2 访问控制

除满足 7.1.4.2 之外，还符合以下要求：
a) 应根据业务需求禁止用户账号的多重并发会话；
b) 应严格限制应用与应用之间调用的权限，按照最小权限原则配置调用权限，并通过安全策略进行控制。

7.2.4.3 安全审计

本项要求包括：
a) 审计范围应覆盖到用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；
b) 审计记录应包括事件的日期和时间、事件类型、事件主体标识、事件客体标识和结果等；
c) 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；
d) 应定期针对审计日志进行人工审计；
e) 应支持按用户需求提供与其相关的审计信息及审计分析报告。

7.2.4.4 运行安全

除满足 7.1.4.3 之外，还符合以下要求：
a) 应具备安全机制防止程序被反编译、反调试；

b） 应确保应用不存在已公布的漏洞，或具备补救措施防范漏洞安全风险。

7.2.4.5 资源控制

除满足 7.1.4.4 之外，还符合以下要求：

a） 应提供资源控制不当的告警及响应；

b） 应对人机接口输入的数据进行有效性检验；

c） 应在会话处于非活跃一段时间或会话结束后终止会话连接。

7.2.4.6 上线前检测

除满足 7.1.4.5 之外，还符合以下要求：

a） 应对应用程序中使用的开源或第三方组件代码进行漏洞检测；

b） 应对已发现的漏洞进行补丁更新或升级。

7.2.4.7 安装安全

除满足 7.1.4.6 之外，还符合以下要求：

a） 安装时应提示用户对其使用的终端资源和终端数据进行确认；

b） 应对操作系统和其他应用软件的正常运行无影响。

7.2.4.8 升级安全

除满足 7.1.4.7 之外，还符合以下要求：

应支持安全机制对升级包的完整性进行校验。

7.2.4.9 卸载安全

除满足 7.1.4.8 之外，还符合以下要求：

a） 删除用户使用过程中生成的数据时应具有提示；

b） 应对工业互联网平台系统和其他应用软件的功能无影响。

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） 应设立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，实施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） 应设立安全主管、安全管理各个方面的负责人岗位，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；

c） 应加强相关部门之间、不同安全管理岗位人员之间的协作沟通，定期召开协调会议；

d） 应根据各职能部门和相关岗位的职责，明确对应的授权审批事项、审批部门和批准人等；

e） 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；

f） 应定期进行常规安全检查，检查内容包括系统日常运行情况、系统补丁更新情况和数据备份时间及备份存储情况等；

g） 应加强与各类供应商、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、合作内容、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) 应制定安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框架等；
b) 应依据工业互联网平台企业业务功能与监管单位要求，以及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、安全建设和安全运维、物理环境等层面的管理内容；
c) 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及时进行修订；
d) 应指定或授权专人负责安全管理制度的制定和修订，并通过正式流程进行发布和版本控制。

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) 应对被录用人员的身份、背景、专业资格和资质等进行审查；
b) 应定期评估员工及其权限适用情况，及时调整员工访问权限；
c) 应及时终止离岗员工的所有访问权限，并按照规范流程取回各种身份证件、钥匙、徽章等以及企业提供的软硬件设备；
d) 应定期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；
e) 当在外部人员物理访问受控区域或接入受控网络系统时，应提前提出书面申请，批准后由专人全程陪同或由专人开设账户及分配权限和期限，并登记备案。

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：

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) 应要求开发单位提供软件设计文档和使用指南；
b) 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。

7.2.5.4.5 系统交付

除满足 7.1.5.4.5 之外，还符合以下要求：

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。

7.2.5.4.6 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；
b) 应确保供应链安全事件信息或威胁信息能够及时传达到客户；
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：

禁止在重要区域接待来访人员。

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) 信息和资产均应指定部门和人员承担责任，资产责任人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；
b) 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；
c) 应对各种设备(包括备份和冗余设备)、线路等定期进行维护管理；
d) 应记录工业互联网平台相关设备的状态(包括外观、电量、指示灯等信息)，对设备进行现场维护(除尘、充电、修理等)；
e) 应对工业互联网平台相关设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
f) 应明确资产变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

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日期和时间、用户、事件类型、事件是否成功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，避免未预期的删除、修改或覆盖等；
c) 不应在审计记录中明文记录敏感数据，如用户口令等。

7.2.5.5.5 配置管理

同 7.1.5.5.4。

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) 应及时向有关主管部门报告监测发现的安全弱点和可疑事件；
b) 应根据实际情况适时对网络安全事件应急预案进行评估和修订；
c) 应定期开展网络安全事件应急预案宣贯培训，确保相关人员熟悉应急预案，并进行应急预案的演练。

7.2.6 物理环境安全要求

7.2.6.1 物理位置选择

同 7.1.6.1。

7.2.6.2 物理访问控制

同 7.1.6.2。

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，可铺设在地下或管道中；
b) 主机房或重要设备区域应设置专人值守的视频监控系统；
c) 主机房或重要设备区域应安装必要的防盗报警设施。

7.2.6.4 防雷击

同 7.1.6.4。

7.2.6.5 防火

除满足 7.1.6.5 之外，还符合以下要求：
机房场地应设置火灾自动报警系统，能够自动检测火情、自动报警，并自动灭火。

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

同 7.1.6.7。

7.2.6.8 温湿度控制

同 7.1.6.8。

7.2.6.9 电力供应

除满足 7.1.6.9 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隔离铺设，避免互相干扰。

7.3 增强级防护要求

7.3.1 接入层安全防护要求

7.3.1.1 接入设备安全防护要求

7.3.1.1.1 设备硬件安全

除满足 7.2.1.1.1 之外，还符合以下要求：

应对芯片存储功能设置读写保护，防止对芯片中的程序或数据进行非授权读写。

7.3.1.1.2 设备系统安全

除满足 7.2.1.1.2 之外，还符合以下要求：

应基于信任根，实现对系统引导程序、操作系统、应用程序等进行可信验证。

7.3.1.1.3 设备接入安全

除满足 7.2.1.1.3 之外，还符合以下要求：

a) 接入设备与工业互联网平台及其他应用建立通信时，应使用双向身份鉴别的方式，防止未授权的访问；

b) 关键接入设备应提供符合法律、法规和密码相关国家标准、行业标准要求的密码算法。

7.3.1.2 接入层网络安全防护要求

7.3.1.2.1 安全通信

同 7.2.1.2.1。

7.3.1.2.2 访问控制

除满足 7.2.1.2.2 之外，还符合以下要求：

应采用白名单控制方式，只允许合法设备接入网络。

7.3.1.2.3 安全审计

同 7.2.1.2.3。

7.3.2 基础设施层安全防护要求

7.3.2.1 计算环境安全防护要求

7.3.2.1.1 身份鉴别

除满足 7.2.2.1.1 之外，还符合以下要求：

应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证一种身份鉴别机制不易伪造。

7.3.2.1.2 访问控制

除满足 7.2.2.1.2 之外，还符合以下要求：

应实现主体是用户级或进程级、客体是文件或数据库表级的访问控制粒度。

7.3.2.1.3 安全审计

除满足 7.2.2.1.3 之外，还符合以下要求：

a） 应能够根据审计记录数据进行分析，并生成审计报表；

b） 应对审计进程进行保护，防止未经授权的中断。

7.3.2.1.4 资源控制

同 7.2.2.1.4。

7.3.2.1.5 恶意代码防范

除满足 7.2.2.1.5 之外，还符合以下要求：

应对防范恶意代码机制进行统一管理，如统一升级和更新等。

7.3.2.1.6 入侵防范

除满足 7.2.2.1.6 之外，还符合以下要求：

应支持基于白名单机制检测运行的进程或程序。

7.3.2.1.7 可信验证

除满足 7.2.2.1.7 之外，还符合以下要求：

可信验证应形成审计记录并进行集中管控，在检测到其可信性受到破坏后进行报警。

7.3.2.2 网络安全防护要求

7.3.2.2.1 架构安全

同 7.2.2.2.1。

7.3.2.2.2 访问控制

同 7.2.2.2.2。

7.3.2.2.3 安全审计

除满足 7.2.2.2.3 之外，还符合以下要求：

应能够根据审计记录数据进行分析，发现异常时及时告警，并生成审计报表。

7.3.2.2.4 恶意代码防范

同 7.2.2.2.4。

7.3.2.2.5 入侵防范

除满足 7.2.2.2.5 之外，还符合以下要求：

a） 应具备分析攻击行为，确定攻击目标范围，协助回溯攻击源头的能力；

b） 应采取技术措施对新型网络攻击行为进行分析，并对攻击行为进行阻断和报警。

7.3.2.2.6 集中管控

本项要求包括：

a) 应划分出特定的网络管理区域，对分布在网络中的安全设备或安全组件进行管控；
b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析；
e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

7.3.2.3 网络设备安全防护要求

7.3.2.3.1 身份鉴别

同 7.2.2.3.1。

7.3.2.3.2 访问控制

同 7.2.2.3.2。

7.3.2.3.3 安全审计

同 7.2.2.3.3。

7.3.2.3.4 资源控制

同 7.2.2.3.4。

7.3.2.3.5 安全策略

同 7.2.2.3.5。

7.3.2.3.6 可信验证

除满足 7.2.2.3.6 之外，还符合以下要求：

应基于可信根对网络设备的系统引导程序、系统程序、重要配置参数等进行可信验证，形成审计记录并进行集中管控，在检测到其可信性受到破坏后进行报警。

7.3.2.4 虚拟化安全防护要求

7.3.2.4.1 虚拟机安全

同 7.2.2.4.1。

7.3.2.4.2 虚拟网络安全

同 7.2.2.4.2。

7.3.2.4.3 虚拟化平台安全

除满足 7.2.2.4.3 之外，还符合以下要求：

a) 平台应由授权管理员进行管理，管理员访问应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证一种身份鉴别机制不易伪造；
b) 应保证不同虚拟机之间的虚拟 CPU 指令隔离；
c) 平台应支持技术手段保证虚拟机迁移过程中数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；
d) 平台应支持对 PKI、SSL 认证等各类数字证书的统一管理，支持用户按需更换。

7.3.3 平台层安全防护要求

7.3.3.1 通用组件安全防护要求

同 7.2.3.1。

7.3.3.2 通用接口安全防护要求

7.3.3.2.1 身份鉴别

同 7.2.3.2.1。

7.3.3.2.2 访问控制

同 7.2.3.2.2。

7.3.3.2.3 网络通信安全

除满足 7.2.3.2.3 之外，还符合以下要求：

a） 应对接口调用流量进行监测，当发现调用次数异常或超出调用权限及时进行报警；

b） 应使用数字证书等方式保证接口数据传输时的机密性和完整性；

c） 应支持通用接口调用链路分析能力，以便分析通用接口调用关系；

d） 通用接口调用关系应开展模式测试，以识别未知漏洞。

7.3.3.3 容器安全防护要求

7.3.3.3.1 构建安全

除满足 7.2.3.3.1 之外，还符合以下要求：

应支持基于黑名单或白名单策略的镜像管理能力。

7.3.3.3.2 分发安全

除满足 7.2.3.3.2 之外，还符合以下要求：

a） 应具备镜像签名校验能力，防止未签名或签名校验失败的镜像部署或上线；

b） 应具备镜像签名密钥管理能力，支持针对不同的镜像使用不同的密钥。

7.3.3.3.3 运行安全

除满足 7.2.3.3.3 之外，还符合以下要求：

应具备容器间流量可视化能力。

7.3.3.3.4 维护安全

同 7.2.3.3.4。

7.3.4 应用层安全防护要求

7.3.4.1 身份鉴别

除满足 7.2.4.1 之外，还符合以下要求：

a） 应支持通过两种或两种以上组合的鉴别机制进行身份鉴别；

b） 应在访问敏感数据、关键业务或系统配置前，对用户身份进行二次鉴别；

c） 应支持用户输入鉴别信息的键盘防劫持机制。

7.3.4.2 访问控制

同 7.2.4.2。

7.3.4.3 安全审计

除满足 7.2.4.3 之外，还符合以下要求：

a） 应具备自动化审计功能，对审计记录数据进行统计、查询、分析及生成审计报表；

b） 应能汇聚服务范围内的审计数据，支持第三方审计。

7.3.4.4 运行安全

同 7.2.4.4。

7.3.4.5 资源控制

同 7.2.4.5。

7.3.4.6 上线前检测

除满足 7.2.4.6 之外，还符合以下要求：

应用程序在上线前或升级后应进行代码审计，形成审计报告，并对审计出的问题进行代码升级完善。

7.3.4.7 安装安全

同 7.2.4.7。

7.3.4.8 升级安全

同 7.2.4.8。

7.3.4.9 卸载安全

同 7.2.4.9。

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委任或授权；

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；

c） 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；

d） 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

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) 应建立针对工业互联网平台的安全监测和应急响应制度，健全监测、处置、应急、备份等流程规范性文件；
b) 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。

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) 应对被录用人员的技术技能进行考核，与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
b) 人员离岗时，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) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，应定期对不同岗位的人员进行技能考核；
d) 获得系统访问授权的外部人员应签署保密协议，不应进行非授权操作，不应复制和泄露任何敏感信息；
e) 关键区域或关键系统不准许外部人员访问。

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：

a) 应定期评审和审核供应商提供的服务，并对其变更内容加以控制；

b) 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。

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) 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等；

b) 应加强对工业互联网设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

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作出规定，并对信息的使用、传输和存储等进行规范化管理；

c) 信息处理设备应经过审批后带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密处理；

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) 应建立中止资产变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

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进行行为审计和数据分析；

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） 对造成业务中断和造成信息泄漏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；
e） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。

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） 在机房选址及设计时，满足 GB 50174 的相关规定；
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境内。

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：
应对机房划分区域并在不同区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

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：
应对机房设置监控报警系统。

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：
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，对机房场地进行防水检测。

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：

应设置冗余或并行的电力电缆线路为工业互联网平台企业相关系统供电。

7.3.6.10 电磁防护

除满足 7.2.6.10 之外，还符合以下要求：

应对工业互联网平台关键设备实施电磁屏蔽。

附 录 A
（资料性）
工业互联网平台企业安全防护范围

图 A.1 给出了工业互联网平台企业安全防护范围示意图。

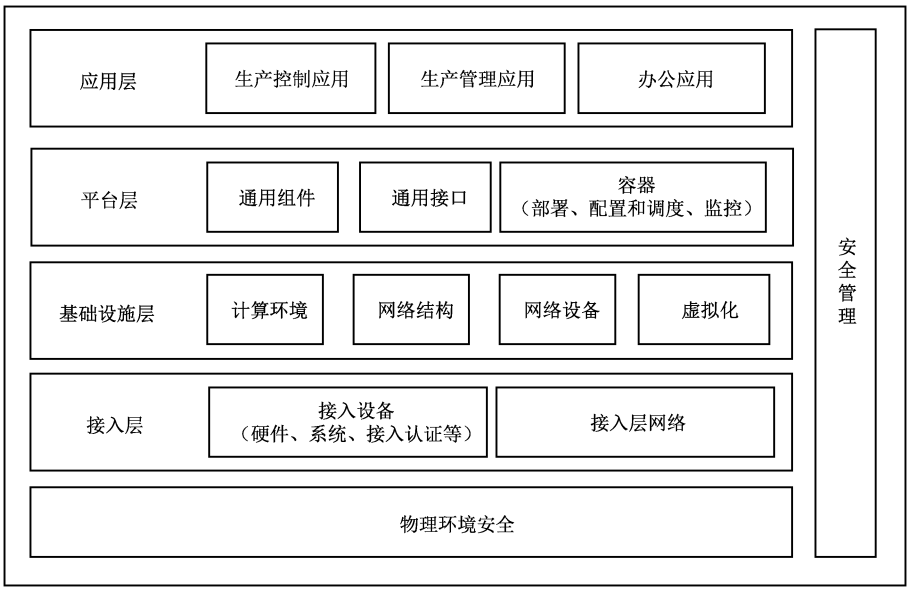

图 A.1 工业互联网平台企业安全防护范围

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] 工业互联网安全分类分级管理办法(工信部网安〔2024〕68号)