ICS 35.030
CCS L 70

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 455—2024

多功能智能杆　网络安全等级保护规范

Multifunctional smart pole—Specifications for network security level protection

2024-06-14 发布　　2024-07-01 实施

深圳市市场监督管理局　　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。

本文件由深圳市工业和信息化局提出并归口。

本文件起草单位：深圳市脉山龙信息技术股份有限公司、深圳市洲明科技股份有限公司、深圳市信息基础设施投资发展有限公司、北京天融信网络安全技术有限公司、金砖国家未来网络研究院(中国·深圳)、深圳大学、深圳市水务科技发展有限公司、深圳市博通智能技术有限公司、深圳市新一代信息技术行业协会、信软测评认证（深圳）集团有限公司。

本文件主要起草人：李海燕、陈铎航、王玉、林奕康、陈政浩、汪书福、林洺锋、陈晓宁、张帆、黄永衡、陈挺、许亚萍、江魁、曾庆彬、周灵军、马龙彪、王先峰、徐笔东、张超、宋建民、陈希、肖华、张勇、杨彪。

多功能智能杆　网络安全等级保护规范

1　范围

本文件规定了多功能智能杆的网络安全等级保护的基本要求、第一级安全要求、第二级安全要求、第三级安全要求和第四级安全要求。

本文件适用于多功能智能杆非涉密对象的网络安全等级的建设和运营管理。

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 20269—2006　信息安全技术　信息系统安全管理要求

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 28181　公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 37025—2018　信息安全技术　物联网数据传输安全技术要求

GB/T 37092　信息安全技术　密码模块安全要求

GB/T 37932—2019　信息安全技术　数据交易服务安全要求

GB/T 39477—2020　信息安全技术　政务信息共享　数据安全技术要求

GB/T 39786—2021　信息安全技术　信息系统密码应用基本要求

GA/T 1049.3—2013　公安交通集成指挥平台通信协议　第3部分：交通视频监视系统

GA/T 1400.4—2017　公安视频图像信息应用系统　第4部分：接口协议要求

DB4403/T 271—2022　公共数据安全要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

多功能智能杆　multifunctional smart pole

通过挂载各类设备提供智能照明、移动通信、城市监测、交通管理、信息交互和城市公共服务等多种功能，并可通过管理平台进行远程监测、控制、管理、校时、发布信息的杆。

注：多功能智能杆又称智慧杆、智能杆。

[来源：DB4403/T 30—2019，3.1.1，有修改]

3.2

多功能智能杆系统网络　network of multifunctional smart pole system

集智能照明、视频采集、移动通信、交通管理、环境监测、气象监测、无线电监测、应急求助和信息交互等诸多功能于一体的复合型公共基础设施网络。

注：多功能智能杆系统网络由多个模块组成，包括杆体、基础地笼、横臂、设备仓和智能门锁等，这些模块能

够挂载并集成多种设备，如语音视频监控设备、无线基站、WiFi、户外多媒体屏幕、新能源汽车充电桩以及各种传感器等。这些设备能够持续产生或接收信息流，通过系统网络的连接和协调，实现各种智能化功能，是未来构建新型智慧城市全面感知网络的重要载体。

3.3

安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

[来源：GB/T 22239—2019，3.2]

3.4

管理平台 management platform

根据多功能智能杆应用场景和数据业务以及安全要求的不同，对各挂载设备业务进行汇聚和分配、远程集中管理、控制、运行监测、数据分析、查询和定位，实现统一管理和运维，保障设备安全运行的系统。

注：管理平台包括服务器、操作系统、网络、软件、应用和存储设备等。

3.5

平台服务商 platform service provider

多功能智能杆管理平台（3.4）的供应方。

3.6

平台服务客户 platform service customer

为使用管理平台（3.4）服务同平台服务商（3.5）建立业务关系的参与方。

3.7

宿主机 host machine

运行虚拟机监视器的物理服务器。

[来源：GB/T 22239—2019，3.8]

3.8

移动互联 mobile communication

采用无线通信技术将移动终端（3.9）接入有线网络的过程。

[来源：GB/T 22239—2019，3.9]

3.9

移动终端 mobile device

在移动业务中使用的终端设备。

注：包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

[来源：GB/T 22239—2019，3.10，有修改]

3.10

无线接入设备 wireless access device

采用无线通信技术将移动终端（3.9）接入有线网络的通信设备。

[来源：GB/T 22239—2019，3.11]

3.11

移动应用软件 mobile application

针对移动终端（3.9）开发的应用软件。

[来源：GB/T 22239—2019，3.13]

3.12

等级保护对象 target of classified protection

多功能智能杆网络安全等级保护工作直接作用的对象。

注：主要包括多功能智能杆、挂载设备、边缘控制器、信息系统、网络设施和数据资源。

3.13

外部网络 external network

多功能智能杆系统网络（3.2）中等级保护对象之外的网络。

3.14

公共数据 common data

公共管理和服务机构及处理大量个人信息的服务平台在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据。

[来源：DB4403/T 271—2022，3.1]

3.15

敏感数据 sensitive data

被不当处理或泄露将对个人、组织或社会造成严重危害的数据。

注：包括个人身份信息、健康信息、金融信息、交易记录、公司机密和国家机密等。

3.16

数据安全 data security

通过采取必要措施确保数据处于有效保护和合法利用的状态以及具备保障持续安全状态的能力。

[来源：DB4403/T 271—2022，3.2]

3.17

挂载设备 mounting equipment

挂载在多功能智能杆（3.1）上，对物体或环境进行信息采集和/或执行操作，或能联网进行通信的装置。

3.18

边缘控制器 edge controller

将挂载设备（3.17）所采集的数据进行汇总、适当处理或数据融合，并进行转发通信的装置。

3.19

密码模块 cryptographic module

能完成密码运算功能并提供调用接口，相对独立的软件或硬件装置。

4 缩略语

下列缩略语适用于本文件。

AP：无线访问接入点（Wireless Access Point）

BIOS：基本输入输出系统（Basic Input Output System）

COM：串行通讯端口（Cluster Communication Port）

CPU：中央处理器（Central Processing Unit）

DDoS：分布式拒绝服务（Distributed Denial of Service）

HTTPS：超文本安全传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）

IaaS: 基础设施即服务（Infrastructure as a Service）

IP：互联网协议（Internet Protocol）

IPv4：互联网协议第4版（Internet Protocol Version 4）

IPv6：互联网协议第6版（Internet Protocol Version 6）

PaaS：平台即服务（Platform as a Service）

RJ45：双绞线电缆连接的物理接口（Registered Jack-Type 45）

SaaS：软件即服务（Software as a Service）
SPI：串行外设接口（Serial Peripheral Interface）
SSH：安全外壳（Secure Shell）
SSID：服务集标识（Service Set Identifier）
TCB：可信计算基（Trusted Computing Base）
TCP：传输控制协议（Transmission Control Protocol）
TPCM：可信平台控制模块（Trusted Platform Control Module）
UDP：用户数据报协议（User Datagram Protocol）
VPN：虚拟专用网络（Virtual Private Network）
WEP：有线等效加密（Wired Equivalent Privacy）
WPS：WiFi保护设置（WiFi Protected Setup）

5 基本要求

5.1 等级保护对象定级

5.1.1 等级保护对象应根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为四个安全保护等级。

5.1.2 四个安全保护等级应按下列要求进行划分：

a) 第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益；
b) 第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；
c) 第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害；
d) 第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害。

5.2 不同等级的安全保护能力

5.2.1 第一级安全保护能力：应能够防护来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。

5.2.2 第二级安全保护能力：应能够防护来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

5.2.3 第三级安全保护能力：应能够在统一安全策略下防护来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。

5.2.4 第四级安全保护能力：应能够在统一安全策略下防护来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。

5.3 安全通用要求

5.3.1 由于多功能智能杆实现业务目标的不同、使用技术的不同、应用场景的不同等多种因素，不同的等级保护对象应包括基础信息网络、信息系统（包含采用移动互联等技术的系统）、管理平台、大数据系统等。

5.3.2 安全通用要求应针对共性化保护需求提出，分为技术要求和管理要求；技术要求应包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等；管理要求应包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理和风险控制等，并应符合GB/T 20269—2006 中 4.1、4.2、5.1、5.2 和 5.3 的要求。

5.3.3 安全通用要求的选择和使用应符合附录 A 的规定，等级保护对象整体安全保护能力的要求应符合附录 B 的规定，等级保护安全框架和关键技术使用要求应符合附录 C 的规定。

5.4 安全扩展要求

5.4.1 安全物理环境

多功能智能杆系统网络的安全物理环境应符合 GB/T 22239—2019 中 6.1.1 的要求。

5.4.2 管理平台应用场景要求

管理平台应用场景要求应符合附录 D 的规定。

5.4.3 移动互联应用场景要求

移动互联应用场景要求应符合附录 E 的规定。

5.4.4 挂载设备应用场景要求

挂载设备应用场景要求应符合附录 F 的规定。

5.4.5 公共数据安全要求

5.4.5.1 承载公共数据的信息系统应符合 DB4403/T 271—2022 中第 7 章和第 8 章的要求，并对信息系统组织开展定级备案、等级测评、安全整改工作；数据处理过程涉及的密码技术应符合 GB/T 39786—2021 中第 5 章的要求。

5.4.5.2 公共数据安全的处理应包括数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境、数据销毁和数据删除等过程。

5.4.5.3 公共数据安全等级与安全要求的关系应符合表 1 的规定。

表 1 公共数据安全等级与安全要求关系

安全等级	安全要求
第一级	基本安全要求
第二级	基本安全要求
第三级	基本安全要求、三级增强安全要求
第四级	基本安全要求、四级增强安全要求

5.5 密码模块安全要求

5.5.1 密码模块安全等级应分为四个等级，分别为安全一级、安全二级、安全三级和安全四级，其

中安全四级要求最高。

5.5.2 不同等级的密码模块对应不同的安全需求和防护能力，应根据应用系统的安全需求和防护能力选择密码模块安全等级。

5.5.3 密码模块的设计、开发和检测应符合 GB/T 37092 的要求。

5.5.4 密码模块安全要求应符合附录 G 的规定。

6 第一级安全要求

6.1 安全通用要求

6.1.1 安全通信网络

6.1.1.1 网络架构

网络架构要求如下：

a) 网络设备（包括边缘控制器）的业务处理能力应满足业务高峰期需要；
b) 网络各个部分的带宽应满足业务高峰期需要；
c) 应配备与实际运行情况相符的网络拓扑架构。

6.1.1.2 通信传输

应采用校验技术使通信传输过程中的数据保持完整性。

6.1.1.3 可信验证

应基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。可信验证要求应符合附录 H 的规定。

6.1.2 安全区域边界

6.1.2.1 边界防护

跨越边界的访问和数据流应通过边界设备提供的受控接口进行通信。

6.1.2.2 访问控制

访问控制要求如下：

a) 应在网络边界根据访问控制策略设置访问控制规则，默认情况下受控接口拒绝所有通信；
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并使访问控制规则数量最小化；
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查。

6.1.3 安全计算环境

6.1.3.1 身份鉴别

身份鉴别要求如下：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b) 应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

6.1.3.2 访问控制

访问控制要求如下：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应根据不同等级要求定期（分为周、月、季、年）对账号进行检查；
d) 应及时删除或停用多余的、过期的账户。

6.1.3.3 入侵防范

入侵防范要求如下：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b) 应关闭不需要的系统服务、默认共享和高危端口。

6.1.3.4 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

6.1.3.5 可信验证

应基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，在检测到其可信性受到破坏后进行报警。可信验证要求应符合附录 H 的规定。

6.1.3.6 数据完整性

应采用校验技术使重要数据在传输过程中保持完整性，包括但不限于调度信息、鉴别数据、重要业务数据和重要个人信息。

6.1.3.7 数据备份恢复

应具备重要数据的本地数据备份与恢复功能，对于特别重要的数据，除本地备份外，应具备云端或远程异地备份功能。

6.2 管理平台安全要求

6.2.1 安全通信网络

安全通信网络要求如下：

a) 管理平台应承载高于其安全保护等级的业务应用系统；
b) 应实现不同管理平台服务客户虚拟网络之间的隔离。

6.2.2 安全区域边界

访问控制应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

6.2.3 安全计算环境

安全计算环境要求如下：

a) 当虚拟机迁移时，访问控制策略应随其迁移；
b) 应支持管理平台为服务客户设置不同虚拟机之间的访问控制策略；
c) 管理平台的服务客户数据、用户个人信息等应存储于中华人民共和国境内。

6.3 移动互联安全要求

6.3.1 安全区域边界

6.3.1.1 边界防护

有线网络与无线网络边界之间的访问和数据流应通过无线接入安全网关设备。

6.3.1.2 访问控制

无线接入设备应开启接入认证功能，不应使用 WEP 方式进行认证；当使用口令时，口令由数字和字母组成，口令长度不应小于 8 位字符。

6.3.2 安全计算环境

对移动终端设备的使用进行管控时，移动终端设备应具备选择软件安装、运行的功能。

6.4 挂载设备安全要求

6.4.1 安全物理环境

安全物理环境要求如下：

a) 挂载设备所处的物理环境不应对挂载设备造成挤压和强振动等的物理破坏；
b) 挂载设备所处的物理环境应能正确反映环境状态；
c) 气象传感器和温湿度传感器不应安装在阳光直射区域。

6.4.2 安全区域边界

授权的挂载设备应通过安全区域接口接入控制进行通信，采用的接口要求如下：

a) RJ45 或光纤以太网通信接口，单个接口通信速率不应低于 1000 Mbps；网络层应采用 IP 协议，并支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，当挂载设备为客户端，边缘控制器为服务端时，挂载设备应支持对多个服务端的传输数据；
b) COM 应支持 RS-232（DB9）或 RS-485；
c) 挂载设备为摄像机，当具备视频监控功能时，接口协议应符合 GB/T 28181 的要求；
d) 挂载设备为摄像机，当具备视频图像信息采集功能时，接口协议应符合 GA/T 1400.4—2017 中 5.2 的要求。

6.4.3 安全运维管理

挂载设备管理应指定人员定期巡视挂载设备、网关节点设备的周边环境，对可能影响挂载设备、边缘控制器正常工作的环境异常进行记录和维护。

6.5 公共数据基本安全要求

6.5.1 数据收集基本安全

数据收集基本安全要求如下：

a) 应对数据收集来源进行鉴别和记录，数据收集来源应合法、正当；
b) 应分析数据类型及收集渠道、目的、用途、范围、频度、方式等；
c) 收集外部机构数据前，应对外部机构数据源的合法性、合规性进行鉴别；
d) 个人信息收集应遵循合法、正当和诚信原则，并获得个人信息主体的明示同意，不应通过误导、欺诈、胁迫或其他违背个人信息主体真实意愿的方式获取其同意；
e) 开展个人信息收集工作应符合 GB/T 35273—2020 中第 5 章的要求；

f） 提供公共服务的移动互联网应用程序或第三方应用，应遵循最小化收集原则，在收集个人信息时，应用程序或第三方应用应告知个人信息主体收集的目的、使用方式及可能的风险，并取得个人信息主体的同意。

6.5.2 数据存储基本安全

数据存储基本安全要求如下：

a） 应制定数据存储相关安全管控措施，包括加密、访问控制、数字水印、完整性校验等；
b） 应制定数据备份与恢复安全策略，建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点；建立数据恢复性验证机制，保障数据的可用性与完整性；
c） 应具备异地数据备份功能；
d） 个人生物识别信息应与个人身份信息分开存储；
e） 不应存储原始个人生物识别信息（如样本、图像等），可存储个人生物识别信息的摘要信息；
f） 个人信息存储期限应为实现个人信息主体授权使用目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外；超出个人信息存储期限后，应对个人信息进行删除或匿名化处理。

6.5.3 数据传输基本安全

数据传输基本安全要求如下：

a） 应制定数据传输相关安全管控措施，包括传输通道加密、数据内容加密、数据接口传输安全等；
b） 应对数据传输两端进行身份鉴别，使数据传输双方可信任；
c） 应采用校验技术使数据在传输过程中保持完整性；
d） 当传输敏感个人信息时，应采取加密、脱敏等安全措施。

6.5.4 数据使用基本安全

数据使用基本安全要求如下：

a） 应制定数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等；
b） 应制定数据统计分析、展示、发布、公开披露等不同数据使用场景的安全管理要求；
c） 应根据不同数据使用场景采取安全处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险；
d） 当利用算法推荐技术进行自动化决策分析时，决策的过程应透明，结果应公平合理；
e） 数据公开前应开展数据安全风险评估，分析公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围等。当涉及敏感个人信息、商业秘密信息，以及可能对公共利益或国家安全产生重大影响时，数据不应公开；
f） 当公开市场预测、统计信息等数据资源时，不应危害国家安全、公共安全、经济安全和社会稳定。

6.5.5 数据加工基本安全

数据加工基本安全要求如下：

a） 应对参与数据加工活动的主体进行合法性、正当性的评估，参与数据加工活动的主体应为合法合规的组织机构或个人；

b) 应在数据加工前，书面明确数据加工目的、范围、期限、规则及数据加工主体的责任与义务；
c) 数据加工活动过程中，当发现可能危害国家安全、公共安全、经济安全和社会稳定时，应停止数据加工活动；
d) 委托他人进行数据加工时，应与其订立数据安全保护合同，明确双方安全保护责任；委托加工处理个人信息时，应约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督，不应超出已征得个人信息主体授权同意的范围。

6.5.6 数据开放共享基本安全

数据开放共享基本安全要求如下：
a) 公共数据提供部门应与公共数据使用部门签署相关协议，明确数据使用目的、共享范围、共享方式、保密约定和安全保护等内容；
b) 公共数据提供部门采用密码技术时，应符合 GB/T 39786—2021 的要求；
c) 政务数据共享应符合 GB/T 39477—2020 中第 6 章的要求。

6.5.7 数据交易基本安全

数据交易基本安全应符合 GB/T 37932—2019 中第 5 章、第 6 章和第 7 章的要求。

6.5.8 数据出境基本安全

数据出境基本安全要求如下：
a) 应分析数据出境不同的业务应用场景；
b) 应遵守国家法律和行政法规规定的数据出境安全监管要求；
c) 符合国家法律和行政法规规定情形的，应提前开展数据出境安全评估及网络安全审查工作，不应发生未授权的数据出境；
d) 中华人民共和国境内的用户访问互联网产生的流量不应被路由至境外；
e) 应建立出境数据的评估、审批及监管控制流程，依据流程实施相关控制并记录过程。

6.5.9 数据销毁与删除基本安全

数据销毁与删除基本安全要求如下：
a) 应制定数据销毁与删除规程，包括数据销毁与删除场景、方式及审批机制，设置相关监督角色，记录数据销毁与删除操作过程等；
b) 当业务终止或组织解散，无数据承接方时，应及时有效销毁其控制的数据；
c) 委托数据合作方完成数据处理后，应要求数据合作方及时销毁委托的相关数据；
d) 根据要求约定删除数据或完成数据处理后无需保留源数据的，应及时删除相关数据；
e) 个人信息删除应符合 GB/T 35273—2020 中 8.3 的要求。

7 第二级安全要求

7.1 安全通用要求

7.1.1 安全通信网络

7.1.1.1 网络架构

网络架构要求如下：

a） 关键网络设备的业务处理能力应满足业务高峰期需要；
b） 网络各个部分的带宽应满足业务高峰期需要；
c） 应根据系统功能、业务流程、网络结构层次、业务服务对象等因素划分不同网络区域，并按照方便安全管理和控制的原则为各网络区域分配地址；
d） 不应将视频采集装置、信息发布屏和公共广播装置等设备的重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的逻辑或物理技术隔离手段；
e） 应配备与实际运行情况相符的网络拓扑架构。

7.1.1.2 通信传输

应采用校验技术使通信传输过程中的数据保持完整性。

7.1.1.3 可信验证

应基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，将验证结果形成审计记录送至安全管理中心。可信验证要求应符合附录 H 的规定。

7.1.2 安全区域边界

7.1.2.1 边界防护

跨越边界的访问和数据流应通过边界设备提供的受控接口进行通信。

7.1.2.2 访问控制

访问控制要求如下：

a） 应在网络边界根据访问控制策略设置访问控制规则，默认情况下受控接口拒绝所有通信；
b） 应删除多余或无效的访问控制规则，优化访问控制列表，并使访问控制规则数量最小化；
c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

7.1.2.3 安全审计

安全审计要求如下：

a） 应在网络边界、重要网络节点进行安全审计，安全审计应覆盖到每个用户；
b） 应对重要的用户行为和重要安全事件进行安全审计；
c） 安全审计记录应包括事件的日期、时间、IP 地址、事件类型、事件是否成功及其他与审计相关的信息；
d） 应对视频采集装置、信息发布屏和公共广播装置的控制操作行为、远程访问用户行为、访问互联网用户行为等，单独进行行为审计和数据分析。

7.1.2.4 可信验证

应基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。可信验证要求应符合附录 H 的规定。

7.1.3 安全计算环境

7.1.3.1 身份鉴别

身份鉴别要求如下：

a) 应对登录的用户进行身份标识和鉴别；
b) 身份标识应具有唯一性；
c) 身份鉴别信息应具有复杂度并定期进行更换；
d) 应具备登录失败处理功能；
e) 当会话结束、非法登录和登录连接超时时，应建立自动退出机制；
f) 当进行远程管理时，应采取措施防止鉴别信息在网络传输过程中被窃听，包括 HTTPS、SSH 和 VPN 等。

7.1.3.2 访问控制

访问控制要求如下：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应阻断无法重命名或删除的默认账户远程登录；
d) 应及时删除或停用多余的、过期的账户；
e) 应授予管理用户所需的最小权限；
f) 应限制未登录用户的使用权限，对匿名用户使用记录进行追溯。

7.1.3.3 安全审计

安全审计要求如下：

a) 应启用安全审计功能，安全审计应覆盖到每个用户；
b) 应对重要的用户行为和重要安全事件进行安全审计；
c) 安全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；
d) 安全审计记录不应受到未批准的删除、修改或覆盖；
e) 应对安全审计记录进行保护和定期备份。

7.1.3.4 入侵防范

入侵防范要求如下：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b) 应关闭不需要的系统服务、默认共享和高危端口；
c) 应通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过测试评估后，及时修补漏洞；
d) 应通过设定终端接入方式或网络地址范围对终端进行限制；
e) 应具备数据有效性检验功能，使通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

7.1.3.5 恶意代码防范

应在关键网络节点处进行恶意代码的检测和清除，维护恶意代码防护机制的有效性，并定期进行升级和更新防恶意代码库。

7.1.3.6 可信验证

应基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。可信验证要求应符合附录H的规定。

7.1.3.7 数据完整性

应采用校验技术使重要数据在传输过程中保持完整性，包括但不限于调度信息、鉴别数据、重要业务数据和重要个人信息。

7.1.3.8 数据备份恢复

数据备份恢复要求如下：

a) 应制定详细的备份数据恢复计划，明确恢复流程和责任人；
b) 应具备重要数据的本地数据备份与恢复功能；
c) 应具备异地数据备份功能。

7.1.3.9 剩余信息保护

鉴别信息所在的存储空间被释放或重新分配前应得到完全清除。

7.1.3.10 个人信息保护

个人信息保护要求如下：

a) 应采集和保存业务必需的用户个人信息；
b) 不应发生未授权访问和非法使用用户个人信息。

7.1.3.11 业务连续性保障

业务连续性保障要求如下

a) 在各种过程风险评估的基础上应制定业务连续性计划；
b) 业务连续性计划应详细列出每一步的行动方案，包括预防措施、应急响应和恢复计划等。

7.1.3.12 系统管理

系统管理要求如下：

a) 应对系统管理员进行身份鉴别，系统管理员应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；
b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

7.1.3.13 审计管理

审计管理要求如下：

a) 应对审计管理员进行身份鉴别，审计管理员应通过特定的命令或操作界面进行安全审计操作；
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

7.2 管理平台安全要求

7.2.1 安全通信网络

安全通信网络要求如下：

a) 应使管理平台不承载高于其安全保护等级的业务应用系统；
b) 应实现不同管理平台服务客户虚拟网络之间的隔离；
c) 应具备根据管理平台服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。

7.2.2 安全区域边界

7.2.2.1 访问控制

访问控制要求如下：

a) 应在虚拟化网络边界设置访问控制机制；
b) 应在不同等级的网络边界设置访问控制机制。

7.2.2.2 入侵防范

入侵防范要求如下：

a) 应检测管理平台服务客户发起的网络攻击行为，并记录攻击类型、攻击时间、攻击流量等；
b) 应检测对虚拟网络节点的网络攻击行为，并记录攻击类型、攻击时间、攻击流量等；
c) 应检测虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。

7.2.2.3 安全审计

安全审计要求如下：

a) 应根据业务需求和安全风险制定安全审计规则和策略；
b) 应对管理平台服务商和管理平台服务客户在远程管理时执行的特权命令进行审计；
c) 应对管理平台服务商和管理平台服务客户的数据和操作进行审计。

7.2.3 安全计算环境

7.2.3.1 访问控制

访问控制要求如下：

a) 在使用用户名和口令的基础上，应使用动态令牌、生物识别和数字证书等技术进行身份验证，提高访问控制的安全性；
b) 应为每个应用或系统分配所需的最小权限，防止用户拥有不必要的过高权限；
c) 当虚拟机迁移时，访问控制策略应随其迁移；
d) 管理平台应为服务客户设置不同虚拟机之间的访问控制策略。

7.2.3.2 镜像和快照保护

镜像和快照保护要求如下：

a) 应对镜像和快照的创建、存储、传输和使用进行严格的管理和控制；
b) 应对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；
c) 应具备虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。

7.2.3.3 数据完整性和保密性

数据完整性和保密性要求如下：

a) 管理平台数据传输过程中的完整性应符合 GB/T 37025—2018 中 6.1 和 7.1 的要求；

b） 应通过封装签名、测试字验证、引用约束等机制，对数据的完整性进行检测；
c） 应对数据的完整性进行校验，防止数据在传输和存储过程中被篡改或损坏；
d） 应使用加密技术对数据进行加密传输和存储。

7.2.3.4 数据备份恢复

数据备份恢复要求如下：
a） 应具备重要数据的本地数据备份与恢复功能，数据备份包括完全数据备份和增量备份；
b） 应对备份信息的备份方式、备份频度、存储介质、保存期等进行规定；
c） 应支持备份程序与应用程序的分离；
d） 应支持对备份数据进行压缩存储。

7.2.3.5 剩余信息保护

剩余信息保护要求如下：
a） 当虚拟机在停止使用或释放时，其内存区域应进行完全清除；
b） 当虚拟机使用的存储空间在重新分配给其他用户或进行数据迁移前，其硬盘或存储设备应进行完全清除。

7.3 移动互联安全要求

7.3.1 安全区域边界

7.3.1.1 边界防护

边界防护要求如下：
a） 应将跨越有线网络与无线网络边界之间的访问和数据流，通过边界设备提供的受控接口进行通信；
b） 应检查或限制非授权设备私自联到内部网络的行为；
c） 应检查或限制内部用户非授权联到外部网络的行为；
d） 应实时监控网络的运行状态，当发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，及时对其进行有效阻断。

7.3.1.2 访问控制

访问控制要求如下：
a） 应在网络边界或区域之间根据访问控制策略设置访问控制规则；
b） 应开启无线接入设备的接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证，加密方式至少包含 SM2 或 SM4；
c） 不应使用 WEP 方式进行认证；当使用口令时，口令长度不应小于 8 位字符；
d） 应对进出网络的数据包进行详细的检查和控制，包括对源地址、目的地址、源端口、目的端口和协议等进行检查。

7.3.1.3 入侵防范

入侵防范要求如下：
a） 应检测非授权无线接入设备和非授权移动终端的接入行为：
b） 应检测对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
c） 应检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；

d) 不应多个 AP 使用同一个认证密钥；
e) 应能够阻断非授权无线接入设备或非授权移动终端。

7.3.2 安全计算环境

7.3.2.1 移动终端管控

移动终端管控要求如下：
a) 应使用终端管理客户端软件对移动终端进行安装、注册和管理；
b) 应接受终端管理客户端软件对移动终端设备的生命周期管理和设备远程控制（如远程锁定、远程擦除等）；
c) 应将移动终端的使用限定在处理指定的业务；
d) 应对移动终端存储的敏感信息采取加密措施，并在未授权情况下不可读；
e) 宜采用专用终端发布直播数据。

7.3.2.2 移动应用管控

移动应用管控要求如下：
a) 应具备选择应用软件安装、运行的功能；
b) 应依据指定证书签名的应用软件进行安装和运行；
c) 应根据软件白名单功能控制应用软件的安装和运行；
d) 应具备接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

7.4 挂载设备安全要求

7.4.1 安全物理环境

安全物理环境要求如下：
a) 应选择在不易受自然灾害和人为破坏的区域安装多功能智能杆；
b) 应对多功能智能杆及其挂载设备进行加固处理，防止被盗或被破坏；
c) 应对多功能智能杆及其挂载设备设置明显的警示标识；
d) 应对多功能智能杆和挂载设备安装防雷击装置。

7.4.2 安全区域边界

7.4.2.1 接入控制

接入控制要求如下：
a) 应设置安全区域边界的划分，并根据安全等级和安全需求进行合理配置；
b) 应采取技术措施对安全区域边界进行接入控制和管理，包括物理隔离、访问控制、监测和审计等；
c) 挂载设备接入控制采用的接口要求如下：
   1) RJ45 以太网通信接口，单个接口通信速率不应低于 1000 Mbps；网络层应采用 IP 协议，并支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，当挂载设备为客户端，边缘控制器为服务端时，挂载设备应支持对多个服务端传输数据；
   2) COM 应支持 RS-232（DB9）或 RS-485；
   3) 挂载设备为摄像机，当具有视频监控功能时，接口协议应符合 GB/T 28181 的要求；

4） 挂载设备为摄像机，当具有视频图像信息采集功能时，接口协议应符合 GA/T 1400.4—2017 中 5.2 的要求。

7.4.2.2 安全控制

7.4.2.2.1 挂载设备

挂载设备要求如下：

a） 应具备网络身份标识；
b） 应具有唯一网络身份标识，可以是 MAC 地址、IP 地址、ID、序列号等设备属性，也可以是以上设备属性经过算法生成的身份标识；
c） 应具备网络通讯接口协议，包括 Modbus 和 backnet 等，具备识别协议的端口号；
d） 应具备生成、存储身份标识的能力，包括密码机制、密钥、证书等；
e） 在接入网络时，密钥存储和交换应安全。

7.4.2.2.2 接入网络

接入网络要求如下：

a） 应支持网络身份标识、MAC 地址、IP 地址、ID、序列号、通信协议、通信端口、密码（对称、非对称）标识以及标识组合的认证鉴别能力；
b） 应支持感知层接入终端身份标识和接入口令的单向认证；
c） 应支持预共享密钥的单向和双向认证。

7.4.2.2.3 访问控制

访问控制要求如下：

a） 应支持通过 ACL 方式控制感知终端对通信网络的访问；
b） 应具备制定和执行访问控制策略的功能，访问控制策略可以是基于 IP 地址、用户、用户组、读/写等操作的一种或多种组合；
c） 应支持黑名单制度，并阻断相关感知终端对通信网络的访问；
d） 接入系统应支持分层分权分域的接入访问控制能力，包括根据不同认证方式分配给不同感知层接入实体的不同层次（设备、网络、业务等）访问能力，根据不同的访问用户和用户组，分配不同的访问权限；
e） 应支持接入系统根据感知终端的数据类型（如业务数据、协议数据、链路数据）进行禁止/放通的访问控制能力；
f） 当认证应答超过规定时限时，接入系统应终止接入系统和感知终端之间的会话；
g） 经过一定次数的认证失败后，接入系统应终止由感知终端发起的建立会话的尝试，并在一定时间间隔后才能继续接入。

7.4.2.3 入侵防范

入侵防范要求如下：

a） 应限制与挂载设备通信的目标地址，防止对陌生地址的攻击行为；
b） 应限制与边缘控制器通信的目标地址，防止对陌生地址的攻击行为；
c） 应定期更新系统和软件漏洞补丁，及时修复已知漏洞，降低被攻击的风险；
d） 应检测非授权无线接入设备和非授权移动终端的接入行为。

7.4.3 安全运维管理

安全运维管理要求如下：

a) 应指定人员定期巡视挂载设备和边缘控制器的安装环境，对影响挂载设备和边缘控制器正常工作的环境异常进行记录和处理；
b) 应对挂载设备、边缘控制器入库、存储、部署、携带、维修、丢失和报废等进行全过程管理；
c) 应对挂载设备边缘控制器的安装位置进行保密性管理。

7.5 公共数据基本安全要求

公共数据基本安全应符合 6.5 的要求。

8 第三级安全要求

8.1 安全通用要求

8.1.1 安全通信网络

8.1.1.1 网络架构

网络架构要求如下：

a) 网络设备的业务处理能力应满足业务高峰期需要；
b) 网络各个部分的带宽应满足业务高峰期需要；
c) 应根据系统功能、业务流程、网络结构层次、业务服务对象等因素划分不同网络区域，并按照方便安全管理和控制的原则为各网络区域分配地址；
d) 不应将视频采集装置、信息发布屏和公共广播装置等设备的重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的逻辑或物理技术隔离手段；
e) 应对通信线路、关键网络设备、关键安全设备(至少包括防火墙、加密模块、入侵检测和防护设备)和关键计算设备(至少包括边缘计算器)进行冗余配置；
f) 应具备不同路由的双链路接入保障能力；
g) 应配备与实际运行情况相符的网络拓扑架构。

8.1.1.2 通信传输

通信传输要求如下：

a) 应采用校验技术、密码技术或特定协议转换技术使通信传输过程中的数据保持完整性；
b) 应采用密码技术或特定协议转换技术使通信传输过程中的数据保持保密性。

8.1.1.3 可信验证

应基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。可信验证要求应符合附录 H 的规定。

8.1.2 安全区域边界

8.1.2.1 边界防护

边界防护要求如下：

a) 应使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；

b） 应对非授权设备私自联到内部网络的行为进行检查和限制；
c） 应对内部用户非授权联到外部网络的行为进行检查和限制；
d） 视频采集装置、信息发布屏和公共广播装置等不应通过无线方式进行组网，其他系统应限制无线网络的使用。

8.1.2.2 访问控制

访问控制要求如下：
a） 应在网络边界根据访问控制策略设置访问控制规则；
b） 应删除多余或无效的访问控制规则，优化访问控制列表，使访问控制规则数量最小化；
c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d） 应根据会话状态信息为进出数据流制定允许/拒绝访问的措施；
e） 通过外部网络对信息系统进行访问时，应使用安全方式接入，对用户和权限进行管理，赋予最小访问权限，控制粒度为用户级；
f） 应根据应用协议和应用内容对进出网络的数据流进行访问控制。

8.1.2.3 入侵防范

入侵防范要求如下：
a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
c） 应采取技术措施对新型网络攻击行为进行分析；
d） 当检测到网络攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间；在发生严重入侵事件时应及时启动报警。

8.1.2.4 恶意代码防范

恶意代码防范要求如下：
a） 应在关键网络节点处进行恶意代码的检测和清除，维护恶意代码防护机制的有效性，并定期升级和更新特征库；
b） 部署在关键网络节点的防恶意代码产品宜与系统内部防恶意代码产品具有不同的防恶意代码库。

8.1.2.5 安全审计

安全审计要求如下：
a） 应在网络边界、重要网络节点进行安全审计，安全审计应覆盖到每个用户；
b） 应对安全审计记录进行保护和定期备份；
c） 安全审计记录应包括事件的日期、时间、IP 地址、事件类型、事件是否成功及其他与审计相关的信息；
d） 应对视频采集装置、信息发布屏和公共广播装置的控制操作行为、远程访问用户行为、访问互联网用户行为等，单独进行行为审计和数据分析；
e） 安全审计记录不应受到未批准的删除、修改或覆盖。

8.1.2.6 可信验证

应基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行

报警，并将验证结果形成审计记录送至安全管理中心。可信验证要求应符合附录 H 的规定。

8.1.3 安全计算环境

8.1.3.1 身份鉴别

身份鉴别要求如下：

a) 应对登录的用户进行身份标识和鉴别；
b) 身份标识应具有唯一性；
c) 身份鉴别信息应具有复杂度要求并定期更换；
d) 应启用登录失败处理功能；
e) 当会话结束、非法登录和登录连接超时时，应建立自动退出机制；
f) 当进行远程管理时，应采取措施防止鉴别信息在网络传输过程中被窃听，包括 HTTPS、SSH 和 VPN 等；
g) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

8.1.3.2 访问控制

访问控制要求如下：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应阻断无法重命名或删除的默认账户直接远程登录；
d) 应及时删除或停用多余的、过期的账户；
e) 应授予管理用户所需的最小权限；
g) 应限制未登录用户的使用权限，对匿名用户使用记录进行追溯；
f) 应由授权主体配置访问控制策略，访问控制策略应规定主体对客体的访问规则；
g) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
h) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；
i) 应提示首次登录用户修改预设的默认口令。

8.1.3.3 安全审计

安全审计要求如下：

a) 应启用安全审计功能，安全审计应覆盖到每个用户；
b) 应对重要的用户行为和重要安全事件进行安全审计；
c) 安全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；
d) 安全审计记录不应受到未批准的删除、修改或覆盖；
e) 应对安全审计记录进行保护和定期备份；
f) 应对安全审计进程的完整性进行保护，降低未经授权中断的风险。

8.1.3.4 入侵防范

入侵防范要求如下：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b) 应关闭不需要的系统服务、默认共享和高危端口；

c） 应通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过测试评估后，及时修补漏洞；
d） 应通过设定终端接入方式或网络地址范围对终端进行限制；
e） 应具备数据有效性检验功能，使通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
f） 应检测对重要节点进行入侵的行为，并在发生严重入侵事件时进行报警。

8.1.3.5 恶意代码防范

恶意代码防范要求如下：
a） 应在关键网络节点处进行恶意代码的检测和清除，维护恶意代码防护机制的有效性，并定期进行升级和更新防恶意代码库；
b） 应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；
c） 通过移动介质进行数据上传时，应在移动介质接入前采用两种或两种以上病毒库对移动介质进行恶意代码查杀。

8.1.3.6 可信验证

应基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，将验证结果形成审计记录送至安全管理中心。可信验证要求应符合附录 H 的规定。

8.1.3.7 数据完整性

数据完整性要求如下：
a） 应采用校验技术或密码技术使重要数据在传输过程中保持完整性，包括但不限于调度信息、鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要媒体内容数据和重要个人信息；
b） 应使用加密技术和数字签名等措施防止数据被未经授权地篡改；
c） 应建立数据备份和恢复机制，防止在数据被篡改或损坏时能及时恢复数据；
d） 应采取多种策略和技术来保护数据的完整性，包括验证、校验、加密、数字签名、备份、恢复、监控、安全控制等措施。

8.1.3.8 数据保密性

数据保密性要求如下：
a） 应使用加密通信协议或 VPN 等技术来保护数据传输安全；
b） 应使用加密技术对敏感数据和重要数据进行加密，防止敏感数据和重要数据被截获或窃取；
c） 应实施访问控制措施，限制对敏感数据和重要数据的访问和使用。

8.1.3.9 数据备份恢复

数据备份恢复要求如下：
a） 应制定详细的备份数据恢复计划，明确恢复流程和责任人；
b） 应具备重要数据的本地数据备份与恢复功能；
c） 应每周至少一次完全数据备份，应每天至少一次增量备份或差分备份；
d） 应具备异地数据实时备份功能；

e） 应具备重要数据处理系统的热冗余。

8.1.3.10 剩余信息保护

剩余信息保护要求如下：

a） 对鉴别信息所在的存储空间，在释放或重新分配前应得到完全清除；
b） 对无法识别特定个人的数据，应进行匿名化处理；
c） 对敏感的个人信息，包括姓名、电话号码、身份证号等，应进行数据脱敏处理。

8.1.3.11 个人信息保护

个人信息保护要求如下：

a） 应采集和保存业务必需的用户个人信息；
b） 不应发生未授权访问和非法使用用户个人信息；
c） 应具备用户个人信息全生命周期管理功能；
d） 应对用户个人信息进行分类分级保护。

8.1.3.12 业务连续性保障

业务连续性保障要求如下：

a） 在各种过程风险评估的基础上应制定业务连续性计划；
b） 业务连续性计划应详细列出每一步的行动方案，包括预防措施、应急响应、恢复计划等；
c） 视频采集装置、信息发布屏和公共广播装置等应进行冗余配置；
d） 当某节点设备出现故障时，应及时切换到备份设备继续运行，切换过程不应对正常工作产生影响。

8.1.4 安全管理中心

8.1.4.1 系统管理

系统管理要求如下：

a） 应对系统管理员进行身份鉴别，系统管理员应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；
b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

8.1.4.2 审计管理

审计管理要求如下：

a） 应对审计管理员进行身份鉴别，审计管理员应通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
b） 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

8.1.4.3 安全管理

安全管理要求如下：

a） 应对安全管理员进行身份鉴别，安全管理员应通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计，管理后台或操作界面应与互联网做物理隔离；

b） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

8.1.4.4 集中管控

集中管控要求如下：

a） 应划分出特定的管理区域，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，并使审计记录留存时间符合国家和行业法律法规要求；
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。

8.2 管理平台安全要求

8.2.1 安全通信网络

安全通信网络要求如下：

a） 应使管理平台不承载高于其安全保护等级的业务应用系统；
b） 应实现不同管理平台服务客户虚拟网络之间的隔离；
c） 应具备根据管理平台服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
d） 应具备根据管理平台服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；
e） 应提供开放接口或开放性安全服务，便于管理平台服务客户接入第三方安全产品或在管理平台计算平台选择第三方安全服务。

8.2.2 安全区域边界

8.2.2.1 访问控制

访问控制要求如下：

a） 应在虚拟化网络边界设置访问控制机制；
b） 应在不同等级的网络边界设置访问控制机制；
c） 应根据安全传输和访问控制的不同，将不同安全级别的网络进行隔离；
d） 应采用多因素认证方式（动态口令、生物识别等），提高身份验证的安全性。

8.2.2.2 入侵防范

入侵防范要求如下：

a） 应检测到管理平台服务客户发起的网络攻击行为，并记录攻击类型、攻击时间、攻击流量等；
b） 应检测到对虚拟网络节点的网络攻击行为，并记录攻击类型、攻击时间、攻击流量等；
c） 应检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；
d） 应在检测到网络攻击行为和异常流量时，及时进行报警。

8.2.2.3 安全审计

安全审计要求如下：

a) 应根据业务需求和安全风险制定安全审计规则和策略；
b) 应对管理平台服务商和管理平台服务客户在远程管理时执行的特权命令进行审计；
c) 应对管理平台服务商和管理平台服务客户的数据和操作进行审计；
d) 应对网络流量、用户行为和安全事件进行全面记录和分析，及时发现异常行为和潜在的攻击行为；
e) 应定期对审计日志进行备份、转存和分析，以便后续的审计和追溯。

8.2.3 安全计算环境

8.2.3.1 身份鉴别

身份鉴别要求如下：
a) 应实施身份标识机制，为每个用户分配唯一的标识；
b) 应采用强密码策略，要求用户使用复杂度较高的密码，并进行周期性更换；
c) 应采取管理平台服务客户首次登录强制修改初始密码措施。

8.2.3.2 访问控制

访问控制要求如下：
a) 在使用用户名和口令的基础上，应使用动态令牌、生物识别和数字证书等技术进行身份验证，提高访问控制的安全性；
b) 应为每个应用或系统分配所需的最小权限，防止用户拥有不必要的过高权限；
c) 当虚拟机迁移时，访问控制策略应随其迁移；
d) 管理平台应为服务客户设置不同虚拟机之间的访问控制策略；
e) 应定期对系统进行安全风险评估和漏洞扫描，及时发现和修复潜在的安全问题；
f) 应对所有软件进行测试和验证，减少因软件缺陷导致的安全问题。

8.2.3.3 入侵防范

入侵防范要求如下：
a) 应能检测虚拟机之间的资源隔离失效，并进行告警；
b) 应能检测到非授权新建虚拟机或重新启用虚拟机，并进行告警；
c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

8.2.3.4 镜像和快照保护

镜像和快照保护要求如下：
a) 应对镜像和快照的创建、存储、传输和使用进行严格的管理和控制；
b) 应对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；
c) 应具备虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
d) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
e) 应将虚拟机镜像和快照文件备份在不同物理存储。

8.2.3.5 数据完整性和保密性

数据完整性和保密性要求如下：
a) 数据传输过程中的完整性应符合 GB/T 37025—2018 中 6.1 和 7.1 的要求；
b) 应通过封装签名、测试字验证、引用约束等机制，对数据的完整性进行检测；
c) 应对数据的完整性进行校验，防止数据在传输和存储过程中被篡改或损坏；

d） 应使用加密技术对数据进行加密传输和存储；
e） 应保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取恢复措施；
f） 应采取管理平台服务客户设置密钥管理措施，使管理平台服务客户自行实现数据的加解密过程。

8.2.3.6 数据备份恢复

数据备份恢复要求如下：
a） 应具备重要数据的本地数据备份与恢复功能，数据备份包括完全数据备份和增量备份；
b） 应对备份信息的备份方式、备份频度、存储介质、保存期等进行规定；
c） 应支持备份程序与应用程序的分离；
d） 应支持对备份数据进行压缩存储；
e） 应能够从备份数据中完整地恢复所有数据，并定期测试备份数据的可恢复性；
f） 应具备异地实时备份功能，利用通信网络将重要数据定时批量传送至备用场地。

8.2.3.7 剩余信息保护

剩余信息保护要求如下：
a） 当虚拟机在停止使用或释放时，其内存区域应进行完全清除；
b） 当虚拟机使用的存储空间在重新分配给其他用户或进行数据迁移前，其硬盘或存储设备应进行完全清除；
c） 当鉴别信息所在的存储空间被释放或重新分配给其他用户前，其鉴别信息应进行完全清除；
d） 当系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前，其资源所在的存储空间应进行完全清除。

8.2.4 安全管理中心

安全管理中心要求如下：
a） 应在技术层面实施系统管理，包括系统管理员的权限鉴别、系统资源和运行配置控制和管理、异常处理、数据和设备的备份与恢复等；
b） 应对系统管理员进行身份鉴别，系统管理员应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；
c） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括身份鉴别、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；
d） 应通过系统管理员对分散在各设备上的审计数据进行收集汇总和集中分析；
e） 应通过系统管理员对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

8.3 移动互联安全要求

8.3.1 安全区域边界

8.3.1.1 边界防护

边界防护要求如下：
a） 应将跨越有线网络与无线网络边界之间的访问和数据流，通过边界设备提供的受控接口进行通信；
b） 应检查或限制非授权设备私自联到内部网络的行为；
c） 应检查或限制内部用户非授权联到外部网络的行为；

d) 应实时监控网络的运行状态，当发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，及时对其进行有效阻断；
e) 应严格控制无线网络的接入，只有经过授权和认证的设备才能接入网络；
f) 应实时监控网络的运行状态，一旦发现异常行为，立即进行阻断，防止潜在的安全威胁扩散。

8.3.1.2 访问控制

访问控制要求如下：
a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则；
b) 应开启无线接入设备的接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证，加密方式至少包含 SM2 或 SM4；
c) 不应使用 WEP 方式进行认证；当使用口令时，口令长度不应小于 8 位字符；
d) 应对进出网络的数据包进行详细的检查和控制，包括对源地址、目的地址、源端口、目的端口和协议等进行检查；
e) 应根据会话状态信息判断用户的访问权限，并决定是否批准其访问特定的网络资源；
f) 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。

8.3.1.3 入侵防范

入侵防范要求如下：
a) 应检测非授权无线接入设备和非授权移动终端的接入行为；
b) 应检测对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
c) 应检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
d) 不应多个 AP 使用同一个认证密钥；
e) 应能够阻断非授权无线接入设备或非授权移动终端；
f) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
g) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

8.3.2 安全计算环境

8.3.2.1 移动终端管控

移动终端管控要求如下：
a) 应使用终端管理客户端软件对移动终端进行安装、注册和管理；
b) 应接受终端管理客户端软件对移动终端设备的生命周期管理和设备远程控制（如远程锁定、远程擦除等）；
c) 应将移动终端的使用限定在处理指定的业务；
d) 应对移动终端存储的敏感信息采取加密措施，并在未授权情况下不可读；
e) 应采用专用终端发布直播数据；
f) 当移动终端在与外部设备或应用进行数据交换时，应采取认证和加密措施；
g) 应采取相应的防丢失和防破坏的技术措施限制移动终端的物理访问；
h) 应对移动终端操作系统和应用程序的安全性，定期进行漏洞扫描和安全更新。

8.3.2.2 移动应用管控

移动应用管控要求如下：
a) 应具备选择应用软件安装、运行的功能；

b) 应依据指定证书签名的应用软件进行安装和运行；
c) 应根据软件白名单功能控制应用软件的安装和运行；
d) 应具备接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力；
e) 应采取相应的加密和数据保护措施实现移动应用软件的数据安全；
f) 应建立完善的移动应用软件管理制度，包括软件的采购、测试、发布、更新等环节的管理要求；
g) 应采取技术措施对移动应用软件进行监控和管理，包括软件的安装、卸载、运行等环节的控制和管理；
h) 应采用专用移动应用软件防止二次打包工具篡改程序文件，以及防止移动应用程序的代码、图片、配置、布局等被增加、修改或删除。

8.4 挂载设备安全要求

8.4.1 安全物理环境

安全物理环境要求如下：
a) 应选择在不易受自然灾害和人为破坏的区域安装多功能智能杆；
b) 应对多功能智能杆及其挂载设备进行加固处理，防止被盗或被破坏；
c) 应对多功能智能杆及其挂载设备设置明显的警示标识；
d) 应对多功能智能杆和挂载设备安装防雷击装置；
e) 应将挂载设备安装在能正确反映所处物理环境状态的位置；
f) 应将挂载设备安装在不影响挂载设备正常工作的位置；
g) 应将挂载设备的气象传感器和温湿度传感器安装在阳光不直接照射的区域。

8.4.2 安全区域边界

8.4.2.1 接入控制

接入控制要求如下：
a) 应设置安全区域边界的划分，并根据安全等级和安全需求进行合理配置；
b) 应采取技术措施对安全区域边界进行接入控制和管理，包括物理隔离、访问控制、监测和审计等；
c) 挂载设备接入控制采用的接口要求如下：
   1) RJ45 以太网通信接口，单个接口通信速率不应低于 1000 Mbps；网络层应采用 IP 协议，并支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，当挂载设备为客户端，边缘控制器为服务端时，挂载设备应支持对多个服务端传输数据；
   2) COM 应支持 RS-232（DB9）或 RS-485；
   3) 挂载设备为摄像机，当具有视频监控功能时，接口协议应符合 GB/T 28181 的要求；
   4) 挂载设备为摄像机，当具有视频图像信息采集功能时，接口协议应符合 GA/T 1400.4—2017 中 5.2 的要求。
d) 应对挂载设备进行监控和数据采集，实现设备的远程管理和控制；
e) 应对挂载设备采取加密传输和身份认证等安全防护措施。

8.4.2.2 安全控制

安全控制应符合7.4.2.2的要求。

8.4.2.3 入侵防范

入侵防范要求如下：

a) 应限制与挂载设备通信的目标地址，防止对陌生地址的攻击行为；
b) 应限制与边缘控制器通信的目标地址，防止对陌生地址的攻击行为；
c) 应定期更新系统和软件漏洞补丁，及时修复已知漏洞，降低被攻击的风险；
d) 应检测非授权无线接入设备和非授权移动终端的接入行为；
e) 应通过配置无线接入设备的认证策略防止多个 AP 使用同一个认证密钥；
f) 应检测针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为。

8.4.3 安全计算环境

8.4.3.1 挂载设备安全

挂载设备安全要求如下：

a) 应采取只有经过授权的用户才可以对挂载设备的软件应用进行配置或变更的措施；
b) 应对所有用户进行身份标识和鉴别，只有通过身份认证的用户才能访问挂载设备；
c) 应对挂载设备连接的边缘控制器（包括读写器）进行身份标识和鉴别；
d) 应对挂载设备连接的其他设备（包括路由器）进行身份标识和鉴别；
e) 应对不同等级用户的身份和权限，设置其对挂载设备的不同访问权限。

8.4.3.2 边缘控制器安全

边缘控制器安全要求如下：

a) 应对边缘控制器的访问进行身份标识和鉴别；
b) 应对合法连接设备（包括挂载设备、路由节点、数据处理中心）进行标识和鉴别；
c) 应根据不同等级用户的身份和权限，设置其对边缘控制器的不同访问权限；
d) 应过滤非法挂载设备和伪造挂载设备所发送的数据；
e) 应授权用户在挂载设备使用过程中对关键密钥进行在线更新；
f) 应授权用户在挂载设备使用过程中对关键配置参数进行在线更新。

8.4.3.3 抗数据重放

抗数据重放要求如下：

a) 应通过时间戳和序列号等方式，对接收的数据进行新鲜性检查，防止历史数据被重放攻击；
b) 应通过数据校验方式，鉴别历史数据的非法修改；
c) 应通过对缓存数据进行严格的管理和控制，防止被恶意利用或重放。

8.4.3.4 数据融合处理

数据融合处理要求如下：

a) 应对不同来源和不同格式的挂载设备数据进行融合处理，使不同种类的数据可以在同一个平台被使用；
b) 应对不同数据之间的依赖关系和制约关系等进行智能处理；
c) 应对挂载设备数据进行去重处理，使每个数据项只被处理一次，防止重复数据处理带来的冗余和误差；

d） 应将不同数据源的数据进行关联分析，找出数据之间的潜在联系和规律，为后续的数据利用提供有价值的信息。

8.4.4 安全运维管理

安全运维管理要求如下：

a） 应实施供应链风险管理策略，使设备的安全性从供应链一直到部署过程中都得到保障；
b） 应指定人员定期巡视挂载设备和边缘控制器的安装环境，对影响挂载设备和边缘控制器正常工作的环境异常进行记录和处理；
c） 应使用强密码或证书来验证设备身份，防止未授权的设备访问多功能智能杆系统网络；
d） 应对挂载设备和边缘控制器的入库、存储、部署、携带、维修、丢失和报废等进行全过程管理；
e） 应指定人员定期巡视挂载设备和边缘控制器的部署环境，对影响挂载设备和边缘控制器正常工作的环境异常进行记录和处理；
f） 应加强对挂载设备和边缘控制器安装位置的保密性管理。

8.5 公共数据基本安全要求

公共数据基本安全应符合6.5的要求。

8.6 公共数据三级增强安全要求

8.6.1 数据收集三级增强安全要求

数据收集三级增强安全要求如下：

a） 应对数据收集过程中的网络环境、系统进行安全评估；
b） 应检查收集数据的来源是可靠和受信任的，防止收集到伪造或篡改过的数据；
c） 在数据收集过程中，应实施严格的权限管理和身份验证机制；
d） 应对收集到的数据进行分类和标记，以便于后续的数据处理、存储和使用。根据数据的敏感程度和重要程度，采取不同的安全措施；
e） 应在数据传输过程中采用加密技术对数据进行加密，并定期更新传输协议和加密算法，以应对潜在的安全威胁；
f） 在收集数据时，应进行数据备份并保存在安全的环境中，应在意外情况下及时恢复数据。

8.6.2 数据存储三级增强安全要求

数据存储三级增强安全要求如下：

a） 应具备异地实时备份功能，利用通信网络将数据实时备份至备份场地；
b） 应具备勒索病毒事前预警、事中阻断及事后恢复的保障能力；
c） 应提供数据处理环节中关联信息系统的热冗余。

8.6.3 数据传输三级增强安全要求

数据传输三级增强安全要求如下：

a） 应对关键网络传输线路及核心设备实施冗余备份；
b） 应对重要数据采取不通过离线或即时的通信方式进行传输。

8.6.4 数据使用三级增强安全要求

数据使用三级增强安全要求如下：

a) 应采取技术措施使汇聚大量数据时不暴露敏感信息；
b) 应对不同数据使用场景采取数字水印等技术，实现数据防泄密及溯源能力；
c) 应对接入或嵌入的第三方应用加强数据安全管理；
d) 宜对接入或嵌入的第三方应用开展技术检测，使其数据处理行为符合双方约定要求。

8.6.5 数据加工三级增强安全要求

数据加工三级增强安全要求如下：

a) 应对数据加工的过程进行评估和监控，并对异常数据的操作行为及时预警和处置；
b) 应对数据加工的结果进行评估和安全审核，防止新数据发生泄露的风险；
c) 应提供安全的数据加工环境（包括网络环境和终端环境等），防止加工过程导致数据泄露和数据破坏等安全风险。

8.6.6 数据开放共享三级增强安全要求

数据开放共享三级增强安全要求如下：

a) 应建立公共数据内部审批机制，包括数据对外共享目的、范围、期限和频次等内容；
b) 应制定统一的数据交换标准和技术规范，促进不同系统之间的数据共享和交互；
c) 应建立开放的元数据标准，方便用户对数据进行整合和使用，支持数据的自由流通和利用；
d) 应采用多方安全计算、动态加密和数字水印等技术，防止数据泄露和被非法获取，实现数据共享的安全性；
e) 在开放共享数据时，对个人敏感信息的处理应遵循相关法律法规，防止数据滥用和侵犯个人隐私。

8.6.7 数据交易三级增强安全要求

数据交易三级增强安全要求如下：

a) 数据的获取、使用、共享和交易应在法律和监管框架内进行；
b) 数据交易应采取安全措施保护数据的安全性和保密性；
c) 数据交易应遵循统一的技术标准和互操作性原则，方便数据的交换和整合；
d) 交易的各方应明确交易数据的收集范围、使用目的和共享范围；
e) 交易的数据应经过清洗、去重和整合等处理过程。

8.6.8 数据出境三级增强安全要求

数据出境三级增强安全要求如下：

a) 应根据跨境数据的重要性和敏感程度，对跨境数据进行分类管理；
b) 应对跨境数据中的高敏感度信息采取严格的安全措施（如加密传输和存储、访问控制等）；
c) 应采取访问控制、权限管理、审计跟踪等安全措施，限制对跨境数据的访问和使用权限；
d) 应对跨境数据的存储采取安全措施（如数据加密存储、访问控制、安全审计等），防止跨境数据被未经授权的访问、篡改或泄露。

8.6.9 数据销毁与删除三级增强安全要求

数据销毁与删除三级增强安全要求如下：

a) 应在中华人民共和国境内对介质存储的数据进行销毁或删除；
b) 应对存储数据的介质或物理设备采取无法恢复的方式进行数据销毁与删除，包括物理粉碎、消磁、多次擦写等手段。

9 第四级安全要求

9.1 安全通用要求

9.1.1 安全通信网络

9.1.1.1 网络架构

网络架构要求如下：

a) 网络设备的业务处理能力应满足业务高峰期需要；
b) 网络各个部分的带宽应满足业务高峰期需要；
c) 应根据系统功能、业务流程、网络结构层次、业务服务对象等因素划分不同网络区域，并按照方便安全管理和控制的原则为各网络区域分配地址；
d) 不应将视频采集装置、信息发布屏和公共广播装置等设备的重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的逻辑或物理技术隔离手段；
e) 应对通信线路、关键网络设备、关键安全设备(至少包括防火墙、加密模块、入侵检测和防护设备)和关键计算设备(至少包括边缘计算器)进行冗余配置；
f) 应根据业务服务的重要程度分配带宽，优先保障重要业务；
g) 应具备不同路由的双链路接入保障能力；
h) 应配备与实际运行情况相符的网络拓扑架构。

9.1.1.2 通信传输

通信传输要求如下：

a) 应采用校验技术、密码技术或特定协议转换技术使通信传输过程中的数据保持完整性；
b) 应采用密码技术或特定协议转换技术使通信传输过程中的数据保持保密性；
c) 应在通信前采用密码技术对通信的双方进行验证或认证；
d) 应采用硬件密码模块对重要通信传输过程进行密码运算和密钥管理，加密方式至少包含SM2 或 SM4；
e) 应使用协议对管理流量与媒体内容数据流等业务流量进行分离传输。

9.1.1.3 可信验证

应基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，将验证结果形成审计记录送至安全管理中心，进行动态关联感知。可信验证要求应符合附录 H 的规定。

9.1.2 安全区域边界

9.1.2.1 边界防护

边界防护要求如下：

a) 应使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；
b) 应对非授权设备私自联到内部网络的行为进行检查和限制；
c) 应对内部用户非授权联到外部网络的行为进行检查和限制；
d) 视频采集装置、信息发布屏和公共广播装置等不应通过无线方式进行组网，系统应限制无线网络的使用；

e） 应有效阻断非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为；
f） 应采取可信验证机制对接入到网络中的设备进行可信验证；
g） 应对敏感数据泄露行为进行检查，准确定出位置，并对其进行有效阻断。

9.1.2.2 访问控制

访问控制要求如下：
a） 应在网络边界根据访问控制策略设置访问控制规则；
b） 应删除多余或无效的访问控制规则，优化访问控制列表，使访问控制规则数量最小化；
c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d） 应根据会话状态信息为进出数据流制定允许/拒绝访问的措施；
e） 通过外部网络对信息系统进行访问时，应使用安全方式接入，对用户和权限进行管理，赋予最小访问权限，控制粒度为用户级；
f） 应根据应用协议和应用内容对进出网络的数据流进行访问控制；
g） 宜在会话结束后终止网络连接。

9.1.2.3 入侵防范

入侵防范要求如下：
a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
d） 当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目的和攻击时间；
e） 当发生严重入侵事件时，应及时启动报警。

9.1.2.4 恶意代码防范

恶意代码防范要求如下：
a） 应在关键网络节点处进行恶意代码检测和清除，并维护恶意代码防护机制有效性，及时升级和更新特征库；
b） 部署在关键网络节点的防恶意代码产品宜与系统内部防恶意代码产品具有不同的防恶意代码库。

9.1.2.5 安全审计

安全审计要求如下：
a） 应在网络边界、重要网络节点进行安全审计，安全审计应覆盖到每个用户；
b） 应对安全审计记录进行保护和定期备份；
c） 审计记录应包括事件的日期、时间、IP 地址、事件类型、事件是否成功及其他与安全审计相关的信息；
d） 应对视频采集装置、信息发布屏和公共广播装置的控制操作行为、远程访问用户行为、访问互联网用户行为等，单独进行行为审计和数据分析；
e） 安全审计记录不应受到未批准的删除、修改或覆盖；
f） 应对审计记录进行保护和定期备份；
g） 应定期对审计记录进行分析，以便及时发现异常行为。

9.1.2.6 可信验证

应基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，将验证结果形成审计记录送至安全管理中心，进行动态关联感知。可信验证要求应符合附录H的规定。

9.1.3 安全计算环境

9.1.3.1 身份鉴别

身份鉴别要求如下：

a) 应对登录的用户进行身份标识和鉴别；
b) 身份标识应具有唯一性；
c) 身份鉴别信息应具有复杂度要求并定期更换；
d) 应启用登录失败处理功能；
e) 当会话结束、非法登录和登录连接超时时，应建立自动退出机制；
f) 当进行远程管理时，应采取措施防止鉴别信息在网络传输过程中被窃听，包括HTTPS、SSH和VPN等；
g) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

9.1.3.2 访问控制

访问控制要求如下：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应阻断无法重命名或删除的默认账户直接远程登录；
d) 应及时删除或停用多余的、过期的账户；
e) 应授予管理用户所需的最小权限；
f) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
g) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
h) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；
i) 应强制首次登录用户修改预设的默认口令；
j) 应限制未登录用户的使用权限，可对匿名用户使用记录进行追溯；
k) 视频采集装置、信息发布屏和公共广播装置等的特权命令应在服务器或专用操作终端执行。

9.1.3.3 安全审计

安全审计要求如下：

a) 应启用安全审计功能，安全审计应覆盖到每个用户；
b) 应对重要的用户行为和重要安全事件进行安全审计；
c) 安全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；
d) 安全审计记录不应受到未批准的删除、修改或覆盖；
e) 应对安全审计记录进行保护和定期备份；
f) 应对安全审计进程的完整性进行保护，降低未经授权中断的风险；
g) 应使用防火墙和入侵检测措施防止未经授权的网络访问；
h) 应定期检查系统防止出现未授权的更改或异常活动。

9.1.3.4 入侵防范

入侵防范要求如下：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b) 应关闭不需要的系统服务、默认共享和高危端口；
c) 应通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过测试评估后，及时修补漏洞；
d) 应通过设定终端接入方式或网络地址范围对终端进行限制；
e) 应具备数据有效性检验功能，使通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
f) 应检测对重要节点进行入侵的行为，并在发生严重入侵事件时进行报警；
g) 应使用复杂且独特的密码，不应使用容易猜测的密码；
h) 应限制对敏感设备和数据中心的物理访问。

9.1.3.5 恶意代码防范

恶意代码防范要求如下：

a) 应在关键网络节点处进行恶意代码的检测和清除，维护恶意代码防护机制的有效性，并定期进行升级和更新防恶意代码库；
b) 应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；
c) 通过移动介质进行数据上传时，应在移动介质接入前，采用两种或两种以上病毒库对移动介质进行恶意代码查杀；
d) 应及时更新系统和应用程序，安装最新的安全补丁；
e) 应使用有效的反病毒软件，定期扫描和检测系统。

9.1.3.6 可信验证

应基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，将验证结果形成审计记录送至安全管理中心，进行动态关联感知。可信验证要求应符合附录 H 的规定。

9.1.3.7 数据完整性

数据完整性要求如下：

a) 应采用校验技术或密码技术使重要数据在传输过程中保持完整性，包括但不限于调度信息、鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要媒体内容数据和重要个人信息；
b) 应使用加密技术和数字签名等措施防止数据被未经授权地篡改；
c) 应建立数据备份和恢复机制，防止在数据被篡改或损坏时能及时恢复数据；
d) 应采取多种策略和技术来保护数据的完整性，包括验证、校验、加密、数字签名、备份、恢复、监控、安全控制等措施；
e) 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

9.1.3.8 数据保密性

数据保密性要求如下：

a） 应使用加密通信协议或VPN等技术来保护数据传输安全；
b） 应使用加密技术对敏感数据和重要数据进行加密，防止敏感数据和重要数据被截获或窃取；
c） 应实施访问控制措施，限制对敏感数据和重要数据的访问和使用；
d） 应对敏感数据和重要数据的访问和使用进行审计和监控，及时发现和处理任何异常行为或活动；
e） 应定期评估数据保密性要求，并根据需要进行更新和改进。

9.1.3.9 数据备份恢复

数据备份恢复要求如下：
a） 应制定详细的备份数据恢复计划，明确恢复流程和责任人；
b） 应具备重要数据的本地数据备份与恢复功能；
c） 应每周至少一次完全数据备份，应每天至少一次增量备份或差分备份；
d） 应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用的实时切换；
e） 应具备重要数据处理系统的热冗余；
f） 应定期对恢复计划的可行性和有效性进行恢复演练；
g） 应定期对灾难恢复机制的可行性和有效性进行灾难恢复演练；
h） 应定期审查数据备份恢复要求，并根据需要进行更新和改进；
i） 应采用新技术和新方法不断优化数据备份恢复策略和流程。

9.1.3.10 剩余信息保护

剩余信息保护要求如下：
a） 对鉴别信息所在的存储空间，在释放或重新分配前应得到完全清除；
b） 对无法识别特定个人的数据，应进行匿名化处理；
c） 对敏感的个人信息，包括姓名、电话号码、身份证号等，应进行数据脱敏处理；
d） 对经过匿名化处理后的数据，应进行加密存储；
e） 应及时删除或匿名化处理剩余信息，降低数据泄露和滥用的风险。

9.1.3.11 个人信息保护

个人信息保护要求如下：
a） 应仅采集和保存业务必需的用户个人信息；
b） 不应发生未授权访问和非法使用用户个人信息；
c） 应具备用户个人信息全生命周期管理功能；
d） 应对用户个人信息进行分类分级保护；
e） 应采取严格的管理和技术防护措施，防止用户个人信息被窃取、被泄露。

9.1.3.12 业务连续性保障

业务连续性保障要求如下：
a） 在各种过程风险评估的基础上应制定业务连续性计划；
b） 业务连续性计划应详细列出每一步的行动方案，包括预防措施、应急响应、恢复计划等；
c） 视频采集装置、信息发布屏和公共广播装置等应进行冗余配置；
d） 当某节点设备出现故障时，应及时切换到备份设备继续运行，切换过程不应对正常工作产生影响；

e） 应定期进行业务连续性演练，模拟真实场景，检验计划的可行性和有效性；
f） 应及时修正演练过程中发现的任何问题，不断完善业务连续性计划。

9.1.4 安全管理中心

9.1.4.1 系统管理

系统管理要求如下：

a） 应对系统管理员进行身份鉴别，系统管理员应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；
b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；
c） 应配置防火墙规则，限制未授权访问和防止恶意软件进入系统。

9.1.4.2 审计管理

审计管理要求如下：

a） 应对审计管理员进行身份鉴别，审计管理员应通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
b） 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；
c） 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。

9.1.4.3 安全管理

安全管理要求如下：

a） 应对安全管理员进行身份鉴别，安全管理员应通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计，管理后台或操作界面应与互联网做物理隔离；
b） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等；
c） 应建立安全日志和事件处置机制，及时响应和处理安全事件，并对其进行跟踪和记录。

9.1.4.4 集中管控

集中管控要求如下：

a） 应划分出特定的管理区域，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，并使审计记录留存时间符合国家和行业法律法规要求；
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；
f） 应具备网络安全实时监测、态势感知、风险预警、统一展示和安全事件应急处置的能力；
g） 系统范围内的时间应由唯一确定的时钟产生，使各种数据的管理和分析在时间上保持一致。

9.2 管理平台安全要求

9.2.1 安全通信网络

安全通信网络要求如下：

a) 应使管理平台不承载高于其安全保护等级的业务应用系统；
b) 应实现不同管理平台服务客户虚拟网络之间的隔离；
c) 应具备根据管理平台服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
d) 应具备根据管理平台服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；
e) 应提供开放接口或开放性安全服务，批准管理平台服务客户接入第三方安全产品或在管理平台选择第三方安全服务；
f) 应具备对虚拟资源的主体和客体设置安全标记的能力，批准管理平台服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；
g) 应提供通信协议转换或通信协议隔离等的数据交换方式，批准管理平台服务客户可以根据业务需求自主选择边界数据交换方式；
h) 应为第四级业务应用系统划分独立的资源池。

9.2.2 安全区域边界

9.2.2.1 访问控制

访问控制要求如下：
a) 应在虚拟化网络边界设置访问控制机制；
b) 应在不同等级的网络边界设置访问控制机制；
c) 应根据安全传输和访问控制的不同，将不同安全级别的网络进行隔离；
d) 应采用多因素认证方式（动态口令、生物识别等），提高身份验证的安全性；
e) 应制定访问控制策略，包括用户身份验证、权限管理等；
f) 应使用入侵检测系统，实时监测和预警潜在的安全威胁。

9.2.2.2 入侵防范

入侵防范要求如下：
a) 应检测管理平台服务客户发起的网络攻击行为，并记录攻击类型、攻击时间、攻击流量等；
b) 应检测对虚拟网络节点的网络攻击行为，并记录攻击类型、攻击时间、攻击流量等；
c) 应检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；
d) 检测到网络攻击行为和异常流量时，应及时进行报警；
e) 当系统涉及无线网络时，应采取措施限制无线网络的访问范围和用户数量，防止未授权用户接入网络。

9.2.2.3 安全审计

安全审计要求如下：
a) 应根据业务需求和安全风险制定安全审计规则和策略；
b) 应对管理平台服务商和管理平台服务客户在远程管理时执行的特权命令进行审计；
c) 应对管理平台服务商和管理平台服务客户的数据和操作进行审计；
d) 应对网络流量、用户行为和安全事件进行全面记录和分析，及时发现异常行为和潜在的攻击行为；
e) 应定期对审计日志进行备份、转存和分析，以便后续的审计和追溯；
f) 应提高安全审计员的安全意识和技能水平，使他们能够准确、及时地发现和处理安全问题；
g) 应定期进行合规性检查和外部安全审计，安全审计工作应规范和有效。

9.2.3 安全计算环境

9.2.3.1 身份鉴别

身份鉴别要求如下：

a) 应实施身份标识机制，为每个用户分配唯一的标识；
b) 应采用强密码策略，要求用户使用复杂度较高的密码，并进行周期性更换；
c) 应采取管理平台服务客户首次登录强制修改初始密码措施；
d) 应限制账户创建和删除的频率和范围，并对账户权限进行最小化原则分配；
e) 应建立远程操作和管理平台之间的双向身份验证机制。

9.2.3.2 访问控制

访问控制要求如下：

a) 在使用用户名和口令的基础上，应使用动态令牌、生物识别和数字证书等技术进行身份验证，提高访问控制的安全性；
b) 应为每个应用或系统分配所需的最小权限，防止用户拥有不必要的过高权限；
c) 当虚拟机迁移时，访问控制策略应随其迁移；
d) 管理平台应为服务客户设置不同虚拟机之间的访问控制策略；
e) 应定期对系统进行安全风险评估和漏洞扫描，及时发现和修复潜在的安全问题；
f) 应对所有软件进行测试和验证，减少因软件缺陷导致的安全问题；
g) 应对所有访问请求进行记录和审计，以便及时发现和处理潜在的安全问题；
h) 应对所有资源实施强制访问控制后，授权人员才能访问相关系统和数据。

9.2.3.3 入侵防范

入侵防范要求如下：

a) 应能检测虚拟机之间的资源隔离失效，并进行告警；
b) 应能检测到非授权的新建虚拟机或重新启用虚拟机，并进行告警；
c) 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

9.2.3.4 镜像和快照保护

镜像和快照保护要求如下：

a) 应对镜像和快照的创建、存储、传输和使用进行严格的管理和控制；
b) 应对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；
c) 应具备虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
d) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
e) 应将虚拟机镜像和快照文件备份在不同物理存储；
f) 应定期备份镜像和快照数据，并建立相应的恢复机制；
g) 应定期对镜像和快照系统进行安全风险评估和漏洞扫描，及时发现和修复潜在的安全问题。

9.2.3.5 数据访问权限控制

数据访问权限控制要求如下：

a) 应实施强密码策略，要求用户提供正确的用户名和密码进行身份验证，防止未授权访问；
b) 应建立业务数据、系统数据和数据库系统等不同级别的用户权限分离管理机制；

c) 应根据用户角色和业务需求对每个用户分配最小的访问权限，限制用户只能访问其所需的数据；
d) 应限制第三方访问默认账户的访问权限，定期修改账户的口令；
e) 应实时监测用户的操作行为，发现异常行为及时报警并采取相应的防范措施。

9.2.3.6 数据完整性和保密性

数据完整性和保密性要求如下：

a) 数据传输过程中的完整性应符合 GB/T 37025—2018 中 6.1 和 7.1 的要求；
b) 应通过封装签名、测试字验证、引用约束等机制，对数据的完整性进行检测；
c) 应对数据的完整性进行校验，防止数据在传输和存储过程中被篡改或损坏；
d) 应使用加密技术对数据进行加密传输和存储；
e) 虚拟机迁移过程中重要数据应完整，在检测到完整性受到破坏时采取恢复措施；
f) 应支持管理平台服务客户设置密钥管理措施，使管理平台服务客户自行实现数据的加解密过程；
g) 应及时发现和处理与数据完整性及保密性相关的安全漏洞；
h) 应将管理平台服务客户数据和用户个人信息等存储在中华人民共和国境内。

9.2.3.7 数据共享与服务

数据共享与服务要求如下：

a) 应支持与政府相关主管部门实现数据传递与共享；
b) 共享给公安和交通部门的数据应符合 GA/T 1049.3—2013 中第 3 章和 GB/T 28181 的要求；
c) 共享给其他业务部门和社会需求方的数据应符合相关的技术标准和管理规定；
d) 应建立规范的数据格式，统一数据交换接口，与使用单位实现多功能智能杆运行、维护、故障及预警等信息的数据传递和数据共享；
e) 应在管理平台中对挂载设备感知的数据进行处理和计算，对外只提供数据处理和计算结果，原始数据原则上不出管理平台；
f) 管理平台不应无故拒绝合理的数据共享需求，在处理数据共享申请时，应遵循服务等级协议 SLA。

9.2.3.8 数据备份恢复

数据备份恢复要求如下：

a) 应具备重要数据的本地数据备份与恢复功能，数据备份包括完全数据备份和增量备份；
b) 应对备份信息的备份方式、备份频度、存储介质、保存期等进行规定；
c) 应支持备份程序与应用程序的分离；
d) 应支持对备份数据进行压缩存储；
e) 应能够从备份数据中完整地恢复所有数据，并定期测试备份数据的可恢复性；
f) 应具备异地实时备份功能，利用通信网络将重要数据定时批量传送至备用场地；
g) 应采用冗余技术设计网络拓扑结构，防止关键节点存在单点故障；
h) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余；
i) 应制定灾难恢复计划，确定在灾难发生时的数据恢复流程和责任人，并定期进行灾难恢复演练。

9.2.3.9 数据销毁

数据销毁要求如下：

a) 应制定明确的数据销毁策略和计划，数据在持有期限到期后应及时销毁，不应超期保存数据；
b) 应对已经明确不再使用或到期需要删除的数据及时进行销毁；
c) 应根据业务需求对个人数据的销毁选择彻底删除或匿名化；
d) 应对不再需要的数据定期进行销毁，防止数据长期留存在系统中被泄露或被攻击者利用；
e) 应按照审计原则建立数据销毁策略和管理制度，明确销毁数据范围和流程，记录数据删除的操作时间、操作人员、操作方式、数据内容等相关信息，方便后续审计和追溯。

9.2.3.10 数据可审计性

数据可审计性要求如下：

a) 审计范围应覆盖业务数据的用户行为，针对数据的重要性设定不同级别的审计记录；
b) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
c) 应对审计数据进行实时分析，并具备预警和告警功能；
d) 应将审计数据长期保存和定期备份，防止审计数据受到未批准的删除、修改或覆盖等。

9.2.3.11 剩余信息保护

剩余信息保护要求如下：

a) 当虚拟机在停止使用或释放时，其内存区域应进行完全清除；
b) 当虚拟机使用的存储空间在重新分配给其他用户或进行数据迁移前，其硬盘或存储设备应进行完全清除；
c) 当鉴别信息所在的存储空间被释放或重新分配给其他用户前，其鉴别信息应进行完全清除；
d) 当系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前，其资源所在的存储空间应进行完全清除；
e) 当退出系统时，应防止存有敏感数据的存储空间被其他非授权用户获取，并及时清除内存空间；
f) 当管理平台服务客户在删除业务应用数据时，管理平台应将存储的所有副本删除。

9.2.4 安全管理中心

安全管理中心要求如下：

a) 应在技术层面实施系统管理，包括系统管理员的权限鉴别、系统资源和运行配置控制和管理、异常处理、数据和设备的备份与恢复等；
b) 应对系统管理员实施严格的身份鉴别机制，并限制其通过特定的命令或操作界面进行系统管理操作；
c) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括身份鉴别、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；
d) 应通过系统管理员对分散在各设备上的审计数据进行收集汇总和集中分析；
e) 应通过系统管理员对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
f) 应对物理资源和虚拟资源按照策略做统一管理调度与分配；
g) 应将管理平台计算平台管理流量与管理平台服务客户业务流量进行分离；
h) 应集中监测网络链路、安全设备、网络设备、服务器等的运行状况。

9.3 移动互联安全要求

9.3.1 安全区域边界

9.3.1.1 边界防护

边界防护要求如下：

a) 应将跨越有线网络与无线网络边界之间的访问和数据流，通过边界设备提供的受控接口进行通信；
b) 应检查或限制非授权设备私自联到内部网络的行为；
c) 应检查或限制内部用户非授权联到外部网络的行为；
d) 应实时监控网络的运行状态，当发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，及时对其进行有效阻断；
e) 应严格控制无线网络的接入，只有经过授权和认证的设备才能接入网络；
f) 应实时监控网络的运行状态，一旦发现异常行为，立即进行阻断，防止潜在的安全威胁扩散；
g) 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换；
h) 应开启无线接入设备接入认证功能，并采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；
i) 不应使多个 AP 用同一个鉴别密钥，并阻断非授权无线接入设备或非授权移动终端。

9.3.1.2 访问控制

访问控制要求如下：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则；
b) 应开启无线接入设备的接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证，加密方式至少包含 SM2 或 SM4；
c) 不应使用 WEP 方式进行认证；当使用口令时，口令长度不应小于 8 位字符；
d) 应对进出网络的数据包进行详细的检查和控制，包括对源地址、目的地址、源端口、目的端口和协议等进行检查；
e) 应根据会话状态信息判断用户的访问权限，并决定是否批准其访问特定的网络资源；
f) 应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换；
g) 应删除多余或无效的访问控制规则，优化访问控制列表，使访问控制规则数量最小；
h) 应定期审查和更新访问控制规则，使其准确和有效。

9.3.1.3 入侵防范

入侵防范要求如下：

a) 应检测非授权无线接入设备和非授权移动终端的接入行为；
b) 应检测对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
c) 应检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
d) 不应多个 AP 使用同一个认证密钥；
e) 应能够阻断非授权无线接入设备或非授权移动终端；
f) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
g) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
h) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
i) 当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

9.3.2 安全计算环境

9.3.2.1 移动终端管控

移动终端管控要求如下：

a) 应使用终端管理客户端软件对移动终端进行安装、注册和管理；
b) 应接受终端管理客户端软件对移动终端设备的生命周期管理和设备远程控制（如远程锁定、远程擦除等）；
c) 应将移动终端的使用限定在处理指定的业务；
d) 应对移动终端存储的敏感信息采取加密措施，并在未授权情况下不可读；
e) 应采用专用终端发布直播数据；
f) 当移动终端在与外部设备或应用进行数据交换时，应采取认证和加密措施；
g) 应采取相应的防丢失和防破坏的技术措施限制移动终端的物理访问；
h) 应对移动终端操作系统和应用程序的安全性，定期进行漏洞扫描和安全更新；
i) 应采取技术措施对移动终端进行监控和管理，包括设备定位、远程擦除数据、远程锁定设备等；
j) 应建立完善的移动终端管理制度，包括设备采购、登记、使用、维修、报废等环节的管理要求；
k) 应定期对移动终端进行安全检查和安全审计。

9.3.2.2 移动应用管控

移动应用管控要求如下：

a) 应具备选择应用软件安装、运行的功能；
b) 应依据指定证书签名的应用软件进行安装和运行；
c) 应根据软件白名单功能控制应用软件的安装和运行；
d) 应具备接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力；
e) 应采取相应的加密和数据保护措施，实现移动应用软件的数据安全；
f) 应建立完善的移动应用软件管理制度，包括软件的采购、测试、发布、更新等环节的管理要求；
g) 应采取技术措施对移动应用软件进行监控和管理，包括软件的安装、卸载、运行等环节的控制和管理；
h) 应采用专用移动应用软件防止二次打包工具篡改程序文件，以及防止移动应用程序的代码、图片、配置、布局等被增加、修改或删除；
i) 应根据实际业务采用专用移动应用软件对移动应用上传文件的类型、大小进行限制；
j) 应建立移动应用软件的测试、审核和发布机制；
k) 应定期对移动应用软件进行安全检查和审计。

9.4 挂载设备安全要求

9.4.1 安全物理环境

安全物理环境要求如下：

a) 应选择在不易受自然灾害和人为破坏的区域安装多功能智能杆；
b) 应对多功能智能杆及其挂载设备进行加固处理，防止被盗或被破坏；
c) 应对多功能智能杆及其挂载设备设置明显的警示标识；

d） 应对多功能智能杆及其挂载设备安装防雷击装置；
e） 应将挂载设备安装在能正确反映所处物理环境状态的位置；
f） 应将挂载设备安装在不影响挂载设备正常工作的位置；
g） 应将挂载设备的气象传感器和温湿度传感器安装在阳光不直接照射的区域；
h） 应对交通信号灯、通信基站、激光雷达、边缘控制器和智能照明等挂载设备采用长时间工作的供电装置；
i） 在可能存在静电风险的环境中，应对多功能智能杆及其挂载设备采取防静电措施。

9.4.2 安全区域边界

9.4.2.1 接入控制

接入控制要求如下：
a） 应设置安全区域边界的划分，并根据安全等级和安全需求进行合理配置；
b） 应采取技术措施对安全区域边界进行接入控制和管理，包括物理隔离、访问控制、监测和审计等；
c） 挂载设备接入控制采用的接口要求如下：
1） RJ45 以太网通信接口，单个接口通信速率不应低于 1000 Mbps；网络层应采用 IP 协议，并支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，当挂载设备为客户端，边缘控制器为服务端时，挂载设备应支持对多个服务端传输数据；
2） COM 应支持 RS-232（DB9）或 RS-485；
3） 挂载设备为摄像机，当具有视频监控功能时，接口协议应符合 GB/T 28181 的要求；
4） 挂载设备为摄像机，当具有视频图像信息采集功能时，接口协议应符合 GA/T 1400.4—2017 中 5.2 的要求。
d） 应对挂载设备进行监控和数据采集，实现设备的远程管理和控制；
e） 应对挂载设备采取加密传输和身份认证等安全防护措施；
f） 应对挂载设备建立完善的接入控制管理制度，包括设备接入的条件、流程和审批权限等。

9.4.2.2 安全控制

安全控制应符合7.4.2.2的要求。

9.4.2.3 入侵防范

入侵防范要求如下：
a） 应限制与挂载设备通信的目标地址，防止对陌生地址的攻击行为；
b） 应限制与边缘控制器通信的目标地址，防止对陌生地址的攻击行为；
c） 应定期更新系统和软件漏洞补丁，及时修复已知漏洞，降低被攻击的风险；
d） 应检测非授权无线接入设备和非授权移动终端的接入行为；
e） 应通过配置无线接入设备的认证策略防止多个 AP 使用同一个认证密钥；
f） 应检测针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
g） 应检测无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
h） 应自动阻断非授权无线接入设备或非授权移动终端的接入，并发出警告或提示信息，及时通知管理员进行处理；
i） 应检测虚拟机与宿主机、虚拟机与虚拟机之间的异常流量，及时发现异常行为并采取相应措施。

9.4.3 安全计算环境

9.4.3.1 挂载设备安全

挂载设备安全要求如下：

a) 应采取只有经过授权的用户才可以对挂载设备的软件应用进行配置或变更的措施；
b) 应对所有用户进行身份标识和鉴别，只有通过身份认证的用户才能访问挂载设备；
c) 应对挂载设备连接的边缘控制器（包括读写器）进行身份标识和鉴别；
d) 应对挂载设备连接的其他设备（包括路由器）进行身份标识和鉴别；
e) 应对不同等级用户的身份和权限，设置其对挂载设备的不同访问权限；
f) 应采用相应的加密技术和校验机制，对挂载设备的数据进行加密和校验；
g) 应建立安全审计机制，对挂载设备的访问和使用进行记录和监控；
h) 应对挂载设备使用的软件进行定期的漏洞扫描和安全更新，及时修复软件漏洞和安全隐患。

9.4.3.2 边缘控制器安全

边缘控制器安全要求如下：

a) 应对边缘控制器的访问进行身份标识和鉴别；
b) 应对合法连接设备（包括挂载设备、路由节点、数据处理中心）进行标识和鉴别；
c) 应根据不同等级用户的身份和权限，设置其对边缘控制器的不同访问权限；
d) 应过滤非法挂载设备和伪造挂载设备所发送的数据；
e) 应授权用户在挂载设备使用过程中对关键密钥进行在线更新；
f) 应授权用户在挂载设备使用过程中对关键配置参数进行在线更新；
g) 应采用加密技术和校验机制，对边缘控制器上的数据进行加密和校验；
h) 应建立安全审计机制，对边缘控制器的访问和使用进行记录和监控。

9.4.3.3 抗数据重放

抗数据重放要求如下：

a) 应通过时间戳和序列号等方式，对接收的数据进行新鲜性检查，防止历史数据被重放攻击；
b) 应通过数据校验方式，鉴别历史数据的非法修改；
c) 应通过对缓存数据进行严格的管理和控制，防止被恶意利用或重放；
d) 应对所有数据操作进行审计和监控，及时发现和处理异常行为或重放攻击。

9.4.3.4 数据融合处理

数据融合处理要求如下：

a) 应对不同来源和不同格式的挂载设备数据进行融合处理，使不同种类的数据可以在同一个平台被使用；
b) 应对不同数据之间的依赖关系和制约关系等进行智能处理；
c) 应对挂载设备数据进行去重处理，使每个数据项只被处理一次，防止重复数据处理带来的冗余和误差；
d) 应将不同数据源的数据进行关联分析，找出数据之间的潜在联系和规律，为后续的数据利用提供有价值的信息；
e) 应采取对敏感数据进行脱敏处理和加密存储等措施，防止挂载设备数据泄露和滥用；
f) 应具备一定的容错能力，使挂载设备数据在损坏或丢失的情况下，保持数据处理的有效性；
g) 应制定统一的数据格式和接口标准等，使不同系统之间能够进行有效的数据交换和处理。

9.4.4 安全运维管理

安全运维管理要求如下：

a) 应实施供应链风险管理策略，使挂载设备的安全性从供应链开始一直到运行过程中都得到保障；
b) 应指定人员定期巡视挂载设备和边缘控制器的安装环境，对影响挂载设备和边缘控制器正常工作的环境异常进行记录和处理；
c) 应对挂载设备和边缘控制器的入库、存储、部署、携带、维修、丢失和报废等进行全过程管理；
d) 应使用强密码或证书验证挂载设备的身份，防止未经授权的连接和访问；
e) 应实施访问控制策略，只有经过授权的设备才可以执行特定的操作；
f) 应从受信任的来源获取固件和软件，并定期更新挂载设备的固件和软件；
g) 应建立漏洞管理流程，定期扫描挂载设备，及时发现安全漏洞和修补已知的漏洞，并对未知漏洞采取措施以降低风险；
h) 应定期备份挂载设备的配置和数据，在需要时能够迅速恢复；
i) 应安装监控系统实时监视挂载设备的活动和网络流量，并建立事件响应计划；
j) 应对挂载设备边缘控制器的安装位置进行保密性管理。

9.5 公共数据基本安全要求

公共数据基本安全应符合6.5的要求。

9.6 公共数据四级增强安全要求

9.6.1 数据收集四级增强安全要求

数据收集四级增强安全要求如下：

a) 应对数据收集过程中的网络环境、系统进行安全评估；
b) 应检查收集数据的来源是可靠和受信任的，防止收集到伪造或篡改过的数据；
c) 在数据收集过程中，应实施严格的权限管理和身份验证机制；
d) 应对收集到的数据进行分类和标记，以便于后续的数据处理、存储和使用。根据数据的敏感程度和重要程度，采取不同的安全措施；
e) 应在数据传输过程中采用加密技术对数据进行加密，并定期更新传输协议和加密算法，以应对潜在的安全威胁；
f) 在收集数据时，应进行数据备份并保存在安全的环境中，以便于在意外情况下能够恢复数据；
g) 在数据收集过程中，应建立应急响应与处置机制，制定详细的安全事件应急预案，以应对突发性的安全事件；
h) 应对数据收集过程进行全面监控和审计，并定期进行安全审计和评估，及时发现和处理潜在的安全风险。

9.6.2 数据存储四级增强安全要求

数据存储四级增强安全要求如下：

a) 应具备异地实时备份功能，利用通信网络将数据实时备份至备份场地；
b) 应建立勒索病毒事前预警、事中阻断及事后恢复的保障机制；
c) 应提供数据处理环节关联信息系统的热冗余；

d) 应建立异地灾难备份中心，提供数据的实时切换。

9.6.3 数据传输四级增强安全要求

数据传输四级增强安全要求如下：

a) 应对关键网络传输线路及核心设备实施冗余备份；
b) 应对重要数据采取不通过离线或即时的通信方式进行传输；
c) 应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

9.6.4 数据使用四级增强安全要求

数据使用四级增强安全要求如下：

a) 应采取技术措施使汇聚大量数据时不暴露敏感信息；
b) 应对不同数据使用场景采取数字水印等技术，实现数据防泄密及溯源能力；
c) 应对接入或嵌入的第三方应用加强数据安全管理；
d) 应对接入或嵌入的第三方应用进行技术检测，使其数据处理行为符合双方约定要求；
e) 应对审计发现超出双方约定的行为及时停止接入。

9.6.5 数据加工四级增强安全要求

数据加工四级增强安全要求如下：

a) 应对数据加工的过程进行评估和监控，并对异常数据的操作行为及时预警和处置；
b) 应对数据加工的结果进行评估和安全审核，防止新数据发生泄露的风险；
c) 应提供安全的数据加工环境（包括网络环境和终端环境等），防止加工过程导致数据泄露和数据破坏等安全风险；
d) 应对加工重要数据的过程进行访问控制，并建立登记、审批机制和留存记录。

9.6.6 数据开放共享四级增强安全要求

数据开放共享四级增强安全要求如下：

a) 应建立公共数据内部审批机制，包括数据对外共享目的、范围、期限和频次等内容；
b) 应制定统一的数据交换标准和技术规范，促进不同系统之间的数据共享和交互；
c) 应建立开放的元数据标准，方便用户对数据进行整合和使用，支持数据的自由流通和利用；
d) 应采用多方安全计算、动态加密和数字水印等技术，防止数据泄露和被非法获取，实现数据共享的安全性；
e) 在开放共享数据时，对个人敏感信息的处理应遵循相关法律法规，防止数据滥用和侵犯个人隐私；
f) 数据的提供者和管理者应保持数据的持续性和可用性，及时更新数据并维护数据的完整性；
g) 应对数据的开放共享进行审计和监督。建立完善的审计机制，对数据的开放和使用进行记录和监控。

9.6.7 数据交易四级增强安全要求

数据交易四级增强安全要求如下：

a) 数据的获取、使用、共享和交易应在法律和监管框架内进行；
b) 数据交易应采取安全措施保护数据的安全性和保密性；
c) 数据交易应遵循统一的技术标准和互操作性原则，方便数据的交换和整合；

d） 交易的各方应对数据的收集、使用和共享过程有清晰的了解和理解；
e） 交易的数据应经过清洗、去重和整合等处理过程；
f） 应建立可追溯性和可审计性机制，对数据的来源、交易过程和使用情况进行记录和监控；
g） 应建立有效的争议解决机制（如协商、调解、仲裁等），帮助双方解决数据交易的争议。

9.6.8 数据出境四级增强安全要求

数据出境四级增强安全要求如下：
a） 应根据跨境数据的重要性和敏感程度，对跨境数据进行分类管理；
b） 应对跨境数据中的高敏感度信息采取严格的安全措施（如加密传输和存储、访问控制等）；
c） 应采取访问控制、权限管理、审计跟踪等安全措施，限制对跨境数据的访问和使用权限；
d） 应对跨境数据的存储采取安全措施（如数据加密存储、访问控制、安全审计等），防止跨境数据被未经授权的访问、篡改或泄露；
e） 应对跨境传输过程中的数据进行加密，并定期更新跨境传输协议和加密算法，防止潜在的安全威胁；
f） 应对跨境数据定期进行安全审查和风险评估，及时发现和处理潜在的安全风险。

9.6.9 数据销毁与删除四级增强安全要求

数据销毁与删除四级增强安全要求如下：
a） 应在中华人民共和国境内对介质存储的数据进行销毁或删除；
b） 应对存储数据的介质或物理设备采取无法恢复的方式进行数据销毁与删除，如物理粉碎、消磁、多次擦写等；
c） 应使用专业的数据恢复工具对销毁的数据进行检测，验证销毁的数据已经被彻底删除；
d） 应建立应急响应与处置机制，及时处置数据销毁或删除过程中突发性的安全事件。

附 录 A
（规范性）
安全要求的选择和使用

A.1 保护对象的差异

A.1.1 保护对象的重要性不同

在网络安全等级保护中，保护对象的重要性越高，其安全保护的要求也越高。对于关键信息基础设施，由于其承载着国家重要数据和业务，涉及国家安全和社会稳定，应采取更加严格的安全保护措施。

A.1.2 保护对象的范围不同

网络安全等级保护涉及的保护对象范围很广，包括信息系统、网络、终端设备、数据等。不同等级的保护对象面临的威胁和攻击的来源、方式和频率也不同，应根据具体情况制定相应的安全保护策略和措施。

A.1.3 保护对象的脆弱性不同

不同的保护对象具有不同的脆弱性，容易受到不同程度的威胁和攻击。某些系统可能更容易受到DDoS攻击，而其他系统则可能更容易受到病毒或恶意软件的攻击。应根据保护对象的脆弱性制定相应的安全保护措施。

A.1.4 保护对象的合规性要求不同

不同等级的保护对象应满足不同的合规性要求。对于三级信息系统，除应满足相关法律法规的要求外，还应进行定期的监督和检查；对于四级信息系统，除应满足三级信息系统的要求外，还应进行定期的审查和评估。

A.2 定级结果的组合

等级保护对象定级后，相对应定级结果的组合应符合表A.1的规定。

表 A.1 等级保护对象定级结果的组合

安全保护等级	定级结果的组合
第一级	S1A1
第二级	S1A2，S2A2，S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A5，S5A4，S5A3，S5A2，S5A1

A.3 保护措施的选择

安全保护措施的选择应依据上述定级结果，进一步细分为下列类别：

a) 保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为S）；

b) 保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务确保类要求（简记为A）；
c) 其他安全保护类要求（简记为G）。

A.4 安全要求的标识

所有安全管理要求均标注为G，安全要求及属性标识应符合表A.2的规定。

表A.2 安全要求及属性的标识

技术管理	分类	安全控制点	属性标识
安全技术要求	安全物理环境	物理位置选择	G
		物理访问控制	G
		防盗窃和防破坏	G
		防雷击	G
		防火	G
		防水和防潮	G
		防静电	G
		温湿度控制	G
		电力供应	A
		电磁防护	S
	安全通信网络	网络架构	G
		通信传输	G
		可信验证	S
	安全区域边界	边界防护	G
		访问控制	G
		入侵防范	G
		可信验证	S
		恶意代码防范	G
		安全审计	G
	安全计算环境	身份鉴别	S
		访问控制	S
		安全审计	G
		可信验证	S
		入侵防范	G
		恶意代码防范	G

表 A.2　安全要求及属性的标识（续）

技术管理	分类	安全控制点	属性标识
安全技术要求	安全计算环境	数据完整性	S
		数据保密性	S
		数据备份恢复	A
		剩余信息保护	S
		个人信息保护	S
		业务连续性保障	A
		系统管理	G
		审计管理	G
		安全管理	G
		集中管控	G
		安全策略	G
		管理制度	G
		制定和发布	G
		评审和修订	G
安全管理要求	安全管理机构	岗位设置	G
		人员配备	G
		授权和审批	G
		沟通和合作	G
		审核和检查	G
	安全管理人员	人员录用	G
		人员离岗	G
		安全意识教育和培训	G
		外部人员访问管理	G
	安全建设管理	定级和备案	G
		安全方案设计	G
		产品采购和使用	G
		自行软件开发	G
		外包软件开发	G
		工程实施	G
		测试验收	G

表 A.2　安全要求及属性的标识（续）

技术管理	分类	安全控制点	属性标识
安全管理要求	安全建设管理	系统交付	G
		等级测评	G
		服务供应商选择	G
		环境管理	G
		资产管理	G
		介质管理	G
		设备维护管理	G
		漏洞和风险管理	G
		网络和系统安全管理	G
		恶意代码防范管理	G
		配置管理	G
		密码管理	G
		变更管理	G
		备份与恢复管理	G
		安全事件处置	G
		应急预案管理	G
		外包运维管理	G
		重要保障期管理	G

A.5　安全要求的选择

安全要求的选择如下：

a) 应根据等级保护对象的级别选择安全要求，第一级选择第一级安全要求，第二级选择第二级安全要求，第三级选择第三级安全要求，第四级选择第四级安全要求，以此作为出发点；
b) 应根据系统服务确保性等级选择相应级别的系统服务确保类（A 类）安全要求；
c) 应根据业务信息安全性等级选择相应级别的业务信息安全类（S 类）安全要求；
d) 应根据系统安全等级选择相应级别的安全通用要求（G 类）；
e) 应针对不同单位或不同对象的特点，分析可能在某些方面的特殊安全保护能力要求，选择较高级别的安全要求；
f) 对于本文件中提出的安全要求无法实现或有更加有效的安全措施可以替代的，应根据定级结果，基于表 A.1 和表 A.2 可以对安全要求进行调整。

A.6　安全要求的调整和补充

A.6.1　组织应分析实际情况和安全需求，依据其他相关安全标准，对安全要求进行调整和补充。

A.6.2　组织根据以下方面调整和补充安全要求：

a) 业务安全需求：应根据组织业务的特殊性，制定符合业务需求的安全要求，使业务正常运行和数据安全；
b) 技术发展趋势：组织应关注新技术的发展趋势，及时调整和补充安全要求，防止新的安全威胁和攻击手段；
c) 风险评估结果：组织应定期进行风险评估，分析保护对象面临的安全威胁和风险。根据风险评估结果，组织应针对性地调整和补充安全要求，加强对薄弱环节的保护；
d) 组织管理需求：组织应根据自身的管理模式和流程，制定符合组织特点的安全管理要求，使安全管理措施得到有效实施；
e) 相关法规和标准：组织应关注相关法规和标准的更新，及时了解最新的安全要求和合规性要求，并将其融入组织的安全保护体系中。

附 录 B
（规范性）
等级保护对象整体安全保护能力的要求

B.1 总体要求

网络安全等级保护的核心，应根据不同安全保护等级的对象选择相适应的安全保护能力。第5章提出了不同级别的等级保护对象的安全保护能力要求，第6章～第9章分别针对不同安全保护等级的对象应具有的安全保护能力提出了相应的安全要求。

B.2 安全措施要求

B.2.1 构建纵深的防御体系

在采取由点到面的各种安全措施时，应从技术和管理两个方面提出安全要求，整体上还应根据各种安全措施的组合从外到内构成一个纵深的安全防御体系。还应从通信网络、网络边界、局域网络内部、各种业务应用平台等各个层次，落实本文件中提到的各种安全措施，构建纵深的防御体系。

B.2.2 采取互补的安全措施

在将各种安全控制落实到特定等级保护对象中时，应根据各个安全控制之间的互补性，综合分析各个安全控制在层面内、层面间和功能间产生的连接、交互、依赖、协调、协同等相互关联关系，将各种安全控制措施共同综合作用于等级保护对象上，提升等级保护对象的整体安全保护能力。

B.2.3 确保一致的安全强度

应将安全功能要求（如身份鉴别、访问控制、安全审计、入侵防范等内容），分解到等级保护对象的各个层面；在实现各个层面安全功能时，应促使各个层面的安全功能保持强度一致。应防止某个层面安全功能的减弱导致整体安全保护能力在这个安全功能上的削弱。当要实现双因子身份鉴别时，应在各个层面均实现基于标记的访问控制，并确保标记数据在整个等级保护对象内部流动时标记的唯一性等。

B.2.4 建立统一的支撑平台

当采用密码技术和可信技术时，应建立统一的支撑平台。该平台应支持高强度身份鉴别、访问控制、数据完整性和数据保密性等安全功能的实现。

B.2.5 进行集中的安全管理

B.2.5.1 对较高级别的等级保护对象，应实现集中的安全管理、安全监控和安全审计。

B.2.5.2 集中管理中心是等级保护对象的安全管理核心，应负责集中管理各个安全控制组件。

B.2.5.3 应通过集中管理实现对各个安全控制组件的统一监控、审计和配置管理，提高安全管理的效率和效果。

B.2.5.4 集中管理中心要求如下：

a) 集中配置管理：应对各个安全控制组件进行集中配置管理，使各个安全控制组件符合统一的安全策略和标准；
b) 统一监控和审计：应对各个安全控制组件的运行状态进行实时监控和审计，及时发现和处理潜在的安全风险和问题；
c) 事件处置和响应：应对发生的安全事件进行快速处置和响应，协调各个安全控制组件采取相应的措施，防止事件的扩大和蔓延；

d) 安全策略管理：应制定和更新安全策略，并使各个安全控制组件实施这些策略；
e) 用户和权限管理：应对用户和权限进行集中管理，只有经过授权的人员能够访问和使用相关资源；
f) 报告和日志分析：应生成安全报告和日志分析结果，为组织的安全管理和决策提供支持。

附 录 C
（规范性）
等级保护安全框架和关键技术使用要求

C.1 总体要求

开展网络安全等级保护工作中应首先明确等级保护对象，多功能智能杆系统网络安全等级保护对象主要包括信息系统、挂载设备和数据资源；在确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。

C.2 工作内容要求

依据国家网络安全等级保护政策和规定，开展组织管理、体制建设、安全规划、安全监测、通报预警、应急处置、态势感知、能力建设、技术检测、安全可控、队伍建设、教育培训和经费保障等工作。

C.3 等级保护安全要求

等级保护安全要求的框架如图C.1所示。

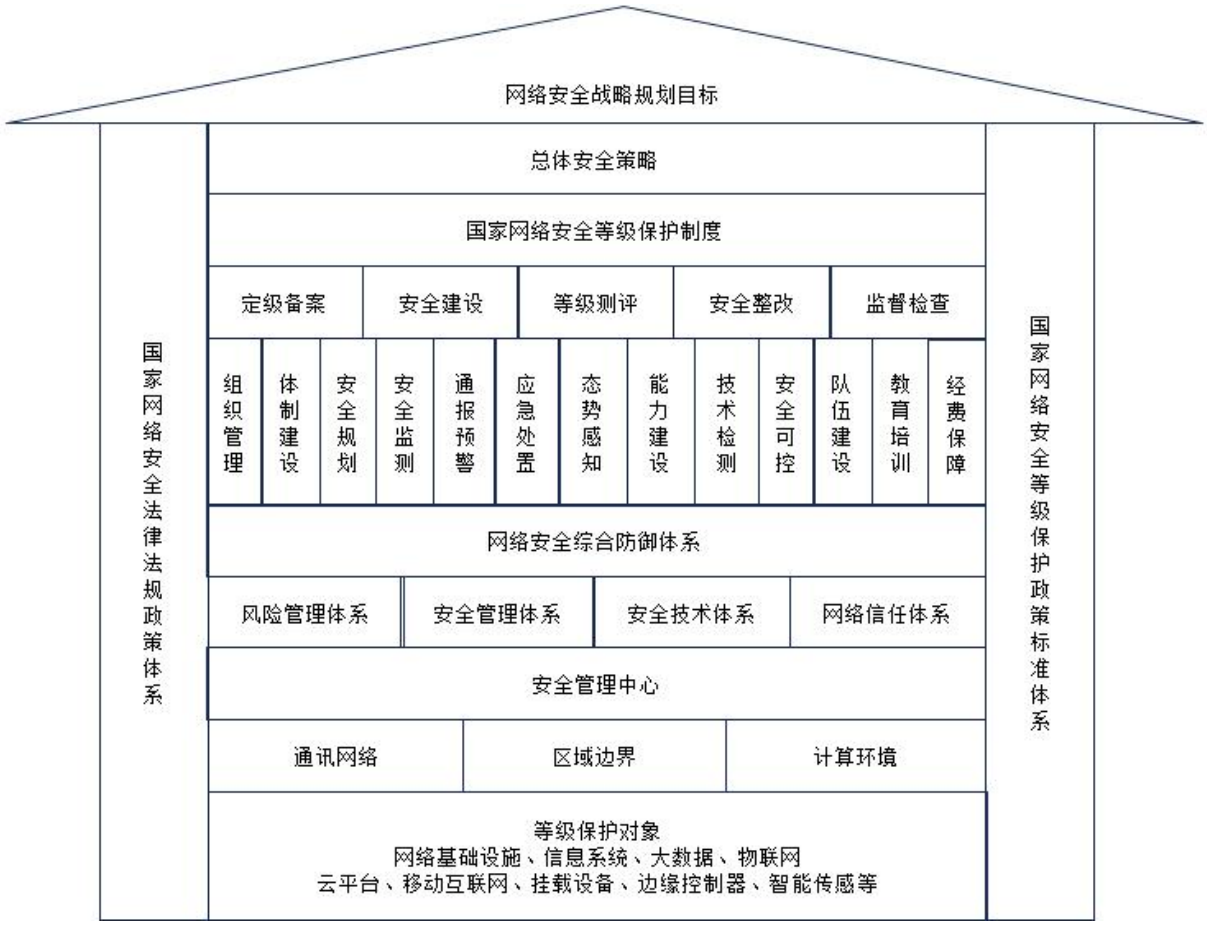


图 C.1 等级保护安全框架

C.4 关键技术使用要求

C.4.1 可信计算技术

应针对计算资源构建保护环境，以TCB为基础，实现软硬件计算资源可信；针对信息资源构建业务流程控制链，基于可信计算技术实现访问控制和安全认证，密码操作调用和资源的管理等，构建以可信计算技术为基础的等级保护核心技术体系。

C.4.2 强制访问控制技术

应在高等级保护对象中使用强制访问控制机制，强制访问控制机制应总体设计和全局考虑，在通信网络、操作系统、应用系统各个方面实现访问控制标记和策略，进行统一的主体和客体的安全标记，安全标记应随着数据全程流动，并在不同的访问控制点之间实现访问控制策略的关联，构建各个层面强度一致的访问控制体系。

C.4.3 审计追查技术

应在大量事件采集、数据挖掘、智能事件关联和基于业务的运维监控技术上，解决海量数据处理瓶颈。

应对审计数据快速提取，分析信息处理中对于检索速度和准确性的需求；同时，还应建立事件分析模型，及时发现高级安全威胁，并追查威胁路径和定位威胁源头，实现对攻击行为的有效防范和追查。

C.4.4 结构化保护技术

结构化保护技术要求如下：

a) 模块化设计：应将系统划分为多个独立的模块，使每个模块具有明确的功能和职责；
b) 层次化设计：应将系统的各个模块按照一定的层次进行组织和管理，防止攻击者对系统的垂直攻击，提高系统的抗渗透能力，在层次化设计中，上层模块可以调用下层模块的功能，而下层模块则不能直接访问上层模块；
c) 形式化描述：应对系统的功能和行为进行形式化描述，使系统的安全功能可以被精确地表述和验证；
d) 抗渗透增强：应利用各种安全技术（如加密技术、防火墙技术、入侵检测技术），增强系统的抗渗透能力，还应定期对系统进行安全漏洞扫描和安全审计，及时发现和修复潜在的安全风险；
e) 可信技术实现：应利用可信技术实现结构化保护，通过采用可信技术防止攻击者对系统的非授权访问和数据篡改等行为，提高系统的安全性。

C.4.5 多级互联技术

多级互联技术要求如下：

a) 安全性：在实现互联互通的过程中，应采取有效的安全措施来保护数据的机密性、完整性和可用性，防止未经授权的访问、泄露和破坏；
b) 异构性：由于不同等级的保护对象可能采用不同的技术架构、操作系统、应用程序等，应采用兼容和协调不同技术环境的互联机制，实现各等级之间的有效互操作；
c) 分布式资源共享和交互：应采用高效的资源管理和调度机制，提升资源共享和交互过程的安全性和可控性，使得各等级保护对象能够根据需要共享和交互数据、计算资源、存储资源等；

d) 动态性：随着业务需求和技术环境的变化，多级互联技术应具备动态调整和适应的能力，并根据实际情况快速调整和优化互联方案，以满足不断变化的需求；

e) 兼容性和扩展性：多级互联技术应能与其他安全技术、系统或平台进行集成，同时还应具备在未来不断引入新技术、新方法和新标准的能力。

附 录 D
（规范性）
管理平台应用要求

D.1 不同管理平台的服务模式架构图

D.1.1 SaaS

管理平台应为用户提供通过互联网访问和使用由第三方提供商在云上托管和管理的软件应用程序；在SaaS模式下，软件的所有管理包括：安装、配置、升级和维护，都由服务提供商负责。

D.1.2 PaaS

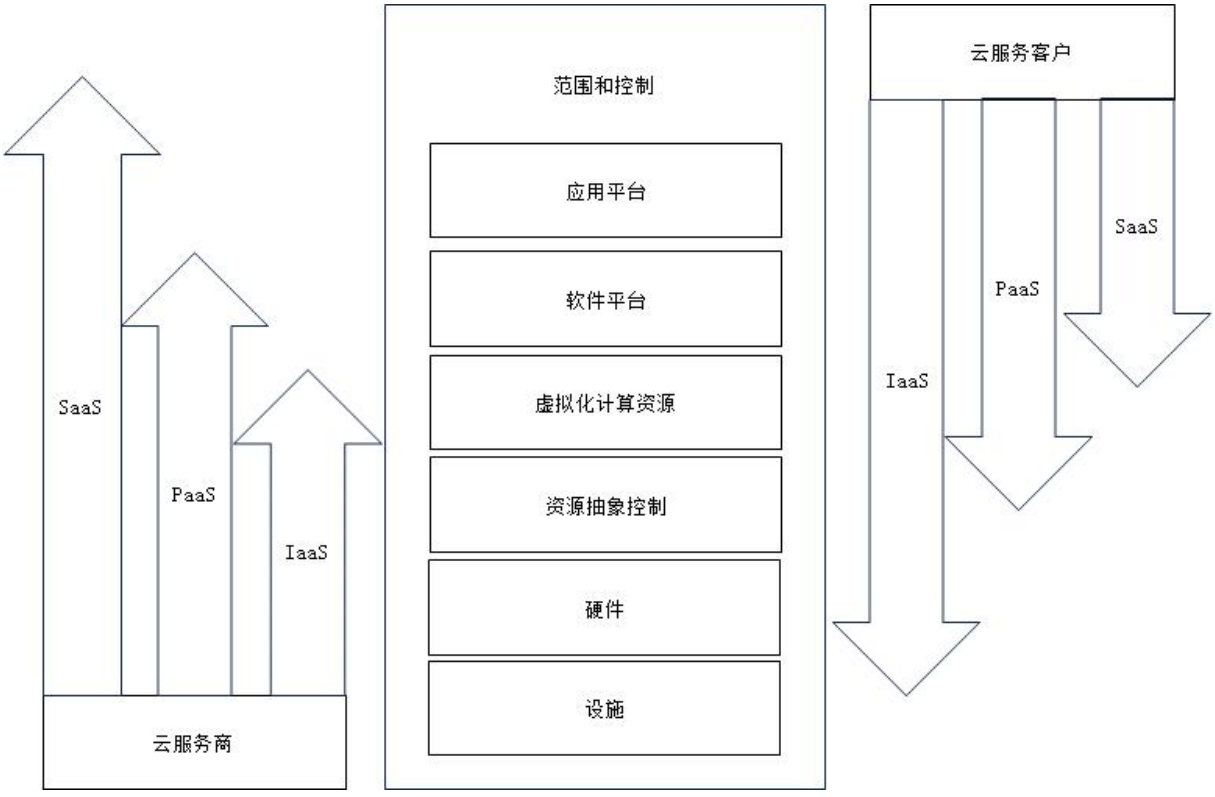
管理平台应为用户提供一个完整的开发和部署环境，使用户能够在这个环境中创建、测试、部署和管理应用程序；管理平台应包括开发工具、数据库服务、中间件、应用服务器、负载均衡器等。

D.1.3 IaaS

管理平台应为用户提供对虚拟化计算资源的访问，用户仅需负责安装、配置、管理、升级和维护他们的操作系统、中间件和应用程序。

D.1.4 服务模式架构图

不同管理平台的服务模式架构图见图D.1。



图D.1 不同管理平台的服务模式架构图

D.2 不同服务模式下管理平台的组成

D.2.1 在IaaS模式下，管理平台应由设施、硬件、资源抽象控制层组成。

D.2.2　在PaaS模式下，管理平台应由设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台组成。

D.2.3　在SaaS模式下，管理平台应由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件组成。

D.3　安全管理责任

D.3.1　SaaS模式

D.3.1.1　SaaS 模式下平台服务商的安全管理责任

SaaS 模式下平台服务商的安全管理责任如下：

a)　应提供和维护 SaaS 应用程序的安全性，包括数据存储和传输的安全；
b)　应对用户身份和访问控制进行管理，仅授权的用户可以访问 SaaS 应用程序；
c)　应提供数据备份和灾难恢复，以防止数据丢失；
d)　应保护用户数据的隐私和合规性。

D.3.1.2　SaaS 模式下平台服务客户的安全管理责任

SaaS 模式下平台服务客户的安全管理责任如下：

a)　应对用户身份和访问控制进行管理，仅授权的员工可以使用 SaaS 应用程序；
b)　应按照 SaaS 应用程序的使用政策和规定，包括数据使用和分享的规则；
c)　应监控员工在 SaaS 应用程序中的活动，及时检测和应对异常行为；
d)　应对应用程序中的敏感数据采取保护和加密；
e)　应遵守公司内部的安全政策和合规性要求。

D.3.2　PaaS模式

D.3.2.1　PaaS 模式下平台服务商的安全管理责任

PaaS 模式下平台服务商的安全管理责任如下：

a)　应建立 PaaS 平台的安全性措施；
b)　应对用户身份和访问控制进行管理，仅授权的开发人员可以访问平台；
c)　应对管理应用程序容器进行隔离和资源管理；
d)　应监控 PaaS 平台的可用性和性能，以检测潜在问题和风险。

D.3.2.2　PaaS 模式下平台服务客户的安全管理责任

PaaS 模式下平台服务客户的安全管理责任如下：

a)　应编写和实施包括防止常见安全漏洞的应用程序代码；
b)　应对用户身份和访问控制进行管理，仅授权的用户可以使用应用程序；
c)　应监控应用程序日志和活动，及时检测和应对安全事件；
d)　应对应用程序中的敏感数据采取保护和加密；
e)　应遵守应用程序开发和部署的安全最佳实践。

D.3.3　IaaS模式

D.3.3.1　IaaS 模式下平台服务商的安全管理责任

IaaS 模式下平台服务商的安全管理责任如下：

a)　应提供和维护云基础设施的物理安全，包括数据中心和网络设备；

b) 应采用虚拟机之间的隔离，管理虚拟化平台的安全性；
c) 应采用防火墙和 VPN 提供网络安全功能；
d) 应采用操作系统和应用程序的更新提供虚拟机映像的安全性；
e) 应监控云基础设施的可用性和安全性，以检测潜在威胁。

D.3.3.2 IaaS 模式下平台服务客户的安全管理责任

IaaS 模式下平台服务客户的安全管理责任如下：

a) 应采用安装安全补丁和配置安全设置，管理操作系统和应用程序的安全性；
b) 应对用户身份和访问控制进行管理，仅授权的用户可以访问虚拟机；
c) 应监控虚拟机和应用程序的日志，及时检测和应对安全事件；
d) 应管理数据的加密和备份，以保护敏感数据。

附 录 E
（规范性）
移动互联应用场景要求

E.1 移动互联应用场景架构

移动互联应用场景架构见图 E.1。

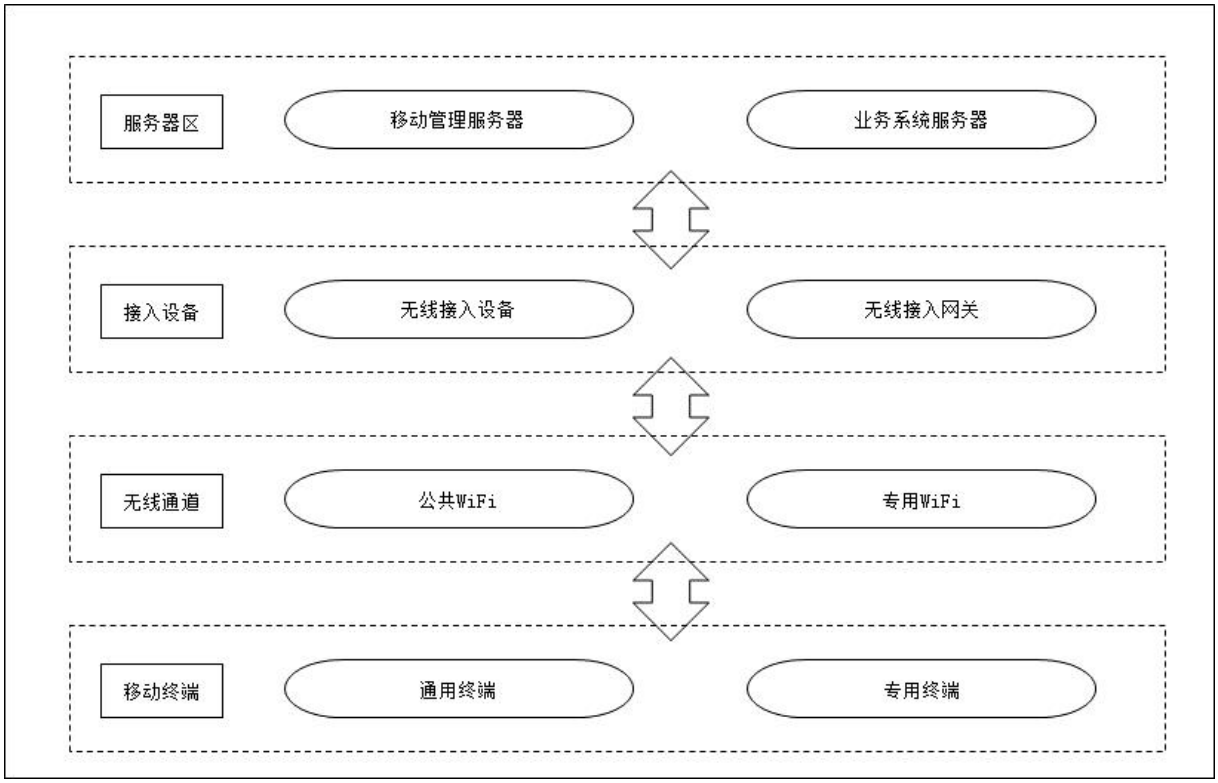


图 E.1 移动互联应用场景架构

E.2 移动互联应用场景安全扩展要求

移动互联应用场景安全扩展要求如下：

a) 数据加密：应对所有敏感数据进行加密处理，包括采用对称加密方式或非对称加密方式，防止被黑客窃取或篡改；
b) 安全认证：应采用短信验证码认证、用户名密码认证、指纹识别认证等方式对用户身份进行验证，使只有合法用户才能访问移动应用程序；
c) 移动终端管控：应采用设备标识、设备安全设置、应用程序安装与卸载等方式对移动终端进行管理和控制；
d) 移动应用管控：应采用应用安全设置、应用数据安全和应用权限管理等方式对移动应用进行管理和控制；
e) 移动应用软件的采购：应选择有信誉和良好声誉的移动应用软件供应商，并要求供应商提供有关其安全措施和流程的详细信息。

附 录 F
（规范性）
挂载设备应用场景要求

F.1 多功能智能杆应用场景

多功能智能杆通过挂载设备实现外部环境感知功能，挂载设备应根据其设备功能进行具体部署。通常采用三层设计，杆体分为顶部、中部和底部，杆体挂载设备符合如下要求：

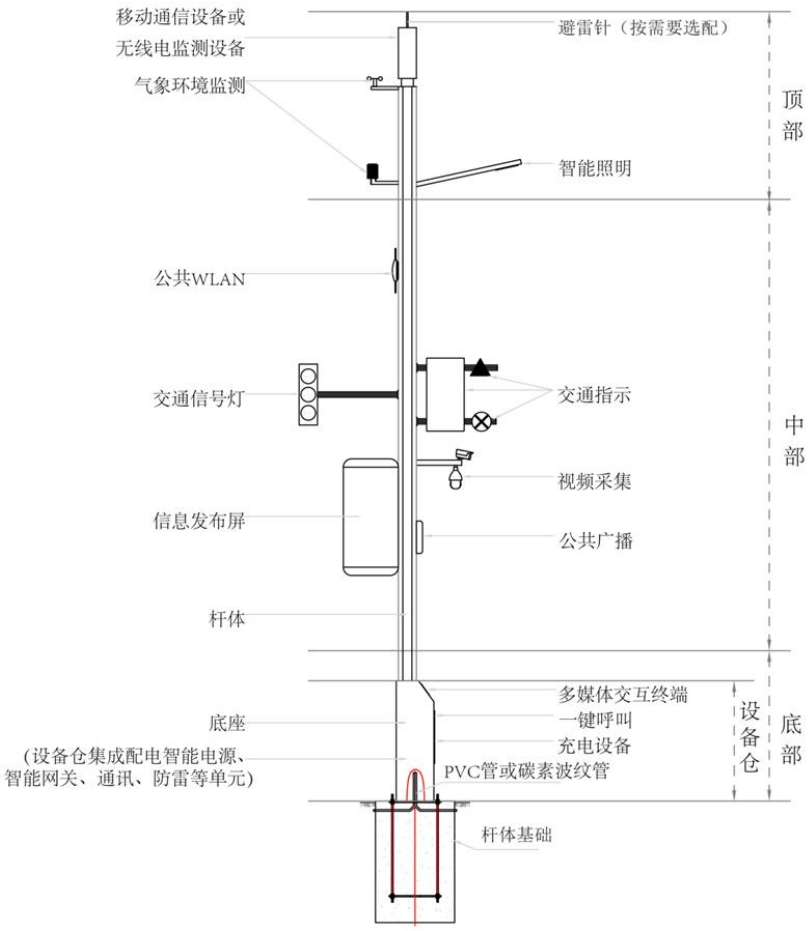
a) 第一层（底部）：宜配置人行信号灯、紧急呼叫、多媒体交互设备、防盗传感器、充电桩等，杆体底座宜安装综合箱，并配置检修门，高度在 2.5 m 以下；

b) 第二层（中部）：宜配置视频安防设备、信息发布屏、机动车信号灯、道路交通标志、公共广播设备等，根据需要设置横杆安装视频安防、交通信号灯等设备，高度范围在 2.5 m～8 m；

c) 第三层（顶部）：宜配置照明设备、移动通信基站、环境监测设备、气象监测设备等，高度在 8 m 以上。

F.2 多功能智能杆部件组成

多功能智能杆部件组成示意图见图 F.1。



图F.1 多功能智能杆部件组成示意图

F.3 管理平台架构

F.3.1 管理平台架构应分为感知层、平台层和应用层。

F.3.2 感知层应由网关实现设施的标准化接入、边缘计算和感知层应智能互联组成。

F.3.3 平台层应由物联网平台基础数字底座、大数据和人工智能平台、业务服务平台组成。

F.3.4 应用层应由智能运维、智慧场景、设施运营和数据运营组成。

F.3.5 管理平台的数据应对接接入城市物联网平台、城市大数据平台、主管部门业务系统等外部系统，平台与物联网之间的通信应使用安全的通信协议防止数据被窃取或篡改。

F.3.6 管理平台架构见图F.2。

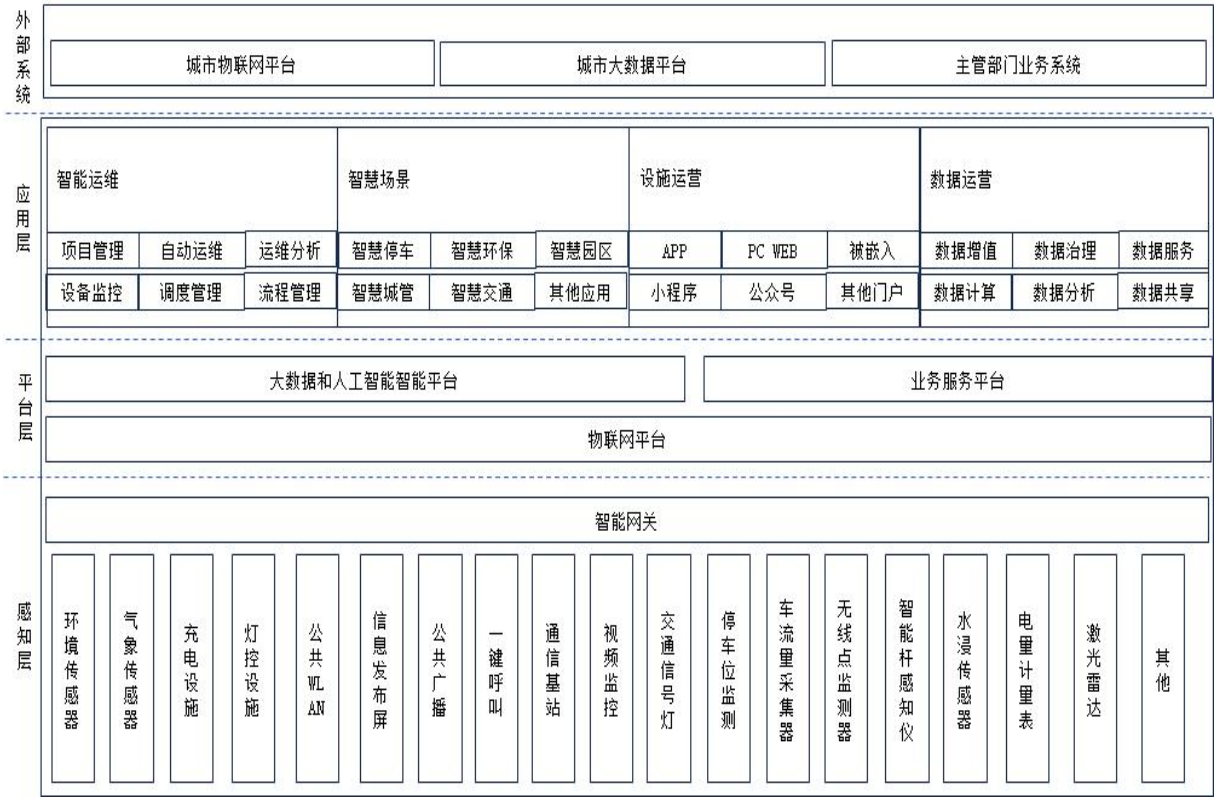


图 F.2 管理平台架构图

F.4 挂载服务

挂载服务见表F.1。

表 F.1 多功能智能杆挂载设备服务功能表

城市服务	基本功能	功能介绍
智慧照明	功能照明	挂载照明设备和智能照明管理设备通过智能化设计与精细化管控，支持路灯照明的智慧远程集中控制、自动调节等功能。
智慧通信	移动通信	挂载移动通信基站设备支持移动通信网络（4G/5G）的信号覆盖和容量提升。
	公共无线网	公共无线网络区域覆盖，用户可实现区域内接入网络。
	物联网通信	为物联网系统提供通信连接的功能。

表 F.1　多功能智能杆挂载设备服务功能表（续）

城市服务	基本功能	功能介绍
智慧安防	图像信息采集	通过监控摄像机采集图像信息，支持城市交通、公共安全服务的智能化管理和运行。
	电子信息采集	通过智能感知设备采集人员、物体等的电子信息，支持城市交通、公共安全服务的智能化管理和运行。
智慧交通	道路交通信号指示	由红、黄、绿三色（或红、绿两色）信号灯向车辆和行人发出通行或停止的交通信号。
	道路交通标志	指导道路使用者有序使用道路的交通标志指示信息，明示道路交通禁止、限制、通行状况、道路状况和交通状况等信息。
	道路交通智能化管理	通过挂载智能设备实现交通流信息、交通事件、交通违法事件等交通状态感知，支持道路交通智能化管理。
	车路协同	通过挂载道路环境的多源感知单元，与车载终端、蜂窝车联网管理平台等联合支持车路协同一体化交通体系。
智慧停车	高效便捷停车	通过将无线通信技术、移动终端技术、北斗定位技术等综合应用于城市停车位的采集、管理、查询、预定。实时更新、查询、预订、导航和服务实现停车位资源利用率的最大化。
智慧环保	环境、气象监测	挂载的环境监测装置应支持环境数据的监测采集，包括大气环境数据、气象环境数据和周边的建筑声光环境等。
智慧联动	互联互通	挂载设备通过边缘计算、物联网模块、分布式存储等实现互联互通。
智慧监测	杆体姿态	为多功能智能杆用电设备提供所需交流和直流供电；杆体姿态监测（加速度、倾斜）；负载用电量监测。
路边停车	路端停车管理	具备路边停车设备供电及网络交互功能，为中、低位视频桩或路牙摄像机等车牌识别设备、ETC 设备等提供用电及网络接口。
无人驾驶	车路协同应用支撑	提供辅助定位基站、数字化标志标牌、边缘计算 MEC 单元、毫米波雷达、激光雷达、边缘服务器设备安装与硬件及信号接口。
充电设备	设施应用支撑	具备双枪或单枪 220 V 交流电动汽车充电功能、电动自行车的充电功能、手机等移动终端充电功能。
智慧应急	特殊位置地段的应急监控	在特殊的位置地段，挂载边坡检测单元、水位检测单元、火灾检测单元。
其他	其他功能	支持公共信息导向、信息发布、能源供给服务、有/无轨电车供电线网。 具备无线电监测、一键呼叫等其他功能。

附 录 G
（规范性）
密码模块安全技术要求

G.1 安全一级

G.1.1 安全一级密码模块提供了最低等级的安全要求，至少应包括“软件/固件安全”“非入侵安全”“自测试”“敏感测试管理”4个安全领域的需要。
G.1.2 密码模块应使用一个核准的安全功能或核准的敏感安全参数建立方法。
G.1.3 应根据软件或固件模块的功能和重要性，选择适当的运行环境。对于关键的系统组件或安全相关的模块，应运行在不可修改或受限的环境中，以减少被攻击的风险。
G.1.4 安全一级硬件密码模块应达到产品级部件的基础要求，还应具备对各种攻击的缓解能力。在没有特殊的物理安全机制要求的情况下，硬件密码模块应建立安全机制防御非入侵攻击和其他潜在威胁。
G.1.5 由于安全一级密码模块本身并不具备物理安全防护能力，应根据物理密码模块和软件密码模块的特性和所面临的威胁分别设计和实施安全措施；物理密码模块应实施防篡改设计、环境监控和物理访问控制等安全措施；软件密码模块应实施代码安全性、运行时环境隔离和权限管理等安全措施。
G.1.6 安全一级密码模块的安全应由操作员负责。

G.2 安全二级

G.2.1 安全二级密码模块应在安全一级的基础上增加拆卸证据、基于角色的鉴别等功能要求。
G.2.2 硬件密码模块的拆卸证据应是拆卸存迹的涂层或封条，或在封盖或门上加防撬锁等手段以提供拆卸证据。
G.2.3 当通过物理方式访问模块内的安全参数时，模块上拆卸存迹的涂层或封条应破碎。
G.2.4 角色鉴别要求密码模块鉴别并验证操作员的角色，应确定其是否有权执行对应的服务。
G.2.5 安全二级硬件密码模块应具有拆卸证据，但不针对探针攻击。
G.2.6 当软件密码模块的逻辑保护由操作系统提供并且运行在可修改的环境中时，应选择基于角色的访问控制（RBAC）或自主访问控制（DAC）实施访问控制。
G.2.7 访问控制措施应防止非授权的执行、修改及读取实现密码功能的软件。
G.2.8 安全二级软件密码模块所在的进程，应由密码模块自己所有，并与调用者在内的其他进程逻辑隔离；应使用不依赖运行环境的安全机制，保护存储的敏感安全参数。

G.3 安全三级

G.3.1 安全三级密码模块在安全二级的基础上，应增强物理安全、身份鉴别、环境保护、非入侵式攻击缓解、敏感参数管理等安全机制。
G.3.2 安全三级密码模块应抵抗直接的探针攻击，且具备防拆卸外壳或封装材料的功能，当有门或盖的入侵，还应具备主动防护功能。
G.3.3 应实施基于身份的鉴别机制，增强基于角色的鉴别机制的安全性，使密码模块达到安全三级的要求。
G.3.4 密码模块应鉴别操作员的身份，并验证经鉴别的操作员是否被授权担任特定的角色及是否能够执行相应的服务。
G.3.5 安全三级要求手动建立的明文关键安全参数应经过加密处理，应使用可信信道或使用知识拆分来输入或输出。

G.3.6　安全三级的密码模块应具备防止电压和温度超范围运行的能力。

G.3.7　应通过环境失效测试（EFT）或具备环境失效保护（EFP）措施，使模块不会因环境异常而被破坏。

G.3.8　安全三级的密码模块应提供非入侵式攻击环境技术的有效性证据和测试方法。

G.4　安全四级

G.4.1　安全四级密码模块是最高安全等级，应在安全一级、安全二级、安全三级所有的安全特性基础上增加拓展特性。

G.4.2　安全四级的密码模块应提供完整的封套保护，在外部电源不供电的情况下，应能检测并响应所有非授权的物理访问。

G.4.3　应能检测从任何方向对密码模块外壳的破坏，并立即将所有未受保护的敏感安全参数置零。

G.4.4　应支持多因素身份鉴别，实施规定的非入侵式攻击的环境办法，并具备EFP和防止错误注入攻击的能力，防止因环境异常带来的安全威胁。

G.4.5　安全四级密码模块应能抵抗使用特制工具进行高强度长时间的攻击。

附 录 H
（规范性）
可信验证要求

H.1 功能框架

H.1.1 可信验证功能框架见图H.1。

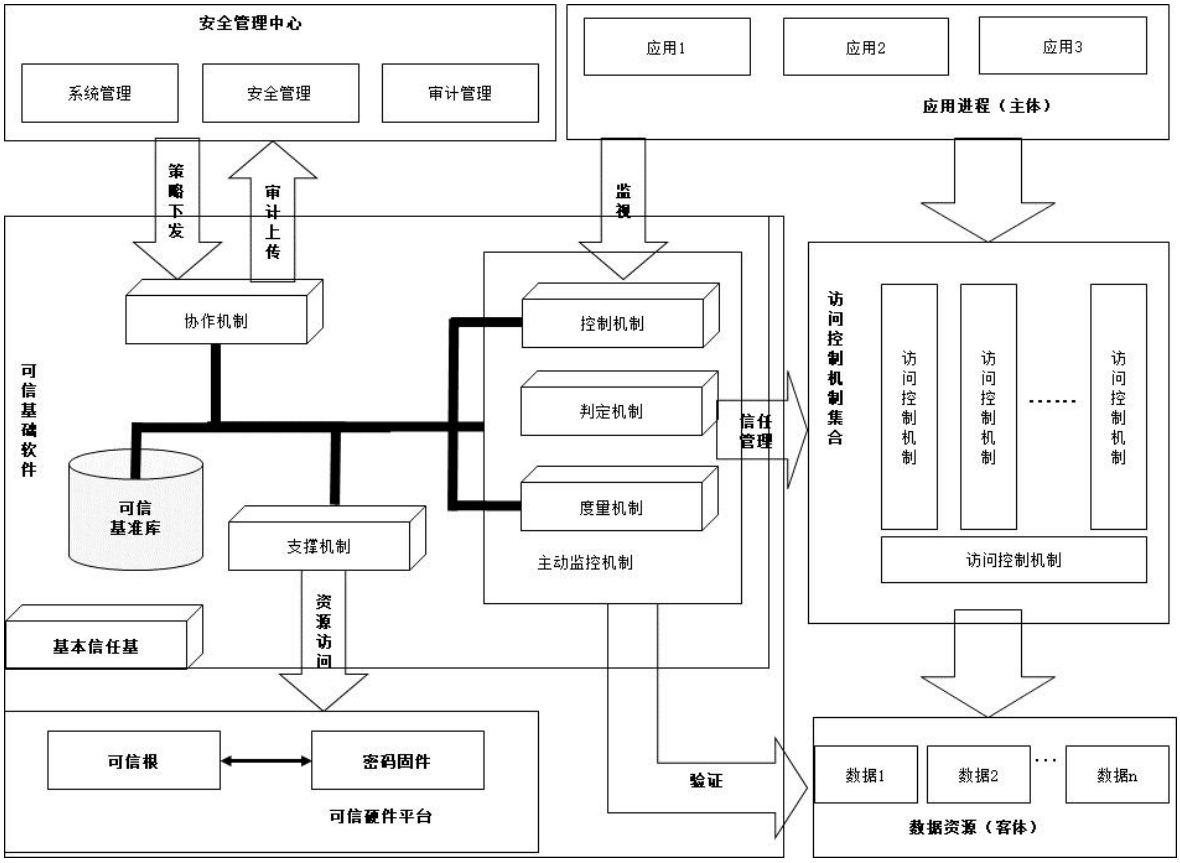


图 H.1 可信验证实现框架图

H.1.2 可信根内部应由密码算法引擎、可信裁决逻辑、可信存储寄存器等部件组成，应向节点提供可信度量、可信存储、可信报告等功能。

H.1.3 可信固件应内嵌在BIOS之中，用来验证操作系统引导程序的可信性。

H.1.4 可信基础软件应由基本信任基、可信支撑机制、可信基准库和主动监控机制组成。其中基本信任基应内嵌在引导程序之中，在节点启动时从BIOS中接过控制权，验证操作系统内核的可信性。可信支撑机制应向应用程序传递可信硬件和可信基础软件的可信支撑功能，并将可信管理信息传送给可信基础软件。

H.1.5 主动监控机制应实现对应用程序的行为监测，应判断应用程序的可信状态，并根据可信状态确定并调度安全应对措施。

H.1.6 主动监控机制根据其功能应包括控制机制、度量机制和决策机制。

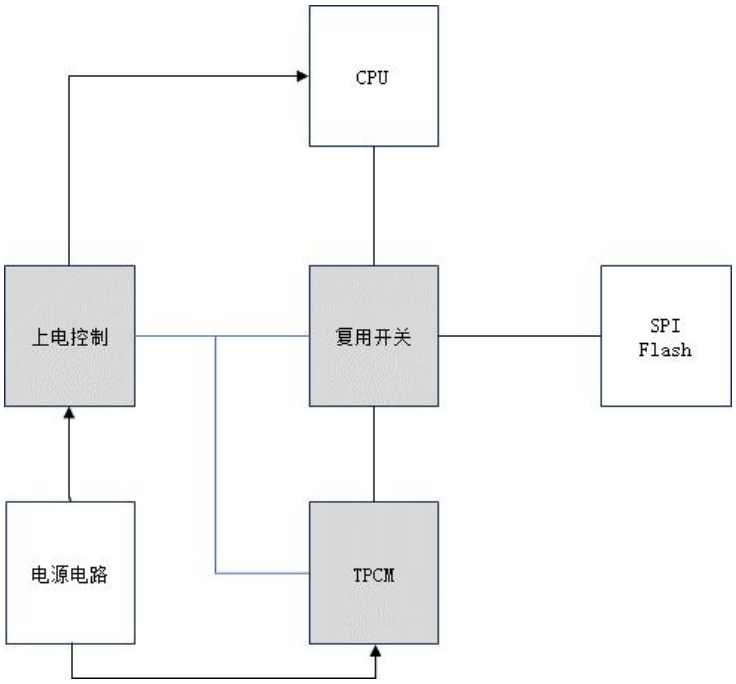
H.1.7 可信判定机制应依据度量结果和预设策略确定当前的安全应对措施，并调用不同的安全机制实施这些措施。

H.2 可信验证硬件改造示例

H.2.1 改造示例图

H.2.1.1 安全通信网络、安全区域边界、安全计算环境的各设备，在硬件系统引入可信根芯片（TPCM），应对设备硬件启动顺序逻辑进行改造，以实现可信验证功能。

H.2.1.2 设备硬件启动顺序逻辑改造示例图见图 H.2。



注： 图中深色的部分为需要增加的电路。

图 H.2 设备硬件启动顺序逻辑改造示例图

H.2.2 改造步骤

改造步骤如下：

a) 当系统上电启动时，应使 CPU 处于断电状态，并使可信芯片和电路正常上电进行验证；
b) 在可信芯片启动后，应对 SPI Flash 中的内容进行可信验证；
c) 应采用哈希值（Hash）校验的方式进行验证，应通过计算 SPI Flash 内容的哈希值，并与预先存储的可信哈希值进行比较，验证 SPI Flash 内容是否被篡改；
d) 当 SPI Flash 内容有更新时，应重新计算哈希值并更新可信哈希值，只有当验证结果符合预期时，才能确认 SPI Flash 内容是可信；
e) 当可信芯片验证 SPI Flash 内容是可信时，应通过上电控制电路对 CPU 进行供电后，才能实施启动并执行操作；
f) 在 CPU 获得供电后，复用开关应切换到 CPU，并使其能够访问 SPI Flash 中的数据和程序；
g) 可信芯片与 CPU 之间应通过 SPI 接口进行通信，并使 CPU 在执行关键操作时与可信芯片保持同步；
h) 可信芯片应通过操作系统内的可信软件基向安全管理中心报告日志和告警信息，以便及时发现和处理潜在的安全问题。

参 考 文 献

[1] DB4403/T 30—2019 多功能智能杆系统设计与工程建设规范