ICS 35.040
CCS L 80

DB4403

深　圳　市　地　方　标　准

DB4403/T XXX—XXXX

多功能智能杆　网络安全等级保护规范

Multifunctional smart pole—Basic requirements for network security level protection

（送审稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 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、信安软件测评认证中心（深圳）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　网络安全等级保护基本要求

1　范围

本文件规定了多功能智能杆网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求。

本文件适用于多功能智能杆网络分等级的非涉密对象的安全建设和监督管理。对于涉及国家秘密的网络，应按照国家保密工作部门的相关规定和标准进行保护。

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—2022　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 30428.7—2017　数字化城市管理信息系统　第7部分：监管信息采集

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 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

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

由杆体、综合箱和综合管道组成，与系统管理平台联网，挂载各类设施设备，提供城市管理与智慧化服务的城市公共设施。

[来源：GB/T 40994—2021，3.1，有修改]

3.2

多功能智能杆网络安全　network security of multifunctional smart pole

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

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 customers

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

虚拟机监视器 hypervisor

运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

[来源：GB/T 22239—2019，3.7]

3.8

宿主机 host machine

运行虚拟机监视器（3.7）的物理服务器。

[来源：GB/T 22239—2019，3.8]

3.9

移动互联 mobile communication

采用无线通信技术将移动终端接入有线网络的过程。

[来源：GB/T 22239—2019，3.9]

3.10

移动终端 mobile device

在移动业务中使用的终端设备，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]

3.11

无线接入设备 wireless access device

采用无线通信技术将移动终端（3.10）接入有线网络的通信设备。

[来源：GB/T 22239—2019，3.11]

3.12

无线接入网关 wireless access gateway

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

[来源：GB/T 22239—2019，3.12]

3.13

移动应用软件 mobile application

针对移动终端（3.10）开发的应用软件。

[来源：GB/T 22239—2019，3.13]

3.14

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。

3.15

外部网络 external network

多功能智能杆网络中等级保护对象之外的网络。

3.16

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]

3.17

敏感数据 sensitive data

包括但不限于未经多功能智能杆行政主管部门批准发布的行业统计数据、行业企事业经营数据、用户数据。

3.18

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]

3.19

挂载设备 mount equipment

挂载在多功能智能杆上，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。

3.20

边缘控制器 edge controller

将挂载设备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。

3.21

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）

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）
IT：信息技术（Information Technology）
PaaS：平台即服务（Platform as a Service）
SaaS：软件即服务（Software as a Service）
SSID：服务集标识（Service Set Identifier）
SSH：安全外壳（Secure Shell）
TCB：可信计算基（Trusted Computing Base）
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 网络安全等级保护

5.1 等级保护对象定级

5.1.1 等级保护对象是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息网络、管理平台、大数据系统、挂载设备、边缘控制器和采用移动互联技术的系统等。

5.1.2 等级保护对象根据其在国家安全、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，由低到高被划分为五个安全保护等级。

5.1.3 根据等级保护对象在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，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侵害程度等因素，等级保护对象由低到高被划分为以下五个安全保护等级：

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；
e) 第五级，等级保护对象受到破坏后，会对国家安全造成特别严重危害。

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：应能够防护免受来自个人的、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：应能够防护免受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免受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免受来自国家级别的、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。

5.2.5 第五级安全保护能力：略。

5.3 安全通用要求

5.3.1 由于多功能智能杆实业务目标的不同、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会以不同的形态出现，表现形式可能称之为基础信息网络、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。形态不同的等级保护对象面临的威胁有所不同，安全保护需求也会有所差异。为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护要求分为安全通用要求和安全扩展要求。

5.3.2 安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，应根据安全保护等级实现相应级别的安全通用要求；安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景选择性实现安全扩展要求。安全通用要求和安全扩展要求共同构成了对等级保护对象的安全要求。

5.3.3 安全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 一般要求

根据多功能智能杆的管理平台、移动互联、挂载设备、公共数据提出了安全扩展要求。对于采用其他特殊技术或处于特殊应用场景的等级保护对象，应在安全风险评估的基础上，针对安全风险采取特殊的安全措施作为补充。

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 公共数据安全原则

为规范公共数据安全的基本要求，防范和抵御数据可能面临的各类安全风险，公共管理和服务机构在处理数据过程中，应遵循下列原则，具体包括：

a) 合法正当原则：公共数据收集采取合法、正当的方式，不应窃取或者以其他非法方式获取数据，数据处理活动过程不应危害国家安全、公共利益，不应损害个人、组织的合法权益；
b) 权责明确原则：采取技术和其他必要的措施保障数据的安全，对数据处理活动中涉及的组织和个人的合法权益负责；
c) 目的明确原则：数据处理活动具有明确、清晰、具体的目的；
d) 明示同意原则：数据相关主体拥有对其个人信息的处理目的、方式、范围等规则的知情权，在进行数据处理活动前应向数据相关主体明示，并获得授权同意，法律、行政法规另有规定的例外情况，从其规定；
e) 最小必要原则：数据处理活动仅处理可满足特定公共服务为目的所需的最少数据类型和数量；
f) 公开透明原则：以明确、易懂和合理的方式公开个人信息处理的范围、目的、规则等，并接受外部监督，法律、行政法规另有规定的例外情况，从其规定；
g) 动态调整原则：数据安全等级随着数据对客体侵害程度的变化进行动态调整，数据重要程度、数据处理活动过程、数据安全管控措施等的变更可能引起数据对客体侵害程度的变化；
h) 全程可控原则：采取必要管控措施确保数据处理活动各环节的可控性，防止未授权访问及处理公共数据，记录数据处理活动各环节过程，记录内容清晰可追溯。

5.4.6 公共数据安全要求

5.4.6.1 承载公共数据的信息系统应按 GB/T 22239—2019 描述的基本要求，同步规划、建设、运营信息系统，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按 GB/T 39786—2021 描述的密码应用基本要求执行。

5.4.6.2 数据处理活动安全要求：数据处理活动围绕数据收集、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、数据销毁与删除 9 个过程，分级阐述公共数据安全要求。

5.4.6.3 当不同级别的数据同时被处理且无法精细化管控时，应“就高不就低”，按照数据对象安全等级最高的要求实施保护。公共数据安全等级与其安全要求的对应关系见表 1。

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、三级增强安全要求、四级增强安全要求
第五级	第五级为非常重要的监督管理对象，其安全要求不在本文件描述

5.5 密码模块安全要求

密码模块安全要求应符合附录 G 的规定。

5.6 安全管理要求

安全管理要求的内容、原则、策略、制度，机构建设、人员管理、风险控制和通用要求应符合 GB/T 20269—2006 的要求。

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

要求如下：

a) 应保证网络设备（包括边缘控制器）的业务处理能力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) 应配备与实际运行情况相符的网络拓扑图。

6.1.1.2 移动互联

移动互联在数据传输过程中，应使用安全协议和强加密算法对数据进行加密，并采用校验技术保证通信过程中数据的完整性。

6.1.1.3 可信验证

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

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。

6.1.2.2 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，默认情况下除允许通信外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，并保证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。

6.1.3 安全计算环境

6.1.3.1 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

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） 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

6.1.3.3 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

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

应采用校验技术保证重要数据在传输过程中的完整性，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等。

6.1.3.7 数据备份恢复

应提供重要数据的本地数据备份与恢复功能。

6.2 管理平台安全要求

6.2.1 安全通信网络

要求如下：

a） 应保证管理平台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

要求如下：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移；
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) 数据完整性和保密性应确保管理平台服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

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

应保证有线网络与无线网络边界之间的访问和数据流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，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

6.3.2 安全计算环境

移动应用的管控，应具有选择软件安装、运行的功能。

6.4 挂载设备安全要求

6.4.1 安全物理环境

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物理破坏，如挤压、强振动；
b) 挂载设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）。

6.4.2 安全区域边界

接入控制应保证只有授权的挂载设备可以接入，接入控制应采用通用的标准接口，并提供以下接口形式：

a) RJ45 或光纤以太网通信接口，单个接口通信速率不低于 1000M；网络层采用 IP 协议，支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，挂载设备为客户端，边缘控制器为服务端，挂载设备支持对多个服务端传输数据；
b) COM 串行通信接口，支持 RS-232（DB9）或 RS-485；
c) 挂载设备为摄像机，且具有视频监控功能时，接口协议应符合 GB/T 28181—2022 的规定；
d) 挂载设备为摄像机，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 中采集接口的规定。

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 公共数据安全要求

6.5.1 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，确保数据收集来源的合法性、正当性，明确数据类型及收集渠道、目的、用途、范围、频度、方式等；
b) 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；
c) 个人信息收集应遵循合法、正当、必要和诚信原则，并获得个人信息主体的明示同意，不应通过误导、欺诈、胁迫或者其他违背个人信息主体真实意愿的方式获取其同意；
d) 应按照 GB/T 35273—2020 中 5.1 至 5.6 规定的要求开展个人信息收集工作；
e) 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，不应因个人信息主体不同意，收集非必要个人信息，而拒绝个人信息主体使用移动互联网应用程序或第三方应用。

6.5.2 数据存储基本安全

要求如下：

a) 应明确数据存储相关安全管控措施，如加密、访问控制、数字水印、完整性校验等；
b) 应明确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) 应提供异地数据备份功能，利用通信网络将数据定时批量传送至备用场地；
d) 个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息（如样本、图像等），仅存储个人生物识别信息的摘要信息；
e) 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

要求如下：

a) 应明确数据传输相关安全管控措施，如传输通道加密、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，确保数据传输双方可信任；
c) 应采用校验技术保证数据在传输过程中的完整性；
d) 当传输敏感个人信息时，应采用加密、脱敏等安全措施。

6.5.4 数据使用基本安全

要求如下：

a) 应明确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，鼓励在保障安全的情况下，开展数据利用；
b) 应明确数据统计分析、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用安全处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险；

d) 存在利用算法推荐技术进行自动化决策分析的情形，应保证决策的透明度和结果公平合理；
e) 数据公开前应开展数据安全风险评估，明确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。涉及敏感个人信息、商业秘密信息的，以及可能对公共利益或者国家安全产生重大影响的，不应公开，法律、法规、规章另有规定的除外；
f) 利用所掌握的数据资源，公开市场预测、统计等信息时，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

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，确保参与数据加工活动的主体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) 开展数据加工活动过程中，知道或应知道可能危害国家安全、公共安全、经济安全和社会稳定的，应立即停止加工活动；
d) 委托他人加工处理数据的，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的，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

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、供应方式、保密约定、数据共享范围、数据安全保护要求等内容；
b) 公共数据提供部门应采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性；
c) 政务信息资源交换平台的政务信息共享应履行 GB/T 39477—2020 第 6 章确定的共享数据安全要求。

6.5.7 数据交易基本安全

应按照 GB/T 37932—2019 的要求开展数据交易，加强交易过程的数据安全保护。

6.5.8 数据出境基本安全

要求如下：
a) 应明确数据出境业务场景，严格遵守国家法律、行政法规数据出境安全监管要求，符合国家法律、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，严禁未授权数据出境行为；
b) 境内用户在境内访问境内网络的，其流量不应路由至境外；
c) 应建立跨境数据的评估、审批及监管控制流程，并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

要求如下：

a) 应建立数据销毁与删除规程，明确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；
b) 如因业务终止或组织解散，无数据承接方的，应及时有效销毁其控制的数据，法律、法规另有规定的除外；
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，法律、法规另有规定或者双方另有约定的除外；
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) 应按照 GB/T 35273—2020 中 8.3 规定的要求执行个人信息删除操作。

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

要求如下：

a) 应保证关键网络设备的业务处理能力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) 应避免将视频采集、信息发布屏和公共广播等直接相关设备等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图。

7.1.1.2 通信传输

应采用校验技术保证通信过程中数据的完整性。

7.1.1.3 可信验证

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，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。

7.1.2 安全区域边界

7.1.2.1 边界防护

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。

7.1.2.2 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，默认情况下除允许通信外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，并保证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 入侵防范

应在关键网络节点处监视网络攻击行为。

7.1.2.4 恶意代码防范

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。

7.1.2.5 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，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 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；
c) 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。

7.1.2.6 可信验证

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

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；
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如 HTTPS、SSH、VPN 等。

7.1.3.2 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） 无法重命名或删除的默认账户，应阻止其直接远程登录；
d） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
e） 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；
f） 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。

7.1.3.3 安全审计

要求如下：
a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 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；
c） 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。

7.1.3.4 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） 应能通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过充分测试评估后，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通过网络进行管理的管理终端进行限制；
e） 应提供数据有效性检验功能，保证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。

7.1.3.6 可信验证

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

应采用校验技术保证重要数据在传输过程中的完整性，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等。

7.1.3.8 数据备份恢复

要求如下：
a） 应提供重要数据的本地数据备份与恢复功能；
b） 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备份场地。

7.1.3.9 剩余信息保护

应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

7.1.3.10 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) 应禁止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

视频采集、信息发布屏和公共广播等直接相关设备应配置冗余，当某节点设备出现故障时，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。

7.1.4 安全管理中心

7.1.4.1 系统管理

要求如下：

a) 应对系统管理员进行身份鉴别，只允许其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。

7.1.4.2 审计管理

要求如下：

a) 应对审计管理员进行身份鉴别，只允许其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。

7.2 管理平台要求

7.2.1 安全通信网络

要求如下：

a) 应保证管理平台承载的业务应用系统不高于其安全保护等级；
b) 应实现不同管理平台服务客户虚拟网络之间的隔离；
c) 应具有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

要求如下：

a) 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；
b) 应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。

7.2.2.2 入侵防范

要求如下：

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

7.2.2.3 安全审计

要求如下：

a) 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，至少包括虚拟机删除、虚拟机重启；
b) 应保证管理平台服务商对管理平台服务客户系统和数据的操作可被管理平台服务客户审计。

7.2.3 安全计算环境

7.2.3.1 访问控制

要求如下：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移；
b) 应允许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。

7.2.3.2 镜像和快照保护

要求如下：

a) 应针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；
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
c) 管理平台应安全可控，宜采用国产操作系统。

7.2.3.3 数据完整性和保密性

要求如下：

a) 应确保管理平台服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；
b) 应确保只有在管理平台服务客户授权下，管理平台服务商或第三方才具有管理平台服务客户数据的管理权限；
c) 应保证虚拟机镜像和快照文件备份在不同物理服务器；
d) 应确保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必要的恢复措施。

7.2.3.4 数据备份恢复

要求如下：

a) 管理平台服务客户应在本地保存其业务数据的备份；

b） 应提供查询管理平台服务客户数据及备份存储位置的能力。

7.2.3.5 剩余信息保护

要求如下：

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

b） 管理平台服务客户删除业务应用数据时，管理平台应将存储中所有副本删除。

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

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

7.3.1.2 访问控制

要求如下：

a） 无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符；

b） 应保证无线网络通过受控的边界设备接入内部网络。

7.3.1.3 入侵防范

要求如下：

a） 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；

b） 应能够检测到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；

c） 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；

d） 当开启 SSID 广播时，应使用 WPA2 和 WPA 混合加密的方式；

e） 应禁用无线接入设备和无线接入网关存在风险的功能，如 SSID 广播、WEP 认证等；

f） 应禁止多个 AP 使用同一个认证密钥。

7.3.2 安全计算环境

7.3.2.1 移动终端管控

要求如下：

a） 应保证移动终端安装、注册并运行终端管理客户端软件；

b） 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如远程锁定、远程数据擦除等；

c） 发布直播数据的移动终端宜为专用终端。

7.3.2.2 移动应用管控

要求如下：

a） 应具有选择应用软件安装、运行的功能；

b） 应只允许指定证书签名的应用软件安装和运行；

c） 专用移动应用软件应具备防二次打包工具篡改程序文件，以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。

7.4 挂载设备安全要求

7.4.1 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物理破坏，如挤压、强振动等；
b） 挂载设备在工作状态所处物理环境应能正确反映环境状态(如气象传感器不应安装在易受非自然现象的热影响源区域)。

7.4.2 安全区域边界

7.4.2.1 接入控制和安全控制

安全区域边界应支持接入实体对通讯网的接入控制和安全控制。

7.4.2.2 接入控制

挂载设备的接入控制提供以下接口形式：

a） RJ45 以太网通信接口，单个接口通信速率不低于 1000M；网络层采用 IP 协议，支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，挂载设备为客户端，边缘控制器为服务端，挂载设备支持对多个服务端传输数据；
b） COM 串行通信接口，支持 RS-232（DB9）或 RS-485；
c） 挂载设备为摄像机，且具有视频监控功能时，接口协议应符合 GB/T 28181—2022 的规定；
d） 挂载设备为摄像机，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 中采集接口的规定。

7.4.2.3 安全控制

7.4.2.3.1 挂载设备

挂载设备在接入网络时，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，如 Modbus、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，应保证密钥存储和交换安全。

7.4.2.3.2 接入网络

接入网络应至少支持如下身份认证鉴别机制之一：

a） 基于网络身份标识、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）等标识以及标识组合的认证鉴别能力；
b） 支持基于感知层接入终端身份标识和接入口令的单向认证；

c) 支持基于预共享密钥的单向和双向认证（预共享密钥是指物联网实体之间进行保密通信的初始密钥）。

7.4.2.3.3 访问控制

挂载设备接入网络时，应支持基于认证鉴定结果进行终端访问控制，包括但不限于以下要求：

a) 支持通过 ACL 方式控制感知终端对通讯网的访问；
b) 支持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) 支持黑名单制，阻断相关感知终端对通信网的访问，包括禁用通信端口；
d) 接入系统应支持分层分权分域的接入访问控制能力，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) 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) 支持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) 支持经过一定次数的认证失败后，接入系统应能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允许继续接入。

7.4.2.4 入侵防范

要求如下：

a) 应能够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) 应能够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。

7.4.3 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；
b) 应对挂载设备、边缘控制器入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全过程管理；
c) 应加强对挂载设备和边缘控制器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。

7.5 公共数据安全要求

公共数据安全应符合 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

要求如下：

a） 应保证网络设备的业务处理能力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） 应避免将视频采集、信息发布屏和公共广播等直接相关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） 应具备通信线路、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)的硬件冗余，保证系统的可用性；
f） 应具备不同路由的双链路接入保障；
g） 应配备与实际运行情况相符的网络拓扑图。

8.1.1.2 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保证通信过程中数据的完整性；
b） 应采用密码技术或特定协议转换技术保证通信过程中数据的保密性。

8.1.1.3 可信验证

可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

要求如下：

a） 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；
b） 应能够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） 应能够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、信息发布屏和公共广播等直接相关设备禁止通过无线方式进行组网，其它系统应限制无线网络的使用，强化无线网络区域边界防护措施，保证无线网络通过受控边界设备接入内部网络。

8.1.2.2 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，默认情况下除允许通信外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，并保证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；

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) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制；
g) 宜在会话结束后终止网络连接。

8.1.2.3 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，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提供报警。

8.1.2.4 恶意代码和垃圾邮件防范

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) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；
c) 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恶意代码库。

8.1.2.5 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，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 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；
c) 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；
d) 应能对视频采集、信息发布屏和公共广播的控制操作行为、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) 应定期对审计记录进行分析，以便及时发现异常行为。

8.1.2.6 可信验证

可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

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；
c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如 HTTPS、SSH、VPN 等；
d) 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

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；无法重命名或删除的默认账户，应阻止其直接远程登录；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 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；
e) 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；
f) 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；
g) 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；
h) 应用系统应提示首次登录用户修改预设的默认口令；
i) 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；
j) 视频采集、信息发布屏和公共广播等直接相关设备的特权命令应在服务器或专用操作终端执行。

8.1.3.3 安全审计

要求如下：

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 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；
c) 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；
d) 应对审计进程进行保护，防止未经授权的中断。

8.1.3.4 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) 应能通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过充分测试评估后，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通过网络进行管理的管理终端进行限制；

e） 应提供数据有效性检验功能，保证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） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

8.1.3.5 恶意代码防范

要求如下：
a） 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；
b） 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

可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，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。

8.1.3.7 数据完整性

要求如下：
a） 采用校验技术或密码技术保证重要数据在传输过程中的完整性，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等；
b） 采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、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等。

8.1.3.8 数据保密性

要求如下：
a） 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
b） 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

8.1.3.9 数据备份恢复

要求如下：
a） 应提供重要数据的本地数据备份与恢复功能，完全数据备份至少每周一次，增量备份或差分备份每天至少一次；
b） 应提供异地数据实时备份功能，利用通信网络将重要数据实时备份至备份场地；
c） 应提供重要数据处理系统的热冗余，保证系统的高可用性；
d） 建立敏感数据样本库，并进行定期维护及时更新，支持其他应用通过多种接口方式使用。

8.1.3.10 剩余信息保护

要求如下：

a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

8.1.3.11 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） 应禁止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） 应对数据进行分类分级保护，加强对重要数据的保护。

8.1.3.12 业务连续性保障

要求如下：
a） 视频采集、信息发布屏和公共广播等直接相关设备应保证工作传输链路的冗余，并能够在发生故障时切换；
b） 视频采集、信息发布屏和公共广播等直接相关设备应配置冗余，当某节点设备出现故障时，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

要求如下：
a） 应对系统管理员进行身份鉴别，只允许其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

要求如下：
a） 应对审计管理员进行身份鉴别，只允许其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

要求如下：
a） 应对安全管理员进行身份鉴别，只允许其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；
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

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，并保证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) 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

8.2 管理平台要求

8.2.1 安全通信网络

要求如下：

a) 保证管理平台不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；
c) 应具有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) 应具有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，允许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

要求如下：

a) 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；
b) 应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。

8.2.2.2 入侵防范

要求如下：

a) 应能检测到管理平台服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
c) 应能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、异常流量情况时进行告警。

8.2.2.3 安全审计

要求如下：

a) 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，至少包括虚拟机删除、虚拟机重启；
b) 应保证管理平台服务商对管理平台服务客户系统和数据的操作可被管理平台服务客户审计。

8.2.3 安全计算环境

8.2.3.1 身份鉴别

要求如下：
a) 当远程管理管理平台计算平台中设备时，管理终端和管理平台计算平台之间应建立双向身份验证机制；
b) 应具有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

要求如下：
a) 应保证当虚拟机迁移时，访问控制策略随其迁移；
b) 应支持管理平台服务客户设置不同虚拟机之间的访问控制策略。

8.2.3.3 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者重新启用虚拟机，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

要求如下：
a) 应针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；
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
c) 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；
d) 应保证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

要求如下：
a) 数据传输过程中的完整性应满足 GB/T 37025—2018 中 6.1 和 7.1 的要求；
b) 应确保管理平台服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；
c) 应确保只有在管理平台服务客户授权下，管理平台服务商或第三方才具有管理平台服务客户数据的管理权限；
d) 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，在检测到完整性受到破坏时，应采取必要的恢复措施；

e) 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，保证数据存储过程完整性，并提供非完整数据的解决措施。
f) 应支持管理平台服务客户部署密钥管理解决方案，保证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

要求如下：
a) 管理平台服务客户应在本地保存其业务数据的备份；
b) 应支持对系统运行时形成重要数据文件进行数据备份；
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) 应提供查询管理平台服务客户数据及备份存储位置的能力；
f) 管理平台服务商的存储服务应保证管理平台服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；
g) 应为管理平台服务客户将业务系统及数据迁移到其他管理平台和本地系统提供技术手段，并协助完成迁移过程。

8.2.3.7 剩余信息保护

要求如下：
a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
b) 管理平台服务客户删除业务应用数据时，管理平台计算平台应将存储中所有副本删除。

8.2.4 安全管理中心

要求如下：
a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；
b) 应保证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分离；
c) 应根据管理平台服务商和管理平台服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；
d) 应根据管理平台服务商和管理平台服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟安全设备等的运行状况的集中监测。

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

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

8.3.1.2 访问控制

无线接入设备应开启接入认证功能，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。

8.3.1.3 入侵防范

要求如下：

a） 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；
b） 应能够检测到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；
c） 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
d） 当开启 SSID 广播时，应使用 WPA2 和 WPA 混合加密的方式；
e） 应禁用无线接入设备和无线接入网关存在风险的功能，如 SSID 广播、WEP 认证等；
f） 应禁止多个 AP 使用同一个认证密钥；
g） 应能够阻断非授权无线接入设备或非授权移动终端。

8.3.2 安全计算环境

8.3.2.1 移动终端管控

要求如下：

a） 应保证移动终端安装、注册并运行终端管理客户端软件；
b） 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如远程锁定、远程数据擦除等；
c） 用于发布直播数据的移动终端宜为专用终端。

8.3.2.2 移动应用管控

要求如下：

a） 应具有选择应用软件安装、运行的功能；
b） 应只允许指定证书签名的应用软件安装和运行；
c） 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；
d） 专用移动应用软件应具备防二次打包工具篡改程序文件，以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；
e） 专用移动应用软件应根据实际业务对移动应用上传文件的类型、大小进行限制。

8.4 挂载设备安全要求

8.4.1 安全物理环境

要求如下：

a） 挂载设备所处的物理环境应不对挂载设备造成物理破坏，如挤压、强振动等；
b） 挂载设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；
c） 挂载设备在工作状态所处物理环境应不对挂载设备的正常工作造成影响，如强干扰、阻挡屏蔽等；
d） 挂载设备（包括交通信号灯、通信基站、激光雷达、智能照明）应具有可供长时间工作的电力供应；
e） 边缘控制器应具有持久稳定的电力供应能力。

8.4.2 安全区域边界

8.4.2.1 接入控制和安全控制

安全区域边界应支持接入实体对通讯网的接入控制和安全控制。

8.4.2.2 接入控制

应保证只有授权的挂载设备和边缘控制器可以接入，接入控制应采用通用的标准接口，提供以下接口形式：

a) RJ45 以太网通信接口，单个接口通信速率不低于 1000M；网络层采用 IP 协议，支持 IPv4 和 IPv6，传输层应支持采用 TCP/UDP 协议，挂载设备为客户端，边缘控制器为服务端，挂载设备支持对多个服务端传输数据；
b) COM 串行通信接口，支持 RS-232（DB9）或 RS-485；
c) 挂载设备为摄像机，且具有视频监控功能时，接口协议应符合 GB/T 28181—2022 的规定；
d) 挂载设备为摄像机，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 中采集接口的规定。

8.4.2.3 安全控制

应符合7.4.2.3的要求。

8.4.2.4 入侵防范

要求如下：

a) 应能够限制与挂载设备通信的目标地址，防止对陌生地址攻击的行为发生；
b) 应能够限制与边缘控制器通信的目标地址，防止对陌生地址攻击的行为发生。

8.4.3 安全计算环境

8.4.3.1 挂载设备安全

要求如下：

a) 应保证只有授权的用户可以对挂载设备上的软件应用进行配置或变更；
b) 应具有对其连接的边缘控制器（包括读卡器）进行身份标识和鉴别的能力；
c) 应具有对其连接的其他设备（包括路由节点）进行身份标识和鉴别的能力。

8.4.3.2 边缘控制器安全

要求如下：

a) 应具备对合法连接设备（包括挂载设备、路由节点、数据处理中心）进行标识和鉴别的能力；
b) 应具备过滤非法挂载设备和伪造挂载设备所发送的数据的能力；
c) 授权用户应能够在挂载设备使用过程中对关键密钥进行在线更新；
d) 授权用户应能够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

要求如下：

a) 应能够鉴别数据的新鲜性，避免历史数据的重放攻击；

b） 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

8.4.3.4 数据融合处理

应对来自挂载设备的数据进行融合处理，使不同种类的数据可以在同一个平台被使用。

8.4.4 安全运维管理

要求如下：

a） 应实施供应链风险管理策略，确保设备的安全性从供应链一直到部署过程中都得到保障；
b） 应确保挂载设备都经过身份验证，只有经过授权的设备能够连接到多功能智能杆网络，使用强密码或证书来验证设备身份，防止未经授权的访问；
c） 应指定人员定期巡视挂载设备和边缘控制器的部署环境，对能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维护；
d） 应对挂载设备和边缘控制器的入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全过程管理；
e） 应加强对挂载设备和边缘控制器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。

8.5 公共数据安全要求

8.5.1 公共数据基本安全要求

三级要求包括公共数据基本安全要求和公共数据三级增强安全要求，公共数据基本安全要求应符合 6.5 的要求。

8.5.2 公共数据三级增强安全要求

8.5.2.1 数据收集三级增强安全

收集外部机构数据前，应对数据收集过程中的网络环境、系统进行安全评估，确保收集数据的机密性、完整性和可用性。

8.5.2.2 数据存储三级增强安全

要求如下：

a） 应提供异地实时备份功能，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关联信息系统的热冗余，保证数据的高可用性。

8.5.2.3 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建设，确保数据传输的网络可用性；
b） 重要数据不应通过离线或即时通信方式传输。

8.5.2.4 数据使用三级增强安全

要求如下：

a) 应采取技术措施保证汇聚大量数据时不暴露敏感信息；
b) 宜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) 宜对接入或嵌入的第三方应用，加强数据安全管理，宜对接入或嵌入的第三方应用开展技术检测，确保其数据处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入。

8.5.2.5 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与监控，对数据加工过程的数据操作行为进行记录、审计，对异常数据操作行为及时预警、处置；
b) 应对数据加工结果进行评估，如产生新数据，应对新数据进行安全审核，确保新数据不存在数据泄露风险；
c) 应提供安全的数据加工环境，包括网络环境、终端环境等，避免加工过程导致数据泄露、数据破坏等安全风险；
d) 加工重要数据的，应加强访问控制，建立登记、审批机制并留存记录。

8.5.2.6 数据开放共享三级增强安全

要求如下：

a) 公共数据提供部门应建立内部审批机制，明确数据对外共享目的、范围、期限、频次等内容；
b) 公共数据提供部门宜对共享的数据采取数字水印等技术，确保共享数据可溯源；
c) 宜采用多方安全计算、同态加密等数据隐私计算技术实现数据共享的安全性。

8.5.2.7 数据交易三级增强安全

三级无增强安全要求。

8.5.2.8 数据出境三级增强安全

三级无增强安全要求。

8.5.2.9 数据销毁与删除三级增强安全

要求如下：

a) 应在中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。

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

要求如下：

a） 应保证网络设备的业务处理能力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） 应避免将视频采集、信息发布屏和公共广播直接相关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技术隔离手段；
e） 应具备通信线路、关键网络设备、关键安全设备和关键计算设备的硬件冗余，保证系统的可用性；
f） 应按照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；
h） 应配备与实际运行情况相符的网络拓扑图。

9.1.1.2 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保证通信过程中数据的完整性;
b） 应采用密码技术或特定协议转换技术保证通信过程中数据的保密性；
c） 应在通信前基于密码技术对通信的双方进行验证或认证；
d） 应基于硬件密码模块对重要通信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

可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，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。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

要求如下：

a） 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；
b） 应能够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） 应能够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、信息发布屏和公共广播等直接相关设备禁止通过无线方式进行组网；其它直接相关系统，应限制无线网络的使用，强化无线网络区域边界防护措施，保证无线网络通过受控边界设备接入内部网络；
e） 应能够在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，对其进行有效阻断；
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，保证接入网络的设备真实可信；

g） 应能够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

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，默认情况下除允许通信外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，并保证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；
e） 应在网络边界对媒体内容数据和其他数据进行区分，媒体内容数据外的其他数据应通过协议转换等手段实现数据交换；
f） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制；
g） 宜在会话结束后终止网络连接。

9.1.2.3 入侵防范

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，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提供报警。

9.1.2.4 恶意代码和垃圾邮件防范

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） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；
c） 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恶意代码库。

9.1.2.5 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，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 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；
c） 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；
d） 应能对视频采集、信息发布屏和公共广播的控制操作行为、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） 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

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，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。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

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；
c） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如 HTTPS、SSH、VPN 等；
d） 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

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） 无法重命名或删除的默认账户，应阻止其直接远程登录；
d） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
e） 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；
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，并依据强制访问控制规则控制主体对有安全标记信息资源的访问；
i） 应用系统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、信息发布屏和公共广播相关设备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

要求如下：

a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 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；

c) 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；
d) 应对审计进程进行保护，防止未经授权的中断。

9.1.3.4 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) 应能通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过充分测试评估后，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通过网络进行管理的管理终端进行限制；
e) 应提供数据有效性检验功能，保证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) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

9.1.3.5 恶意代码防范

要求如下：

a) 应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；
b) 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。

9.1.3.6 可信验证

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，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。可信验证要求应符合附录 H 的规定。

9.1.3.7 数据完整性

要求如下：

a) 采用密码技术保证重要数据在传输过程中的完整性，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等；
b) 采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、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等；
c) 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

要求如下：

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

9.1.3.9 数据备份恢复

要求如下：

a) 应提供重要数据的本地数据备份与恢复功能，完全数据备份至少每周一次，增量备份或差分备份至少每天一次；
b) 应提供异地数据实时备份功能，利用通信网络将重要数据实时备份至备份场地；
c) 应提供重要数据处理系统的热冗余，保证系统的高可用性；
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) 建立敏感数据样本库，并进行定期维护及时更新，支持其他应用通过多种接口方式使用。

9.1.3.10 剩余信息保护

要求如下：

a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

9.1.3.11 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) 应禁止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) 应对数据进行分类分级保护，加强对重要数据的保护。

9.1.3.12 业务连续性保障

要求如下：

a) 视频采集、信息发布屏和公共广播直接相关设备应保证工作传输链路的冗余，并能够在发生故障时切换；
b) 视频采集、信息发布屏和公共广播直接相关设备应配置冗余，当某节点设备出现故障时，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。

9.1.4 安全管理中心

9.1.4.1 系统管理

要求如下：

a) 应对系统管理员进行身份鉴别，只允许其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。

9.1.4.2 审计管理

要求如下：

a) 应对审计管理员进行身份鉴别，只允许其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。

9.1.4.3 安全管理

要求如下：
a) 应对安全管理员进行身份鉴别，只允许其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；
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。

9.1.4.4 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，并保证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) 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

9.2 管理平台安全要求

9.2.1 安全通信网络

要求如下：
a) 保证管理平台不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；
c) 应具有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) 应具有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，允许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) 应提供对虚拟资源的主体和客体设置安全标记的能力，保证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，保证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

要求如下：

a) 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；
b) 应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。

9.2.2.2 入侵防范

要求如下：

a) 应能检测到管理平台服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
c) 应能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、异常流量情况时进行告警。

9.2.2.3 安全审计

要求如下：

a) 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，至少包括虚拟机删除、虚拟机重启；
b) 应保证管理平台服务商对管理平台服务客户系统和数据的操作可被管理平台服务客户审计。

9.2.3 安全计算环境

9.2.3.1 身份鉴别

要求如下：

a) 当远程管理管理平台计算平台中设备时，管理终端和管理平台之间应建立双向身份验证机制；
b) 应具有管理平台服务客户首次登录强制修改初始密码措施。

9.2.3.2 访问控制

要求如下：

a) 应保证当虚拟机迁移时，访问控制策略随其迁移；
b) 应允许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。

9.2.3.3 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者重新启用虚拟机，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

要求如下：

a) 应针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；
b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；
c) 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；
d) 应保证虚拟机镜像和快照文件备份在不同物理存储。

9.2.3.5 数据访问权限控制

要求如下：

a) 应支持制定安全策略，并根据安全策略启用控制用户对数据的访问；
b) 应实现业务数据、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，同时对用户访问应分配最小访问权限；
c) 数据提供给第三方访问时，应严格限制默认账户的访问权限，定期修改账户的口令；
d) 数据管理员应定期汇总数据库账户/权限列表给部门经理审核，定期清理不必要的账户和权限。

9.2.3.6 数据完整性和保密性

要求如下：

a) 应确保管理平台服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；
b) 应保证只有在管理平台服务客户授权下，管理平台服务商或第三方才具有管理平台服务客户数据的管理权限；
c) 应使用校验技术或密码技术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必要的恢复措施；
d) 应支持管理平台服务客户部署密钥管理解决方案，保证管理平台服务客户自行实现数据的加解密过程。

9.2.3.7 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、GA/T 1400.4—2017 和 GB/T 28181—2022 的规定；
c) 共享给城管部门的数据应符合 GB/T 30428.7—2017 的规定；
d) 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；
e) 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，未来可方便对接城市数字化管理系统或智慧城市管理系统；
f) 挂载设备感知数据的处理和计算应在管理平台中进行，对外只提供结果，原始数据原则上不出管理平台；例外情况需要得到相关主管部门的批准；

g） 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。如存在争议，上升相关部门进行决策。

9.2.3.8 数据备份恢复

要求如下：

a） 管理平台服务客户应在本地保存其业务数据的备份；
b） 应提供查询管理平台服务客户数据及备份存储位置的能力；
c） 管理平台服务商的管理平台存储服务应保证管理平台服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；
d） 应为管理平台服务客户将业务系统及数据迁移到其他管理平台和本地系统提供技术手段，并协助完成迁移过程。

9.2.3.9 数据销毁

要求如下：

a） 各业务部门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销毁，禁止超期保存数据，对留存期限有明确规定的，按相关规定执行；
b） 对于已经明确不再使用或需要到期删除的数据应进行销毁；
c） 个人数据的销毁根据业务需求选择彻底删除或匿名化；
d） 遵守审计原则，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、操作方式、数据内容等相关信息。

9.2.3.10 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行为记录；
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） 应能够根据记录数据进行分析，并生成审计报表；
d） 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

9.2.3.11 剩余信息保护

要求如下：

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
b） 管理平台服务客户删除业务应用数据时，管理平台应将存储中所有副本删除。

9.2.4 安全管理中心

要求如下：

a） 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；
b） 应保证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分离；
c） 应根据管理平台服务商和管理平台服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；
d） 应根据管理平台服务商和管理平台服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟安全设备的运行状况的集中监测。

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

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

9.3.1.2 访问控制

无线接入设备应开启接入认证功能，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。

9.3.1.3 入侵防范

要求如下：

a) 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；
b) 应能够检测到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；
c) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
d) 当开启 SSID 广播时，应使用 WPA2 和 WPA 混合加密的方式；
e) 应禁用无线接入设备和无线接入网关存在风险的功能，如 SSID 广播、WEP 认证等；
f) 应禁止多个 AP 使用同一个认证密钥；
g) 应能够阻断非授权无线接入设备或非授权移动终端。

9.3.2 安全计算环境

9.3.2.1 移动终端管控

要求如下：

a) 应保证移动终端安装、注册并运行终端管理客户端软件；
b) 移动终端应接受移动终端管理服务端的生命周期管理、设备远程控制，如远程锁定、远程数据擦除等；
c) 应保证移动终端只用于指定业务；
d) 用于发布直播数据的移动终端宜为专用终端。

9.3.2.2 移动应用管控

要求如下：

a) 应具有选择应用软件安装、运行的功能；
b) 应只允许指定证书签名的应用软件安装和运行；
c) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；
d) 移动终端应能够接受移动终端管理服务，推动的移动应用软件管理策略，并根据策略对软件实施管控；
e) 专用移动应用软件应具备防二次打包工具篡改程序文件，以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；
f) 专用移动应用软件应根据实际业务对移动应用上传文件的类型、大小进行限制。

9.4 挂载设备安全要求

9.4.1 安全物理环境

要求如下：

a) 挂载设备所处的物理环境应不对挂载设备造成物理破坏，如挤压、强振动等；
b) 挂载设备在工作状态所处物理环境应能正确反映环境状态（如气象传感器不应安装在易受非自然现象的热影响源区域）；
c) 挂载设备在工作状态所处物理环境应不对挂载设备的正常工作造成影响，如强干扰、阻挡屏蔽等；
d) 关键挂载设备（包括交通信号灯、通信基站、激光雷达、智能照明）和边缘控制器应具有可供长时间工作的电力供应(应具有持久稳定的电力供应能力)。

9.4.2 安全区域边界

9.4.2.1 接入控制和安全控制

安全区域边界应支持接入实体对通讯网的接入控制和安全控制。

9.4.2.2 接入控制

应保证只有授权的挂载设备和边缘控制器可以接入，接入控制应采用通用的标准接口，提供以下接口形式：

a) RJ45 以太网通信接口，单个接口通信速率不低于 1000M；网络层采用 IP 协议，支持 IPv4 和 IPv6，传输层支持采用 TCP/UDP 协议，挂载设备为客户端，边缘控制器为服务端，挂载设备支持对多个服务端传输数据；
b) COM 串行通信接口，支持 RS-232（DB9）或 RS-485；
c) 挂载设备为摄像机，且具有视频监控功能时，接口协议应符合 GB/T 28181—2022 的规定；
d) 挂载设备为摄像机，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 中采集接口的规定。

9.4.2.3 安全控制

安全控制应符合7.4.2.3的要求。

9.4.2.4 入侵防范

要求如下：

a) 应能够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) 应能够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。

9.4.3 安全计算环境

9.4.3.1 挂载设备安全

要求如下：

a) 应保证只有授权的用户可以对挂载设备的软件应用进行配置或变更；
b) 应具有对其连接的边缘控制器（包括读写器）进行身份标识和鉴别的能力；

c） 应具有对其连接的其他设备（包括路由器）进行身份标识和鉴别的能力。

9.4.3.2 边缘控制器安全

要求如下：

a） 应具备对合法连接设备（包括挂载设备、路由节点、数据处理中心）进行标识和鉴别的能力；
b） 应具备过滤非法挂载设备和伪造挂载设备所发送的数据的能力；
c） 授权用户应能够在挂载设备使用过程中对关键密钥进行在线更新；
d） 授权用户应能够在挂载设备使用过程中对关键配置参数进行在线更新。

9.4.3.3 抗数据重放

要求如下：

a） 应能够鉴别数据的新鲜性，避免历史数据的重放攻击；
b） 应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

9.4.3.4 数据融合处理

要求如下：

a） 应对来自挂载设备的数据进行融合处理，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，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令。

9.4.4 安全运维管理

要求如下：

a） 应实施供应链风险管理策略，确保设备的安全性从供应链一直到部署过程中都得到保障；
b） 应确保挂载设备都经过身份验证，只有经过授权的设备能够连接到多功能智能杆网络，使用强密码或证书来验证设备身份，防止未经授权的访问；
c） 应指定人员定期巡视挂载设备和边缘控制器的部署环境，对可能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维护；
d） 应对挂载设备和边缘控制器的入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全过程管理；
e） 应实施访问控制策略，确保只有授权的设备才可以执行特定的操作；
f） 应定期更新挂载设备的固件和软件，以修补已知的安全漏洞，确保只能从受信任的来源获取固件和软件更新；
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，以便在需要时能够迅速恢复；
i） 应部署监控系统，实时监视挂载设备的活动和网络流量，建立事件响应计划，以便在发现安全事件时能够迅速采取行动；
j） 应加强对挂载设备和边缘控制器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。

9.5 公共数据安全要求

9.5.1 公共数据四级基本安全要求

四级要求包括公共数据基本安全要求和公共数据四级增强安全要求，基本安全要求应符合6.5的要求。

9.5.2 公共数据四级增强安全要求

9.5.2.1 数据收集四级增强安全要求

四级无增强安全要求。

9.5.2.2 数据存储四级增强安全要求

应建立异地灾难备份中心，提供数据的实时切换。

9.5.2.3 数据传输四级增强安全要求

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。

9.5.2.4 数据使用四级增强安全要求

四级无增强安全要求。

9.5.2.5 数据加工四级增强安全要求

四级无增强安全要求。

9.5.2.6 数据开放共享四级增强安全要求

四级无增强安全要求。

9.5.2.7 数据交易四级增强安全要求

四级无增强安全要求。

9.5.2.8 数据出境四级增强安全要求

四级无增强安全要求。

9.5.2.9 数据销毁与删除四级增强安全要求

四级无增强安全要求。

10 第五级安全要求

第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本文件中进行描述。

附 录 A
（规范性）
安全要求的选择和使用

A.1 安全要求的概述

由于等级保护对象承载的业务不同，对其的安全关注点会有所不同，有的关注信息的安全性，即关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的关注业务的连续性，即关注保证系统连续正常的运行，免受对系统未授权的修改、破坏，从而导致系统崩溃引起业务中断。

A.2 保护对象的差异

不同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。

A.3 定级结果的组合

等级保护对象定级后，对形成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.4 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保证类要求（简记为 A）；
c) 其他安全保护类要求（简记为 G）。

A.5 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

表 A.2　安全要求及属性标识（续）

技术管理	分类	安全控制点	属性标识
安全技术要求	安全物理环境	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
		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

表 A.2　安全要求及属性标识（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	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
		系统交付	G
		等级测评	G

表 A.2　安全要求及属性标识（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	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.6　安全要求的选择

对于确定了级别的等级保护对象，应依据表 A.1 的定级结果，结合表 A.2 使用安全要求，按照以下过程进行安全要求的选择：

a) 根据等级保护对象的级别选择安全要求。方法是根据本文件，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) 根据定级结果，基于表 A.1 和表 A.2 对安全要求进行调整。根据系统服务保证性等级选择相应级别的系统服务保证类（A 类）安全要求；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；根据系统安全等级选择相应级别的安全通用要求（G 类）；

c) 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或其他标准的补充安全要求。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，可以对安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

A.7　安全要求的调整和补充

保证不同安全保护等级的对象具有相应级别的安全保护能力是安全等级保护的核心。选用本文件中提供的安全要求是保证等级保护对象具备一定安全保护能力的一种途径和出发点，在此出发点的基础上，可以参考等级保护的其他相关标准和安全方面的其他相关标准，调整和补充安全要求，从而实现等级保护对象在满足等级保护安全要求基础上，又具有自身特点的保护。

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是保证不同安全保护等级的对象具有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 10 章分别针对不同安全保护等级的对象应该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

从技术和管理两个方面提出安全要求，在采取由点到面的各种安全措施时，在整体上还应保证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，保证等级保护对象整体的安全保护能力。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，形成纵深防御体系。

B.2.2 采取互补的安全措施

以安全控制的形式提出安全要求，在将各种安全控制落实到特定等级保护对象中时，应考虑各个安全控制之间的互补性，关注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，保证各个安全控制共同综合作用于等级保护对象上，使得等级保护对象的整体安全保护能力得以保证。

B.2.3 保证一致的安全强度

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，应保证各个层面安全功能实现强度的一致性。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削弱。例如，要实现双因子身份鉴别，则应在各个层面均实现基于标记的访问控制，并保证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

针对较高级别的等级保护对象，提到了使用密码技术、可信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均要基于密码技术和可信技术，为了保证等级保护对象的整体安全保护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、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

针对较高级别的等级保护对象，提到了实现集中的安全管理、安全监控和安全审计等要求，为了保证分散于各个层面的安全功能在统一策略的指导下实现，各个安全控制在可控情况下发挥各自的作用，应建立集中的管理中心，集中管理等级保护对象中的各个安全控制组件，支持统一安全管理。

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

在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；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；应针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

应依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、安全监测、通报预警、应急处置、态势感知、能力建设、监督检查、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。

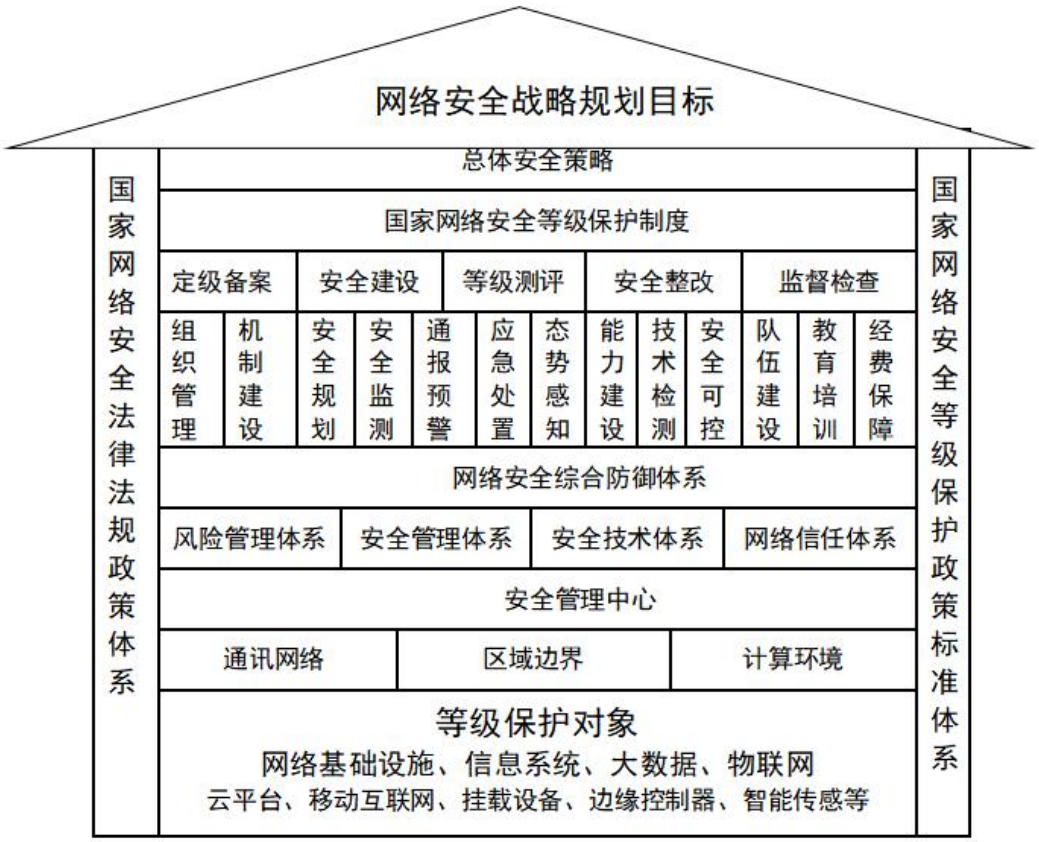


图 C.1　等级保护安全框架

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，以可信计算基（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，强制访问控制机制需要总体设计、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

应立足于现有的大量事件采集、数据挖掘、智能事件关联和基于业务的运维监控技术，解决海量数据处理瓶颈，通过对审计数据快速提取，满足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，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

应通过良好的模块结构与层次设计等方法来保证具有相当的抗渗透能力，为安全功能的正常执行提供保障。高等级保护对象的安全功能可以形式表述、不可被篡改、不可被绕转，隐蔽信道不可被利用，通过保障安全功能的正常执行，使系统具备源于自身结构的、主动性的预防能力，利用可信技术实现结构化保护。

C.4.5　多级互联技术

应在保护各等级保护对象自治和安全的前提下，有效控制异构等级保护对象间的安全互操作，从而实现分布式资源的共享和交互。随着对结构网络化和业务应用分布化动态性要求越来越高，多级互联技术应该在不破坏原有等级保护对象正常运行和安全的前提下，实现不同等级之间的多级安全互联、互通和数据交换。

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

软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）是三种基本的平台服务模式，如图 D.1 所示。

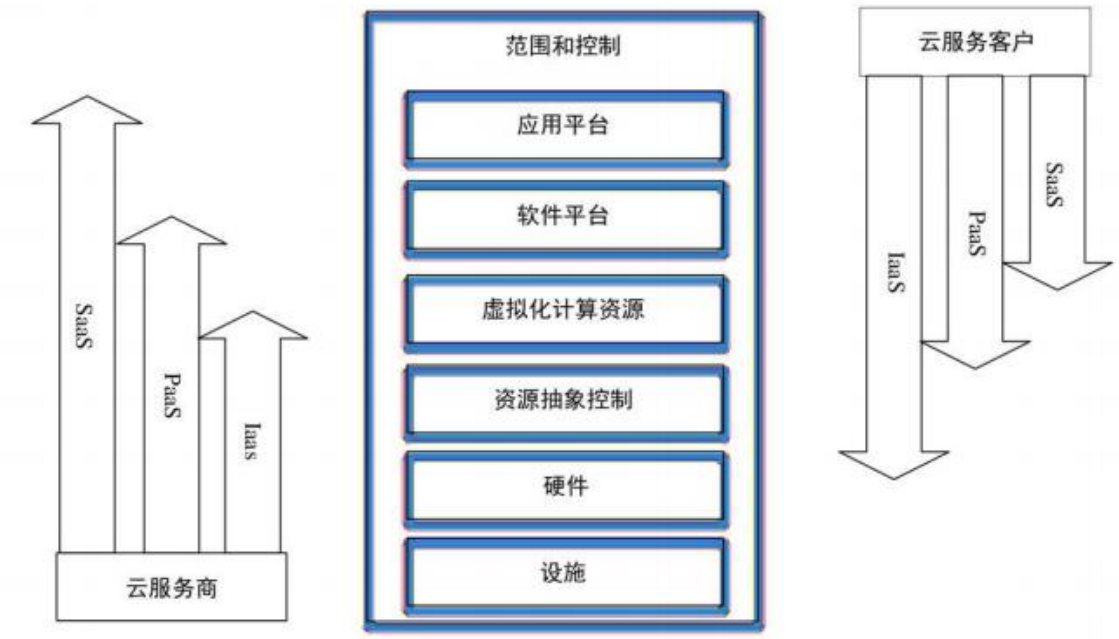


图 D.1 管理平台服务模式与控制范围的关系

D.2 不同服务模式下管理平台的组成

在不同的服务模式中，平台服务商和平台服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。在基础设施及服务模式下，管理平台由设施、硬件、资源抽象控制层组成；在平台及服务模式下，管理平台包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在软件及服务模式下，管理平台包括设施、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。

D.3 安全管理责任

D.3.1 不同服务模式下的安全管理责任

不同的服务模式下，平台服务商和平台服务客户的安全管理责任会有所不同，但都需要合作，以确保整体安全性和合规性。在任何服务模式下，都应考虑安全最佳实践，并根据具体情况来管理和维护安全性。

D.3.2 SaaS（软件即服务）模式

D.3.2.1 SaaS（软件即服务）模式下平台服务商的安全管理责任

SaaS（软件即服务）模式下平台服务商的安全管理责任如下：

a) 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) 管理用户身份和访问控制，确保只有授权的用户可以访问 SaaS 应用程序；
c) 提供数据备份和灾难恢复，以防止数据丢失；
d) 遵守法规和行业标准，以保护用户数据的隐私和合规性。

D.3.2.2 SaaS（软件即服务）模式下平台服务客户的安全管理责任

SaaS（软件即服务）模式下平台服务客户的安全管理责任如下：

a) 管理用户的访问权限，确保只有授权的员工可以使用 SaaS 应用程序；
b) 遵守 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) 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) 确保敏感数据的适当保护和加密，符合法规要求；
e) 遵守公司内部的安全政策和合规性要求。

D.3.3 PaaS（平台即服务）模式

D.3.3.1 PaaS（平台即服务）模式下平台服务商的安全管理责任

PaaS（平台即服务）模式下平台服务商的安全管理责任如下：

a) 提供和维护 PaaS 平台的安全性，包括应用程序运行时环境；
b) 提供身份和访问管理（IAM）控制，确保只有授权的开发人员可以访问平台；
c) 管理应用程序容器的安全性，包括隔离和资源管理；
d) 监控 PaaS 平台的可用性和性能，以检测潜在问题。

D.3.3.2 PaaS（平台即服务）模式下平台服务客户的安全管理责任

PaaS（平台即服务）模式下平台服务客户的安全管理责任如下：

a) 编写和部署安全的应用程序代码，包括防止常见的安全漏洞；
b) 管理应用程序的访问控制和身份验证，确保只有授权的用户可以使用应用程序；
c) 监控应用程序日志和活动，及时检测和应对安全事件；
d) 确保应用程序中的敏感数据得到适当的保护和加密；
e) 遵守应用程序开发和部署的安全最佳实践。

D.3.4 IaaS（基础设施即服务）模式

D.3.4.1 IaaS（基础设施即服务）模式下平台服务商的安全管理责任

IaaS（基础设施即服务）模式下平台服务商的安全管理责任如下：

a) 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) 管理虚拟化平台的安全性，确保虚拟机之间的隔离；
c) 提供网络安全功能，如防火墙和虚拟专用网络（VPN）；
d) 提供虚拟机映像的安全性，包括操作系统和应用程序的安全更新；
e) 监控云基础设施的可用性和安全性，以检测潜在威胁。

D.3.4.2 IaaS（基础设施即服务）模式下平台服务客户的安全管理责任

IaaS（基础设施即服务）模式下平台服务客户的安全管理责任如下：

a) 管理操作系统和应用程序的安全性，包括安装安全补丁和配置安全设置；
b) 设置适当的访问控制和身份验证措施，确保只有授权的用户可以访问虚拟机；
c) 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) 管理数据的加密和备份，以保护敏感数据；
e) 遵守合规性要求，如数据隐私法规和行业标准。

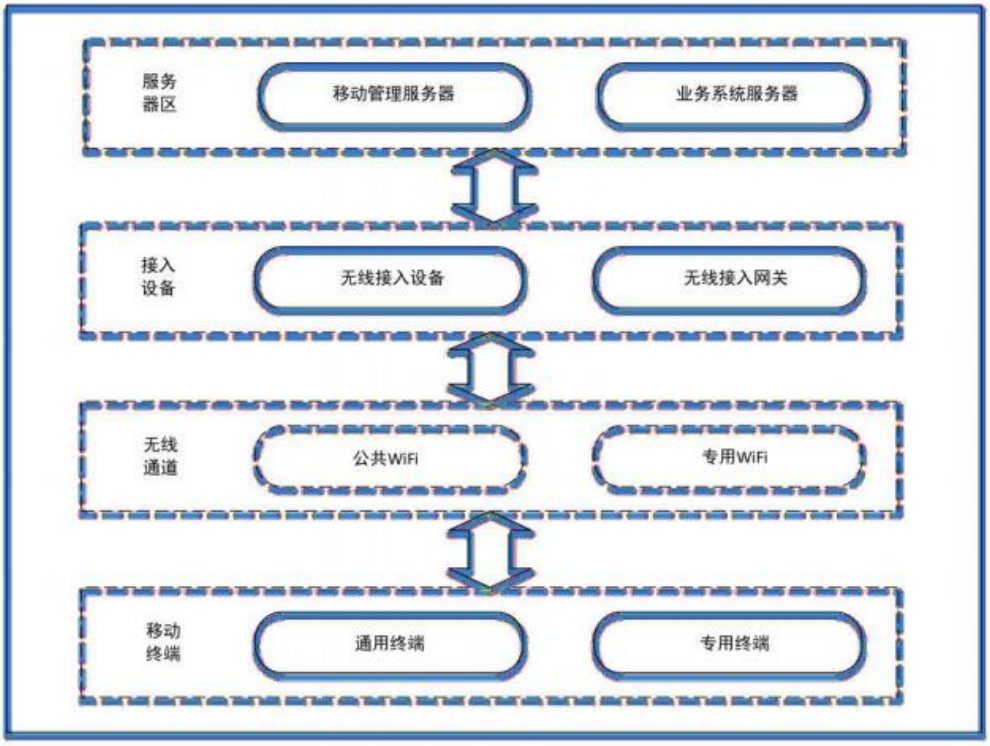
附 录 E
（规范性）
移动互联应用场景要求

E.1 移动互联应用架构

采用移动互联技术的等级保护对象其移动互联部分由移动终端、移动应用和无线网络三部分组成，移动终端通过无线通道连接无线接入设备接入，无线接入网关通过访问控制策略限制移动终端的访问行为，如图 E.1 所示，后台的移动终端管理系统负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。

E.2 移动互联安全扩展要求

移动互联安全扩展要求主要针对移动终端、移动应用和无线网絡部分提出特殊安全要求，与安全通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求。



图E.1 移动互联应用架构

附 录 F
（规范性）
挂载设备应用场景要求

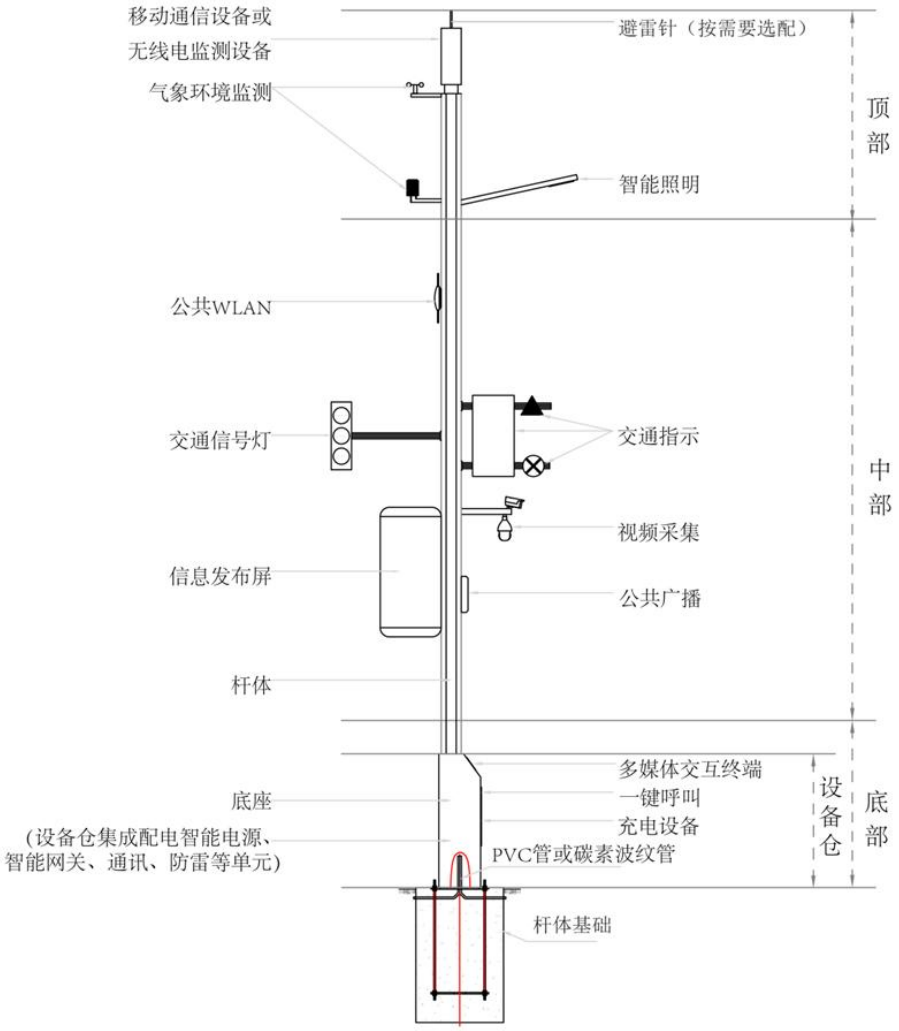
F.1 多功能智能杆应用场景

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，各部场景应用符合如下要求：

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，适宜高度 2.5 米以下；
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，适宜高度 2.5 米~8 米；
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，适宜高度 8 米以上。

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　管理平台架构分为感知层、平台层和应用层。

F.3.2　感知层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。

F.3.3　平台层由物联网平台基础数字底座、大数据和人工智能平台、业务服务平台三部分组成，是整个管理平台的能力中枢，解决场景孤岛，实现服务和业务治理。

F.3.4　应用层包括智能运维、智慧场景、设施运营和数据运营。

F.3.5　管理平台的数据可以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该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。

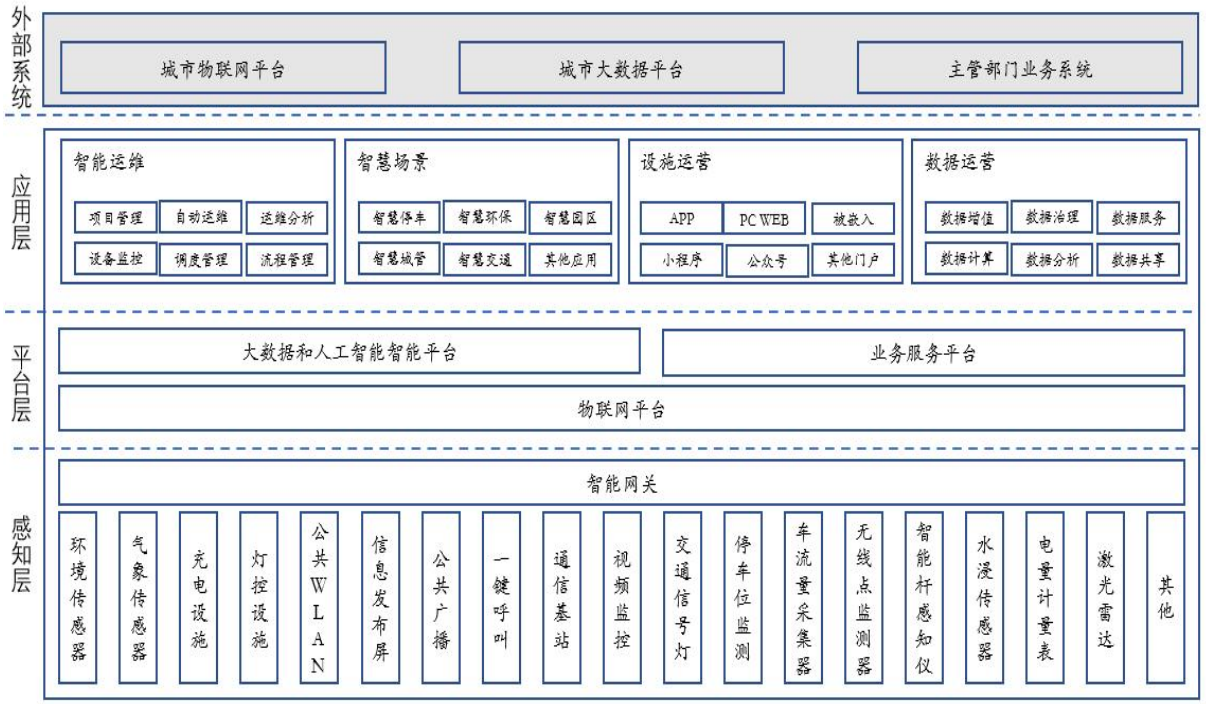


图 F.2　管理平台架构图

F.4　挂载服务

多功能智能杆覆盖的城市服务和挂载服务功能见表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。
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。

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者停止的交通信号。
	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、告示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、预定、导航和服务。可实现停车位资源利用率的最大化。
智慧环保	环境、气象监测	挂载环境监测设施后，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	支持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	支持双枪或者单枪220V交流电动汽车充电功能，支持电动自行车的充电功能，提供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。 无线电监测、一键呼叫等其它功能。

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 安全一级密码模块是基础级，提供了最低等级的安全要求，至少包括“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 密码模块应当至少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 软件或固件模块可以运行在不可修改的、受限的或可修改的运行环境中。
G.1.4 安全一级硬件密码模块除了需要达到产品级部件的基础要求之外，没有其他特殊的物理安全机制要求。模块实现的针对非入侵攻击或其他攻击的缓解方法需要有文档记录。
G.1.5 安全一级密码模块一般不具有物理安全防护能力。
G.1.6 对于物理密码模块，探针攻击和对部件的直接观察都是可行的；对于软件密码模块，对操作系统、应用和数据的访问都是可行的。
G.1.7 安全一级密码模块的安全应当由操作员负责。

G.2 安全二级

G.2.1 安全二级密码模块在安全一级的基础上增加了拆卸证据、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可以是拆卸存迹的涂层或封条，或者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就应破碎。
G.2.4 角色鉴别要求密码模块鉴别并验证操作员的角色，以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 当安全第二软件密码模块的逻辑保护由操作系统提供，可以运行在可修改的环境中，该环境应实现基于角色的访问控制或自主访问控制，但自主访问控制应当能够定义新的组，通过访问控制列表（ACL）分配权限，以及将一个用户分配给多个组。
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当由密码模块自己所有，并且与调用者在内的其他进程逻辑隔离；应当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，增强了物理安全、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 安全三级密码模块可以抵抗直接的探针攻击，并且具有防拆卸外壳或封装材料，若有门或盖的入侵，也可以提供主动防护的功能。
G.3.3 安全三级要求基于身份的鉴别机制，以提高安全二级中基于角色的鉴别机制的安全性。
G.3.4 密码模块需要鉴别操作员的身份，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是经过加密的、使用可信信道或使用知识拆分来输入或输出，以有效保护明文关键安全参数或密钥分量的输入和输出。

G.3.6　安全三级的密码模块应有效防止电压、温度超出模块正常运行范围对密码模块安全性的破坏，能够通过环境失效测试（EFT）或具备环境失效保护（EFP）确保不会因环境异常而破坏模块的安全性。

G.3.7　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标准中的最高安全等级。

G.4.2　本等级保护安全一级、安全二级、安全三级中所有的安全特性，并增加一些拓展特性。

G.4.3　安全四级的密码模块提供完整的封套保护，无论外部电源是否供电，都能够检测并响应所有非授权的物理访问。

G.4.4　从任何方向穿透密码模块的外壳都会以很高的概率被检测到，并立即将所有未受保护的敏感安全参数置零。

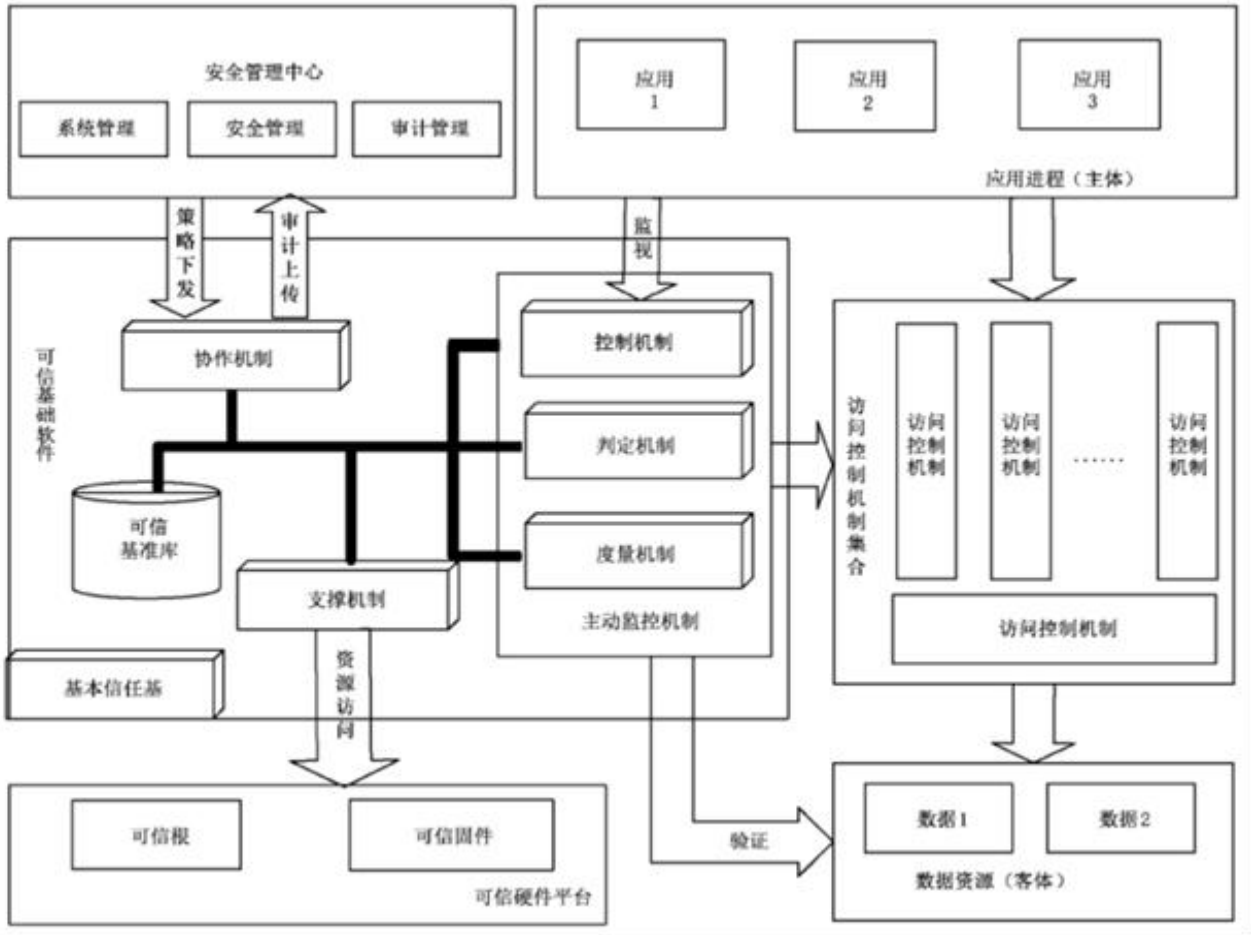
G.4.5　支持多因素身份鉴别，至少包括“已知某物、拥有某物、物理属性”中的两个；实现规定的非入侵式攻击的环境办法；具有EFP和防止错误注入攻击的能力，从而能防止因环境异常带来的安全威胁。

G.4.6　安全四级密码模块可以抵抗使用特制工具的高强度长时间攻击。

附 录 H
（规范性）
可信验证要求

H.1 功能框架

H.1.1 可信验证是基于可信根，构建信任链，一级度量一级，一级信任一级，把信任关系扩大到整个计算节点，从而确保计算节点可信的过程，可信验证实现框架如图H.1所示。



图H.1 可信验证实现框架图

H.1.2 可信根内部有密码算法引擎、可信裁决逻辑、可信存储寄存器等部件，可以向节点提供可信度量、可信存储、可信报告等可信功能，是节点信任链的起点。

H.1.3 可信固件内嵌在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，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 可信基准库存放节点各对象的可信基准值和预定控制策略。主动监控机制实现对应用程序的行为监测，判断应用程序的可信状态，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可以分成控制机制、度量机制和决策机制。控制机制主动截获应用程序发出的系统调用，既可以在截获点提取监测信息提交可信度量机制，也可以依据判定机制的决策，在截获点采取控制措施。度量机制依据可信基础库度量可信基础软件、安全机制和监测行为，确定其可信状态。

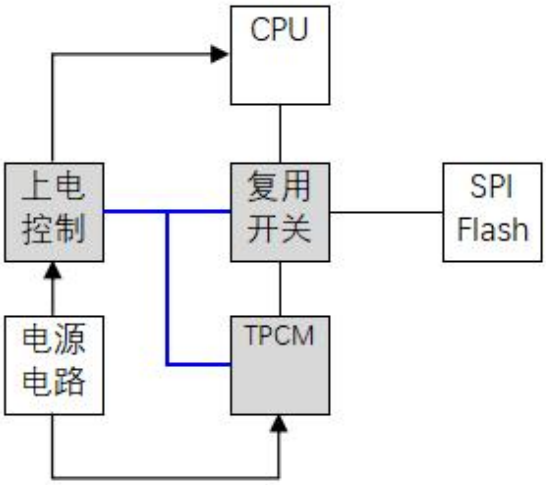
H.1.7　可信判定机制依据度量结果和预设策略确定当前的安全应对措施，并调用不同的安全机制实施这些措施。

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（可信平台控制模块 TPCM），需做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　图 H.2 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

H.2.2.1　系统上电后，CPU 处于断电状态，可信芯片和电路正常上电。

H.2.2.2　可信芯片启动后将对 SPI Flash 中的内容进行可信验证，验证可采用哈希值（Hash）校验的方式进行，出厂预先采集可信的哈希值，后续每次启动时校验，如有更新则刷新哈希值。如果进行验证为符合预期，则证明 SPI Flash 内容为可信的。

H.2.2.3　通过 GPIO 控制上电控制电路对 CPU 供电；复用开关切换到 CPU 时，使得 CPU 可以访问 SPI Flash；可信芯片通过从 SPI 与 CPU 进行通信，并通过操作系统内的可信软件基上报日志与告警信息至安全管理中心。

参 考 文 献

[1] GB/T 40994—2021 智慧城市 智慧多功能杆 服务功能与运行管理规范
[2] DB4403/T 271—2022 公共数据安全要求