CSA 云安全联盟标准

CSA GCR XXXX—XXXX

物联网安全规范

IoT Security Specification

（征求意见稿）

2022 - XX - XX 发布

云安全联盟大中华区　　发布

目　　次

前　言

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

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由云安全联盟大中华区归口。

本文件主要起草单位：华为技术有限公司、北京智慧云测设备技术有限公司、福州物联网开放实验室有限公司、阿里云计算有限公司、北京安数云信息技术有限公司、北京方研矩行科技有限公司、北京江南天安科技有限公司、北京蔷薇灵动科技有限公司、北京天融信网络安全技术有限公司、北京芯盾时代科技有限公司、广州赛宝认证中心服务有限公司、杭州安恒信息技术股份有限公司、杭州迪普科技股份有限公司、杭州宇链科技有限公司、江苏易安联网络技术有限公司、上海市数字证书认证中心有限公司、上海物盾信息科技有限公司、新华三技术有限公司、浙江大华技术股份有限公司、中数通信息有限公司、北京中宇万通科技股份有限公司、上海吉大正元信息技术有限公司、上海安几科技有限公司、深圳万物安全科技有限公司、北森云计算有限公司。

本文件主要起草人：余晓光、安涛、张天辰、姚博龙、杨洪起、陈冠直、刘苏、熊瑛、张志宇、张韩、刘克松、孙绵、季文东、杨晴、蒋晓、周学庆、赵仰梅、胡志军、张宇、张俊江、滕海明、秦益飞、田稼泉、郑大义、李澄宇、杨炳年、许亚萍、范博、许涛、詹特伦、张浩、于振伟、夏永涛、郭鹏程、姚凯。

1 范围

本文件给出了物联网系统应该具备的安全相关的技术或能力要求,规定了物联网安全对象及各相关方的安全责任。

本文件提供各应用工业物联网领域的设备厂商或甲方构建安全的物联网系统的指导,也可为各组织制定自身的物联网安全标准提供参考。

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，注明日期的引用文件，仅该日期对应的版本适用于本文件；不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 7665—2005 传感器通用术语

GB/T 25069—2010 信息安全技术 术语

GB/T 33474—2016 物联网 参考体系结构

GB/T 37044—2018 信息安全技术 物联网安全参考模型及通用要求

GB/T 17799.1-2017 电磁兼容 通用标准 居住、商业和轻工业环境中的抗扰度

GB/T 17799.2-2003 电磁兼容 通用标准 工业环境中的抗扰度试验

ISO 22301:2019 业务连续性管理体系

3 术语、定义和缩略语

3.1

传感器 Transducer/sensor

能感受被测量并按照一定的规律转换成可用输出信号的器件或装置,通常由敏感元件和转换元件组成。

[GB/T 7665—2005，定义3.1.1]

3.2

感知终端 Perception Terminal

能对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

[GB/T 37044—2018，定义3.2]

3.3

保密性 Confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

3.4

完整性 Integrity

保卫资产准确性和完整的特性。

3.5

授权 Authorization

赋予某一主体可实施某些动作的权力的过程。

3.6
信任 Trust
两个元素之间的一种关系：元素x 信任元素y，当且仅当x 确信y 相对于一组活动，元素y 将以良好定义的方式实施，且不违反安全策略。

3.7
客体 Object
信息的载体。

3.8
主体 Subject
引起信息在客体之间流动的人、进程或设备等。

3.9
隐蔽通道 Covert Channel
允许进程以违背系统安全策略的方式传输信息的通信信道。

4 物联网安全技术框架

图4-1给出了物联网安全技术框架结构：

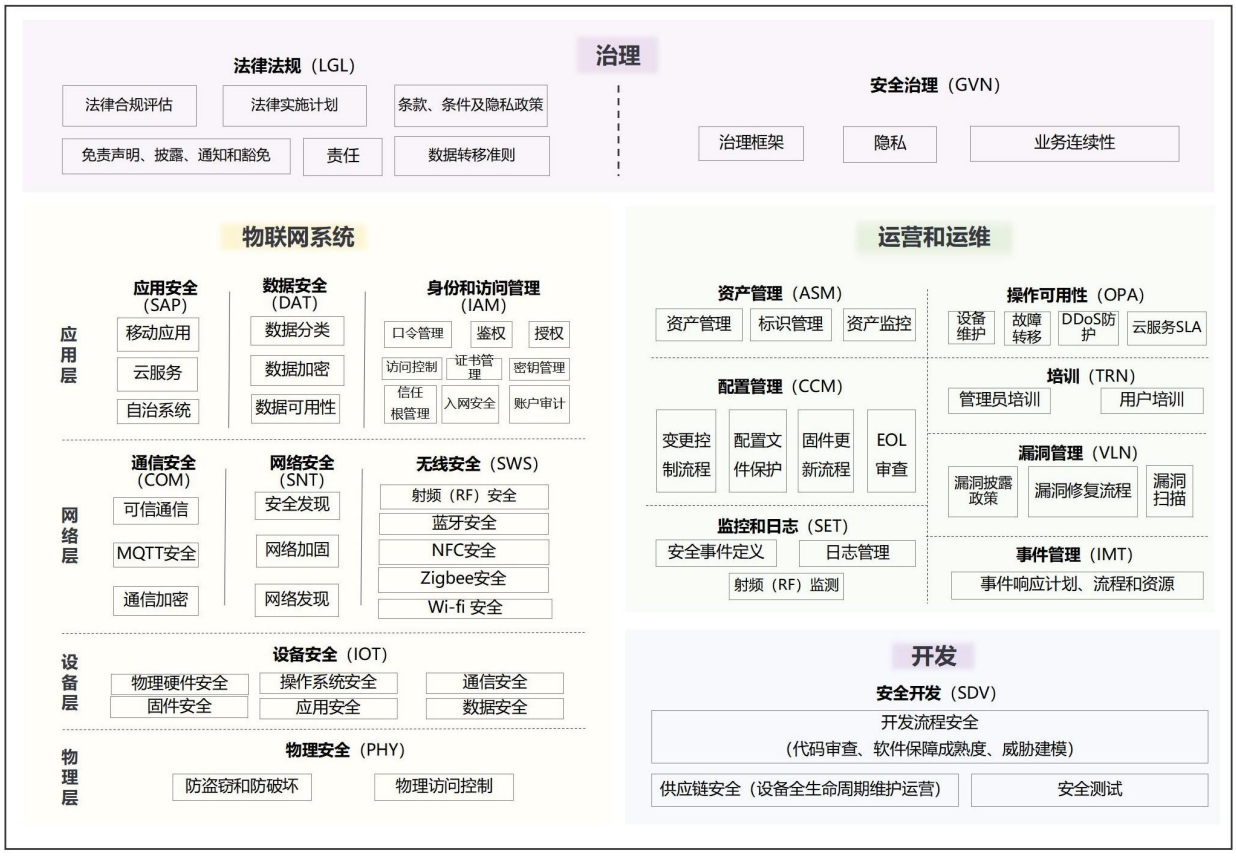

图4-1 物联网安全技术框架

物联网安全技术框架主要是在合法合规的基础上，通过安全治理、物联网系统安全防护、运营和运维以及安全开发来进行设计。

法律法规的遵从主要是通过对法律合规进行评估，并落实实施计划和制定相关文件，包括需遵循的隐私政策的声明、相关方责任、明确数据转移准则等。

安全治理主要通过分析物联网所特有的安全需求，提出有针对性的安全策略方针，从而形成适用于物联网业务的安全治理方案。

物联网系统安全防护主要从物理层、设备层、网络层、应用层展开设计，包括物理安全、设备安全、网络安全、通信安全、无线安全、应用安全和数据安全这几个层面。

安全运营和运维描述了安全控制的具体技术实现，主要通过安全事件管理、漏洞管理、日志监控审计、安全配置管理、安全培训、安全操作管理和资产管理等措施保障。

安全开发主要通过对整个开发流程的安全措施和策略、供应链安全及安全测试的实施来保障。

5 物联网安全要求

5.1 物理安全

5.1.1 防盗窃和防破坏

5.1.1.1 物联网设备部署

物联网设备部署安全要求如下：

a) 物联网设备应部署在安全场所中，并采用防盗窃和防破坏的措施；

b) 物联网设备选址和部署，应避免不受控的非安全场所；

c) 对设备或主要部件进行固定，并设置明显的不易除去的标识；

d) 宜安装防盗报警系统或视频监控系统；

e) 户外部署的重要感知终端宜设置在视频监控范围内；

f) 户外部署的关键感知终端应具有定位装置。

5.1.1.2 设备物理防护

设备物理防护安全要求如下：

a) 感知节点设备所处的物理环境应不能对感知节点设备造成物理破坏；

b) 物联网设备电源线和通信线缆应隔离铺设，避免相互干扰；

c) 关键物联网设备应实施电磁屏蔽；

d) 感知节点设备所处物理环境的设计文档中应明确提出有关感知节点设备具有防挤压、防强振动等能力的要求；

e） 应采取对感知节点设备所处物理环境的防挤压、防强振动等防护措施；

f） 感知节点设备所处的物理环境中，应具备基本的防火、防静电的措施，具备基本的防潮、防水的措施。

5.1.1.3 工作状态环境保护

感知节点设备在工作状态所处环境的保护要求如下：

a） 感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响；

b） 感知节点设备所处物理环境的设计文档中应明确提出有关感知节点设备在工作状态所处物理环境的要求；

c） 确保感知节点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；

d） 应采取对感知节点设备所处物理环境防强干扰、防阻挡屏蔽等防护措施，确保其具有良好的信号收发；关键感知层网关须具有定位装置。

5.1.1.4 防雷击

防雷击安全要求如下：

a） 野外部署的感知节点设备应具有防雷击措施；

b） 对野外部署的感知节点设备，已经通过接地系统安全接地；

c） 应采取防止感应雷措施，如设置防雷保安器或过压保护装置等；

d） 防雷装置应通过验收或国家有关部门的技术检测。

5.1.1.5 电力供应

电力供应安全要求如下：

a） 关键感知节点设备应具有可供长时间工作的电力供应；

b） 应明确关键感知节点设备、关键网关节点设备电力供应设计或验收文档中有关电力供应的要求；

c） 应采取保障关键感知节点设备、关键网关节点设备长时间工作的电力持久稳定供应措施；

d） 应提供技术和管理手段监测感知终端的供电情况，并能在电力不足时及时报警；

e） 应具有相关电力供应措施的运行维护记录。

5.1.1.6 设备选型

设备选型安全要求如下：

a） 感知节点设备选型应满足质量、性能和安全需求；

b) 选用感知终端产品时，感知终端产品已经取得具备资格的机构授予的质量认证证书；（其中，具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定认定的机构）；

c) 能够满足 GB/T 4208-2017 确定的外壳防护等级（IP 代码）要求；

d) 应通过 GB/T 17799.1-2017（电磁兼容 通用标准 居住、商业和轻工业环境中的抗扰度）、GB/T 17799.2-2003（电磁兼容 通用标准 工业环境中的抗扰度试验）或有关的专用产品或产品类兼容抗扰度标准进行的电磁兼容抗扰度试验，且性能满足需求。

5.1.2 物理访问控制

5.1.2.1 访问控制策略

访问控制策略安全要求如下：

a) 应制定物联网设备网络访问控制策略，包括策略控制下的主体、客体，及有策略覆盖的被控制的主体与客体间的操作；

b) 客体应包括物联网物理设备及设备物理端口；

c) 应控制的操作包括物联网物理设备的配置、启动、关机、故障恢复（重启、冗余切换）等，物联网设备物理端口的配置、读、写等。

5.1.2.2 物理访问流程要求

物理访问流程要求如下：

a) 应建立物联网设备物理安全流程，限制对物联网边缘设备的物理访问，进行物理访问授权；

b) 应制定物联网设备的物理访问授权、控制等制度，规定物联网设备被盗、损坏、未经授权的组件访问、将导线连接到设备端口，以及监视设备操作以危害设备（或获得进一步访问、或非法监控）的处置办法；

c) 应制定和维护对物联网设施具有访问权限的人员名单，定期对授权访问人员名单进行评审和批准，根据职位、角色对物联网设施进行物理访问授权。

5.1.2.3 物理访问监控

物理访问监控要求如下：

a) 应实施物理访问监控，监视对物联网的物理访问以检测物理安全事件，并作出响应；

b) 应设置防盗报警系统，识别潜在入侵、实时入侵报警并发起适当的响应行为；

c) 应采用自动化设备识别入侵，并实施自动响应动作，如采用视频监控，并保留视频记录；

d) 定期审查物理访问日志；

e） 在发生事件或发现事件迹象的情况下审查物理访问日志。

5.1.2.4 物理接触防护

物理接触安全要求如下：

a） 对于需要防止人为接触需求的感知终端设备（如视频监控设备），其部署地应选择需要借助辅助工具（如架设楼梯、开锁）才能接触到的位置或装置内；

b） 关键设备机房应安装电子门禁系统，对机房外的设备机柜安装门锁，防止非授权人员物理访问，并保存物理访问的记录，并定期对访问记录进行评审；

c） 应在访问物联网设施前对人员的访问权限进行验证；

d） 在需要对访客进行陪同和监视的环境下应对访问者的进行陪同和监视；

e） 对于较容易进入且拥有可移动介质驱动器的计算机应采取带锁、卸载或禁用等手段提高安全性；

f） 应将服务器放置在带锁的区域并采用认证保护机制；

g） 物联网的网络设备应放置在只能由授权人员访问的符合环境；

h） 应采取安全防护措施对物联网设施内的传输线路进行物理访问控制；

i） 应对物联网的输出设备进行物理访问控制以防止非授权人员获得输出信息。

5.1.3 物理硬件安全

5.1.3.1 设备标识

设备标识安全要求如下：

a） 物联网设备应具备不可篡改的唯一标识；

b） 物联网设备应具有唯一硬件序列号，硬件序列号存储在安全存储区域，具备防篡改、不可擦写功能。

5.1.3.2 物理攻击保护

物理攻击保护要求如下：

a） 物联网设备宜具备物理攻击保护或预警能力；

b） 宜在硬件调试接口处添加环氧树脂涂层，防止逆向工程；

c） 宜具备数据的物理保护机制，防止攻击者通过去除芯片表面封装层而获取存储器数据；

d） 宜具备在受到暴力移除或拆卸时的防护预警机制。

5.2 设备安全要求

5.2.1 固件安全

固件安全要求如下：

a) 应支持 OTA 升级能力，对远程下载的固件更新文件的来源进行校验、确保固件下载传输通道可信，防止中间人劫持或者嗅探；

b) 应具备对固件升级文件完整性校验机制，确保固件升级失败后，原有固件的可用性；

c) 应在固件有更新时及时提示用户进行升级以及时修复存在的漏洞。

5.2.2.1 漏洞修复

漏洞修复要求如下：

a) 应及时修复固件中存在的漏洞并禁用隐蔽通道；

b) 固件内部不应存在已知公开的高危、严重的 CVE 漏洞及后门账号、测试账号或魔数并可登录、管理设备或服务。

5.2.2.2 固件安全防护

固件安全防护要求如下：

a) 对物联网设备芯片，应采取必要的防护措施防止固件被篡改；

b) 设备芯片，应具备安全启动硬件保护机制，宜具备安全域隔离功能，提供可信执行环境；

c) 应使用拆卸存迹硬质涂层，防止直接观察和探测芯片内容以及在拆卸或移动芯片后留下证据；

d) 宜具有硬件随机数发生器、密钥生成和加解密运算技术，加解密运算宜仅在可信执行环境内部处理；

e) 可信执行环境（Trused Execution Environment，TEE）是应一个由处理器直接管理的隔离区域，在可信执行环境中运行的代码完全隔离于系统以及 Hypervisor；

f) 对于支持安全元件（SE）的芯片，还应具备固件芯片的物理写保护的功能，防止固件被篡改并具备侧信道攻击防护机制；

注：安全元件（Secure Element）简称 SE，通常以芯片形式提供。为防止外部恶意解析攻击，保护数据安全，在芯片中具有加密/解密逻辑电路。本来用于智能卡(Smart Card)中的 IC 芯片中，但现在在携带电中的 UICC(一种 SIM 规格)，SD 等芯片也实现了同样的功能。

g) 固件不能通过串口读取等手段提取出来,应具备对固件中的关键代码及重要数据进行防篡改和防逆向的功能；不应将登录用户名、口令等登录凭证明文存储在设备固件中。

5.2.2 操作系统安全

5.2.2.1 操作系统加固

操作系统加固要求如下：

a) 操作系统进行服务裁剪时，应符合模块最小化原则，仅保留必须的模块；

b) 操作系统宜进行安全加固；

c） 物联网设备操作系统应保证集成安全。

5.2.2.2 操作系统权限控制

操作系统权限控制要求如下：

a） 对于支持多个用户账号的系统，用户权限分配应遵循最小权限原则，普通用户只拥有系统赋予的最小权限，禁止越权操作；

b） 系统应具备远程控制请求的身份验证和接入认证机制，避免非法用户或应用控制系统；

c） 系统在安装应用时应获得用户授权，并拒绝安装被用户拒绝的应用；

d） 应用安装时，权限分配应采取授权最小化原则，系统应能禁止所有未被允许权限的使用；

e） 系统应对不同的应用进程及数据之间实施适当的访问控制管理措施，不同应用程序的进程及数据不能非授权访问；

f） 系统不应预留任何未公开帐号，所有帐号应可被操作系统管理；

g） 为了防止系统和资源被非法访问，应对系统人机接口及跨信任网络的机机接口选择合适的身份认证机制；

h） 不应存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊 URL 等。

5.2.2.3 操作系统启动安全

操作系统启动安全要求如下：

a） 操作系统启动时应先进行安全认证；

b） 物联网设备在进行操作系统启动时，宜提供安全启动机制进行系统的完整性保护，当安全验证通过后，系统才能正常启动。

5.2.2.4 操作系统补丁

操作系统补丁要求如下：

a） 应具备操作系统更新机制，且更新前宜得到用户确认；

b） 更新时，应对更新文件的来源和完整性进行校验；

c） 更新失败时，应保证系统的可用性并给予用户相应的提示，且安全属性与升级前一致，必要时提供回退机制恢复到更新之前的状态；

d） 对于执行了回退机制的操作系统，应在外围配置充分的安全防护措施，规避已知的安全漏洞利用行为；

e） 应具备通过补丁或软件升级的方式消除安全漏洞的功能。

5.2.2.5 第三方组件更新

第三方组件更新要求如下：

a) 操作系统中的第三方组件（或开源组件）应具备更新机制，且更新前宜得到用户确认；

b) 更新前应进行充分的安全验证，验证内容包括不限于，功能验证、性能验证、关联组件兼容性验证；

c) 更新时，应对更新文件的来源和完整性进行校验；

d) 更新失败时，应具备保证系统的可用性并给予用户相应的提示，且安全属性与升级前一致，必要时提供回退机制恢复到更新之前的状态；

e) 应具备通过补丁或软件升级的方式消除安全漏洞的功能。

5.2.2.6 系统及服务安全配置

系统及服务安全配置要求如下：

a) 对具备调试功能的设备，应限制调试进程在操作系统中的访问权限和操作权限，防止权限设置过高导致权限滥用；

b) 对于能够安装外部应用的系统，应提供对系统 API 的访问控制功能机制，防止应用对系统接口的非授权调用；

c) 对于可配置服务的操作系统，应具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控；

d) 登录口令宜应具有一定复杂度要求，字符长度应不少于八位，且必须由大小写字母、数字和特殊符号中两种或两种以上类型组成；

e) 对于支持远程连接的设备，其操作系统应使用安全的通信协议保障通道安全，包括具备建立通道时的身份鉴别和传输数据的机密性与完整性保护机制；

f) 对于通过 Web 进行远程管理的设备，对其进行管理和配置的行为应经过登录认证，其登录和退出过程应有日志记录。记录内容应至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的 IP 地址等信息。

5.2.2.7 系统行为审计

系统行为审计要求如下：

a) 应具备记录用户对设备操作的功能，记录包括但不限于用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果；

b) 宜自动将设备异常关机、重启、文件系统损坏等异常状态下产生的告警信息记入日志；

c） 对于具备文件系统的操作系统，应具备按帐号分配日志文件读取的功能，防止日志文件被非法读取，且对于日志文件的删除操作仅允许管理员帐号处理；

d） 应具备当在日志分配的存储空间耗尽前（建议不超过存储空间的 95%），能够按照操作系统的设置决定采取措施的功能。例如，报警并丢弃未记录的信息、暂停日志录入、覆盖以前的日志等。

5.2.3 应用安全

5.2.3.1 软件身份验证

软件身份验证要求如下：

a） 物联网设备上安装的应用软件应具备身份验证机制；

b） 应用具备防范越权操控和身份伪冒的功能，防止对身份验证数据进行暴力攻击破解；

c） 应对设备密码、设备认证信息等关键安全信息进行加密处理，不应在日志和配置文件中明文记录关键安全信息。

5.2.3.2 软件攻击防范

软件攻击防范要求如下：

a） 物联网设备上安装的应用软件应具备攻击防范机制；

b） 设备上安装的应用宜具备防伪冒、防应用二次打包/篡改和防逆向反编译功能；

c） 应具备对输入数据格式的检验过滤机制，对于使用传统 Bin 应用编译宜在编译过程采用安全编译选项，降低内存攻击漏洞的影响。

5.2.4 数据安全

5.2.4.1 本地数据存储

本地数据存储要求如下：

a） 应对物联网设备的本地数据存储进行保护；

b） 具备存储过程中对关键安全信息的机密性和完整性保护机制，对数据库的连接、访问应有 IP 等白名单控制；

c） 登录密码应禁止使用弱口令，如 admin、123456 及重复数字口令及容易被他人猜测到或被破解工具破解的口令，包含但不限于简单数字或字母的口令。

5.2.4.2 第三方软件数据权限

第三方软件数据权限要求如下：

a） 应对第三方软件的数据权限进行访问控制；

b） 对于能够安装第三方应用的系统，应具备对第三方应用软件访问数据权限的控制功能，能够发现或记录非授权应用访问数据。

5.2.4.3 个人信息安全

个人信息安全要求如下：

a） 物联网设备采集数据涉及个人信息时，应对个人隐私进行保护；

b） 个人信息的收集、存储、使用、传输、披露应符合 GB/T 35273-2020《信息安全技术 个人信息安全规范等个人信息保护国家标准要求》，具备个人信息去标识化能力；

c） 使用个人信息时，应不能超出与收集个人信息时所声称的目的具有直接或合理关联的范围，满足个人信息存储时间最小化要求，超出上述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；

d） 应准确记录和存储第三方处理个人信息的情况；

e） 传输和存储个人敏感信息时，应采用加密等安全措施；

注：采用密码技术时宜遵循密码管理相关国家标准。

f） 个人生物识别信息应与个人身份信息分开存储；

g） 原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：

1）仅存储个人生物识别信息的摘要信息；

2）在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；

3）在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

注1：摘要信息通常具有不可逆特点，无法回溯到原始信息。

注2：个人信息控制者履行法律法规规定的义务相关的情形除外。

5.3 网络安全要求

5.3.1 安全发现

5.3.1.1 入侵防范

入侵防范要求如下：

a） 物联网应具有多维度的入侵检测与防御能力，能够记录攻击事件并提供报警；

b） 应定期对物联网业务平台的操作系统、应用软件等进行漏洞扫描，及时发现存在的漏洞，并能够及时修补漏洞；

c） 应通过限定网络地址范围等方式对与终端通信的设备进行限制，避免来自陌生地址的攻击行为；

d) 应通过限定网络地址范围等方式对与后端（业务平台、接入网关等）通信的终端设备进行限制，避免对陌生地址的攻击行为；

e) 物联网关键网络节点处应具备检测、防止或限制从外部/内部发起的网络攻击行为的能力；

f) 应能进行入侵防御策略配置和管理，对网络行为进行分析和监测，发现网络攻击行为及时告警；

g) 应能够对网络攻击进行相关记录，记录攻击源 IP、攻击类型、攻击目标、攻击时间等。

5.3.1.2 恶意代码防范

恶意代码防范要求如下：

a) 物联网应具备恶意代码攻击防护能力，并维护恶意代码防护机制的升级和更新；

b) 应在物联网边界处、关键节点处应部署具备恶意代码攻击防护能力的设备，及时发现恶意代码攻击入侵行为，并能够进行有效阻断；

c) 应能进行恶意代码防护策略配置和管理，定期升级和更新防恶意代码库。

5.3.1.3 安全审计

安全审计要求如下：

a) 应对物联网系统中接入的物联网终端进行安全审计，能够对感知终端的接入登出操作、针对感知终端的入侵攻击、感知终端拆卸、感知终端的异常行为、用户对感知终端的访问及修改行为进行审计；

b) 审计日志内容应至少包含日期/时间、事件类型、事件主体、事件描述，成功/失败的信息及其他与审计相关的信息，并生成审计报表；

c) 应能够对审计进程进行保护，防止未经授权的中断；

d) 应建立审计记录定期备份机制，避免受到未预期的删除、修改或覆盖等；

e) 审计系统应支持以 SYSLOG、JDBC、FTP、API 接口等方式采集业务日志数据，支持对采集到的日志数据进行范式化、标准化处理，支持将采集到的所有安全组件日志向相关系统进行报送；

f) 具备审计记录查阅功能，按类型、日期对审计报告进行筛选查询。

5.3.2 网络加固

5.3.2.1 安全架构设计

安全架构设计要求如下：

a) 物联网应具有稳固的架构设计，具备业务所需的性能、高可用性保障，并进行分区分域管理；

b) 物联网设备应具备足够的处理性能；应保证网络各个部分的带宽满足业务高峰期需要；

c) 应按照业务的重要程度给予物联网设备带宽保障；

d) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余；

e） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

f） 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。

5.3.2.2 网络访问控制

网络访问控制要求如下：

a） 应对物联网设备执行严格的访问控制，关闭非必要的端口，阻断非必要的网络连接；

b） 应禁用业务需求以外的通信端口，在各区域之间设置访问控制规则，默认情况下除业务所需通信外的访问应被拒绝；

c） 宜控制同一区域内部的相互访问，访问控制策略应可基于 IP 地址及端口、用户/用户组、读/写等操作、有效时间周期、敏感标记等的一种或多种组合设定；

d） 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；

e） 应在重要区域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。

5.3.3 网络发现

5.3.3.1 身份标识和认证

身份标识和认证要求如下：

a） 物联网感知终端应具有唯一身份标识；

b） 接入物联网系统中的设备应具备可用于物联网系统中通信识别的身份标识，如设备 ID、序列号、Mac 地址等，身份标识需要在物联网感知终端所在的业务系统中具有唯一性；

c） 身份标识应具备防篡改保护；

d） 接入系统应能使用身份标识对物联网设备进行身份鉴别和安全认证。

5.3.3.2 终端资产管控

终端资产管控要求如下：

a） 应对物联网网络中的物联网感知终端进行资产发现和资产识别；

b） 接入系统应对接入物联网网络的物联网感知终端进行主动扫描发现，并能基于物联网指纹库对物联网终端进行资产识别分类；

c） 应对发现的资产生成便于查询维护的资产列表，列表显示信息包括但不限于资产 ID、IP、MAC、类型、厂商、系统、上线时间等；

d） 应具备针对物联网终端的黑白名单准入机制，如基于 IP、MAC、序列号、ID 对接入系统的物联网感知终端进行准入控制，仅有授权的终端可以接入；应具备对物联网终端行为的分析建模能力，可通过行为基线比对实现对物联网感知终端的动态准入和异常阻断。

5.3.4 射频安全

5.3.4.1 身份鉴别

身份鉴别要求如下：

a） 应具备唯一身份标识；

b） 标识应具备防假冒、防篡改保护机制；

c） 应通过对射频设备标签、读写器的身份鉴别，防范身份伪造，恶意篡改数据等。

5.3.4.2 指令响应

射频设备应只响应协议或者制造商规定指令，其他指令不予响应。

5.3.4.3 传输安全

传输安全要求如下：

a） 射频设备应建立安全传输流程，保障数据传输安全；

b） 应具备数据传输防篡改保护机制；

c） 应保障通信链路（空中接口、网络传输）传输过程中的数据完整性；

d） 应对通信链路(空中接口、网络传输)中传输的数据信息进行加密保护；

e） 射频设备分为标签、读写器，应对标签、读写器数据传输时进行安全保护及验证，防止中间人攻击、数据更改。

5.3.4.4 口令及存储安全

口令及存储安全要求如下：

a） 射频设备应具备口令验证机制，存储访问保护机制；

b） 应只允许通过口令验证的读写器访问其用户区，不同存储区的访问口令宜不相同；

c） 读写器应采用密码算法实现对标签信息读写、密钥存储、密码更新的保护；

d） 读写器应采用口令对读写标签信息等功能分配权限，基于不同权限设置不同口令进行访问控制；

e） 通过射频设备的访问口令机制应对各个不同存储的信息进行匹配，基于不同权限进行数据资源获取。

5.3.4.5 射频设备升级

射频设备升级要求如下：

a） 射频设备应具备更新安全性校验功能；

b） 读写器应具有授权的程序安装与更新能力；

c） 读写器应具备初始化权限的控制能力；

d） 标签应具备程序更新安全性校验功能。

5.3.5 蓝牙安全

5.3.5.1 身份鉴别

身份鉴别要求如下：

a） 应具备唯一身份标识；

b） 标识应具备防假冒、防篡改保护机制；

c） 应通过对蓝牙设备身份鉴别，防范身份伪造，恶意篡改数据等。

5.3.5.2 传输及故障处理

传输及故障处理要求如下：

a） 应具有通信完整性校验机制；

b） 设备之间通讯链路应启用加密；

c） 应具有通信安全机制以防重放、防中间人攻击；

d） 数据传输应采用保密措施；

e） 应采用数字签名或密码算法或组合算法保障数据的来源可鉴别；

f） 应具有通信延时和中断的处理机制。

5.3.5.3 设备认证及重要数据保护

设备认证及重要数据保护要求如下：

a） 蓝牙设备应采用双向认证，保障信息源唯一性，并支持源验证功能，保护重要数据；

b） 应具有通信完整性校验机制；

c） 应支持源验证功能，即支持消息认证码或数字签名与消息来源相关；

d） 应保障消息源的消息认证码或数字签名的唯一性；

e） 应对存储在接入设备中的重要数据进行保护，避免非授权的访问；

f） 应具备对存储数据的完整性保护机制，实现对鉴别信息、协议转换规则、审计记录等重要数据的完整性保护。

5.3.6 NFC 安全

5.3.6.1 身份鉴别

身份鉴别要求如下：

a） 应具备唯一身份标识；

b） 标识应具备防假冒、防篡改保护机制；

c） 应通过对 NFC 身份鉴别，防范身份伪造，恶意篡改数据等。

5.3.6.2 指令响应

NFC应只响应协议或者制造商规定指令，其他指令不予响应。

5.3.6.3 传输安全

传输安全要求如下：

a） NFC 应建立安全传输流程，保障数据传输安全；

b） 应具备数据传输防篡改保护机制；

c） 应保障通信链路（空中接口、网络传输）传输过程中的数据完整性；

d） 应对通信链路(空中接口、网络传输)中传输的数据信息进行加密保护；

e） NFC 数据传输时应进行安全保护及验证，防止中间人攻击、数据更改。

5.3.6.4 口令及存储安全

口令及存储安全要求如下：

a） NFC 应具备口令验证机制，存储访问保护机制；

b） 应只允许通过口令验证的读写器访问其用户区，不同存储区的访问口令宜不相同；

c） 应通过 NFC 的访问口令机制对各个不同存储的信息进行匹配，基于不同权限进行数据资源获取。

5.3.6.5 更新升级

更新升级要求如下：

a） NFC 应具备更新安全性校验功能；

b） 应具备初始化权限的控制能力。

5.3.7 ZigBee 安全

5.3.7.1 身份鉴别

身份鉴别要求如下：

a） 应具备唯一身份标识；

b） 标识应具备防假冒、防篡改保护机制；

c） 通过对 ZigBee 设备身份鉴别，防范身份伪造，恶意篡改数据等。

5.3.7.2 安全传输及故障处理

安全传输及故障处理要求如下：

a） 应具有通信完整性校验机制；

b） 设备之间通讯链路应启用加密；

c） 应具有通信安全机制以防重放、防中间人攻击；

d） 数据传输应采用保密措施；

e） 应采用数字签名或密码算法或组合算法保障数据的来源可鉴别；

f） 应具有通信延时和中断的处理机制；

g） 应通过对 ZigBee 设备通信传输、通信延时、终端处理机制完善，保障数据传输安全性。

5.3.7.3 设备认证及重要数据保护

设备认证及重要数据保护要求如下：

a） 设备应采用双向认证，保障信息源唯一性，并支持源验证功能，保护重要数据；

b） 应具有通信完整性校验机制；

c） 应支持源验证功能，即支持消息认证码或数字签名与消息来源相关；

d） 应保障消息源的消息认证码或数字签名的唯一性；

e） 应对存储在接入设备中的重要数据进行保护，避免非授权的访问；

f） 应具备对存储数据的完整性保护机制，实现对鉴别信息、协议转换规则、审计记录等重要数据的完整性保护；

g） 应通过对 ZigBee 设备消息源、消息发送双方验证鉴别，识别身份，保障数据存储安全。

5.3.8 Wi-Fi 安全

5.3.8.1 身份鉴别

身份鉴别要求如下：

a） 应具备唯一身份标识；

b） 标识应具备防假冒、防篡改保护机制；

c） 应通过对 WiFi 设备身份鉴别，防范身份伪造，恶意篡改数据等。

5.3.8.2 安全传输及故障处理

安全传输及故障处理要求如下：

a） 应具有通信完整性校验机制；

b） 设备之间通讯链路应启用加密；

c） 应具有通信安全机制以防重放、防中间人攻击；

d） 数据传输应采用保密措施；

e） 应采用数字签名或密码算法或组合算法保障数据的来源可鉴别；

f） 应具有通信延时和中断的处理机制；

g） 应通过对 WiFi 设备通信传输、通信延时、终端处理机制完善，保障数据传输安全性。

5.3.8.3 设备认证及重要数据保护

设备认证及重要数据保护要求如下：

a） 设备应采用双向认证，保障信息源唯一性，并支持源验证功能，保护重要数据；

b） 应具有通信完整性校验机制；

c） 应支持源验证功能，即支持消息认证码或数字签名与消息来源相关；

d） 应保障消息源的消息认证码或数字签名的唯一性；

e） 对存储在接入设备中的重要数据进行保护，避免非授权的访问；

f） 具备对存储数据的完整性保护机制，实现对鉴别信息、协议转换规则、审计记录等重要数据的完整性保护；

g） 通过对 WiFi 设备消息源、消息发送双方验证鉴别，识别身份，保障数据存储安全。

5.4 通信安全要求

5.4.1 可信通信

5.4.1.1 通信防护

通信防护要求如下：

a） 各类通信模块应具备安全通信的防护能力；

b） 连接终端通信接口时，物联网终端应根据不同的连接状态/模式给用户相应的提示；

c） 通信模块应支持安全的通信协议，遵守协议安全要求，并提供加密算法和完整性保护算法；

d） 应禁止使用 MD5、SHA-1、DES、RSA-1024 等不安全的加密算法，应使用国家级商用密码算法，并遵守相关规定及要求。通信模块应具备抗侧信道攻击能力。

5.4.1.2 身份认证

身份认证要求如下：

a） 应对每次通信进行有效的身份认证；

b） 对于每次的通信交互，均应采用双向认证和动态认证两种认证方式；

c） 身份认证的秘钥应采用动态秘钥，并确保每一台设备和每一次通信秘钥的独立性和安全性；

d） 当身份认证超时，应终止当前的会话。在经过一定次数（最多 5 次）的鉴别失败后，应终止新的接入尝试，至少 30 分钟内不能再尝试建立新的连接。

5.4.1.3 通信数据有效性

通信数据有效性要求如下：

a) 对通信的数据进行有效性效验；

b) 在收到一次通信后，应对通信的数据进行多因子的有效性验证，依据应用场景国家相关安全性要求，对验证内容至少应包含以下方式中的两种：

1) 序列号：长度要求至少 16 位，并具备合理的初始化规定和报文顺序打乱后的恢复规定；

2) 时间戳：对时间戳的精度要求精确到秒级，并统一使用 UTC 或其他全局性时钟；

3) 标识符：整个传输系统中，各实体应具有唯一的标识符，并具备防篡改保护，通信中应包含一个唯一的源标识符和宿标识符。

5.4.2 MQTT 安全

5.4.2.1 客户端安全

客户端安全要求如下：

a) 实现者应提供身份验证机制对客户端身份进行验证；

b) 实现者在服务端基于客户端提供的信息或身份认证结果，可以对客户端对某些资源访问进行限制。

5.4.2.2 服务端身份验证

应实现者应允许服务端通过应用消息向客户端发送服务端凭证用于身份验证或在客户端和服务端之间使用虚拟专用网络确保客户端连接的是指定的服务器。

5.4.2.3 报文和消息保护

报文和消息保护要求如下：

a) 实现者在应用消息中包含哈希值或在客户端和服务端之间使用虚拟专用网络确保应用消息完整性；

b) 实现者应对应用消息的内容进行加密或在客户端和服务端之间使用虚拟专用网络保证数据的保密性；

c) 应保证控制报文和应用消息新鲜性，实现者应考虑应用消息的内容中包含时间序列的数据信息，保障时间序列不被篡改；

d) 实现者应考虑适当的策略或使用签名技术实现端到端的不可抵赖性。

5.4.2.4 客户端和服务端盗用检测

实现者应考虑适当的策略来保障客户端和服务端是互相关联的，而不会出现被冒名或盗用的情形。

5.4.2.5 异常行为检测

实现者应考虑适当的安全规则，并在服务端实现监视客户端行为，检测潜在安全风险。当服务端发现违反安全规则行为的客户端时，可以断开其连接并可采用适当的方式对其后续行为进行阻断。

5.4.2.6 身份凭据安全

实现者在使用身份凭据时，应考虑凭据的有效期和采用适当的策略更换审批凭据。

5.4.3 通信加密

通信加密要求如下：

a) 应支持国家密码管理主管部门批准使用的密码算法，使用国家密码管理主管部门认证核准的密码产品，遵循相关密码国家标准和行业标准；

b) 应按照国家相关保密部门要求采用合适的加密算法、密匙长度和密匙管理机制；

c) 密码长度应符合业界安全规范；

d) 对于特定的敏感数据或机密数据，应采用通道加密和数据加密的双重加密方式。

5.4.4 物联网设备通信安全

通信安全要求如下：

a) 物联网设备的网络通信，应符合相关国家标准要求；

b) 使用无线接入网络技术的物联网终端，通信安全应符合 ISO/IEC 27033-6 信息技术--安全技术--网络安全--第 6 部分：保护无线 IP 网络访问中的规定；

c) 使用有线网络技术的物联网终端，通信安全应符合 GB/T 29234—2012 基于公用电信网的宽带客户网络安全技术要求中的规定；

d) 物联网设备的网络通信配对，应对密钥进行保护；

e) 在进行通信配对时，应采用 PKI 密钥协商、量子密钥分发等方式，确保会话密钥不被泄露；

f) 用于传输加密的密钥不应硬编码在代码中。

5.4.5 数据传输安全

数据传输安全要求如下：

a) 如设备需要与平台或其他终端应用进行数据交互，则在传输之前应进行双向认证；

b) 应通过安全的网络传输协议进行通信，保护通信内容的机密性和完整性。

5.5 应用安全要求

5.5.1 移动 APP

移动APP要求如下：

a) 应为移动应用程序建立安全计划，确保移动设备接收来经过批准/受信任存储库的更新；

b) 应仅允许使用预先批准的移动设备来管理物联网设备，确保移动设备将身份/密钥材料存储在由硬件支持的安全存储位置（如 Android KeyChain/KeyStore 和 iOS KeyChain）；

c) 移动 APP 应经过加固防护并具备防逆向能力。宜采取防逆向攻击的加固手段，例如混淆代码、整体 Dex 加固等。

5.5.2 云服务

云服务要求如下：

a) 应向所有云服务器、服务和网关提供数字证书，建立受信任的通信；

b) 应将云网关配置为仅接受来自受信任设备的通信，将授权设备列入白名单，并记录来自未授权设备的尝试通信；

c) 应与云服务提供商（CSP）签署隐私协议，确保有适当的安全控制措施保护敏感数据（个人身份信息（PII）/受保护的健康信息（PHI））；

d) 应云服务配置应符合安全要求，具体可参阅 CSP 安全指南文档以满足安全防护目标；

e) 对于支持设备部署的基础设施即服务（IaaS）和平台即服务（PaaS）云实施，应确保定期更新并及时修补云组件；

f) 应监视所有应用程序编程接口（API）调用并对潜在的 API 滥用报警；

g) 应验证连接到云服务的 IoT 设备身份，拒绝对任何未通过身份验证的设备的访问，并记录该访问尝试，并为一定时间段内触发安全警报的失败次数设置阈值；

h) 应对 IoT 服务管理控制台进行身份验证，对访问管理控制台的每个操作员和管理员提供唯一身份，并对登录操作记录审计日志；

i) 应对登录到云服务的管理控制台强制实施多因素身份验证；

j) 应将所有云 API 的范围限制为特定的 Internet 协议（IP）地址、网关或应用程序；

k) 应限制每个 API 的允许操作（如只读、读/写等）；

l) 应使用防病毒和基于主机的安全监测，保护用于远程访问云管理控制台的主机免受恶意软件感染。防病毒和基于主机的安全监测必须满足如下功能：

   1) 使用前检查电子或光学介质上的任何文件以及通过网络接收的文件中是否存在恶意代码；

   2) 使用前检查电子邮件附件和下载是否包含恶意代码或不必要的文件类型。 此检查在不同节点（如电子邮件服务器、台式计算机和组织的网络入口点）进行；

3) 检查网络流量（例如超文本标记语言（HTML），JavaScript 和超文本传输协议（HTTP））是否存在恶意代码；

4) 插入时检查可移动媒介（如 USB 令牌和硬盘驱动器、光盘（CD）、数字视频光盘（DVD）、FireWire 设备和外部串行高级技术附件设备）；

5) 检查无文件恶意软件；

6) 基于主机的安全监测，如完整性检查器、防火墙或入侵防御/检测系统，应识别出表明系统故障或损害的不正常现象或异常情况。 此外，这些工具应有助于确认系统以最佳、有弹性和安全的状态运行。

5.5.3 自治系统

自治系统要求如下：

a) 应设计和部署将安全关键功能与非安全关键功能分开的自治系统；

b) 应对实施环境进行控制，以验证自主系统的安全运行，并在非强制安全运行时改变状态；

c) 应设计能够在传感器退化环境（例如全球导航卫星系统（GNSS）、摄像机、光探测和测距（LIDAR）、无线电探测和测距（雷达）等）中运行的弹性自主控制系统。使用诸如可相互验证的信息、同步定位和映射（SLAM）或将系统更改为故障等状态的机制；

d) 应在系统内实施入侵检测/预防功能，使用基于签名和基于行为的机制，基于行为的机制应确定系统的“安全基线”，并确定异常情况，如意外的通信和行为；

e) 应尽可能实现支持安全关键消息的身份验证和完整性检查的加密安全过程；

f) 应设计并实现了自治系统的状态机，国家应包括故障安全和故障操作能力，网络安全事件应该触发这些状态之一的状态变化。故障操作事件应立即要求人工干预；

g) 应评估和测试操作员/乘员与自主系统的交互作用，以验证操作员/乘员在发生网络异常问题时控制和/或解决网络异常问题的能力。

5.6 数据安全要求

5.6.1 数据分类

数据分类要求如下：

a) 应明确物联网数据分类的对象和范围，制定数据分类的标准和管理制度；

b) 应明确物联网数据的分级标准与覆盖范围，尽量函盖所有数据域；

c) 应体现物联网数据典型业务特征和合理梳理物联网数据，明确物联网数据的责任主体和职责；

d) 应基于法律法规和业务需求确定物联网数据的特征和维度，明确数据分类分级细则。

5.6.2 数据加密

数据加密要求如下：

a) 应依据国家密码管理标准选择合规的加密方法对特定敏感的物联网数据进行加密保护；

b) 应明确物联网敏感数据完整性和保密性，对数据在传输、存储过程中采用合规的加密策略或存储技术。

5.6.3 数据可用性

数据可用性要求如下：

a) 应保证感知节点通信数据的可用性；提供关键物联网网关和通信线路冗余，并支持网络传输质量保证功能；重要数据应有多重备份；

b) 感知节点在传输其采集到的数据时，应对数据新鲜性做出标识；数据在备份时应与原数据具有相同的访问控制权限和安全存储要求，确保数据一致性；

c) 应定期对物联网数据进行备份和恢复，实现对存储数据的冗余管理，保护数据的可用性。

5.7 身份和访问管理安全要求

5.7.1 口令管理

5.7.1.1 口令生成

口令生成要求如下：

a) 自动生成的口令应具有随机性，且长度不少于 6 个字符；

b) 设备出厂时应为每个设备帐号随机生成默认口令或者在第一次入网时强制修改默认口令；

c) 对于使用默认口令的设备，每次登录时应提醒用户修改口令，直到用户修改口令；

d) 用户设置的口令应符合如下基本策略：

1) 口令长度不少于 8 个字符；

2) 口令允许的最大长度不少于 64 个字符；

3) 口令至少包含数字、小写字母、大写字母以及特殊字符中的两类字符。

5.7.1.2 口令使用

口令使用要求如下：

a) 口令传输应采用安全通道或加密后传输；

b) 应默认对输入框中的口令进行掩盖显示；

c) 应禁止口令从输入框中复制的功能；

d) 用户登录成功后应无法查看自己的口令；

e） 口令的鉴别过程应具备防暴力破解功能，如超过设定尝试次数后，应锁定操作帐号或者操作 IP 一段时间。

5.7.1.3 口令管理

口令管理要求如下：

a） 所有口令都应可修改，不能使用硬编码口令；

b） 用户修改口令前，应提供验证旧口令以及对新口令再次确认的功能；

c） 存储口令时应加密；

d） 存储的口令应具有防破解机制，包括但不限于添加变量、限制对口令文件的访问和修改等；

e） 应不能通过用户操作界面或 API 读取口令明文；

f） 应提供在忘记帐号或者口令的情况下，通过物理手段或其他方式将设备恢复到出厂状态的功能；

g） 口令复杂度策略应可配置，并支持管理员根据应用场景配置强化的口令复杂度策略；

h） 应具备显示口令安全强度的能力；

i） 应具备口令定期强制修改的机制；

j） 口令修改应记录审计日志，包括但不限于用户 ID、时间、操作内容、IP 地址及操作结果等信息。

5.7.2 鉴权

鉴权要求如下：

a） 应对接入物联网的设备进行身份标识和鉴别；

b） 应对登录物联网系统的用户进行身份标识和鉴别；

c） 物联网系统的身份验证应支持多因子认证方式；

d） 应保证鉴别信息所在的存储空间释放时或重新分配前得到完全清除。

5.7.3 授权

授权要求如下：

a） 应保证只有授权的感知节点可以接入；

b） 物联网系统用户授权应遵循最小够用原则；

c） 移动物联网设备应实施地理围栏限制以监控设备位置，收集位置数据前需经过用户授权。

5.7.4 访问控制

访问控制要求如下：

a） 应制定严格的访问控制策略。如访问控制列表、白名单等方式，实现对物联网设备的访问控制；

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） 感知节点和其他设备（网关、其他感知节点）通信时，应根据安全策略对其他设备进行权限检查；

d） 感知节点进行更新配置时，应根据安全策略对用户进行权限检查；

e） 访问控制策略应覆盖接入网络的全部节点；

f） 应确保访问和数据流通过受控接口进行通信。

5.7.5 证书管理

证书管理要求如下：

a） 各个节点用户进行证书申请时，应验证证书申请者身份；

b） 应防止非法签发和越权签发证书。通过审批的证书申请应提交给 CA，由 CA 签发与申请者身份相符的证书；

c） 应保证证书管理的可审计性，对于证书的任何处理都应做日志记录。通过对日志文件的分析，可以对证书事件进行审计和跟踪；

d） 设备证书需要定期更新，至少 6 个月更新一次，在线证书申请，建议采用 CMP v2 协议进行通信。

5.7.6 秘钥管理

密钥管理要求如下：

a） 应对密钥生命周期的各个阶段采取妥善的安全管理。包括密钥生成，存储，使用更新，撤销和销毁；

b） 一个密钥应当专职一种功能，不应让一个密钥兼任几种功能；

c） 应根据密钥的职责和重要性，对密钥进行级别划分；

d） 密钥应有足够的长度并定期更换；

e） 密钥生成要保障随机性或能够抵御穷举攻击；

f） 秘钥存储确保密钥的秘密性，真实性以及完整性；

g） 密钥安全使用时不应允许密钥以明文的形式出现在密钥设备之外；

h） 密钥备份，应采用安全方式存储，并且具有不低于正在使用的密钥的安全控制水平；

i） 应支持秘钥更新密钥和新密钥同时存在时应处于同等的安全保护水平下；

j） 应支持秘钥的撤销/存档/销毁；

k） 应支持密钥安全审计；

5.7.7 信任根管理

5.7.7.1 可信根证管理

可信根证要求如下：

a) 可信根证书的增加，应将可信根证书的证书文件在本地进行保存，若存在上级根证书管理机构，同时需要将增加的可信根证书长传至上级根证书管理机构。同时记录可信根证书的归属方，提供服务内容及责任主体，联系人等相关信息，在进行信息确认及审核后，对可信列表进行整体签发后生效；

b) 当现有可信根证信息发生改变或者需要延期时，可使用修改功能对当前的可信根证进行信息调整，在进行信息确认及审核后，对可信列表进行整体签发后生效；

c) 对于已经失效或者已经入根到根 CA 的根证机构，应将该机构从现有可信列表中删除，在进行信息确认及审核后，对可信根证列表整体签发后生效；对于登记过的可信根证，可进行信息查询及预览，便于了解当前已经签发的可信根证信息是否详实可靠。

5.7.7.2 可信域管理

可信域管理要求如下：

a) 增加可信域应且只应基于已保存并经过验证的可信根证书。新增可信域后，应对可信根证书进行整体签发后生效；

b) 在已经保存的可信根证书下，当已经维护的可信域发生改变后，应使用修改的功能将可信域的信息更新，对可信根证书列表进行整体签发后生效；

c) 当可信域本身失效或不在使用时，应将该可信域从他所属的可信根证书中删除，删除后应对可信根证列表进行整体签发后生效；

d) 对于登记过的可信域，应支持名称、功能所属可信根证书等信息进行查询。

5.7.7.3 审核与签发

审核与签发要求如下：

a) 可信根证书及可信域发生变化时应进行内容审核，如果申请的内容不正确，需要退回重新提交变更申请，如果内容正确且符合系统要求，则审核通过，应使用最新信息进行可信根证书列表签发；

b) 应使用根 CA 所持有根证书对当前最新的可信根证书列表及可信域进行签发。

5.7.7.4 版本管理与发布

版本管理与发布要求如下：

a) 每次使用签发功能后，应生成一个对应的可信根证书列表版本，发布服务默认提供最新版本的可信根证书列表，如果需要查询历史版本的可信根证书列表，可以在版本管理功能中查询历史版本，利用版本号获取对应版本的可信根证书列表；

b) 每次使用签发功能后，应产生一个可信根证书列表发布版本号，用来标识此次签发版本，并通过发布服务将可信根证书列表发布并允许下载；

5.7.8 入网安全

入网安全要求如下：

a） 应制定物联网系统的身份管理策略，并建立入网审核机制；

b） 应采取保障入网安全的技术手段，保证入网账户/设备具备合法的身份；

c） 应基于数字身份的鉴权、授权建立入网访问控制机制。

5.7.9 账户审计

账户审计要求如下：

a） 应具备物联网账户管理机制，并定期进行审核；

b） 应对所有账户开通、变更、删除制定规范化管理流程；

c） 应每年至少审核一次物联网系统中的用户、管理员、服务和设备账户；

d） 应采取措施禁用所有被认为不必要的账户，包括未经授权且已过期的账户；

e） 应制定严格的物联网账户审计策略，审计功能支持启动和关闭；

f） 对于每一个审计记录，应至少记录事件发生的日期、时间、事件的类型、主体身份和成功或失败事件，能将每个可审计事件与引起该事件的用户身份相关联；根据法律法规要求及审计记录的重要程度制定审计记录留存时间，最低不少于 180 天；

g） 审计记录应能覆盖物联网身份和访问管理的全部适用场景；

h） 应具备账户审计数据防丢失能力；

i） 应具备物联网账户审计记录管理能力。

5.8 资产管理要求

5.8.1 资产管理

资产管理要求如下：

a） 应编制并保存与物联网保护对象相关的资产清单，包括资产类别（含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等内容；

b） 应根据物联网资产的重要程度对资产进行标识管理；

c） 应对物联网信息资产进行规范化管理，如根据信息的重要程度、敏感程度或用途不同进行分类。

5.8.2 标识管理

标识管理要求如下：

a） 应对物联网中的对象进行标识，其标识符应具备足够的编码空间、灵活性和可扩展性、独立性和兼容性；

b） 对物联网中对象的标识，应具备防篡改能力；

c） 为提高数据可用性，感知终端在传输其采集到的数据时，应对数据新鲜性做出标识；

d） 物联网设备应具有身份标识能力。

5.8.3 资产监控

资产监控要求如下：

a） 对物联网所有合法连接设备应具备监测能力。包括终端节点、路由节点、数据处理中心的设备及其组件进行持续监测，及时发现设备及其组件完整性受到损坏或失效，并具备报警功能；

b） 户外部署的重要感知终端宜设置在视频监测范围内，关键感知终端应具有定位装置；

c） 应监测物联网所有合法连接设备及其组件与资产清单的一致性；

d） 对物联网重要信息资产应具备监控能力。对物联网重要信息资产的管理和应用进行监控，包括监控重要信息的存储不被篡改，传输不被未授权的监听、重放，资产的联机状态、资产故障以及未授权的访问等；

e） 应监控对物联网所有合法连接设备及其组件的变更，所有变更必须经过主管人员批准，重要变更需要经过安全评估和更高一级主管领导批准；监控未授权的资产变更；

f） 应保护物联网监控记录。对物联网所有合法连接设备及其组件的监控记录需要保存，通常保存时间按照审计记录的保存要求执行；保护监控记录的安全且不得篡改，宜采用相应的密码技术保护监控记录的安全，防止篡改；对监控记录须进行检查和分析，并给出结论，发现问题应报告主管人员。

5.9 操作可用性管理要求

5.9.1 设备维护

物理设备维护应该满足如下要求：

a） 无人值守设备宜在设备柜门上锁，并采用双重锁具机制；

b） 无人值守设备场站宜配套安装视频安防系统，安防摄像机应无死角监控设备场站；

c） 宜通过视频摄像装置实时监视无人值守设备现场情况，包括但不限于现场人、环境监视等，出现异常情况（如火情、汛情、人为破坏等），应能进行识别及告警，并联系管理人员进行处理；

d） 宜使用便携式专用调试终端进行设备系统维护；

e） 宜对设备现场维护过程进行视频监控，对维护过程中的违规行为（如未佩戴安全帽、未穿工作服、未佩戴防触电装备等）进行识别及告警，并联系管理人员进行处理。

5.9.2 故障转移

物联网产品故障转移要求如下：

a) 应设计云服务以支持节点和网关的区域故障切换。每年进行一次测试，以确保在单个区域脱机时故障切换是自动的；

b) 应将无线传感器网络（WSN）网关设计为群集形式，在单个网关脱机时能够有效处理重负载并支持故障切换。配置物联网节点在主网关出现故障时联系备份网关。至少每年测试一次故障转移能力和减载/分配能力；

c) 应使用部署到地理区域的节点群集来构建大都市范围的 WSN 部署，以最小化互连点并减少长途通信量。

5.9.3DDoS 防护

物联网产品 DDoS 防护要求如下：

a) 应设置监测程序，以识别和警报从物联网设备传输的异常增大的流量；

b) 应部署网络监控工具，监控物联网拥塞情况。在检测到拥塞通信时，建立优先的业务流（例如，区分服务）或执行动态重路由（例如，WSN/软件定义网络（SDN））；

c) 宜在网关上缓存消息至少一天（或更长时间，取决于您的环境），以确保 IoT 节点脱机时消息的可用性。

5.9.4 云服务 SLA

与云服务提供商就正常运行时间百分比和响应时间（针对事件/修补程序定义服务级别协议（SLA））协商一致，并在服务质量合同中明确违反SLA所应承担的责任。

5.10 配置管理要求

5.10.1 配置文件保护

物联网产品配置文件保护要求如下：

a) 应对通过评估的固件要合理地保护和存储，防止被非法修改；

b) 应采用双重控制、标准化加密认证等方式对固件进行保护；

c) 设备所安装的软件（例如固件等）在运送、存储和使用时，应遵循双重控制的原则，防止在未授权情况下对软件的修改和/或替换；

d) 在产品生产完成后出厂前，或在产品生产完成后经销商售出前，设备和其任何组件都应存放在受保护的、访问受控的区域内，或将设备封装在具有防攻击特性的包装中，以防止非法接触设备或其组件。

5.10.2 固件更新流程要求

设备应对固件进行有效保护，包括但不限于：

a） 设备固件及对固件的任何改动都应经过严格的流程控制，以保证固件中不含隐藏的和非法的功能；

b） 如果设备具备固件更新能力，则设备更新固件时应通过加密机制验证更新固件的完整性和真实性；如果未确认其完整性和真实性，设备应拒绝进行固件更新并删除验证失败的固件；

c） 设备固件应验证下载到设备的应用程序，如果设备支持更新应用软件和/或配置，设备必须通过可靠的安全加密机制验证更新应用软件和/或配置的完整性和真实性，如果未确认其完整性和真实性，设备应拒绝进行软件更新并删除验证失败的软件；

d） 终端宜具备固件升级能力，且发布的固件应经过签名，且签名算法是已知且安全的；

e） 终端若具有一些基本配置文件，升级后应能保持此类配置文件的内容完整和有效。同时此类配置文件应能够基于开放的接口进行读取。

5.11 监控和日志要求

5.11.1 日志管理

日志管理要求如下：

a） 应支持对各类系统事件、非正常行为以及操作行为的审计及记录；

b） 应支持将系统所有审计数据上传至态势感知管理平台，由物联网态势感知管理平台对审计事件进行集中存储，存储的审计日志留存记录至少保留；

c） 应具备获取终端日志文件并查看信息的能力；

d） 应记录包括但不限于登录、注销、添加、删除、修改用户、授权、取消权限、鉴权、修改用户口令等日志；

e） 操作事件应包括对业务系统配置参数的修改，对重要业务数据的创建、删除、修改、查询等；

5.11.2 射频监测

a） 应建立企业物联网无线检测能力；

b） 应基于无线检测能力主动搜索网络中的非法无线设备；

c） 应主动搜索与知名僵尸网络客户对客户（C2C）地址/端口的网络通信；

d） 应具备检测并记录与供应商IP地址的未授权通信的能力。

e） 应具备禁用任何已识别的设备/通信的能力，能够在发生违规行为是采取控制措施，并调查违规原因。

5.12 漏洞管理要求

5.12.1 漏洞披露政策

物联网产品漏洞披露政策应符合如下要求：

a) 厂商应公开漏洞披露政策；

b) 漏洞披露政策应包含联系机制；

c) 厂商披露的漏洞通告应该包含：

1)安全通告唯一标识ID；

2) 安全通告标题；

3) 安全通告的日期及时间；

4) 漏洞唯一标识ID；

5) 漏洞等级；

6) 漏洞描述及漏洞影响；

7) 漏洞所影响的设备型号及版本；

8) 漏洞修复补丁/升级程序。

5.12.2 漏洞管理要求

物联网产品漏洞管理应符合如下要求：

a) 厂商应该有漏洞修复流程，所有漏洞都必须按照漏洞修复流程执行。

漏洞修复参考流程：漏洞发现 -> 漏洞评估 -> 漏洞处理 -> 漏洞验证。

1)漏洞发现，通过漏洞/威胁情报，渗透测试，SRC漏洞提报等活动及时发现产品漏洞；

2)漏洞评估，评估是否为漏洞，产品是否受漏洞影响，哪些产品受影响等；

3)漏洞处理，定位漏洞根因，确定漏洞修复方案，完成产品漏洞修复；

4)漏洞验证，在所有受影响产品都完成漏洞修复后，需要进行复验确保漏洞确实都完成修复。

b) 应具备漏洞管理系统，对漏洞全生命周期进行追踪管理；

c) 漏洞管理系统应该要求每个漏洞都具备如下信息：

1)漏洞唯一标识ID

2)漏洞等级；

3)漏洞影响；

4)漏洞根因；

5)漏洞状态；

6)漏洞修复方法。

d) 漏洞管理应该提供查找每个漏洞对应的受影响的产品型号和版本的方法，并提供所涉产品型号和版本漏洞的修复方法；

e) 漏洞管理应建立避免漏洞修复引入新漏洞的规范、流程。

5.12.3 漏洞扫描

物联网产品漏洞扫描应符合如下要求：

a) 应具备已知漏洞的自动化漏洞扫描能力；

b) 应具备漏洞库定期更新机制，厂商应该有方式获取支持扫描的漏洞列表；

c) 物联网设备发布之前，应该经过漏洞扫描测试，且漏洞扫描报告应作为一个配置管理项被归档；

d) 厂商应将物联网设备通过漏洞扫描测试作为产品发布的一个必要验证条件，且提供漏洞扫描报告结果。

5.13 事件管理要求

5.13.1 事件响应计划、流程和资源

物联网产品事件响应计划、流程和资源应符合如下要求：

a) 应制定流程规范，支持业务流程和技术措施实施。同时根据 IT 服务管理政策和程序，对安全相关事件进行分类和分级，并确保事件管理的及时性和彻底性；

b) 应制定物联网事件管理计划，包括但不限于：

1) 确定每个物联网系统的业务和技术联络点（POC），并在发生事故时告知这些利益相关者他们的角色和责任；

2) 定义第三方组织在事件响应中的角色（例如，供应商和服务提供商）；

3) 定义从设备捕获的日志/审核数据的保管链；

4) 建立上报程序并定义必须在设备商执行的取证活动，考虑从联网设备实时获取自动取证功能。

c) 应维护并定期更新适用监管机构、地方和国家执法官员以及其他法律管辖机构的联系人联系方式；

d) 信息安全事件应通过符合适用法律、法规或监管合规义务的预定义通信渠道进行报告；

e) 在信息安全事件发生后，需要适当的取证程序，包括监管链，以提供证据以支持受相关司法管辖的潜在法律行动；

f) 应建立事件响应指标来监控和量化信息安全事件的类型、数量和成本；

g) 应建立信息安全事件处理流程。

5.14 安全开发要求

5.14.1 开发流程安全

生产厂商应维护开发安全文档，包含所有与物理硬件、程序软件、流程、责任人员及其它安全相关的安全机制和措施（所涵盖内容对在开发环境下安全相关组件设计和实现的完整性保护是必要的）。

5.14.2 供应链安全

设备生产厂商应维护运营管理指南，包含记录安全相关组件的整个生命周期管理以及将其集成到单个终端设备的方式，包括但不限于以下内容：

1)生产和个人化的数据；

2)物理位置和生产时间；

3)维修；

4)移除操作；

5)丢失或被盗。

5.14.3 安全测试

物联网产品安全要求如下：

a) 设备生产厂商如使用加密芯片或模块产品，宜在产品选型阶段采购通过国家密码管理局商用密码检测中心认证相关密码芯片或模块；

b) 云服务提供商宜通过信息安全等级保护测评与商用密码应用安全性评估。

5.15 安全治理要求

5.15.1 治理框架

5.15.1.1 明确责任部门与人员

安全治理应明确责任部门与人员，具体要求如下：

a) 应明确其法定代表人或主要负责人对信息安全负全面领导责任，包括为信息安全工作提供人力、财力、物力保障等；

b) 应任命物联网安全负责人和物联网安全保护工作部门，物联网保护负责人应由具有相关管理工作经历和物联网保护专业知识的人员担任，参与有关物联网处理活动的重要决策直接向组织主要负责人报告工作；

c) 信息安全负责人和信息安全保护工作部门的职责应包括但不限于：

1) 全面统筹实施组织内部的信息安全工作，对信息安全负直接责任；

2) 组织制定信息保护工作计划并督促落实；

3) 制定、签发、实施、定期更新隐私政策和相关规程；

4) 开展信息安全影响评估；

5） 组织开展信息安全培训；

6） 在产品或服务上线发布前进行检测；

7） 进行安全审计；

8） 与监督、管理部门保持沟通，通报或报告信息安全事件处置等情况。

d） 应为信息安全负责人和信息安全保护工作部门提供必要的资源，保障其独立履行职责。

5.15.1.2 人员管理与培训

人员管理与培训要求如下：

a） 应与从事信息安全岗位上的相关人员签署保密协议，对大量接触敏感信息的人员进行背景审查；

b） 应明确内部涉及信息安全不同岗位的安全职责，建立发生安全事件的处罚机制；

c） 应定期（至少每年一次）或在隐私政策发生重大变化时，对信息安全岗位上的相关人员开展专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

5.15.1.3 安全审计

安全审计要求如下：

a） 应对隐私政策、相关规程和安全措施的有效性进行审计；

b） 应建立自动化审计系统，监测记录信息处理活动；

c） 审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；

d） 应防止非授权访问、篡改或删除审计记录；

e） 建立审计记录定期备份机制，避免受到未预期的篡改或删除等。

5.15.2 隐私

5.15.2.1 隐私保护要求

物联网产品应遵守法律规定的相关隐私政策。

5.15.3 业务连续性

业务连续性要求如下：

a） 宜满足 ISO 22301：2019 业务连续性管理体系标准的要求；

b） 应充分识别业务风险并评估其对业务的影响程度；

c） 应制定完备的业务连续性计划并有效实施至少3个月。

附 录 A

（资料性）

本文件各章节内容与CSA IoT安全控制框架的映射关系

如表 1 所示：

表 1 标准各章节内容分与 CSA IoT 安全框架的映射关系

本文件章节	CSA IoT 安全控制框架控制域
物理安全要求	物理安全
设备安全要求	物联网设备安全
网络安全要求	网络安全
通信安全要求	通讯安全
无线安全要求	射频安全（RF）
应用安全要求	应用安全
数据安全要求	数据安全
身份和访问管理安全要求	身份和访问管理
资产管理要求	资产管理
操作可用性管理要求	操作可用性
配置管理要求	配置管理
监控和日志要求	监测和记录
漏洞管理要求	漏洞管理
事件管理要求	事件管理
安全开发要求	安全系统开发生命周期
法律法规要求	法律
安全治理要求	治理