ICS 35.020
CCS L 80

T/CS

团 体 标 准

T/CS 443—2026

智能设备安全控制技术规范

Technical specification for safety control of intelligent device

2026－06－24 发布 2026－06－24 实施

中国商品学会 发 布

目　　次

前言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 总体要求 1
4.1 基本原则 1
4.2 安全架构 1
5 物理防护 2
5.1 防拆保护 2
5.2 环境防护 2
5.3 接口防护 2
5.4 介质保护 2
6 身份认证 2
6.1 认证要求 2
6.2 认证机制 2
6.3 认证分级 3
7 数据安全 3
7.1 数据分类 3
7.2 数据存储 3
7.3 数据传输 3
7.4 数据完整 3
7.5 数据脱敏 3
8 设备运行 4
8.1 启动安全 4
8.2 固件安全 4
8.3 系统加固 4
8.4 漏洞管理 4
8.5 恶意代码防护 4
9 网络通信 5
9.1 网络接入 5
9.2 通信协议 5
9.3 边界防护 5
9.4 入侵检测 5
10 安全监测 6
10.1 安全日志 6
10.2 事件监测 6
10.3 事件响应 6

10.4 安全审计 6
11 运维管理 7
11.1 安全配置 7
11.2 补丁管理 7
11.3 数据备份 7
12 安全管理制度 7
参考文献 8

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专利的责任。

本文件由河南城建学院提出。

本文件由中国商标学会归口。

本文件起草单位：河南城建学院、余姚市富运电子科技有限公司、上海芙达机械制造有限公司、宁波泓耀光电部件有限公司、百家云（宁波）标准技术服务有限公司。

本文件主要起草人：张洛花、黄福贵、刘洪、方科杰、赵红、唐寿生、禹伟伟、童嘉韬。

智能设备安全控制技术规范

1 范围

本文件规定了智能设备物理防护、身份认证、数据保护、设备运行、网络通信、监测响应及运维管理等方面的安全控制要求。

本文件适用于智能设备在安全控制过程中的设计、实施与管理。

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 25069 信息安全术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

智能设备 intelligent devices

具备测量、控制与通信功能，内置处理器的装置，用于实现智能控制任务。

[来源：GB/T 36211-2018,3.1.1,有修改]

3.2

明文形式 plaintext

未经过加密或其他保护处理、可被直接识别的数据表示形式。

3.3

会话 session

用户完成身份认证后，系统为维持其登录状态而建立的交互过程。

4 总体要求

4.1 基本原则

4.1.1 智能设备安全控制应进行分级保护，根据设备的重要性、业务影响程度及数据敏感性确定安全控制强度。

4.1.2 智能设备安全控制应覆盖设备全过程，包括设计、开发、部署、运行及运维阶段。

4.1.3 智能设备应使用最小必要功能，仅启用满足业务需求的功能、端口及服务。

4.1.4 智能设备应安全可控，应支持安全策略配置、状态监测及异常处置能力。

4.2 安全架构

4.2.1 智能设备安全架构应采用分层设计，至少包括设备层、通信层和应用层，各层之间应进行安全隔离。

4.2.2 不同安全域之间应采用访问控制机制进行隔离，跨域访问应进行身份认证。

4.2.3 智能设备应支持基于身份的访问控制机制，对用户或设备访问请求进行动态验证。

4.2.4 智能设备宜支持零信任安全架构模式，对所有访问请求进行持续验证，不应基于网络位置默认信任。

注： 零信任安全架构是指不默认信任设备或网络位置，对访问请求均进行验证的一种安全控制方式。

5 物理防护

5.1 防拆保护

5.1.1 智能设备应具备防拆卸或防篡改能力，防止未经授权的物理接触导致安全风险。

5.1.2 对关键部件或存储区域，应采取防拆结构设计。

5.1.3 设备被非法拆卸或开启时，宜具备功能限制措施。

5.2 环境防护

5.2.1 智能设备应具备与其应用环境相适应的防护能力，防止因外部环境因素影响设备安全运行。

5.2.2 根据应用场景，设备应具备防水、防尘、防高温、防低温或防腐蚀等能力。

5.2.3 环境因素可能影响设备安全功能时，应采取保护措施或进行安全隔离。

5.3 接口防护

5.3.1 智能设备的物理接口应采取防护措施，防止未授权接入。

5.3.2 未使用的接口应关闭或进行物理封堵。

5.3.3 对调试接口应进行权限限制。

5.4 介质保护

5.4.1 存储敏感数据的物理介质应采取保护措施，防止被非法读取、复制或篡改。

5.4.2 设备报废、维修或转移时，应对存储介质进行数据清除。

5.4.3 宜采用加密存储、安全芯片等技术手段。

6 身份认证

6.1 认证要求

6.1.1 智能设备应对用户及接入设备实施身份认证，未经认证的主体不应获得访问权限。

6.1.2 身份认证信息应具有唯一性，不同用户或设备不应共用认证标识。

6.1.3 智能设备应支持基于口令的身份认证机制，口令长度不应少于8位，应包含字母、数字及符号中至少两类，宜每90天更换口令一次。

6.1.4 对连续认证失败的情况应进行限制，连续失败次数不应超过5次，超过后应采取临时锁定措施。

6.1.5 身份认证信息在存储和传输过程中应采用加密保护措施，不应以明文形式存储或传输。

6.2 认证机制

6.2.1 智能设备应支持至少一种身份认证方式，包括口令认证、证书认证或基于硬件的认证方式。

6.2.2 对远程访问或高风险操作，宜采用多因素认证机制。

6.2.3 身份认证成功后，会话在无操作状态下的超时时间不应超过30 min。

6.2.4 应对认证过程进行记录，记录内容应包括认证时间、认证主体及认证结果。

6.3 认证分级

6.3.1 应根据业务重要性及安全风险，对身份认证机制进行分级管理。

6.3.2 认证强度宜划分为以下等级：

a) 一级认证：采用单因素认证；
b) 二级认证：采用双因素认证；
c) 三级认证：采用多因素认证。

示例：用户登录设备时同时输入口令、使用手机验证码，并通过指纹识别完成三次验证。

6.3.3 对涉及重要业务或敏感数据的访问，应采用不低于二级认证强度。

示例：重要业务或敏感数据的访问包括访问设备管理平台、查询或导出用户信息、查看设备运行数据等。

6.3.4 对涉及关键控制或高风险操作的访问，应采用三级认证强度。

示例：对涉及关键控制或高风险操作的访问包括设备远程控制、关键参数配置修改、固件升级、权限变更、系统初始化等。

7 数据安全

7.1 数据分类

7.1.1 智能设备应对处理的数据进行分类分级管理，根据数据的重要性和敏感程度划分数据类别及安全等级。

7.1.2 数据分类宜至少包括以下类型：

a) 一般数据；
b) 重要数据；
c) 敏感数据。

7.1.3 不同类别数据应采取差异化保护措施，数据敏感性越高，保护强度应越高。

7.2 数据存储

7.2.1 智能设备存储数据时，应采取访问控制措施，防止未授权访问。

7.2.2 敏感数据不应以明文形式存储，应采用加密或脱敏方式进行保护。

7.2.3 数据存储应具备完整性保护措施，能够检测数据被篡改的情况。

7.2.4 对敏感数据的访问应进行记录，记录内容应包括访问主体、访问时间及访问结果。

注1：访问对象是指被访问的数据资源或数据类别。
注2：访问行为是指对数据执行的操作类型，如查询、新增、修改、删除、导出等。
注3：访问结果是指访问操作的执行情况，如成功、失败或被拒绝等。

7.3 数据传输

7.3.1 数据在传输过程中应采用加密保护措施，可采用进行数据脱敏。

7.3.2 数据传输宜采用安全通信协议，协议版本不宜低于TLS 1.2。

7.3.3 传输敏感数据时，应对数据完整性进行校验。

7.4 数据完整

7.4.1 智能设备应具备数据完整性校验机制，能够识别数据在存储或传输过程中被篡改的情况。

7.4.2 数据完整性保护宜采用校验码、哈希算法或数字签名等技术手段。

7.5 数据脱敏

7.5.1 对涉及敏感数据的展示或共享，应进行数据脱敏处理。

7.5.2 数据脱敏处理应保证在不影响业务使用的前提下，降低敏感信息暴露风险。

7.5.3 常见脱敏方式包括但不限于数据遮蔽、替换、泛化或加密处理。

7.5.4 对个人敏感信息进行脱敏时，宜满足以下要求：

a) 标识信息应部分隐藏；
b) 关键字段应不可逆处理；
c) 脱敏后数据不应直接识别特定个人。

8 设备运行

8.1 启动安全

8.1.1 智能设备应建立可信启动机制，确保设备仅加载经过验证的合法软件。

注： 可信启动是指在设备启动过程中逐级验证软件完整性与合法性的机制。

8.1.2 启动过程应对固件、操作系统及关键配置进行完整性校验，校验方式宜采用数字签名或哈希校验。

8.1.3 启动验证失败时，设备不应进入正常运行状态，应进入安全模式或停止启动。

8.1.4 启动安全机制应防止未授权固件加载。

8.2 固件安全

8.2.1 固件应进行完整性保护，发布前应进行数字签名。

8.2.2 固件升级应进行来源认证及完整性校验，未经验证的固件不应安装。

8.2.3 固件更新过程应采用加密传输方式。

8.2.4 固件应具备防回滚机制，不应允许降级至存在已知安全漏洞的版本。

8.2.5 固件更新失败时，应具备恢复机制，保证设备可正常启动。

8.3 系统加固

8.3.1 智能设备应关闭不必要的端口、服务及功能组件。

8.3.2 系统口令复杂度应满足以下要求：

a) 长度不应少于 8 位；
b) 应至少包含字母、数字及特殊字符中的两类。

8.3.3 系统应限制登录失败次数，连续失败次数不应超过5次。

8.3.4 应对关键系统资源（包括CPU、内存、存储）进行使用监测，资源异常时应进行反馈。

8.4 漏洞管理

8.4.1 智能设备应建立漏洞管理机制，包括漏洞识别、评估、修复和验证等环节。

8.4.2 应定期开展漏洞扫描，扫描周期不应超过90天。

8.4.3 对高危漏洞应在发现后24 h内完成评估并制定修复方案，并在48 h或72 h内完成修复。

8.4.4 漏洞修复后应进行验证，确保漏洞已被有效消除。

8.4.5 应能及时获取国家信息安全漏洞库或相关通告信息。

8.5 恶意代码防护

8.5.1 智能设备应具备恶意代码防护能力，防止病毒、木马等恶意程序运行。

8.5.2 应对可执行程序进行来源验证，未经授权的软件不应运行。

8.5.3 恶意代码特征库或检测规则应定期更新，更新周期不宜超过30天。

8.5.4 检测到恶意代码时，应采取隔离、清除或阻断措施。

8.5.5 应记录恶意代码检测及处置过程。

9 网络通信

9.1 网络接入

9.1.1 智能设备接入网络前，应进行身份认证，未经认证的设备不应接入网络。

9.1.2 网络接入应采用接入控制机制，限制未授权设备接入。

9.1.3 对接入设备应进行唯一标识管理，标识应具有唯一性。

9.1.4 应对接入设备的网络行为进行监测，对异常接入行为进行识别和处置。

9.2 通信协议

9.2.1 智能设备网络通信应采用安全通信协议，不应使用存在已知安全漏洞的协议版本。

9.2.2 采用基于传输层的安全通信协议时，协议版本不宜低于TLS 1.2。

9.2.3 涉及敏感数据的通信应进行加密处理，不应以明文形式传输。

9.2.4 通信双方应进行身份认证，宜采用双向认证机制。

示例：设备通过验证平台证书确认连接对象的合法性，同时平台通过验证设备证书确认接入设备的身份。

9.2.5 网络通信应具备完整性保护机制，宜采用消息认证码或数字签名方式。

9.2.6 应采取措施防范重放攻击，宜通过随机数、时间戳或会话标识实现。

示例：在设备控制指令通信过程中，攻击者可能截获合法指令并重复发送，导致设备重复执行操作。通过在通信数据中引入时间戳或随机数，可使设备识别重复请求并拒绝执行，从而防止重放攻击。

9.3 边界防护

9.3.1 智能设备网络边界应设置访问控制机制，限制非授权访问。

9.3.2 应对进出网络边界的数据流进行控制，禁止非法访问和异常通信。

9.3.3 应部署边界防护设备，如防火墙、网关等，对网络流量进行过滤和控制。

9.3.4 应对外部访问进行最小化开放，仅开放业务必要端口和服务。

9.3.5 应对网络边界访问行为进行记录。

9.4 入侵检测

9.4.1 智能设备或其所在网络应具备入侵检测能力，对异常网络行为进行监测。

9.4.2 入侵检测应至少识别以下行为：

a) 非法访问尝试；
b) 异常流量行为；
c) 已知攻击特征行为。

9.4.3 入侵检测规则或特征库应定期更新，更新周期不宜超过30天。

9.4.4 入侵检测及处置过程应记录。

10 安全监测

10.1 安全日志

10.1.1 智能设备应对关键安全事件进行记录。

10.1.2 安全日志记录内容应至少包括：

a) 事件发生时间；
b) 事件类型；
c) 操作主体标识；
d) 事件结果。

10.1.3 安全日志时间应与统一时间源保持同步。

10.1.4 安全日志保存期限不应少于6个月。

10.1.5 应采取保护日志完整性，防止未授权删除或篡改。

10.1.6 安全日志应支持查询、导出及分析功能。

10.2 事件监测

10.2.1 智能设备应具备安全事件监测能力。

10.2.2 智能设备应至少监测以下安全事件：

a) 身份认证失败；
b) 异常访问行为；
c) 恶意代码检测事件；
d) 网络攻击行为。

10.2.3 对关键安全事件应实现实时或近实时监测。

10.2.4 安全事件监测规则应定期更新，更新周期不宜超过30天。

10.2.5 应对异常行为进行关联分析，提高事件识别准确性。

10.3 事件响应

10.3.1 智能设备应对安全事件进行响应，包括事件识别、分析、处置及恢复等环节。

10.3.2 应根据安全事件影响程度进行分级响应。

10.3.3 宜具备自动化响应能力，对已知攻击行为可自动采取阻断、隔离或限流措施。

10.3.4 应对事件处理过程进行跟踪和验证，确保问题得到有效解决。

10.4 安全审计

10.4.1 应对设备运行及安全事件进行审计。

10.4.2 安全审计应覆盖以下内容：

a) 用户操作行为；
b) 系统配置变更；
c) 安全事件处理过程。

10.4.3 应定期开展安全审计，审计周期不应超过12个月。

10.4.4 审计结果应形成报告，并用于安全改进。

10.4.5 审计数据应妥善保存，防止泄露或篡改。

11 运维管理

11.1 安全配置

11.1.1 智能设备应对系统配置进行统一管理。

11.1.2 应制定安全配置基线，并对设备配置进行基线校验。

注： 安全配置基线是指设备在运行过程中应满足的最低安全配置要求。

11.1.3 安全配置应覆盖以下内容：

a) 账户及权限配置；
b) 网络服务配置；
c) 安全功能配置；
d) 日志与审计配置。

11.1.4 应对配置变更进行控制，未经授权的配置变更不应实施。

11.1.5 配置变更应进行记录，记录内容应至少包括变更时间、变更内容及操作人员。

11.1.6 应定期开展配置核查，核查周期不应超过90天。

11.2 补丁管理

11.2.1 智能设备应对系统及软件补丁进行统一管理。

11.2.2 应及时获取补丁信息，包括操作系统、应用软件及第三方组件补丁。

11.2.3 补丁安装前应进行测试验证，确保不影响系统正常运行。

11.2.4 补丁安装后应进行验证，确认补丁已正确生效。

11.2.5 应记录补丁管理在获取、测试、安装及验证等环节的过程。

11.3 数据备份

11.3.1 智能设备应对关键数据进行定期备份。

11.3.2 关键数据备份频率不应低于每月1次。

11.3.3 重要数据宜采用异地备份或多副本存储方式。

11.3.4 应定期开展数据恢复测试，测试周期不应超过12个月。

11.3.5 数据恢复过程应确保在发生故障时能够及时恢复业务。

11.3.6 备份数据应采取访问控制及加密保护措施。

12 安全管理制度

12.1 安全管理制度应至少包括：

a) 安全责任制度；
b) 访问控制制度；
c) 运维管理制度；
d) 安全事件处理制度。

12.2 应明确安全管理职责，落实到具体岗位。

12.3 应定期开展安全培训，提高相关人员安全意识。

12.4 安全管理制度应定期评审和更新，评审周期不应超过5年。

参 考 文 献

[1] GB/T 20988-2025 网络安全技术 信息系统灾难恢复规范
[2] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 25069-2022 信息安全技术 安全术语
[4] GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求
[5] GB/T 35273-2020 信息安全技术 个人信息安全规范
[6] GB/T 38636-2020 信息安全技术 传输层密码协议（TLCP）
[7] JR/T 0071.2-2020 金融行业网络安全等级保护实施指引 第2部分：基本要求