ICS 97.030
CCS Y 60

中华人民共和国国家标准

GB/T 41789—2022

智能家用电器的通用安全技术要求

General safety technology requirements for intelligent household appliances

2022-10-12 发布　　2023-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

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

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国轻工业联合会提出。

本文件由全国家用电器标准化技术委员会(SAC/TC 46)归口。

本文件起草单位：中国家用电器研究院、青岛海尔智能技术研发有限公司、上海奥航智能科技有限公司、公安部第三研究所、美的集团股份有限公司、安徽众家云物联网科技有限公司、惠而浦(中国)股份有限公司、中家院(北京)检测认证有限公司、青岛国创智能家电研究院有限公司、北京小米电子产品有限公司、青岛海尔科技有限公司、广东产品质量监督检验研究院、长虹美菱股份有限公司、海信家电集团股份有限公司、珠海格力电器股份有限公司、广东美的制冷设备有限公司、松下家电(中国)有限公司、台州市产品质量安全检测研究院、杭州萤石软件有限公司、美的网络信息服务(深圳)有限公司、无锡小天鹅股份有限公司、北京亚都环保科技有限公司、西安庆安制冷设备股份有限公司、安徽中认倍佳科技有限公司、广东天际电器股份有限公司、广东顺德格意威登电器有限公司、深圳市智慧湾科技有限公司。

本文件主要起草人：马德军、冯承文、胡志强、刘继顺、丁宁、魏明然、王滨后、徐祥智、赵鹏、谢厂节、洪焕健、陈灿峰、张艳丽、井皓、余华超、陈峰峰、陈坚波、陈林、陈进、赵希枫、沈开阳、周小俊、翁晓伟、胡思冬、张革、王小慧、沙露、刘杰、吕全彬、杨洪文。

引　言

相对于传统家电，智能家电的安全会有非常多的不确定性，如外部通信网络的引入对智能家电的安全、信息安全以及功能安全可产生影响；智能家电系统由智能家电、网络系统、控制终端、服务平台等共同组成，智能家电的安全依赖于智能家电系统的支持；家用电器增加智能化功能后，有些电器性质就转变为无人照看的电器，需根据不同的应用场景增加相应的技术要求才能确保家电的安全运行；智能家电人机交互方式的多样性也使智能家电的安全状况发生相应的变化；智能家电的安全涵盖全生命周期，涉及智能家电销售、安装、运行、维修、维护、回收、再利用等。

因此，为了解决家用和类似用途电器由于具有了智能化功能以及由这些具有智能化功能的器具所组成的系统在生命周期中可能出现各种安全风险问题，需要一份安全标准来进行总体规范。

本文件给出了判断具有智能化功能的家用和类似用途电器是否安全的技术要求，建议同时使用对应电器安全标准，以便更全面地评估智能家用电器的安全性。

智能家用电器的通用安全技术要求

1 范围

本文件规定了智能家用电器的术语和定义、缩略语、电器安全要求、信息安全要求、功能安全要求、指示、标识和说明。

本文件适用于单相器具额定输入电压不超过 250 V，其他器具额定电压不超过 480 V 的智能家用电器（以下简称“智能家电”）。

注 1：本文件涉及家用和类似用途电器应用了智能化技术后预计可能产生的危险。

注 2：本文件还涉及了智能家电设备联动和在特定应用场景下的安全要求。

注 3：本文件中涉及的家用和类似用途机器人的安全要求还需要考虑应用其他附加要求。

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—2022 信息安全技术 术语

GB/T 28219—2018 智能家用电器通用技术要求

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 36423 智能家用电器操作有效性通用要求

GB/T 37024—2018 信息安全技术 物联网感知层网关安全技术要求

GB 38189—2019 与通信网络电气连接的电子设备的安全

GB/T 40979 智能家用电器个人信息保护要求和测评方法

GB/T 41387 信息安全技术 智能家居通用安全规范

IEC 60335（所有部分） 家用和类似用途电器 安全（Household and similar electrical appliances—Safety）

IEC 60335-1:2020 家用和类似用途电器 安全 第 1 部分：通用要求（Household and similar electrical appliances—Safety—Part 1: General requirements）

IEC 62368-1:2018 音频、视频、信息和通信技术设备 第 1 部分：安全要求（Audio/video, information and communication technology equipment—Part 1: Safety requirements）

3 术语和定义

GB/T 25069—2022、GB/T 28219—2018 界定的以及下列术语和定义适用于本文件。

3.1

智能家用电器 intelligent household appliances

应用了智能化技术或具有了智能化能力/功能的家用和类似用途电器。

注：智能家用电器也称智慧家电、人工智能家电等。

[来源:GB/T 28219—2018,3.8]

3.2

授权 authorization

根据预先认可的安全策略,赋予主体可实施相应行为权限的过程。

[来源:GB/T 25069—2022,3.559]

3.3

加密 encipherment encryption

对数据进行密码变换以产生密文的过程。

[来源:GB/T 25069—2022,3.278]

4 缩略语

下列缩略语适用于本文件。

ADB:安卓调试桥 (Andorid Debug Bridge)

AES:高级加密标准(Advanced Encryption Standard)

API:应用程序接口(Application Programming Interface)

APP:应用程序(Application)

ARP:地址解析协议(Address Resolution Protocol)

DHCP:动态主机设置协议(Dynamic Host Configuration Protocol)

DNS:域名系统(Domain Name System)

ECC:椭圆曲线密码学(Elliptic Curve Cryptography)

FTP:文件传输协议(File Transfer Protocol)

HTTP:超文本传输协议(Hyper Text Transfer Protocol)

ICMP:互联网控制报文协议(Internet Control Message Protocol)

IP:互联网协议(Internet Protocol)

NTP:网络时间协议(Network Time Protocol)

OTA:空中下载技术(Over-the-Air Technology)

PSK:预共享密钥(Pre-shared Key)

SSH:安全外壳协议(Secure Shell)

URL:统一资源定位系统(Uniform Resource Locator)

5 电器安全要求

5.1 基本要求

智能家电应符合 IEC 60335-1:2020 或 IEC 60335(所有部分)的要求,与通信网络电气连接的智能家电还应符合 GB 38189—2019 的适用要求。

5.2 泄漏电流

具备远程控制/联动控制的智能家电,总泄漏电流按照 IEC 60335-1:2020 规定的限值,取较大值作为限值,而不应将系统中各部分的限值数值累加。

5.3 天线端子绝缘

应符合 IEC 62368-1:2018 中 5.4.5 的要求。

5.4 防止外部电路产生瞬态电压的保护措施

应符合 IEC 62368-1:2018 中 5.4.10 的要求。

5.5 电网电源和由同轴电缆构成的外部电路之间的绝缘

应符合 IEC 62368-1:2018 中 5.5.8 的要求。

5.6 外部电路引起的预期接触电压和接触电流

应符合 IEC 62368-1:2018 中 5.7.7 的要求。

5.7 来自外部电路的接触电流总和

应符合 IEC 62368-1:2018 中 5.7.8 的要求。

5.8 内部和外部布线

智能家电的内部和外部布线应符合 IEC 62368-1:2018 中 6.5 的要求,取 IEC 60335(所有部分)和 IEC 62368-1:2018 中最严酷的要求。

5.9 连接附属设备引起着火的安全防护

应符合 IEC 62368-1:2018 中 6.6 的要求。

5.10 开关

在工作时移动的电动智能家电和组合型智能家电,或带有易触及的运动部件的智能家电,应在明显的位置上设置有可以手动关闭或停止的优先序按钮或拉杆,可以停止智能家电在正常或危险工作时的当前操作,且应在智能家电外表面显著位置设置按钮或拉杆的明显标识。

5.11 伸缩天线或拉杆天线

应符合 IEC 62368-1:2018 中 8.12 的要求。

5.12 辐射

应符合 IEC 62368-1:2018 中第 10 章的要求。

6 信息安全要求

6.1 通用要求

智能家电应符合 GB/T 40979 和 GB/T 41387 的要求。

智能家电需保护的数据和信息分类见附录 A。

权限控制功能是对智能家电相关操作权限的管理和控制,只有符合权限控制的用户才能对智能家电进行相应配置和操作。

本章要求中部分条款分为基本要求和增强要求,基本要求为必选项,增强要求是根据需要为达到更高的信息安全保护所设置,为可选推荐项。

6.2 设备标识与鉴别

6.2.1 唯一标识码

唯一标识码要求可分为基本要求和增强要求。

基本要求如下：

智能家电应具备唯一标识码，且具有逻辑或物理的安全机制保护标识不被修改、擦除。智能家电唯一标识码是能够在网络中唯一标识智能家电的编码，每台智能家电至少具备一个唯一标识码，一台智能家电原则上对应一个唯一标识码，针对组合智能家电可以一台智能家电对应多个唯一标识码。

增强要求如下：

唯一标识码应采用硬件安全区域、安全模块或安全芯片进行存储。

6.2.2 身份鉴别

身份鉴别要求如下：

a) 智能家电应具有向控制终端和服务平台单向身份鉴别的能力；

b) 智能家电整机应与内部的通信模块及其他存储或处理智能家电需保护的数据和信息的模块或元器件具有绑定关系。

6.3 物理安全

物理安全要求如下：

a) 有安全防护需求的智能家电在设计中应提供物理保护机制，在受到暴力移除或拆卸时应有有效的报警和防护机制，智能家电应具备一定的防物理攻击的能力，保护其内部数据不被篡改和窃取；

b) 应无法通过内部和/或外部暴露的物理走线、引脚或接口等媒介获取智能家电需保护的数据和信息。

6.4 接口安全

智能家电应采取以下措施保护接口安全：

a) 智能家电硬件应避免非必要地暴露物理接口，在出厂前应关闭不必要的硬件端口，不预留后门，对于可物理接入的调试接口，应能在软件中关闭；

b) 关闭所有未使用的网络接口和逻辑端口；

c) 应默认关闭可直接进入智能家电系统的特权能力或接口（如工厂 OTA、未公开功能接口、调试后门等），如实属业务必要，应具备鉴权机制；

d) 在初始化状态下，智能家电网络接口应能防止向未经认证的用户泄露相关安全信息，如设备配置、内核版本、固件版本、操作系统版本和应用软件版本等；

e) 应仅为用户分配最小必要的接口访问权限；

f) 应有打开和关闭通信接口的开关机制，接入外部通信时应具有身份鉴别机制。

6.5 地理位置信息鉴别

具备地理位置信息获取和上送能力的智能家电，应满足以下要求：

a) 应对地理位置信息获取和上送的硬件模块进行保护，防止被不正当移除、关闭或破坏；

b) 应对地理位置信息进行有效保护，防止其被未授权访问、非法采集和篡改。

6.6 环境适应性

环境适应性为增强要求，具体要求如下：

a) 环境条件或操作条件发生变化时，智能家电的信息安全应能达到与环境相适应的安全水平；

b) 智能家电应具有针对环境的安全保护机制，当遇到异常环境（如温度、电压、电磁辐射、光照等）时，应采取有效措施，使智能家电需保护的数据和信息不被窃取或者泄露。

6.7 固件安全

固件安全要求可分为基本要求和增强要求。

基本要求如下：

a) 应具备固件更新机制，更新前应取得用户确认；

b) 应对远程下载的固件更新文件的来源进行校验；

c) 应具备固件下载传输通道安全机制，防止中间人攻击或嗅探；

d) 应具备对固件升级文件完整性校验的机制；

e) 应确保固件升级失败后，保持原有固件的可用性；

f) 应确保固件不能通过串口读取等手段提取出；

g) 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；

h) 不应将登录用户名、口令等登录凭证明文存储在固件中；

i) 应防止未授权的固件回退，即通过 OTA 功能进行智能家电更新时，智能家电端应拒绝旧版固件更新；只有在授权的情况下，固件才可以回退到比当前版本更低的版本；

j) 智能家电的启动过程应具备自检功能，应能对智能家电固件的完整性和真实性进行自检，出现问题时，智能家电及其功能应以安全的方式自动失效。

注：自检包括完整性和真实性，其目标是检查固件、针对有篡改迹象的安全机制以及智能家电是否处于被攻破状态。

增强要求如下：

固件应加密存储。

6.8 操作系统安全

6.8.1 一般要求

带有操作系统的智能家电应符合 6.8.2～6.8.7 的要求。

6.8.2 操作系统集成安全

智能家电在进行操作系统服务裁剪时，应符合模块最小化原则，仅保留必须的模块。

6.8.3 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鉴别机制，防止非法用户或应用控制操作系统；

c) 系统不应预留任何未公开账号，所有账号应可被操作系统管理；

d) 不应存在绕过正常身份鉴别机制直接进入到系统的隐秘通道，如特定端口、特定客户端、特殊 URL 等；

e) 智能家电在进行远程访问或远程操作时应设置安全的用户口令，口令要定期进行修改，口令需要有一定的复杂性、强度或长度的要求，口令最小字符长度应为 8 个字符，由大小写字母、数字、特殊符号中的两种或两种以上类型组成。

6.8.4 操作系统安全启动认证

启动操作系统时，应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，系统方能正常启动。

6.8.5 操作系统配置安全

对于具备调试功能的智能家电，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。

6.8.6 服务配置安全

服务配置安全要求如下：

a) 对于能够安装外部应用程序的系统，操作系统应对调用接口进行权限控制，调用与用户隐私相关的接口应获取用户明确授权；

b) 对于支持远程连接的智能家电，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；

c) 对于通过网页(Web)进行远程管理的智能家电，对其进行管理和配置的行为应经过登录认证，其登录和退出过程需有日志记录，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。

6.8.7 内存的硬件级访问控制机制

智能家电应有用于内存的硬件级访问控制机制，如智能家电的控制器提供内存保护单元。

6.9 应用安全

6.9.1 一般要求

能运行应用程序(APP)的智能家电应符合 6.9.2～6.9.4 的要求。

6.9.2 默认口令安全

默认口令安全要求如下：

a) 智能家电不应使用默认的统一口令，应默认设置不同的口令，或要求用户初次使用时更改口令；

b) 默认口令的生成机制应能降低针对智能家电进行的自动攻击风险，例如，口令应具备足够的随机性；

c) 当智能家电使用基于密码技术的鉴别机制时，采用的密码技术应与其性能、风险和用途相匹配；

d) 当用户登录智能家电进行鉴别时，智能家电应向用户或管理员提供一种机制来更改所使用的鉴别信息；

e) 智能家电应采取措施，防止通过网络登录接口对鉴别机制进行暴力破解。

6.9.3 漏洞管理

漏洞管理要求如下：

a) 公布漏洞管理策略应包括漏洞通报联系信息和漏洞处置流程信息，应通过周期性的漏洞评估来确保对智能家电安全漏洞的及时监测；
b) 应能确保对新发现的漏洞进行及时的评估和分类处理；
c) 应具备能够持续监控、发现和修复产品和服务安全漏洞的安全机制；
d) 应能通过使用适当、已声明的安全协议来提供机密性、完整性、真实性和防止重放的安全保护；
e) 智能家电应验证更新内容的完整性和真实性；
f) 应基于国家信息安全漏洞库(CNNVD)作为漏洞评测依据。

6.9.4 应用完整性和真实性

应用完整性和真实性要求如下：
a) 智能家电应验证应用的完整性和来源的真实性；
b) 智能家电应用应对自身的完整性和来源的真实性执行自检。

6.10 通信安全

6.10.1 非明文传输和安全认证

非明文传输和安全认证要求可分为基本要求和增强要求。
基本要求如下：
a) 关键安全参数应采用非明文方式传输，保障通过远程接入网络访问时的关键安全参数的保密性；
b) 采用密码技术保障传输安全时，密码技术相关联网和安全功能模块应经过评估，并支持密码算法、组件、参数更新；
c) 如用户可以通过网络直接访问智能家电，则智能家电应在进行用户身份鉴别后，才能通过网络接口访问智能家电功能；
d) 如用户可以通过网络直接访问智能家电，则智能家电应在进行用户身份鉴别后，才能通过网络接口按照使用说明书的规定修改安全相关配置参数(如权限管理、网络密钥配置、口令变更等)，但 ARP、DHCP、DNS、ICMP、NTP 等网络服务协议除外；
e) 对于与智能家电有关的关键安全参数，制造商应具备安全管理流程；
f) 智能家电应将与其他智能家电或应用通信的信道进行加密，并在会话结束时及时销毁会话密钥；
g) 智能家电不应将用于传输加密的密钥硬编码写在程序代码中，应通过 PSK(预共享密钥)密钥导出等方式生成传输加密的密钥；
h) 智能家电与平台端进行通信时，应在数据传输之前向平台端提供身份鉴别，检查控制权限是否与身份匹配，以防止越权或非授权控制；
i) 智能家电之间直接进行通信时，应在数据传输之前验证对方的身份是否合法，检查控制权限是否与身份匹配，以防止越权或非授权控制；
j) 智能家电通信应使用滚动码或计数器机制，当请求操作计数大于智能家电计数才准许智能家电执行该操作指令，以防止他人通过抓包重放控制请求来对智能家电进行非授权的控制；
k) 智能家电应根据操作系统类型默认关闭高风险管理服务或信息数据服务，如 FTP、SSH、远程登录协议(Telnet)、HTTP、ADB 等；
l) 智能家电通信应有防重放攻击的有效性校验(例如，时间戳等)，以防止通信内容被截取后的“重放攻击”。

增强要求如下：

智能家电通信时应在数据传输之前进行双向认证，验证双方真实身份是否合法，检查控制权限是否与身份匹配，以防止越权或非授权控制。

6.10.2 通信端口安全

通信端口安全要求如下：

a) 端口开放应遵循最小化原则，默认关闭非必须使用的端口，如 Telnet、SSH 等服务端口；对于必须使用的端口，使用后应立即关闭；

b) 智能家电应提示用户所有开放的端口，并告知对业务影响。用户可自主选择对服务端口开放或关闭的配置功能，避免存在用户未知且无法关闭的服务端口。

6.10.3 智能家电接入网关安全

具备接入网关功能的智能家电，应满足 GB/T 37024—2018 中 6.2 的要求，对于安全等级要求较高的应用场景，应满足 GB/T 37024—2018 中 7.2 的要求。

6.11 数据安全

6.11.1 永久性关键安全参数存储

智能家电应采取措施确保关键安全参数存储安全，要求如下：

a) 采取安全的方式存储智能家电上永久存储介质中的关键安全参数；

b) 出于安全目的在智能家电中使用该智能家电的唯一标识时，应防止通过物理、电气或软件等手段进行篡改；

c) 任何用于软件更新的完整性和真实性检查以及与智能家电软件中相关通信服务保护的关键安全参数，应对于每个智能家电都是唯一的，且其生成方式宜考虑降低对各类智能家电受到自动攻击的风险。

6.11.2 输入数据验证

智能家电应对输入数据进行验证，包括远程控制端通过用户界面输入的数据、通过应用程序编程接口（API）输入的数据等。

6.11.3 安全存储

智能家电的安全存储要求分为基本要求和增强要求。

基本要求如下：

a) 智能家电应提供安全存储功能，保护存储数据的完整性和可用性；

b) 有机密性要求的智能家电需保护的数据和信息在其进行存储时，应保护其机密性。

增强要求如下：

智能家电需保护的数据和信息采用硬件安全区域、安全模块或安全芯片进行存储。

6.11.4 内存数据安全要求

智能家电应对关键安全参数的存在时间和使用次数进行控制，当使用完毕或超时时，关键安全参数及其过程信息应立即从内存中被清除。

6.11.5 人机交互的信息安全要求

智能家电的人机交互过程应遵循国家、行业相关管理规定，确保用户个人敏感信息安全。对予以保

密的信息，人机交互界面呈现应采取隐藏或隐秘的方式，如对银行卡号信息部分屏蔽等。

6.12 密码功能

6.12.1 密钥生成

有密钥生成功能的智能家电，密钥生成要求可分为基本要求和增强要求。

基本要求如下：

a) 产生的非对称密钥，应满足参数的合法性检查、密钥长度等要求；

b) 产生的对称密钥，应采用多级密钥体系进行管理，如采用设备唯一标识参与派生；

c) 产生的会话密钥，应确保每次会话的密钥不可预期，且具有对应的密钥更新机制；

d) 产生的非对称密钥、对称密钥、会话密钥应满足密钥长度要求和随机性要求；

e) 密钥生成后，除非对称密钥的公钥之外，其他密钥应不可导出；

f) 如未采用硬件方式存储的非关键或临时性密钥，则应以加密、混淆、白盒密钥等逻辑防护措施进行存储。

增强要求如下：

a) 应采用硬件安全模块、安全芯片保护密钥的机密性与完整性；

b) 产生的非对称密钥、对称密钥、会话密钥都应具有对应的密钥更新机制。

6.12.2 密码运算

有密码运算功能的智能家电，密码运算要求如下：

a) 密码运算应在隔离的安全环境里执行，密钥明文不应出现在安全环境以外；

b) 在进行密码运算的过程中，应用进程中不应出现任何密钥数据；

c) 应采用具有足够强度的公开算法进行密码运算，如 SM2、SM3、SM4、SM9、AES、ECC、RSA、SHA256；

d) 应采用足够长度的密钥进行密码运算，如对称算法密钥不少于 128 位、RSA 算法密钥不少于 2 048 位、ECC 算法密钥不少于 224 位。

6.12.3 密钥管理

有密钥管理功能的智能家电，密钥管理要求如下：

a) 确定各密钥的用途，防止非授权的更改和替换；

b) 对于存储在智能家电内的固定密钥，不准许把密钥明文从高安全性的组件传送至低安全性的组件中去；

c) 会话密钥及密钥过程信息使用完毕后应立即从内存中清除；

d) 当密钥不再需要时，应将其销毁；

e) 在密钥被销毁之后，不应有任何信息可用来恢复已销毁的密钥。

6.12.4 随机数

有随机数功能的智能家电，随机数应满足 GB/T 32915 的要求。

6.13 个人信息保护

智能家电应保护用户个人信息，应遵循 GB/T 35273、GB/T 40979 的要求。

6.14 审计日志

智能家电应具备对智能家电需保护的数据和信息的操作和安全事件的审计功能并生成审计日志，

检测到潜在的安全侵害时，应采取合适的响应机制，要求如下：

a） 审计日志应包括日期、时间、操作用户、操作类型等信息；

b） 审计日志中不应包含关键安全参数和个人敏感信息（如用户口令等）；

c） 智能家电应能保护已存储的审计日志，以避免未授权的修改、删除、覆盖等；

d） 智能家电应有日志上传功能。

7 功能安全要求

7.1 安全策略

7.1.1 本地安全优先级应高于远端

智能家电的电器安全不应仅依赖于网络，硬件和安全控制软件保护应作为智能家电的安全保护屏障，在断网或网络状况不佳和无人操作或操作人员缺乏操作知识的情况下，智能家电应能确保自身安全。

7.1.2 机械部件作为最终的安全保护

当智能家电的电子控制部件发生故障或失效，宜采用机械结构部件来实现安全保护，避免引发安全事故。如任何情况下，机械钥匙都能确保从内部或外部开门。

7.2 对可预见的安全风险进行预判和保护

智能家电在启动之前和运行过程中应能对可预见的安全风险进行预判和保护。

智能家电根据具体品类有对应的安全要求，设计原则见附录 B。

7.3 被各种意外打断或中断不能引起功能安全问题

智能家电对于正确的命令应能正确应答，当接收到无效命令（包括错误顺序的命令、未知命令、错误模式下的命令、错误的命令参数）时，应能够不受影响而正常运行。

智能家电在使用智能家电内部和外部感知数据时，应检查数据是否存在安全异常。

智能家电断电、上电、启动、再启动或停止等动作不会对附近的人体、宠物、周围环境造成危害。智能家电不会在动作中断或停止时，由于重新启动而对人体、宠物、周围环境造成危害，不会对智能家电造成损害。也不会由于意外事件引起的停止而对人体造成危害，或者不会对智能家电造成损坏。

智能家电在无人监控状态下出现故障或紧急情况时，应能采取相应的安全保护措施，进行紧急处置和干预，不会对人体、宠物、周围环境造成危害，不会对智能家电造成损害。智能家电在发生可修复性故障时，会进入到故障保护模式，但相关人机交互、网络通信和其他一些基本的安全功能应保持正常。

电磁干扰原因造成的智能家电误动作，智能家电即使发生误动作也不会对人体、宠物、周围环境造成危害，不会对智能家电造成损害。

智能家电运行出现异常时，应进行与故障性质对应的适当的处理，以免造成安全问题。

7.4 人机交互方式的安全

可远程操作的智能家电在开始运行前，应先在智能家电上取得授权，在取得授权后才可以进行远程操作，在对智能家电进行远程操作前，应先获取该智能家电当前的状态。

智能家电接收远程操作指令后应向远程端反馈是否执行成功以及当前状态的情况，如智能家电发生故障，该故障应反映在人机交互的界面上。

当收到远程操作指令后，智能家电应能判断是否会导致安全问题，对于导致安全问题的指令应不予

执行并给出警告提示。

智能家电的人机交互可不依赖于外部网络，如断网或网络状况不佳时，智能家电可以通过其他替代性的人机交互方式对智能家电进行操作，不影响智能家电的正常使用，尤其是基础人机交互功能的使用。

智能家电的人机交互方式需考虑用户的使用场景，这些使用场景下不应使用户产生不安全的问题。

7.5 智能家电的配网和绑定

智能家电的配网和绑定应满足以下要求：

a) 智能家电的配网过程应具备网络认证等安全认证措施，确保在授权用户知情或控制下才能执行配网相关操作；

b) 智能家电需进入到配置状态才可进行配网操作，在规定时间内未进行配网操作应自动退出配置状态；

c) 智能家电在同一时段内应只能绑定一个用户，该用户可以将智能家电的控制权分享给其他用户；

d) 智能家电应能将智能家电和用户的绑定记录存储在服务平台、管理单元或本机中，绑定后的智能家电在使用过程中应对于绑定记录进行验证，验证通过后方可正常使用；

e) 智能家电进行用户解绑时应及时清除本机存储的个人信息，并通知服务平台、管理单元对其存储的用户相关数据进行清除或匿名化处理；

f) 当智能家电端重置并有新的用户绑定该智能家电时，应先清除云端原用户的绑定记录，方可进行绑定操作；

g) 智能家电更换使用主人或用户解绑时应及时清除本机存储的个人信息，并通知服务平台、管理单元对其存储的用户相关数据进行清除或匿名化处理；

h) 智能家电的配网信息和绑定数据应使用安全存储。

7.6 恢复出厂设置

智能家电进行恢复出厂设置，应满足以下要求：

a) 智能家电恢复出厂设置后应完全清除智能家电中联网数据、个人信息和绑定信息，确保存储空间被释放或重新分配前得到完全清除；

b) 应对不再使用的数据信息及其所有副本销毁，如因网络问题，导致信息无法同步，相关信息需在网络恢复后进行数据清除。

7.7 通信

7.7.1 基本要求

对于支持与公共网络通信的软件，应将通信部分划分为独立的软件模块。

通信应由智能家电通过提供以下措施的软件予以建立、实施和终止。

a) 提供涉及以下方面的数据完整性保护：

1) 数据损坏；

2) 地址损坏；

3) 时间或顺序错误；

4) 永久性地“自动发送”或重复；

5) 数据传输中断。

注：数据完整性指数据没有遭受以未授权方式所作的更改或破坏的特性。

b) 提供对于通信进行检测和响应的手段，包括由于任何原因出现的通信信息不完整、截断、包含错误，或者虽然传递的信息格式正确，但超出该类型信息的预期范围等情况。

c) 提供 IEC 60335-1:2020 中表 R.1 规定的控制故障/错误条件的措施。

通过视检以及 IEC 60335-1:2020 中 R.3.2.2 中对软件体系结构的试验，按照 IEC 60335-1:2020 中 R.3.3 对软件的评估检查其符合性。

7.7.2 远程操作会话时长

智能家电的远程操作会话时间不应过长，如超过规定时长，应重新建立会话以及密钥协商。

7.7.3 支持睡眠方式的智能家电安全要求

对于通信部件支持睡眠方式的智能家电，在状态发生变化或需对外发送报警信息时，应能够被唤醒，确保信息及时上报，避免漏报安全事件。

7.8 应用软件的安全

7.8.1 应用软件的管理

智能家电上运行的应用软件，应满足以下要求：

a) 可运行各种应用软件的智能家电，厂商提供的应用软件应通过信息安全、兼容性、功能性的测试，并由该智能家电厂商的授权地址提供；

b) 非预装或非授权的应用软件在安装时应对用户有安全风险提示，经授权用户同意并确认后方可安装；

c) 如安装的应用软件需获取智能家电相关联数据，则应经过授权用户的同意和确认。

7.8.2 应用软件更新

智能家电上运行应用软件，其更新应满足以下要求：

a) 智能家电应具备更新过程相关信息提示功能，含更新正常及异常相关信息提示；

b) 智能家电应验证更新固件的完整性和真实性，如未确认其完整性和真实性，智能家电应拒绝进行固件更新，并删除更新的内容；

c) 智能家电应具有硬件、软件版本对比功能，以确认升级前后的版本信息符合预期；

d) 脱机更新时，应提供安全存储介质进行固件包交付，对固件包的内容应进行签名和加密操作；更新前需要进行管理员校验，如 PIN、密码认证等；

e) 在线更新时，应首先对更新源进行合法性认证，认证操作完成后还应建立安全通道，密文传输更新指令；

f) 更新失败时，应具备智能家电处于安全状态的有效的机制，如自动恢复到未更新时系统的版本，且该版本能正常使用；

g) 应采用防止应用软件版本被降级的措施，防止有安全漏洞的版本被恢复。

7.9 带有操作系统智能家电的用户管理

7.9.1 登录验证

远程操作者身份应通过登录验证后，才能对智能家电进行操作，否则不准许通过远程操作的方式对智能家电进行操作，当验证连续失败次数达到上限值，则锁定该操作者，间隔一定时间后通过有效验证或系统管理员进行解锁操作方可继续。

7.9.2 身份鉴别

智能家电进行身份鉴别的代码逻辑应进行正确的判断，应验证凭证完全正确才能通过认证，应能防止通过空认证凭据跳过认证判断，直接进入控制逻辑。

7.9.3 用户设置

用户设置满足以下要求：

a) 智能家电应设置多种权限用户，如超级用户、普通用户、访客、租客、维修用户等；智能家电的安装配置、系统固件更新、应用软件更新、用户设置应由具有相应权限的用户操作和管理；

b) 远程诊断和维修应由智能家电拥有者的操作授权；

c) 系统软件更新应由智能家电拥有者确认；

d) 智能家电的角色和用户设置应符合 GB/T 36423 的要求。

7.10 维修

当智能家电出现故障或问题时，应经用户的权限许可后，智能家电维修管理者才能通过网络远程接入智能家电并对其进行远程操作。维修管理者通过远程对智能家电进行操作前应停止智能家电常规操作，使智能家电进入到维修状态方可进行维修操作。

7.11 报废

智能家电准备报废时，应将运行期间的所有网络和数据信息一并删除，智能家电本体上的数据也应删除。

7.12 综合场景安全考虑

智能家电应能根据关联其他智能家电、操作人员意图、使用场景等进行综合的安全分析，如关联其他智能家电或操作者发出有损安全的指令，智能决策系统将判断不予执行并给出进一步的处理意见或信息提示。智能家电的智能决策系统给出的进一步操作方案不应对智能家电和操作者产生安全问题，如产生安全问题将停止智能家电当前的操作。

智能化场景宜考虑网络延迟及执行延迟，预留足够的时间使操作执行成功，推荐自动控制延迟时间不低于 50 ms，延迟应具有随自动化场景嵌套深度增加而增加的机制。

智能家电之间可通过联动方式进行智能家电间的操作指令传输，在联动操作时应根据参与联动操作的家电状态，使得联动操作前一级智能家电发出的指令不能引起后一级智能家电的安全问题。进行通信时应在数据传输之前验证对方的身份是否合法，检查控制权限是否与身份匹配，以防止越权或非授权控制。

联动的应用场景应根据厂商提供的文件说明进行联动设置，不应随意通过不同智能家电间进行设置。智能家电在设置时的操作权限，应由用户确认，该操作的使用不应引起智能家电的安全问题。

7.13 日志管理

智能家电应有保存日志记录的能力，该日志可以保存在智能家电中，也可以定期同步到用户授权的云平台中，智能家电应能对日志数据的存储空间进行管理，确保数据不溢出。

智能家电可以保留产品生命周期内的日志数据，在设备和用户解绑后，应提示用户是否销毁日志或匿名化处理，根据用户提示进行销毁或处理。在该产品生命周期结束后，应能对用户个人信息相关日志销毁或匿名化处理。

8 指示、标识和说明

8.1 指示、标识

智能家电应明确标出在其预期配置中的所有外部接口或物理输入或输出接口及所支持的通信协议。

智能家电的各种对外通信接口，应有相对应的配网和网络状态指示，指示不限于智能家电本身。

8.2 说明

8.2.1 通用要求

智能家电应能提供其所有设计功能、安全功能和管理功能的配置说明文件，该文件可以是随机附带的说明书，也可以是电子版说明书。说明书中应包括智能家电在配置、使用、维护、报废过程中可能会引起的安全风险以及出现安全问题的基本解决方案。智能家电在其预期配置中的所有外部接口或物理输入或输出接口列表及所支持的通信协议说明。

8.2.2 配置管理安全指南

智能家电生产厂商应提供并维护智能家电的配置管理安全指南，包括但不限于以下要求：

a) 智能家电或随机附件上需要有通信方式的说明；
b) 应向用户提供安全的配置安装指南；
c) 针对用户提供维护处理的操作指导；
d) 应覆盖整个智能家电，包含固件、应用程序、证书、口令、密钥和配置等；
e) 应覆盖智能家电的整个生命周期，包括初始化、运行、维护和报废等。

8.2.3 安全维护指南

智能家电生产厂商应提供安全维护指南，包括但不限于以下要求：

a) 维护方法应以文档形式明确给出；
b) 维护方法应通过周期性的软件评估来确保对智能家电软硬件问题监测；
c) 维护方法应能确保对新发现的软硬件问题进行及时的评估和分类处理；
d) 维护方法应能确保对可能影响智能家电安全的新发现软硬件问题及时生成补救措施。

8.2.4 更新指南

智能家电生产厂商应提供说明智能家电更新机制的指导文档。

智能家电所采用的更新机制应确保安全，包括但不限于以下要求：

a) 通过使用适当、已声明的安全协议来提供机密性、完整性、真实性和防止重放的安全保护；
b) 智能家电应验证更新内容的完整性和真实性；
c) 智能家电如未确认更新内容的完整性和真实性，则应拒绝进行更新，并删除更新的内容。

附 录 A
（资料性）
智能家电需保护的数据和信息分类

智能家电需保护的数据和信息分类见表 A.1。

表 A.1 智能家电需保护的数据和信息分类

分类	描述	保护需求
公开安全参数	与安全性相关的公开信息，一旦被修改，会威胁到智能家电安全。包括但不限于：公钥、公钥证书、自签名证书、安全配置数据、智能家电唯一标识码等	完整性/真实性
关键安全参数	与安全相关的秘密信息，这些信息被泄露或被修改后会危及智能家电的安全性。关键安全参数可以是明文形式的，也可以是经过加密的。包括但不限于：认证、MAC地址和数据加密使用的对称密钥、私钥、访问控制列表等	完整性/真实性/机密性
固件	在智能家电内部与智能家电安全性相关所有程序代码	完整性/真实性/机密性
智能家电的操作系统	智能家电中使用的操作系统	完整性
智能家电的应用软件	智能家电中安装的应用程序代码集合	完整性/真实性
固件版本信息	智能家电当前固件的版本信息	完整性
智能家电运行数据	智能家电运行过程中产生的相关数据	完整性
家电通信过程数据	智能家电与外部实体通信过程的数据	完整性/真实性/机密性
地理位置信息	智能家电当前的位置信息	完整性/真实性/机密性
个人信息	属于用户的，不属于安全功能数据的信息，如用户身份标识、用户口令等信息	完整性/真实性/机密性

附 录 B
（资料性）
有特殊安全要求的智能家电设计原则

B.1 有儿童或宠物保护需求的智能家电设计原则

对于有儿童或宠物保护需求的智能家电，宜考虑远程启动功能对安全性的影响。如智能家电确有远程启动需求，应具有检测是否存在伤害儿童或宠物等安全隐患的功能，判断有儿童或宠物进入空间内则该智能家电无法启动。推荐远程操作的开启时间有限制，远程操作完成后需关闭远程启动功能，并在下次使用前重新进行授权开启。

B.2 周期性工作的智能家电设计原则

周期性工作的智能家电在远程启动时，需进行完整的运行参数设置过程后方可启动运行，智能家电在运行过程中一旦出现安全问题，可通过远程方式终止运行，一旦该运行周期结束后，需重新进行运行参数设置。

B.3 烹饪类智能家电设计原则

烹饪类智能家电在使用过程中会有火、油烟、高温等危险产生，宜考虑远程启动功能对安全性的影响，但允许有其他远程操作功能（如设置参数、查询状态、关闭），烹饪类智能家电进入到快速升温并超过正常工作温度时，应停止烹饪周期并关闭。

B.4 电动器具类智能家电设计原则

电动工具类智能家电的远程启动和旋转不应导致危险，有人照管的电动器具类智能家电不准许远程启动。

B.5 电加热类智能家电设计原则

电加热类智能家电宜考虑远程启动功能对安全性的影响，但允许有其他远程操作功能（如设置参数、查询状态、关闭），电加热类智能家电进入到快速升温并超过正常工作温度时，应停止加热。

B.6 手持式智能家电设计原则

手持式智能家电不准许远程启动。

B.7 移动类智能家电设计原则

移动式智能家电应能检测障碍物的位置，防止碰伤或人员跌倒的风险，防跌、缠绕电线。

B.8 电池供电类智能家电设计原则

考虑网络待机状态、电池没电或电池功率过小等因素对智能家电的影响。