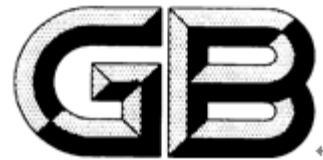


ICS 97.120

CCS K 32



中华人民共和国国家标准

GB/T XXXXX—202X

家用和类似用途电自动控制器空中下载 (OTA) 技术要求

automatic electrical controls for household and similar use

OTA technical requirements

(征求意见稿)

2022-XX-XX 发布

2022-XX-XX 实施

国家市场监督管理总局
中国国家标准化管理委员会

发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略词	2
5 分类	2
6 要求	2
6.1 通用要求	2
6.2 体系要求	2
6.3 连接与通信能力	3
6.4 下载实施	3
6.5 电源	4
6.6 安全性	5
6.7 静默升级方式的额外要求	5
6.8 标识	5
7 测试方法	6
7.1 测试条件	6
7.2 网络连接可靠性测试	6
7.3 固件发现及下载测试	6
7.4 运行固件更新测试	7
7.5 固件成功率的测试	7
7.6 静默升级机制的补充测试	7
7.7 测试报告	7

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。

本文件由全国家用控制器标准化技术委员会（SAC/TC 212）提出并归口。

本文件主要起草单位：XXXX。

本文件主要起草人：XXXX。

家用和类似用途电自动控制器空中下载（OTA）技术要求

1 范围

本文件规定了家用和类似用途电自动控制器（以下简称“控制器”）空中下载（OTA）的分类、要求、测试方法，并界定了相关的术语和定义、缩略语。

本文件适用于家用和类似用途电自动控制器的空中下载功能。

本文件不适用于电视机、手机、计算机等音视频及信息类产品的控制器。

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 14536.1 家用和类似用途电自动控制器 第1部分：通用要求

GB/T 25069 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 41387-2022 信息安全技术—智能家居通用安全规范

3 术语和定义

下列术语和定义适用于本文件

3.1

软件 software

电子控制系统中由数字数据和指令组成的部分。

3.2

固件 firmware

可烧录在硬件（芯片）底层的、使设备得以运行的软件。

3.3

空中下载 over-the-air (OTA)

以无线方式从远程服务器下载固件内容并用于执行的处理过程。

3.4

正常工作 normal operation

控制器按照供应商提供的使用说明中规定的持续工作状态。

3.5

静默升级 silent upgrade

无需用户参与，控制器根据预设机制自动完成升级。

注：虽然在静默升级的过程中无需用户参与，但控制器的静默升级功能开启需要明确得到用户首肯，如在控制器的操作界面或者移动应用界面，由用户确认。

3.6

完整性验证数据 integrity validation data

用以检测数据或文件中的错误或变化的值。

4 缩略词

下列缩略词适用于本文件。

2G 第二代移动通信技术 (the 2nd Generation Mobile Communication Technology)

3G 第三代移动通信技术 (the 3rd Generation Mobile Communication Technology)

4G 第四代移动通信技术 (the 4th Generation Mobile Communication Technology)

5G 第五代移动通信技术 (the 5th Generation Mobile Communication Technology)

CNVD 国家信息安全漏洞共享平台(China National Vulnerability Database)

CNNVD 中国国家信息安全漏洞库(China National Vulnerability Database of Information)

RSSI 接收的信号强度指示(Received Signal Strength Indication)

NB-IoT 窄带物联网 (Narrow Band Internet of Things)

5 分类

控制器在执行空中下载时，分为命令升级、推送升级、静默升级三种方式。

6 要求

6.1 通用要求

6.1.1 控制器应具备更新自身部分或全部运行固件的能力。

6.1.2 控制器及其服务器在设计时，应具备机制将当前固件运行版本与服务器的版本进行比对确认。

对比和更新应采取至少一条以下方式：

a) 命令升级

在控制器本地的控制界面或配套的移动应用界面，由人工操作发起版本查询，在通告结果并得到确认后开始的空中升级。

b) 推送升级

控制器及其服务器在运行中，通过提前设定的机制，自动进行版本查询，当有可升级版本时，在控制器本地的控制界面或配套的移动应用界面中提示信息，由人工操作确认空中升级的开始。

c) 静默升级

控制器及其服务器在运行中，通过提前设定的机制，自动进行版本查询，当有可升级版本时，自动完成控制器升级。

6.2 体系要求

6.2.1 固件升级信息记录

控制器进行OTA升级时，厂商应记录升级信息，包括但不限于：

- a) 软件升级的目的；
- b) 软件升级可能影响家电设备的功能；
- c) 目标家电，及其最新已知配置和升级兼容性的数据信息；
- d) 如何执行软件升级以及执行软件升级的先决条件；
- e) 确认软件升级已经执行并成功通过验证和确认的信息。

6.2.2 管理体系

家用电器制造商应建立软件升级管理体系，确保5.2.1的信息存储在安全服务器上，该信息至少保留10年，并进行访问控制。除终端用户外，涉及OTA相关操作的人员应取得制造商或第三方的资质认可。

6.3 连接与通信能力

控制器宜采用模块化设计，如网络通信部件采用接口方式与控制器主控部分进行软硬件分离。

6.3.1 连接能力

控制器应支持2G、3G、4G、5G、蓝牙、Wi-Fi等无线通信方式中一种或多种功能，且应具备断线重连功能。

6.3.2 通信能力

控制器以及指定辅助升级的移动终端应满足如下要求：

- a) 控制器在联网或连接指定辅助升级的移动终端后，持续收发数据的丢包率应不大于0.3%；
- b) 控制器在联网或连接指定辅助升级的移动终端后，通讯系统连接可用率应不低于99.9%，单次离线时长应不超过2 min；
- c) 控制器在联网或连接指定辅助升级的移动终端后，网络下载速度应大于20KB/s；
- d) 使用Wi-Fi技术实现空中下载的控制器，应能在信号强度不低于-85 dBm的环境下完成空中下载。

6.4 下载实施

6.4.1 设备注册阶段

控制器与服务器进行握手通信，获取设备在服务器的唯一识别码以及业务私钥等信息的设备注册阶段，应满足以下要求：

- a) 设备唯一识别码与服务器进行交互，长度应不超过64个字节且内容不包含特殊字符，自动控制器在本地应有接口可以读取；
- b) 自动控制器在获取到服务器下发的唯一识别码及业务私钥后，应安全存储这些信息。

6.4.2 版本确认阶段

控制器与服务器取得通信进行版本对比，存在可升级固件版本时，非静默升级机制下取得人工操作确认的阶段，应满足以下要求：

- a) 控制器在本地运行以及网络端存储的固件版本，应当至少包括软件版本信息、适用硬件版本或批次信息。版本号的字符使用范围为0~9、A~Z、“.”和“_”；

- b) 进行版本确认时，当固件包大小超过存储空间时不应转入下载；
- c) 有定时自动发起可升级固件查询的机制时，时间间隔不应超过24 h，如定时间隔中有其他查询进行，可顺延计时；
- d) 在版本确认的过程中，控制器发生网络断开或电源中断的情况，恢复正常后应能继续或重新进行版本确认；
- e) 除静默升级外，在固件下载开始前，应具备取消下载动作的功能；
- f) 发起版本确认或者查询，应有重试和超时退出机制，版本查询的结果宜有上报到服务器的功能。

6.4.3 固件下载阶段

控制器与服务器通信，将目标版本固件从网络下载到本地并存储的阶段，应满足以下要求：

- a) 升级包应进行加密，设备下载升级包后应解密并校验固件完整性；
- b) 对于网络单元与固件运行单元间需要多级通讯传递，或者完成云端下载后，固件有解压缩和差分过程的，程序固件应包含完整性验证数据，在最终完成固件存储时，进行完整性校验；
- c) 对于 GB/T 14536.12-2008 中规定的B类或C类控制器，其固件传输过程和存储过程中进行的数据校验，应采用GB/T 14536.1中H.12.12.2.3和H.12.12.2.4的方法或其他能证明可提供等效及更高的安全水平的方法；
- d) 在固件下载阶段，若控制器出现超过60s原有功能不能正常工作的情况，应在本机界面或移动控制界面给予用户时间预期的提示；
- e) 在下载的过程中，出现电源中断，重新启动后控制器应保持以前的可用版本，且保持固件发现和下载功能正常；
- f) 在下载的过程中，网络出现异常，控制器应固件保持以前的可用版本，且保持固件发现和下载功能正常；
- g) 固件下载的结果，应有上报到服务器的功能。

6.4.4 固件切换阶段

控制器将下载完成的目标固件切换为运行固件的阶段，应满足以下要求：

- a) 固件应包含完整性验证数据，控制器应对固件进行完整性校验，如果未确认其完整性和真实性，那么控制器应拒绝进行固件更新；
- b) 固件切换或者安装前，应进行升级前置条件检查，正在执行有时序要求的任务时（如烹饪、洗涤、除霜等对子单元任务发生的先后顺序或时间间隔有既定的要求）宜完成当前任务后完成切换，如果不符合条件，应启动相应升级退出或者延时流程并上报到服务器；
- c) 在执行固件切换时，若控制器出现超过60s原有功能不能正常工作的情况，应在本机界面或移动控制界面给予用户时间预期的提示；
- d) 在控制器完成固件切换之前，不应出现以前的可用版本和目标版本固件同时无法恢复的情况；
- e) 控制器如未能切换固件版本成功，应能够保持控制器处于安全状态，如保持以前的可用版本或者自动再次启动更新；
- f) 固件切换的结果，应有上报到服务器的功能。

6.5 电源

6.5.1 控制器如能源供应为电池或采用对能源供应有限制的方式时，静默升级不允许开始；

注：能源供应有限制，如对供电的时间段有限制等可能导致升级有可预见的中断风险的情况。

6.5.2 命令升级和推送升级应由软件设计在充足电量下执行，宜在显示界面给予保证电量和有效供电的提示。

6.6 安全性

6.6.1 控制器中涉及个人信息安全的部分，应符合 GB/T 35273—2020 中第 5 章~第 10 章的要求。

6.6.2 控制器物理安全，应符合 GB/T 41387-2022 中 6.1 的要求。

6.6.3 除满足 6.6.1 和 6.6.2 的安全要求外，控制器还应满足以下要求：

- a) 固件应进行安全保护（如关闭硬件调试接口等），不应通过串口读取等常规手段从设备中提取关键代码及敏感数据。关键代码及敏感数据（如 ID、鉴别数据、密钥、证书等）应采取保护措施，具备防篡改、防逆向功能；
- b) 固件不应使用包含 CNVD/CNNVD 已公布 90d 以上的高危及以上未处置的第三方库和开源组件；
- c) 固件下载云端到设置端的传输通道应防止劫持或嗅探；
- d) 若在线升级是在家电设备业务运行中进行，该软件升级不应影响家电设备运行安全。
- e) 在固件下载阶段和固件切换阶段应有重试机制，重试超过 10 次的在核算成功率时计为当次失败，控制器的 OTA 升级应进行可靠性测试，成功率不低于 99.99%。

6.7 静默升级方式的额外要求

对于 GB/T 14536.1-2008 中规定的 C 类控制器，不允许进行静默升级。

6.7.1 功能说明

应明确告知用户控制器具备空中下载功能和静默升级机制，并说明静默升级的触发机制、可能引起的风险和主要解决方案并获得用户首肯，包括但不限于配套的移动应用界面、本机应用界面等方式。且用户在不需静默升级时应有方法关闭功能。

6.7.2 对控制器功能的影响

使用静默升级方式的控制器，升级过程中应满足以下要求：

- a) 在固件下载的过程中，控制器应能保持正常工作，对于可以远程控制的控制器的，其基于网络的远程控制功能应正常；
- b) 有计时或者类似功能的控制器，在执行固件下载的过程中时间基准的偏差应不大于 2%；

注：有指示自然时间或记录一段时间的长短的测量功能的控制器，如钟表或烹饪计时器。提供粗略预估时间的控制器不在此范围内，如洗衣机控制器

- c) 在固件升级的过程中，控制器的功能丧失的时间应小于 3s；

注：控制器完成切换后，如涉及系统重新启动，系统启动时间不计入功能丧失的时间

- d) 在固件完成切换前后，控制器的工作状态应保持一致；

注：工作状态包括控制器的待机/运行状态及用户设定。如空调控制器的开机/待机和目标温度设定

- e) 对于含蜂鸣器等发声器件的控制器，在进行静默升级的过程中，不应产生额外噪声。

6.8 标识

控制器的标识应满足以下要求：

- a) 控制器应具备网络标识，宜具备空中升级的标识，且标识清晰、规范；
- b) 控制器在其预期配置中的所有外部接口及所支持的通信协议标识清晰、规范；
- c) 清晰明确地标示硬件版本，并与提供的文档保持内容一致。对于软件版本，宜在具备显示条件的系统（如有屏幕/移动界面等）展示给用户。

7 测试方法

7.1 测试条件

7.1.1 Wi-Fi 技术升级测试条件

支持 Wi-Fi 技术升级的控制器，软件测试条件如下：

- a) 测试用路由器、控制器位于同一测试房间，控制器分布于路由器半径5m范围内；
- b) 在测试房间内测得的同频Wi-Fi干扰信号RSSI值均小于-65dBm；
- c) 测试路由器下的设备连接总数，不超过10台，且不运行视频播放等高流量应用。

7.1.2 蓝牙或 NB-IoT 等技术升级测试条件

支持蓝牙或 2G、3G、4G、5G 等 NB-IoT 技术的控制器，测试条件如下：

- a) 辅助升级的数据移动终端不运行其他占用内存应用，不播放视频或其他高流量应用；
- b) 辅助升级的数据移动终端与控制器距离不超过10 m，不要有遮挡物；
- c) 辅助升级的数据移动终端或控制器要处于空旷位置，能正常接收基站信号。

7.2 网络连接可靠性测试

- 7.2.1 控制器联网或连接指定的辅助升级移动终端后，使用厂商提供的工具或指令集，以 500 ms 的周期发送指令并监控应答，各发送 5000 个数据包，丢包率应满足 6.3.2 中 a) 的要求。
- 7.2.2 被监测的控制器数量应不少于 5 台，所有设备的总监测时间累计应不少于 500 h。控制器联网或连接指定的辅助升级移动终端后，后台记录统计离线事件发生的次数和时间，并计算系统连接可用率，应满足 6.3.2 中 b) 的要求。
- 7.2.3 控制器联网或连接指定的辅助升级移动终端后，通过工具或指令集触发数据持续下载，至少持续 60s，并监控下载速率，应满足 6.3.2 中 c) 的要求。
- 7.2.4 在控制器或其指定的辅助升级终端联网后，关闭其电源，等待 30s 后重新开启电源，待其自动完成重新连接后，并进行 7.2.1 的测试，应满足 6.3.1 中 b) 的要求。
- 7.2.5 在控制器联网后，关闭路由器电源，等待 30s 后重新开启电源，待路由器正常工作后，再等待 30s，检查控制器是否在线，并进行 7.2.1 的测试，应满足 6.3.1 中 b) 的要求。

7.3 固件发现及下载测试

- 7.3.1 构造一个大小超过控制器存储大小的测试用升级包，并设置好规则，监控控制器是否会转入固件下载，应符合 6.4.2 中 b) 的要求；
- 7.3.2 构造一个符合要求的测试用升级包，并设置好规则，对于命令升级，监测用户查询到新版本的时间；对于推送升级，监测用户收到版本推送的时间，对于静默升级，在 24 小时后检查控制器运行的版本是否更新。其结果应符合 6.4.2 中 c) 的要求。
- 7.3.3 构造一个符合要求的测试用升级包，并设置好规则，控制器应能够成功转入固件下载状态；在下载完成后，检查控制器内存储空间的二进制内容，与服务器的固件内容作比较应完全一致，以及服务器中的日志，应符合 6.4.3 中 d) 和 g) 的要求。
- 7.3.4 重复 7.3.3 的测试方法，在下载固件的过程中，关闭其电源，等待 30s 后恢复电源，检查控制器的功能，并重复 7.3.3 的测试，应满足 6.4.3 中 e) 要求。
- 7.3.5 重复 7.3.3 的测试方法，在下载固件的过程中，关闭路由器电源，等待 30s 后恢复电源，过程中检查控制器的功能，在路由器正常工作后再等待 30s 后重复 7.3.3 的测试，应满足 6.4.3 中 e) 的要求。

7.4 运行固件更新测试

- 7.4.1 控制器通电后软件正常工作，构造一个完整性被篡改的升级包，执行软件升级，检查控制器存储空间的内容以及升级日志，应满足 6.4.4 中 a) 的要求；
- 7.4.2 控制器通电后正常工作，分别在控制器待机、工作的过程中执行 7.3.3 的测试条件，检查控制器的工作状态和升级日志，并满足 6.4.4 中 b) 和 c) 的要求；
- 7.4.3 重复 7.3.3 的测试步骤，在软件进行切换的过程中，将控制器断电，20s 后恢复通电工作，并重复 5 次后稳定供电工作，软件应能够继续完成切换。并符合 6.4.4 中 e) 要求。

7.5 固件成功率的测试

控制器应进行 OTA 升级的可靠性测试，如前 1000 次全部成功的可以结束测试，否则累计完成 10000 台次测试并计算成功率，应符合 6.6 中 e) 的要求。

7.6 静默升级机制的补充测试

对于采用静默升级机制的控制器，应补充以下测试：

- 7.6.1 检查控制器配套的说明文件，应符合 6.7.1 的要求；
- 7.6.2 控制器通电后正常工作，经过 7.3.3 的测试条件，在过程中操作控制器并观察其功能运转，包括具备远程操作功能的使用，应符合 6.7.2 中 a) 和 c)、d)、e) 的要求；
- 7.6.3 对于有计时功能的控制器，通电后正常工作，经过 7.3.3 的测试条件，在固件下载过程中的进行计时检查，符合 6.7.2 中 b) 的要求。

7.7 测试报告

测试报告里至少应包括如下内容：

- a) 本文件编号和名称；
 - b) 控制器的型号，硬件版本信息，原固件版本信息，目标固件版本信息；
 - c) 不符合本文件规定的测试项目及原因；
 - d) 日期、地点和人员等。
-