附件 2

《智能语音控制器通用安全技术要求》

（征求意见稿）

编制说明

《智能语音控制器通用安全技术要求》

标准起草工作组

二〇二三年二月

目　录

《智能语音控制器通用安全技术要求》

编制说明

（征求意见稿）

一、工作简况

1、任务来源

依据国标委发〔2021〕12 号《国家标准化管理委员会关于下达 2021 年第一批推荐性国家标准计划及相关标准外文版计划的通知》（项目编号为 20210747-T-604），全国家用自动控制器标准化技术委员会将制定《智能语音控制器通用安全技术要求》标准列入 2021-2023 年度标准工作计划。本标准主要起草单位广东美的制冷设备有限公司，广东中创智家科学研究有限公司等，计划完成时间 2023 年。

2、主要工作过程

起草阶段：

工作组成立后， 标准起草工作组展开了对标准草案的编制工作，由于疫情原因，工作组先择取产业链上的龙头企业，在网络上进行多次讨论，就本标准涉及的理论、技术、产业等主要问题，进行了深入的交流研讨，使标准制定的技术方向和实现路径得到进一步的确认。确定了本标准制定的技术路线和结构框架。

2022 年 4 月 28 日，工作组在线上召开《智能语音控制器通用安全技术要求》国家标准起草会议，讨论和完善《智能语音控制器通用安全技术要求》工作组讨论稿。参与本次会议的还有来自方太、万和、松下、博西、苏泊尔等数十家单位的专家代表，各专家代表围绕着标准草案进行了热烈的讨论。会议讨论主要集中在语音控制器的功能安全、攻击类型上，会上讨论出了可能攻击的类型及试验方法，并从技术维度涵盖软件、硬件、网络部分的安全设计原则，补充了行业中智能语音与家电结合后的安全要求相关缺少的内容，首次从设计、使用、售后阶段导出相关安全设计原则和测试评估方法。从而使标准能够提高智能产品安全性，为家庭环境使用的语音控制器提供相关检验评价依据，促进语音控制器相关行业的健康发展。

会后，经过数月的修改完善，于 2022 年 12 月工作组形成标准征求意见稿，并将征求意见材料进行完善后发送标委秘书处，启动征求意见流程。

3、主要参加单位和工作组成员及其所做的工作等

根据国家标准制修订工作程序的要求，全国家用自动控制器标准化技术委员会组织标准的起草工作，组建《智能语音控制器通用安全技术要求》国家标准起草工作组，本标准起草工作组单位与成员涵盖产业链上主要企业。工作组由广东美的制冷设备有限公司担任工作组组长单位，广东中创智家科学研究有限公司担任工作组副组长单位，全面负责标准的具体起草与编写工作。秘书处负责协调标准起草工作，其余组员负责收集、分析国内外相关技术文献和资料，结合实际应用经验，对技术内容进行归纳、总结，并对各方面的意见和建议进行归纳、分析，以及文件材料的编制。

二、标准的编制原则和主要内容

1、编制原则

本标准依据 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》的规则和要求进行编制。根据生产实际和应用，本标准在已有控制器通用安全技术标准的基础上，充分考虑带智能语音控制功能的所有种类家用和类似用途电子控制器的产品特点、应用环境及安全问题等，增加制定带智能语音控制功能的所有种类家用和类似用途电子控制器在安全技术方面的标准。本标准基于推动带智能语音控制功能的所有种类家用和类似用途电子控制器及相关产业发展的原则，以需求为导向，以企业为主体，以技术产品方案为基础，走产学研相结合的路线，力争在智能语音控制器的安全技术方面填补国内空白，最大限度促进我国带智能语音控制功能的所有种类家用和类似用途电子控制器产品的技术提高与发展。同时，起草组在标准编制的过程中一贯坚持开放、全面和可用性等主要衡量指标，跟踪国内外相关领域技术发展态势，融合众家所长的基本指导思想，并遵守以下原则：

1) 从实现功能、优化成本、推进产业化等因素出发，以面向应用为原则，作为评判技术方案的依据；
2) 以现有技术方案为基础，在听取专家意见的基础上，形成客观标准技术方案；
3) 在充分技术方案的基础上，将各技术方案进行融合，纳入统一的标准体系；
4) 充分考虑未来应用产品的需求和技术发展的要求，标准实施是开放式建立，递进式推进。

2、主要内容

针对带智能语音控制功能的所有种类家用和类似用途电子控制器的存在的安全技术问题，本标准规范了其范围，术语、定义及缩略语，技术要求，技术规范及语音性能测试要求，本标准适用于智能语音控制器的设计、研发、生产及测试。

本标准草案主要内容主要包括：

1) 范围：IEC 60704-1 和 IEC60704-2 覆盖的带智能语音控制功能的所有种类家用和类似用途电子控制器（以下简称“智能语音控制器”）。
2) 术语、定义及缩略语：依据国内外现有智能语音交互相关的标准，规定了与智能语音控制器相关的 23 个定义及 9 个缩略语。
3) 技术要求：本标准从通用技术，硬件、软件、信息四个方面对智能语音控制器涉及的安全问题提出要求与规范。
    a) 通用技术要求：智能语音控制器应符合 GB/T 14536.1-2008 及其相应的控制功能的特殊要求。
    b) 硬件安全要求：规定了智能语音控制器的硬件保护措施，包括以下四个方面：
        i. 物理安全要求：规定了智能语音控制器的物理保护措施，防止攻击者通过物理手段以实现对其进行入侵。
        ii. 硬件接口安全要求：规定了智能语音控制器的硬件接口保护措施，防止攻击者通过硬件接口实现对其进行入侵。
        iii. PCB 安全要求：规定了智能语音控制器的 PCB 保护措施，防止攻击者通过 PCB 板的丝印、走线等信息对其进行入侵。
        iv. 芯片安全要求：智能语音控制器的芯片调试功能端口应采用防护机制来保护端口的安全。
    c) 软件安全要求，规定了智能语音控制器的软件层面上的技术要求及安全措施，包括以下两个方面：
        i. 性能安全要求：规定了智能语音控制器的 4 个性能最低要求，具体地，语音唤醒成功率、命令字识别成功率、误唤醒频次。
        ii. 应用软件要求：规定了智能语音控制器的应用软件保护措施，防止攻击者通过功能应用软件实现对其进行入侵。
    d) 信息安全要求规定了智能语音控制器的信息层面上的技术要求及安全措施，包括以下六个方面：

i. 语音监听安全要求：规定了智能语音控制器的语音监听应符合 GB/T 40660-2021 中第 4～11 章的要求。

ii. 传输安全要求：规定了智能语音控制器各执行主体之间进行数据传的保护措施。

iii. 认证安全要求：规定了智能语音控制器的用户认证机制及认证信息。

iv. 操作系统安全要求：规定了智能语音控制器的操作系统应符合 GB/T 34976-2017 操作系统安全技术要求。

v. 数据安全要求：规定了智能语音控制器中数据的可用性、完整性、保密性及剩余数据保护等安全要求。

vi. 隐私安全要求：规定了智能语音控制器应符合 GB/T 35273—2020 信息安全技术 个人信息安全规范。

4) 技术规范：与技术要求一一对应的，本标准从通用技术，硬件、软件、信息四个方面对（3）中所述技术要求提出对应的试验方法。

a) 通用技术规范：所有试验都应在 GB/T 2421.1-2020 规定的测量和试验用标准大气条件下进行，其他检验由制造商自定，如语音模组技术规格书中标注的工作温度等参数范围如果比本文件规定的范围更宽泛，环境适应性测试时按本文件中标注的参数范围进行测试。

b) 硬件安全规范包括物理安全处理检测方法、硬件接口安全处理检测方法、PCB 板级防护检测方芯片安全检测方法；

c) 软件安全规范包括性能安全测试、固件安全测试、功能软件接口安全测试、应用软件安全测试；

d) 信息安全测试要求包括语音监听安全测试、传输安全测试、认证安全测试、操作系统安全测试、数据安全测试、隐私安全测试。

5) 语音性能测试要求：规定了智能语音控制器的语音性能测试应满足的基本要求包括通用要求、测试场地要求、测试数据要求、测试噪声要求、测试记录要求、测试拾音距离要求、测试声级计放置要求。

三、主要试验（或验证）情况分析

a) 技术内容确定依据

本标准对于带智能语音控制功能的所有种类家用和类似用途电子控制器与传统电自动控制器在安全领域进行技术分析，明确了带智能语音控制功能的所有种类家用和类似用途电子控制器在通用安全要求、硬件安全要求、软件安全要求、信息安全要求方面的安全技术要求及规范。本标准根据当前国内智能家电、智能控制器及相关产品的研发和生产情况，并参阅国内现有的相关标准，如GB/T 14536.1-2008、GB/T 36464.1-2020、GB/T 36464.2-2018等进行制定，力求制定后的标准具有科学性、合理性和复现性，试验方法具有可操作性和实用性。这些要求的规定将保证带智能语音控制功能的所有种类家用和类似用途电子控制器的基本安全。

b)在行业试用（或验证）的情况分析

本标准的技术内容经过编制组成员确定后，针对带智能语音控制功能的所有种类家用和类似用途电子控制器的设计原则、技术要求、技术规范及性能测试，在制定过程中特别是报批前进行了大量的试验验证工作。试验项目涵盖了草案中涉及的全部项目。试验验证采取1种方式进行：

1) 由工作组内的企业在企业实验室按照实际设计开发流程，进行试验验证。如：广东美的制冷设备有限公司中的开发部门以及有资质的实验室中进行测试验证，得到了参编企业的一致认可。

2) 信息安全部分的测试送入国内有信息安全测试资质的实验室，如：公安部第三研究所，进行测试并对相关出现的问题进行整改，完成了整个标准的试验验证工作。

通过试验验证，并结合目前我国带智能语音控制功能的所有种类家用和类似用途电子控制器整体研发情况来看，90%以上厂家已经或通过技术升级可以达到。考虑到用户要求、国家对网络安全和个人信息的法律法规和要求，以及保持必要的技术前瞻性，标准规定的指标是恰当的，可行的。

四、标准涉及专利及知识产权情况说明

本标准不涉及知识产权。

五、预期达到的社会效益、对产业发展的作用等情况

《智能语音控制器通用安全技术要求》国家标准的制定和发布规范了带智能语音控制功能的所有种类家用和类似用途电子控制器的范围、术语、定义及缩略语、技术要求、技术规范及语音性能测试要求，为智能语音控制器企业产品的设计、研发、生产、

测试提供了依据，规范了在智能语音控制器行业中的通用安全技术要求，奠定了通用安全技术基础，填补了行业空白，为带智能语音控制功能的所有种类家用和类似用途电子控制器行业提供统一的衡量规范，推动网络化、智能化技术的应用。在产业化的推进过程中，将为我国带智能语音控制功能的所有种类家用和类似用途电子控制器相关产业的健康快速发展和竞争力提升提供保障。

六、采用国际标准和国外先进标准情况

本标准无采用国际标准。

本标准为国内先进水平。

七、与现行法律、法规、规章及相关标准协调性

本标准与现行相关法律、法规、规章及相关标准协调一致。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议说明

本标准建议为推荐性标准。

十、贯彻标准的要求和措施建议

在本标准正式发布后，工作组将根据部分生产商的需求进行宣贯培训。

建议本标准批准发布 6 个月后实施。

十一、废止现行相关标准的建议

无。

十二、其他应予说明的事项

无。