ICS 97.120

K 32

中 华 人 民 共 和 国 国 家 标 准

GB/T ×××××—××××

智能语音控制器通用安全技术要求

General safety technical requirements for intelligent voice controls

点击此处添加与国际标准一致性程度的标识

（工作组讨论稿）

（本稿完成日期：2023-02-20）

××××-××-××发布　　××××-××-××实施

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

本文件由中国电器工业协会提出。

本文件由全国家用自动控制器标准化技术委员会（SAC/TC 212）归口。

本文件起草单位：

本文件主要起草人：

引　言

智能语音是指智能系统通过机器感知技术实现声音采集、语音识别、语义理解等信息处理的过程，利用自然语言理解等技术来进行分析，从而实现人机对话、智能判析和决策的一整套计算过程。简单来说就是让计算机、智能仪表、手机甚至家电和玩具都能像人一样“能听会说”的技术。

企业在智能语音领域上有一定的基础，目前处于受众定制细分、个性化服务进行突破的阶段。一方面，老人、儿童等人群的相关功能性、生活性的产品有望成为智能语音未来发展的一个入口。另一方面，不同的场景也为智能语音提供新的发展途径。例如通过控制养老院、母婴室等不同场景的家居设备，从而满足不同人群的需求。而语音与家电的结合也催生了“语音智能电控器”。

由于传统电控器主要关注硬件、电气方面的内容，随着智能技术的融合，迫切需要增加相应规范来适应变化。并且由于智能技术普遍使用大数据、无线网络，所以在信息安全、隐私方面也需要相应规范。因为智能语音技术不同于Wifi和蓝牙等其他无线传输技术，智能语音技术依赖于用户的声音来实现特定功能，如家电控制、信息查询和身份识别等功能。通过声学传感器来对用户的声音进行采集，然后利用语音识别模块对用户的语音进行识别并且对其语义进行理解，操作这些步骤的前提是对用户的声音进行保存和处理，在保存用户声音的时候，就需要注意保护用户的声学特性和语音内容等涉及用户隐私的地方，同时在分析、传输等处理操作的时候，也需要注意信息和隐私的安全，因此需要相应的规范来保障智能语音控制的安全要求。

智能语音控制器通用安全技术要求

1 范围

本文件规定了智能语音控制器安全的分类、技术要求、测试方法等。

本文件适用于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“语音控制器”）的安全评估。

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 2421-2020 环境试验 概述和指南
GB/T 3947-1996 声学名词术语
GB/T 9002-2017 音频、视频和视听设备及系统词汇
GB/T 14536.1-2008 家用和类似用途电自动控制器 第1部分：通用要求
GB/T 20270-2006 信息安全技术 网络基础安全技术要求
GB/T 20271-2006 信息安全技术信息系统通用安全技术要求
GB/T 34083-2017 中文语音识别互联网服务接口规范
GB/T 34976-2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法
GB/T 35273-2020 信息安全技术 个人信息安全规范
GB/T 36464.1-2018 信息技术 智能语音交互系统 第1部分：通用规范
GB/T 36464.2-2018 信息技术 智能语音交互系统 第2部分：智能家居
GB/T 37973-2019 信息安全技术 大数据安全管理指南
GB/T 40660-2021 信息安全技术生物特征识别信息保护基本要求
GB/T 41387-2022 信息安全技术 智能家居通用安全规范
YD/T 1886-2015 移动终端芯片安全技术要求和测试方法
JR/T 0092-2019 移动金融客户端应用软件安全管理规范

3 术语和定义、缩略语

下列术语、定义及缩略语适用于本文件

3.1 定义

3.1.1

语音控制器 voice control

通过语音识别，将语音指令转换为设备控制指令从而对设备进行功能控制的一种控制器。

3.1.2

语音识别 speech recognition

具有人类声学特性的语音信号转换为电信号再转换为用户能识别指令的过程。

3.1.3

唤醒命令字 wakeup command word

用于唤醒处于关键字识别状态的语音交互系统所用的结构化关键字。

[来源：GB/T 36464.1-2020，3.18]

3.1.4

命令字识别 command word recognition

一种基于语音识别语法的语音识别方式，是在语音识别语法规则限定的范围内，对于给定的语音输入，语音识别引擎给出语音识别语法覆盖范围内的文本或拒识做为识别结果。

[来源：GB/T 34083-2017，3.3]

3.1.5

连续语音识别 continuous speech recognition

识别任意的连续语音，并给出相对应的文本。

注：连续语音识别不限制用户说话的词汇、内容和方式，用户可以以任意说的形式输入语音。

[来源：GB/T 34083-2017, 3.4]

3.1.6

语音唤醒 speech wakeup; voice trigger

处于音频流监听状态的语音交互系统，在检测到特定的特征或事件出现后，切换到命令字识别、连续语音识别等其他处理状态的过程。

[来源：GB/T 36464.1-2020，3.17]

3.1.7

误唤醒 false wakeup

语音唤醒过程中出现的，无音频流或音频流中没有出现唤醒命令字时，语音系统被唤醒的现象。

[来源：GB/T 36464.1-2020，3.19]

3.1.8

噪声 noise

语音采集过程中，采集到的由非有效语音信号源发出的，能干扰、影响对有效语音信号的理解或处理的声音信号。

[来源：GB/T 36464.1-2020，3.27]

3.1.9

白噪声 white noise

用固定频带宽度测量时，频谱连续并且均匀的噪声。白噪声的功率谱密度不随频率改变。

注：白噪声不一定是无规噪声。

[来源：GB/T 3947-1996，2.13]

3.1.10

白噪声攻击 white noise attacks

把攻击语音指令加入到白噪声中，对目标语音控制模块进行攻击的一种攻击方式。

3.1.11

麦克风阵列 microphone array

由具有确定空间拓扑结构的多个麦克风组成的，对信号的空间特性进行采样并滤波的系统。

[来源：GB/T 36464.1-2020，3.23]

3.1.12

语音控制器的正常功能 normal functionfor voice control module

根据产品特性和需求，在预先规划中的功能。

3.1.13

语音控制器的非正常功能 abnormal function for voice control module

根据产品特性和需求，不在预先规划中的功能。

3.1.14

唤醒率 wake up success rate

语音唤醒的成功率，唤醒命令字能够唤醒成功的次数除以唤醒总次数，一般以百分比的形式表示。

3.1.15

混淆指令/隐藏语音指令 obfuscated command / hidden voice command

把攻击性的语音指令混入某种正常的语音当中的语音指令。

3.1.16

谐波失真 harmonic distortion

输入信号为正弦波信号时，用输出信号中的谐波信号与总输出信号之比表示的幅度非线性。

注：这些信号可以用功率、电压或声压表示。

[来源：GB/T 9002-2017，4.2.3]

3.1.17

信噪比 signal-to-noise ratio

参考电压与噪声电压之比，取以10为底的对数乘以20。

注：单位为分贝（dB）。

[来源：GB/T 9002-2017，4.2.2]

3.1.18

可听声 audible sound

能引起听觉的声振荡或声振荡引起的听觉，频率范围约为16Hz至16kHz。

[来源：GB/T 9002-2017，4.1.2]

3.1.19

超声 ultrasound; ultrasonic sound

频率高于可听声频率上限的声振荡。

[来源：GB/T 9002-2017，4.1.3]

3.1.20

海豚音攻击 dolphin attacks

通过把语音指令加入到超声中，进而对语音设备进行控制的攻击方式。

注：海豚音攻击也可以被称为**交互式隐蔽攻击**（SurfingAttacks**和**）**超声波攻击**（ultrasound attacks）

3.1.21

不可逆性 irreversibility

由生物特征识别比对信息无法推断出其对应生物特征识别原始信息的特性。

[来源：GB/T 40660-2021，3.7]

3.1.22

识别成功率 successful recognition rate

命令字识别的成功率，命令字能够被正确识别的次数除以总次数，一般以百分比的形式表示。

3.1.23

误识别 false wakeup and recognition

一种误唤醒后，进行语音识别的过程。

3.2 缩略语

下列缩略语适用于本文件：

ASR：语音识别（Automatic Speech Recognition）

NLU：自然语音理解（Natural Language Understanding）

RT60：表示从声音突然停止到声压级降低60dB所用的时间（Reverberation Time 60db）

EUT：被测试设备（Equipment Under Test）

USB：通用串行总线（Universal Serial Bus）

UART：通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）

SPI：串行外设接口（Serial Peripheral Interface）

OTA：空中下载（Over the Air）

CAN：控制器局域网（Controller Area Network）

PCB：印制电路板（Printed Circuit Board）

4 技术要求

4.1 通用要求

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。

4.2 硬件安全要求

4.2.1 物理安全要求

语音控制器硬件物理安全应符合GB/T 41387-2022中第6.1.1节的要求。

4.2.2 硬件接口安全要求

语音控制器硬件接口应符合GB/T 41387-2022中第6.5.1节的要求。

4.2.3 PCB 安全要求

语音控制器PCB板应有以下部分或全部保护措施，以避免安全风险问题：

a) PCB板上的丝印不应存在敏感信息；
b) PCB上所有接口的丝印信息简化处理，提高非法获取硬件信息的难度；
c) PCB上关键芯片应去除logo或做覆盖防护；
d) PCB关键信号的布线，应用物理手段增加辨别线路走线的难度，避免被探测；
e) PCB关键模块应采取物理金属外壳罩保护；
f) PCB油墨选择深色，提高辨识线路走线的难度；

4.2.4 芯片安全要求

4.2.4.1 芯片调试安全要求

语音控制器的芯片应符合YD/T 1886-2015中第5章的要求。

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，采用以下部分或全部方式：

a) 隐藏调试功能端口。在保证设备正常工作能力的前提下，应采用物理手段隐藏前期调试所用的各类硬件接口（如 JTAG、SWID、UART 等），避免攻击者通过这些接口获取接口实现的细节信息。
b) 在程序中禁用调试功能端口。电控端主控芯片的JTAG/SWD/UART等调试或通信端口可控，在产品形态下，禁止输出关键调试信息。
c) 增加访问控制机制。应对用户设置一定访问权限，如删除默认账户或修改默认口令等，避免用户直接访问芯片内部固件信息。

4.2.4.2 芯片加密参数安全要求

语音控制器的芯片应符合YD/T 1886-2015中第6.1章的要求。

语音控制器的芯片的硬件加密模块输入的非公开加密参数应保持完整性和机密性，采用以下部分或全部方式：

a) 如果秘钥存储在DRAM，则增加相应的纠错码；
b) 在对语音控制器的存储芯片进行整体加密时，保持其与硬件特征信息相关；
c) 口令、指纹、图形密码不应作为秘钥使用。

4.2.4.3 芯片固件存储安全要求

语音控制器的芯片应符合YD/T 1886-2015中第7.2章的要求。

语音控制器的芯片应保持其内部存储的固件在运行过程中的完整性、可用性和机密性，并符合以下要求：

a) 语音控制器的芯片固件存储于安全受控区域时，缺省状态保证不可修改性；

b) 语音控制器的芯片固件存储外部区域时，需附加检错码或数字签名保护其完整性；

c) 语音控制器的芯片固件进行加密存储时，加密参数应符合本文件4.2.2.2的要求。

4.2.4.4 存储芯片完整性要求

语音控制器的芯片应符合YD/T 1886-2015中第8.1章的要求。

a) 采用NAND Flash作为存储载体的语音控制器芯片应具备检错与纠错功能，以保护其存储单元的完整性；

b) 以DRAM作为存储载体的语音控制器芯片应具备检错与纠错功能，以保护其存储单元的完整性。

4.2.4.5 应用处理器芯片完整性要求

语音控制器的芯片应符合YD/T 1886-2015中第8.3章的要求。

a) 语音控制器的芯片应保证其在使用的国家或地区可使用，应将出厂商和硬件版本等信息存储于芯片内部信息中；

b) 语音控制器的芯片硬件特征信息需与内部存储的固件绑定，如果发生固件程序被篡改，或芯片被替换，语音控制器应能停止加载芯片固件并反馈异常。

4.2.4.6 芯片故障检测与恢复要求

语音控制器的芯片应符合YD/T 1886-2015中第8.4章的要求。

语音控制器的芯片应能够检测到存在运行故障状态并实现终端硬件复位，使整个家电终端重新处于可控状态。应在芯片内部或者外部增设看门狗电路，保护终端系统的可靠运行。

4.3 软件安全要求

4.3.1 性能安全要求

4.3.1.1 语音唤醒成功率最低要求

语音控制器语音唤醒成功率应符合表1规定。

表1 语音控制器最低唤醒成功率

环境	唤醒成功率
安静	88%
噪音	85%

4.3.1.2 命令字识别成功率最低要求

语音控制器命令字识别成功率应符合表2规定。

表2 语音控制器命令字识别成功率

距离	环境	命令字识别成功率
1米	安静	85%
3米		85%
5米		80%
1米	噪音	85%
3米		80%
5米		75%

4.3.1.3 误唤醒频次最低要求

a) 噪音条件下，语音控制器应满足24小时内误唤醒频次不高于3次；
b) 安静条件下，语音控制器应满足24小时内误唤醒频次不高于1次。

误唤醒频次应符合GB/T 36464.2-2018中第5.3.3的要求。

4.3.2 应用软件安全要求

4.3.2.1 应用软件签名安全要求

智能语音控制器的应用软件应包含供应商和或者开发者的数字签名信息和软件属性信息（如版本名称、版本信息和描述等）。

4.3.2.2 应用软件身份认证安全要求

应用软件身份认证安全应符合下列要求：

a) 智能语音控制器的应用软件应支持身份认证登录，且执行身份认证操作时的要素应相互独立；
b) 使用手势密码、短信密码、生物特征信息或图形验证码作为认证要素，应满足JR/T 0092-2019中5.1.1 d的要求；
c) 使用图形验证码作为认证要素时，客户端源文件中不应包含图形验证码文本内容。

4.3.2.3 应用软件认证信息安全要求

智能语音控制器的应用软件应对于输入的用户名和登录密码提供安全性措施。

4.3.2.4 应用软件认证失败处理安全要求

智能语音控制器的应用软件应提供认证失败处理机制。

4.3.2.5 应用软件权限控制安全要求

智能语音控制器的应用软件向系统申请权限时应遵循最小化原则以及合理的申请方式。

4.3.2.6 应用软件抗攻击能力安全要求

智能语音控制器的应用软件可以抵御静态分析、动态调试。

4.4 信息安全要求

4.4.1 语音监听安全要求

按6.4.1测试，语音控制器应符合GB/T 40660-2021中第4～11章的要求。

4.4.2 传输安全要求

满足下列要求：

a) 各执行主体之间进行数据传输时，应保证数据传输的完整性和机密性，应符合GB/T 37973-2019中第6章的要求；
b) 检测到数据完整性遭受破坏时，应采取新措施恢复或重新获取数据；
c) 所传输的数据需分类分级管理，分类分级应符合GB/T 37973-2019中第7章的要求。

4.4.3 认证安全要求

满足下列要求：

a) 用户认证需要具备基本标识，标识需确保在信息系统生存周期内的唯一性；
b) 应为用户提供确保其身份真实性的前提下，不被其他用户发现或滥用的保护；
c) 应按GB/T 20271-2006中4.3.1.1.2的要求，对用户认证鉴别时应根据用户标识提供不同鉴别方式；
d) 认证信息包括但不限于私钥、身份标识等敏感数据应加密存储，应符合GB/T 37973-2019 中8.3和8.6的要求，不可明文传输；
e) 身份认证过程需符合GB/T 20270-2006中第5章网络安全功能基本要求。

4.4.4 操作系统安全要求

应符合 GB/T 34976-2017 操作系统安全技术要求。

4.4.4.1 身份鉴别

满足下列要求：
a) 用户进入操作系统前宜先建立用户标识；
b) 在操作系统的整个生存周期内保证用户的唯一标识，以及用户名或别名、UID等之间的一致性；
c) 在用户执行任何与安全功能相关的操作前对用户进行鉴别；
d) 至少支持口令鉴别、基于令牌的动态口令鉴别、生物特征鉴别（如指纹、虹膜）、数字证书鉴别、图形鉴别等机制的一种进行身份鉴别，每次登录系统都需鉴别身份；
e) 在用户执行鉴别信息修改操作前，应经过身份鉴别；
f) 需采用加密方法对鉴别信息的存储进行保护；
g) 将用户进程与所有者用户相关联，是用户进程的行为可以追溯到进程的所有者用户；
h) 将系统进程动态地与当前服务要求者用户相关联，使系统进程的行为可以追溯到当前服务器要求者用户。

4.4.4.2 访问控制

满足下列要求：
a) 允许命名用以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；
b) 主体的访问控制属性至少应包括：读、写、执行等；
c) 客体的访问控制属性应包含可分配给主体的读、写和执行等权限；
d) 授权的范围应包括主体和客体及相关的访问控制属性，同时应指出主体和客体对这些规则应用的类型；
e) 对系统中的每一个客体，都应能够实现由客体的创建者以用户指定方式确定其对该客体的访问权限；
f) 客体的拥有者对其拥有的客体应具有全部控制权，允许客体拥有者把该客体的控制权分配给其他主体。

4.4.4.3 安全审计

满足下列要求：
a) 审计内容应包括：系统运行记录、报警记录、操作日志、用户行为记录、应用软件运行日志等；
b) 能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏；
c) 仅允许授权管理员访问审计日志；
d) 操作系统用户应能够定义审计跟踪的阈值；
e) 当为审计分配的存储空间耗尽时，应能按操作系统用户的设置决定采取的措施，包括：报警并丢弃未记录的审计信息、暂停审计、覆盖以前的审计记录等。

4.4.4.4 升级能力

满足下列要求：

a) 支持操作系统的更新升级；
b) 至少采取一种安全机制，保证升级过程的安全性；
c) 保证升级后的系统安全属性与升级前保持一致；
d) 升级失败时，系统应能够回滚，并保证系统完整性，且安全属性与升级前一致；
e) 至少采取一种安全机制，保证升级的时效性，例如自动升级，更新通知等手段。

4.4.5 数据安全要求

4.4.5.1 数据可用性

满足下列要求：

a) 语音控制器在传输其采集到的数据时，应对数据新鲜性做出标识；
b) 语音控制器应能够鉴别数据的新鲜性，避免历史数据的重放攻击；

4.4.5.2 数据完整性

满足下列要求：

a) 语音控制器应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
b) 语音控制器应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

4.4.5.3 数据保密性

满足下列要求：

a) 语音控制器应对重要数据采用密码算法进行存储和传输加密保护，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
b) 语音控制器中重要数据加密算法应符合国家密码相关规定；

4.4.5.4 剩余数据保护

满足下列要求：

a) 语音控制器应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除；
b) 语音控制器应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除；

4.4.6 隐私安全要求

应符合GB/T 35273—2020的要求。

语音控制器在操作用户隐私信息时应遵循合法、正当、必要的原则，其生产制造商采取技术和其他必要的措施保障用户隐私信息的安全，对其隐私信息处理活动对隐私信息主体合法权益造成的损害承担责任。语音控制器中所有涉及隐私安全的操作，应在国家法律、标准规范范围内进行。

4.4.6.1 隐私数据收集

应满足下列要求：

a) 语音控制器生产制造商采集隐私数据时应具有明确、清晰、具体的个人信息处理目的；

b) 语音控制器生产制造商采集隐私数据时向个人信息主体明示个人信息处理目的、方式、范围、规则等，征求其授权同意;
c) 语音控制器生产制造商采集隐私数据时只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量,目的达成后，应及时删除个人信息;
d) 语音控制器生产制造商采集隐私数据不可出售、不可转让；
e) 语音控制器采集隐私数据应符合GB/T 35273—2020第5章的要求。

4.4.6.2 隐私数据存储

应满足下列要求：

a) 语音控制器生产制造商应具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；
b) 存储的隐私数据应具有定时清理机制；
c) 语音控制器存储个人隐私数据时应符合GB/T 35273—2020第6章的要求。

4.4.6.3 隐私数据使用

应满足下列要求：

a) 语音控制器生产制造商应以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。
b) 语音控制器生产制造商应向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。
c) 语音控制器生产制造商隐私数据仅限于改善产品及用户体验，不可用于获取商业利益。
d) 语音控制器使用隐私数据时应符合GB/T 35273—2020第7章的要求。

5 技术规范

5.1 通用技术规范

除非另有规定，所有试验都应在GB/T 2421-2020规定的测量和试验用标准大气条件下进行。

环境适应性试验后的功能检查，型式检验时在所有环境适应性试验完成后统一进行功能检查，其他检验由制造商自定；如果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。

5.2 硬件安全规范

5.2.1 物理安全处理检测方法

通过以下方法确认对物理安全处理是否满足要求：

a) 检查芯片内是否设置光敏检测电路、温度检测电路、电压电路检测、温度检测电路以及频率检测电路等模块，对芯片工作环境进行监控，当攻击者通过去除芯片表面封装层而试图获取存储器数据时，检测模块是否会产生警告信息；或者核查是否对芯片内部总线以及存储器等重要敏感电路部分添加物理保护层；或者核查是否具有抗功耗分析攻击的能力；
b) 通过暴力移除或者拆卸操作，验证智能家居终端是否具有防护预警机制，如将预警信息上传至智能家居应用服务平台等方式。

5.2.2 硬件接口安全处理检测方法

通过以下方法确认对硬件接口的安全处理是否满足要求：

a) 对于具有console接口的设备，检查用户是否需要配置用户名，口令等方式鉴别才能进行登录，是否已禁止直接登录；口令是否符合长度不少于八位，并使用大小写字母、数字、特殊符号等方式两种或两种以上组成的复杂口令；
b) 使用无线和有线外围接口传输数据，验证是否具有通过指示灯或显示屏灯方式监控数据传输状态的功能，在不同的传输状态，监控显示是否有差异；
c) 检查具备调试功能的接口，在出厂时是否设置为默认关闭；
d) 使用暴力破解工具对硬件接口进行暴力破解，检测其是否具备防爆力破解的功能
e) 审查厂商提交的文档，查看硬件接口是否支持一机一密鉴别机制。

5.2.3 PCB 板级防护检测方法

通过以下方法确认对PCB板级防护的安全处理是否满足要求：

a) 检查PCB板上，有没有版本、功能性丝印或者丝印不涉及敏感信息，则认为达到PCB板级防护安全要求；
b) 检查PCB板上芯片，如已经做好覆盖防护或者抹去logo等敏感信息，则认为达到PCB板级防护安全要求；
c) 检查PCB板上，如关键信号有内部走线，并且不可被探测，应用物理手段增加辨别线路走线的难度，则认为达到PCB板级防护安全要求。

5.2.4 芯片安全的检测方法

5.2.4.1 调试安全检测

检测方法参考5.2.2节。

5.2.4.2 加密参数安全检测

通过以下方法确认加密参数安全是否符合要求：

a) 检测存储在DRAM中的会话秘钥是否添加附加的纠错码；
b) 通过软件模拟存储芯片整体硬件加密过程，检测加密参数是否与移动终端硬件特征信息相关；
c) 检测用户口令、用户指纹、图形密码是否直接作为密码使用。

5.2.4.3 固件存储安全检测

通过以下方法确认固件存储安全是否符合要求：

a) 检测固件是否存储在安全受控存储区域，缺省状态是否可修改；
b) 芯片固件存储于芯片内部受控访问存储区域的，检查是否附加检错码保护其完整性；
c) 芯片固件存储于芯片内部受控访问存储与区域的，检测是否附加数字签名保护其完整性；
d) 检测芯片固件是否采取安全删除措施，芯片固件是否可以恢复；
e) 芯片固件采用加密存储的，检测加密参数是否与移动终端硬件特征信息相关。

5.2.4.4 存储芯片完整性检测

通过以下方法确认存储芯片完整性是否符合要求：

a) 检测以Flash作为存储载体的芯片是否具备检错与纠错功能，以保护其存储单元的完整性；
b) 检测以DRAM作为存储载体的芯片是否具备检错与纠错功能，以保护其存储单元的完整性。

5.2.4.5 应用处理器芯片安全检测

通过以下方法确认应用处理器芯片安全是否符合要求：

a) 检测应用处理器芯片的版本号是否为该国或地区许可使用的；

b) 修改应用处理器芯片固件或者更换应用处理器芯片，检测终端能否正常启动。

5.2.4.6 故障检测与恢复机制检测

检测应用处理器芯片是否在其内部或者外部设置看门狗电路。

5.3 软件安全规范

5.3.1 性能安全测试

通过根据正常功能编写的测试语料、测试用例，对功能进行测试，如果测试都能通过，与预期功能表现一致，则认为是满足正常功能测试。测试语料包括：

a) 控制指令语料；

b) 唤醒命令字语料；

c) 多媒体技能语料，包括但不限于音乐播放语料、电台播放语料、有声资源播放语料；

d) 资讯类语料，包括但不限于天气查询语料、日期查询语料、日程安排查询语料；

e) 闲聊测试语料。

5.3.1.1 语音唤醒成功率：

按照附录A进行下列操作：

a) 循环播放一个唤醒音频100次，统计唤醒成功率；

b) 播放来自不同样本的100个唤醒音频，统计唤醒成功率。

5.3.1.2 命令字识别成功率

按照附录A进行下列操作：

a) 使用人工嘴播放唤醒命令字和命令词，使用分贝仪测量设备麦克风处的声压值为65dBA；

b) 播放1500次唤醒命令字和命令词，命令字被正确识别的次数记为X1；

c) 命令字识别成功率 = X1/1500。

5.3.1.3 误唤醒频次

应按下列操作：

a) 循环播放噪声24小时，要求噪声中不含有唤醒命令字的音频内容；

b) 安静条件下，设备静置24小时。

5.3.1.4 非常用表达功能安全测试

通过根据正常使用而刻意编写的反例测试语料、测试用例，对使用功能进行测试，如果测试功能都没误识别、执行，并且反馈相应提示，则认为对于非常用表达功能安全符合要求。

测试语料包括但不限于：

a) 测试语料的否定说法，例如正确指令是：打开空调，测试语料是：不要打开空调；

b) 更换动作主体，例如正确指令是：打开空调，对应的测试语料是：打开风扇；

c) 用测试主体相关的闲聊语料测试，例如：空调放哪里比较好；
d) 特定功能的边界范围测试。应用软件安全测试

5.3.1.5 应用软件签名安全测试

检查智能语音控制器的应用软件是否在展示出包含供应商或者开发者的数字签名信息和软件属性信息（如版本名称、版本信息和描述等）

5.3.1.6 应用软件身份认证安全测试

a) 检查智能语音控制器的应用软件是否采用了适宜的认证要素，包括但不限于手势密码、短信验证码、生物特征信息和图形验证码；检查各个身份认证要素是否相互独立，即部分要素的损坏或者邪路不应导致其他要素损坏或者泄露；
b) 手势密码为至少连续不间断的4个点；短信验证码应仅可成功使用一次，且在规定时间内使用，短信验证码具备长度和随机性的要求，短信验证码所在的短信内容中，告知了用户短信验证码的发送方、用户以及有效时间；声纹要素符合JR/T 0164-2018要求；其他生物特征认证要素，符合国家和相关信息安全管理要求，能够防止非法存储、复制和重放；
c) 图形验证码具有使用时间限制并仅能使用一次，图形验证码由服务器生成，客户端源文件中不包含图形验证码文本内容。

5.3.1.7 应用软件认证信息安全测试

检查智能语音控制器的应用软件是否对认证信息提供了安全性措施，包括但不限于采用了替换输入框原文、逐字符加密、字符加密、防范键盘窃听、自定义软键盘，或者通过其他方式保证攻击测试无法获取输入信息的明文。

5.3.1.8 应用软件认证失败安全测试

检查智能语音控制器的应用软件是否有认证失败处理机制，包括但不限于采取结束会话、限制非法登录次数和自动退出等措施；检查应用软件在认证失败后，提供的认证失败信息是否模糊，是否包含用户的账号、密码等敏感数据。

5.3.1.9 应用软件权限控制安全测试

检查智能语音控制器的应用软件权限申请设计是否遵循了最小化原则；检查智能语音控制器的应用软件在申请个人信息的权限时，是否逐一同步告知了用户申请权限的目的，表述是否明确且清晰

用户拒绝客户端应用软件的某权限申请后，应用软件最多再提示一次，用来解释该权限的申请原因，以及无此权限的后果。若用户坚持拒绝后，则应用软件不应频繁向用户申请该权限，但支持App正常运行，或用户主动选择使用的某一具体功能触发征得同意的动作，不属于频繁干扰情形

5.3.1.10 应用软件抗攻击能力安全测试

使用静态分析、动态调试等操作对应用软件进行攻击，检查智能语音控制器的应用软件是否具有抵御静态分析、动态调试的能力。

语音内容应该保持中立。使用一些敏感词语测试产品反馈，对产品的回复进行内容审核，要求回复内容不涉及种族歧视、色情、教唆、暴力等。

5.3.1.11 抵御非法攻击的安全测试

使用 22kHz、30kHz、50kHz 的唤醒音频分别对产品进行 10 次唤醒测试，检查产品是否能被唤醒。

5.4 信息安全的测试

5.4.1 语音监听安全测试

应按下列操作：

a) 只进行用户授权的监听行为，验证产品说明书中是否明确表述和提示用户，打开语音功能会收集个人语音信息；
b) 对已授权的监听行为，验证产品是否仅存储语音信息的摘要信息；
c) 在使用声纹识别实现识别身份、认证等功能后，验证产品删除掉可提取个人生物识别信息的原始数据；
d) 验证摘要信息的不可逆性，确保通过摘要信息无法回溯到原始信息。

5.4.2 传输安全测试

应按下列操作：

a) 验证设备实际通信过程中的数据加解密和完整性校验是否与预期的正确结果相符；
b) 破坏数据完整性，验证数据恢复机制的有效性；
c) 按GB/T 20270-2006中的第6章进行测试。

5.4.3 认证安全测试

按GB/T 20270-2006第5章、第6章和第7章中的要求，对身份认证进行测试。

5.4.4 操作系统安全测试

应按 GB/T 34976-2017 中第 6 章的要求测试。

5.4.5 隐私安全测试

5.4.5.1 隐私数据收集测试

应按下列操作：

a） 核查语音控制器生产制造商是否对隐私数据的采集的数据具有明确、清晰、具体的说明。核查采集用户数据的清单，包括但不限于数据类型、采集方式、采集目的等。
b） 核查语音控制器生产制造商是否就隐私数据的采集的目的、方式、范围、规则对用户进行明确、清晰的说明，并提出授权许可。
c） 核查采集的用户个人信息是否是业务应用必需的。
d） 核查采集的隐私数据不可转让不可出售。

5.4.5.2 隐私数据存储测试

应按下列操作：

a） 核查向个人信息主体明示的隐私数据的存储相关协议；
b） 核查是否制定了有关用户个人信息保护的管理制度和流程。
c） 核查是否采用技术措施限制对用户个人信息的访问和使用；
d） 核查语音控制器生产制造商所采取的管理措施和技术手段，判断是否能够保护个人信息的保密性、完整性、可用性；
e） 核查存储的隐私数据是否存在定期的清理机制。

5.4.5.3 隐私数据使用

应按下列操作：

a） 核查语音控制器生产商是否向个人信息主体明示的隐私数据的使用范围、目的、规则等，并具有明确的用户许可授权；

b） 核查语音控制器生产商隐私数据的使用是否有接受外部及用户监督的机制；

c） 核查语音控制器生产制造商是否具有向个人信息主体提供查询、更正、删除、撤回、投诉等方法。

d） 核查语音控制器生产制造商是否为了商业用途使用隐私数据。

附 录 A
（规范性）
语音性能测试

A.1 测试基本要求

A.1.1 通用要求

测试过程的通用要求见下：

a) 所有测试均按语音模组技术规格书规定的标准测试配置条件下，配备标准规格的麦克风和语音播放元器件进行测试；
b) 所有测试均在典型混响环境下测试（RT60的值在0.2s～0.4s）。
c) 所有测试均保证信噪比差值不小于10dB（回声噪音环境除外）；
d) 人工嘴语音指令和环境噪声的声音音量均以声级计接收到的声音分贝为准，单位dB(A)，应在测试开始前调整人工嘴和环境噪声源音箱的音量，使声级计在3min内测得平均噪声（声压级）符合测试项目规定值；
e) 按被测设备（EUT）布局图来布置测试设备和环境噪声源设备，每次测试仅施加一个噪声源。

A.1.2 语音测试场地要求

语音测试场地要求应符合IEEE 2899.1标准

A.1.3 语音测试集要求

测试用语音测试集要求应符合IEEE 2899.3标准

A.1.4 语音测试噪声要求

测试用噪声要求应符合IEEE 2899.3标准

A.1.5 语音性能测试记录要求

测试报告要记录每次测试的测试语音库和相关测试参数，至少包括：

a) 测试语音库、测试语音音量；
b) 测试环境类别、环境噪声音量；
c) 测试位置、测试角度、拾音距离；
d) 样品编号、详细测试记录。

A.1.6 拾音距离

人工嘴与被测设备（EUT）的水平直线距离L有1m、3m、5m三种拾音距离测试方案，在人工嘴不同测试角度下，分别按不同拾音距离进行测试。具体选择哪一种或多种拾音距离来测试，应按语音模组在整机产品中实际使用情况而定。

如果制造商在技术规格书中规定了其他特殊的拾音距离，应按所规定的拾音距离进行测试。

A.1.7 声级计放置要求

声级计应位于被测设备（EUT）的麦克风主入声口平面，并与麦克风尽量靠近（两者之间距离不超过50mm），但不能碰到EUT的外壳，避免发音震动引起的干扰。

参 考 文 献

[1] GB/T 20272-2019　信息安全技术 操作系统安全技术要求

[2] GB/T 21028-2007　信息安全技术 服务器安全技术要求

[3] GB/T 34835-2017　电气安全与信息技术和通信技术网络连接设备的接口分类

[4] GB/T 34083-2017　中文语音识别互联网服务接口规范

[5] GB/T 21023-2007　中文语音识别系统通用技术规范

[6] GB/T 25068.3-2010　信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护

[7] JB/T XXXX-XXXX　家用及类似用途智能家电控制器 语音模组技术规范（报批稿）