ICS 17.040.30
N 10

团　体　标　准

T/CAMETA XXX—2024

人形机器人人机交互与安全技术规范

Human robot interaction and safety technical specifications for humanoid robots

（征求意见稿）

2024-XX-XX 发布　　2024-XX-XX 实施

中国机电一体化技术应用协会　　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这些专利的责任。

本文件由中国机电一体化技术协会提出并归口。

本文件参编单位：哈工大机器人技术与系统全国重点实验

本文件主要起草人：

1 范围

本标准规定了人形机器人在X方面的技术要求，适用于人形机器人在工业、服务、医疗等领域的应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性应用而构成本文件必不可少的条款。其中，标注日期的引用文件，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 5226.1-2019 机械电气安全 机械电气设备 第1部分:通用技术条件

GB/T 36530-2018 机器人与机器人装备 个人助理机器人的安全要求

GB/T 36008-2018 机器人与机器人装备协作机器人

GB 11291.1-2011 工业环境用机器人 安全要求 第1部分：机器人

GB 11291.2-2013 机器人与机器人装备 工业机器人的安全要求 第2部分：机器人系统与集成

GB/T 38244-2019 机器人安全总则

GB/T 41393—2022 娱乐机器人 安全要求及测试方法

GB/T 38260-2019 服务机器人功能安全评估

GB/T 39785—2021 服务机器人 机械安全评估与测试方法

GB/T 18029.13-2008 轮椅车 第13部分：测试表面摩擦系数的测定

GB/T 16855.1-2018 机械安全 安全控制系统 第1部分：设计通则

GB 28526-2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

ISO/IEC 18033（所有部分） 信息技术 安全技术 加密算法（Information technology—Security techniques—Encryption algorithms）

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 43969-2024 智能语音控制器通用安全技术要求

GB/T 31488-2015 安全防范视频监控人脸识别系统技术要求

GB/T38671-2020 信息安全技术远程人脸识别系统技术要求

GB/T 38244 机器人安全总则

3 术语和定义

GB/T 36530—2018、 GB/T 38244-2019、GB/T5226.1-2019、GB/T 31488-2015 界定的以及下列属于和定义适用于本文件。

3.1

人形机器人 humanoid robot

人形机器人，也被称为仿人机器人，是指模仿人类外观和行为特征的机器人。它们通常具有类似人类的头部、躯干、四肢等结构，并且能够模拟人类的行走、手势、面部表情等动作。

3.2

准静态接触 quasi-static contact

人机交互过程中人员与机器人系统部件之间的接触，这种接触人员身体部位可能被夹在机器人系统运动部件，以及另一个机器人单元固定或运动部件之间。

[改写 GB/T 36008—2018，定义 3.4]

3.3

暂态接触 transient contact

人机交互过程中人员与机器人系统部件之间的接触，这种接触人员的身体部位没被夹住，并从机器人系统运动部件上反弹或撤回。

[改写 GB/T 36008—2018，定义 3.5]

3.4

人机交互 human-robot interaction

HRI

人和机器人通过用户接口交流信息和动作来执行任务。

示例：通过语音、视觉和触觉方式交流。

3.5

安全交互空间 **secure interactive space**

为确保人员安全和机器人正常运行而设定的特定区域。这个空间定义了人形机器人可以安全操作的边界，以防止其运动对周围的人员或物品造成伤害。

3.6

语音控制器 speech control

通过语音识别，将语音输入转换为设备交互或功能控制指令，从而对设备进行交互或功能控制的一种控制器。

3.7

语音识别 speech recognition

将人类的声音信号转化为文字或者指令的过程。

[来源：GB/T 21023-2007,3.1]

3.8

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]

3.9

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]

3.10

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所需的特征或事件时，语音唤醒系统被唤醒的现象。

[来源：GB/T 36464.1-2020,3.19]

3.11

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]

3.12

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]

3.13

白噪声攻击 white noise attacks

攻击者向语音识别系统输入一些带有攻击指令的白噪声语音信号，以此来干扰语音控制器安全的一种攻击方式。

3.14

唤醒识别率 wake up failure rate

唤醒命令字唤醒失败的次数和唤醒总次数之比。

3.15

二次唤醒识别率 second wake up

在首次唤醒和当次的监听结束之间的唤醒。

3.16

二次唤醒识别率 second wake up failure rate

二次唤醒测试过程中，二次唤醒总次数减去二次唤醒成功次数的结果，与二次唤醒总次数之比。

3.17

交互对象 interative object

与人形机器人进行信息交互的对象总称，包括人体，环境，操作对象等

3.18

识别区域 recognition region

人形机器人识别系统划定的确定的区域，进入该区域的人可被机器人识别系统有效识别。

3.19

人机界面 human-robot interface

人形机器人与人进行视觉、听觉、力觉等多模态信息及行为交互的软硬件接口。

3.20

人体特征 body feature

个体或群体的行为特征和生物学特征集合。

3.21

目标特征 object feature

人形机器人感知对象的信息集合。

3.22

姿态估计 pose estimation

对机器人本体及交互对象相对于空间坐标原点位置和角度状态的测量计算。

4 基本要求

4.1 通用要求

面向人机交互的人形机器人系统应采用模块化设计，并包括运动控制模块、感知模块、电源管理模块、安全模块、通信模块及用户界面模块等功能模块。硬件系统应支持总线接口并具备实现 I/O 扩展以及各种通信接口的柔性扩展能力。软件系统不仅需要支持各种硬件模块的控制和管理，还应具备高可靠性、实时性、安全性等特点。

4.2 硬件系统要求

4.2.1 控制器模块

控制器模块应具备浮点运算能力、逻辑运算能力、接口扩展能力，并应具有实时操作系统。主控平台应具备通用的如串口、以太网、USB、VGA、LCD 等接口。

4.2.2 传感器模块

具备检测人机交互和机器人与物体之间的力交互的六维力传感器，具备检测机器人与物体或人的接触情况的触觉传感器，提供接触位置、压力分布等信息，具备视觉传感器，测距传感器，辅助检测碰撞，提供视觉及深度信息，用于物体识别、人体特征识别和环境感知，并且图像采集模块应具备高清晰度图像采集能力，并支持多种图像格式的输入。

4.2.3 电源模块

电源模块应支持多种电源输入方式，如直流电源、电池等，提供高效的电源转换器，确保稳定的电源输出。同时具备过载保护功能，防止电源损坏。

4.2.4 安全模块

具备紧急停止按钮，能在紧急情况下，迅速停止机器人的所有运动。

4.2.5 通信模块

硬件接口应具备良好的兼容性，同类总线设备硬件应使用 RJ45、D 型数据接口连接器等通用、一致的封装以及对应引脚信号的接口。

I/O 接口模块应包含数字量输入输出，模拟量输入输出，具备以太网、Can 总线、RS232/RS485 接口、USB、SD 卡等接口。

4.2.6 告警模块

系统应具备告警模块，并根据告警信息，以声光形式输出警告。

4.3 软件系统要求

人形机器人软件系统应具有独立运行的运动控制软件系统，并提供直观的用户界面，方便用户进行参数设置、状态监控等操作，此外应开放相应的接口以供二次开发调用。

4.3.1 运动控制软件系统

为满足人形机器人运动控制功能要求，机器人应配备运动控制软件系统，并应开放如表 1 所示的函数接口。

表 1 运动控制软件系统应开放的函数接口

函数名	描述
运动操作函数	a）上位机系统相关运动函数，主要为上肢控制，包括关节空间运动与笛卡尔空间运动，并提供直线运动、圆弧运动以及各运动之间的平滑过渡函数； b）其他运动函数； c）运动学正逆解； d）控制使前后左右移动
机器人状态操作函数	a）读取机器人当前运动状态（运动暂停、停止等标志位）； b）运动停止，终止当前运动； c）运动暂停，暂停当前运动，且可以继续未完成运动； d）运动中断，中止当前运动，完成其他操作后可继续回到原本任务完成运动； e）设定运动模式； f）读取、获得、放弃控制权限（其中权限范围由制造商给定）； g）清除错误
I/O 读写操作函数	读取、设定指定 I/O
文件读写操作函数	读取、修改、保存目标文件

运动控制软件系统应具备如下程序扩展功能：

a）指令自定义添加功能：

1）通过用户自定义方式定义系统中的新指令；

2）在系统中注册用户自定义的新指令；

3）使用所定义的新指令编写运动控制程序。

b）运动规划扩展功能：

1）预留接口添加运动规划算法；

2）直接替代系统中的运动规划算法;

4.3.2 用户界面

用户界面应提供便捷的参数调整功能，让用户可以根据具体应用场景调整机器人的行为模式、速度、力量等。提供状态监控功能，实时显示机器人的运行状态。在用户界面提供一键紧急停机功能，确保在出现异常情况时能迅速停止机器人的动作，通过声、光提示人形机器人系统运行状态，输出警告。

4.3.3 识别模块

具备识别模块，对作业场景、作业对象、人体特征信息进行处理、检测及类别判断的软件功能单元。

4.3.4 决策模块

根据作业任务中识别模块输出的条件，判断人形机器人行为输出的软件功能单元。

4.3.5 故障诊断

机器人软件系统应具备硬件设备故障的软件诊断功能，确保硬件工作异常的人机交互过程安全。

5 人形机器人力觉与触觉交互系统技术要求

5.1 安全保护功能

人形机器人应符合以下要求：

a） 每次开机或重置时，机器人应有自检和报错功能；

b） 非正常运行或操作不当，机器人应能保证安全状态，并有报警等提示，解除后仍可使用；

c） 机器人应具有保护性停止功能和独立的紧急停止功能；

d） 安全相关的速度控制和力控制功能；

5.2 控制系统安全

机器人控制系统安全应满足 GB/T 38244-2019 中 7.1 的要求。

5.3 机器人停止功能

5.3.1 紧急停止功能

人形机器人应具备紧急停止能力，每个能够启动机器人运动或造成其他可能的危险状况的指令装置应具备手动触发紧急停止功能，且满足以下要求：

e） 符合 GB 11291.1-2011 中 5.4 和 GB/T5226.1-2019 第 9.2.3.4.2 的要求；

f） 优于机器人的其他控制；

g） 停止所有受控的危险；

h） 若机器人处于安全状态，移除机器人驱动器的驱动源；

i） 保持有效直至复位；

j） 消除可由机器人控制的任何其他危险；

k） 只能手动复位，复位后（机器人）不会自动重启；

l） 应根据 GB/T5226.1-2019 中 9.2.2 选择类别 0、类别 1、类别 2 的停止功能；

紧急停止装置应符合 GB5226.1-2019 中 10.7 和 GB/T16754 的设计要求。

若指令装置没有紧急停止按钮（如语音界面、基于远程应用的电脑屏幕），则应确保现有机器人或附近的紧急停止装置能使机器人达到同样等级的安全状态。

5.3.2 保护性停止功能

人形机器人应具有至少一种保护型停止功能，保护型停止功能通过以下途径控制安全防护的危险：停止机器人所有运动、撤除机器人驱动器的动力、中止由机器人系统控制的任何其他危险等方式来控制安全防护的风险。保护性停止功能可由手动或控制逻辑自动启动。

5.4 稳定性控制

人形机器人应具有足够的静稳定性和动稳定性，在所有预定和合理可预见情况中应稳定，在正常使用条件下，不应优于其稳定性的不足对使用者造成危险。同时应设计防滑和防倾倒

机制，确保机器人在移动过程中不会因外力作用而失控。

5.5 接触式传感

在许多人机交互任务中需要接触式传感（力觉、触觉）。机器人需要能准确探测出微小的接触力，并对此做出合理方式的反馈。接触式传感应符合 GB/T 36530-2018 中 6.5.2.2 的要求。

5.6 人机交互安全

5.6.1 安全交互空间

为防范人形机器人各关节或机体的运动对附近的人员或物品造成损伤，制造商必须采用各种限制机器人交互空间的方式，如机械方式、电气控制方式、软件编程方式等，同时在说明书明确指示机器人在运行中可能出现的各种安全风险和预防方法。

人形机器人应在安全交互空间内行动，当人员或物体误进入具备伤害风险的空间或机器人超出安全交互空间时，人形机器人应具备联锁保护和防护功能，防止用户误触或误操作导致事故。

5.6.2 交互动作控制

机器人的交互动作应当设计得既柔顺又可预测，尽可能模仿人类的行为模式，提高与人类用户的亲和力。并且确保在与环境或用户互动时，不会出现无法预料的动作，此外，还应能够根据不同的使用场景调整自身的行为方式。

5.6.3 接触情况

人形机器人（Collaborative-Robot）的手臂安全碰撞速度和接触力是一个非常重要的安全指标。在设计和使用人形机器人时，必须确保其在人机交互时或与其他物体接触时候不会对人员造成伤害。这种接触可能是在预期的使用中人与机器人在人机交互过程中产生的接触，也可能是未遵循工作程序导致的偶然性接触，甚至可能是失效模式下的异常接触。通常，可将机器人系统与人体部位之间的接触类型分为准静态接触和瞬态接触。

5.6.4 安全交互速度控制

为了减小暂态接触的风险，人形机器人系统应限制机器人系统运动部件的速度，以确保机器人在与人类或其他物体发生碰撞时不会对人员造成伤害。这个速度上限值通常取决于惯性（质量）以及机器人可解除暴露身体区域的最小区域尺寸。

人形机器人人机交互安全相关的速度控制还应满足 GB/T 38244-2019 中 7.6 和 GB-T 36008-2018 中 5.5.5.6 的要求。

5.6.5 安全交互力控制

对于面向人机交互的人形机器人，交互力应可控并表明输出力或者力矩的范围。

人形机器人人机交互安全相关的力控制应通过相关的接触传感器（例如力传感器等）和反应机制来实现，使得机器接触力不能超出极限，以确保机器人在与人类或其他物体接触时不会对人员造成伤害。

最大安全接触力/扭矩的量化要求通常是根据机器人的设计、材料以及碰撞后的能量损失等因素进行确定的。GB-T 36008-2018 中的附录 A 提供了如何确定最大安全接触力的信息。

5.6.6 自主决策能力

对于具备自主决策能力的机器人，应标明自主决策能力使用范围，自主决策行为和动作应安全可控，且控制优先级低于用户。

5.7 用户界面设计

在与人机交互过程中，当交互控制设备（例如：操纵杆、操作控制面板、语音和手势识别系统以及其他设备）被用于控制人形机器人时，交互控制设备在人机交互操作过程中应具备适当的安全性和可靠性，符合 GB/T 38260—2019 中 7.3.8 的相应技术要求。

6 人形机器人自然视觉交互系统技术要求

6.1 人形机器人自然视觉交互技术安全要求

6.1.1 人脸识别性能安全要求

人脸识别技术在人形机器人中用于识别不同的人物，实现个性化交互和服务。其性能安全要求主要包括高准确率、可靠性和抗干扰性。系统需要在各种环境条件下都能稳定工作，包括不同的光照、角度和表情变化，同时能抵抗外部干扰，如伪装、遮挡等，以保证安全性。

表 1 人脸识别系统技术安全要求

技术要求	描述	标准
准确率	衡量人脸识别系统整体性能的指标，它表示系统正确识别人脸（包括正确接受和正确拒绝）的比例。	≥90%
宏平均	一种评估指标，用于处理类别不平衡问题。在人脸识别中，宏平均计算每个类别的指标（如 FAR 或 FRR）	≥90%
微平均	另一种评估指标，它首先计算所有类别的总体真正例和假正例，然后基于这些总数计算指标。	≥90%
错误接受率	系统错误地将不同人的人脸识别为同一个人的比例。	≤10%
错误拒绝率	系统错误地将同一个人的两张人脸图像识别为不同人的比例。	≤10%

6.1.2 人体姿态估计性能安全要求

人体姿态估计技术使机器人能够理解和预测人体动作，对于人机交互至关重要。其性能安全要求包括准确性、实时性和鲁棒性。系统需要能够精确识别人体关节的位置和姿态变化，并能实时响应人体动作变化，同时在复杂环境中，如人群密集或背景杂乱的情况下，仍能准确估计人体姿态。

表 2 人体姿态估计系统技术安全要求

技术要求	描述	标准
单人姿态估计	准确的单人姿态估计有助于机器人正确理解人的意图和动作，避免因误解导致的碰撞或错误响应。	≥90%
多人姿态估	在多人环境中，准确的多人姿态估计对于确保机器人正	≥90%

计	确响应每个人的指令至关重要，应保持准确率在90%~95%之间以避免混淆和潜在的安全风险。	
人体姿态跟踪	动态的姿态跟踪确保机器人能够实时响应人的动作变化，保持准确率在 90%~95%之间对于紧急情况下的快速反应和安全操作至关重要。	≥90%
3D 人体姿态估计	三维姿态估计提供了更精确的空间信息，应保持准确率在 90%~95%之间有助于机器人避免进入人的私人空间或执行可能造成伤害的动作。	≥90%

6.1.3 字符识别性能安全要求

字符识别技术使人形机器人能够识别和理解文本信息。其性能安全要求包括高识别率、速度和适应性。系统应具有高识别率，以确保文本信息的准确读取，同时需要快速响应，以适应实时交互的需求。此外，系统还需要能够识别不同字体、大小和风格的文本。

表 3 字符识别性能安全要求

技术要求	描述	标准
准确率	识别正确的字符数量占所有识别出的字符数量的比例。	≥90%
召回率	识别正确的字符数量占实际字符数量的比例。	≥90%
平均编辑距离	将 OCR 系统输出的文本转换为原始文本所需的最少编辑操作次数（如插入、删除、替换）的平均值。	≤0.05

6.1.4 物体识别性能安全要求

物体识别技术要求具备高准确性和实时性，能够快速、准确地识别和分类物体。这对于安全监控、自动驾驶等应用至关重要。此外，系统应具备鲁棒性，能够在动态环境中有效工作，确保及时、准确的检测和分类。

表 4 物体识别性能安全要求

技术要求	描述	标准
准确率	衡量物体识别系统整体性能的指标，它表示所有样本中模型正确预测的比例	≥90%
宏平均准确率	给所有类别相同的权重，能够平等看待每个类别，但值	≥90%

	会受稀有类别影响，更加关注类别少的样本。	
微平均准确率	先对数据集中的每一个实例不分类别进行统计建立全局混淆矩阵，然后计算相应指标。	≥90%
平均精度均值	评估目标检测性能的黄金标准，它计算每一个类别的平均精度（AP），然后对所有类别的 AP 求平均值。	≥95%

6.1.5 物体抓取性能安全要求

物体抓取性能安全是人形机器人操作物体的基本安全规范要求，是实现人形机器人稳定物体抓取重要前提。其性能安全要求主要包成功率、鲁棒性和抗干扰性。系统需要在各种环境条件下都能稳定工作，包括不同环境光照、角度变化、遮挡等，以保证安全性。

表 5 物体抓取性能安全要求

技术要求	描述	标准
物体位姿估计	指确定物体在空间中的位置和方向的能力。	≥4 级
抓取成功率	机器人在一次抓取任务中成功抓取目标物体的比例	≥90%
稳定性	机器人抓取过程中不会发生滑落或损坏物体	≥90%
矩形指标	抓取角度在抓取真值的 30°范围内，认为抓取是正确的 Jaccard 指数	≥25%
重复定位精度	衡量机器人在重复执行相同任务时的定位准确性，确保抓取的一致性和可靠性	≤1mm
规划时间	接收图像和返回计划抓取之间的时间	≤0.08 秒

6.2 人形机器人自然视觉交互隐私安全要求

6.2.1 采集安全要求

采集安全应确保数据采集的服务安全和终端设备的物理安全，包括但不限于：

a） 具备安全芯片、可信赖的计算环境等保障生物认证类视觉数据安全性的方案；

b） 减少设备向系统外部传递信息，关闭无用端口，包括但不限于：前期的调试接口、程序烧录及诊断测试接口；

c） 采集设备应具有物理安全防护措施，包括但不限于防干扰、防拆卸等措施，确保数据采集终端设备的物理安全。

d） 对于业务必须开放的接口，采取接口鉴权机制，防止接口被非法调用；

e） 定期审查配置设备，设备具备固件自动升级能力，且采取安全的更新方式；

f） 具备视觉数据分类和敏感隐私数据检测能力；

g） 具备物理遮蔽手段，能够通过镜头盖、旋转、伸缩等物理方式在关闭摄像服务时提供遮蔽。

6.2.2 传输安全要求

感知设备和应用之间的网络与传输安全，应满足：

a） 接入认证

1） 应当利用安全插件进行终端异常分析等，实现终端入侵防护，避免发生借助终端攻击网络关键节点等行为；

2） 强制进行单向/双向认证机制，阻止非法节点接入；

b） 通道加密，视觉数据的传输安全原则应当满足；

1） 支持但不限于采用专用内网、安全协议的方式保证数据的安全传输方式；

2） 实现加载内容的过滤和访问限制；

3） 采用视觉加密算法传输加密后的视频数据，保证数据机密性；

4） 具有数据的完整性及时效性检验功能。

6.2.3 存储安全要求

系统在收集和使用视觉数据时，首先对数据进行分类分级，然后使用视觉加密算法加密存储视觉隐私数据。应满足如下要求：

a） 用户按照存储需要,将不同的信息存储在不同的密箱中,且密箱之间是相互隔绝的，对其他 用户不可见；

b） 系统中的应用卸载或账户注销后，系统应当具备删除内部存储的所有文件的能力；

c） 外部存储可用于数据共享，开发者应谨慎使用外部存储，避免将用户的隐私数据写入外部存储；

d） 使用加密机或者密钥托管服务管理用户主密钥和数据密钥；

e） 存储用户视觉隐私数据的设备应具备对隐私数据快速加密的能力。

6.2.4 存储安全要求

处理组件应提供相应的身份鉴别和访问控制机制,确保只有合法的用户或应用程序才能发起数据 处理请求。

a） 算法安全，主要面临算法黑箱、算法模型缺陷等风险，应满足如下要求：

1） 对核心算法的框架和组件进行严格的测试管理和安全认证，减少因算法漏洞和后门等引发安全风险；
2） 充分评估算法潜藏偏见和歧视，避免产生与预期不符甚至伤害性结果，确保系统决策结 果可控；
3） 应保证算法的准确性，鲁棒性和可解释性，保证算法的核心指标是可验证的；
4） 算法应具备一定的防对抗攻击能力，以防止经过特殊构造产生的样本让分类器的分类结果不可靠；
5） 加强 AI 模型的保护，采用高强度的加密算法对 AI 模型进行保护，或者采用其他更高级的数据保护机制进行保护。

b） 身份鉴别与访问控制，应满足如下要求：
1） 对于 FTP 服务密码、登录密码、外部系统接口认证密码等隐私数据，应加密存储；
2） 应具备对第三方软件访问数据权限的控制能力，能够发现或记录非授权应用访问数据；
3） 对隐私级别高的视觉数据设置双因子或多因子的身份鉴别机制；
4） 对数据库账号异地登陆的情况给予提示；
5） 确保参与模型训练的数据集的内容安全，并保障数据集的完整性和代表性，防止数据投毒攻击；
6） 对生物特征数据所有用途、目的和方式都应提供可靠的安全手段，包括但不限于独立存储、数据加密、本地处理、拒绝上传等。

6.2.5 应用安全要求

人工智能视觉隐私数据的应用安全应满足如下要求：

a） 构建完善的应用管控保障机制，提供应用签名、内存保护、恶意网址检测、流量监控等措施 保障应用安全；
b） 数据发布前，应当对隐私数据采取去标识化、匿名化等技术实现数据脱敏；
c） 敏感视觉数据在存储和应用时应支持脱敏；
d） 应具备代码安全审计功能，尤其防止反编译导致密钥丢失；
e） 人工智能产品或应用在保证信息安全的同时，保证功能安全；
f） 数据共享时，应采用安全共享手段，包括但不限于同态加密、联邦学习等方式；
g） 已发布或已授权共享的数据，应支持用户数据的可溯源、数据流通过程的可监控。

6.2.6 其他安全要求

应针对涉及未满 14 周岁的儿童的视觉隐私数据采取专门措施，确保：

a) 只有在征得父母或者监护人的同意等情况下才可以处理；

b) 在父母或监护人未同意的情况下收集的儿童人工智能视觉隐私数据应立即予以删除。

7 人形机器人自然语音交互技术要求

7.1 硬件安全要求

7.1.1 物理安全要求

物理安全符合以下要求：

a）应具备数据的物理包含机制；

b）应具备在收到暴力移除或拆卸时的防护预警机制。

7.1.2 硬件接口安全要求

硬件接口安全符合以下要求：

a）对于使用无线和有线外围接口的设备，宜通过指示灯或显示屏等方式，提供数据传输状态的监控功能；

b）对于具有调试功能的接口，应在出厂时设置为默认关闭。

7.2 软件安全要求

7.2.1 功能安全要求

5.2.1.1 唤醒失败率要求

语音唤醒失败率应符合表 1 规定。

表 1 唤醒失败率要求

环境条件	唤醒失败率		
	拾音距离 1m	拾音距离 3m	拾音距离 5m
安静*	<7%	10%	12%
噪声*	<10%	13%	15%
* 安静及噪声环境条件按 GB/T 43969-2024 附录 A 给出的分类。			

5.2.1.2 二次唤醒失败率要求

语音二次唤醒失败率应符合表 2 规定。

表 2 二次唤醒失败率要求

环境条件	二次唤醒失败率		
	拾音距离 1m	拾音距离 3m	拾音距离 5m
安静*	<5%	8%	10%
噪声*	<8%	11%	13%
* 安静及噪声环境条件按 GB/T 43969-2024 附录 A 给出的分类。			

5.2.1.3 命令字识别异常率要求

命令字识别异常率要求符合表 3 规定。

表 3 命令字识别异常率要求

环境条件	命令字识别异常率		
	拾音距离 1m	拾音距离 3m	拾音距离 5m
安静*	<12%	15%	20%
噪声*	<15%	20%	25%
* 安静及噪声环境条件按 GB/T 43969-2024 附录 A 给出的分类。			

5.2.1.4 误唤醒频次要求

安静及噪声环境条件分别进行测试，误唤醒频次符合以下要求：

a）噪声环境条件下，应符合 24h 内误唤醒频次不高于 3 次；

b）安静环境条件下，应符合 24h 内误唤醒频次不高于 1 次；

5.2.1.5 白噪声攻击稳健性要求

对于白噪声攻击后的语音识别系统应具有稳健性，在受到白噪声攻击后，语音控制器应保持功能逻辑正常，安全性不受影响。

7.2.2 应用软件安全要求

5.2.2.1 应用软件签名安全要求

应用软件应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）。

5.2.2.2 应用软件认证信息安全要求

应用软件应对于认证信息提供安全性措施。

5.2.2.3 应用软件认证失败处理安全要求

应用软件应对于认证失败处理机制。

5.2.2.4 应用软件权限控制安全要求

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。

7.3 信息安全要求

7.3.1 语音监听安全要求

语音监听安全符合以下要求：

a）应确保所有用户的音频数据都得到保护，不会被未经授权的人员访问或使用；

b）在用户未授权的情况下，不允许保存用户音频；

c）对于监听到的非业务逻辑需要的音频，应舍弃掉。

7.3.2 传输安全要求

传输安全符合以下要求：

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；

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。

7.4 操作系统安全要求

7.4.1 调试安全要求

具备调试功能的语音控制器符合以下要求：

a）用户进入操作系统前宜先由用户标识，在操作系统的整个生存周期内保证用户的唯一标识；

b）在用户执行任何与安全功能相关的操作前应对用户进行鉴别；

c）宜采用加密方法对鉴别信息的存储进行保护；

d）将用户进程与所有者用户相关联，是用户进程的行为应可以追溯到进程的所有者用户。

7.4.2 访问控制要求

具备可访问存储区域的语音控制器符合以下要求：

a）应遵循最小权限原则，只能访问所需完成任务所需的资源和信息，不应越权访问其他资源和信息；

b）针对未授权的访问，应具有阻止其访问的能力；

c）针对不同角色的用户，包括但不限于普通使用者、开发调试人员等，应分配不同的权限。

7.4.3 OTA 更新能力要求

对于带 OTA 更新功能的语音控制器符合以下要求：

a）对于具有操作系统 OTA 更新功能的语音控制器，应支持操作系统的 OTA 更新；

b）应至少采取一种安全机制，保证 OTA 更新过程的安全性；

c）OTA 更新后的系统安全属性应不低于 OTA 更新前的系统安全属性；

d）OTA 失败时，系统应能够回滚，并保证系统完整性，且安全属性与 OTA 更新前一致；

e）宜至少采取一种安全机制，保证 OTA 的时效性，例如自动 OTA，更新通知等手段。

7.5 数据安全要求

7.5.1 数据可用性

数据可用性符合以下要求：

a）在传输其采集到的数据时，应对数据新鲜性做出标识；

b）应能够鉴别数据的新鲜性，避免历史数据的重放攻击。

7.5.2 数据完整性

数据应在存储和处理过程中保证完整性。

7.5.3 数据保密性

数据保密性符合以下要求：

a）应对数据采用密码算法进行存储和传输保密保护；

b）重要数据加密算法应符合 ISO/IEC 18033（所有部分）相关要求。

7.6 隐私安全要求

7.6.1 通则

按 GB/T 35273-2020 的要求，人形机器人自然语言交互在交互相关隐私信息时应遵循合法、正当、必要的原则，其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。人形机器人自然语言

交互过程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。

7.6.2 隐私数据收集

隐私数据收集符合以下要求：

a）人形机器人在人机交互过程中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）人形机器人在人机交互过程中采集隐私数据时应向被采集者（以下简称“使用方”）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）人形机器人在人机交互过程中采集隐私数据时，只处理满足使用方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）人形机器人在人机交互过程中采集的隐私数据不可出售、不可转让；

e）在关闭唤醒状态或语音功能下，禁止采集隐私数据。

7.6.3 隐私数据存储

隐私数据存储符合以下要求：

a）人形机器人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；

b）存储的隐私数据应具有定时清理机制。

7.6.4 隐私数据使用

隐私数据使用符合以下要求：

a）人形机器人制造商应向交互对象以明确、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）人形机器人制造商应向交互对象提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账号、投诉等方法；

c）人形机器人制造商意思数据仅限于改善产品及交互体验。

8　人形机器人力觉与触觉交互检测方法

8.1 测试条件

7.1.1 测试前提条件

测试前应准备以下文件：

a）测试相关设计文件、图样及接口说明；；

b）　产品说明书、操作手册、维护手册等。

在测试前机器人应进行适当的预热，机器人应处于正常工作状态，确保整个测试过程中以安全的方式操作。

7.1.2 测试环境要求

除本文件或详细规范另有规定外，所有测试应在下列条件下进行：

c）温度：室内 0℃~40℃，室外温度应在制造商规定的工作温度范围内；

d）　相对湿度：0%~80%；

e）气压：86kPa~106kPa；

f）地面或坡面：摩擦系数在 0.75~1.0 范围内，根据 GB/T 18029.13-2008 测量。

如果制造商指定的环境条件超出以上条件，应在测试报告内说明。

8.2 安全保护功能测试

根据机器人操作说明对机器人进行开机和重置操作，观察是否有自检和报错功能。

根据机器人操作说明配置机器人参数时，对错误的运行参数设置进行测试，启动运行后观察能否安全使用。

结合使用说明书，观察机器人是否具备单独的电源开关和紧急停止装置，并按照说明书规定方法模拟操作紧急停止装置，检查紧急停止装置是否满足功能要求。

8.3 控制系统安全测试

控制系统安全测试按照 GB/T 16855.1-2018 或 GB 28526-2012 规定的方法及逆行评估。

8.4 机器人停止功能测试

8.4.1 紧急停止功能测试

通过视觉检查、实际实验、在操作中观察，人形机器人在正常工作状态下，按下紧急停止按钮或运行具有停止功能的软件。人形机器人在紧急停止后不应对人员造成二次伤害，且有使人员脱离危险状态的措施。人形机器人的紧急停止功能应符合 6.3.1 中的要求。

8.4.2 保护性停止功能测试

人形机器人应具备一种或多种保护性停止功能，在正常工作状态下，每次模拟一种可触发保护性停止的条件，观察人形机器人是否进入保护性停止状态。人形机器人的保护性停止功能应符合 6.3.2 中的要求。

8.5 稳定性测试

8.5.1 静稳定性测试

按照以下方法进行测试：

a) 平面测试：将人形机器人放置在平坦、稳定的平面上，如实验室桌面或特制的测试平台上。观察机器人在静止状态下是否能够保持平衡，不出现倾倒或滑动现象；

b) 倾斜测试：将测试平面逐渐倾斜，模拟机器人在斜坡或不平整地面上的工作环境。观察机器人在不同倾斜角度下的平衡表现，记录能够保持平衡的最大倾斜角度；

c) 外力干扰测试：在机器人静止状态下，施加轻微的外力干扰，如轻推或轻拉。观察机器人是否能够迅速恢复平衡状态，并记录恢复平衡所需的时间。

8.5.2 动稳定性测试

按照以下方法进行测试：

a)步态稳定性测试：进行行走、奔跑等动态动作的测试，以评估机器人在这些高度动态活动中的稳定性和平衡能力；

b)地形适应性测试：测试机器人在受到突然干扰或在不平坦地形上行走时的稳定性和恢复能力；

c)负载稳定性测试：给机器人附加不同重量的负载，测试其在携带负载时的行走稳定性。

8.6 人机交互安全测试

8.6.1 安全交互空间测试

根据人形机器人结构形式和运行机制进行相关实验及检查， 验证安全交互空间是否符合产品说明书标称范围，对存在风险的工作空间，通过外置的机器人交互空间干扰试验装置对其交互空间施加干扰以验证安全联锁装置的有效性，可参照 GB/T 39785—2021 中 5.4.4 的相关适用性标准测试验证。

8.6.2 交互动作控制测试

对于具备人机交互功能的机器人，进行实际交互，观察机器人运动柔顺性，并观察是否存在执行危险的未定义交互动作。

8.6.3 安全交互速度控制测试

按照以下步骤进行测试 ：

a) 检查制造商对机器人动作速度控制的限值说明；

b) 按照其结构形式和运行机制进行相应操作试验及检查；

c)通过适宜的速度测量设备和加速度传感器机器人动作速度进行测量，安全适用的速度限制值应参考制造商说明或参考 GB/T 36008—2018 中的附录 A.3.6 给出的数值。

8.6.4 安全交互力控制测试

按照以下步骤进行测试 ：

a) 检查制造商对机器人交互作用力控制的限值说明；

b) 按照其结构形式和运行机制进行相应操作试验及检查；

c) 通过适宜的力传感器进行接触测量，通过将机器人在准静态、暂态情况下与人接触产生的压力和力的测量结果与标准给出的机器人功率与力阈值进行比较，可以判定机器人的安全性。

d) 对具备拟人手的夹抓挤压功能特征的执行器，其典型性的参考 GB/T 38124—2019 中“5.3.1 手指指力”、“5.3.2 手臂负载能力”等适用性标准测试验证。

8.6.5 自主决策能力测试

机器人开机进行实际操作检查，验证自主决策操作是否符合产品说明书标注的安全性；自主决策能力启用时，验证人工操作机器人的优先级是否满足 6.6.6 规定的要求。

8.7 用户界面测试

检查制造商对机器人与人交互的操作控制装置设计说明，并通过视觉检查、实际试验进行验证。

8.8 接口及互换性测试

验证机器人各类接口的功能，以及不同设备、模块之间的兼容性，确保接口和模块均满足控制需求。

9 人形机器人自然视觉交互检测方法

9.1 基本测试要求

测试方法应包括两方面：

——机器人视觉算法测试；

——机器人视觉整机测试。

9.2 测试集安全要求

测试数据库安全要求如下：

a） 测试数据库的收集、委托处理、共享、转让等应满足 GB/T 35273 及 GB/T 40660 中关于信息收集、委托处理、共享、转让的相关要求；

b）测试数据应进行脱敏处理；

c）测试数据应加密存储；

d）测试数据存储设备应有专人负责保管。

9.3 测试集数据要求

测试集数量应不少于 20000 张。

9.4 整机视觉安全测试要求

9.4.1 一般要求

应根据应场景进行测试，对应的测试结果不应低于机器人视觉算法测试结果。

注：跨场景应用的机器人宜分别在室内、室外环境下进行整机测试。

9.4.2 室内要求

9.4.2.1 电磁兼容性

电磁发射应符合 GB/T 17799.4 的要求，电磁抗扰度应符合 GB/T 17799.2 的要求。

9.4.2.2 气候环境适应性

测试环境温度应为制造商宣称的温度限值。

9.4.2.3 防护等级

防护等级应满足 GB/T 4208 规定的 IP65 的要求。

9.4.3 室外要求

9.4.3.1 电磁兼容性

电磁发射应符合 GB 17799.3 的要求，电磁抗扰度应符合 GB/T 17799.1 的要求。

9.4.3.2 气候环境适应性

测试环境温度应为制造商宣称的温度限值。

9.4.3.3 防护等级

防护等级应满足 GB/T 4208 规定的 IP65 的要求。

9.5 测评方法及公式

9.5.1 准确率为对于给定的数据集，正确分类的样本数占全部样本数的比率，见公式（1）。

$$accuracy = \frac{TP + TN}{TP + FP + TN + FN} \times 100\% \quad (1)$$

accuracy——准确率；

TP——真正样本数；

TN——真负样本数；

FP——假正样本数；

FN——假负样本数。

9.5.2 宏平均准确率指对每一个类别分别计算指标值，即把每个类别视作二分类情况进行统计，然后 再对所有类的结果取算术平均值，见公式（2）：

$$acroAcc = \frac{1}{n}\sum_{i=1}^{n}\frac{TP_i + TN_i}{TP_i + FP_i + TN_i + FN_i} \times 100\%$$

式中;

AcroAcc——宏平均准确率；

TPi——i 类任务的真正样本数；

TNi——i 类任务的真负样本数；

FPi——i 类任务的假正样本数；

FNi——i 类任务的假负样本数。

9.5.3 微平均准确率指计算每个类别的真正、真负、假正、假负平均值，然后计算类别预测的统计指 标，见公式（3）：

$$MicroAcc = \frac{\overline{TP} + \overline{TN}}{\overline{TP} + \overline{FP} + \overline{TN} + \overline{FN}} \times 100\%$$

式中；

MicroAcc——微平均准确率

 ——真正样本数的平均值；

 ——真负样本数的平均值；

 ——假正样本数的平均值；

 ——假负样本数的平均值。

9.5.4 错误接受率

错误接受率（FAR）应按照 GB/T 38427.1—2019 中 3.4 的要求进行计算。

9.5.5 错误拒绝率

错误拒绝率（FRR）应按照 GB/T 38427.1—2019 中 3.5 的要求进行计算。

9.5.6 字符识别准确率指对于给定的数据集，被正确识别的字符占所有识别出的字符数的比率，见公式 （4）：

$$precision = \frac{TP}{TP + FP} \times 100\%$$

式中；

 ——字符识别准确率；

TP——真正样本数；

FP——假正样本数。

9.5.7 字符识别召回率指对于给定的数据集，被正确识别的字符占实际字符数的比率，见公式（5）：

$$recall = \frac{TP}{TP + FN} \times 100\%$$

式中；

 ——字符识别召回率；

TP——真正样本数；

FN——假负样本数。

9.5.8 编辑距离为字符串 A 到字符串 B 最少需要的操作次数。操作次数为更改一个字符，删除一个字符或增 加一个字符。对整篇文档所有行的编辑距离取平均值，即可求得到平均编辑距离，见公式（6）：

$$AED = \frac{1}{n} \sum_{i=1}^{n} edit_i \times 100\%$$

式中；

AED——平均编辑距离；

$Edit_i$——假负样本数。

9.5.9 对象关键点相似度(oks)通过计算真值和预测人体关键点的相似度，测评人体骨骼关键点检测算法，见公式（7）：

$$OKS = \frac{\sum_i \exp(-d_i^2 / 2s^2 \cdot v_i)}{\sum_i v_i}$$

式中；

di ——预测关键点 i 和真实关键点 i 之间的欧氏距离；

s——尺度因子，通常设置为关键点标注的最大边缘长度；

v_i——二值指示函数，如果关键点（i）是可见的，则（vi = 1），否则（vi = 0）；

$\Sigma_i v_i$——所有可见关键点的总数。

9.5.9 单人姿态估计通过以任一单张测试集图片中的人进行关键点检测后获得的一组关键点，计算出人与关键点的相似度作为标量，并人为给定阈值 T，通过所有图片的 oks 计算平均精度（AP），见公式（8）：

$$AP = \frac{\sum \delta(oks > T)}{\sum 1}$$

式中；

AP——平均精度；

oks——对象关键点相似度；

T——指定的阈值。

9.5.10 多人姿态估计即同时检测和估计多个人体的关键点位置和姿势信息，对复杂场景中多人人体 姿态计算平均精度（AP），见公式（9）：

$$AP = \frac{\sum_m \sum_p \delta(oks_{mp} > T)}{\sum_m \sum_p 1}$$

式中；

AP——平均精度；

oks_{mp}——第 m 个图像中的第 p 个人的对象关键点相似度；

T——指定的阈值。

10 人形机器人自然语音交互检测方法

10.1 通用检测条件

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同一进行功能检查，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。

10.2 硬件安全检测方法

10.2.1 物理安全检测方法

物理安全检测方法及结果判定如下：

a）检测方法：

1）检查人形机器人语音控制器的硬件是否具备数据的物理保护机制；

2）通过暴力移除或拆卸硬件，检测人形机器人语音控制器是否具有防护预警机制。

b）预期结果：

1）人形机器人语音控制器的硬件具备数据的物理保护机制；

2）人形机器人语音控制器的硬件宜具备在受到暴力移除或拆卸时的防护预警机制。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.2.2 硬件接口安全检测方法

硬件接口安全检测方法及结果判定如下：

a）检测方法：

1）检查在使用无线和有线外围接口接入设备传输数据时，是否由指示灯或显示屏等方式展示数据传输状态；

2）检查具备调试功能的接口，在出厂时是否设置为关闭。

b）预期结果：

1）人形机器人语音控制器在传输数据给无线或有线外围接口设备时，宜使用指示灯或显示器等方式，提供数据传输状态的监控功能；

2）人形机器人语音控制器具备调试功能的接口，在出厂时设置为默认关闭。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.3 软件安全检测方法

10.3.1 功能安全检测方法

6.3.1.1 唤醒失败率检测方法

唤醒失败率检测方法、预期结果及结果判定如下：

a）检测方法：

按照附录 A 中的环境，选取 10 个唤醒音频，每个音频循环播放 100 次，按照公式（1）计算唤醒失败率：

$$F_{w1}=\frac{1000-Y_1}{1000}\times 100\% \quad (1)$$

式中：

F_{w1}——唤醒失败率，%；

Y_1——统计唤醒成功次数；

1000——测试总次数。

b）预期结果：

根据不同的适用场景，唤醒失败率满足适用场景的要求。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.1.2 二次唤醒失败率检测方法

二次唤醒失败率检测方法、预期结果及结果判定如下：

a）检测方法：

按照附录 A 中的环境，选取 10 个唤醒音频，每个音频循环播放 100 次，按照公式（2）计算唤醒失败率：

$$F_{w2}=\frac{1000-Y_2}{1000}\times 100\% \qquad (2)$$

式中：

F_{w2}——二次唤醒失败率，%；

Y_2——统计唤醒成功次数；

1000——测试总次数。

b）预期结果：

根据不同的适用场景，二次唤醒失败率满足适用场景的要求。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.1.3 命令字识别异常率检测方法

命令字识别异常率检测方法、预期结果及结果判定如下：

a）检测方法：

按照附录 A 中的环境，使用人工嘴播放唤醒命令字和命令词，播放 1000 次唤醒命令字和命令词，按照公式（3）计算命令字识别异常率：

$$F_c = \frac{1000 - Y_3}{1000} \times 100\% \quad (3)$$

式中：

F_c——命令字识别异常率，%；

Y_3——命令字和命令词被正确识别的次数；

1000——测试总次数。

b）预期结果：

根据不同的适用场景，唤醒失败率满足适用场景的要求。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.1.4 误唤醒频次检测方法

误唤醒频次检测方法、预期结果及结果判定如下：

a）检测方法：

1）按照附录 A 中的误唤醒噪声集，噪声播放设备播放误唤醒噪声集，统计误唤醒品尝此次记为X_1；

2）EUT 静置 24h 于附录 A 中规定的安静环境，统计误唤醒频次记为X_2。

b）预期结果：

误唤醒频次不超过规定次数。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.1.5 白噪声攻击稳健性测试

白噪声攻击稳健性检测方法、预期结果及结果判定如下：

a）检测方法：

使用白噪声混合正常功能指令词攻击语音识别系统，检查在受到白噪声攻击后，语音控制器是否可保持功能逻辑正常，安全性是否受到影响。

b）预期结果：

受到白噪声攻击后，人形机器人语音控制器保持功能逻辑正常，安全性不受影响。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.3.2 应用软件安全检测方法

6.3.2.1 应用软件签名安全测试方法

应用软件签名安全检测方法、预期结果及结果判定如下：

a）检测方法：

检查应用软件是否包含供应商和/或开发商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。

b）预期结果：

应用软件包含供应商和/或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。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.2.2 应用软件认证信息安全测试方法

应用软件认证信息安全检测方法、预期结果及结果判定如下：

a）检测方法：

检查应用软件对于认证信息是否提供安全性措施。

b）预期结果：

应用软件对于认证信息提供安全性措施。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.2.3 应用软件认证失败安全测试方法

应用软件认证失败安全检测方法、预期结果及结果判定如下：

a）检测方法：

检查应用软件对于认证失败是否有相应的处理机制，包括但不限于拒绝访问等。

b）预期结果：

应用软件对于认证失败具有相应的处理机制，包括但不限于拒绝访问等。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.3.2.4 应用软件权限控制安全测试方法

应用软件权限控制安全检测方法、预期结果及结果判定如下：

a）检测方法：

检查应用软件在向系统申请权限时是否遵循了最小化原则，是否采用合理的申请方式。

b）预期结果：

应用软件在向系统申请权限时遵循了最小化原则，是否采用合理的申请方式。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.4 信息安全检测方法

10.4.1 语音监听安全测试方法

语音监听安全测试方法、预期结果及结果判定如下：

a）检测方法：

1）检查所有用户的音频数据都得到保护，不会被未经授权的人员访问或使用；

2）检查在用户未授权的情况下，是否保存用户音频；

3）检查监听到的非业务逻辑需要的音频是否舍弃掉。

b）预期结果：

1）所有用户的音频数据都得到保护，不会被未经授权的人员访问或使用；

2）在用户未授权的情况下，不保存用户音频；

3）舍弃掉监听到的非业务逻辑需要的音频。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.4.2 传输安全测试方法

传输安全测试方法、预期结果及结果判定如下：

a）检测方法：

1）检查各执行主体之间进行数据传输时，是否保证数据传输的完整性和机密性；

2）检测到数据完整性遭受破坏时，采取新措施恢复或重新获取数据。

b）预期结果：

1）各执行主体之间进行数据传输时，保证数据传输的完整性和机密性；

2）检测到数据完整性遭受破坏时，采取新措施恢复或重新获取数据。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.4.3 操作系统安全测试方法

6.4.3.1 调试安全测试方法

调试安全测试方法、预期结果及结果判定如下：

a）检测方法：

1）检查用户在进入操作系统前是否先具有用户标识，并且是否保证在操作系统的整个生存周期内用户标识的唯一性；

2）检查在用户执行任何与安全功能的相关操作前，是否对用户进行鉴别；

3）检查是否采用加密方法对鉴别信息的存储进行保护；

4）检查用户进程是否与所有者用户相关联，用户进程的行为是否可追溯到进程的所有者用户。

b）预期结果：

1）用户进入操作系统前先有用户标识，在操作系统的整个生存周期内用户标识的唯一性；

2）在用户执行任何与安全功能的相关操作前对用户进行鉴别；

3）采用加密方法对鉴别信息的存储进行保护；

4）将用户进程与所有者用户相关联，使用户进程的行为可追溯到进程的所有者用户。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.4.3.2 访问控制安全测试方法

访问控制安全测试方法、预期结果及结果判定如下：

a）检测方法：

1）检查对访问存储区域的权限分配是否遵循了最小权限原则；

2）检查是否具有阻止未授权的访问的能力；

3）检查是否针对不同角色的用户，分配了不同的权限。

b）预期结果：

1）对访问存储区域的权限分配遵循了最小权限原则，只能访问所需完成任务所需的资源和信息，不应越权访问其他资源和信息；

2）具有阻止未授权的访问的能力；

3）针对不同角色的用户，分配不同的权限。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

6.4.3.3 升级能力安全测试方法

升级能力安全测试方法、预期结果及结果判定如下：

a）检测方法：

1）检查语音控制器是否支持操作系统的更新升级；

2）检查语音控制器升级时是否采取安全机制；

3）检查语音控制器升级后的系统安全属性是否低于升级前的系统安全属性；

4）检查语音控制器升级失败后，系统是否能够回滚，并是否能保证系统的完整性和安全属性；

5）检查语音控制器是否采用了至少一种安全机制，如自动升级，更新通知等手段保证升级的时效性。

b）预期结果：

1）语音控制器支持操作系统的更新升级；

2）语音控制器升级时至少采取了一种安全机制，保证升级过程的安全性；

3）语音控制器升级后的系统安全属性不低于升级前的系统安全属性；

4）升级失败后，系统应能够回滚，并保证系统的完整性，且安全属性与升级前一致；

5）语音控制器应采用至少一种安全机制。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.5 数据安全检测方法

10.5.1 数据可用性检测方法

数据可用性检测方法、预期结果及结果判定如下：

a）检测方法：

1）检查在传输其采集到的数据时，是否对数据新鲜性做出标识；

2）检查是否能够鉴别数据的新鲜性。

b）预期结果：

1）在传输其采集到的数据时，对数据新鲜性做出标识；

2）能够鉴别数据的新鲜性，避免历史数据的重发攻击。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.5.2 数据完整性检测方法

数据完整性检测方法、预期结果及结果判定如下：

a）检测方法：

检查数据在传输和处理过程中是否保证完整性。

b）预期结果：

数据在传输和处理过程中保证完整性。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.5.3 数据保密性检测方法

数据保密性检测方法、预期结果及结果判定如下：

a）检测方法：

1）检查对数据是否采用密码算法进行存储和传输加密保护；

2）检查重要数据加密算法是否符合 ISO/IEC 18033（所有部分）相关要求。

b）预期结果：

1）对数据采用密码算法进行存储和传输加密保护；

2）重要数据加密算法符合 ISO/IEC 18033（所有部分）相关要求。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.6 隐私安全检测方法

10.6.1 隐私数据收集检测方法

隐私数据收集检测方法、预期结果及结果判定如下：

a）检测方法：

1）检查人形机器人制造商采集隐私数据时是否具有明确、清晰、具体的个人信息处理目的；

2）检查人形机器人制造商采集隐私数据时，是否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；

3）检查人形机器人制造商采集隐私数据时，是否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，是否及时删除个人信息；

4）检查人形机器人制造商对采集的隐私数据是否进行出售、转让；

5）检查人形机器人制造商是否在关闭唤醒状态或语音功能下，采集隐私数据。

b）预期结果：

1）人形机器人制造商采集隐私数据时具有明确、清晰、具体的个人信息处理目的；

2）人形机器人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；

3）人形机器人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，目的达成后及时删除个人信息；

4）人形机器人制造商对采集隐私数据不进行出售、转让；

5）在关闭唤醒状态或语音功能下，不采集隐私数据。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.6.2 隐私数据存储检测方法

隐私数据存储检测方法、预期结果及结果判定如下：

a）检测方法：

1）检查人形机器人制造商是否具备与所面临的安全风险相匹配的安全能力，是否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；

2）检查人形机器人制造商对存储的隐私数据是否具有定时清理机制。

b）预期结果：

1）人形机器人制造商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；

2）人形机器人制造商对存储的隐私数据具有定时清理机制。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

10.6.3 隐私数据使用检测方法

隐私数据使用检测方法、预期结果及结果判定如下：

a）检测方法：

1）检查人形机器人制造商是否以明确、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；

2）检查人形机器人制造商是否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；

3）检查人形机器人制造商隐私数据是否仅限于用于改善产品及用户体验。

b）预期结果：

1）人形机器人制造商以明确、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；

2）人形机器人制造商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；

3）人形机器人制造商隐私数据仅限于用于改善产品及用户体验，不用于获取商业利益。

c）结果判定：

若满足全部预期结果，则该项目测评通过。

《人形机器人人机交互与安全技术规范》

编制说明

一 工作简况

（一） 任务来源

工信部在《人形机器人创新发展指导意见》中提出，到2025年，人形机器人创新体系初步建立，“大脑、小脑、肢体”等一批关键技术取得突破，确保核心部组件安全有效供给。到2027年，人形机器人技术创新能力显著提升，形成安全可靠的产业链供应链体系，构建具有国际竞争力的产业生态，综合实力达到世界先进水平。

1. 人形机器人人机交互与安全技术规范标准

• 行业需求：随着人形机器人市场的不断扩大，行业内对于人机交互技术规范的需求日益迫切。为了保障机器人的性能和用户体验，需要制定统一的技术规范标准。

• 技术创新：随着语音识别、自然语言处理、计算机视觉等技术的不断创新，人形机器人的交互能力得到了显著提升。这些新技术的应用也推动了人机交互技术规范标准的制定和完善。

• 政策引导：政府及相关机构对于人形机器人产业的发展给予了高度关注，并出台了一系列政策措施来引导和规范产业的发展。这些政策也为人机交互技术规范标准的制定提供了有力支持。

2. 人形机器人安全技术规范标准重要性

• 保障人员安全：人形机器人与人类共存于同一环境中，因此必须确保其安全性，以避免对人员造成伤害。安全技术规范标准的制定和实施可以有效降低机器人运行过程中的安全风险。

• 提升机器人可靠性：通过制定安全技术规范标准，可以对机器人的设计、制造、使用等环节进行规范，从而提升机器人的可靠性和稳定性。

• 推动产业发展：安全技术规范标准的制定和实施有助于提升整个行业的安全水平，增强消费者的信任度和购买意愿，从而推动人形机器人产业的健康发展。

•国际合作与交流加强：随着人形机器人产业的全球化发展，国际合作与交流将越来越频繁。各国将共同制定和完善人机交互与安全技术规范标准，以推动全球人形机器人产业的协同发展。

（二） 国内关于人形机器人人机交互与安全技术规范的制定情况及最新要求

随着人形机器人技术的快速发展和广泛应用，制定相关的人机交互与安全技术规范标准变得尤为重要。这些标准不仅有助于规范人形机器人的研发、生产和销售等环节，还能

保障用户的安全和隐私权益，推动人形机器人行业的健康发展。

已发布的标准

1、《人形机器人分类分级应用指南》：

该标准定义了人形机器人通用、结构、智能相关的术语名词，并从结构外观、移动方式、智能模型等方面进行分类指导。

按照具身智能、下肢运动、上肢作业、应用环境等作为分级要素，将人形机器人划分为 L1-L4 四个技术等级。

适用于人形机器人的研究、开发、生产、评估和应用推广。

2、《具身智能智能化发展阶段分级指南》：

该标准规定了具身智能技术领域的智能化等级划分依据。

采用系统功能性、自主性、泛化性的分级原则，按照感知、认知、决策、自主等核心能力作为分级要素，将智能化等级从基础到高级智能化水平划分为 G1-G5 五个阶段。

但在人形机器人力觉与触觉交互系统技术要求，人形机器人自然视觉交互系统技术要求，人形机器人自然语音交互技术要求，人形机器人自然视觉交互检测方法等领域还没有相关标准，在此背景下，哈工大机器人技术与系统全国重点实验室结合自身在人形机器人交互安全方面所积累的丰富经验，作为主编单位承担了《人形机器人人机交互与安全技术规范》的标准编制工作。

（三） 标准编制的目的、意义

人形机器人人机交互与安全技术规范标准的编制目的和意义在于：

编制目的：

1. 确保安全：首要目的是确保人形机器人在与人类交互的过程中不会对人类造成伤害，同时保障机器人自身的安全。通过制定明确的安全规范，可以降低事故发生的概率，保护用户和设备的安全。

2. 提升交互体验：优化人机交互方式，使机器人能够更好地理解用户的意图和需求，提供更精准、更人性化的服务。这有助于提升用户对机器人的满意度和信任度。

3. 推动技术创新：通过制定技术规范，为人形机器人的研发提供明确的指导和方向。这有助于推动技术创新和产业升级，促进人形机器人技术的快速发展。

4. 规范市场秩序：建立统一的技术规范标准，有助于规范市场秩序，防止恶意竞争和不合格产品的出现。这有助于保护消费者的权益，维护市场的公平竞争环境。

编制意义

1. 保障用户权益：规范标准的制定和实施，可以保障用户在使用人形机器人过程中的权益和安全。这有助于提升用户对机器人的信任度和满意度，推动人形机器人市场的健康发展。

2. 促进产业升级：通过制定技术规范标准，可以推动人形机器人产业的升级和转型。这有助于提升整个行业的竞争力，促进产业的可持续发展。

3. 引领国际潮流：中国在人形机器人人机交互与安全技术规范标准的制定方面取得领先地位，有助于引领国际潮流，推动全球人形机器人技术的快速发展。这有助于提升中国在国际舞台上的影响力和话语权。

4. 推动社会进步：人形机器人作为新兴技术，具有广泛的应用前景和巨大的社会价值。通过制定技术规范标准，可以推动人形机器人在医疗、教育、娱乐等领域的广泛应用，为社会进步和发展做出积极贡献。

（四） 标准特点

1.本标准在 GB/T 5226.1-2019 机械电气安全 机械电气设备 第 1 部分:通用技术条件

GB/T 36530-2018 机器人与机器人装备 个人助理机器人的安全要求

GB/T 36008-2018 机器人与机器人装备协作机器人

GB 11291.1-2011 工业环境用机器人 安全要求 第 1 部分：机器人

GB 11291.2-2013 机器人与机器人装备 工业机器人的安全要求 第 2 部分：机器人系统与集成

GB/T 38244-2019 机器人安全总则

GB/T 41393—2022 娱乐机器人 安全要求及测试方法

GB/T 38260-2019 服务机器人功能安全评估

GB/T 39785—2021 服务机器人 机械安全评估与测试方法

GB/T 18029.13-2008 轮椅车 第 13 部分：测试表面摩擦系数的测定

GB/T 16855.1-2018 机械安全 安全控制系统 第 1 部分：设计通则

GB 28526-2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

ISO/IEC 18033（所有部分） 信息技术 安全技术 加密算法（Information technology—Security techniques—Encryption algorithms）

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 43969-2024 智能语音控制器通用安全技术要求

GB/T 31488-2015 安全防范视频监控人脸识别系统技术要求

GB/T38671-2020 信息安全技术远程人脸识别系统技术要求

GB/T 38244 机器人安全总则等国家标准指导下进行人形机器人人机交互与安全技术规范编制。并规定人形机器人力觉与触觉交互系统技术要求，人形机器人自然视觉交互系统技术要求，人形机器人自然语音交互技术要求，人形机器人自然视觉交互检测方法等模块的基本要求。

（四）主要工作过程

1. 编制准备阶段

二 标准编制 2024 年 5 月-6 月。主编单位接到编制任务后，组织专业技术人员成立编制组，开展大量的资料收集和前期调研工作，编写完成标准大纲、标准初稿等。

2. 征求意见阶段

2024 年 10 月出完成标准草案的完善，并小范围内部征求意见，根据反馈意见修改形成征求意见稿，全面公开征求意见。

3. 送审阶段

2024 年 12 月将进行专家审查，并根据专家审查意见修改了送审稿，最终形成报批稿。

4. 报批阶段

未进行

二 标准编制原则

（一）科学性原则：本标准编制是在科学理论和实践经验基础上，确保技术要求和规范具有科学性和可行性，能够有效指导实际施工过程。

（二）统一性原则：本标准编制统一了各方的要求和标准，确保项目参建单位在制定说明书时过程中能够按照该标准进行操作，参照统一标准，减少歧义。

（三）公正性原则：本标准编制过程公正、公平、透明，确保标准的制定过程中各方利益的平衡，不偏袒任何一方，保证标准的客观性和公信力。

（四）可操作性原则：本标准编制时充分考虑了实际操作性，确保项目参建单位能够对照标准的要求进行人形机器人人机交互与安全技术规范搭建，避免标准过于理论化或难以实施的情况。

（五）合规性原则：本标准编制符合国家法律法规和相关行业的规范和标准，确保标准的合法性和合规性，遵循国家政策和法律要求。

三 标准主要内容

1. 内容：本标准界定了人形机器人力觉与触觉交互系统技术要求，人形机器人自然视觉交互系统技术要求，人形机器人自然语音交互技术要求，人形机器人自然视觉交互检测方法等模块的基本定义、概念、各重要模块的功能、性能参数及可靠性等。

2. 范围：本文件适用于人形机器人研发设计单位、生产制造企业、科研院所、行业协会以及第三方服务商进行人形机器人系统开发、应用。

3. 规范性引用文件：本标准编制时引用的标准规范等文件；

4. 术语与定义：对本标准中所涉及的名词术语进行定义；

5. 缩略语：对本标准中的缩略语进行解释；

四 预期经济效果

人形机器人人机交互与安全技术规范标准的实施，预期将带来显著的经济效果。首先，它将促进人形机器人人机交互与安全技术标准化和产业化，降低研发和生产成本，提高产品的市场竞争力。其次，规范的实施有助于提升产品质量和生产效率，降低企业的技术更新成本。同时，规范的制定和推广将推动技术创新，促进新产品和服务的开发，开拓新的市场机会。长远来看，这将有助于提升整个人形机器人的智能化水平，增强中国制造业在全球市场的竞争力，为经济增长注入新动力。

五 采用国际标准和国外先进标准情况

在编制人形机器人人机交互与安全技术规范标准过程中，我们充分借鉴了国际标准和国外先进标准，结合国内实际情况进行了深入研究与修订。通过与国际接轨，确保我国人形机器人人机交互与安全技术规范标准达到国内先进水平，为产业发展提供有力支撑。

六 与有关的现行法律、法规和强制性国家标准的关系

在编制人形机器人人机交互与安全技术规范标准过程中，我们严格遵循了相关的现行法律、法规和强制性国家标准，确保标准的合规性和权威性。同时，我们也充分考虑了人形机器人人机交互与安全技术规范标准的发展趋势和应用需求。

七 重大分歧意见的处理经过和依据

本标准在起草过程中未出现重大分歧意见。

八 标准性质的说明

建议本标准为推荐性标准。

九 贯彻标准的要求和措施建议

本标准经征求各相关方意见，已形成共识，标准实施之日起，各相关方将遵照执行。

十 废止现行有关标准的建议

无。

十一 主要起草单位和联系方式

本标准主编单位：哈工大机器人技术与系统全国重点实验室

本标准参编单位：XXXXX，XXXXX

本标准主要起草人：XXX、XXX、