ICS 97.120
CCS L66

团　　体　　标　　准

T/CI 1070—2025

应用于生活支援场景的服务机器人安全设计规范

Safe operation of service robots applied in life support scenarios

2025-06-30 发布　　2025-06-30 实施

中国国际科技促进会　发 布

湖北科学技术出版社　出 版

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。

本文件由重庆大学提出。

本文件由中国国际科技促进会归口。

本文件起草单位：重庆大学、重庆工商大学、山东理工大学、四川文理学院、中兴通讯股份有限公司、安徽理工大学、天台智能制造研究院。

本文件主要起草人：苏晓杰、敖文刚、孙艺倬、李钊、刘彪、孙少欣、王硕玉、杨旭、朋子涵、张骏、戴前进。

本文件为首次发布。

应用于生活支援场景的服务机器人安全设计规范

1 范围

本文件规定了应用于生活支援场景的服务机器人安全相关设计内容、总体要求，并给出机械、电气、控制、交互、定位、隐私等基础要求和安全技术指标。

本文件适用于生活场景下（如家庭、养老院、康复中心等室内场景）应用的机器人安全体系框架、机器人安全技术模型、安全交互等相关安全设计。

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 5226.1 机械电气安全 机械电气设备 第1部分:通用技术条件

GB/T 11291.1 工业环境用机器人 安全要求 第1部分：机器人

GB/T 12643 机器人与机器人装备 词汇

GB/T 15843.1 信息技术 安全技术 实体鉴别 第1部分：总则

GB 16754 机械安全 急停功能 设计原则

GB/T 21023 中文语音识别系统通用技术规范

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 44581 商用自主地板处理机 特殊要求

SJ/T 11380 自动声纹识别（说话人识别）技术规范

ISO 12100：2010 机械安全性 设计通用原则 风险评估和风险降低

3 术语和定义

下列术语和定义适用于本文件。

3.1

额定自主移动速度 rated autonomous movement speed

在开放空间内，机器人在自主导航模式下运行时的最大速度。

[来源：GB/T 44581,有修改]

3.2 机器人本体和操作 robot body and operation

3.2.1

机器人移动平台 mobile platform

能使移动机器人实现运动的全部部件的组装件。

注：移动平台包含一个用于支承负载的机架或底盘。

［来源：GB/T 15843.1,3.11］

3.2.2

正常工作状态 normal operating status

机器人在生活场景下正常运行的状态。

3.2.3

自主导航模式 automatic navigation mode

机器人控制系统按照轨迹规划任务程序自主行走的一种工作方式。控制模式转换应优先在停车状态下完成，并设置安全确认，防止误操作导致意外运行。

3.2.4

手动模式 manual mode

由人工通过控制装置（如操作杆、遥控设备或接口）直接操纵机器人运动和操作的模式。

3.3 减速距离传感器 deceleration distance sensor

3.3.1

激光雷达 lidar

通过主动发射并接收反射回来的激光，实时测量目标的位置、距离，形成点云图像，可用于环境感知的传感器。

3.3.2

主动结构光视觉 structured light vision

将结构化（点结构、线结构、面结构或光学编码）的光线投射到物体表面，获取视觉图像后，通过计算图像中结构光的变形（或飞行时间等）来确定被测物体的三维尺寸和位置信息，可用于环境感知的传感器。

3.3.3

单目视觉 monocular vision

仅利用单个摄像头进行视觉信息采集的技术。由于单目采集深度信息不够精确，通常需结合深度测量传感器或基于运动视差计算三维信息。

3.3.4

双目视觉 binocular vision

基于视差原理，利用两个安装在不同位置的成像设备，同时获取被测物体的两幅图像，通过计算图像对应特征点之间的位置偏差，来获取物体和环境空间的三维几何信息的技术。

3.3.5

里程计 odometer

用于测量载体运动的速度、姿态和位置信息。

3.3.6

主传感器 main sensor

在多传感器融合系统中，发挥最主要作用的传感器。

3.4 **机器人视觉、语音、隐私信息** robot vision, speech, and privacy information

3.4.1

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,定义 3.1]

3.4.2

语音唤醒 speech wake up :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。

3.4.3

声纹模型 voiceprint model

对声纹特征进行描述的数学模型.

[来源：SJ/T 11380.定义 3.1.3]

3.4.4

人脸图像 face image

以图像存储或传输的人脸数据形式，包括可见光、红外或 3D 采集的自然人脸信息。

注：人脸图像可从设备收集或通过视频、数字照片等获取，主要类型包括可见光图像、非可见光图像（如红外图像）三维图像等。

3.4.5

人脸特征 face feature

从人脸图像提取的反映自然人脸部信息特征的参数。

3.4.6

人脸识别数据 face recognition data

可识别自然人身份的人脸图像或人脸特征。

3.4.7

人脸识别数据主体 face recognition data subiect

人脸识别数据所标识或关联的自然人。

注：人脸识别数据主体简称数据主体。

3.4.8

信息安全 information security

保护信息的保密性、有限性和可用性，确保其真实性、可核查性、抗抵授权性和可靠性，以防止篡改。

[来源：GB/T 25069，,定义 2.1.52]

3.4.9

非法 illegality

使信息系统安全的某一部分被避开或失去作用的行为,可能产生对信息系统的侵入。

注：也称“违规”。

3.4.10

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信联系方式、通信记录和内界账号密码、财产信息、征信信息、行踪轨迹,住宿信息,健康生理信息、交易信息等。

[来源：GB/T 35273.定义 3.11]

3.5 **机器人定位、导航及避障** robot localization, navigation and obstacle avoidance

3.5.1

SLAM **技术** SLAM technology

根据自身与环境特征的位置关系，通过概率算法，实现自身定位，同时建造出增量式环境地图的技术。

3.5.2

位姿 pose

空间位置和姿态的合称，对于在平面场地工作的机器人，位姿可以简化为由二维平面坐标和机器人航向角构成的三维向量。

注：改写 GB/T 12643，定义 4.5。

3.5.3

轨迹规划 trajectory planning

根据具体任务,解算并生成机器人位姿的时间序列，形成相应的行进路径。

3.5.4

定位 localization

在环境地图上识别或分辨机器人的位姿。

3.5.5

导航 navigation

根据轨迹规划，控制机器人从起始位姿通过特定路径达到目标位姿。

注：改写 GB/T 12643，定义 7.6。

3.5.6

避障 obstacle avoidance

机器人在行进过程中，根据实时环境感知信息，调整轨迹或采取规避措施以避让障碍物，并在避障后恢复到预期轨迹或重新规划路径。

3.5.7

重定位 relocalization

机器人的当前位姿丢失以后，重新获取新的位姿的过程。

4 机械安全要求

4.1 结构安全要求

4.1.1 一般要求

生活支援机器人本体结构应满足以下要求：

a) 生活支援机器人本体应保证在正常运行时产生的扭曲变形量≤0.5 mm/m，抗弯刚度≥200 N·m²，确保不会引发功能故障和安全风险。

b) 本体覆盖件的曲率半径应≥3 mm，抗冲击强度≥5 J，防止碰撞时产生锐边或结构失效。

4.1.2 驱动轮与从动轮

生活支援机器人的驱动轮与从动轮应满足以下安全要求：

a) 驱动轮牵引力系数≥0.4，从动轮承载力≥150 kg，动态侧倾角≤5°，确保各类负载下稳定运行；

b) 随车轮运动的线束防护等级不低于 IP54，弯曲半径≥5 倍线径，耐磨系数≥0.8，抗拉断力≥200 N。

4.1.3 电池仓及盖板

生活支援机器人的电池仓及盖板应满足以下安全要求：

a) 电池或电池组应通过隔间或单独的外壳提供支撑和保护，并具备有效的散热设计，避免过热；

b) 电池或电池组应提供限位装置，确保在移动机器人启动、停止和正常行驶时，电池或电池组在任何方向上的移动量不超过 15 mm；

c) 用于制作电池或电池组隔间的外壳材料应能阻燃，并具备适当的强度；

d) 电池仓盖板与电池裸露金属接头之间一般留有不小于 30 mm 的空间。如能够确保盖板与接头之间具有足够的绝缘性能，可以减少到 10 mm；

e) 电池仓内表面的材质应能抵抗电解液的化学影响，应采取措施防止电解液排放到地面。

4.2 执行机构安全要求

执行机构应配备紧急停止开关，且该开关应易于访问，用于切断各执行机构的电源，能够在不超过 0.5 s 的时间内切断电源，确保机器人能够迅速停止。该紧急停止开关可并入底盘急停装置中或作为单独的急停装置提供使用。

a）机器人底盘运行机构

1) 底盘额定自主移动速度不超过 1.5 m/s；

2) 底盘执行电机必须采用伺服电机实现闭环控制，且额定电压不超过 24 V，最大电压不超过 36 V；

3) 底盘正常停止运行时减速距离不超过 0.5 m，紧急情况停止运行时减速距离不超过 0.1 m；

4) 底盘具备自检功能，当传感器失效或机器人底盘运动状态与期望状态不同时进行警报提醒，等待人工处理。

b）机器人机械臂

1) 机械臂应满足 GB 11291.1 的相关要求；

2) 机械臂应采用协作机械臂，防止在工作期间对人体造成伤害；

3) 机械臂具备过载保护，在超负荷工作时自动停止或减速运行，防止损坏设备；

c）机械臂末端执行器

末端执行器安全力矩应≤5 N·m，动态力控阈值≤40 N，静态力控阈值≤20 N，防止意外伤害人体或夹碎易损物品。

4.3 外壳保护能力

生活支援机器人各功能部件外壳的防护等级应达到IP65，能够有效防尘，并能承受来自水流的侵入，确保机器人在恶劣环境下正常工作。

5 电气安全要求

5.1 接地

生活支援机器人保护联接电路，应满足GB 5226.1中8.2.3的要求。生活支援机器人上宜采用导电链，导电橡胶及导电轮等方式进行接地保护。

5.2 电压等级

机器人各单元的峰值电压不得超过36 V，且应具备有效的过电压保护设计，避免电压超标导致的电气故障。

5.3 绝缘

5.3.1 除蓄电池外的所有带电部件与机器人本体之间的绝缘电阻,应大于等于1000 Ω乘以系统标称电压，蓄电池与机器人本体之间的绝缘电阻应大于等于50 Ω乘以系统标称电压。

5.3.2 绝缘材料具有良好的耐湿性能，可达到IP65等级。

5.3.3 绝缘材料能耐受常见化学物质（如清洁精和消毒液）的腐蚀，保证长期使用中的安全性。

5.4 保护电路

机器人设计需要考虑全身电路的保护，包括充放电过程，对设备分流分压的安全保护。

a）电源管理具备过压、过流、过温保护，防止因为瞬间电压导致对人体的危害和设备的损坏。

1) 输入电压≥36 V时触发硬切断（响应时间≤1 ms），锁定后需人工复位；

2) 持续电流＞12 A（额定10 A）或瞬态峰值＞25 A/100 μs时切断电路(响应≤5 ms)；

3) 电源模块表面温度≥70 ℃时强制断电，温度回落至≤50 ℃后允许自动恢复。

b）电池管理系统应将电池保持在其正常工作电压阈值范围内进行充电或放电，如果超过正常限值，应限制或关闭充电或放电；电池管理系统应确保电池在充放电过程中始终处于正常工作电压范围内，并配备过压、过流、过温保护措施。

5.5 传感器与控制器

机器人的传感器和控制器需要可以独立运行并安全可靠，同时具有意外形况的保护。

a）用于障碍物检测的接触式或非接触式传感器应确保实际工况下的可靠性；

b）控制器应具有独立的运行安全监控设计，当控制失效时，应确保生活支援机器人处于停止状态，当监测到传感器失效时应及时提醒并保证处于停止状态，直至有效。

5.6 低电量保护

以电池为主要动力的移动机器人，宜具备电池低电量保护功能，防止过放损坏电池。且具备电量分级预警功能（如20%低电量预警、10%强制停机），并具备电池健康状态监测，用户可实时看到电池健康状态，避免长期使用导致的性能衰减。

6 机器人控制安全

6.1 控制模式安全要求

控制模式可分为自动模式、手动模式、半自动模式，模式切换应满足GB/T 5226.1中9.2.3的要求，应防止为未经授权和意外触及导致的模式切换，控制模式转换应优先在停车状态下完成，并设置安全确认，防止误操作导致意外运行。且具备权限分级管理机制，例如通过生物识别或多因素认证确保操作者身份合法性，并记录所有模式切换操作日志以追溯责任。手动模式应具有最高优先级。

a） 自动模式：系统基于预设程序或智能算法独立完成作业任务，无须人工持续干预；

b） 手动模式：操作者通过人机界面（HMI）或物理控制装置直接操控设备动作；

c） 半自动模式：人机协同作业模式，系统执行基础动作序列，操作者进行关键决策。

6.2 失速保护

移动机器人的运行速度超出自身限定的可控范围，即为失速状态。处于失速状态的移动机器人应能及时自动安全停止运行，并发出警报信息，等待人工介入处理。且测量速度监控的规划参考ISO 10218-1，确保不同厂商设备的一致性和可比性。

6.3 通讯中断保护

当移动机器人与通信网络系统中断通信超过一定时间（可由制造商自行定义，一般不超过10 s）时，移动机器人应能自动安全停止运行，发出警报信息，等待人工介入处理。当移动机器人与无线遥控手动装置通讯终端时，应具备自动停车功能。

6.4 导航丢失保护

导航丢失保护是指移动机器人在自动运行状态下，车体位置及姿态超出理论规划的最大位置偏差值（小于10 cm），或无法检测到地标时的保护措施，最大位置偏差值由制造商根据实际工况确定。

当移动机器人在运行过程中出现导航丢失时，移动机器人应当立即停止运行，发出报警信息，等待人工介入处理。

6.5 超时保护

当机器人某个动作或安全检测超出预设时间（可由制造商自行定义），可能会导致安全风险时，应设置超时保护。

当超时保护被激活时，移动机器人应当立即停止运行，发出报警信息，等待人工介入处理。

6.6 稳定性

机器人稳定性是安全运行过程中的必须条件，是确保机器人在运行过程中能够保持平衡、避免倾覆、应对避障或失控的关键性能指标。

a）一般要求

移动机器人应在所有操作位置以及所有装卸和行驶过程中保持稳定。同时，机器人全身应具备碰撞检测功能，具备成多模态传感器（如激光雷达、视觉摄像头）实现实时环境感知，关于碰撞中的力/力矩受限范围可参考 ISO/TS 15066，确保碰撞时的动态响应。

b）行驶稳定性

1) 加速：最大加速度应与正常运行期间的负载稳定性要求相匹配；
2) 减速：对于正常减速运行，包括安全停车时，减速度应满足负载稳定性要求；紧急停车时，最大减速度应考虑负载稳定性要求；
3) 转向时应满足移动机器人及负载的稳定性要求。同时，应具备结合生活空间环境信息的能力。

c）载货平台的稳定性

1) 载货平台（包含双臂的抓取）应确保移动机器人在任何运行状态（包括停和负载转移）下，负载均保持在制造商设计的范围内，不能产生因负载移动而导致的任何风险；
2) 当载货平台移动时，应确保负载不会发生跌落、倾覆、挤压等风险。

7 定位、导航、避障安全要求

7.1 一般要求

服务机器人在生活场景下使用时应满足以下安全设计：

a）在所有操作模式以及所有停止和行驶过程中，确保定位精度达到标准要求，且当定位精度超出设定范围时，应自动进入安全停机模式，并发出报警信号；

b）制造商应在系统运行前对使用方人员进行可验证的培训，且培训内容应涵盖系统的操作、故障排查、紧急停机和安全措施等，培训效果应进行评估并记录；

c）制造商应亲自在实际使用场景下进行地图构建，并评估危险区域和限制区域，标记并设置虚拟围栏或物理障碍物进行禁止通行。系统应具备实时监控功能，能自动检测并警告用户进入危险区域；

d）设计合理的体积大小，确保机器人能在实际使用场景下正常导航；

e）机器人应搭载多种传感器，并确保其感知范围不低于 360°，在实际使用场景下没有感知盲区，并具备动态调整感知范围的能力，以适应不同环境。

7.2 定位性能

该性能为机器人在手动模式或自主导航模式下，沿路径到达指定目标点的能力。

在室内生活场景下测试，机器人在手动模式或自主导航模式下，到达目标点的位置准确度应≤0.1 m，姿态准确度应≤0.05 弧度，并且必须提供超出精度范围时的报警机制，以确保安全使用。

7.3 重定位性能

该性能为机器人开机启动以及在某些场景中丢失位姿信息后，重新确定位姿的能力，包括重定位成功率、重定位时间、重定位准确度。

在室内生活场景下测试，重定位成功率应≥90%，重定位时间应≤10 s，重定位准确度应≤0.1 m，姿态准确度应≤0.05 弧度，并要求在重定位过程中保证不低于上述要求的实时监控功能。

7.4 导航性能

该性能为机器人在工作环境下的轨迹规划能力和运动控制能力。

在室内生活场景下测试，机器人在自主导航模式运行情况下，车体位置及姿态偏差值应严格限制在≤0.1 m（位置）和≤0.05 弧度（姿态），超过此范围时，应自动进行安全停机并报警。

当机器人在导航过程中出现导航丢失时，机器人应当立即停止运行，发出报警信息，等待人工介入处理。

7.5 避障性能

该性能为机器人在工作环境下对静态和动态障碍物识别和避让的能力。

在室内生活场景下测试，机器人避障率应达到 100%，在自主导航模式运行时，障碍物和移动机器人（包括负载）之间应保持 0.5 m 的最小间隙，小于此间隙时，机器人应立即停止并发出报警信号，确保及时反馈用户操作。

8 交互安全

8.1 紧急停止

机器人配备紧急停止按钮，以便在机器人与人或环境交互过程中发生紧急情况下立即停止所有运动。

a）急停装置应符合 GB/T 16754 第 4.1.3 条定义的 0 类或 1 类停止功能要求，且其安全控制系统性能等级至少满足第 4.1.5.1 条的 PL=c 或 SIL1；

b）紧急停止按钮应位于机器人的易访问位置，按钮特征特殊且突出，防止混淆且易于按下；

c）按下紧急停止按钮后，机器人应在 500 ms 内停止所有动作，且停止时间应通过功能安全验证；并且一旦按下，需要经过复位或重新启动程序才能继续机器人操作；

d）急停按钮应安装在操作人员易于快速触达的位置，同时确保机械臂运动轨迹不会因误触导致急停失效；

e）禁止为紧停按钮触发的紧急停止信号设计屏蔽回路；

f）远程无线控制急停功能需具备独立于主控系统的失效保护机制，当无线信号中断或干扰时，机

器人应自动进入停止状态。

8.2 通信稳定

机器人的通信稳定性是确保其正常运行和安全操作的关键因素。机器人应确保本机通信和无线通信的稳定性，以避免由于通信故障导致的意外事件发生。

a）机器人应采用稳定可靠的通信协议，确保机器人与遥控设备或其他设备之间的通信畅通无阻。

b）机器人的运算需要满足实时性要求，即运算时滞应 ≤100 ms，并需在通信协议中设计容错机制，确保时滞超限时触发安全保护动作。在通信过程中，机器人需要及时响应控制指令，快速执行相应动作，以确保操作的及时性和灵活性。

c）与云端通信时，机器人应支持主备双通道冗余（如光纤+4G/5G 异构网络），主通道中断后 3 秒内完成切换，边缘端缓存关键指令并实施分级冗余策略，优先保障控制指令传输。

8.3 安全感知

机器人应具有一定环境感知能力，能够识别和避免与人和家居环境发生碰撞。

a）机器人应至少配备激光雷达、视觉摄像头、超声波传感器三类传感器，并满足以下性能：检测距离≥5 m，检测精度≤±10 mm，响应时间≤200 ms。这些传感器可以实时获取周围环境的信息，识别障碍物的位置和距离，以便机器人及时做出反应。

b）在机械臂或移动底盘关键接触点部署六维力传感器，实时监测接触力与力矩。例如碰撞检测：通过力阈值判断意外接触（如人体碰撞），触发紧急停机（响应时间≤50 ms）。触觉反馈：结合柔性材料（如硅胶缓冲层），动态调整接触力以减轻冲击（如网页 4 提到的缓冲设计）。异常载荷识别：检测机器人运动中的异常阻力（如卡死、过载），联动报警系统。

c）机器人应具备人体检测功能，可以识别人体的存在并做出反应。当任务执行过程中，检测到人体进入 1.5m 范围内时，机器人应立即将移动速度降至≤0.3 m/s，并在 0.5 s 内完成避障路径规划，关注和预测人的状态，以确保人员的安全。

d）机器人的外部设计应考虑发生碰撞时的安全性。安全机构可采用柔软材料或防撞设计，以减轻碰撞对人体和环境的伤害，确保在发生碰撞时人员和家居环境不会受到重大损害。

e）在机器人无法避免碰撞或产生异常情况时，报警机制需满足：声报警≥80 dB（距 1 m 处），光报警频闪≥2 Hz，且报警触发后机器人应自动进入锁定状态，需人工解除后方可恢复运行，提醒周围人员并引起注意，以减少意外事件发生的可能性。

8.4 安全操作

机器人操作过程中，应确保机器人手臂或夹爪的运动速度和力度适中，以避免造成意外损伤。

a）机器人应具备动态力反馈系统可以实时监测机器人手臂或夹爪与周围环境的接触力，并根据反馈信息对力度进行调整。

b）机器人应引入力控制技术可以实现机器人手臂或夹爪的力度控制，使其在操作过程中可以根据外部力感知动态调整自身的力度以适应操作场景。

c）机器人应智能地响应交互力的变化，及时做出合适的反应，保障操作过程中的安全性。

d）机器人应引入柔顺控制算法，实现根据目标位置和环境情况对机器人运动轨迹进行优化，避免

突然性的加速和减速，确保操作过程中的稳定性和安全性。

e）在机器人设计阶段应预设安全速度和力度的上限值，限制机器人手臂或夹爪的最大运动速度和力度。一旦超过设定的限制，机器人会自动停止或减速。

9 视觉、语音、隐私信息安全规范

9.1 一般要求

服务机器人在生活场景下使用时应满足以下安全规范：

a）使用人脸信息，语音信息身份验证来确保只有授权用户可以访问，防止数据泄露和未授权访问；

b）对于交互过程中的用户隐私信息保护。

9.2 人脸识别安全防御技术

该性能完成机器人在用户尝试访问时进行人脸识别，保证仅合法用户有权限访问和操作机器人系统。

活体检测应支持多模态动态验证（如随机组合眨眼、唇动、头部转动），并集成 3D 结构光或红外检测技术，防御高精度面具或深度伪造攻击，确保图片、视频等无法通过验证，确保活体检测的效果，从而保障验证安全。

9.3 语音识别安全防御

该性能完成机器人在用户尝试访问时进行语音识别，保证仅合法用户有权限访问和操作机器人系统。

a）语音模仿

提高语音识别算法提取特征的细粒度，声纹识别系统需符合 FAR≤0.01%（错误接受率）和 FR≤5%（错误拒绝率）的阈值要求，并支持多因素认证（如声纹+动态口令或设备指纹）；

b）录音重放

活体检测通过检测录音设备及回放设备的信道模式噪声，从而有效检测出唤醒语音是否为录音重放，确保是合法用户。

9.4 隐私安全

对用户隐私的保护是机器人设计、开发和应用中不可忽视的重要环节。隐私安全的主要是对有效信息的保护。

a）一般要求

1) 信息传输加密机制需使用 TLS 1.2 及以上协议或国密 SM2/SM4 算法，且密钥长度≥256 位，并符合 GB/T 35273 的要求；

2) 机器人的数据信息不应被非授权(非法)访问、篡改或删除；

3) 机器人应阻止非授权(非法)信息的人侵,包括对此类信息的识别、判断、阻止与提示功能；

4) 机器人需在检测到非授权操作后 5 s 内启动以下动作：①阻断当前操作链路；②自动生成安全日志并上传至独立审计服务器；③通过 API 接口触发安全平台实时告警，同步通知用户和管理员；

5) 机器人应具有信息溯源机制。

b）保密

1) 组成：机器人应设置保密模块,包括硬件和软件,以实现密钥管理、密码算法及信息管理；
2) 数据加解密：机器人在与外界进行信息交换时,应具备数据加解密功能；机器人作为信息交换发送方时,应对明文数据报文进行加密处理形成密文；机器人作为信息交换接收方时,应对密文进行解密处理形成明文数据报文机器人的数据信息不应被非授权(非法)访问、篡改或删除；
3) 密钥管理：机器人应具备密钥管理功能。密钥管理包括密钥生成、储存、更换、分发；
4) 非授权(非法)操作处理：当机器人操作者采取一些方法(包括恶意代码、网络攻击等),超出自身的权限访问/修改/删除等本无权访问/修改/删除等的资源时,机器人应提示非授权(非法)操作,并通知信息控制者存在非授权(非法)操作或者报警,并阻止操作。通知方式包括但不限于短信、电子邮件等；
5) 信息可溯源：机器人在信息处理过程中,应记录信息处理日志(包括 log 文件等)，包括：授权的操作指令记录、非授权的操作指令记录、恶意代码执行记录、网络攻击记录。

T/CI1070—2025

团 体 标 准

应用于生活支援场景的服务机器人安全设计规范

T/CI 1070—2025

*

湖北科学技术出版社出版发行

武汉市雄楚大街268号湖北出版文化城B座

13—14座 (430070)

总编室:（027）87679429

湖北新华印务有限公司印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 1 字数 9 千字

2025年6月第一版 2025年6月第一次印刷

书号: 155706 · 132 定价：53元