



中华人民共和国国家标准

GB/T 38244—2019

机器人安全总则

General principles of robot safety

2019-10-18 发布

2020-05-01 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 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总则 3

 4.1 概述 3

 4.2 基本原则 3

 4.3 设计原则 4

 4.4 风险评估和风险减小 4

5 机械安全 6

 5.1 几何因素 6

 5.2 物理特性 6

 5.3 人类功效学 6

 5.4 防护装置和保护装置 6

 5.5 补充保护措施 6

6 电气安全 7

 6.1 与电击有关的安全 7

 6.2 与能量有关的安全 7

 6.3 与着火有关的安全 7

 6.4 与热有关的安全 8

7 控制系统安全 8

 7.1 通则 8

 7.2 控制电路和控制功能 8

 7.3 急停功能 8

 7.4 保护性停止 9

 7.5 速度控制 9

 7.6 力控制 9

8 信息安全 9

 8.1 基础原则 9

 8.2 身份识别 9

 8.3 保密 10

 8.4 非授权(非法)操作处理 10

 8.5 信息可溯源 10

 8.6 个人相关信息 10

9 其他安全 10

 9.1 与辐射有关的安全 10



9.2 与化学有关的安全 11

9.3 与生物有关的安全 11

9.4 与爆炸有关的安全 11

10 使用信息 11

10.1 概述 11

10.2 标志 11

10.3 用户手册 12

附录 A（资料性附录） 主要危险列表 13

附录 B（资料性附录） 主要安全标准 15

参考文献 18



前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家机器人标准化总体组提出并归口。

本标准起草单位：沈阳新松机器人自动化股份有限公司、苏州苏相机器人智能装备有限公司、中国科学院沈阳自动化研究所、深圳市优必选科技股份有限公司、科大讯飞股份有限公司、中国电子技术标准化研究院、中国科学院重庆绿色智能技术研究院、哈工大机器人集团股份有限公司、苏州傲特敏机器人技术服务有限公司、科沃斯商用机器人有限公司、机械工业仪器仪表综合技术经济研究所、北京康力优蓝机器人有限公司、华测检测认证集团股份有限公司、重庆鲁班机器人技术研究院有限公司、东北大学、芜湖赛宝机器人产业技术研究院有限公司、山东鲁能智能技术有限公司、中国家用电器研究院、广州赛宝认证中心服务有限公司、北京机械工业自动化研究所有限公司。

本标准主要起草人：王宏玉、徐方、孙立宁、瞿卫新、李志海、庞建新、袁杰、许玮、马万钟、刘云柱、何国田、石胜君、黄小中、郑旭、刘雪楠、黄庆、林远长、姜杨、程炎、曹际娜、尹作重、唐忠华、吴震、何鹏林、杨永敏、刘晓帆、刘世昌、宋吉来、张锋、牟昱。

机器人安全总则

1 范围

本标准规定了机器人安全总则、机械安全、电气安全、控制系统安全、信息安全、其他安全要求和使用的信息。

本标准适用于机器人的设计、生产、检测、使用和维修等。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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—2008 机械电气安全 机械电气设备 第1部分:通用技术条件

GB/T 12265.3 机械安全 避免人体各部位挤压的最小间距

GB/T 16754 机械安全 急停 设计原则

GB/T 16855.1 机械安全 控制系统有关安全部件 第1部分:设计通则

GB/T 16856—2015 机械安全 风险评估 实施指南和方法举例

GB/T 23821 机械安全 防止上下肢触及危险区的安全距离

GB 28526 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

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

机器人 robot

具有两个或两个以上可编程的轴,以及一定程度的自主能力,可在其环境内运动以执行预定任务的执行机构。

[GB/T 36530—2018,定义 3.2]

3.2

安全 safety

没有不可接受的风险。

[GB/T 20438.4—2017,定义 3.1.8]

3.3

伤害 harm

对人体健康的损害或损伤,对财产或环境的损害。

[GB/T 20002.4—2015,定义 3.1]

3.4

危险区 hazard zone; danger zone

人员暴露于至少具有一种危险的环境。

注:这种暴露可能立即或在一定时间之后对人员产生伤害。

[GB/T 15706—2012, 定义 3.11]

3.5

风险 risk

伤害发生的概率和伤害严重程度的组合。

[GB/T 15706—2012, 定义 3.12]

3.6

风险估计 risk estimation

确定伤害、危害可能达到的严重程度和伤害发生的概率。

[GB/T 15706—2012, 定义 3.14]

3.7

风险分析 risk analysis

机器限值的确定、危险识别和风险估计的组合。

[GB/T 15706—2012, 定义 3.15]

3.8

风险评价 risk evaluation

以风险分析为基础,判断是否已达到减小风险的目标。

[GB/T 15706—2012, 定义 3.16]

3.9

风险评估 risk assessment

包括风险分析和风险评价在内的全过程。

[GB/T 15706—2012, 定义 3.17]

3.10

本质安全设计措施 inherently safe design measure

通过改变机器设计或工作特性,而不是使用防止装置或保护装置来消除危险或减小风险的保护措施。

[GB/T 15706—2012, 定义 3.20]

3.11

防护装置 guard

设计为机器的组成部分,用于提供保护的物理屏障。

[GB/T 15706—2012, 定义 3.27]

3.12

联锁装置 interlocking device

联锁 interlock

用于防止危险机器功能在特定条件下(通常是指只要防护装置未关闭)运行的机械、电气或者其他类型的装置。

[GB/T 15706—2012, 定义 3.28.1]

3.13

使用信息 information for use

由信息载体(如文本、文字、标记、信号、符号、图表)组成的保护措施,可单独或组合使用这些载体向使用者传递信息。

[GB/T 12643—2013, 定义 3.22]

3.14

机械安全 mechanical safety

在机械生命周期内,物理上(机械机构产生的直接伤害)所有风险被降低到可接受的,确保其不产生

损伤或危害健康的能力。

3.15

保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程,或不被其利用的特性。

[GB/T 25069—2010,定义 2.1.1]

3.16

完整性 integrity

保护信息准确性和完整的特性。

注: 改写 GB/T 25069—2010,定义 2.1.42。

3.17

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010,定义 2.1.20]

3.18

信息安全 information security

保护、维持信息的保密性、完整性和可用性,也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[GB/T 25069—2010,定义 2.1.52]

3.19

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”。

3.20

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、通信通讯联系方式、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。

[GB/T 35273—2017,定义 3.1]

4 总则

4.1 概述

4.1.1 本标准涉及的安全包括人身、财产和环境安全,主要危险参见附录 A。

4.1.2 本标准给出的主要安全标准参见附录 B。

4.2 基本原则

4.2.1 机器人产生的伤害应控制在可接受的范围内。

4.2.2 应通过本质安全设计措施减小或消除伤害。

4.2.3 如通过本质安全设计措施消除或充分减小与其相关的伤害不可行,则应使用安全防护和补充保护措施来减小伤害。

4.2.4 通过本质安全设计措施、安全防护和补充保护措施不能减小的遗留伤害应采取使用信息和培训来减小。

4.2.5 即使机器人不受控制也不应产生伤害,否则应对其进行隔离或强迫其停止运动。

4.3 设计原则

机器人安全性设计原则如图 1 所示。

基本要求如下：

- a) 最小风险设计：首先在设计上消除风险，若不能消除已判定的风险，应通过设计方案的选择将其风险降低到可接受的水平。
- b) 采用安全装置：应采用永久性的、自动的或其他安全防护装置，使风险减少到可接受的水平。
- c) 采用告警装置：应采用告警装置来检测或标示危险，并发出告警信号。告警标记或信号应明显，避免人员对信号作出错误反应。
- d) 制定专用规程并进行培训：专用规程为保证机器人的安全操作而制定的规程，包括个人防护装置的使用方法等。对从事机器人安全相关的工作人员，应进行培训和资格认定。

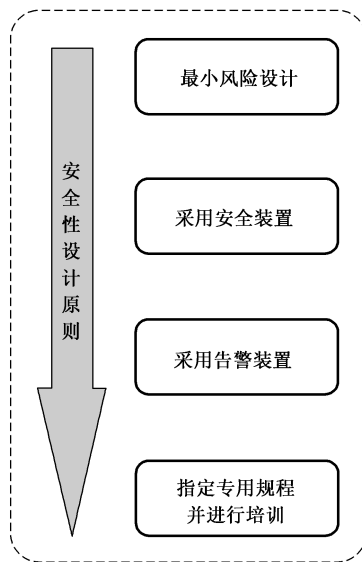


图 1 安全性设计原则示意图

4.4 风险评估和风险减小

为确保机器人安全，应在设计、使用等阶段对其进行风险评估和风险减小。风险评估和风险减小工作为反复迭代的过程，如图 2 所示。

机器人风险评估过程包括风险分析和风险评价。其中风险分析包括机器人限制的确定、危险识别和风险估计。风险分析提供了机器人风险评定所需的信息，进而最终对机器人是否需要减小风险做出判断。风险分析后，应进行风险评价，以确定是否需要减小风险。如果需要减小风险，应按顺序从以下四方面考虑：

- a) 本质安全设计；
- b) 安全防护或补充安全保护措施；
- c) 限制的改变（使用限制、空间限制、时间限制、其他限制）；
- d) 人员培训。

风险评估可确定每个危险状态或事故场景的最高风险，通常以等级、指数或分数表示被评估风险的大小。机器人风险评估工具宜使用数值评分法，见 GB/T 16856—2015 中 6.4。用一个具体数值代表可接受的风险水平，能够为风险减小决定过程提供关键依据。选择一个数值要比使用定性术语更精确，更快地做出选择，同时避免不同评估工具造成的分析差异。

为了最大程度的减小风险，应考虑下述四种因素：

- a) 机器人在生命周期所有阶段内的安全；

- b) 机器人执行其功能的能力；
- c) 机器人的易用性；
- d) 制造、使用和拆卸机器人的成本。

注 1：对这些原则的最佳应用需掌握机器人的使用、事故历史和健康记录、可用的风险减小技术以及有关机器使用的法律体制方面的知识。

注 2：当技术发展后出现了风险更低的等效机器人设计，则在特定时间内可接受的机器设计可能不再合理。

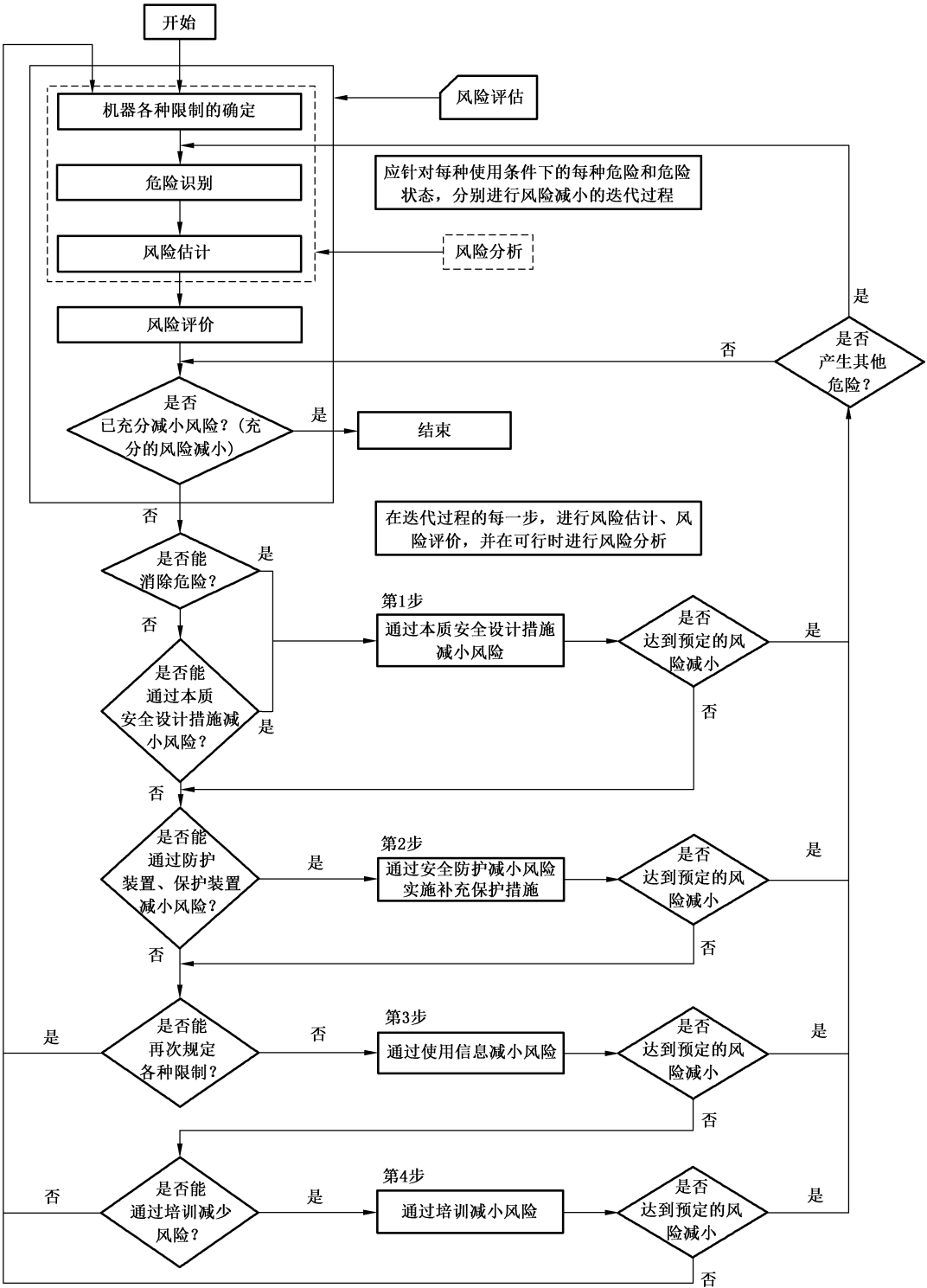


图 2 风险评估和风险减小过程示意图

5 机械安全

5.1 几何因素

应满足以下要求：

- a) 在不影响其功能的情况下,可接近的机器人机械部件不应应对人员和周围环境产生伤害；
- b) 机器人机械部件的形状和相对位置应符合 GB/T 12265.3 或 GB/T 23821 的规定。

5.2 物理特性

应满足以下要求：

- a) 应限制驱动力在可接受范围内,确保被驱动部件不会产生机械危险；
- b) 应通过限制运动部件的质量、速度的方式限制其动能；
- c) 应限制并采取措施减小噪声、振动和有害物质的排放；
- d) 应避免外部环境(海拔、温湿度、冲击等)变化引起的危险；
- e) 应使用能承受正常使用过程中产生的物理、化学作用的材料；
- f) 机器人的设计应使其具有足够的稳定性,并使其在规定的使用条件下可以安全使用。

5.3 人类功效学

设计机器人机械时应考虑人类功效学原则,并注意以下要求：

- a) 机器人使用过程中不应导致使用者有紧张姿势和动作；
- b) 应考虑人力的可及范围、控制机构的操纵及人体各部位的解剖学结构,使机器人容易操作；
- c) 应尽可能限制噪声、振动和热效应(如极端温度)；
- d) 手动控制装置的选用、位置和标记应清晰可见、可识别,可立刻进行安全操作,位置和运动与作用一致,并且操作不能引起附加风险。

5.4 防护装置和保护装置

应满足以下要求：

- a) 应采用防护装置和保护装置以防止机器人部件对人员产生伤害；
- b) 机器人正常运行期间应根据风险的类别或等级选择不同的防护装置；
- c) 应通过安全防护减少噪声、振动和有害物质；
- d) 维护或修理等阶段需要进入危险区时,机器人的设计应在不妨碍人员执行任务的前提下,使用保护人员的安全防护装置；
- e) 如不能通过重量分布等本质安全设计措施实现稳定性,则应采取保护措施如地脚螺栓、锁定装置等,保持机器人的稳定性。

5.5 补充保护措施

当本质安全设计和安全防护措施不能达到降低风险的要求时,应采用补充保护措施实现降低风险。对避免或限制伤害的较为有效的机械相关保护措施包括但不限于以下补充保护措施：

- a) 隔离和能量耗散的措施；
- b) 提供方便且安全搬运机器人及其重型零部件的装置。

如需进入机器人内部,则应考虑以下要求：

- a) 被困人员逃生和救援措施；
- b) 安全进入机器的措施。

6 电气安全

6.1 与电击有关的安全

机器人应具备在直接接触或间接接触情况下的电击防护能力。机器人在正常工作条件下和在单一故障(包括随之引起的其他故障)状态下运行应不引起电击危险。电击危险产生的原因及减小危险措施示例如表 1 所示。如有必要可提供警告标识,以提醒使用人员。

表 1 电击危险产生的原因及减小危险措施示例

可能造成伤害的原因	减小危险的方法示例
接触正常情况下带危险电压的裸露零部件	用固定的或锁紧的盖、安全联锁装置等防止使用人员接触带危险电压的零部件;使可触及的带危险电压的电容器放电
正常情况下带危险电压的零部件和可触及的导电零部件间的绝缘被击穿	采用基本绝缘并把可触及的导电零部件和电路接地,这样,由于过流保护装置在规定时间内断开发生低阻抗故障的零部件,使接触危险电压的可接触性受到限制;或者在零部件间安装一个与保护地相连的金属屏蔽,或者在零部件间采用双重绝缘或加强绝缘,以便使可触及零部件间的绝缘不会被击穿
接触与峰值电压超过 42.4 V 或直流电压超过 60 V 的通信网络连接的电路	限制这种电路的可触及性和接触区域,把它们与未接地的、接触不受限制的零部件隔离开
使用人员可触及绝缘被击穿	使用人员可触及的绝缘应当有足够的机械强度和电气强度以减少与危险电压接触的可能性
从带危险电压的零部件流向可触及零部件的接触电流(泄漏电流),或保护接地连接失效。接触电流可包括接在一次电路和可触及零部件之间电磁兼容(EMC)滤波组件所产生的电流	把接触电流限制在规定值内,或提供更可靠的保护接地连接

6.2 与能量有关的安全

大电流电源或大电容电路的相邻电极间短路时,由于燃烧、起弧、溢出熔融金属等原因可能导致伤害或着火,甚至接触带安全电压的电路也可能造成伤害。

应采用包括但不限于以下方法来减小或避免这种危险:

- a) 隔离;
- b) 屏蔽;
- c) 使用安全联锁装置。

6.3 与着火有关的安全

过载、元器件失效、绝缘击穿或连接松动产生的过高温度都可能导致着火危险。应确保机器人内着火点产生的火焰不会蔓延到火源近区以外,避免对机器人的周围造成损害。

应采用包括但不限于以下方法来减小或避免这种危险:

- a) 提供过流保护装置;
- b) 使用符合要求的适当燃烧特性的结构材料;

- c) 选择的零部件、元器件和消耗材料能避免产生可能引起着火的高温；
- d) 限制易燃材料的用量；
- e) 把易燃材料与可能的点燃源屏蔽或隔离；
- f) 使用防护外壳或挡板，以限制火焰只在机器人内部蔓延；
- g) 使用合适的材料制作外壳，以减小火焰向机器人外蔓延的可能性。

6.4 与热有关的安全

正常工作条件下的高温可能造成危害，表现为接触烫热的可触及零部件引起灼伤、绝缘等级下降和安全元器件性能降低、引燃可燃液体。

应采用包括但不限于以下方法来减小或避免这种危险：

- a) 采取措施避免可触及零部件产生高温；
- b) 避免使温度高于液体的引燃点；
- c) 如果不可避免接触烫热的零部件，应提供警告标识。

7 控制系统安全

7.1 通则

与机器人安全相关的控制系统(电气、液压、气动、软件)及部件应满足以下要求：

- a) 任何部件的单个故障不应导致安全功能的丧失；
- b) 只要合理可行，单个故障应在提出下一项功能需求之时或之前被检测到；
- c) 出现单个故障时，始终具有安全功能，且安全状态应维持到出现的故障已得到解决；
- d) 所有可合理预见的故障应被检测到；
- e) 检测出的故障在解决之前，机器人应保持安全状态；
- f) 确保安全控制系统的所有装置正常运行后，机器人方可运行。

应按 GB/T 16855.1 或者 GB 28526 规定的方法确定控制系统的性能等级。

7.2 控制电路和控制功能

应符合以下要求：

- a) 控制功能应包含但不限于启动、停止、急停、操作模式、安全功能装置(双手控制、使动、止动等)；
- b) 保护性联锁应确保危险发生时，机器人安全停机；危险解除前其“遮蔽”的危险的机器人功能不能执行；
- c) 应能避免接地故障、电压中断、电路连续性以及干扰引起的功能失常；
- d) 失效时的控制功能应包含但不限于使用经验证元件和经验证的技术、监控、冗余/多样性；
- e) 对控制电路执行的每一项安全功能应进行评估，宜确定机器人的具体安全功能提供怎样的风险降低水平，依次确定执行该安全功能的控制电路所要求的置信度等级；
- f) 控制电路执行的安全功能信息应包括安全功能名称、功能的描述、按 GB/T 16855.1 要求的性能等级或/和按 GB 28526 要求的安全完整性等级。

7.3 急停功能

机器人的失控会对周围人或环境造成伤害时应设置一个手动启动的急停功能。该急停功能应满足以下要求：

- a) 应符合 GB 5226.1—2008 中 9.2.5.4.2 的要求；

- b) 优先于机器人的其他控制；
- c) 中止所有的危险；
- d) 切断机器人驱动器的驱动源(飞行相关机器人不适用)；
- e) 消除可由机器人控制的任何其他危险；
- f) 保持有效直至复位；
- g) 只能手动复位,复位后不会自动重启；
- h) 应依据 GB 5226.1—2008 中 9.2.2 选择类别 0、类别 1、类别 2 的停止功能；
- i) 急停输出信号在撤除机器人动力后应一直有效。

急停装置应符合 GB 5226.1—2008 中 10.7 和 GB/T 16754 的设计要求。针对不同种类的机器人的急停装置应制定不同的性能等级。

7.4 保护性停止

机器人应具有一个或多个保护型停止电路,可用来连接外部保护装置。

此停止电路应通过停止机器人所有运动、撤除机器人驱动器的动力、中止可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危险。停止功能可由手动或控制逻辑启动。

7.5 速度控制

应满足以下要求：

- a) 危险评估应确定机器人的安全相关的速度范围,超出这个范围可能对机器人或周围人员造成伤害；
- b) 应在机器人可接触的移动部分进行速度监测,只有有权限的人可调节允许最大速度值。控制机器人的速度以确保其移动速度不超过安全相关的速度限制；
- c) 设计安全相关的速度控制以避免发生故障,应有超速报警。

7.6 力控制

安全相关的力控制应通过安全相关的接触传感器(例如力传感器等)或其他控制方式来实现,使机器人接触力不能超出极限。应至少满足以下要求：

- a) 接触力的反应足够快,使力保持在安全的力限制范围内；
- b) 在发生接触事故后,应避免对人或设备造成伤害。

8 信息安全

8.1 基础原则

机器人应满足以下要求：

- a) 机器人在网络(包括互联网、局域网等)中,应具有信息传输加密机制；
- b) 机器人的数据信息不应被非授权(非法)访问、篡改或删除；
- c) 机器人应阻止非授权(非法)信息的入侵,包括对此类信息的识别、判断、阻止与提示功能；
- d) 机器人不应拒接授权(合法)用户对信息和资源正常使用；
- e) 机器人应具有信息溯源机制。

8.2 身份识别

机器人在信息处理的过程中应对信息控制者进行身份标识处理。信息控制者是经过登记注册、身份验证,并具有唯一有效标识。

标识可以是自定义编码(如用户名)、通信网络接入码(如手机号)等,但应统一标识类型,并与设备安全保密资源(如密码)建立对应关系,具有唯一性。

系统应实施标识信息管理和维护,确保不被非法访问、篡改或删除。

8.3 保密

8.3.1 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。

8.3.2 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。

8.3.3 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。

8.4 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。

8.5 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:

- a) 授权的操作指令记录;
- b) 非授权的操作指令记录;
- c) 恶意代码执行记录;
- d) 网络攻击记录。

8.6 个人相关信息

机器人关于个人信息的收集、保存、使用、共享、转让、公开披露等处理活动应符合 GB/T 35273 的要求。

9 其他安全

9.1 与辐射有关的安全

机器人产生的某种形式的辐射会对使用人员或维修人员造成伤害,辐射通常包括声波(音频)辐射,射频辐射,红外线、紫外线和电离辐射,以及高强度可见光和相干光(激光)辐射。应减小这种危险。

减小这种危险的方法包括但不限于:

- a) 限制潜在辐射源的能量等级;
- b) 屏蔽辐射源;
- c) 使用安全联锁装置;
- d) 如不可避免暴露于辐射危险时提供警告标识。

9.2 与化学有关的安全

机器人工作时产生的化学危险分为直接危险和间接危险。直接危险为人体可能因吸入有毒的蒸汽或烟雾,或者人体与这些材料接触而引起对人体的直接伤害,例如由危险化学品、臭氧等引发的危害。间接危险为腐蚀等化学作用可能会引发电击等其他的危险,例如由电化学腐蚀、酸雨、盐雾等引发的接地电阻变大等。应减小这种危险。

减小化学危险的方法包括但不限于:

- a) 尽可能避免使用存在潜在危险的化学品;
- b) 如使用危险化学品应通过容器、通风等措施对其进行限制和隔离;
- c) 提供警告标识。

9.3 与生物有关的安全

生物危险为动物、植物、微生物等进入机器人内部可能引起的危险。生物危险可能不是直接危险,而是由生物等引起的次生危险,例如动物或植物的进入导致的绝缘损坏,真菌、细菌对塑料、金属防护外壳的破坏等。应减小这种危险。

减小这种危险的方法包括但不限于:

- a) 采用防止生物进入的外壳;
- b) 使用药剂;
- c) 采用防霉菌材料。

9.4 与爆炸有关的安全

爆炸危险为爆炸性气体聚集引起的危险,例如机器人内部酸性电池充电产生的可燃性气体、从外部进入的易燃易爆气体等。应减小这种危险。

减小这种危险的方法包括但不限于:

- a) 内部采用不产生爆炸气体的零部件;
- b) 防止外部爆炸性气体进入;
- c) 采取必要的通风措施。

10 使用信息

10.1 概述

使用信息由文本、文字、标记、信号、符号或图表等组成,以单独或联合使用的形式向使用者传递信息。使用人群不仅包含用户,也包含维护人员。

机器人的标志和符号应通俗易懂、应清晰且可长久保持。

10.2 标志

机器人的标志应在机器人的外部可被清楚的分辨。以下标志应被标明在机器人产品上:

- a) 生产商的商业名称;
- b) 机器人名称;
- c) 机器人系列或型号;
- d) 生产序列号;
- e) 电源相关参数;
- f) 任何法律要求的标志(适宜时)。

10.3 用户手册

用户手册应随机器人一起提供以保证机器人可以按设计要求被使用,用户手册应包含但不限于以下内容:

- a) 使用环境条件的说明;
- b) 产品外观及尺寸说明;
- c) 产品技术参数说明;
- d) 预期条件下的安全性说明;
- e) 应用限制的说明;
- f) 按规定用途使用的说明;
- g) 使用和操作的说明;
- h) 维护和维修的说明;
- i) 安全警告的说明。

如用户在安装或维护时应采取必要的预防措施,应在用户手册中说明。关于机器人的处理和废弃的信息应提供说明。



附 录 A
(资料性附录)
主要危险列表

主要危险如表 A.1 所示。

表 A.1 主要危险列表

类型	危险源	潜在后果
机械危险	——锐边； ——粗糙或光滑表面； ——旋转或运动部件； ——机械的移动； ——机械的不稳定； ——重力； ——储存的能量； ——姿势； ——重复活动； ——可见性； ——部件设计、位置或识别错误	——刺穿或刺破； ——滑倒、绊倒和跌落； ——剪切； ——摩擦或磨损； ——碰撞； ——砸伤； ——喷射； ——疲劳； ——其他因人为错误引起的后果； ——财产损失
电气危险	——电弧； ——静电现象； ——带电部件； ——与高压带电部件间无足够的距离； ——过载； ——短路； ——故障条件下变为带电部件； ——热辐射； ——爆炸； ——火焰	——烧伤； ——电伤； ——跌倒或甩出； ——着火； ——电击； ——融化颗粒的射出； ——热辐射引起的伤害； ——中毒； ——烫伤； ——财产损失
控制危险	——动力故障； ——意外停机； ——意外启动； ——传感器失灵； ——意外启动； ——传感器失灵； ——软件功能失灵； ——控制器失灵	——失控； ——砸伤； ——夹伤； ——碰伤； ——财产损失
信息危险	——泄露； ——拦截； ——入侵； ——恶意代码	——失控； ——财产损失； ——人身伤害； ——事故

表 A.1 (续)

类型	危险源	潜在后果
其他危险	——辐射引起的危险； ——化学危险； ——动物、植物、微生物等进入机器人内部可能引起的危险； ——爆炸气体引起的危险	——失控； ——财产损失； ——人身伤害； ——事故



附 录 B

(资料性附录)

主要安全标准

B.1 概述

本附录给出了机器人相关机械安全、电气安全、控制系统安全和信息安全主要安全标准。对于有特殊要求的机器人还可能涉及所列标准之外的其他标准。

B.2 机械安全标准

GB/T 8196 机械安全 防护装置 固定式和活动式防护装置的设计与制造一般要求 (GB/T 8196—2018, ISO 14120:2015, IDT)

GB/T 12265.3 机械安全 避免人体各部位挤压的最小间距

GB/T 15706 机械安全 设计通则 风险评估与风险减小 (GB/T 15706—2012, ISO 12100:2010, IDT)

GB/T 16655 机械安全 集成制造系统 基本要求 (GB/T 16655—2008, ISO 11161:2007, IDT)

GB/T 16754 机械安全 急停 设计原则 (GB/T 16754—2008, ISO 13850:2006, IDT)

GB/T 16755 机械安全 安全标准的起草与表述规则 (GB/T 16755—2015, ISO Guide 78:2012, MOD)

GB/T 18831 机械安全 与防护装置相关的联锁装置 设计和选择原则 (GB/T 18831—2017, ISO 14119:2013, IDT)

GB/T 19670 机械安全 防止意外启动 (GB/T 19670—2005, ISO 14118:2000, MOD)

GB/T 19671 机械安全 双手操纵装置 功能状况及设计原则 (GB/T 19671—2005, ISO 13851:2002, MOD)

GB/T 19876 机械安全 与人体部位接近速度相关的安全防护装置的定位 (GB/T 19876—2012, ISO 13855:2010, IDT)

GB/T 23821 机械安全 防止上下肢触及危险区的安全距离 (GB/T 23821—2009, ISO 13857:2008, IDT)

GB/T 35076 机械安全 生产设备安全通则

B.3 电气安全标准

GB 4706.1 家用和类似用途电器的安全 第1部分:通用要求 (GB 4706.1—2005, IEC 60335-1:2004, IDT)

GB 4943.1 信息技术设备 安全 第1部分:通用要求 (GB 4943.1—2011, IEC 60950-1:2005, MOD)

GB/T 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 5226.1—2019, IEC 60204-1:2016, IDT)

GB 8898 音频、视频及类似电子设备 安全要求 (GB 8898—2011, IEC 60065:2005, MOD)

GB/T 18209.1 机械电气安全 指示、标志和操作 第1部分:关于视觉、听觉和触觉信号的要求

(GB/T 18209.1—2010, IEC 61310-1:2007, IDT)

GB/T 18209.2 机械电气安全 指示、标志和操作 第2部分:标志要求(GB/T 18209.2—2010, IEC 61310-2:2007, IDT)

GB/T 18209.3 机械电气安全 指示、标志和操作 第3部分:操动器的位置和操作的要求(GB/T 18209.3—2010, IEC 61310-3:2007, IDT)

GB/T 19436.1 机械电气安全 电敏保护设备 第1部分:一般要求和试验(GB/T 19436.1—2013, IEC 61496-1:2008, IDT)

GB/T 19436.2 机械电气安全 电敏保护设备 第2部分:使用有源光电保护装置(AOPDs)设备的特殊要求(GB/T 19436.2—2013, IEC 61496-2:2006, IDT)

GB 19436.3 机械电气安全 电敏防护装置 第3部分:使用有源光电漫反射防护器件(AOPDDR)设备的特殊要求(GB 19436.3—2008, IEC 61496-3:2001, IDT)

GB/T 19436.4 机械电气安全 电敏保护设备 第4部分:使用视觉保护装置(VBPD)设备的特殊要求(GB/T 19436.4—2016, IEC/TR 61496-4:2007, IDT)

GB/T 34835 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(GB/T 34835—2017, IEC/TR 62102:2005, IDT)

B.4 控制系统安全标准

GB/T 16855.1 机械安全 控制系统安全相关部件 第1部分:设计通则(GB/T 16855.1—2018, ISO 13849-1:2015, IDT)

GB/T 16855.2 机械安全 控制系统安全相关部件 第2部分:确认(GB/T 16855.2—2015, ISO 13849-2:2012, IDT)

GB/T 20438.1 电气/电子/可编程电子安全相关系统的功能安全 第1部分:一般要求(GB/T 20438.1—2017, IEC 61508-1:2010, IDT)

GB/T 20438.2 电气/电子/可编程电子安全相关系统的功能安全 第2部分:电气/电子/可编程电子安全相关系统的要求(GB/T 20438.2—2017, IEC 61508-2:2010, IDT)

GB/T 20438.3 电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求(GB/T 20438.3—2017, IEC 61508-3:2010, IDT)

GB/T 20438.4 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语(GB/T 20438.4—2017, IEC 61508-4:2010, IDT)

GB/T 20438.5 电气/电子/可编程电子安全相关系统的功能安全 第5部分:确定安全完整性等级的方法示例(GB/T 20438.5—2017, IEC 61508-5:2010, IDT)

GB/T 20438.6 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2 和 GB/T 20438.3 的应用指南(GB/T 20438.6—2017, IEC 61508-6:2010, IDT)

GB/T 20438.7 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述(GB/T 20438.7—2017, IEC 61508-7:2010, IDT)

GB 28526 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(GB 28526—2012, IEC 62061:2005, IDT)

GB/Z 29638 电气/电子/可编程电子安全相关系统的功能安全 功能安全概念及 GB/T 20438 系列概况(GB/Z 29638—2013, IEC/TR 61508-0:2005, IDT)

GB/T 34136 机械电气安全 GB 28526 和 GB/T 16855.1 用于机械安全相关控制系统设计的应用指南(GB/T 34136—2017, IEC/TR 62061-1:2010, IDT)

B.5 信息安全标准

- GB/T 20984 信息安全技术 信息安全风险评估规范
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 29841.3 卫星定位个人位置信息服务系统 第3部分:信息安全规范
- GB/T 31916.1 信息技术 云数据存储和管理 第1部分:总则
- GB/T 35273 个人信息安全规范
- GB/T 37025 信息安全技术 物联网数据传输安全技术要求

B.6 机器人安全标准

- GB 11291.1 工业环境用机器人 安全要求 第1部分:机器人(GB 11291.1—2011,ISO 10218-1:2006 及 ISO 10218-1/Cor.1:2007,IDT)
- GB 11291.2 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 11291.2—2013,ISO 10218-2:2011,IDT)
- GB/T 20867 工业机器人 安全实施规范
- GB/T 33261 服务机器人模块化设计总则
- GB/T 33262 工业机器人模块化设计规范
- GB/T 33263 机器人软件功能组件设计规范
- GB/T 33265 教育机器人安全要求
- GB/T 36008 机器人与机器人装备 协作机器人(GB/T 36008—2018,ISO/TS 15066:2016,IDT)
- GB/T 36013 锄草机器人安全要求
- GB/T 36530 机器人与机器人装备 个人助理机器人的安全要求(GB/T 36530—2018,ISO 13482:2014,IDT)
- GB/T 37392 冲压机器人通用技术条件
- GB/T 37394 锻造机器人通用技术条件
- GB/T 37395 送餐服务机器人通用技术条件
- GB/T 37415 桁架式机器人通用技术条件
- GB/T 37416 洁净机器人通用技术条件

参 考 文 献

- [1] GB/T 12643—2013 机器人与机器人装备 词汇
 - [2] GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小
 - [3] GB/T 20002.4—2015 标准中特定内容的起草 第4部分:标准中涉及安全的内容
 - [4] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语
 - [5] GB/T 25069—2010 信息安全技术 术语
 - [6] GB/T 36530—2018 机器人与机器人设备 个人护理机器人安全要求
 - [7] ISO 9355-3 Ergonomic requirements for the design of displays and control actuators—Part 3: Control actuators
-