



中华人民共和国国家标准

GB/T 20867.1—2024

代替 GB/T 20867—2007

机器人 安全要求应用规范 第 1 部分：工业机器人

Robotics—Application specification for safety requirements—
Part 1: Industrial robot

2024-08-23 发布

2025-03-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言.....Ⅲ

引言.....Ⅴ

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 风险评估与风险减小.....2

 4.1 一般要求.....2

 4.2 危险识别.....2

 4.3 风险估计.....2

 4.4 风险评价.....3

 4.5 风险减小.....3

5 设计要求及保护措施.....3

 5.1 通则.....3

 5.2 通用要求.....3

 5.3 致动控制.....5

 5.4 与安全相关的控制系统性能.....5

 5.5 停止功能.....5

 5.6 降速控制.....6

 5.7 操作方式.....6

 5.8 示教控制.....6

 5.9 同时运动控制.....7

 5.10 协同操作要求.....7

 5.11 奇异性保护.....9

 5.12 单轴限位.....9

 5.13 无驱动源运动.....9

 5.14 起重措施.....9

 5.15 电连接器.....10

6 安装、试运行和功能测试.....10

 6.1 安装.....10

 6.2 试运行和功能测试.....10

7 编程.....11

 7.1 一般要求.....11

 7.2 编程前.....11

7.3 编程中.....11

7.4 返回自动操作.....12

7.5 编程数据.....12

7.6 程序验证(程序校验).....12

8 使用和维护.....12

8.1 一般要求.....12

8.2 自动操作.....12

8.3 故障查找.....12

8.4 维护.....13

9 使用信息.....13

9.1 使用说明书.....13

9.2 培训.....13

附录 A (资料性) 机器人风险评估示例.....15

附录 B (资料性) 典型工业机器人危险列表.....19

参考文献.....21



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。

本文件是 GB/T 20867《机器人 安全要求应用规范》的第1部分。GB/T 20867 已经发布了以下部分：

——第1部分：工业机器人。

本文件代替 GB/T 20867—2007《工业机器人 安全实施规范》，与 GB/T 20867—2007 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 更改了范围(见第1章,2007年版的第1章)；
- 增加了“术语和定义”(见第3章)；
- 更改了“安全分析”为“危险识别及风险评估”(见第4章,2007年版的第3章)；
- 删除了“基本设计要求”(2007年版的第4章)；
- 更改了“机器人设计和制造”为“设计要求及保护措施”(见第5章,2007年版的第5章)；
- 删除了“机器人系统的安全防护和设计”(2007年版的第10章)；
- 更改了“安装、试运行和功能测试”(见第6章,2007年版的第8章)；
- 增加了“编程”(见第7章)；
- 更改了“使用和维护”(见第8章,2007年版的第7章)；
- 更改了“使用信息”(见第9章,2007年版的第9章和第10章)；
- 增加了“机器人风险评估示例”(见附录A)；
- 增加了“典型工业机器人危险列表”(见附录B)。

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。

本文件由中国机械工业联合会提出。

本文件由全国机器人标准化技术委员会(SAC/TC 591)归口。

本文件起草单位：北京机械工业自动化研究所有限公司、立宏安全设备工程(上海)有限公司、中国科学院沈阳自动化研究所、重庆凯瑞机器人技术有限公司、德凯质量认证(上海)有限公司、杭州海康机器人股份有限公司、遨博(北京)智能科技股份有限公司、法奥意威(苏州)机器人系统有限公司、埃夫特智能装备股份有限公司、珞石(山东)智能科技有限公司、沈阳新松机器人自动化股份有限公司、机科发展科技股份有限公司、东莞市大研自动化设备有限公司、重庆鲁班机器人技术研究院有限公司、重庆凯瑞认证服务有限公司、河北工业大学、北京航空航天大学、深圳市越疆科技股份有限公司、江苏汇博机器人技术股份有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、苏州大学、中国科学院重庆绿色智能技术研究院、中汽检测技术有限公司、乐聚(深圳)机器人技术有限公司、上海沃迪智能装备股份有限公司、深圳市湾测技术有限公司、苏州艾利特机器人有限公司、深圳云天励飞技术股份有限公司、中国计量大学、重庆大学、北京鹏鹏科创科技发展有限公司、中关村机器人产业创新发展有限公司、创客天下(北京)科技发展有限公司。

本文件主要起草人：杨书评、侯红英、王恒之、李本旺、韩志雄、李志海、孙元栋、宋仲康、管越、姚庭、阮伟伟、唐燕生、张锋、张胜、肖大放、张驰、王松、孙添飞、王嘉、魏洪兴、陶永、王茂林、刘培超、王振华、陈淦萍、陈国栋、何国田、曹懿莎、冷晓琨、朱志昆、曹伟、童上高、陈卓贤、姜宇、刘颖、唐聪、袁杰、杨金、

陈辉、雷建勇、孙恺、孙振江、牟宏磊、刘晶晶、蒙洋、王烁石。

本文件及其所代替文件的历次版本发布情况为：

——2007 年首次发布为 GB/T 20867—2007；

——本次为第一次修订。

引 言

本文件是 GB 11291.1—2011 的配套文件,目的是增加 GB 11291.1—2011 的可操作性,便于工程技术人员、管理人员及用户更准确、全面的使用和实施安全标准。

GB/T 20867《机器人 安全要求应用规范》拟由两个部分组成。

——第 1 部分:工业机器人。目的是增加 GB 11291.1—2011 的可操作性。

——第 2 部分:工业机器人系统与集成。目的是增加 GB 11291.2—2013 的可操作性。



机器人 安全要求应用规范

第1部分：工业机器人

1 范围

本文件规定了工业机器人安全标准 GB 11291.1—2011 应用实施的步骤和细则。
本文件适用于工业机器人(以下简称“机器人”)的设计、生产、销售、管理和使用。

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 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 11291.1—2011 工业环境用机器人 安全要求 第1部分:机器人
GB/T 12265 机械安全 防止人体部位挤压的最小间距
GB/T 12644 工业机器人 特性表示
GB/T 12668.502—2013 调速电气传动系统 第5-2部分:安全要求 功能
GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小
GB/T 16855.1—2018 机械安全 控制系统安全相关部件 第1部分:设计通则
GB/T 17799.2 电磁兼容 通用标准 第2部分:工业环境中的抗扰度标准
GB/T 17799.4 电磁兼容 通用标准 第4部分:工业环境中的发射
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 36008—2018 机器人与机器人装备 协作机器人
GB/T 42598 机械安全 使用说明书 起草通则

3 术语和定义

GB 11291.1—2011 界定的以及下列术语和定义适用于本文件。

3.1

风险评估 risk assessment

包括风险分析和风险评价在内的全过程。

[来源:GB/T 15706—2012,3.17]

3.2

协同操作 collaborative operation

专门设计的机器人在规定的工作空间内直接与人一同工作的状态。

[来源:GB 11291.1—2011,3.4]

3.3

安全空间 safeguarded space

由周边安全防护装置确定的空间。

[来源:GB 11291.1—2011,3.25.4]

4 风险评估与风险减小

4.1 一般要求

应按照 GB/T 15706—2012 的要求对机器人全生命周期过程中的设置、调试、示教、操作和维护等进行风险评估,并采取必要的风险减小措施。机器人风险评估示例见附录 A。

注: GB/T 15706—2012 附录 B 给出了机器常见的危险、危险状态和危险事件示例。

4.2 危险识别

任何机器人都应进行危险识别,危险识别是风险评估中最重要的步骤。只有危险被识别后,才能采取风险减小对应的措施。

危险识别的目的是形成一份危险、危险状态和/或危险事件的列表,该列表能够描述危险状态可能在何时以何种方式导致伤害的事故场景。

典型工业机器人危险列表见附录 B。

4.3 风险估计

4.3.1 通则

识别出的机器人危险应进行风险估计。风险估计的目的是确定每个危险状态的最高风险,通常以等级、指数或者分数表示估计风险的大小。风险估计应通过伤害的严重程度和该伤害发生的概率这两个风险要素,对每种危险的风险进行估计。

注: GB/T 15706—2012 中 5.5.2 描述了所有风险要素。

4.3.2 风险要素——伤害的严重程度

每个危险事件可能造成几种不同严重程度的伤害。评估一系列具有代表性严重程度的风险并考虑能够实际发生的最严重(可信的最坏情况)的伤害有助于确定伤害的严重程度。

伤害的严重程度的估计应符合 GB/T 15706—2012 中 5.5.2.2 的规定。

示例:伤害的严重程度可分为:

- 灾难性
导致死亡或永久残废的伤害或疾病(不能返回工作);
- 严重的
导致人体严重虚弱的伤害或疾病(能回到某些岗位工作);
- 中等的
要求救护的显著伤害或疾病(能够回到相同岗位上工作);
- 轻微的
至多需要急救的轻伤或没有受伤(损失少量或不损失工作时间)。

4.3.3 风险要素——伤害发生的概率

风险估计的所有方法都需要通过考虑下列情况,估计伤害发生的概率:

- a) 人员在危险中的暴露程度(见 GB/T 15706—2012 中 5.5.2.3.1);
- b) 危险事件发生的概率(见 GB/T 15706—2012 中 5.5.2.3.2);
- c) 在技术和人员方面避免或限制伤害的可能性(见 GB/T 15706—2012 中 5.5.2.3.3)。

4.3.4 风险估计工具

为了支持风险评估过程,可从 GB/T 16856—2015 中给出的风险评估工具中选用一种工具或方法:

- a) 风险矩阵法;
- b) 风险图法;
- c) 数值评分法。

另外,还可使用综合方法的混合型工具。

4.4 风险评价

风险评价的目标是:

- 如果有,确定哪些危险状态需要进一步减小风险;
- 确定是否达到所要求的风险减小,且没有引入进一步的危险或增加其他风险。

如果经风险评价后采用了保护和(或)风险减小措施,应重新进行风险评估迭代过程以验证其是否能够有效减小风险。

4.5 风险减小

根据风险评估结果,应按照 GB/T 15706—2012 中图 1 给出的风险减小迭代三步法,采取第 5 章~第 9 章给出的风险减小措施将机器人的风险减小至可接受水平。

5 设计要求及保护措施

5.1 通则

机器人本体通用部分设计应符合 GB 11291.1—2011 规定的基本安全要求。

5.2 通用要求

5.2.1 动力传递部件

机器人运动是通过其动力传动部件(如:电机轴、齿轮、传动带或者链等)实现。这些部件若通过固定式防护装置(如:机械臂体外壳)单独和/或整体进行防护,则防护装置之间相对运动的间隙应符合 GB/T 12265 的要求;若通过联锁防护装置(如:带有接触感应装置/传感器的外壳)进行防护,则其安全控制回路应满足 GB/T 16855.1—2018 规定的性能等级(PL)为 PL=d 或者 GB 28526 规定的安全完整性等级(SIL)为 SIL=2 的要求。防护装置的应用场景和典型特征(非包含全部安全特征)见表 1。

表 1 防护装置的应用场景和典型特征

防护装置类别	应用场景 (对应安全防护的危险区域)	特征
固定式防护装置	在机械的正常工作过程中,不要求人员进入危险区域; 因操作、维护等原因不允许身体部位直接接触及危险区域	在安全防护的危险区域附近保护人员; 防止身体部位接触危险区; 只有通过专用工具才能移除
联锁防护装置	在机械正常工作过程中,阻止人员接触危险区域	在所安全防护的危险区附近保护人员; 当联锁防护装置打开时,立即中断或者阻止危险的发生

5.2.2 动力损失或变化

动力损失或变化涉及的动力包含电提供的动力和非电提供的动力(如机械、液压、气动、真空和磁力等)。

电气部件选型考虑器件失效率的影响,并优先考虑保持整个回路的安全功能完整性。电气提供动力的变化或者损失不应造成以下危险:

- 电源供电不稳定造成的电气部件损坏;
- 电气部件损坏导致的功能缺陷;
- 供电突然中断导致机械臂本体姿态的改变,以及关联物品(物料)状态的改变;
- 电源重启(包含瞬间重启和正常重启)导致的任何危险运动。

非电气提供的动力的损失或变化不应造成以下危险:

- 机械臂及其相关部位的移动、运动和倾斜等;
- 末端执行器上的工具、工装以及工装上物品的脱落。

注:末端执行器的安全设计见 GB/Z 43065.1—2023。

5.2.3 部件故障

机器人所有组成部件设计应防止或降低由于装配、储存、运输、使用和维护过程中出现退化性或突发性失效时发生危险。

机器人动力传动部件,如电机、减速器、同步带和传动轴等应使用固定或移动的防护装置阻止危险发生。

示例:可调机械限位装置可在抱闸失效或传动轴断裂时,阻止轴关节继续朝一个方向持续运动,从而降低损伤人体或周围设备的风险。

机器人机械储能部件,如平衡缸、弹簧和平衡飞轮等应粘贴醒目的危险类别、危险等级标识,以及部件维护指导说明,防止和降低由于误操作引起对人体或周围设备的伤害。

平衡缸应粘贴危险标识和具备压力值显示表,用于观测压力值是否正常。当处于正常区间以外时应及时维护,同时应提供维护过程能量受控释放和储蓄的操作说明。

5.2.4 能源

机器人设计应防止或能减小由于动力源损失或失效情况下机器人自身部件损伤及对人体和周围设备的伤害。

电机抱闸选型时,下电状态抱闸吸合转矩应小于电机允许瞬时最大转矩,同时应大于最大负载时保持转矩。当电源突然断开情况下,不应造成电机减速机承受瞬时转矩过大而导致部件故障,且能有效制动降低对人体和周围设备损伤风险。

5.2.5 储能

机器人上的警示标识应标明:

- a) 储能装置位置;
- b) 储能类型(可用电容、电池、液压、气动和弹簧等图形表示);
- c) 文字提示内容。

使用说明书应明确相关储能的装置以及储能受控释放的措施,必要时,还应提供相匹配的图纸。

5.2.6 电磁兼容性(EMC)

机器人及其控制系统应按 GB/T 17799.2 以及 GB/T 17799.4 的要求通过 EMC 测试。机器人及

其系统通过 EMC 测试后,不对相关机器人及其系统做设计修改,应保持和测试通过的 EMC 设计一致,否则应重新测试。

5.2.7 电气设备

机器人设计应满足 GB/T 5226.1 的要求,并考虑使用环境中电磁干扰、静电放电、射频干扰、浪涌和漏电等因素引发的异常通信故障,这些故障可导致部件烧毁、数据传输错误、异常下电停机和其他危险运动。

示例:如电磁干扰防护不足导致控制器误发送、漏发送目标位置信息至驱动器,会引发伺服报警停机对机器人产生冲击损伤或引发错误运动导致撞击等危险。

5.3 致动控制

启动电源或运动的致动控制装置的设计和制造应满足 GB 11291.1—2011 中 5.3 所列的对意外操作防护、状态指示、标签和单点控制的要求。

5.4 与安全相关的控制系统性能



控制系统安全相关部件也称为安全控制系统(SRP/CS),包括机械、电气、可编程电子、液压、气动和软件。

与安全相关的控制系统性能表述按照 GB/T 16855.1—2018 中规定的 PL 和类别,或者按照 GB 28526 规定的 SIL 和硬件容错要求。使用这些可供选择的标准来设计与安全相关的控制系统时,应达到降低风险的同等水平。

与安全相关的控制系统至少应满足 GB 11291.1—2011 中 5.4.2 的要求。这些要求对应于 GB/T 16855.1—2018 所描述的 PL d、类别 3。也可依据风险评估的结论,采取可达等同性能的替代准则(见 GB 11291.1—2011 中 5.4.3),这时应满足 GB/T 16855.1—2018 中 6.2 所列的对应类别的要求。

5.5 停止功能

5.5.1 一般要求

每台机器人都应有保护性停止功能和独立的急停功能。这些功能应具有与外部保护装置连接的措施。

5.5.2 急停功能

每个能启动机器人运动或造成其他危险状况的控制站都应有手动的急停功能,该急停功能设计应满足以下条件:

- a) 急停功能的安全性能符合 GB 11291.1—2011 中 5.4 的要求;
- b) 急停装置设计在容易接近的位置,如示教器、控制柜及其他能启动机器人运动或造成其他危险状况的控制站;
- c) 急停装置的设计采用手掌或拳(例如蘑菇头式)触及操动的按钮装置、拉线操作开关或不带机械防护装置的脚踏开关,但不限于上述型式;
- d) 急停装置是红色,其后面的背景色着黄色;
- e) 急停确定选择 0 类或 1 类停止功能的作用,急停的类别选择取决于机械的风险评估;
- f) 急停控制优先于机器人的其他控制;
- g) 急停功能尽快停止所有的危险运行,消除可由机器人控制的任何其他危险;
- h) 急停信号发出切断机器人驱动器的驱动源;

- i) 急停信号的发出在未经手动复位前保持有效直至复位,若有几个急停装置,则在所有操作件复位前电路不应恢复,手动操作急停装置的操作件的触头确保直接断开操作件;
- j) 急停电路本身的复位不应启动机器人的任何运动,如果急停或动力源故障引起的逻辑判别错误或存储状态丢失,则产生一个急停信号并在存储或逻辑顺序复位后才可开始操作;
- k) 如果具有急停输出功能,符合 GB 11291.1—2011 中附录 D 的要求。

注: 急停功能的更多信息见 GB/T 16754。

5.5.3 保护性停止

机器人应具有一个或多个保护性停止电路,该保护性停止功能的设计应满足以下条件。

- a) 保护性停止的安全性能符合 GB 11291.1—2011 中 5.4 的要求。
- b) 保护性停止设计一个或多个供外部连接的装置。
- c) 保护性停止外接装置的安装使用,循序制造商提供的安全距离规定决定。
- d) 保护性停止电路确定选择 0 类或 1 类停止功能的作用。
- e) 保护性停止功能尽快停止机器人所有运动。
- f) 保护性停止功能能撤除机器人驱动器的动力。
- g) 保护性停止功能能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。
- h) 保护性停止功能的复位采用手动或控制逻辑自动方式复位,未进行复位前不应引起机器人的任何动作。
- i) 当机器人可能具有 2 类停止功能的额外保护停止功能,该功能不会导致驱动电源被切断,但在机器人停止后需要对停止状态进行监控,一旦机器人检测到停止状态下的任何意外动作或检测到的保护停止功能失效应导致 0 类停止。检测停止状态的安全性能按 GB 11291.1—2011 中 5.4 的要求。
- j) 当机器人可能具有 2 类停止功能的额外保护停止功能,电力驱动系统符合 GB/T 12668.502—2013 的安全操作停止(SOS)要求。

5.6 降速控制

机器人应具备降速控制功能,在降速控制方式下操作时应满足以下条件。

- a) 降速控制方式下操作时,机器人末端执行器的安装法兰和工具中心点(TCP)的速度小于或等于 250 mm/s。
- b) 降速控制方式下操作或编程时,具备可选择小于或等于 250 mm/s 的速度的方式和指令。
- c) 降速控制功能设计和构建成任何单个可合理预见的故障出现时,安装法兰和工具中心的速度不超过降速功能的限定速度。当超过降速功能的限定速度,触发保护性停止。
- d) 降速控制功能回路设计的安全性能符合 GB 11291.1—2011 中 5.4 的要求。

5.7 操作方式

机器人操作方式包括自动方式、手动降速方式和手动高速方式。机器人应至少具备自动方式和手动降速方式。操作方式应符合 GB 11291.1—2011 中 5.7 的要求。

自动方式下,出现急停、伺服报警、触发安全防护时,自动操作方式应被停止。如程序正在运行时触发安全防护,程序将被暂停或停止,在报警清除前,不应启动。

手动方式下,自动操作是被禁止的,无法通过三位使能装置以外的方式让机器人使能或启动程序。

5.8 示教控制

示教控制应符合 GB 11291.1—2011 中 5.8 的要求。

使能装置应在手动降速方式和手动高速方式下生效。使能装置应与安全控制系统的停止电路或其他等效安全停止电路相连接。

5.9 同时运动控制

5.9.1 单示教盒控制

单个示教盒可连接到一台或多台机器人的控制器。在手动方式操作时,机器人系统的所有功能都应在唯一示教盒的控制下。单示教盒控制应符合 GB 11291.1—2011 中 5.9.1 与 5.9.2 的要求。

5.9.2 安全设计要求

处于同一示教盒控制下的所有机器人,应处于相同的操作模式(如手动或自动模式),并且处于相同的状态(如打开或关闭电源)。示教盒应提供允许一个或多个机器人处于伺服断开状态的能力,以满足测试、排除故障及运行错误的需求,处于伺服断开状态的机器人不会包含在同时运动中。

对于包含在同时运动中的机器人,应满足以下控制要求:

- a) 在被激活前应被单独的选择;
- b) 在被选择时,所有机器人应处于相同的操作模式下(如手动降速);
- c) 被选中的机器人应提供有清晰可见的指示,这个指示可在示教盒或控制柜或机器人本体上;
- d) 只有被选择的机器人可允许运动;
- e) 对于已被激活的机器人,应提供反激活(停止激活)的功能。



5.10 协同操作要求

5.10.1 一般要求

协同操作是共用同一工作空间的人员和机器人之间的一种状态。

为协同操作而设计的机器人处于协同操作状态时,应有可视的指示并符合以下的一个或多个要求:

- a) 停止;
- b) 手动引导;
- c) 速度、位置监控;
- d) 设计对动力及反作用力的限制/控制系统对动力及反作用力的限制。

5.10.2 停止

协同工作空间中有人时,机器人应停止运动。人离开协同工作空间后,机器人可恢复自动操作。安全适用的受监控停止应符合 GB/T 36008—2018 中 5.5.2 的要求。

机器人应配置能够检测操作者是否处于协同工作空间内的安全适用设备。

机器人应在操作者进入协作工作空间时提前切换到安全适用的受监控停止状态,并一直保持这一状态,直到操作者离开协作工作空间。

若操作者进入协作工作空间时机器人还未进入安全适用的受监控停止状态,则会引发保护性停止(0类停止)。

5.10.3 手动引导

如果机器人具有手动引导功能,手动引导装置应在末端执行器附近。手动引导应符合 GB/T 36008—2018 中 5.5.3 的要求。

操作者进入协同工作空间进行手动引导操作应满足以下两个条件之一：

——在触发安全适用的受监控停止后，操作者才被允许进入协同工作空间手动靠近机器人末端执行器的引导设备以完成手动引导的任务，否则应引发保护性停止；

——机器人系统满足 5.10.5 的要求。

手动引导速度应小于或等于 250 mm/s。

5.10.4 速度、位置监控

机器人和操作者之间应随时维持一个保护性间距，以实现风险减小。当间距小于保护性间距时，机器人应保护性停止。速度与分离监控应符合 GB/T 36008—2018 中 5.5.4 的要求。

保护性距离可由公式(1)进行评估。

$$S_p = S_h + S_r + S_s + C + Z_d + Z_r \quad \dots\dots\dots (1)$$

式中：

S_p ——保护性距离；

S_h ——由操作员位置改变对保护性间距产生影响的部分；

S_r ——由机器人系统反应时间对保护性间距产生影响的部分；

S_s ——由机器人系统停止距离对保护性间距产生影响的部分；

C ——侵扰距离，由 GB/T 19876 定义，是身体的一部分在被检测到之前所侵入传感区的距离；

Z_d ——操作员在协同工作空间中的位置不确定性，其由当前传感设备的测量误差导致；

Z_r ——机器人系统的位置不确定性，其由机器人位置测量系统的精度导致。

5.10.5 设计对动力及反作用力的限制/控制系统对动力及反作用力的限制

机器人应满足功率与力限制要求进行设计，以保持机器人系统相关危险在风险评估中指定的阈值以下。可按照以下限值之一确定阈值：

a) 法兰或 TCP 处的最大动态功率为 80 W 或最大静态力为 150 N；

b) 采用 GB/T 36008—2018 附录 A 中规定的限值。

如超过阈值，应启动保护性停止。

功率与力限制应符合 GB/T 36008—2018 中 5.5.5 的要求。

协作机器人还可通过相关措施来降低机器人接触风险，降低风险的方法可参考 GB/T 36008—2018 中 5.5.5.4 的内容。安全设计方法包括：

a) 限制力或扭矩；

b) 限制运动部件的速度；

c) 限制动量、机械功率或能量(作为质量与速度的函数)；

d) 使用轴及空间的安全软限位功能；

e) 使用安全适用的受监控停止功能；

f) 使用传感器预测或检测接触(例如逼近与接触检测，以减少准静态力)。

功率与力限制的测试中应遵循以下规则。

a) 明确机器人适用的末端执行器，且末端执行器表面不应有尖锐或锋利边缘；在机器人携带可能对人体造成危险的末端执行器(如焊接、打磨)时，不应与操作者发生碰撞。

b) 机器人以 100% 安全限制速度运行，模拟碰撞人体部位产生的暂态力或挤压力不应超过阈值。可降低安全速度以保证碰撞力不超过阈值。为避免损坏设备，机器人的速度应由慢到快依次测试。

c) 测试点为路径中速度最大点，路径中保持最大速度的时间应尽可能长，并通过外部设备对机

机器人的最大运行速度进行测量与确认。

d) 碰撞力的方向应与仪器表面垂直。

5.11 奇异性保护

在手动降速方式下,机器人的控制应满足下列之一。

- 由示教盒激活协调运动时,在机器人通过或纠正奇异点前停止机器人运动并警告示教员。
- 产生可听或可视的警告信号,并继续通过奇异点。通过时,机器人各轴的运动速度应小于或等于 250 mm/s。
- 在奇异点可被控制而不产生任何危险运动的情况下,不需要额外的保护。

5.12 单轴限位

5.12.1 一般要求

应提供限位装置在机器人周围建立限定空间的措施。应提供安装可调机械挡块的措施,以便限制机器人主轴(具有最大位移的轴)的运动。制造商应遵循 5.12.2 或 5.12.3 的要求,或两者兼备。

注:这种方法能通过提供获取和安装外部机械停止装置的工程信息和说明来实现。使用安全等级软限位和空间限制(见 5.12.3)也能满足这一要求。

5.12.2 轴的机械及机电限位装置

轴的机械及机电限位装置应符合 GB 11291.1—2011 中 5.12.2 的规定。

机器人安装使用前应检查 2 轴、3 轴的限位装置,配备可调机械和非机械限位装置。

机器人在额定负载、最大速度和最大或最小臂长的条件下碰触机械挡块时,应中止运动。

5.12.3 轴及空间的安全软限位

轴及空间的安全软限位应符合 GB 11291.1—2011 中 5.12.3 的规定。

5.12.4 动态限位装置

动态限位装置应符合 GB 11291.1—2011 中 5.12.4 的规定。

如果机器人带有动态限位装置,则通过不同负载和速度检查其功能是否有效,并应符合 GB/T 16855.1—2018 规定的 PL d 和类别 3 要求(除非安全评估需要另一个类别)。

5.13 无驱动源运动

无驱动源运动应符合 GB 11291.1—2011 中 5.13 的规定。

使用说明书宜包含该装置(重力和释放制动装置)的局部图纸、操作说明和专业/经培训人员操作要求。

警示标识应包含:

- a) 可能造成次生危险的图形或者符号;
- b) 可能产生次生危险部位的说明;
- c) 简单易懂的操作提示。

5.14 起重措施

起重措施应符合 GB 11291.1—2011 中 5.14 的规定。

应在机械臂本体以及相关位置处标明起重点位置并配有警示标识,警示标识可用图形表示,并符

合使用说明要求。

5.15 电连接器

电连接器应符合 GB 11291.1—2011 中 5.15 的规定。

若电连接器分离或破裂可能引起机器人的危险运动,则在设计时应采取保护措施,如捆扎、配对和啮合等。

6 安装、试运行和功能测试

6.1 安装

机器人应按制造商的使用说明书的要求进行安装,并按 GB/T 12644 作为安装期间的补充指导。安全防护措施应通过危险识别和风险评估后进行判定。使用前,用户应重新检查安全要求,以确保安全防护装置运行可靠:

- a) 所有的安全防护装置应在预定的使用条件下进行试验,其不足之处应进行修改;
- b) 应重新检查作业任务,保证安全防护不会妨碍其作业任务的完成;
- c) 应复查安全防护装置的作用,保证其不易于失去作用或绕过安全防护装置。

6.2 试运行和功能测试

6.2.1 一般要求

机器人在安装或再置位后的启动(包括首次启动)和测试中,应遵循下述条款的规定。这些规定同样适用于机器人中软件或硬件更换之后和影响其运行的维修之后。

6.2.2 限定空间的指定

所有的机器人都应安装安全防护装置。若计划中的安全防护装置在进行试运行和功能测试前尚未就位,则应在运行前采取安装限定空间的临时措施(如安装链条、轻便墙板和警示栅栏等)。

6.2.3 人员的限制

在调试和功能测试期间,安全防护装置生效前,不允许人员进入安全防护空间。

6.2.4 安全和运行检验

应按照制造商的使用说明书进行机器人的试运行和功能测试,并做好如下的准备工作:

- a) 通电前检查:
 - 1) 机器人已按使用说明书正确安装,且稳定性好;
 - 2) 电气连接正确,电源参数(如电压、频率、干扰级别等)在规定的范围内;
 - 3) 其他设施(如水、空气、燃气等)连接正确,且在规定的界限内;
 - 4) 通信连接正确;
 - 5) 外围设备和系统连接正确;
 - 6) 已安装好限定空间的限位装置;
 - 7) 已采用安全防护措施;
 - 8) 周边的环境符合规定(如照明、噪声等级、湿度、温度和大气污染等)。
- b) 通电后检查:
 - 1) 机器人控制装置的功能如启动、停机和操作方式选择(包括键控锁定开关)符合预定要

- 求,机器人能按预定的操作系统命令进行运动;
- 2) 机器人各轴都能在预期的限定范围内进行运动;
 - 3) 急停及安全停机电路及装置有效;
 - 4) 可与外部电源断开和隔离;
 - 5) 示教装置的功能正常;
 - 6) 安全防护装置和联锁的功能正常,其他安全防护装置(如围栏和/或警示装置)就位;
 - 7) 在“慢速”时,机器人能正常运行,并具有作业能力;
 - 8) 在自动(正常)操作方式下,机器人运行正常,且具有在额定负载和要求的速度下完成预定作业的能力。

6.2.5 机器人重新启动步骤

机器人的软件、硬件及任务程序更换以及修理或维护后,重新启动时应遵循如下步骤:

- a) 通电前,检查硬件的任何变化或附加物;
- b) 为了正常运行,对机器人进行功能性测试。

7 编程

7.1 一般要求

进行编程时,应在安全防护空间外进行。当示教员不得不进入安全防护空间内进行编程时,则应采用必要的附加安全防护措施,并通过 5.6 中的操作状态选择要求暂停安全防护装置(如联锁门和/或现场传感装置)的保护功效。

7.2 编程前

在编程前,采取以下附加安全防护措施:

- a) 示教员应按照培训要求进行培训,并在实际的机器人上进行训练和熟悉包括所有安全防护措施在内的所推荐的编程步骤;
- b) 示教员应目检机器人和安全防护空间,确保不存在产生危险的外界条件;
- c) 示教盒的运动控制和急停控制应进行功能测试,以保证正常操作;
- d) 示教操作开始前,应排除故障和失效;
- e) 示教员进入安全防护空间前,所有的安全防护装置应确保在位,且在预期的示教方式下能起作用;
- f) 进入安全防护空间前,应要求示教员进行编程操作,但不能进行自动操作。

7.3 编程中

在编程过程中,采取以下附加安全防护措施:

- a) 示教期间仅允许示教编程人员在防护空间内;
- b) 示教员应具有和使用有单独控制机器人运动功能的示教盒;
- c) 示教期间,机器人运动只能受示教装置控制,机器人不应响应来自其他地方的遥控命令;
- d) 示教员应具有单独控制在安全防护空间内的其他设备运动控制权,且这些设备的控制应与机器人的控制分开;
- e) 若在安全防护空间内有多台机器人,而围栏的安全门开着或现场传感装置失去作用时,所有的机器人都不应进行自动操作;

- f) 机器人系统中所有急停装置都应保持有效；
- g) 示教时,机器人的运动速度应小于或等于 250 mm/s,具体的速度选择宜考虑万一发生危险,示教员有足够的时间脱离危险或停止机器人的运动；
- h) 编程时,应关断机器人驱动器不需要的动力(必需的平衡装置应保持有效)。

7.4 返回自动操作

在启动机器人进行自动操作前,示教员应将暂停使用的安全防护装置功能恢复。

7.5 编程数据

应保留任务程序和维修程序的记录。

程序数据不使用时,应储存在可传送的媒体(如纸、磁盘等)中,并存放在合适的保护环境中。

7.6 程序验证(程序校验)

程序验证是确认机器人的编程路径及处理性能与应用时所期望的路径和处理性能是否一致的方法。验证可以是程序路径的全部或一段。程序验证的人员应尽可能在安全防护空间外执行。需要人员在安全防护空间内完成程序验证时,应满足以下条件:

- a) 程序验证在机器人运动速度小于或等于 250 mm/s 时进行,除机器人的运动控制仅使用握持-运行装置或使能装置外,还应满足编程时的安全防护要求；
- b) 当要求在机器人的运行速度大于 250 mm/s 时,校验人员在安全防护空间内检查已编程的作业任务和与其他设备相互配合关系,应采用以下的安全防护要求:
 - 第一个循环应采用小于或等于 250 mm/s 的速度进行,然后仅由编程人员用键控开关谨慎地操作,分步增加速度；
 - 安全防护空间内的工作人员应使用使能装置或与其安全级别等效的其他装置；
 - 应建立安全工作步骤以使在安全防护空间内的人员的危险减至最小。

8 使用和维护

8.1 一般要求

机器人在使用时(如示教编程、程序验证、自动操作、故障查找和维护)应满足安全要求。在使用和维护期间,应为机器人的每位操作者提供安全防护措施。

8.2 自动操作

仅在满足下列要求时,才能启动机器人进行自动操作:

- a) 预期的安全防护装置都在位,并且能起作用；
- b) 在安全防护空间内没有人；
- c) 遵守安全操作规程。

8.3 故障查找

故障查找应在安全防护空间外进行。当不能实行,且机器人设计时已考虑到需要在安全防护空间内进行故障查找,则应采用下列安全要求:

- a) 担负故障查找的人员要经过特别的核准和对这种工作进行过培训；
- b) 进入安全防护空间内的人员应使用使能装置使机器人运动；

- c) 制定安全操作规程,使安全防护空间内的人员对危险的暴露降至最低。

8.4 维护

8.4.1 一般要求

为了确保机器人连续安全运行,应制定检查和维护的程序并考虑制造商的建议。

8.4.2 维护要求

为避免机器人的维修人员受到危险的伤害,应按照制造商的使用说明书对人员进行安全防护和安全培训。

尽可能使维修人员在安全防护空间外进行作业,如将机器人放置于某一预定的位置。

当不得不在安全防护空间内完成维护任务时,根据风险评估来选择以下给出的安全防护措施。

- a) 应使用切断动力源的步骤关断机器人并受控地释放所积蓄的能量或锁定能源。
- b) 当机器人已上电,要求维修人员进入安全防护空间内进行维修时,满足以下要求:
 - 1) 进入安全防护空间前应完成下列步骤:
 - 对机器人进行目检,以判断是否存在可能引起误动作的条件;
 - 为确保示教盒能进行正常操作,使用前进行功能测试;
 - 若发现某些故障或误动作的条件,则维修人员在进入安全防护空间之前进行排除或修复。
 - 2) 在安全防护空间内的维修人员应拥有机器人的总的控制权,且:
 - 机器人控制应脱离自动操作状态;
 - 机器人应不能响应任何远程控制信号;
 - 所有机器人的急停装置应保持有效。

启动机器人进入自动操作状态前,应恢复暂停作用的安全防护装置的功效。

9 使用信息

9.1 使用说明书

使用说明书应满足 GB 11291.1—2011 第 6 章的规定,制造商应提供标志(如标记、符号)和使用说明书(如操作、维护手册)。

使用说明书的编制应满足 GB/T 42598 的要求。

9.2 培训

9.2.1 一般要求

使用机器人的用户应确保其编程、操作、维修人员参加安全培训,并获得胜任该工作的能力。培训宜与操作现场相结合。

9.2.2 培训的目标

培训的目的是要参加培训的人员了解到下列信息:

- a) 安全器件的用途和它们的功能;
- b) 专门涉及健康和安全的规程;
- c) 通过机器人的运行而形成的各种危险;

- d) 与特定的机器人有关的工作任务和用途；
- e) 安全的基本概念。

9.2.3 培训的要求

培训应满足以下要求：

- a) 学习适用的安全规程和机器人制造商的安全建议；
- b) 理解所安排的任务的明确含义；
- c) 掌握用于完成所指定的作业任务的所有控制装置及其功能的识别和说明如慢速控制、示教盒操作、急停步骤、切断步骤、单点控制等；
- d) 识别与作业有关的危险,包括辅助设备带来的危险；
- e) 识别安全防护措施,包括安全防护装置的类型、安全防护装置的能力或挑选方案、所选择的器件的功能、器件的功能测试方法、所选器件的限止性以及从识别危险开始的安全操作步骤、对人员的安全防护装备等；
- f) 掌握保证安全防护装置和联锁装置功能正常的测试方法。

9.2.4 再培训的要求

当系统变更,人员变化和事故发生以后,为了确保安全操作,应对相关人员重新进行安全培训。



附录 A

(资料性)

机器人风险评估示例

A.1 概述

本附录以焊接机器人为例,给出如何按照第 4 章的要求对机器人的危险进行风险评估,并给出了风险减小建议。

A.2 机器人的描述

该焊接机器人由接受专业人员的作业人员,每天 16 h 连续进行生产操作。正常生产时,作业人员无需进入。由于生产过程的需求,作业人员需要接近焊接机器人区域进行本体操作及维护,正常每 8 h 需要进入危险区域 4 次~6 次,每次 5 min。

A.3 危险识别

在机器人限定空间内,由于焊接机器人机构移动以及转台的前后移动,造成的作业人员上肢或身体的撞击或切割危险。

注:基于 GB 11291.1—2011 附录 A,本文件的附录 B 给出了典型工业机器人的主要危险表。

A.4 风险估计

A.4.1 选择的风险估计工具

危险识别后,通过 A.4.2 中的风险要素,对危险状态进行风险估计。

本示例选择 GB/T 16856—2015 中 6.3 给出的风险图法对危险进行风险估计。

A.4.2 风险要素的确定

A.4.2.1 伤害的严重程度(S)

伤害的严重程度分为:

- S1:轻微伤害(通常能恢复;例如:擦伤、裂伤、划伤等需要急救的轻伤等);
- S2:严重伤害[通常不能恢复,包括死亡;例如:肢体被切断、撕裂或挤压,骨折,需要缝线的严重伤害,严重的骨骼损伤(MST)等]。

在本示例中,机器人区域撞击风险,机器人工作范围内,作业人员在机器人的限定区域活动,误操作时,机器人有撞击到作业人员的风险,造成作业人员伤亡或者挤压伤残风险,工时损失超过 2 d。因此伤害的严重程度为 S2。

A.4.2.2 暴露于危险的频率和(或)持续时间(F)

暴露于危险的频率和(或)持续时间分为:

- F1:很少到经常和/或持续时间短的暴露(每个工作班次不超过 2 次或每个工作班次累积暴露时间不超过 15 min);
- F2:频繁到连续和/或持续时间长的暴露(每个工作班次超过 2 次或每个工作班次累积暴露时间超过 15 min)。

在本示例中,每个班次进入 4 次~6 次,每次 5 min,累积超过 15 min,作业人员产生风险的频率增

加。因此暴露于危险的频率和(或)持续时间为 F2。

A.4.2.3 危险事件发生的概率(O)

危险事件发生的概率分为：

- O1:低(不可能,可假定不可能发生:在安全应用方面得到证实和公认的成熟技术;坚固耐用);
- O2:中(可能有时发生:在最近 2 年内观察到的技术故障。由经过良好培训、知晓风险、岗位工作经验超过 6 个月的作业人员做出的不恰当操作);
- O3:高[可能频繁发生:经常观察到的技术故障(每 6 个月或更短)。由未经过培训、岗位工作经验不足 6 个月的作业人员做出的不恰当操作]。

在本示例中,机器人周围的安全产品功能部件未经功能安全认证,在 3 个月内出现过安全失效的记录;岗位作业人员班次变更频繁,并且新作业人员更换频率较快,作业人员出错的概率增加。因此危险事件发生的概率为 O2。

A.4.2.4 规避或减小伤害的可能性(A)

规避或减小伤害的可能性分为两类。

- 1) A1:在某些情况下可能:
 - 如果焊接机器人的运动速度小于或等于 250 mm/s,且暴露作业人员熟悉风险和危险状态或即将发生危险事件的迹象,作业人员也应能够察觉到危险状况并且能够做出反应;
 - 取决于特定条件(温度,噪声,人类工效学等)。
- 2) A2:不可能。

在本示例中,机器人速度快,危险区域覆盖较大,作业人员容易靠近机器人运动范围;安全装置触发机器人停止时有安全距离要求。因此规避或减小伤害的可能性为 A2。

A.4.2.5 风险等级确认

在图 A.1 中,每个节点代表一个风险参数,节点的每条分枝代表参数的一个等级(例如:轻微程度或严重程度)。

对于每个危险状态,每个参数都分配一个等级。在风险图上,路径从起点开始,然后在每个节点处依照所选择的等级沿着适当的分枝前行,最末的分枝指向与已选择的等级(分枝)组合相关的风险水平或风险值。最终的结果是一个定性的、用术语、数字或字母表示的风险水平或风险值,例如“低”“中”“高”,或 1~6,或 A~F。

注:更多信息见 GB/T 16856—2015。

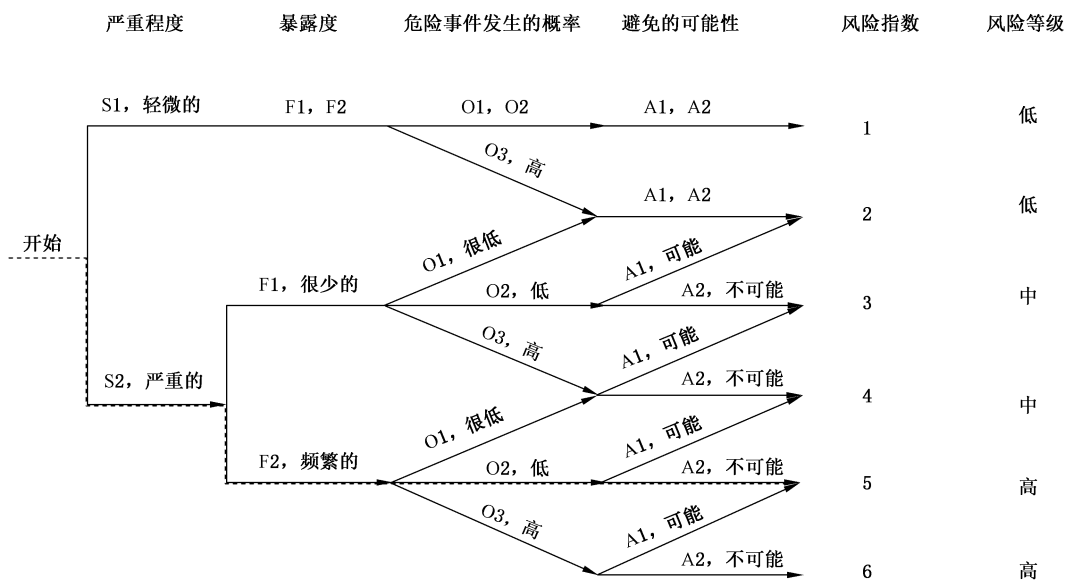


图 A.1 用于风险估计的风险图例

A.5 风险评价

由于焊接机器人机构上下移动产生对人员双手造成的挤压或卷入危险,最严重时可能造成作业人员死亡,并且作业人员在每 2 h 就会进入内部更换机器人的焊丝及清理,暴露在该风险之下。因此,在不使用任何防护措施的情况下,该风险的风险指数为 5,风险等级为高,是不可接受的。

A.6 风险减小措施

基于风险评估的结果,根据风险减小“三步法”按顺序采用以下多种风险减小措施。

- a) 第一步:本质安全设计措施
若作业人员在手动模式下进行调试时,确保焊接机器人的运动速度 $\leq 250\text{ mm/s}$ 。
- b) 第二步:安全防护措施/或补充保护措施
 - 焊接机器人本体周围采用围栏进行整体隔离,减小作业人员和机器人的直接接触;
 - 作业人员进入到机器人本体危险区域时,通过安装在安全门上的联锁装置使机器人立即停止;
 - 焊接机器人本体危险区域可通过区域扫描仪、AI 预警眼等存在检测装置,防止作业人员在危险区域作业时机器人被意外启动。若选择采取 SRP/CS 相关的措施,其 SRP/CS 安全等级应至少达到 SIL 2 或者 Cat3,PL d 的要求,见 5.4。
- c) 第三步:使用信息
该信息包括但不限于以下内容:
 - 加贴安全标识,提示机器人生命周期不同阶段剩余风险及的警告;
 - 操作说明和相关培训;
 - 管理措施(行政、法规类)。

A.7 采取风险减小措施后的风险评估

采取风险减小措施后,应针对识别出的风险再次进行安全评估,直达到可接受的风险程度。若作业人员进入焊接机器人工作区域,安全围栏的开口采用安全门开关,通过安全回路的控制,实

现焊接机器人停机,区域扫描仪或 AI 预警眼可判定区域内有作业人员,设备不能启动安全复位,此组合措施可减低暴露在危险区域的频率(F2 减小为 F1),以及危害发生的可能性(A2 减小到 A1),在 0 不变的情况下,该类风险达到可接受程度(风险指数为 2,风险等级为低)。

经风险分析的每个风险点应进行上述风险评估过程。



附录 B
(资料性)

典型工业机器人危险列表

本附录基于 GB 11291.1—2011 附录 A 的主要危险列表,以焊接机器人应用产生的危险状态和危险事件为例给出了主要危险表,见表 B.1。

表 B.1 主要危险表

危险分类	周期任务	危险区	事故场景	
			危险	危险事件
机械危险	示教、维护、设置、操作、5S 清洁、拆卸、包装、运输	机器人区域、限定空间	撞击	机器人手臂或附加轴的任一部件的运动(正常或奇异) 附加轴的运动
		机器人区域、限定空间	切割或切断	产生剪切动作的移动或旋转
		机器人区域、限定空间	缠结	腕部或附加轴的旋转
		机器人区域、与固定物体周围	拉入或陷进	机器人手臂和任何固定物体之间
		限定空间	压碎	机器人手臂或附加轴的任一部件的运动(正常或奇异); 机器人手臂和任何固定物体之间
		机器人区域、限定空间	挤压	维护期间释放制动装置手动解除抱闸,由于重力因素导致的额外危险; 拆除/移除/更换机器人的部件/组件和装置
		机器人区域	刺穿或刺破	接触机器人锐角、锐边和毛刺
		机器人区域	侧翻	运输时机器人姿态重心过高
		机器人区域	滑倒、绊倒或跌落	互联电缆等零部件造成的滑倒、绊倒危险
		电气控制柜、终端箱、机器上的控制面板	人与带电物件的接触(直接接触)	与带电部件或连接件的接触; 带电部件外露; 在故障条件下,变成带电部件
电气危险	示教、维护、设置、操作、5S 清洁		人与带电物件的间接接触	带电部件的绝缘失效或维修时接地连接失效所引起的间接接触伤害
		配电柜、机器人系统	电磁干扰	机器人柜内接线时可能会有静电风险
		机器人控制系统	着火	因过载、过电流、过电压或者不适当设计所造成线材或零部件燃烧着火
热危险	设定、运行	机器人系统	烧伤或烫伤	机器人在工作中温度超过人体所能承受的极限
		机器人系统	热源辐射引起的伤害	因不适当设计及电气外壳通风不良而引起的热辐射

表 B.1 主要危险表（续）

危险分类	周期任务	危险区	事故场景	
			危险	危险事件
噪声危险	设定、运行	操作区域	不适	电机或减速器异常工作产生的异响； 运动部件或不平衡的旋转部件； 当固定螺栓松动或密封件损坏是会产生异常噪音
人机工程学危险	示教、维护、设置、操作、5S清洁	示教盒	不健康的姿势或过度用力(反复用力)	不良设计的示教盒
		在装/卸工件和安装或设置工具处	对手臂或腿脚在解剖学上的考虑不足	控制装置的不合适位置
		位于或接近机器人单元处	手动控制装置的设计位置及标识不当	控制装置的无意操作
		位于或接近机器人单元处	视觉显示单元的设计或位置不当	对显示信息的误解； 示教器闪烁、炫光、阴影、频闪效应； 可视性-局部照明不足
意外启动、意外超限运动/超速	示教、维护、设置、操作、5S清洁	位于或接近机器人单元处	能源的故障/紊乱	对机器人附加轴的机械危害
		位于或接近机器人单元处	能源中断后的恢复	机器人或附加轴的意外运动
		位于或接近机器人单元处	对电气设备的外部影响	因电磁干扰,电控装置的不可预见行为
		位于或接近机器人单元处,其中机器人部件是通过应用电能或液压维持安全状态的	电源故障(外部电源)	因机器人手臂制动的释放引起的控制失效； 制动的释放导致机器人部件在残余力(惯性力、重力、弹性/储能装置)的作用下意外运动
		位于或接近机器人单元处	控制电路故障(硬件或软件)	机器人或附加轴的意外运动
		位于或接近机器人单元处	机器失稳或翻转	无约束的机器人或附加轴(它们靠重力保持其位置)跌落或翻倒
组合危险	设定、运行	限定空间	控制系统失效	不可靠的控制系统失效(非预期启动,非预期过度运作)； 电源失效及欠压导致过电流及不正当的操作
		限定空间	机器失稳或翻转	无约束的机器人或附加轴(它们靠重力保持其位置)跌落或翻到

参 考 文 献

- [1] 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
- [2] GB/T 16754 机械安全 急停功能 设计原则
- [3] GB/T 16856—2015 机械安全 风险评估 实施指南和方法举例
- [4] 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
- [5] GB/Z 43065.1—2023 机器人 工业机器人系统的安全设计 第1部分:末端执行器



