



中华人民共和国国家标准

GB 11291.2—2013/ISO 10218-2:2011
代替 GB 11291—1997

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

Robots and robotic devices—Safety requirements for industrial robots
—Part 2: Robot systems and integration

(ISO 10218-2:2011, IDT)

2013-12-17 发布

2014-11-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

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	2
4 危险识别和风险评估	4
4.1 通则	4
4.2 布局设计	4
4.3 风险评估	5
4.4 危险识别	6
4.5 消除危险和降低风险	7
5 安全要求和保护措施	7
5.1 通则	7
5.2 与安全相关的控制系统性能(硬件/软件)	7
5.3 设计和安装	8
5.4 机器人运动限制	11
5.5 布局	12
5.6 机器人系统操作方式的应用	14
5.7 示教盒	16
5.8 保养和维修	17
5.9 集成制造系统(IMS)接口	18
5.10 安全防护	19
5.11 协作机器人的操作	25
5.12 机器人系统的试运行	27
6 安全要求和保护措施的验证和确认	28
6.1 通则	28
6.2 验证与确认的方法	28
6.3 必需的验证与确认	29
6.4 保护设备的验证与确认	29
7 使用资料	29
7.1 通则	29
7.2 说明手册	30
7.3 标志	33
附录 A (资料性附录) 重大危险清单	34
附录 B (资料性附录) 与保护装置相关的各标准之间的关系	37
附录 C (资料性附录) 物料进出点的安全防护	38

附录 D (资料性附录) 多个使能装置的操作	41
附录 E (资料性附录) 协作机器人的概念应用	42
附录 F (资料性附录) 工序观测	43
附录 G (规范性附录) 安全要求和措施的验证方法	46
参考文献	57

前 言

本部分的全部技术内容为强制性。

GB 11291《机器人与机器人装备 工业机器人的安全要求》分为两个部分：

- 第1部分：机器人；
- 第2部分：机器人系统与集成。

本部分为GB 11291的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用翻译法等同采用国际标准ISO 10218-2:2011《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》(英文版)。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

- GB/T 3766—2001 液压系统通用技术条件(ISO 4413:1998, EQV)
- GB 5226.1—2008 机械安全 机械电气设备 第1部分：通用技术条件(IEC 60204-1:2005, IDT)
- GB/T 7932—2003 气动系统通用技术条件(ISO 4414:1998, IDT)
- GB/T 8196—2003 机械安全 防护装置 固定式和活动式防护装置设计与制造一般要求(ISO 14120:2002, MOD)
- GB 11291.1—2011 工业环境用机器人 安全要求 第1部分：机器人(ISO 10218-1:2006, IDT)
- GB/T 12644—2001 工业机器人 特性表示(ISO 9946:1999, EQV)
- GB/T 15706—2012 机械安全 设计通则 风险评估和降低风险(ISO 12100:2010, IDT)
- GB 16655—2008 机械安全 集成制造系统 基本要求(ISO 11161:2007, IDT)
- GB 16754—2008 机械安全 急停 设计原则(ISO 13850:2006, IDT)
- GB/T 16855.1—2008 机械安全 控制系统有关安全部件 第1部分：设计通则(ISO 13849-1:2006, IDT)
- GB/T 17454(所有部分) 机械安全 压敏保护装置[ISO 13856(所有部分)]
- GB 17888(所有部分) 机械安全 进入机械的固定设施[ISO 14122(所有部分)]
- GB/T 18831—2010 机械安全 带防护装置的联锁装置设计和选择原则(ISO 14119:1998, MOD)
- GB/T 19436.1—2004 机械安全 电敏防护装置 第1部分：一般要求和试验(IEC 61496-1:1997, IDT)
- GB/T 19670—2005 机械安全 防止意外启动(ISO 14118:2000, MOD)
- GB/T 19876—2012 机械安全 与人体部位接近速度相关防护设施的定位(ISO 13855:2010, IDT)
- GB 23821—2009 机械安全 防止上下肢触及危险区的安全距离(ISO 13857:2008, IDT)
- 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(IEC 62061:2005, IDT)

本部分的技术内容和组成结构与ISO 10218-2:2011《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》(英文版)相一致，只在需要的地方，做了下列编辑性修改：

- 大写的英文缩写保留英文原名；
- 删去了原文中不符合我国标准编写的字句。

本部分由中国机械工业联合会提出。

GB 11291.2—2013/ISO 10218-2:2011

本部分由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本部分起草单位:北京机械工业自动化研究所、北京航空航天大学、沈阳新松机器人自动化股份有限公司。

本部分主要起草人:杨书评、赖维德、王海丹、高雪芹、王思斯、邹凤山。

引 言

制定 GB 11291 的本部分是为了识别在工业机器人单元和生产线中集成和安装工业机器人系统时存在的特定危险。

对特定的机器人系统而言,危险是以单一形式频繁发生的。危险的数目和类型直接关系到自动化过程的性质和安装的复杂性。根据使用的机器人类型、使用机器人的目的、机器人安装、编程、操作和维护的方式的不同,这些危险导致的相关风险也有所不同。

为了理解 GB 11291 的本部分的要求,用一个词语语法来区分绝对要求和推荐做法或建议采取的行动。用“应”来识别 GB 11291 的本部分的必须要求。这些要求必须完成,除非提供替代说明或有风险评估确定的合适的替代。用“宜”来识别建议、推荐采取的行动或要求的可能解决方法,但可能有其他替代,建议采取的行动不是绝对的。

由于工业机器人在应用中的危险具有可变性质,GB 11291 的本部分为保证机器人集成和安装安全提供指导。由于工业机器人使用的安全性受特定机器人系统的设计影响,虽然同样重要,其补充目的是提供机器人系统和单元在设计、构造和使用信息方面的指导。该系统机器人部分的要求,可见 GB 11291.1。

提供安全的机器人系统或单元取决于各“利益相关方”的合作——“利益相关方”是指共担责任以提供安全工作环境为最终目的的实体。利益相关方可认定为制造商、供应商、集成者和用户(负责使用机器人的实体),但都以安全的(机器人)机器为共同目标。GB 11291 的本部分中的要求可能被分配给某利益相关方,但在相同要求下,会出现多类利益相关方职责重叠的情况。使用 GB 11291 的本部分时,请读者注意,即使没有在“被分配的”利益相关方任务中具体提出,所有确定的要求也可适用于这些相关方。

本部分是对仅涵盖机器人领域的 GB 11291 的第 1 部分的完善和补充。GB 11291 的本部分增加了符合 GB/T 15706 和 GB 16655 的其他信息。国际标准以 C 类标准的形式识别和响应工业机器人集成、安装中存在的特有危险和使用工业机器人的要求。新的技术要求包括(但并不仅限于):GB 11291.1 中关于安全控制系统性能、机器人停止功能、使能装置、程序验证、无缆示教盒规范、协作机器人规范以及安全更新设计方面内容的新要求实施说明。

GB 11291 的本部分和 GB 11291.1 组成了机器人和机器人设备的系列标准。其他标准涉及集成机器人系统、坐标系和轴运动、一般特性、性能规范及其测试方法、词汇和机械接口。需要指出的是这些标准不仅内在相关,并且与其他国际标准相关。

为了便于阅读 GB 11291 的本部分,“机器人”和“机器人系统”是指在 GB 11291 的第 1 部分中定义的“工业机器人”和“工业机器人系统”。

图 1 描述了在机器人系统中使用的机械标准范围的关系。GB 11291 的第 1 部分中只涵盖机器人的内容,GB 11291 的本部分涵盖系统和单元。机器人单元可包括其他机器,这些机器有自己的 C 类标准,机器人系统可以成为 GB 16655 涵盖的集成制造系统的部分,GB 16655 反过来也可以参考其他相关的 B 类和 C 类标准。

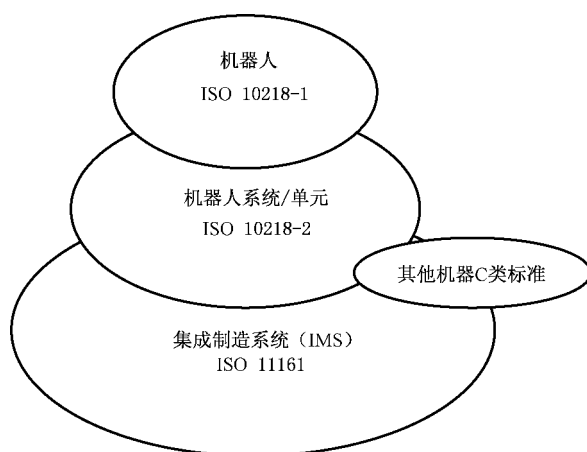


图 1 各标准间关系示意图

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

1 范围

GB 11291 的本部分规定了工业机器人、工业机器人系统和工业机器人单元集成的安全要求,工业机器人和工业机器人系统已在 GB 11291.1 中定义。集成包括以下方面:

- a) 工业机器人系统或单元的设计、制造、安装、运行、维护和报废;
- b) 工业机器人系统或单元的设计、制造、安装、运行、维护和报废的必要资料;
- c) 工业机器人系统或单元的部件设备。

本部分描述了与这些系统有关的基本危险和危险情况,并提出了消除和充分降低与这些危险相关的风险的要求。虽然噪声被定为是工业机器人的一种主要危险,但是本部分不予考虑。本部分也规定了对作为集成制造系统的部分的工业机器人系统的要求。本部分不专门涉及关于加工过程中的危险(如激光辐射、弹出碎片、焊接烟雾)。其他标准适用于这些加工过程中的危险。

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/T 16855.1—2008 机械安全 控制系统有关安全部件 第1部分:设计通则(ISO 13849-1:2006, IDT)

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(IEC 62061:2005, IDT)

ISO 4413 液压系统通用技术条件(Hydraulic fluid power—General rules and safety requirements for systems and their components)

ISO 4414 气动系统通用技术条件(Pneumatic fluid power—General rules and safety requirements for systems and their components)

ISO 8995-1 工作场所的照明 第1部分:室内(Lighting of work places—Part 1: Indoor)

ISO 9946 工业机器人 特性表示(Manipulating industrial robots—Presentation of characteristics)

ISO 10218-1 工业环境用机器人 安全要求 第1部分:机器人(Robots and robotic devices—Safety requirements—Part 1: Industrial robots)

ISO 11161 机械安全 集成制造系统 基本要求(Safety of machinery—Integrated manufacturing systems—Basic requirements)

ISO 12100 机械安全 设计通则 风险评估和降低风险(Safety of machinery—General principles for design—Risk assessment and risk reduction)

ISO 13850 机械安全 急停 设计原则(Safety of machinery—Emergency stop—Principles for design)

ISO 13854 机械安全 避免人体各部位挤压的最小间距(Safety of machinery—Minimum gaps to avoid crushing of parts of the human body)

ISO 13855 机械安全 与人体部位接近速度相关防护设施的定位(Safety of machinery—Positioning of safeguards with respect to the approach speeds of parts of the human body)

ISO 13856(所有部分) 机械安全 压敏保护装置(Safety of machinery—Pressure-sensitive protective devices)

ISO 13857 机械安全 防止上下肢触及危险区的安全距离(Safety of machinery—Safety distances to prevent hazard zones being reached by upper and lower limbs)

ISO 14118 机械安全 防止意外启动(Safety of machinery—Prevention of unexpected start-up)

ISO 14119 机械安全 带防护装置的联锁装置 设计和选择原则(Safety of machinery—Interlocking devices associated with guards—Principles for design and selection)

ISO 14120 机械安全 防护装置 固定式和活动式防护装置设计与制造一般要求(Safety of machinery—Guards—General requirements for the design and construction of fixed and movable guards)

ISO 14122(所有部分) 机械安全 进入机械的固定设施(Safety of machinery—Permanent means of access to machinery)

IEC 60204-1 机械安全 机械电气设备 第1部分:通用技术条件(Safety of machinery—Electrical equipment of machines—Part 1: General requirements)

IEC 61496-1 机械安全 电敏防护装置 第1部分:一般要求和试验(Safety of machinery—Electro-sensitive protective equipment—Part 1: General requirements and tests)

IEC 61800-5-2 调速电气传动系统 第5-2部分:安全要求 功能性(Adjustable speed electrical power drive systems—Part 5-2: Safety requirements—Functional)

IEC/TS 62046 机械安全 人体检测用防护设备的应用(Safety of machinery—Application of protective equipment to detect the presence of persons)

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用 application

机器人系统的预期使用,即机器人系统的加工工艺、任务和预期目的。

示例:点焊、喷漆、装配、码垛。

3.2

协作机器人 collaborative robot

在规定的协作工作空间(3.3)内,为与人直接交互而设计的机器人。

3.3

协作工作空间 collaborative workspace

在安全防护空间内,机器人与人在生产活动中可同时执行任务的工作空间。

3.4

控制站 control station

机器人系统的部分,包括一个或多个控制装置,用以激活或停止系统或系统部件的功能。

注:控制站可以是固定式的(如控制面板)或移动式的(如控制示教盒)。

3.5

远距离防护 distance guard

防护不是完全围住危险区域,而是借助于它的尺寸和它到危险区域的距离来防止或减少进入。

示例:周边护栏或隧道护卫设施。

3.6

集成 integration

将机器人和其他设备或另外的机器(含其他机器人)组合成能完成如零部件生产的有益工作的机器系统。

注：这种机器构建包括系统的安装要求。

3.7

集成者 integrator

设计、提供、制造或组装机器人系统、集成制造系统的实体,该实体负责安全策略,包括保护装置、控制接口以及控制系统的互连。

注：集成者可以是制造商、组装人员、工程公司或用户。

3.8

集成制造系统 integrated manufacturing system; IMS

为了制造、处理、移动或包装零部件或组件,由原材料处理系统连接,并由控制器(即 IMS 控制器)实现互连,采用协同方式工作的一组机器。

[GB 16655—2008,定义 3.1]

3.9

工业机器人单元 industrial robot cell

包含相关的机器和设备以及相关的安全防护空间和保护装置的一个或多个机器人系统。

3.10

工业机器人生产线 industrial robot line

由在单独或相连的安全防护空间内执行相同或不同功能的多个机器人单元和相关设备构成。

3.11

安全状态 safe state

机器或设备部件不存在即将发生的危险状态。

3.12

联动 simultaneous motion

在单个控制站的控制下,两台或多台机器人同时运动。它们可以用共有的数学关系实现协调或同步。

3.13

空间 space

三维容积。

3.13.1

操作空间 operating space, operational space

当实施由任务程序指令的所有运动时,实际用到的那部分限定空间(3.13.2)。

[GB/T 12643—2013,定义 4.8.3]

3.13.2

限定空间 restricted space

由限位装置限制的最大空间中不可超出的部分。

[GB/T 12643—2013,定义 4.8.2]

3.13.3

安全防护空间 safeguarded space

由周边安全防护装置确定的空间。

3.14

确认 validation

通过检验和提供客观证据,对特定的预期用途所需的特殊要求已得到满足。

3.15

验证 verification

通过检验和提供客观证据,对规定要求已得到满足的认定。

4 危险识别和风险评估

4.1 通则

4.1.1 机器人的运行特点与其他机器和设备的运行特点有明显的不同之处:

- a) 机器人能够在大操作空间进行高能量运动;
- b) 例如由于改变了操作要求,机器人手臂的初始运动和路径不确定,且可以改变;
- c) 机器人的操作空间,可能会和其他机器人操作空间或其他机器和相关设备的工作区发生部分重叠;
- d) 当机器的致动器通电时,可能要求操作员贴近机器人系统进行工作。

4.1.2 在选择和设计适当的安全防护措施以充分降低风险之前,有必要确定危险,并评估与机器人及其应用相关的风险。降低风险的技术措施有以下几项基本原则:

- a) 通过设计消除危险或通过替代减少危险;
- b) 防止操作员接触危险或在操作员接触危险之前控制危险到达安全状态;
- c) 在干预期间降低风险(例如:示教)。

4.1.3 实现这些原则包括:

- a) 设计允许在安全防护空间外执行任务的机器人系统;
- b) 创造安全防护空间和限定空间;
- c) 在安全防护空间内需要干预时,提供其他安全防护。

4.1.4 这种类型机器人的应用及其与其他机器及相关设备的关联,将影响安全防护措施的设计和选择。这些应符合当前的工作,并当需要时可使示教、设置、维护、程序验证和故障排除等操作安全地进行。

4.2 布局设计

机器人系统和单元的布局设计是消除危险和降低风险的关键环节。在布局设计过程中应考虑以下因素:

- a) 建立单元或生产线的物理极限(三维),包括更大单元或系统(集成制造系统)的其他部件:
 - 1) 在设计图纸上确定布局的比例和原点;
 - 2) 在现有的设施内(按比例)确定各部件的位置和尺寸。
- b) 工作空间、通道和间隙:
 - 1) 确定机器人系统的最大空间,建立限定空间和操作空间,确定如厂房支柱的障碍物周围所需间隙;
 - 2) 通行路线(行人通道、访客路线、单元或生产线周边安全防护装置外的物料搬运);
 - 3) 支持设施(电气、燃气、水、真空、液压、通风设备)和控制系统的通道和安全路径;
 - 4) 检修、清洁、故障排除和维护的通道和安全路径;
 - 5) 电缆/其他致使滑倒、绊倒和摔倒的危险因素;
 - 6) 电缆桥架。

c) 人工干预——布局设计宜允许在安全空间外执行要求人工干预的任务,如果上述不可行并且干预时需要机器的带电运动,应提供合适的使能装置,使能装置设计成可以控制:

- 1) 整个机器人单元;
- 2) 机器人单元中的一个区域;
- 3) 单元内选定的机器或设备。

注:更多内容见 ISO 12100。

d) 设备的人体工程学和人机界面:

- 1) 操作的可视性;
- 2) 控制装置的清晰度;
- 3) 控制装置与机器人的明确结合;
- 4) 区域控制设计的惯例;
- 5) 工件相对于操作员的位置;
- 6) 可预见的误用;
- 7) 协作操作。

e) 环境条件:

- 1) 通风;
- 2) 焊接火花。

f) 工件/工具更换的装载与卸载。

g) 周边安全防护的考虑。

h) 急停装置和单元可能区域的位置和要求(例如:局部停止或全单元停止)。

i) 使能装置的位置和要求。

j) 注意所有部件的预期用途。

风险评估应该确定超出限定空间的其他所需空间,以划定安全防护空间。

4.3 风险评估

4.3.1 通则

由于机器人系统始终是集成到一个特定的应用中,因此集成者应进行风险评估,以确定降低风险的措施,这些措施要能充分降低集成应用中存在的风险。需要特别注意的例子是:为了实现集成应用,个别机器去除了安全防护的情况。

风险评估可以进行系统性分析和对与机器人系统相关的、整个生命周期(即试运行、调整、生产、维护、检修、报废)的风险进行评估。

每逢需要时,风险评估后就采取措施降低风险。重复此过程是通过实施保护措施尽量消除危险与减少风险的迭代过程。

风险评估包括:

- a) 确定机器人系统的限制(见 4.3.2);
- b) 危险识别(见 4.4);
- c) 风险估计;
- d) 风险评价。

4.3.2 机器人系统的限制

机器人系统的集成,首先在 ISO 12100,ISO 11161 以及其他适用的 C 类标准中描述了其预期用途规范和限制。该规范宜包括,例如:

- a) 使用限制：
 - 1) 功能、预期用途以及合理可预见的误用的描述；
 - 2) 不同用户模式的描述；
 - 3) 包括人工干预的过程序列的分析；
 - 4) 接口、工具和设备的描述；

注 1: 建议对这些装置应考虑到相关的 C 类标准。

- 5) 实用连接；
 - 6) 制造商提供的从 ISO 10218-1 的使用中得到的信息,包括降低风险的应用措施；
 - 7) 所需的电力供应及其设备；
 - 8) 要求的或预计的用户的技能(能力)。
- b) 空间限制(见 5.5 布局描述):
 - 1) 机器运动所需范围；
 - 2) 安装和维护所需空间；
 - 3) 操作员作业和其他人工干预所需空间；
 - 4) 重构能力(ISO 11161)；
 - 5) 所需通道(见 5.5.2)；
 - 6) 地基；
 - 7) 供给和废物排放装置或设备所需空间。
- c) 时间限制：
 - 1) 机器及其部件(易磨损件,工具等)的预期寿命限制；
 - 2) 工艺流程图和时间分配；
 - 3) 推荐的检修间隔。
- d) 其他限制：
 - 1) 环境(温度,室内或室外使用,灰尘和湿气的耐受性等)；
 - 2) 预期用途和环境所需的清洁程度；
 - 3) 加工物料的性能；
 - 4) 危险环境；
 - 5) 经验教训,即研究和比较,包括类似操作和系统可能的意外和事故报告。

注 2: 其他国家标准和地方法规也可提供动力源和安全处理及安装要求的重要信息。

4.4 危险识别

4.4.1 通则

附录 A 中机器人和机器人系统的主要危险列表是按照 ISO 12100 的描述进行危险识别和风险评估的成果。

特定的应用(例如焊接、激光切割和加工)和机器人系统与其他机器相互作用(例如挤压、剪切和冲击)可以造成进一步的危险(例如烟雾、气体、化学物质和热物质)。这些危险应该列为特定应用风险评估的个别依据。

4.4.2 任务识别

为了确定可能发生的危险情况,有必要识别机器人系统及其相关设备的操作员要执行的任务。集成者应识别和记录这些任务。应咨询用户,以保证能识别与机器人单元相关的所有合理可预见的危险情况(任务和危险组合),包括间接的相互作用(例如,与系统任务无关,但会暴露于与系统相关的危险中的人员)。这些任务包括(但不限于):

- a) 过程控制和监测；
- b) 工件装载；
- c) 编程和验证；
- d) 无需解除的操作员简短干预；
- e) 装配(例如:夹具更换、工具更换)；
- f) 故障诊断；
- g) 故障排除(例如:设备堵塞、部件跌落、事件恢复、异常情况)；
- h) 控制危险能量(包括夹具、夹钳、转台和其他设备)；
- i) 维护和修理；
- j) 设备清洗。

4.5 消除危险和降低风险

识别危险后,有必要在采用适当措施前,评估与机器人系统相关的风险,以充分降低风险。降低风险的措施基于以下基本原则:

- a) 通过设计消除危险或通过替代降低其风险；
- b) 通过安全防护措施防止操作员接触危险,或在操作员接触危险之前确保危险降至安全状态；
- c) 提供诸如使用资料、培训、标记、人员保护设备等补充性保护措施。

包含于第 5 章的要求来源于:根据 ISO 12100 对附录 A 中识别的危险用降低风险措施反复处理。集成者应确保按照第 5 章的要求充分降低风险评估中识别的风险。如果没有充分降低风险,应进一步采取降低风险的措施,直到风险被充分降低。

5 安全要求和保护措施

5.1 通则

机器人系统和单元的集成,应符合本部分的要求。此外,机器人单元或机器人生产线应根据 ISO 12100 的相关危险的原则来设计,所述危险在本部分未专门涉及(例如锋利边缘)。机器人系统的设计宜按照人体工程学原则,确保易操作和易维护。机器人系统的设计应避免人员暴露于危险中。

注 1:并非本部分确定的所有危险适用于每个机器人系统,各机器人系统之间,与给定危险情况相关的风险水平也不相同。

注 2:第 6 章是本条款各项要求的推荐验证方法。

5.2 与安全相关的控制系统性能(硬件/软件)

5.2.1 通则

与安全相关的控制系统(电气、液压、气动和软件)至少应满足 5.2.2 所列的性能准则,除非风险评估的结果确定一种替代的性能准则(如 5.2.3 所述)适用。在使用资料中,应清楚地说明机器人系统和任何供给设备的与安全相关的控制系统性能。

注 1:与安全相关的控制系统也可称为 SRP/CS(控制系统的与相关安全的部件)。

对于本部分,与安全相关的控制系统性能表述为:

- 性能等级(PL)和类别,如 GB/T 16855.1—2008 中 4.5.1 所述；
- 安全完整性等级(SIL)和硬件容错要求,如 GB 28526—2012 中 5.2.4 所述。

这两项标准以类似的但不同的方法述及功能安全。这些标准的要求应被应用于预期使用的各个与安全相关的控制系统中。设计者可以选用两个标准中的一个。使用资料中应包括确定与安全相关的控

制系统性能的必要数据和准则。

注 2: 与 GB/T 16855.1 和 IEC 62061 的比较,在 ISO/TR 23849 中进行描述。

其他标准提供可供选择的性能要求,如北美的“控制可靠性”条款也可使用。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。

根据 IEC 60204-1,与安全相关的控制系统的任何失效应导致 0 类或 1 类的停止。

5.2.2 性能要求

控制系统有关安全部件的设计,应遵照 GB/T 16855.1—2008 所描述的 PL=d、结构类别 3,或遵照
GB 28526—2012 所描述的 SIL2、硬件 1 级容错,验证测试间隔不少于 20 年。

这里特别是指:

- a) 任何部件的单一故障不会导致安全功能的丧失;
- b) 只要合理可行,在有关安全功能的下一个指令发出时或发出前,应检测出单一故障;
- c) 当发生单一故障时,安全功能始终有效,且应维持安全状态直到故障排除;
- d) 应检测到所有可合理预见的故障。

这些要求相当于 GB/T 16855.1—2008 中所描述的结构类别 3。

注:检测单一故障的这种要求并不意味着所有故障都将被检测到。因此,未检测到故障的累积,可能导致意外输出
信号和使机器处于危险状态。

5.2.3 其他控制系统性能准则

对机器人系统及其预期应用进行综合风险评估的结果,可确定与安全相关的控制系统的性能,除
5.2.2所述之外,是能保证该应用的。

应特别指出选择了这些与安全相关的性能准则中的哪一个,并且与受影响设备一起提供的使用资
料中,应包括适当的限制和警告信息。

5.3 设计和安装

5.3.1 环境条件

机器人系统和机器人单元保护措施的设计应考虑到如周围温度、湿度、电磁干扰、照明等环境条件。
由于技术限制,这些可能导致对周围环境的某些要求。

选择的机器人、机器人系统和单元部件应能承受预期的运行条件和环境条件。

5.3.2 控制器位置

在自动操作时,控制器和设备(例如:焊接控制器、气动阀门等)应放置在安全防护空间外,使人员能
清晰看到机器人限定空间并进行控制。

5.3.3 致动控制器

致动控制器应满足 IEC 60204-1 的要求。控制器的设计应符合 ISO 10218-1。机器人系统不应响
应任何可能会造成危险情况的或外部远程命令。

5.3.4 动力要求

机器人和其他设备所有动力源(例如:气动、液压、机械、电力动力源)应满足机器和部件的制造商所
规定的要求。电源装置应符合 IEC 60204-1 中的要求,液压动力装置应满足 ISO 4413 中的要求,气压
动力装置应满足 ISO 4414 中的要求。

5.3.5 等电位联结/接地要求(接地)

保护联结和功能联结应符合 IEC 60204-1 的要求。

5.3.6 能源隔绝

应提供隔绝有害能源、避免人员暴露于危险的方法。这些方法应仅在断开能源的位置是保险和/或安全的。

机器人系统的每种能源宜有单独的切断装置。多机器人或大型设备,每种能源有必要有多个切断装置。每个装置的控制范围应在断开装置的把手旁清晰标出(例如文字或符号)。

注:能源可以是电气的、机械的、液压的、气动的、化学的、热学的、势能的和动能的等。

5.3.7 储能控制

应提供控制和/或受控地释放储存的危险能量的方法。应贴上标签以识别储能的危险。

注1:储存能源可以是气压蓄压器或液压蓄压器、电容器、电池、弹簧、平衡块、飞轮和重力等。

注2:悬臂轴造成的重大危险取决于频率和持续暴露时间(例如:在安装的时候站在机器人手臂的下方)。可行的是设计出机械阻隔系统或手持控制系统以保护暴露于危险的储能环境中的人员,该系统具有如风险评估确定的、根据 5.2.2 或 5.2.3 设计的控制性能。

5.3.8 机器人系统和单元的停止功能

5.3.8.1 通则

每个机器人系统或单元都应具有保护性停止功能和独立的急停功能。各功能应具有与其他保护装置或急停装置连接的能力。

5.3.8.2 急停功能

按照 IEC 60204-1 和 ISO 13850 的要求,每个能启动运动或其他危险功能的控制站都应有手动启动的急停功能。

致动急停功能应停止单元内的或单元与工作空间其他区域之间接口处的所有机器人运动和其他危险功能。

机器人系统应有影响系统所有相关部件的单独的急停功能。就大型系统而言(如多机器人或多单元),有必要分割控制范围。在这样的情况下,应通过执行任务的要求或系统性能(如设备结构,周边防护的位置)来设置控制范围。控制范围应在急停装置旁清晰标出(如文字或符号)。

如果两个或多个机器人的限定空间发生部分重叠,或如果两个或多个机器人可进入同一安全防护空间,那么该空间应该是同一工作空间。一个工作空间的所有急停装置应具有相同的控制范围。

控制范围可包括多个工作空间。使用资料应包括每个急停装置控制范围的信息。

即使控制站不工作,机器人系统的急停功能也应保持有效。

根据 IEC 60204-1,选择 0 类或 1 类的停止功能应通过风险评估确定。

急停功能至少应符合 5.2.2 的要求,除非风险评估确定其他性能准则适用。

注:某些保护性停止电路会以手动方式自动旁路,不适合连接急停装置。

提供急停输出信号时:

- 撤除机器人系统动力后,输出应一直有效;
- 如果撤除机器人系统动力后输出无效,应产生一个急停信号。

5.3.8.3 保护性停止

机器人系统应设计有一个或多个的保护性停止电路,可用来连接外部保护装置。按照 IEC 60204-1,

0类或1类停止的选择应通过风险评估确定。

如果外部动力驱动系统符合 IEC 61800-5-2,可用 2类停止。

这个保护性停止功能应能使所有机器人系统的运动停止,并且导致终止由机器人系统控制的其他任何危险功能。这个停止可由手动或控制逻辑启动。

保护性停止功能的性能应符合 5.2.2 或 5.2.3 的要求。

5.3.9 相关设备的关闭

机器人系统应安装成相关设备的关闭不会造成危害或危险情况。

5.3.10 末端执行器(机械臂工具端)要求

末端执行器应设计和构造成:

- a) 能源供应(如电力、液压、气动、真空的动力)的损失或变化不会导致负载释放,否则会造成危险情况;
- b) 负载和末端执行器共同产生的静态和动态力都在负载容量和机器人动态响应范围之内;
- c) 手腕板(安装法兰)及配件正确对齐(耦合);
- d) 使用时可拆卸工具被牢固连接;
- e) 如果可拆卸工具的释放可能导致危险状况,那么只有在指定位置或者在特定的可控条件下,才允许可拆卸工具被释放;
- f) 末端执行器在其预期寿命内承受预期力。

如果可行,能源可以不给机器人致动器输出原动力,只输出给末端执行器以排除故障。

注:该特性是机器人制造商提供的一个有用的选择,并不是 ISO 10218-1 中的要求。

在正常操作的预定参数基础上,如果末端执行器故障导致潜在危险状况,使用资料应该包括末端执行器的预期寿命。

机器人系统操作之前,机器人工具中心点(TCP)应使用机器人制造商提供的位置补偿特性进行调整。应提供避免危险状况的措施(例如:机械保护用的气动或真空软管;诸如弹簧加载的附加夹具的自固位装置)。

5.3.11 紧急恢复过程

使用资料应包括机器人系统相关设备故障矫正的详细说明,以及机器人制造商关于机器人在紧急或异常情况下无需驱动源就能运动的说明。如果需要标志或标签,应粘贴标志或标签或提供粘贴的说明。

5.3.12 警告标志

当机器人或系统其他设备部分的警告标志由于安装或集成变得模糊时,提供其他同等有效的警告方法(例如将另一个警告标志放在可见位置)。

5.3.13 照明

应确定所需任务的照明水平,并在使用资料中详细说明。

应为机器人系统提供适合于有关操作的整体照明,否则,尽管有正常亮度的环境照明,也可能造成一定风险。机器人系统的设计和构造应避免可能造成麻烦的阴影区,避免刺目耀眼强光以及由于照明使运动部件产生危险的频闪效应。应为需要经常检查调整的内部零部件和维修区域提供适当的照明。应经常检查和调整的区域,照明度应至少为 500 lx(见 ISO 8995-1)。

注:需要考虑照明的区域包括工作站、进入区等。

5.3.14 应用危险

机器人系统的集成也应考虑到与工艺和工具(例如焊接、激光切割和机械加工)相关的应用危险(例如烟雾、气体、化学物品和热物质)。

与其他机器接口的要求应如使用资料中规定的,遵循制造商的指导。

5.3.15 使能装置

示教盒和其他的使能装置以及它们的集成应符合 ISO 10218-1(其他信息见附录 D)。

如果要求安全空间内多人受保护,应给每个人都提供使能装置。与单个机器人控制器关联的所有使能装置应具有相同的功能(控制范围)。

控制系统应联锁,这样可以使使能装置控制单元区域内的所有危险,否则在手动操作过程中,人员可能暴露于危险情况下(例如当在辅助设备上或其他机器人上工作时,站在相邻机器人的限定空间内就会有重叠的限定空间)。

在被使能装置控制(停止)后,联锁的、危险的机器人功能将要求有一个独立动作去重启。

注 1: 联锁使能装置的控制范围取决于布局、空间、预期任务和这些任务预期的工作位置。遵循 5.2.2,设计控制措施来防止在手动操作中同时激活,重叠的机器人。

注 2: 工序监测见附录 F。

5.4 机器人运动限制

5.4.1 通则

机器人设备的设计和集成,应减少人员可能暴露于危险中的情况。机器人系统可具有潜在的大操作容积(最大空间),尤其是处理大工件时。放置周边防护装置以最大尺寸防护人员免遭机器人系统带来的危险(安全防护空间),可能导致不必要的大容积围护结构,它超出了机器人执行任务所需空间(操作空间)。为缩减安全防护空间,可通过提供集成或限制机器人系统运动的外部装置,以限制最大空间(限定空间)。

5.4.2 建立安全防护空间和限定空间

应通过周边防护来建立安全防护空间。建立安全防护空间应充分考虑机器的位置和布局以及安全防护空间内的危险。

机器人系统的限定空间应通过限制机器人、末端执行器、夹具和工件的运动来建立。限定空间宜比最大空间小。限定空间在安全防护空间内并与操作空间尽可能匹配,这是合理可行的。

周边防护装置不应安装在比限定空间更接近危险的地方,如果按照 5.4.3 把周边防护装置设计为限位装置,那么周边防护装置要为安全防护空间和限定空间建立一段边界。

操作员工作站(如部件加载位置)可能需要额外的保护。动态限制(见 5.4.4)、联锁安全防护以及其他安全防护可用于保证操作员在工作站不会暴露于危险中。

5.4.3 限制运动的方法

限制机器人系统的运动可以通过对机器人必不可少的方法(如制造商提供的轴及空间的安全软限位或机械限位)来实现,也可以通过安装外部限位装置或两者结合来实现。限制方法用于限制机器人执行任务的空间,即是通过使用限位装置使得限定空间比最大空间小。

限位装置分为两类:机械式限位装置和非机械式限位装置。机械式的物理上约束机器人不超出指定的界限。非机械式的没有限制机器人本身的运动,而是通过机器人控制器系统启动停止。因此,非机械式限位装置要求集成者在建立机器人限定空间时,要考虑机器人停止距离。

任何连接到机器人控制器的与安全相关的控制器都应该满足 ISO 10218-1 的要求。

应正确调整和固定限位装置。当设计所需的限制运动范围的方法时,应遵循以下要求之一:

——如果提供机械式停止,应满足 ISO 10218-1 中限位装置的要求,并且当适用时,也要满足 ISO 10218-1 中动态限位装置的要求。

——如果提供限制运动范围的替换方法,它们的设计、构造和安装至少应满足 ISO 10218-1 中轴限制的要求。这些方法至少应符合 5.2.2 的要求,除非风险评估确定其他性能准则适用。与限制方式有关的停止距离应包含于限定空间的所有计算中。停止时间和距离的信息和度量见 ISO 10218-1。

当使用非机械式限位装置时,包括轴及空间的安全软限位(见 ISO 10218-1),限定空间应根据机器人的实际负载确定。如果机器人速度由满足 5.2.2 的监控系统控制,限定空间可根据配置速度限制来确定。否则,限定空间应根据机器人最大速度来确定。

如果按照机器人制造商的说明使用机器人内置的轴及空间的安全软限位特性,有关利用该方法建立的程序设定限制的信息应包括在使用资料中。

在把周边防护装置设计为限位装置情况下,将用风险评估的结果来确定该防护装置的设计要求、强度要求和挠度要求。

注 1: 对根据实际负载来补偿速度的机器人,当机器人承担的负载比额定负载低的时候,最容易发生状况。

注 2: 限定空间定义为机器人运动实际停止处,而非启动停止处。可通过机械式限位装置(如硬挡块)的位置来明确地加以确定。非机械式限位装置的位置,要求考虑激活时间和机器人停止距离。这包括轴和空间的安全软限位配置。

注 3: 设计用于保护机器的一些装置(如过流保护和碰撞传感器),不适合用作限位装置,除非是符合 ISO 10218-1,经过特别设计、测试并且确定为适合作为限制运动用途的安全装置。

注 4: 只有当机器人不能导致防护装置发生危险变形时,通常周边防护装置作为限位装置才是可行的。

5.4.4 动态限制

动态限制是在机器人系统一段周期中,机器人系统的限定空间发生的自动受控改变。当机器人执行其任务程序时,可利用控制装置进一步限制限定空间内的机器人运动,控制装置例如是(但不限于)凸轮操纵的限位开关、光幕或控制激活的可缩回的机械限位器。为此,机械式限位装置应能在额定负载和额定速度的条件下,停止机器人运动。相关的与安全有关的控制系统应符合 5.2 的性能要求。

使用资料中应有确定动态限制区域的位置的信息。对于非机械式限位装置,应包括启动停止的区域边界和机器人实际停止的区域(限定空间)。

注: 通过一个机器人服务于两个工作站的方式,动态限制可被用于设计两个可交替选择的限定空间,以提高工作单元生产率。

5.5 布局

5.5.1 周边安全防护

根据 5.10,周边安全防护措施应通过使用防护装置或传感保护设备来实现。保护装置的选择应考虑以下方面:

——预期的运行压力;

——被加工物料的影响,特别是给机器人系统上下料;

——其他相关的外部影响(如很脏的空气妨碍光电保护装置的使用)。

越过或通过机械式防护的安全距离应满足 ISO 13857 的要求。距连锁防护装置及其他断开装置的最小距离应满足 ISO 13855 的要求。通过保持最小间隙来避免挤压的地方应满足 ISO 13854 的要求。

5.5.2 干预通道

安装机器人系统时,应对特殊安装和预期任务进行基于任务的风险评估,以确定机器人限定空间内

可能的被困点和被夹点。

需要使用手动高速方式的任务,提供的最小间隙应为 0.5m。要求该间隙处于算出的危险停止位置与建筑物、结构物、周边防护装置、公共设施区域之间,其他机器和设备不会特别支持可能造成被困点或被夹点的机器人功能(见 ISO 13854)。

示例:机器人功能的支持部分可包括夹具、上料站、物料处理设备和加工相关设备。

只要可行,布局的设计应使操作员在安全空间外执行任务。有必要在安全空间内执行任务时,应具有安全的、充分的到达任务位置的通道。进入路径和方式应使操作员不会暴露于危险,包括滑倒、绊倒或摔倒等危险。

安全防护空间内的通道设计应考虑,如:

- 电缆槽,容易绊倒的区域;
- 人工上下料所需进入的频率;
- 负载的物理特性;
- 逗留和观察区域;
- 服务位置(如终点改变);
- 易进入的维护单元(如安全区域之外)。

应提供永久性通道装置,同时考虑任务的频率和人机工程学方面内容。

控制器(如示教盒、机器人控制柜)宜放置在靠近通道装置的地方,以提高操作员的操作便利性。当需要靠近的、装有元件的电气设备(如例行维修服务)安装得正常到达平面之上时(如机器顶部),应提供接近方法(如工作平台)。应使用风险评估的结果来确定适当的方法,给距离通道平面 0.4 m 到 2.0 m 高度的相关装置提供通道(见 IEC 60204-1)。

电气罩的安装应使门可以完全打开,即使在门打开的时候逃生通路也要总是可用。以下情况时,可满足以上要求:

- a) 考虑到逃生方向,门容易推至关闭位置。
- b) 当门完全打开的时候,余留间隙不少于 500 mm(也见 IEC 60364-7-729)。

平台、通道、楼梯、活梯和固定梯子的选择与设计应符合 ISO 14122 的相关部分。

应提供安全防护措施,防止单元之间有操作员进入,或在操作员接触之前使相邻单元中的危险转变为安全状态。

应提供安全防护措施来降低由于物料在相邻单元之间的进出转移而产生的对操作员的危险。

5.5.3 物料搬运

在风险评估中,应考虑到与物料搬运相关的危险(如缠结、物料跌落以及与机器人系统的连接)。

物料进入或退出安全空间的地方,应采取措施以阻止未检测到的人员进入危险区域。这些措施应阻止人员接触危险,或在不造成其他危险的情况下、接触危险之前,使危险转变为安全状态。开口宜减小至物料可以通过所需的最小尺寸(见 5.10.7)。

5.5.4 工序观测

工序观测宜在安全防护空间外进行。按照风险评估确定的结果,可通过提供安全站位和观测位置(如平台、狭窄过道、远程视觉系统)来实现。

当工序观测只能在安全防护空间内进行时,应使用 5.6.4.2 和 5.6.4.3 规定的操作方式。当这些方式不能使用时,应提供单独控制方式。该方式应提供必要的安全防护措施以保证操作员在进行工序观测时不会处于危险状况。更多信息可参照附录 F。

5.6 机器人系统操作方式的应用

5.6.1 通则

一个单元内有多个机器人系统时,单元内每个机器人系统可分别选择操作方式,或所有相关机器人系统选择共同的操作方式。如果每个机器人系统应分别选择操作方式,就不必把所有机器人系统转换到手动方式。非手动操作的机器人应保持安全状态,独立于选定的操作方式,并且不会造成危险。

下列要求适用于机器人系统或机器人单元。不包括对机器人单元中不执行机器人任务的设备的要求。应进行风险评估,确定由于这个其他设备产生的风险而必须采取的任何进一步措施。机器人系统以手动方式运行时,强烈推荐所有其他不执行机器人任务的设备都处于并保持在安全状态。

5.6.2 选择

应通过适当的方法来避免未经授权的和/或无意的方式选择。

这些方法应只能启动已选方式,而不应独立地启动机器人系统操作或相关机器的其他危险操作。应有独立驱动来启动机器人系统操作。

应提供已选操作方式的明确显示。

工作方式的改变应不会导致危险情况。

5.6.3 自动方式

5.6.3.1 通则

以自动方式进入安全防护空间时,应导致可能出现危险或危险情况的所有设备的保护性停止。

5.6.3.2 自动方式的选择

机器人系统自动方式的选择不应覆盖或重置任何保护性停止或急停情况。

自动方式的选择应在安全防护空间外完成。如果使用示教盒或示教控制选择自动方式,应在安全防护空间外以独立谨慎的动作启动自动操作。

切换到自动方式时,应能导致保护性停止或急停。

5.6.3.3 自动操作的启动

自动操作应在安全防护空间外启动。

应在所有相关的安全防护都起作用时,才可能启动自动操作。

5.6.3.4 手动重置、启动/重启和意外启动

5.6.3.4.1 机器人系统的启动和重启应是明白简单的操作。启动和重启应要求相关的安全功能和/或保护措施是起作用的。

与安全相关的控制功能至少应符合 5.2.2 的要求,除非风险评估确定其他的性能准则适用。

5.6.3.4.2 应提供启动联锁,以防止接入或中断和恢复动力供应时,自动启动危险操作。启动联锁应通过谨慎的人为动作重置。

应提供重启联锁,防止以下任一项操作后危险操作自动重启:

- a) 安全防护功能的致动;
- b) 单元操作方式的改变。

按照 ISO 14118,人员在安全防护空间内时,应保护人员而防止机器人单元启动和重启。

启动和重启控制器应位于安全防护空间外,手动致动,应不能在安全防护空间内被启动。

手动重置功能应完成以下所有事项：

- 在与安全相关的控制系统内,通过独立的手动操作装置提供；
- 如果所有安全功能和安全防护是有效的,才能完成；
- 不能自行启动运动和危险状况；
- 通过谨慎的动作；
- 使控制系统能接受单独启动指令；
- 只有从通电位置脱开致动器时才能接受。

在每个控制位置,操作员应能确保无手动重置功能人在安全防护空间内。启动和重启致动控制器的位置宜允许清楚和无障碍地看到安全防护空间。

如果无法实现该要求,应提供现场感应在整个安全防护空间内来检测操作员。

5.6.3.4.3 如果现场感应无法实现,应提供其他保护措施防止意外启动。这些保护措施可包括：

- a) 对位于安全防护空间内的危险设备实行多重隔离或封锁；
- b) 在开放位置封锁防护装置(门)；
- c) 安全防护空间内放置附加的限时重置装置。

如果这些都无法实现,应提供启动前的声音-视觉警告信号：

- 在安全防护空间内能完全看到和听到；
- 提供一段启动前延时,使操作员有足够时间从安全防护空间出去。

应在安全防护空间内放置足够多的易于识别和接近的急停装置,使它们可以在启动前延时段完成操作。

注：选择保护措施的层次结构,见 4.5。

5.6.4 手动方式

5.6.4.1 通则

需要人工干预时,本地控制应由单个示教盒或符合 ISO 10218-1 的类似的控制站来实现。

注：当驱动力施加于任何机器人轴或末端执行器时,手动控制被应用于从安全防护空间内控制机器人的任何装置。

这包括通过示教控制器驱动动力的机器人,不管是使用机器人首选的手动控制还是主级/次级示教控制。

只要可行,控制装置和控制站应放置得使操作员能观察工作区和危险区域。

停止控制设备应放置在每个启动控制装置旁边。

系统应设计和构造成：当系统置于本地控制下时,防止从任何其他动力源启动运动或改变本地控制的选择。

5.6.4.2 手动低速

在手动低速方式下,选定的 TCP 速度不应超过 250 mm/s。宜能够选择低于 250 mm/s 的速度。风险评估的结果应该决定是否需要使最大降速低于 250 mm/s,或决定机器人系统中的其他设备是否需要在低速状态下运行。

根据 ISO 10218-1,在手动低速方式下,只有和一个使能装置连接时,才允许机器人或机器人系统的任何部件运动。使能功能的与安全相关控制性能应符合 5.2 的要求。

5.6.4.3 手动高速

该方式只限于程序验证,不应用于生产。所有的手动点动应在低速方式下。高速方式只有在应用情况要求机器人系统以手动高速方式运行的特殊情况下才能使用。在手动高速方式下,选定的 TCP 速度可以超过 250 mm/s。机器人系统要符合 ISO 10218-1 中的自动操作方式的要求,提供的示教盒应符合 ISO 10218-1 的要求,并且在使用资料中要求示教盒的使能装置要在启动运动之前进行功能性检测,

以保证正确的操作。

5.6.5 人工干预的远程访问

机器人系统可能是支持网络的(如局域网、调制解调器或互联网),它允许远程访问来进行诊断、技术咨询和测试等。

如果操作员要远程控制机器人系统,操作员物理上远离机器人(如在较远的办公室中),应满足以下要求:

- a) 当机器人系统在手动方式下,才能进行人工远程控制;
- b) 一次只能激活一个控制源——本地的或远程的——(单点控制);
- c) b)中所列控制类型不得使本地选择无效,也不能造成本地危险情况;
- d) 只能从本地控制激活人工远程控制功能;
- e) 所有可能产生危险的控制器功能(如机器人运动、控制危险设备的强制输出、以危险方式影响机器人的数值改变、安全功能的确认、保持运行等)只能有单一选定的控制源;
- f) 如 5.4.3 所述,通过轴和空间的安全软限位对机器人运动进行限制,而与此有关的远程参数改变,不应在没有通过本地确认前以及确认没有造成危险前生效;
- g) 本地控制(控制面板、示教盒等)的指示应显示机器人系统正被远程控制;
- h) 只有机器人系统在手动低速下,才应执行人工干预;
- i) 如果在安全防护空间内无人并且防护装置激活时,远程功能可在无任何本地活动的情况下执行;
- j) 当需要有人在安全防护空间内时,远程操作员执行的可能造成危险的控制功能,只在本地操作员按下使能装置而启动功能时才能执行;
- k) 远程动作不需要的、可能造成危险的任何设备应保持在安全状态。

使用资料应包括执行远程任务的远程和本地操作员培训的适当要求。

5.7 示教盒

5.7.1 通则

在安全防护空间内使用的示教盒和示教控制装置应符合 ISO 10218-1 的要求。

示教盒的急停功能应符合 5.3.8.2。

配有电缆的示教盒应该具备一根足够长的电缆,可使示教员以安全方式(如不会因为电缆长度不够而越过设备去到示教点)执行预期任务。电缆应能承受使用位置的预期环境条件。

应采取合适措施存放示教盒,以使造成危险的损坏可能性降到最小。可拆卸示教盒和无缆示教盒的存放应把非激活急停装置误认为激活的可能性降到最小。

5.7.2 无线或可拆卸装置/通信的要求

机器人系统使用无缆或可拆卸示教盒时,应遵循以下要求:

- a) 示教盒应符合 ISO 10218-1。
- b) 示教盒的急停功能和使能装置应符合 ISO 10218-1 中的要求。
- c) 意外地控制机器人系统的可能性应通过以下方法避免:
 - 1) 识别正在被操作的机器人的明确方法;
 - 2) 保证通信完整性的连接方法(如登录、加密、防火墙等);
 - 3) 显示连接持续性的明确方法(如屏幕显示)。
- d) 单个的无缆示教盒不应同时连接到一个以上的机器人系统上;该系统可由一个或多个机器人

组成。

- e) 在手动方式下,任何激活的示教盒(与机器人系统匹配)的通信功能缺失(如超出范围或者缺少电池电源),都应导致所有被控制设备的保护性停止或急停。没有独立谨慎的动作,通信的重新建立不应重启(见 ISO 10218-1 和 IEC 60204-1)。
- f) 应提供从示教盒(如操作员主动动作)上断开机器人控制的明确方法,而当设备注销时,应清晰可辨使与安全相关功能不再激活;提供适当的存储或设计,应避免混淆激活的和非激活的急停装置;使用资料应包括存储和设计的描述。
- g) 根据 ISO 10218-1,示教盒应提供单点控制。

5.7.3 联动的控制

单个的示教盒可控制具有多个机器人的系统的联动。每个机器人应在激活前被选定。选定后,所有机器人应有同一操作方式(如手动慢速)。按照 ISO 10218-1,应提供指示,说明哪个机器人将被激活(选定要移动)。只有被选定的机器人应被激活。根据 5.2.2,系统内任何没被选定的机器人不应移动、不应造成危险。

注:这可以通过保持在保护性停止的状态来实现。

5.7.4 机器人系统(协作机器人)的手动引导

为协作操作设计的机器人系统,可能在任务的协作段用到手动引导控制器。这些相同的控制器可能用到“示教引导”方法。当含有这些控制器时,应符合 ISO 10218-1 中描述的要求。

5.8 保养和维修

5.8.1 通则

机器人系统的设计应包括检查和维护步骤,以确保机器人和机器人系统可以持续安全操作。检查和维护程序应考虑到生产厂商的建议。

为保证正确操作,使用资料应包括对设备的与安全相关部件(如急停装置,使能装置)进行周期性功能检测的要求。

5.8.2 保养的安全防护要求

机器人系统的设计和构造应使得:在操作、调试和保养期间,能安全进入需要干预的所有区域。保养宜在安全防护空间外进行。当需要在安全防护空间之内进行维护时,按照以下要求优先选择安全防护装置:

- a) 应为系统提供控制和隔离危险能量(如断路器,泄压装置,能量隔离控制系统)的本地装置。使用资料应包括要求能量控制和隔离的维护任务的细节,以及当需要危险能源时预先要考虑的那些事情。
- b) 应为次级服务任务提供有效的备选保护措施,次级服务任务是生产需要预先考虑到的和不可或缺的,要在没有能源隔离情况下执行;控制危险能源或者位置监控的控制措施包括以下一项或多项:
 - 1) 提供安全防护装置,使任务安全地执行;
 - 2) 将设备置于预先设定好的安全监测位置或环境中(偏差应导致保护性停止状况);
 - 3) 为人员进入安全防护空间提供专有控制(使用资料中应定义并提供专有控制的步骤);
 - 4) 提供特定的操作方式,至少要满足 5.2.2 中对特定明确任务的要求。

5.8.3 保养进入点的安全防护

为保养或服务任务的通道提供防护装置时,防护装置应有足够的尺寸,使必要的工具、物料和人员容易通过。

给非频繁维护或服务任务提供固定式防护装置时,固定式防护装置应只用一个工具就能拆卸掉。

当需要维护和例行维护任务的常用通道时,应通过保护装置对进入点进行安全防护,较好的是移动式防护装置。移动式防护装置到达安全防护位置时不应启动开始指令。

如果当移动式防护装置关闭时还可能停留在安全防护区域内,应采用其他措施防止重启。这些包括重启联锁、现场感应或锁住防护开口的设施。如果提供重启联锁和现场感应,那么,根据风险评估,现场感应装置至少应符合 IEC 61496-1 中 2 类的要求。

5.8.4 保养时相邻单元的安全防护

当使用具有垂直探测电场的电敏保护设备(ESPE),以防止因维修干预而从一个单元内意外进入相邻单元时,可基于风险评估(不同于 ISO 13855 规定),用接近速度和穿透率来计算最小距离(安全)。

注:使用固定防护装置来代替 ESPE 时,指导见 5.10.6.1。

5.9 集成制造系统(IMS)接口

5.9.1 通则

如 ISO 11161 所述,与机器人系统有联系但不被机器人控制器直接控制的其他机器和设备,应包含在风险评估、分区配置、安全防护之中以及控制设备范围之内。特定的 C 类标准也适用于其他机器。机器人系统集成还应考虑机器人可控的和不可控的危险,但这些危险是指由安全防护空间内相关的机器设备或进/出安全防护空间引起的。

5.9.2 急停

机器人系统应有作用于机器所有相关部件的单独的急停功能。急停功能应符合 5.3.8.2。

控制范围可包括多个区域。使用资料应包括每个急停装置的控制范围的信息。

5.9.3 IMS 的与安全相关的部件

IMS 和机器人系统之间任何与安全相关的控制接口应满足 5.2.2 中的要求。当它们有危险时保护装置应保护 IMS 每个区域内以及至相邻区域(如传送设备)的接口处的通道,以防止危险(也可见 5.10)。

5.9.4 本地控制

操作要求应确定对本地控制的需求。当选择了本地控制时,IMS 控制系统应被告知这种状况,并且不能使本地控制无效。本地控制期间,急停功能和保护性停止功能应始终保持可操作。

选择和取消本地控制的装置应接近机器人或机器或在本地控制下的辅助装置。从安全防护空间内取消本地控制的装置不应造成危险状况。如果本地控制可从安全防护空间内取消,在任何危险状况发生之前,应有必要从安全防护空间外独立确认。

5.9.5 使能装置

当需要其他使能装置时,应符合 5.3.15。使能装置功能应是联锁的并与 IMS 的区域一致,在这些区域中机器人系统、机器或相关进程于手动操作期间可以联动。

5.9.6 方式选择

方式选择应符合 ISO 10218-1。

5.9.7 任务区域的实施

IMS 的设计应便于安全人工干预(包括维护)。对于某些人工干预,停止整个 IMS 是不切实际的,该情况下,IMS 应隔离到区域内,使操作员能安全地执行他们的任务,而 IMS 的其余部分能以不同的操作方式运行。

使机器人系统集成到一个任务区域应符合 ISO 11161。

5.10 安全防护

5.10.1 通则

当设计不能去除危险或不能充分降低风险时,那么应应用安全防护。到危险区域的通道应被安全防护装置保护,如防护装置和保护装置。也需要补充保护措施,如人员保护设备、培训和使用信息。也可参见 4.5。

防护装置和保护装置可用于:

- 防止接近危险;
- 在接近前终止危险;
- 防止意外操作;
- 容纳部件和工具;
- 限制其他加工中的危险(噪声、激光、辐射等)。

防护装置和保护装置应符合 ISO 12100。

ISO 12100 中给出选择安全防护措施的更多要求以及更多的补充措施。

附录 B 中有一些适用于保护措施的标准的概述。

5.10.2 周边安全防护

防护装置(隔开距离或围护,见 5.10.4)或传感保护装置(见 5.10.5)应被用于周边安全防护。

选择周边安全防护应考虑安全防护空间内的所有危险——不仅是与机器人系统有关的。危险的例子包括:

- a) 其他机器、设备和工序;
- b) 跌落或弹出的物体;
- c) 不规律的或过多的机器停止时间;
- d) 机器不能在循环的中途停机;
- e) 危险的散发(如噪声、振动、辐射、有害物质)。

选择也应考虑任务需求,例如:

- 接近的频率;
- 物料装卸;
- 维护;
- 质量检查;
- 危险接近度;
- 工序要求。

5.10.3 最小(安全)距离

5.10.3.1 通则

所有安全防护装置应安全地安装,位置要相隔一段距离,防止接近危险。即人员不能翻越、钻过、绕过或穿过安全防护装置。

5.10.3.2 防护装置的最小(安全)距离

固定式或活动式防护装置应符合 ISO 14120 的要求。任何危险到固定式或活动式防护装置的最小距离应根据 ISO 13857 的相关要求确定。当防止接近防护装置时,应根据 ISO 13857 确定最小安全距离。

有关防护装置开口的最小距离应符合 ISO 13857 的相关要求。

5.10.3.3 保护装置的最小(安全)距离

提供跳闸功能(例如联锁装置、当被致动时发出保护性停止信号的传感保护设备)的保护装置,它们的最小安全距离应根据 ISO 13855 的相关要求确定。

当保护装置提供现场传感功能来防止启动或重启时(例如当保护装置持续感应检测区域内的人或人体部位,并且保持保护性停止时),对最小距离不作要求,但是装置应符合 5.10.5.3。

注:仅用现场传感安全防护装置来防止启动或重启的危险时,在接近前使用其他安全防护装置来防止接近或造成停止的危险。

5.10.3.4 提供间隙的最小(安全)距离

当保护装置通过跳闸功能提供保护,防止缺少间隙(见 5.2.2)时,应根据 ISO 13855,以机器人速度作为接近速度计算出最小距离(即 $K = \text{机器人速度}$)。

当保护装置以现场传感功能来提供间隙(见 5.2.2)时,对最小距离不作要求,但是装置应符合 5.10.5.3。

5.10.4 防护装置的要求

5.10.4.1 通则

所有防护装置应满足 ISO 12100 和 ISO 14120 的适用要求。与防护装置相关的联锁装置应满足 ISO 14119 的要求。

固定式防护装置应只能通过使用工具拆除。当防护装置被拆除时,其固定系统应保持连接在防护装置或机器上。这个要求无需应用到易拆除的固定式防护装置上,例如,当机器要完全大检修,或拆除后转移到另一现场之时。

周边安全防护装置不应安装在比限定空间更靠近危险的地方,除非有以下之一情况:

- 按照 5.4.3,周边安全防护装置设计成为限位装置;或者
- 风险评估确定其他安全防护装置是适用的。

5.10.4.2 固定距离防护装置的一般要求

任何固定式防护装置的开口不应使人能越过、钻过、绕过或穿过(开口或间隙)而到达防护装置和使人接近危险。

应使用 ISO 13857 来确定:从防护装置底面到相邻站立面的开口和防护装置中的任何开口的合适尺寸。至于最小安全距离,见 5.10.3.2。

防护装置的高度应距离相邻行走面至少 1 400 mm。

5.10.4.3 联锁的活动式防护装置的一般要求

与活动式防护装置相关的联锁装置应满足的 ISO 14119 要求。

活动式防护装置处于其关闭位置时应防止操作员到达危险区域。

活动式防护装置的开启应有延迟或远离危险,并且不能进入安全防护空间。

在操作员通过防护装置可能接近危险前,应提供联锁把任何危险转化为安全状态。为达到该目的,移动式防护装置的定位应符合 ISO 13855(也可见 5.10.3.2)。

用于启动开始闭合(控制防护装置)的移动式防护装置,应满足的 ISO 14120 要求。

联锁功能至少应满足 5.2.2 的要求。重置致动器应符合 5.6.3.2 的规定。

5.10.4.4 带防护锁的活动式防护装置的一般要求

在危险降至安全状态前,当操作员有可能开启联锁活动式防护装置且有可能到达危险区域时,除了控制联锁之外还应提供防护锁。

防护锁应符合以下要求:

- a) 只有防护装置关闭并上锁(如围栏上的门),才允许致动危险的机器功能;
- b) 只要存在由于危险的机器功能存在而导致的危害风险,那就保持防护装置处于关闭并上锁的位置。

当要使用如速度的过程参数作为一个锁定或解锁条件时,这就构成安全功能的一部分,并且应满足像联锁功能一样的功能性安全要求。

5.10.4.5 允许进入安全空间的活动式防护装置

安全防护空间的设计、建造或安装,应具有防止人员困于其中的方法。例如,无论是否提供动力,都可通过从安全防护空间内手动打开活动式防护装置或在其打开位置锁定进入门的方法来做到。

5.10.5 传感保护设备

5.10.5.1 通则

当一项应用需要频繁接触、需要进行人机交互、需要机器或工序具备良好可视性时,或在提供固定式防护装置不符合人体工程学时,则通常选择传感保护设备。然而,有一些特定的应用,因其某些特性决定,不能以传感保护设备作为其唯一保护措施。例如:

- a) 机器可能会弹出材料、切屑或零件;
- b) 有烫伤或其他辐射致伤的风险;
- c) 不能承受的噪声水平;
- d) 环境可能会对保护设备的功能产生不利的影响;
- e) 正在加工处理的材料会影响保护措施的有效性。

存在这些情况时,就需要额外的或其他安全措施。

电敏保护设备(ESPE),如光幕和激光扫描仪,应符合 IEC 61496-1 相关部分的规定。

压敏保护设备,如垫板、刃口和缓冲器等,应符合 ISO 13856 的相关要求。

这些装置的应用宜符合 IEC/TS 62046 的要求。

5.10.5.2 启动保护性停止的传感保护设备

传感保护设备用于启动保护性停止时,其位置应离每种危险有一段距离,足以保证危险被消除,或

在接近的操作员的任何身体部分触及危险之前,达到安全状况。

注 1: 在安全防护空间内,危险处在不同地点,因而所述距离需确保每个危险可控。

应牢固安装和定位传感保护设备,防止操作员接近检测区域(如到检测区域的上边、下边、周围或穿过检测区域)造成危险。应提供以下功能:

- a) 当危险状况发生时传感保护设备被致动,应启动保护性停止;
- b) 致动传感保护设备后,应防止被传感保护设备防护的危险状况发生任何危险动作或情况,直到传感保护设备被重置;
- c) 当传感保护设备被重置后,被传感保护设备防护的危险状况可能发生,但是该重复不会自行启动这些危险状况。

ISO 13855 中的公式用于确定从各方向接近的、从危险(危险区)到传感保护设备的最小距离。

注 2: 按照 ISO 13855,用于计算最小距离的 K 最小值为 1 600 mm/s。

当操作员或其身体部分停留在安全防护空间内时,应采取额外措施来防止发生危险情况,如意外启动。这些措施包括:

- 提供重启联锁;
- 感知安全防护空间内存在操作员[例如,电敏保护设备(ESPE)或压力垫],以保持保护性停止状态。

注 3: 若使用现场传感保护设备,建议操作员不要绕行检测区域,例如,攀爬到机器的部件上。

若在重置控制的位置有可能看不到操作员,应提供补充保护措施,以防止联锁重启的重置(例如,安全防护空间内的限时附加重置控制)。应通过谨慎人工动作来执行联锁重启的重置,例如操纵手动致动器。也可见 5.6.3.3。

5.10.5.3 用于现场感应防止启动的传感保护设备

传感保护设备只用于现场传感功能(即在其检测区内,不断地感知人或人身体部分的存在),它应结合其他安全措施(例如联锁防护装置)使用,以在需要时确保发生危险前机器处于非危险状态。

现场传感装置的检测区,其位置和构形应使整个检测区都将检测到人或人身体部分。必要处应提供补充措施,确保检测区没有可规避处,例如操作员停留于检测区和危险区之间,或跨过检测区进入危险区。防止人停留于检测区之间和危险区的措施例子有:

- 使用斜面,防止站在机架/机器脚上;
- 围栏的内表面没有可攀爬的突出物。

5.10.6 手动装载、卸载或搬运工作站(手动工作站)的安全防护

5.10.6.1 通则

应提供措施确保操作员不会受到由于手工生产交界站的运作(例如,粉碎、剪切、缠结危险)带来的进一步危险。

允许的间隙和开口应符合 5.10.4.1 规定。手动工作站的设计应确保操作员在安全防护空间内不能接触到危险[也可见下列的 a)、b)、c)]。

注 1: 协作空间要求在 5.11 中给出。

为达到 1 400 mm 的高度,可采取的附加保护措施有:

- a) 防止操作员在安全防护空间内暴露于与应用有关的危险中。例如,零件的弹射、焊接火花等。
- b) 防止操作员在安全防护空间内接近危险,或在操作员接近前,使安全防护空间内的这些危险转化为安全状态。
- c) 当机器人系统和操作员接近到同一(共有的)工作空间时,确保他们不会同时占据工作空间。这可通过以下两点实现:

- 1) 防止机器人系统任一部分进入操作员占用的工作空间,或使机器人系统在操作员到达前,使机器人系统处于安全状态;
- 2) 防止操作员进入有机器人系统任一部分占据的工作空间,或在操作员到达机器人系统前,使机器人系统处于安全状态。

注2: 由于人体工程学的原因,根据栅栏形状的保护作用和风险评估结果,1 000 mm~1 400 mm 的高度是可以接受的。

5.10.6.2 对移动的手动工作站的附加要求

移动的手动工作站(如旋转的转台、滑动的夹具)自身可具有危险性。应提供措施防止操作员接近这些危险,或在接近危险前,将危险转为安全状态。

移动站和任一固定元件(如机器零件、防护装置等)之间的间隙,包括附加的保护措施,不应超过120 mm。或许有必要使用附加措施,以防止剪切危险和阻断危险。

5.10.6.3 对有共用空间手动工作站的附加要求

使用现场感应来检测共用工作空间内的操作员时,感应装置的检测区应包括整个共用工作空间区域。

当不能使用现场感应装置时,应提供重启连锁。应提供其他措施防止重启连锁的不慎重置,从而防止操作员还在工作空间内时机器人系统的移入工作空间。这种措施可包括在独立的手动重置的条款中。

手动重置时,在重置装置的地方应该能看到整个共用工作空间。如果不能,应使用进一步措施,例如,防护区内的限时附加重置控制。

5.10.7 物流开口的安全防护

许可物料进出的进入安全防护空间的开口应具备必要的最小尺寸,以允许物料通过。应避免物料和开口侧边之间的可能挤压/切断的危险,或采取补充保护措施(如使用铰链式连锁门)加以避免。

如果可能接近危险,应根据风险评估采取措施,以防止接近危险,或探测到进入的人员或人身的一部分,并应在接近危险前,使危险转为安全状态(见 ISO 13857 关于部分身体进入的规定和附录 C)。

物料进出的开口以 ESPE 加以防护时,ESPE 应允许通过下列之一的功能来使物料通过,并且应防止物料自身进入安全防护空间,或 ESPE 应允许通过其他方式使物料通过(见 IEC/TS 62046):

- a) 抑制功能,暂时停用 ESPE 功能以允许物料通过(进/出);
- b) 改变保护区(例如遮隐),使物料得以通过;这种情况下,应能观测到 ESPE 制造商指示的最小距离(见 IEC/TC 62046)。

抑制功能应符合 GB/T 16855.1 的要求,抑制和遮隐功能的执行等级,不应反向影响由 ESPE 风险评估决定的安全功能的执行等级。见 5.10.10。

5.10.8 多个相邻机器人单元的安全防护

应采取措施确保机器人单元内的操作员不受相邻单元的危险侵害。

应采取措施防止机器人单元内的操作员进入相邻单元,或确保操作员遭遇相邻单元的或因其导致的危险前,将相邻单元内的危险转为安全状态。

当为此目的使用固定式防护装置时,要求高度取决于两(相邻)机器人单元中的危险(因为可以从任一单元进入),但是高度最低应为 1 400 mm。

除了固定式防护装置以外,可采取其他措施,例如:

- 电敏保护设备;

- 压力垫；
- 相邻单元同时关闭。

应按照 4.5 的规定选择恰当的措施。

当因生产操作需要抑制保护措施时,抑制功能的功能性安全水平至少和风险评估确定的功能性安全水平一样。

5.10.9 工具更换系统的安全防护

末端执行器和工具更换系统的选择和设计应遵循动力供应的损耗或恢复不会导致危险的原则。若不可行,应提供其他消减任何危险的安全措施。

如果使用工具更换系统,工具更换系统的设计应确保误用不会导致危险状况。具有工具更换功能的末端执行器的释放或拆卸,应防止释放在可能导致危险的位置进行。

工具更换系统应符合预期的静态和动态要求(例如急停情况和动力损失)。

5.10.10 抑制

抑制是在机器人系统周期的一段时间内,安全防护功能被自动控制地暂时中止。

对于机器上正在执行的工艺,有必要时才应提供抑制。抑制的完成应使得:当抑制结束后,应能检测到仍在危险区域的人员。

抑制可与任何能够发出保护性停止电信号的安全防护装置结合使用。

当至少满足以下条件之一时,允许实施抑制功能:

- a) 有其他方法保持安全(如危险区入口由合格材料阻挡);
- b) 人员接触不到危险;
- c) 不启动停止,则不触及危险。

抑制功能应自动地启动和关闭。这可通过恰当选用和放置传感器来实现,或某些情况下,通过安全控制系统(可包括符合 ISO 10281-1 的轴及空间的安全软限位)发出的信号来实现。出现不正确的信号、序列或抑制传感器或信号器的计时的时候,均不应实施抑制功能(见 IEC 61496-1)。

抑制功能性能等级应达到与安全控制系统性能等级相等的等级,上述安全控制系统性能等级是由被抑制的保护性功能的风险评估所确定的。抑制功能的性能等级不应保护功能的性能等级产生不利影响。在发生故障的情况下,应阻止实施随后抑制功能,直到故障排除。

根据风险评估,有必要用显示器来表明要求抑制功能何时是有效的。显示器会警示正常保护性功能的暂停。

抑制信息,包括装置、位置、区域和功能性,应包括在使用资料中。

5.10.11 安全防护的暂停

要求暂停安全防护的任务,例如机器人示教,应具有操作的专用模式,该操作的专用模式按照该任务的风险评估决定,自动选择合适的安全防护装置。

操作模式的选择应通过安全手段(例如,可锁定的选择装置、密码、存取码)来完成,并应符合 5.2.2 的要求。

应满足以下要求:

- a) 不应出现因该模式被激活而重新开始自动操作的可能性;
- b) 自动操作应只能从安全防护空间外启动;
- c) 控制模式功能应和暂停的保护功能有相等的性能等级;
- d) 在暂停功能发生错误到错误更正前应防止随后出现暂停;
- e) 方式选择装置之处、单元入口之处和任何涉及的操作员站之处,应提供有安全设备已暂停的视

觉指示；

f) 为控制所有危险,应激活替代保护措施;这些替代保护措施应提供相等的保护等级。

安全防护要被暂停时,应做到以下几点:

- 任务不需要的机器和设备应该处于保护性停止状态;
- 任务需要的机器和设备应该处于操作员的直接控制下。

当需要手动暂停安全防护时,集成者应提供紧急境况下的使用信息,例如,发现并消除故障和更换安全防护装置。

5.11 协作机器人的操作

5.11.1 目的的通用描述

协作是共用同一工作空间的人员和机器人之间的一种特殊操作。它只是:

- 用于预定任务;
- 当激活了所有要求的保护措施时才有可能实施;
- 用于符合 ISO 10218-1 的、具有专为协作操作设计的特性的机器人。

注:应用示例见附录 E。

集成者应在使用资料中加入协作操作所需的安全保护装置和模式选择的信息。

5.11.2 一般要求

由于在协作工作空间内,人和机器人空间距离有缩小的可能性,因而在操作过程中可能发生人与机器人之间的物理性接触。应提供保护措施始终确保操作员的安全。

应满足以下要求:

- a) 集成者应进行如 4.3 描述的风险评估(见附录 E 的应用示例)。风险评估应考虑整个协作任务和工作空间,至少包括:
 - 1) 机器人特性(如负载、速度、力、功率);
 - 2) 含有工件的末端执行器的危险(如人体工程学结构、锐缘、突出物、使用工具更换装置工作);
 - 3) 机器人系统布局;
 - 4) 操作员站位接近机器人手臂的情况(如防止在机器人下工作);
 - 5) 操作员的位置和路径相对于零件定位、结构的定向(如夹具、建筑支架、墙壁)和夹具上危险位置的关系;
 - 6) 夹具设计、夹板布局和操作、其他相关危险;
 - 7) 任何手动控制机器人导向装置的设计和布置(如可及性、人体工程学等);
 - 8) 特定应用上的危险(如温度、零件的弹射、焊接飞溅);
 - 9) 由使用必要的人员保护设备导致的限制;
 - 10) 环境考虑因素[如化学的、射频的(RF)、辐射的等];
 - 11) 相关的安全功能执行准则。
- b) 集成到协作工作空间的机器人应满足 ISO 10218-1 的要求。
- c) 用于现场检测的保护性装置应符合 5.2.2 的要求。
- d) 用于协作工作空间内的附加保护性装置应符合 5.2 的要求。
- e) 安全防护的设计应该防止或检测到任何人员进一步进入协作空间外的安全防护空间内。如果闯入协作空间外的安全防护空间内,应导致机器人停止和中断并且所有危险。
- f) 周边的安全防护应防止或检测到任何人员进入安全防护空间的非协作部分。

- g) 如果与机器人系统连接或附属于机器人系统并存在潜在危险的其他机器,其本身在协作空间内,那么这些机器与安全相关的功能至少应符合 5.2 的要求。
为协作操作配置的机器人宜使用图 2 所示的符号标签。

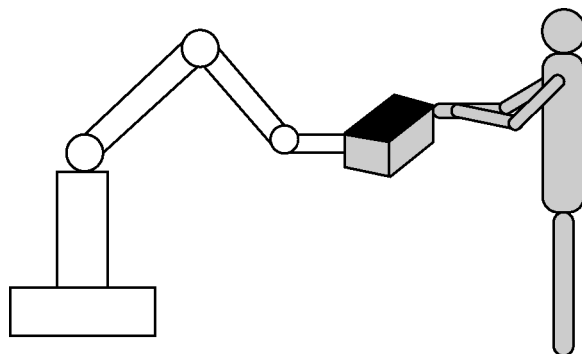


图 2 标签设计建议

5.11.3 协作工作空间的要求

操作员能够直接和机器人交互的协作工作空间应清晰定义(如地面标记、标志等)。

人员/操作员应得到各保护装置的综合保护,同时机器人性能特性应符合 ISO 10218-1 规定,根据 5.2.2 这将导致结束所有危险。

任何情况下一人以上(操作员)进行协作操作时,每一个人均应得到符合 5.2.2 的控制装置的保护。

协作工作空间的设计应能使操作员易于执行所有任务,并且设备和机器的位置不应导致额外危险。只要可能,宜用轴及空间的安全软限位来减少可能的自由移动范围。

机器人系统宜安装成或留有最小 500 mm(20 in)的间隙,该间隙是从机器人(包括手臂、任何连接夹具和工件)操作空间到建筑物、结构物、公共设施、其他机器及设备区域的距离,它允许人体通过并可能造成被困点和被夹点。没留这个最小间隙的地方,当人员在静止环境处于被困点或被夹点危险的 500 mm 范围之内时,应采取附加保护措施停止机器人运动,以提供保护。如果存在动态运动(如直线跟踪),需予以特殊考虑(见 ISO 13854)。

注:根据 5.11.5.4 和 5.11.5.5 设计的不同系统,参数可不同。

5.11.4 自主操作与协作操作之间的转变

自主操作与协作操作之间的交接点是协作应用特别关键的部分。设计应使自主操作转变为协作操作和再还原为自主操作时机器人不会对人员造成危险。

5.11.5 协作工作空间内的操作

5.11.5.1 通则

设计协作操作时,应适当选择 5.11.5.2~5.11.5.5 的一个或多个安全特性,以确保为工作单元中面临潜在危险的所有人员提供安全的工作环境。ISO 10218-1 提供了对协作操作中使用的机器人的要求和性能特性,如 5.11.2~5.11.5 中所述。

协作操作的所选安全特性中,任何检测到的故障,应根据 5.3.8.3 导致保护性停止。这种停止后,自主操作不应被恢复,直至被协作工作空间外的谨慎重启动作所重置。

5.11.5.2 安全适用的受监控停止

如果协作工作空间里没有人,机器人应自主地操作。如果人员进入协作工作空间,机器人应停止运

动,依照 ISO 10218-1 保持安全适用的受监控停止状态,以允许操作员和机器人直接交互(例如,给末端执行器加装零件)。

5.11.5.3 手动导向

若满足下列要求,应允许手动导向操作:

- a) 当机器人到达移交位置,根据 ISO 10281-1,就发出一个安全适用的受监控停止指令;
- b) 操作员应有符合 ISO 10281-1 的要求的导向装置,将机器人移动到期望位置;
- c) 操作员应能清楚看到整个协作工作空间;
- d) 当操作员释放导向装置时,根据 ISO 10281-1,就发出一个安全适用的受监控停止指令。

5.11.5.4 速度和分离监控

机器人系统的设计需使操作员和机器人在动态情况下能够安全分离,这样的机器人系统应使用符合 ISO 10281-1 要求的机器人。

机器人速度、最小分隔距离和其他参数应由风险评估决定。

注:有关协作机器人操作的附加信息和指南将包含在 ISO/TS 15066(目前正在起草中)中。

5.11.5.5 由设计或控制决定的功率和力限制

设计通过功率和力的限制来控制危险的机器人系统,应使用符合 ISO 10281-1 要求的机器人。

功率、力和人体工程学的参数应该通过风险评估决定。

注:有关协作机器人操作的附加信息和指南将包含在 ISO/TS 15066(目前正在起草中)中。

5.12 机器人系统的试运行

5.12.1 通则

试运行计划应包括机器人系统试运行期间人员的保护措施信息。在重大改变后或对安全操作有影响的维护之后,这些措施也可适用于机器人系统。

5.12.2 临时安全防护装置的选择

临时安全防护装置应保护人员免于遭遇如风险评估起初判明的同种危险。如果在开始上电启动测试和验证之前预期的安全防护还是无效,或不到位,那么适当的安全防护方法应在进行之前到位。

注:在机器人单元的初始装配期间,所有最终的安全防护装置安装之前,可能需要保护。所以,建议在设备开始启动期间,替换的安全防护装置(例如链条或活动墙)应安装到位,以提供有效的人员保护。选择替换的安全防护装置应考虑的因素包括:参与人员的培训级别、这种暂时情况的时间长度、其他人员对该单元的可达性、设备运行类型、在给定时间内运行的设备以及该设备呈现的危险。

作为最低限度,应建立意识屏障来确定限定空间。

所有的临时安全防护装置应在试运行信息中指明,并包括在使用资料中。

临时安全防护装置和保护措施可包括:

- a) 和试运行完毕系统的相同,但是临时安装;
- b) 在可选应用中使用不同的装置;
- c) 临时的障碍物;
- d) 专用写程序;
- e) 认知方式;
- f) 特定培训。

5.12.3 初始启动程序计划

应建立初始启动程序,该程序应包括(但不限于):

- a) 在通电之前,应验证已经按计划安装:
 - 1) 机械座与稳定性;
 - 2) 电气连接;
 - 3) 公用设施连接;
 - 4) 通讯连接;
 - 5) 外围设备和系统;
 - 6) 用于限制最大空间的限位装置。
- b) 应提供指令,使得在施加驱动力之前,所有人员退出安全防护空间。
- c) 施加驱动力之后,应验证:
 - 1) 急停电路/装置能够正常工作;
 - 2) 每一个轴能够运动并按预期受到限制;
 - 3) 机器人能按预期对基本操作系统的运动命令进行响应;
 - 4) 认知方式(音频/视频)如预期有效;
 - 5) 所有安全防护装置或临时安全防护装置功能如预期有效;
 - 6) 慢速控制被激活,且功能发挥如预期有效。

注:确保机器人和设备按照预期的方式运动/运行,这在初始上电时特别关键。

6 安全要求和保护措施的验证和确认

6.1 通则

机器人系统的制造商或集成者应按照第4章和第5章所述原则,提供对机器人系统设计与构造的验证和确认。

宜复查风险评估,评价是否所有合理可预见的危险均被确定,是否采取了纠正措施。

注:由于附录A中所确定的所有危险并非都适用于每个机器人系统,与给定危害情况相关的风险等级在不同的机器人系统中是不同的,而特定的机器人系统应用中含有附录A中没有确定的危险。需进行风险评估,以便为给定的机器人系统确定适当的保护措施。

6.2 验证与确认的方法

通过下列方法实现验证和确认,但不限于此:

- A 目视检查;
- B 实际测试;
- C 测量;
- D 操作中观察;
- E 复查特定应用原理图、电路图和设计素材;
- F 复查和安全相关的应用软件和/或软件文档;
- G 复查基于任务的风险评估;
- H 复查布局图和文件;
- I 复查使用说明和资料。

见表G.1。

6.3 必需的验证与确认

附录 G 列出了专用性能要求,这些要求对应该验证或确认的机器人系统安全至关重要。应使用适当的方法评估这些要求,以决定系统的设计和构造是否充分满足要求。

注 1:并非表 G.1 所列的所有项目有必要应用于每个机器人系统。可能有示例说明不可能验证和/或确认某些项目。

注 2:表 G.1 既非全面性的也非有限定性的。根据专用机器人系统设计,可能存在附加验证要求。

注 3:确保所有适用项目被验证和/或确认,这是集成者的职责。

注 4:如果以表 G.1 作为检查表,需要重审和限制表的内容,以代表被评估的实际机器人系统配置和合适的评估方法。

6.4 保护设备的验证与确认

应验证已安装的抵御已识别危险的保护设备,是否按照制造商的使用说明正确使用,是否恰当地应用于机器人系统。

- a) 为防止接近危险,应通过下列内容来实现:
 - 1) 靠近危险前使危险停止;
 - 2) 防止无意操作造成危险;
 - 3) 防护好部件和工具(例如防范松动的物件、飞溅的抛射物);
 - 4) 控制其他过程危险(如噪声、激光和辐射)。
- b) 已安装的安全防护设备应进行以下方面的验证:
 - 1) 防护装置的类型、开口的尺寸、防护装置的放置、正确的安全距离和高度;
 - 2) 从安全空间内不能致动重置控制;
 - 3) 保护装置的类型、检测能力、保护装置的放置、正确的安全距离、尺寸等;
 - 4) 旁路和抑制功能。
- c) 应验证已提供了补充保护措施:
 - 1) 使用说明;
 - 2) 培训材料;
 - 3) 警告;
 - 4) 人员保护设备;
 - 5) 规程;
 - 6) 其他适当的措施。

注:每个保护措施或许不能满足 a)~c) 的每个规范,需视其所针对的危险而定。

7 使用资料

7.1 通则

使用资料应包括系统安全及其正确使用必需的信息及指示,并且应为使用者提供任何其他危险相关的信息及警告。也应包括来自组成的机器的制造商的使用资料。

使用资料应该由文件、标示、信号、符号或图标组成,用于向用户传达重要的安全相关信息。

使用资料中不同部分的风格及内容,宜照顾预期读者的教育水平、技术理解能力及技能水平。使用资料宜用适宜读者的语言编写。

使用资料应反映出集成系统的预期使用情况,也应反映出可预见的误用情况。

为了减轻危害,使用资料应包括:

- 对培训的要求；
- 对个人保护设备的要求；
- 对附加防护或保护装置的要求(见 ISO 12100)。

集成机器人系统的使用资料应满足 ISO 12100 的要求。

注 1: 也可见 IEC 62079, 有关用户信息的框架结构及描述部分。

注 2: 也可见 IEC 60204-1。

7.2 说明手册

7.2.1 通则

说明手册应考虑到机器人系统使用中的各个环节,包括运输、装配、安装、试运行、操作使用(包括开机、关机、设置、示教/编程或进程切换、操作、清洁、错误查询及维修),在适当情况下应包括结束试运行、拆卸及处理方面的内容。

说明手册应包括机器人系统与上层及下层进程之间的接口(物理接口、机械接口及功能接口)信息。特别是,说明手册应包括 7.2.2~7.2.10 中的内容。

7.2.2 搬运

机器人系统运输、搬运及存储方面的信息应包括(例如):

- a) 各个机器的存储条件;
- b) 尺寸及质量数值,重心的位置;
- c) 搬运指示(比如指示起重设备着力点的图示)。

7.2.3 安装和试运行

机器人系统安装和试运行方面的信息应包括(例如):

- a) 安装/固定及振动阻尼方面的要求;
- b) 装配及安装条件;
- c) 使用及维修所需空间;
- d) 允许的环境条件(如:温度、湿度、振动、电磁辐射);
- e) 机器人系统与电源之间的连线说明(尤其是过流保护方面的内容);
- f) 废物清除/处理的建议;
- g) 如果需要,应加入用户必须采取的保护措施方面的建议,例如附加防护栏(见 ISO 12100),安全距离、安全标志及信号;
- h) 首次使用和投入生产前,应贯彻机器人系统及其防护系统的初始测试及试验(包括低速控制的功能测试)的指南。

7.2.4 试运行测试或初始启动程序的信息

此信息应包括(但不局限于):

- a) 通电之前,验证:
 - 1) 机器人物理安装正确并稳固;
 - 2) 电气连接正确,动力(电压、频率、干扰位准)处于特定范围内;
 - 3) 接地正确(等电位);
 - 4) 控制系统中与安全相关的部件正确安装;
 - 5) 其他公共设施(例如,水、空气、燃气)连接正确,且在特定范围内;
 - 6) 外部设备(包括联锁装置)连接正确;

- 7) (使用时)构建限定空间的限位装置已安装;
 - 8) 已采用恰当的安全防护手段;
 - 9) 按照说明设置物理环境(如,照明和噪声水平、温度、湿度、大气污染物);
 - 10) 所有程序的合适版本(正常控制和与安全相关的)已经被确认,并且是已经安装的版本(工程变更管理)。
- b) 通电后,验证:
- 1) 启动、停止和模式选择(包括键锁开关)的控制装置功能按预期运行;
 - 2) 每个轴能够移动,并按照预期受限;
 - 3) 急停和保护性停止(如果含有的话)电路和设备功能正常;
 - 4) 与外部电源断开和隔离是可能的;
 - 5) 示教再现功能正常;
 - 6) 环境条件具备兼容性[例如,爆炸、腐蚀、潮湿、灰尘、温度、电磁干扰(EMI)、射频干扰(RFI)和静电放射(ESD)];
 - 7) 所有防护设施、保护装置、使能装置和连锁装置功能均如预期运行;
 - 8) 所有其他防护措施均到位(如屏障、报警装置);
 - 9) 手动模式下,机器人运行正常,并能搬运产品或工件;
 - 10) 自动(正常)模式下,机器人运行正常,并能按照额定速度和负载执行预期任务。

试运行测试或初始启动程序,也宜在任何维护任务或系统修改之后执行,所述维护任务及修改可能会影响所设计和安装的机器人系统的完整性。

7.2.5 系统信息

机器人系统本身的信息应包括,例如:

- a) 系统、它的配件、它的防护装置和/或保护装置的详细描述;
- b) 机器人系统的预期广泛应用,包括禁止的用途(如果有的话),如果合适可以考虑原机器人系统的变化;
- c) 以控制系统执行的安全功能来描述的安全要求规范、离散的停止电路、安全控制器及安全的通讯;
- d) 其他控制器功能、操作面板、示教盒、使能装置、感知指示器;
- e) 图标(布局、控制、电气、液压、气动等);
- f) 关于其他危害的数据,例如辐射、燃气、蒸汽、灰尘以及震动等,以上数据是依据所使用的测量方法而产生的;
- g) 关于电力设备的技术文件(参照 ISO 6020 系列);
- h) 等电位连接(接地)要求规范。应按照 IEC 60204-1 进行电气接地(等电位);
- i) 用以证明机器人系统服从命令要求的文件;
- j) 对原本提供给组成机器的保护措施进行的修改;
- k) 末端执行器(臂端工具)负载分析、万一能量损失的情况、人为干预考虑,维护和预期寿命;
- l) 其他机器的接口要求;
- m) 动态限区的位置;
- n) 系统的预期寿命。

7.2.6 系统的使用

集成系统使用方面的信息应包括,例如:

- a) 剩余风险,设计者所设计的保护措施不能消除的风险;

- b) 由于某些应用或使用一些附件导致的特别的风险,以及这些应用所需的特殊的防护装置;
- c) 合理可预见的误用和禁用;
- d) 物料的流动;
- e) 使用目的;
- f) 任务区及相关的剩余风险(见 ISO 11161);
- g) 操作员任务、位置以及执行任务的路径;
- h) 各种控制和保护装置的控制范围(见 ISO 11161)(例如:保护装置、保护装置的重置、使能装置、急停、控制站、分离方式);
- i) 手动控制器(致动器)、使能装置、保护性停止装置的描述;
- j) 设置和调节;
- k) 停止方式及方法(尤其是急停);
- l) 故障识别和定位、修理以及干预后的重启;
- m) 使用和训练所需的个人防护设备;
- n) 可能影响安全功能的部件更换或可选设备的增加(包括软硬件)之后,所需的任何测试或试验的说明;
- o) 应从通道拆除示教盒的说明;
- p) 故障紧急排除和系统设备紧急恢复的说明;
- q) 远程控制操作的培训要求;
- r) 未使用的无缆示教盒的存储位置或设计,防止无效急停的使用;
- s) 与安全有关设备的定期功能性测试要求;
- t) 工序唯一消耗品的正确选择、准备、应用和维护的指南。

7.2.7 维护

维护信息应包括,例如:

- a) 安全功能检查的内容和频率;
- b) 需要一定专业知识或特殊技能因而宜专门地由熟练技术人员(如维修工、专家)进行的维护操作的说明;
- c) 不需要特殊技能因而可以由用户(如操作者)进行的维护操作(如消耗件的更换)的说明;
- d) 能使维修团队合理开展其工作(尤其是找错工作)的图表;
- e) 更换与安全相关的零件的信息(制造商零件编码、零件规格);
- f) 制造商联系信息,以便更换零件;
- g) 要求能源控制和隔离的任务;
- h) 手动暂停安全防护措施的安全工作实践。

7.2.8 报废

应包括报废、分解和处理方面的信息。

7.2.9 紧急状况

紧急状况的信息应包括,例如:

- a) 使用的防火设备的类型;
- b) 可能排放或泄漏有害物质的警告;
- c) 列出对付其影响的方法(如果可能的话)。

7.2.10 机器人的特定信息

机器人的特定信息应包括,例如:

- a) 根据 ISO 9946 的信息;
- b) 根据 ISO 10218-1 的信息;
- c) 在适当情况下,使用示教盒的手动高速控制的信息;
- d) 限位装置安装的说明,包括数量、位置和档块能力调整的程度,包括对于数量、位置和提供任何非机械限位装置的说明,还包括动态限位的能力;
- e) 使能装置的数量和操作的说明以及附加装置的安装说明;
- f) 在最大位移和运动时三轴的停止时间和距离或角度的信息;
- g) 用于润滑、制动或机器人传输系统内部的任何液体或润滑剂的规格;
- h) 运动和负载能力限制范围的信息,包括最大质量、工件以及工件夹紧装置的重心位置;
- i) 机器人或机器人系统所达到的相关标准的信息,包括第三方认证的任何标准;
- j) 如可行,有关机器人联动和程序员/操作员所需的特殊培训的说明;
- k) 紧急情况或无驱动力时机器人非正常运动的说明;
- l) 通过使用安全软轴和空间限位方式建立的可编程限位;
- m) 对于设计用于协作操作的机器人系统方面,参考 5.11(确定要被满足的要求和操作的类型),申明机器人适合集成为协作机器人。

7.3 标志

机器人系统标志应明显、易读、不可擦除,并至少具有以下细则:

- 制造商的名称和完整地址,如果可以,以及授权代理商的名称和完整地址;
- 机器名称;
- 系列或型号;
- 序列号(如果有的话);
- 建造年份,即制造过程完成的年份;
- 如果设计和建造的机器是用于潜在的爆炸性环境中,应标以相应标志。

附 录 A
(资料性附录)
重大危险清单

表 A.1 为机器人和机器人系统的重大危险清单。

注：表 A.1 清单来自 ISO 12100。

表 A.1 重大危险清单

序号	类型或组	危险情况示例		涉及条款
		来源	潜在后果	
1	机械危险	<ul style="list-style-type: none"> ● 机器人臂任何部分、末端执行器或机器人单元移动部分的运动(包括返回) ● 外部轴的运动(包括处于服务位置的末端执行器工具) ● 在末端执行器或外部轴、正被操控零件及相关设备上的锐利工具的旋转或运动 ● 任何机器人轴的旋转运动 ● 跌落或弹射出的材料及制品 ● 末端执行器故障(分离) ● 宽松的衣服、长发 ● 机器人手臂和任何固定物体之间 ● 末端执行器和任何固定物体之间(护栏、横梁等) ● (跌入)夹具之间,来回往返物体之间,以及公共设施之间 ● 在自动模式下被困操作员无法(经单元门)离开机器人单元 ● 夹具或夹持器的意外运动 ● 工具的意外释放 ● 处置操作时机器或机器人单元部件的意外运动 ● 末端执行器或相关设备(包括机器人控制的外部轴,特别是磨轮加工等)的意外运动或激活 ● 储备源潜在能量的意外释放 	<ul style="list-style-type: none"> ➤ 挤压 ➤ 剪切 ➤ 切割或切断 ➤ 纠缠 ➤ 拖入或困住 ➤ 碰撞 ➤ 刺伤或穿刺 ➤ 摩擦、磨损 ➤ 高压流体/煤气注入或喷射 	4.1; 4.2; 4.2 d) 6); 4.2 f); 4.3; 4.4; 4.4.1; 4.4.2 d); 4.4.2 f); 4.5; 5.2; 5.2.1; 5.2.2; 5.2.3; 5.3; 5.3.2; 5.3.6; 5.3.7; 5.3.8.2; 5.3.9; 5.3.10; 5.5.1; 5.5.2; 5.5.3; 5.5.4; 5.6.4; 5.8; 5.9; 5.10.2; 5.10.3; 5.10.6.1; 5.10.6.2; 5.10.6.4; 5.10.7; 5.11; 5.11.4; 5.11.5.4
2	电气危险	<ul style="list-style-type: none"> ● 接触带电部件或连接器(机器的电器柜、端子箱、控制面板) ● 系统内、电气柜和终端的不同电压的混淆,如驱动电源、控制电源(24 V vs 110 V) ● 与电器(电子)电路的分立元件的接触,如电容 ● 暴露于电弧光中 ● 采用高压或高频加工,如静电喷漆,感应加热 ● 高压焊接应用 	<ul style="list-style-type: none"> ➤ 触电死亡 ➤ 电击 ➤ 灼伤 ➤ 熔化粒子的喷射 	4.4.1; 5.3.2; 5.3.6; 5.3.7; 5.8.2; 5.10.6.1; 5.10.6.2; 5.10.7

表 A.1 (续)

序号	类型或组	危险情况示例		涉及条款
		来源	潜在后果	
3	热能危险	<ul style="list-style-type: none"> ● 与末端执行器或相关设备、工件连接的热表面(如焊枪、锻压机的热材料、注塑模、磨削和去毛刺) ● 低温表层或物体(深冷加工) ● 加工过程中的爆炸性环境,如油漆(雾化颗粒、粉末涂装)、易燃溶剂、磨削、铣削灰尘 ● 工艺需要的极端温度[熔料、做饭或取暖的炉子(高压炉)、冷冻柜或冷却装置等] ● 易燃材料(内部集尘系统、冲洗池、密封剂涂抹装置) 	<ul style="list-style-type: none"> ➤ 灼伤(热或冷) ➤ 辐射伤害 	5.3; 5.5.2; 5.5.4
4	噪声危害	<ul style="list-style-type: none"> ● 高噪声源的特殊应用(如水切割机、冲压机、泵和阀门、金属清除设备) ● 妨碍听力或阻碍接收警告危险的声音讯号的噪声水平,包括无法通过正常交谈来协调人员活动的情况 	<ul style="list-style-type: none"> ➤ 丧失听力 ➤ 丧失平衡 ➤ 丧失意识、迷失方向 ➤ 周围情况或分神的任何其他(如机械的)后果 	噪声不属于本部分的范围
5	震动危害	<ul style="list-style-type: none"> ● 和震动源直接接触 ● 连接件、紧固件松动 ● 组件或零件未对准 	<ul style="list-style-type: none"> ➤ 疲劳 ➤ 损伤神经 ➤ 心血管疾病 ➤ 冲击 	4.2; 4.3; 4.4; 4.5; 5.5.2; 5.5.9
6	辐射危害	<ul style="list-style-type: none"> ● 电磁场干扰机器人系统的正常运作 ● 暴露于与加工相关的辐射中,如弧焊、激光 	<ul style="list-style-type: none"> ➤ 灼伤 ➤ 损伤眼睛和皮肤 ➤ 相关疾病 	4.2; 4.3; 4.4; 4.5; 5.5.2; 5.5.9
7	材质危害	<ul style="list-style-type: none"> ● 接触被掩盖在有害液体下的部件 ● 机械和电子部件的故障 ● 接触腐蚀性烟雾和尘埃 	<ul style="list-style-type: none"> ➤ 致敏 ➤ 火灾 ➤ 化学灼伤 ➤ 吸入性疾病 	4.2; 4.3; 4.4; 4.5; 5.5.2; 5.5.3
8	人体工程学危害	<ul style="list-style-type: none"> ● 设计不当的示教盒、人机界面触摸屏或操作面板(太远或太高) ● 设计不当的装载卸载位置(如元件箱位和装货/卸货区距离太远) ● 设计不当的使能装置 ● 控制装置的安置或确认不当(例如难以够到) ● 需要接近的零件安置不当(故障排除、修理、调整) ● 对危险识别模糊、局部照明不足或者遮蔽 	<ul style="list-style-type: none"> ➤ 不良位姿或过分努力(重复性过度劳累) ➤ 疲劳 	4.2 d); 4.3; 4.4; 4.5; 5.3.2; 5.3.13; 5.5; 5.5.2; 5.5.3; 5.9

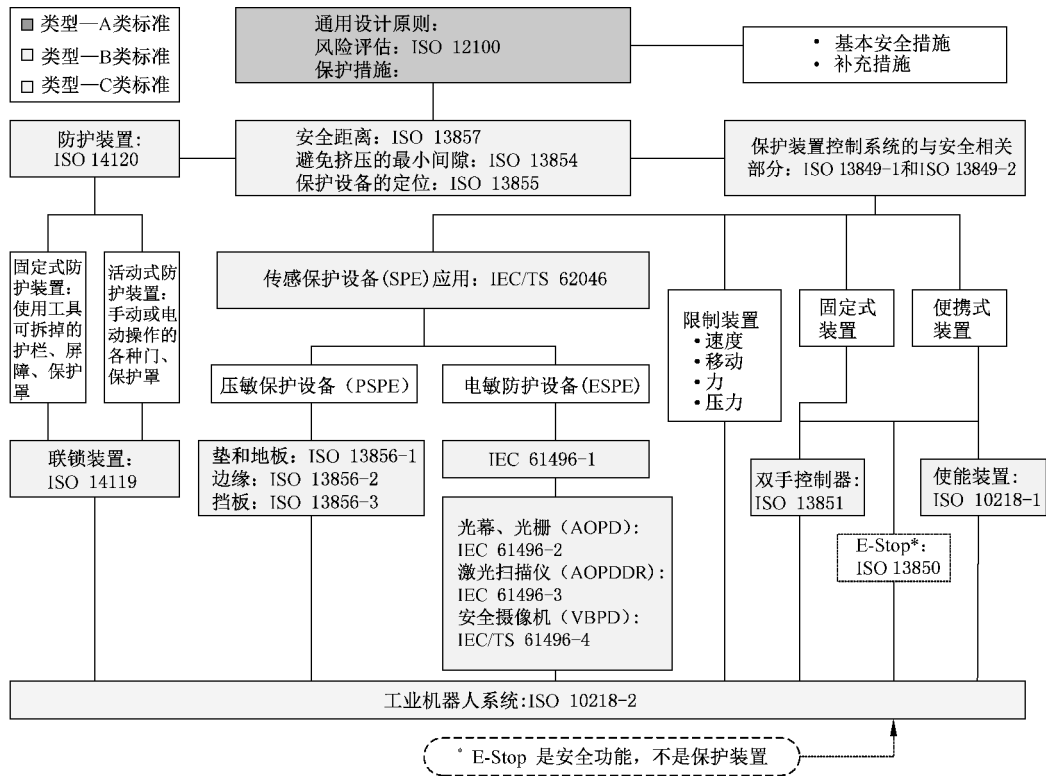
表 A.1 (续)

序号	类型或组	危险情况示例		涉及条款
		来源	潜在后果	
9	与机器使用环境相关的危险	<ul style="list-style-type: none"> ● 在地震区安装的设备 ● 能源的电磁干扰或湧波 ● 湿度 ● 温度 	<ul style="list-style-type: none"> ➤ 灼伤 ➤ 疾病 ➤ 打滑、跌落 ➤ 呼吸系统损害 ➤ 冲击 	4.1; 4.2; 5.2; 5.3; 5.5
10	多种因素结合的危险	<ul style="list-style-type: none"> ● 机器人系统被一人开启,而另一人未想到机器人系统已开启 ● 多个故障/状况引起的危险 ● 对实际问题的误判和执行错误或不必要动作引发的综合问题 ● 加重危险程度的行为,如为避免锋利的边缘,反而碰到灼热表面 ● 握持装置意外释放后余力导致的运动(惯性力、重力、弹簧/能量存储装置) ● 安全防护装置功能无法如期正常运转 	<ul style="list-style-type: none"> ➤ 多种因素结合的危险或危险状况导致的任何其他后果 	4.2; 4.3; 4.4; 4.5; 5.2; 5.3.10; 5.6.3.3; 5.8; 5.9; 5.9.1;

附录 B

(资料性附录)

与保护装置相关的各标准之间的关系



附录 C
(资料性附录)
物料进出点的安全防护

C.1 输送机处防止进入的一般考虑

物料输送系统可以是工业机器人系统的集成部分,它输送物料进出安全防护空间。一般,物料输送系统包括所有类型的输送机(例如带式输送机、动力和非动力辊子输送机、板式输送机等),并且由于其差异性,不可能将各式各样安全防护要求均描述出来。经常必须进行风险评估,以确保识别、评估和合理控制所有危险。以下几点宜给予考虑(见图 C.1):

- a) 宜尽可能方便地在干预点设置安全进入装置(如联锁门),以防止人员寻找穿过物料输送系统的通道。
- b) 物料输送系统不宜存在能接触任何危险的任何开放区域。
- c) 沿输送机边进入的风险(如通过使用倾斜面防止)。
- d) 越过或全身通过的风险(如通过边界防护装置、输送机高度、ESPE 来防止)。
- e) 抓在并悬挂在输送机上方的风险。

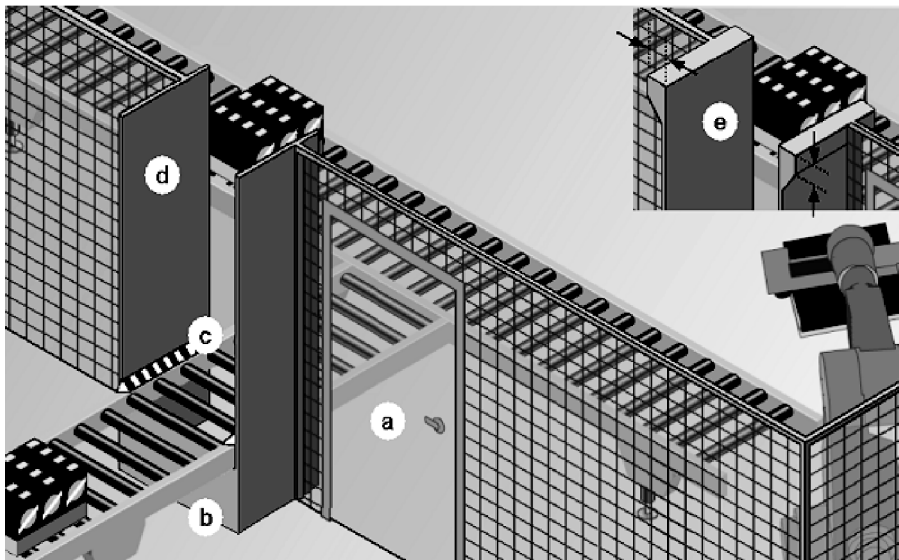


图 C.1 防止进入输送机处的措施的示例

C.2 小开口示例(见图 C.2)

开口尺寸宜适合物料尺寸。
从开口处不宜到达危险区域。

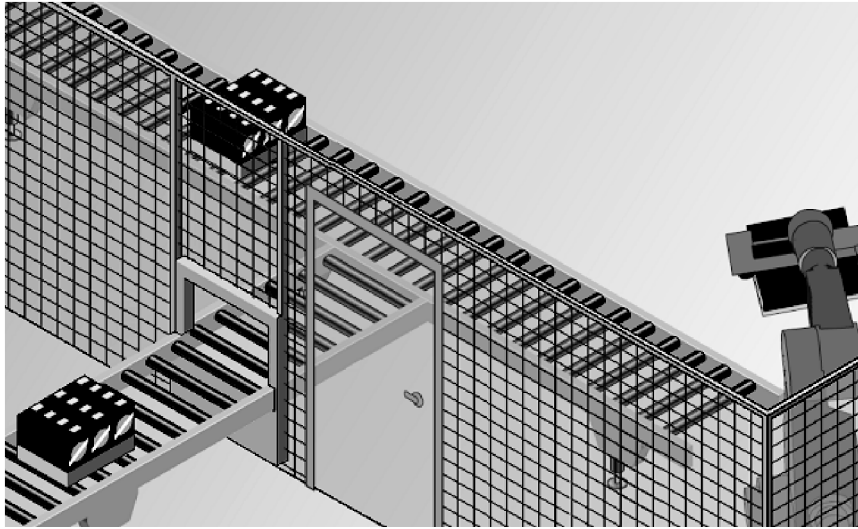


图 C.2 物料通过防护装置的小开口进入

C.3 隧道示例

足够深的隧道可防止到达危险区域(见图 C.3)。

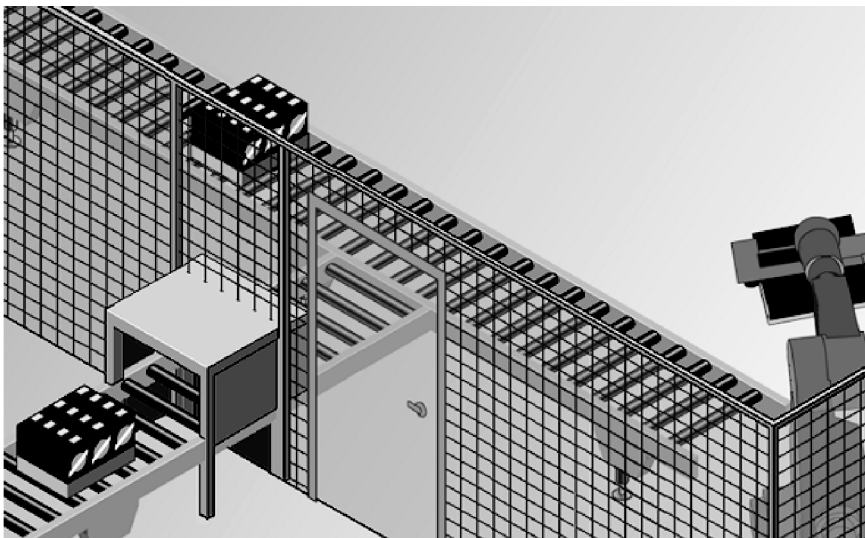


图 C.3 用于增加到危险的距离的隧道

C.4 带 ESPE 的安全防护示例

ESPE 感应到物体进入;然而,由于抑制功能,允许产品通过(显示出具有交叉的光束)(见图 C.4)。

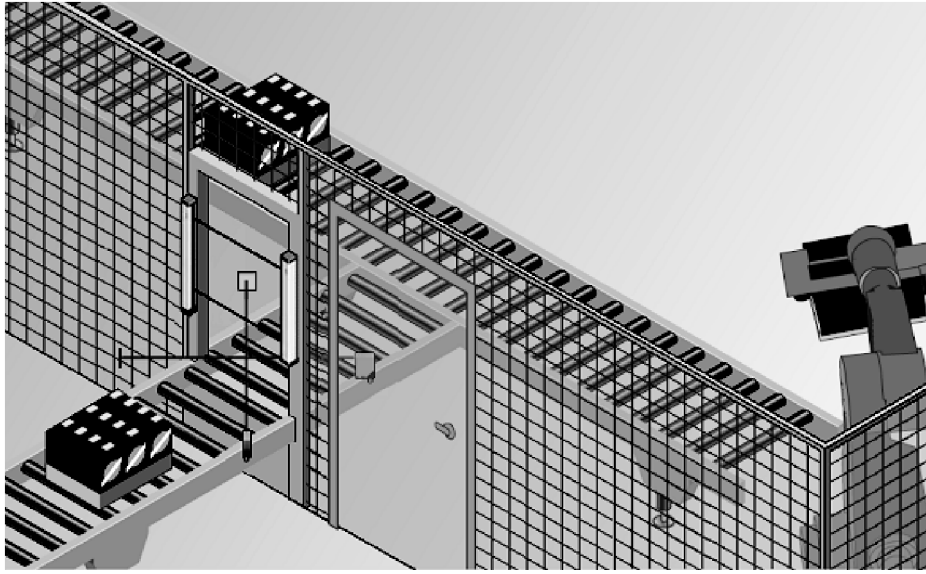


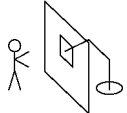
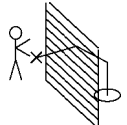
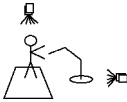
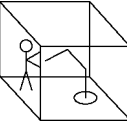
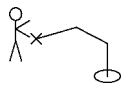
图 C.4 带 ESPE 的安全防护

附 录 D
(资料性附录)
多个使能装置的操作

表 D.1 机器操作和两个使能装置的位置的真值表

		人员 A		
		位置 1	位置 2	位置 3
人员 B	位置 1	关	关	关
	位置 2	关	开	关
	位置 3	关	关	关
注: 机器操作应是: 只有在两个使能装置都处于位置 2(使能的中间位置)的时候才被使能。				

附录 E
(资料性附录)
协作机器人的概念应用

应用类型		描述	安全防护措施	目的
	移交窗口	<ul style="list-style-type: none"> —自主的 —在安全防护空间内自动操作 —机器人移进窗口 —进入期间不中断自动化操作 	<ul style="list-style-type: none"> —工作空间周围的固定式或感应式防护装置 —在窗口附近降低速度和减小工作空间 —窗外没有机器人工作空间 —当窗口下缘小于 1 m, 使用根据 5.10.3 的防护装置 	<ul style="list-style-type: none"> —装载、卸载 —测试、钳工修理、清洗 —服务
	交接面窗口	<ul style="list-style-type: none"> —自主的 —在安全防护空间内自动操作 —机器人停在交接面窗口处并且被手工移动到交接面外面 	<ul style="list-style-type: none"> —工作空间周围的固定式或感应式防护装置 —在窗口外和附近降低速度并且减小工作空间 —引导运动的保持-运行控制 	<ul style="list-style-type: none"> —自动叠垛/卸垛 —引导组装 —引导填充/卸除 —测试、钳工修理、清洗 —服务
	协作工作空间	<ul style="list-style-type: none"> —自主的 —在公共(协作)工作空间内自动操作 —当人员进入公共(协同)工作空间, 机器人减速和/或停机 	<ul style="list-style-type: none"> —使用一个或多个传感器的人体检测系统 —根据距离进行减速(5.11.5.4) —如果有恰当的安全保护措施, 在禁区被侵入时机器人安全地停机, 并在禁区清空后自动重启 	<ul style="list-style-type: none"> —共同装配 —共同处理 —测试、钳工修理、清洗 —服务
	检查	<ul style="list-style-type: none"> —自主的 —在安全防护空间内自动操作 —人员进入协作工作空间, 同时机器人继续运行但速度降低和减小移动 	<ul style="list-style-type: none"> —工作空间周围的固定式或感应式防护装置 —人体检测系统或使能装置 —进入工作空间后降速或减小工作空间 —防止误用的措施 	<ul style="list-style-type: none"> —检查与调整工序, 如焊接应用
	手动引导机器人	<ul style="list-style-type: none"> —具体的应用工作空间 —手动引导移动 —沿着路径手动引导 	<ul style="list-style-type: none"> —降低速度 —保持-运动控制 —根据应用的危险而定的协作工作空间 	<ul style="list-style-type: none"> —手动引导组装、喷漆等

注: 要求见 5.11。

附 录 F
(资料性附录)
工序观测

F.1 通则

工序观测可理解为一种技术安全措施和安全行为要求的结合,通过限制速度、横向路径和断开不需要的运动对操作者提供最大可能的保护。

依照需要,通过使用替代的保护措施来减少保护措施的情况下,宜进行自动化生产过程的临时观测。宜使用技术安全措施,防止发生合理可预见的误用。

为了能够分析对操作者的行为要求并将其转化为行动,上述行动方式宜成为集成者和未来用户之间密切接触的主题。

如果发生残留风险,例如熔融金属颗粒飞溅,宜建立图 F.1 所示的概念。

注:本附录根据 ISO 11161:2007 的附录 D 改编而来。

F.2 对工序观测的评论

见图 F.1。

- a) 是否需要近距离观察工作过程? 能否用合适的 C 类标准规定的相关操作方式来控制工作过程? 附加系统,如摄像机或结构物上的噪声装置是否有用?
是否与未来用户进一步磋商过? 用户是否详细阐述过附加操作方式在将要进行的生产中绝对有必要使用?(例如,由于公差变化很大、生产调整、质量检查)?
- b) 是否对协商的结果,特别是附加操作方式的原因作了记录? 相比于正常操作,这个附加操作方式的应用是否仍限制在预期使用范围的必要程度内?
- c) 建议对具有附加操作方式应用的机器人系统的预期用途作出详细说明并列入技术文档。为进行危险分析和风险评估,安全策略(见第 4 章)宜包括预期用途。建议考虑特殊情况(人员接近生产加工)。
- d) 依靠设计措施避免危险,在降低风险时是最优先的考虑。由于这种情况不易实现,因此,宜特别考虑降低风险的技术安全措施。一方面,技术措施宜把降低风险当作目的,另一方面,宜尽最大可能采用最少的附加操作方式,从而避免误用,例如通过:
 - 1) 速度的安全限制和横向路径的安全限制只达到要求的水平;
 - 2) 停顿后,手动重启运动部件;
 - 3) 操作方式不需要的危险运动/轴的安全断开;
 - 4) 防止工具自动更换;
 - 5) 防止托板更换;
 - 6) 防止把冷却润滑剂置于高压下;
 - 7) 手动确认冷却剂释放(眼伤);
 - 8) 紧急情况下易于接近停机装置(急停);
 - 9) 访问必须经过授权,例如,通过按键开关或密码。
- e) 如果通过技术手段已经使风险充分降低,则可以提供附加操作方式。
- f) 反复过程宜继续下去,直到用尽技术措施。

- g) 如果风险评估显示剩余风险不可接受,集成者宜核查用户是否能够作出必要的努力通过其他方法来降低风险,例如:
 - 1) 具备特殊技能的员工;
 - 2) 提供正规指导(书面举证);
 - 3) 人员的防护设备(如防护眼镜、防护鞋、穿合适的服装);
 - 4) 另附有关附加运作方式操作说明。
- h) 如果集成者得知用户不能满足以上要求,则不宜提供机器人系统的附加操作方式。
- i) 如果集成者得知用户能够通过附加措施充分满足要求,宜将这些措施根据集成者和用户之间的协议记录下来,并将其作为要求加入操作手册,同时将其作为机器人系统的标记或警告标志。
- j) 与附加操作方式相关的所有信息,宜在操作手册中记录:
 - 1) 预期用途;
 - 2) 可预见的误用的防范措施;
 - 3) 操作与功能的描述;
 - 4) 用户根据 e)和 f)步骤采取的措施;
 - 5) 与维护和控制相关的其他要求。

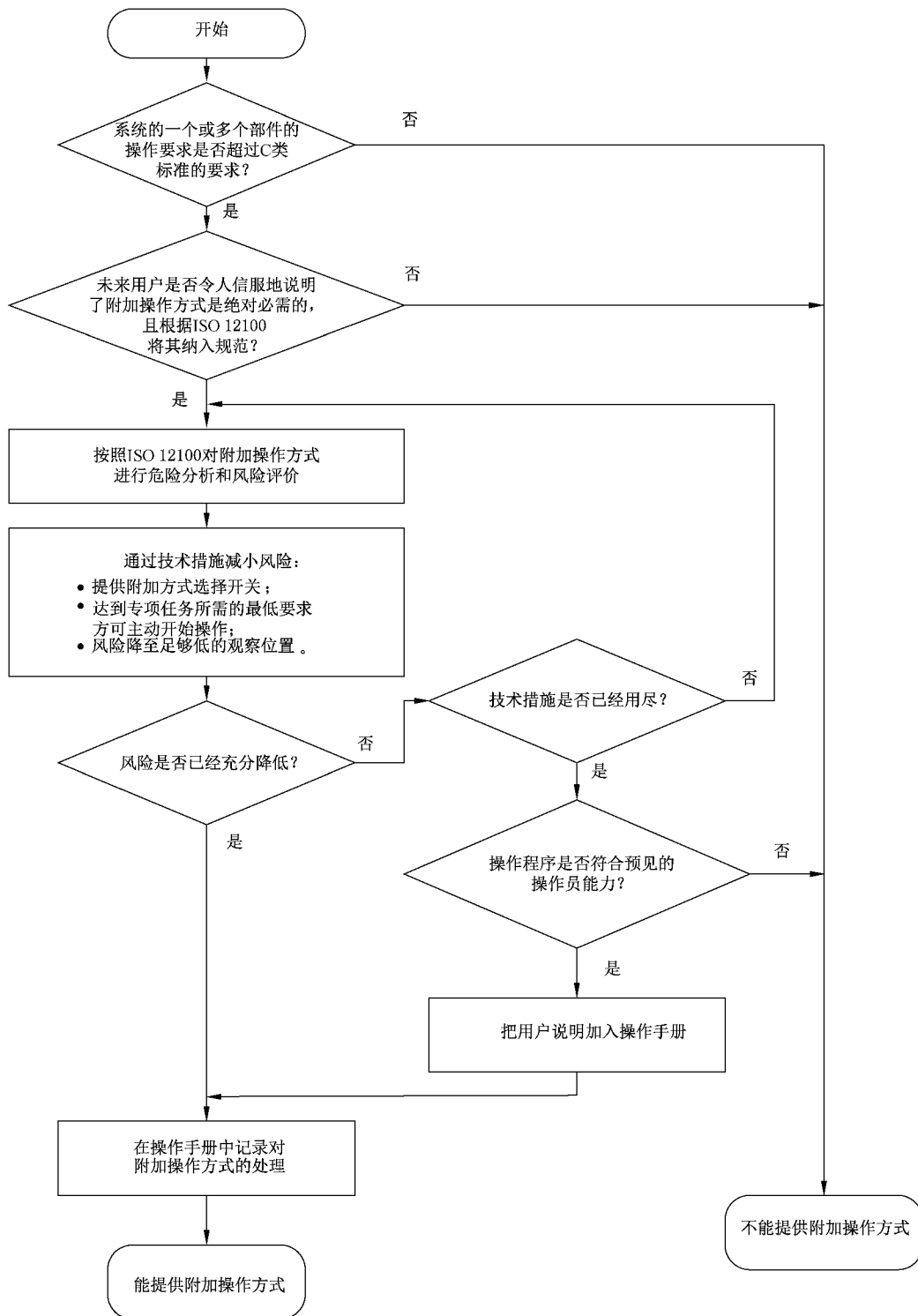


图 F.1 工序观测中的保护措施

附录 G
(规范性附录)

安全要求和措施的验证方法

表 G.1 列出了被认为对应该验证和/或确认的机器人安全非常重要的具体性能要求。
本表的使用,见 6.3 的注。

表 G.1 安全要求和措施的验证方法

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.2	与安全相关的控制系统性能(硬件/软件)									
5.2.1	在使用资料中陈述性能的能力、数据及准则,以确定性能	×								×
5.2.2	性能是 PL=d,结构类别 3					×	×			×
5.2.2	性能是 SIL 2、硬件 1 级容错,验证测试间隔不少于 20 年					×	×			×
5.2.3	风险评估结果用于确定性能							×		×
5.3	设计和安装									
5.3.1	根据条件设计和选择系统	×			×					×
5.3.2	自动方式选择应在安全防护区域外进行	×	×			×				
5.3.3	致动控制应满足 IEC 60204-1 的要求	×								
5.3.3	机器人系统不应响应任何外部远程控制命令或导致危险状况的条件		×		×					
5.3.4	所有动力源应符合制造商的要求	×		×		×				×
5.3.4	电器外罩门应完全打开,并且逃生路线永远畅通	×	×	×	×					
5.3.5	保护性连接应满足 IEC 60204-1 的要求	×		×						
5.3.6	提供隔离危险能源的方法	×	×			×				
5.3.6	应清楚地标注危险能源隔离方法	×								
5.3.7	应提供危险能量的可控释放的方法	×	×			×				
5.3.7	应清楚地标注危险能量的可控释放的方法	×								
5.3.8.1	机器人系统应有保护性停止功能		×			×				
5.3.8.1	机器人系统应有独立急停功能		×			×				
5.3.8.1	保护性停止和急停功能应有连接外部保护装置的接口	×	×			×				
5.3.8.2	能启动机器人运动或其他危险功能的每个控制站应具备急停功能	×	×			×				
5.3.8.2	致动停止功能应停止单元内所有机器人的运动和其他危险的功能		×			×				
5.3.8.2	应具有单独的系统急停或多重功能的控制范围		×			×				
5.3.8.2	单个工作空间内所有急停装置具有相同的控制范围		×			×				
5.3.8.2	在使用资料中有控制范围信息	×								×

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.3.8.2	急停功能应遵守 5.3.8.2 的规定		×	×		×				
5.3.8.2	急停功能应是停止类别 0 或 1		×			×				
5.3.8.2	急停功能应符合 PL=d,类别 3;除非风险评估确定了其他性能规范									×
5.3.8.2	机器人系统电力供应撤除时,急停输出信号(如果提供了)应继续有效,否则应产生急停信号		×	×						×
5.3.11	使用资料中有应急恢复程序	×								×
5.3.11	将应急恢复程序标志或标签贴在机器人系统上,或提供粘贴说明	×								×
5.3.12	标志模糊不清时,应提供其他同等有效的警示措施	×								×
5.3.13	在使用资料中应确定并指明所需任务的照明级别	×		×	×					×
5.3.13	已提供适用于操作的整体照明	×	×	×	×			×		
5.3.14	机器人系统集成应考虑应用的危险性	×			×			×		×
5.3.14	对其他机器的接口要求应遵照使用资料中指定的制造商指导				×	×			×	×
5.3.15	附加的使能装置及其集成应符合 GB 11291 的规定	×			×	×		×	×	×
5.3.15	为安全防护空间内的预期人数提供充足的附加使能装置	×			×	×		×	×	×
5.3.15	与单个机器人控制相关联的多个使能装置具有相同的功能性		×		×		×			×
5.3.15	在单元的某些区域内人员处于附加机器人或其他设备的危险下,处于这些区域的使能装置是联锁的		×		×	×	×	×	×	×
5.3.15	附加联锁设备需要单独进行重启		×		×	×				×
5.4	限制机器人运动									
5.4.2	充分考虑安全空间内的位置、布局和危险,由周边防护设施建立起安全防护空间	×	×		×			×	×	×
5.4.2	通过限制机器人、末端执行器、夹具和工件的运动,建立起了机器人限定空间		×	×				×	×	
5.4.2	限定空间位于安全防护空间内	×	×						×	×
5.4.2	周边安全防护装置的安装不应比限定空间更接近危险,或根据 5.4.3 将周边安全防护装置设计成为限位装置	×	×				×		×	×
5.4.3	机器人的机械式限位装置遵守 ISO 10218-1	×	×	×					×	×
5.4.3	机器人的非机械式限位装置遵守 ISO 10218-1		×				×		×	×
5.4.3	用于机器人非机械式限位装置的控制系統符合 ISO 10218-1,除非风险评估确定另一个性能		×				×	×	×	×
5.4.3	限位空间的任何计算,均包括了与限位装置有关的制动距离		×	×					×	×
5.4.3	已正确调整和固定式限位装置	×	×	×			×			×

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.4.3	使用非机械式限位装置,包括轴及安全软限位(ISO 10281-1)时,根据有实际负载的机器人决定限定空间		×	×			×		×	×
5.4.3	如果机器人速度由满足 5.2.2 要求的监控系统限定,限定空间可以以实际速度为基础。否则,限定空间以机器人的最大速度为基础		×	×			×		×	×
5.4.3	使用资料中包括程序化的安全适用的和空间限位的信息								×	×
5.4.3	将周边防护设施设计为限位装置的情况下,风险评估用来确定防护装置的设计、强度和挠度							×	×	×
5.4.4	动态机械限位装置能够停止具有额定负载和速度的机器人		×	×	×				×	×
5.4.4	和动态限制有关的安全控制符合 5.2 的性能要求					×	×			×
5.4.4	在使用资料中已确定动态限制区的位置						×		×	×
5.5	布局									
5.5.1	周边安全防护已经根据 5.10 的规定实施	×	×	×		×	×		×	×
5.5.1	对保护性装置的选择考虑到预期的加工应力、对被加工材料的影响和其他相关的外部影响	×	×		×				×	×
5.5.1	越过或穿过机械式防护装置的安全距离符合 ISO 13857 的规定	×		×					×	
5.5.1	离连锁防护装置的最小安全距离符合 ISO 13857 的规定	×		×					×	
5.5.1	防止挤压的最小间隙符合 ISO 13857 的规定	×		×					×	
5.5.2	在要求使用手动高速的任务区中保持 500 mm 的最小余隙	×		×	×			×	×	
5.5.2	只要可行,布局设计允许在安全防护空间外执行任务	×							×	×
5.5.2	提供安全恰当的进入方式,通向安全防护空间内的任务位置	×			×			×	×	×
5.5.2	进入的路径和方法无危险	×			×			×	×	
5.5.2	为高频率任务提供永久性进入方法	×			×			×	×	×
5.5.2	为触及不到的高度上的电气设备提供进入方法	×		×					×	
5.5.2	给距离通道平面 0.4 m~2.0 m 高度的相关装置提供进入方法	×		×				×	×	
5.5.2	根据 ISO 14122 选择/设计平台、通道、楼梯、活梯和固定梯子	×		×					×	×
5.5.2	相邻单元之间提供安全防护装置	×	×	×	×			×	×	
5.5.2	物料传送期间,提供相邻单元的安全防护装置	×	×	×	×			×	×	
5.5.3	人员进入材料进出安全防护空间的危险区,会受到检测	×	×		×				×	
5.5.3	安全防护措施防止接触到危险或使危险转化为安全状态	×	×		×				×	
5.5.4	为安全防护空间内的工序观测提供符合 5.6.4.2 和 5.6.4.3 的操作方式或一个单独的控制方式		×			×	×	×		×
5.6	机器人系统操作方式的应用									
5.6.1	在一个多机器人单元中,未被选来进行操作的机器人系统仍处于安全状态		×		×	×		×	×	

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.6.1	单元中未被手动操作的其他机器人不产生危险		×		×	×		×	×	
5.6.2	应避免未经授权的和/或无意的的方式选择	×	×			×	×			
5.6.2	选择方式只启动选定方式而不会启动操作	×	×		×	×	×			
5.6.2	需要用来启动机器人操作的单独致动功能	×	×		×	×	×			
5.6.2	提供操作方式的明确指示	×	×		×					
5.6.2	改变操作方式不会造成危险情况		×		×	×	×			
5.6.3.1	自动方式下进入安全防护空间导致保护性停止		×		×	×	×			×
5.6.3.2	选择自动方式不会覆盖保护性停止或急停状态		×		×	×	×			
5.6.3.2	自动方式的选择设置在安全防护空间外	×	×		×	×	×		×	×
5.6.3.2	切换自动方式导致停止		×		×	×				
5.6.3.3	自动操作从安全防护空间外开启		×		×	×	×		×	
5.6.3.3	所有安全防护装置启动后才可能开启自动方式		×		×	×	×		×	
5.6.3.4	启动和重启是简单操作	×	×		×					×
5.6.3.4	保护措施在启动和重启前运行	×	×			×	×			×
5.6.3.4	安全相关的控制功能遵循 5.2.2 的规定					×	×	×		×
5.6.3.4	提供启动和重启的手动致动联锁		×			×	×			
5.6.3.4	人员在安全防护空间内时,为保护人员而防止启动和重启	×	×		×	×	×		×	×
5.6.3.4	在安全防护空间内,不能启动手动致动的启动和重启控制器	×	×		×	×			×	×
5.6.3.4	提供功能性安全和保护措施,以确保在启动和重启前没有人员在安全防护空间内		×		×	×	×			×
5.6.3.4	必要时,提供现场感应或视听启动前的警告信号		×		×	×	×	×		
5.6.3.4	在安全防护空间内提供易接近的急停装置	×							×	×
5.6.4.1	手动操作干预期间,本地控制使用的是示教盒	×				×	×		×	×
5.6.4.1	控制装置的位置使操作者能够观察到工作区域	×			×				×	
5.6.4.1	停止控制装置设置在每个启动控制装置的旁边	×			×	×			×	×
5.6.4.1	本地控制期间防止其他来源的控制		×			×	×			×
5.6.4.2	已经利用偏置特性来完成机器人工具中心点(TCP)的调整		×	×			×		×	×
5.6.4.2	工具中心点的最大速度不能超过 250 mm/s		×	×	×		×			×
5.6.4.2	风险评估的结果决定是否需要降低速度							×		
5.6.4.2	机器人系统部件及机器人的运动需要功能性使能装置		×		×	×	×			×
5.6.4.3	满足 ISO 10218-1 和示教盒的要求	×	×							×
5.6.4.3	使用资料包括了使能装置的功能性测试									×
5.6.5	手动方式时才有可能使用远程控制		×		×		×	×		×

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.6.5	远程控制期间一次只能有一个单独控制源工作		×		×		×			×
5.6.5	不能因为远程控制而使本地选择无效或导致危险状况		×		×		×			×
5.6.5	只有从本地操作控制才可能激活远程功能		×		×		×			×
5.6.5	远程改变轴和空间的安全软限位参数存在限制		×				×			×
5.6.5	具有激活的远程控制的指示	×	×			×				×
5.6.5	手动高速模式下防止进行远程控制		×			×				×
5.6.5	使用资料提供了手动远程干预的要求							×		×
5.7	示教盒									
5.7.1	在安全防护空间内使用的示教盒遵循 ISO 10218-1 的规定	×	×			×	×			×
5.7.1	示教盒的急停功能遵循 5.3.8.2 的规定	×	×	×		×			×	×
5.7.1	配有电缆的示教盒具备一根足够长和耐用的电缆	×	×	×					×	×
5.7.1	妥善存放示教盒以防损坏	×			×	×		×	×	×
5.7.2	无缆或可拆卸示教盒需满足 ISO 10218-1 的要求	×	×		×	×				×
5.7.2	急停和使能设备满足 ISO 10218-1 的规定	×	×		×	×				×
5.7.2	避免意外控制	×	×		×	×	×			×
5.7.2	无缆示教盒不可与多个机器人系统同时连接	×	×		×	×	×			×
5.7.2	信号丢失导致停止和谨慎的重启行为		×		×	×				×
5.7.2	断开和存储符合要求	×	×		×	×			×	×
5.7.2	提供单点控制		×		×		×			×
5.7.3	多机器人示教控制器得到哪个机器人正在被控制的指示	×	×						×	
5.7.3	选定的所有多个机器人在同一操作方式下	×	×			×	×			×
5.7.3	未被选择的机器人不会出现危险		×		×	×			×	×
5.7.4	手动引导的控制器符合 ISO 10218-1 的规定	×	×			×	×	×		×
5.8	保养和维修									
5.8.1	提供检查和维修程序,考虑制造商的推荐并允许持续的安全操作	×			×			×	×	×
5.8.1	使用资料包括了设备的与安全相关零件的周期功能性测试要求	×							×	×
5.8.2	系统的设计要能安全地进行维护	×	×					×	×	×
5.8.2	利用使用资料中的有关细节,使系统具有控制危险能量的方法	×	×		×	×			×	×
5.8.2	在没有能量隔离的情况下,对于确定要执行的任务,系统具备足够的可替代的安全防护装置	×	×		×	×		×	×	×
5.8.3	防护装置要有足够尺寸以便容易进入	×	×	×					×	×

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.8.3	为不经常进行的维护或服务任务提供的固定式防护装置,只有使用工具方可移去	×	×							×
5.8.3	由保护性装置及较好是活动式防护装置保护常用进入点。移动式防护装置到达安全防护位置时不启动开始指令	×	×			×		×	×	×
5.8.3	当活动式防护装置已关闭,并可能仍停留于安全防护区域内时,提供附加保护措施	×	×			×	×	×	×	×
5.8.3	与重启连锁连接的现场感应装置符合 IEC 61496-1 类型 2 的最低要求	×	×			×	×	×		×
5.9	集成制造系统(IMS)接口									
5.9.1	系统的风险评估和集成要考虑安全空间内其他设备带来的危险	×						×	×	×
5.9.2	IMS 具有单独的急停功能,可影响该机器的所有相关部件	×	×		×	×			×	×
5.9.2	急停符合 5.3.8.2 的要求	×	×			×			×	×
5.9.2	使用资料包括了每个急停装置的控制范围的信息									×
5.9.3	IMS 与机器人之间的相关安全控制器符合 5.2.2 的规定					×	×		×	×
5.9.3	安全电路影响到区域内和与相邻区域接口处的危险运动	×	×		×	×	×		×	×
5.9.4	选择本地控制后,通知 IMS 控制系统		×			×				×
5.9.4	IMS 不能覆盖本地控制		×			×	×			
5.9.4	急停和保护性停止功能在本地控制期间仍可运行		×		×	×	×			
5.9.4	选择本地控制的装置接近被控设备	×			×				×	×
5.9.4	从安全防护空间内断开本地控制的选择不引发危险状况	×	×		×	×			×	×
5.9.4	如果选择断开能够发生在安全防护空间内,则要求从单元外进行单独确认		×		×	×			×	×
5.9.5	附加使能装置符合 5.3.15 的规定		×			×	×			×
5.9.5	使能装置是连锁的并和 IMS 区域一致		×		×	×	×		×	×
5.9.6	方式选择符合 ISO 10218-1 的规定		×			×	×			×
5.9.7	IMS 的设计要易于进行安全手动干预,如果必要,IMS 要进行分区	×	×		×	×		×	×	×
5.9.7	根据 ISO 11161 将机器人系统集成到一个任务区					×			×	×
5.10	安全防护									
5.10.1	防护装置和保护性装置符合 ISO 12100 的要求									×
5.10.2	周边安全防护装置的选择要考虑所有危险和任务	×			×			×	×	
5.10.3.1	安全防护装置应安装牢固,位置合适	×		×	×				×	
5.10.3.2	固定式和移动式活动式的防护装置满足 ISO 14120 的要求			×		×			×	

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.10.3.2	距固定式和活动式防护装置的任何危险的最小距离,根据 ISO 13857 的相关要求决定			×		×			×	
5.10.3.2	为防止进入防护装置,利用 ISO 13857 决定最小安全距离			×		×			×	
5.10.3.3	防止启动和重启的现场感应保护装置遵循 5.10.5.3 的规定	×	×		×				×	×
5.10.3.4	提供间隙的现场感应保护装置遵循 5.10.5.3 的规定	×	×		×				×	×
5.10.4.1	所有防护装置满足 ISO 12100 和 ISO 14120 中的适用要求	×								×
5.10.4.1	和防护装置有关的联锁装置满足适用要求	×	×			×				×
5.10.4.1	固定式防护装置需要工具来移除	×	×							
5.10.4.1	当防护装置拆除时,在要求之处,固定系统连接在防护装置或机器上	×	×							
5.10.4.1	周边安全防护装置的安装地点要比限定空间更远离危险(见 5.10.4 的例外情况)	×		×				×	×	
5.10.4.2	防护装置底部和地板之间的间隙或防护装置内的其他间隙,不允许人员越过、钻过、绕过或穿过该防护装置而遭遇危险			×	×				×	
5.10.4.2	防护装置的高度至少为 1 400 mm			×						
5.10.4.3	和活动式防护装置相关的联锁装置满足适用要求		×			×				×
5.10.4.3	处于关闭位置的活动式防护装置防止操作员到达危险区域	×			×				×	
5.10.4.3	活动式防护装置向侧面或远离危险的方向打开,而且不能进入安全防护空间内	×	×						×	
5.10.4.3	在操作员接近危险前,通过联锁将任何危险转化成安全状态		×		×					
5.10.4.3	活动式防护装置位置安放恰当(见 5.10.3.2)			×					×	×
5.10.4.3	用于启动开始闭合(控制防护装置)的移动式防护装置满足的适用要求		×			×				×
5.10.4.3	活动式防护装置联锁功能至少满足 5.2.2 的要求					×				×
5.10.4.3	活动式防护装置的重置致动器满足 5.6.3.4 的要求					×				×
5.10.4.4	要求之处,除了控制联锁还提供防护锁		×			×				×
5.10.4.4	防护锁符合 5.10.4.4 a) 和 5.10.4.4b) 的规定		×		×					×
5.10.4.4	用作锁定或解锁条件的进程参数满足和联锁功能相同的功能性安全要求		×			×	×	×		×
5.10.4.5	安全防护空间具备防止人员被困于其中的方法		×						×	×
5.10.5.1	电敏和压敏保护设备满足适用要求									×
5.10.5.2	用于启动保护性停止的感应防护设备位置安放恰当			×					×	×
5.10.5.2	牢固安装传感保护设备,安装位置处于操作员无法接近的检测区域	×	×	×					×	
5.10.5.2	如果危险状况发生时传感保护装置启动,应引发保护性停止		×			×	×			×

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.10.5.2	传感保护装置启动后,应防止传感保护设备保护的危險状况发生任何危險运动或情况,直到传感保护设备复位		×			×	×			
5.10.5.2	传感保护设备复位不会自行引发危險状况		×			×				
5.10.5.2	借助运动部件朝向趋近方向的最大延伸距离,使用最小安全距离公式确定从各方向到传感保护设备的最小距离			×						×
5.10.5.2	当操作员的部分身体停留在安全防护空间内时,应采取额外措施,防止危險情况		×			×	×		×	
5.10.5.2	如果操作员可能无法知道重置控制器的位置,采取补充保护措施以防止重启联锁的复位		×			×	×		×	
5.10.5.2	重启联锁的复位需要谨慎的人工操作		×							
5.10.5.3	用于防止启动的现场感应保护装置结合其他安全措施来使用		×			×	×		×	
5.10.5.3	定位和配置现场感应装置,使处于整个检测区内的人员或人体的一部分可被检测到	×	×						×	
5.10.5.3	需要之处,提供补充措施确保无法接近检测区	×	×		×				×	
5.10.6.1	提供措施确保操作员不会暴露于因操作手动物料装卸站而造成的进一步危險中	×			×					
5.10.6.1	采取措施防止操作员暴露于和应用有关的危險中	×	×		×	×			×	×
5.10.6.2	采取措施防止操作员接近由于手动站移动造成的危險	×	×		×				×	×
5.10.6.2	移动站和任何固定元件之间的间隙不超过 120 mm			×					×	
5.10.6.3	使用现场感应来检测共用工作空间内的操作员时,感应装置的检测区覆盖整个共用工作区		×	×			×		×	
5.10.6.3	共用工作区设有重启联锁时,要提供措施防止重启联锁不慎复位	×	×			×				
5.10.6.3	在共用工作空间内进行手动重置时,在重置装置的地方应该能看到整个共用工作空间,或者应用附加措施	×	×			×			×	×
5.10.7	要有物料进出开口的最小尺寸	×	×	×					×	
5.10.7	避免物料和开口侧边存在挤压/切断的危險	×	×						×	
5.10.7	防止接近危險,或检测到接近危險	×	×			×		×	×	
5.10.7	借助抑制功能或改变保护区(如空白),电敏防护装置(ESPE)允许物料通过	×	×	×	×	×			×	×
5.10.7	抑制功能满足 GB/T 16855.1 的要求					×				×
5.10.7	抑制功能和保护区改变(如空白)的功能性安全等级至少和 ESPE 风险评估决定的等级一致					×		×		×
5.10.8	已经采取措施防止操作员接近相邻单元的危險,或终止相邻单元的危險	×	×		×			×	×	
5.10.8	防止接近相邻单元危險的固定式防护装置最低高度为 1 400 mm			×					×	

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.10.8	除固定式防护装置外对其他措施的选用符合 4.5 的规定							×	×	×
5.10.8	为生产操作采取的抑制措施,其功能性安全水平由风险评估确定		×			×	×	×		×
5.10.9	末端执行器和工具更换系统的设计和构造,应遵循动力供应的损失或恢复不会导致危险的原则	×	×			×		×		×
5.10.9	工具更换系统的设计确保误用不会导致危险情况	×	×			×		×		×
5.10.9	工具更换只能在工具更换位置进行		×			×	×		×	
5.10.9	工具更换系统满足预期的静态和动态要求		×	×				×		×
5.10.10	抑制功能仅限于在必要的工序中使用	×				×	×	×	×	×
5.10.10	抑制终止后,危险区域内的人员不能检测不到		×					×	×	
5.10.10	只要抑制条件恰当,自动地启动和终止抑制功能		×		×	×	×			
5.10.10	抑制功能获得的安全性能等级和被抑制的保护性功能相当		×			×	×	×		×
5.10.10	抑制功能的性能等级不会反向影响保护性功能的性能等级		×			×	×	×		×
5.10.10	抑制功能出现故障情况下,排除故障前不能再运行连续的抑制功能		×			×	×			
5.10.10	使用资料包括了对抑制的方法、位置、区域和功能性的描述								×	×
5.10.11	需要暂停安全防护措施的任务具有专用操作方式	×	×			×	×	×		×
5.10.11	操作方式的选择通过安全方法完成	×	×			×	×			×
5.10.11	安全防护自动暂停时,满足 5.10.11a)~5.10.11f)的要求	×	×		×	×				×
5.10.11	安全防护自动暂停时,任务不需要的设备处于保护性停止状态,或者处于操作员的直接控制下		×		×			×	×	
5.10.11	提供紧急境况下需手动暂停安全防护的使用资料									×
5.11	协作机器人									
5.11.1	使用资料包括了要求的安全防护措施和方式选择的描述									×
5.11.2	集成者已经完成考虑到整个协作工作空间的风险评估[指 5.11.2 a)]							×	×	×
5.11.2	协作工作空间内的机器人满足 ISO 10218-1 的要求					×	×		×	×
5.11.2	用于存在检测的保护性装置满足 5.2.2 的要求					×	×			×
5.11.2	协作工作空间的附加保护性装置满足 5.2 的要求					×	×			×
5.11.2	设计和安装安全防护装置,防止或检测到人员进一步进入(协作空间外的)单元	×	×		×			×	×	
5.11.2	如果人员闯入协作空间外的安全防护空间,机器人停止,而危险中止		×		×				×	
5.11.2	周边安全防护防止或检测到人员进入非协作的安全防护空间	×	×		×				×	

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)									
		A	B	C	D	E	F	G	H	I	
5.11.2	协作空间内连接的其他机器具有与安全相关的功能,这些机器符合 5.2 的要求,除非风险评估另有结论					×	×	×		×	
5.11.3	操作员直接和机器人交互的协作工作空间应清晰定义(如地面标记、标志等)	×			×				×		
5.11.3	和保护性设备结合在一起的机器人性能特征符合 5.2.2 的规定		×			×	×			×	
5.11.3	一人以上进行协作操作时,每个人均根据 5.2.2 得到控制装置的保护	×	×			×	×	×			
5.11.3	协作工作空间允许执行简单任务	×	×		×			×		×	
5.11.3	设备的位置不会引起额外危险	×			×			×	×		
5.11.3	在小于 500 mm 余隙的区域,附加保护性措施防止人员陷于被困或被夹的危险	×	×	×				×	×	×	
5.11.4	从自主操作到协作操作,再转回自动操作期间,不可危及人身安全	×	×		×	×	×	×	×	×	
5.11.5.1	选择合适的协作机器人操作安全特性							×		×	
5.11.5.1	所选安全特性中被检测到的故障,根据 5.3.8.3 会导致保护性停止		×			×	×	×		×	
5.11.5.1	如果检测到故障,从协作工作空间外进行谨慎重置后,自主操作才能恢复		×		×	×	×		×		
5.11.5.2	如果使用安全适用的监控性停止技术,当人员进入协作工作空间时,机器人停止运动,并保持安全适用的监控性停止状态		×		×	×		×	×		
5.11.5.3	如果手动引导操作,当机器人达到移交位置,根据 ISO 10281-1 导致一个安全适用的停止		×		×	×	×			×	
5.11.5.3	手动引导装置满足 ISO 10281-1 的要求		×			×	×			×	
5.11.5.3	如果手动引导操作,需要清楚地看到整个协作工作空间	×			×				×		
5.11.5.3	当操作员释放引导装置时,根据 ISO 10281-1 导致一个安全适用的监控性的停止		×		×	×	×			×	
5.11.5.4	如果使用速度和位置监控技术,协作空间内的机器人符合 ISO 10281-1 要求的					×	×		×	×	
5.11.5.4	通过风险评估确定参数,ISO/TS 15066 提供了指南							×	×	×	
5.11.5.5	如果利用功率和力的限制技术,协作空间内的机器人符合 ISO 10281-1 的要求					×	×		×	×	
5.11.5.5	通过风险评估确定参数,ISO/TS 15066 提供了指南							×	×	×	
5.12	机器人系统的试运行										
5.12.1	试运行计划包括试运行期间需要的保护措施(临时安全防护措施)信息	×							×	×	×

表 G.1 (续)

参考章节	安全要求和/或措施	验证和/或确认方法(见 6.2)								
		A	B	C	D	E	F	G	H	I
5.12.2	临时防护措施防止风险评估确定的危险发生	×	×					×	×	×
5.12.2	最低限度,已建立警示屏障来确定限定空间	×							×	
5.12.2	使用资料中已确定了临时安全防护措施									×
5.12.3	初始启动程序计划至少包括 5.12.3 中所列各项									×
注：“×”表示需要验证。										

参 考 文 献

- [1] GB/T 12643—2013 工业机器人 词汇
- [2] ISO 13849-2, Safety of machinery—Safety-related parts of control systems—Part 2: Validation
- [3] ISO 13851, Safety of machinery—Two-hand control devices—Functional aspects and design principles
- [4] ISO 14123-1, Safety of machinery—Reduction of risks to health from hazardous substances emitted by machinery—Part 1: Principles and specifications for machinery manufacturers
- [5] ISO 14123-2, Safety of machinery—Reduction of risks to health from hazardous substances emitted by machinery—Part 2: Methodology leading to verification procedures
- [6] ISO 14159, Safety of machinery—Hygiene requirements for the design of machinery
- [7] ISO 14738, Safety of machinery—Anthropometric requirements for the design of workstations at machinery
- [8] ISO/TS 15066¹⁾, Robots and robotic devices—Safety requirements—Industrial collaborative workspace
- [9] ISO 19353, Safety of machinery—Fire prevention and protection
- [10] ISO/TR 23849, Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
- [11] IEC 60204 (all parts), Safety of machinery—Electrical equipment of machines
- [12] IEC 60364-7-729, Low-voltage electrical installations—Part 7-729: Requirements for special installations or locations—Operating or maintenance gangways
- [13] IEC 61496-2, Safety of machinery—Electro-sensitive protective equipment—Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs)
- [14] IEC 61496-3, Safety of machinery—Electro-sensitive protective equipment—Part 3: Particular requirements for Active Opto-electronic Protective Devices responsive to Diffuse Reflection (AOPDDR)
- [15] IEC/TR 61496-4, Safety of machinery—Electro-sensitive protective equipment—Part 4: Particular requirements for equipment using vision based protective devices (VBPD)
- [16] IEC 62079, Preparation of instructions—Structuring, content and presentation
- [17] EN 563, Safety of machinery—Temperatures of touchable surfaces—Ergonomics data to establish temperature limit values for hot surfaces
- [18] EN 1093 (all parts), Safety of machinery—Evaluation of the emission of airborne hazardous substances
- [19] EN 1127-1, Explosive atmospheres—Explosion prevention and protection—Part 1: Basic concepts and methodology
- [20] EN 1127-2, Explosive atmospheres—Explosion prevention and protection—Part 2: Basic concepts and methodology for mining
- [21] EN 1837, Safety of machinery—Integral lighting of machines
- [22] EN 12198 (all parts), Safety of machinery—Assessment and reduction of risks arising

1) 制定中。

from radiation emitted by machinery

[23] CEN/TR 14715, Safety of machinery—Ionizing radiation emitted by machinery—Guidance for the application of technical standards in the design of machinery in order to comply with legislative requirements

[24] BGIA/DGUV study—Procedural Guideline for the Arrangement of Workplaces with Collaborative Robots
