ICS 25.040.30
J 28

中华人民共和国国家标准

GB/T 39402—2020

面向人机协作的工业机器人设计规范

Design specification of collaborative industrial robot

2020-11-19 发布　　2021-06-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本标准起草单位:遨博(北京)智能科技有限公司、北京机械工业自动化研究所有限公司、北京航空航天大学、首都师范大学、安徽配天机器人技术有限公司、清能德创电气技术(北京)有限公司、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、武汉科技大学、上海沃迪智能装备股份有限公司、广东省智能制造研究所、清华大学、莱茵技术(上海)有限公司、深圳吉阳智能科技有限公司。

本标准主要起草人:魏洪兴、宋仲康、赵永利、崔元洋、邵振洲、杨书评、谈金东、朱志昆、刘刚、王钰、刘颖、李煜、王泽涵、张俊丰、赵晓飞、闵华松、童上高、周雪峰、肖曦、肖玲、黄永衡。

引　言

在工业生产中，人类擅长解决那些精度要求不高但有一定灵活度要求的问题，而机器则适合解决具有高精确性、高强度以及高承载力特点的作业。为了保证足够的安全性，在传统的机器人应用中，一般配备防护装置，以防止对操作人员造成伤害。因此在这种环境下，人工干预或配合的工作就很难使用机器人系统来完成。而面向人机协作的工业机器人，不仅具备机器人的性能特点，同时还能与人协同操作，可大幅拓宽机器人的应用领域，提升生产效率。本标准提供了一种面向人机协作的工业机器人设计规范，为制造商以及集成商制造和使用具备人机协同操作功能的工业机器人提供标准依据。

面向人机协作的工业机器人设计规范

1 范围

本标准规定了面向人机协作的工业机器人的术语和定义、设计原则和设计要求、使用信息、验证和确认方法。

本标准适用于面向人机协作的工业机器人的设计和开发。

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 5226.1—2019 机械电气安全 机械电气设备 第1部分：通用技术条件

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

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

GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小

GB/T 16754—2008 机械安全 急停 设计原则

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—2003 电磁兼容 通用标准 工业环境中的抗扰度试验

GB 17799.4—2012 电磁兼容 通用标准 工业环境中的发射

GB/T 20438.1—2017 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 36008—2018 机器人与机器人装备 协作机器人

3 术语和定义

GB/T 15706—2012、GB 11291.1—2011界定的以及下列术语和定义适用于本文件。为便于使用，以下重复列出了GB/T 15706—2012、GB 11291.1—2011中的某些术语和定义。

3.1

危险 hazard

潜在的伤害源。

[GB/T 15706—2012，定义3.6]

3.2

风险 risk

伤害发生的概率与伤害严重程度的组合。

[GB/T 15706—2012，定义3.12]

3.3

风险评估 risk assessment

风险分析和风险评价的全过程。

注：改写GB/T 15706—2012，定义3.17。

3.4

协作操作　collaborative operation

规定了一种专门设计的机器人系统与操作者工作于协作工作空间中的行为。

注：改写 GB 11291.1—2011，定义 3.4。

3.5

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。

注：改写 GB 11291.1—2011，定义 3.5。

3.6

人机协作的工业机器人　collaborative industrial robot

具备人机协同操作功能的多关节机械手或多自由度工业机器人。

3.7

静态碰撞保护　quasi-statics collision protection

机器人在有源（带电）处于静止状态时，外部人或设备与机器人发生非预期物理碰撞触发的机器人安全保护功能。

3.8

安装姿态自适应　mounting pose adaptation

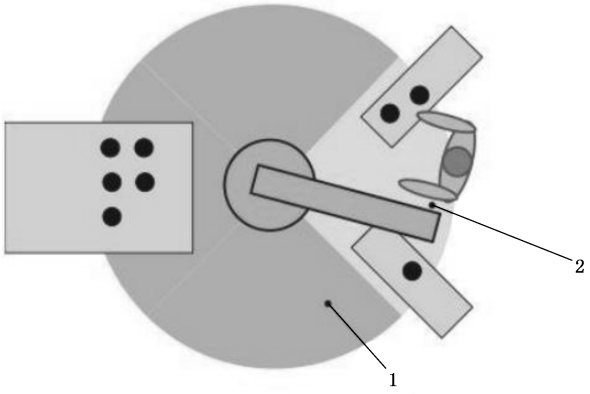
机器人可自我感知当前安装姿态，并依据姿态感知结果调整软件算法以使机器人运行在正确的状态。

4　设计原则

4.1　通则

为了避免碰撞或限制接触力，设计中应使用安全控制系统实时监控人机协作的工业机器人的运行速度及其输出功率。为了满足人机协同工作的柔性化生产需求，面向人机协作的工业机器人应具备尺寸小，且能安装在复杂狭小工作空间内的特点。

GB/T 36008—2018 描述了包括面向人机协作的工业机器人及其相关系统集成的安全性要求，该机器人的操作特性与传统机器人系统及其他机器系统截然不同。在面向人机协作的工业机器人操作中，操作者可近距离地工作在加载了动力的机器人旁边，且可在协作空间中发生物理接触（协同工作空间示例见图 1，俯视图）。



说明：

1——操作空间；

2——协同工作空间。

图 1　协同工作空间示例

任何面向人机协作的工业机器人系统设计都应满足保护性指标，以保证在机器人进行协作作业时操作者的安全。另外，风险评估也是必要的，在该机器人系统应用时，对其进行相应的危险识别和风险估计，采取措施降低风险。

4.2　危险识别与风险评估

4.2.1　通则

面向人机协作的工业机器人应符合 GB 11291.1—2011 的要求，在集成使用时应符合 GB 11291.2—2013 的规定。

集成商应对 GB 11291.1—2011 中所述的协作操作进行风险评估，特别要考虑到操作者和机器人系统之间所涉及的潜在接触或者可合理预见的接触，另外，操作者在协作交互中预计的可达性也要考虑。

在机器人应用集成方案的设计中，使用者应参与集成方案的风险评估和工作空间设计。

4.2.2　危险识别

机器人与机器人系统的主要危险列表按 GB 11291.2—2013 中附录 A 规定，是按 GB/T 15706—2012 的规定进行危险识别和风险评估的结果。特定的协作应用（例如搬运、激光切割和加工）可造成进一步的危险（例如烟雾、气体、化学物质和热物质）。这些危险应编制为特定协作应用风险评估中的独立依据。

危险识别的流程应至少包含以下内容：

a）　机器人相关的危险，包括：

　　1）　机器人的特性（例如载重、速度、力、动力、力矩、功率、几何形状、表面形状与材料等）；

　　2）　操作者与机器人发生的物理接触；

　　3）　操作者临近机器人的潜在危险（例如工作于机器人下方）；

b）　机器人系统的相关危险，包括：

　　1）　末端与工件的危险，包括缺少人体工学设计、锋利边缘、工件缺损、凸出、使用换刀装置等；

　　2）　有关零件摆放、结构朝向的操作者运动与位置（固定结构、建筑支撑、墙等），以及固定物的危险位置；

3） 固定物设计、堆砌码放与操作以及其他危险；
4） 与操作者或生产线上其他设备发生物理接触；
5） 任何手控的机器人引导设备的设计与摆放(例如可达性、人体工学、潜在误用、来自控制与状态指示中可能的混淆等)；
6） 周边设备的影响(例如毗邻机器人的保护罩被移开、激光切削的逼近等)；

c） 应用的相关危险，包括：
1） 过程中的特定危险(例如温度、部件迸出、焊接飞溅等)；
2） 个人防护性装备使用所导致的限制；
3） 人体工学设计的不足(例如导致缺失注意力、不合理操作等)。

4.2.3 任务识别

集成商在使用协作机器人开发人机协作应用的过程中，所有在合理范围内可预见的任务与危险都应一同进行识别并评估安全性。协作任务的特性如下：

a） 操作者和运动的机器人系统处在协作空间下的频繁性；
b） 操作者与机器人系统接触力(例如手动引导、与工具或工件的物理交互等)；
c） 机器人系统自主操作与协作操作之间的过渡；
d） 协作操作完成之后，进行自动或手动重启机器人系统的动作；
e） 多人任务；
f） 协作空间中的任何额外任务。

4.2.4 消除危险与降低风险

识别危险后，有必要在采取适当措施前，评估面向人机协作的工业机器人的系统相关风险，以充分降低风险。这些措施基于以下基本原则，按优先顺序列出(见 GB 11291.2—2013 的 4.1.2)：

a） 通过设计消除危险或通过替代降低风险；
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(例如停车、限制力、限制速度)；
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。

对于传统机器人系统来说，降低风险可由分隔操作者和机器人系统来实现。而对协作操作来说，机器人系统及其工作空间在设计与应用时，降低风险应重点列出。针对协作操作风险降低的方法在第 5 章规定。

5 设计要求

5.1 通则

应依据 GB/T 36008—2018 以及 GB 11291.1—2011 中有关降低危险的原则来设计机器人。

机器人和机器人系统的设计及制造应达到 5.2 的要求。

5.2 通用要求

5.2.1 电磁兼容性(EMC)

机器人的设计和制造应符合 GB/T 17799.2—2003 及 GB 17799.4—2012 的要求，检查项目见表 1。

表 1　电磁兼容(EMC)检查项目

序号	检查项目	依据标准章条号
1	150 kHz～30 MHz 传导发射	GB 17799.4—2012 表 2
2	30 MHz～1 000 MHz 辐射发射	GB 17799.4—2012 表 1 中 1.1
3	静电放电	GB/T 17799.2—2003 表 1 中 1.3
4	射频调幅电磁场	GB/T 17799.2—2003 表 1 中 1.2
5	快速瞬变	GB/T 17799.2—2003 表 2 中 2.2、表 4 中 4.2
6	浪涌	GB/T 17799.2—2003 表 2 中 2.3、表 4 中 4.3
7	射频共模	GB/T 17799.2—2003 表 2 中 2.1、表 4 中 4.1
8	工频磁场	GB/T 17799.2—2003 表 1 中 1.1

5.2.2　电气要求

机器人电气设备的设计及制造应符合 GB/T 5226.1—2019 的相关要求。

机器人有可能与操作者在进行协同操作时发生直接物理接触的裸露部分，电气参数应设置在人体可接受的安全电压范围内，电压不应高于 36 V。

5.2.3　防护等级

机器人在与操作者进行协同操作时有可能发生直接的物理接触，机器人应具备防护性能，以保证机器人本身控制系统的可靠性与安全性。与人发生物理操作时，任何情况下均不能伤害操作者。机器人应至少满足以下条件：

——机器人 IP 防护等级达到 IP42 或以上；

——机器人具备防静电安全设计；

——机器人具备防意外触电安全设计。

5.2.4　安装要求

机器人应具备安装姿态自适应功能，确保机器人在底座上安装、吊装、壁装及其他特定安装方式下均能正常工作，并保证机器人在改变安装位置后拖动示教功能的安全性。

5.3　机械设计

5.3.1　机械结构

面向人机协作的工业机器人的机械结构设计应考虑到人与机器人的协同工作，因此，机器人各个关节的机械连接方式应考虑人的身体部位不会被机器人夹伤或挤压。

机器人与人及工作单元内周边设备在协同工作时，直接发生接触的部分不应有锋利的边缘、突起的棱角等易产生危险的机械结构。

在人机协同工作时，对于机器人与人或设备能发生直接接触的机械结构，应充分考虑降低发生物理接触时的伤害，应至少采用以下一种设计方式：

a)　增加接触表面积：

　　1)　圆边与圆角；

　　2)　平滑表面；

3） 兼容性的表面。

b） 吸收能量，延长能量传递时间，降低冲击力：

1） 缓冲衬垫；

2） 可变形的组件；

3） 兼容性的关节与连杆。

c） 限制运动质量。

d） 设计可变刚度的驱动关节。

机器人各关节的机械连接方式，应充分考虑不增加额外的风险。各关节的机械连接机构应采用平滑过渡的机械结构设计，不应使机器人外观结构上有直接的突出部分。

因机器人机械机构设计而导致人体部位可能被夹住或锁死的，应在机器人有该风险部位增加明显风险标识，并在用户使用手册上明确指出。

5.3.2 刹车装置

设计机器人刹车方案时，应确保机器人在无驱动源（例如断电）状态下刹车处于抱闸锁死状态，并在任意姿态下都不会由于自身重力而发生非人为操作的移动。

在紧急情况或异常情况下，去除机器人驱动源（例如断电），机器人各关节应仍能在人为干预下运动，确保在意外夹到操作员等紧急异常情况下，可人为移开机器人，解除紧急情况或异常情况。此方式下，机器人刹车设备应确保机器人在无驱动源状态下，各关节能够在一个成年人的外力作用下移动。解除紧急情况或异常情况的操作应易于接近、易于操作，且具备防误操作设计。在用户信息手册上应明确指出这种操作的说明，且应有培训人员应对紧急或异常情况的建议。

用户信息手册上应包含对重力或释放刹车装置可导致的额外危险的警告。只要可行，警告标识应贴于解除紧急情况或异常情况装置的附近。

5.4 人机交互界面

5.4.1 总体要求

面向人机协作工业机器人的人机交互界面设计应考虑提升人机交互的易用性、直观性以及安全性。

5.4.2 示教界面

机器人示教界面应显示机器人实时状态参数，包括在选定坐标系下的姿态及位置参数。示教界面应提供不同坐标系选项，用户可据此选择在不同的坐标系下来示教机器人。机器人的姿态及位置参数应依据用户选择的不同坐标系而改变。

机器人示教界面应提供示教时机器人运动速度控制选项，用户可在示教状态下实时控制机器人在安全速度下运行。

机器人示教界面应提供机器人仿真界面选项。进入仿真界面后，真实机器人在任何情况下均不能发生运动。仿真界面下，用户对机器人的所有运动控制均由仿真机器人体现。

示教界面应提供直观形象的机器人关节控制、末端位置控制、末端姿态控制显示。

5.4.3 编程方式

面向人机协作的工业机器人的编程方式应具备模块化、任务级、简单易用等特性，确保人机协作的可靠交互性。编程界面应至少提供以下编程方式中的一种：

——采用树状编程结构，控制流程清晰显示在操作界面上，确保用户可快速排查控制逻辑；

——采用任务级编程方式，将常用固定的运动控制指令集合为一个任务模块，用户可直接调用；

——采用可视化编程方式，用户可依据单个编程指令操作机器人运动到相应位姿，实时观察机器人状态。

机器人运行工程文件的编写应具备可实时修改、调试方便等功能，降低用户使用门槛。应至少包含以下几种功能：

——工程文件可进行新建、保存、打开文件及进行缺省配置；

——工程文件可进行启动、暂停、继续、停止和单步操作；

——编辑工程文件时，可进行撤销、恢复、剪切、复制、粘贴、删除操作；

——编辑工程文件时，可使用常用简单编程指令来编写程序；

——可设置及调用变量；

——提供脚本文件导入功能；

——提供协作编程选项，例如手动引导、轨迹示教（机械臂可自动学习用户示教轨迹及以往的运行轨迹）等功能。

5.4.4 界面管理

机器人软件应至少包含以下界面设置、显示及接口功能：

——显示锁屏时间及锁屏密码；

——显示机器人日志信息，包括日期、时刻、消息类别、消息描述等信息；

——显示机器人控制柜、示教器及各关节电压电源温度状态；

——直接在机器人软件界面进行版本升级，并具备版本信息显示功能；能够清晰显示并区分不同版本；

——提供坐标系标定功能，坐标系标定完成后，用户根据不同应用场景对机器人进行示教及编程；

——提供工具标定功能，用户可在使用不同工具时进行工具参数切换；

——进行外部设备设置，以同其他机器人或外部设备进行通信及控制；

——具备离线编程功能，对用户开放离线接口，用户可快速导入第三方离线编程软件数据到控制系统。

5.5 外部接口设计

5.5.1 功能设计

面向人机协作的工业机器人应具备强大、便捷的外部设备融合能力，提升人机协作功能的多样化需求。用户可在外部设备扩展界面下添加扩展设备，方便集成应用。机器人外部接口应包含但不限于以下功能：

a) 脚本语言扩展库。脚本语言的扩展库应涵盖机器人的所有控制功能，可充分利用脚本语言的特性，使软件具备更高的扩展性和移植性，并且能够充分地利用脚本语言丰富的库资源，使机器人软件扩展更加灵活，功能更加丰富。

b) 通用软件开发包 SDK。提供了一套基于标准协议的机器人控制接口，使得用户能够更加便捷、快速地将机器人集成到自己的项目中。

c) 脚本编辑器软件。为用户提供了一套完整的脚本开发环境，使得用户可在离线的情况下，对机器人进行编程工作。编程结束后脚本可直接在机器人示教器软件中运行。

d) 机器人控制器插件接口。允许第三方开发者根据自己的需求扩展示教器软件功能，使得软件具有无限扩展的能力。例如：

1) 将机械手爪添加到控制器软件中，可显示在人机交互界面上；

2) 将 Modbus 设备添加到控制器软件中，可显示在人机交互界面上；

3） 将智能相机集成到控制器软件中，可显示在人机交互界面上；

4） 码垛工艺包等等。

e） 提供机器人操作系统(ROS)接口，使得用户可依托 ROS 平台上强大的功能包和扩展库，快速、便捷开发机器人应用。

5.5.2 状态和指示

指令装置的状态应在任何时候都清晰显示，如电源开启、操作模式、故障报警等。对于操作者来说，状态指示应放在明显的位置。

在远程控制时，每个指令装置应清楚地识别其控制的机器人的部件。远程控制系统的设计和制造应针对：

——机器人的相关部件；

——相关功能。

5.5.3 连接和断开

无论有意或无意的任何指令装置的连接、断开和重连接，或指令装置发生连接故障时，若继续运行任务会导致不可接受的风险，则机器人应启动保护性停止。

远程控制时，机器人应设计、制造成仅对来自预定控制单元的信号做出反应。

5.5.4 接口使用权限管理

即使通过远程访问，也应采取措施以避免未授权的控制或参数改变。根据风险评估，应提供避免非授权使用的方法(例如密码保护)。例如使用钥匙或加密狗装置以避免非预定的机器人启动或运动，制造商应设置不同用户的不同访问权限。

5.6 协同操作要求

5.6.1 功能要求

应依据 GB/T 36008—2018 以及 GB 11291.1—2011 中有关协同操作的原则来设计机器人协作功能。

5.6.2 安全监控停止

安全监控停止特性使机器人停止运动，以允许操作员在协作工作空间中和机器人直接交互并完成任务(例如给终端执行器加装零件)。如果协作工作空间里没有人，机器人可自主地操作。若该安全监控停止功能激活，机器人应停止运动，此时协作人员才可进入协作工作空间。只有在操作者离开协作工作空间以后，机器人系统才可无干预地自行恢复。

机器人在进入、退出安全监控停止状态时，应对操作者发出明显的状态指示，机器人应依据 GB 11291.1—2011 的 5.5.3 配置保护性停止功能。

5.6.3 手动引导

在该协同操作方法中，操作者可使用手动设备向机器人系统发送运动指令或者直接手动拖动机器人进行协同操作。在操作者被允许进入协作工作空间控制手动引导任务之前，机器人应处在安全监控停止状态。操作者应手动激活机器人手动引导协同操作功能，以完成任务。

触发机器人进入、退出手动引导状态的装置应为三位置使能设备，三位置使能设备应满足 GB 11291.1—2011 的 5.8.3 要求。

在手动引导协同操作模式下，操作者应时刻握持手动引导三位置使能设备，可在紧急或异常情况下立即按紧或松开三位置使能设备，停止机器人的运动。同时，操作者应可随时快速触发机器人急停装置，机器人急停装置应符合 GB/T 16754—2008 的要求。

机器人在手动引导下的降速速度应依据风险评估来确定，但末端 TCP 速度不能超过 250 mm/s(见 GB 11291.2—2013 的 5.6.4.2)。

如果超过了该降速速度，机器人应立即进入保护性停止状态。

机器人在进入、退出手动引导协同操作状态时，应对操作者发出明显的状态指示。

5.6.4 速度与分离监控

在该协同操作方法中，机器人系统与操作者可能在协作工作空间中并行移动。操作者与机器人之间应随时维持一个保护性间距，以降低风险。机器人在运动期间，距离操作者的距离不应近于该保护性间距。当间距小于保护性间距时，机器人系统停止。当操作者远离机器人时，维持保护性间距的机器人系统可自行恢复。当机器人系统减速时，保护性间距也相应减小。

速度与分离监控作用于协作工作空间内所有人。如果保护性措施的性能被协作空间内的人数限制，那么最大人数应在使用信息中列出。如果超出了该最大数目，将产生保护性停止。

如果机器人危险部件与操作者之间的间距小于保护性间距，机器人系统应：

a) 启动保护性停止；

b) 启动连接到机器人的安全适用功能(依据 GB 11291.2—2013 的 5.11.2)，关闭所有危险工具。

机器人控制系统可避免干涉保护性间距，有如下可能，包含但不限于：

a) 减速，接下来可切换到安全监控停止状态；

b) 绕行，执行不干涉保护性间距的另一个路径，继续激活速度与分离监控。

当实际间距满足或超过保护性间距时，机器人运动可恢复。

5.6.5 功率与力限制

在该协同操作方法中，机器人系统(含工件)与操作者的物理接触可预计产生或未预计产生。功率与力限制的协作操作要求机器人系统是为这种特殊操作专门进行设计的。风险降低既可通过机器人固有的安全措施，也可通过安全相关的控制系统来完成。

机器人在与人或设备发生非预期物理接触后，且物理接触力或功率超过设计的限制阈值时，机器人应立即进入安全监控停止状态或保护性停止(停止类型 0，依据 GB/T 5226.1—2019)并保持，或机器人应立即向发生物理接触的反方向运动一段距离，远离操作者或设备后，立即进入安全监控停止状态或保护性停止(停机类型 0，依据 GB/T 5226.1—2019)并保持停止状态。机器人向反方向的运动距离应依据风险评估来设定，在任何时候不能导致与操作者或设备发生二次非预期物理接触。

当机器人在进入停止状态后，只有在人为干预下才能使机器人退出当前停止状态。机器人在进入、退出由功率与力限制功能触发的停止状态时，应对操作者发出明显的状态指示。

支持协作操作且带有功率和力限制的机器人，可采用配置阈值的方法，例如力、力矩、速度、动量、机械功率、轴限范围或空间范围来保证操作者与机器人协同工作的安全性。

操作者可依据风险评估结果修改机器人功率或力限制的阈值。修改机器人功率与力的限制的界面应具备安全访问权限限制功能，只有具备访问权限的操作者才能修改功率或力的阈值。机器人在接收到修改指令后，应对操作者发出明显的状态指示，确保修改成功。

5.7 与安全相关的控制系统性能

5.7.1 一般要求

与安全相关的控制系统(电气、液压、气动和软件)至少应满足 5.7.2 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(见 5.7.2)是适当的。在与设备一起提供的资料中,应清楚地说明该设备部件所满足的与安全有关的控制系统性能。

与安全相关的控制系统性能要求和类别应符合 GB/T 16855.1—2018 的要求。

5.7.2 性能准则

当涉及与安全相关的控制系统时,与安全相关的部件应设计成:

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安全功能需求之时或之前被检测出来;

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。这个要求属于 GB/T 16855.1—2018 中所描述的类别 3。

注:这个单个故障检测的要求并不意味着所有故障都被发现。因此,未检测到的故障的积累可能导致机器的意外输出和危险情况。故障检测的可行措施的实例是检查继电器触点的连接运动或监测多余的电气输出。宜做出合适的故障模式分析,以确认所有可合理预见的故障都得到考虑。

5.7.3 其他控制系统性能准则

机器人及其预期应用进行综合风险评估的结果,可以用来确定该应用需要的,与安全有关的控制系统的性能要求,该性能要求不是针对类别 3 的,而是针对类别 2 或类别 4 的。其他性能准则在 GB/T 16855.1—2018 中说明。

5.8 与安全相关的零部件

5.8.1 与安全相关的控制器

与安全相关控制器的设计是机器全部设计过程中的一个完整子过程。在提供的安全功能中,无论作为本质安全设计的一部分,还是作为安全防护装置或保护装置,与安全相关控制器的设计都是风险减小策略的一部分。

对于每种安全功能,应在安全要求技术规范中规定和记录其特征和所需的性能等级(PL)。本标准的性能等级定义为每小时危险失效的概率。5 种性能等级(a～e)的规定范围见表 2。

表 2 性能等级(PL)

性能等级(PL)	每小时平均危险失效概率 p(1 h)
a	$10^{-5} \leqslant p < 10^{-4}$
b	$3\times10^{-6} \leqslant p < 10^{-5}$
c	$10^{-6} \leqslant p < 3\times10^{-5}$
d	$10^{-7} \leqslant p < 10^{-6}$
e	$10^{-8} \leqslant p < 10^{-7}$
注:除了每小时平均危险失效概率外,其他措施也宜达到相应的性能等级。	

从对机器进行风险评价开始,设计者应确定与安全相关控制器的作用,该作用并不减小受控机器的所有风险,而是应用特定的安全功能减小一部分风险。

在 GB/T 20438.1—2017 中,有关安全控制系统完成安全功能的能力用安全完整性等级(SIL)给出。表 3 给出了两种概念(PL 和 SIL)的关系。

PLa 级与 SIL 无对应的等级,它主要用于轻微的风险减小,通常与伤害可逆。SIL3 对应的 PLe 级为最高的等级。

表 3　性能等级(PL)与安全完整性等级(SIL)之间的关系

性能等级(PL)	SIL (参见 GB/T 20438.1—2017)
a	无对应等级
b	1
c	1
d	2
e	3
注：SIL4 专门用于流程工业中可能的灾难事件。	

与安全相关的控制器应实时监控机器人的运行状态，在机器人发生故障或其他非安全情况时可触发保护性停止或紧急停止。安全控制器系统应至少满足以下一项：

——控制器 PL 大于或等于 d(GB/T 16855.1—2018)；

——控制器 SIL 大于或等于 2(GB/T 20438.1—2017)；

——控制器系统构架采用双通道安全冗余设计，至少具备两个或以上主控芯片，单一故障不会导致安全功能的丧失；

——控制器系统架构采用多通道安全冗余设计，选用 SIL 大于或等于 2 或 PL 大于或等于 d 的安全芯片作为主控芯片。

5.8.2　编码器系统

编码器系统作为实施感知机器人位姿信息的传感系统，应具备高安全性系统设计，确保在编码器发生单一故障时不会导致机器人安全功能丧失。机器人编码器系统应至少满足以下一项：

——针对机器人每个关节的位置和姿态信息的感知，至少具备两个编码器；

——编码器系统 SIL 大于或等于 2；

——编码器系统 PL 大于或等于 d。

编码器系统应至少包含编码器、编码器数据处理器、编码器数据传输器。

5.9　机器人安全功能

5.9.1　机器人停止功能

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

应依据 GB/T 36008—2018 以及 GB 11291.1—2011 中有关停止功能的原则来设计机器人停止功能。

5.9.2　速度限制功能

机器人应具备速度限制功能，用户可通过人机交互界面设置末端工具中心点(TCP)或关节最大运动速度。在触发机器人速度限制功能后，机器人的运行参数(TCP 速度、关节速度等)应限制在设置值内，确保人机协作安全性。

机器人应开放速度限制功能触发接口，用户可通过此接口触发机器人进入速度限制运动模式。此接口应至少满足以下条件之一：

——接口采用双通道或多通道安全冗余设计，确保在发生单一故障时不会丧失安全功能；

——接口采用标准的安全通信协议，用户将安全控制指令通过安全协议下发到接口。

5.9.3 轴及空间的安全软限制

机器人应具备轴及空间的安全软限制功能，用户可通过人机交互界面对单轴的运动进行限制。用户可限制轴的运行速度或运动范围。

使用软限制的控制系统应符合 5.7 的要求。如果超出了安全软限制范围，应激活保护性停止。

安全软限制应设置为一个系统没有上电时不能改变的稳定状态，且不应动态地变更。改变安全软限制的权利应受密码保护并是安全的。一旦设置，安全软限制应在系统上电后一直处于激活状态。

应依据 GB/T 36008—2018 以及 GB 11291.1—2011 中有关轴及空间限位的原则来设计机器人轴及空间限位。

5.9.4 静态碰撞保护

机器人应具备静态碰撞保护功能。机器人在有源(带电)静止状态下，当操作人员或其他物体与机器人发生碰撞且碰撞力超过安全阀值时，机器人应沿碰撞力的方向做被动移动，以保证操作人员或其他物体与机器人发生非预期碰撞时，减少对人员、其他物体以及机器人的伤害。

应依据 GB/T 36008—2018 以及 GB 11291.1—2011 中有关风险评估结果来设计机器人静态碰撞保护功能。

5.9.5 奇异保护

经过奇异点的运动会产生很高的轴转速。这些高速度可能是非预定的且会导致对用户、机器人和在场人员的风险。

机器人经过奇异点的运动，应采取以下措施：

a) 经过奇异点的 TCP 速度不高于 250 mm/s；

b) 机器人避开奇异点，例如通过调整路径规划实现；

c) 在机器人通过奇异点时停止机器人运动并发出警告，或在协作运动期间进行回避。

6 使用信息

使用信息应符合 GB/T 36008—2018 以及 GB 11291.1—2011 的规定，制造商应提供标志(例如标记、符号)和使用说明材料(例如操作、维护手册)。

使用信息包括机器人的正确使用信息。使用信息应不仅针对用户，也针对维护人员。

使用说明和本标准要求的文本，应用机器人销售地国家的官方语言书写。

标识、符号和书面警告应明确易懂，尤其关于机器人功能的内容。易懂的记号(象形图)的使用优先于书面警告。

7 验证与确认

7.1 通则

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

应复查风险评估，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。宜进行风险评估，以便为给定的机器人系统确定适当的保护措施。

7.2 验证与确认方法

机器人的安全验证与确认方法如表 4 所示，但不限于表 4。

表 4 验证与确认方法表

编号	验证与确认方法
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

具体方法见表 A.1 安全要求和措施的验证方法。

7.3 验证与确认要求

表 A.1 给出了专用性能要求和措施的验证方法，这些要求对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。

附 录 A
（规范性附录）
安全要求和措施的验证方法

表 A.1 列出了具体安全要求和措施的验证方法。

表 A.1 安全要求和措施的验证方法

参考章条号	安全要求和/或措施	验证和/或确认方法(见 7.2)								
		A	B	C	D	E	F	G	H	I
5.2	通用要求									
5.2.1	符合指定标准要求，达到防护目的	—	√	—	—	—	√	—	—	√
5.2.2	符合指定标准要求，电气参数设置在安全电压范围内，达到安全防护目的	—	√	—	—	√	√	√	—	√
5.2.3	机器人达到指定防护等级，具有防静电、防意外触电功能	—	√	—	—	—	√	√	—	√
5.2.4	机器人具备安装姿态自适应功能	√	√	—	√	—	—	—	√	√
5.3	机械设计									
5.3.1	不应有易于伤人的机械结构	√	—	√	√	—	—	√	√	√
5.3.2	刹车装置抱闸锁死时应不能被外界移动	—	√	—	—	—	—	√	—	√
5.4	人机交互界面									
5.4.2	示教界面应提供直观形象的机器人示教相关的显示信息	√	√	—	√	—	√	—	—	√
5.4.3	编程方式应具备模块化、任务级、简单编程功能，确保人机协作的可靠交互性	√	√	—	√	√	√	√	—	√
5.4.4	机器人软件界面应具有机器人相关的丰富操作界面	√	—	—	√	—	√	—	—	√
5.5	外部接口设计									
5.5.1	在使用资料中有控制范围信息	√	—	—	—	—	—	—	—	√
5.5.2	指令装置应充分考虑安全空间内的位置、布局和危险	√	√	—	√	—	√	√	—	√
	机器人系统不响应任何指令装置会导致危险状况的命令	—	√	—	√	—	—	—	—	—
	远程控制期间一次只能有一个单独控制源工作	—	√	—	√	—	√	—	—	√
5.5.3	连接或断开机器人系统不引发危险状况	√	√	—	√	√	—	√	—	√
5.6	协同操作要求									
5.6.2	符合指定标准要求，机器人具备安全监控停止功能	√	√	—	√	—	—	√	—	√
5.6.3	机器人具备手动引导功能，进入、退出手动引导装置符合标准要求，手动引导速度在标准范围内	√	√	√	√	—	—	—	—	√
	工具中心点的最大速度不能超过 250 mm/s	—	√	√	√	—	√	—	—	√
5.6.4	机器人具备标准要求功能，符合指定标准要求	√	√	—	√	—	—	√	√	√
5.6.5	机器人具备标准要求功能	—	√	√	√	—	√	—	√	√

表 A.1（续）

参考章条号	安全要求和/或措施	验证和/或确认方法（见 7.2）								
		A	B	C	D	E	F	G	H	I
5.7	与安全相关的控制系统性能									
5.7.1	在使用资料中陈述性能的能力、数据及准则，以确定性能	√	—	—	—	—	—	—	—	√
5.7.2	PL 大于或等于 d，结构类别 3	—	—	—	—	√	√	—	—	√
5.7.3	风险评估结果用于确定与安全相关的控制系统性能要求	—	—	—	—	—	—	√	—	√
5.8	与安全相关的零部件									
5.8.1	控制器 PL 大于或等于 d(GB/T 16855.1—2018)	—	—	—	—	√	√	√	—	√
	控制器 SIL 大于或等于 2(GB/T 20438.1—2017)	—	—	—	—	√	√	√	—	—
	控制器系统构架采用双通道安全冗余设计，至少具备两个或以上主控芯片，单一故障不会导致安全功能的丧失	—	—	—	—	√	√	√	—	—
	控制器系统架构采用多通道安全冗余设计，选用 SIL 大于或等于 2 或 PL 大于或等于 d 的安全芯片作为主控芯片	—	—	—	—	√	√	√	—	—
5.8.2	针对机器人各关节的位置和姿态信息感知，至少具备两个或以上编码器	—	—	—	—	√	√	√	—	—
	编码器系统 SIL 大于或等于 2	—	—	—	—	√	√	√	—	—
	编码器系统 PL 大于或等于 d	—	—	—	—	√	√	√	—	—
5.9	机器人安全功能									
5.9.1	机器人具备保护性停止功能和独立的急停功能	√	√	—	√	—	√	√	—	√
5.9.2	机器人具备速度限制功能	—	√	√	√	√	√	√	—	—
	机器人开放速度限制功能触发接口	—	√	√	√	√	√	√	—	—
	接口采用双通道或多通道安全冗余设计，确保在发生单一故障时不会丧失安全功能	—	—	—	—	√	√	√	—	—
	接口采用标准的安全通信协议，用户将安全控制指令通过安全协议下发到接口	—	—	—	—	√	√	√	—	—
5.9.3	机器人具备轴及空间的安全软限制功能	√	√	√	√	—	—	√	√	—
	如果超出了安全软限制范围，应激活保护性停止	√	√	√	√	—	—	√	√	—
	改变安全软限制的权利应受密码保护并是安全的	√	√	√	√	—	—	√	√	—
5.9.4	机器人具备静态碰撞保护功能	√	√	—	√	√	—	√	√	—
5.9.5	机器人具备奇异保护	√	√	—	√	—	—	√	—	—
	经过奇异点的 TCP 速度不高于 250 mm/s	√	√	—	√	—	—	√	—	—
	机器人应避开奇异点，如通过调整路径规划实现	√	√	—	√	—	—	√	—	—
	在机器人通过奇异点时停止机器人运动并发出警告，或在协作运动期间进行回避	√	√	—	√	—	—	√	—	—

注：“√”表示适用；“—”表示不适用。