



中华人民共和国医药行业标准

YY 9706.278—2023

医用电气设备 第 2-78 部分：康复、评定、 代偿或缓解用医用机器人的基本安全和 基本性能专用要求

Medical electrical equipment—Part 2-78: Particular requirements for
basic safety and essential performance of medical robots for rehabilitation,
assessment, compensation or alleviation

(IEC 80601-2-78:2019, MOD)

2023-03-14 发布

2026-05-01 实施

国家药品监督管理局 发布

目 次

前言	I
引言	II
201.1 范围	1
201.2 规范性引用文件	2
201.3 术语和定义	2
201.4 通用要求	5
201.5 ME 设备试验的通用要求	6
201.6 ME 设备和 ME 系统的分类	6
201.7 ME 设备标识、标记和文件	6
201.8 ME 设备对电击危险的防护	7
201.9 * ME 设备与 ME 系统对机械风险的防护	7
201.10 对不需要的或过量的辐射危险(源)的防护	12
201.11 对超温和其他危险(源)的防护	12
201.12 控制器和仪表的准确性和危险输出的防护	12
201.13 ME 设备危险情况和故障状态	13
201.14 可编程医用电气系统(PEMS)	13
201.15 ME 设备的结构	13
201.16 * ME 系统	15
201.17 * ME 设备和 ME 系统的电磁兼容性	15
202 电磁兼容——要求和试验	15
206 可用性	15
208 * ME 设备和 ME 系统中报警系统的通用要求、测试和指南	15
210 * 生理闭环控制器的开发要求	16
211 * 家庭护理环境中使用的 ME 设备和 ME 系统的要求	16
附录 A (资料性) 通用指南的原理说明	18
附录 AA (资料性) 专用指南和原理说明	19
附录 BB (资料性) 态势感知的指南和示例	41
参考文献	52
索引	54

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。

《医用电气设备》系列标准分为两部分：

——第 1 部分：通用和并列要求；

——第 2 部分：专用要求。

本文件是第 2-78 部分。

本文件修改采用 IEC 80601-2-78:2019《医用电气设备 第 2-78 部分：康复、评定、代偿或缓解用医用机器人基本安全和基本性能的专用要求》。

本文件与 IEC 80601-2-78:2019 的技术差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在 201.2“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的 GB 9706.1—2020 代替 IEC 60601-1:2005+AMD1:2012；
- 用等同采用国际标准的 YY/T 0316—2016 代替 ISO 14971:2007；
- 用修改采用国际标准的 YY 9706.102—2021 代替 IEC 60601-1-2:2014；
- 用修改采用国际标准的 YY/T 9706.106—2021 代替 IEC 60601-1-6:2010+AMD1:2013；
- 用修改采用国际标准的 YY 9706.108—2021 代替 IEC 60601-1-8:2006+AMD1:2012；
- 用修改采用国际标准的 YY/T 9706.110—2021 代替 IEC 60601-1-10:2007+A1:2013；
- 用修改采用国际标准的 YY 9706.111—2021 代替 IEC 60601-1-11:2015；
- 增加了规范性引用文件 YY/T 1474；
- 删除了规范性引用文件 IEC 62366-1:2015；
- 删除了规范性引用文件 ISO 22523:2006。

——删除了 202.4.2.3.1 增补的内容，第 202 章修改为“YY 9706.102—2021 适用”。原因是英文原文中 202.4.2.3.1 的内容，YY 9706.102—2021 已有。

——删除了 206.4.2 和 206.5 及附录对应内容。IEC 原文中对 IEC 60601-1-6 的修改，仅限于更改引用标准的版本号及对引用标准的新版增加资料性注，删除后，与 YY/T 9706.106—2021 保持一致。

本文件做了下列编辑性改动：

——用我国标准 GB/T 30659 代替资料性引用的 ISO 22523；

——增加了参考文献 IEC 62366-1:2015。

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。

本文件由国家药品监督管理局提出。

本文件由全国医用电器标准化技术委员会医用电子仪器标准化分技术委员会(SAC/TC 10/SC 5)归口。

引 言

医用电气设备安全标准也称为 9706 系列标准,拟由通用标准、并列标准、专用标准、指南和解释构成。

- 通用标准:医用电气设备应普遍适用的安全标准,即符合医用电气设备定义的设备均应满足此基础标准要求。
- 并列标准:医用电气设备应普遍适用的安全标准,但多数情况下仅限于具有某些特定功能或特性的设备才需要满足此类标准要求。
- 专用标准:某一类医用电气设备应适用的安全标准,且并非所有的医用电气设备都有专用标准。
- 指南和解释:对涉及的标准中相关要求的应用指南和解释说明。

本文件修改和补充了 GB 9706.1—2020《医用电气设备 第 1 部分:基本安全和基本性能的通用要求》,下称通用标准。

附录 AA 包含一些要求的基本原理,它包括某些要求产生的背景 and 原因,以及识别需要解决的相关的危险。本文件中星号(*)作为标题的第一个字符或段落或表格标题的开头,表示在附录 AA 中有与该项目相关的专用指南和原理说明。

医用电气设备 第 2-78 部分:康复、评定、 代偿或缓解用医用机器人的基本安全和 基本性能专用要求

201.1 范围

除下述内容外,通用标准的第 1 章适用。

201.1.1 范围

替换:

本文件规定了预期与患者产生身体接触、实现患者肢体运动功能的康复、评定、代偿或缓解的医用机器人的基本安全和基本性能。

本文件适用于预期与患者产生身体接触、实现患者肢体运动功能的康复、评定、代偿或缓解的医用机器人。

如果一章或一条明确指出仅适用于 ME 设备或 ME 系统,章或条的标题和正文会说明。如果不是这种情况,与此相关的章或条同时适用于 ME 设备和 ME 系统。

注:参考通用标准的 4.2。

本文件不适用于:

- 假肢和矫形器(GB/T 30659);
- 轮椅车(GB/T 18029 系列标准);
- 诊断成像设备(如磁共振设备,YY 9706.233);
- 个人助理机器人(GB/T 36530)。

201.1.2 目的

替换:

本文件的目的是为上述医用机器人建立专用的基本安全和基本性能要求。

201.1.3 * 并列标准

增补:

本文件引用通用标准第 2 章以及本文件 201.2 所列的适用的并列标准。

201.1.4 专用标准

替换:

在 9706 系列标准中,专用标准可依据所考虑的专用 ME 设备,修改、替换或删除通用标准和并列标准中包含的要求。并可增补其他基本安全和基本性能要求。

专用标准要求优先于通用标准。

在本文件中,GB 9706.1—2020 称为通用标准。并列标准用它们各自的文件编号表示。

本文件中章和条的编号通过加前缀“201”与通用标准对应(例如,本文件中 201.1 对应通用标准第 1 章的内容),或者通过加前缀“20×”与适用的并列标准对应,此处×是对应的文件编号的末位数字(例

如,本文件的 211.7 对应并列标准 YY 9706.111—2021 第 7 章的内容)。

对通用标准文本的变更,规定使用下列词语:

“替换”即通用标准或适用的并列标准的章和条完全由本文件的内容所替换。

“增补”即本文件的内容作为通用标准或适用的并列标准的补充。

“修改”即对通用标准或适用的并列标准的章和条改为本文件的内容。

作为对通用标准增补的条、图和表从 201.101 开始编号。然而,由于通用标准中术语的编号从 3.1 至 3.147,因此,本文件中增补的术语从 201.3.201 开始编号。增补附录的编号为 AA、BB 等,增补列项的编号用 aa)、bb)等表示。

对于增补到并列标准中的条、图或表从 20×开始编号,此处“×”是对应文件编号中末位数字,例如,202 对应 YY 9706.102,208 对应 YY 9706.108。

“本标准”一词是通用标准、任何适用的并列标准及本文件的统称。

若本文件中没有相对应的章和条,则通用标准或适用的并列标准中的章和条,即使可能不相关,也均适用。对通用标准或适用的并列标准中的任何部分,即使可能相关,若不采用,则本文件对其给出说明。

201.2 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。

除下述内容外,通用标准的第 2 章适用。

替换:

YY/T 0316—2016 医疗器械 风险管理对医疗器械的应用(ISO 14971:2007,IDT)

YY/T 1474 医疗器械 可用性工程对医疗器械的应用(YY/T 1474—2016,IEC 62366:2007,IDT)

YY 9706.102—2021 医用电气设备 第 1-2 部分:基本安全和基本性能的通用要求 并列标准:电磁兼容 要求和试验(IEC 60601-1-2:2007,MOD)

YY/T 9706.106—2021 医用电气设备 第 1-6 部分:基本安全和基本性能的通用要求 并列标准:可用性(IEC 60601-1-6:2013,MOD)

YY 9706.108—2021 医用电气设备 第 1-8 部分:基本安全和基本性能的通用要求 并列标准:通用要求,医用电气设备与医用电气系统报警系统的测试和指南(IEC 60601-1-8:2006+AMD1:2012,MOD)

增补:

YY/T 9706.110—2021 医用电气设备 第 1-10 部分:基本安全和基本性能的通用要求 并列标准:生理闭环控制器开发要求(IEC 60601-1-10:2007+A1:2013,MOD)

YY 9706.111—2021 医用电气设备 第 1-11 部分:基本安全和基本性能的通用要求 并列标准:在家庭护理环境中使用的医用电气设备和医用电气系统的要求(IEC 60601-1-11:2015,MOD)

201.3 术语和定义

GB 9706.1—2020 界定的以及下列术语和定义适用于本文件。

修改:

201.3.63

* 医用电气设备 **medical electrical equipment**

ME 设备 ME equipment

增补：

注：参见图 AA.1。

201.3.65

移动的 mobile

增补：

注：移动的还包括用于支撑患者从一处移动到另一处的设备。

201.3.144

* 可穿戴的 **body-worn**

替换：

预期用途包括运行时由患者穿着或附加在患者衣服上的可携带的设备。

增补：

201.3.201

* 驱动应用部分 **actuated applied part**

应用部分的子类，提供能够主动控制与患者运动功能相关的物理交互，执行 RACA 机器人(201.3.212)的临床功能。

注 1：“主动控制”指通过 RACA 机器人控制，包括患者或操作者的共同控制。

注 2：主动控制物理互动包括位置控制、力控制、阻抗控制、导纳控制或其他控制来调节 RACA 机器人和患者互动的方式。

注 3：每一个驱动应用部分均为通用标准 9.8.1 驱动系统的一部分。

201.3.202

缓解 alleviation

用于纾缓患者损伤所引起的症状。

注：如 RACA 机器人为减少损伤带来的痛苦或其他副作用而进行的物理治疗。

201.3.203

* 评定 **assessment**

量化或协助量化患者损伤程度的程序。

注 1：“评定”不应与“风险评估”相混淆。

注 2：此定义中的“评定”一词侧重于身体功能和结构的受损程度，而非活动受限或参与受限的程度(参考文献[2]，第 4 章)。

注 3：“评定”与“测量”和“诊断”不同，“测量”通常指测量的生理参数(如 RACA 机器人测量的患者手部的的位置)，通常与传感器相关，或由传感器直接输出。这些测量数据被用于量化损伤(如本体感受、运动规划等)。损伤不同于潜在的病变，而是潜在病变的临床表现，临床医生可以利用量化损伤的“评定”来支持其诊断，从而确定相关病理或监控病变过程或恢复情况。见附录 AA 中的示例。

201.3.204

临床功能 clinical function

ME 设备或 ME 系统按制造商规定实施的重要临床操作。

注 1：临床功能通常属于 ME 设备或 ME 系统的预期用途，且与患者有关。

注 2：在本文件中，重要临床操作包括：

- 支持对受损患者的诊断；
- 对患者损伤的治疗、缓解或监测。

[IEC/TR 60601-4-1;2017,3.6]

201.3.205

代偿 compensation

通过身体结构的支承,或通过身体功能的支承或替换来减轻患者损伤。

注:代偿可通过外用矫形器等方式实现。代偿不包括受损运动功能的改善,后者属于康复。

201.3.206

紧急停止 Emergency stop

手动触发使 RACA 机器人停止,以避免伤害。

注 1:紧急停止是在其他风险规避手段均不可用时的“最后手段”。

注 2:和保护性停止不同,紧急停止后,机器无法自动重启。

注 3:激活紧急停止并不会关掉 RACA 机器人的所有电源。具体情况见通用标准的 9.2.4。

201.3.207

*** 损伤 impairment**

身体功能或结构出现问题,如严重偏离或缺失。

注 1:此处的“问题”指身体及其功能的生物医学状态偏离(负面)了公认的人均正常水平。能够通过普遍认知的功能评价来获知受损的情况。损伤通常由疾病或意外产生,但也存在天生的缺陷。

注 2:本文件仅涉及 ME 设备或 ME 系统,因此仅论证患者的损伤而非正常的因衰老导致的损伤。

[ISO 9999:2016,定义 2.11]

201.3.208

医用机器人 medical robot

用作 ME 设备或 ME 系统的机器人。

[IEC/TR 60601-4-1:2017,定义 3.20]

201.3.209

运动功能 movement function

由构成患者运动控制系统的一个或多个感官、神经肌肉骨骼或运动相关的身体功能。

注 1:“感官”“神经肌肉骨骼”和“运动相关”出自[1]中的身体功能分类。

注 2:RACA 机器人无需满足所有情况。

201.3.210

*** 保护性停止 protective stop**

RACA 机器人(201.3.212)出于基本安全和基本性能的目的,自动运行的操作中断行为,通过可编程医用电气系统(PEMS)/可编程电子子系统(PESS)能够实现重启。

注 1:另见 ISO 8373:2012 的 5.17。

注 2:保护性停止的定义与紧急停止或正常停止相反:分类见表 201.102。

注 3:“自动运行”表示 RACA 机器人一直在检测有潜在危险的情况,如有发现,则运行停止程序。

注 4:术语与 YY/T 9706.110—2021 的 3.11 中定义的后备模式有关。

注 5:即使在运动停止过程中,执行器也不一定失效。在某些情况下,执行器可能将患者或患者四肢固定在一个稳定位置。

201.3.211

*** 康复 rehabilitation**

用以改善与患者损伤有关的运动功能的治疗。

示例:重新学习上肢或下肢的运动控制,恢复肌肉强度和耐力。

注 1:若患者因事故、疾病或先天因素(如大脑性麻痹)发生损伤,则可进行康复治疗。此外,康复治疗还可减缓神经退行性疾病(如帕金森和多发性硬化)导致的身体功能损失。

注 2:此处的定义与世界卫生组织(WHO)的定义不同,为与本文件范围相符合,其仅涉及后的一个子集。

201.3.212

康复、评定、代偿和缓解用医用机器人 rehabilitation, assessment, compensation and alleviation robot
RACA 机器人

由制造商提供的用于实施康复、评定、代偿或缓解的医用机器人,通常包括一个驱动应用部分。

201.3.213

*** 机器人 robot**

具有一定程度自主性的由编程驱动的,在其环境中运动以完成预期任务的机械装置。

201.3.214

*** 态势感知 situation awareness**

操作者对 RACA 机器人在其环境中行为的感知、理解和预测。

注 1: 态势感知使 RACA 机器人的操作者能够及时地对 RACA 机器人的行为做出适当反应,无论是在正常使用还是在单一故障状态下。

注 2: 态势感知与可用性工程过程有直接联系。但 IEC 62366-1:2015 将态势感知与“感知”和“认知”两个概念的使用联系起来。更多信息见附录 AA。

201.3.215

*** 步行式 walking**

安装并投入使用后,预期通过运动表面和 RACA 机器人的间歇性接触,进行从一个位置运动到另一个位置的往复运动的移动设备。

示例: 下肢动力外骨骼是一种用于移动患者的步行式 RACA 机器人。

注: 步行式是一种新的便携式 ME 设备和 ME 系统类别,如图 AA.1 所示。

201.4 通用要求

除下述内容外,通用标准的第 4 章适用。

201.4.2.3 评价风险

在 4.2.3.1 前增补:

201.4.2.3.101 概述

在执行风险管理过程时,应考虑 RACA 机器人的自主程度。

注 1: IEC/TR 60601-4-1 规定应考虑自主程度对风险管理过程的影响。例如,相较于由操作者来执行某项作业,由 RACA 机器人完全自主地完成可能风险更低,或正好相反。

注 2: 自主程度可能提高 RACA 机器人的性能、增加其功能或改善其可用性。但自主程度过高也会增加系统的复杂性,从而导致危险情况增多,情况更加复杂。制造商的风险管理过程应把其复杂性考虑在内。应对一个或多个 PESS 的自主性进行具体审查。

注 3: 操作者的作业不同或其与 RACA 机器人的交互不同,操作者扮演的角色也不同。RACA 机器人的自主程度越高,操作者的态势感知越重要。

可通过检查风险管理文档来检验是否符合要求。

201.4.2.3.102 * 风险管理与态势感知

制造商应确认风险管理过程缺失态势感知后会出现的危险或危险情况,而操作者应监督 RACA 机器人的作业或与其交互,从而将风险降至可接受水平。制造商应在随附文件中提供必要信息。

可通过检查风险管理文档或随附文件(如适用)来检验是否符合要求。

YY/T 1474 中规定应对危害相关使用场景进行总结性评价。鉴于态势感知评价的主观性,对与危害相关的使用场景进行形成性评估就足够了。

注:更多指南请参见附录 BB。

201.4.3 基本性能

增补:

表 201.101 为可能导致 RACA 机器人出现不可接受风险的基本性能潜在来源及其所属条款。

表 201.101 潜在基本性能

潜在基本性能	条款
RACA 机器人的运动或力/力矩	201.12.101
评定测量	201.12.102

201.4.7 * ME 设备的单一故障状态

增补:

注:特别是在单一故障状态下,态势感知对于保持基本安全和基本性能来说非常重要,尤其是当操作者操作 RACA 机器人进行具体作业时。例如,对于操作者的认知问题,可以采用两种警告方式(如光和声)来确保 ME 设备是单一故障安全。

201.5 ME 设备试验的通用要求

除下述内容外,通用标准的第 5 章适用。

201.5.9.1 应用部分

增补条款:

201.5.9.1.101 驱动应用部分

驱动应用部分通过检查和参考随附文件来进行识别。

201.5.9.2.1 试验指

增补:

通用标准中提到的测试应另用 YY 9706.111—2021 图 1 中的小号试验指进行(如适用)。

201.6 ME 设备和 ME 系统的分类

通用标准第 6 章适用。

201.7 ME 设备标识、标记和文件

除下述内容外,通用标准的第 7 章适用。

201.7.2.4 附件

替换:

如果因附件标识混淆导致不可接受的风险,制造商应遵循 YY/T 0316—2016 的 6.2,优先考虑风险控制。

附件的标记应在风险管理过程中被识别,但至少要有:

- 制造商的名称或商标;
- 型号;
- 序列号或批号(如适用);
- 制造年份或失效日期(如适用)。

注 1: 制造商符号、序列号、批号、制造年份和失效日期,请参见 YY/T 0466.1。

注 2: 序列号、批号或批次标识,以及制造日期可以用人可读的代码或通过自动识别技术[例如条形码或射频识别(RFID)]来提供。

附件进行标记不可行时,这些标记可以贴在独立的包装上。

201.7.9.2.5 ME 设备的说明

在第一段的列表中增补:

- 应充分说明对具有一定自主程度的功能(包括启动程序、重启程序、关闭程序和保持),供操作者形成充分的态势感知。

201.7.9.2.9 运行说明

在第一段最后增补:

其中还应包括态势感知(见 201.4.2.3.102)相关风险管理过程规定的信息。

201.7.9.3.1 概述

在第一段的项目列表中增补:

- 对维修服务人员能够造成危险的、具有一定程度自主性功能的说明。

201.8 ME 设备对电击危险的防护

除下述内容外,通用标准第 8 章适用。

201.8.3 应用部分的分类

增补:

注: 驱动应用部分的分类同应用部分,应为 B 型应用部分、BF 型应用部分或 CF 型应用部分。

201.9 * ME 设备与 ME 系统对机械风险的防护

除下述内容外,通用标准的第 9 章适用。

201.9.1 医用电气设备机械事故

表 19 本章涉及的机械危险

增补：

功能性异位危险(源)	201.9.101
------------	-----------

201.9.2 与运动部件相关的机械危险

201.9.2.1 概述

增补：

RACA 机器人,特别是可穿戴的或步行式,在执行其预期用途过程中,可能会接触其运动环境范围内的物体,例如,墙、不同的行走表面或桌椅等。如适用,制造商应在风险管理过程中考虑这些问题。如适用,应给出安全信息以降低风险。

注: 制造商可根据 GB/T 36530—2018 中 5.10.8 的制定风险控制措施(GB/T 36530—2018 将风险控制描述为风险降低),降低其与环境中物体发生接触的风险(GB/T 36530—2018 用到“安全相关障碍”这一术语)。

为完成其预期用途,RACA 机器人会移动患者的一个或多个身体部位,因此风险管理过程应考虑不同的停止程序(见表 201.102),如自动停止程序。

表 201.102 不同的停止程序

功能	紧急停止	保护性停止	正常停止
情况	紧急情况	异常状态	预期操作
触发方式	手动	自动	手动或自动
要求	应满足 9.2.4	应满足 9.2.101	设计规定
重启方式	手动	手动或自动	不适用
使用频率	不频繁	常见至不频繁	频繁
预期影响	立即停止危险情况	控制风险至可接受水平	暂停操作

201.9.2.2.1 概述

增补：

若 RACA 机器人为完成其预期用途,需要与环境中物体接触,则机器人与环境的空间不作为俘获区域来考虑。风险管理过程应对这种情况进行评估。

201.9.2.3 与运动部件相关的其他机械危险

201.9.2.3.1 * 非预期的运动

替换与增补条款：

201.9.2.3.1.101 控制器非预期的运动

除非通过可用性工程过程对于预期的患者(例如:有特殊需求的患者)得出不同结论,或该启动不会

导致不可接受的风险,控制器应妥善放置、凹进或以其他方式进行保护,使其不会意外启动。

注:控制器可以被理解为控制设备上由操作者操作的用户界面,如开关、操纵杆、触摸屏(包括智能设备)、转盘或旋钮。

通过检查 ME 设备,并且若控制器作为主要操作功能的一部分,则通过检查可用性工程文件来检验是否符合要求。

201.9.2.3.1.102 * 与患者、操作者或 RACA 机器人共同控制相关的非预期运动

制造商应识别与患者、操作者或 RACA 机器人共同控制相关的非预期运动或力/力矩,并在风险管理过程中阐明。如存在不可接受风险,应采取额外风险控制措施。

若 RACA 机器人的运动是根据患者运动功能相关生理信号(如肌电、心电或脑电信号)来控制的,则应纳入风险管理过程。如果是通过可编程电子子系统实施,通用标准第 14 章适用。

注:与共同控制相关的非预期运动多出现于 RACA 机器人的正常操作中,RACA 机器人的运动通常是由患者能力、操作者意图、患者移动意图和机器人控制系统决定的。非预期运动不是操作者或环境中其他人员希望的结果。

可通过检查风险管理文档来检验是否符合要求。

201.9.2.3.1.103 与意外能量释放相关的非预期运动

制造商应在风险管理过程中阐明与意外能量释放有关的非预期运动。如存在不可接受风险,应采取额外风险控制措施。

注:能量来源包括承载弹簧、压力容器(液压或气动)、平衡物、飞轮等。储存的电能被释放时会导致执行器发生非预期运动。

可通过检查 ME 设备和风险管理文档来检验是否符合要求。

201.9.2.3.1.104 与启动、重启或正常停止相关的非预期运动

RACA 机器人在启动、重启或正常停止程序期间或开始时,可能发生非预期运动。

制造商应在风险管理过程中说明这种非预期运动。如存在不可接受风险,应采取额外风险控制措施。

注:与启动或重启相关的非预期运动包括因上次操作遗留的内部软件状态导致的突然、快速运动。

可通过检查 ME 设备和风险管理文档来检验是否符合要求。

201.9.2.3.1.105 与保护性停止相关的非预期运动

保护性停止可能导致非预期运动。制造商应在风险管理过程中说明这种非预期运动。如存在不可接受风险,应采取额外风险控制措施。

注:与保护性停止相关的非预期运动包括因在突然失去电力或支承的状况下,由重力或惯性引起的非预期运动。

可通过检查 ME 设备和风险管理文档来检验是否符合要求。

201.9.2.3.2 过冲终端限位

增补:

当患者可用力进行主动运动时,通用标准中表 33 的第 4 行适用。

若 RACA 机器人有其他控制模式,则应考虑最不利的测试场景。

增补:

201.9.2.3.101 超出个体患者运动预设范围的运动

在风险分析中,制造商应考虑当运动超出个体患者运动预设范围时会造成的危险。

注 1: 制造商可以考虑以下风险控制措施以将风险降至可接受的水平:

- 限制 RACA 机器人的运动,使其不得超过预设的运动范围(如位置、角度、速度、加速、减速和急拉);或
- 限制输出力或力矩,使其不得超过预设的力或力矩范围。

上述风险控制措施可通过机械和/或电子方式实施,亦可通过 PESS 实施,此时操作者可对控制措施进行配置。

可通过检查风险管理文档和以下测试来检验是否符合要求:

- 输出力或力矩受风险控制措施限制的功能测试;或
- 201.9.2.3.2 中规定的测试,其运动受风险控制措施限制。

操作者可针对每次训练课程或每位患者,考虑患者运动功能的能力、限制和改善对 RACA 机器人的运动设置具体限制。

注 2: 若超过预设范围的运动会导致不可接受的风险,为确保单一故障安全,可采用的风险控制措施包括:将相关部件更换为满足要求的高完善性部件;或采用两套独立的控制链。

201.9.2.4 急停装置

增补:

若 RACA 机器人需要在间断的监护下使用或没有监护,且患者可能需要激活紧急停止,患者就是急停装置的操作者。根据风险管理过程,制造商应在随附文件中提供充分信息,其中应包括对患者操作急停装置能力的要求,以及患者应得到充分的培训以确保适当的态势感知。

可通过检查随附文件和风险管理文档来检验是否符合要求。

201.9.2.5 患者的释放

在第一段的列表中增补:

- RACA 机器人的停止可能使患者处于危险情况。例如,未能在规定时间内释放患者可能导致危险情况发生。因此,在某些情况下可能会要求能够手动移动在关机状态下的 RACA 机器人或其部件,从而释放患者。

在风险管理过程中,应特别注意以下内容:

- 患者因受伤或意识不清导致的能力受限;
- 操作者可获得性受限或没有;
- 态势感知;
- 患者可以是操作者;
- RACA 机器人可能在家庭护理环境中使用(见 YY 9706.111—2021)。在这种情况下,非专业操作者可能无法或不能将患者从 RACA 机器人上释放下来;
- 将患者从 RACA 机器人上释放下来可能需要不止一个操作者。

增补:

201.9.2.101 保护性停止功能

如需设置一个或更多保护性停止功能,则应满足以下所有要求:

- 将风险降低至可接受水平;
- 由 PEMS/PESS 自动触发;

——遵循通用标准第 14 章“可编程医用电气系统(PEMS)”(如适用)。

除非 PEMS/PESS 的自动重启不会导致不可接受的风险,否则应由操作者手动进行重启。

保护性停止可保持驱动力,从而将风险降低至可接受水平。

可通过检查 ME 设备、风险管理文档和功能测试来检验是否符合要求。

201.9.3 与面、角和边相关的机械危险

增补:

注:袖口、皮带等纺织品和柔性构件也可能存在粗糙表面、尖角和锐边。

201.9.8 * 支承系统相关的机械危险

201.9.8.1 概述

第一破折号替换:

——支承、悬挂和驱动系统的结构应基于 201.9.8.2 和各系统的总载荷进行设计。

在第一段的列表中增补:

——对于其驱动应用部分需要重复运动的 RACA 机器人,如果风险评估显示在预期使用寿命内的过早失效会导致不可接受的风险,则应通过适当的疲劳或耐久性试验对实施的风险控制措施进行验证。

注:有关支承、悬挂和驱动系统的示例,请参见附录 AA 中的 201.9.8,其提供了 RACA 机器人制造商关于上述系统类型和如何确定其总载荷的说明。

可通过检查 ME 设备、设计文件和风险管理文档来检验是否符合要求。

增补:

RACA 机器人支承系统可能包括支撑、悬挂或驱动系统以及 RACA 机器人的驱动应用部分(满足各自驱动系统部件的定义)。RACA 机器人自身也可能是支承系统(如例 6;附录 AA 的 201.9.8 中提到的步行式下肢外骨骼 RACA 机器人)。RACA 机器人也可能由多个不同的支承、悬挂或驱动系统构成,且每个系统的总载荷均不同。制造商应在风险管理过程中对每个系统进行识别和评估。

注 101:更多有关支承、悬挂或驱动系统的解释,请参见附录 AA 的 9.8。

若支承系统失效会导致不可接受的风险,其结构强度应符合通用标准中表 21 的拉伸安全系数。制造商应确定各支承、悬挂或驱动系统每个部件各自的总载荷。

注 102:通用标准中表 21 的 A 类或 B 类的选择不仅取决于总载荷,还取决于材料的拉伸强度。请参见通用标准中表 21 的脚注。A 类需能够准确得知总载荷和材料拉伸强度。若两者其一无法确定,则适用表 21 中的 B 类。

注 103:需支承或悬挂的患者面临的常见危险是在支承或悬挂系统发生机械故障后失去平衡和跌倒。

注 104:支承或悬挂系统可对抗重力使患者保持一个姿势。

注 105:可通过适当的人体试验装置进行型式试验,来支撑风险管理过程(如人体质量分布,参见通用标准中图 A.19)。

201.9.8.2 拉伸安全系数

在第一段后增补:

注 101:对于 RACA 机器人,支承系统包括支承、悬挂和驱动系统。而 RACA 机器人的驱动应用部分按定义来说属于驱动系统的部件。

注 102:为给出结构强度要求,通用标准中表 21 的 A 类或 B 类的选择不仅取决于总载荷,还取决于材料的拉伸强

度。请参见通用标准中表 21 的脚注。A 类需能够准确得知总载荷和材料拉伸强度。若两者其一无法确定,则适用表 21 中的 B 类。

注 103: 其他证明预期使用寿命内结构完整性的方法还包括疲劳测试或使用高完善性的元器件。

替换表 21 后的最后两段,脚注除外:

可通过检查 ME 设备和风险管理文档来检验是否符合 201.9.8.1 和 201.9.8.2 的要求。在必要时还可配合以下方面的测试:

- 支承、悬挂或驱动系统的结构;
- 所用材料的规格和描述;
- 上述材料的加工说明;
- 根据附录 AA 对总载荷进行的承重计算/说明;以及
- 如有必要,可通过试验证明仍保持在制造商规定的范围内。

应对被测支承装置逐渐加载至总载荷乘以所要求的拉伸安全系数的载荷。被测的支承装置在 1 min 内能够保持平衡或者,即便失败,也不会导致不可接受的风险。

201.9.8.3.1 概述

增补:

注 1: 通用标准的 9.8.3 仅适用于支承患者或操作者全身重量的支承或悬挂系统。示例与原理请参见通用标准附录 A 的 9.8.3.3。

注 2: 若 RACA 机器人需要与升降机或起吊装置一同使用,则参见 GB/T 20404,其中提到了 9706(所有部分)未涉及的其他有关危害的指导。

注 3: 附录 AA 的 201.9.8 介绍了该条在不同 RACA 机器人上的应用示例。

增补:

201.9.101 与功能性异位相关的机械危险

风险管理过程中应说明与患者和驱动应用部分功能性异位相关的危险。

可通过检查风险管理文档来检验是否符合要求。

201.10 对不需要的或过量的辐射危险(源)的防护

通用标准第 10 章适用。

201.11 对超温和其他危险(源)的防护

通用标准第 11 章适用。

201.12 控制器和仪表的准确性和危险输出的防护

除下述内容外,通用标准第 12 章适用。

增补:

201.12.101 RACA 机器人运动或力/力矩

制造商应通过风险管理过程识别出可预测的、与 RACA 机器人驱动应用部分的运动或力/力矩缺

失或降低相关的危险。若该运动或力/力矩属于临床功能,制造商应明确正常状态和单一故障状态下的性能限制。若超出性能限制会导致不可接受的风险,则该运动或力/力矩是基本性能。在这种情况下,制造商应采取风险控制措施将风险降低至可接受水平。

注:运动或力/力矩的特征取决于多种不同的因素:空间坐标、时机、速度、稳定性、幅度、压力、正位/异位、安装和其他相关因素。

可通过检查设计文件/性能限制来检验是否符合要求。必要时也可检查随附文件、风险管理文档和进行功能测试。

201.12.102 评定测量

制造商应通过风险管理过程识别出可预测的、与 RACA 机器人评定测量缺失或降低相关的危险。若该评定测量属于临床功能,制造商应明确正常状态和单一故障状态下的性能限制。若其缺失或降低会导致不可接受的风险,则该评定测量是基本性能。在这种情况下,制造商应采取风险控制措施将风险降低至可接受水平。

可通过检查设计文件/性能限制、随附文件、风险管理文档和进行功能测试来检验是否符合要求。

201.13 ME 设备危险情况和故障状态

除下述内容外,通用标准第 13 章适用。

201.13.2 单一故障状态

增补:

201.13.2.101 可能导致态势感知缺失的部件故障

201.4.2.3.102 针对会导致态势感知缺失的部件提出了要求。

注 1: 这些部件通常会影响操作者的感知和/或理解,从而影响态势感知。例如,与声音/视觉/触觉相关的部件向操作者提供的反馈。

注 2: 并非所有暂时性态势感知缺失都与部件失效、基本安全和基本性能存在直接联系。例如,如果显示 RACA 机器人状态信息的显示器故障,操作者很容易发现信息丢失并做出适当反应。

201.14 可编程医用电气系统(PEMS)

通用标准第 14 章适用。

201.15 ME 设备的结构

除下述内容外,通用标准第 15 章适用。

201.15.1 ME 设备控制器与指示器的布置

增补:

注: 控制器和指示器的可用性对态势感知有重要影响。

201.15.3.1 * 概述

表 28 机械强度试验的适用性

增补：

ME 设备类型	试验相关条款
步行式	推力(15.3.2)
	冲击(15.3.3)
	坠落(201.15.3.4.101)
	模压应力消除(15.3.6)
	跌倒(201.15.3.101)

201.15.3.4 坠落试验

增补：

201.15.3.4.101 步行式 RACA 机器人

步行式 RACA 机器人、附件和设备部件应能承受从通用标准中表 29 所属高度自由落体至坚硬表面所带来的应力。

通过下列试验来检验是否符合要求：

被测样品(不施加任何载荷),置于 $50\text{ mm} \pm 5\text{ mm}$ 厚的硬木(例如, $> 600\text{ kg/m}^3$)板上方提到如通用标准中表 29 所规定的高度,硬木板平放于混凝土地面或类似的硬质基础上。试样从正常使用可能放置的每种姿态(不施加任何载荷运输状态)坠落三次。且所有可固定部件均按照使用说明书进行固定。试验后,任何导致一个不可接受风险的损坏,则测试不通过。

201.15.3.101 步行式 RACA 机器人跌倒

正常使用步行式 RACA 机器人时,若不慎跌倒,应不得造成基本安全或基本性能的缺失。

如有必要,可通过检查风险管理文档和进行功能测试来检验是否符合要求。

注 1: 跌倒指失去平衡,从正常使用的位置跌落。例如,步行式 RACA 机器人站在正常使用的位置,然后倾斜,直到达到一个不稳定的位置,然后从这个位置自由地倒在地上。

注 2: 实施风险控制措施是解决此问题的一种方法,防止步行式 RACA 机器人在正常使用过程中跌倒。

201.15.4.3 电池

通用标准的 15.4.3.1 前增补：

201.15.4.3.101 概述

除通用标准中 15.4.3 的要求外,非锂电池还应根据通用标准的 4.8 和图 5 的原则,遵守现行电池技术相关的国家标准或行业标准适用的安全要求。任何与电池技术相关的国家标准或行业标准未涵盖的危险(源)应按照通用标准的 4.2.3.2 进行处理。

应通过检查电池设计文档,进行相关的国家标准或行业标准中明确的测试,或在适用情况下,检查

风险管理文档,来检验是否符合要求。

201.15.4.5 预置控制器

增补:

注 1: 本条款是指与手动可调硬件预置控制器相关的风险,而通用标准的其他章节(如第 12 章)并没有完全表述这些风险。

注 2: 与软件预置相关的风险由通用标准的其他部分(如第 12 章或第 14 章)表述。

增补:

201.15.4.101 无线的手持式和脚踏式控制装置

通用标准中 15.4.7 的要求适用于无线的手持式和脚踏式控制装置。

201.16 * ME 系统

通用标准的第 16 章适用。

201.17 * ME 设备和 ME 系统的电磁兼容性

除下述内容外,通用标准的第 17 章适用。

增补:

注: 更多信息见第 202 章。

202 电磁兼容——要求和试验

YY 9706.102—2021 适用。

202.4.3 * 通用测试条件

202.4.3.1 配置

增补:

制造商应考虑单一故障情况并在风险管理文档中进行表述。但对于电磁兼容性测试,通用标准的单一故障情况要求不适用。

206 可用性

YY/T 9706.106—2021 适用。

208 * ME 设备和 ME 系统中报警系统的通用要求、测试和指南

除以下内容外,YY 9706.108—2021 适用。

增补:

注: 附加信息见附录 AA 第 208 章。

210 * 生理闭环控制器的开发要求

除以下内容外,YY/T 9706.110—2021 适用。

增补:

注:附加信息见附录 AA 第 210 章。

211 * 家庭护理环境中使用的 ME 设备和 ME 系统的要求

除以下内容外,YY 9706.111—2021 适用。

211.7.4 使用说明书

增补:

211.7.4.101 RACA 机器人的增补要求

随附文件应以非专业操作者能理解的方式解释 PEMS 自主程度的影响。

注:非专业操作者对 RACA 机器人自主行为的理解是操作者态势感知和可用性工程的关键。

可通过检查随附文件和可用性工程文件来检验是否符合要求。

211.10.1.1 机械强度的通用要求

表 1 非转移时可运行的设备的机械强度测试的适用性

增补:

ME 设备的使用和类型	通用标准或本文件规定的试验相关条款	YY 9706.111—2021 规定的试验相关条款
非转移时可运行的步行式设备	推力(15.3.2)	
	冲击(15.3.3)	
	坠落(201.15.3.4.101)	
		抗震[10.1.3a)]
		振动[10.1.3c)]
	模压应力消除(15.3.6)	
	跌倒(201.15.3.101)	

表 2 转移时可运行的设备机械强度测试的适用性

增补：

ME 设备的使用和类型	通用标准或本文件规定的试验相关条款	YY 9706.111—2021 规定的试验相关条款
转移时可运行的步行式设备	推力(15.3.2)	
	冲击(15.3.3)	
		自由落体[10.1.3d)]
		抗震[10.1.3a)]
		振动[10.1.3c)]
	模压应力消除(15.3.6)	
	跌倒(201.15.3.101)	

附 录

除下述内容外,通用标准的附录适用。

附 录 A

(资料性)

通用指南的原理说明

A.1 通用指南

增补:

鉴于 RACA 机器人具有一定程度的自主性以及下列几个方面,故对 RACA 机器人的要求不同于其他 ME 设备和 ME 系统:

- a) 或者是可穿戴式的,
- b) 或者是将患者从一个位置移动到其他位置,
- c) 或者是在较长时间内与患者有近距离接触,
- d) 或者是连续不断地移动患者的身体部位,
- e) 或者是与患者交换能量(动能或势能),或将力传递给患者,
- f) 或者控制患者与 RACA 机器人之间的不同级别的协作,以及
- g) 或者是需要处理来自患者的多模态传感器输入来执行物理交互控制。

若干个这些方面的组合使 RACA 机器人是独特的。

附录 AA
(资料性)
专用指南和原理说明

AA.1 通用指南

附录 AA 为本文件的重点要求提供了简明的原理说明,且适用于熟悉本文件主题但没有参与本文件制定的人员。理解重点要求的原理对正确应用本文件是很重要的。此外,随着临床实践和技术的发展变化,相信下述要求的原理说明将有助于对本文件进行必要的修订。

AA.2 具体章节和条款的基本原理

以下是本文件中具体章节和条款的原理说明,其中章节和条款编号与本文件正文中相应的章节和条款编号相同。

条款 201.3.63 ME 设备

通用标准中图 A.20 旨在阐明手持的、可携带的、移动的和可转移的 ME 设备之间的关系。然而,没有对步行式 ME 设备进行分类。图 AA.1 包含了该新分类。

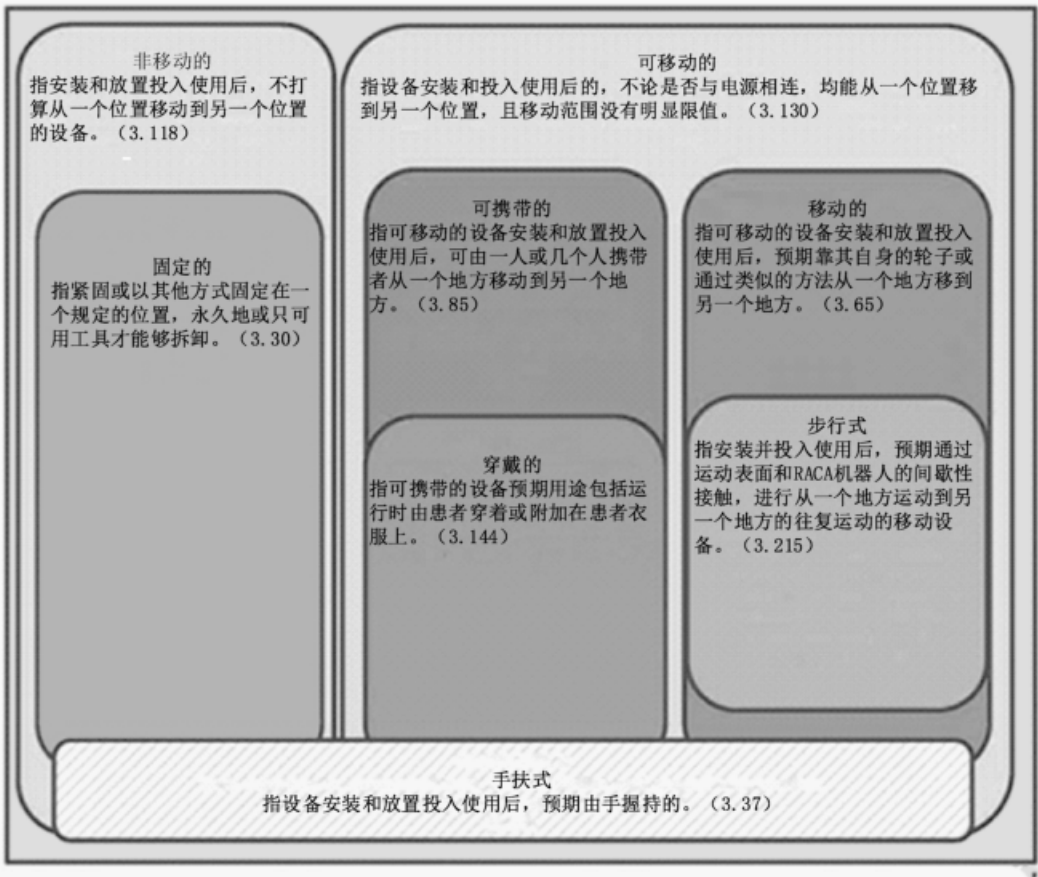


图 AA.1 描述设备、附件或设备部件术语之间的关系

条款 201.3.144 穿戴的

在通用标准中,可穿戴的设备的定义与图 A.20 不一致。具体来说,图 A.20 表明,可穿戴的设备是可携带的设备的一个有向子集,而通用标准的 3.144 中的定义表明可穿戴的设备是可转移的设备(而非可携带的设备)的一个有向子集。

条款 201.3.201 驱动应用部分

应将驱动应用部分视为通用标准中描述的应用部分,但同时需要考虑本文件中定义的附加注意事项。

条款 201.3.203 评定

为阐明测量、评定和诊断之间的关系,这里举例:

RACA 机器人将外骨骼应用于患者各手臂上,可以用于各种各样的神经学的评定,比如评定患者的本体感受。例如,遮挡患者视线,RACA 机器人将患者的一只手臂运动到指定位置,之后患者在指导下将另一只手臂运动到镜像位置。重复测量可用于评定患者的准确性、一致性等。

在本例中:

- a) RACA 机器人在执行作业时测量患者手部位置(即确定患者另一手臂与 RACA 机器人移动的手臂的镜像匹配程度)。
- b) RACA 机器人通过测量患者的手部位置来评定患者两手臂镜像匹配的准确性和一致性,从而评定患者的本体感受损伤程度。
- c) 临床医生使用该评定和其他检测结果来诊断患者(如短暂性脑缺血发作)或监测恢复情况(如中风后)。

条款 201.3.207 损伤

ISO 9999:2016 定义的术语是基于世界卫生组织 2001 年《国际功能、残疾和健康分类》^[16] 提供的更复杂的定义并修订的:

“损伤指身体结构或生理功能(包括心理功能)的丧失或异常。此处的‘异常’严格意义上指相比于公认统计标准的显著差异(即在公认标准规范内与总体均值的偏差),并且应该仅在这个意义上使用。”

条款 201.3.210 保护性停止

由于 RACA 机器人有一定程度的自主性,会有因基本安全而自动触发停止程序的能力。这就需要新的术语来区分这一新的停止功能与紧急停止。其他标准使用“保护性停止”这一术语,对此我们已经引用并做修改。具体在于,本文件不允许手动触发保护性停止,相反,ISO 13482:2014 允许手动和自动触发保护性停止。在紧急停止后接着手动操作触发保护性停止,这会使操作者对在紧急情况下使用哪种停止程序感到困惑。

另外,保护性停止和紧急停止的另一个区别是紧急停止不能自动重新启动。按照 201.9.2.101 的规定,对于 RACA 机器人,保护性停止可以手动或自动重新启动。只有经风险管理过程确认,才允许自动重启。

保护性停止示例:RACA 机器人检测到某种与控制回路不稳定性相关的振荡,随后触发停止程序。

条款 201.3.211 康复

如 201.3.211 中注 3 所述,本文件中康复的定义不同于世界卫生组织所给的定义。世界卫生组织

《世界残疾报告》(2011年)将康复定义为:“帮助已经或可能将要残疾的个人,在与其环境的相互作用中实现和维持最佳功能的一系列措施。”该定义涵盖了各种各样的潜在干预措施,包括身体的、认知的和作业疗法。本文件中康复的定义旨在聚焦于在本文件的范围内康复治疗的子集,以处理与患者损伤相关的运动功能,并强调其他与康复有关的术语。

患者因疾病或伤害受到损伤后的康复是一个复杂的过程。根据患者的具体情况,康复过程未必是相同的。通常,当急性护理措施结束,康复过程开始时,效果并不明显。而且,康复过程何时结束往往不易鉴定。

康复、评定、代偿和缓解过程可以以串行或并行方式进行。

根据 ISO 9999:2016 的 2.10,“功能”(作为术语“康复”的一部分)是“身体功能、身体结构、活动和参与的涵盖性术语,表示个体(健康状况)与其情境因素(环境和个人因素)之间相互作用的积极方面。”

条款 201.3.213 机器人

自主性是 IEC/TR 60601-4-1:2017 的 3.4 定义的一个术语,指在没有或有限操作干预的情况下监测、生成、选择和执行临床功能的能力(有待调整)。

自主性

在没有或有限操作者干预的情况下,监测、生成、选择和执行临床功能的能力。

注 1: 在通用语言中术语“自主性”用来表示“零自主程度”或“完全自主程度”,而不允许表示介于二者的中间程度。

建议谨慎使用术语“自主性”,并尽可能使用术语“自主程度(DOA)”来替代。

注 2: 术语“零自主性”和“完全自主性”可以用来表示“零自主程度”和“完全自主程度”,且不会混淆。

注 3: 术语“自主性”这一定义是根据 ISO 8373:2012 的 2.2 的定义得出的。所做修改的原因参阅 IEC/TR 60601-4-1:2017 的 A.2。

[来源:IEC/TR 60601-4-1:2017,3.4]

监测(动词)

收集和解释必要信息,以感知 ME 设备或 ME 系统、患者、操作者或环境的状态。

注: 源自 Kaber 和 Endsley^[21],他们将该术语定义为“包括接收与感知系统状态相关的所有信息(如扫描可视化显示)”。

[来源:IEC/TR 60601-4-1:2017,3.23]

生成(动词)

根据监测任务的结果,为实现预定目标制定合理的方案。

注: 源自 Kaber 和 Endsley^[21],他们将该术语定义为“为实现目标制定方案或任务策略”。

[来源:IEC/TR 60601-4-1:2017,3.11]

选择(动词)

从生成的方案中选定一个具体方案。

注: 源自 Kaber 和 Endsley^[21],他们将该术语定义为“选定一个具体方案或策略”。

[来源:IEC/TR 60601-4-1:2017,3.42]

执行(动词)

实施选定的方案。

注：源自 Kaber 和 Endsley^[21]，他们最初使用“实行”而不是“执行”。

[来源：IEC TR 60601-4-1:2017,3.9]

条款 201.3.214 态势感知

态势感知可以简单地解释为“一种对态势的适当感知”^[17]。虽然这一通用概念在许多领域得到广泛认同，但在试图应用态势感知这一概念以理解其重要性和相关性时，就需要有一个更准确的定义。因此，多年来提出了许多不同的定义（见参考文献[18]回顾）。在 ISO 标准中，目前唯一对态势感知作出定义的是 ISO 11064-7:2006 的 3.4：“操作者/用户对受控系统和/或过程情况的理解与任何当时的实际情况之间的关系”。在 IEC 标准中，目前唯一对态势感知作出定义的是 IEC 61924-2:2012 的 3.1.75：“水手对所提供的航行和技术信息的感知，对其含义的理解，以及对其在近期的状态的预测，这些都是对情况作出及时反应所必需的要素。态势感知包括模式感知”。显然，最后一种定义遵循的是 Endsley 给出的最通俗的定义，其用三级法对态势感知的含义进行了提炼：

“态势感知指在大范围的时间和空间内对环境要素的感知、对其含义的理解以及对其近期状态的预测”。

这里采用 Endsley 的三级法来定义态势感知。

Endsley 的三个级别方法如图 AA.2 所示，其阐明了充分的态势感知过程：对某种情况的感知（如 RACA 机器人的行为），对这种情况及其重要性的理解，以及对未来潜在的状态和事件的预测（这种预测取决于决策）。

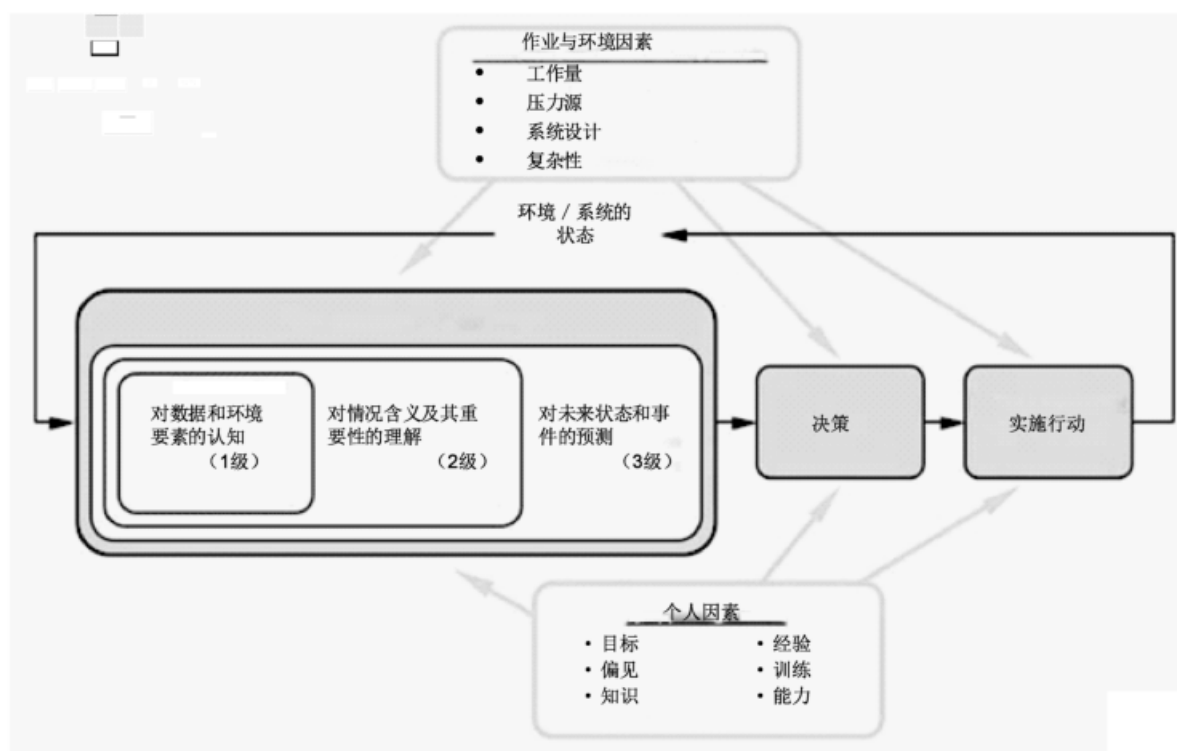
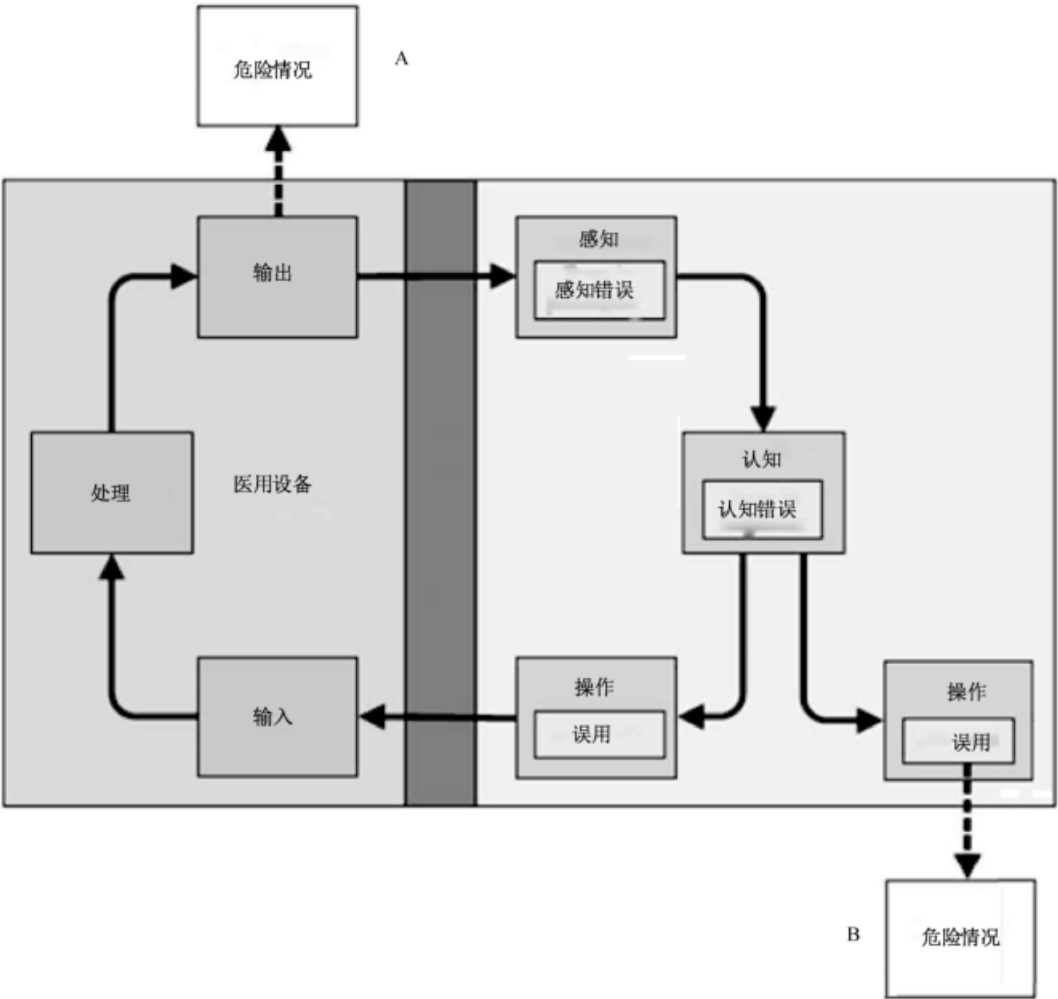


图 AA.2 Endsley 的态势感知理论模型

（基于参考文献[20]，由 Peter Lankton 博士于 2007 年 5 月绘制）

图 AA.2 为 IEC 62366-1:2015 图 A.1 的右侧部分,将其复制到这里为图 AA.3。



标引序号说明：

A —— 由该医用设备的响应而引起的危险情况。

B —— 由用户的操作或者操作不足而引起的危险情况,其中操作是作用于患者或者是从该医用设备获取信息但却使用了不同的医用设备。

其中,将感知理解为感知或缺乏感知,将认知理解为认知或缺乏认知,将行动理解为行动或缺乏行动。阴影较浅的错误框是可能发生错误的位置。

来源:IEC 62366-1:2015 图 A.1。

图 AA.3 用户-医用设备交互模型

表 AA.1 说明了图 AA.2 和图 AA.3 之间的映射关系。

表 AA.1 图 AA.2 和图 AA.3 之间的映射关系

图 AA.2 框图	图 AA.3 框图
Endsley 的态势感知模型	IEC 62366-1:2015
感知(态势感知的 1 级)	感知
理解(态势感知的 2 级)	认知
预测(态势感知的 3 级)	—
决策	—
动作实施	操作
环境状态	—
作业与环境因素	—
个人因素	—
—	输入(ME 设备)
—	过程(ME 设备)
—	输出(ME 设备)
—	危险情况(ME 设备和用户)

综上所述,图 AA.2 更倾向于操作者,而图 AA.3 同时倾向于操作者和 ME 设备。图 AA.2 中的一个重要元素是环境,环境是由 ME 设备的预期用途定义的。虽然认知暗含预测和决策这两层含义,但在 IEC 62366-1 中都没有明确提及,因此可能会被制造商忽略。

应该注意的是,态势感知也与 RACA 机器人的环境有关。IEC 指南 109:2012 的 3.3 将环境定义为:“一个产品或系统所在的周围的事物,包括空气、水、土地、自然资源、植物、动物、人类及其相互关系”。构成 RACA 机器人环境的范围取决于其环境本身。具体而言,RACA 机器人的环境包括患者以及和患者和/或 RACA 机器人相互作用的任何事物,包括但不限于以下:

- 其他 RACA 机器人;
- 其他医用设备,如轮椅;
- 其他设备;
- 人类或动物;
- 操作者;
- RACA 机器人所在房间或区域的环境条件,如
 - 光照条件,
 - 物理障碍(如椅子、门和墙),
 - 地面或楼层(如是水平的吗,是平坦的吗);
- 家庭护理环境的具体情况,如拥挤的人行道、地铁、公共交通、公共场所等。

条款 201.4.2.3.102 风险管理和态势感知

尽管将一定程度的自主性加入到系统中可以提高系统的许多能力,但航空业等其他行业的经验表明,提高自主程度有时会导致伤害风险的增加(见参考文献[21])。早期研究和调查已经表明,提高自主程度带来的一个问题就是,它会导致操作者态势感知的缺失,反过来又会导致误用。更具体而言,缺失态势感知可能导致两种潜在的失效模式^[21]:

- a) 操作者未发现问题;

b) 操作者未理解问题。

根据问题的本质,这两种失效模式中的任何一种都能够导致误用,从而对 RACA 机器人的使用带来危险情况。

为符合 201.4.2.3.102 的要求,当制造商识别出可能导致不可接受风险的与态势感知相关的危险(源)或危险情况时,制造商应遵循风险管理过程,识别并实施充分的风险控制。随附文件中的必要信息应包括以下内容:

- 可能导致态势感知缺失的危险(源)或危险情况的描述,包括
 - 任何警告信号和该危险情况的可能结果,以及
 - 操作者为将风险降低到可接受水平所应采取的必要措施;
- 如有必要,应在随附文件和 RACA 机器人的适当位置提供显著标记(如警告、注意等);
- 风险管理过程所识别的操作者培训措施也应涵盖这些信息,以将风险降低到可接受的水平。

在正常使用 RACA 机器人的过程中,机器人可能会具有不同程度的自主性以执行不同的作业,从而使得操作者和 RACA 机器人的责任分工不同。通常情况下,随着 RACA 机器人自主程度的增加,缺失态势感知的可能性亦会增加。关于将自主程度与风险联系起来以及态势感知缺失的进一步指导,请参阅 IEC TR 60601-4-1:17 的 5.4.2 和附录 D。有关改善态势感知的方法,请参阅 BB.3。

条款 201.3.215 步行式

- 步行式 RACA 机器人可以按照制造商的意图在不同的场景下运行,其可能会影响风险管理过程,例如:
- 患者自由行走(除步行式 RACA 机器人外,不需要任何其他支承);
- 患者使用拐杖、助行器/助行车等额外的辅助工具自由行走;
- 由不是患者的操作者支承行走;
- 由悬挂系统进行支撑或固定行走。

条款 201.4.7 ME 设备单一故障状态

第 BB.4 章中推荐了一些可用于评定是否保持充分的态势感知的示例方法。

条款 201.9.2.3.1 非预期运动

运动通常是 RACA 机器人的主要操作功能(IEC 62366-1:2015),尤其是 RACA 机器人支承的患者运动。使能或禁能 RACA 机器人的驱动运动功能的开/关控制器,应该区别于直接控制运动的控制器。这些开/关控制器应妥善放置、凹进或以其他方式进行保护,使其不会意外启动或禁用。

直接控制 RACA 机器人运动的控制器通常不用于高精度的轨迹控制,因此造成的 RACA 机器人的运动,以及患者的运动,很可能是部分无意识的运动(在准确的时机或位置下)。

对于 RACA 机器人,非预期运动会伴随着其他运动而发生,这种其他运动不同于操作者所期望的在准确的时机和/或位置下的运动,或者不是由操作者精确定义的运动。当有意开启与患者运动相关的主要操作功能时,RACA 机器人会对运动产生如此主动的影响。由于下述原因,可能会发生非预期运动。

- 涉及到准确的时机,或运动的准确轨迹,RACA 机器人可能会触发并控制操作者(可能是患者)非预期的运动。根据定义,这种情况会在机器人具有一定程度的自主性时发生(更多信息请参阅 IEC TR 60601-4-1:17)。RACA 机器人的操作通常由操作者、患者或 RACA 机器人共享(请参见 9.2.3.1.102)。
- 假设 RACA 机器人,操作者、患者和 RACA 机器人本身可以共享对运动功能的控制(不止一个控制点,请参见 9.2.3.1.102),且每个运动都可能是某一个操作者有意为之,并非其他操作

者,这将导致一定程度上非预期运动。

例如,操作者(在本例中是治疗师)设计一个训练运动(预期的)。患者需要作为二级操作者开始运动。若患者作为二级操作者,无意地开始了运动,该运动是非预期的;运动正确,但时机不对。

——患者对 RACA 机器人的特定控制可能会使得控制精度受限,例如,若使用生物物理信息时控制界面是“隐含的”;直接运动控制可能缺乏精度,从而导致非预期的速度、运动范围、运动时机、运动协调和停止。

制造商应处理风险管理过程中非预期运动的各个方面;为了防止不可接受的风险,应实施额外的风险控制。

注: ISO 10218-1:2011 的 5.8~5.10,在超过单一控制的情况下,可以帮助制造商实行与非预期运动相关的风险管理过程。

条款 201.9.2.3.1.102 患者、操作者和 RACA 机器人之间共享控制的非预期运动

共享控制是系统控制的一个概念,即多个控制者同时控制一个系统。

共享控制是 RACA 机器人的特征,它由 RACA 机器人、患者或操作者中的二者或者多者的共同控制组成。例如,在这种情况下,受控系统通常包括患者的一个或多个肢体,以及 RACA 机器人的一部分,包括与肢体接触的驱动应用部分。在共享控制中,该系统由患者或 RACA 机器人进行控制(见图 AA.4)。在某些情况下,操作者还可以直接与 RACA 机器人的某一部分进行交互(触摸),从而控制同一系统的运动,例如对用于实现临床功能的 RACA 机器人编写运动程序。在这种情况下,三个不同的控制者都是主动性的,如患者、操作者和 RACA 机器人。这三个控制者中每一个都有自己的运动意图。这些意图可能是相同的,或者至少是相似的。但它们也可能会产生相互冲突。从控制者即患者、操作者或 RACA 机器人的角度来看,这样的冲突可能会引发“非预期运动”。在评估具有共享控制的系统时,这种从控制者角度可能带来的冲突是需要考虑的一个重要方面。

在 RACA 机器人的共享控制系统中,患者的运动意图可能反映在运动结果中。如果由此产生的运动与操作者的意图或理解不一致,则可能对操作者造成“非预期运动”的危险,详情请参阅 201.9.2.3.1.102。

在 RACA 机器人的共享控制系统中,即使与操作者的运动意图一致,但运动结果不一定与患者的运动意图一致。这种不一致性可能会给患者带来“非预期运动”的危险,详情请参阅 201.9.2.3.1.102。

图 AA.4 是一个典型的共享控制系统的框图,其中患者和 RACA 机器人共同控制患者肢体的运动。图 AA.5 是一种扩展,其中操作者,即治疗师,直接参与控制患者的肢体运动,而 RACA 机器人通过其驱动应用部分与之连接。图 AA.6 是另一种扩展,其中操作者通过调节 RACA 机器人,间接参与控制患者肢体的运动,而 RACA 机器人通过其驱动应用部分与之连接。如这些图例所示,患者与 RACA 机器人之间的相互作用力和共享位置,提供了如驱动应用部分术语中使用的物理交互的示例。

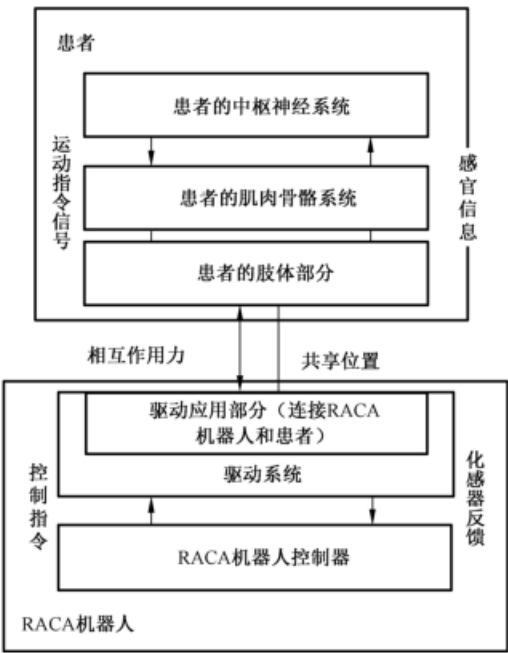


图 AA.4 RACA 机器人共享控制系统框图:由患者和 RACA 机器人进行控制

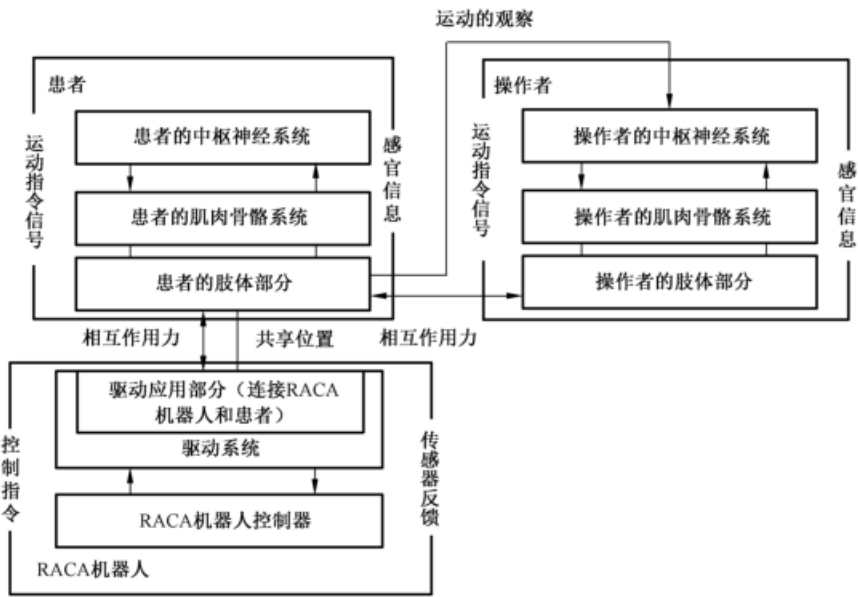


图 AA.5 RACA 机器人共享控制系统框图:由患者、操作者和 RACA 机器人进行控制

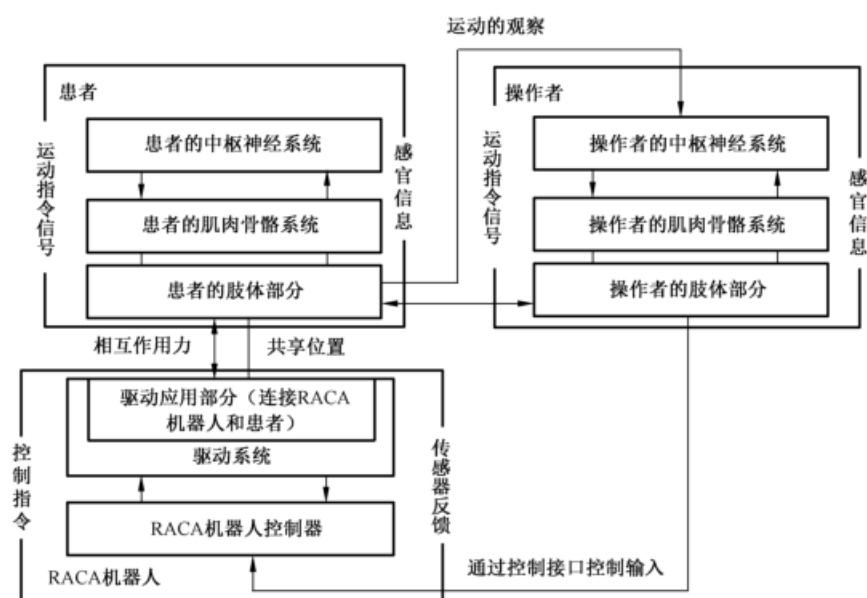


图 AA.6 RACA 机器人共享控制系统框图:由患者和 RACA 机器人进行控制,以及操作者调节

对于操作者和患者,这里其控制视为由他们的中枢神经系统和神经肌肉运动控制构成。在 RACA 机器人中,其控制视为由机器人的“自包含的”控制器构成,即控制算法。控制算法的对象可以多种多样,如位置控制、轨迹控制、力控制或阻抗控制。控制算法也可以设定为只对患者运动做出反应。

示例 1: 具有运动相关生物信号输入的 RACA 机器人的共享控制

RACA 机器人可以使用患者的运动相关生物信号作为其输入之一,以跟随患者的意图和/或运动以实现其预期用途。它也可能有助于降低患者非预期运动的风险。

图 AA.7 说明了步行式 RACA 机器人的示例。

图 AA.8 说明了 RACA 机器人的特定框图,它与患者构成一个共享的控制系统。在本例中,患者和 RACA 机器人的控制器相互作用,不仅通过驱动应用部分,还通过生物信号共同控制患者的肢体和 RACA 机器人的结构。

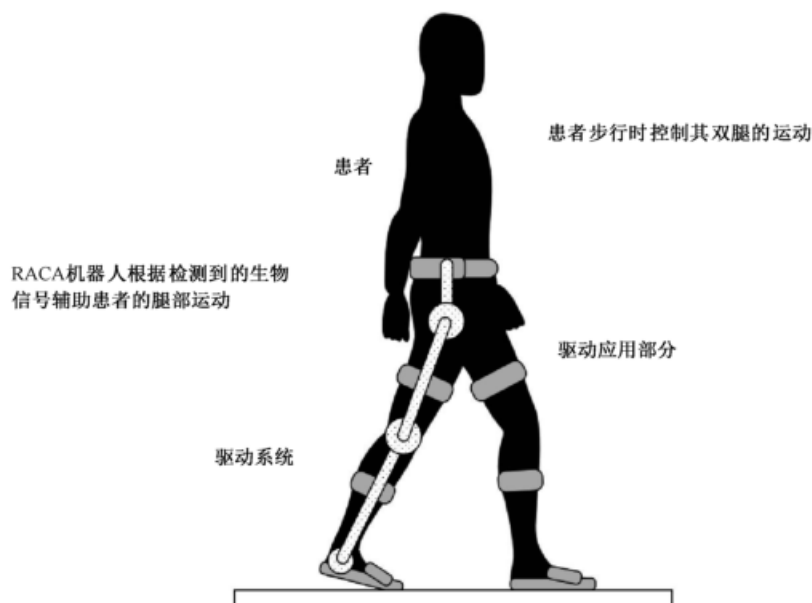
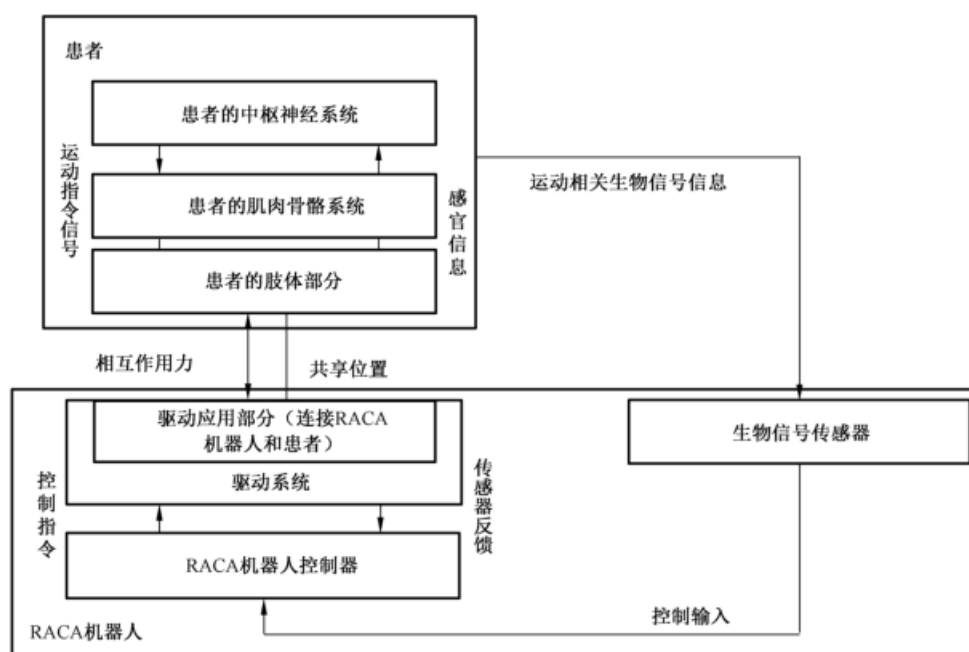


图 AA.7 以运动相关生物信号为输入的 RACA 步行机器人



注：“运动相关生物信号信息”的箭头一般与患者框相连，因为它的具体来源取决于所使用的生物信号的类型（如脑电图来源于中枢神经系统，肌电图来源于肌肉骨骼系统，运动信号来源于身体各个部分）。

图 AA.8 以运动相关生物信号为输入的 RACA 步行机器人的系统框图

示例 2：在患者协同控制下 RACA 机器人的共享控制

RACA 机器人（如用于手臂运动的神经康复）可以使用“患者协同控制”，这是一种控制策略，其目的在于使患者的努力最大化，并且只在需要时提供所需助力，以实现特定的目标，如达到预定的目标位置。

这种到达预定目标的运动可以由操作者设置一种路径，控制患者部位从当前位置移动至运动所预期的目标位置。可以实施一种围绕期望轨迹的力通道（亦称为“虚拟隧道”），如果患者在隧道内运动，RACA 机器人允许其自由不受阻碍，同时 RACA 机器人控制器以实现零相互作用力为目标；但是若切换到柔顺轨迹控制，RACA 机器人则引导患者在将要越过虚拟隧道壁时，以正确方向朝着目标运动。正常情况下作业将由患者执行，当误差变得特别大时，RACA 机器人接管运动控制，或者至少开始支承患者。

这也有助于降低患者非预期运动的风险；这样 RACA 机器人就可以防止出现较大的运动误差。

图 AA.9 说明了这样一种 RACA 机器人的示例，这里机器人是一种带有固定框架的手臂外骨骼，可控制肩部、肘部和腕部关节的运动。

图 AA.10 说明了这种 RACA 机器人的特定框图，它与患者构成一个共享的控制系统。在本例中，患者与 RACA 机器人的控制器通过测量驱动应用部分相互作用力来进行相互作用。这种力直接影响患者身体的运动和 RACA 机器人的物理结构，同时对于 RACA 机器人来说也是一种明确的反馈信号。

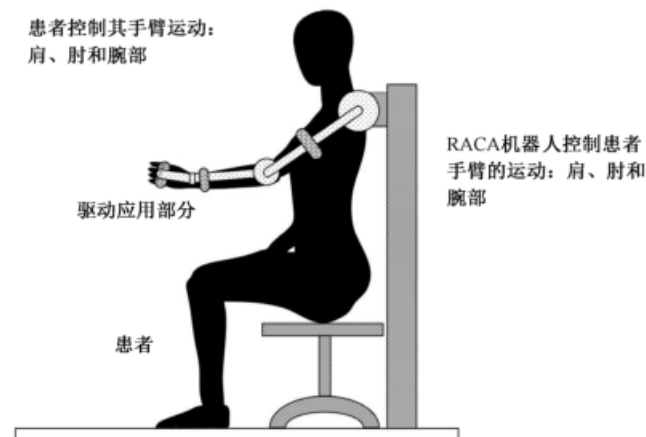


图 AA.9 采用患者协作式共享控制策略的手臂康复外骨骼 RACA 机器人

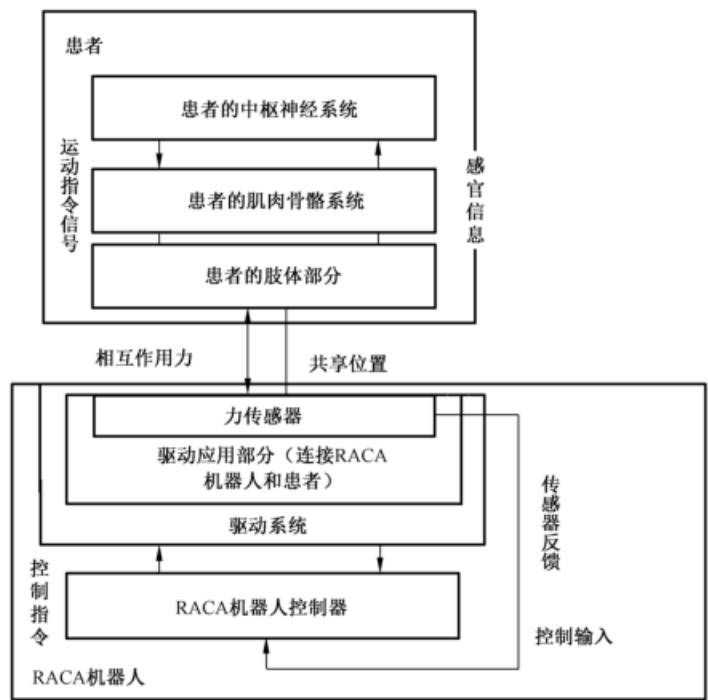
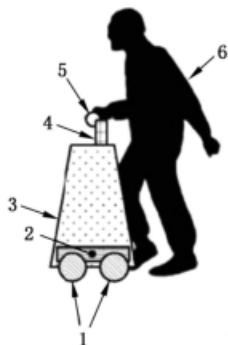


图 AA.10 采用患者协作式共享控制策略的手臂康复外骨骼系统框图

示例 3：手杖式 RACA 机器人的共享控制示例

图 AA.11 说明了一种手杖式 RACA 机器人，它根据测量到的脚部运动来判断患者的意图，并动态地启动和关闭制动器，以支承处于步态康复期间的患者。在适当的时候使用制动器比使用拐杖更容易让患者保持稳定，并使更长时间不间断的步态康复训练成为可能。



- 标引序号说明：
- 1——车轮(支承系统)；
 - 2——制动系统(驱动系统)；
 - 3——主干(支承系统)；
 - 4——把手(支承系统)；
 - 5——手柄(驱动应用部分)；
 - 6——患者。

图 AA.11 用于行走康复的手杖式 RACA 机器人

在本例中,手杖式 RACA 机器人和患者组成了一个共享控制系统。图 AA.12 说明了由一个手杖式 RACA 机器人和患者组成的共享控制系统框图。

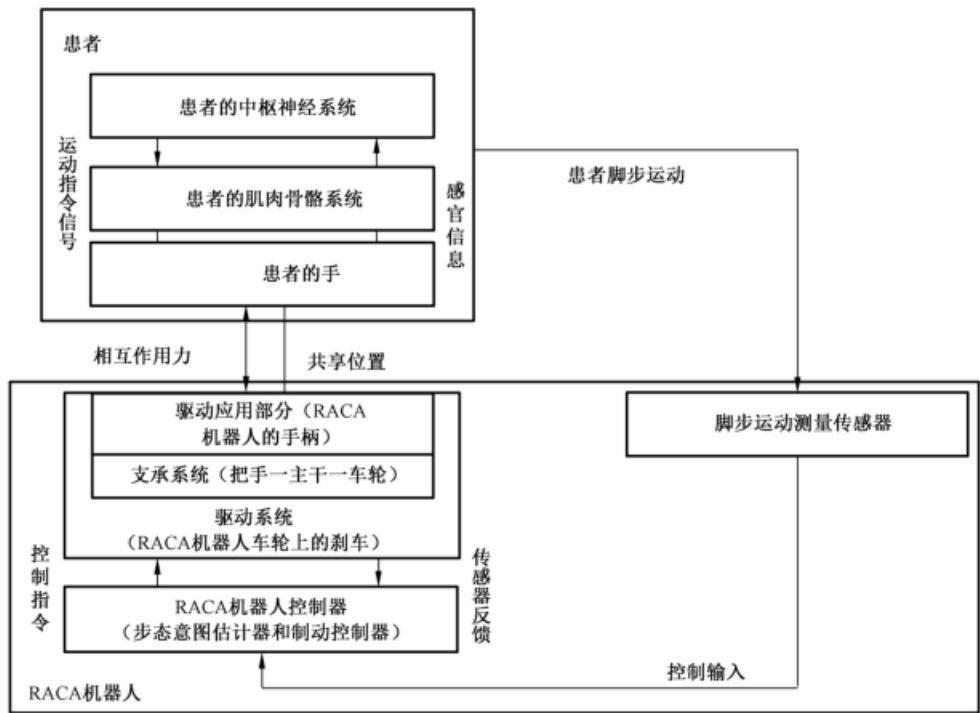


图 AA.12 手杖式 RACA 机器人系统框图

在图 AA.12 中,患者根据其中枢神经系统的运动指令行走,同时通过机器人的反作用力使躯干保持稳定。在每个步态周期中,反作用力借助于施加在车轮上的制动力矩,随时间而变化。因此,患者的步态运动是由患者的中枢神经系统和机器人制动系统进行控制。

条款 201.9.8 支承系统相关的机械危险

以下示例旨在展示驱动、支承和悬挂系统之间的区别,并在 RACA 机器人不同概念中指出驱动应用部分,但没有必要展示实际的训练情况。每个示例都有相似的细节,以帮助那些可能只考虑某个特定示例的读者。

示例 1: 用于下肢的机械臂式 RACA 机器人

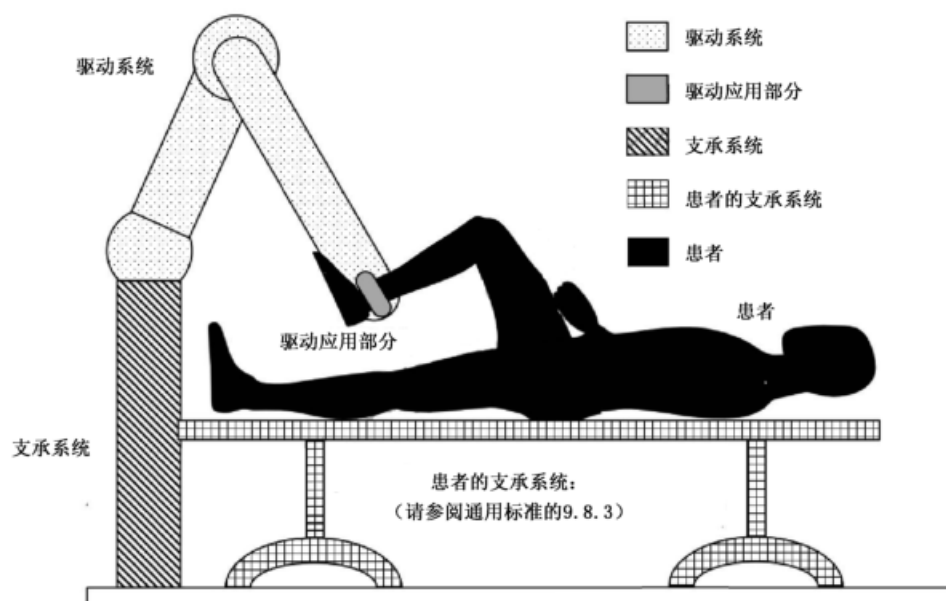


图 AA.13 用于下肢的机械臂式 RACA 机器人示例

制造商可识别驱动应用部分的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢的重量、所识别部件支承的驱动应用部分的重量,以及患者下肢的最大输出力,来确定所识别部件的总载荷。

制造商可识别驱动系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢的重量、所识别部件支承的驱动系统部分的重量包括驱动应用部分的总重量,以及患者下肢的最大输出力,来确定所识别部件的总载荷。

制造商可识别支承系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢的重量、驱动系统的重量包括驱动应用部分的总重量、所识别部件支承的部分支承系统的重量,以及患者下肢的最大输出力,来确定所识别部件的总载荷。

在本例中,患者的支承系统(即图 AA.13 中的床)是 RACA 机器人的一部分,由患者的整个体重静态和动态地进行加载;因此,通用标准 9.8.3 的特定要求适用于支承系统。这归因于机械故障可能构成一种不可接受的风险。

确定总载荷需要包含惯性力,因为 RACA 机器人部件或患者的下肢以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

锁紧机构或终端限位上的总载荷可以用与支承系统或驱动系统的其他部分相同的方式进行确定。然而制造商应该注意符合通用标准中表 21 的拉伸安全系数并不总是意味着通过了过冲终端限位试验。在通用标准的 9.2.3.2 规定的过冲终端限位试验中,终端限位在正常使用和合理预见的误用下,均需要承受住达到终端限位的冲击力。

示例 2: 用于上肢机械臂式 RACA 机器人

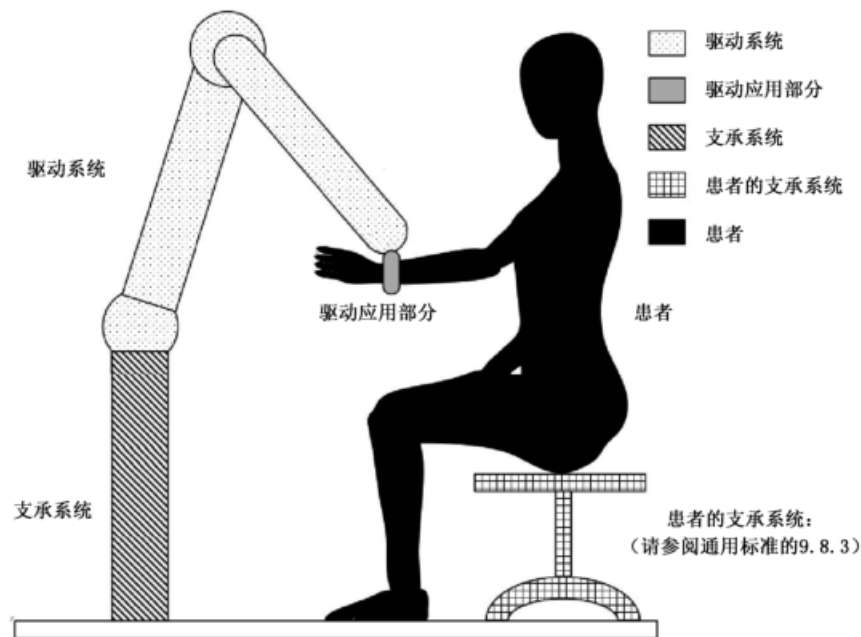


图 AA.14 用于上肢的机械臂式 RACA 机器人示例

制造商可识别驱动应用部分的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者上肢的重量、所识别部位支承的驱动应用部分的重量,以及患者上肢的最大输出力,来确定所识别部件的总载荷。

制造商可识别驱动系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者上肢的重量、所识别部位支承的驱动系统部分的重量包括驱动应用部分的总重量,以及患者上肢的最大输出力,来确定所识别部件的总载荷。

制造商可识别支承系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者上肢的重量、驱动系统的重量包括驱动应用部分的总重量、所识别部件支承的部分支承系统的重量,以及患者上肢的最大输出力,来确定所识别部件的总载荷。

在本例中,患者的支承系统(即图 AA.14 中的椅子)是 RACA 机器人的一部分,由患者的整个体重静态和动态地进行加载;因此,通用标准 9.8.3 的特定要求适用于支承系统。这归因于机械故障可能构成一种不可接受的风险。

确定总载荷需要包含惯性力,因为 RACA 机器人部件或患者的上肢以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

锁紧机构或终端限位上的总载荷可以用与支承系统或驱动系统的其他部分相同的方式进行确定。然而制造商应该注意符合通用标准中表 21 的拉伸安全系数并不总是意味着通过了过冲终端限位试验。在通用标准 9.2.3.2 规定的过冲终端限位试验中,终端限位在正常使用和合理预见的误用下,均需要承受住达到终端限位的冲击力。

示例 3: 用于上肢的外骨骼式 RACA 机器人

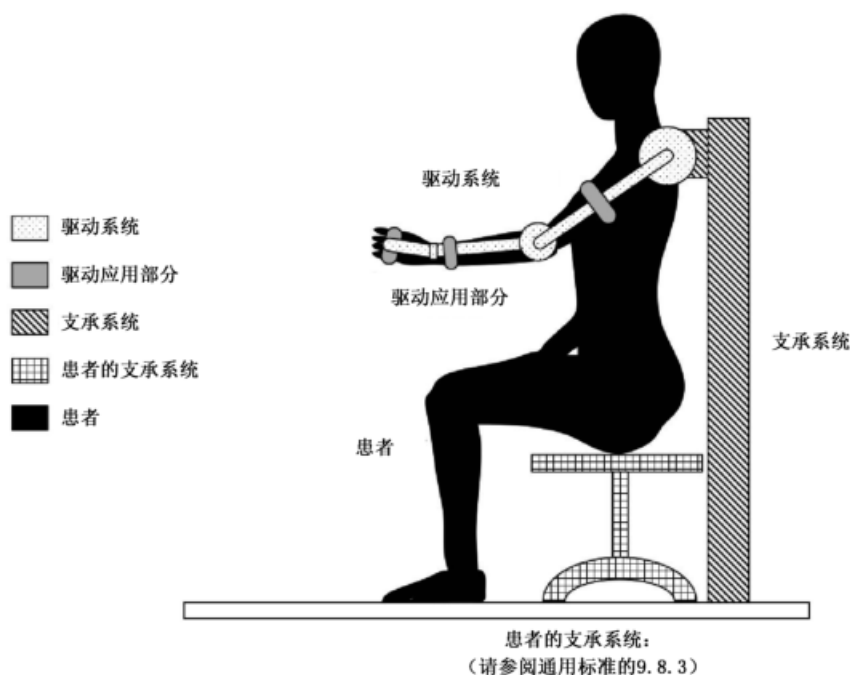


图 AA.15 用于上肢的外骨骼式 RACA 机器人示例

制造商可识别驱动应用部分的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者上肢部分的重量、所识别部件支承的驱动应用部分的重量,以及患者上肢对所识别部件的最大输出力,来确定所识别部件的总载荷。

制造商可识别驱动系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者上肢部分的重量、所识别部件支承的驱动系统部分的重量包括驱动应用部分的总重量,以及患者上肢对所识别部件的最大输出力,来确定所识别部件的总载荷。

制造商可识别支承系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者上肢的重量、驱动系统的重量包括驱动应用部分的总重量、所识别部件支承的部分支承系统的重量,以及患者下肢的最大输出力,来确定所识别部件的总载荷。

在本例中,患者的支承系统(即图 AA.15 中的椅子)是 RACA 机器人的一部分,由患者的整个体重静态和动态地进行加载;因此,通用标准 9.8.3 中的具体要求适用于支承系统。这归因于机械故障可能构成一种不可接受的风险。

确定总载荷需要包含惯性力,因为 RACA 机器人部件或患者的上肢以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

锁紧机构或终端限位上的总载荷可以用与支承系统或驱动系统的其他部分相同的方式进行确定。然而制造商应该注意符合通用标准中表 21 的拉伸安全系数并不总是意味着通过了过冲终端限位试验。在通用标准 9.2.3.2 规定的过冲终端限位试验中,终端限位在正常使用和合理预见的误用下,均需要承受住达到终端限位的冲击力。

示例 4: 用于膝关节的外骨骼式 RACA 机器人

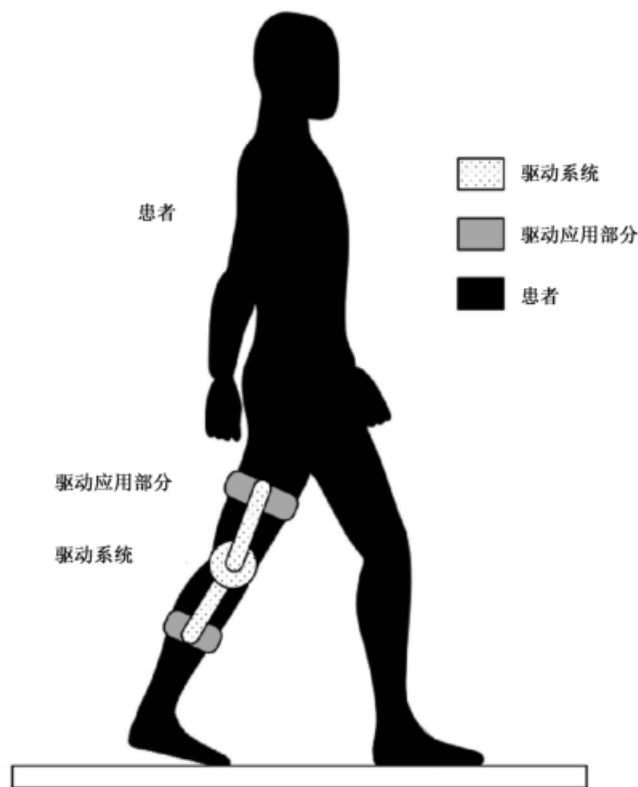


图 AA.16 用于膝关节外骨骼式 RACA 机器人示例

制造商可确定驱动应用部分的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢部分的重量、所识别部件支承的驱动应用部分的重量,以及患者膝关节对所识别部件的最大输出力,来确定所识别部件的总载荷。

制造商可识别驱动系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢部件的重量、所识别部件支承的驱动系统部分的重量包括驱动应用部分的总重量,以及患者膝关节对所识别部件的最大输出力,来确定所识别部件的总载荷。

确定总载荷需要包含惯性力,因为 RACA 机器人部件和患者的膝关节以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

锁紧机构或终端限位上的总载荷可以用与支承系统或驱动系统的其他部分相同的方式进行确定。然而制造商应该注意符合通用标准中表 21 的拉伸安全系数并不总是意味着通过了过冲终端限位试验。在通用标准 9.2.3.2 规定的过冲终端限位试验中,终端限位在正常使用和合理预见的误用下,均需要承受住达到终端限位的冲击力。

示例 5: 用于膝关节的柔性人工肌肉式 RACA 机器人

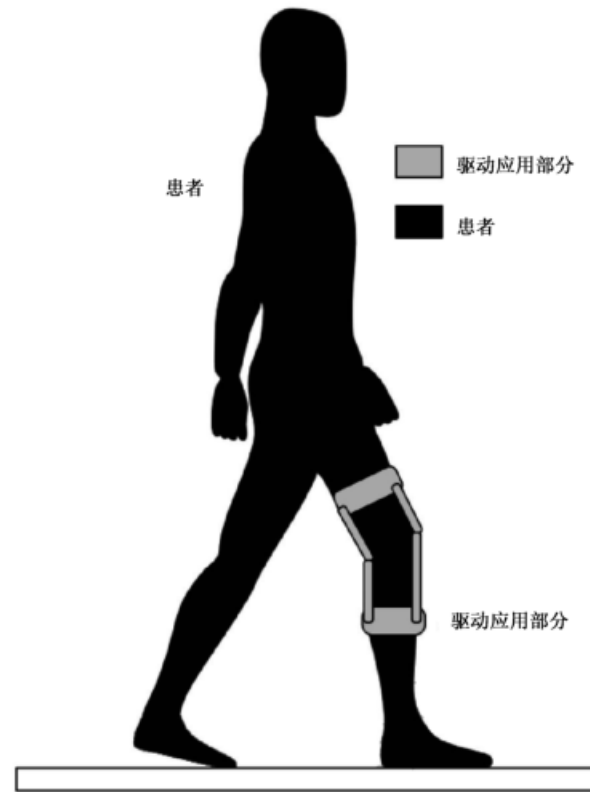


图 AA.17 用于膝关节的柔性人工肌肉式 RACA 机器人示例

将人工肌肉放置在膝盖周围,起着屈肌和伸肌的作用。在本例中,柔性人工肌肉接触患者的躯体来传递它们的输出力。因此,它们既是驱动应用部分,又是驱动系统。

制造商可识别驱动应用部分(以及驱动系统)的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢部分的重量、所识别部件支承的驱动应用部分的重量,以及患者膝关节对所识别部件的最大输出力,来确定所识别部件的总载荷。

确定总载荷需要包含惯性力,因为 RACA 机器人部件和患者的膝关节以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。由于延伸率的原因,可以采用与通用标准中表 21 第 1 行相同的结构完整性等级。通用标准 9.8.2 的附件 A 给出了通用标准中表 21 第 1 行适用于非金属材料延伸率的原因说明。

示例 6: 用于下肢的外骨骼式步行 RACA 机器人

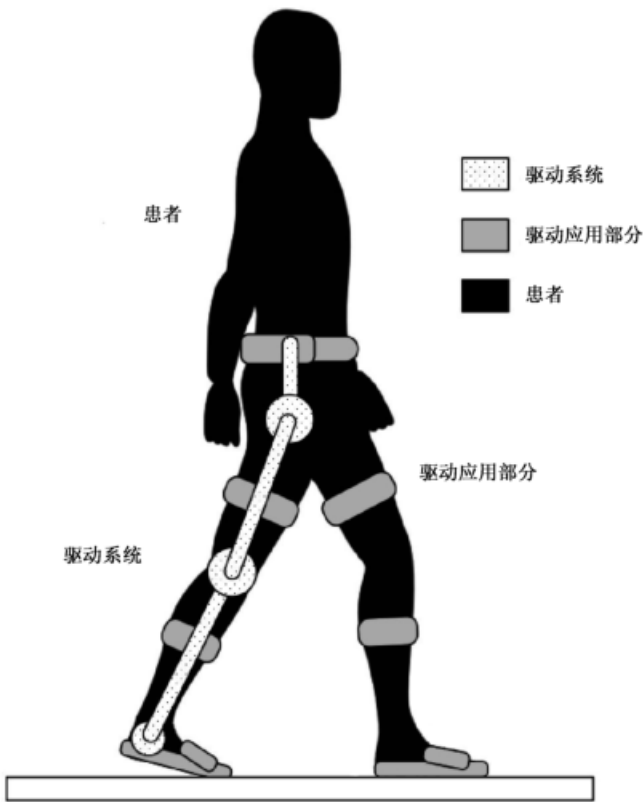


图 AA.18 外骨骼式步行 RACA 机器人示例

制造商可识别驱动应用部分的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢部分的重量、所识别部件支承的驱动应用部分的重量,以及患者下肢对所识别部件的最大输出力,来确定所识别部件的总载荷。

制造商可识别驱动系统的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者下肢部分的重量、所识别部件支承的驱动系统部分的重量包括驱动应用部分的总重量,以及患者下肢的最大输出力,来确定所识别部件的总载荷。

确定总载荷需要包含惯性力,因为 RACA 机器人部件和患者下肢以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

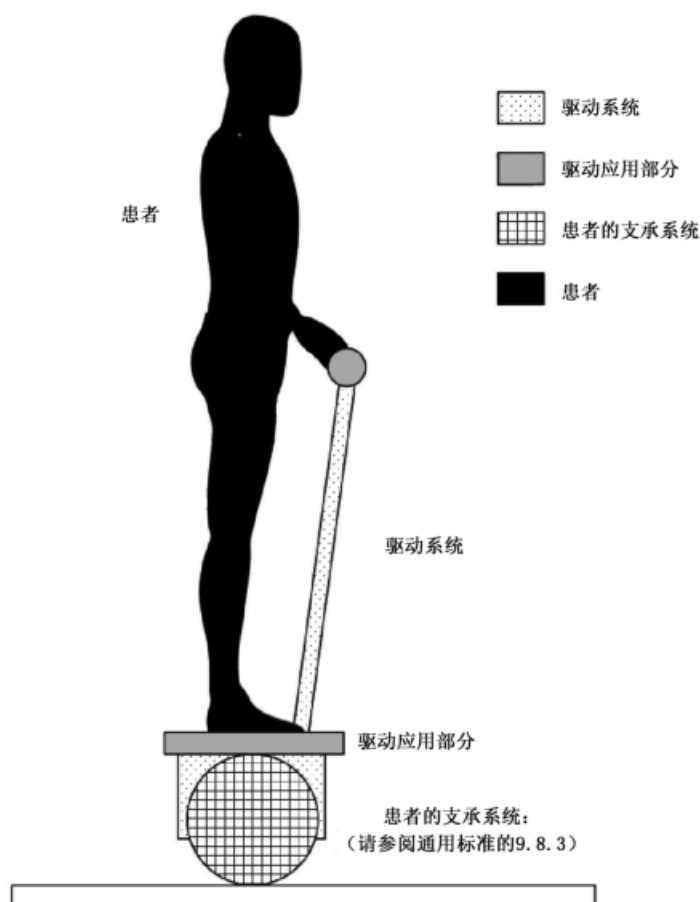
锁紧机构或终端限位上的总载荷可以用与支承系统或驱动系统的其他部分相同的方式进行确定。然而制造商应该注意符合通用标准中表 21 的拉伸安全系数并不总是意味着通过了过冲终端限位试验。在通用标准 9.2.3.2 规定的过冲终端限位试验中,终端限位在正常使用和合理预见的误用下,均需要承受住达到终端限位的冲击力。

注 1: 在类似本例的共享控制系统中,用于保持患者和 RACA 机器人的稳定性和避免跌倒的技术尚未开发出来。为保持稳定,通常可以使用额外的设备,如拐杖、助行器、扶手和/或高架的体重支承系统。此外,通常还需要操作者(治疗师)的帮助来保持稳定性。如果需要额外的设备,制造商可以确定驱动系统的机械故障风险是否不可接受。考虑由于机械故障而导致动力缺失或退化后的情况,这也有助于风险评估。这个高架的体重支承系统可以包含一个悬挂系统。

注 2: 一部分患者的体重可以向下施加到驱动应用部分上,这会增加驱动系统底部的总载荷。在本例中,增加的负载在正常使用中可能很小,因为驱动应用部分上的载荷是取决于患者与 RACA 机器人之间的异位程度所致,在安装过程和操作过程中自然会减少这种情况。最后,制造商可以考虑将载荷包含于拉伸安全系数中。

注 3：如果在正常使用下的行走过程中打算使驱动系统的底部直接接触地面，则制造商可考虑在底部上的总载荷，就是地面反作用力的峰值。根据参考文献[12]，即使当下楼梯时，人体的步态对地面反作用力的峰值可高达体重的 1.5 倍。因此，制造商可以根据其预期用途，将 RACA 机器人重量的 1.5 倍或更少施加在底部的总载荷上。如果患者的脚部会踩在底部，则需要考虑患者的体重。

示例 7：用于垂直平衡控制的 RACA 机器人



可能需要添加机械保护装置以确保基本安全。

图 AA.19 用于平衡控制的 RACA 机器人示例

垂直平衡控制是运动功能的一部分。通过支撑台和把手(驱动应用部分,如图 AA.19 所示)所提供的支承力进行主动控制,以使患者保持直立姿态。因此,驱动应用部分提供能够主动控制与患者运动功能相关的物理交互,这与 201.3.209 中定义的术语一致。

制造商可识别驱动应用部分或驱动系统的部件,其故障可能导致不可接受的风险。制造商可以根据患者的重量、所识别部件支承的部分 RACA 机器人的重量,以及由于 RACA 机器人的运动而产生的最大动态负载,来确定所识别部件的总载荷。

在本例中,患者的支承系统(即图 AA.19 中的电机轴、轮轴、轮胎、支撑台和把手)是 RACA 机器人的一部分,它由患者的整个体重静态和动态地加载;因此,通用标准 9.8.3 的特定要求适用于支承系统。这归因于机械故障可能构成一种不可接受的风险。

确定总载荷需要包含惯性力,因为 RACA 机器人以不可忽视的速度进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

注 4：如果需要额外的设备,例如,高架的体重支承系统以避免跌落,制造商可以确定驱动系统发生机械故障的风

险是否可以接受。考虑由于机械故障而导致的驱动系统缺失或退化后的情况,这也有助于风险评估。这个高架的体重支承系统可以包含一个悬挂系统。

注 5: RACA 机器人的重量和/或患者的重量可以根据它们/他们的质量和正常使用中的身体倾斜度来估算。

注 6: 制造商可考虑,当由一个或多个轴承支承时,电机轴不会因磨损而损坏。

示例 8: 具有步态跟随功能的体重支承式 RACA 机器人。

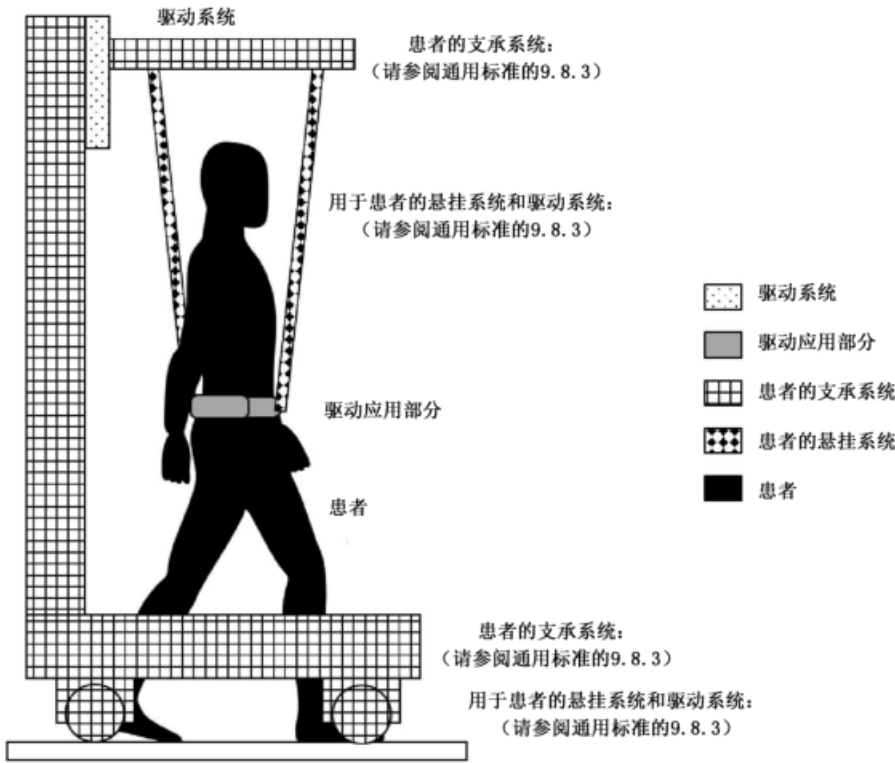


图 AA.20 具有步态跟随功能的体重支承式 RACA 机器人示例

腿部的支承功能作为步行的子功能也是一种运动功能。通过悬吊带(如图 AA.20 所示,驱动应用部分)所提供的支承力进行主动控制,以实现患者行走(在行走过程中使患者保持直立),并且不会干扰其步态。因此,驱动应用部分提供能够主动控制与患者运动功能相关的物理交互,这与 201.3.209 中定义的术语一致。

制造商可识别驱动应用部分的部件,这些部件的失效可能会导致不可接受的风险。制造商可以根据患者的总重量、预期被设备支承的患者重量的部分,以及所识别部件支承的驱动应用部分的重量,来确定所识别部件的总载荷。

制造商可识别支承系统、悬挂系统或驱动系统的部件,它们的故障可能导致不可接受的风险。制造商可以根据患者的重量(或该重量的一部分)、驱动系统部分的重量包括驱动应用部分的总重量、所识别部件支承的驱动系统部分的重量,以及所识别部件支承的悬挂系统部分的重量,来确定所识别部件的总载荷。

在本例中,用于患者的支承系统和悬挂系统是 RACA 机器人的一部分,并通过患者的整个体重静态和动态地加载;因此,通用标准 9.8.3 中的特定要求适用于支承系统。这归因于机械故障可能构成一种不可接受的风险。

确定总载荷需要包含惯性力,因为 RACA 机器人部件或患者以不可忽略的速度总载荷进行运动。

根据给定的总载荷信息,制造商应能够更准确地计算出外力。如果材料拉伸强度和所有预期外力可量化,并且精确已知,则通用标准中表 21 的 A 类适用。否则,表 21 的 B 类适用。

锁紧机构或终端限位上的总载荷可以用与支承系统或驱动系统的其他部分相同的方式进行确定。然而制造商应该注意符合通用标准中表 21 的拉伸安全系数并不总是意味着通过了过冲终端限位试验。在通用标准 9.2.3.2 规定的过冲终端限位试验中,终端限位在正常使用和合理预见的误用下,均需要承受住达到终端限位的冲击力。

条款 201.15.3.1 概述

通用标准(及其指南)15.3.1 的机械试验仍适用于经修改的定义穿戴的。在本文件中,穿戴的是可携带的(而不是在通用标准中定义的可转移的一种有向子集)的一种有向子集。尽管可携带的和可穿戴的设备的坠落试验不同,但与可携带的(15.3.4.2)相比,可穿戴的设备坠落试验的条件(15.3.4.1)更为严格。因此,对于可穿戴的 RACA 机器人,仅应进行可穿戴式坠落试验(15.3.4.1)。对于步行式 RACA 机器人,粗鲁搬运试验是不合适的,因为它是针对轮式可转移的设备而定义的。对于轮式移动的 RACA 机器人(因此,非步行式),粗鲁搬运测试适用。例如,用于配合步行式 RACA 机器人的轮式移动框架/机身应满足粗鲁搬运试验的要求。

条款 202.4.3 通用测试条件

增补的内容与 YY 9706.102—2021 中 4.2 一致。众所周知,EMC 环境下单一故障状态的试验是不可实现的。但是,IEC 60601-1-2:2014 中并未明确排除单一故障情况下的 EMC 试验。

某些单一故障状态将对 ME 设备或 ME 系统的 EMC 性能产生重大不利影响。一些 EMC 技术将干扰导向到大地或散布在电路组件中。如果在 EMC 试验期间中断了保护性接地导体或模拟了电磁干扰滤波器中某个组件的故障,则很难满足此并列标准的 EMC 要求。因此,EMC 试验规定在正常条件下而非单一故障情况下进行。

如 YY 9706.102—2021 中规定为抗扰度试验电平 of 电磁骚扰被视为单一故障状态,根据 YY 9706.102—2021 中 4.2 的要求,可理解为对 ME 设备和 ME 系统无需进行抗扰度试验。由于它们被认为是使用环境的代表,因此本并列标准(以及参考本并列标准的专用标准)中规定的抗扰度试验电平在 4.2 的背景下不应被视为单一故障状态。单一故障状态可能会与导致危险的预期电磁骚扰相结合产生。或者,在某种用于防止可能导致危险的电磁干扰的方法中可能存在单一故障状态。在风险管理过程中应考虑这些危险(源)。

(请参阅 YY 9706.102—2021 中 4.2 的基本原理)。

第 208 章 ME 设备和 ME 系统中报警系统的通用要求、测试和指南

当 RACA 机器人配备有符合 YY 9706.108—2021 的报警系统时,制造商应特别重视态势感知,以确定操作者是否有能力意识到造成报警状态的危险情况,以及避免不可接受风险所需的适当反应。

第 210 章 生理闭环控制器开发的过程要求

并列标准 YY/T 9706.110—2021 在很多地方使用术语“心理模型”,例如,YY/T 9706.110—2021 的附录 A。操作者具有 ME 设备或 ME 系统的心智模型这一概念就是指态势感知。特别地,心智模型类似于态势感知的一部分,理解 ME 设备或 ME 系统的状态。

第 211 章 家庭护理环境中使用的 ME 设备和 ME 系统的要求

在考虑供非专业操作者使用的 RACA 机器人的态势感知时,应特别强调非专业操作者在感知、理解和预测 RACA 机器人动态行为能力方面的有限教育和经验。

附录 BB

(资料性)

态势感知的指南和示例

BB.1 概述

本附录提供了将态势感知的概念应用于 RACA 机器人设计的指南。首先,简要介绍了态势感知在其他行业的历史,以帮助制造商了解其重要性及其重要性发展。然后,后续章节提供了有关如何维持和评估态势感知的指南。最后,在 BB.5 中,提供了 RACA 机器人的示例,以说明如何应用态势感知的概念。

BB.2 态势感知的简要背景

随着动态系统的复杂性或自主程度的提高,态势感知在动态系统中变得越来越重要,这可能导致态势感知的缺失或不足。通过回顾系统设计历史和其他行业的事故,可以认识和理解态势感知的重要性。

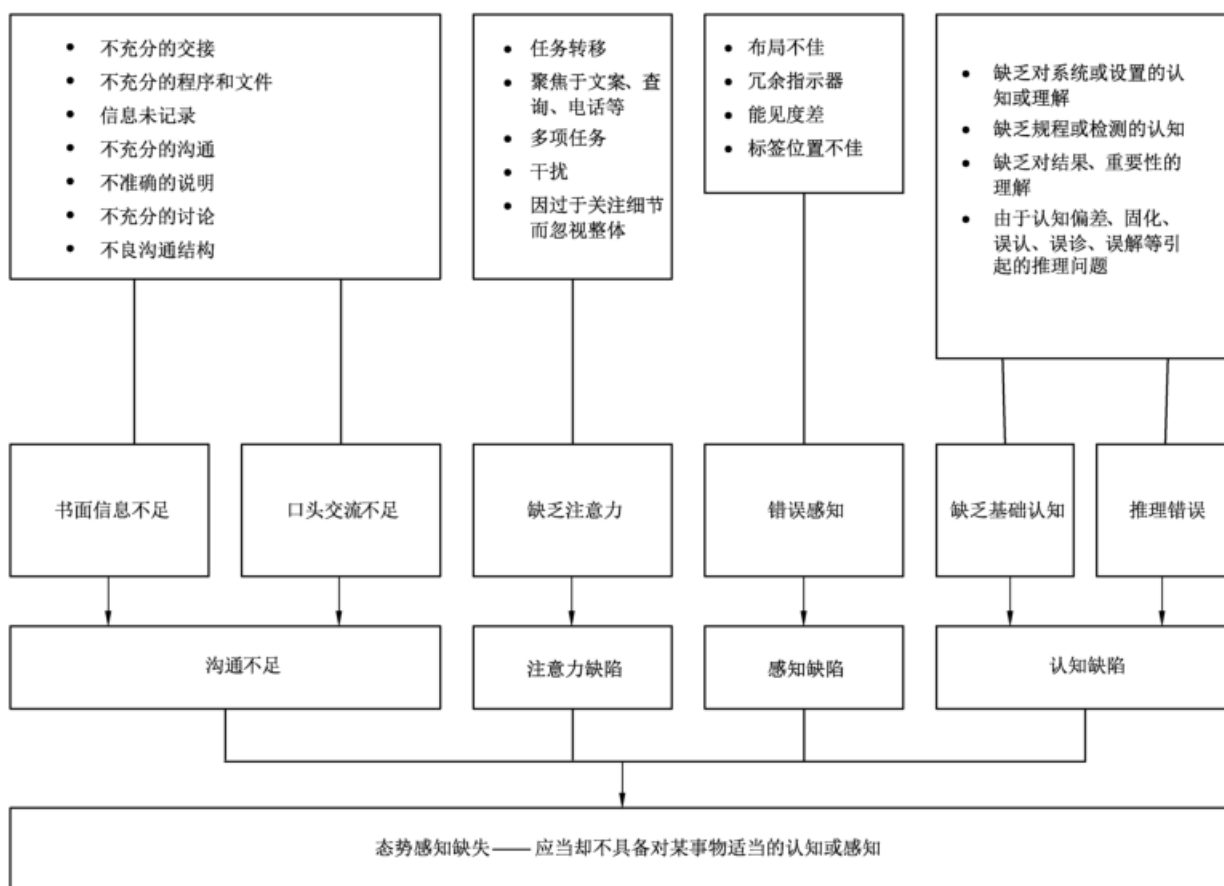
自 20 世纪 80 年代末以来,自动化和计算机化技术已在许多行业中逐渐普及,特别是航空业也参与到这次革命中。例如,需要飞行员按序操控显示器来调节大量仪表盘的(传统驾驶舱)已被大型计算机屏幕(玻璃驾驶舱)取代,以实现更高的飞行控制自主权。Endsley^[23]发现,超过 88% 的人为失误导致的航空事故均归因于态势感知问题。同样,另一项分析发现,在 200 多起飞机事故中,态势感知不佳是主要原因^[24]。过去几十年来,基于对态势感知重要性的认识,飞机驾驶舱的设计发生了重大变化。

在许多医学领域,态势感知也得到了注意和分析。热点之一就是紧急救护。医院的紧急救护令所有的医生、护士和技术人员都倍感压力。他们不仅面临着高度变化、复杂和不确定的患者状况,而且还有事关生死的斗争。影响医疗保健结果和患者安全的因素包括非技术性技能,例如:团队合作、领导才能、决策和态势感知,其中态势感知是影响决策和效果的核心因素。因此,与态势感知相关的问题以及在紧急救护环境中进行评估的方法已被提出至少十年了,例如,Cooper 的综述文章^[25]。

1995 年,Gaba 等人将态势感知引入了麻醉领域^[26]。后来,态势感知被确定为麻醉师非技术性技能(ANTS)分类和行为评级工具中的四个主要非技术性技能之一,并且对于其他三个主要非技术性技能,决策、团队合作和任务管理而言,它被认为是极其重要的^[27]。2009 年,在一项前瞻性多中心研究中,海恩斯(Haynes)用手术安全性检查表锻炼手术组的态势感知。该病例表现为围术期并发症减少、手术部位感染减少、无计划返回手术室的人数减少及死亡率降低^[28],态势感知已经被认为是决策的关键组成部分,使其对医疗护理的效果有直接影响^[28]。

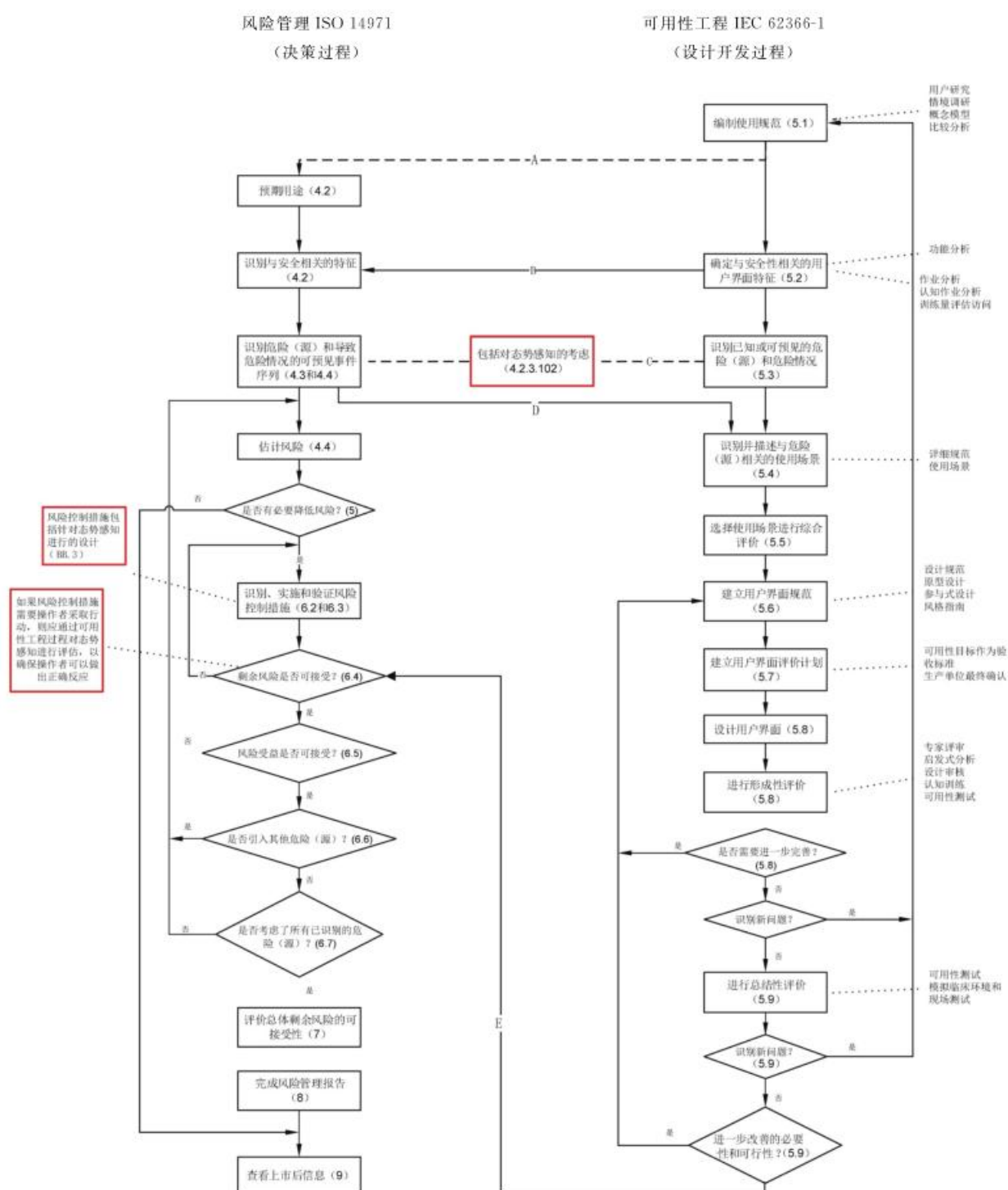
上述在航空、紧急救护和麻醉领域的例子说明了各个行业对态势感知重要性的广泛认可。上述各行业和许多其他行业已意识到,未能解决态势感知问题会导致致命的后果。因此,这些行业已经直接在系统或产品的设计阶段以及之后的验证过程中采取措施考虑态势感知问题。

自动化和计算机化技术已被用于减少复杂动态系统中的操作者的工作量,该系统负责子系统并实现目标。具有自主程度的复杂动态系统通常被设计成通过自动控制循环对细节操作进行处理,并通过计算机程序进行决策。当使用具有自主程度的复杂动态系统时,根据系统提供的信息操作者将成为对系统进行监督的管理人员。然而,复杂动态系统的某些故障或意想不到的差异可能会导致在使用时发生危险情况。如果未适当维持态势感知,则操作者可能会在动态情况下忽略或延迟其响应,从而不可避免地出现危险情况。因此,在产品阶段,应考虑所有可能导致态势感知缺失的情况。图 BB.1 很好地说明了符合考虑态势感知缺失这一要求的示例^[29]。此处,近因指最接近或直接造成态势感知缺失的原因。

图 BB.1 态势感知丧失的所有近因^[29]

态势感知与现有过程的关系如图 BB.2 所示,该图是由 IEC 62366-1:2015 的图 A.4 修改而来的。该图有三处更改(见红色文本框),它们说明了两种常见情况,在这些情况下态势感知会对现有过程造成影响。

- 第一种情况讲述了最初被识别为用户界面规范(IEC 62366-1:2015 的 5.2)中一部分的危险(源)或危险情况。目前,可用性和风险之间的联系包括对态势感知的特殊考虑(201.4.2.3.102)以及注释(YY/T 0316—2016 的 6.2 和 6.3),两者见图 BB.2 中的红色文本框,以提醒制造商风险控制应为态势感知而设计。
- 第二种情况讲述了风险控制,这种风险控制在初步使用规范和确定与安全有关的用户界面特征(IEC 62366-1:2015 的 5.1 和 5.2)之后识别和实施的,以解决作为风险管理过程(YY/T 0316—2016 的 6.2 和 6.3)的一部分而识别的危险(源)和危险情况。根据 YY/T 0316—2016 中 6.4 的新注释(见图 BB.2 中的红色文本框),制造商需要认识到,如果这些新的风险控制措施需要态势感知,则制造商需要重新返回到可用性工程,以确保操作者具有足够的态势感知,以使风险控制有效。



由 IEC 62366-1:2015 图 A.4 修改而得。

图 BB.2 态势感知、风险管理过程(YY/T 0316—2016)和可用性工程过程(IEC 62366-1:2015)之间的关系

BB.3 针对态势感知设计 RACA 机器人

RACA 机器人是具有一定程度自主性的复杂动态系统。若因态势感知的缺失或不足导致无法接受的风险, 则通过“可用性工程过程”和“风险管理过程”降低风险的选项如下:

- a) 设计具有各种听觉/视觉/触觉信号(例如:警报/指示器/显示器)的 RACA 机器人,并按系统级顺序和持续时间进行排列,以减少注意力和感知缺陷。
- b) 基于清晰明确的逻辑设计 RACA 机器人,以便任何受过训练的操作者都可以判断 RACA 机器人按其模式运行的原理,以及 RACA 机器人将如何运行以减少认知缺陷。
- c) 设置足够的标准操作规程(SOP)、操作者信息以及(如有必要)培训计划(包括验证),以便受过培训的操作者可以通过与 RACA 机器人、其他用户和环境进行充分的沟通来操作 RACA 机器人。

可通过核查可用性工程文件和风险管理文档来检验是否符合要求。

BB.4 评估操作者的态势感知

BB.4.1 概述

为了评估执行 BB.3 中给出的设计原则的有效性,需要在可用性工程过程中评估 RACA 机器人操作者的态势感知。通常,RACA 机器人操作者可以是医生、治疗师或患者。由于这些不同类型的操作者可能具有不同的培训、教育经历或能力,所以他们可能具有不同的与态势感知相关的要素和度量。同时建议,如附录 AA 和图 AA.2 中所述,应对态势感知的所有三个级别:感知、理解和预测进行考虑。这三个级别应同时反映在与态势感知相关的要素和度量的内容中。

整个评估可能包括态势感知要素分析和使用 IEC TR 62366-2:2016 中所述技术的一种或多种实际测量方式(请参见 IEC TR 62366-2:2016 中表 E.1)。这些技术应包括对态势感知的预测水平的考虑。针对于其他领域中可能适用于 RACA 机器人的技术,在参考文献[30]中进行了描述,并在参考文献[31]中进行了回顾。

BB.4.2 态势感知要素分析

RACA 机器人制造商可以使用与参考文献[32]中描述的方法类似的要素分析对态势感知进行评估。要素分析的目的在于,在考虑 RACA 机器人的基本安全和基本性能时,找到使用 RACA 机器人所需的三个级别的态势感知要素,与危险(源)或危险情况相对应。建议使用“态势感知”要素分析至少涵盖非结构化访问和目标导向的任务分析(GDTA)程序^[33]。这些非结构化访问与 IEC 62366-1:2015 的 5.2 和 5.4 的要求有关。要素分析的结果应构成可用性工程文件的一部分。

对于非结构化访问,建议制造商的专家采访一些医生和治疗师,以收集态势感知的所有可能要素。每次访问都可以先简要介绍预开发的 RACA 机器人的基本安全和基本性能以及态势感知的概念。然后,应要求受访者描述为使用此类 RACA 机器人而构建“足够的态势感知”所必需的要素。访问还应关注动态要素,并尽量不包括预先确定的医学知识或任何静态程序(例如,应谈论“在患者使用 RACA 机器人进行治疗之前,患者应注意哪些情况”,而不是谈论“应使用 RACA 机器人解决哪些类型的损伤”)。

如果可能,可以以头脑风暴的方式进行访问,建议询问有关态势感知所有三个级别的态势感知要素。访问后,所有收集到的可能的态势感知要素被归类为附录 AA 和图 AA.2 中所述的三级态势感知,并分配给应该具有这些要素的人员(例如:医生、治疗师或患者)。

为了构建“足够的态势感知”,访谈可以完全独立于 RACA 机器人采用的实际技术(即,器械原型是非必需的),并且受访者不必熟悉 RACA 机器人,可以鼓励他们谈论所需的态势感知,以对 RACA 机器人的类型进行普遍考虑。然而,由于设计是一个迭代过程;也可以在后期阶段使用原型进行非结构化访问。

为了确保由非结构化访问确定的上述态势感知要素完整且与 RACA 机器人的态势感知要素相关,建议制造商的专家进行目标导向的任务分析(GDTA)(请参见图 BB.3)。目标导向的任务分析使用四

- 层方法：
- a) 确定主要目标；
 - b) 确定实现其主要目标所必需的子目标；
 - c) 确定为达到子目标而需要采取的操作者行动，这个子目标是基于根据足够的态势感知所支持的决策而确定的，以及
 - d) 识别生成成功决策和行动所必需的态势感知要素，如图 BB.2 所示。

对于 RACA 机器人，主要目标 1.0(见图 BB.3)可以设置为“将与态势感知相关的风险降低到可接受的水平”。可以将 1.X 子目标设置为由制造商确定的每种危险(源)或危险情况，其中操作者应对作业进行监控或与 RACA 机器人进行交互(即采取行动)，以将风险降低到可接受水平(见 201.4.2.3.102 中的增补内容)。根据收集到的可能的态势感知要素，可能需要对特定子目标进行现场测试，以便分配或识别哪些要素对应所需态势感知的哪个级别。不同类型的操作者，例如：康复医生、治疗师和患者，可能会产生不同的目标导向的任务分析结果。

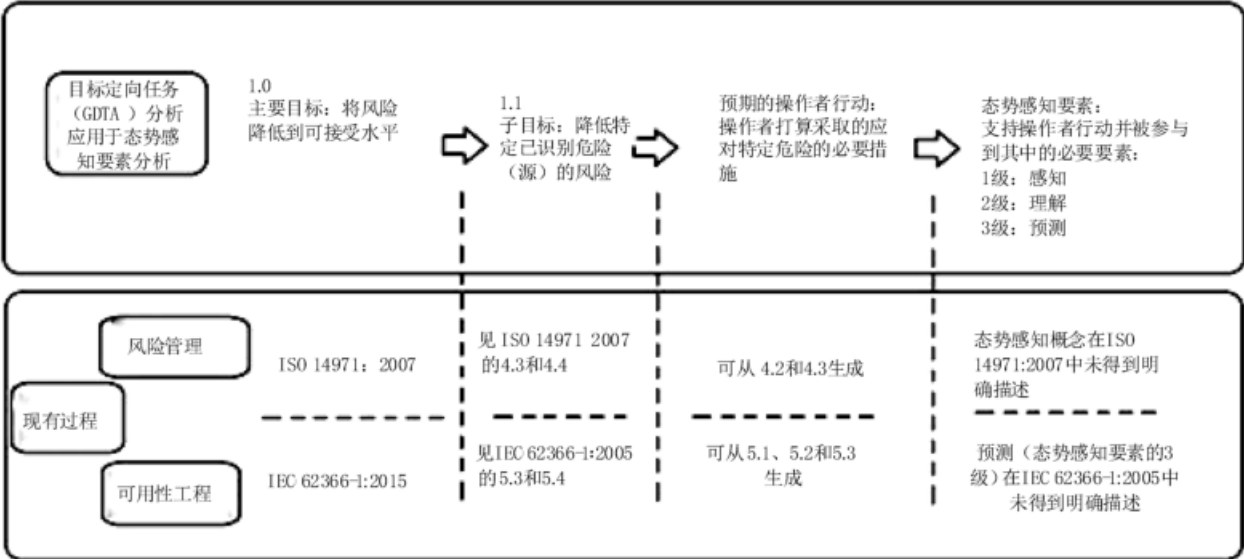


图 BB.3 目标导向的任务分析与风险管理和可用性工程过程之间的关系

态势感知要素的结果可以用作检查点，以验证是否已按照 BB.3 中给出的设计原则来设计和制造 RACA 机器人，或者如果它们与用户界面相关，则可以集成到用户界面规范(IEC 62366-1:2015 的 5.6)中，并用于 IEC 62366-1:2015 所定义的用户界面的形成性评价(IEC 62366-1:2015 的 5.8)。

BB.5 将态势感知概念应用于 RACA 机器人的示例

BB.5.1 概述

此处提供了有关 RACA 机器人的 4 个示例，以说明如何将态势感知的概念应用于识别与 201.4.2.3.102 中要求的相关危险(源)或危险情况。

除风险管理过程和可用性工程过程(如图 BB.2 所示)外，可以通过执行非结构化访问和目标导向的任务分析(GDTA)来确定态势感知要素(如图 BB.3 所示)。将与 RACA 机器人制造商和操作者(例如：医生、治疗师或患者)进行的非结构化访问用于确定危险(源)或危险情况，并查找相关态势感知要素。目标导向的任务分析被用于识别和对已识别的危险(源)或危险情况分类，并将相应的态势感知要素分为三个级别(感知、理解和预测)。

BB.5.2 用于患者户外移动辅助的 RACA 机器人的设计过程(家庭护理环境)

注 1: 在本例中,误用会造成危险情况。

此 RACA 机器人示例旨在为家庭护理环境中的室外患者(例如:步行的或坐轮椅的)提供移动辅助。本例说明了在评估和处理态势感知时需要同时考虑第三级别(预测)和环境。本例类似于驾驶汽车,需要避免因汽油耗尽而陷入困境。在本例中,仅考虑单个子目标。

对于本例中的每个步骤,都引用了 YY/T 0316—2016 和 IEC 62366-1:2015 中各自最相关的条款,以帮助使本示例中的这些过程和图 BB.2 中所示的流程图保持一致。

- a) 识别危险情况(YY/T 0316—2016 的 4.3 和 4.4)。
 - 如果 RACA 机器人电量耗尽,患者可能会被困,导致相关伤害。
- b) 估算风险并确定是否有必要降低风险(YY/T 0316—2016 的 4.4 和第 5 章)。
 - 是,有必要降低风险。
- c) 识别风险控制(YY/T 0316—2016 的 6.2)。
 - 操作者:首先进行规划,然后再进行户外远足,确保可以在电池电量耗尽之前完成此项活动。
- d) 描述使用场景,并确定是否需要进一步考虑态势感知。
 - 在此使用场景下,操作者行动被视为一项“作业”。若风险控制需要操作者参与,那么制造商需要了解:操作者是否能根据他们所掌握的信息,做出预期反应进行风险控制?针对此问题,需要分析操作者的态势感知能力(见图 BB.2 中红色的新注释,与 YY/T 0316—2016 的 6.4 相邻)。
 - 由于本例中的风险控制需要操作者参与,因此在可用性工程过程中,制造商有必要考虑操作者是否有足够的态势感知。
 - 本例是危险相关使用场景。
- e) 识别在上述使用场景中态势感知缺失后可能发生的危险(源)或危险情况,例如,如表 BB.1 所示,使用目标导向的任务分析(以满足 201.4.2.3.102 的要求)。

表 BB.1 在 BB.5.2 中使用目标导向的任务分析的示例

主要目标	子目标		预期操作者行动	态势感知要素
	已识别的危险情况	降低风险的方法		
1.0 将与态势感知相关的风险降低到可接受水平	1.1 患者可能会被困,导致相关伤害(例如:在寒冷的天气中)	避免陷入电池电量耗尽、患者被困的情况	患者: 首先进行规划,然后再进行户外远足,确保可以在电池电量耗尽之前完成此项活动	患者: 1 级(感知):观察电池的初始容量(即开始远足之前)和预期的工作环境(例如:地形、温度、与充电器的接近程度)。 2 级(理解):了解电量耗尽后,机器人将停止运动。了解不同的使用方式可能会以不同的速率消耗电池电量。了解不同的环境会改变功耗(例如:温度和地形梯度)。 3 级(预测):根据预期的使用情况预测 RACA 机器人的电池电量将何时耗尽,并确定策略以最大程度地减少因电池电量消耗而导致被困的风险

注 2: IEC 60601-1:2005 和 IEC 60601-1:2005/AMD1:2012 的 11.8 解决了断电问题,但旨在处理断电造成的直接后果(例如:RACA 机器人坠落)。

f) 实施风险控制措施/详细说明、设计和使用用户界面(YY/T 0316—2016 的 6.2 和 IEC 62366-1:2015 的 5.6~5.8)。

- 用户界面特征:

- 根据电池容量,还可根据使用模式、温度,向患者指示“剩余距离”估计值;

- 在使用说明中涵盖基于不同使用模式下的行动距离或范围估计,以帮助操作者/患者了解不同条件(例如:环境温度和地形梯度)下的电池使用情况。

g) 遵循风险管理过程和可用性工程过程的后续步骤。

BB.5.3 由单个操作者(治疗师)同时使用的多个 RACA 机器人的设计过程

注:在本例中,出现任何相关错误使用的前提是存在危险情况。

本例基于计划在临床环境中使用的 RACA 机器人,单个操作者(治疗师)同时使用多个 RACA 机器人对多位患者进行监护(即每位患者都有自己的 RACA 机器人,并假设每个 RACA 机器人的型号相同)。在这种情况下,操作者对每位患者进行间断监护或无监护。可在风险管理过程或可用性工程过程中识别危险(源)或危险情况。本例说明了紧急停止装置对态势感知的要求,而在某些情况下,可能无法保证足够的态势感知。在本例中,针对目标导向的任务分析,仅对单个子目标进行了考虑(尽管通常可能有多个子目标)。

对于本例中的每个步骤,都引用了 YY/T 0316—2016 和 IEC 62366-1:2015 中各个最相关的条款,以帮助使本示例中的这些过程和图 BB.2 中所示的流程图保持一致。

a) 识别危险情况(YY/T 0316—2016 的 4.3 和 4.4)。

- RACA 机器人可能会使患者关节的伸展或屈曲的距离过远或频率过快。

b) 估算风险并确定是否有必要降低风险(YY/T 0316—2016 的 4.4 和第 5 章)。

- 是,有必要降低风险。

c) 识别风险控制(YY/T 0316—2016 的 6.2)。

- 治疗师:停止发生故障的 RACA 机器人的运动(例如:紧急停止)。

d) 描述使用场景,并确定是否需要进一步考虑态势感知。

- 在此使用场景下,操作者行动被视为一项“作业”。若风险控制需要操作者参与,那么制造商需要了解:操作者是否能根据他们所掌握的信息,做出预期反应进行风险控制?针对此问题,需要分析操作者的态势感知能力(见图 BB.2 中红色的新注释,与 YY/T 0316—2016 的 6.4 相邻)。

- 由于本例中的风险控制需要操作者参与,因此在可用性工程过程中,制造商有必要考虑操作者是否有足够的态势感知。

e) 识别在上述使用场景中态势感知缺失后可能发生的危险(源)或危险情况,例如,如表 BB.2 所示,使用目标导向的任务分析(以满足 201.4.2.3.102 的要求)。

表 BB.2 在 BB.5.3 中使用目标导向的任务分析的示例

主要目标	子目标		预期操作者行动	态势感知要素
	被识别的危险情况	降低风险的方法		
1.0 将与态势感知相关的风险降低到可接受水平	1.1 RACA 机器人可能会使患者关节的伸展或屈曲的距离过远或频率过快	在 RACA 机器人出现意外行为的情况下维持安全	治疗师： 停止发生故障的 RACA 机器人的运动	治疗师： 1 级(感知)：同时监控多个 RACA 机器人。 2 级(理解)：了解 RACA 机器人何时开始以非预期的方式运动或运行。 3 级(预测)：能够预测运动/运行应是怎样的：如果检测到非预期的运动/运行，对情况的严重程度进行预测可使治疗师确定他们应做出怎样的迅速反应(例如：如果他们与患者所处房间不同)

f) 实施风险控制措施/详细说明、设计和使用用户界面(YY/T 0316—2016 的 6.2 和 IEC 62366-1:2015 的 5.6~5.8)。

- 用户界面特征：
 - 减少由错误感知引起错误使用的可能性(请参见 IEC 62366-1:2015 的图 D.1)。在用户界面设计中,对于操作者而言,告知危险情况的信号或指示应为可察觉和可区分的；
 - 减少由错误认知(理解)引起错误使用的可能性(请参见 IEC 62366-1:2015 的图 D.1)，随附文件应以操作者可以理解的方式对危险情况进行充分说明；
 - 减少由错误预测引起错误使用的可能性,随附文件应对 RACA 机器人进行充分说明，以便操作者可以预测危险情况的演变。
- 添加紧急停止装置。
- 更新用户界面规范,然后设计并使用用户界面。

g) 遵循风险管理过程和可用性工程过程的后续步骤。

BB.5.4 由治疗师指导的用于康复治疗 RACA 机器人的设计过程

注：在本例中,态势感知问题集中在患者身上,而非 ME 设备的硬件上。

在本例中,操作者包括患者和训练有素的治疗师,他们对患者如何使用 RACA 机器人的临床功能进行监护。在风险管理过程中考虑并识别与患者状况相关的危险(源)或危险情况。

本例说明了制造商如何通过使用标准操作规程(SOP)、使用说明和/或培训计划与治疗师的态势感知水平综合,从而降低风险。在本例中,针对目标导向的任务分析,仅对单个子目标进行了考虑(尽管通常可能有多个子目标)。

对于本例中的每个步骤,都引用了 YY/T 0316—2016 中各个最相关的条款,以帮助使本例中的这些过程和图 BB.2 中所示的流程图保持一致。

- a) 识别危险情况(YY/T 0316—2016 的 4.3 和 4.4)。
 - 当患者处于不适合继续进行康复治疗的状态时,可能会受伤。
- b) 估算风险并确定是否有必要进行风险控制(YY/T 0316—2016 的 4.4 和第 5 章)。
 - 是,有必要进行风险控制。

- c) 识别风险控制措施(YY/T 0316—2016 的 6.2)。
- 治疗师:按一下急停按钮,停止 RACA 机器人,必要时进行急救,然后将患者从 RACA 机器人中释放出来。
- d) 如果风险控制需要治疗师的参与,那么制造商需要了解:治疗师是否能够根据他们所掌握的信息,做出预期的反应进行风险控制? 针对此问题,需要分析治疗师的态势感知能力(见图 BB.2 中红色的新注释,与 YY/T 0316—2016 的 6.4 相邻)。
- 由于治疗师正在参与风险控制,因此制造商有必要对态势感知进行考虑。
- e) 描述使用场景,并确定是否需要进一步考虑态势感知。
- 在此使用场景下,治疗师行动被视为一项“作业”。若风险控制需要治疗师参与,那么制造商需要了解:治疗师是否能根据他们所掌握的信息,做出预期反应进行风险控制? 针对此问题,需要分析治疗师的态势感知能力(见图 BB.2 中红色的新注释,与 YY/T 0316—2016 的 6.4 相邻)。
- 由于本例中的治疗师正在参与风险控制,因此在可用性工程过程中,制造商有必要考虑治疗师是否有足够的态势感知。
- 本例是危险相关使用场景。尽管 IEC 62366-1:2015 的 5.5 说明,通常所有与危险有关的使用场景都应使用总结性评价来进行评价,由于评价态势感知的主观本质,应认为对这种与风险相关的使用场景进行形成性评估是足够的。
- f) 识别态势感知缺失后可能发生的危险(源)或危险情况,例如:表 BB.3 所示,使用目标导向的任务分析(以满足 201.4.2.3.102 的要求)。

表 BB.3 在 BB.5.4 中使用目标导向的任务分析的示例

主要目标	子目标		预期操作者行动	态势感知要素
	已识别的危险情况	降低风险的方法		
1.0 将与态势感知相关的风险降低到可接受水平	1.1 当患者处于不适合继续进行康复治疗的状态时,可能会受伤	防止患者在状况不佳的情况下受到伤害	治疗师: 停止 RACA 机器人,必要时进行急救,然后将患者从 RACA 机器人中释放出来	治疗师: 1 级(感知):注意患者面色异常、颤抖或说话困难的情况。 2 级(理解):了解患者状况不佳。 3 级(预测):如血压下降,患者可能会晕倒,或患者肌张力过高,其可能会伤害自己

- g) 实施风险控制措施(YY/T 0316—2016 的 6.2)。
- 建立足够的标准操作规程(SOP),来检查患者状况、调整康复机器人的参数、为治疗师提供使用说明书或培训项目:
 - 降低由感知引起的风险,对操作者进行培训,以检查患者的状况;
 - 降低由理解引起的风险,对操作者进行培训,以确定患者的不适状况;
 - 降低由预测引起的风险,对操作者进行培训,以预测患者的近期的状况。
- h) 遵循风险管理过程和可用性工程过程的后续步骤。

BB.5.5 利用拐杖支撑的下肢外骨骼的设计过程

注:本例中,在单一故障情况(SFC)下的操作者行动,说明了考虑态势感知有助于降低风险。

如图 BB.4 所示,用于康复治疗的下肢外骨骼是一种步行式 RACA 机器人,旨在通过特定程序(如站立、行走或坐下)对损伤患者进行训练。拐杖是患者的主要支撑系统。操作者由患者和训练有素的负

责监控康复治疗进行的治疗师担任。步行式 RACA 机器人的所有运动均由治疗师通过 RACA 机器人上的按钮触发,或由患者通过安装在拐杖中的遥控器触发。



图 BB.4 RACA 外骨骼步行机器人

以外骨骼式 RACA 机器人的常见单一故障情况(电机过热)为例。在 RACA 机器人切断其电机电源以进行自我保护之后,可能会出现危险情况,可在风险管理过程或可用性工程过程中进行确定。例如:可以引入警告信号,指示由于电机过热而即将断电,作为一项额外的风险控制措施,要求操作者安全停止 RACA 机器人的运行。

本例中,针对目标导向的任务分析,仅对单个子目标进行了考虑(尽管通常可能有多个子目标)。本例说明了在单一故障情况后,需要操作者应具有的姿态感知。

对于本例中的每个步骤,都引用了 YY/T 0316—2016 和 IEC 62366-1:2015 中各个最相关的条款,以帮助使本示例与这些过程和图 BB.2 中所示的流程图保持一致。

- a) 识别危险情况(YY/T 0316—2016 的 4.3 和 4.4)。
 - 由于电机过热,RACA 机器人可能会突然停止运行,患者可能失去平衡并跌倒,即处于危险状况。
- b) 估算风险并确定是否有必要降低风险(YY/T 0316—2016 的 4.4 和第 5 章)。
 - 是,有必要降低风险。
- c) 识别风险控制(YY/T 0316—2016 的 6.2)。
 - 患者:按任意键停止外骨骼的运动,站立、坐下或蹲下时使用拐杖保持平衡,然后寻求帮助。
 - 治疗师:请患者坐下休息,并帮助其保持稳定。
- d) 描述使用场景,并确定是否需要进一步考虑姿态感知。
 - 在此使用场景下,操作者行动被视为一项“作业”。若风险控制需要操作者参与,那么制造商需要了解:操作者是否能根据他们所掌握的信息,做出预期反应进行风险控制。针对此问题,需要分析操作者的姿态感知能力(见图 BB.2 中红色的新注释,与 YY/T 0316—2016 的 6.4 相邻)。
 - 由于本例中的风险控制需要操作者参与,因此在可用性工程过程中,制造商有必要考虑操作者是否有足够的姿态感知。
- e) 识别在上述使用场景中姿态感知缺失后可能发生的危险(源)或危险情况,例如:如表 BB.4 所示,使用目标导向的任务分析(以满足 201.4.2.3.102 的要求)。

表 BB.4 在 BB.5.5 中使用目标导向的任务分析的示例

主要目标	子目标		预期操作者行动	态势感知要素
	已识别的危险情况	降低风险的方法		
1.0 将与态势感知相关的风险降低到可接受水平	1.1 在检测到电机过热后,由于 RACA 机器人突然停止运行,患者可能会跌倒	当警告信号指示由于电机过热而即将断电时,请确保稳定性	患者: 按任意键停止 RACA 机器人,站立、坐下或蹲下时使用拐杖保持平衡,然后寻求帮助。 治疗师: 请患者坐下休息,帮助其保持稳定	操作者(患者和治疗师): 1级(感知):注意警告信号。 2级(理解):了解这意味着电机系统过热。 3级(预测):能够预测,如果操作者未采取适当的措施,RACA 机器人将切断其电机电源,并在近期(例如:30 s 后)突然停止运行。这可能会导致患者跌倒

- f) 实施风险控制措施/详细说明、设计和使用用户界面(YY/T 0316—2016 的 6.2 和 IEC 62366-1:2015 的 5.6~5.8)。
- 用户界面特征:
 - 减少由错误感知引起误用的可能性(请参见 IEC 62366-1:2015 的图 D.1);例如:在用户界面设计中,对于操作者而言,由于过热导致即将关闭的信号或指示应是可察觉和可区分的;
 - 减少由错误认知(理解)引起误用的可能性(请参见 IEC 62366-1:2015 的图 D.1),随附文件应以操作者可以理解的方式对电机断电的原因进行充分说明;
 - 减少由错误预测引起误用的可能性,随附文件应对 RACA 机器人进行充分说明,以便操作者可以预测电机断电的情况。
 - 更新用户界面规范,然后设计并使用用户界面。
- g) 遵循风险管理过程和可用性工程过程的后续步骤。

参 考 文 献

- [1] GB/T 30659—2014 假肢和矫形器 要求和试验方法
- [2] GB/T 36530 机器人和机器人设备 个人助理机器人的安全要求
- [3] YY 9706.233—2021 医用电气设备 第 2-33 部分:医疗诊断用磁共振设备的基本安全和本性能专用要求
- [4] ISO 7176 (all parts) Wheelchairs
- [5] ISO 8373:2012 Robots and robotic devices—Vocabulary
- [6] ISO 9999:2016 Assistive products for persons with disability—Classification and terminology
- [7] ISO 10535:2006 Hoists for the transfer of disabled persons—Requirements and test methods
- [8] ISO 10218-1:2011 Robots and robotic devices—Safety requirements for industrial robots—Part 1: Robots
- [9] ISO 11064-7:2006 Ergonomic design of control centres—Part 7: Principles for the evaluation of control centres
- [10] IEC 60601-1-9:2007 Medical electrical equipment—Part 1-9: General requirements for basic safety and essential performance—Collateral Standard: Requirements for environmentally conscious design IEC 60601-1-9:2007/AMD1:2013
- [11] IEC 61924-2:2012 Maritime navigation and radiocommunication equipment and systems—Integrated navigation systems—Part 2: Modular structure for INS—Operational and performance requirements, methods of testing and required test results
- [12] IEC 62366-1:2015 Medical devices—Part 1: Application of usability engineering to medical devices
- [13] IEC/TR 60601-4-1:2017 Medical electrical equipment—Part 4-1: Guidance and interpretation—Medical electrical equipment and medical electrical systems employing a degree of autonomy
- [14] IEC Guide 109:2012 Environmental aspects—Inclusion in electrotechnical product standards
- [15] IEC TR 62366-2:2016 Medical devices—Part 2: Guidance on the application of usability engineering to medical devices
- [16] International Classification of Functioning, Disability and Health—ICF, World health organisation, 2001 [viewed 2019-01-23].
- [17] Smith, K., Hancock, P.A., 1995. Situation awareness is adaptive, externally directed consciousness. *Hum. Factors* 37 (1), 137-148
- [18] Beringer, D. B., and Hancock, P. A. (1989). Exploring situational awareness: A review and the effects of stress on rectilinear normalisation. In *Proceedings of the Fifth International Symposium on Aviation Psychology* (Volume 2, pp. 646-651). Columbus: Ohio State University
- [19] Endsley, M., 1988. Design and evaluation for situational awareness enhancement. *Proceedings of the Human Factors Society 32nd Annual Meeting*. HFES, Santa Monica, p. 97-101
- [20] Endsley, M. R., 1995a. Toward a theory of situation awareness in dynamic-systems. *Hum. Factors* 37 (1), 32-64
- [21] Kaber, D.B., & Endsley, M.R. (2003). The effects of level of automation and adaptive

automation on human performance, situation awareness and workload in a dynamic control task. *Theoretical Issues in Ergonomic Science*, 3, 1-40

[22] J. Nilsson and A. Thorstensson, "Ground reaction forces at different speeds of human walking and running," *Acta Physiologica Scandinavica*, vol. 136, no. 2, p. 217-227, 1989

[23] Endsley, M. R. 1995b. A taxonomy of situation awareness errors. In R. Fuller, N. Johnston, & N. McDonald (Eds.), *Human Factors in Aviation Operations* (pp. 287-292). Aldershot, England: Avebury Aviation, Ashgate Publishing

[24] Hartel, C.E.J., Smith, K., Prince, C., 1991. Defining aircrew coordination. Sixth International Symposium on Aviation Psychology, Columbus, Ohio

[25] Cooper, S., J. Porter, L. Peach. 2014. Measuring situation awareness in emergency settings: a systematic review of tools and outcomes. *Open Access Emergency Medicine* 2014;6, 1-7

[26] Gaba DM, Howard SK, Small SD; Situation awareness in anesthesiology. *Hum Factors* 1995; 37;20-31

[27] Fletcher G, Flin R, McGeorge P, Glavin R, Maran N, Patey R (2003): Anaesthetists' Non-Technical Skills (ANTS): Evaluation of a behavioural marker system. *Br J Anaesth* 2003; 90: 580-8

[28] Schulz CM, Endsley MR, Kochs EF, Gelb AW, Wagner KJ.; Situation Awareness in Anesthesia Concept and Research 2013 Mar;118(3):729-42

[29] Patrick J., N. James, 2004. A task-oriented perspective of situation awareness. Ch 4 of *A cognitive approach to situation awareness: theory and application*, Ashgate, 2004

[30] Endsley, M. R. 1995c. Measurement of situation awareness in dynamic systems. *Hum Factors* 1995;37(1):65-84

[31] Salmon, P., Stanton, N.A., Walker, G., Green, D., 2006. Situation awareness measurement-A review of applicability for C4i environments. *Applied Ergonomics*, vol. 37, 2006, p. 225-238

[32] Endsley, M. R., 1993. A survey of situation awareness requirements in Air-to-Air Combat fighters. *The International Journal of Aviation Psychology*, Vol 3, p. 157-168

[33] Kirwan, B. and Ainsworth, L.K. (1992) *A guide to task analysis*. London: Taylor & Francis Ltd

[34] Haynes AB, Weiser TG, Berry WR, Lipsitz SR, Breizat AH, Dellinger EP, Herbosa T, Joseph S, Kibatala PL, Lapitan MC, Merry AF, Moorthy K, Reznick RK, Taylor B, Gawande AA; Safe Surgery Saves Lives Study Group; A surgical safety checklist to reduce morbidity and mortality in a global population. *N Engl J Med* 2009; 360:491-9

索 引

ME 设备	GB 9706.1—2020,3.63
ME 系统	GB 9706.1—2020,3.64
保护性停止	3.210
操作者	GB 9706.1—2020,3.73
代偿	3.205
电磁兼容性(EMC)	IEC 60601-1-2;2014,3.2
缓解	3.202
患者	GB 9706.1—2020,3.76
机械危险	GB 9706.1—2020,3.61
基本安全	GB 9706.1—2020,3.10
基本性能	GB 9706.1—2020,3.27
紧急停止	3.206
可编程医用电气系统(PEMS)	GB 9706.1—2020,3.90
可穿戴的	GB 9706.1—2020,3.144
移动的	GB 9706.1—2020,3.65
临床功能	3.204
型号或类型参考	GB 9706.1—2020,3.66
评定	3.203
驱动应用部分	3.201
随附文件	GB 9706.1—2020,3.4
损伤	3.207
伤害	GB 9706.1—2020,3.38
危险(源)	GB 9706.1—2020,3.39
危险情况	GB 9706.1—2020,3.40
危险相关使用场景	IEC 62366-1;2015,3.8
医用机器人	3.208
应用部分	GB 9706.1—2020,3.8
预期用途	GB 9706.1—2020,3.44
正常使用	GB 9706.1—2020,3.71
肢体运动功能	3.209
制造商	GB 9706.1—2020,3.55
主要操作功能	IEC 62366-1;2015,3.11

