



中华人民共和国国家标准

GB/T XXXXX. 1—XXXX/ISO 22166-1: 2021

机器人 服务机器人模块化 第1部分：通用要求

Robotics -- Modularity for service robots – Part1: General requirements

(ISO 22166-1: 2021, Robotics -- Modularity for service robots – Part1:
General requirements, IDT)

征求意见稿

XXXX – XX – XX 发布

XXXX – XX – XX 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

目次	I
前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 一般原则	7
4.1 总则	7
4.2 模块化一般原则	7
4.2.1 通则	7
4.2.2 可组合性	7
4.2.3 可集成性	7
4.2.4 互操作性	7
4.2.5 模块粒度	7
4.2.6 平台独立性	8
4.2.7 开放性	8
4.2.6 复用性	8
4.2.9 安全	8
4.2.9 安全性	8
4.3 抽象	8
4.4 电气接口和通信协议	9
4.5 互换性	10
4.6 模块属性	10
4.6.1 通则	10
4.6.2 模块识别	11
4.7 仿真	11
4.8 互操作性的数据类型	11
5 安全和安全性原则	12
5.1 总则	12
5.2 机器人系统级安全	13
5.3 模块级安全	14
5.4 安全性的通用方面	15
5.5 将安全性设计到模块中的步骤	16
5.6 模块的物理安全性	16
5.7 模块的网络安全性	16
6 模块设计的硬件部分	17

6.1 总则	17
6.2 模块硬件部分的要求和指南	17
6.2.1 机械接口	17
6.2.1.1 通则	17
6.2.1.2 连接的精度和可靠性	18
6.2.1.3 连接刚度	19
6.2.1.4 机械连接器和连接	19
6.2.2 电源接口	20
6.2.3 模块说明的其他方面	20
7 模块设计的软件部分	20
7.1 总则	20
7.2 信息模型	21
7.2.1 通则	21
7.2.2 模块间的信息交换模型	21
7.2.3 属性访问模型及其访问	22
7.2.4 错误处理和恢复模型	22
7.2.5 软件模块的互操作性	23
7.3 软件模块的架构模型	24
7.3.1 通则	24
7.3.2 软件模块的要求	25
7.4 具有软件部分的模块的安全/安全性相关要求	26
7.4.1 通则	26
7.4.2 与安全/安全性管理器模块的交互	27
8 使用信息	27
8.1 总则	27
8.2 标识或指示	28
8.3 用户信息	28
8.4 服务信息	29
附录 A (资料性) 机器人模块模板	30
附录 B (资料性) 机器人模示例	32
附录 C (资料性) 服务机器人模块化案例	42
附录 D (资料性) 机器人测试指南	51
参考文献	55

前 言

本文件按照 GB/T 1.1-2020 给出的规则起草。

本文件为《机器人 服务机器人模块化》的第 1 部分。

本文件由中国机械工业联合会提出。

本文件由全国机器人标准化技术委员会（SAC/TC159）归口。

本文件起草单位：北京机械工业自动化研究所有限公司、深圳云天励飞技术股份有限公司、遨博（北京）智能科技有限公司、立宏安全设备工程（上海）有限公司、清能德创电气技术（北京）有限公司、苏州协同创新医用机器人研究院、首都师范大学、苏州博众机器人有限公司、苏州大学、清华大学、中国科学院自动化研究所、苏州欧力机器人有限公司。

本文件主要起草人：袁杰、魏洪兴、李立言、王健、杨书评、邵振洲、苏衍宇、邹翼博、潘长勇、赵明全、王硕、欧勇胜。

引 言

本文件的制定是为了应对快速发展的服务机器人行业。目前,服务机器人市场覆盖了许多小型细分领域,人们很难开发出所需的特殊的和广泛适用的组件。预计服务机器人的市场规模和应用将显著增长,其功能的数量及其范围也会增加。为了实现服务机器人的广泛应用和互操作发展,需要一种通用的制造服务机器人的方法。本文件列出了常见的要求。

一方面,目前,在服务机器人设计中,采用依赖于制造商的架构方法给设计和开发带来了困难;在服务机器人的产品升级中,模块的替换和重复利用几乎是不可能的。另一方面,研究界也建立了一个庞大的机器人模块化设计知识库,并继续开发新的实现模块化的方法,但没有一种方法被广泛使用并产生重要影响。在这种情况下,本文件可以帮助服务机器人行业在市场所要求的成本下生产出所需的高质量的产品,并且迫切需要新的方法来帮助市场发展以应对全球挑战。

本文件有关服务机器人模块化和服务机器人模块的互操作,聚焦于安全、(信息)安全、连接性(从硬件和软件的角度)和功能等主要问题,这对于改变服务机器人的格局,加快新型服务机器人市场的形成至关重要。本文件将服务机器人模块化分为具有硬件和/或软件部分的基础模块和复合模块。制定本要求和指南以便实现基于模块的设计方法,在特定的服务机器人和服务机器人系统应用中满足用户对其易于配置的要求。这些问题被分为(a)安全和(信息)安全,(b)互操作的指南。此外,实现开放模块化方法使模块易于被其他具有相同接口规范的模块所替代,但可能需要增强其功能性。

现行的安全标准(例如,GB/T 36530、GB 11291.1、GB 11291.2、GB/T 36008)规定的安全要求既适用于系统层面,也适用于单个模块层面。本文件关于模块的安全指南的制定以确保机器人系统安全符合C类标准。在采用开放模块化方法时,安全问题非常重要,因此其也被包含在本文件中(例如,与IEC/TC 44和IEC/TC 65安全相关的工作项目保持一致)。

GB/T XXXX系列标准的未来部分将在特定类型的机器人模块方面包括更多的具体要求,例如,具有硬件和/或软件部分的基础和复合模块,以及特定类型的服务机器人,例如,移动仆从机器人、身体辅助机器人、载人机器人和在专业环境中的服务机器人。

机器人 服务机器人模块化

第1部分：通用要求

1 范围

本文件提出了在各种环境（包括个人和专业领域）应用的开放模块设计和服务机器人模块集成的要求与指南。

本文件适用于下列用户：

- 模块化服务机器人框架开发者（规定了服务机器人的性能框架）；
- 模块设计者和/或制造商（服务于终端用户或机器人集成商）；
- 服务机器人集成商（选择适用模块构建模块化系统）。

本文件包括如何将现有的安全标准应用于服务机器人模块的指南。

本文件不是安全标准。

本文件适用于服务机器人，但是本文件提出的模块化原则并不限制在机器人使用，也可以供其他领域的框架开发人员、模块制造商和模块集成商使用。

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

GB/T 16977 机器人与机器人装备 坐标系和运动命名原则（ISO 9787，IDT）

GB/T 35763 工业通信网络 网络和系统安全 系统安全要求和安全等级（IEC 62443-3-3，IDT）

GB/T 34989 连接器 安全要求和试验（IEC 61984，IDT）

ISO/TR 22100-4 机械安全 与ISO 12100的关系 第4部分：机械制造商考虑相关IT安全(网络安全)方面的指南（Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects）

ISO/IEC 27032 信息技术 安全技术 网络安全指南（Information technology — Security techniques — Guidelines for cybersecurity）

IEC 61076-1 电子设备连接器 产品要求 第1部分：通用规范（Connectors for electronic equipment—Product requirements — Part 1: Generic specification）

IEC/TS 62443-1-1 工业通信网络 网络与系统安全 第1-1部分：术语 概念和模型（Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models）

IEC 62443-2-1 工业通信网络 网络与系统安全 第2-1部分：建立工业自动化和控制系统安全程序（Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program）

NIST SP 800-154 以数据为中心的系统威胁建模指南（Guide to data-centric system threat modelling）

NIST SP 800-160 vols 1 and 2 可信赖安全系统工程中多学科方法的系统安全工程考虑 (Systems security engineering considerations for a multidisciplinary approach in the engineering of trustworthy secure systems)

3 术语和定义

下列术语和定义适用于本文件。

ISO与IEC在以下网址进行术语数据库维护以供标准化使用：

——ISO 在线浏览平台：<http://www.iso.org/obp>

——IEC Electropedia：<http://electropedia.org>

3.1 一般术语 general terms

3.1.1

抽象层 abstraction layer

允许以不同的和通用的更抽象的方式访问系统的部分或全部功能的系统接口。

注：当系统是一个模块时，一个模块的抽象层与之相同。

3.1.2

连接器 connector

允许系统各部分之间连接和断开的物理机制。

示例：

通信、电力、机械连接。

3.1.3

电气接口 electrical interface

连接器和电气性能的结合，用以功率、模拟或数字信号的传输。

3.1.4

运行生命周期 execution life cycle

有限状态机规定的某部分功能运行过程中的所有阶段。

3.1.5

误差 error

计算值、观察值或测量值或条件与真值、规定值或理论上正确值或条件之间的差异。

[来源：IEC 60050-192:2015, 192-03-02]

3.1.6

失效 failure

按要求执行的能力的损失。

[来源：IEC 60050-192:2015, 192-03-01]]

3.1.7

故障 fault

由于内部状态，无法按要求执行。

[来源：IEC 60050-192:2015, 192-04-01]]

3.1.8

功能 function

系统、部件或模块的既定目标或特定动作。

[来源：ISO/IEC/IEEE 24765, 3.1206-5, 有修改]

3.1.9

功能安全 functional safety

整体安全中与EUC和EUC控制系统相关的部分，它取决于E/E/PE安全相关系统和其他风险降低措施正确执行其功能。

[来源：GB/T 20438.4-2017，3.1.12]

3.1.10

硬件抽象层 hardware abstraction layer**HAL**

包含硬件部分的组件/模块的抽象层，利用抽象层通过软件接口提供对组件/模块的控制。

注：硬件抽象层的目的一般是使不同的模块可以通过相同的软件接口访问。

3.1.11

信息模型 information model

实体在受控环境中的抽象和表示，包括它们的属性、特征和操作以及它们彼此关联的方式。

注：信息模型独立于任何特定的存储、软件使用、协议或平台。

3.1.12

(信息)安全 security

保密性、完整性和可用性的组合。

[来源：ISO/TR 17522:2015，3.19]

3.2 组件相关术语 terms related to component

3.2.1

组件 component

某独立的和可识别的部分，与其他的部分组合可以组成更大的部分。

注1：组件可以是软件或硬件。一个主要是软件或硬件的组件可以被认为是软件组件或硬件组件。

注2：组件不需要有任何关于模块化的特定属性。

注3：组件和模块在一般术语中可以互换，但为了避免混淆，模块的术语涉及了组件，而组件需符合本文件的规定。

注4：一个模块可以是一个组件，但是一个组件不必是一个模块。

3.2.2

软件组件 software component

由计算机编程算法实现的组件。

3.2.3

硬件组件 hardware component

由物理元素及其工作中可能需要的嵌入式软件组成的组件。

3.3 组件相关术语 terms related to component

3.3.1

可组合性 composability

能够使用各种组合在逻辑上和物理上(不需要适应模块或额外的接口工作)将模块组合成新的模块的能力。

注：“集成”一般意味着付出巨大努力，“组合”一般意味着付出有限努力。

3.3.2

构形 configuration

按照一定数量和类型连接和设置模块，组合成复合模块的组合方式，以实现模块化机器人作为一个整体所期望的功能。

注1：GB/T 12643也定义了构形（关节），但是此处是不同的概念。

注2: 该术语描述了某一过程的结果, 即某种状态。造成这种状态的过程包含在术语配置(3.3.3)中。

3.3.3

配置 configuring

设置模块的数量、类型、连接方式以及模块的设置, 以实现模块化服务机器人作为一个整体的预期功能。

3.3.4

粒度 granularity

一个机器人模块可以被分解为独立模块的程度。

3.3.5

硬件部分 hardware aspects

模块及其物理互连所必需的属性和功能的信息, 以及工作环境的物理属性所允许范围的信息。

注1: 物理互连信息包括机械属性(材料、形状、姿态、尺寸、力/力矩)、电气和电磁属性、气动和液压属性。

注2: 工作环境特性包括力、温度、湿度、振动和机械冲击、照明和噪声(声音和电磁)。

3.3.6

基础设施 infrastructure

以支持模块和系统的工作的结构化设施和资源。

3.3.7

接口 interface

两个或多个功能模块之间的共享边界, 由适合于功能、信号交换和其他特性的各种特性定义。

[来源: ISO/IEC/IEEE 24765:2017, 3.2058, 定义1]

3.3.8

互操作性 interoperability

在模块之间进行通信、执行程序或传输数据或供电的能力, 或以某种方式在物理上和/或逻辑上组合模块的能力, 这种方式要求用户拥有很少或完全不了解单个模块的特征。

3.3.9

互换性 interchangeability

允许模块能够被另一个模块替换的特性。

注: 这种互换性与一个制造商或不同制造商生产的模块有关。

3.3.10

机械接口 mechanical interface

与其他模块连接的物理方式, 用于传递物理力, 便于模块功能和/或配置结构。

注1: 传递的物理力包括作为计划功能一部分的预期目的受控力, 以及故意(例如, 结构支撑)和非故意(例如, 缓冲)的非受控力。

注2: GB/T 12643使用该术语来定义操作机和末端执行器之间的机械接口。在本文件中, 该语有更广泛的含义, 包括机器人模块之间的任何机械接口。

3.3.11

模块化 modularity

允许系统被分离成独立模块并重新组合的特性。

3.3.12

模块 module

组件或利用已定义的接口和属性配置文件进行组件的组装, 以促进系统设计、集成、互操作和重复使用。

注1: 一个模块可能同时具有硬件和软件两个部分。其可以由其他组件(硬件和软件)或其他模块(硬件和软件)组成。

注2：并不要求也不阻止使用开源软件来实现部分或全部开放模块的功能。

注3：虽然开放的模块概念上是黑盒模块的对立面,但是其在本文件中仍视为一个黑盒模块,即如果机器人系统遵循本文件,其他模块应该仅能通过其官方的、产商规定模块接口与开放模块进行通信。

注4：开放模块不一定是复合模块,复合模块也不一定是开放模块。

3.3.13

包 package

所有软件二进制文件、配置信息和设计功能所需的模块软件部分的支持文件的集合。

注：包可以依赖于其他包。

3.3.14

模块属性 module property

模块的特性或特征。

示例：

硬件的一个模块属性是执行器的扭矩。软件的一个模块属性是对新指令的响应时间。

3.3.15

模块属性文件 module property profile

模块属性子集值的目录。

3.3.16

服务质量 quality of service

为了实现预期的整体工作,模块服务于与其连接的其他模块的最低性能水平。

3.3.17

重新配置 reconfiguration

改变模块化机器人的配置,以实现对模块化机器人功能的预期改变。

3.3.18

复用性 reusability

能够采用以前设计和制造的模块的能力,以促进新模块和机器人系统的开发,并实现所需的不同功能。

3.3.19

机器人模块 robot module

作为模块化机器人系统某部分的模块。

注1：并非模块化机器人系统中使用的所有模块都必须是机器人模块,但如果一个模块的主要目的是用于模块化机器人系统,那么它就是一个机器人模块。

注2：机器人模块作为服务机器人模块化的重要组成部分,如附录B中示例。

3.3.20

自我配置 self-configuration

自我重构 self-reconfiguration

必要时,无需对系统/子系统进行外部交互,自动改变模块化机器人的配置,但是,该程序的启动除外。

注：通常,机械和电气连接需要手动(重新)配置,自动配置用于软件部分的(重新)配置。

3.3.21

软件部分 software aspects

有关模块和其接口以及该模块功能的执行生命周期所需的外部软件性能信息。

3.4 模块分类术语

3.4.1

基础模块 basic module

模块不能分解成更小模块。

示例：服务机器人的基础模块可以定义为输入模块、处理模块、输出模块或基础设施支持模块。

3.4.2

复合模块 composite module

由两个或多个的模块构成的模块。

注：模块制造商可以选择编写其复合模块的内部结构文件，包括可能访问的内部接口或替换一些内置模块的文件化程序。但是，在一些情况下，出于满足要求的目的，本文件中定义的复合模块被认为是“黑盒模块”。

3.4.3

硬件模块 hardware module

模块的实现完全由物理部件组成，不能通过通信接口从外部进行访问，包括机械部件、电子电路和一些软件，如固件。

注：硬件模块具有硬件部分。它由硬件组件组成。

示例1：没有电子的机械关节；其硬件方面包括尺寸、运动性能，两端的固定板，材料，刚度，最大允许的力和扭矩等。

示例2：增强型机械关节，包括一个微控制器、控制器上的软件和电机，以控制刚度或阻尼等特性；其硬件方面还包括为嵌入式电子设备和嵌入式电机供电的连接器的连接，包括规定电压和电流限制。

3.4.4

软件模块 software module

完全由编程算法组成的模块。

注：软件模块具有软件部分。它由软件组件组成。

3.5 主功能模块的特征 characterization of modules regarding principal function

3.5.1

致动器模块 actuator module/actuating module

其主要功能是响应其他模块的指令，移动机器人或改变机器人周围世界以完成机器人系统的任务的输出模块。

3.5.2

通信模块 communication module

向其他媒介开放通信接口或提供模块之间互连的模块。

注：与其他媒介连接的接口可以通过Wi-Fi、移动网络、以太网等连接。

3.5.3

计算模块 computing module

为软件模块提供计算资源的模块。

注：计算资源是用于执行软件的硬件，可以包括分布式模块。

3.5.4

基础设施模块 infrastructure module

提供设施和资源以支持其他模块工作的模块。

注1：例如，其他模块使用的设施包括用于物理连接点的机械框架，以及用于通信和动的电缆，电缆可以连接到框架上。

注2：例如，其他模块使用的资源包括电源、内存和处理器、机器人间或机器人与服务器之间的通信桥(或集线器)。

3.5.5

感知模块 sensing module

用于收集机器人周围世界或机器人状态数据的输入模块,供其他模块使用以支持机器人系统执行其任务。

3.5.6

监督模块 supervisor module

检查其他模块的状态的软件模块,可控制一种状态到另一种状态的转换,使各模块具有适合的工作顺序。

4 一般原则

4.1 总则

第4章介绍了在服务机器人中使用模块化基本理念。为了描述这些概念,应该使用SysML (OMG SysML),其定义了系统工程应用的通用建模语言的图形类型,并且其还支持指定、分析、设计、验证和确认。为了满足模块化原则,制造商应完成验证和确认的程序。

4.2 模块化一般原则

4.2.1 通则

本条款解释了模块设计应遵循的通用原则。虽然这些原则部分是推荐性的,但是模块设计者应:

- 记录所选择的模块化方法;
- 为集成商使用这些模块,提供所有必要的信息。

这些原则可以通用地应用于具有硬件或软件部分面的模块。在本章中,除非另有说明,模块在最广泛意义上指基本模块或复合模块。

4.2.2 可组合性

模块的设计应在逻辑和物理上组装成复合模块,以执行更复杂的操作,并满足操作和安全要求。组合应基于接口提供的信息以达到不需要内部结构信息的目的。模块可以在数据库或存储库中组合,使其重复使用变得更实际,将在7.2.2中进一步讨论。

4.2.3 可集成性

模块硬件部分和软件部分的设计应使它们能集成为更大的系统,以完成预期的目标服务或功能。为了模块可靠的连接方式,应设计适当的接口。模块化系统的安全方面将在第5章中讨论。

4.2.4 互操作性

模块应设计成能与其他模块连接。它们应该易于连接,并且应该允许通过适当的连接器共享电源和数据。为允许数据交换,应在第7章规定的适当层次上定义和实现接口协议。

4.2.5 模块粒度

模块的功能应在模块化框架中以适当的粒度实现：基础模块和复合模块。基础模块和复合模块的示例见附件B。

4.2.6 平台独立性

模块的设计应该能够在不同的服务机器人上实现，或者在不进行重大修改的情况下与不同的模块组合在一起。软件模块应可以通过微小的修改，可以在不同的平台上运行，例如，嵌入式计算系统、Linux、Windows或实时操作系统。在不同的服务机器人系统中使用的硬件模块应可以在不同的平台上运行。

4.2.7 开放性

本文件中，开放性应包括具有硬件部分的模块的机械和电气接口，模块间的软件接口包括：由具有硬件和软件部分模块组成的经过定义的参考架构以及模块在安全、安全性和测试方法的设计。

模块的重复使用应该通过提供相关信息来支持，例如，它们对集成商的依赖性和不兼容性。

注：相关信息包括源代码、文件、计算机辅助设计(CAD)模型、电路图、设计经验、系统架构、软件层次、接口规范等。

4.2.6 复用性

复用性是指模块通过适当定义的接口在不同平台上使用和重复使用的能力。模块的接口设计应做到模块可重复使用。

允许重复使用的相关接口包括软件接口、模块间的连接器以及模块硬件部分之间的连接。

在适当的情况下，应该通过管理构建、配置和重新配置、升级可能性和模块的整体维护要求来支持模块的复用性。

4.2.9 安全

在所有与安全相关的应用中，模块的设计应符合相关的安全标准。此外，模块的设计还应支持模块化系统的整体安全。模块制造商应提供必要的信息以支持集成商进行系统的安全设计。

4.2.9 安全性

具有软件部分或通信接口的模块应设计成可阻止未经授权的方式或人员的试图访问。此外，它们的设计应支持模块化系统的整体安全性。

4.3 抽象

应该使用抽象层来定义硬件和软件之间的标准接口，为了：

- 支持互操作性和复用性；
- 简化仿真和建模；
- 形成事实的独立性和平台独立性。

注1：例如，可以同时使用红外传感软件模块和超声传感软件模块来获得机器人到附近物体的距离。这两个模块可以分别使用红外传感器和超声波传感器的设备驱动读取距离值。在这种情况下，即使这两个模块使用相同的数据，这两

个模块可能无法重复使用和互操作，因为每个模块使用它们自己的设备驱动程序。为了保证这两个读取距离值的模块复用性，需要一个抽象的设备驱动程序，之后可以使用不同的感知模块，即使许多制造商提供不同类型的距离测量传感器。

注2:软件模块中的软件部分使用抽象层来访问伺服电机、激光传感器等硬件设备。

注3:在本文件中，可选择使用硬件抽象层或其他形式的设备驱动程序(见7.3)。如果一个模块化机器人系统的特定实施可以通过直接调用设备驱动程序的软件功能来实现，这也是允许的。抽象包括在底层通信技术不同的情况下使用翻译技术。

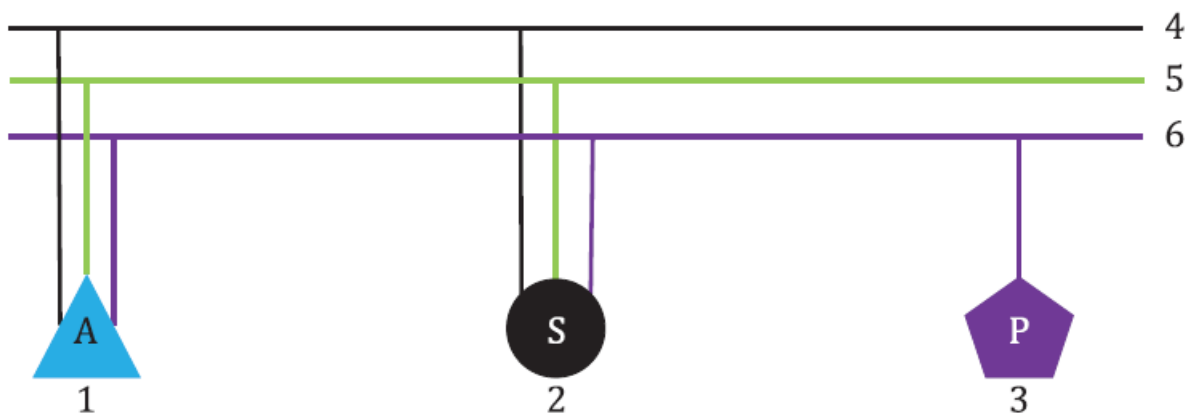
4.4 电气接口和通信协议

电气接口和通信协议应该符合已经存在的标准。

注1:数据总线和通信网络的接口包括硬件和软件部分。通用接口布置的概念性示例如图1所示，包括了功能、电源和操作环境。

注2:表1展示了一些通信协议的案例。通信协议经常被植入软件中，有时也植入硬件中。其如ISO/IEC 7498-1中定义的OSI参考模型中的第2层到第7层所示。

电气接口的硬件设计不应由于接近其他电线或设备而使通信受到干扰。只能使用标准化的连接器。



说明:

- 1—执行器
- 2—传感器
- 3—电源
- 4—环境
- 5—功能
- 6—电源

图1 模块间通用接口布置的概念性示例（详见第六章）

表1 可用于模块的通信协议示例

参考	类型	备注
ISO 11898-1/2和EN 50325-4/5	CAN 和CANopen	CAN媒体接入单元子层通常在收发ICs中实施，CAN数据连接层协议和物理信号子层在CAN协议控制器中实现，CANopen应用层通常在微控制器上运行的软件中实施。
ISO/IEC/IEEE 8802-3:2017 IETF 793 或 ISO/IEC 14766 (TCP)、	Ethernet 和 TCP/IP	在 PHYs 和 MAC 中实施，PHYs 和 MAC 可选择集成在特定技术的控制器上。（该协议在世界范围内广泛使用）。

IETF RFC 768 (UDP)、 RFC 791 (IPv4)、 RFC 2460 (IPv6)		
IEC 62680 和USB CDC	USB	USB通信设备类(CDC)是一个复合的通用串行总线设备类。
IEC 61158	现场总线	IEC 61158对常用的现场总线协议进行标准化,包括基础总线、现场总线、WorldFIP、CC-link、EtherCAT Modbus-RTPS、SERCOS等。

4.5 互换性

模块的互换性和重组与模块的连接性密切相关,可以分为不同的级别;本文件考虑了以下内容:

- 1级:仅制造商或机器人系统集成商可互换模块;
- 2级:当机器人关闭时,用户可以互换模块;
- 3级:在机器人启动时(热插拔),用户可以互换模块;
- 4级:机器人自身可互换模块(激活驱动的热插拔)。

自我配置(3级和4级)可能导致错误操作或危险情况。相关的安全和安全性问题在第5章中讨论。为了避免模块状态的不明确,应该避免对正在进行的机器人功能进行自我配置。

模块制造商应提供模块的互换性级别。不同的级别互换性对连接器的设计、安全和安全性、耐久性、模块文件等方面的要求有不同的意义,如表2所示。

表2 不同级别互换性的推荐

级别	交换频率	连接器设计	文件	安全	软件
1	低	可以将机械和电气部简单分开连接	具备技术知识的读者	应包括交换后的风险评估问题	安装和配置可以复合,包括手动调整
2	中-高	更合适的复合插头	不具备技术知识的读者	需要为用户提供安全限制。系统在通电时进行一致性检查	包的组织,自动解决依赖
3	高	具备热插功能的复合插头	不具备技术知识的读者	需要为用户提供安全限制。当其他功能正在执行时,系统需要执行一致性检查。	运行时,自动加载、卸载和切换模块
4	高	具有热插拔功能和大容差自动连接的复合插头	不具备技术知识的读者	安全限制需要以机器可读的形式提供。当其他功能正在执行时,系统需要执行一致性检查。	运行时,自动加载、卸载和切换模块

模块化机器人系统的信息模型应提供关于模块属性和单个模块关于互换和自我配置能力的信息。

4.6 模块属性

4.6.1 通则

模块属性应该存储在模块属性文件中。当一个模块被转移使用或重复使用时,模块文件应与该模块一起使用或重复使用。

注：对存储的性质没有要求。

4.6.2 模块识别

模块应该使用由制造商发布的字符串或数字代码来命名或识别。此外，产品本身和供应商也应该使用类似的名称或标识码进行标识。这些信息可用于基于模块的服务机器人设计，模块可以(半)自动地配置机器人系统。如果模块使用数据总线，其应该在请求时将自己的ID传递给其他模块和监督模块。

模块可以自动配置机器人的硬件(包括结构)和软件。

如果模块可以进行自动配置，制造商提供的识别模块的信息应该包括：

- 模块类型和/或模块ID；
- 制造商名称和/或制造商ID；
- 模块版本；
- 生产日期；
- 序列号。

从系统安全性的角度来看，模块的识别应通过安全相关模块的身份验证程序的适当设计来验证。

4.7 仿真

如果使用仿真来验证一个模块的设计和性能，应注意所使用模块的限制和约束。特别是，安全和安全性应在预期应用中的实际测试中进行验证。

为了对模块化系统进行适当的仿真，模块制造商应提供模块仿真所需的相关信息。框架设计人员应明确哪些信息是必要的以及应以何种形式提供这些信息(例如，在纸上或作为可导入仿真工具的参数文件)。用于仿真的模块信息包括：

- 物理特性，包括其物理属性(例如，尺寸、质量、密度、静态和动态特性、结构强度等)和外观；
- 电气特性，如工作所需的峰值功率和平均功率；
- 可执行的一般控制算法；
- 输入(传感器)或输出(执行器)模块的接口，确定要交换的信息的格式和类型；
- 传感器模块从仿真环境获取信息的方法；和
- 执行器模块在仿真环境中工作的方法。

注1:各种模块的详细规范不在本文件的讨论范围内。

注2:可在模块模板内提供仿真数据。

4.8 互操作性的数据类型

模块化框架应定义在模块化框架和中间件中使用的数据类型。其包括IEC/TR 62390中常见的整型和实数数值数据类型的精度。

模块化框架还应定义通用复合数据类型约定，并推荐定义以下约定。也有少量的通用复合数据类型建立在这些基础上(见OMG RLS(机器人本地化服务))，即：

- a) 空间中的一个位置是相对于某个坐标系定义的，该坐标系根据实施以定义固定的位置和方向。坐标可以在笛卡尔正交坐标系中用一组三个实数(x, y, z)给出。也可以用一对数字(x, y)给出，但可以解释为z=0的三元组；

b) 朝向可以用两种方式之一确定。三维空间中, 朝向一般以四元数的形式给出, 该四元数转换为四元组 (c, su, sv, sw) ; 其中, (u, v, w) 为旋转轴, c 和 s 分别为半旋转角的余弦和正弦。或者, 绕 z 轴的旋转只能作为绕 z 轴的旋转角度给出, 该角度以弧度为单位;

c) 移动机器人的位置和朝向由 ISO 19649 和 ISO 9787 规定的标准坐标系给出;

d) 2D 和 3D 对象的几何数据从现有标准中选择。

模块化框架还可定义参考或限制, 如何在模块间输入/输出数据应该结构化。

模块制造商应在模块框架定义的允许范围内为其模块选择合适的数据类型和数据结构。数据类型和数据结构的信息应在模块描述中说明(模块示例见附件B)。

5 安全和安全性原则

5.1 总则

本条款提供了如何将已发布的安全和安全性标准的要求应用于模块和基于模块的系统设计中的原则。其不得作为偏离适用的安全和安全性标准的理由。

注: 安全可以从单个模块的级别(通常由模块制造商完成)和服务机器人系统的级别(通常由集成商完成)进行评估。

在机器人设计和机器人模块设计中, 安全和安全性是两个相互影响的不同设计方面。机器人系统和/或机器人模块的安全性漏洞可能导致与安全相关的危险。因此, 机器人模块制造商应通过风险评估, 评估与安全性相关的属性在预期使用中造成的危害的可能性, 设计人员应通过模块设计来减小这种危害。

服务机器人系统的某个模块的安全性漏洞可导致整个服务机器人系统出现安全性漏洞, 从而造成危害。模块制造商应意识到模块的安全性漏洞可能会在机器人系统中演变。因此, 机器人设计人员在模块化设计时需要考虑安全和安全性问题。

现有适用于机器人和机器人系统安全标准, 包括:

- 用于对机械风险评估和风险降低的 GB/T 15706;
- 用于工业机器人的 ISO 10218-1、ISO 10218-2 和 ISO/TS 15066;
- 用于个人助理机器人的 ISO 13482;
- 用于医疗机器人各方面的 IEC/TR 60601-4-1、IEC 80601-2-77 和 IEC 80601-2-78; 和
- 用于功能安全的 ISO 13849-1、IEC 61508 系列、and IEC 62061。

在一个模块化机器人系统软件中, 会涉及到机器人的各种各样的模块。ISO/IEC/IEEE 12207:2017 和 ISO/IEC/IEEE 15288:2015 定义了软件开发生命周期, 以确保达到所要求的质量。GB/T 20438.3 规定了作为控制系统安全相关部分的软件的安全要求。软件的安全要求仅适用于软件中与安全相关的部分, 见 7.2 和 7.4。

当采用模块化的设计方法时, 提高多用途的服务机器人系统的重新配置能力的应考虑 GB/T 15706 中描述的风险评估和风险减小的过程, 确保满足安全要求, 即使添加/删除/重新配置模块, 例如: 重新配置后再次进行风险评估。这些要求既可应用于系统级别, 又可应用于模块级别。除正常的基于安全风险评估外, 设计人员和/或服务机器人集成商还应结合安全性风险评估, 以评估安全结果。例如, 可以通过添加模块来降低危险情况。但是, 机器人系统的模块结构的任何改变, 需要重新评估模块重新配置后的安全和安全性风险。

评估机器人系统和模块安全性, 应使用以下标准:

- ISO/TR 22100-4 用于机械的信息技术安全方面;
- ISO/IEC 27032 用于网络安全的一般准则;
- IEC/TS 62443-1-1 用于术语、概念和模型;

- IEC 62443-2-1用于工业自动化安全程序;
- GB/T 35763 用于控制系统的安全级别;
- NIST SP 800-154用于数据中心系统威胁建模;
- NIST SP 800-160卷1和卷2用于系统安全工程。

图2显示了相关的安全和安全性风险是多大以及如何解决。模块制造商和集成商(以及适用情况下的模块框架设计人员)应遵守现有的适用的安全标准的规定和要求,如图2水平线所示。模块的安全性风险评估应参考模块安全分析中相同的预期用途、可预见的误用和“机器限制”(如 GB/T 15706-2012, 5.3)。安全性风险评估和减小的过程,如图2垂直线所示,应是一个迭代过程:等效于GB/T 15706-2012第4章图1中的步骤1和步骤2,或者在各自进程结束时。安全和安全性风险的评估和减小的复合过程(如图2对角线)应是一个迭代过程。如果安全性实施措施与预期的安全功能(为了满足安全要求)实施发生冲突,应优先降低安全风险,同时仍应尽可能降低安全性风险。

注2:模块制造商可以尝试不同的单独的安全功能的实施,但仍然需要满足安全要求。或者在不损害安全功能的情况下尽可能地扩展安全性措施。

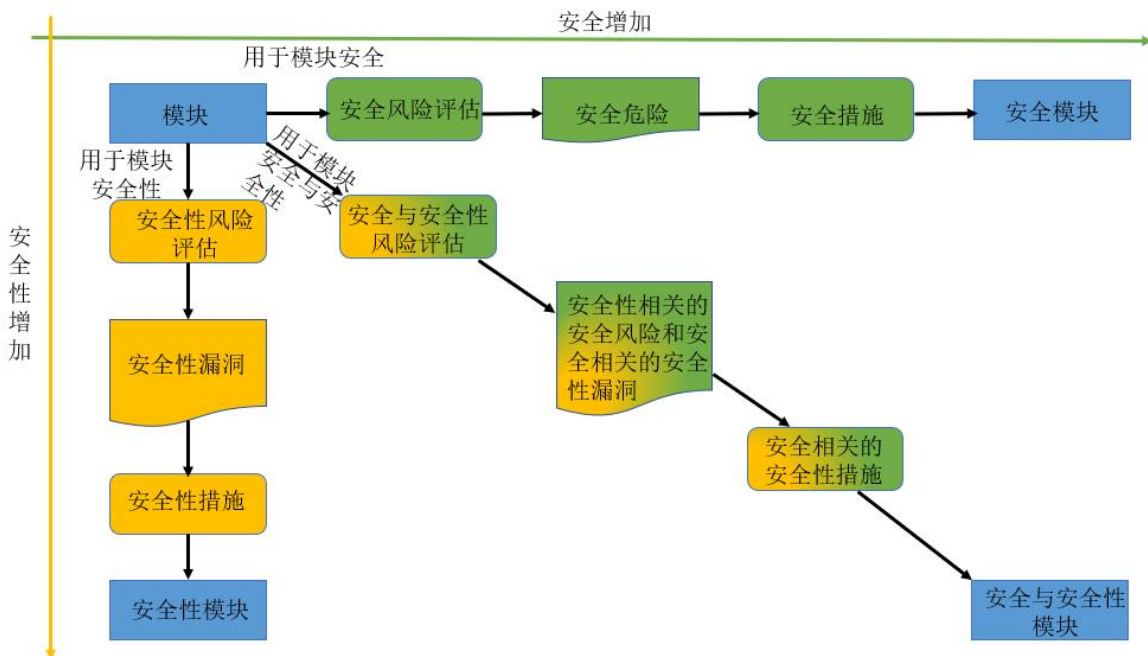


图2 机器人模块的安全与安全性考虑

模块制造商应考虑模块的预期使用和用于确定各种应用领域所要求的技术(例如,机械、电磁、软件、安全性、环境、生物、化学、可用性等)。此外,模块制造商应确定并列出现用例,包括具体的限制和不适用的情况。虽然模块化可能在预期应用领域的现有标准中,没有明确适用范围,但现有标准中提出的原则对于提出适当的模块要求和测试方法是有用的。关于测试机器人模块的详细信息见附录D。

模块集成商应考虑以下信息:

- 与外部系统的关系(物理布局、界面等);
- 模块和系统级的维护指引。

5.2 机器人系统级安全

由机器人模块组成的机器人系统的安全性评估方法与没有模块的机器人系统的安全性评估方法之间没有不同。这些方法已经包括在现有的标准中。

模块化服务机器人框架开发人员负责：

- 设计各个服务机器人模块的架构和组成；
- 确保模块间安全信号的正确连接和处理；
- 评估典型应用用例所需的机器人安全。

注1:典型的应用用例包括不同的级别安全、安全性、复合安全与安全性、和质量。

注2: 信号既包括进或出模块的紧急停止信号等硬件信号，也包括通过有线或无线网络交换的数据信号，在这种情况下，网络应满足功能安全要求。

模块制造商应负责明确模块的预期应用。

模块集成商应负责：

- 符合5.1提及的适用机器人安全标准；
- 说明系统的预期使用，并将其与模块制造商提出的预期用例的相关性和紧密性进行比较，和
- 遵守模块制造商规定的安全原则，包括使用所需的条件。

如果机器人系统或其应用发生变化，那么风险评估应考虑这些变化，示例见附录C。如果最终用户想改变模块化机器人系统，风险评估应包括由于可能出现的配置所导致的风险。

注3:适用的使用限制和必要的安全注意事项及相应步骤是机器人系统用户手册的一部分。

模块化服务机器人框架开发人员应采用风险减小的设计措施，以确保以下：

- 整体安全信号和错误状态以及使用和传输的规则；
- 所有模块应具备的安全功能或最低安全性能；
- 核心项目应包括在安全级别的文件中。

5.3 模块级安全

模块的设计应考虑已发布的适用于电气和机械安全标准(机器人模块测试见附件D)。软件的安全要求在5.4中讨论。

如果电机具有停止功能，模块应提供符合IEC 61800-5-2相应的安全功能。

为了避免模块间通信失效，系统应该使用黑通道通信(见IEC 62280和IEC 61784-3)。在这种情况下，模块的可靠性应设计成与安全相关，并构建保证安全功能可靠性的路径。

性能等级(PL)或安全完整性等级(SIL)应归属于安全功能的实施。PL/SIL可用于评估整个机器人系统的安全功能的整体性能。模块制造商应发布模块与其他模块之间共享的所有安全功能的PL或SIL。模块中与安全无关的信号可能仍然有用，并向其他模块报告与安全有关的功能。

设计机器人模块所遵循的过程可能不同于常规的系统设计，因为模块设计人员/制造商在设计阶段无法获得最终具体应用(只知道典型的用例场景)。

机器人模块制造商可以通过以下步骤来确保符合适当和充分的安全设计要求，包括：

1. 定义预期用例，并为每个用例尽可能多地描述相关细节；
2. 对于每个用例，都应该进行假设机器人系统设计。应考虑模块的所有可预见应用。还应考虑模块在可合理的可预见的误用；

注1:必要时，可以假定系统有安全监督(见7.2和7.4)。

3. 对于每个预期的用例应用，应该确定潜在的危险(GB/T 15706—2012，附录B，包括应该考虑的潜在危险列表)；

4. 为了进行安全风险评估，应该将模块视为单个模块，并考虑其在预期用例应用中可能造成哪些潜在危险。

模块的安全需求应基于一些假设的最坏的用例；

5. 模块制造商应对每个预期用例完成安全风险评估，并为模块内任何与安全相关的功能定义适当的PL。在模块中构建与安全相关的本地监督功能可能是合适的，见7.2中的“安全监督”。

注2:并非在所有情况下都需要采取所有步骤。

模块制造商应记录预期用例及其假设，并向模块集成商提供以下信息：

- 模块使用信息；
- 模块安全运行的环境条件；
- 模块的安全相关功能信息；
- 模块提供给其他模块的数据信息，可能对模块外的安全有意义(例如，安全监督内)。

注3:IEC 60204-1提供了操作界面和紧急停止等功能的安全要求，并与模块相关。

作为一个例子，移动机器人平台安全系统的两种可能的实施显示，在真实世界里具有更多(安全相关)特性的模块更容易集成与使用。

示例：

由两个不同制造商提供的复合模块具有以下特点：

—— 平台1有电机，其机械地限制平台的最大速度为1m/s。平台控制器接受期望的移动速度作为当前速度的输入和输出，但这两个信号都不与安全相关的，也没有性能等级评级；

—— 平台2最大速度可达2m/s。平台控制器通过高性能等级提供安全相关的速度控制。因此，期望的速度输入和当前的速度输出是与安全相关的。

机器人集成商设计了一个具有平台1的移动机器人，其简单的安全系统由激光扫描模块组成，具有固定的保护范围，当机器人以1m/s的速度运行时，能够及时停止。

当使用平台2代替平台1时，机器人集成商应大幅增加激光扫描仪的保护范围，以适应可能的2m/s最大速度。其将决定使用2号平台的安全相关的速度控制功能。在这种情况下，当平台实际高速运行时，才需要最大的保护区域。对于缓慢的停止操作，可以减少保护范围。

实例表明，当使用平台2时，系统具有其所需的安全特性，则更能适应不断变化的环境要求。

注4:使用速度控制和改变保护范围要求激光扫描模块和安全监督模块都支持这一功能。

5.4 安全性的通用方面

模块级安全应确保单个模块能够抵御未经授权的访问，以防止攻击，从而影响模块的机密性、完整性和可用性，例如：

- 未经授权访问内部数据(可能影响知识产权或个人数据)；
- 未经授权访问和更改模块配置和内部参数设置(可能影响安全)；
- 由于攻击导致的模块或者模块化机器人的损坏或无法正常使用。

对机器人系统的模块进行篡改应作为一种安全隐患，因为机器人系统或者其部分可能由于安全系统的损坏导致不受控制的移动。为了确认模块的安全性等级，见附录D。

网络安全是一个不断发展的领域，需要在模块设计中加以考虑，因此应该考虑最新的发展。所提出的设计与前面各子条款中提出的安全步骤有很强的相似性。

注1:目前没有可供参考的安全性能等级。

根据安全风险评估的结果，选择模块和模块化服务机器人的保护措施，考虑以下因素：

- 暴露于潜在的入侵者(内部人员和外部人员)；
- 未经授权的访问可能造成的潜在危害(例如，对可用性或安全的影响)；
- 入侵者获取访问的潜在动机(例如，访问有价值的隐私数据)。

为了实现系统级安全性，所有交换数据的连接模块都应能为未经授权访问物理数据端口提供充分保护。模块内部的通信、模块之间的通信和机器人系统外部的通信应区别对待。

注2:在机械和机器人系统中几乎所有的现代安全装置和安全相关功能都存在某种通信和(嵌入式)软件。几乎任何软件都有可能受到行为和安全功能改变的影响。如果该模块与其他模块或机器人系统之外共享数据，那么未经授权的访问和影响的机会就会更大。第7章描述了更多的细节。

本文件使用安全及安全性的综合级别对模块进行分类，如下：

1. 无安全或安全性需要：这种不需要综合安全和安全性要求可以适用于不会伤害人且不连接任何外部系统的小型 and 轻型机器人；

2. 安全性需要：适用于模块的预期用途，包括机器人内部通信或与外部系统通信。第6章介绍了硬件方面的安全措施和第7章介绍了软件和通信方面的安全措施；

3. 在某些情况下，可以设计一个安全但具有潜在不安全性的系统；这应该取决于应用是否可以接受；

4. 综合安全和安全性需要：只有同时满足了安全和安全性要求，系统才能被认为是安全的。确保足够的安全和安全性风险评估所需遵循的流程，如图2所示。

注3:只有硬件而没有软件的系统，如安全开关，这是少数例外，尽管不具备安全性，可以认为是安全的。

5.5 将安全性设计到模块中的步骤

机器人模块制造商应采用以下步骤，以确保适当和充分的安全性设计要求：

1. 从安全性角度定义模块的用例。这些用例与为安全而定义的用例相似，但也可以不同；

2. 应考虑模块的预期和潜在应用。

注：如果有必要，可以设想系统具有安全性监督(见7.2和7.4)。

3. 设计人员应完成每个用例的安全性风险评估，以提出模块维护的安全性需求，以保障模块和系统的安全性；

4. 模块内软件应符合7.4的安全性要求；

5. 检查7.4的安全数据交换的指南；

6. 防止对模块的非法访问，检查5.7的硬件指南；。

7. 安全性风险评估应独立地对每个模块进行，并在步骤2中定义的用例场景中评估结果。

5.6 模块的物理安全性

模块制造商在模块设计时应考虑的物理安全性的以下几个方面，而集成商则应考虑模块化机器人系统的物理安全性：

—— 通信端口安全；

—— 外部对内部组件的物理访问。

注：模块可以通过总线系统传递给相邻的模块。因此，安全漏洞可以从一个模块传播到另一个模块。

模块制造商和集成商应考虑以下措施来限制对模块或系统通信端口的访问，例如：

—— 门闩传感器(不要求安全性，但需要知道是否处于打开或关闭状态)；

—— 采用物理钥匙的机械锁；

—— 采用闩锁执行器的机械锁。

没有安全性措施的模块只能在受保护的环境中使用，例如，内部研究实验室环境，或仅限于小型和轻型服务机器人使用。

5.7 模块的网络安全性

模块(或其固件和软件)应该:

- 禁止未经授权的篡改;
- 为模块存储、处理和交换提供安全性保障;
- 提供通信安全保障。

注1:采用网络安全措施的必要性取决于模块的预期用途。

模块的网络安全应设计为实现以下安全性目标:保密性、完整性和可用性。在进行网络安全性风险评估和减小时,应考虑以下:

- 保密性措施示例:安全开机、身份验证(例如,密码)、数据加密;
- 完整性措施示例:访问控制和权限、校验;
- 完整性和保密性措施的示例:数据保安、安全通信;
- 可用性措施的示例:安全代码更新、足够的通信带宽、冗余。

注2:IEC 62443系列标准包括了工业自动化系统的一般安全方面。一个覆盖机器安全性方面的标准正在制定中;IEC/TR 63074介绍了与控制系统的功能安全有关的安全性方面。

6 模块设计的硬件部分

6.1 总则

本章描述了具有硬件部分的模块,包括硬件模块,的互操作性和复用性的要求和指南。对于具有硬件部分的模块,表3显示为了实现有效的模块化设计框架并实现本文件中提出的互操作性、安全和(信息)安全要求时应考虑的主要连接问题。具有硬件部分的模块的示例以及如何解决也一并进行了说明。设计硬件模块或具有硬件部分的模块(例如,执行器),需要考虑安全、(信息)安全、电源、信号以及机械结构。

注:硬件模块或具有硬件部分的模块的连接问题可以是物理的(例如,电源、数据),也可以是更抽象的交互(例如,安全、(信息)安全、环境、机制)。例如,如果一个模块连接到(信息)安全,则该模块存在(信息)安全相关的问题与其他与(信息)安全相关的模块以某种方式进行数据交换。

表3 模块框架的连接性示例

模块/交互	环境	机械	数据	动力	(信息)安全	安全
执行器(A)	√	√	√	√	√	√
电源(P)			(√)	√	√	√
传感器(S,数字/模拟)	√	√	√	√	√	√
软件计算(CS)			√	√	√	√
监督(SU)			√		√√	√
用户界面(UI)	√		√	√	√	√

6.2 模块硬件部分的要求和指南

6.2.1 机械接口

6.2.1.1 总则

模块应提供机械接口和连接器的规格，例如：

- 连接器和接口的规格；
- 带有占位符的连接器规范(模块非必须的盲或空连接器)；
- 针对不同的物理耐久性和尺寸要求，连接器的多种物理尺寸规格，例如：针对操作机不同部件的预期用途；
- 数据总线和/或电源回路的机械连接规格；
- 接口规范，该规范允许数据总线或电源通过模块形成回路，即使模块本身不需要连接它们(例如，机械连接)。

注1:虽然建议在模块中集成连接器，但在结合模块的机械连接和分离的物理运动上面临特殊的设计挑战，同时为了保持数据、电源、安全和安全性的连接器预期操作，连接器处于连接和非连接状态。如果鲁棒性设计规范不能满足预期用途的要求，则模块可能会带来安全和性能风险，最终导致故障和失效。

应该对模块与其他模块的连接和分离进行适当的测试和确认。如果适用，使用信息应说明测试和确认是必须的。模块应附有支撑开展模块与其他模块的连接和分离测试验证的使用信息。使用信息应包括具有硬件部分的模块之间的连接和功能的信息，例如：

- 在静态和预计动态运动情况下，模块对准、模块定位和模块锁定的期望刚度；
- 在模块接口的机械定位和锁定过程中，数据、信号和电源不被损坏；
- 在模块预期用例中，机械连接器的规定精度和刚度所需的机械连接/锁定机制。

考虑到模块的预期用途和规定的用例，在模块规定的寿命内，模块可能会断开连接和重新连接一定次数。在适用情况下，可以使用以下设计：

- 使用渐进过盈配合，使物理接触点连接在一起而不损坏；
- 使用同轴和/或锥形结构，以减少在配合期间的角或横向运动，以避免接触点磨损，撕裂和损坏；
- 采用环形结构创建多个接触点，增加物理连接的分布，提高机械连接的精度；
- 使用兼容的材料和结构构建更具兼容性机械连接，通过扩展结构分布机械力以避免单点故障。

注2:工业机器人接口标准可应用于服务机器人模块，例如，ISO 9409-1、-2和ISO 11593。

模块制造商应提供机械接口规范，以便其他模块制造商或集成商使用，包括：

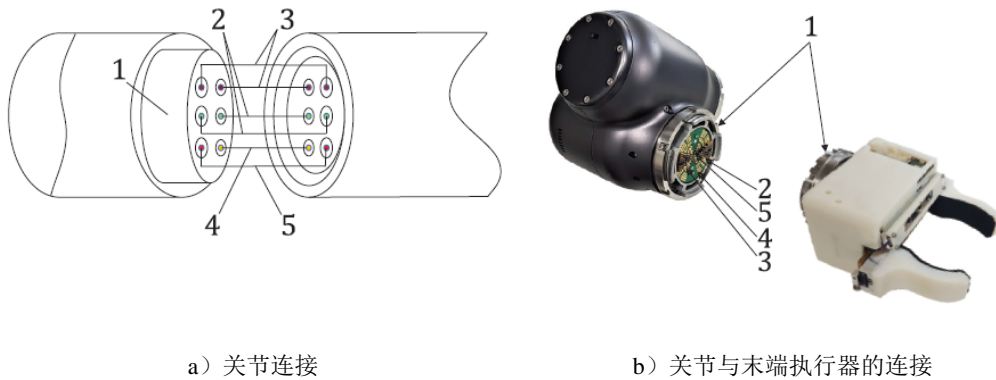
- 机械零件的CAD数据；
- 插头的制造商和型号；
- 插针分配。

6.2.1.2 连接的精度和可靠性

在服务机器人模块化设计中，模块之间的连接根据预期用途应具有以下连接特征，如图3所示：

- 电源；
- 数据；
- (信息)安全；
- 安全；
- 机械。

与安全有关的模块应保证它们之间的连接安全。模块应该规定它们之间的连接精度。



说明

- 1 机械
- 2 数据
- 3 电源
- 4 (信息) 安全
- 5 安全

图 3 模块关节所需连接特征示例

使用信息应包括模块连接器的可靠性规范，包括：

- 关节锁定后的平移和旋转量。即：一旦关节被锁定，将不可能产生任何运动；
- 模块接口的鲁棒性和可靠性参数。用于对准的机械表面的磨损和电源、数据和安全的整体连接可承受连接/断开循环的最少次数；
- 模块接口的耐久性。在模块频繁更换或可能出现污垢和过载等极端条件的情况下，模块应经过验证并确认具体的循环次数。最少循环次数由制造商规定。

模块制造商至少应该满足模块化框架中定义的要求，或者定义其自己的规范，以满足预期应用。

6.2.1.3 连接刚度

模块和模块接口应具有足够的刚度，以通过验证或者确认的过程将静态和动态的力和力矩在模块间的传递，通常称为包络线设计。为了限制模块相对于模块另一端的几何形量，可以在模块接口或模块另一端的三个轴(x、y、z)上规定最大加载扭矩和力。

对于模块，包括其接口，应规定可施加的力和/或力矩，以便满足以下要求：

- 物理模块另一端的最大几何形变小于规定值；
- 最大扭力加载时，最大旋转形变小于规定值。

6.2.1.4 机械连接器和连接

在可能情况下，模块应能使用最少或不使用工具来连接。如果模块相对较小，可手动(即无辅助装置)安装。对于较重的模块，可使用吊装支撑，机械接口应设计成能够适较大安装力的量件、接口碰撞或高速接触等情况，而不会对机械接口造成损坏。

制造商应推荐规定测试，以评估在特殊用例应用下采用的连接/断开的耐久性(见附件D)。

如果连接器集成在模块中，则应提供模块安全连接/断开的必要说明。

注：推荐一种用于单电缆解决方案的特殊类型连接器，特别是在电机驱动和运动控制应用中，该连接器集成了机械接口、电源、数据和安全信号，同时提供安全连接/断开的必要说明。

根据需要，电气连接器应符合IEC 61076-1和/或IEC 61984中提出的要求。

连接器的选择和定位应符合以下：

- 合力/运动轨迹在规定限制内；
- 电气、气动、液压和机械形式能源要求；
- 数据通信及其完整性的要求；和
- 符合已发布的相关安全要求(见第5章)。

在设计模块的集成细节中，应该考虑电气、气动或液压连接器的机械负载和力。应确保下列：

- 在尺寸和电气上，不同连接器的正确的物理交互；
- 减少接口内不同连接器之间的EMC/EMI；
- 通过接口内的集成连接器进行流体动力传动时，无液体或气体泄漏。

6.2.2 电源接口

电源为所有执行机构提供动力或能量。制造商应选择合适的供电类型，如电气(交流或直流)、气动或液压，例如，制造商应重点关注广泛应用的供电电压，如5V、12V、24V或48V。

制造商应规定电源的额定值和最大输出负载能力。该模块应设计为可增加其他模块的最小储存。如果模块可以任意重新处理，则无法预先确定某个模块的最大功率是多少。

示例：

每个臂关节需要5A电流，因此，如果他们中的六个关节串联成一个臂，第一个模块需要能够承受30A。

电源可以有电池或其他储能系统，并可以与电源管理系统协同工作，实现智能化。

6.2.3 模块说明的其他方面

对于每一种具有硬件部分的模块，都应该规定重要的特性或参数，示例如下：

- 运动学和动力学特性，例如，几何参数、质量、质心、转动惯量和坐标变换；
- IEC 60529定义的防护等级（IP）。

如相关，应定义以下与操作环境相关的方面：

- 工作环境条件，如温度和湿度范围；
- 涉及与人接触的应用的生物相容性。

注：生物相容性问题包括细胞毒性、致敏性、刺激/皮内刺激，急性全身性毒性，亚慢性毒性，遗传毒性，植入型，血液相容性，慢性毒性，致癌性和生物降解性。

对于传感器和执行器，应该规定模块的具体特性，例如：

- 精度和分辨率；
- 传感器：灵敏度、传感范围、响应频率（如有）和内部坐标系中的位姿(如适用)；
- 执行器：精度、最大和额定功率/扭矩、最大和额定速度和内部坐标系中的姿态(如适用)。

7 模块设计的软件部分

7.1 总则

考虑到服务机器人系统中软件模块的特殊需求，本章描述了具有软件部分的模块的互操作性和复用性的设计的要求和指南。信息模型用于实现互操作性和复用性。因此，模块应具有合适的信息模型。由于模块的内部细节不在本文件的重点中，本章侧重于模块之间的接口，定义了模块的外部输入和外部输

出。由于具有相同功能的不同模块应是可互换的，因此需要通过规定应用层服务允许的通信模型以定义输入和输出模块的数据流类型。通信模型的示例包括发布/订阅模型、客户端/服务器模型、黑板共享内存模型(见表4)。机器人软件模块可以基于中间件框架进行开发，例如，包括ROS、OpenRTM，OPRoS和OROCOS。在第5章介绍了具有软件部分的模块的安全和安全性方面。

表4 不同用途的软件通信接口模型

序号	信息类型	支持信息交换模型	备注
1	数据	发布/订阅模型	数据可以通过一个或多个通信模型传输。数据在模块之间、集成开发环境(或工具)和模块之间进行交换。
		客户端/服务器模型	
		黑板共享内存模型	
2	包	客户端/服务器模型	在集成开发环境(或工具)和模块之间交换文件。

7.2 信息模型

7.2.1 通则

服务机器人系统中具有软件部分的模块应该提供软件接口，用以访问输入/输出数据、调用服务或处理事件。因此，软件组件在内部提供一些功能，使得数据可以通过通信API或消息格式进行修改，或者调用远程服务，并返回结果；在事件发生时，运行适当的进程，其中远程数据和远程服务由其他软件组件提供。

此外，具有软件部分的模块可以访问硬件组件，并能够读取模块的配置文件来初始化和正确地操作它们。可以直接或通过设备驱动程序或HAL。其中HAL允许软件模块访问硬件组件，而不需要修改模块的代码。

此外，提供消息格式用于软件的控制和维护，如文件的下载和上传(例如，软件、配置文件、应用程序包)，以及软件模块的执行控制(例如，启动、停止、暂停、恢复等)。

注：可以使用现有的规范来定义软件模块，例如，用于服务接口的OMG RoIS(机器人交互服务)或用于表示位置和坐标系统的OMG RLS(机器人定位服务)。

7.2.2 模块间的信息交换模型

模块应用于模块之间信息交换，而信息包括变量的值、服务的调用、事件的处理以及文件的内容，例如，软件组件的可执行代码、配置文件或包。变量、服务和事件定义于具有软件部分的模块中。变量类型分为周期变量和非周期变量，服务类型分为阻塞(同步)服务和非阻塞(异步)服务。

由于存在许多国际化的和事实上的通信协议，所以没有规定两个或多个具有软件部分的模块之间的协议。注意，对远程主机的远程访问是使用本章中的消息格式执行的，其由中间件提供。该中间件还可以支持本地主机中软件模块之间的信息交换。

注：本地主机和远程主机分别指目前已登录的作为软件模块的计算模块和软件通过通信协议想要连接的其他计算模块。

具有软件部分的模块之间的信息交换模型应支持以下内容：

- a) 读写数据；
- b) 调用服务；
- c) 事件注册和处理；

d) a) 至c) 项要求的服务质量(例如,与安全相关的值、实时特性、安全性)。

实时情况下的响应时间应该包括总体数据传输和服务调用时间。

在其他软件模块的实例中,模型应该至少支持以下一种优选的数据读写方法:

- 有响应的请求、无响应的请求;
- 订阅/发布;
- 黑板(通过共享内存)。

制造商可以采用其他方法,但互操作性要求应在模块模板中提供。

模块制造商应设计信息交换的消息格式,以满足以下要求:

- 支持中间件;
- 支持两个或多个中间件之间信息交换的编/解码规则;
- 支持信息7.2.3、7.2.4和7.4.2中规定的子条款。

7.2.3 属性访问模型及其访问

一个具有软件部分的模块应使用其属性值,以保证模块正确执行,以及其初始化值的设置其初始化值。该模块应具有以下属性:

- a) 模块的制造商信息;
- b) 执行环境,例如,OS类型、执行类型(周期性、偶发、非实时、实时等)、执行类型为周期性的环境执行周期等;
- c) 支持的通信方式(例如,发布/订阅、客户端/服务器、黑板等);
- d) 安全性级别(机密性、完整性、身份验证、密钥中的位数);
- e) 安全相关信息(例如,要求的PL或SIL标识)。

此外,该模块应该具有以下属性:

- f) 外部提供的(阻塞或非阻塞)服务调用;
- g) 外部提供的信息;
- h) 正确执行必要的初始值;
- i) 确保模块运行和安全的相应的软硬件要求。

如果一个模块需要一个特定的事件序列和/或命令被正确初始化,或者如果模块需要一个特定的开关事件序列,模块应管理这些序列,例如,监督模块。

示例1:

在机器人系统的上面部分开始运行之前,所有的车轮模块都要进行正确的运行。

示例2:

在激光传感器模块或相机模块用于安全导航之前,应该初始化并运行。

服务机器人级上的序列需要由系统集成商实现和配置,并且可以由模块控制(例如,监督模块)。

具有软件部分的模块应提供读取配置文件,并根据配置文件的内容设置软件组件的属性和将修改的规定属性写入至具有特定属性的配置文件的功能。模块应使用模型定义的功能读取配置文件来初始化软件组件,提供软件组件的服务,并访问存储的数据。该模块应该支持以下:

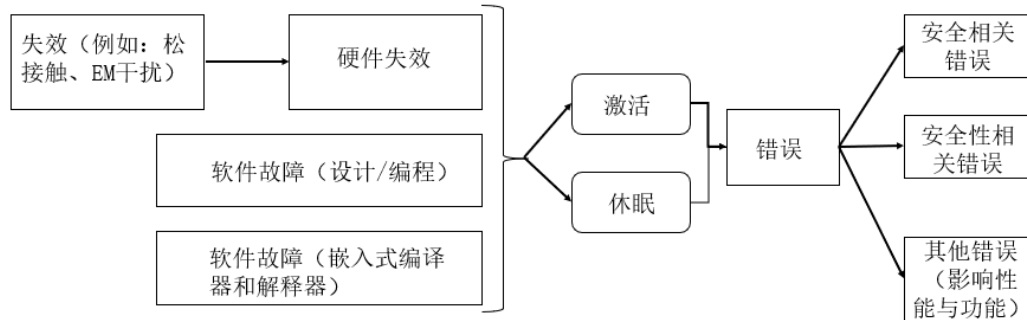
- 设置属性值;
- 获取属性值。

7.2.4 错误处理和恢复模型

模块中的错误会导致服务机器人故障或非正常运行。这些错误会导致机器人服务陷入危险状况。为避免这种场景发生，应尽快发现故障，并确保故障得到纠正，防止出现危险状况。

注1:错误是故障的外显表示。

将故障分为与安全有关的故障和与安全无关的故障，如图4所示，可以通过安全/安全性管理器进行管理。注意，根据应用程序和运行环境，与安全相关的故障可能是由安全无关的故障产生的结果。



注：错误可能由硬件或软件故障导致，后者有硬件失效导致。失效可以是休眠的，并不影响系统的运行，直至由某些因素激活，例如，系统状态的特殊联合。

图4 安全相关与非安全相关的失效

具有软件部分的模块处理错误应该支持以下方式来处理和恢复错误状况：

- 向/自外部模块(见图6)发送和接收错误状态和错误恢复数据，例如，安全管理器模块；
- 错误分为“安全相关错误”、“安全性相关错误”和“其他错误”，由应用规定；

注2:非安全错误包括在其他错误中。

- 支持执行生命周期内(见图6)的安全(见7.3)；
- 提供未知错误的处理方法。

模块设计人员应该根据错误的类型定义适当的反应。对于与安全相关的错误，可以要求将错误迅速反馈给系统层(例如，安全管理器模块)。此外，与安全性相关的错误应在系统层上处理(例如，安全性管理器模块)。其他错误在尽可能低的层次上处理(例如，模块本身)。

用于识别和处理错误的模块应具有足够的可靠性。此类模块的性能级别至少应与处理错误相关的任何安全功能所需的性能级别一样高。

如果有两个或更多的外部模块能够处理相同的错误，这些模块应该设置优先顺序以发送响应/命令至错误。

7.2.5 软件模块的互操作性

模块应该能够与不同制造商开发的模块进行通信和交互。

为保证服务机器人模块之间的有效互操作性，应在模块数据表中提供以下项目：

- a) 模块间需要交换的信息(见7.2.2)；
- b) 模块管理信息(见7.4.2)；
- c) 模块属性配置文件中使用的信息(见7.2.3)；和
- d) 错误处理和恢复信息(见7.2.4)。

为保证服务机器人模块之间有效的互操作性和复用性，应提供以下项目：

- e) 定义模块和中间件之间的信息模型(见7.2.2)。

为保证服务机器人模块之间有效的互操作性和复用性，提供以下项目：

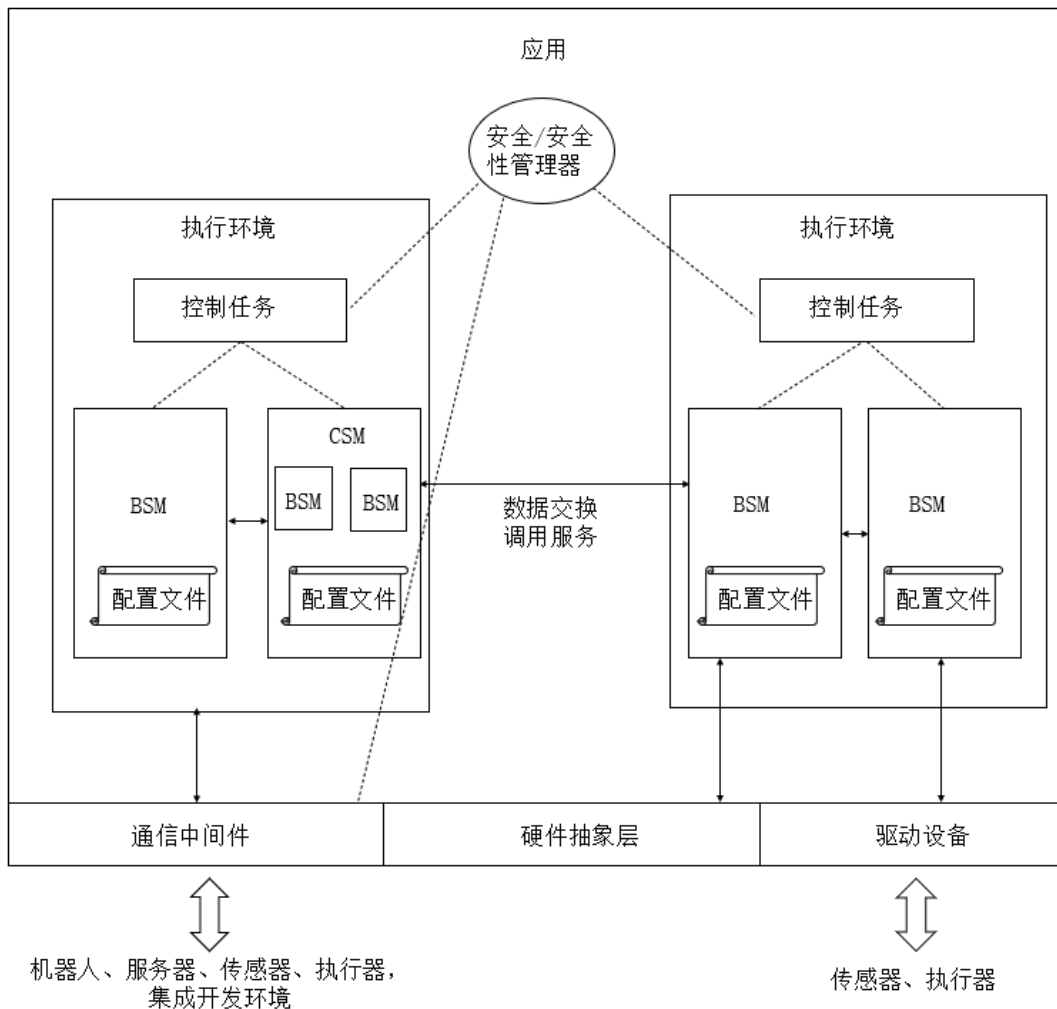
- f) 定义硬件抽象层或设备驱动程序的模型。

注：属性配置文件存储在配置文件存储库中。

7.3 软件模块的架构模型

7.3.1 通则

软件模块的架构模型应包括执行环境和控制任务。用于安全和安全性的模型应该包括安全管理器和安全性管理器。图5说明了软件模块及其相互关系，展示了若干相互连接的软件模块的示例。一些模块是基础软件模块，而另一些模块是复合模块，因为其可以分解为更小的模块。图5展示了两种执行环境，其本质上是独立的控制线程，可以托管或不托管在不同的处理器上。一个单独的安全和安全性管理器观察模块的整体行为，（该模块）通过硬件抽象接口/设备驱动程序和通信中间件与其他模块进行通信。安全或者安全性管理器作为独立的模块单独实现。安全管理器仅接收与安全相关的软件模块的相关数据。



说明：

BSM 基础软件模块

CSM 复合软件模块

----- 控制路径

图5 服务机器人模块化的软件框架结构

配置文件存储库管理模块使用的配置文件。

执行环境是由一个或多个软件模块和一个控制任务组成的元素。控制任务在执行环境中协调软件模块，并管理它们的任何实时约束。

应用是一个根据用户需要控制机器人系统的元素，由一个或多个执行环境组成。应用利用应用程序包，包括软件模块、初始化值和步骤以及用于执行应用程序的相关资源。

抽象机制，例如，硬件抽象接口，帮助软件模块访问与硬件依赖特性无关的硬件。软件模块可以通过抽象机制对相应的硬件进行读写，使得软件模块具有可移植性。模块包括使用抽象机制访问传感/执行部件的软件模块，通过抽象机制从设备获取数据并将数据传递给其他模块。

通信中间件使软件模块和软件组件进行信息交换。中间件可以监督与软件模块、组件和应用程序相关的文件，并根据需要从服务器和/或机器人上传/下载所需的相关文件。通信中间件可以根据表4中所示的信息交换模型在执行环境中实施。注意，本文件中没有定义中间件。

安全性管理器应管理软件模块间发生的安全性问题和根据需要，管理其他部分发生的安全性问题。例如，安全性管理器可以监控未经授权的用户访问等风险。

安全管理器应管理软件模块间发生的安全问题和根据需要，管理其他部分发生的安全问题。例如，安全管理器应监控软件模块的执行状态，检测是否违反了限制或如果机器人进入危险状态，（如果进入该状态）则将机器人带入安全状态。

7.3.2 软件模块的要求

具有软件部分的模块包括可执行代码和配置文件，其中配置文件存储模块属性值，以支持模块的正确执行。

示例1:

模块属性：版本号、OS类型、提供的服务方法、周期性执行等执行类型、偶发和非实时以及相关的硬件相关模块属性。模块属性值：初始化值、执行软件模块所必需的值，例如，OS类型，支持的通信协议，支持的服务类型和事件类型。

示例2:

基础软件模块：距离计算模块，其通过硬件抽象接口从适当的硬件读取测量到的距离数据（例如，超声波传感器、红外传感器或激光传感器），将数据转换成正确的标准格式，并将转换后的数据发送给其他软件模块。更复杂的模块示例是立体距离测量模块，或运行在从传感（相机）模块接收的图像流之上的目标检测模块。**示例3:**

一个复合软件模块的典型示例是操作软件模块，其由执行器控制模块、轴同步模块、逆运动学模块、路径规划模块等基础软件模块组成，示例见附件B。

软件模块的设计应满足以下要求：

- a) 支持通过已定义的信息模型与其他模块进行信息交换（见7.2.2）；
- b) 支持服务质量（例如，实时性）的条款规定；
- c) 具有唯一的标识符，并可获得正确操作和互操作性所需的模块属性值；

示例4:

软件模块案例的复用性、互操作性和可组合性的信息包括OS类型、通信协议类型、服务的接口类型和使用的数据类型。

- d) 为应用中的每个软件模块创建一个或多个具有唯一标识符的实例；
- e) 由管理其执行生命周期的控制任务控制，如图6所示；
- f) 支持依赖于软件模块可能出现的错误类型、模块属性配置文件以及与其他模块的连接情况的模块级安全；
- g) 如果模块能够访问外部模块，则支持模块级安全；

- h) 具有配置文件，其中包括7.2.3中定义的模块属性值；
- i) 支持软件平台独立性。

注1:本文件允许软件模块或模块内的软件组件在不同的操作系统下，通过不同的编程语言、不同的文档文件格式或数据库执行。

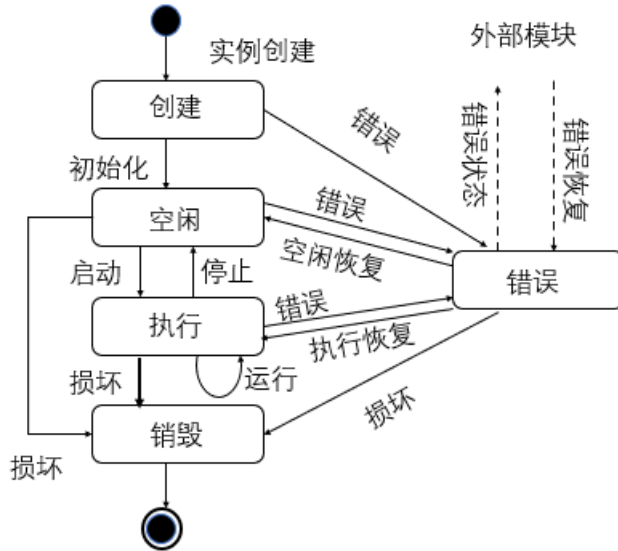


图6 包含错误处理的软件模块的执行生命周期

软件模块应符合图6所示的执行生命周期，该生命周期执行以下行为：当软件模块被创建时，模块进入“创建”状态。当软件模块初始化时，“初始化”事件发生。当事件“启动”发生时，软件模块的执行被启动。当事件“停止”发生时，软件模块的执行被停止，以及事件“运行”发生在每个给定的周期。当软件模块执行完成后从内存中卸载或被移除时，发生“损坏”事件。当软件模块的任何状态发生错误时，则引发事件“错误”。当错误在相应的创建、空闲或执行状态下被恢复时，会引发“空闲恢复”和“执行恢复”事件。尤其，有两种类型的事件，“空闲恢复”和“执行恢复”是为错误恢复运行设计的。注意，每个事件都会导致相关的功能被调用；实时模块定期执行“运行”事件执行相关功能。

注2:当与安全相关的软件模块处于“错误”状态时，与安全相关的错误导致与安全相关的故障被发送给其他外部模块，（这些模块）处理错误并返回正确的恢复值。外部模块一个示例是软件模块或能够处理错误以避免进入危险情况的模块。典型的案例如图5所示的安全管理器。

对于控制系统安全相关部分的错误处理，错误恢复程序(尤其是执行恢复)应遵循GB/T 15706 和ISO 14118，以防止意外启动造成的危害。

7.4 具有软件部分的模块的安全/（信息）安全相关要求

7.4.1 通则

安全相关软件模块按照第5章进行设计。与网络安全有关的模块的安全性详见5.7至5.10。本子条款描述了安全/安全性管理器模块(见图5)，用于管理模块内部无法处理的安全/安全性问题。注意，安全/安全性管理器模块可以作为一个集成模块实现，也可以作为两个独立模块实现，即安全模块和安全性模块。模块也可以采用冗余架构，以满足相关的PL/SIL。

安全性管理器模块是一个管理机器人及其模块安全性的模块，可以设置或执行安全性策略以管理对安全性问题的响应。注意，当一个模块与外部模块交换数据时，如值和文件，可能会出现安全性问题或

者未经授权的用户在没有得到有效许可的情况下获得了访问机器人的权利等。当一个模块与外部或内部模块交换数据时，通过加密、认证等适当的网络安全措施，相应的数据不应被窃听或修改。当机器人外部的消息发送者下载程序或配置文件或接收控制命令时，消息发送者的授权由安全/安全性管理模块监控。

7.4.2 与安全/安全性管理器模块的交互

安全相关模块应向安全管理器模块提供以下信息，以处理模块化软件安全：

- 模块提供的错误信息；
- 模块接收到的错误恢复信息。

安全管理器模块应综合处理从各安全相关模块收到的错误信息，并提供信息对各模块进行停止或安全操作。停止操作可分为停止机器人操作和停止与特定事件相关的模块操作。停止和重启应遵循适用的安全标准，例如，GB/T15706（通用）、GB/T 5226.1（停止）和ISO 14118（启动）。

当一个模块使用通信方法与外部或内部模块交换数据时，应该对完整性和身份进行验证。特别是，在外部开发/监控工具和服务器之间进行通信时，应该验证其完整性和身份。在使用不支持安全性的现场总线的情况下，物理安全性应该保证只有经过授权的用户才能对现场总线进行物理访问。此外，网络安全应在必要时保证以下数据的传输：

- 包、软件模块及其配置文件；
- 各软件模块执行状态的控制；
- 模块的输入和输出数据。

安全性管理器应与安全管理器一起协作，即使机器人因服务攻击的拒绝或其他类似问题而无法与外界通信，其也可以按照机器人自身的策略操作。因此，安全/安全性管理器模块应具有以下功能：

- 如果安全管理器发现安全性问题，安全性管理器将安全信息发送给安全管理器；
- 安全管理器根据预先设定的安全策略控制模块。

8 使用信息

8.1 总则

模块制造商应充分提供与其模块相关的文件，以便第三方可以根据提供的文件使用模块（例如，集成到一个更大的系统中，或创建与所提供的模块交互操作的其他模块）。模块制造商应提供模块所符合的标准清单，以及这些标准所要求的文件。本章包含支持模块化的附加文件的要求。

服务机器人集成商应提供服务机器人系统用户完整的机器人使用信息，应包括以下内容：

- 提供整个系统的手册；
- 在机器人上增加或更换警告标志及其他标记和指示；
- 提供一个系统构成图规划，该构成图规划展示显示了组成机器人的所有模块的连接。

服务机器人集成商应向服务机器人系统的用户提供机器人中每个模块的使用信息。。

服务机器人集成商应在其文件中说明用户允许对服务机器人系统进行哪些修改（例如，模块交换）。

使用信息由正确使用模块以执行模块预期任务的信息组成。用户可以是（但不限于）机器人制造商、模块设计人员、模块测试人员或参与模块维护的人员。

标识、符号和书面警告应易于理解和明确，以提供模块的详细信息。对于基础模块，信息应包括模块类型（输入、计算、处理、基础设施和输出）。对于复合模块，应该提供使用不同基础模块和通用模块的详细信息。

象形图之类的符号可用于明确表示的警告或说明操作环境。所有的印刷标记都应清晰易读，经久耐用。有关安全的标识应遵循现有安全标准的要求和原则。如果可能的话，优先使用象形图而不是书面警告，以方便在不同区域使用该模块。

模块制造商应同时提供打印版本和电子版本的使用信息，并考虑人为因素和文件的可用性。

模块的描述应使用附录A中规定的机器人模块模板。模板中未包含的其他信息在可能的情况下应以类似的格式显示。

如果提供指示，应在模块上或模块的文件中用标识来描述。

8.2 标识或指示

模块上的标识应是在模块外部可识别的图案。标识应根据需要尽可能详细，但至少应包括模块供应商的名称或等效标识、模块的型号或编号和正常使用的标识，包括在已发布的相关安全标准中要求的所有标识或指示。

对于具有硬件部分的模块，标识应可见、易读和耐久，并至少应包括以下：

- 制造商的名称；
- 序列号；
- 安全和（信息）安全认证标识，如适用。

软件模块至少应在其文件中包含以下信息，如用户手册或用于分发软件模块的电子存储媒介上的文本文件：

- 制造商的名称；
- 软件模块类型和版本号；
- 操作系统类型；
- 序列号。

8.3 用户信息

应项用户提供模块信息以便正确和可预期使用的模块用户信息。用户信息应包括以下：

a) 模块的详细描述：

- 模块的使用说明，
- 所包含的基础模块和/或复合模块的简要说明，
- 具有硬件部分的模块的描述，
- 制造商的名称和联系方式、制造商的国家，
- 模块类型和版本号，
- 模块中包含的内部连接特征（连接器的方向，插针分配等），
- 编号，如果需要，
- 电源的额定参数（例如，电源电压或额定范围（DC/AC），额定频率（如必要），气压等），
- 额定功率（瓦特）或额定电流（安培），
- 通信类型，如果使用，
- 安全认证标识，如果合适，
- 安全性特征，如果合适，
- 质量（kg）和三维尺寸（mm），
- 具有软件部分模块的描述，
- 制造商的名称和联系方式、制造商的国家，

- 模块类型和版本号，
- 操作系统类型和详细信息，
- 编号，如果需要，
- 模块的使用检查清单。例如，适合该接口的模块类型、支持的硬件模块（例如，适当的机械/电气接口）或兼容的软件模块，
 - 模块运行环境，
 - 软件模块的安装方法（如有），
 - 连接其他模块的详细信息；
 - 第4章所列的模块需要符合的原则；
- b) 合适的应用案例，包括其安全和（信息）安全相关信息；
- c) 模块属性值的设置和调整细节；
- d) 可更换的基础模块和复合模块列表（如有）；
- e) 已知故障或错误列表；
- f) 电池充电方法，如果相关；
- g) 模块的搬运信息，详细说明抓取点和搬运点；
- h) 消耗品清单及其维护周期。

在集成模块时，维护安全功能所需的与安全相关的信息，如果合适，应该以结构化和明确定义的格式提供。

8.4 服务信息

服务信息应包括维护模块正确操作的说明，详细说明需要特定技术知识或专业技能的任务，这些任务需要由适当的人员（例如，维修人员、专家等）执行。

服务信息应包括以下：

- a) 模块的详细描述及其维护要求；
- b) 适当的物理操作环境信息（例如，视觉模块的光照强度、大气中的污染物、极端温度等）；
- c) 相关信息（如适用）：
 - 设置、维护计划和额定运行参数说明，
 - 检查维护的操作流程，
 - 检查频率，
 - 模块功能测试的频率和方法，
 - 调整、维护和维修的指南，
 - 推荐的具有硬件部分模块的备件清单，
 - 所需和提供的工具清单；
- d) 详细的机械图和电气框图；
- e) 已知错误、误差列表及其描述；
- f) 消耗品清单及其维护周期。

附 录 A
(资料性)
机器人模块模板

A.1 通用模板

本文件介绍了各种各样的模块，为了统一，模块描述应遵循一个通用的模块模板，以便形成规范的格式。表A.1所示为机器人模块模板，制造商应使用该模板来描述其模块的详细信息。表A.1中斜体部分表示模板各部分应包含的信息。制造商应该使用该模板来描述其模块的详细信息。如合适，也可提供其他信息。

表A.1 机器人模块模板的标准描述

模块名称： <i>特定模块或模块类的自然语言名称。</i>
描述： <i>模块概述、模块是什么、模块用途以及如何预期应用场景中使用：描述机器人模块的应用场景，以便在必要时可以执行验证测试。</i>
制造商： <i>模块开发人员的联系信息。包括设计人员、制造商或供应商的详细信息。</i>
模块ID： <i>制造商唯一的模块产品参考编号</i>
示例： <i>模块的典型使用案例</i>
硬件部分： <i>关于硬件部分的概要细节，见第6章(如果可能，通过示例表示)</i>
软件部分： <i>关于软件部分的概要细节，见第7章(如果可能，通过示例表示)</i>
模块属性： <i>模块属性列表(见第6和7章)</i>
输入： <i>模块输入列表</i>
输出： <i>模块输出列表</i>
功能/功能性： <i>模块接受输入并处理输入以确定输出的一种描述。推荐使用合适的图表来说明功能(例如，附录C中给出的线、圆或SysML方法)。</i>
基础设施： <i>所提供的infrastructure支持和/或环境保护的类型(例如，电线、数据库管理系统、具有或不具有安全/安全性措施的数据总线、IP保护等)</i>
安全： <i>模块级和系统级安全的安全相关要求(例如：满足要求的性能水平)(见 5.1-5.3 条)</i>
安全性 <i>模块级和系统级安全性的安全性要求(例如，防止未经授权的访问，或保证适合的隐私水平等)。该安全性要求应该包括硬件和软件部分。(见5.1、5.4-5.7条)</i>

建模:

应用于各种测试场景的模块的数学或物理描述 (例如, 虚拟模块模型)

A.2 机器人模块模板的特定硬件扩展

常用模板说明见表A.1; 表A.2给出了具有硬件部分的模块应该提供的附加信息。

表A.2 具有硬件方面模块的附加信息

属性:
具有硬件部分的模块的属性列表, 例如, 物理尺寸, 接口类型, 机械和电气特性。
输入:
输入列表, 例如, 数字/模拟传感器和控制信号, 以及模块之间的其他通信等。
输出:
输出列表, 例如, 数字/模拟输出, 角度/位置/速度/扭矩输出等。
功能性:
对于具有硬件部分的模块, 这主要与互换性和互操作性有关。建议将模块按照功能视角进行划分, 例如, 其内部元素/结构、与外部模块的连接性以及包括人在内的操作环境中的相关特性。
基础设施:
基础设施要求: 模块对系统其他部分的要求, 例如, 可用电力, 结构支撑、散热等。
环境约束: 当关闭和运行过程中, 模块对外部条件的限制, 例如, 温度、湿度、最大允许的机械冲击等。
建模:
模块动力学应用于各种目的的数学或物理描述, 例如, 性能模拟, 功能评估和场景确认。

附录 B
(资料性)
机器人模示例

B.1 具有硬件方面模块的示例

B.1.1 旋转驱动关节

<p>模块名称： 旋转驱动关节</p>
<p>描述： 模块化机器人关节连接两个连续的连杆，并提供一个旋转自由度的运动。模块化关节由电机、减速齿轮、电源线、信号线和控制电路组成。该关节由电力驱动。关节可以通过内部传感器感知其转动角度和扭矩。</p>
<p>制造商： ISO Inc.</p>
<p>模块ID： Joint J001</p>
<p>示例： 该关节可用于移动传感器，也可与其他关节(例如，6或7个自由度)组合形成操作机。</p>
<p>硬件部分： — 001B型法兰两端与电源连接器、CAN总线、安全扭矩开关连接 — 集成电子设备的USB直接接入的服务端口 — IP等级：IP 54</p>
<p>软件部分： 通信协议：CANOpen</p>
<p>模块属性： — 尺寸：Ø80 mm × 70mm — 重量：1.2 kg — 减速比：1:30 — 关节范围：±270° — 最大关节速度：90° /s — 最大扭矩：100Nm/20Nm 向前/向后 — 关节刚度：最大负载时，最大位移0.5 mm/1° — 额定扭矩：10Nm — 连接器额定电流：10A — 功耗：50W — 准确性：±0.5° — 重复性：±0.3° — 限制[扭矩(Nm)，位置(rad)，速度(rad/s)]</p>
<p>输入： — 位置(rad)、速度(rad/s)、扭矩(Nm)指令 — 安全功能的信号 — 控制相关参数</p>
<p>输出：</p>

<ul style="list-style-type: none"> — 实际位置(rad)、速度(rad/s)、扭矩(Nm) — 状态、警告、错误、电流、电压、温度、诊断信息
<p>功能性:</p> <p>该关节可用于位置模式、速度模式或力模式。其可以设置为当超过限制时,提供警告并进入停止模式(无安全功能)。</p> <p>内部构形(CAN ID、限制等)可以通过USB访问</p>
<p>基础设施:</p> <ul style="list-style-type: none"> — 电源: 24V dc (18V - 30V)、50W — 操作条件: +5℃至 +35℃。湿度< 90% 不凝结
<p>安全:</p> <ul style="list-style-type: none"> — 按照IEC 61800-5-2提供安全功能。 — 为了保护模块(无安全功能),当出现以下情况时,模块停止并进入错误状态:过载(机械、电气)故障、编码器传感器故障、过热。 <p>仓库物流服务机器人的电源应进行验证,检查电源是否符合可集成性、互换性、安全性等基本原则。</p>
<p>安全性:</p> <p>法兰001B和USB端口的盖子需要标准的工具访问。</p>
<p>建模:</p> <p>参见运动学和动态模型的模型文件。静态模型参数包括保持力矩、额定力矩和失速力矩;动态模型参数包括速度、加速度和带宽。</p>

B.1.2 电源

<p>模块名称:</p> <p>电源电池模块</p>
<p>描述:</p> <p>带电源管理系统的电池模块,提供24V DC输出。</p>
<p>制造商:</p> <p>ISO Inc.</p>
<p>模块ID:</p> <p>Power supply P001</p>
<p>示例:</p> <p>该电源可用于移动机器人平台或外骨骼上</p>
<p>硬件部分:</p> <p>电源连接器(2 pin)</p> <p>数据I/O连接器(4 pin)</p> <p>IP等级: IP65</p>
<p>软件部分:</p> <p>通讯协议:RS232, 电池管理软件包括报警</p>
<p>模块属性:</p> <ul style="list-style-type: none"> — 额定规格: 24V, 5A 连续, 最大 20A。 — 容量:5Ah — 电源输出:25V(满载)、21V(电源管理开关断开) — 充电:28V至35V, 输入电流达5A
<p>输入:</p>

充电电源输入 电池开/关
输出： 功率输出 电池错误
功能性： 电池需要通过数字输入接通电源。数字信号输出低电量警告和错误。
基础措施： —操作条件:+5℃至+35℃。湿度< 90%，不凝结。
安全： 为了保护模块(无安全功能)，在以下情况下，模块停止并进入错误状态:过载、过热、低电量、过度放电。
安全性： N/A
建模： 请访问网站(通过提供URL链接)下载用例场景的行为模型。

B.2 具有软件部分模块示例

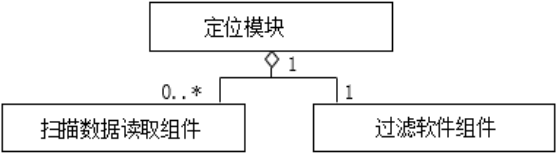
B.2.1 识别

模块名称： 视觉识别模块
一般描述： 该模块可用于人脸识别。通常构建一个数据库包含于某增强的人脸识别模块中。在动态模块中，硬件（例如，摄像头和3D扫描仪）被用来提供一个动态数据流。模块的结果各不相同，例如，数据库中给定目标数据与注册的数据之间的匹配比例，或数据库中ID号或名称的最佳匹配
制造商： ISO Inc.
模块ID： VRM0001
示例： 人脸识别
硬件部分： 无
软件部门： 获取数据(输入图像)、人脸识别、输入结果(已识别人脸的名称)
模块属性： — 数据库位置，例如：路径、IP和端口号或URL — 使用的识别类别，例如，眼睛、正面脸、全身、上半身等 — 图像大小(像素) — 每秒图像帧数(如果输入的是一种动态图像)
输入： 图像或图像流
输出：

<p>按规定的置信(或准确性)进行视觉识别的结果,例如,已识别的人的姓名,如James, Eve, Adam等(在人脸识别方面)</p>	
<p>功能/功能性:</p> <ul style="list-style-type: none"> —— 从摄像头模块获取图像(或图像流)数据,用于人类识别; —— 从图像数据中检测人脸;拍下带有ID号的人脸照片;提取人脸特征点;计算它们之间的距离; —— 从数据库中找到与此计算值最接近的人脸照片(或人脸特征点);返回所选人脸照片的ID号 	<pre> classDiagram class 视觉识别模块 class 人脸识别模块 class 图片感知读取模块 视觉识别模块 "0..1" o-- 人脸识别模块 视觉识别模块 "1" o-- "1..*" 图片感知读取模块 </pre>
<p>基础措施:</p> <p>中间件、数据库</p>	
<p>安全:</p> <p>不适用于预期的用例场景</p>	
<p>安全性:</p> <p>出于隐私的身份验证、数据库机密性</p>	
<p>建模:</p> <p>不适用</p>	

B.2.2 定位

<p>模块名称:</p> <p>定位模块</p>
<p>描述:</p> <p>个人机器人必须知道其在参考坐标系中的位姿(位置和方向),该过程称为定位。定位模块使用激光扫描模块来获得姿势。</p>
<p>制造商:</p> <p>ISO Inc.</p>
<p>模块ID:</p> <p>ID由制造商提供</p>
<p>示例:</p> <p>基于激光扫描的定位</p>
<p>硬件部分:</p> <p>无</p>
<p>软件部分:</p> <p>获取数据(输入图像)、计算、与参考(如地标)等进行比较,通过过滤软件过滤姿态</p>
<p>模块属性:</p> <ul style="list-style-type: none"> — 模块所使用的感应模组数目及类型(例如,激光扫描仪的角度及光束数目等) — 地标、地图信息或危险区域信息的位置,例如,路径、IP和端口号或URL
<p>输入:</p> <p>扫描数据(来自激光扫描模块)</p> <p>来自车轮控制模块的运动数据,例如,移动距离和朝向</p>
<p>输出:</p> <p>机器人置信(或精度)的姿态</p>

<p>功能/功能性:</p> <ul style="list-style-type: none"> —— 从激光扫描模块获取数据; —— 从车轮控制模块获取数据; —— 使用数据和过滤器获得姿态估计; —— 将估计值与参考姿态进行比较; —— 更新姿势 	 <pre> classDiagram class 定位模块 class 扫描数据读取组件 class 过滤软件组件 定位模块 o-- "0..*" 扫描数据读取组件 定位模块 o-- "1" 过滤软件组件 </pre>
<p>基础措施:</p> <p>中间件</p>	
<p>安全:</p> <p>当机器人进入危险区域时, 按适用标准进行警告或停止</p>	
<p>安全性:</p> <p>身份验证</p>	
<p>建模:</p> <p>不适用</p>	

B.3 通用复合模块示例

B.3.1 通则

所有服务机器人都具有可确定的高级功能。这些功能包括人机界面、导航和定位、操作、从一个地方到另一个地方的移动, 并根据适用的安全标准确保安全。机器人模块通常可用于复合模块, 实现此类典型的高级功能。本条款给出了之前没有讨论过, 但被认为对实现各种服务机器人应用很重要的更高级别的模块。

复合模块是包含机械、电子和软件部件的模块的组合。这些模块通常具有更复杂的属性, 例如, 具有多个自由度的模块化操作机和集成控制器、执行器、传感器、控制软件、安全功能等。

对于任何复合模块, 模板中显示的最少功能应该在模块的属性配置文件以及模块的输入和输出定义中进行规定。输入和输出通常是模块之间数据通信。每个常用模块的模板应该提供一个简要概述和最少规范。此类模块的制造商可以根据需要增加更多的功能。

B.3.2 操作机模块

操作是一个复杂的运动, 涉及不同层级的模块化, 例如, 单个关节控制, 与移动的协调操作和使用不同的末端执行器。

<p>模块名称:</p> <p>操作机模块</p>
<p>描述:</p> <p>通过关节连接形成的末端执行器操作的铰接系统的刚性连接部件的组合, 所有部件均用定义的机械接口连接。如果制造商的预期在协作应用中使用一个模块, 那么设备中可能需要附加安全相关功能, 例如, 对待老年人或在专业环境中。</p>
<p>制造商:</p> <p>联系信息</p>
<p>模块ID:</p> <p>制造商对此模块构形的唯一产品参考编号</p>
<p>示例:</p> <p>一种6自由度的机器人操作机, 其末端可附着二个2根手指的末端执行器。模块化设计使用户可以重新配置操作机, 使其具有4-7个自由度, 以满足规定要求。本示例中的操作机具有一个超声波传感器, 能够检测距离20cm以内的物体。</p>
<p>硬件部分:</p>

<p>—— 支座、外壳、电机、机械接口</p>	
<p>软件部分：</p> <p>—— 运动学模块；</p> <p>—— 通信协议的执行；</p> <p>—— 手臂控制模块；</p> <p>—— 关节控制协调模块</p>	
<p>模块属性：</p> <p>—— 自由度：关节类型(2D、3D、旋转/棱柱)，操作机构形；</p> <p>—— 关节范围：运动范围，运动误差；</p> <p>—— 连接关节的连接模块的长度和位置(或类型)；</p> <p>—— 一定姿态范围下的有效载荷：静态和动态条件下末端执行器允许的重量(kg)或力(N)；</p> <p>—— 手臂相对于手臂参考的操作范围(m × m × m)；</p> <p>—— 末端执行器的最大速度(m/s)和加速度(m/s²) (可能取决于姿态)</p>	
<p>输入：</p> <p>制造商应定义一个指令的枚举列表，例如：</p> <p>—— 根据姿态和速度指令操作位置；</p> <p>—— 移动到四元数指定的空间姿态；</p> <p>—— 末端执行器的力/速度限制</p>	
<p>输出：</p> <p>定义为x, y, z(米)的实际空间姿态和朝向的四元数</p> <p>—— 末端执行器的实际空间速度；</p> <p>—— 实际和投影的空间包络线；</p> <p>—— 单个关节的实际速度、加速度和力(扭矩)(m/s, rad/s)；</p> <p>—— 操作状态、警告、错误、实际电流、电压、温度</p>	
<p>功能/功能性：</p> <p>—— 正运动学、逆运动学、运动规划、动力学；</p> <p>—— 启动/停止运动(启用、禁用)；</p> <p>—— 过载检测、状态检测(OK/error)、制动/保持、使能/禁用功能；</p> <p>—— 供给、停止、中心位置接口；</p> <p>—— 提供设置/获得力/扭矩、设置/获得位置、基于抽象接口设置/获得速度接口；</p> <p>—— 如果需要，定期向所有关节发送力/扭矩值；</p> <p>—— 为了提高性能，由轨迹发生器预测运动和包络线</p>	
<p>基础措施：</p> <p>—— 连接/关节框架提供机械支持；</p> <p>—— 附加在夹具上快速锁；</p> <p>—— 电源；</p> <p>—— 通信总线；</p> <p>—— 操作机的本地和/或分布式控制器</p>	
<p>安全：</p> <p>如第5章所述，该模块遵循适用的安全标准(例如，IEC 61508-3或IEC 60204-1)。</p> <p>模块的保护性停止功能符合ISO 13849-1的PL d要求。</p>	

<p>模块安全:模块提供以下安全功能</p> <ul style="list-style-type: none"> —— 碰撞力限制达PL b(敏感皮肤); —— 过载限制; —— 速度限制控制按照ISO 10218规定的关于速度控制系统安全:该模块提供了以下与安全相关的信息: —— 模块状态; —— 为了减少碰撞风险(PL a), 由轨迹发生器预测运动和包络线; —— 在3D空间中以额定速度计算制动距离; —— 设置末端执行器速度; —— 可能导致主要故障或性能下降的内部错误的规定
<p>安全性: 该模块可以提供以下一个或多个安全性功能</p> <ul style="list-style-type: none"> —— 所有模块间通信遵循第7条章提出的准则; —— 使用错误检测机制的所有输入; —— 仅接受授权供应商的目标输入; —— 运动指令信息的使用, 包括授权
<p>建模:</p> <ul style="list-style-type: none"> —— 操作机的静态和动态虚拟模型, 包括末端执行器、关节动力学和包络线

B.3.3 移动平台模块

移动性是一种复杂的运动, 可以涉及不同层级的模块化, 例如, 不同的运动构形、不同的移动行为以及与移动相关的协调操作。

<p>模块名称:</p> <p>移动平台模块</p>
<p>一般描述:</p> <p>运动模块, 包括:</p> <ul style="list-style-type: none"> —— 运动系统包含悬架系统、转向系统, 驱动机构系统; —— 有效负载舱; —— 运动方式: 传统轮式、全轮式、球轮式、各种腿式和腿式构形、混合运动方式、攀、爬、游泳等。
<p>制造商:</p> <p>联系信息</p>
<p>模块ID:</p> <p>制造商对该模块构形的唯一产品参考编号</p>
<p>示例:</p> <p>装有紧急按钮, 激光测距仪和缓冲器的轮式移动底座</p>
<p>硬件部分:</p> <ul style="list-style-type: none"> —— 执行器模块; —— 缓冲器模块; —— 电池模块 ; —— 移动底座控制硬件 —— 激光测距模块; —— 结构件模块; —— 硬件方面的通信模块;
<p>软件部分:</p> <ul style="list-style-type: none"> —— 移动底座控制软件 ; —— 位置感知软件; —— 通信软件 ; —— 执行器控制模块; —— 触摸感应软件; —— 协调模块;

<p>—— 电池管理模块;</p>	<p>—— 安全管理器</p>
<p>模块属性:</p> <p>—— 机械配置: 车轮类型/数量、车轮布置和构形及总体尺寸;</p> <p>—— 有效负载: 在规定的条件下(例如, 质量、尺寸、温度等)可携带的负载限制;</p> <p>—— 移动速度: 在可预见的工作场景下的最高速度、直行、转弯、平/斜坡、空载、满载;</p> <p>—— 空载状态下的重量、重心(COG);</p> <p>—— 空载和满载条件下的最大坡度角和最大台阶高度;</p> <p>—— 全服务下的电池持续时间和充电时间</p>	
<p>输入:</p> <p>制造商应该提供一个用于移动模块的指令枚举列表:</p> <p>—— 运动速度和方向;</p> <p>—— 控制相关参数: 地面条件、障碍和环境;</p> <p>—— 障碍检测(数字和/或模拟);</p> <p>—— 保护性和/或紧急停止</p>	
<p>输出:</p> <p>定义为x, y, z(米)的实际空间姿态和朝向的四元数</p> <p>—— 电机转动信息: 方向、角度;</p> <p>—— 加速、电机扭矩/电流;</p> <p>—— 状态(OK/error), 警告, 电流, 电压, 温度;</p> <p>—— 错误、安全相关的运行条件;</p> <p>—— 安全相关性能水平(PL水平取决于建议的用例应用);</p> <p>—— 非安全超声波近程障碍检测;</p> <p>—— 障碍检测状态;</p> <p>—— 夹持检测状态;</p> <p>—— 保护性和/或紧急停止状态</p>	
<p>功能/功能性:</p> <p>—— 局部运动控制和运动学;</p> <p>—— 启用/禁用功能;</p> <p>—— 紧急制动;</p> <p>—— 内部模块状态检查;</p> <p>—— 电源和电池管理</p>	
<p>基础措施:</p> <p>—— 提供机械支持的底盘框架</p> <p>—— 电源干线;</p> <p>—— 通信</p>	
<p>安全:</p> <p>如第5章所述, 该模块遵循适用的安全标准(例如, IEC 61508-3或IEC 60204-1)。</p> <p>—— 在配置系统的规定速度下可选择的停止距离;</p> <p>—— 机器人提供集成安全电路以连接与安全相关的传感器和模块;</p> <p>—— 模块提供的每个安全功能 PL a to e;</p>	

<p>—— 模块提供的性能级别：紧急停止(PL d)、保护性停止输入(PL d)</p>
<p>安全性： 所有模块对模块的通信应遵循第5章中提出的原则</p> <ul style="list-style-type: none"> —— 错误检测机制以保证通信数据的完整性； —— 目标位置仅接受来自授权供应商/模块； —— 运动指令必须包括授权使用信息
<p>建模： 移动平台的虚拟静态和动态模型</p>

B.3.4 人机交互模块

人机交互(HRI)模块为人与机器人交互提供了一种方法，使人能够了解机器人的意图，并向机器人提供指令或信息。

<p>模块名称： 人机交互模块</p>
<p>描述： HRI模块具有以下功能：</p> <ul style="list-style-type: none"> —— 检测/识别某人； —— 通过语音、声音、光线、触摸屏与人(用户)交互
<p>制造商： 联系信息</p>
<p>模块ID： 制造商对此模块构形的唯一产品参考编号</p>
<p>示例： 仅语音消息和信息被发送给第一次被摄像头识别与确认的用户。</p> <ul style="list-style-type: none"> —— HRI模块包含人脸识别模块、扬声器模块等子模块； —— 协调软件模块用于管理子模块的接口或数据的顺序； —— TTS模块将文本翻译成语音； —— 指示状态和预期运动的灯
<p>硬件部分：</p> <ul style="list-style-type: none"> —— 扬声器模块； —— 触屏； —— 灯
<p>软件部分：</p> <ul style="list-style-type: none"> —— 协调软件模块； —— TTS软件模块； —— 触屏交互软件； —— 人脸识别/确认模块
<p>模块属性：</p> <ul style="list-style-type: none"> —— TTS软件模块、在扬声器上播放的消息格式； —— 人脸识别模块、数据库格式； —— 触摸屏的API； —— 状态和错误信息； —— 工作条件，例如，环境温度、湿度范围
<p>输入：</p> <ul style="list-style-type: none"> —— 在扬声器中播放的消息； —— 用户从触摸屏输入

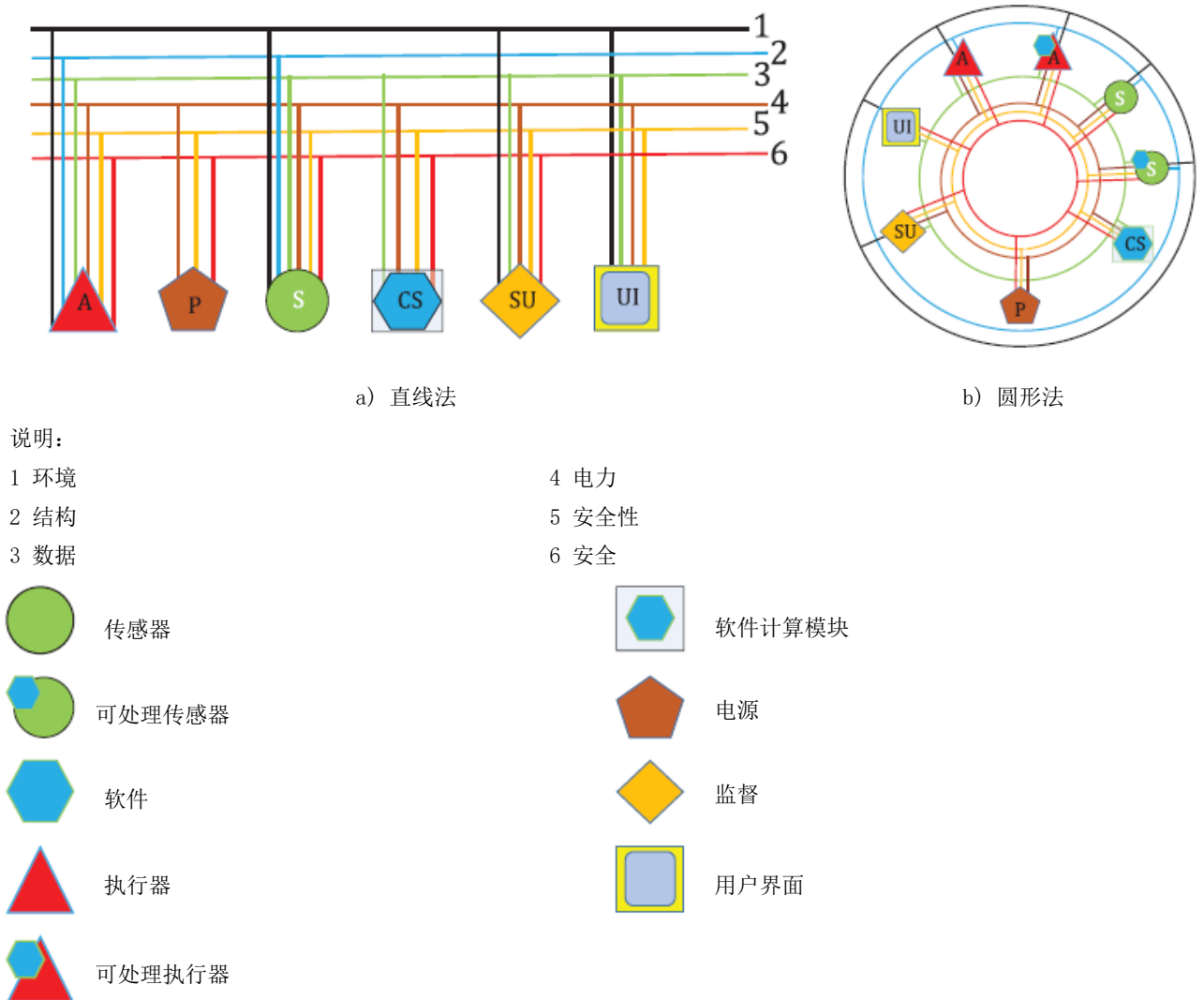
<p>输出:</p> <ul style="list-style-type: none"> —— 人员检测/确认结果; —— 状态(连接到数据库和识别服务器); —— 错误(系统或人员检测); —— 用户从触摸屏上输入的传输 	
<p>功能/功能性:</p> <p>人脸识别模块, 通过识别模块:</p> <ul style="list-style-type: none"> —— 操作模式; —— 语音软件模块, 通过扬声器将文本转换为语音; —— 协调软件模块, 管理接口和数据的序列; —— 通过触摸屏进行用户交互; —— 手势识别模块; —— 语音指令识别模块 	<pre> graph TD A[通信模块] --- B[人机交互协调模块] B --- C[文本转语音模块] B --- D[识别模块] C --- E[扬声器模块] </pre>
<p>基础措施:</p> <p>中间件、外部识别服务器、具有图片和消息的数据库</p>	
<p>安全:</p> <p>如第5章所述, 该模块遵循适用的安全标准 (例如, IEC 61508-3或IEC 60204-1)。</p> <ul style="list-style-type: none"> —— 功能安全模块开发的评估(IEC 61508系列); —— 用户警示信息(根据相关的ISO标准); —— 人为因素和可用性 	
<p>安全性:</p> <ul style="list-style-type: none"> —— 模块只能通过安全数据访问; —— 通过确保最低置信水平来防止人脸识别的滥用; —— 通过安全连接访问数据库和识别服务器 	
<p>建模:</p> <p>不适用</p>	

附录 C
(资料性)
服务机器人模块化案例

C.1 总则

在以下章节中，介绍了服务机器人模块化设计的典型案例，这些案例采用了本文件中提出的概念和指南；其包括硬件设计、软件设计以及第5至7章所述的安全和安全性方面。在C.2中，提出了一个使用模块化的概念，采用模块化设计的基础的移动机器人系统，包括了移动操作等高级功能，以提供各种服务功能。此外，本文件在C.3中，提出了一种用于个人护理的身体辅助机器人。

在配置带有硬件部分的模块时，连接性问题可以用示意图表示。图C.1中给出了两种实例方法，分别是基于Virk^[49]的直线法和基于Norman^[50]的圆形法，可以用以说明在服务机器人设计中模块之间的连接性。此处定义了一组常用的模块图标，并将它们连接起来形成特定应用设计。



图C.1 机器人模块化的连接示意图及示例模块

直线法表示已定义的模块图标与其他模块的连接性，通过规定的交互变量以传统的数据总线线图表示，其包括安全、安全性、电源、数据通信(以各种方式表示，例如，特定的数字总线或简单的模拟或数字信号线)、机械接口和工作环境的适当保护(例如，水、尘、振动等)。圆形法通过圆形格式表示模

块化连接的细节。这两种方法是可互换的，允许通过满足相关互操作性需求的接口连接个别模块来设计和呈现特定的功能。

许多模块包含智能特性，在这种情况下，它们应该需要一系列数据连接功能以满足互操作性需求；例如，电源模块可以具有智能电源管理功能，因此可能需要数据连接；这可以通过一系列协议（例如，CAN, I2C, TCP/IP, USB）来实现。

根据程序（例如，SysML），还有其他方式和方法来表示系统中的模块化方面。

C.2 移动机器人系统模块化

该模块化设计的服务机器人的案例是一个基于移动平台的配送机器人，其可以在拥挤的环境中操作，将物体交给给人；其由一个移动平台以及用于识别物体的各种传感器组成。其主要行为使用了Brook^[51]的方法，具体如下：

- 移动到指定位置
- 移动过程中，识别物体并避免潜在危险

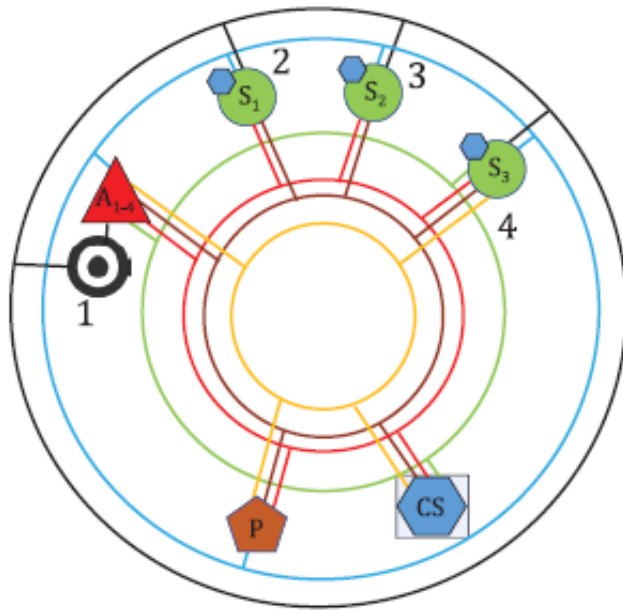
图C.2 a)展示配送服务机器人的具有硬件和软件部分的模块构形，该机器人可在拥挤环境中具备避障能力而进行导航，同时通过加密方式确保未经授权人访问数据的安全性。图C.2 b)展示了一个可视化的案例。该用例场景应该预见安全注意事项、安全性注意事项和与安全相关的安全性注意事项。为满足安全要求，所使用的模块应能满足配送服务机器人应用中所需的安全要求。该配送服务机器人拥有不同类型的具有硬件部分的模块，包括车轮模块、执行器模块、激光雷达模块、2D图像摄像头模块、红外摄像头模块、计算模块和电源模块。四个驱动轮安装在一个移动平台上，并由一个计算模块控制所需的移动。注意，各模块应按照第5章中建议的流程，与配送机器人的特定应用一致，进行安全、安全性及与安全相关的安全性风险评估，应提供与硬件部分相关的信息（或属性），以确保相应软件模块的正常运行。特别是，配送包裹的机械模块应组装完好，以便于容易重新配置。应识别出运行环境中的静态对象，以便执行适当的行为，例如，转向目标或避障。与动态安全相关的对象（例如，人）应该涉及更严格的安全要求。

图C.2 c)说明了软件模块的配置，可使用具有硬件部分的模块实现所需的行为，如图C.2 a)。注意，为了方便，这里不关注模块的硬件和软件部分之间的关系。图C.2中显示了用例场景中所需的各种软件模块的总体功能。配送机器人的软件模块大致可以分为以下几类：

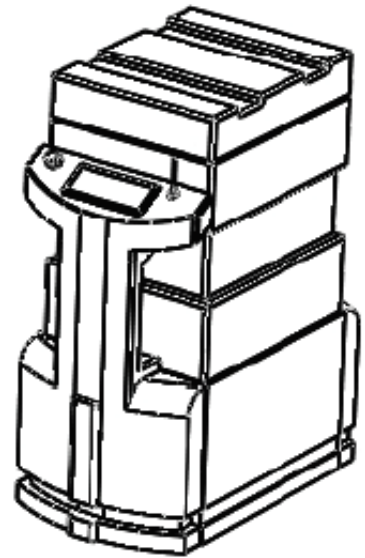
- 1) 识别模块；
- 2) 一个或多个数据交换模块；
- 3) 安全性模块；
- 4) 导航模块；
- 5) 避障模块；
- 6) 移动控制模块；
- 7) 安全模块。

该识别模块可包括用于识别授权个体的个人识别模块的人脸识别和用于识别与安全有关的物体的物体识别模块。数据交换模块用于在配送机器人、服务器和其他适当的机器人内部的模块之间进行数据交换。诸如移动到目标位置和识别特定人员等指令都是通过数据交换模块接收的。因此，指令应该被加密/保护，并且由具有正确授权的模块传输和读取。如果解密失败或给定指令的权限不正确，安全性模块应该发出警示，监视操作过程，并执行适当的安全措施。如果发生的安全性情况可能导致安全问题，该模块应通知安全模块，以确保能够实施适当的安全措施。导航模块由建图模块、定位模块和路径规划模块组成。导航模块将下一个航路点发送给移动控制模块。此外，导航模块检查机器人是否在危险区域作业，如果机器人进入危险状态，则向安全模块发送报警通知。避障模块应向导航模块提供机器人避障信息。当然，障碍避让模块可以包含在导航模块中。安全模块应管理机器人的安全相关危害，包括根据安全和安全性风险考虑确定的与安全相关的危害。安全模块应从识别模块、数据交换模块、安全性模块、

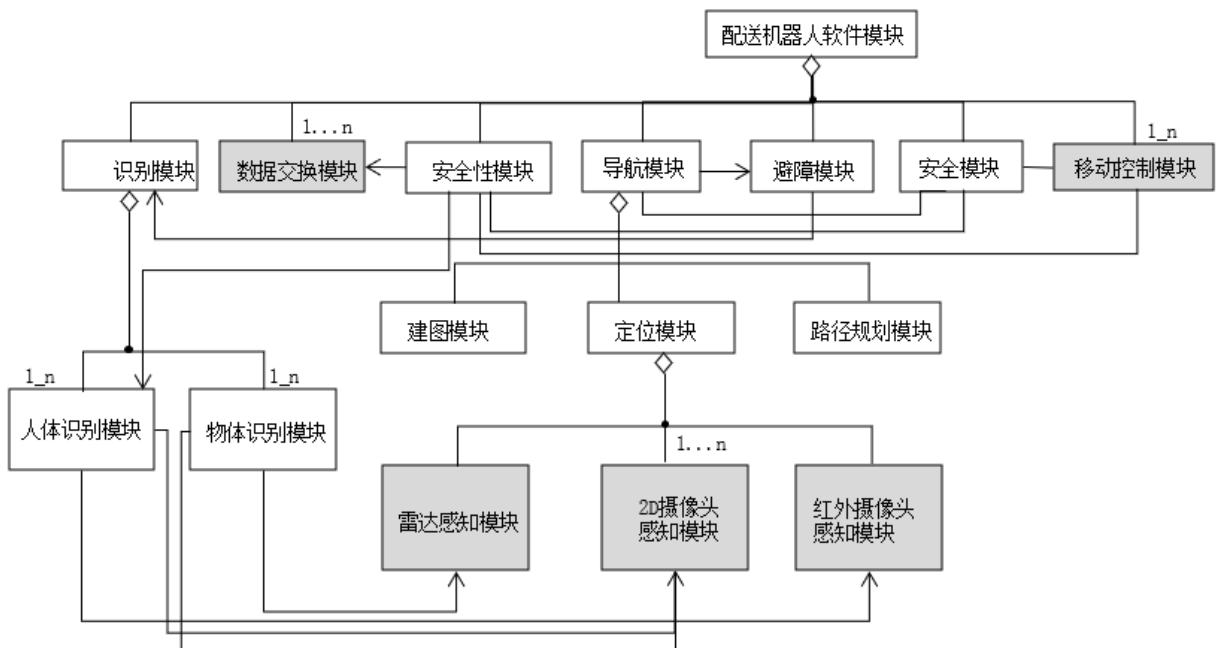
导航模块和移动控制模块中收集和分析与安全相关的数据。移动控制模块包括用于控制车轮模块中的四个执行器(A₁₋₄)的软件模块。根据分析结果，应考虑和执行适当的安全性、安全和与安全性相关的安全措施。定位模块使用传感模块生成机器人当前姿态，而传感模块包括激光雷达传感模块、二维摄像头传感模块和红外摄像头传感模块，通过相应的软件模块获取所需的传感信息。请注意，应提供配送机器人所使用的软件模块的属性文件，以确保其按计划运行。图C.2c)框中的阴影表示软件模块与具有硬件部分的模块的通信。



a) 具有硬件部分的模块



b) 配送机器人示例图片



c) 软件模块

说明:

- 1 车轮
- 2 红外摄像头
- 3 雷达传感器
- 4 2D摄像头

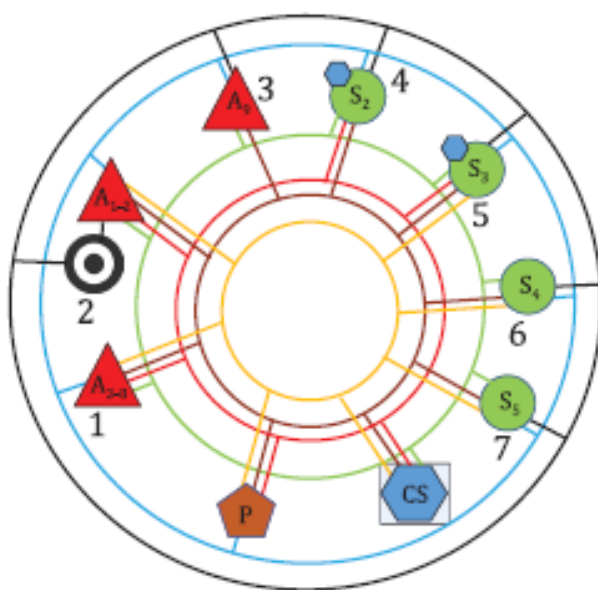
图C.2 具有移动平台的配送机器人的设计示例

为了扩展移动配送机器人平台以执行移动操作机行为,可以将取放操作包括到移动操作中,以强化机器人从一个位置取物至另一个位置取物,并把物体交给给人。操作行为具体如下:

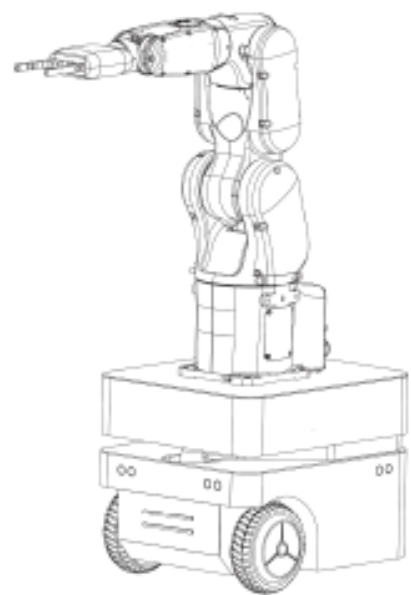
- 取-放物体;
- 取-移动-放物;
- 操作过程中,识别物体并避免潜在风险。

机器人导航到指定位置后,操作机精确地操作至目标物体的位置,以完成所需的拾取操作任务。通常情况下,精确的定位应与借助合适的感知反馈数据(例如,来自视觉系统)进行的微调相结合。在图C.3中,设计了6个执行器模块(A_{3-8})配合传感器模块完成拾取任务。采用模块化方法的优点是操作相关模块可以很容易地引入现有的移动平台,同时以一种安全的方式,与其他模块共享感知信息的公共数据链接,以及使用相同的电源模块(P)、相同的软件计算模块(CS)和相同的感知模块(S_1-S_3)的移动平台。因此,在该机器人移动平台的例子中,采用模块化方法的优点是每个行为和功能可以通过使用一个适合的模块组合获得,设计的接口连接提供一种方便的方式接入更多模块,以普遍增强对其他应用的设计。

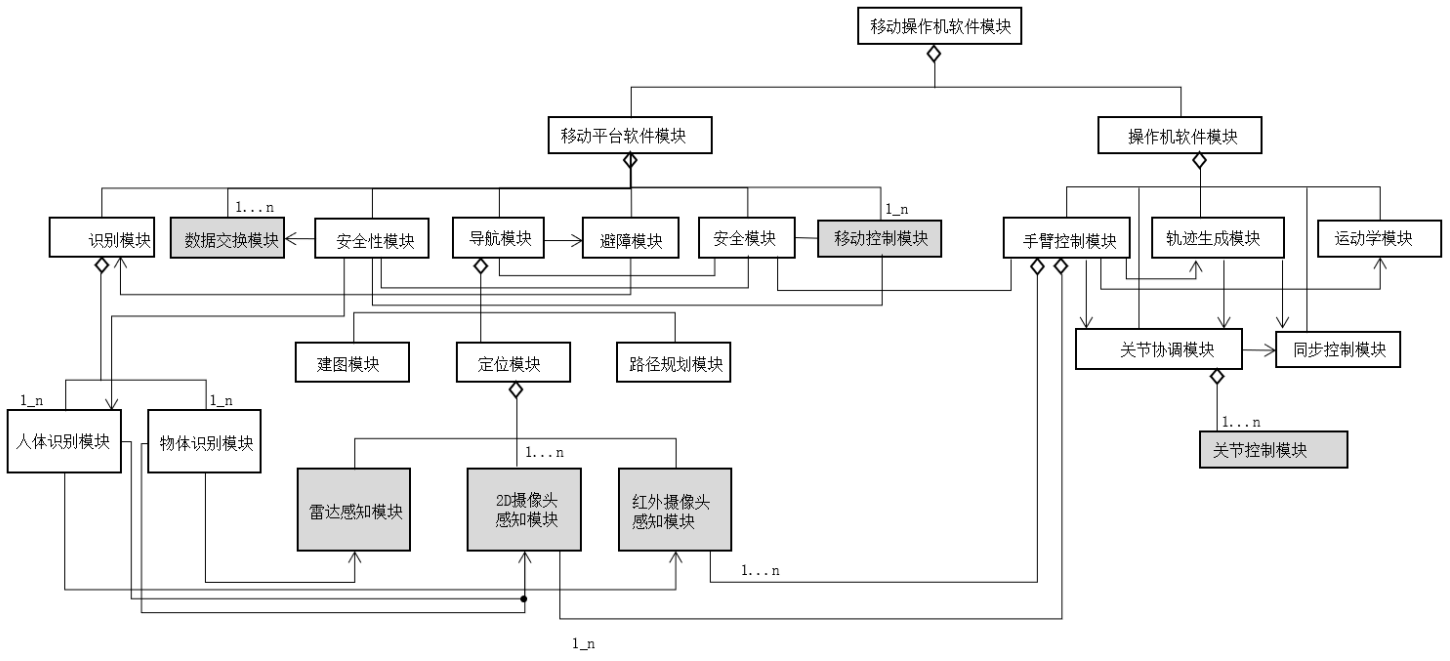
对于移动操作机,在配送服务机器人的软件模块中添加了一些用于操作目标物体的软件模块。特别是控制操作机的安全、安全性及安全性相关的安全问题应保证得到控制,移动底盘和控制模块应在安全模块的严格管理下检查和使用来自2D/红外摄像头感知模块的数据。当然,手臂控制模块需要从摄像头感知模块接收目标物体的位姿,并利用运动学模块生成所需的轨迹来实现给定的位姿。关节协调模块应接收生成的轨迹,并将要移动的距离和方向发送给关节控制模块,其对每个执行器进行适当的控制。特别是,同步模块应该在关节协调模块中使关节同步。



a) 具有硬件部分的模块



b) 移动操作机示例图片



c) 软件模块

说明:

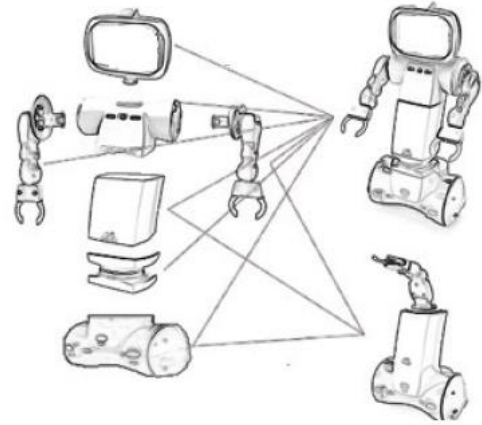
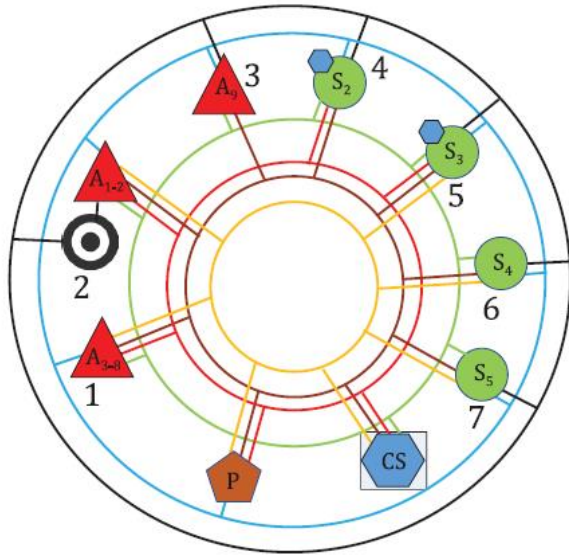
- | | |
|-----------|--------|
| 1 操作机的执行器 | 5 2D雷达 |
| 2 车轮 | 6 触屏 |
| 3 扬声器 | 7 麦克风 |
| 4 雷达传感器 | |

注1: 安全性模块与安全模块可以位于操作机模块中
 注2: 移动平台和操作机的软件模块宜在独立的计算板上

图C.3 移动操作机的设计示例

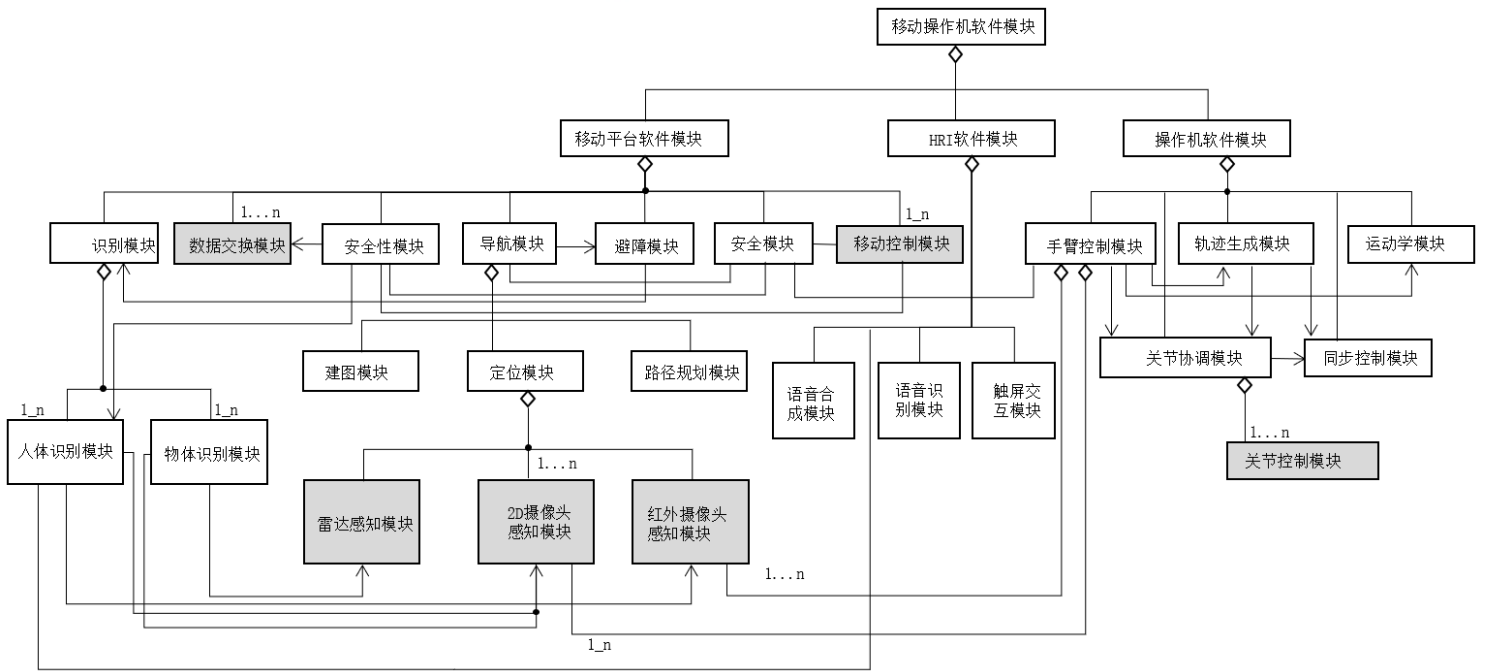
移动仆从机器人设计用于在家庭或公共环境中移动, 执行各种服务任务或与人交互。应该使用自然的人机交互界面, 让非专业人士以自然的方式使用机器人, 同时避免与静止和移动的安全相关障碍发生碰撞。为了执行人的指定行为, 仆从机器人应能够通过特定的用户界面(例如, 图形界面、对话界面和手势界面)接收人类指令或信息。因此, 要使用移动平台模块和操作机模块扩展配送机器人, 主要行为应包括人-机器人交互模块。人-机器人模块的行为如下:

- 语音交互;
- 手势交互;
- 触屏交互。



a) 具有硬件部分的模块

b) 移动仆从机器人



c) 软件模块

说明:

- 1 操作机的执行器
- 2 车轮
- 3 扬声器
- 4 雷达传感器
- 5 2D雷达
- 6 触屏
- 7 麦克风

注1: 安全性模块与安全模块可以位于操作机模块中

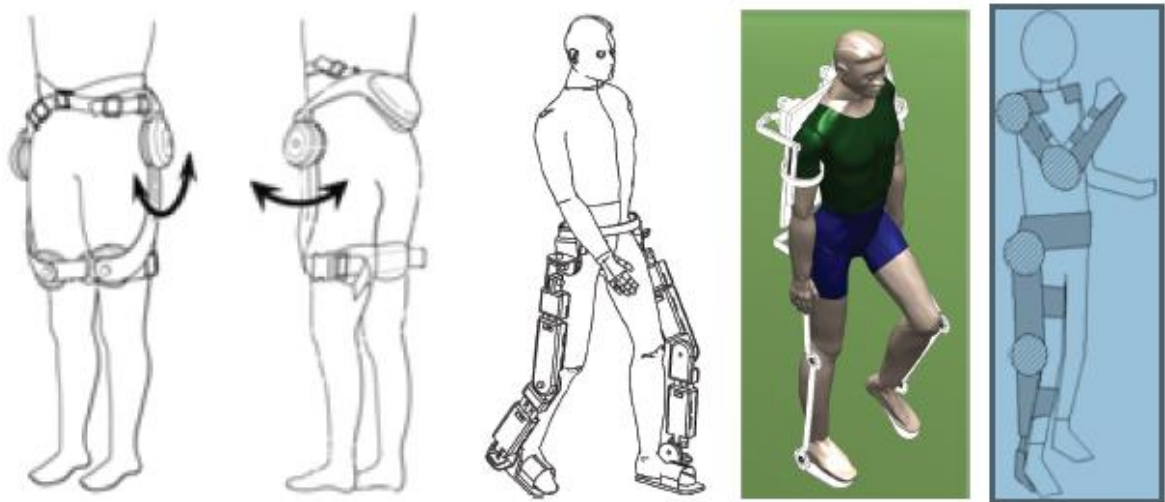
注2: 移动平台和操作机的软件模块宜在独立的计算板上

图C.4 移动仆从机器人设计

在图C. 4中包含两个传感器以接收人的指令。第一个是触屏模块(S₄)，其提供图形界面，用户可以
直接、明确地向机器人发出指令。第二个是麦克风传感器模块(S₅)，其提供对话界面，用户可以以自然
的语音方式发出语音命令。所有传感器可以再次与图C. 3中的移动操作机共享相同的电源(P)、相同的计
算模块(CS)和初始传感器模块(S₂-S₃)。针对移动仆从机器人，在移动操作机的软件模块中添加了HRI软
件模块。用于HRI的其他软件模块应包括不同语言的语音识别模块、语音合成模块、控制触屏的触摸屏
交互模块和用于检测物体和人姿态的2D/红外摄像头感知模块。特别需要注意的是，触屏交互模块与安全
性模块相连接，需要对访问控制进行管理，防止未经授权的人访问机器人。

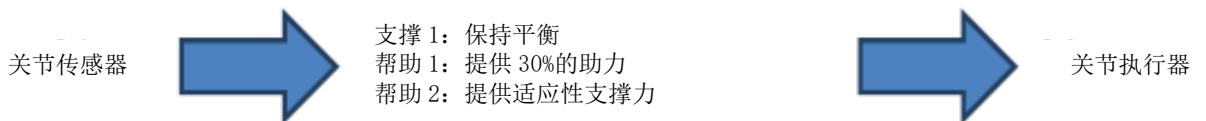
C. 3 外骨骼机器人系统模块化

身体辅助机器人旨在帮助用户执行所需的运动任务，对人的能力提供补充或增强。从模块化的角度
来看，其集中在利用可互换的模块以适应人体关节的变化，并形成外部辅助能量以支持人体所需的运动。
为此，我们将集中在的身体辅助机器人/外骨骼上，图C. 5给出了一些示例。



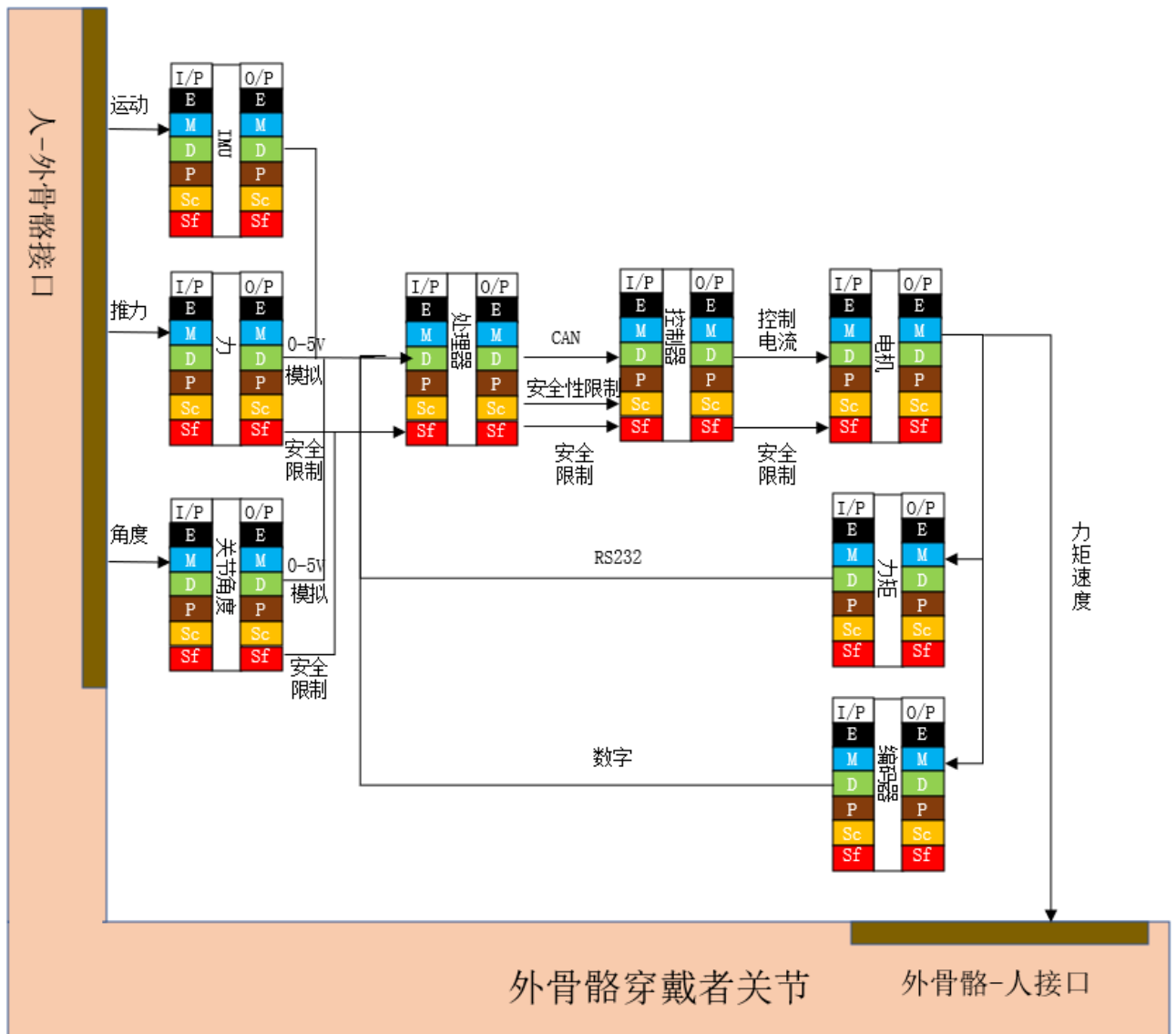
图C. 5 个人助理应用的身体辅助机器人（从左向右：臀、下身、下身加肩和全身外骨骼）

可穿戴移动外骨骼能够用于支持各种人体运动任务，例如，站立时的稳定性、坐-立/立-坐转换的
物理支持、行走和上/下楼梯。穿戴外骨骼可用于锻炼应用，各种操作模式可以描述为一组行为，如图
C. 6所示。



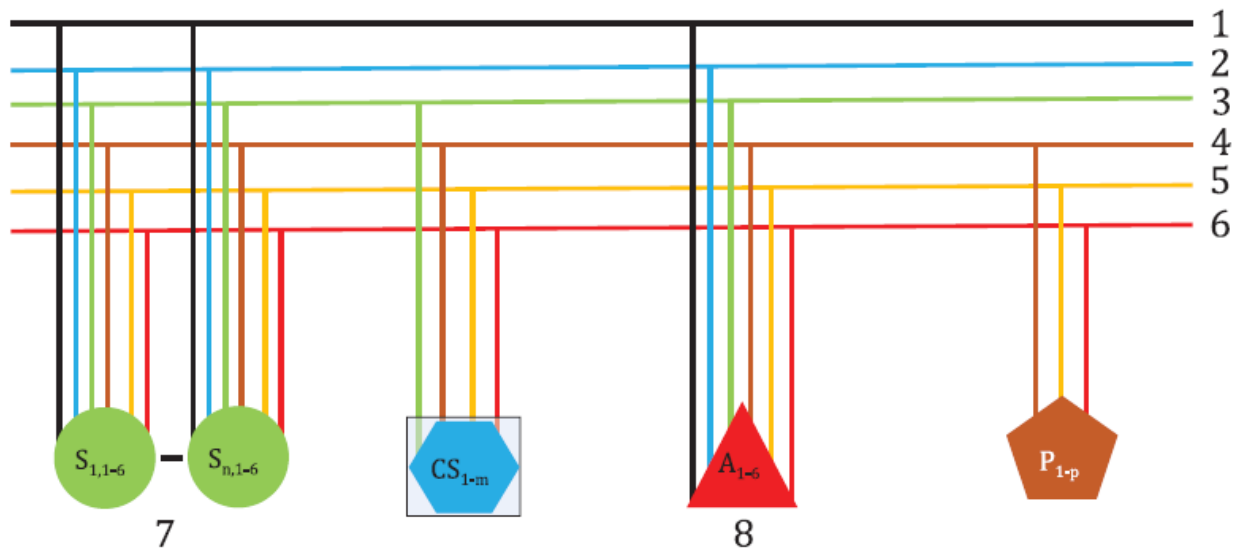
图C. 6 可穿戴移动外骨骼的操作行为

这些行为可以通过采用模块化方法在单个人体关节上进行所需的运动控制来实现。图C. 7显示了采
用模块化设计方法将物理恢复/辅助力应用于单个关节的一般方面，其使用了人体运动感知模块，包括
各种传感器，例如，惯性测量单元(IMU)，力和关节角度传感器以检测期望的关节运动，并作为输入来
确定信息以控制电机提供关节所需的扭矩。在设计中，通过采用机器人模块接口协议，满足相关的安全
关节角度限制的安全问题应包括其中，在第5章中已讨论过该安全问题。注意，为了更清晰，一些问
题被省略了，例如，电源细节、人体运动数据的安全性和环境方面的问题。



图C.7 单关节控制辅助外骨骼的设计

可以为其他下体关节设计这样的模块化框架，并将这些关节级子系统在适当配置架构中进行连接，以实现所需的可穿戴外骨骼；这样就可以控制人体关节以获得所需的运动支持系统。例如，图C.8展示了臀部，双腿的膝盖和脚踝关节应通过六组传感器和执行器来确定一个6自由度可穿戴外骨骼以支持人的运动，例如，在矢状面散步，并使用了图C.8中的线方法表示，其中n是用于臀部、膝盖和脚踝关节的传感器数量，m是使用软件计算模块的数量，p是整个外骨骼中使用的电源的数量。



说明:

- 1 环境
- 2 结构
- 3. 数据
- 4 电源

- 5 安全性
- 6 安全
- 7 臀、膝盖和脚踝关节的传感器
- 8 臀、膝盖和脚踝关节的执行器

图C.8 支撑运动任务的六自由度外骨骼，如行走

附录 D (资料性) 机器人测试指南

D.1 总则

机器人模块制造商应测试模块的性能、安全和安全性，并在适当的情况下，通过适当设计的测试方法提供足够的证据，以验证其模块适用于预期用例。

注：在本文件的未来修订中为模块制造商开发广泛可接受的测试方法是一个长期目标。

当前版本通过建议资料性的测试方法帮助制造商探索开发测试方法，以检验其机器人模块产品的模块化原则。制造商应对其模块进行确认和验证过程。

D.2 确定必要测试

机器人模块制造商应开发测试方法，以建立适用于第4章中提出的模块化原则和第5章中提出的指南的安全、安全性和性能特性。模块的安全和安全性测试应根据预期用例通过可识别的危险或可预见的危险来进行。在风险分析过程中，可以对发现的危害进行讨论和记录。不同适用的国际机器人安全标准，可以制定要求和保护措施，从而将特定危险情况的风险降低到可接受的水平(例如，安全限制)。性能和功能测试应参考第6章和第7章执行。

测试可包括但不限于以下测试，部分测试见第D.3条：

- 机械安全测试；
- 机械性能测试；
- 电气安全和电磁兼容性测试；
- 电气和电磁性能测试；
- 与安全相关的软件测试；
- 安全性测试；
- 环境测试；
- 生物和化学安全测试；
- 互操作性测试；
- 互换性测试；
- HRI或人为因素和可用性测试；
- 人工智能软件安全和性能测试。

D.3 安全与安全性的符合性测试

D.3.1 通则

安全是模块在安全相关应用中的基本要求，应确认保护用户免受伤害的措施。模块的安全性能应该通过风险分析来确定。安全测试应根据支持风险评估过程所需的证据来进行。以下内容提供了指南和示例以帮助进一步开发服务机器人模块的安全测试。

D.3.2 机械安全测试

机械参数的规范，例如，形状、重量、最大负载、重心等，是制造商考虑机械安全的关键问题。若干ISO标准提出了制定机械安全测试的方法，例如，ISO 12100:2010和ISO 13482:2014使用风险评估来进行测试，以满足安全要求。ISO 12106:2017定义了一种在恒定振幅、均匀温度和固定应变比的应变控制下测试单轴变形试件的疲劳性能的方法。

D.3.3 电气安全与电磁兼容测试

电流、电压、导体之间的爬电距离、辐射波的能量等是识别模块电气安全性的常用可测参数。已经根据电气安全和EMC标准制定了相关规范。例如，IEC 60204-1:2016规定了电气设备安全的一般要求，IEC 60990:2016规定了电流的测量方法，IEC 61000系列标准涵盖了EMC方面。

D.3.4 安全相关的软件测试

ISO/IEC/IEEE 12207:2017和ISO/IEC/IEEE 15288:2015定义了软件开发生命周期。为了满足所需的安全相关性能水平，软件测试包括基于规格的测试(例如，等价划分、分类树、边界值分析)、基于结构的测试(例如，语句测试、分支测试、决策测试)和基于经验的测试(例如，错误推测)。ISO/IEC/IEEE 29119系列标准定义了软件测试的概念、过程、文档和技术。

D.3.5 安全性测试

ISO/IEC TS 30104:2015描述了物理安全机制。除了物理形式外，ISO/IEC 27001:2013和ISO/IEC 27002:2013还规定了安全性管理要求和ISO/IEC 27032:2012所述的网络空间安全控制实践原则。ISO/IEC 15408系列标准建立了信息技术安全的评价规范，ISO/IEC 19896系列标准规定了测试人员和评估人员的能力要求。密码模块的测试要求在ISO/IEC 24759:2017有说明。

D.3.6 生物和化学安全测试

ISO 14123-1:2015为控制机械排放的有害物质对健康造成的风险而建立了原则。ISO 10993系列提供了生物相容性的评价方法，以确定是否符合生物和化学安全的要求。

D.4 性能符合性测试

D.4.1 通则

应测量和测试模块的性能，以确认模块符合其设计要求。虽然大多数参数是制造商可以测量的，应考虑测量单位的ISO/IEC 17025:2017能力或良好实验室规范(GLP)。

D.4.2 机械性能测试

制造商应规定若干参数来定义一个模块的机械性能。例如，质量、速度、力、压力等力学变量。结构强度是制约模块性能的重要特性之一。在各种应用场景中，特别是串联连接时，都应该考虑到这一点。整体性能或强度受到该系列中最弱的点或模块的限制。在机械工程中，应考虑在三维坐标轴上作用于模块上的力和力矩，其中最大应力原则上不应超过材料的极限。制造商应通过此性能测试为客户提供材料力学性能，以评估其模块连接的整体强度和状况。

在结构性能中，可以根据可能的应用或情况，例如，模块在静态负载或动态负载下使用，预先执行各种受力和弯矩条件。测试可以考虑：

- 作用在1到3个轴上的力和力矩(单个或联合)；
- 静态力和力矩；
- 动态力和力矩，包括冲击，周期和任意条件。

测试应使用校准的力计进行力评估，使用校准的扭矩传感器进行扭矩评估。制造商应向客户提供足够的证据作为参考。

D.4.3 电气安全与电磁性能测试

例如，电池、光探测和测距、无线通信等电气和电磁模块提供其相应的而功能，且其具有规定的电容、电流、电压、频率、强度等。电、电磁参数决定了模块的性能。

电池模块是服务机器人的电源，其容量对所支持功能的运行时间有显著影响。IEC 60086-1:2015用于标准化原电池组规格。

探测光的频率和强度会影响传感模块的分辨率和灵敏度。ISO/TS 19159系列标准定义了使用各种技术对传感器进行校准和验证。非接触式电敏感传感器的一般设计要求可参考IEC 61496-1:2012。

无线模块的信号强度将决定通信质量。信息和通信技术标准可参考ISO/IEC JTC 1的工作。

D.4.4 人工智能软件性能测试

一般软件的性能取决于编码的完成情况，而人工智能(AI)的性能可以通过不断增加的数据而演变。如果该模块已嵌入AI，制造商可能需要对其进行持续评估，并分析其性能是否符合设计要求，并不会引起任何不可接受的安全问题。

AI的一个重要元素是数据，ISO/IEC TR 20547-2:2018提供了大数据用例和衍生要求。有关人工智能的标准仍在制定中。

D.4.5 环境测试

环境条件通常用统计变量来描述，例如，温度、湿度、空气质量等。环境是产品功能和生命周期的一个重要因素。制造商应确认模块是否能够在预期的环境中以规定的性能运行。

IEC 60721-3-1:2018环境参数分组及其对产品的重要性进行了分类。IEC 60068的系列标准描述了对应于各种环境条件的测试方法。IEC 60529:2013定义了电气设备外壳提供的保护程度，以确定IP等级。如果环境条件发生变化，则新条件应包含在测试用例中。

由于不同的材料，模块应有不同的应力测试方法，以便在更短的时间内进行环境测试。SSD（固态硬盘）可作为业务机器人的基本存储模块。以SSD为例，基于NAND闪存的SSD可以随着温度的升高而加速老化。根据JEDEC标准的固态硬盘(SSD)要求和耐久性测试方法，JESD 218B.01中的6.1.3中表3，66°C下96小时的数据保存测试相当于在30°C下存储1年。

D.4.6 人为因素和可用性测试

人为因素和可用性是用户界面的特征，影响着用户与模块之间的交互。这些交互包括身体接触、感知信息以及后续的决策。人因工程和可用性工程是指通过应用关于人类行为、能力、限制和其他特征的知识来设计和开发用户界面，以促进模块的使用。对设计的用户界面的评估可作为人为因素和可用性测试。这些测试可以识别可能的使用错误和用户满意度。

使用错误是指用户的行为(或缺乏行为)不符合制造商的设计期望，导致任务未完成。此外，使用错误可能会引起危害，对用户和模块造成伤害。例如，模块的机电连接器组装失败可能会破坏物理结构，可能会对人造成电击。如果用户错误与严重危害相关，制造商可能需要考虑将可用性测试作为安全要求的一部分。一个设计良好的用户界面可以实现正确的用户操作，防止使用错误可能导致的伤害，直接影响用户满意度，从而影响产品的价值。为了获得良好的人为因素设计和可用性的证据，确认测试需要以科学地、严谨地收集数据。

进行人为因素和可用性测试以确认设计，并证明模块可由预期用户用于预期用途而没有不可接受的风险。测试包含：

- 用户界面代表测试模块的设计；
- 参与者代表目标用户；
- 任务代表测试模块的用例场景（制造商应规定通过/不通过的标准）；
- 条件代表实际使用环境。

测试可以通过观察参与者操作任务的表现，记录使用错误的发生情况，采访参与者的使用经历。应对收集的数据进行分析，将证据和模块符合制造商声称的人为因素和可用性说明的论证联系起来。ISO/TS 20282-2:2013为可用性测试规定了一种基于用户的总结性测试方法。

D.4.7 验证和确认

验证和确认可用于确认硬件模块分别满足设计规范和应用的要求。规格应在附件A的模板中描述，其中涉及力学、硬件、通信、安全/安全性、输入和输出的应明确规定，以符合互换性、互操作性和粒度等基本原则。

验证应贯穿于产品设计开发的整个过程，例如，概念设计阶段采用形式化方法以及型式试验阶段采用第三方测试。

应明确规定硬件模块的用例和相应的关键属性。为了进一步确认模块是否满足应用需求，需要应用相关确认方法。例如，仓库物流移动平台的关节模块应该在特定场景中根据已发布的标准进行确认。

参考文献

- [1] ISO 8373:2012 Robots and robotic devices — Vocabulary
- [2] ISO 9409-1 Manipulating industrial robots — Mechanical interfaces — Part 1: Plates
- [3] ISO 9409-2 Manipulating industrial robots — Mechanical interfaces — Part 2: Shafts
- [4] ISO 10218-1 Robots and robotic devices — Safety requirements for industrial robots— Part 1: Robots
- [5] ISO 10218-2 Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration
- [6] ISO 10303 (all parts) Industrial automation systems and integration — Product data representation and exchange
- [7] ISO 10993 (series) Biological evaluation of medical devices
- [8] ISO 11593 Manipulating industrial robots — Automatic end effector exchange systems — Vocabulary and presentation of characteristics
- [9] ISO 12106:2017 Metallic materials — Fatigue testing — Axial-strain-controlled method
- [10] ISO 13482 Robots and robotic devices — Safety requirements for personal care robots
- [11] ISO 13849-1 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
- [12] ISO 14123-1:2015, Safety of machinery — Reduction of risks to health resulting from hazardous substances emitted by machinery — Part 1: Principles and specifications for machinery manufacturers
- [13] ISO/TS 15066 Robots and robotic devices — Collaborative robots
- [14] ISO/TS 19159 (series) Geographic information — Calibration and validation of remote sensing imagery sensors and data
- [15] ISO 19649 Mobile robots — Vocabulary
- [16] ISO/TS 20282-2:2013 Usability of consumer products and products for public use — Part 2: Summative test method
- [17] ISO/IEC 7498-1 Information technology — Open systems interconnection — Basic reference model: The basic model
- [18] ISO/IEC 15408 (series) Information technology — Security techniques — Evaluation criteria for IT security
- [19] ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories
- [20] ISO/IEC 19896 (series) IT security techniques — Competence requirements for information security testers and evaluators
- [21] ISO/IEC TR 20547-2:2018 Information technology — Big data reference architecture — Part 2: Use cases and derived requirements
- [22] ISO/IEC/CD 23053 Framework for Artificial Intelligence (AI) Systems Using Machine Learning
- [23] ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules
- [24] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- [25] ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for

information security controls

- [26] ISO/IEC TS 30104:2015 Information technology — Security techniques — Physical security attacks, mitigation techniques and security requirements
- [27] ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes
- [28] ISO/IEC/IEEE 15288 Systems and software engineering — System life cycle processes
- [29] ISO/IEC/IEEE 29119 (series)
- [30] IEC 60068 (all parts) Environmental testing
- [31] IEC 60086-1 Primary batteries — Part 1: General
- [32] IEC 60204-1 Safety of machinery — Electrical equipment of machines — Part 1: General requirements
- [33] IEC 60529 Degrees of protection provided by enclosures (IP Code)
- [34] IEC/TR 60601-4-1 Medical electrical equipment — Part 4-1: Guidance and interpretation — Medical electrical equipment and medical electrical systems employing a degree of autonomy
- [35] IEC 60721-3-1 Classification of environmental conditions — Part 3-1: Classification of groups of environmental parameters and their severities — Storage
- [36] IEC 60990 Methods of measurement of touch current and protective conductor current
- [37] IEC 61000 (all parts) Electromagnetic compatibility (EMC)
- [38] IEC 61496-1 Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests
- [39] IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems
- [40] IEC 61784-3:2016 Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses — General rules and profile definitions
- [41] IEC 61800-5-2 Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional
- [42] IEC 62061 Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems
- [43] IEC 62280 Railway applications — Communication, signaling and processing systems - Safety related communication in transmission systems
- [44] IEC/TR 62390 Common automation device — Profile guideline
- [45] IEC 62443 (all parts) Industrial communication networks — Network and system security
- [46] IEC/TR 63074 ED1 Security aspects related to functional safety of safety-related control systems
- [47] ITU-T F. 747. 3 Requirements and functional model for a ubiquitous network robot platform that supports ubiquitous sensor network applications and services, 2013
- [48] NIST SP 800-37 Rev. 1 Guide for applying the risk management framework to Federal information systems: a security life cycle approach
- [49] Virk GS, CLAWAR modularity for robotic systems, International Journal of Robotics Research, Vol 22, Issue 3 - 4, pp265 - 277, 2003
- [50] Norman P Modularity — The degree to which a system' s components may be separated and combined, Ross Robotics, 2017
- [51] Brooks RA, A robust layered control system for a mobile robot, IEEE Journal of Robotics and Automation, Volume 2(1), 1986

- [52] OMG Hardware Abstraction Layer for Robotic Technology [https:// www .omg .org/ spec/ HAL4RT/](https://www.omg.org/spec/HL4RT/)
- [53] OMG Robotic Localization Service v1.1, 2012
- [54] OMG Robotic interaction service framework (ROISTM), v 1.2, 2018
-