ICS 25.040.30
J 28

中华人民共和国国家标准

GB/T 38260—2019

服务机器人功能安全评估

Service robot functional safety assessment

2019-12-10 发布　　2020-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　符号及缩略语 …… 5
4　功能安全评估要求及流程 …… 5
4.1　要求 …… 5
4.2　功能安全评估流程 …… 7
5　危险识别和风险评估 …… 9
5.1　概述 …… 9
5.2　危险识别 …… 9
5.3　风险评估 …… 10
6　功能安全管理 …… 10
6.1　目的 …… 10
6.2　要求 …… 10
7　安全相关控制功能规范要求(SRCF) …… 11
7.1　目的 …… 11
7.2　SRCF 要求规范 …… 12
7.3　SRCS 的要求 …… 13
8　安全相关控制系统(SRCS)设计与整合 …… 15
8.1　目的 …… 15
8.2　一般要求 …… 15
8.3　每种安全功能技术实现的要求 …… 15
9　检验和确认 …… 22
9.1　概述 …… 22
9.2　安全要求检验和确认 …… 22
9.3　SRCS 确认 …… 23
9.4　SRCS 系统安全完整性确认 …… 23
附录 A(规范性附录)　确定 SIL——风险图 …… 25
附录 B(规范性附录)　服务机器人危害种类 …… 27
附录 C(规范性附录)　安全要求 …… 33
附录 D(资料性附录)　SRCS 使用信息 …… 38
附录 E(资料性附录)　服务机器人功能安全管理相关修改程序及文件要求 …… 39
参考文献 …… 42

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由国家机器人标准化总体组提出并归口。

本标准起草单位：上海电器科学研究所(集团)有限公司、上海机器人产业技术研究院有限公司、哈工大机器人集团有限公司、北京康力优蓝机器人科技有限公司、纳恩博(北京)科技有限公司、重庆德新机器人检测中心有限公司、深圳中智科创机器人有限公司、北京出入境检验检疫局检验检疫技术中心、广州艾罗伯特机器人技术咨询有限公司、广东加华美认证有限公司上海分公司、宝时得科技(中国)有限公司、上海木木机器人技术有限公司、青岛钢铁侠科技有限公司、上海方立数码科技有限公司、浙江孚宝智能科技有限公司、中国电子技术标准化研究院、上海添唯认证技术有限公司、上海擎朗智能科技有限公司、东莞市豪铖电子科技有限公司、上海电器科学研究院、上海电器设备检测所有限公司。

本标准主要起草人：沈文婷、邢琳、于振中、刘雪楠、杜超、彭鹏、王智锋、宝暄、黄鸿鸣、苏敏、丁玉才、鲁博丽、张锐、张鼎、贾国强、李通、刘云柱、牛曦杰、胡林、郑军奇、朱晓鹏。

引　言

服务机器人主要在非工业环境中为人类提供服务，由于使用环境多样，与人类接触频繁，其安全性显得尤为重要。服务机器人的安全相关控制系统(以下简称 SRCS)在实现整个服务机器人安全方面发挥着重要作用。

本标准阐述了 GB/T 20438 系列标准框架内的服务机器人领域的具体应用，采用 GB/T 15706、GB/T 16855.1 和 GB/T 16855.2 中提及的风险评估、机械安全控制系统的设计和确认方法，参考 GB 28526 和 ISO 13482 中的功能安全规范要求，制定了相关技术内容。

本标准为服务机器人设计人员、SRCS 的设计和确认人员、控制系统制造商、第三方检测认证机构等单位使用。本标准为达到服务机器人所需的功能安全等级陈述了相关方法并做出了规定要求。

本标准属于 C 类标准。对于按照 C 类标准设计和制造的机器，当 C 类标准中的条款与 A 类或 B 类标准中所述的条款不一致时，优先采用 C 类标准。

服务机器人在提供服务时需要人机互动、协作和互联，当服务机器人的 SRCS 用作功能安全评估的一部分时，在很多情况下，可以达到降低机器风险的目的。

本标准涵盖服务机器人相关的危害、危害情况或危害事件的描述。对于特定的服务机器人，公认的危害源往往是特定的。危害的数量和类型直接与服务机器人应用的特性、安装复杂度以及人机交互整合的水平相关。这些危害相关的风险随机器人的使用和本身用途的类型以及安装、编程、操作和维护的方式而变化。

服务机器人功能安全评估

1 范围

本标准规定了服务机器人控制系统功能安全评估要求及流程、危害识别和风险评估、功能安全管理、安全相关控制功能(以下简称 SRCF)规范要求、SRCS 的要求、SRCS 的设计与整合以及检验和确认、服务机器人自身或以协同方式共同工作的机器人组的危害直接引起的风险的特征等内容。确立了涉及预期降低直接接近服务机器人或直接使用服务机器人而造成的人身伤害或财产损害的风险的功能安全等内容。

本标准适用于以单独和(或)组合的方式使用的服务机器人相关控制系统的功能安全,以协同方式共同工作的服务机器人群组的功能安全评估可参照此标准。

本标准不适用于需要或要求由其他标准或法规为保护人身免遭危害、财产危害所提出的全部要求(例如:防护、非电气联锁或非电气控制),电气控制设备自身引起的电气危害(例如:电击,见 GB 5226.1)。

注:各类型的服务机器人都需要满足其特殊的要求,以提供充分的安全。

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 4943.1 信息技术设备 安全 第 1 部分:通用要求

GB/T 5226.1 机械电气安全 机械电气设备 第 1 部分:通用技术条件

GB/T 15706—2012 机械安全 设计通则 风险评估与风险减小

GB/T 15969.3 可编程序控制器 第 3 部分:编程语言

GB/T 16754 机械安全 急停 设计原则

GB/T 16855.1—2018 机械安全 控制系统有关安全部件 第 1 部分:设计通则

GB/T 16855.2 机械安全 控制系统安全相关部件 第 2 部分:确认

GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第 3 部分:软件要求

GB/T 23821 机械安全 防止上下肢触及危险区的安全距离

GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

GB/T 37242 机器人噪声试验方法

GB/T 37283 服务机器人 电磁兼容 通用标准 抗扰度要求和限值

GB/T 37284 服务机器人 电磁兼容 通用标准 发射要求和限值

ISO 13482:2014 机器人和机器人设备 个人护理机器人的安全要求(Robots and robotic devices—Safety requirements for personal care robots)

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

IEC 60529 外壳防护等级(IP 代码)[Degrees of protection provided by enclosures (IP Code)]

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

服务机器人　sevice robot

除工业自动化应用外，能为人类或设备完成有用任务的机器人。

注 1：工业自动化应用包括(但不限于)制造、检验、包装和装配。

注 2：用于生产线的关节机器人是工业机器人，而类似的关节机器人用于供餐的就是服务机器人。

[GB/T 12643—2013，定义 2.10]

3.1.2

安全相关控制系统　safety-related control system

其失效可能导致风险立即增加的控制系统。

注：SRCS 包括由电气、电子、可编程电子控制电路等组成的全部控制系统，其失效可能导致功能安全的降低或丧失。

3.1.3

服务机器人功能安全　service robot functional safety

服务机器人控制系统的安全部分，取决于 SRCS 的正确功能、其他技术安全相关系统和外部风险降低设施。

注 1：改写 GB/T 20438.4—2017，定义 3.1.12。

注 2：仅考虑服务机器人系统中取决于 SRCS 正确功能的功能安全。

注 3：ISO/IEC 定义安全为免除不能接受的风险。

3.1.4

风险　risk

伤害发生概率和伤害发生严重程度的组合。

[GB/T 15706—2012，定义 3.12]

3.1.5

安全功能　safety function

其失效会立即造成风险增加的机器功能。

[GB/T 15706—2012，定义 3.30]

注：GB/T 15706—2012 中 3.28.1～3.28.9 给出了保护装置的示例。

3.1.6

安全相关控制功能　safety-related control function

由具有规定的完整性等级的 SRCS 执行的控制功能，预期用于保持机器的安全状况或防止风险立即增加。

3.1.7

SRCS 诊断功能　SRCS diagnostic function

预期用于检测 SRCS 故障，并在检测出故障时产生特定输出信息或动作的功能。

注：该功能预期用于检测可能导致 SRCF 危险失效并引发特定故障反应功能。

3.1.8

SRCS 故障反应功能　SRCS fault reaction function

当 SRCS 范围内的故障被 SRCS 诊断功能检测出时，所触发的功能。

3.1.9

安全完整性等级　safety integrity level

一种离散的等级，用于规定分配给 SRCS 的 SRCF 的安全完整性要求。

注 1：改写 GB/T 20438.4—2017，定义 3.5.8。

注 2：有三种可能的等级，SIL4 为最高，SIL1 为最低。

3.1.10

每小时危险失效概率　probability of dangerous failure per hour

1 小时内危险失效平均概率。

注：PFH_D 不应与要求失效概率(PF_D)相混淆。

3.1.11

目标失效值　target failure value

预期要达到的 PFH_D，为满足规定的安全完整性要求。

注 1：改写 GB/T 20438.4—2017，定义 3.5.17。

注 2：目标失效值以每小时危险失效概率的术语定义。

3.1.12

平均危险失效时间　mean time to dangerous failure

预期的危险失效平均时间。

3.1.13

诊断覆盖率　diagnostic coverage

进行自动诊断试验操作而导致危险硬件失效概率的降低。

注 1：改写 GB/T 20438.4—2017，定义 3.8.6。

注 2：诊断覆盖率(DC)可用下列公式计算：

$$DC = \sum \lambda_{DD} / \lambda_{Dtotal}$$

式中：

λ_{DD} ——检测到的危险硬件失效比率；

λ_{Dtotal} ——总的危险硬件失效比率。

3.1.14

失效　failure

SRCS、子系统或子系统元素执行要求功能的能力的终止。

注 1：改写 GB/T 20438.4—2017，定义 3.6.4；GB/T 15706—2012，定义 3.34。

注 2：失效是随机的(硬件)或系统的(硬件或软件)。

3.1.15

危险失效　dangerous failure

使 SRCS、子系统或子系统元素处于潜在危险或非功能状态的失效。

注 1：改写 GB/T 20438.4—2017，定义 3.6.7。

注 2：潜在是否变成事实取决系统的通道结构，例如：在为提高安全性的多通道系统中，危险硬件失效很少会导致整体危险或非功能状态。

注 3：在多通道子系统中，该子系统危险失效概率可能比构成子系统的通道的危险失效率低。而 SRCS 的危险失效概率不会比构成 SRCS 的任何子系统的危险失效概率低(这出自本标准子系统的特别定义)。

注 4：危险失效通常导致执行 SRCF 出现失效或潜在失效。

3.1.16

安全失效　safe failure

SRCS，SRCS 子系统或 SRCS 子系统元素不引起潜在的危险失效。

注 1：改写 GB/T 20438.4—2017，定义 3.6.8。

注 2：安全失效不会导致执行 SRCF 出现失效或潜在失效。

3.1.17

共因失效　common cause failure

一种失效，为一个或多个事件导致的结果，在多通道(冗余结构)子系统中引起两个或多个单独通道同时失效，从而导致 SRCF 失效。

注 1：改写 GB/T 20438.4—2017，定义 3.6.10。

注 2：该定义与 GB/T 15706—2012 和 IEV 191-04-23 给出的不同。

3.1.18

随机硬件失效　random hardware failure

在硬件中，由一种或多种机能下降可能产生的、按随机时间出现的失效。

注：改写 GB/T 20438.4—2017，定义 3.6.5。

3.1.19

系统性失效　systematic failure

有确定方式和原因的失效，只能通过修改设计或制造过程、操作步骤、文件或其他有关因素予以消除。

[GB/T 20438.4—2017，定义 3.6.6]

注 1：仅正确维修而不修改通常将不能消除失效原因。

注 2：通过模拟失效原因可能诱发系统失效。

注 3：包括人为错误的系统失效原因的示例有：

——安全要求规范；

——硬件设计、制造、安装和/或操作；

——软件设计和/或执行。

3.1.20

安全相关软件　safety-related software

在安全相关系统中，用于实现 SRCF 的软件。

3.1.21

检验　verification

通过检查（如试验、分析），证实 SRCS、其子系统或子系统元素满足有关规范设定的要求。

注 1：改写 GB/T 20438.4—2017，定义 3.8.1；GB/T 21109.1—2007，定义 3.2.92。

注 2：检验结果应提供证明文档作为客观性凭证。

示例：

检验活动包括：

——对输出（各阶段文件）评审，保证符合该阶段的目标、要求，同时考虑该阶段的特定输入；

——设计评审；

——对设计产品进行试验，确保按照其相关规范执行；

——在系统的不同部分以逐步方式集成时，要进行整合试验，通过环境试验，确保所有部分以规定的方式协同工作。

3.1.22

确认　validation

通过检查（如试验、分析）证实 SRCS 满足具体应用的功能安全要求。

注：改写 GB/T 20438.4—2017，定义 3.8.2。

3.1.23

性能等级　performance level

在可预期条件下，用于规定 SRP/CS 执行安全功能的离散等级。

3.1.24

控制系统有关安全部件　safety-related part of a control system

控制系统中响应有关安全输入信号并产生有关安全输出信号的部件。

注 1：SRP/CS 的组成，以有关安全的输入信号被触发为起始点（例如：制动凸轮和位置开关滚轮等），以控制文件的动力输出（例如：接触器的主触点等）为终止点。

注 2：如果监测系统用于诊断，也可认为它们是 SRP/CS。

3.1.25

伤害　harm

直接或间接地对人身的损伤或对人体健康的损害。

注：改写 GB/T 20438.4—2017，定义 3.1.1。

3.1.26

风险评估　risk assessment

风险分析和对风险进行定性、定量评价的全过程。

注：改写 ISO 13482:2014，定义 3.8。

3.2　符号及缩略语

下列缩略语适用于本文件。

Cat.：类别(Category)

CCF：共因失效(Common cause failure)

DC：诊断覆盖率(Diagnostic converage)

DC_{avg}：平均诊断覆盖率(Average diagnostic converage)

E/E/PES：电气/电子/可编程电子系统(Electrical/Electronic/Programmable System)

EMC：电磁兼容性(Electro magnetic compatibility)

FB：功能块(Function block)

I/O：输入/输出(Input/Output)

LVL：有限可变语言(Limited variability language)

$MTTF_d$：平均危险失效时间(Mean time to dangerous failure)

PFH_D：每小时危险失效概率(Probability of dangerous failure per hour)

PL：性能等级(Performance level)

PL_r：所需的性能等级(Requirement of performance lever)

SIL：安全完整性等级(Safety integrity level)

SRASW：有关安全的应用软件(Security-related applications software)

SRCF：安全相关控制功能(Safety-related control function)

SRCS：安全相关控制系统(Safety-related control system)

SRESW：有关安全的嵌入式软件(Security-related embedded software)

SRP/CS：控制系统有关安全部件(Safety-related part of a control system)

SRS：安全相关软件(Safety-related software)

4　功能安全评估要求及流程

4.1　要求

4.1.1　为评估服务机器人 SRCS 是否达到功能安全要求，宜由一个评估组完成并且达成共识，该评估组应由具备不同学科知识、多种经验和专业技能的专家组成。明确实施项目的评估组组长，按照本标准开展风险评估工作并在执行过程中全面负责，将评估结果和(或)建议报告给相关人员。根据风险评估需要的技能和专业知识选择评估组成员。评估组应包括下列人员：

——能回答关于机械设计和功能方面技术问题的人员；

——具备机械操作、调试、保养、维修等实际经验的人员；

——了解类机器人产品事故历史的人员；

——熟悉有关法规、标准，包括 GB/T 15706—2012 以及与所评估机械有关的具体安全问题的人员；

——了解人为因素的人员。

不同的团队针对相似的情况的分析所形成的详细结果若存在差异，应尽量完善评估组的知识和专业技能，提高该风险评估结果的可信度。

4.1.2 应对服务机器人整体安全生命周期、电子/电气/可编程电子系统(E/E/PES)安全生命周期和软件安全生命周期的所有阶段进行功能安全评估。进行功能安全评估时应考虑在服务机器人整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期的每一个阶段中开展的活动和获得的输出并判断其是否满足第 5 章～第 9 章内容。

4.1.3 进行安全评估时应对服务机器人整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期活动及相关信息和设备(硬件和软件)所涉及的所有人员进行访问。

4.1.4 功能安全评估应贯穿于服务机器人整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期，并且可在每个安全生命周期阶段之后或在几个安全生命周期阶段之后开展，条件为在已确定的危险出现之前能采取一次功能安全评估。

4.1.5 如果把工具用作服务机器人整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期任何活动的评价或设计的一部分，这些工具本身应经受功能安全评估。

注 1：系统、编译器和主机目标系统可作为工具的例子。

注 2：评价使用这些工具的程度取决于这些工具对 E/E/PES 安全相关系统功能安全的影响。

4.1.6 功能安全评估应考虑如下内容：

——先前所做的功能安全评估工作(一般包括以前的安全生命周期阶段)；

——对整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期进一步执行功能安全评估的计划和战略；

——对先前的功能安全评估的建议以及已做更改的程度。

4.1.7 对于服务机器人整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期不同阶段的功能安全评估应制定计划并保持一致。

4.1.8 功能安全评估活动计划应规定：

——承担功能安全评估的各方；

——每次功能安全评估的输出；

——功能安全评估的范围(在建立功能安全评估的范围时，有必要规定用作每个评估活动输入的文档和它们的状态)；

——所涉及的安全主体；

——要求的资源；

——承担功能安全评估各方的独立水平；

——与应用相关的承担功能安全评估各方的能力。

4.1.9 在进行功能安全评估之前，功能安全评估计划应得到执行功能安全评估的各方和负责正在评估的安全生命周期各阶段功能安全管理的各方的批准。

4.1.10 在功能安全评估结束时应做出接受、有条件地接受或不接受的建议。

4.1.11 承担功能安全评估的各方应能够胜任其工作。

4.1.12 除非在应用领域的标准中另有说明，进行功能安全评估的人、部门或组织的最低独立水平应符合表 1 和表 2 的规定。表 1 和表 2 中的相关内容说明如下：

——HR：它所规定的独立水平为规定的后果(表 1)或安全完整性等级(表 2)而极力推荐的最低等级。如果使用更低的独立水平则应详细说明不适用 HR 水平的理由。

——NR：它所规定的独立水平对于规定的后果(表 1)或安全完整性等级(表 2)而言，被认为不够，并不推荐此等级。如果采用该独立水平则应详细说明其理由。

——“/”：不推荐或反对使用的规定独立水平。

注 1：应用表 1 之前，参见应用领域中现有的好的做法，以便定义后果的种类。这些后果出现在要求操作时 E/E/PES 安全相关系统的失效事件中。

注 2：在公司内部，可根据公司的机构和专家的情况而定。如要求独立的人和部门则不得不请某个外部的组织。相反，如果公司存在熟悉风险评估和安全相关系统应用的内部组织，该组织为独立并且与公司负责开发的主要组织分开(用管理或用其他资源等方法)，则可使用它们自身的资源满足独立组织的要求。

注 3：对于独立的人、独立的部门和独立的组织的定义分别参见 GB/T 20438.4—2017 的 3.8.11、3.8.12 和 3.8.13。

4.1.13 在表 1 和表 2 中，使用 HR^1 或 HR^2(不能两个都用)，取决于特定应用领域的诸多因素，如果可以使用 HR^1，则 HR^2 被认为不需要；如果 HR^2 可用，则 HR^1 被认为 NR(不推荐的)。如果应用领域没有标准，应详细说明选择 HR^1 或 HR^2 的理由。选择 HR^2 比选择 HR^1 更合适的因素包括：

——相同设计的经验不足；

——复杂程度很高；

——设计新颖度很高；

——技术新颖度很高；

——设计特征标准化程度不足。

4.1.14 在表 1 中，最低独立水平应基于具有最高安全完整性等级的 E/E/PE 安全相关系统执行的安全功能。

表 1 执行功能安全评估各方的最低独立水平

最低独立水平	后果(见 4.1.12 的注 2)[a,b]			
	A	B	C	D
独立的人	HR	HR^1	NR	NR
独立部门	/	HR^2	HR^1	NR
独立组织 (见 4.1.12 的注 2)	/	/	HR^2	HR

[a] 详细说明见 4.1.12(包括注)和 4.1.13。

[b] 典型的后果：后果 A——较轻的伤害(如功能的暂时丧失)；后果 B——对一个或多个人的严重的、永久的伤害、致一人死亡；后果 C——致 2 人以上死亡；后果 D——致使 10 人以上死亡。

表 2 进行功能安全评估各方的最低独立水平

最低独立水平	安全完整性等级(SIL)[a,b]			
	1	2	3	4
独立的人	HR	HR^1	NR	NR
独立部门	/	HR^2	HR^1	NR
独立组织 (见 4.1.12 的注 2)	/	/	HR^2	HR

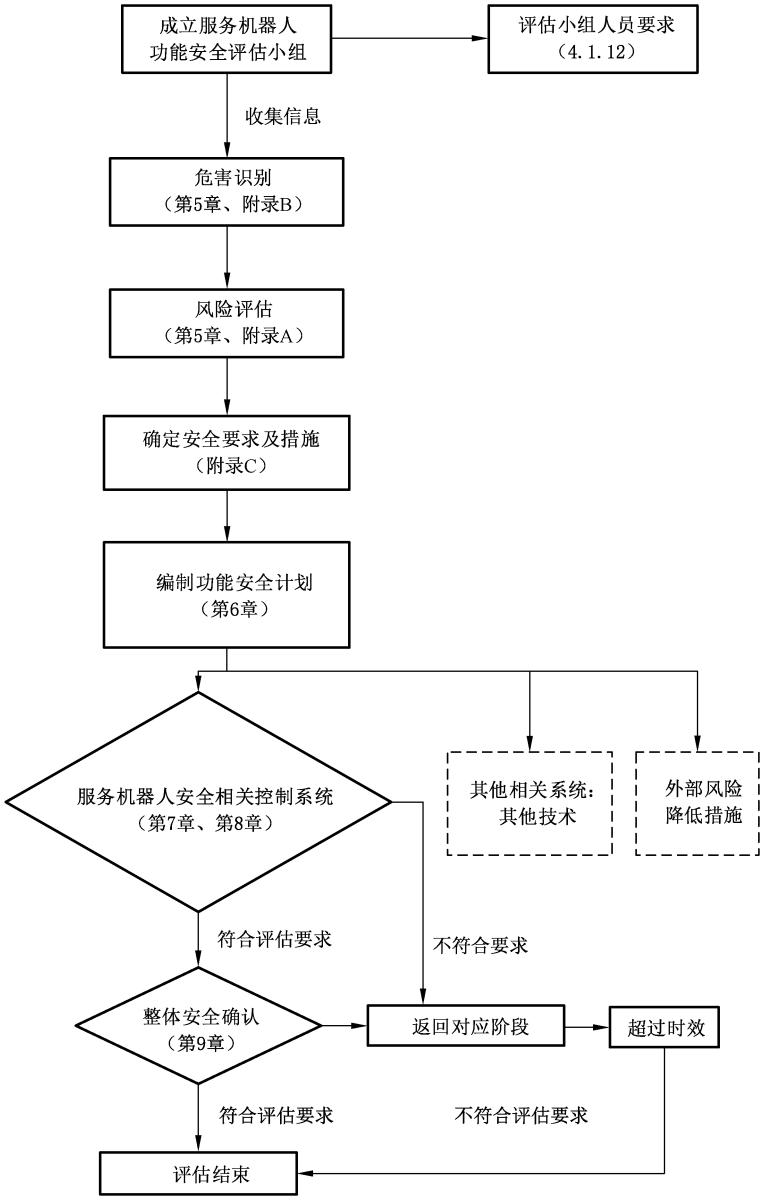
[a] 详细说明见 4.1.12(包括注)、4.1.13 和 4.1.14。

[b] SIL 等级的确认方法见附录 A。

4.2 功能安全评估流程

在进行服务机器人安全相关控制系统功能安全评估过程中，应符合图 1 所示流程，评估流程的详细

内容见表3。



说明：虚框部分的技术内容不在本标准的范围之内。

图1　服务机器人功能安全评估流程

表3　服务机器人功能安全评估流程及概述

序号	流程节点	目的	范围	要求	输入	输出
1	成立服务机器人功能安全评估小组	执行服务机器人功能安全相关系统评估，判断被评估对象是否达到功能安全要求	服务机器人功能安全相关系统	4.1.12	服务机器人相关信息	组织结构、组员分工及工作计划

表 3（续）

序号	流程节点	目的	范围	要求	输入	输出
2	危险识别	识别服务机器人可能出现的特定的任何危险	服务机器人可能出现的所有危险项	第 5 章及附录 B	功能描述、应用场景、服务对象	被识别的危险项
3	风险评估	对危险项定性、定量的分析，确定服务机器人安全相关控制系统的安全完整性等级	安全相关控制系统、其他相关系统、外部风险	第 5 章及附录 A	被识别的危险项	风险评估报告
4	确定安全要求及措施	保护操作者之外的人、动物或者其他安全相关物体不受任何伤害，确保操作者的安全	安全相关控制系统、其他相关系统、外部风险	附录 C	风险评估报告	安全相关控制系统的安全要求及措施
5	编制功能安全计划	规范服务机器人安全相关控制系统的设计、整合、检验和确认过程	安全相关控制系统	第 6 章	安全相关控制系统的安全要求及措施	功能安全计划
6	服务机器人安全相关控制系统	规范服务机器人安全相关控制系统的设计及实现	安全相关控制功能及系统	第 7 章、第 8 章	功能安全计划、功能描述、硬件及软件实现方案	关于“设计及实现”的评估报告
7	整体安全确认	用于功能安全相关控制系统的确认程序的要求	所有功能安全相关控制系统操作和维护程序以及控制要求	第 9 章	设计及实现评估报告、安全要求检验和确认方法	检验和确认报告
8	评估结束	/	/	/	设计及实现评估报告、检验和确认报告	功能安全评估报告

5 危险识别和风险评估

5.1 概述

风险评估均采用 GB/T 15706—2012 为其提供要求和指导，包括基于危险识别的风险分析，服务机器人的危险种类见附录 B。

5.2 危险识别

每一个设计过程都应有特定的危险识别，危险识别应能够识别服务机器人中可能出现特定的任何

危险。附录 B 包含了一份典型的危险清单，这些危险均为服务机器人可能出现的危险。当然，这一列表未包含所有的危险可能性，如：

a) 服务机器人系统可能因为其特殊设计具有的其他危险；
b) 使用造成的其他危险；
c) 可预见的误用；
d) 机器人自主决策可能出现的不可确定性带来的危险：
   1) 机器人自主决策的不确定性和错误决策；
   2) 知识水平、经验和身体状况不同的用户以及其他接触的人；
   3) 正常但意外的服务机器人运动；
   4) 预期外的运动。

5.3 风险评估

风险评估应考虑服务机器人在整个安全生命周期中所处的危险环境，并仔细注意在各种情况下，服务机器人可能会接触到的与安全有关的物体。风险评估过程见图 2。

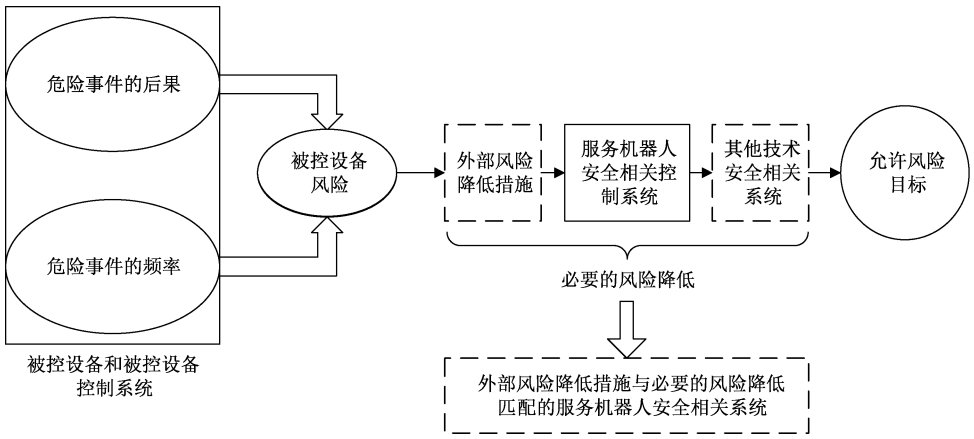


图 2 服务机器人风险评估过程

在采用所有安全设计和保护措施以后，其他风险对于服务机器人，应被评估并证明它已被降至可接受的水平。

应根据具体情况，设计适当的风险评估方法。应根据该事件进行评估（例如：允许机器人与安全设备或其他与安全有关的物体接触），评估结果不会造成任何不可接受的风险。

如果使用其他方法的风险参数用于风险评估，那么应检验其是否恰当。

6 功能安全管理

6.1 目的

本章规定了为达到 SRCS 所要求的功能安全所必需的管理和技术工作。

6.2 要求

6.2.1 起草功能安全计划

对于每个 SRCS 设计项目，都应起草功能安全计划，并形成文档，必要时，应及时更新。该计划应包括第 5 章～第 9 章规定的运行控制程序。

功能安全计划内容应根据具体情况而定，其中包括：

a） 项目规模；

b） 复杂程度；

c） 设计和技术新颖程度；

d） 设计特点标准化程度；

e） 如果失效可能的后果。

起草功能安全计划时应注意：

a） 确定第7章～第9章规定的有关活动。

b） 描述为满足规定的功能安全要求而采取的方针和策略。

c） 描述为实现应用软件、开发、集成、检验和确认的功能安全的措施。

d） 确定第7章～第9章中规定对执行和检查各项工作负责的人员、部门或者其他单位和资源。

e） 确定或建立相关程序和资源以便记录和维护同SRCS功能安全相关的信息（参见附录D），如：

1） 危险识别和风险评价的结果；

2） 用于安全相关功能及其安全要求的设备；

3） 负责维护功能安全的机构；

4） 达到和保持功能安全（包括SRCS修改）所需的程序。

f） 描述考虑相关机构问题时的配置管理（参见附录E）策略，例如：被授权的人及该机构的内部结构。

g） 建立检验计划，应包括：

1） 进行检验的细节；

2） 执行检验的人员、部门或单位的详细情况并设立相应的负责人；

3） 检验策略和技术的选择；

4） 试验设备的选择和使用；

5） 检验活动的选择；

6） 验收准则；

7） 用于评估检验结果的方法。

h） 建立确认计划，其中包括：

1） 进行确认的细节；

2） 机器操作有关模式（如正常操作、设置）的确定；

3） 参照受检验的SRCS的要求；

4） 适用于确认的技术策略，例如：分析方法或统计试验；

5） 验收准则；

6） 出现失效时采取的行动，以满足验收要求。

注：确认计划应指出SRCS及其子系统是否进行常规测试、形式测试和（或）抽样测试。

6.2.2 实施功能安全计划

实施功能安全计划，应确保立即跟踪，并完满地解决由于下列原因造成的SRCS相关的问题：

——第7章～第9章规定的活动；

——检验活动；

——确认活动。

7 安全相关控制功能规范要求（SRCF）

7.1 目的

本章规定由SRCS执行SRCF的要求。

7.2 SRCF 要求规范

7.2.1 概述

7.2.1.1 减少风险的措施

依据附录 C 中提出的风险降低策略，安全功能的任何需要应被确定。因此，应主要采用以下两种保护措施减少风险：

——减少在元件级的故障概率。其目的为减少影响安全功能的故障或失效的可能性。可通过增加元件可靠性来实现，例如：为了把致命故障或失效减到最少或排除故障（见 GB/T 16855.2），选用经检验的零件和（或）应用经检验的安全原则。

——改善控制系统有关安全部件（SRP/CS）的结构，其目的为避免故障的危害影响。一些故障可以检测到，而且需要冗余和（或）监测结构。

可单独或组合应用这两种措施。对某些技术，通过选择可靠的零件或排除故障可实现风险减少；但对于其他技术，可能需要冗余和（或）监测系统来实现风险减少。另外，还应考虑共因失效（CCF）。

7.2.1.2 一般要求

如果被选择的安全功能由 SRCS 执行（全部或部分地），那么，应规定相关 SRCF。

各 SRCF 规范应包括：

——功能要求规范（见 7.2.3）；

——安全完整性要求规范（见 7.2.4）。

上述项目应在安全相关软件（SRS）中形成文件。

注 1：当非电气设备结合电气手段执行安全功能时，本标准将不考虑应用于非电气设备的目标失效值。电气手段涵盖了所有依据电气原理操作的装置和系统，包括：

——机电装置；

——非可编程电子装置；

——可编程电子装置。

注 2：SRS 需要按照版本控制，作为配置管理程序的一部分（参见附录 E）。

安全要求规范应经过检验确保在预期应用中的一致性和完整性。

注 3：例如：它可以通过检验、分析、核对表获得。参见 GB/T 20438.7—2017 中 B.2.6。

7.2.2 可用信息

应使用下列信息制定各 SRCF 功能要求规范和安全完整性要求规范：

——服务机器人风险评价结果应包括针对各种特定危害的风险降低过程所必需的所有安全功能。

——服务机器人操作特性，包括：

- 操作模式；
- 循环时间；
- 响应时间性能；
- 环境条件；
- 人机交互（例如：指令识别、语音、表情、触摸屏、肢体手势等）；
- 维护（例如：清洁、维修等）。

——所有和 SRCF 相关的信息，都可能影响 SRCS 的设计，例如：

- SRCF 预期实现或防止的机器行为的描述；
- SRCF 之间以及 SRCF 与任何其他功能（无论机器内外）之间的所有界面；

- SRCF 要求的故障反应功能。

注：在开始 SRCS 重复设计过程前，有些信息可能不可用或未被充分定义，故在设计过程中，可能要求更新 SRCS 安全要求规范。

7.2.3 SRCF 功能要求规范

7.2.3.1 SRCF 功能要求规范应描述各个需要执行的 SRCF 的细节，包括：

——SRCF 应激活或禁用的机器条件（例如：操作模式）；

——可能同时激活，但会造成冲突动作的那些功能之间的优先权；

——各 SRCF 的工作频率；

——各 SRCF 要求的响应时间；

——SRCF 同其他机器功能之间的接口；

——要求的响应时间（例如：输入、输出装置）；

——各 SRCF 的描述；

——故障反应功能以及机器重新启动或继续运转等操作的各种限制的描述，以防初始故障即导致机器停止运行；

——工作环境描述（例如：温度、湿度、灰尘、化学物质、机械振动和冲击）；

——试验以及各种相关设施（例如：试验设备、试验接入端口）；

——预期用于 SRCF 机电装置的操作循环周期、工作循环周期和（或）使用类别。

7.2.3.2 计划用于电磁环境的 SRCS（例如：住宅）应符合 GB/T 37283 的要求。

7.2.4 SRCF 的安全完整性要求规范

7.2.4.1 每个 SRCF 的安全完整性要求应来自风险评估，以确保达到必要的风险降低。本标准安全完整性要求表示为 SRCF 每小时危害失效概率的目标失效值。

7.2.4.2 每个 SRCF 的安全完整性要求应按照 GB 28526 依照 SIL 规定并形成文档。方法实例见附录 A。当要求的 SRCF 安全完整性低于 SIL1 时，应符合 GB/T 16855.1 最低要求的 B 类。

7.2.4.3 如果产品标准为 SRCF 规定了 SIL，该规定应优先于附录 A。

7.3 SRCS 的要求

7.3.1 要求的安全性能

通过控制系统执行保护措施的安全性能应符合本章要求。服务机器人控制系统功能的性能等级（PL）要求或安全完整性等级（SIL）要求应通过 8.3.1 或 5.3 确定，并应符合 GB/T 16855.1 的要求。该过程应包含检验和确认。

7.3.2 机器人停止功能

服务机器人遇到障碍物、人等，应具备停止或绕开功能；制动性能（减速）满足安全要求，不会产生对障碍物、人等造成伤害的撞击或发生其他危害。

机器人在设计时，应考虑安全停止，确保在任意速度下的故意刹车，不会发生翻车、失控或者机器人零件和载荷的落下等产生危险的情形。停止状态可以根据服务机器人类型而变化，因此机器人的停止状态由服务机器人制造商决定。

7.3.3 操作空间的限制

可通过操作空间的限制实现风险降低，包括：

——限制服务机器人在限定范围内运动；或

——防止机器人进入该限制空间。

如果通过软件限制能够实现服务机器人在额定负载和速度下停止，允许使用该手段定义和减少限制空间。

产品不同行为对空间的要求需在用户使用说明或其他途径进行明确。

7.3.4 安全相关的速度控制

通过风险评估确定服务机器人速度的限值，超过该限值服务机器人可能产生的危害。速度可以通过计算服务机器人可触及运动部件的代表位置点的速度确定。只有经授权人员允许才能调整最大速度。

根据服务机器人执行任务的不同，可以设定不同的速度限值。改变速度限值应基于风险评估。

服务机器人的速度应确保其运动部件的速度不会超过安全相关的速度要求。

对安全相关的环境感知应符合 ISO 13482:2014 中的 6.1，执行这个功能时，应避免危害碰撞，包括人、动物以及安全相关的物件。

7.3.5 稳定性控制

服务机器人应在所有预期和合理可预见的使用情况下保持稳定，稳定性功能安全性能应符合 ISO 13482:2014 中的 6.1。

7.3.6 安全相关的力的控制

服务机器人的任何部件，对人或其他与安全有关的物体施加的力，应在最大安全接触力限制范围之内加以控制。对最大安全接触力或者扭矩的定量要求应通过符合人体工程学的实验仔细检查确认。

7.3.7 机器人急停

在任何情况下，急停功能都应为可用和可操作的，在服务机器人的各种运行模式中，该功能应优先于所有其他功能，并且不应削弱为解脱陷入危险人员而设计的任何便利性。

急停功能不应用于代替安全防护措施和其他安全功能，而宜设计作为一种补充防护措施。

根据风险评估，急停功能的设计应使得在急停装置动作后，以合适的方式停止服务机器人的危险运行和操作，而不产生附加风险，并且无需任何人的进一步干预。

合适的方式可包括：

——选择最合适的减速率；

——应用预定的停机顺序。

急停功能的设计应符合服务机器人操作者做出使用急停装置的决定时，无需考虑急停产生的后果。

7.3.8 用户界面的设计

当控制设备（例如：操纵杆、操作控制面板、语音和手势识别系统以及其他设备）被用于控制服务机器人时，它们在操作过程中应具有适当的可靠性。

该命令装置固定或不固定在服务机器人上，其对机器人的电气连接应不会造成危险。

在手动和半自主机器人控制模式中，命令设备应提供单独或组合的机器人功能控制。

7.3.9 运行模式

服务机器人应被设计成在一个特定的模式下进行操作，如果风险评估显示自动/手动两种模式之间的切换存在潜在的危害，那么机器人将在模式改变之前立即执行停止功能。该模式不应自行切换或造成其他危害。对于所有运行模式，应明确哪些安全功能可用，哪些禁用。

服务机器人的运行模式包括：自主模式、手动模式、半自主模式和维护模式。

7.3.10 手动控制设备

在手动控制机器人实现相关部件启动或动作时，服务机器人应设计有醒目的手动控制装置和操作界面。

7.3.11 其他

以上未提及的服务机器人 SRCS 的要求，但在进行风险评估中被确认需要执行的 SRCS 的要求，应根据生产厂商或使用者的具体需求设计实现。

8 安全相关控制系统(SRCS)设计与整合

8.1 目的

SRCS 设计或选择要求，以满足安全要求规范中规定的功能和安全完整性要求。

8.2 一般要求

按 GB/T 16855.1 的规定，服务机器人 SRCS 的选择或设计(包括总体硬件、软件体系结构、传感器、执行元件、可编程电子器件、嵌入式软件，应用软件等)均应符合下列要求：

a) 识别 SRCS 执行的每种安全功能所需要的 PL，见附录 A。

b) 每种安全功能技术实现的要求：

1) 硬件系统要求；

2) 软件系统要求；

3) 系统确认。

c) 在设计和集成时，应考虑可维护性和可测试性，以便执行 SRCS 的这些特性。SRCS 设计，包括诊断和故障反应功能，应形成文件，文件应：

1) 精确、完整、简明；

2) 适合预期目的；

3) 可存取、可维护；

4) 版本可以控制。

d) 在 SRCS 设计、开发和执行期间，执行的工作结果应在适当阶段验证。

8.3 每种安全功能技术实现的要求

8.3.1 硬件要求(性能等级)

服务机器人执行安全相关控制系统中安全相关功能的技术为液压、机电、可编程电子等，服务机器人 SRCS 的有关安全部件完成安全功能的能力通过确定 PL 表示。对于所选的完成安全功能的每个 SRCS 和(或)SRCS 的组合，都应完成其 PL 的估计。

应通过估计以下参数确定 SRP/CS 的 PL：

——单个元件 $MTTF_d$ 的值；

——DC；

——CCF；

——结构；

——安全功能在故障条件下的性能；

——有关安全的软件；

——系统性失效；

——预期环境条件下，完成安全功能的能力。

图 3 给出了与每个通道的 $MTTF_d$ 组合的类别以及为了达到安全功能要求的 PL 的 DC_{avg} 的选择。

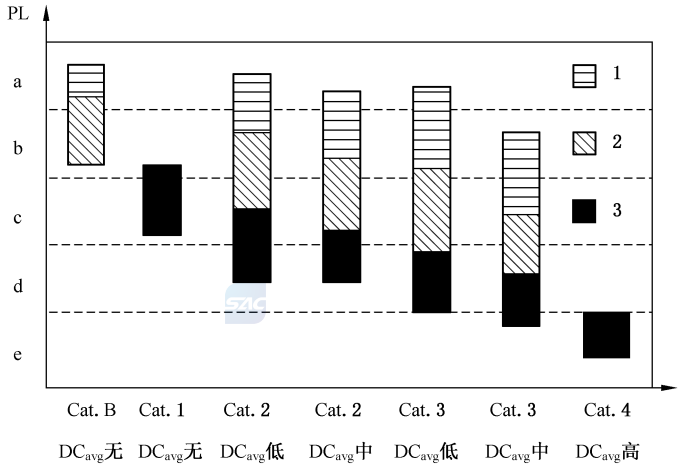
对于 PL 的估计，图 3 给出了与 DC_{avg} 一起的类别（水平轴）和每个通道的 $MTTF_d$（柱形图）。图中的阴影代表了每个通道的 $MTTF_d$ 的 3 个范围（低、中、高），它可选择用于达到要求的 PL。

使用图 3 中的简单方法应确定 SRCS 的类别以及每个通道的 DC_{avg} 和 $MTTF_d$。

对于类别 2、类别 3 和类别 4，应采用足以防止共因失效的措施。

考虑到这些参数，图 3 提供了确定由 SRCS 实现的 PL 的方法图解。类别（包括共因失效）和 DC_{avg} 的组合确定选择图 3 中的那一列。根据每个通道的 $MTTF_d$，应选出有关直方柱的 3 个不同阴影区域中的一个。

这些区域的纵向位置确定能在竖轴上读出的要求的 PL，如果该区域有两种或三种可能的 PL，表 4 中给出了所达到的 PL。数字更精确的 PL 的选择取决于每个通道 $MTTF_d$ 的精确值。



说明：

PL ——性能等级；

1 ——每个通道的 $MTTF_d$ = 低；

2 ——每个通道的 $MTTF_d$ = 中；

3 ——每个通道的 $MTTF_d$ = 高。

图 3 PL 和每个通道的类别、DC_{avg} 和 $MTTF_d$ 的关系

表 4 估计由 SRCS 达到的 PL 的简单程序

类别	B	1	2	2	3	3	4
DC_{avg}	无	无	低	中	低	中	高
每个通道的 $MTTF_d$							
低	a	不包括	a	b	b	c	不包括
中	b	不包括	b	c	c	d	不包括
高	c	c	c	d	d	d	e

对于复杂电子，服务机器人 SRCS 可按 GB 28526—2012 中的第 6 章，确定性能等级所对应的安全完整性等级。

8.3.2 软件要求

8.3.2.1 一般要求

有关 SRCS 的嵌入式软件或应用软件的所有生命周期内的活动，应主要考虑避免软件生命周期内出现的故障（见图 4）。以下要求的主要目标为易读、易理解、可测试及可维护的软件。

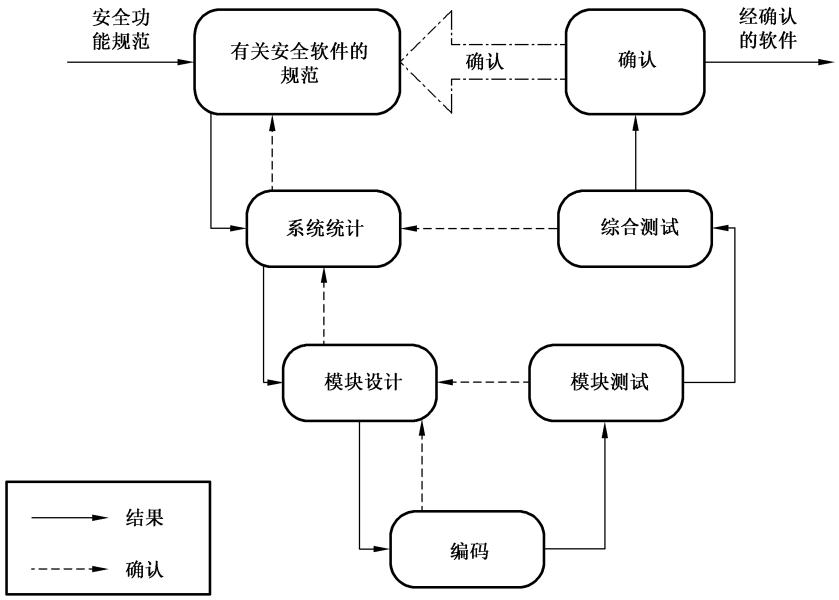


图 4 软件安全生命周期的简单 V 模型

8.3.2.2 有关安全的嵌入式软件（SRESW）

对于用于 PL_r 为 a～d 的元件的 SRESW，应采用以下基本方法：

——对软件安全生命周期内的活动进行检验和确认，见图 4；

——对技术规范和设计进行归档；

——模块化和结构化设计和编码；

——系统性失效的控制；

——使用基于软件方法用于诊断随机的硬件失效时，正确执行的检验；

——功能测试，例如：黑盒子测试；

——修改后，合适的软件安全生命周期内的活动。

对于用于 PL 为 c 或 d 的零件的 SRESW，应采用以下附加方法：

——满足一定的计划管理和质量管理系统的要求；

——对软件安全生命周期内所有的相关活动进行归档；

——用以识别所有的结构项目和与 SRESW 有关的释放文件的结构管理；

——符合安全要求和设计的结构规范；

——使用合适的编程语言和便于使用的基于计算机的工具；

——模块化和结构化编程，区别于非有关安全软件、具有充分定义接口的受限模块大小，采用设计和编码标准；

——用控制流程分析，通过遍查/复查来验证编码；

——扩展的功能测试，例如：灰盒子测试、性能测试或仿真；

——冲击分析以及修改后软件安全周期内适当的活动。

对于 PL_r＝e 的元件，SRESW 应符合 GB/T 20438.3—2017 中第 7 章的要求。在规范、设计和编码中采用多性时，对于用在类别 3 或类别 4 的 SRP/CS 中的两个通道，可用上述用于 PL_r 为 c 或 PL_r 为 d 的方法达到 PL_r＝e。

注 1：这类方法的具体描述参见 GB/T 20438.7。

注 2：对于在设计和编码中具有多样性的 SRESW，类别 3 或类别 4 的 SRCS 使用的零件，通过只考虑结构方面代替每行编码的检查来复查软件局部等方法可减小采取措施避免系统性失效这方面的努力。

8.3.2.3 有关安全的应用软件（SRASW）

软件安全生命周期（见图 4）适用于 SRASW。

满足以下要求并且以 LVL 编写的 SRASW，可使 PL 达到 a～e。如果在一个元件中的 SRASW 的一部分影响到几种 PL 不同的安全功能，则应采用与最高 PL 有关的安全要求。用于 PL_r 为 a～e 的零件的 SRASW，应采用以下基本措施：

——对开发周期进行检查和确认，见图 4；

——对技术规范和设计进行归档；

——模块化和结构化编程；

——功能性测试；

——修改后适当的开发。

对用于 PL_r 为 c～e 的元件的 SRASW，应采用或推荐采用以下提高效率的附加措施（较低效率用于 PL_r 为 c，中等效率用于 PL_r 为 d，较高效率用于 PL_r 为 e）：

a) 应复查有关安全软件的技术规范，使生命周期内涉及的所有人员可得到该规范，且应包括以下内容的描述：
   1) 具有要求的 PL 的安全功能以及相关的工作模式；
   2) 性能准则，例如：反应时间；
   3) 具有外部信号界面的硬件结构；
   4) 外部失效的探测和控制。

b) 工具、库和语言应选择：
   1) 可放心使用的合适工具：对于达到 PL＝e 的一个元件及其工具，该工具应符合适当的安全标准；如果使用了带有不同的工具的两种不同零件，则可放心使用。采用的技术特征应能检测可导致系统性错误（例如：数据类型不匹配、意义不明确的动态存储地址、不完善的命令界面、递归、指针算法等）的条件。检查宜主要在编译时间内不能仅在运行时间内进行。工具宜加强语言子集和编码指南，或者至少督促或引导开发者使用它们。
   2) 只要合理可行，宜采用经确认的功能模块（FB）库—工具制造商提供的有关安全的功能模块（FB）库（PL＝e），或符合本标准且用途已被确认的详细功能模块（FB）库。
   3) 宜采用合理的适用于模块化方法的 LVL-子集，可包括 GB/T 15969.3 中认可的语言子集。强烈推荐采用图示语言（例如：功能模块图、梯形图）。

c) 软件设计的特征应为：
   1) 半正式的方法描述数据和控制流，例如：状态图或程序流程图；
   2) 主要由源自有关安全的经确认的功能模块库的功能模块实现模块化和结构化设计；
   3) 限制了编码大小的功能模块；
   4) 编码在功能模块内执行，功能模块宜有一个入口和一个出口点；

5） 三个阶段的结构模型，输入→处理→输出（见图 5）；

6） 在唯一一个程序位置安全输出的安排；

7） 使用用于检测外部失效的技术和用于在输入、处理和输出模块内置于安全状态的预防性编程技术。

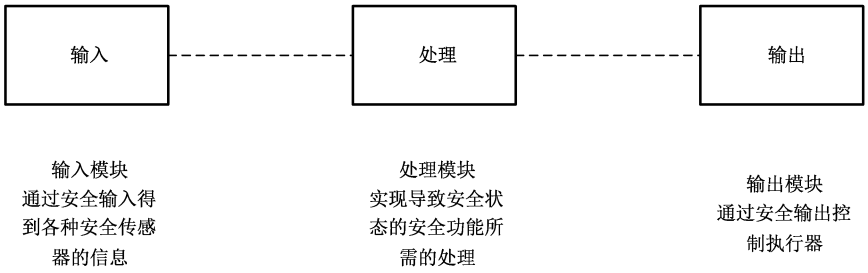


图 5 软件的一般结构模型

d） 当 SRASW 和非 SRASW 组合在一个元件中时：

1） SRASW 和非 SRASW 应在与有明确定义的数据链接的不同 FB 中编码；

2） 不应存在非有关安全数据和有关安全数据的逻辑组合，因为这可导致有关安全信号的完整性下降。例如：结构控制有关安全信号的地方采用逻辑“非”组合有关安全和非有关安全的信号。

e） 软件执行/编码：

1） 代码宜易读、易懂及可测试，为此宜使用符号变量（代替显式硬件地址）；

2） 应使用合理的或公认的编码指南；

3） 宜使用应用层（预防性编程）可用的数据完整性和真实性检查（例如：范围检查）；

4） 代码宜接受仿真测试；

5） PL＝d 或 PL＝e 时，宜通过控制和数据流分析检验。

f） 测试：

1） 合适的确认方法为功能性行为和性能准则（例如：时序性能）的黑盒子测试；

2） PL＝d 或 PL＝e 时，推荐由分析边界值开始进行试验；

3） 宜制定试验计划，且宜包括具有完成准则和所需工具的试验用例；

4） I/O 测试应保证在 SRASW 内正确使用有关安全信号。

g） 文件：

1） 应对所有生命周期和修改活动进行归档；

2） 文件应完整、可用、易读和易懂；

3） 源程序正文中的代码文档应包括具有合法实体的模块标题，功能和 I/O 描述，版本和所使用的库函数模块的版本，以及网络/声明及公告中足够的注释。

h） 验证：如复查、检查、遍查或其他的合适活动。

i） 结构管理：宜建立程序和数据的备份，以识别和归档文件、软件模型、验证/确认结果以及与 SRASW 具体版本有关的工具结构。

j） 修改 SRASW 后，应进行影响分析以保证规范性。修改后应执行合适的生命周期内的活动。应控制修改访问权限且应归档修改历史。

注：修改不影响已在使用的系统。

k） 验证仅针对专用代码，对于经验证的库函数则不必重复验证。

8.3.2.4 基于软件的参数化

应考虑把基于软件的有关各参数进行参数化，作为软件安全要求规范中要描述的 SRCS 设计的一

个方面。采用 SRCS 供应商提供的专门软件工具进行参数化。该工具应有自己的标识(名称、版本等)且防止未经授权的修改,例如:采用密码。

应保持所有用于参数化的数据的完整性。这应通过采取措施控制以下方面来达到:

——控制有输入的范围;

——传输前控制数据损坏;

——从参数传输进程中控制错误的影响;

——控制完整参数传输的影响;或

——控制参数化所用工具的硬件和软件故障和失效的影响。

参数化工具应符合对 SRCS 的所有要求,可使用特别的程序设定有关安全参数。该程序应包括通过以下两种方式之一确认 SRP/CS 的输入参数:

——修改后的参数重新发送至参数工具;或

——确认参数完整性的其他合适方式。

包括随后的确认,例如:通过合适的技术熟练人员确认、通过参数化工具自动检查的方式确认等。

注 1:当使用不是专门预定用于该目的的装置进行参数化时,这一点尤其重要(例如:个人电脑或相当的装置)。

在传输/转发过程中,用于编码/译码的软件模块以及用户用于有关安全参数可视化的软件模块,应至少在功能方面采用多样性以避免系统性失效。

注 2:基于软件参数化的文件显示所使用的数据(例如:预定义的参数集),用于识别与 SRCS 有关的参数所必需的信息,完成参数化的人员以及其他相关信息(例如:参数化日期)。

注 3:对基于参数化的软件进行以下的检验:

——检验每个有关安全参数的正确设置(最小值、最大值和典型值);

——检验有关安全参数是否进行了合理性检查,例如:使用无效值等;

——检验是否防止了有关安全参数未经授权的修改;

——检验用于参数化的数据/信号的产生和处理是否能够保证不导致安全功能丧失。

8.3.3 系统确认

8.3.3.1 概述

确认 SRCS 有关安全部件提供的安全功能是否符合其规定特性,根据技术规范要求,确认与安全相关的输出信号的正确性,以及与输入信号的逻辑相关性。应确认 8.3.3.2～8.3.3.9 的试验项目。

8.3.3.2 有关安全停止功能

有关安全的停止功能(例如:由安全防护装置触发)制动后,一旦有必要,应使机器进入安全状态。这种停止功能应优先于由操作原因引起的停止。

服务机器人一般包含速度控制、超速停止功能、避障停止功能,触碰开关停止功能、紧急停止功能、导航绕行功能等紧急停止功能测试,具体测试方法如下:

a) 速度测试:在平坦、干燥的水泥路面上、室内平整的地面上进行,在手动/自动控制模式下,使机器人以正常速度、最大速度运行,测试机器人的正常速度与最大速度。

b) 超速测试:使机器人以超过最高运行速度的情况下,测试机器人是否会停止运行。

c) 避障停止功能测试:在手动/自动控制模式下,避障停止功能测试为服务机器人在直线轨迹上以规定速度自动运行,通过障碍物触发避障传感器(激光/超声波等),引起服务机器人保护性停止,测试从停止位置到障碍物位置的距离。

d) 触碰开关功能测试:在手动/自动控制模式下,触碰开关停止功能测试为规定速度运行的服务机器人,在直线轨迹上预先标志的地点按下触碰开关按钮后,机器人应紧急停止,并保持停止状态直至系统重启。

e) 紧急停止功能测试：根据 GB/T 16855.1—2018 中表 8 的规定，急停功能应按附加要求中 GB/T 16754 规定检测，急停功能在任何时间都应可用和可操作，在机器的各种运行模式中，该功能应优先于所有其他功能，并且不应削弱为解脱陷入危险人员而设计的任何便利性。直到急停功能手动复位以前，任何启动指令（预定的、非预定的或意外的）对由于急停功能的作用而停止的那些操作应无效。

f) 导航和绕行功能测试：

1) 导航功能测试，导航功能为机器人导航运动模块依靠定位摄像头/激光传感器、底盘轨迹推算提供的信息，通过避障传感器等感知周围障碍物，通过应用端获取导航运动或者舞蹈运动任务，并依靠路径规划模块、舞蹈解析模块等子系统实现有加减速限制的机器人自主运动；

2) 绕行功能测试，通过在机器人运行轨迹上设置障碍物，触发机器人避障传感器避障功能，从而激发机器人的导航模块自动修正行驶轨迹，并实施绕行的机器人功能测试。

8.3.3.3 手动复位功能

防护装置发出停止指令后，停止状态应保持到有安全重启状态为止，通过复位防护装置，解除停止指令，再重新恢复安全功能。

手动复位功能应：

——通过 SRCS 内的一个独立的手动操作装置提供；

——只有所有安全功能和防护装置处于工作状态时才能实现复位；

——自身不能引起移动或危险状态；

——谨慎操作；

——使控制系统能接受独立的启动指令；

——只有制动器从其接通（on）位置脱开才能完成。

提供手动复位功能的有关安全部件 PL 的选择，应使得手动复位功能不削弱相关安全功能的安全要求。

8.3.3.4 启动/重启功能

只有危险状态不可能存在的情况下，重启功能才能自动发生。

启动和重启的规定也适用于能够遥控的服务机器人。

8.3.3.5 局部控制功能

当服务机器人通过诸如便携式控制装置或悬吊式操纵装置进行局部控制时，应符合以下要求：

——选用的局部控制应位于危险区之外；

——局部控制应只有在风险评价定义的区域才有可能触发危险状态；

——局部控制和主要控制之间的切换不应产生危险状态。

8.3.3.6 抑制功能

抑制功能不应导致任何人暴露于危险状况下。抑制期间安全环境应由其他方式提供。

抑制结束时，SRCS 的所有安全功能都应恢复。

提供抑制功能的有关安全部件的 PL 的选择应使得抑制功能不会削弱有关安全功能必需的安全水平。

8.3.3.7 响应时间

SRCS 的响应时间为机器全部响应时间的一部分。必需的机器全部响应时间能够影响有关安全部

件的设计，测试方法为按压机器人急停按钮或者触发机器人避障系统，测试机器人 SRCS 停止运动所需的时间。

8.3.3.8 有关安全的安全参数

当有关安全参数（例如：位置、速度、温度或压力等）偏离了当前的限制时，则控制系统应启动相应的措施（例如：启动停止功能、警告信号、警报等）。

如果 SRCS 中有关安全数据手动输入错误能够导致危险状态，那么应在 SRP/CS 中提供数据检查系统，例如：极限值、格式化和（或）逻辑输入值的检查。

8.3.3.9 能量源的波动、损失和恢复

当能量级的波动超出了设计工作范围时（包括能量供应损失），SRCS 应连续提供或触发能使机器系统其他部件保持安全状态的输出信号。

9 检验和确认

9.1 概述

在降低风险的过程中，所有与机器人安全有关的服务机器人性能值都应检验，包括在附录 C 中提到的有关控制系统需要的性能。

所有安全要求均应根据其相关检验标准进行检验，检验和检验方法的详细信息如下：

——A 检查：检查服务机器人或设备结构的状况，使用人类的感官而不需要任何专门的检查设备；当机器人不在操作时，检查通常在视觉或声学上进行的；

——B 实际测试：在正常和异常情况下测试服务机器人或其设备；功能测试（如故障注入测试）、循环测试（如耐力测试）、性能测试（如刹车性能测试）；

——C 测量：将服务机器人的性能的真实值与特定的极限值进行比较；

——D 在操作过程中观察：（如方法 A）在正常和异常情况下检查服务机器人或设备的功能，如额定载荷、过载情况和影响条件；

——E 检查电路图：通过结构或电路图的设计（如电气、气动、液压）和相关规范检查；

——F 软件检查：结构化检查，或通过软件代码的设计和相关的规范（代码检查或测试软件代码应该遵循的）；

——G 审查任务风险评估：结构审查或通过风险分析、风险评估和相关文件；

——H 检查布局图纸及相关文件：结构回顾或浏览布局设计图纸和相关文件。

9.2 安全要求检验和确认

安全要求检验和确认方法标准如表 5 所示，其中 A、B、C、D、E、F、G、H 代表的含义见 9.1。

表 5 危害项的安全要求检验和确认方法标准

序号	危害项	检验和确认
1	充电电池有关的危害	A、B、C、E、H
2	能量存储和供应的危害	A、B、C、E、H
3	系统启动和重新启动	B、D、F
4	静电势	B、C、E

表 5（续）

序号	危害项	检验和确认
5	机器人形状	A、C、G、H
6	噪声	C、D
7	电磁兼容	B、C、D
8	对身心健康的影响	A、C、D、H
9	机器人运动可能造成的危害	C、D、F、G
10	耐久性不足造成的危害	B、D、E、H
11	周围环境的影响	B、C、D、F、H
12	不正确的自主决策和行为造成的危害	B、C、D、F、G
13	与运动部件接触造成的危害	A、B、H
14	使用者对机器人缺乏认识	B、D、F、G
15	定位和导航方式	B、F、G

9.3 SRCS 确认

9.3.1 目的

用于 SRCS 的确认程序的要求，包括：检查和 SRCS 测试，以保证达到安全要求规范中陈述的要求。SRCS 确认可形成适用于服务机器人设计的确认活动的一部分。

9.3.2 一般要求

9.3.2.1 应按照预定计划执行 SRCS 确认。

注 1：有些情况，安全确认只能在安装后才能完成（例如：应用软件开发在安装后才能确定）。

注 2：可编程序的 SRCS 确认由硬件、软件要求确认组成。软件确认要求包括在 8.3.2 中。

9.3.2.2 SRCS 要求规范（见 7.2）中规定的各 SRCF、所有 SRCS 操作和维护程序应通过试验和（或）分析进行确认。

9.3.2.3 SRCS 安全确认的测试应形成恰当文档，对各 SRCF 应有下列陈述：

a） 安全确认计划使用的 SRCS 版本和试验的 SRCS 版本；

b） 在 SRCF 试验（或分析）中，在 SRCS 安全确认计划期间具体涉及规定的要求；

c） 使用的工具和设备连同校准数据；

d） 每次试验结果；

e） 期望结果和实际结果的差异。

9.3.2.4 产生差异时，必要时应进行纠正活动和重新测试，并形成文件。

9.4 SRCS 系统安全完整性确认

针对服务机器人控制系统的复杂程度，若为复杂电子设计，同时需达到 PL＝d 时，可使用 GB 28526—2012 相关设计要求，具体内容见 GB 28526—2012 第 6 章，同时需满足以下内容：

a） 在规范、设计和集成阶段暴露失效的功能测试，和在 SRCS 软件/硬件的确认期间应采用避免失效的功能测试。包括检验（例如：通过检查或试验）以评估 SRCS 是否受到保护，防止有害环境的影响，并应符合安全要求规范。

b) 干扰抗扰度测试用以保证 SRCS 能够满足电磁兼容相关要求。对于 SRECS 子系统或子系统元件不必执行电磁干扰的抗扰度测试，SRCS 对它的预期应用有足够的抗扰度，通过分析可以表现出来。

c) 要求的安全失效系数(Safe failure fraction)大于或等于 90%时应执行故障插入测试，这些试验应在 SRCS 硬件中引入或模拟故障，结果应形成文件。

此外，下列一个或多个考虑 SRCS 的复杂性和指定的 SIL 的分析技术组应适用：

a) 静态分析和失效分析；

b) 静态、动态分析和失效分析；

c) 模拟和失效分析。

此外，下列一个或多个考虑 SRCS 的复杂性和指定的 SIL 的测试技术组应适用：

a) 黑盒测试：在实际功能状态下的动态行为试验，从而暴露失效，满足 SRCS 功能规范，并评定 SRCS 的有效性和鲁棒性；

b) 如果安全失效系数小于 90%应执行故障插入(注入)测试。这些试验应在 SRCS 硬件中引入或模拟故障，其结果形成文件；

c) 应执行“最坏情况”测试，以评定用分析技术指定的极端(即最坏)情况；

d) 现场试验：使用来自不同应用的现场经验作为一种措施，以避免 SRCS 确认期间出现故障。

附 录 A
（规范性附录）
确定 SIL——风险图

A.1 一般要求

本附录描述了一种风险图方法，目的为说明一般原理。这种定性方法可以通过对与受控设备和受控设备控制系统有关的风险因素的了解确定服务机器人 SRCS 的 SIL。当风险模型符合表 A.1 中说明的内容时，这种方法尤为有效。

当采用定性方法时，为了简化问题，引用一些参数共同描述当服务机器人 SRCS 失效或不可用时危险情况的性质。选择合适的参数，将这些参数结合起描述分配到 SRCS 的 SIL。这些参数：

——允许对产生的风险进行合理的分级；

——包括关键风险评估因素。

A.2 危险事件分类

危险事件可参照附录 B 提供的示例，根据使用环境、实现功能、使用人群等不同，服务机器人可能产生的危险事件会有所变化，不局限于附录 B 所提供的内容，需与被测对象的生产商、使用者等共同确认。

通过对危险事件的不同参数分类及组合，可获得服务机器人 SRCS 的 SIL。对以下参数进行危险事件分类，具体内容见表 B.1：

——危险事件的后果严重性 S：严重程度由低至高，分别为 S1、S2、S3；

——发生危险的概率 P：由低至高，分别为 P1、P2；

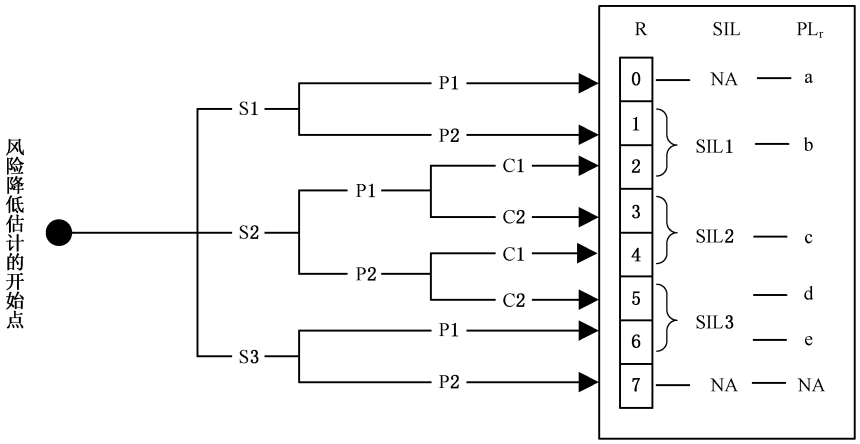
——危险事件的可控性 C：可控程度由低至高，分别为 C1、C2。

表 A.1 风险评估相关参数表

风险参数		分类	备注
危险事件的后果严重性	S1	小碰擦	对于 S1、S2、S3 的解释，应考虑意外的后果和正常康复
	S2	造成局部伤害（如骨折等）	
	S3	造成严重伤害（如死亡等）	
发生危险的概率	P1	低概率（小于或等于 1 次/天）	在连续运行的情况下发生危险的概率
	P2	高概率（大于或等于 2 次/天）	
危险事件的可控性	C1	正常控制	正常控制：通过控制系统或急停等装置能够控制危险事件的进行
	C2	异常控制（不可控）	

A.3 风险图实现

风险图实现见图 A.1。



说明：R 表示风险等级，通过 0～7 表示风险的由低至高，NA 表示不适用。

图 A.1　风险图

附 录 B
（规范性附录）
服务机器人危害种类

风险评估的重要步骤之一为危险识别分析。

这种类型的分析采用系统识别过程分析可能由系统或机器基于一些规范引起的潜在危害。系统程序包括对其功能规范或接口的分析，以及已经发现的类似产品的危害，或者一般危害类型的综合列表。

考虑到服务机器人的广泛应用，可提供所有应用程序在其结果中应覆盖的最小危害列表。

表 B.1 已经提供了一份联合清单，作为对最低覆盖率的建议，可以由任何特定的风险识别运动获取。具体的危害识别方法的结果可以和列表进行比较，如果结果发现并没有覆盖整个列表中的所有危害，那么危害识别结果应被扩展或扩充以覆盖其余的危害。

表 B.1 服务机器人的危害

序号	危害项	危害分析		有关的安全条款	备注
		危害	潜在后果		
1	充电电池有关的危害	电池过载	起火，排放有害气体和物质	C.2	
2		过放电电池充电	起火，排放有害气体和物质	C.2	
3		与充电电池端子接触	电击危害	C.2	
4		电池短路	起火，排放有害气体和物质	C.2	
5		过充电	起火、爆炸起火、爆炸、漏液	C.2	
6		强制放电	起火、爆炸、漏液起火	C.2	
7	电池组充放电的危害	过压充电	起火、爆炸、漏液	C.2	
8		过流充电	起火、爆炸、漏液	C.2	
9		欠压充电	起火、爆炸、漏液	C.2	
10		过载	起火、爆炸、漏液	C.2	
11		外部短路	起火、爆炸、漏液	C.2	
12		反向充电	起火、爆炸、漏液	C.2	
13	能量存储和供应的危害	高电压接触带来的危害	电击、起火	C.3	
14		电气元件/部件在故障条件下供电	电击	C.3	
15		与高气压能源接触带来的危害	压碎、切割、分离、伤害	C.3	高能量的机械部件包括旋转/快速运动的部件、高压液压或气动、燃料组件

表 B.1（续）

序号	危害项	危害分析		有关的安全条款	备注
		危害	潜在后果		
16	能量存储和供应的危害	与高水压能源接触带来的危害	压碎、切割、分离、伤害	C.3	高能量的机械部件包括旋转/快速运动的部件、高压液压或气动、燃料组件
17		与高化学能源接触带来的危害	起火、刺激	C.3	
18		与高温/高热能接触带来的危害	起火、灼伤	C.3	
19		储能不受控制的释放(快速放电/爆炸)	起火、灼伤、压碎、刺伤、切割	C.3	储存的能量可以在气动和液压蓄能器、电容器、电感、电池、弹簧、平衡和飞轮等
20		断电	压碎、分离、失载、失控	C.3	
21		意外断电	压碎、分离、失载	C.3	
22		能量过载	起火	C.3	
23		局部断电(局部暂时限制用电)	其他危害	C.3	
24		静电放电的危害	起火、爆炸	C.3	
25		温度循环	起火、爆炸、漏液	C.3	
26		振动	起火、爆炸、漏液	C.3	
27		加速度冲击	起火、爆炸、漏液	C.3	
28		跌落	起火、爆炸	C.3	
29	系统启动和重新启动	意外/非期望启动	其他危害	C.4	
30		启动/重启期间发生意外	其他危害	C.4	
31	机器人形状	边缘锋利	切割、切断、刺穿、擦伤	C.6	
32		在运动部件间存在孔或间隙	破碎、切断、刺穿、擦伤	C.6	
33		有危害的分离部件或掉落部件	破碎、夹住	C.6	
34		碰撞时,危害的机器人形状轮廓	撞击伤害、破碎、夹住、切割	C.6	

表 B.1（续）

序号	危害项	危害分析		有关的安全条款	备注
		危害	潜在后果		
35	噪声	有害的噪声	失聪、不安、意识丧失、失去平衡	C.7	
36		超声波噪声	失聪、不安、意识丧失、失去平衡	C.7	
37	与运动部件接触造成的危害	缺乏静音操作	与人接触时造成人体伤害	C.14	
38	危害抖动	有害的振动	肌腱炎症、不适、背痛、神经症、关节炎、眩晕	C.14	
39		振动产生的清晰度减小	用户不正确的操作带来的危害	C.14	
40	有害的物质或者液体	与服务机器人排放的有害物质接触	烧伤、烦躁	C.14	
41		服务机器人发出的有害气体	刺激、过敏、窒息、致盲	C.14	
42		与机器人接触引发的过敏反应	过敏	C.14	
43	周围环境的影响	高浓度粉尘	火灾、其他危害 设备短路，开关接触不良，通风不良	C.12	
44		沙粒	磨损表面造成边缘锋利，运动部件受到干扰工作不稳定；制动性能退化	C.12	
45		机器人接触到雪、冰	运动部件受到干扰，可能引发短路；传感器受到干扰；其他危害	C.12	
46		接触水	引起短路、功能缺失、电源断电	C.12	
47		机器人接触到盐水	机器人外形发生变化，某些功能缺失；电源发生故障或者短路等	C.12	
48		高海拔环境	易发热； 较大的温度变化使产品外壳容易变形、龟裂，密封结构容易破裂	C.12	
49		强光环境	视觉定位用相机、传感器等可能受到干扰	C.12	
50		机器人附近有超声波噪声	传感器被干扰，导致避障等功能失效	C.12	
51		干燥环境	静电，可能导致部分功能失效	C.12	

表 B.1（续）

序号	危害项	危害分析		有关的安全条款	备注
		危害	潜在后果		
52	极端天气	高温	烧伤、压力、烦恼	C.12	
53		低温	冻伤、烧伤、压力、烦恼	C.12	
54		清晰度减少	用户不正确的操作带来的危害	C.12	
55	危害辐射	机器人对人体发出有害辐射	烧伤、眼外伤	C.12	
56		机器人对人体发出有害光线	眼外伤	C.12	
57	电离辐射	机器人发出有害的电离辐射	对人体造成一定的危害	C.8	
58	电磁兼容	安全功能丧失	依据各功能定义	C.8	
59		电磁干扰造成机器人动作错误	依据各功能定义	C.8	
60		有危害的机器人运动	破碎、冲击、切割、破损、碰撞	C.8	
61		机器人处于不安全状态	破碎、冲击、切割、破损、烧伤	C.8	
62	对身心健康的影响	机器人运行需要的压力	肌肉拉伤	C.9	
63		运行环境带来的身体不适	肌肉疲劳	C.9	
64		用户身高不符合要求	身体紧张、肌肉疲劳、肌肉损伤障碍	C.9	
65		人机交互界面不清晰或者图像显示部件安装不合理	用户身体不适	C.9	
66		反应缓慢，控制系统错乱、控制界面过于复杂	精神紧张、疲劳	C.9	
67		服务机器人可视范围小	其他人为造成的危害	C.9	
68	机器人运动可能造成的危害	机械结构不稳定（翻倒、坠落、过度倾斜）	挤压、囚困、装载物掉落	C.10	
69		机械体不稳定，在装卸时出现错误（如翻倒）	挤压、囚困、装载物掉落	C.10	
70		模式切换时不稳定	挤压、囚困、装载物掉落	C.10	
71		运行模式不稳定	碰撞、载荷降低、对环境造成危害	C.10	
72		翻转时不稳定	挤压、剪切、载荷降低	C.10	
73		运行不稳定，下降或者上升时出现不稳定	对环境造成危害、释放有害物质	C.10	

表 B.1（续）

序号	危害项	危害分析		有关的安全条款	备注
		危害	潜在后果		
74	机器人运动可能造成的危害	不稳定的碰撞	挤压、切割、载荷降低	C.10	
75		失控碰撞	碰撞、对环境造成危害	C.10	
76		机器人部件出现脱离	碰撞	C.10	
77		附加约束时机器人出现不稳定	碰撞、冲击	C.10	
78		去除约束时不稳定	碰撞、冲击	C.10	
79		用户接触和离开的过渡阶段不稳定	损伤、挤压	C.10	
80		过渡时失控	挤压、损伤	C.10	
81		与有关安全部件产生碰撞	钝力外伤、切割损伤	C.10	
82		与动物接触时发生碰撞	伤害动物，引起一系列恐慌	C.10	
83		与其他机器人碰撞	碰撞、失去负载	C.10	
84		与脆弱物体发生碰撞	物体挤压、对环境的危害、释放有害物质、燃烧	C.10	
85		与墙壁以及其他障碍物碰撞	物体挤压、对环境的危害、释放有害物质	C.10	
86		未能及时发现物体导致碰撞	与安全相关部件碰撞	C.10	
87		接触时对身体的危害	剪切、破损	C.10	
88		不具有触觉传感器的部件与其他物体发生碰撞	钝力损伤、破损	C.10	
89	耐久性不足造成的危害	由于耐力不足局部破损	其他危害	C.11	
90	不准确的自主决策和行为造成的危害	在执行任务时产生危害	其他危害	C.13	
91	与运动部件接触造成的危害	与其他部件的有害接触	切割、破损	C.14	
92	定位和导航方式	意想不到的定位错误	碰撞、冲击、翻转	C.16	
93		进入盲区或未规定工作区域	碰撞、冲击、翻倒、给未定对象服务、对儿童或宠物造成伤害	C.16	
94		进入未规定的上坡、下坡、凹坑、台阶	碰撞、冲击、翻倒	C.16	

表 B.1（续）

序号	危害项	危害分析		有关的安全条款	备注
		危害	潜在后果		
95	定位和导航方式	导航时路线上出现影响安全的相关部件	碰撞、冲击、触发安全部件对环境造成影响	C.16	
96	其他危害项	不充分或错误的指导培训材料	用户操作错误导致不良后果	附录 D	
97		用户穿戴外套如眼镜外套等，导致控制能力下降	控制不准确，导致不好的结果	附录 D	
98		产品和说明书未充分警示残余风险	用户操作错误导致不良后果	附录 D	

附 录 C
（规范性附录）
安 全 要 求

C.1 概述

服务机器人应符合安全要求。如果出现第5章中描述的服务机器人可能出现的危害，应确认安全要求、对应的SIL以及所要采取的相应措施，保护操作者之外的人、动物或者其他安全相关物体不受任何伤害，确保操作者的安全。

C.2 充电电池有关的危害

如果服务机器人拥有一个集成的内置电池充电系统，则应防止人员意外接触机器人上的充电接头和它的充电系统而受危害。此外，充电系统应防止由于过载或深度放电的电池充电而出现的任何危害。

电池和电池组以及充放电装置的外壳应使用防火防护外壳。

对于电池和电池组以及充放电系统，其测试方法和技术要求可参考相关电池标准要求。若服务机器人用电池和电池组的安全标准发布后，应符合其适用的标准。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 充电系统的设计应确保仅当服务机器人与其连接时，才开始启动充电；
b) 充电系统应显示充电状态，或在电池完全充满时发出信号；
c) 充电系统的设计，应能自动监督电池的正确充电，从而防止由于深度放电的电池过载或充电造成的危险。

C.3 能量存储和供应的危害

服务机器人应防范与它的能量有关的所有危害发生。服务机器人的电气和机械安全性能应按GB/T 5226.1和GB 4943.1的相关要求以及服务机器人的电气和机械安全标准，按照适用的标准设计。任何暴露于服务机器人周围的人都应受到保护，应防止其与机器人上的带电部分直接或间接的接触。应提供一种隔离任何危害能源的方法（如：电气、机械、液压、气动、化学和热）。这种危害的能源应被清楚地识别，并且如果重新连接将导致危害发生，隔离器应能够被锁定。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 用于保护危险能量部件的防护装置或外壳，其设计应符合IEC 60529定义的电气危险的适当IP等级，而其他由风险评估决定的危险，则应符合ISO 13857规定的安全距离；
b) 在出现过热的地方，应采用散热措施（例如：散热器、气流）。如果使用风扇，宜使用风扇控制装置。

C.4 系统启动和重新启动

服务机器人在启动后，不得立即执行任何危险动作。机器人在系统启动和重新启动时伺服电机不会出现任何过放电现象，系统电路应保持足够安全冗余，电容受潮或其他原因易导致系统启动或重启时起火爆炸。

由于直接启动电流大，电应力大，应有针对的加强结构件的强度，避免直接启动造成不可逆的损坏。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 在启动时，应借助安全相关功能，停用机械手、移动平台和其他运动部件（以防止任何意外行为）。仅在通过传感器确认危险情况不存在时，应用功能才能被启用。如果机器人在启动后立即进入自主模式，则应采用该措施。

b) 服务机器人应在受监视的静止状态下启动，并只能通过使用者操作的方式恢复正常操作。

C.5 静电势

服务机器人应能够避免由静电势和放电引起对人类和其他安全物体的所有伤害。静电放电保护应足以保证用户不需要个人防护。服务机器人应能够避免静电放电引起的危害。

服务机器人需严格预防静电电量达到一定程度引起的火灾。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

电气设备外壳的使用应符合 GB/T 5226.1 规定，以避免接触带电部件。

C.6 机器人形状

在设计机器人的形状和外部部件时，应考虑机器人的设计意图，避免其可能造成的危害，例如：压碎、切割等。

机器人突出部分尽量保持钝角设计，避免机器人出现过于尖锐的突出部分，机器人经常与人接触部分的表面材料宜具有一定弹性。

任何过于突出的部分应有防护装置或防护措施，安装位置设计应安全可靠，不应因偶然碰撞而失效。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 应提供锋利边缘和尖角的衬垫，以消除剪切、刺伤、切割的危险和减少冲击的危险；

b) 使用固定的或活动式防护装置遮盖危险的运动部件；

c) 若承载危险负载（例如：锐利或尖锐的物体），应调整机器人的速度和行为。

C.7 噪声

服务机器人不应使靠近的人受到其噪声（包括超声波和次声波）的危害，可能的危害包括：令人心情紧张、耳鸣等症状以致听力衰退、心烦意乱身体不适、平衡感变差、失去意识甚至导致身体内脏器官损伤。

服务机器人产生的噪声强度，不能对没有佩戴特殊防护装备的使用者产生危害。

服务机器人应符合 GB/T 37242 的规定。

对于上述危害，如果适用，应采用下列之一的安全防护及补充保护措施：

a) 附加的吸声材料，例如：泡沫、隔板、窗帘、涂料；

b) 使用主动噪声消除（抗噪声）机制。

C.8 电磁兼容

在工作场景中，服务机器人正常工作所产生的骚扰电平不应妨碍其他设备按预定方式工作，其电子系统的抗电磁干扰能力，在正常可预见的所有可能的情况下不应出现有可能导致危害的异常运动和异

常状态。

服务机器人应符合 GB/T 37283 和 GB/T 37284 的规定。

服务机器人产生的电磁骚扰不应超过其预期使用场合允许的水平。服务机器人对电磁骚扰应具有足够的抗干扰水平，以保证其在预期使用环境中可以正确运行。

对于上述危害，如果适用，应采用下列之一的安全防护及补充保护措施：

应通过对入射辐射的电磁屏蔽，将风险减小到可接受的等级。

C.9 对身心健康的影响

服务机器人在提供服务时，不应对身心健康（身体和心理）造成影响。

与人有肢体接触的服务机器人，其接触部位材质应避免使用过敏材料（如镍、铬和部分橡胶材料会使皮肤产生过敏反应），接触部位形状应符合人体工学设计要求。

服务机器人构造中若使用有液体材料，应保证其不会因泄露对人产生伤害。

服务机器人的造型设计，应避免令人产生心情紧张、厌恶等不适感。

服务机器人与人的交互方式设计，应尽量简单易用，利于人的理解，并避免因让使用者需经常性留意某些紧急或异常状态而导致的精神紧张以致疲劳等不适。

应通过风险评估，尽量消除服务机器人对人可能造成的心理负面影响。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a） 减震（悬挂）机制的使用；

b） 使用姿势支撑物。

C.10 机器人运动可能造成的危害

与安全相关部件接触的时候避免机器人作危害运动，机器人与其他部件接触的时候避免机器人本身的不稳定。机器人运动过程中或者静止时，具有足够的稳定性，避免因摔倒等造成人身或环境危害。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a） 使用稳定性控制功能；

b） 检测不稳定性的即将发生，及行动（或不行动）以减少伤害；

c） 限制操作机的速度或范围；

d） 防止过载的装置。

C.11 耐久性不足造成的危害

服务机器人的设计应保证它的耐久性，在使用的整个过程中不会产生危害。服务机器人的最低耐久性要求由其风险评估决定。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a） 监测/调节施加的力量的控制功能；

b） 使用主动散热方式（例如：风扇或其他冷却系统）；

c） 在必要的情况下，应监控服务机器人的内部温度，尤其在热源附近；如果温度超过限制，机器人应以适当的方式做出反应（例如：以安全的方式关闭）；

d） 监控服务机器人的生命周期，并在维护时间或寿命结束时通知使用者。

C.12 周围环境的影响

服务机器人应在可预期的环境下运行，且在运动过程中不会发生危害。机器人应避免受到环境中的灰尘或者沙影响而发生危害。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 防止灰尘堆积的机制（例如：强制通风或清洗机制）；

b) 灰尘检测和警告指示，以告知使用者执行必要的行动；

c) 位于外壳开口处的空气过滤器；

d) 使用加热融化雪或冰，或蒸发水分或小水滴，从而使服务机器人变干而不会造成后续的危险；

e) 去除表面的水分/湿气（例如：使用雨刷）；

f) 从外部去除表面的雪或冰（例如：用热水清洗）；

g) 主动探测雪/冰/冷空气情况，并且在雪/冰层积聚到不可接受的水平前执行一个保护性的停止，机器人应就停止的原因给使用者做适当的指示；

h) 服务机器人应整合安全防护功能，用以确保定期停止或停机维修（通常包括检查、清洗或部件更换）。机器人应向使用者提供以这个目的关闭的指示，基于本要求的目的，关机的时间间隔应取决于如因腐蚀、砂、灰尘和雪的堆积，而到达不可接受的风险等级所需的时间。

C.13 不正确的自主决策和行为造成的危害

具有自主决策和行为能力的服务机器人，应避免因机器人决策信息不全面等因素导致的不正确决策或行为对人造成伤害后果，或对环境造成危害后果。

例如：运动服务机器人应为人提供一杯水，但其错误地提供了一杯茶，这或许不会带来严重伤害后果，但若其使用了已有破损甚至已有锋利切口的玻璃杯，这就有可能对用户造成划伤甚至更严重的伤害；载人机器人在正常平坦地面做紧急规避动作，可能仅对人造成些许惊吓，不至产生严重人身伤害后果，但在湿滑地面的紧急规避行为，可能导致机器人滑倒甚至翻覆，从而对人造成伤害。

服务机器人可通过提高其决策行为的可靠性（例如：采用更好的传感器等），或通过限定机器人的使用条件和环境，降低因机器人不够全面的甚至错误的行为决策所可能导致的对人产生伤害的风险。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 传感器和传感算法的能力/可靠性应提高到一个没有不可接受的风险发生的水平。

b) 识别算法的设计方式，应能计算出某一决策为正确的概率（例如：正确识别某个安全相关物体的概率）并且可以被监视。对于具有高不确定性结果的决策，应使用替代方法和（或）附加信息进行重新评估。如果重新评估后，不确定依然不能接受，应寻求外部援助或启动保护停止。

c) 对导致危险状况的决策，应进行确定性检查。

d) 决策应由多样的感应原则加以验证。

C.14 与运动部件接触造成的危害

服务机器人的设计应确保暴露的部件造成的危险的风险在可接受的程度，如电机轴，齿轮，传动带，车轮，履带或连杆机构。服务机器人应符合 GB/T 23821 的设计要求，以防止危害发生。服务机器人的结构设计中，应避免自身的运动部件被不恰当地人为触及，造成人或机器人的伤害。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 服务机器人的设计，应使可接触的运动部件的数量降至最低；

b) 服务机器人的设计，应使运动部件不暴露在外，如电机轴、齿轮、传动带、车轮、履带或连杆机构。

C.15 使用者对机器人缺乏认知

风险评估表明，操作者对机器人缺乏认知具有危害性，需要采取措施降低风险。例如：在安静的环境中，机器人运动时轮子与地面、电机转动均会发出声音降低危害，并且不违反其他噪声排放规定；机器人在导航过程中检测到人或其他障碍物时有自主避障，不用担心会撞到人或其他障碍物；有肢体动作的服务机器人，在其动作的过程中需要与人保持一定距离，且机器人的肢体不会主动与人直接接触。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 应提供声波发生器，以警告使用者潜在的危险情况；

b) 应提供警告灯或其他光学装置，以警告使用者和第三方，有服务机器人出现；

c) 若有安全相关物体在其保护性停止空间内，则服务机器人应停止，并在物体离开后继续执行其任务。

C.16 定位和导航方式

服务机器人应具有足够的准确导航、自主避障的能力，规划合理的运动路线，在运动时与安全相关部件碰撞时不会造成预见之外的危害。机器人位置环境变化时，在定位和导航发生故障不会导致不可预期的危害。定位不确定时不会导致运动平台或者机器人相关部件发生危害性运动。

对于上述危害，如果适用，应采用以下安全防护及补充保护措施：

a) 监测定位的稳定性和可信度，并在不稳定的定位时，进入安全状态；

b) 不稳定定位的补偿，例如：通过使用里程计或其他传感器数据。

应采用不低于风险评估决定的频率，以新信息（例如：从内部传感器或外部源）更新导航地图，以防止因使用了旧地图而产生的风险。

附 录 D
（资料性附录）
SRCS 使用信息

D.1 目的

应提供 SRCS 信息，使用户能够开发程序，以保证在机器使用和维护期间保持 SRCS 所要求的功能安全。

D.2 安装、使用与维护文件

安装、使用与维护文件见 GB/T 15706—2012 中第 6 章提供的一般信息，起草随机文件时应予以考虑。

文档应提供 SRCS 的安装、使用和维护信息，应包括：

a) 设备、安装和装配的全面描述。
b) SRCS 预期使用的陈述和防止可预见的误用的必要措施。
c) 实际环境信息（例如：照明、震动、噪音等级、大气污染）（适合时）。
d) 概略（框）图（适合时）。
e) 电路图。
f) 检验试验时间间隔或寿命。
g) SRCS 功能和机器电气控制系统功能之间的交互作用描述（包括互连接线图）。
h) 必要措施描述，保证 SRCS 功能从机械电气控制系统功能中分离出来。
i) 如果需要，暂停 SRCF（例如：用于手工编程，程序检验），为保持安全所提供的防护和措施的描述。
j) 有关编程信息。
k) 适于 SRCS 维护要求的描述，包括：
   1) 用于记录机器维护历史的日志。
   2) 为保持 SRCS 功能安全需要进行的日常维护活动，包括：有预定寿命的元件日常更换。
   3) SRCS 中出现故障或失效时要遵循的维护程序，包括：
      - 故障诊断和修理程序；
      - 修理后确认正确操作程序；
      - 维护记录要求。
   4) 维护、重新试运转必需的工具和适用于维护工具、设备的程序。
   5) 定期测试规范、预防维护和纠正维护规范。

注 1：定期试验为确认正确操作和检测故障必要的功能试验。

注 2：预防性维护为保持 SRCS 所需性能而采取的措施。

纠正维护包括将 SRCS 带回到设计状态的特定故障发生后采取的措施。

附 录 E
（资料性附录）
服务机器人功能安全管理相关修改程序及文件要求

E.1 修改程序

E.1.1 在 SRCS 设计、集成和确认期间（例如：SRCS 安装和试运行时）修改时，本附录规定的修改程序适用。

E.1.2 修改 SRCS 的要求源自于下列情况，例如：

——安全要求规范的变化；

——实际使用条件；

——附带事件/偶然事故经验；

——加工材料变化；

——机器修改或其操作模式改变。

注：按照 SRCS 的使用信息（附录 D）或说明书对其进行的干预（例如：调整、设置、修理），本附录不考虑修改。

E.1.3 要求修改 SRCS 的原因应生成文件。

E.1.4 要求的修改及其影响应进行分析，以建立 SRCS 的功能安全效果。

E.1.5 修改的效果分析和其对 SRCS 功能安全影响的分析应形成文件。

E.1.6 以经过修订的文件为基础，在执行任何修改前应准备一个完整的行动计划，并形成文件。

E.2 配置管理程序

E.2.1 配置管理程序应按照功能安全计划（见 6.2.1）执行，应考虑下列因素：

a) 各修改过程的计划。

b) 决策过程和各 SRCS 相关决定的文件。

c) 改变要求程序的按时间顺序排列的文档（例如：工作日志），包括：

1) 识别可能受影响的危害；

2) 改变要求（硬件或软件）的描述；

3) 改变要求的原因；

4) 做决定（和每个决定的授权）；

5) 影响分析；

6) 重新检验（对各阶段）和重新确定；

7) 受改变要求活动影响的所有文件；

8) 在改变过程中执行的所有活动和执行这些活动的人或实体。

d) 下列信息的文件，允许随后审查：

1) 配置状况；

2) 版本状态；

3) 所有修改和批准的理由；

4) 修改的细节。

E.2.2 适当改变控制过程的程序应考虑下列要求：

a) 为每个 SRCS 版本定义唯一的基线程序。

b) 基线的所有配置项目的定义。这至少应包括：

1) 安全要求分析和规范。
2) 有关设计文件。
3) 硬件或软件模块。
4) 试验计划和结果。
5) 检验和确认报告。
6) 已存在的软件部分，这些软件部分将并入 SRCS。
7) 创建和试验用的开发环境。
8) 所有配置项有唯一标识的准确维护，保持 SRCS 的完整。
9) 改变控制程序，从而：
   - 阻止未授权的修改；
   - 文件改变要求；
   - 分析所提出的改变要求的影响，批准或拒绝；
   - 所有批准的修改细节和授权文件；
   - 在硬件或软件开发中，在适当点建立配置基线，并记录集成测试，该测试证明基线为正确；
   - 保证所有硬件和软件基线的构造。
10) 效果分析，应对每个改变要求进行评定。该评定应包括合适的危害分析，并应考虑 SERCS 其他所有修改活动。
11) 对 SERCS 所有可接受的修改，返回到 SERCS 的硬件和软件适当的设计阶段(例如：规范、设计、集成、安装)。所有后续阶段应按照本标准执行。
12) 执行所有必要的操作，以证明已达到规定的安全完整性。
13) 对执行必要的改变要求活动的授权应取决于影响分析的结果。

E.2.3 变更控制过程的文件应至少包括：

a) 每个修改过程的计划。
b) 上述提及的要求和程序文件。
c) 决策过程和有关 SERCS 的决定做出的文件。
d) 改变要求程序的按时间顺序排列的文档(例如：工作日志)，包括：
   1) 识别可能受影响的危害；
   2) 改变要求(硬件或软件)的描述；
   3) 改变要求的原因；
   4) 做决定(和每个决定的授权)；
   5) 影响分析；
   6) 重新检验(对各阶段)和重新确定；
   7) 受改变要求活动影响的所有文件；
   8) 在改变过程中执行的所有活动，和执行这些活动的人或实体。
e) 下列信息的文件，允许随后审查：
   1) 配置状况；
   2) 版本状态；
   3) 所有修改和批准的理由；
   4) 修改的细节。

E.3 文件

E.3.1 文件应：

——精确和简明；

——让使用的人容易理解；

——适合其预期目的；

——容易获取和保持。

E.3.2 SRCS 的设计者应区别出用户相关的文件与设计和建造相关的文件。

E.3.3 文件应有标题和名称，指明其内容范围。

E.3.4 文件应有修订索引（版本号），从而能够区别文件的不同版本。

参 考 文 献

[1] GB/T 12643—2013 机器人与机器人装备 词汇

[2] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语

[3] GB/T 20438.7 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述

[4] GB/T 21109.1—2007 过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求