ICS 29.020
CCS K 09

中华人民共和国国家标准化指导性技术文件

GB/Z 44938.1—2024/IEC TS 62998-1:2019

机械电气安全　第1部分:用于保护人员安全的传感器

Electrical safety of machinery—Part 1:Safety-related sensors used for the protection of persons

（IEC TS 62998-1:2019,Safety of machinery—Safety-related sensors used for the protection of persons,IDT）

2024-12-31 发布　　2025-07-01 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……Ⅴ
引言……Ⅵ
1　范围……1
2　规范性引用文件……1
3　术语和定义……2
3.1　特性和性能……3
3.2　可信度……4
3.3　规程和结构的商议……5
3.4　系统相关术语……7
3.5　融合……8
3.6　安全相关信息……8
3.7　试验……10
3.8　用户类别……11
3.9　验证和确认……12
4　生命周期以及与安全相关控制系统(SCS)的相互联系……13
4.1　通则……13
4.2　危险和风险分析……15
4.3　对应 SRS/SRSS 性能等级……16
5　设计和开发阶段……17
5.1　通则……17
5.2　SRS/SRSS 功能……17
5.3　设计分析……18
5.4　模拟……18
5.5　感应区……19
5.6　安全相关区……19
5.7　自动化相关区……19
5.8　检测能力和可信性……19
5.9　用户界面……23
6　集成和安装阶段……25
6.1　通则……25
6.2　将 SRS 融合到一个 SRSS 中……26
6.3　用户校准……29
7　工作、维护和修改阶段……30

8 验证和确认……30
8.1 通用要求……30
8.2 SRS/SRSS 的验证……30
8.3 SRS/SRSS 的确认……31
8.4 分析……32
8.5 试验……33
9 使用说明……35
附录 A(资料性) 系统性能力的检查……37
附录 B(资料性) 用户类别……38
B.1 SRS/SRSS 用户类别和本文件所涵盖的用户类别……38
B.2 融合所涉及的用户类别……38
附录 C(资料性) 功能分解和/或整合……41
附录 D(规范性) 模拟模型的生成和应用……43
D.1 概述……43
D.2 使用建议……43
D.3 模拟目标及实现措施……43
D.4 验证……44
附录 E(资料性) 儿童属性和行为……46
E.1 概述……46
E.2 身体部位的尺寸……46
附录 F(资料性) 环境影响……50
F.1 概述……50
F.2 环境影响应用示例 1……50
F.3 环境影响应用示例 2……51
附录 G(资料性) 导致 SRS/SRSS 安全相关功能丧失的故障、失效和影响……53
G.1 概述……53
G.2 危险失效……55
G.3 正常运行……56
G.4 作为安全相关信息一部分的触发故障反应功能和置信度信息的信号……56
附录 H(资料性) 试验因素……58
H.1 概述……58
H.2 机械影响试验……58
附录 I(资料性) 功能、安全相关信息和融合的示例……61
I.1 功能示例……61
I.2 安全相关信息示例……61
I.3 融合示例……63

参考文献……66

图 1　测量准确度和测量不确定度……4
图 2　SRS 结构示例 1……13
图 3　SRS 结构示例 2……14
图 4　SRSS 结构示例……14
图 5　SRS/SRSS 危险和风险分析流程……15
图 6　SRS/SRSS 的安全相关信息……24
图 A.1　使用安全相关传感器标准对系统性能力进行检查的示例……37
图 C.1　功能和物体之间的相互联系……41
图 C.2　在 SRSS 中执行的功能示例……42
图 D.1　验证流程……45
图 E.1　儿童身高……47
图 E.2　儿童胸深……47
图 E.3　儿童头宽……48
图 E.4　儿童头长……49
图 G.1　因丧失或绕过安全功能而导致额外风险的故障、失效或错误组合……53
图 G.2　在设计和开发阶段防止因危险失效而导致系统性故障的系统性能力分析……54
图 G.3　针对导致故障反应功能的系统性故障的应对方式……56
图 G.4　针对产生相关置信度信息的错误的应对方式……56
图 I.1　SRS 在道路交叉口的应用示例……61
图 I.2　提供判定和置信度信息的 SRS/SRSS 示例……62
图 I.3　SRS/SRSS 提供测量和置信度信息的示例……62
图 I.4　将 2 个 SRS 融合到一个 SRSS 以产生组合感应区的第一个示例……63
图 I.5　SRS 安全相关信息的融合……64
图 I.6　根据 SRS 使用说明和 SRSS 安全要求规范进行的验证和确认方法……64
图 I.7　将 2 个 SRS 融合到一个 SRSS 以产生组合感应区的第二个示例……65

表 1　所需要的最低 SRS/SRSS 性能等级与安全性能等级之间的对应关系……16
表 2　SRS/SRSS 功能(在适当的情况下)……18
表 3　包含环境要求的标准……21
表 4　在高要求模式下因环境干扰导致危险失效(检测能力丧失)的限值……22
表 5　在高要求率条件下所需要的最低包含概率/判定概率……25
表 6　两个 SRS 融合之后所适用的 SRSS 最高性能等级……28
表 7　用于评估验证措施和验证结果的方法……31
表 8　需要提供的使用说明概览……36

表 B.1　各种用户类别的角色和任务……38
表 B.2　(使用检测单元、SRS/SRSS 元件或 SRS 子系统的)不同集成类型所涉及的用户类别……39
表 D.1　低复杂度 SRS/SRSS 的模拟目标与措施……43
表 D.2　高复杂度 SRS/SRSS 的模拟目标与措施……44
表 E.1　儿童身高……46
表 E.2　儿童胸深……47
表 E.3　儿童头宽……48
表 E.4　儿童头长……48
表 F.1　符合 IEC 60721-3-5 的环境影响和等级示例 1……50
表 F.2　符合 IEC 60721-3-3 的环境影响和等级示例 2……52
表 G.1　表 G.2 数值计算所使用的要求率……55
表 G.2　高要求率条件下因环境影响所导致的危险失效(检测能力丧失)限值……55
表 H.1　机械影响试验的试验计划和试验结果示例……59

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分:标准化文件的结构和起草规则》的规定起草。

本文件是 GB/Z 44938《机械电气安全》的第 1 部分。GB/Z 44938 已经发布了以下部分:

——第 1 部分:用于保护人员安全的传感器;

——第 2 部分:保护人员安全的传感器的应用示例。

本文件等同采用 IEC TS 62998-1:2019《机械安全　用于保护人员安全的传感器》。文件类型由 IEC 的技术规范调整为我国的国家标准化指导性技术文件。

本文件做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《机械电气安全　第 1 部分:用于保护人员安全的传感器》;

——附录 E 增加了注,补充说明中国儿童属性和行为测量数据信息。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本文件起草单位:北京机床研究所有限公司、西安交通大学、中国石油大学(北京)、厦门夏博电子科技有限公司、广东拓斯达科技股份有限公司、永林电子股份有限公司、上海长江汲智传感技术有限公司、郑州煤机智能工作面科技有限公司。

本文件主要起草人:薛瑞娟、王金江、吴翟、张颖、林启敬、黄祖广、赵立波、吴怡然、张培森、高知国、王楚婷、罗国希、李诗文、梁振锋、林启程、薛文锋、张文琦。

引　言

安全相关传感器主要用于存在人员受伤风险的机械设备上。安全相关传感器可使机器在有人处于危险状况前回复到安全状态，从而实现人员保护。目前，传感器行业主要使用通用功能安全标准IEC 61508系列标准，或者具体领域的机械标准IEC 62061和ISO 13849系列标准作为安全相关产品的设计指南，但这些标准并未就对于在特定环境条件下如何避免设计失败或无法检测指定物体，给出足够的指导，可能导致无法承受的人员风险。GB/Z 44938明确了传感器或传感器系统的功能安全，规范了传感器和传感器系统在系统性方面的开发与集成的要求，填补了具体传感器设计标准与电气、电子和可编程电子控制系统的通用功能安全标准之间系统性能力验证方面的空白，GB/Z 44938拟由3个部分组成。

——第1部分：用于保护人员安全的传感器。目的在于提高我国机械电气设备的安全水平，保障相关从业人员的人身安全，指导保护人员安全的传感器的设计制造与生产使用过程，规范保护人员安全的传感器的功能、安全及试验要求。

——第2部分：保护人员安全的传感器的应用示例。目的在于为使用第1部分提供指南和应用示例。

——第3部分：传感器技术和算法。目的在于指导如何正确实施算法以防止人们承受不可容忍的风险。

GB/Z 44938可提高传感器或传感系统的功能安全水平，为安全相关传感器制造商和安全相关传感器系统集成商提供指导。

机械电气安全　第1部分:用于保护人员安全的传感器

1　范围

本文件规定了关注系统性能力的用于保护人员安全的安全相关传感器(SRS)和安全相关传感器系统(SRSS)在开发、集成方面的要求。

本文件仅适用于下述条件:

——使用传感器实现人员保护;并且

——将传感器视作子系统或子系统元件的电气控制系统功能安全标准;以及

——特定产品传感器标准(比如IEC 61496(所有部分)和IEC 60947-5-2)并不包含必要规定或特定产品传感器标准尚未发布。

使用各种安全相关传感器标准进行系统性能力验证的示例见附录A。

本文件所有要求和研究方法均仅限于通过下述方式实现人员保护:

——检测潜在危险物体;

——检测人体、人体部位及与人体有关物体进入危险区域;或者

——识别这些部位与其他物体之间的差异。

注1:在公共场合使用SRS/SRSS不仅要求对人进行检测,还要求检测与其有关的设备,比如轮椅、拐杖和输液架等。

传感器和传感器系统的性能等级参照现有功能安全标准(比如IEC 62061,IEC 61508(所有部分)和ISO 13849(所有部分)中的定义。

注2:为简单起见并避免误用,本文件未像IEC 61496-1那样进行类型定义或联系。通过关联现有性能等级(PL)、安全完整性等级(SIL)或SIL要求限度(子系统)(SILcl),以简化终端用户的使用过程。

需要特别注意检测功能和检测能力可信度。环境影响和室内外应用试验均被定义并且会先影响检测功能和检测能力的可信度。

注3:环境影响及其分类和试验步骤主要参照通用环境标准的要求。只有在缺乏相关标准的情况下,才会提供更具体的要求和试验。

本文件也适用于其他行业的人员保护应用,比如农业或地铁站等公共场所的人员保护。

与IEC 61508-2不同,本文件并未考虑和涉及实际应用要求(比如过程或元件等)。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 28526—2012　机械电气安全　安全相关电气、电子和可编程电子控制系统的功能安全(IEC 62061:2005,IDT)

ISO 7250(所有部分)　用于技术设计的基本人体测量(Basic human body measurements for technological design)

ISO 13849(所有部分)　机械安全控制系统安全相关部件(Safety of machinery—Safety-related

parts of control systems)

注：GB/T 16855(所有部分) 机械安全 控制系统安全相关部件[ISO 13849(所有部分)]

ISO 25119(所有部分) 农业和林业拖拉机和机械控制系统安全相关部件(Tractors and machinery for agriculture and forestry—Safety-related parts of control systems)

注：GB/T 38874(所有部分) 农林拖拉机和机械 控制系统安全相关部件[ISO 25119(所有部分)]

ISO 26262(所有部分) 道路车辆功能安全(Road vehicles—Functional safety)

注：GB/T 34590(所有部分) 道路车辆 功能安全[ISO 26262(所有部分)]

IEC 60068(所有部分) 环境试验(Environmental testing)

IEC 60204-1 机械安全机械电气设备 第1部分：通用要求(Safety of machinery—Electrical equipment of machines—Part 1：General requirements)

注：GB/T 5226.1—2019 机械电气安全 机械电气设备 第1部分：通用技术条件(IEC 60204-1:2016，IDT)

IEC 60721(所有部分) 环境条件分类(Classification of environmental conditions)

注：GB/T 7247.1—2024 激光产品的安全 第1部分：设备分类和要求(IEC 60825-1:2014，IDT)

IEC 60825-1 激光产品的安全 第1部分：设备类别和要求(Safety of laser products—Part 1：Equipment classification and requirements)

注：GB/T 17799.7—2022 电磁兼容 通用标准 第7部分：工业场所中用于执行安全相关系统功能(功能安全)设备的抗扰度要求(IEC 61000-6-7:2014，MOD)

IEC 61000-6-7:2014 电磁兼容性(EMS) 第6-7部分：通用标准 工业场所中与安全相关的系统(功能安全)中执行功能的设备的抗扰度[Electromagnetic compatibility (EMS)—Part 6-7：Generic standards—Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety)in industrial locations]

注：GB/T 17799.7—2022电磁兼容 通用标准 第7部分：工业场所中用于执行安全相关系统功能(功能安全)设备的抗扰度要求(IEC 61000-6-7:2014，MOD)

IEC 61010-1 测量、控制和实验室用电气设备的安全要求 第1部分：一般要求(Safety requirements for electrical equipment for measurement，control，and laboratory use—Part 1：General requirements)

注：GB 4793.1—2007 测量、控制和实验室用电气设备的安全要求 第1部分：通用要求(IEC 61010-1:2001，IDT)

IEC 61508(所有部分) 电气、电子和可编程电子安全相关系统的功能安全(Functional safety of electrical/electronic/programmable electronic safety-related systems)

注：GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分)]

IEC 61784-3 工业通讯网络 配置文件 第3部分：功能安全现场总线 通用规则及配置文件定义(Industrial communication networks—Profiles—Part 3：Functional safety fieldbuses—General rules and profile definitions)

注：GB/T 34040—2017 工业通信网络 功能安全现场总线行规 通用规则和行规定义(IEC 61784-3:2016，IDT)

IEC 62061:2021 机械安全 安全相关控制系统的功能安全(Safety of machinery—Functional safety of safety-related control systems)

注：GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全(IEC 62061:2005，IDT)

IEC 62471 灯与灯系统的光生物安全(Photobiological safety of lamps and lamp systems)

CEN/CENELEC 导则14 儿童安全 标准使用导则(Child safety—Guidance for its inclusion in standards)

3 术语和定义

下列术语和定义适用于本文件。

3.1 特性和性能

3.1.1

自动化相关区 automation related zone

感应区的一部分,在该区域内检测规定的物体,以执行与自动化相关的功能。

3.1.2

安全相关区 safety-related zone

感应区的一部分,在该区域内检测规定的安全相关物体。

3.1.3

感应区 sensing zone

按长度、面积或体积定义的区域,在其中检测到物体会执行 SRS 或 SRSS 功能。

3.1.4

系统性能力 systematic capability

在按照安全手册要求使用的情况下,元件的系统性、安全完整性满足安全功能特定 SIL 等级要求的可信度(分为 SC 1~SC 4 的不同等级)。

注1:系统性能力是根据避免和控制系统性故障的要求所确定(见 IEC 61508-2 和 IEC 61508-3)。

注2:系统性失效机制取决于元件自身特性。举例来说,如果元件仅由软件构成,则只需考虑软件失效机制。而对于包括硬件和软件的元件来说,则有必要同时考虑系统性的硬件和软件失效机制。

注3:元件在特定安全功能方面具备 SC N 级系统性能力,意味着在按照安全手册要求使用的情况下,该元件的系统性安全完整性满足 SIL N 级安全功能的要求。

[来源:GB/T 20438.4—2017,3.5.9]

3.1.5

检测 detection

某个物理属性存在和/或某个物理属性数值的确定。

注:例如,分类就是一个检测过程,其中包括接收物理信号和滤波等其他步骤。

3.1.6

检测能力 detection capability

在制造商规定的使用限值内进行检测的能力。

3.1.7

检测能力缺失 loss of detection capability

无法在制造商规定使用限值内达到检测目的的 SRS/SRSS 事件。

注:检测能力缺失由检测能力下降引起。在分析因检测完整性下降而引起危险状态时,需要注意检测能力下降问题。

3.1.8

物理属性 physical property

被测物体的一种可测量属性。

3.1.9

测量准确度 measurement accuracy

测量准确度的准确性 accuracy of measurement accuracy

被测变量的测量值和真实值之间的接近程度。

注:见图1。

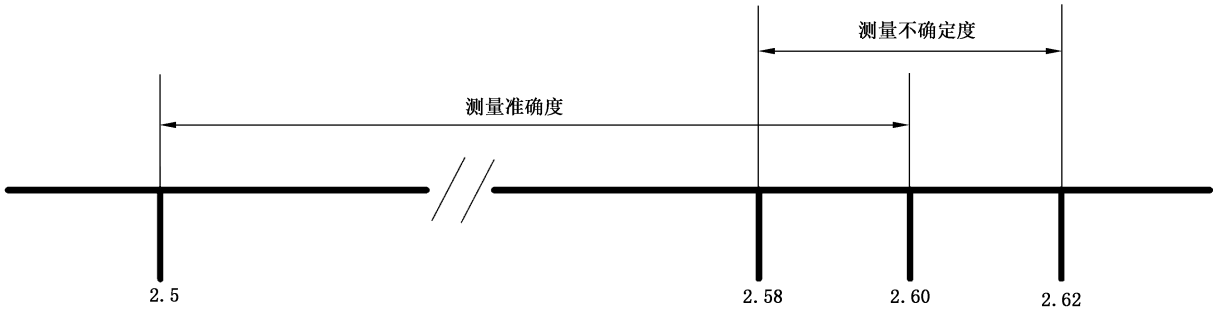


图 1　测量准确度和测量不确定度

[来源:ISO/IEC Guide 99:2007,2.13,有修改]

3.1.10

测量不确定度　measurement uncertainty

根据所使用的信息,用于表征被测量数值离散程度的非负参数。

[来源:ISO/IEC Guide 99:2007,2.26,有修改]

3.2　可信度

3.2.1

可用性　availability

能够按要求呈现某种状态的能力。

注1:可用性取决于物品的可靠性、可恢复性和可维护性以及维护支持性能在内的综合特性。

注2:可用性可以通过“可用性相关措施”所定义的方法进行量化。

[来源:GB/T 2900.99—2016,192-01-23,有修改]

3.2.2

可信度　dependability

能够在需要时按要求执行的能力。

注1:可信度包括可用性、可靠性、可恢复性、可维护性以及维护支持性能,在某些情况下还包括耐久性、安全性等其他特性。

注2:可信度是多种时间相关质量特性的总称。

[来源:GB/T 2900.99—2016,192-01-22,有修改]

3.2.3

可靠性　reliability

在已知条件下和时间内,按要求且无故障地执行功能的能力。

注1:时间间隔期间可用适用于该物品的单位表示,比如日历时间、工作周期、行程距离等,而且单位要清晰说明。

注2:已知条件包括影响可靠性的各个方面,比如工作模式、应力等级、环境条件和维护情况等。

注3:可靠性可以通过“可靠性相关概念:测量”所定义的方法进行量化。

[来源:GB/T 2900.99—2016,192-01-24,有修改]

3.2.4

误差　error

计算、观察或测量得到的数值或条件与实际、指定或理论上的正确数值或条件之间的偏差。

[来源:GB/T 2900.99—2016,192-03-02,有修改]

3.2.5

失效　failure

产品完成预定功能的能力发生中断。

注1：失效后，产品就有了故障。

注2："失效"是一个事件，"故障"是一种状态，区分两者。

注3：这里定义的"失效"概念并不适用于仅由软件构成的产品。

注4：实际中，术语"故障"和"失效"常作为同义词使用。

3.2.6

危险失效　failure to danger

可能导致无法在规定响应时间内执行安全相关功能的失效。

3.2.7

故障　fault

因内部状态导致不能完成预定功能。

注1：产品故障通常是由产品自身或其生命周期早期阶段的缺陷引起，比如规范、设计、制造和维护等。见潜在故障。

注2：使用规范、设计、制造、维护或误用等修饰词来说明故障原因。

注3：故障类型可能与相关的失效类型有关，比如老化故障和老化失效。

注4：形容词"有故障的"表示产品有一个或多个故障。

[来源：GB/T 2900.99—2016，192-04-01，有修改]

3.3　规程和结构的商议

3.3.1

风险分析　risk analysis

系统性地使用可用信息以确定危险或预估风险。

[来源：ISO/IEC Guide 51：2014，3.10]

3.3.2

降低风险的措施　risk reduction measure

保护措施　protective measure

消除危险或降低风险的行动或方法。

示例：自身安全设计；防护装置；人员防护设备；使用和安装说明；工作组织；培训；设备使用；监督。

[来源：ISO/IEC Guide 51：2014，3.13]

3.3.3

可承受风险　tolerable risk

在已知背景下能被当前社会价值观接受的风险水平。

[来源：ISO/IEC Guide 51：2014，3.15，有修改]

3.3.4

设计和开发　design and development

将一个想法或要求转化为产品的行为。

注：设计和开发过程通常包含一系列确定的步骤，从最初的想法、将其转换为正式的规范、到建造可工作的原型产品以及任何用于支持产品生产或服务条款所需要的资料。

3.3.5

仿真　simulation

通过计算建立 SRS/SRSS 或子部件的模型或通过软件行为模型对某项功能的性能和子系统的规模与交互进行系统性的和/或随机的分析。

3.3.6

校准　calibration

在特定条件下，让指示数值和测量结果之间建立起关系的一组参考标准的操作。

注1：本术语的基础是“不确定度”。

注2：指示数值和测量结果之间的关系从原则上使用校准图表示。

注3：作为参照的规格可以是长期或暂时置于感应区内的带刻度物体。

注4：本文件仅关注用户侧的校准。SRS/SRSS生产过程中的校准——属于设计和开发阶段的分析过程，制造商基于此实现规定的检测能力——本文件并不涉及。

[来源：IEC 60050-311:2001,311-01-09,有修改]

3.3.7

校准步骤　calibration procedure

在按照已知方法执行的具体测量过程中，对所使用的一组操作进行记录、验证和确认的步骤。

注：本文件所指校准步骤包括校准和调节。

[来源：IAS 校准和试验实验室认证计划定义，2018，有修改]

3.3.8

机械　machinery

配有或将会配备驱动系统的机器组件，其中驱动系统由若干零部件根据特定的应用目标组合而成，至少有一个零件是运动的。

注1：术语“机械”也包括为了同一个应用目的，将其组装、控制到一起以实现整体功能的若干台机器的组件。

注2：GB/T 15706—2012的附录A提供了机器的一般性图示。

[来源：GB/T 15706—2012,3.1,有修改]

3.3.9

安全相关系统　safety-related system

同时满足下述功能的指定系统：

——为达到或保持EUC（被控设备）安全状态而实施必要的安全功能；而且

——打算依靠系统自身或结合其他E/E/PE安全相关系统以及其他降低风险措施，达到预定安全功能所必需的安全完整性。

[来源：GB/T 20438.4—2017,3.4.1,有修改]

3.3.10

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

机器控制系统中负责执行安全功能的部分。

注1：一个SCS指的是为了实施相应的安全子功能所必需的一个或多个子系统的组合。

注2：SCS和GB 28526中的SRECS类似。

注3：一台机器的SCS数量等于其安全功能的数量。一个SCS对应一个专门的安全功能。

注4：SCS在GB/T 20438.4—2017的3.4.1中具有不同于安全相关系统的含义。

3.3.11

安全相关传感器　safety-related sensor；SRS

执行安全相关功能的一个或多个传感单元组合。

注1：当SRS用作SRSS的一部分时，SRS认为是SCS的一个子系统，或者是SCS中的一个子系统元件。

注2：一个传感单元可能包含一个或多个传感元件。

3.3.12

安全相关传感器系统　safety-related sensor system；SRSS

两个及以上用于执行安全相关功能的安全相关传感器的组合。

3.3.13

电敏保护设备　electro-sensitive protective equipment；ESPE

配合实现保护脱扣或人员检测的一组装置和/或部件，至少包含：

——一个检测设备；

——控制/监控装置；

——输出信号开关装置和/或一个安全相关数据接口。

注：ESPE是用作降低风险措施的一种防护设备。

3.4 系统相关术语

3.4.1

子系统 subsystem

SCS顶层架构设计的实体，其中若任何子系统出现危险失效，则将导致安全相关控制功能的危险失效。

注1：一个完整的子系统由多个可识别的独立子系统元件组成，这些子系统元件组合到一起以实现分配给子系统的功能模块。

注2：此处定义的子系统与日常用语相区分，日常使用的“子系统”是某个实体的任意部分，而IEC 62061中使用的“子系统”却有明确的术语分层体系：“子系统”仅指一个系统的第一层细分部分。再往下层的细分部分则称为“子系统元件”。

[来源：IEC 62061:2024，3.2.4，有修改]

3.4.2

子系统元件 subsystem element

子系统的一部分，由单个或任意一组用于执行一个或更多的元件功能部件组成。

注：元件可能由硬件和/或软件构成。

[来源：GB 28526—2012，3.2.6，有修改]

3.4.3

复杂性 complexity

一个以多个子系统元件或子功能复杂交互为特点的SRS/SRSS或安全功能的属性。

注1：一个SRS/SRSS的复杂性程度可能取决于供应链中的角色或视角。在开发过程中，制造商会认为某个SRS因有许多交互子系统元件和大量外部影响需要考虑而高度复杂，但是按照预定用途在限值范围内使用这个SRS的集成商则会将其视作一个黑盒子，从而认为其复杂度较低。

注2：复杂系统或功能的详细行为无法通过简单计算得到。

3.4.4

要求率 demand rate

在一定时间内引起SRS/SRSS执行安全相关功能的事件数量。

注1：低要求模式指的是SRS/SRSS仅在需要时且要求率不大于每年一次的条件下执行安全相关功能的工作模式。

注2：高要求模式指的是SRS/SRSS仅在需要时且要求率大于每年一次的条件下执行安全相关功能的工作模式。作为参考，表G.1给出了高要求率数据[所述数值符合ISO 13849(所有部分)]。

注3：连续模式指的是SRS/SRSS持续(连续)执行安全相关功能的工作模式。实际上，在连续模式下用要求率的限制因素是SRS/SRSS的响应时间。

注4：SRS/SRSS安全相关功能的要求率能够与SCS中所执行安全相关功能的要求率不同。

3.4.5

安全状态 safe state

EUC(被控设备)达到安全性要求时的状态。

示例1：安全状态可能由判定概率信息决定。

示例2：安全状态可能由置信度信息决定。

注：安全状态可能与各种输出信号有关，具体取决于预定用途和所执行的SRS/SRSS功能。

[来源：GB/T 20438.4—2017，3.1.13，有修改]

3.4.6

正常运行条件　normal operating condition

尽可能接近正常使用时合理范围的运行条件。

3.4.7

正常运行　normal operation

SRS/SRSS 按照预期且无故障运行时的状态。

3.4.8

预定用途　intended use

符合产品或系统所提供信息或者(在没有这些信息时)对使用方式的一般理解的用途。

[来源:ISO/IEC Guide 51:2014,3.6]

3.4.9

使用限值　limit of use

输出单元在检测能力、感应区、环境、安装和安全相关信息等方面的限制条件,以及 SRS/SRSS 制造商或将 SRS 集成到 SRSS 的集成商所提供的 SRS/SRSS 性能等级的限制条件。

注:在确认SRS/SRSS是否适合预定用途的应用时,使用限值至关重要。

3.5　融合

3.5.1

调准　alignment

对 SRS 测量值进行处理以实现一致的时间和空间基准。

3.5.2

多样性　diversity

执行一项所需功能的不同方式。

注:多样性通过不同的物理方法或不同的设计方式达成。

[来源:GB/T 20438.4—2017,3.3.7,有修改]

3.5.3

融合　fusion

在显性或隐性知识框架中组合或关联数据或信息的行为或过程,以提高检测、识别或表征实体的能力(或提供新的能力)。

3.5.4

冗余　redundancy

提供一种以上执行某项功能的方法。

注:故意提供执行某项功能的不同(多样)方法降低出现共因失效的可能。

[来源:GB/T 2900.99—2016,192-10-02,有修改]

3.6　安全相关信息

3.6.1

模拟信号　analog signal

直接表示相应变量数值大小的信号。

注1:模拟信号可以是数值连续或离散的信号,也可以是时间连续或离散的信号。比如,气动终端控制元件中的压力具有数值和时间均连续的信息参数(压力值),同时也有位置调制脉冲信号作为基于计算机的控制器的输出信号。

注2:对应GB/T 2900.56—2008的术语351-21-53。

[来源:IEC 60050-351:2013,351-41-24,有修改]

3.6.2

包含区间　coverage interval

根据已有信息,包含具有规定概率 SRS/SRSS 测量信息真实值集合的区间。

注:包含区间不一定位于所选被测量数值的中心。

[来源:ISO/IEC Guide 99:2007,2.36,有修改]

3.6.3

包含概率　coverage probability

SRS/SRSS 测量信息真实值集合落在规定包含区间内的概率。

注:包含概率也被称为"置信度"。

[来源:ISO/IEC Guide 99:2007,2.37,有修改]

3.6.4

置信度信息　confidence information

用于安全相关概率测量补充的 SRS/SRSS 测量信息或判定信息。

注:置信度信息在SRS/SRSS提供测量信息的条件下包含了包含概率和包含区间,在SRS/SRSS提供判定信息的条件下包含了判定概率。

3.6.5

判定概率　decision probability

判定信息正确无误的概率。

3.6.6

数字信号　digital signal

时间离散的信号,信号所包含的信息由已明确定义、个数有限的离散值来表示,各值均可由该信号的特征量之一随时间来取。

[来源:IEC 60050-702:1992,702-04-05]

3.6.7

二进制数字信号　binary digital signal

二进制信号　binary signal

每一个信号元都具有两个允许离散值中的某个值的数字信号。

[来源:IEC 60050-704:1993,704-16-03]

3.6.8

***n* 位数字信号　n-ary digital signal**

***n* 位信号　n-ary signal**

每一个信号元都具有 n 个允许离散值中的某个值的数字信号。

[来源:IEC 60050-704:1993,704-16-05]

3.6.9

串行数字传输　serial digital transmission

串行传输　serial transmission

在两点间的单一通道上顺序传输信号元。

3.6.10

并行数据传输　parallel digital transmission

并行传输　parallel transmission

在两点间适当数量的并行通道上同时传输一组信号元。

[来源:IEC 60050-704:1993,704-16-28]

3.6.11

故障反应功能　fault reaction function

当 SRS/SRSS 诊断功能在 SRS/SRSS 内检测到故障时所启动的功能。

3.6.12

故障响应时间　fault response time

从 SRS/SRSS 信号发出到启动故障反应功能并在输出单元上提供适当安全相关信息之间的最大时间。

3.6.13

判定信息　decision information

表示 SRS/SRSS 中执行各变量值判定的结果的信息。

注1：例如，某个物体进入安全相关区的判定结果会导致一个切换信号。

注2：变量值是物体或环境信息的属性。

3.6.14

SRS/SRSS测量信息　SRS/SRSS measurement information

表示各被测变量值的信息。

注：例如，以 n 位数字输出信号的形式表示物体在感应区中的位置。

3.7　试验

3.7.1

验收试验　acceptance test

向客户展示产品达到验收要求的合同程序。

[来源：GB/T 2900.99—2016，192-09-03，有修改]

3.7.2

耐久试验　endurance test

研究产品属性如何受到持续或重复施加规定应力影响时所执行的操作。

[来源：GB/T 2900.99—2016，192-09-07，有修改]

3.7.3

现场试验　field test

在用户工作条件下进行的试验。

注：在试验时，可监控或记录工作、环境、维护和测量的条件。

[来源：GB/T 2900.99—2016，192-09-06]

3.7.4

实验室试验　laboratory test

在预设和受控条件下（可能无法模拟现场条件）执行的试验。

[来源：GB/T 2900.99—2016，192-09-05，有修改]

3.7.5

维护试验　maintenance test

定期在产品上执行的试验，目的是确认产品性能（在经过必要的调整后）仍能维持在规定限值内。

[来源：GB/T 2900.83—2008，151-65-25，有修改]

3.7.6

鉴定试验　qualification test

确认产品性能符合规范要求的验证过程。

注：鉴定试验通常在开始产品大规模生产之前进行。

[来源：GB/T 2900.99—2016，192-09-04，有修改]

3.7.7

例行试验　routine test

在制造期间或之后对每个产品都要进行的试验。

注：例行试验在产品供应之前进行。

3.7.8

模拟试验　simulation test

施加预定用途下预期环境和工作应力进行的试验。

注：实际上，试验条件仅能达到与实际使用条件近似的水平，其复现精度叫做模拟度。

[来源：GB/T 2900.99—2016，192-09-18，有修改]

3.7.9

系统试验　system test

对整个系统进行的试验，目的在于确定与各功能规范不一致之处。

注：系统试验主要用于验证，但是也可能包括一些确认过程。

[来源：GB/T 2900.99—2016，192-09-25，有修改]

3.7.10

试验　test

确定是否符合预定用途或具体应用要求的测试。

注：如果试验结果表明符合预期，则将其用于确认过程。

[来源：GB/T 19000—2016，3.11.8，有修改]

3.7.11

型式试验　type test

对采用某种设计的一个或多个被测设备进行试验，以确定设计是否满足规范。

[来源：GB/T 2900.25—2008，411-53-01，有修改]

3.8　用户类别

3.8.1

集成商　integrator

将一个 SRS 和/或 SRSS 集成到一个 SCS 和/或机械中或者将一个 SRS 集成到一个 SRSS 中的实体。

注1：集成商可能是制造商、装配商、设计加工企业或用户。

注2：本文件所指的集成商可能是一个SRSS、SCS或机械的制造商。

注3：集成商最初在ISO 11161中被定义为“设计、提供、制造或组装一套集成制造系统且负责安全策略（包括控制系统的防护措施、控制接口和相互连接等）的实体”。本文件对该定义进行了修改，以涵盖从集成到机械定义已涵盖的集成制造系统间的相关阶段。

3.8.2

供应商　supplier

SRS/SRSS供应商　SRS/SRSS supplier

在供应链行为中的角色主要是将产品或服务以及相关使用说明提供给客户并最终提供给操作员的组织机构。

注1：供应链行为包括将自然资源、原材料、部件和相应信息转换成提供给最终用户组织的最终产品。

注2：本文件所指供应商可能是生产SRS、SRSS或使用SRS/SRSS的机械的制造商。

3.8.3

用户　user

SRS/SRSS用户　SRS/SRSS user

表示客户组织中的一群人或个人。

注：一个用户可能是集成商、机械制造商或操作员。

3.9 验证和确认

3.9.1

失效模式和影响分析 failure modes and effects analysis;FMEA

定性分析方法,主要包括对子部件可能出现的失效模式和故障及其在不同层次上的影响进行的研究。

注:不使用GB/T 2900.99—2016中“故障模式和影响分析(fault mode and effects analysis)”的说法,因为故障是一种状态,因此在逻辑上不可能具有某种模式,而失效模式指的是状态的变化。

[来源:GB/T 2900.99—2016,192-11-05,有修改]

3.9.2

故障树分析 fault tree analysis;FTA

使用故障树进行演绎分析。

注:见故障树 。

[来源:GB/T 2900.99—2016,192-11-08]

3.9.3

正式设计评审 formal design review

对设计及其要求进行独立且有记录的审查,以评估设计满足相关产品明确或隐含要求的能力。

注1:此处的“设计”包括要求、规范、图纸和支持文档等。

注2:有关设计评审实践的更多详情,见IEC 61160。

[来源:GB/T 2900.99—2016,192-12-07,有修改]

3.9.4

检查 inspection

审查某个产品设计、产品、过程或装置是否满足具体要求或基于专业评估满足一般要求。

注:对一个过程的检查可能包含对人员、设施、技术和方法等的检查。

3.9.5

生命周期 life cycle

产品从概念到废弃所经历的一系列可区分的阶段。

示例:一个典型的系统生命周期包括:概念和定义;设计和开发;制造、安装和调试;运行和维护;中期升级或寿命延长;以及停用和处理。

注:具体阶段视应用而定。

[来源:GB/T 2900.99—2016,192-01-09]

3.9.6

预计 prediction

用于获取某个量的预计数值的计算过程。

[来源:GB/T 2900.99—2016,192-11-01]

3.9.7

可靠性模型 reliability model

用于预计或估算可靠性大小的数学模型。

注1:关于可靠性建模的更多详情,见IEC 61703中的术语“可靠性、可用性、可维护性和维护支持的数学表示”。

注2:建模技术能应用到可维护性和可用性等其他可信度特性。

[来源:GB/T 2900.99—2016,192-11-02,有修改]

3.9.8

验证 verification

通过提供客观证据以证实产品满足规定的要求。

注1：验证使用的客观证据是检查或其他形式的判定结果，比如执行替代计算或审查文档等。

注2：为了验证而执行的动作有时被称为鉴定过程。

注3："已验证（verified）"用于表示对应的状态。

[来源：GB/T 19000—2016，3.8.12，有修改]

3.9.9

确认　validation

通过提供客观证据以证实产品满足预定用途或特定应用要求。

注1：确认所需客观证据是试验或其他形式的判定结果，比如执行替代计算或审查文档等。

注2："已确认（validated）"用于表示对应的状态。

注3：确认时所使用的条件是真实条件或模拟条件。

[来源：GB/T 19000—2016，3.8.13，有修改]

4　生命周期以及与安全相关控制系统（SCS）的相互联系

4.1　通则

用作防护措施的安全相关传感器（SRS）（见图2和图3）或安全相关传感器系统（SRSS）（见图4）应执行5.2所述功能。

一个SRS至少应包括：

——一个检测单元；

——一个处理单元；以及

——一个输出单元（输入单元是不必须的）。

一个SRSS至少包括两个SRS以及处理单元和输出单元（输入单元可选）。

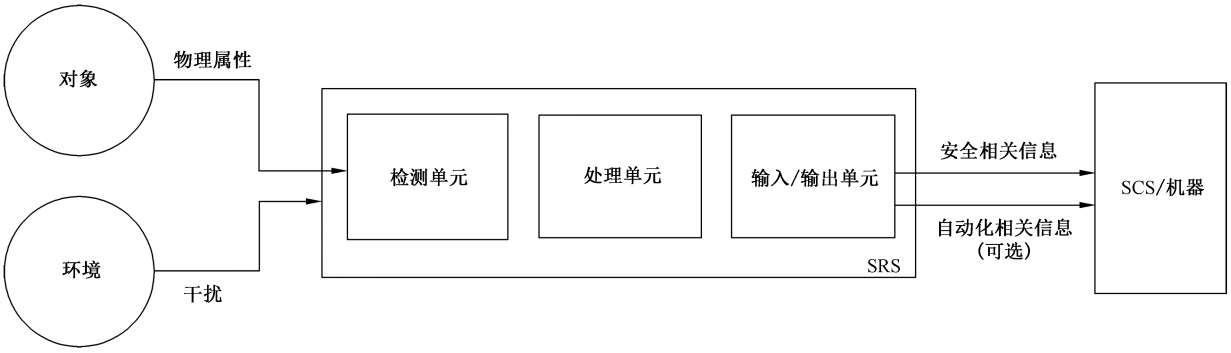


图2　SRS结构示例1

注1：在构造SRS时，使用单独或公用的检测、处理和输出单元来执行安全相关和自动化相关功能。

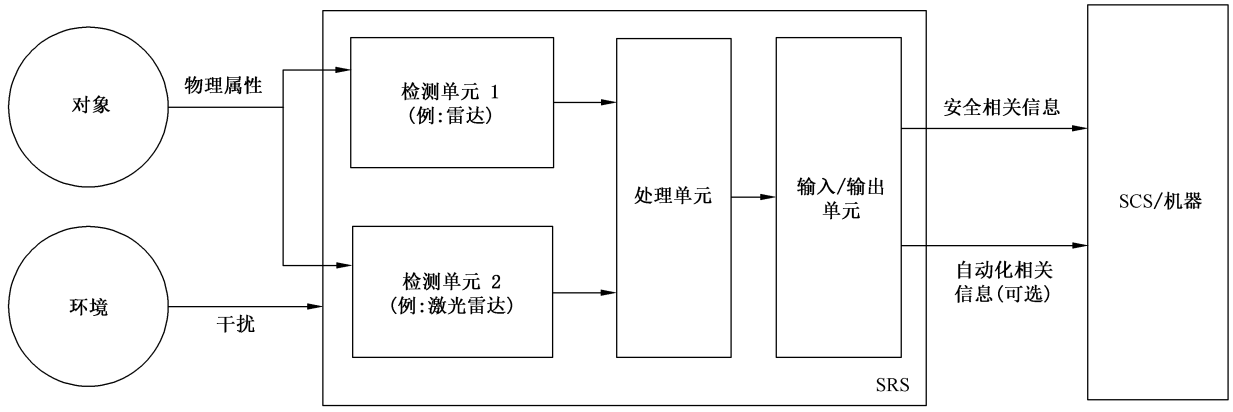


图 3 SRS 结构示例 2

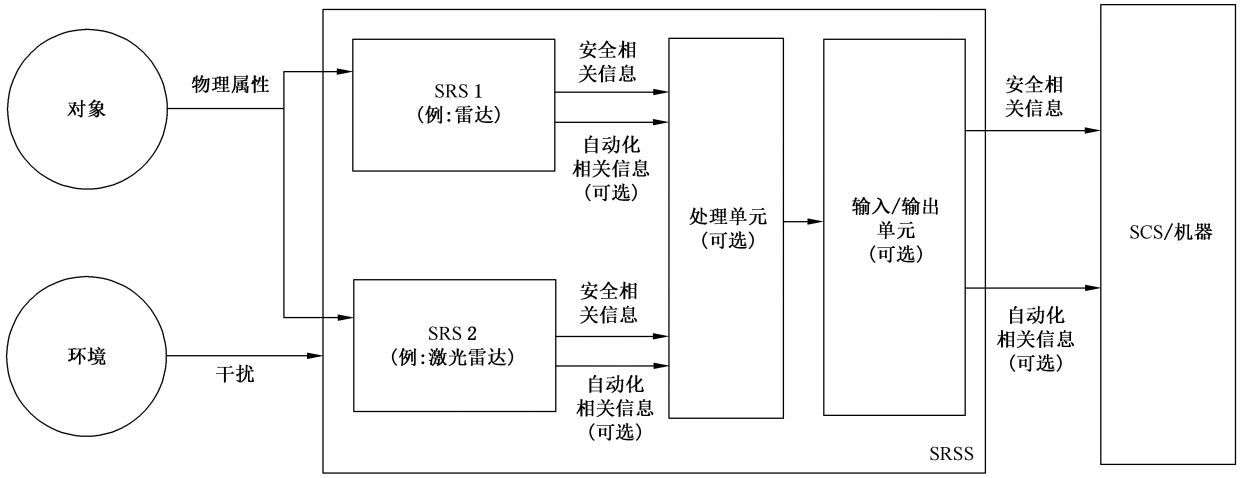


图 4 SRSS 结构示例

检测单元会采集物体属性和/或环境影响的相关信息来执行检测功能,并将其作为输入提供给处理单元。

注 2:检测单元包含一个或不包含发射元件。

处理单元靠对检测单元生成的信息进行处理来执行处理功能,从而产生安全相关信息。

注 3:处理单元是模拟和/或数字单元。

输入/输出单元:

——连接到一个 SCS/机器;

——会提供安全相关信息;

——可以接收安全相关信息;而且

——可以提供自动化相关信息。

如果在输入/输出单元中使用了安全相关通信网络,则其应满足相应标准的要求(比如功能安全现场总线应符合 IEC 61784-3)。

SRS/SRSS 制造商应根据本文件要求确定相应的技术和组织措施,以实现整个生命周期内的系统性能力,在此过程中须考虑 SCS 功能安全标准所规定生命周期的各个阶段或下述阶段:

——危险和风险分析;

——设计和开发阶段;

——集成和安装阶段；

——运行、维护和修改阶段。

SRS/SRSS 文档应为 SCS 文档的一部分。

注 4：SRS/SRSS 安全要求规范是 SCS 安全要求规范的一部分。

注 5：术语“文档（documentation）”不仅限于传统意义上的文件，还有数据文件和数据库信息等意思。

4.2 危险和风险分析

4.2.1 通则

危险和风险分析应用于：

——确定 SRS/SRSS 会造成的潜在危险；以及

——为风险分析的结果，确定所需要的安全性能等级（比如 PL，SIL 或 SILcl）。

在开始 SRS/SRSS 设计和开发过程之前，宜先按照机械设备的现场应用要求完成有关的风险分析，如图 5 所示。分析结果是安全要求规范的重要组成部分。在 SRS/SRSS 设计和开发过程中，应确定 SRS/SRSS 所产生的危险，并应在安全要求规范中增加相应的防范措施。应随 SRS/SRSS 向各用户类别提供相关使用说明。

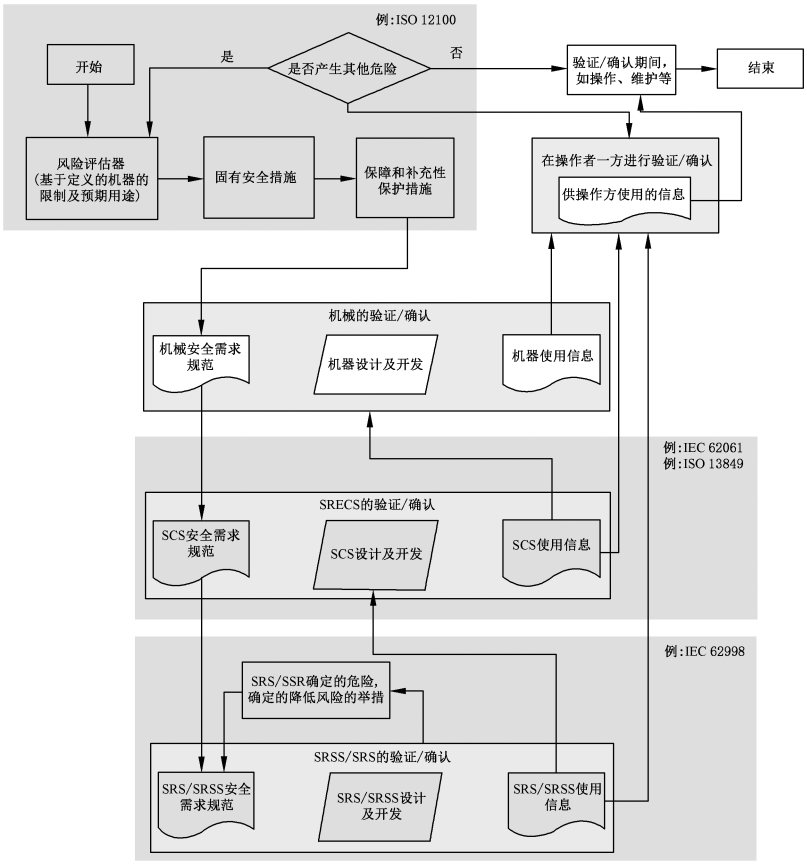


图 5 SRS/SRSS 危险和风险分析流程

4.2.2 由 SRS/SRSS 造成的危险

4.2.2.1 通则

制造商应分析 SRS/SRSS 可能带来的潜在危险，并采取措施将风险降低到符合相关标准的容许范围内。

注1：SRS/SRSS带来的危险可能来自光辐射、超声波辐射以及暴露在电离辐射中。

注2：相关标准或法规规定了针对危险电磁辐射所提供的保护[见EN 50499,EN 50527(所有部分)及EN 50346;超声波技术见ISO 16148]。

结果应记录在案。

4.2.2.2 光辐射危险

针对安全相关辐射的保护措施应按照IEC 60825-1。

针对安全不相关辐射的保护措施应按照IEC 62471。

4.2.2.3 电气事故

针对电击的保护措施应按照IEC 60204-1或IEC 61010-1。

4.2.3 所需SRS/SRSS性能等级

应根据预定用途执行符合相关标准的风险分析和降低风险过程。如果可通过安全相关控制系统实现降低风险的目的,则风险降低过程应建立在整个降低风险过程输出信息的基础上。达到预期风险降低目的所需要的安全相关控制系统安全性能等级(比如PL,SIL或SILcl)以及对应的SRS/SRSS性能等级(见4.3)应使用下述方法之一予以确定:

——所需要的安全相关控制系统安全性能等级符合C类机器的特定标准;

——达到预定风险降低目的所需要的安全相关控制系统安全性能等级符合通用或具体领域功能安全标准[比如ISO 13849(所有部分),IEC 62061,IEC 61508(所有部分),ISO 26262(所有部分),ISO 25119]。

注1：预定用途通常总称为“应用(application)”。应用能够指某个具体型号的机器、电气设备在某个领域(比如机械领域)的一般应用或者如IEC 61508(所有部分)所述一般性地用作安全相关工作系统的一部分。

注2：在工业机械安全方面,最基础的是ISO 12100。机械制造商能够按照ISO 12100所述进行风险评估和风险降低过程,以确定危险、预估风险以及充分降低风险。ISO 12100与B类和C类标准之间的关系见ISO TR 22100-1;ISO 13849-1和ISO 12100之间的关系见ISO TR 22100-2。

4.3 对应SRS/SRSS性能等级

应按照第5章所述流程使用SRS/SRSS性能等级。

所需要的最低SRS/SRSS性能等级对应的安全性能等级如表1所示。

表1 所需要的最低SRS/SRSS性能等级与安全性能等级之间的对应关系

安全相关文件	SRS/SRSS性能等级 A	SRS/SRSS性能等级 B	SRS/SRSS性能等级 C	SRS/SRSS性能等级 D	SRS/SRSS性能等级 E	SRS/SRSS性能等级 F
ISO 13849(所有部分)	PL a	PL b	PL c	PL d	PL e	
IEC 62061			SILcl 1	SILcl 2	SILcl 3	
IEC 61508			SIL 1	SIL 2	SIL 3	SIL 4
待定[a]						

表 1　所需要的最低 SRS/SRSS 性能等级与安全性能等级之间的对应关系（续）

安全相关文件	SRS/SRSS性能等级 A	SRS/SRSS性能等级 B	SRS/SRSS性能等级 C	SRS/SRSS性能等级 D	SRS/SRSS性能等级 E	SRS/SRSS性能等级 F
注1：规定的各种性能等级可能会使最终用户感到迷惑。本文件并未使用IEC 61496中定义的类型（Type），因为具体设计方法要与本文件所述的一般性方法明确区分开来。 注2：SRS/SRSS中安全相关电气、电子和软件部分安全性能等级的对应源于一个事实，那就是所提供的风险降低措施也会受到系统性能力的限制（比如环境影响、EMC、检测能力和检测技术等）。						
[a] 表1确立了本文件所述性能等级和ISO 13849（所有部分）、IEC 62061以及IEC 61508（所有部分）安全性能等级之间的对应关系。当然，今后还可确立与其他安全性能等级之间的对应关系，比如ISO 25119（所有部分）中的农业PL以及ISO 26262（所有部分）中的ASIL等。						

供应商应在使用说明中介绍所确定的 SRS/SRSS 性能等级（比如 SRS 性能等级 B）和安全性能等级（比如 PL，SIL 或 SILcl）。使用说明应明确（无歧义地）指出：

——元件/子系统描述和安全性能等级符合安全相关控制系统的参考标准；以及

——SRS/SRSS 性能等级符合本文件用于系统性能力检验的要求。

示例：传感器子系统SIL 2符合IEC 62061。SRS性能等级D符合本文件用于系统性能力检验的要求。

5　设计和开发阶段

5.1　通则

SRS/SRSS 的设计和开发应至少涵盖下述内容：

——确定预定用途；

——按照 5.2 确定所需要的 SRS/SRSS 功能；

——将得到的安全相关要求记录在安全要求规范中；

——根据安全性能等级和参考标准（见 4.3）对安全相关电气、电子和软件进行设计；

——按照 5.3 和 5.4 通过模拟进行设计分析。

注：IEC 61508-1：2010，7.6.2.11要求E/E/PE安全相关系统具备SIL 4安全功能（例如性能等级F的SRS/SRSS），需要反复斟酌是否能对某些风险参数进行修改以规避对于SIL 4安全功能的要求。

5.2　SRS/SRSS 功能

对于所有 SRS/SRSS 性能等级而言，SRS/SRSS 应：

——由制造商定义并根据表 2 中的总体说明将其分解为具体功能；以及

——在使用说明中明确指出。

安全相关功能应：

——在规定环境条件下执行；

——在制造商规定的使用限值条件下执行；而且

——记录在安全要求规范中。

表 2　SRS/SRSS 功能（在适当的情况下）

功能	总体说明
SRS/SRSS功能	确定目标物体在下述条件下随时间的变化： ——具备规定的物理属性； ——在规定的应用中； ——在环境条件下。 并提供相应的输出信息
安全相关功能	SRS/SRSS 安全相关物体的功能出现故障或性能不佳，会导致检测能力降低并超过本文件所述限值从而造成危险失效的部分
自动化相关功能	SRS/SRSS安全相关物体检测功能出现故障或性能不佳，不会导致危险失效的部分
危险物体检测功能	负责检测会构成危险源的相关物体，进入或处于安全相关区内的安全相关功能部分
人员检测功能	负责检测用于表示人或人体部位的安全相关物体进入或处于安全相关区内的安全相关功能部分
注：在设计和开发期间需要表2所述的功能，并在应用中也要基于此确定机器安全功能的哪一部分由SRS/SRSS提供。有关安全功能分解的更多信息请见附录C。	

5.3　设计分析

对于所有 SRS/SRSS 性能等级而言，SRS/SRSS 设计都应分析以下内容：

——安全相关功能在 5.8.3.3 规定的环境条件下的危险失效；

——在 5.8.3.4 规定的环境条件下的正常运行；

——安全相关物体物理属性的类型和组合与检测技术之间的关系；以及

——检测能力限值及其可信度。

注 1：作为验证过程一部分的设计分析方法其定义见 8.4。

注 2：用于检测的算法也是分析的一部分。

对于 SRS/SRSS 性能等级 C，D，E 和 F 而言，SRS/SRSS 的设计应对执行自动化相关功能时安全相关功能的危险失效进行分析。

5.4　模拟

对于 SRS/SRSS 性能等级 D，E 和 F 而言，设计分析应包含通过模拟确定 SRS/SRSS 安全相关功能符合下述要求的过程：

——在容许的部件条件下；

——在规定的任务时间范围内；以及

——在制造商规定的使用限值极限。

模拟应由制造商实施，且最少应使用下述条件：

——确定性的和/或随机性的计算值；

——来自部件供应商的数据；

——来自后续合格性试验的数据；以及

——设计和开发期间的研究数据。

应通过型式试验对模拟进行验证。

注：有关SRS/SRSS分析所用模拟过程的构造和应用，见附录D。

5.5 感应区

供应商应在适当情况下提供感应区的相关信息。

感应区内任意位置的一个或多个物体(见 5.8.2.2 和 5.8.2.3)不应造成安全相关区内检测能力的下降,或者应使输出单元产生相应的安全相关信息。

5.6 安全相关区

供应商应提供安全相关区的有关参数信息。

安全相关区内任意位置的一个或多个物体(见 5.8.2.2 和 5.8.2.3)应:

——能被检测到;而且

——应使输出单元产生相应的安全相关信息。

5.7 自动化相关区

供应商应在适当情况下提供自动化相关区的信息。

注:出于质量控制或过程控制目的的自动化相关功能能够在自动化相关区内执行。

对 SRS/SRSS 性能等级 C,D,E 和 F 而言,自动化相关区内任意位置的一个或多个物体(见 5.8.2.4):

——不应导致安全相关功能的危险失效;而且

——能够使输出单元产生自动化相关信息。

5.8 检测能力和可信性

5.8.1 通则

应对 SRS/SRSS 的检测能力及其可信性进行分析和试验,包括下述几个方面:

——5.8.2 中定义的物体类别和物理属性;

——使用限值;

——SRS/SRSS 性能等级;

——可预见的误用;

——5.8.3.3 中在考虑下述可信性因素时针对危险失效所规定的环境影响:

- 完整性,
- 可靠性,
- 安全性;

——5.8.3.4 中在考虑下述可信性因素时针对正常运行所定义的环境影响:

- 可用性,
- 鲁棒性。

对于 SRS/SRSS 性能等级 A 和 B 而言,进行相应的试验就足够了,可省去分析步骤。

5.8.2 物体类别和物理属性

5.8.2.1 通则

物体应由制造商定义且可根据其物理属性进行检测以执行表 2 所述的功能。

物体应被定义为:

——用于执行人员检测功能的物体;

——用于执行危险物体检测功能的物体;

——用于执行自动化相关功能的物体。

用于检测安全相关物体的物理属性应：

——根据制造商安全要求规范中的定义，能够代表安全相关物体的特征；

——适用于人员检测功能和危险物体检测功能（如表 2 所述）所使用的检测技术。

注 1：物体的物理属性能够包含但不限于：吸收率（物理）、吸收率（电磁）、面积、电容、密度、介电强度、延展性、弹性、电荷、电导率、电阻、电场、辐射、流量、流动性、频率、硬度、感抗、内阻、强度、辐照度、长度、位置、亮度、发光、可锻性、磁场、不透明度、透过性、电容率、照射、反射率、强度、温度、热导率、速度和体积。

注 2：物理属性限制范围的定义能够采用最新标准（比如应用标准以及传感器相关的产品标准等）。

应确定 SRS-SRSS 功能适用的物理属性限制范围，并在使用说明中提供。

5.8.2.2 人员和相关属性

制造商应在适当条件下规定用于人员检测的物理属性，以及人员检测功能适用的物理属性限制范围。

设计和开发时应使用所规定的物理属性限制范围。

成年人及其身体部位的长度、面积和体积属性应符合 ISO 7250（所有部分）。

注 1：在 ISO 7250（所有部分）中，仅考虑了成年人。

如果 SRS/SRSS 要用于检测儿童：

——制造商应规定 14 岁以下所考虑的年龄范围；

——应使用 CEN/CENELC 导则 14 中附录 C 和附录 D 所列出的具体年龄段的行为和发展特征；

——制造商应规定表示儿童身体或部位的尺寸，而且宜考虑附录 E 的相关要求。

应根据皮肤和衣物属性得到反射率属性。

若使用放射物实现检测功能，则应核查与波长的关系。

注 2：有关反射率的更多信息见相关标准（比如 IEC 61496-3，ANSI/ITSDF B56.5：2012，ISO 15622，ISO 18497）。

除非预定用途有特殊要求，否则均应默认为漫反射。

除非预定用途有特殊要求，否则均应假设成人的步行速度在 0 mm/s 到 1 600 mm/s 之间。

注 3：按照 ISO 13855 的规定，在工业环境中的速度为 1 600 mm/s。在现场要采取典型的组织措施，提醒工作人员严禁奔跑。

除非预定用途有特殊要求，否则均假设成人的加速度在 0 mm/s^2～2 000 mm/s^2 之间。

注 4：根据[79]的规定，成人初始正常步行速度为 1 600 mm/s 时，其加速度为 2 000 mm/s^2。

注 5：人在奔跑时会有不同的速度和加速度。

在适当的情况下，制造商应在考虑附录 E 中相关行为的前提下，规定儿童的速度和加速度属性。

5.8.2.3 危险物体

在适当的情况下，制造商应指定用于危险物体检测的物理属性，以及执行危险物体检测功能的物理属性限制范围。

5.8.2.4 自动化物体

在适当的情况下，制造商应指定用于执行 SRS/SRSS 性能等级 C、D、E 和 F 自动化相关功能的物体。

注：规范用于说明是在何种条件下进行的设计和开发，来研究自动化物体对 SRS/SRSS 安全相关功能的影响。

5.8.3 环境影响

5.8.3.1 通则

制造商应指定会导致 SRS/SRSS 可信性下降的环境影响。

应在考虑下述因素的前提下对指定环境影响造成的潜在可信性下降问题进行分析：

——预定用途；

——SRS/SRSS 的传感器技术；

——安全相关物体的物理属性。

5.8.3.2 条件和约束

SRS/SRSS 制造商应确定预定用途下的环境条件和约束。环境参数及程度应从 IEC 60721(所有部分)中选取，并考虑以下(但不限于)各方面：

a) 室内和/或室外使用(遮挡或不遮挡)；

b) 固定运行和/或移动运行；

c) 温度和湿度；

d) 降雨(雨、雪或冰雹)和风；

e) 压力(周围空气、水等)；

f) 太阳辐射和热辐射；

g) 凝结和结冰；

h) 雾、尘、沙和盐雾；

i) 振动和冲击；

j) 动物和植物(比如长霉)；

k) 化学影响；

l) 电和电磁影响；

m) 机械载荷；

n) 声音。

注1：附录F提供了关于如何使用所列环境条件的示例。

面向具体应用的机械标准可能会提供 a)～n)所列一些或全部环境条件的详细要求。

针对具体领域或机器类型规定环境要求的标准如表 3 所示。

表 3 包含环境要求的标准

标准	应用领域/具体机器类型
IEC 60654-1	工业过程测量和控制设备运行条件
ISO 15003	农业工程电气和电子设备耐环境条件试验
EN 50125-1	铁路应用设备的环境条件　第1部分：铁路机车及车载设备
ISO 15998	土方机械使用电子部件的机器控制系统(MCS)功能安全的性能标准和试验
IEC 60721-3-3	环境条件分类　第3-3部分：环境参数组及其严酷程度的分类分级在有气候防护措施的地方固定使用
IEC 60721-3-4	环境条件分类　第3部分：环境参数组及其严酷程度的分类分级　第4节：在没有气候防护措施的地方固定使用
IEC 60721-3-5	环境条件分类　第3部分：环境参数组及其严酷程度的分类分级　第5节：地面车辆上的设备
IEC 60721-3-6	环境条件分类　第3部分：环境参数组及其严酷程度的分类分级　第6节：船舶环境

制造商应指定所有相关环境影响在危险失效和正常运行条件下的限制范围。

注2：环境条件主要用于分析和试验，以及说明使用限值。比如，类型和范围的使用限值可以是0 ℃～50 ℃的工作温度。

注3：有些标准可能并不会涵盖所有环境条件。能使用可用的公开文件研究其对检测技术的影响。[80]中提供了一个有关下雪条件的示例。

5.8.3.3 危险失效

在下述条件下，SRS/SRSS 安全功能在超出表 4 规定限值时不应因为失去检测能力而导致危险失效：

——预定用途下的环境条件符合 5.8.3.1 的分析；而且

——位于安全相关区内的任意位置的应用相关物体（包括安全相关物体）。

表 4 仅用于提供总体约束，应和 5.8.3.3 所述相关内容配合使用。应在应用层面分析相关环境条件，以确定检测能力丧失预计会出现的频率和持续时间以及要求率是否会导致可预见的危险情况。如果会导致危险状况，则不应将表 4 所述限制用作约束条件，而是应采取进一步的措施。

示例1：任何检测能力丧失或下降都会立即导致危险状况。

示例2：导致检测能力丧失或下降的环境影响也会增加风险水平，比如引起检测能力下降的降雪增加了汽车的制动距离。

制造商应使用下述方法分析相关环境条件对检测能力的影响：

——在可能发生检测能力丧失的条件下，按照 5.8.3.2 中的影响进行模拟和/或试验；以及

——确定会导致检测能力丧失的影响（量化）限值。

制造商在设计和开发阶段应记录分析结果、所确定的限值以及是否符合表 4 数据。

表 4 在高要求模式下因环境干扰导致危险失效（检测能力丧失）的限值

SRS/SRSS性能等级	每年危险失效的最长累计时间
A	1 h
B	5 min
C	1 min
D	5 s
E	0.5 s
F	响应时间

注1：最大值的定义基于这样一个事实，那就是环境条件下的偶发影响与 ISO 13849-1 通用标准中对完整性的概率要求是一致的。危险失效持续时间限值取自 PFHD 值。表 G.1 说明了它们之间的联系。

如果一个 SRS/SRSS 的响应时间长于表 4 中规定的最长持续时间，则可用其替换掉表中的数值。SRS/SRSS 并不需要提供比所规定响应时间还快的检测能力。如果危险失效的持续时间被限定为 SRS/SRSS 的响应时间，则表明没有累计持续时间方面的限制。

如果制造商不能确保因检测能力丧失所引起的危险失效持续时间低于表 4 所述限值，则制造商应通过分析证明为何不能在 SRS/SRSS 中采取足够的措施以达到表 4 的限值要求，并通过下述一项或多项措施以实施图 G.2 所示的额外方案之一：

——定义使用限值以避免在特定环境条件下发生危险失效，并额外提供相应的使用说明；或者

——确定限值在特定要求率条件下可满足公式（G.1）的要求，并额外提供相应的使用说明；或者

——确定 SRS/SRSS 检测能力下降的类型和数值，并额外提供相应的使用说明。

证明、确定和定义的结果均应记录在案。

注2：为用户提供的适当信息包括在相关环境影响条件下降低包含/判定概率或避免发生危险失效的措施（比如安装警告说明、现场试验、降低相应风险的替代措施等），或者是在应用中未达到这些限值时可能导致的后果（见附录G）。

5.8.3.4 正常运行

制造商应按照 5.8.3.2 对每一种相关环境影响进行分析，并确定在多大限值内 SRS/SRSS 可正常运行。

根据 5.8.3.2 所述的所有相关环境影响，SRS/SRSS 制造商应：

——通过符合 IEC 60068(所有部分)的环境试验和/或经过验证的模拟证明在规定限值内可以正常运行；

——指定当数值超出安全要求规范所规定限值时能够降低环境因素对可用性不利影响的措施；

——为用户提供 SRS/SRSS 正常运行限值的有关信息；

——针对在正常运行限值之外使用 SRS/SRSS 时提供相关措施的额外信息(如果有的话)。

示例：措施可包括：

- 用于提示过大的环境影响可能导致可用性降低的，或者用于触发备选运行状态的传感器输出信号；
- 具有较低检测能力但对环境影响有更高的鲁棒性的 SRS/SRSS 备选运行状态。如果能够配合机器的危险运动那么这种备选状态是可实现的。[比如在大雨或下雪条件下由于传感器检测距离会下降而适当降低自动导引车(AGV)速度]

所有限值均主要以数值形式提供，见附录 F 中的示例。

注：在正常运行条件下所定义的要求主要是为了实现在相应可信度下的可用性和鲁棒性。如果不能正常运行，绕过安全功能的风险将会提高。

5.9 用户界面

5.9.1 通则

制造商应在安全要求规范中规定安全相关用户界面的类型和性能。

用户界面的类型和性能应足以执行预定用途的安全相关功能，并至少包含以下内容：

——安装；

——(输入/输出单元上的)安全相关信息；

——在整个生命周期内降低用户界面风险的组织措施(比如对检测能力的维护试验)。

注：本文件不涉及用作SRS/SRSS输入的用户界面的操作步骤，比如使SRS/SRSS开始工作所进行的配置或供电过程。本文件主要目的是为系统性能力的评估提供指导。

用户界面的性能应在整个生命周期内有效，而且供应商应告知用户在 SRS/SRSS 整个生命周期内的所有步骤(比如试验)，其中需考虑下述几个方面：

——将安全相关信息集成到一个安全相关控制系统中；

——在最终用户侧投入运行；

——工作期间的故障处理；

——维护(比如更换)。

5.9.2 安装

供应商应告知用户以下信息：

——检测单元/SRS/SRSS 在安装位置方面的限制(比如只能顶部安装)；

——感应区与检测单元/SRS/SRSS 安装面或基准点之间的相对位置；

——检测单元/SRS/SRSS 的安装位置和限制；

——SRS/SRSS 在安装之后的检测能力；

——SRS/SRSS 感应区的位置和形状；

——防止或监测由安装变化引起危险失效的措施(比如基准点、基准、力矩限值和形状边界等)。

如果供应商提供了安装支架,那么在合理条件下应尽可能将其用于型式试验和验收试验。

5.9.3 安全相关信息

5.9.3.1 通则

制造商应规定 SRS/SRSS 所提供的安全相关信息(见图 6)。

安全相关信息包括:

——确定作为判定信息提供的物理属性是否存在的结果;和/或

——作为测量信息提供的物理属性的数值;和

——它们相应的置信度信息。

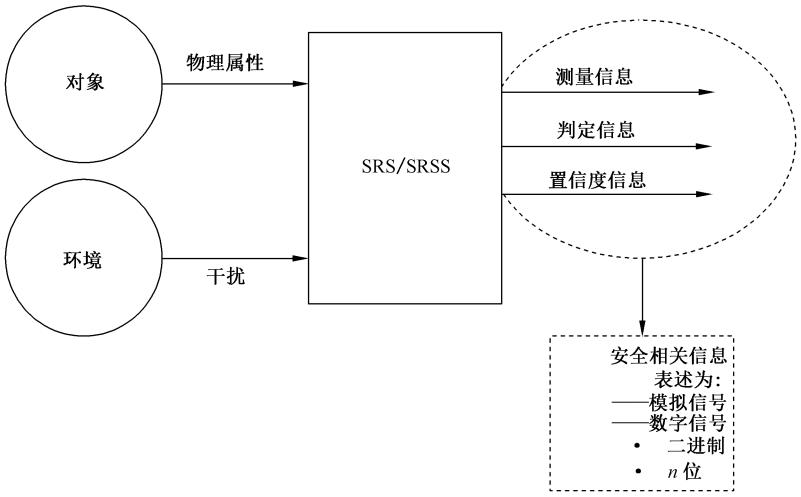


图 6 SRS/SRSS 的安全相关信息

由 SRS/SRSS 输出单元提供的安全相关信息应属于以下信号类型:

——模拟;和/或

——数字二进制或 n 位数据,通过下述方式传输:

- 串行传输通道,和/或
- 并行传输通道。

注 1:输出单元能够提供三种类型的电信号。模拟电信号(比如电流、电压等)、模拟和数字混合电信号(比如电流和 HART 协议或二进制开关和 I/O 链路等)以及数字输出信号(比如通过现场总线协议,有线或无线传输的信号)。

应指定触发故障反应的信号及其故障响应时间,并在性能等级为 C 到 F 的 SRS/SRSS 相应使用说明中提供。

注 2:触发故障反应的信号示例见 G.4。

5.9.3.2 测量、判定和置信度信息

制造商应在适当条件下指定测量信息,并在使用说明中提供相应的内容。

注 1:测量信息能够包括测量的类型和单位[比如单位为毫米(mm)的距离,单位为开尔文(K)的温度等]以及输出单元所用信号的类型和描述(比如二进制数字信号,串行传输通道上的信息传输协议等)。

制造商应在适当条件下指定判定信息,并在使用说明中提供相应的内容。

注 2:判定信息包括判定原则(规定区域内具有规定尺寸的物体)以及输出单元上对应的信号(比如满足条件时输出高电平信号,不满足条件时输出低电平信号)。

制造商应在适当条件下指定安全相关信息的置信度信息。置信度信息应包含：

——包含概率和包含区间(如果 SRS/SRSS 提供测量信息的话)；和/或

——判定概率(如果 SRS/SRSS 提供判定信息的话)。

系统性故障和误差会影响所述置信度信息。如果通过用户校准能够对误差进行补救，那么相应措施宜符合 6.3 的要求。

注 3：置信度信息是常量或随时间变化的变量。

注 4：置信度信息是由输出单元和/或使用说明中的模拟和/或数字信号提供。

注 5：包含区间不能用于离散的判定信息。

所需要的最低包含概率和或判定概率应与表 5 或公式(1)一致。

表 5　在高要求率条件下所需要的最低包含概率/判定概率

SRS/SRSS性能等级	A	B	C	D	E	F
预设的高要求率	1/24 h	1/h	1/h	4/h	4/h	4/h
包含概率(提供测量信息时)	$>1-2.4\times10^{-3}$	$>1-1\times10^{-5}$	$>1-3\times10^{-6}$	$>1-2.5\times10^{-7}$	$>1-2.5\times10^{-8}$	$>1-2.5\times10^{-9}$
判定概率(提供判定信息时)	$>1-2.4\times10^{-3}$	$>1-1\times10^{-5}$	$>1-3\times10^{-6}$	$>1-2.5\times10^{-7}$	$>1-2.5\times10^{-8}$	$>1-2.5\times10^{-9}$
注：在表5中使用了相等的包含概率和判定概率数值，因为它们会导致相同的风险上升程度。						

如果具体应用的要求率与表 5 所述不同，则应使用公式(1)。

$$P>1-\frac{L}{D} \qquad \cdots\cdots(1)$$

式中：

P ——含概率或判定概率；

L ——SRS/SRSS 性能等级对应的 PFH 上限；

D ——指的是具体应用的要求率。

注 6：PFH上限能取自通用功能安全标准，比如IEC 62061或ISO 13849-1。

5.9.3.3　响应时间

应指定从被测物理属性发生变化到输出单元上安全相关信息发生变化之间的时间。

若 SRS/SRSS 提供了置信度信息、测量信息或判定信息，则它可有不同的响应时间。宜明确(没有歧义)地规定这些不同的响应时间。

制造商应分析具有规定物理属性的指定安全相关物体是否能够在规定使用限值和响应时间内被检测到。

注：在使用限值内(比如安全相关区的尺寸)，能够规定以具体属性(比如速度)实现物体检测的响应时间。

6　集成和安装阶段

6.1　通则

SRS/SRSS 制造商应规定：

——在适当情况下，提供进一步将一个 SRS/SRSS 集成到 SCS 以实现安全相关功能的措施(比如针对系统性能力验证所实施的试验以及在集成之后对安全相关信息的适当使用)；

——在适当情况下，提供通过 6.2 所述融合方法进一步将两个或更多 SRS 集成到一个 SRSS 中的

措施；

——在适当情况下，提供在用户侧安装一个 SRS/SRSS 以实现 SRS/SRSS 安全相关功能的措施（比如需要按照安全条件对安全相关区的正确设定进行检查）；以及

——在适当情况下，提供在用户侧进行校准以实现 6.3 所述检测能力的措施。

SRS/SRSS 供应商应在使用说明中提供适当的集成和安装信息。

6.2 将 SRS 融合到一个 SRSS 中

6.2.1 通则

将两个或更多 SRS 融合到一个 SRSS 中有助于实现比单个 SRS 更大的使用限值。

6.2 提供了 SRS 集成到一个 SRSS 中的集成商（在 6.2 中被称作 SRSS 集成商）将两个或更多 SRS 融合到一个 SRSS 中的具体要求（见图 4）。

6.2 仅适用于以下条件：基于安全相关物体的物理属性将两个或更多 SRS 融合到一个 SRSS 内，且 SRS 的物理属性符合制造商规定或供应商所提供使用说明中的限制范围。

注 1：6.2 并不适用于更高层次的功能，比如物体识别或分类以及复杂物理模型。

注 2：检测单元、SRS、SRSS 的集成以及它们与传感器融合之间的关系都在附录 B（用户类别）和附录 I（功能、安全相关信息和融合的有关示例）中有更详细的说明。

注 3：6.2 并未涉及一个 SRS 内检测单元的组合。SRS 内检测单元组合（见图 3）的一个例子就是不同传感器技术的组合，比如 LIDAR（激光检测和距离检测）检测单元和雷达检测单元的组合使用。这部分内容见 SRS 制造商提供的要求。

注 4：默认将 SRS 融合到 SRSS 中的用户集成商并不像 SRS/SRSS 制造商那样能够熟练地确定 SRS/SRSS 的检测能力。集成商需要参照 SRS 提供的使用说明（见附录 B）。

注 5：默认将 SRS 融合到 SRSS 中的用户集成商应熟悉安全相关信息的融合。集成商通常都具有将安全相关信息融合所用到的信号处理技术。

使用两个或更多 SRS 的 SRSS 在设计和开发时应至少考虑下述事项：

——确定 SRSS 的预定用途；

——在考虑已确定 SRS 功能的前提下，规定最终的 SRSS 功能；

——将最终的安全相关要求记录到安全要求规范中；

——如果 SRSS 性能等级高于 SRS 性能等级（见 6.2.7），则安全相关硬件和软件的设计要求应符合表 1 所述安全性能等级（PL、SIL 或 SILcl）。

SRSS 集成商应：

——按照 6.2.2 规定使用两个或更多 SRS 的 SRSS 的使用限值；

——确认每个 SRS 的使用限值均符合 SRS 供应商所提供的使用说明要求；

——验证改进的 SRSS 使用限值（比如检测能力和安全相关信息）是否符合 6.2.9；

——向用户提供有关 SRSS 和每个 SRS 的相应使用说明。

6.2.2 融合之后的使用限值

SRSS 集成商应规定并记录 SRSS 使用限值，包括以下几个方面：

——检测能力（见 6.2.3）；

——感应区（见 6.2.4）；

——环境条件下的可信性（见 6.2.5）；

——安全相关信息（见 6.2.6）；

——SRS 性能等级（见 6.2.7）；

——融合后的响应时间（见 6.2.8）。

如果将两个或更多 SRS 融合到一个 SRSS 后的特性相较于制造商所规定每个 SRS 的特性有所改善、下降或保持不变，那么 SRSS 集成商应规定并记录使用限值。

注 1：所述检测能力的各个方面包括物体位置、物体尺寸、响应时间或测量准确度等。在感应区方面的改善是对区域范围的扩展。

注 2：SRSS 检测能力的改善通过组合使用安装在不同位置的 2 个 SRS 感应区来实现尺寸更小的公共感应区。最终，从预定用途的角度看，就实现使用限值的改善（见图 I.1）。

6.2.3 融合之后的检测能力

SRSS 集成商应指定最终达到的 SRSS 检测能力，包括以下几个方面：

——SRS 的检测能力；

——SRS 的使用限值；

——用于 SRS 检测的物理属性；

——SRS 之间可能出现的相互干扰；

——SRS 安全相关信息的调准。

注 1：如果有一个以上 SRS 要同时使用探头辐射（比如光照或雷达波或发射电磁辐射等），那么 SRSS 的检测能力可能会因为 SRS 的相互干扰而受损。

注 2：检测能力所包含的各项内容（比如位置精度或响应时间等）取决于 SRS 输出数据的精确调准（比如坐标或时序偏差都会导致测量误差或融合传感器数据的不一致）。

SRSS 集成商应按照 8.5 进行试验，从而验证 SRSS 最终的检测能力，而且应在报告中额外说明“融合之后”的试验结果。

6.2.4 融合之后的感应区

SRSS 集成商应指定最终的感应区，包括：

——制造商规定的 SRS 感应区；

——指定的 SRS 检测能力；

——SRS 的使用限值；

——SRS 之间的干扰影响；

——SRS 的安装和相对朝向；

——SRS 安全相关信息的调准。

在融合之后的感应区内应确保 SRSS 集成商所规定的 SRSS 检测能力。

注：安装时的机械调准误差或 SRS 安全相关信息的调准容差都会影响融合后的感应区。

SRSS 集成商应按照 8.5 验证 SRSS 最终的感应区，而且应在报告中额外说明“融合之后”的试验结果。

6.2.5 融合之后环境条件下的可信性

SRSS 集成商应指定所有相关环境影响的限值，包括：

——SRS 危险失效时的限值；

——SRS 正常运行时的限值。

除使用模拟方法进行分析的要求之外，应满足 5.8.3.3 中关于不能因 SRS/SRSS 安全相关功能中检测能力丧失而导致危险失效的要求。

注：因为 SRSS 集成商通常都没有关于 SRS 内传感器技术的足够信息，所以不能使用模拟方法。

在考虑 SRS 制造商所规定不发生危险失效的环境限值的前提下，SRSS 集成商应指定 SRSS 不会出现危险失效的每一种环境影响限值。

在考虑 SRS 制造商所规定正常运行环境限值的前提下,SRSS 集成商应指定 SRSS 可正常运行的每一种环境影响限值。

6.2.6 融合之后的安全相关信息

SRSS 集成商应指定 SRSS 处理单元中执行的逻辑功能以及 SRSS 所提供的安全相关信息,包括:

——SRS 的测量信息;

——SRS 的判定信息;

——对应的置信度信息。

如果 SRSS 所提供安全相关信息的置信度高于单个 SRS,那么置信度的改善以及 SRSS 的相关置信度信息应:

——基于 SRS 的置信度信息;

——考虑 SRSS 的详细处理算法;而且

——由适当的方法提供保障(比如误差传递计算或模拟)。

注 1:一般而言,融合通常由SRSS执行的大量算法实现,比如使用中心极限定理、卡尔曼滤波、贝叶斯网络等算法。在这些方法中,有些需要详细的知识背景才能确定最终的安全相关信息和对应置信度信息。

注 2:有关误差传递的更多详情见ISO/IEC Guide 98-1。

若 SRS 安全相关信息不一致,则其融合过程会导致更低的 SRSS 置信度或检测能力。SRSS 集成商应分析是否以及在何种条件下会出现不一致,以及这种不一致会如何影响检测能力和置信度信息。

SRSS 的置信度信息应满足表 5 或公式(1)的要求。

6.2.7 融合之后的 SRSS 性能等级

SRSS 集成商应指定最终的传感器性能等级,包括:

——制造商规定的每个 SRS 的传感器性能等级;

——制造商规定的 SRS 使用限值;

——SRS 的置信度信息;

——SRS 传感器技术的多样性和/或冗余性。

在下述条件下,适用于融合了两个 SRS 安全相关信息的 SRSS 的最高性能等级如表 6 所示:

——SRSS 提供的安全相关信息具有更高的可信性;

——每个 SRS 都提供了 SRSS 的安全相关信息;

——SRS 安装或/或配置所引起的某个 SRS 检测/测量性能下降(比如因环境影响导致)由其他 SRS 提供了补偿。

表 6 两个 SRS 融合之后所适用的 SRSS 最高性能等级

SRS 2性能等级	SRS 1性能等级					
	A	B	C	D	E	F
A	B	B	C	D	E	F
B	B	C	C	D	E	F
C	C	C	D	D	E	F
D	D	D	D	E	E	F
E	E	E	E	E	F	F
F	F	F	F	F	F	F

表 6 所述限制同样适用于两个以上 SRS 的组合使用。

表 6 仅限一次性使用(未考虑连续使用)。

注：如果3个SRS组合使用(性能等级分别为A、A和B),那么融合之后的性能等级限制为B。

应通过分析进行验证。

6.2.8 融合之后的响应时间

SRSS 集成商应指定从被测物理属性发生变化到 SRSS(该 SRSS 由两个或更多 SRS 融合而成)输出单元提供的安全相关信息发生相应变化之间的时间。

6.2.9 融合之后的验证和确认

SRSS 集成商应按照 6.2.3、6.2.4 和 6.2.7 对 SRSS 进行验证和/或确认。

该过程可能会需要更多的校准措施。

示例：在SRSS中组合使用SRS时,可能会有下述校准问题：

——以相对或绝对值提供测量数据；

——以不同的物理单位提供测量数据；

——空间变换；

——映射(比如将 3D 数据映射到 2D 空间)；

——不同的坐标系统(比如欧氏坐标、极坐标、柱坐标等)；

——不同的度量单位和刻度。

6.3 用户校准

6.3.1 通则

SRS/SRSS 制造商应规定,在应用中是否需要执行校准程序以达到预定检测能力并满足 5.8 的要求。

示例：在下述情况下可能需要执行校准程序：

——SRS/SRSS 的测量准确度随时间发生改变并且后续检测能力超出制造商规定限值,由此可能引起危险失效或无法正常运行；

——在投入运行期间需要在应用中调节 SRS/SRSS 以对测量准确度失效进行修正,从而达到预定的检测能力(比如确定应用中的温度,并基于此进行调节,从而减小“系统性误差”)。

如果 SRS/SRSS 提供了在运行期间的自动校准和调节功能,那么即使未能达到校准合格标准,SRS/SRSS 也不应出现危险失效。

6.3.2 校准程序和设备

制造商应：

——对用户执行的校准程序进行说明,包括：

- 应规定何时以及如何执行校准程序,
- 指明哪个设备需要执行校准;或

——提供必要的设备：

- 说明所需设备和/或 SRS/SRSS 装置的安装、配置和工作模式,
- 规定验证和/或确认措施。

注：在SRS/SRSS安装之后且开始运行之前,或者在重新安装、更换部件、定期重新校准之后,执行校准程序。

若校准程序中包含一个或多个软件程序(比如用于采集、处理和记录校准数据的计算和分析结果),则其开发过程应符合 SCS 标准。相关措施应与要求率以及规定性能等级的 SRS/SRSS 所执行

校准程序的影响相适应。

6.3.3 校准的验证和确认

制造商应规定：

——验证/确认期间的条件（比如安装位置和环境条件）；

——开始或退出校准程序的（验证/确认过程）合格标准（比如测量不确定度，工作时间等）；

——在精度超出校准合格标准时对 SRS/SRSS 进行调节；

——校准程序的误差及其在合格标准中的影响；以及

——校准程序执行期间的条件。

供应商应提供有关如何在用户侧记录校准结果的信息。若未达到校准合格标准，SRS/SRSS 也不应出现危险失效。

示例：合格标准可以是：

- 对于一个相对湿度（RH）传感器而言，校准程序的合格标准为±2%；
- 对于距离测量而言，合格标准可是测量准确度和测量不确定度的限值。

注 1：为了达到要求的合格标准，执行一次以上的验证和调节。

注 2：按照 8.5 在现场试验中执行验证。

7 工作、维护和修改阶段

SRS/SRSS 制造商应规定相应的措施，以实现下述目标：

——在工作期间实现安全相关功能；

——在维护期间验证安全相关功能；

——在修改时实现安全相关功能。

SRS/SRSS 供应商应在使用说明中提供与产品工作、维护和安装有关的信息。

8 验证和确认

8.1 通用要求

应进行验证和确认以确保 SRS/SRSS 的系统性能力。

8.2 SRS/SRSS 的验证

在设计和开发阶段，应通过分析和/或试验对 SRS/SRSS 安全要求规范中的要求进行验证。

对于 D、E 和 F 性能等级的 SRS/SRSS，其制造商应以文件形式制定验证计划，计划应包括：

——参照 SRS/SRSS 安全要求规范中的具体要求；

——详细说明在设计和开发阶段的何阶段进行了验证；

——详细说明执行验证的人员、部门或单位；

——按照 8.4 通过分析挑选验证方法；

——参照试验计划和生成的文件，按照 8.5 通过试验选择验证；

——评估验证结果时所使用的合格标准和方法。

注 1：SRS/SRSS 的验证计划能够是整个 SCS 验证和确认计划的一部分。

注 2：验证计划能够是 E/E/PES 安全计划的一部分。

可通过要求管理工具实现对 SRS/SRSS 安全要求规范中具体要求的参考，该工具应在验证计划

中提及(在适当的情况下)。

除非 SCS 功能安全所使用的标准有不同的要求,否则应采用表 7 所述方法。

表 7　用于评估验证措施和验证结果的方法

方法/验证措施	SRS/SRSS性能等级					
方法/验证措施	A	B	C	D	E	F
评估验证计划和结果	不需要	不需要	不需要	检查: ——完整性 ——是否正确实施	检查: ——完整性 ——是否正确实施	检查: ——完整性 ——是否正确实施
评估是否满足安全要求规范	检查: ——是否满足	检查: ——是否满足	检查: ——要求完整性 ——是否正确实施 ——是否满足	检查: ——要求完整性 ——是否正确实施 ——是否满足	检查: ——要求完整性 ——是否正确实施 ——是否满足	检查: ——要求完整性 ——是否正确实施 ——是否满足
评估分析过程	不需要	不需要	检查: ——方法是否正确 ——是否正确实施 ——没有危险失效条件	检查: ——方法是否正确 ——是否正确实施 ——没有危险失效条件	检查: ——方法是否正确 ——是否正确实施 ——没有危险失效条件	检查: ——方法是否正确 ——是否正确实施 ——没有危险失效条件
评估试验过程	检查: ——试验计划是否合适 ——是否完成试验	检查: ——试验计划是否合适 ——是否完成试验	检查: ——试验计划是否合适 ——是否完成试验	检查: ——试验计划是否合适 ——是否完成试验	检查: ——试验计划是否合适 ——是否完成试验	检查: ——试验计划是否合适 ——是否完成试验
评估使用说明	不需要	不需要	不需要	检查: ——完整性是否符合第8章要求	检查: ——完整性是否符合第8章要求	检查: ——完整性是否符合第8章要求

如果不满足表 7 要求,则应指定对评估结果的修正措施并附在合适的位置。

应按照表 7 要求对修正措施进行实施和再次验证。

8.3　SRS/SRSS的确认

SRS/SRSS 制造商应规定在整个生命周期内的确认措施,并考虑以下方面:

——SRS/SRSS 的正确集成(比如安装或由输出单元提供的安全相关信息);

——安全相关功能所需要的相应降低风险措施;

——不能有 SRS/SRSS 产生的无法容许的危险(比如光辐射应符合 4.2.2.2 的要求);

——符合 8.5.3 和 8.5.4 的适当试验方法和试验装置(比如用于现场试验或耐久试验);

——符合 8.4 的适当分析方法(比如检查);

——试验和分析的步骤;

——试验和分析结果文档。

制造商应将确认措施和步骤记录在案,并由供应商以适当的方式在使用说明中提供。

如果确认措施和过程导致不合规的情况,则供应商应在使用说明中提供适当的用户侧措施。

注 1:包括供应商关于不合规产品的信息。

在适当情况下,应告知用户需要对确认结果进行归档和审查。

通常只有在设计和开发阶段的后期才可能规定确认措施和程序。应核查 SRS/SRSS 确认的结果,而且有必要在应用中执行初次检查/试验。出于这些方面的考虑,本文件不要求提供与验证计划相当的确认计划。

注 2:文档分为不同的部分,分别由制造商和供应商定义。制造商文档主要说明与其行业知识有关的措施和过程。供应商可能更熟悉用户侧应用并具备这方面的专业优势。

8.4 分析

应通过分析对以下方面进行验证和确认:

——部件特性对 SRS/SRSS 检测能力的影响;

——SRS/SRSS 满足安全要求规范和本文件(比如 5.2 中规定的 SRS/SRSS 功能)的要求;

——在下述条件下对用户界面的正确集成:

- 将 SRS 集成到 SRSS 中(适当情况下),
- 将 SRS/SRSS 集成到 SCS 中(适当情况下),
- 将 SRS/SRSS 集成到机器中(适当情况下);以及

——最终用户应用中的 SRS/SRSS 性能满足制造商规定的 SRS、SRSS、SCS 和/或机器性能。

对于性能等级 C、D、E 和 F 的 SRS/SRSS 而言,应在防止出现危险失效方面进行定量分析。

在 SRS/SRSS 设计和开发期间,会在适当的抽象水平上通过安全分析进行验证。

定量分析方法可预测失效发生的频率或持续时间,而定性分析方法只能确定失效却无法预测失效频率或持续时间。

这两种分析方法都依赖于对相关故障类型和故障模型的了解。

定性分析方法包括但不限于:

——在系统、设计或过程级进行定性 FMEA;

——定性 FTA;

——通过模拟模型进行估算;

——通过检查进行分析;以及

——通过正式设计审查进行分析。

注 1:在SRS/SRSS验证期间进行检查的方法需要检测技术和检测能力可信性方面的专业知识。

定量安全分析是对定性安全分析的补充。它们用于验证表 4、表 5、公式 (1)和公式(G.1)中规定的目标值。

定量分析方法包括但不限于:

——定量 FMEA;

——定量 FTA;

——通过模拟模型进行预测,比如:

- 马尔可夫模型,
- 各可靠性模型的可靠性框图。

注 2:选用相应分析方法的另一个原则就是它们的执行方式。归纳分析方法(比如FMEA,马尔可夫建模)是从下向

上的方法，从已知条件预测未知影响。演绎分析方法（比如FTA和可靠性框图）是自上而下的方法，从已知影响开始去寻找未知原因。

8.5 试验

8.5.1 通则

应通过试验对以下方面进行验证和确认：

——部件特性对 SRS/SRSS 检测能力的影响；

——用于模拟的模型准确性（如果适用）；

——SRS/SRSS 满足安全要求规范和本文件（比如 5.2 中规定的 SRS/SRSS 功能）的要求；

——在下述条件下对用户界面的正确集成：

- 将 SRS 集成到 SRSS 中（适当情况下），
- 将 SRS/SRSS 集成到 SCS 中（适当情况下），
- 将 SRS/SRSS 集成到机器中（适当情况下）；以及

——最终用户应用中的 SRS/SRSS 性能满足制造商规定的 SRS、SRSS、SCS 和/或机器性能。

供应商应以适当的方式在使用说明中提供在用户侧执行验证性确认所需要的试验及试验装置。

注：规定SCS和/或机器涵盖在SRS/SRSS集成期间所可能产生的额外信息，这些信息与最终用户侧SRS/SRSS的最终性能有关。对SCS和/或机器供应商没有更多的要求。

8.5.2 试验类别

制造商应使用下述一项或多项内容对试验做出规定：

——型式试验（在 SRS 设计和开发期间用于对检测能力进行型式试验评估）；

——合格试验（对 SRS 中使用的部件进行合格性评估）；

——例行试验（用于对生产线上的某个部件进行 100% 的试验）；

——耐久试验（用于展示产品在预期寿命期间的耐久性）；

——实验室试验（在设计和开发期间作为模拟过程的一部分对模型的正确性进行验证）；

——维护试验（对机器进行改动之后在操作员侧对 SRSS 安全相关区的正确定位进行验证）；

——系统试验（用于验证是否将 SRS 正确集成到了一个 SRSS 中）；

——模拟试验（验证 SRS 在环境条件下的安全相关功能是否与 SRS 预定用途下的规定值一致）；

——验收试验（SRS 制造商和 SCS 集成商在规定要求上达成一致）；

——现场试验（验证在环境条件下操作员侧的安全相关功能）。

注1：型式试验由制造商或一家授权企业在取自正常生产或预生产过程的一个或多个被测件上进行，主要目的是评估产品性能是否完全取决于SRS/SRSS设计。型式试验在新开发产品或进行过重大设计修改的产品上进行。

注2：验收试验通常由制造商在客户（比如集成商）在场的情况下实施，以验证制造商提供的SRS是否满足规范中提出的各项要求。

注3：在SRS/SRSS安装完成后的运行期间，有必要在操作员处通过规定的维护试验验证检测能力完整性和/或安全相关区定位。在这种情况下，制造商应告知操作员必需的步骤和设备。维护试验通常与特定国家和应用领域的法规有关，其中规定了例如必须执行维护试验时的试验周期。

注4：如果SRS/SRSS的某个安全相关功能作为试验软件模块的一个功能块执行的话，系统试验会受到相应的影响。在使用该软件模块的SCS进行系统试验时，被测软件模块在软件集成试验期间被进行进一步验证。

注5：在操作员处的现场试验期间，比较有用的一种做法是，在试验计划中提前确定主要关注对SRS/SRSS安全相关功能的哪些影响，并以适当的方式将它们记录下来。比如，使用观测区域与现场试验中SRS/SRSS相同的带时间戳相机将雾记录下来。

8.5.3 试验方法和试验装置

SRS/SRSS 制造商应规定相关试验方法。

注1：试验方法的一个例子是在对正常运行和无危险失效能力进行光照干扰试验时，使用规定特性能够代表实验室试验期间自然光的卤钨光源。

若进行实验室试验，则试验方法宜尽可能与确认、测量可追溯性及估算测量不确定度有关的测量原理保持一致。试验设备的相关要求应尽可能在精度和校准方面保证合理可行。

注2：有关最佳实践的指导见ISO/IEC 17025。

注3：也参照其他适用文件（比如ISO/IEC Guide 98-3）。

SRS/SRSS 制造商应对试验装置做出规定并应确保以下内容尽可能合理可行：

——制造商规定的安装条件和安装支架；

——制造商规定的感应区尺寸；

——下述装置输出信息的使用：

- 检测单元，
- 处理单元，
- 输出单元；

——以可重复的方式表示安全相关物体属性；

——试验装置和所使用试验设备的可重复性。

注4：如何选择测试设备以及如何作为输入信息精准且可追溯地向SRS/SRSS被测设备（DUT）提供安全相关物体物理属性的方式是一个需要从技术和经济方面考虑的问题。比如，要想充分控制所有因素对试验结果和可重复性的影响，可能需要大量的实验设备。在实验室试验装置中使用的有些设备，可能对于某些试验（比如降雪室、造雾室等）来说可能过于昂贵。因此，应通过分析确定是否有，以及有哪些种类的实验设备对于目标传感器性能等级和规定性能（比如在雾气环境下的高低限值）是不适用的。在有些情况下，对实验室试验设备的投资对于传感器性能等级E来说可能是合理的，但是对于性能等级A来说却不尽合理。通过分析可能可以提出使用现场试验代替实验室试验来进行型式试验的不同方案。

试验装置包括代表被测设备的 SRS/SRSS 和执行试验所使用的设备。环境试验的试验方法和试验装置均应尽可能合理可行，并满足相关标准的要求[比如 IEC 60068（所有部分），IEC 61496（所有部分），IEC 60529，IEC 60947-5-2]。

在试验功能安全 EMC 时，除非有具体应用或产品相关的标准（比如 IEC 60947-5-3，IEC 61496-1 或 IEC 62061），否则所使用的试验方法和试验装置应符合 IEC 61000-6-7：2014 中相应 SIL 等级的要求。

注5：如果标准中没有提供型式试验所使用的试验装置[比如IEC 60068（所有部分）]，那么能够使用其他方法。在[2]中提供了一个示例。另一个示例是，参照安全相关传感器的产品标准[比如IEC 61496（所有部分）]的试验装置。

8.5.4 试件

SRS/SRSS 制造商在进行下述试验时应对试件做出规定：

——确定检测能力的试验；

——确定安全相关区正确位置的试验；

——在试件插入时确定相应安全相关信息的试验。

应规定的试件特性包括下述几个方面：

——SRS/SRSS 所使用的一种或多种检测技术；

——用于检测的相关物体属性（见 5.8.2）的表示；

——使用试件的试验类别（比如型式试验、例行试验还是维护试验）；以及

——SRS/SRSS 的预期应用。

在尽可能合理可行的前提下,试件应按照相关标准使用。

在用于确认 SRS/SRSS 的检测能力时,SRS/SRSS 制造商应指定试件,而且供应商应将试件属性记录在使用说明中。

注:试件仅是整个试验设备的一部分。在最终用户执行维护试验或制造商在进行型式试验时,需要特别注意。

示例:定义可以是:

- 在 IEC 61496-2 中,使用光学检测技术的 AOPD 型式试验中,试件表示成人;
- 在 EN 16580 或 IEC 61032 中,试件表示儿童。

8.5.5 试验计划和试验结果

SRS/SRSS 制造商应规定并记录试验计划,试验计划包含以下内容:

——通过试验进行验证和确认的相关内容(见 8.5.1);

——试验类别的相关内容(见 8.5.2);

——试验方法和试验装置的相关内容(见 8.5.3);

——试验步骤(包括判定试验成功或失败的标准);

——被测设备数量(比如部件、SRS、SRSS 等);以及

——被测设备的唯一标识信息(比如序列号)。

——表 6 所述措施。

注:对于某些试验方法(比如验收试验)而言,最好能确定 SRS 制造商和客户(比如将 SRS 集成到 SCS 中的集成商)都能通用的试验计划。这样能够降低未定义试验装置和设备产生不同结果的风险。

试验结果应记录在试验报告中。试验结果应标明“失败”或“成功”。

也能够使用其他措辞,但宜确保与试验无关的人员(比如对验收试验结果进行评估的集成商)轻松且明确识别试验结果。

试验结果应用于:

——通过评估显示与试验计划的一致性;以及

——安全要求规范的验证。

9 使用说明

SRS/SRSS 的使用说明应提供与安装、使用和维护有关的信息。应包括有关设备和安装的全面介绍。

注 1:使用说明归档在客户文档内。若使用说明标题为“安全手册”,则会与 IEC 61508(所有部分)中的具体要求产生混淆。

使用说明应适合供应商所规定 SRS/SRSS 用户的需要,且包括下列因素:

——应用领域;

——使用限值(SRS/SRSS 如果用在用户侧的特定应用中,则在确认过程中尤其需要使用限值);

——将两个或更多 SRS 集成到一个 SRSS 中;

——将两个或更多 SRS/SRSS 集成到一个 SCS 中。

所需要的(所有相关)使用说明包括但不限于表 8 所规定的内容。

注 2:根据供应链角色分类的使用说明见附录 B。

表 8　需要提供的使用说明概览

章节	需要提供的使用说明概览(完整内容见参考文献)
4.3	SRS/SRSS性能等级、安全性能等级(PL,SIL或SILcl)和参考标准
5.2	符合总体说明的SRSS功能(见表2)
5.5	有关感应区的信息(在适当情况下)
5.6	有关安全相关区的信息
5.7	有关自动化相关区的信息(在适当情况下)
5.8.2.1 5.8.2.2 5.8.2.3	执行SRS/SRSS功能时遵守的物理属性限值(比如长度、面积、体积、反射率、速度等用于人员检测的属性和/或用于危险物体检测的属性)
5.8.3.1 5.8.3.3 5.8.3.4	与SRSS检测能力可信性有关的环境影响(危险失效条件和正常运行条件)
5.8.3.3	相关环境条件对检测能力丧失影响的分析结果以及在应用中超出限值的后果的相关信息
5.8.3.3	如果使用了附录G中的一种其他方法,则应提供该方法的有关信息
5.9.2	有关检测单元/SRS/SRSS安装的信息
5.9.3	输出单元提供的安全相关信息(测量信息、判定信息和置信度信息等)
5.9.3.1	触发故障反应功能的信号及其故障响应时间
5.9.3.3	响应时间
6.1	有关集成和安装的信息
6.2.1	融合所使用的每个SRS的使用说明
6.2.2 6.2.3 6.2.4 6.2.5 6.2.6 6.2.7	SRSS在融合后的使用限值(检测能力、感应区、危险失效和正常运行条件下的环境条件类型和限值、安全相关信息、SRSS性能等级)
6.2.8	融合为SRSS之后的响应时间
6.3.1 6.3.2	为了达到规定的检测能力而在应用中执行的校准程序(在适当情况下)
6.3.3	用户校准的验证和确认相关的信息
第7章	关于运行、维护和修改的信息
8.5.1	对在用户处执行验证和确认所使用的试验和试验装置的说明

附 录 A
（资料性）
系统性能力的检查

对用于人员保护的安全相关控制系统而言，其功能安全标准要求对系统性能力进行检查。可使用不同的安全相关传感器标准方法（图 A.1 提供了一个示例）。在 SRS/SRSS 使用说明中宜指明并提供所用标准的列表。

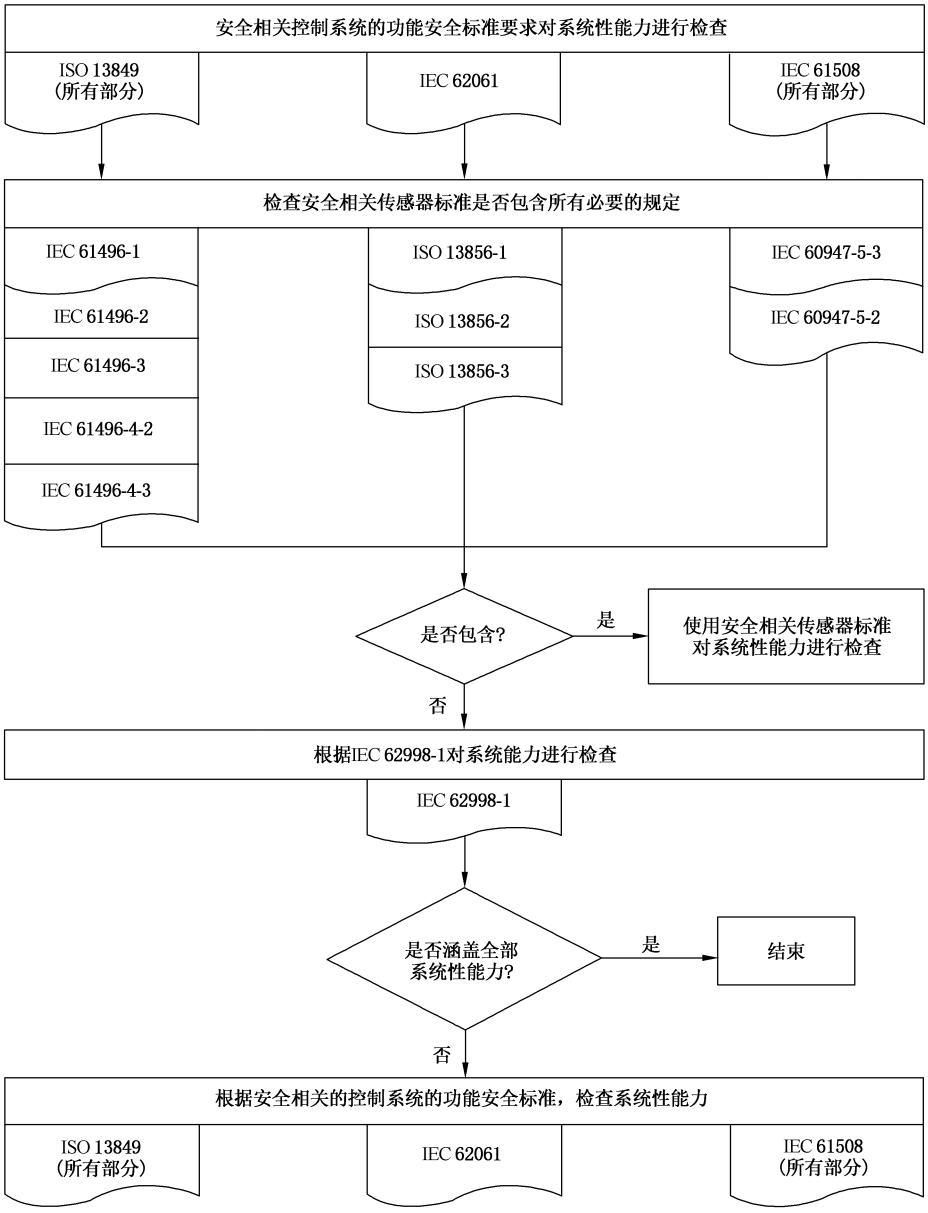


图 A.1 使用安全相关传感器标准对系统性能力进行检查的示例

另一种方法是通过组合使用安全相关传感器标准所涉及的方面以及本文件未涵盖的方面，对系统性能力进行检查。

附 录 B
（资料性）
用户类别

B.1 SRS/SRSS用户类别和本文件所涵盖的用户类别

本文件涉及不同的用户类别，包括使用本文件内容的用户类别以及将SRS/SRSS用作产品的用户类别。表B.1提供了用户类别的概览。

表B.1 各种用户类别的角色和任务

用途	SRS/SRSS制造商	将SRS集成到SRSS中的集成商	将SRS/SRSS集成到SCS中的集成商	机械制造商	最终用户
本文件内容	使用本文件内容的下述用户： ——SRS制造商；以及 ——将SRS用到SRSS或SCS中的供应商	使用本文件内容的下述用户： ——将SRS集成到SRSS中的集成商；以及 ——将SRSS集成到SCS中的供应商	未涉及	未涉及	未涉及
将SRS用作产品	负责以下内容的SRS制造商和供应商： ——执行例行试验和/或型式试验	——作为SRSS集成商的SRS用户； ——按照SRS使用说明进行操作	——作为SCS集成商的SRS用户； ——按照SRS使用说明进行操作	——作为机械制造商和供应商的SRS用户； ——按照SRS使用说明进行操作	——SRS安全相关功能的用户； ——执行维护试验； ——执行现场试验； ——按照SRS使用说明进行操作
将SRSS用作产品	负责以下内容的SRSS制造商和供应商： ——比如执行例行试验和/或型式试验	负责以下内容的SRSS集成商和供应商： ——比如按照例行试验和/或型式试验对SRSS进行系统试验	负责将SRSS集成到SCS中的集成商： ——比如按照例行试验和/或型式试验对SCS进行系统试验	作为机械制造商和供应商的SRSS用户： ——按照SRSS使用说明进行操作	SRSS安全相关功能的用户： ——执行维护试验； ——执行现场试验； ——按照SRSS使用说明进行操作

注1：表中第一行列出了所涉及的用户类别。一个组织可能涵盖不同的用户类别。比如，传感器制造商可能是集成商，机器制造商可能是集成商，一个可编程逻辑控制器的制造商也可能是集成商。
注2：表中第一列显示了所涉及用户类别最关心的内容。
注3：表中其他单元列出了所涉及用户类别的相应角色和任务示例。

B.2 融合所涉及的用户类别

融合的理论定义（见3.5.3）导致了一个结果，那就是每个集成步骤（从检测单元直到整个机器）、它

们在装置内的相互连接以及对应执行的逻辑功能,都是一种融合行为。

本文件将“融合”的特定用户类别限定为涉及两个或更多 SRS 的 SRSS 集成(见表 B.2 中序号 5)。表 B.2 基于所使用的元件、所执行的功能以及其他判定条件等方面的区别,列出了本文件所涉及的不同的集成类型和相应用户类别。

表 B.2 (使用检测单元、SRS/SRSS 元件或 SRS 子系统的)不同集成类型所涉及的用户类别

序号	集成类型	本文件涉及的用户类别	本文件涵盖的元件/子系统	集成之后所执行的功能	判定依据
1	将一个或更多检测单元集成到SRS中	SRS制造商	检测单元、处理单元以及提供安全相关信息的输入/输出单元	表 2 所述的 SRS 功能	符合本文件讨论范畴。 本文件内容的复杂性要求具备使用某种检测技术的专业技能
2	将一个或更多检测单元直接集成到 SRSS 中,或者将检测单元与 SRS 的组合集成到 SRSS中	未涉及	—	—	检测单元所提供的组合检测功能要求对检测技术具有深入的了解。 在考虑将 SRS 集成到 SRSS 之前,有必要了解SRS的内部原理
3	将一个或更多检测单元集成到SCS中	未涉及	—	—	整体安全功能和提供安全相关信息的检测单元所需要的专业技能存在很大的不同。 本文件不考虑且未涵盖该部分内容
4	将一个 SRS 集成到SRSS中	未涉及	—	—	未预见到有实际用途。 仍然是一个SRS。由SRS制造商负责(见序号1)
5	将两个或更多 SRS 集成到 SRSS中	将SRS集成到SRSS 中的集成商	处理单元 提供安全相关信息的输入/输出单元 根据安全相关信息执行的逻辑功能 作为子系统执行SRS功能(参见表2)的SRS	在SRSS内部执行逻辑功能(见图C.2)的SRSS功能(见表2)	符合本文件讨论范畴。 参照6.2的要求。 本文件内容关于将 SRS 融合到 SRSS中的复杂度仅要求具备有限的使用检测技术的专业技能
6	将两个或更多 SRS 集成到 SRSS中	SRSS制造商	检测单元 处理单元 提供安全相关信息的输入/输出单元 根据安全相关信息执行的逻辑功能 作为子系统执行SRS功能(见表2)的SRS	在 SRSS 内部执行逻辑功能(见图C.2)的 SRSS 功能(见表2)	符合本文件讨论范畴。 本文件内容的复杂性要求具备使用不同传感器技术的专业技能

表 B.2 （使用检测单元、SRS/SRSS 元件或 SRS 子系统的）不同集成类型所涉及的用户类别（续）

序号	集成类型	本文件涉及的用户类别	本文件涵盖的元件/子系统	集成之后所执行的功能	判定依据
7	将两个或更多SRSS集成到SRSS中	未涉及	—	—	未预见到有实际用途。 对于这种类型的集成而言，所必需的SRS应直接合并到最终SRSS中（由将SRS集成到SRSS中的集成商负责），或者完全由SRSS制造商处理
8	将一个或更多SRS与一个或更多SRSS的组合集成到SRSS中	未涉及	—	—	通常认为，此类组合方式遗漏相关影响的风险过高。 对于这种类型的集成而言，所必需的SRS应直接合并到最终SRSS中（由将SRS集成到SRSS中的集成商负责），或者完全由SRSS制造商处理

附 录 C
（资料性）
功能分解和/或整合

SRS/SRSS 功能包括 5.2 部分的安全相关功能和可选的自动化相关功能。安全相关功能的基础是人、人体部位和/或危险物体的物理属性，如图 C.1 所示。

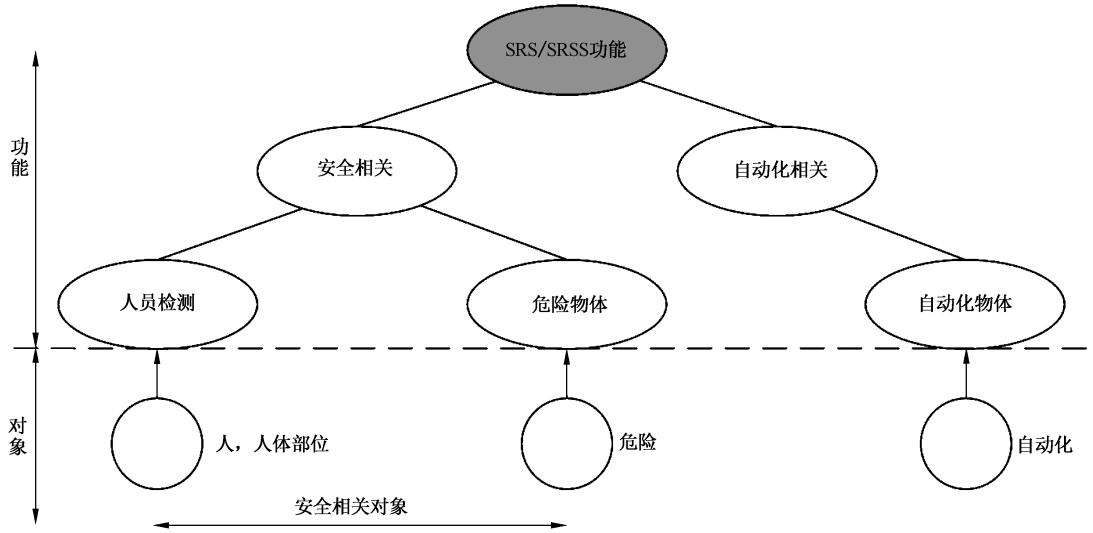


图 C.1 功能和物体之间的相互联系

一个 SRS/SRSS 的安全相关功能可能会用于执行 SCS 中的安全功能（作为子系统的子功能见 IEC 62061）。图 C.2 提供了采用图 4 所示结构执行安全相关功能以及将它们集成到 SRSS 中的一个示例。

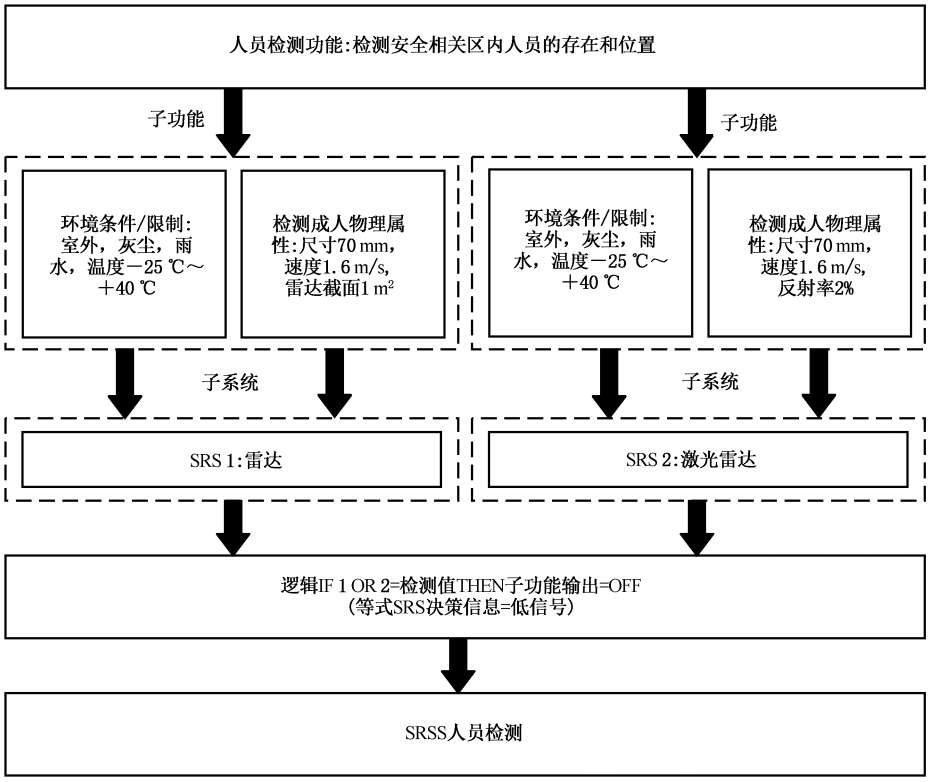


图 C.2　在 SRSS 中执行的功能示例

附 录 D
（规范性）
模拟模型的生成和应用

D.1 概述

附录 D 提供了关于模拟模型生成和应用的说明，这些模型主要用于：
——包含模拟过程的设计分析（见 5.4）；或者
——代替或补充物理试验装置的使用限值验证（如 8.5 所述）。

D.2 使用建议

制造商应确定 SRS/SRSS 的复杂度。如果满足以下条件，则可将 SRS/SRSS 定义为低复杂度：
——可完全确定系统性条件下的特性；以及
——采用断电关停原理。
在低复杂度情况下，表 D.1 适用，而在所有其他情况下，表 D.2（针对高复杂度情况）适用。

D.3 模拟目标及实现措施

如果 5.4 强制要求使用模拟，则相应的目标和措施（用于检测和避免安全相关失效）应参照表 D.1（低复杂度）或表 D.2（高复杂度）。

表 D.1 低复杂度 SRS/SRSS 的模拟目标与措施

相应传感器性能等级的措施/目标	D	E	F
使用模拟的目的			
为设计和开发提供支持	建议	建议	非常建议
对影响和失效进行后果分析	建议	非常建议	非常建议
对 SRS/SRSS 的性能进行确认	建议	非常建议	非常建议
前提、限制和接近条件对模拟结果的影响分析	非常建议	非常建议	非常建议
数值精度和误差对模拟结果的影响分析	建议	建议	非常建议
模拟子部件的分解和分别验证	建议	建议	建议
使用历史悠久且口碑极佳的计算机辅助设计工具	建议	建议	建议
按照 GB 28526—2012，6.11.3.1 和 6.11.3.4 要求开发模拟模型	—	—	建议
对基准试验结果和模拟输出进行定量对比（包括边界数据和灵敏度分析）	—	建议	非常建议
对基准试验结果和模拟输出进行定性对比（包括趋势、总体特性）	建议	—	—
部件级建模（包括边界数据）	—	—	建议
模块级建模（包括外设的边界数据）	建议	建议	—

表 D.1　低复杂度 SRS/SRSS 的模拟目标与措施（续）

相应传感器性能等级的措施/目标	D	E	F
已验证的子部件模型和已知交互特性的综合建模	建议	建议	建议
说明： 在SRS/SRSS设计/开发和确认过程中没有关于使用模拟的相关建议。 建议：建议在该性能等级传感器的设计/开发和确认过程中使用模拟。如果不适合使用模拟模型对SRS/SRSS的系统性行为进行分析，而试验能够提供系统性能力方面的足够理解，那么可忽略模拟。 非常建议：非常建议在该性能等级传感器的设计/开发和确认过程中使用模拟。如果没有使用模拟，那么应详细说明合理的原因。			

表 D.2　高复杂度 SRS/SRSS 的模拟目标与措施

相应传感器性能等级的措施/目标	D	E	F
使用模拟的目的			
为设计和开发提供支持	建议	非常建议	非常建议
对影响和失效进行后果分析	非常建议	非常建议	非常建议
对SRS/SRSS的性能进行确认	非常建议	非常建议	非常建议
前提、限制和接近条件对模拟结果的影响分析	非常建议	非常建议	非常建议
数值精度和误差对模拟结果的影响分析	建议	非常建议	非常建议
模拟子部件的分解和分别验证	建议	建议	建议
使用历史悠久且口碑极佳的计算机辅助设计工具	建议	建议	建议
按照GB 28526—2012中6.11.3.1和6.11.3.4要求开发模拟模型	—	建议	建议
对基准试验结果和模拟输出进行定量对比（包括边界数据和灵敏度分析）	建议	非常建议	非常建议
对基准试验结果和模拟输出进行定性对比（包括趋势、总体特性）	—	—	—
部件级建模（包括边界数据）	—	建议	建议
模块级建模（包括外设的边界数据）	建议	—	—
已验证的子部件模型和已知交互特性的综合建模	建议	建议	建议
说明： 在SRS/SRSS设计/开发和确认过程中没有对于使用模拟的相关建议。 建议：建议在该性能等级传感器的设计/开发和确认过程中使用模拟。如果不适合使用模拟模型对SRS/SRSS的系统性行为进行分析，而试验能够提供系统性能力方面的足够理解，那么可忽略模拟。 “非常建议”：非常建议在该性能等级传感器的设计/开发和确认过程中使用模拟。如果没有使用模拟，那么应详细说明合理的原因。			

D.4　验证

应对用于设计或确认的模拟进行验证（见图 D.1）。

验证方法应至少能够发现导致错误或误差的以下原因：

——错误或不精确的输入数据；

——错误或不精确的模拟模型；

——错误或不精确的模拟工具。

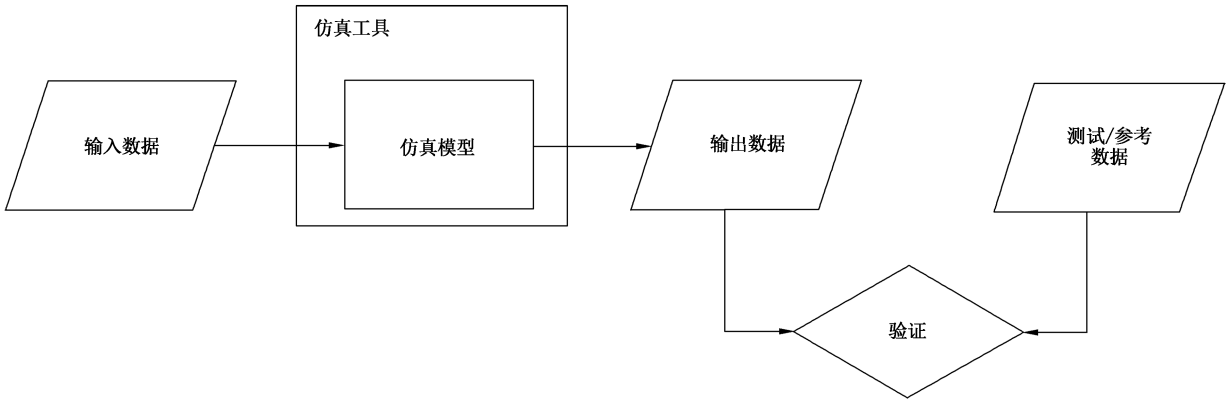


图 D.1　验证流程

应将模拟结果和专用基准试验的实验/试验结果进行比较，以对模拟进行详细验证。

用作真实数据的基准应：

——包含模拟模型有关的所有系统部件；

——在使用模拟对定量特性进行建模的条件下，允许进行定量比较；

——代表某种与安全功能相关的状况（比如关键失效或限制情形）。

比较应包含以下几个方面：

——定性和定量特征；

——预测精度；

——关键参数的灵敏度。

对模拟模型进行验证的其他方法包括：

——对模拟模型和模型输入数据进行走查式检查；

——对不同来源的输入数据进行比较；

——对子模块进行具体的试验和验证；

——检查测量数据的统计分布是否可由随机模拟（比如蒙特卡洛模拟）重现；

——将模拟结果与其他模拟模型所产生的结果进行比较。

对模拟工具进行确认的其他方法包括[见 GB 28526—2012 中 6.4.1.2 b)]：

——具体试验；

——对它们在特定安全相关系统上的输出进行单独确认；

——工具配置和相关经验的文档。

附 录 E
（资料性）
儿童属性和行为

E.1 概述

根据 ISO/IEC Guide 50,14 岁以下的人被定义为儿童。

根据特定年龄儿童的发展,儿童在运动策略(包括爬行、步行、跑步等)或探索策略(包括对潜在风险的认识以及从风险中学习)中的行为特征与成年人不同。

表示儿童身体或身体部位的尺寸如 E.2 所述。

如果试件代表儿童或其身体部位,亦可见 8.5.4。试件尺寸并不一定要与 E.2 列出的身体部位尺寸相等。检测技术的具体应用或限值可能也需要考虑。

E.2 身体部位的尺寸

表 E.1～表 E.4 以及图 E.1～图 E.4 提供了一些儿童身体部位尺寸的示例。它们都基于日本和美国的人体测量数据。表中使用了从这些数据得出的男性和女性的最小或最大值,并列出了最具代表性的限制数值。在可行的情况下,建议使用来自日本的最新数据。否则,也可使用中国和美国的数据。

注 1:日本和美国数据的更多详情可参见参考文献[81]和[82]。

注 2:中国儿童身高和胸深数据详见 GB/T 26158—2010。

注 3:中国儿童头宽和头长数据详见 GB/T 26160—2010。

表 E.1 儿童身高

年龄	5% 值 mm		50% 值 mm		95% 值 mm	
	美国	日本	美国	日本	美国	日本
1	686	712	725	779	785	849
2	796	812	841	874	904	918
3	869	890	932	960	994	1 029
4	928	960	994	1 015	1 065	1 098
5	989	1 020	1 070	1 076	1 150	1 164
6	1 044	1 081	1 136	1 158	1 205	1 231
7	1 104	1 134	1 198	1 206	1 271	1 274
8	1 144	1 198	1 246	1 286	1 335	1 351
9	1 210	1 130	1 299	1 299	1 399	1 421
10	1 249	1 289	1 347	1 376	1 453	1 519
11	1 318		1 408		1 511	
12	1 353		1 465		1 575	
13	1 400		1 522		1 643	

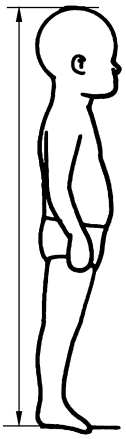


图 E.1　儿童身高

表 E.2　儿童胸深

年龄	5%值 mm		50%值 mm		95%值 mm	
	美国	日本	美国	日本	美国	日本
1	89	96	110	113	118	128
2	98	105	116	113	126	128
3	103	110	119	121	135	131
4	108	112	123	124	138	137
5	110	112	128	126	147	139
6	116	113	133	131	151	144
7	121	122	137	135	156	148
8	118	129	138	137	164	153
9	126	122	144	145	171	153
10	125	133	146	151	175	172
11	134	—	157	—	197	—
12	141	—	161	—	195	—
13	153	—	171	—	221	—

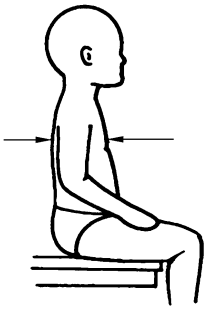


图 E.2　儿童胸深

表 E.3　儿童头宽

年龄	5%值 mm		50%值 mm		95%值 mm	
	美国	日本	美国	日本	美国	日本
1	115	125	124	133	131	146
2	124	126	131	136	140	147
3	126	131	133	140	141	152
4	128	132	136	142	144	153
5	129	134	137	144	146	154
6	131	136	138	145	147	156
7	131	136	140	144	149	155
8	133	138	140	148	149	158
9	134	138	142	146	150	157
10	134	135	142	149	151	160
11	136	—	143	—	152	—
12	136	—	144	—	154	—
13	137	—	145	—	153	—

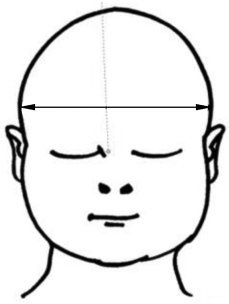


图 E.3　儿童头宽

表 E.4　儿童头长

年龄	5%值 mm		50%值 mm		95%值 mm	
	美国	日本	美国	日本	美国	日本
1	149	146	161	156	168	171
2	160	153	172	162	184	174
3	165	155	175	165	185	178
4	167	158	178	168	189	178
5	169	157	179	168	192	178
6	173	162	182	172	194	183

表 E.4　儿童头长(续)

年龄	5%值 mm		50%值 mm		95%值 mm	
	美国	日本	美国	日本	美国	日本
7	171	161	181	172	193	181
8	170	164	183	172	195	181
9	172	161	185	176	197	185
10	173	164	185	176	196	186
11	174	—	186	—	198	—
12	171	—	186	—	197	—
13	173	—	189	—	198	—

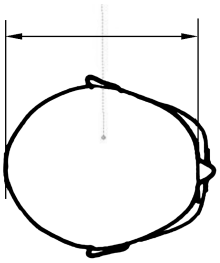


图 E.4　儿童头长

附 录 F
（资料性）
环境影响

F.1 概述

附录 F 针对如何应用 5.8.3.2 所述环境影响提供了一些示例。

F.2 环境影响应用示例 1

一个基于光学传感器的 SRS/SRSS 为工业现场自动驾驶电动车的防撞功能提供安全相关信息。车辆需要在不同的制造设施之间运行并且需要穿越没有遮挡的室外区域。SRS/SRSS 位于车辆外面（无法避免降水影响）。

通过分析已经确定了对于 SRS/SRSS 有以下环境影响：

——温度和湿度；

——雾；

——降水（雨、雪和冰雹）；

——太阳辐射；

——凝结和结冰；

——粉尘和沙土；

——动物；

——振动和冲击；

——电和电磁影响。

5.8.3.2 未列出的环境影响因素在该特定示例中无关，因此已被忽略。

IEC 60721（所有部分）中的相关内容包括 IEC 60721-3-0（简介）和 IEC 60721-3-5（地面车辆装置）。

在 IEC 60721-3-5 中，所提供的限值均为发生概率极低的极端情况。环境影响很难达到规定限值，而且只会在很短时间内达到限值。简单起见，本例忽略了储存条件。

与检测能力有关的各类环境影响以及具体应用的改动如表 F.1 所述。

表 F.1 符合 IEC 60721-3-5 的环境影响和等级示例 1

环境影响	符合 IEC 60721-3-5 的等级	限值	限值改动	备注
温度	5K3	−40 ℃～+40 ℃		达到下限的时间大约为每年 10 h。达到上限的时间大约为每年 5 h（见 IEC 60721-2-1）
温度变化率	5K3	5 K/min		从室内到室外（反之亦然）可能会导致更大的变化率
相对湿度	5K3	95%		
降雨	5K3	6 mm/min		极端降雨每年可能只会出现几分钟
降雪	—	适当考虑		IEC 60721（所有部分）没有规定数字限值

表 F.1　符合 IEC 60721-3-5 的环境影响和等级示例 1（续）

环境影响	符合 IEC 60721-3-5 的等级	限值	限值改动	备注
雾	—	适当考虑		IEC 60721(所有部分)没有规定数字限值
结冰		适当考虑		IEC 60721(所有部分)没有规定数字限值
太阳辐射		1 120 W/m^2	700 W/m^2	尽量使用遮蓬以防止太阳光直射
动物	5B2	适当考虑昆虫,长霉		
振动(正弦波)幅值/加速度谱密度	5M2	3.3 mm(频率2 Hz～9 Hz) 10 m/s^2(9 Hz～200 Hz) 15 m/s^3(200 Hz～500 Hz)		在行驶在平坦光滑地面上的电动车上运行
振动(宽带)幅值/加速度谱密度	5M2	1 m^2/s^3(10 Hz～200 Hz) 0.3 m^2/s^3(200 Hz～500 Hz)		在行驶在平坦光滑地面上的电动车上运行
冲击(峰值加速度)	5M2	100 m/s^2		Ⅰ类
冲击(峰值加速度)	5M2	300 m/s^2		Ⅱ类
沙土 粉尘	5S2	0.1 g/m^3 3.0 mg/(m^2·h)		

IEC 60721-3-5 中的等级有:5K3/5B2/5S2/5M2。

IEC 60721-3-5 并未规定关于雾的具体条件。如果雾对 SRS/SRSS 有关键影响,依据其他信息源(比如天气档案)规定限值。

由于车辆处于运动过程中,因此考虑喷溅水的影响。

可以预见的是,当进入或离开室内环境时,温度和湿度会快速变化,从而可能引起 SRS/SRSS 上出现凝结。因此考虑凝结对检测能力可信性的影响。

F.3　环境影响应用示例 2

一个基于固定摄像头的 SRS/SRSS 被用于监控一栋工厂建筑的半遮蔽门口区域。SRS/SRSS 和感应区都暴露在室外天气条件下,但是不受降水和日光的直接影响。

通过分析已经确定了对于 SRS/SRSS 有以下环境影响:

——温度和湿度;

——雾;

——凝结和结冰;

——间接的太阳辐射;

——粉尘和沙土;

——振动和冲击;

——电和电磁影响。

5.8.3.2 未列出的环境影响因素在该特定示例中无关,因此已被忽略。

IEC 60721(所有部分)的相关内容包括 IEC 60721-3-0(前言)和 IEC 60721-3-3(在有天气防护措施的位置的固定使用)。简单起见,本例忽略了储存条件。

与检测能力有关的各类环境影响以及具体应用的改动如表 F.2 所述。

表 F.2　符合 IEC 60721-3-3 的环境影响和等级示例 2

环境影响	符合 IEC 60721-3-3 的等级	限值	限值改动	备注
温度	3K6	－25 ℃～＋55 ℃		
温度变化率	3K6	0.5 K/min		
相对湿度	3K6	100%		
凝结	3K6	有可能		
太阳辐射		700 W /m^2		
振动(正弦波)幅值/加速度	3M1	0.3 mm(2 Hz～9 Hz) 1 m/s^2(9 Hz～200 Hz)		
冲击(峰值加速度)	3M1	40 m/s^2		L类

IEC 60721-3-3 中的等级有:3K6/3M1。

附 录 G
（资料性）
导致SRS/SRSS安全相关功能丧失的故障、失效和影响

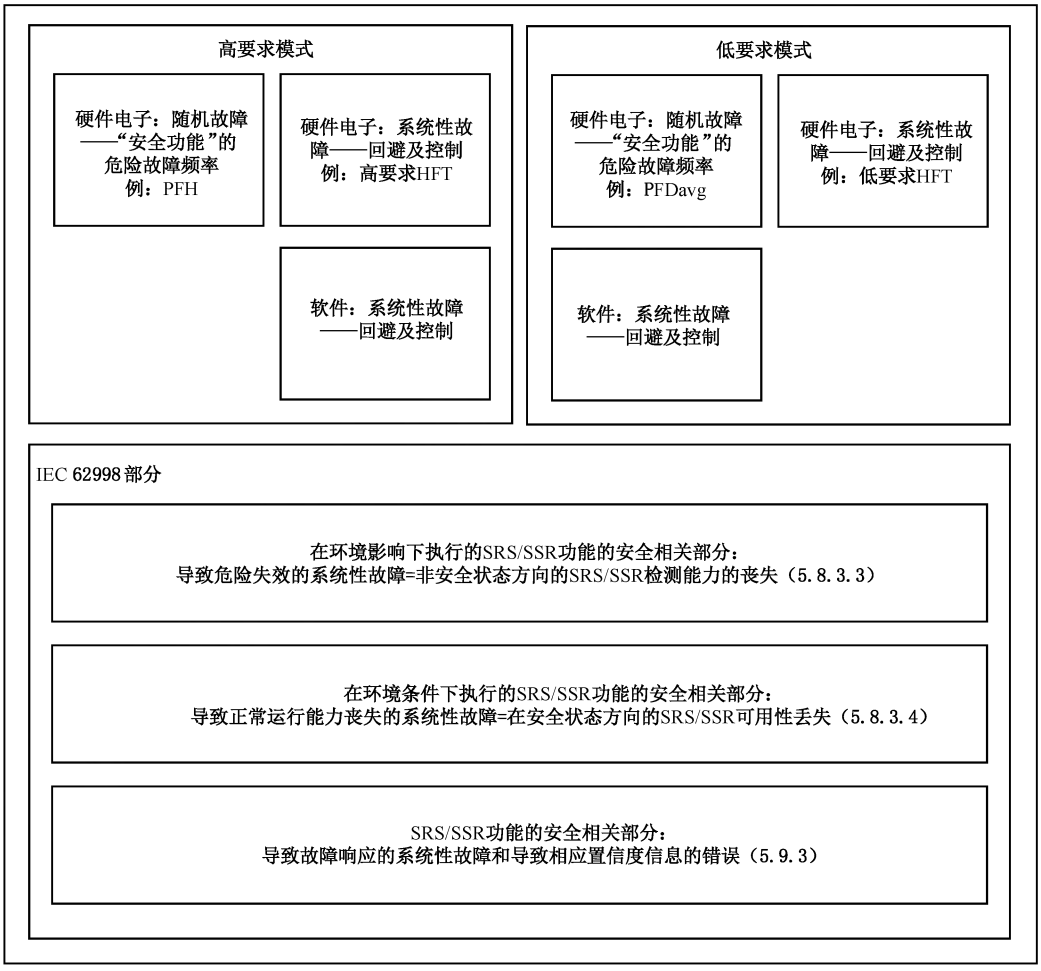
G.1 概述

附录G介绍了无危险失效要求(见5.8.3.3)和SCS及最终安全相关系统所规定故障和/或失效之间的关系。

SRS/SRSS中硬件电路、软件和系统性能力的故障与失效要作为各独立部分综合起来考虑(图G.1所示)。

累计危险失效时长(见表3)并未考虑可由PFH值(每小时危险失效平均频率)表示其特性的随机硬件电路故障。

注：PFH值适用于随机故障，且仅在对与SRS/SRSS系统性能力相关的系统性故障进行限值量化时用作参考。



图G.1 因丧失或绕过安全功能而导致额外风险的故障、失效或错误组合

本文件主要关注：

——导致检测能力危险失效的系统性故障；

——导致正常运行能力丧失的系统性故障；

——输出单元触发故障反应功能的相应信号；以及

——导致输出单元产生相应置信度信息的错误。

本文件对因检测能力丧失而引发系统性故障并进而导致危险失效或正常运行能力丧失的完整分

析流程如图 G.2 所示。

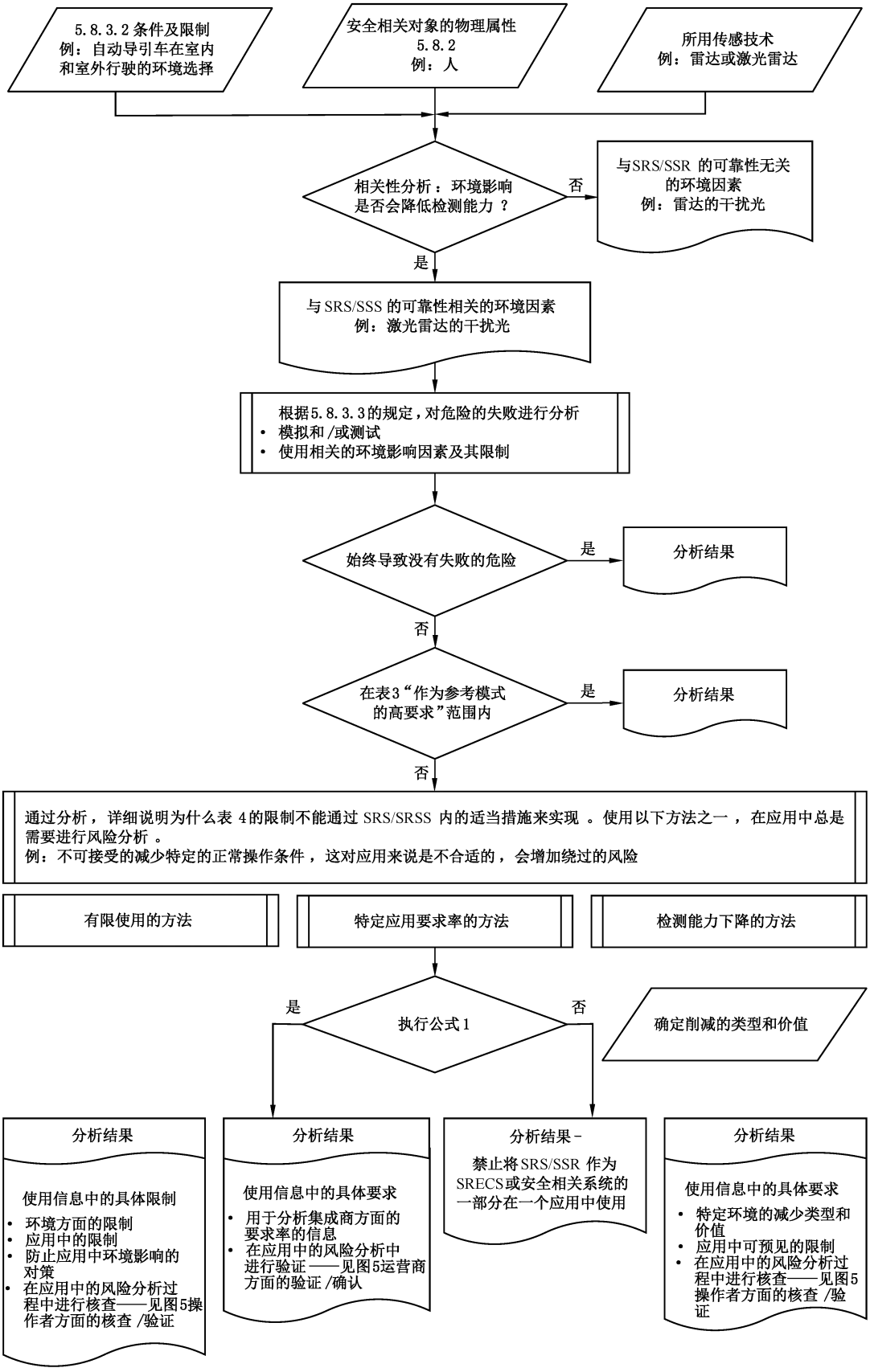


图 G.2　在设计和开发阶段防止因危险失效而导致系统性故障的系统性能力分析

如图 G.2 所示,其中提供了一个对应 SRS/SRSS 具体应用要求率的选项。在表 4(危险失效分析)中,高要求率仍是首要的定义基准。

G.2 危险失效

按照 5.8.3.3 的要求进行控制设计期间的会造成因 SRS/SRSS 安全相关功能检测能力丧失而导致危险失效系统性故障(见 5.8.3.2 对相关环境类型的规定限值要求)。

表 G.2 是表 G.1 的缩减版,与表 4 相当。表 G.2 提供了累计失效时间,关注的是硬件电路中危险失效的频率限值。

注:本文件首次对安全相关传感器规定了控制和规避会导致危险失效的系统性故障的量化限值。能预见的是,在有些应用中可能无法达到这些限值要求,因此就需要如图G.2所述的其他方案。

表 G.1 表 G.2 数值计算所使用的要求率

要求率		1/24 h		1/h		4/h		10/h		60/h	
SRS/SRSS 等级	年/年[a]	PFH	PL	PFH	PL	PFH	PL	PFH	PL	PFH	PL
A	1.1×10^{-4}	4.8×10^{-6}	b	1.1×10^{-4}	无	4.6×10^{-4}	无	1.1×10^{-3}	无	6.8×10^{-3}	无
B	9.5×10^{-6}	4.0×10^{-7}	d	9.5×10^{-6}	b	3.8×10^{-5}	a	9.5×10^{-5}	a	5.7×10^{-4}	无
C	1.9×10^{-6}	7.9×10^{-8}	e	1.9×10^{-6}	c	7.6×10^{-6}	b	1.9×10^{-5}	a	1.1×10^{-4}	无
D	1.6×10^{-7}	6.6×10^{-9}	e	1.6×10^{-7}	d	6.3×10^{-7}	d	1.6×10^{-6}	c	9.5×10^{-6}	b
E	1.6×10^{-8}	6.6×10^{-10}	e	1.6×10^{-8}	e	6.3×10^{-8}	e	1.6×10^{-7}	d	9,5E-07	d
[a] 表示一年内危险失效的最大累计时长。											
不相关						ISO 13849-1所述条件被用作表G.2的基准						

表 G.2 高要求率条件下因环境影响所导致的危险失效(检测能力丧失)限值

SRS/SRSS性能等级	一年内危险失效的最大累计时长
A	1 h
B	5 min
C	1 min
D	5 s
E	0.5 s
F	响应时间

如有证据显示表 G.2 中的限值不适用,那么也可使用图 G.2 所示的其他方法。若要使用这些方法,则制造商和供应商要以适当的方式提醒用户和/或集成商特别注意。

如果要使用针对应用中特殊要求率的方法,则使用公式(G.1)。

$$A<\frac{L\times H}{D} \qquad \cdots\cdots(G.1)$$

式中:

A——累计危险失效时长,单位为小时每年(h/年);

L——相应 SRS/SRSS 性能等级的 PFH 上限,单位为次每小时(次/h);

H——8 760，单位为小时每年(h/年)；

D——应用中的特殊要求率，单位为次每小时(次/h)。

注1：SRS/SRSS性能等级PFH上限主要关注硬件电路中危险失效的频率限值(见表G.1)。

注2：如果SRS/SRSS安全相关功能的要求率高于每年一次，则使用公式(G.1)。

对于特殊要求率的应用来说，如果要求率低于每年一次，则建议使用 1/8 760=1.142E^{-4} 的恒定值。

G.3 正常运行

SRS/SRSS 可用性下降(比如因环境影响导致的可用性下降)会增加对绕过安全相关功能的刺激。因此，要满足 5.8.3.4 所述的相关要求。

G.4 作为安全相关信息一部分的触发故障反应功能和置信度信息的信号

SRS/SRSS 内会导致安全相关信息危险失效的系统性故障需引发输出单元会触发故障反应功能的信号。

详细的要求和措施(比如用于避免硬件电路或软件的故障)要符合有关对 PL、SIL 或 SILcl 的要求(见表 1)。

触发故障反应功能的信号可能是判定或置信度信息的一个元素，但是不宜等于表示正常运行条件的测量或判定信息。如图 G.3 所示，触发故障反应功能的信号可能是置信度信息的一部分。

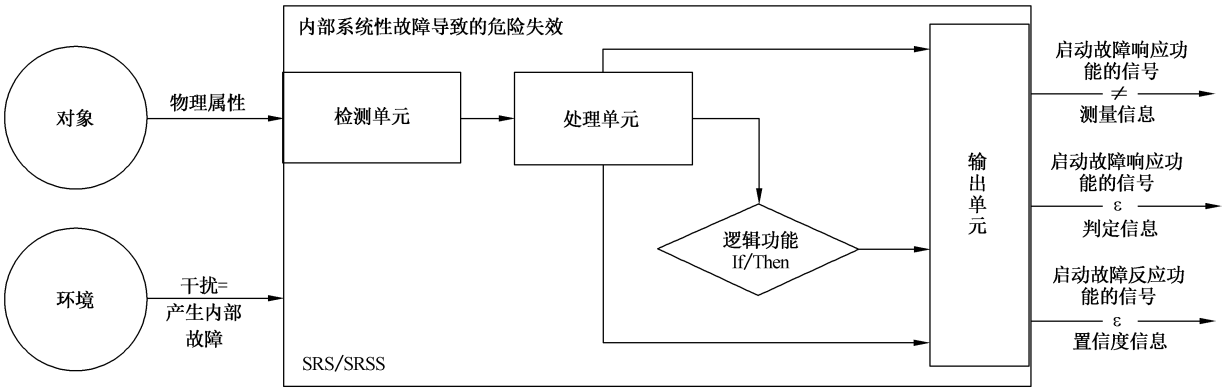


图 G.3 针对导致故障反应功能的系统性故障的应对方式

错误与故障不同，它们最终都会因为环境影响和 SRS/SRSS 内在缺陷而发生(见图 G.4)。

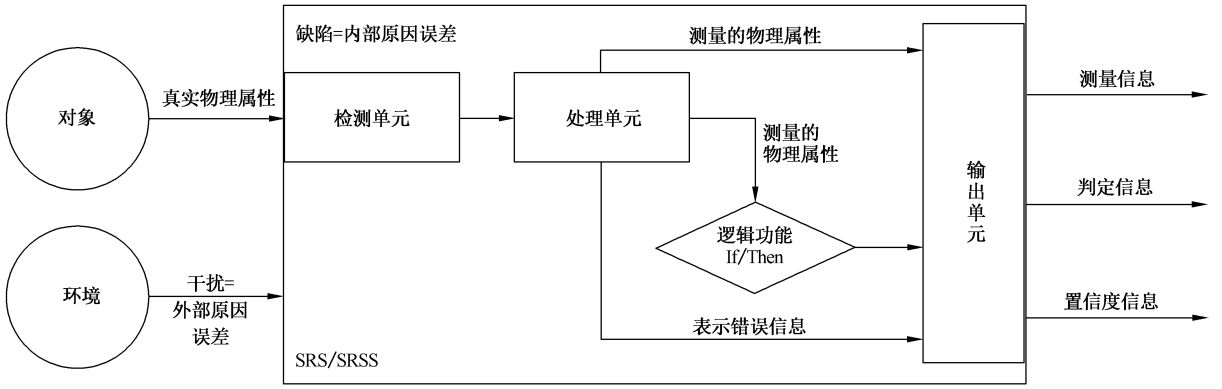


图 G.4 针对产生相关置信度信息的错误的应对方式

使用下述错误来指定置信度信息：

——(物理属性)测量值与实际值之间的误差;
——造成测量不确定度的错误;
——降低判定信息判定概率的错误。
置信度信息要符合 5.9.3.2 所述规定。

附 录 H
（资料性）
试验因素

H.1 概述

为了进行设计验证以及对 SRS/SRSS 安全相关功能进行确认，可能需要进行相应的试验。与典型的产品标准相比，本文件并不提供预定的试验装置或固定的试验方法。本文件仅针对如何定义试验装置和方法提供指导。这些都由制造商指定（见 8.5.3）。

试验需要建立在安全要求规范所规定的要求基础上。它包括被预定用途和被测物体所限定的环境要求。此外，在设计和开发期间的分析（比如 FMEA 结果）也会导致额外的必须进行的试验。

H.2 提供了一个制造商指定的机械影响试验的案例。

H.2 机械影响试验

在 SRS/SRSS 安全相关功能要求物体或执行机构与检测单元接触的任何地方，都需要确认传感器及其功能对机械影响的鲁棒性。

注：比如，对于所使用的压敏SRS来说，下述静态载荷就是相关的机械影响。

一种静态载荷试验方法和试验装置就是使用一个接触面积（尺寸、形状）与设想被测物体类似但质量为其最大质量的两倍的试件进行。

在试验过程中，试件先与检测元件接触 8 h 以试验其是否能正常运行。在此期间，传感器应继续检测物体并产生相关的输出。8 h 后，将被测物体移除，传感器在 2 min 内恢复原始状态并检测到被测物体已经移除。

另一种静态载荷试验方法和试验装置所使用的试件和设想被测物体相比，具有类似的接触面积尺寸和形状，质量在后者的最小和最大质量之间。

在试验过程中，试件先与检测元件接触 8 h 以试验其是否能正常运行。在此期间，传感器继续检测物体并产生相关的输出。8 h 后，将被测物体移除，传感器 2 min 内恢复原始状态并检测到被测物体已经移除。

最后一种静态载荷试验方法和试验装置是让一个人来作为设想的被测物体。

在试验过程中，这个人先与检测元件接触以试验其是否能正常运行，并无特定时间要求。人走开后，传感器在 2 min 内恢复原始状态并检测到人已经离开。

表 H.1 提供了 8.5.5 对机械影响试验所要求的试验计划和试验结果示例。

表 H.1　机械影响试验的试验计划和试验结果示例

试验要求	试验类别	试验方法/试验装置	试验步骤	设备数量/设备标识	试验结果
根据安全要求规范检测最大质量120 kg的物体	作为实验室试验进行的型式试验	SRS中心点施加固定载荷时的正常运行条件试验 将SRS安装在平整混凝土表面(代表工业车间) 执行时的天气条件 −25 ℃及90% 相对湿度 试件质量：120 kg +5 kg 试件平面面积： (15±2) cm×（30±2)cm;其他试件尺寸不受控制	a) 接通SRS电源。 b) SRS保持在开通(ON)状态。 c) 将一个试件置于SRS中心平面处。 d) 在响应时间内SRS输出单元变为关闭(OFF)状态。 e) 将试件留在中心处8 h。 f) SRS输出单元保持在关闭(OFF)状态。 g) 移除试件。 h) SRS输出单元在2 min内变为开通(ON)状态	首批连续生产产品中的3个SRS	若所有设备均通过试验，则试验成功
				序列号10001	设备通过
				序列号10002	设备通过
				序列号10003	设备通过
					试验成功
根据安全要求规范检测最小质量25 kg的物体	作为实验室试验进行的型式试验	SRS中心点施加固定载荷时的正常运行条件试验 将SRS安装在平整混凝土表面(代表工业车间) 执行时的天气条件 −25 ℃及90% 相对湿度 试件质量： 25 kg (−5 kg) 试件平面面积： 15 cm(+/−2 cm)×30 cm(+/−2 cm)；其他试件尺寸不受控制	a) 接通SRS电源。 b) SRS保持在开通(ON)状态。 c) 将一个试件置于SRS中心平面处。 d) 在响应时间内SRS输出单元变为关闭(OFF)状态。 e) 将试件留在中心处8 h。 f) SRS输出单元保持在关闭(OFF)状态。 g) 移除试件。 h) SRS输出单元在2 min内变为开通(ON)状态	首批连续生产产品中的3个SRS	若所有设备均通过试验，则试验成功
				序列号10001	设备通过
				序列号10002	设备通过
				序列号10003	设备未通过
					试验失败

表 H.1　机械影响试验的试验计划和试验结果示例(续)

试验要求	试验类别	试验方法/试验装置	试验步骤	设备数量/设备标识	试验结果
安全要求规范所规定SRS安全相关功能的20年任务时间	作为实验室试验进行的耐久性试验	SRS中心点施加固定过载时的正常运行条件试验 将SRS安装在平整混凝土表面(代表工业车间) 执行时的天气条件 −25 ℃及90%相对湿度 试件质量: 240 kg+5 kg 试件平面面积: (15±2) cm×(30±2)cm;其他试件尺寸不受控制	a) 接通SRS电源。 b) SRS保持在开通(ON)状态。 c) 将一个试件置于SRS中心平面处。 d) 在响应时间内SRS输出单元变为关闭(OFF)状态。 e) 将试件留在中心处8 h。 f) SRS输出单元保持在关闭(OFF)状态。 g) 移除试件。 h) SRS输出单元在2 min内变为开通(ON)状态。 i) 检查是否有任何机械损伤	首批连续生产产品中的1个SRS	若所有设备均通过试验,则试验成功
				序列号1004	设备通过,试验成功
安全要求规范所规定SRS安全相关功能的20年任务时间	作为现场试验进行的维护试验	中心点施加静态载荷条件下的无危险失效试验 按照具体应用要求安装SRS。 具体应用的现场环境因素。 执行检查的人员(检察员)代表试件 试验频率为至少每年一次	a) 接通SRS电源。 b) SRS保持在开通(ON)状态。 c) 检察员站在SRS中心处。 d) SRS输出单元变为关闭(OFF)状态。 e) 检察员离开SRS。 f) SRS输出单元在2 min内变为开通(ON)状态。 g) 检查是否有任何机械损伤	最终用户处的每个SRS 被测SRS的序列号	记录到最终用户的检查报告中

附 录 I
（资料性）
功能、安全相关信息和融合的示例

I.1 功能示例

使用一个激光雷达 LIDAR（作为 SRS）对工业现场两条道路的交叉口进行监控。两条道路都供 AGV 和行人使用。任务是避免 AGV 撞到行人，同时收集路过行人的数量以便对车辆进行路径优化。

SRS 的布置可保证其安全相关区能够覆盖交叉口以及两条道路的临近区域（见图 I.1）。

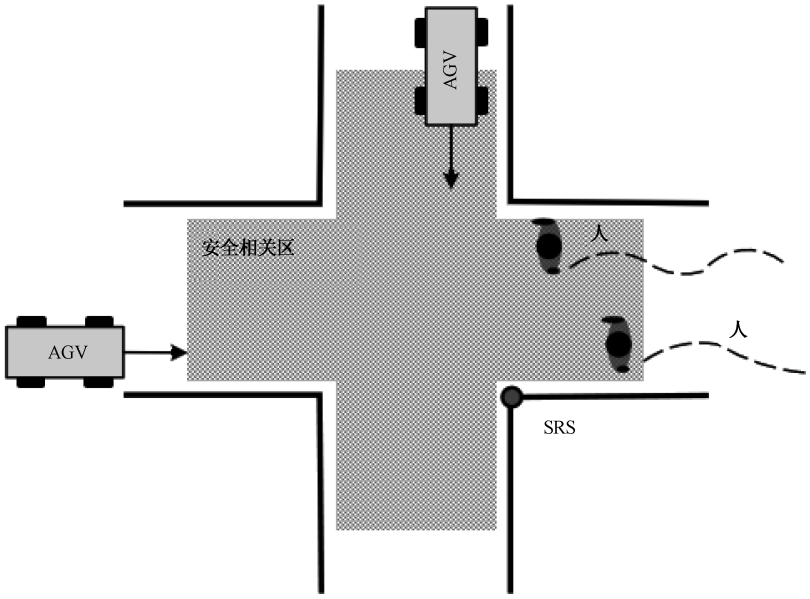


图 I.1 SRS 在道路交叉口的应用示例

SRS 的安全相关功能规定为：检测预设安全相关区内的行人和 AGV 车辆，如果发现两个安全相关物体相向接近，它就会产生安全相关信息以降低车辆在路口的速度。

安全相关物体包括行人和危险物体（AGV 车辆）。从这个角度来看，安全相关功能其实是人员检测功能和危险物体检测功能的一种组合。

除了安全相关功能外，SRS 还会通过对路过行人的计数来收集交通数据。因为仅对人员而非车辆进行追踪和计数，因此对该自动化相关功能而言他们是唯一的自动化物体。

确保自动化相关功能的执行不会造成性能等级 C 到 F 的 SRS 安全相关功能的危险失效。具体来说，需避免同时对大量行人进行追踪和计数来防止安全相关功能的响应时间延长并超出规定限值。

I.2 安全相关信息示例

使用 6.2 所述的简化融合方法，可利用输出单元提供的安全相关信息将 SRS/SRSS 进一步集成到 SCS 以及/或者将 SRS 集成到 SRSS 中。

制造商规定 SRS/SRSS 输出单元是否提供判定信息和/或测量信息。

如果具备规定属性的一个或多个物体没有进入规定的安全相关区，那么表示判定信息的信号能够明确区分。如果具备规定属性的物体进入了安全相关区，系统需提供对应的置信度信息。

注 1：图 I.2 提供了一个物体的示例，仅有其位置信息（能在安全相关区内）被用作判定属性。

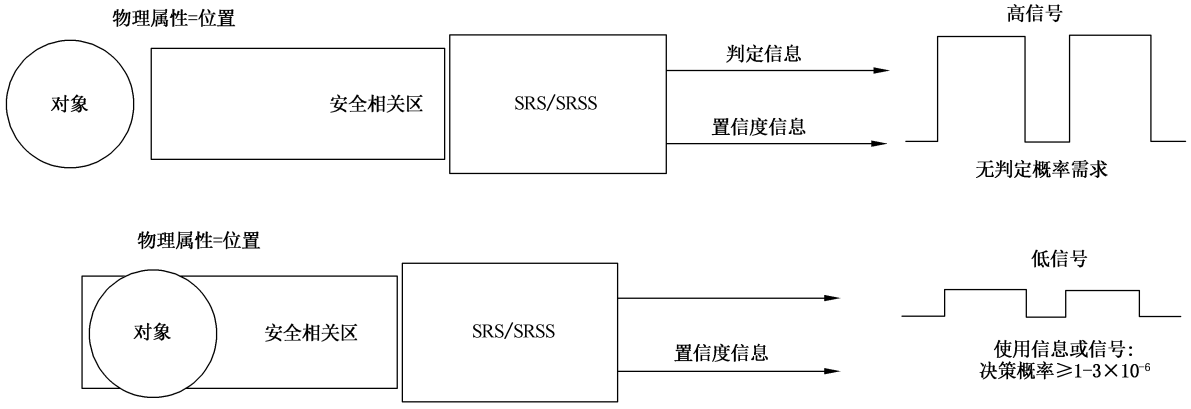


图 I.2　提供判定和置信度信息的 SRS/SRSS 示例

如果物体位于安全相关区外,那么不需要以判定概率值表示的置信度信息。对应的判定信息可由(比如)高电平信号表示。在 SRS/SRSS 故障、错误或失效情况下,不需要判定概率的有关信息。

如果物体位于安全相关区内,那就需要以判定概率值表示的置信度信息。在图 I.2 中,对应的判定信息由低电平表示。在这种情况下,故障、错误或判定信息失效会导致危险失效。判定概率值满足表 5 相应公式(1)的要求。

图 I.3 展示了一个 SRS/SRSS 提供安全相关区内物体位置属性的测量和置信度信息的示例。

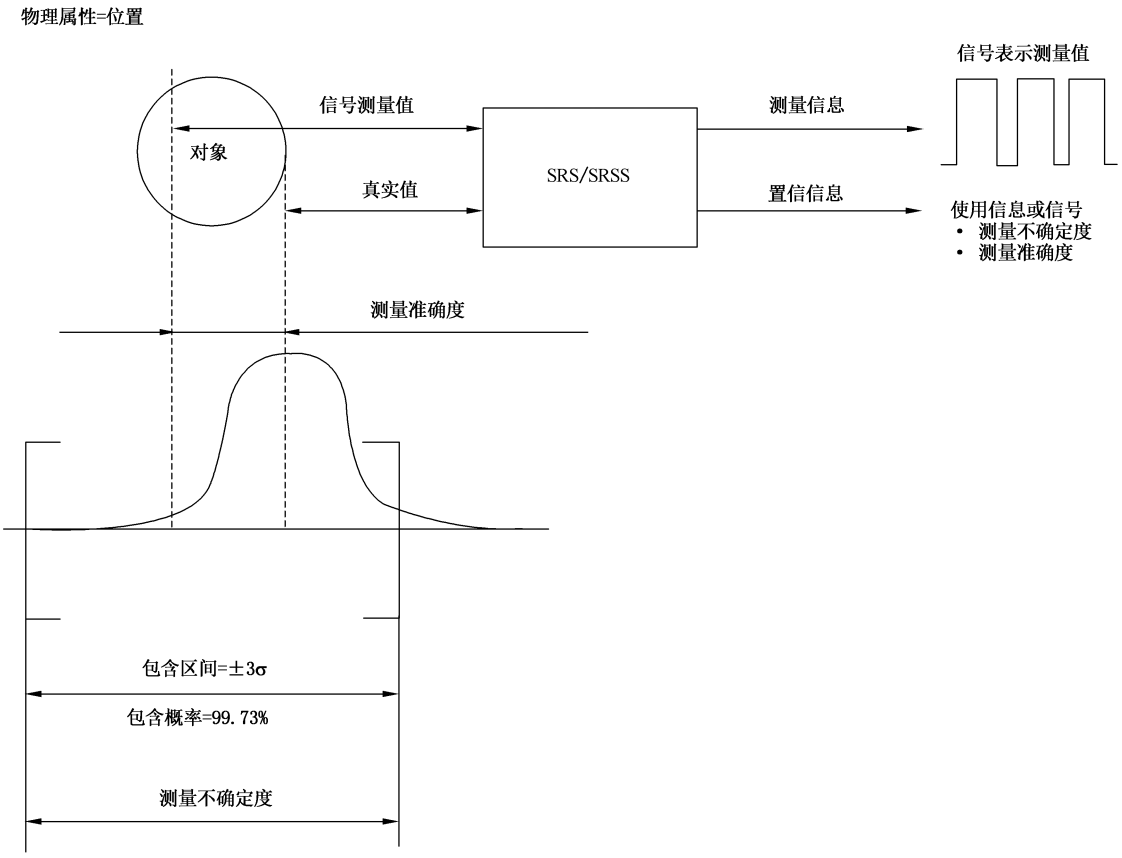


图 I.3　SRS/SRSS 提供测量和置信度信息的示例

注: 图 I.3 所示为正态分布。也可能出现其他分布。

测量信息会将安全相关区内的实际测量值连续地表示为相应的信号。在本例中,置信度信息通过测量准确度和测量不确定度表示位置这个物理属性。基于测量准确度和不确定度的包含概率满足表 5 和公式(1)的要求。置信度信息可作为额外的电信号或在使用说明中提供。

I.3 融合示例

通过将两个或更多 SRS 融合到一个 SRSS 中所能实现的,例如检测能力的改善取决于预定用途以及在规定限值内使用 SRS 传感器技术。

如图 I.4 所示,融合之后的 SRSS 感应区相较 SRS 感应区是减小的。仅考虑静态情况下,使用不同传感器技术对检测能力的改善只在 SRSS 规定约束条件下有效。在 SRSS 感应区内,融合对检测能力的改善仅对物体 1 有效。由于物体 2 被物体 1 遮挡,因此只有 SRS 2 能够在相应检测能力范围内检测到物体 2。

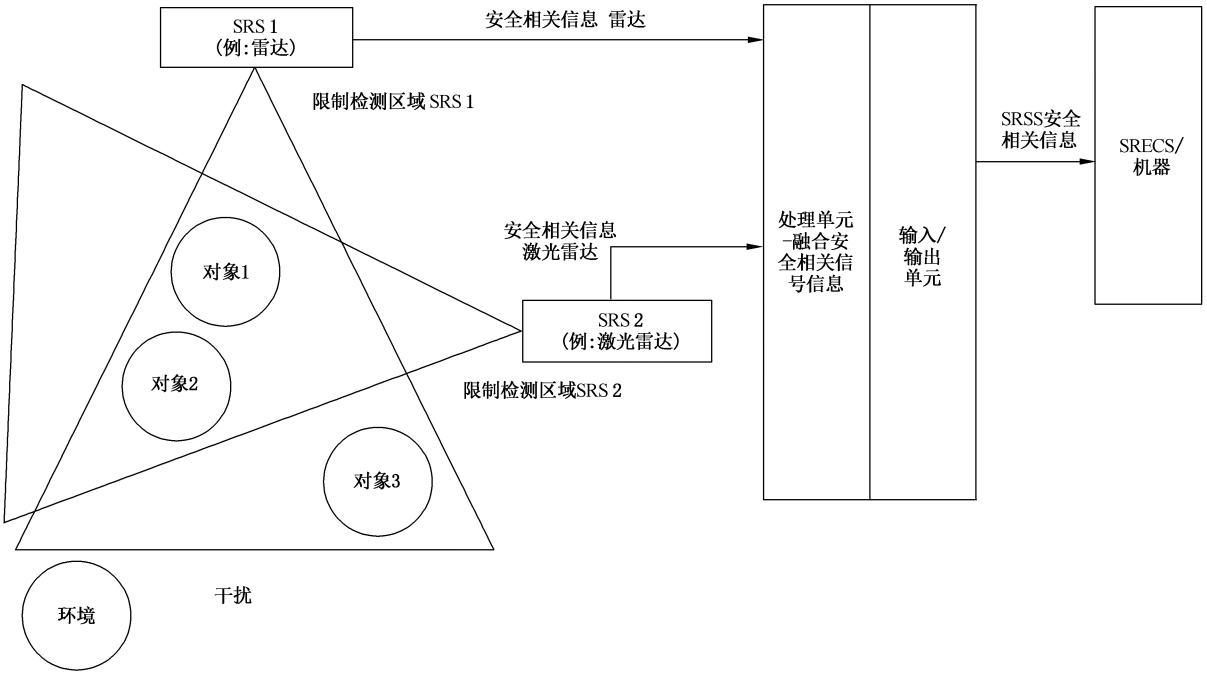


图 I.4 将 2 个 SRS 融合到一个 SRSS 以产生组合感应区的第一个示例

在融合之后,SRS 所提供的安全相关信息由 SRSS 处理单元使用恰当的逻辑功能执行。物体是否处于感应区内的相关信息可能会以位置测量信息或表示物体进入了 SRS 所监控的安全相关区的简单判定信息的方式提供。此外,SRS 制造商需向 SRSS 集成商提供信息的置信度(见图 I.5)。

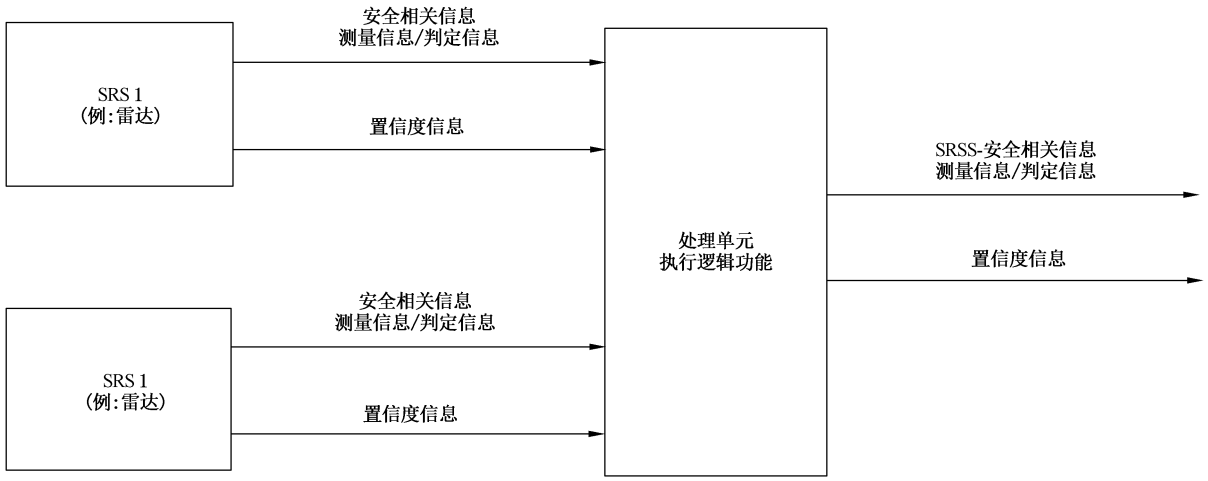


图 I.5　SRS 安全相关信息的融合

最后,SRSS 所实现的检测能力改善需要在考虑 SRSS 安全要求规范所规定预定用途的前提下由 SRSS 集成商进行验证和确认。SRSS 集成商需在使用说明中向用户提供使用限值的相关信息(见图 I.6)。

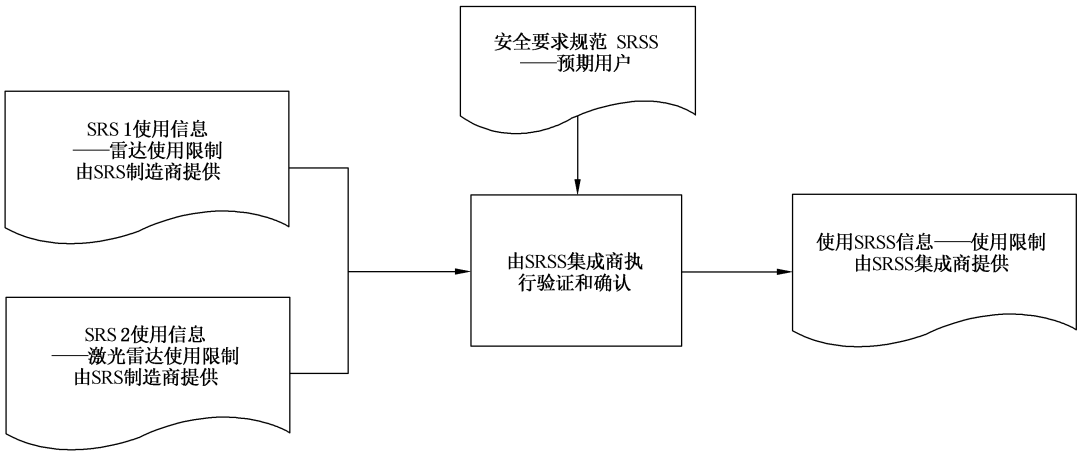


图 I.6　根据 SRS 使用说明和 SRSS 安全要求规范进行的验证和确认方法

图 I.7 所示是一个典型的有多台自主导航车在过道上运行的 AGV 应用案例。通过将 AGV 上安装的 SRS 1 和墙壁上安装的 SRS 2 进行融合,可拓展角落处的安全相关区,从而避免 AGV 和行人相撞。

SRS 1 是一个使用 TOF 摄像头作为检测单元的 SRS。SRS 1 的安装是朝向 AGV 的行进方向,可根据 AGV 和行人的移动速度确定出安全相关区。它会检测行人或障碍物,并将判定信息提供给 AGV 作为“正常”“减速”或“停下”等条件下的安全相关信息。

SRS 2 是一个使用激光雷达作为检测单元的 SRS。SRS 2 安装在过道角落的墙壁上,并且根据总坐标系进行了校准。它可根据机器人和行人的移动速度确定出安全相关区。它能检测从盲点相互接近的 AGV 和行人,并将判定信息提供给 AGV 作为“正常”“减速”或“停下”等条件下的安全相关信息。

SRS 1 和 SRS 2 通过融合被集成到了一个 SRSS 中。SRS 1 和 SRS 2 的安全相关信息采用或(OR)逻辑进行集成,然后 SRSS 将判定信息作为“正常”“减速”或“停下”等条件下的安全相关信息提供给 AGV。

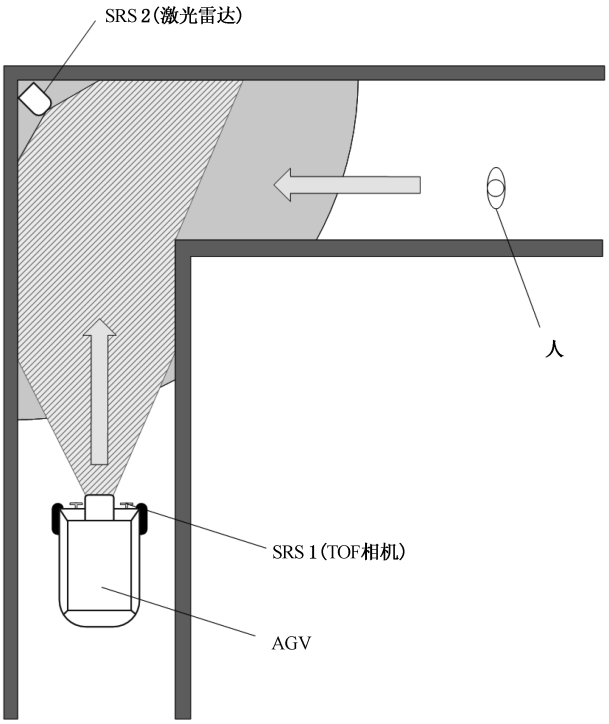


图 I.7　将 2 个 SRS 融合到一个 SRSS 以产生组合感应区的第二个示例

注：在 IEC TR 62998-2 中提供了更详细的应用案例。

参 考 文 献

[1] GB/T 2900.25—2008 电工术语 旋转电机

[2] GB/T 2900.56—2008 电工术语 控制技术

[3] GB/T 2900.83—2008 电工术语 电的和磁的器件

[4] GB/T 2900.99—2016 电工术语 可信性

[5] GB/T 15706—2012 机械安全 设计通则 风险评估和降低风险

[6] GB/T 19000—2016 质量管理体系 基础和术语

[7] GB/T 20438.1—2017 电气、电子和可编程电子安全相关系统的功能安全 第1部分:一般要求

[8] GB/T 20438.4—2017 电气、电子和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

[9] GB/T 23686—2018 电子电气产品环境意识设计

[10] GB/T 26158—2010 中国未成年人人体尺寸

[11] GB/T 26160—2010 中国未成年人头面部尺寸

[12] GB/T 27000—2006 合格评定 词汇和通用原则

[13] ISO 9000:2015 Quality management systems—Fundamentals and vocabulary

[14] ISO 11161 Safety of machinery—Integrated manufacturing systems—Basic requirements

[15] ISO 13849-1 Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design

[16] ISO 13856-1 Safety of machinery—Pressure-sensitive protective devices—Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors

[17] ISO 13856-2 Safety of machinery—Pressure-sensitive protective devices—Part 2: General principles for design and testing of pressure-sensitive edges and pressure-sensitive bars

[18] ISO 13856-3 Safety of machinery—Pressure-sensitive protective devices—Part 3: General principles for design and testing of pressure-sensitive bumpers, plates, wires and similar devices

[19] ISO 15003 Agricultural engineering—Electrical and electronic equipment—Testing resistance to environmental conditions

[20] ISO 15622 Intelligent transport systems—Adaptive cruise control systems—Performance requirements and test procedures

[21] ISO 15998 Earth-moving machinery—Machine-control systems (MCS) using electronic components—Performance criteria and tests for functional safety

[22] ISO 16148 Gas cylinders—Refillable seamless steel gas cylinders and tubes—Acoustic emission examination (AT) and follow-up ultrasonic examination (UT) for periodic inspection and testing

[23] ISO 18497 Agricultural machinery and tractors—Safety of highly automated agricultural machines—Principles for design

[24] ISO TR 22100-1 Safety of machinery—Relationship with ISO 12100—Part 1: How ISO 12100 relates to type-B and type-C standards

[25] ISO TR 22100-2 Safety of machinery—Relationship with ISO 12100—Part 2: How ISO 12100 relates to ISO 13849-1

[26] ISO 25119 (all parts) Tractors and machinery for agriculture and forestry—Safety-related

parts of control systems

[27] IEC 60050-151 International Electrotechnical Vocabulary—Part 151: Electrical and magnetic devices

[28] IEC 60050-191:1990 International Electrotechnical Vocabulary—Chapter 191 Dependability and quality of service

[29] IEC 60050-192 International Electrotechnical Vocabulary (IEV)—Part 192: Dependability

[30] IEC 60050-311 International Electrotechnical Vocabulary—Part 311: Electrical and electronic measurements—General terms relating to measurements

[31] IEC 60050-351 International Electrotechnical Vocabulary—Part 351: Control technology

[32] IEC 60050-411 International Electrotechnical Vocabulary—Part 411: Rotating machinery

[33] IEC 60050-702 International Electrotechnical Vocabulary—Part 702: Oscillations, signals and related devices

[34] IEC 60050-704 International Electrotechnical Vocabulary—Part 704: Transmission

[35] IEC 60068-2-1 Environmental testing—Part 2-1:Tests A: Cold

[36] IEC 60068-2-2 Environmental testing—Part 2-2: Tests B: Dry heat

[37] IEC 60068-2-6 Environmental testing—Part 2-6: Tests—Test Fc: vibration(sinusoidal)

[38] IEC 60068-2-14 Environmental testing procedures—Part 2-14: Tests—Test N:Change of temperature

[39] IEC 60068-2-27 Environmental testing—Part 2-27: Tests—Test Ea and guidance:Shock

[40] IEC 60068-2-31 Environmental testing—Part 2-31: Tests—Test Ec: Rough handling shocks, primarily for equipment-type specimens

[41] IEC 60068-2-75:2014 Environmental testing—Part 2-75: Tests—Test Eh: Hammer tests

[42] IEC 60068-2-78 Environmental testing—Part 2-78: Tests—Test Cab: Damp heat, steady state

[43] IEC 60529 Degrees of protection provided by enclosures (IP Code)

[44] IEC 60654-1 Industrial-process measurement and control equipment—Operating conditions—Part 1:Climatic conditions

[45] IEC 60721-2-1 Classification of environmental conditions—Part 2-1: Environmental conditions appearing in nature—Temperature and humidity

[46] IEC 60721-3-0 Classification of environmental conditions—Part 3: Classification of groups of environmental parameters and their severities—Introduction

[47] IEC 60721-3-3 Classification of environmental conditions—Part 3: Classification of groups of environmental parameters and their severities—Section 3: Stationary use at weatherprotected locations

[48] IEC 60721-3-4 Classification of environmental conditions—Part 3: Classification of groups of environmental parameters and their severities—Section 4: Stationary use at non—weatherprotected locations

[49] IEC 60721-3-5 Classification of environmental conditions—Part 3: Classification of groups of environmental parameters and their severities—Section 5: Ground vehicle installations

[50] IEC 60721-3-6 Classification of environmental conditions—Part 3: Classification of groups of environmental parameters and their severities—Ship environment

[51] IEC 60947-5-2 Low-voltage switchgear and controlgear—Part 5-2: Control circuit devices and switching elements—Proximity switches

[52] IEC 60947-5-3 Low-voltage switchgear and controlgear—Part 5-3: Control circuit devices and switching elements—Requirements for proximity devices with defined behaviour under fault conditions (PDDB)

[53] IEC 61010-1 Safety requirements for electrical equipment for measurement, control, and laboratory use—Part 1: General requirements

[54] IEC 61032 Protection of persons and equipment by enclosures—Probes for verification

[55] IEC 61160 Design review

[56] IEC 61496 (all parts) Safety of machinery—Electro-sensitive protective equipment

[57] IEC 61496-1 Safety of machinery—Electro-sensitive protective equipment—Part 1: General requirements and tests

[58] IEC 61496-2 Safety of machinery—Electro-sensitive protective equipment—Part 2: Particular requirements for equipment using active opto-electronic protective devices(AOPDs)

[59] IEC 61496-3 Safety of machinery—Electro-sensitive protective equipment—Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR)

[60] IEC TS 61496-4-2 Safety of machinery—Electro-sensitive protective equipment—Part 4-2: Particular requirements for equipment using vision based protective devices(VBPD)—Additional requirements when using reference pattern techniques (VBPDPP)

[61] IEC TS 61496-4-3 Safety of machinery—Electro-sensitive protective equipment—Part 4-2: Particular requirements for equipment using vision based protective devices(VBPD)—Additional requirements when using stereo vision techniques (VBPDST)

[62] IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety related systems—Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[63] IEC 61508-3 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements

[64] IEC 61703 Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[65] IEC 62368-1:2018 Audio/video, information and communication technology equipment—Part 1: Safety requirements

[66] ISO/IEC Guide 50 Safety aspects—Guidelines for child safety in standards and other specifications

[67] ISO/IEC Guide 51:2014 Safety aspects—Guidelines for their inclusion in standards

[68] ISO/IEC Guide 98-1 Uncertainty of measurement—Part 1: Introduction to the expression of uncertainty in measurement

[69] ISO/IEC Guide 98-3 Uncertainty of measurement—Part 3: Guide to the expression of uncertainty in measurement

[70] ISO/IEC Guide 99:2007 International vocabulary of metrology—Basic and general concepts and associated terms (VIM)

[71] ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories

[72] EN 16580 Windows and doors—Wetness and splash water proof door leaves—Test and classification

[73] EN 50125-1 Railway applications—Environmental conditions for equipment—Part 1: Rolling

stock and on-board equipment

[74] EN 50346 Information technology—Cabling installation—Testing of installed cabling

[75] EN 50364 Product standard for human exposure to electromagnetic fields from devices operating in the frequency range 0 Hz to 300 GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications

[76] EN 50499 Procedure for the assessment of the exposure of workers to electromagnetic fields

[77] EN 50527 (all parts) Procedure for the assessment of the exposure to electromagnetic fields of workers bearing active implantable medical devices

[78] ANSI/ITSDF B56.5, Safety Standard for Driverless, Automatic Guided Industrial Vehicles and Automated Functions of Manned Industrial Vehicles

[79] "Temporal symmetries during gait initiation and termination in nondisabled ambulators and in people with unilateral transtibial limb loss", Journal of Rehabilitation Research and Development. 2005 Mar-Apr;42(2):175-82

[80] "Indoor Snowfall Simulation Chamber for Realizing Uniform Snowfall". Bong Keun Kim and Yasushi Sumi. 2015 IEEE International Conference on Advanced Intelligent Mechatronics (AIM) July 7-11, 2015. Busan, Korea

[81] Japanese children size DATA "Report of children size Data Base for increasing safety of machinery 2008", by the Japan Machinery Federation and Research Institute of Human Engineering for Quality Life

[82] "Physical Characteristic of Children—As related to Death and Injury for Consumer Product Design an Use", UM-HSRI-BI-75-5 Final Report Contract FDA-72-70 May 1975

[83] "Visibility reduction based performance evaluation of vision-based safety sensors", Bong Keun Kim, Yasushi Sumi, Ryusuke Sagawa, Kenji Kosugi, and Shigeto Mochizuki. 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems(IROS)Congress Center Hamburg

[84] International accreditation service (IAS), IAS Calibration and testing laboratory accreditation programs definitions, 2018