



中华人民共和国国家标准

GB 28526—2012/IEC 62061:2005

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

**Electrical safety of machinery—Functional safety of safety-related electrical,
electronic and programmable electronic control systems**

(IEC 62061:2005, Safety of machinery—Functional safety of safety-related
electrical, electronic and programmable electronic control systems, IDT)

2012-06-29 发布

2013-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

中 华 人 民 共 和 国
国 家 标 准
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 28526—2012/IEC 62061:2005

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)

网址: www.gb168.cn

服务热线: 010-68522006

2012年12月第一版

*

书号: 155066·1-45582

版权专有 侵权必究

目 次

前言	V
引言	IV
1 范围	1
2 规范性引用文件	2
3 术语和定义、缩略语	3
3.1 按字母顺序排列的定义表	3
3.2 术语和定义	4
3.3 缩写	11
4 功能安全管理	12
4.1 目的	12
4.2 要求	12
5 安全相关控制功能规范要求(SRCF)	13
5.1 目的	13
5.2 SRCF 要求规范	13
6 安全相关电气控制系统设计与整合(SRECS)	14
6.1 目的	14
6.2 一般要求	15
6.3 检测 SRECS 故障时的行为(SRECS 的)要求	15
6.4 SRECS 系统安全完整性要求	16
6.5 安全相关电气控制系统选择	17
6.6 安全相关电气控制系统(SRECS)设计和开发	17
6.7 子系统实现	21
6.8 实现诊断功能	32
6.9 SRECS 硬件实现	33
6.10 软件安全要求规范	33
6.11 软件设计和开发	34
6.12 安全相关电气控制系统集成和测试	39
6.13 SRECS 安装	40
7 SRECS 使用信息	40
7.1 目的	40
7.2 安装、使用与维护文件	40
8 安全相关电气控制系统确认	41
8.1 目的	41
8.2 一般要求	41
8.3 SRECS 系统安全完整性确认	41

9 修改	42
9.1 目的	42
9.2 修改程序	42
9.3 配置管理程序	43
10 文件	44
附录 A (资料性附录) SIL 分配	46
附录 B (资料性附录) 安全相关电气控制系统(SRECS)设计示例 使用条款 5、6 的概念和要求	52
附录 C (资料性附录) 嵌入式软件设计和开发指南	57
附录 D (资料性附录) 电气/电子部件的失效模式	63
附录 E (资料性附录) 按照 GB/T 17799.2—2003 用于工业环境的 SRECS 电磁现象(EM)和 提高的抗扰度水平	67
附录 F (资料性附录) 共同原因失效(CCF)敏感度评估方法	69
图 1 IEC 62061 与其他有关标准的关系	VII
图 2 SRECS 设计和开发过程的工作流程	19
图 3 子系统的功能模块安全要求配置(见 6.6.2.1.1)	20
图 4 子系统设计和开发流程(见图 2 的 6B 框)	23
图 5 功能块分解成冗余功能块元素和其相关的子系统元素	24
图 6 子系统 A 逻辑表示	28
图 7 子系统 B 逻辑表示	29
图 8 子系统 C 逻辑表示	29
图 9 子系统 D 逻辑表示	30
图 A.1 SIL 分配过程的工作流程	46
图 A.2 用于风险评估的参数	47
图 A.3 SIL 分配过程形式示例	51
图 B.1 功能分解的术语	52
图 B.2 机器示例	53
图 B.3 SRCF 要求说明	53
图 B.4 分解功能块结构	53
图 B.5 SRECS 的结构初步概念	54
图 B.6 各子系统(SS1 到 SS4)内嵌诊断功能的 SRECS 体系结构	55
图 B.7 子系统 SS3 内嵌诊断功能的 SRECS 体系结构	55
图 B.8 对于 SRECS 的 PFHD 评估	56
表 1 IEC 62061 和 ISO 13849-1 建议应用范围(修订中)	VIII
表 2 本标准概述和目标	1

表 3	安全完整性等级;SRCF 目标失效值	14
表 4	本例使用的子系统 1 和子系统 2 的特性(见 6.6.3.3 注)	21
表 5	子系统体系结构限制:使用本子系统的 SRCF 可能要求的最大 SIL	25
表 6	体系结构限制:分类相关的 SILCL	26
表 7	危险失效概率	27
表 8	SRECS 的信息和文件	45
表 A.1	严重程度(Se)分类	48
表 A.2	暴露的频率(Fr)和持续时间分级	48
表 A.3	概率(Pr)分类	49
表 A.4	避免或限制伤害的概率(Av)等级	50
表 A.5	用于决定伤害概率级别的参数(CI)	50
表 A.6	SIL 分配矩阵	50
表 D.1	电气/电子部件失效模式率示例	63
表 E.1	SRECS 的电磁现象(EM)和提高的抗扰度	67
表 E.2	RF 场试验选择频率	68
表 E.3	传导 RF 场选择频率	68
表 F.1	CCF 评估准则	69
表 F.2	CCF 因素(β)评估	70

前 言

本标准的 5、6.4、6.6.3、6.10、6.12 为强制性,其余为推荐性条款。

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 IEC 62061:2005《机械安全 安全相关电气、电子和可编程电子控制系统安全功能》。

本标准作了下列编辑性修改:

——标准名称改为《机械电气安全 安全相关电气、电子和可编程电子控制系统安全功能》;

——删除国际标准前言。

本标准由中国机械工业联合会提出。

本标准由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本标准负责起草单位:国家机床质量监督检验中心、中国科学院沈阳计算技术研究所有限公司。

本标准参加起草单位:固高科技(深圳)有限公司、北京凯恩帝数控技术有限责任公司、济南凌康数控技术有限公司、苏州市华测检测技术有限公司、浙江凯达机床集团有限公司。

本标准主要起草人:黄祖广、尹震宇、赵钦志、杨京彦、黄麟、于东、龚小云、张承瑞、杨洪丽、朱平、何宇军、胡毅。

引 言

由于自动化的结果,要求增加生产、降低操作人员体力,机械安全相关电气控制系统(以下简称 SRECS)在实现整个机械安全方面发挥日益重要的作用。此外,SRECS 自身日益采用复杂的电子技术。

在没有标准之前,人们不太情愿接受 SRECS 的安全相关功能来处理重大机器危险,因为这类技术的性能存在不确定性。

本标准作为机械设计师、控制系统制造商和集成厂商和规范涉及的其他人员、SRECS 的设计和确认人员使用。它为达到所需的性能陈述方法和规定要求。

本标准阐述了 IEC 61508 框架内机器领域的具体应用。它主要为了完善在发生重大机器危险(见 ISO 12100-1 第 3.8 项)情况下执行安全相关电气控制系统的规范。

本标准提供机器 SRECS 机械部分特有的功能安全框架。它只包括安全生命周期中从安全要求配置到安全确认过程之间的相关方面。各项要求提供了安全使用机器的 SRECS 的相关信息,它与 SRECS 寿命的后阶段有关。

当 SRECS 用作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。典型的案例是联锁防护装置的使用,当它被打开,意味着危险区域被访问时,便主动向电气控制系统发出信号,停止危险的机器操作。同样,在自动化操作中,通常用来实现机器加工正确操作的电气控制系统,经常可以通过减少控制系统失效直接造成的危险,以达到安全。本标准提供下列方法和要求:

- 指定由 SRECS 执行的各个安全相关控制功能要求的安全完整性等级;
- 使 SRECS 设计适合指定的安全相关控制功能;
- 设计的集成安全相关子系统符合 ISO 13849;
- 确认 SRECS。

本标准预期用于 ISO 12100-1 描述的降低系统风险的框架范围内,并根据 ISO 14121(EN 1050)描述的原则,同风险评估一起使用。安全完整性等级(SIL)分配的建议性方法在资料性附录 A 中提供。

考虑到电气控制系统内随机故障或系统故障的概率和结果,给出了协调 SRECS 性能和预期风险降低的措施。

图 1 显示本标准与其他相关标准的关系。

表 1 对应用本标准和 ISO 13849-1 的修订版提出建议。

IEC 62061 和 ISO 13849-1(修订中)规定机械安全相关控制系统设计和实施的要求。在标准范围内,使用其中任何一个,可以推定满足相关基本安全要求。表 1 总结 IEC 62061 和 ISO 13849-1(修订中)的范围。

注: ISO 13849-1 当前正由 ISO TC 199 和 CEN TC 114 制定中。

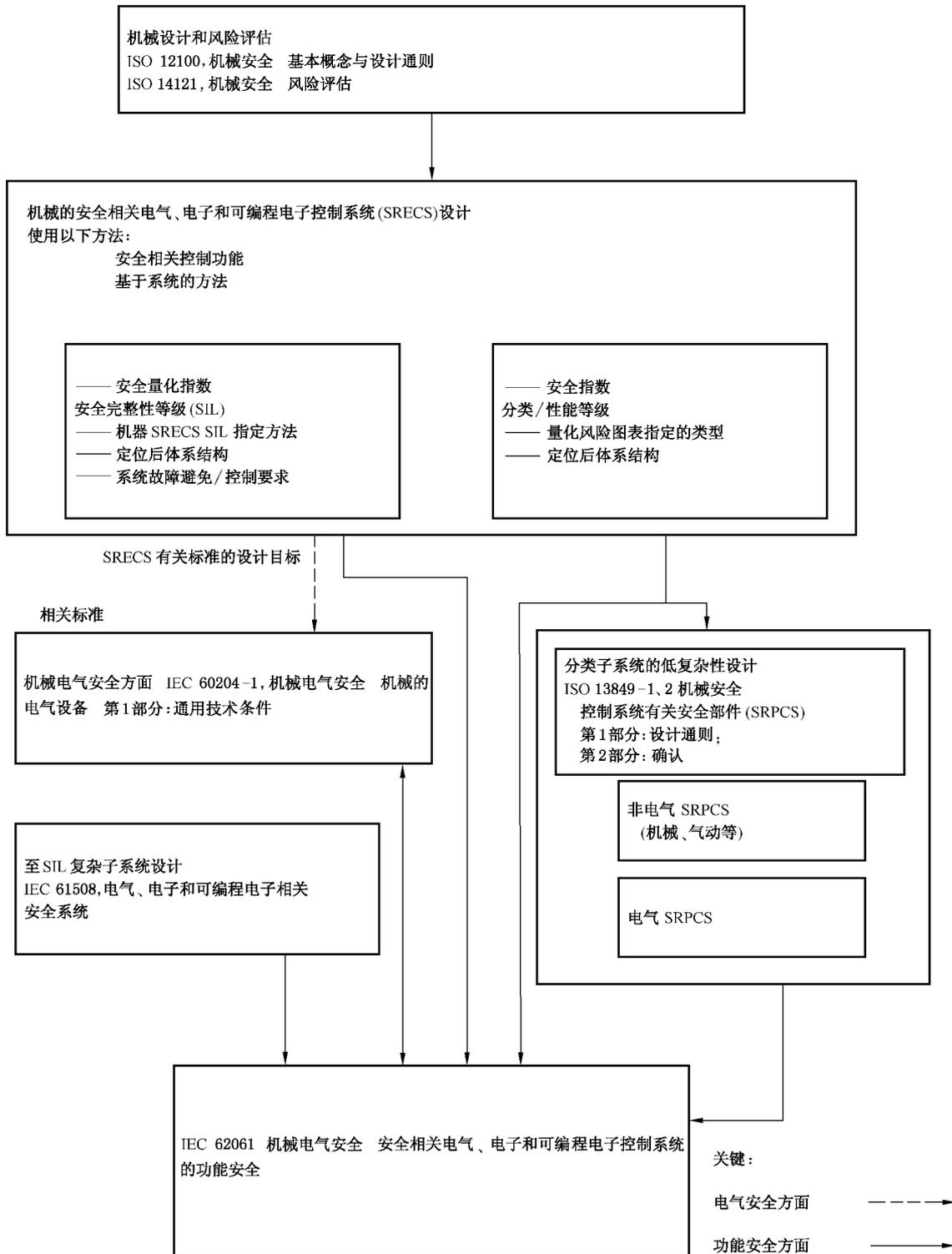


图 1 IEC 62061 与其他有关标准的关系

表 1 IEC 62061 和 ISO 13849-1 建议应用范围(修订中)

	执行安全相关控制功能的技术	ISO 13849-1(修订中)	IEC 62061
A	非电气,例如液压	X	未包括在内
B	机电,例如继电器或非复杂电子	限指定结构(见注 1)并达到 PL=e	所有结构并达到 SIL3
C	复杂电子,例如可编程	限指定结构(见注 1)并达到 PL=d	所有结构并达到 SIL3
D	A 与 B 组合	限指定结构(见注 1)并达到 PL=e	X 见注 3
E	C 与 B 组合	限指定结构(见注 1)并达到 PL=d	所有结构并达到 SIL3
F	C 与 A 组合,或 C 与 A 和 B 组合	X 见注 2	X 见注 3
<p>“X”表示该项目由本列标题所示的标准处理。</p> <p>注 1: 指定结构在 EN ISO 13849-1(修订版)附录 B 规定,提供性能等级量化的简化方法。</p> <p>注 2: 对于复杂电子:按照 EN ISO 13849-1(修订版)使用指定的结构,达到 PL=d 或按照 IEC 62061 的任何结构。</p> <p>注 3: 对于非电气技术,按照 EN ISO 13849-1(修订版)规定的部件作为子系统。</p>			

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

1 范围

本标准对机械安全相关电气电子和可编程电子控制系统(SRECS)的设计、集成和确认,规定要求和给出建议(见注1和注2)。

本标准适用于单独的或组合的方式来使用的控制系统,以使工作时非便携式的机器执行安全相关控制功能,包括以协调方式共同工作的一组机器,而不适用于手提工作机器。

注1:在本标准里,“电气控制系统”这一术语表示“电气、电子和可编程电子(E/E/PE)控制系统”,“SRECS”表示“安全相关电气、电子和可编程电子控制系统”。

注2:在本标准里,假设复杂可编程电子子系统或子系统元素的设计符合IEC 61508有关要求。本标准提供使用方法,而不是这类子系统和子系统元素作为SRECS的部件的开发。

本标准是应用标准,不限制或阻碍技术进步。它不包括需要或要求由其他标准或法规为保护人身免遭危险的所有要求(例如防护、非电气联锁或非电气控制)。各类型的机器都有独特的要求需要满足,以提供充分的安全。

本标准:

——仅涉及预期降低直接接近机器或直接使用机器而造成的人身伤害或健康危害的风险的功能安全要求;

——限于机器自身或以协调方式共同工作的机器组的危险直接引起的风险;

注3:降低由其他危险引起的风险的要求在有关领域的标准中提供。例如,机器是加工活动的一部分时,机械电气控制系统功能安全要求应满足其他要求(如GB/T 21109),只要有关加工安全。

——没有规定机械非电气(例如液压、气动)控制元素性能要求;

注4:虽然本标准要求特别针对电气控制系统,但规定的框架和方法可以适用于使用其他技术的控制系统的安全相关部件。

——不包括电气控制设备自身引起的电气危险(例如电击,见GB 5226.1)。

本标准特定条款的目标见表2。

表2 本标准概述和目标

条款	目标
4 功能安全管理	为达到SRECS功能安全要求,规定必要的管理和技术活动
5 安全相关控制功能规范要求	建立程序,规定安全有关控制功能的要求。这些要求以功能要求规范和安全完整性要求规范的术语表述
6 安全相关电气控制系统的设计与整合	为满足功能安全要求,规定SRECS的选择准则和/或设计和实现方法。包括: 选择系统结构; 选择安全相关硬件和软件; 设计硬件和软件; 验证设计的硬件和软件满足功能安全要求