ICS 29.020
K 09

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

目　　次

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。

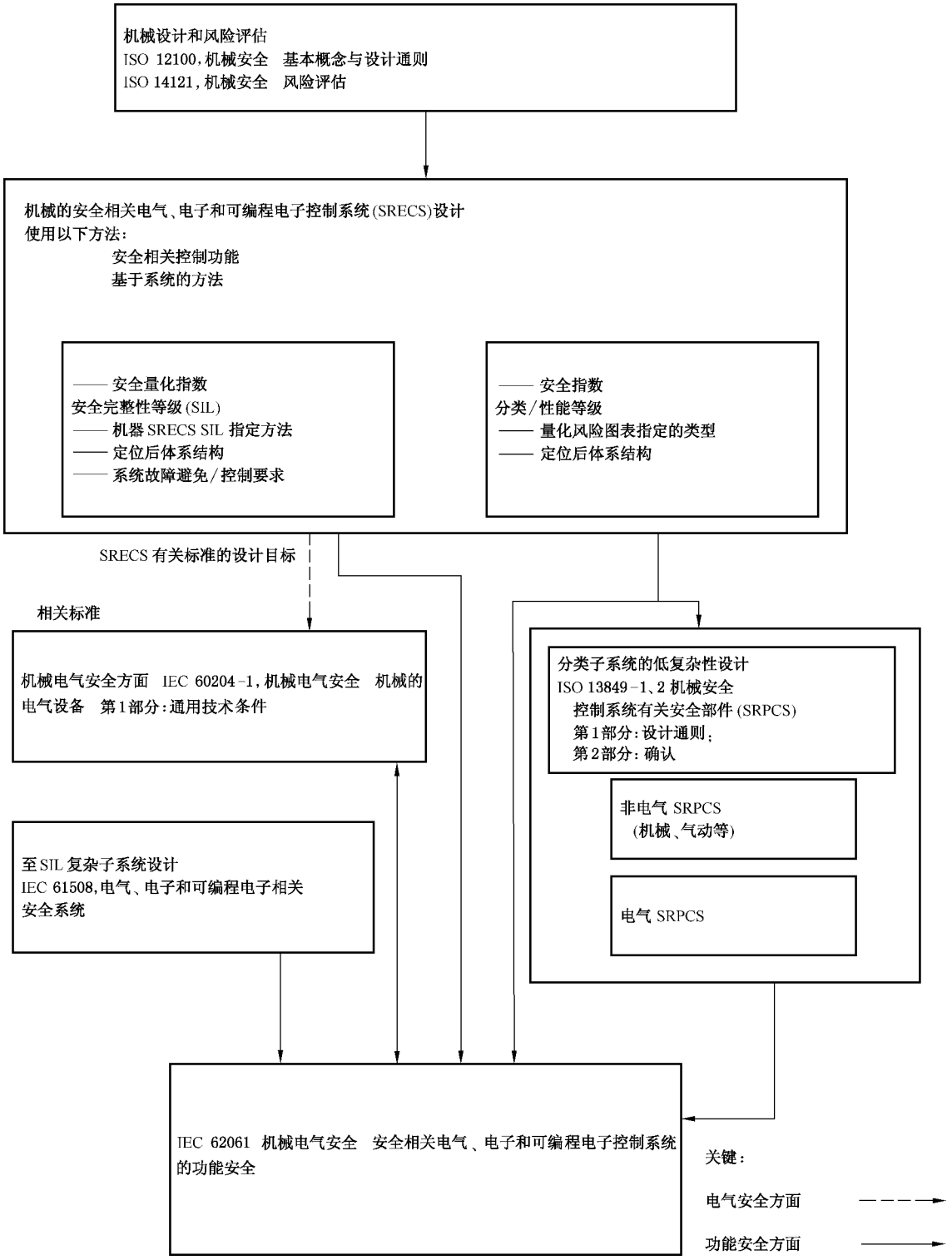

图 1 IEC 62061 与其他有关标准的关系

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

"X"表示该项目由本列标题所示的标准处理。

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。

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。

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。

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