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.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 5 字数 145 千字
2012 年 12 月第一版 2012 年 12 月第一次印刷
*
书号:155066·1-45582 定价 66.00 元

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。

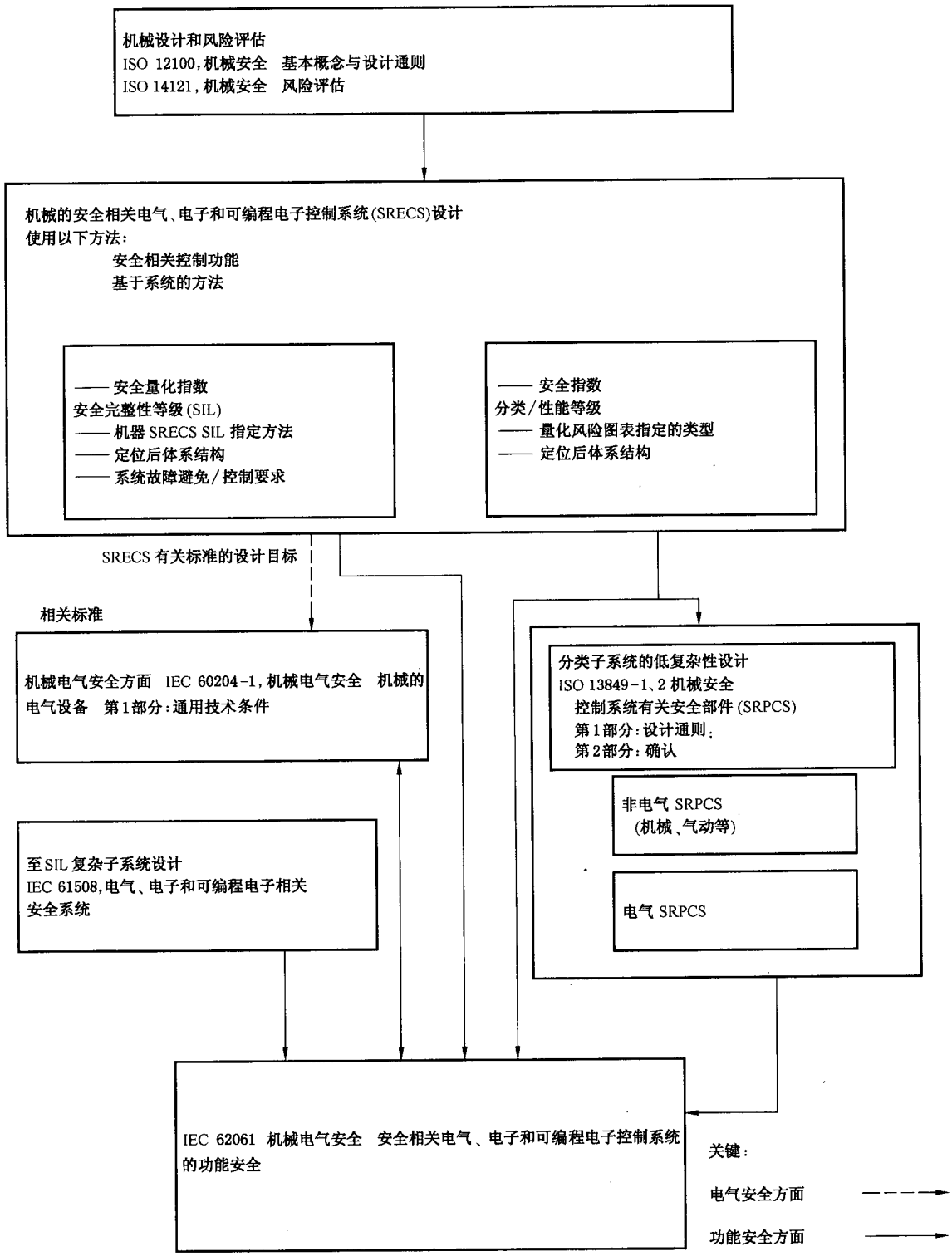


图 1 IEC 62061 与其他有关标准的关系

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

表 2（续）

条　款	目　标
7 SRECS 使用信息	规定提供 SRECS 使用信息的要求，这些资料随机器提供。包括： 提供用户手册和程序； 提供维修手册和程序
8 安全相关电气控制系统的确认	规定适用于 SRECS 的确认流程的要求。包括对 SRECS 的检查和测试，确保其达到安全要求规范中所述的要求。
9 安全相关电气控制系统的修改	当修改 SRECS 时，规定修改程序的要求，包括： 对 SRECS 进行任何修改前，做适当计划和验证； 完成任何修改后，满足 SRECS 安全要求规范

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 5226.1—2008　机械电气安全　机械电气设备　第 1 部分：通用技术条件（IEC 60204-1:2005，IDT）

GB/T 15706.1—2007　机械安全　基本概念与设计通则　第 1 部分：基本术语和方法（ISO 12100-1:2003，IDT）

GB/T 15706.2—2007　机械安全　基本概念与设计通则　第 2 部分：技术原则（ISO 12100-2:2003，IDT）

GB/T 16855.1—2008　机械安全　控制系统有关安全部件　第 1 部分：设计通则（ISO 13849-1:2006，IDT）

GB/T 16855.2—2007　机械安全　控制系统有关安全部件　第 2 部分：确认（ISO 13849-2:2003，IDT）

GB/T 16856.1—2008　机械安全　风险评价　第 1 部分：原则（ISO 14121-1:2007，IDT）

GB/T 16856.2—2008　机械安全　风险评价　第 2 部分：实施指南和方法举例（ISO/TR 14121-2:2007，IDT）

GB/T 17799.2—2003　电磁兼容　通用标准　工业环境中的抗扰度试验（IEC 61000-6-2:1999，IDT）

GB 18209.1—2010　机械电气安全　指示、标志和操作　第 1 部分：关于视觉、听觉和触觉信号的要求（IEC 61310-1:2007，IDT）

GB 18209.2—2010　机械电气安全　指示、标志和操作　第 2 部分：标志要求（IEC 61310-2:2007，IDT）

GB 18209.3—2010　机械电气安全　指示、标志和操作　第 3 部分：操动器的位置和操作的要求（IEC 61310-3:2007，IDT）

GB/T 20438.2—2006　电气/电子/可编程电子安全相关系统的功能安全　第 2 部分：电气/电子/可编程电子安全相关系统的要求（IEC 61508-2:2000，IDT）

GB/T 20438.4—2006　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（IEC 61508-4:1998，IDT）

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(IEC 61511-1:2003,IDT)

IEC 61508-3 电气/电子/可编程电子安全相关系统功能安全 第3部分:软件要求(Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements)

3 术语和定义、缩略语

3.1 按字母顺序排列的定义表

术 语	定义编号
应用软件 application software	3.2.46
体系结构限制 architecture constraint	3.2.36
体系结构 architecture	3.2.35
共同原因失效 common cause failure	3.2.43
复杂部件 complex component	3.2.8
控制功能 control function	3.2.14
危险失效 dangerous failure	3.2.40
要求 demand	3.2.25
诊断覆盖率 diagnostic coverage	3.2.38
电气控制系统 electrical control system	3.2.3
嵌入式软件 embedded software	3.2.47
失效 failure	3.2.39
故障 fault	3.2.30
容错 fault tolerance	3.2.31
全可变语言类型 full variability language (FVL)	3.2.48
功能块 function block	3.2.32
功能块元素 function block element	3.2.33
功能安全 functional safety	3.2.9
硬件安全完整性 hardware safety integrity	3.2.20
危险(来自机械的) hazard (from machinery)	3.2.10
危险状况 hazardous situation	3.2.11
高要求或连续模式 high demand or continuous mode	3.2.27
有限可变语言类型 limited variability language (LVL)	3.2.49
低复杂性部件 low complexity component	3.2.7
低要求模式 low demand mode	3.2.26
机械控制系统 machine control system	3.2.2

表（续）

术　语	定义编号
机械(机器)　machinery (machine)	3.2.1
平均失效间隔时间　Mean Time To Failure (MTTF)	3.2.34
每小时危险失效概率　probability of dangerous failure per hour (PFH_D)	3.2.28
验证试验　proof test	3.2.37
防护措施　protective measure	3.2.12
随机硬件失效　random hardware failure	3.2.44
风险　risk	3.2.13
安全失效　safe failure	3.2.41
安全失效系数　safe failure fraction	3.2.42
安全功能　safety function	3.2.15
安全完整性　safety integrity	3.2.19
安全完整性等级　safety integrity level (SIL)	3.2.23
安全相关控制功能　safety-related control function (SRCF)	3.2.16
安全相关电气控制系统　safety-related electric control system (SRECS)	3.2.4
安全相关软件　safety-related software	3.2.50
SIL 要求限度　SIL claim limit	3.2.24
软件安全完整性　software safety integrity	3.2.21
SRECS 诊断功能　SRECS diagnostic function	3.2.17
SRECS 故障反应功能　SRECS fault reaction function	3.2.18
子系统　subsystem	3.2.5
子系统元素　subsystem element	3.2.6
系统失效　systematic failure	3.2.45
系统安全完整性　systematic safety integrity	3.2.22
目标失效值　target failure value	3.2.29
确认　validation	3.2.52
验证　verification	3.2.51

3.2　术语和定义

下列术语和定义适用于本文件。

3.2.1

机械　machinery

机器　machine

由若干零、部件组合而成，其中至少有一个零件是可以运动的，并具有适当的机械操作执行机构、控制和动力电路等。它们的组合具有一定应用目的，如物料的加工、处理、搬运或包装等。

“机械”这一术语也包括机器的组合，即将同一应用目的若干台机器安排、控制得如同一台完整机器那样发挥它们的功能。

注 1：在这用的“组合”这一术语在通常意义上不仅是电气部件的组合。

注 2：改写 GB/T 15706.1—2007，定义 3.1。

3.2.2

机械控制系统　machine control system

对来自于过程、其他机械元素、操作人员或外部控制设备的输入作出响应，并且生成输出，使机械按照预定方式工作的系统。

3.2.3

电气控制系统　electrical control system

包括机械控制系统的所有电气、电子和可编程电子部件，用于提供操作控制、监控、联锁、通信、保护和安全相关控制功能。

注：安全相关控制功能可以由执行非安全相关功能的机械控制系统的一个完整的或独立的部件执行。

3.2.4

安全相关电气控制系统　Safety-related electric control system

SRECS

其失效可能导致风险立即增加的机械电气控制系统。

注：SRECS 包括由电源电路和控制电路组成的全部电气控制系统，其失效可能导致功能安全的降低或丧失。

3.2.5

子系统　subsystem

SRECS 高层结构设计的实体，其中任何子系统的失效将导致安全相关控制功能失效。

注 1：完整的子系统可能由许多可识别的及单独的子系统单元构成，一起分配到子系统执行功能块的作用。

注 2：该定义局限于 GB/T 20438.4 的一般定义：按照设计相互作用的一组元素，可能包括相互作用的硬件、软件和人。系统中的某一元素可以自成另外的系统，成为子系统。

注 3：在公开语言中，“子系统”可以指一个实体的任何细节部分。与此不同的是，本标准使用的术语“子系统”是术语学明确规定的层次范围内：“子系统”是系统的第一级细分。由子系统进一步细分而产生的部分称为“子系统元素”。

3.2.6

子系统元素　subsystem element

子系统的一部分，由单一元件或任何元件组构成。

3.2.7

低复杂性元件　low complexity component

该类元件：

——失效模式已很好确定；并且

——故障情况下的行为能完全确定。

注 1：改写 GB/T 20438.4—2006，定义 3.4.4。

注 2：在故障条件下，低复杂性元件的行为可以通过分析和/或试验方法确定。

注 3：子系统或子系统元素包含一个或多个限位开关，可能通过插入其中的机电继电器操作，一个或多个触头切断电动机就是低复杂性元件的示例。

3.2.8

复杂元件　complex component

该类元件：

——失效模式没有很好确定；或

——故障情况下的行为不能完全确定。

3.2.9

功能安全　functional safety

机械及机械控制系统的安全部分，取决于 SRECS 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—2006，定义 3.1.9。

注 2：本标准只考虑机械应用中取决于 SRECS 正确功能的功能安全。

注 3：ISO/IEC 指南 51 定义安全为免除不能接受的风险。

3.2.10

危险(来自机器的)　hazard

潜在的伤害身体或损害健康源。

注 1：改写 GB/T 15706.1—2007，定义 3.6。

注 2：危险这一术语可由其起源或预计伤害的性质(如，电击危险、挤压危险、切割危险、中毒危险、火灾危险)进行规定。

3.2.11

危险状况　hazardous situation

人员暴露于有危险的环境。

注：改写 GB/T 15706.1—2007，定义 3.9。

3.2.12

防护措施　protective measure

降低风险的措施。

注：改写 GB/T 15706.1—2007，定义 3.18。

3.2.13

风险　risk

伤害发生概率和伤害发生严重程度的综合。

[GB/T 15706.1—2007，定义 3.11]

3.2.14

控制功能　control function

评估输入信息或信号并产生输出信息或动作的功能。

3.2.15

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 15706.1—2007，定义 3.28]

注：该定义不同于 GB/T 20438.4 和 GB/T 16855.1 的定义。

3.2.16

安全相关控制功能　Safety-Related Control Function

SRCF

由具有规定的完整性等级的 SRECS 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。

3.2.17

SRECS 诊断功能　SRECS diagnostic function

预期用于检测 SRECS 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。

3.2.18

SRECS 故障反应功能　SRECS fault reaction function

当 SRECS 范围内的故障由 SRECS 诊断功能检测出时，引发该功能。

3.2.19

安全完整性　safety integrity

在所有规定情况下，SRECS 或其子系统圆满执行所要求的安全相关控制功能的概率。

注 1：改写 GB/T 20438.4—2006，定义 3.5.2。

注 2：项目的安全完整性等级越高，其未能执行所要求的安全相关控制功能的概率就越低。

注 3：安全完整性由硬件安全完整性（见 3.2.20）和系统安全完整性（见 3.2.22）组成。

3.2.20

硬件安全完整性　hardware safety integrity

SRECS 或其子系统安全完整性的一部分，包含危险的随机硬件失效概率和结构限制两方面的要求。

注：改写 GB/T 20438.4—2006，定义 3.5.5。

3.2.21

软件安全完整性　software safety integrity

SRECS 或其子系统的系统安全完整性部分，涉及软件在所有规定条件下，规定时间段内，在可编程电子系统中执行其安全相关控制功能的能力。

注 1：改写 GB/T 20438.4—2006，定义 3.5.3。

注 2：软件安全完整性一般不能精确量化。

3.2.22

系统安全完整性　systematic safety integrity

SRECS 或其子系统安全完整性的一部分，关于在危险模式下，与其阻止系统失效（见 3.2.45）有关。

注 1：改写 GB/T 20438—2006，定义 3.5.4。

注 2：系统安全完整性通常不能精确量化。

注 3：系统安全完整性要求适用于 SRECS 或其子系统的硬件和软件两方面。

3.2.23

安全完整性等级　safety integrity level

SIL

一种离散的等级（三种可能的等级之一），用于规定分配给 SRECS 安全相关控制功能的安全完整性要求。在这里，安全完整性等级 3 是最高的，安全完整性等级 1 是最低的。

注 1：改写 GB/T 20438.4—2006，定义 3.5.6。

注 2：本标准不考虑 SIL4，通常不适合与机械相关联的风险降低要求。适合 SIL4 的要求，见 GB/T 20438.1 和 GB/T 20438.2。

3.2.24

SIL 要求限度（子系统）　SIL Claim Limit（for a subsystem）

SILCL

可被称作 SRECS 子系统关于结构限制和系统安全完整性的最大 SIL。

3.2.25

要求　demand

引起 SRECS 执行 SRCF 的事件。

3.2.26

低要求模式　low demand mode

指操作模式，在该模式下，对 SRECS 提出操作要求的频率不大于每年一次或不大于两倍验证试验频率。

注：按照 GB/T 20438.1 和 GB/T 20438.2 对于低要求操作模式设计的设备，在本标准中，不适合用做 SRECS 的一部分。低要求操作模式被认为与 SRECS 的机械应用无关。

3.2.27

高要求或连续模式　high demand or continuous mode

指操作模式，在该模式下，对 SRECS 提出操作要求频率大于每年一次，或大于两倍验证试验频率。

注 1：改写 GB/T 20438.4—2006，定义 3.5.12。

注 2：低要求操作模式被认为与 SRECS 的机械应用无关。所以，在本标准里，SRECS 仅认为是工作在高要求或连

续模式。

注 3：要求模式指为了使机器转换到规定状态，安全相关控制功能只根据请求（要求）执行。对安全相关控制功能提出要求前，SRECS 不影响机械工作。

注 4：连续模式指安全相关控制功能永久（连续）执行。如 SRECS 连续控制机械和其功能会导致危险的（危险）失效。

3.2.28

每小时危险失效概率　probability of dangerous Failure per Hour

PFH_D

1 小时内危险失效平均概率。

注：PFH_D 不应与要求失效概率（*PFD*）相混淆。

3.2.29

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—2006，定义 3.5.13。

注 2：目标失效值以每小时危险失效概率的术语定义。

3.2.30

故障　fault

指异常状态，该状态可能引起 SRECS、子系统或子系统元素降低或丧失执行所要求功能的能力。

注：改写 GB/T 20438.4—2006，定义 3.6.1。

3.2.31

容错　fault tolerance

在出现故障或失效时，SRECS、子系统或子系统元素继续执行要求功能的能力。

注：改写 GB/T 20438.4—2006，定义 3.6.3。

3.2.32

功能块　function block

SRCF 最小的元素，其失效可以导致 SRCF 失效。

注 1：在本标准中，SRCF(F)可以被看作是功能块(FB)的逻辑与，如：$F=FB_1$ 与 FB_2 与 FB_n

注 2：功能块这样定义与 GB/T 15969.3 及其他标准所使用的不同。

3.2.33

功能块元素　function block element

功能块的一部分。

3.2.34

平均失效间隔时间　Mean Time To Failure

MTTF

平均失效间隔时间期望。

[IEV 191-12-07，修改]

注：MTTF 通常表示失效间隔时间的平均期望值。

3.2.35

体系结构　architecture

SRECS 中硬件和软件元素的具体配置。

注：改写 GB/T 20438.4—2006，定义 3.3.5。

3.2.36

体系结构限制　architecture constraint

一套体系结构要求，用于限制可以乘坐子系统的 SIL。

注：体系结构限制的要求见 6.7.6。

3.2.37

验证试验　proof test

在 SRECS 系统及其子系统中，该试验可以检测其故障和降级，如必要，以便 SRECS 及其子系统可以回复到“新”状况或尽量接近该状况。

注 1：改写 GB/T 20438.4—2006，定义 3.8.5。

注 2：验证试验用于确认 SRECS 是否处于保证规定的安全完整性状态。

3.2.38

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—2006，定义 3.8.6。

注 2：诊断覆盖率（*DC*）可用下列公式计算：

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

其中，λ_{DD} 为检测到的危险硬件失效比率，λ_{Dtotal} 为总的危险硬件失效比率。

3.2.39

失效　failure

SRECS、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—2006，定义 3.6.4 和 GB/T 15706.1—2007，定义 3.32。

注 2：失效是随机的（硬件）或系统的（硬件或软件）。

3.2.40

危险失效　dangerous failure

使 SRECS、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—2006，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 SRECS 的危险失效概率不会比构成 SRECS 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。

3.2.41

安全失效　safe failure

SRECS、SRECS 子系统或 SRECS 子系统元素的失效不引起潜在的危险。

注 1：改写 GB/T 20438.4—2006，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。

3.2.42

安全失效系数　Safe Failure Fraction

SFF

不会导致危险失效的子系统整体失效率系数。

注：安全失效系数（*SFF*）可用下列公式计算：

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

式中：

λ_S　——安全失效比率；

$\Sigma\lambda_S + \Sigma\lambda_D$　——整体失效比率；

λ_{DD}　——诊断功能检测的危险失效比率；

λ_D　——危险失效比率。

在计算随机硬件失效概率时考虑了 SRECS 中每个子系统的诊断覆盖率（如果有）；在确定硬件安全完整性的结构体系限制时已经考虑了安全失效系数（见 6.7.7）。

3.2.43

共同原因失效　Common Cause Failure

CCF

一种失效，它是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—2006，定义 3.6.10。

注 2：该定义与 GB/T 15706.1 和 IEV 191-04-23 给出的不同。

3.2.44

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—2006，定义 3.6.5。

3.2.45

系统失效　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—2006，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。

3.2.46

应用软件　application software

由 SRECS 设计人员研发的特定应用的软件，一般包含逻辑流程图、限制条件以及用于控制适当输入、输出、计算和决定的表达式，以满足 SRECS 的功能要求。

3.2.47

嵌入式软件　embedded software

软件，由制造商提供。该软件是 SRECS 的一部分，通常不能修改。

注：固件和系统软件为嵌入式软件的例子。

3.2.48

全可变语言　Full Variability Language

FVL

语言的一种类型，可提供实现多种功能和应用的能力。

注 1：改写 GB/T 21109.1—2007，定义 3.2.81.1.3。

注 2：使用 FVL 系统的典型的例子是通用计算机。

注 3：FVL 通常用于嵌入式软件，很少用于应用软件。

注 4：FVL 例子包括：Ada、C、Pascal、指令表、汇编语言、C^{++}、Java、SQL。

3.2.49

有限可变语言　Limited Variability Language

LVL

语言的一种类型，为实现安全要求规范提供组合预定的、应用特定的、库功能的能力。

注 1：改写 GB/T 21109.1—2007，定义 3.2.81.1.2。

注 2：LVL 提供与要求功能相一致的接近功能以获得应用。

注 3：GB/T 15969.3 给出 LVL 典型例子。它们包括梯形图、功能方块图和顺序功能图。LVL 不考虑指令表和结构文本。

注 4：使用 LVL 的系统典型例子：为机械控制配置的可编程逻辑控制器(PLC)。

3.2.50

安全相关软件　safety-related software

在安全相关系统中，用于实现安全相关控制功能的软件。

3.2.51

验证　verification

通过检查(如试验、分析)，证实 SRECS、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—2006，定义 3.8.1 和 GB/T 21109.1—2007，定义 3.2.92。

注 2：验证结果应提供证明文档作为客观性凭证。

示例：验证活动包括：

——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。

3.2.52

确认　validation

通过检查(如试验、分析)证实 SRECS 满足具体应用的功能安全要求。

注：改写 GB/T 20438.4—2006，定义 3.8.2。

3.3　缩写

CCF	共同原因失效 Common Cause Failure (s)
DC	诊断覆盖率 Diagnostic Coverage
EMC	电磁兼容性 Electromagnetic Compatibility
FB	功能模块 Function Block
FVL	全可变语言 Full Variability Language
I/O	输入/输出 Input/Output
LVL	有限可变语言 Limited Variability Language
PFH_D	每小时危险失效概率 Probability of dangerous Failure per Hour
MTTF	平均失效间隔时间 Mean Time To Failure
MTTR	平均恢复时间 Mean Time To Restoration
P_{TE}	危险传输错误概率 Probability of dangerous Transmission Error
SFF	安全失效系数 Safe Failure Fraction
SIL	安全完整性等级 Safety Integrity Level
SILCL	安全完整性等级(SIL)要求限度(针对子系统) Safety Integrity Level (SIL) Claim Limit (for subsystems)
S-R	安全相关 Safety-Related
SRECS	安全相关电气控制系统 Safety-Related Electrical Control System
SRCF	安全相关控制功能 Safety-Related Control Function
SRS	安全要求规范 Safety Requirements Specification
SYS	系统 System

4 功能安全管理

4.1 目的

本条规定了为了达到 SRECS 所要求的功能安全所必需的管理和技术工作。

4.2 要求

4.2.1 对于每个 SRECS 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 章至第 9 章上规定的运行控制程序。

注 1：功能安全计划内容应按照根据具体情况而定，其中包括：

——项目规模；

——复杂程度；

——设计和技术新颖程度；

——设计特点标准化程度；

——如果失效可能的后果。

该计划尤其应注意下列各项：

a) 确定第 5 章至第 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、验证和确认的功能安全的策略。

d) 确定第 5 章至第 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 SRECS 功能安全相关的信息。

注 2：应考虑下列因素：

——危险识别和风险评价的结果；

——用于安全相关功能及其安全要求的设备；

——负责维护功能安全的机构；

——达到和保持功能安全（包括 SRECS 修改）所需的程序。

f) 描述考虑相关机构问题时的配置管理（见 9.3）策略，例如被授权的人及该机构的内部结构。

g) 建立验证计划，应包括：

- 进行验证的细节；
- 执行验证的人员、部门或单位的详细情况；
- 验证策略和技术的选择；
- 试验设备的选择和使用；
- 验证活动的选择；
- 验收准则；
- 用于评估验证结果的方法。

h) 建立确认计划，其中包括：

- 进行确认的细节；
- 机器操作有关模式（如正常操作、设置）的确定；
- 对照受验证的 SRECS 的要求；
- 适用于确认的技术策略，例如分析方法或统计试验；
- 验收准则；
- 出现失效时采取的行动，以满足验收要求。

注 3：确认计划应指出 SRECS 及其子系统是否进行常规测试、型式测试及/或抽样测试。

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

——第 5 章至第 9 章规定的活动；

——验证活动；

——确认活动。

5 安全相关控制功能规范要求(SRCF)

5.1 目的

本条规陈述程序，它规定由 SRECS 执行 SRCF 要求。

5.2 SRCF 要求规范

5.2.1 概述

5.2.1.1 依据 GB/T 15706.1、GB/T 15706.2 和 GB/T 16856 提出的风险降低策略，安全功能的任何需要将可能被确定。

5.2.1.2 如果被选择的安全功能由 SRECS 执行(全部或部分地)，那么，应规定相关 SRCF(见 3.2.16)。

5.2.1.3 各 SRCF 规范应包括：

——功能要求规范(见 5.2.3)；

——安全完整性要求规范(见 5.2.4)。

上述项目应在安全要求规范(SRS)中形成文件。

注 1：当非电气设备结合电气手段来执行安全功能时，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(见 9.3)。

5.2.1.4 安全要求规范应该经过验证确保在预期应用中的一致性和完整性。

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

5.2.2 可用信息

应使用下列信息来制定各 SRCF 功能要求规范和安全完整性要求规范：

——机器风险评价结果应包括针对各种特定危险的风险降低过程所必需的所有安全功能；

——机器操作特性，包括：

- 操作模式；
- 循环时间；
- 响应时间性能；
- 环境条件；
- 人机交互(例如修理、设置、清洁)；

——所有和 SRCF 相关的信息，都可能影响 SRECS 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 SRECS 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

SRECS 安全要求规范。

5.2.3 SRCF 功能要求规范

5.2.3.1 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)；

——可能是同时激活，但会造成冲突动作的那些功能之间的优先权；

——各个 SRCF 的工作频率；

——各 SRCF 要求的响应时间；

——SRCFs 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；

——故障反应功能以及例如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。

5.2.3.2 除了 GB/T 17799.2 要求外，当 SRECS 计划用于工业环境时，电磁(EM)抗扰度等级在附录 E 有规定。计划用于另外的 EM 环境的 SRECS(例如住宅)应具有其他的 EMC 标准规定的抗扰度等级(例如住宅环境，应具有 GB/T 17799.1)。

注 1：在规定 EM 抗扰度等级时，需要考虑在不同的 EMC 标准中的使用的等级是否涵盖了 SRECS 应用中可能发生的情况，即使这种情况发生概率很低。

注 2：SRECS 功能安全的 EM 抗扰度性能准则见 6.4.3。

5.2.4 SRCF 的安全完整性要求规范

5.2.4.1 每个 SRCF 的安全完整性要求应来自风险评价，以确保达到必要的风险降低。在本标准中，安全完整性要求表示为 SRCF 每小时危险失效概率的目标失效值。

5.2.4.2 每个 SRCF 的安全完整性要求应按照表 3 依照 SIL 规定并形成文档。方法实例见附录 A。

表 3 安全完整性等级：SRCF 目标失效值

安全完整性等级(SIL)	每小时危险失效概率(PFH_D)
3	$\geqslant 10^{-8} \sim < 10^{-7}$
2	$\geqslant 10^{-7} \sim < 10^{-6}$
1	$\geqslant 10^{-6} \sim < 10^{-5}$

注：当要求的 SRCF 安全完整性低于 SIL1 时，应满足 GB/T 16855.1 B 最低要求的 B 类。

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

6 安全相关电气控制系统设计与整合(SRECS)

6.1 目的

本条款规定 SRECS 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(见 5.2)。

6.2 一般要求

6.2.1 SRECS的选择或设计应符合安全要求规范(见5.2)和有关软件安全要求规范(见6.10),并考虑本标准的适当要求。

6.2.2 SRECS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)应符合6.5或6.6。不管使用哪种方法,SRECS均应符合下列要求:

a) 硬件安全完整性要求,包括:
   - 硬件安全完整性体系结构限制(见6.6.3.3);
   - 随机硬件危险失效概率要求(见6.6.3.2);

b) 系统安全完整性要求(见6.4),包括:
   - 失效避免要求;
   - 系统故障控制要求;

c) 对故障检测SRECS行为要求(见6.3);

d) 安全相关软件设计和开发要求(见6.10和6.11)。

6.2.3 SRECS设计应考虑人的能力和局限(包括可合理预见的误操作),且分配给操作人员、维护人员和其他可能与SRECS交互的人员的工作合适。所有操作员界面的设计应遵循良好人为因素的惯例(见GB/T 18209系列),并应提供合适等级的培训和操作员知识,尤其对大批量生产的子系统,其操作员可能是公众成员。

注:设计目标应是防止或消除由操作人员或维护人员所造成的可合理遇见错误。如不可能,应采用其他方法(例如完成前用手动再次确认),将操作员错误的可能性将至最低,保证可预见错误不会导致风险增加。

6.2.4 在设计和集成时,应考虑可维护性和可测试性,以便执行SRECS的这些特性。

6.2.5 SRECS设计,包括诊断和故障反应功能,应形成文件。文件应:

——精确、完整、简明;

——适合预期目的;

——可存取、可维护;

——版本可以控制。

6.2.6 在SRECS设计、开发和执行期间,执行的工作结果应在适当阶段验证。

6.3 检测SRECS故障时的行为(SRECS的)要求

6.3.1 硬件容错大于零的任何子系统的危险故障检测可导致特定故障反应功能的运行。

在故障部分修理期间,规范可以允许隔离子系统的故障部分以便机器可以继续安全操作。在这种情况下,如故障部分未在估计的最长,即假设以随机硬件失效概率(见6.7.8)计算的时间内修理,那么,应执行第二故障反应,以保持安全状态。

如SRECS在最初设计为在线维修时,隔离故障部分只能在SRS规定的部分而不增加SRECS随机硬件危险失效概率的情形下使用。

在硬件已经没有容错的能力的故障出现后,应采用6.3.2的规定。

注:在可靠性模式下,恢复系统运行的平均时间(见IEV 191-13-08)需要考虑诊断试验间隔、维修时间以及恢复前的任何其他迟延。

6.3.2 需要故障诊断功能以得到需要的随机硬件危险失效概率和子系统为零容错的场合,故障检测和规定的故障反应在SRCF产生的危险情况可能出现前执行。

例外(对于6.3.2):就执行特定SRCF子系统而言,如硬件容错率为零且诊断试验率与要求的比率之比超过100,那么,该子系统的诊断试验间隔应能使子系统满足随机硬件危险失效概率的要求。

6.3.3 故障反应功能作为 SRCF 的一部分被规定为 SIL3，该故障反应导致机器停止，继而，通过 SRECS 的机器正常操作(例如使机器重新启动)将不可能进行，直到该故障已经修复或校正。对于规定的安全完整性低于 SIL3 的 SRCF，故障反应功能(例如重启正常操作)执行后机器的行为应根据有关故障反应功能规范而定(见 5.2.3)。

6.4 SRECS 系统安全完整性要求

注：这些要求在“系统级”应用，在该级别，子系统互连以实现 SRECS。有关子系统实现的相关要求见 6.7.8。

6.4.1 避免系统硬件失效的要求

6.4.1.1 应采取以下措施：

a) SRECS 应按照功能安全计划设计和执行(见 4.2)；
b) 子系统的适当选择、组合、安排、组装、安装，包括电线、电缆以及任何内部连接；
c) 按照制造商规范使用 SRECS；
d) 使用制造商的应用说明书，例如目录表、安装说明书和使用良好的工程惯例(见 GB/T 16855.2，D.1)；
e) 使用具有可兼容操作特性的子系统(见 ISO 13849-2，D.1)；
f) SRECS 应按照 GB 5226.1 予以保护；
g) 按照 GB 5226.1 规定防止功能接地的损失；
h) 不应使用部件工作未加说明的模式(例如可编程设备的“保留”寄存器)；
i) 考虑可预见的误用、环境变化或更改。

6.4.1.2 另外，考虑到 SRECS 的复杂性和由 SRECS 执行这些功能需要的 SIL，至少应采用下列一项技术和/或措施：

a) SRECS 硬件设计审查(例如检查或浏览)：通过审查和/或分析，找出规范和执行之间的差异；

注 1：为了揭示规范与执行之间的差异，与实现、执行和产品使用相关的任何疑点或潜在弱点应以文档记录，以期能得到解决；考虑到，对于检查程序，作者是被动的，而检查员是主动的，而在程序上，作者是主动的，检查员是被动的。

b) 咨询工具诸如模拟或分析的计算机辅助设计包装能力和/或为执行系统设计程序使用的计算机辅助设计工具，该计算机辅助设计工具带可用的和已经试验过的预设计元素；

注 2：这些工具的完整性可以通过具体测试、或广泛的使用满意的历史、或通过独立的正在设计的特定的 SRECS 输出验证予以证明。见 6.11.3.4。

c) 模拟：按照子系统的性能和正确的计算以及其子系统交互作用，执行 SRECS 设计的系统性和完整性同一化。

示例：SRECS 功能可以通过软件行为模式在计算机上模拟(见 6.11.3.4)，如单独的子系统或子系统元素具有各自的模拟行为，它们连接的线路响应通过查看各个子系统或子系统元素的页边数据进行检查。

6.4.2 系统性故障的控制要求

应采取下列措施：

a) 掉电的使用：SRECS 应予以设计该功能，以使在失去供电时，可以达到或保持机器的安全状态；
b) 控制临时子系统失效影响的措施：SRECS 应按下列方式设计，如：
——单独子系统或子系统的一部分的电压变化(例如中断，电压降)不会导致危险(例如电压中断将影响电动机的电路，而不应在电源恢复时，造成意外启动)。

注 1：见 GB 5226.1 的有关要求。

特别是:过电压或欠电压应尽早查明,这样,可以通过掉电程序或切换到第二个动力单元使所有输出可以转换到安全状态;

必要时,过电压或欠电压应尽早查明,内部状态可以保存在非易失性存储器中,这样,可以通过掉电程序使所有输出设置为安全状态,或通过掉电程序或切换到第二个动力单元使所有输出可以转换安全状态。

——来自物理环境或子系统的电磁干扰影响不会导致危险;

c) 为控制来自任何数据通信过程(包括传输差错、重复、删除、插入、重新排序、程序或数据残缺、延迟和假消息)所引起的错误影响和其他影响的措施;

注 2:更多信息见 GB/T 18657.1、GB/T 24339.1、EN 50159-2 和 GB/T 20438.2。

注 3:术语"假消息"指的是信息的真实内容未经正确鉴别。例如,从不安全的组件发来的消息被错误地鉴别为来自安全组件的消息。

d) 当危险故障在某个界面出现时,在因该故障可能出现而造成的危险前,应执行故障反应功能。当使硬件容错降低至零的故障发生时,该故障反应应在估计的 MTTR(见 6.7.4.4.2g)超过时发生。

列项 d)要求适用于子系统和子系统的所有其他部分输入、输出的界面(例如,光帘的输出信号切换设备,防护装置位置传感器的输出),该子系统集成时包含或需要电缆连接。

注 4:不要求对其自身的子系统或子系统元素必须检测它的输出故障。在诊断测试执行后,故障反应功能也可以由后续的任何子系统引发。

6.4.3 电磁(EM)抗扰度

除 GB/T 17799.2 和附录 E 给出的 EM 现象外,SRECS 应满足以下功能安全性能准则:

——不应引进非安全条件或危险;

——不损失 SRCF;

——由可能会受到暂时或永久骚扰的 SRECS 来执行 SRCF,则应在危险可能出现前,达到或维持机械的安全状态。若 EM 现象可能导致元件破坏,应(例如通过分析)确保功能安全不受影响,包括通过降低会造成局部破坏的 EM 现象的值。

注:对应 EM 现象在附录 E 给出的所有值而考虑 SRECS 的行为。

6.5 安全相关电气控制系统选择

若供方对 SRECS 提供安全要求规范涉及的特别功能,可以选择满足安全要求规范以及 6.3、6.4 和 6.6.1 的预设计的 SRECS,而不用客户设计。

注:预设计的 SRECS 是根据 6.6 中专用 SRECS 设计与开发的一种可选选择。

6.6 安全相关电气控制系统(SRECS)设计和开发

6.6.1 一般要求

6.6.1.1 SRECS 应按照 SRECS 安全要求规范设计和开发(见 5.2)。

6.6.1.2 应遵照明确的结构化设计过程并形成文件(见 6.6.2)。

6.6.1.3 在检测出故障时,如有必要使用诊断以达到要求的安全完整性,SRECS 应执行规定的故障反应功能(见 5.2 和 6.3)。

6.6.1.4 如果 SRECS 或 SRECS 的一部分(即其子系统)既要执行 SRCF,还要执行其他功能,那么应该认为其硬件、软件在安全上是相关的,除非它可以显示执行 SRCF 和其他功能之间是充分独立的(即

正常操作或任何其他功能的失效不影响 SRCF)。

注：执行的充分独立可以通过显示非安全和安全相关部分之间的相关失效概率等同于 SRECS 的安全完整性等级来确定。

6.6.1.5 对于执行不同安全完整性等级的安全相关控制功能的 SRECS 或其子系统，其硬件、软件应要求最高安全完整性等级，除非它能显示执行不同安全完整性等级的安全相关控制功能是充分独立的。

注：执行时的充分独立性可以通过显示执行不同完整性等级的 SRCFS 的部分之间的依赖性失效概率等同于由 SRECS 取得的安全完整性等级来确定。

6.6.1.6 非数字数据通信的互联(例如电线、电缆)应被视为与其相连接的某个子系统的一部分(见 6.4.2 中 d))。

6.6.1.7 当数字数据通信用作 SRECS 执行的一部分时，它应按照 SRCF 的 SIL 目标满足 GB/T 20438.2 的有关要求。

6.6.1.8 SRECS 的使用信息应规定 SRECS 设计年限必需的技术和措施，以保持其安全完整性等级。

6.6.2 设计和开发过程

设计和开发应遵照明确规定的程序，应考虑由图 2 所示过程包含的所有方面。

注：本标准的方法是从安全要求规范规定的要求开始，对 SRECS 采用结构化设计程序。图 3 显示该设计过程的工作流程和适用于不同层面的术语。

6.6.2.1 系统结构设计

6.6.2.1.1 SRECS 安全要求规范内规定的各个 SRCF 应分解成功能块结构，如图 3 所示。该结构应形成文档，包含下列内容：

——结构描述；

——各功能块安全要求(功能、完整性)；

——各功能块输入和输出定义。

注 1：分解过程应面向全面描述 SRCF 的功能和完整性要求的功能块结构。该过程应向下加至这一层面，它允许将各功能块确定的功能和完整性要求配置到各子系统，在该场合下，将功能块的完整功能要求配置到子系统是可能的。然而，虽然将多个功能块配置到单一子系统是可能的，但不可能将一个功能块配置到几个具有单独功能和完整性要求的子系统中。欲配置一个功能块的功能要求到冗余子系统元素，见 6.7.4。

注 2：各功能块的输入输出是传输信息，例如速度、位置、操作模式等。

注 3：功能块是 SRCF(见 3.2.16)的功能表示，不包括 SRECS 的诊断功能(见 3.2.17)。针对本标准，诊断功能被认为是单独的功能，对于 SRCF(见 6.8)，可以拥有不同的结构。

6.6.2.1.2 SRECS 体系结构的初始概念应按照功能块结构创建。

注：安全相关控制体系结构的开发商，负责设备配置的机构以及软件开发者之间应进行协作。由于软件安全要求和可能的软件结构变得更加精确，可能对 SRECS 硬件结构造成影响。由于这个原因，只有 SRECS 结构设计人员、子系统供方、软件开发者以及机械设计人员(必要时)或用户之间的密切合作才有助于减少潜在的系统失效。

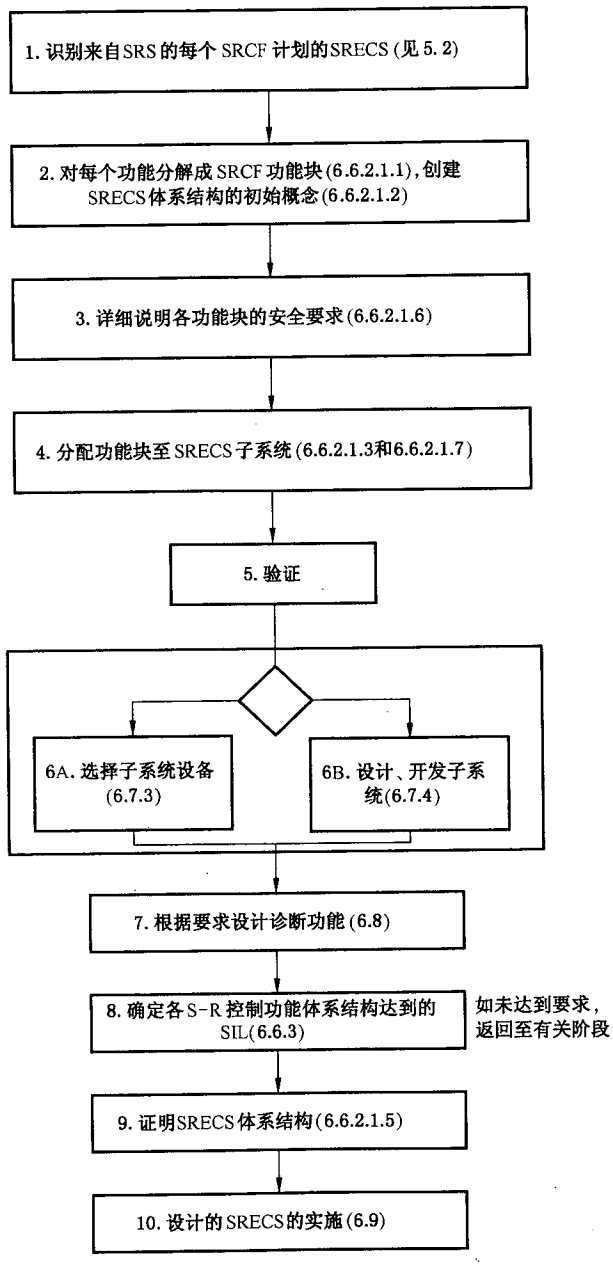


图 2　SRECS 设计和开发过程的工作流程

6.6.2.1.3　各功能块应配置到 SRECS 体系结构内的子系统。一个以上的功能块可以配置到一个子系统。

6.6.2.1.4　每个子系统和为该子系统配置的功能块应清楚识别。

6.6.2.1.5　体系结构应设文档,描述其子系统和相互关系。

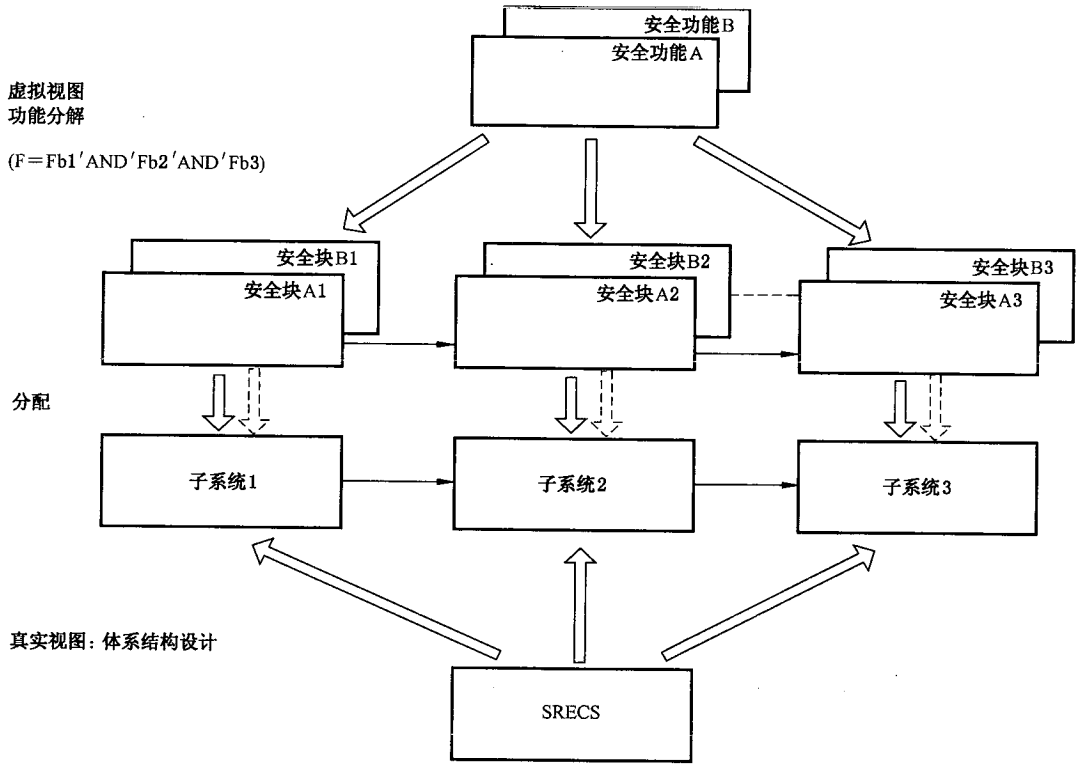


图 3　子系统的功能模块安全要求配置(见 6.6.2.1.1)

6.6.2.1.6　各功能块的安全要求应按对应 SRCF 的安全要求规范中的规定，依照：

——功能要求(例如输入信息、内部操作(逻辑)和功能块输出)；

——安全完整性要求。

6.6.2.1.7　子系统的安全要求应是为其配置的各个功能模块的安全要求。如果为子系统配置多个功能块，那么最高的完整性要求适用(见 6.6.3)。这些要求应形成文档并作为子系统安全要求规范。

6.6.3　SRECS 安全完整性评估要求

6.6.3.1　概述

由 SRECS 实现的 SIL，对于每一个 SRCF 应认为由 SRECS 分别完成。

由 SRECS 完成的 SIL 应由子系统的危险随机硬件失效概率、体系结构限制和构成 SRECS 的子系统的系统安全完整性来确定。已实现的 SIL 小于或等于系统安全完整性和体系结构限制的任何子系统的最低 SILCLs 值。

6.6.3.2　硬件安全完整性

6.6.3.2.1　由于危险随机硬件失效而导致的各 SRECS 的危险失效概率应等于或小于安全要求规范规定的目标失效值。

注：与 SIL 相关的目标值在表 3 中列出。

6.6.3.2.2　由于危险随机硬件失效而导致的各 SRECS 危险失效概率的评估，考虑下列因素：

a)　与各 SRCF 相关的 SRECS 的体系结构在考虑中；

注：这包括子系统的哪些失效模式是串行配置(即任何失效引起相关要执行的 SRCF 的失效)和哪些是并行(冗余)配置(即同时发生的失效)。

b)　各子系统其各个分配功能块的失效率的估计值，在任何模式为执行其配置的功能块可能会引

起 SRECS 的危险失效。

6.6.3.2.3 危险失效概率的评估应基于各相关子系统危险随机硬件失效概率，源于使用 6.7.2.2 要求的信息，对于子系统之间的数字数据通信过程，如适用，包括 6.7.2.2(k)。SRECS 的危险随机硬件失效概率为参与执行 SRCF 的所有子系统危险随机硬件失效概率的和，适当时，还应包括数字数据通信过程危险传输错误的概率：

$$PFH_D = PFH_{D1} + \cdots + PFH_{Dn} + P_{TE}$$

注 1：该方法以功能块定义为基础，它表明任何功能块失效将会导致 SRCF 失效(见 3.2.16)。

注 2：除了数字数据通信以外的互联被认为是子系统的一部分。

6.6.3.3 体系结构限制

根据体系结构限制，由 SRECS 实现的 SIL 小于或等于参与执行 SRCF 的任何子系统的最低 SILCL(见 6.7.6)。

注：例如，SRECS 包括两个串联的子系统(子系统 1 和子系统 2)，假设 SFF 和各子系统容错率如表 4 所示。对于 SRECS 评估的 PFH_D 为 8×10^{-8}，相当于 SIL3。但是，根据表 5，子系统 2 的体系结构限制可能由 SRECS 实现的 SIL 限定为 SIL2。

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)

子系统	硬件容错	SFF	根据体系结构的 SIL 要求限制(见表 5)
1	1	95%	SIL3
2	1	80%	SIL2

6.6.3.4 系统安全完整性

SRECS 实现的 SIL 小于或等于参与执行 SRCF 的任何子系统的最低 SILCL。

注：按照 6.7.4 实现的子系统的系统安全完整性，以 6.7.9 描述的措施给定 SILCL 为 SIL3。

6.7 子系统实现

6.7.1 目标

目标是实现子系统满足其配置的功能块的所有安全要求(见图 3)。可以考虑两种方法。

——选择足以满足该子系统的要求的设备，即应该满足配置功能块的各安全要求规范和本标准的要求；

——通过组合功能块元素和规定他们如何安排及交互，进行子系统的设计和开发。

6.7.2 子系统实现的一般要求

6.7.2.1 子系统应按照其安全要求规范(见 6.6.2.1.7)通过选择(见 6.7.3)或设计(见 6.7.4)来实现，并考虑 6.2 的所有要求。包含复杂部件的子系统，对于要求的 SIL，适当时，应遵照 GB/T 20438.2 和 IEC 61508-3 的规定。

例外：子系统设计包含了复杂部件作为子系统元素的场合，可采用 6.7.4.2.3。

6.7.2.2 下列信息应适用于各个子系统：

a) SRCF 使用的子系统的功能规范和界面；

b) 任何模式下声明的评估失效率(源于随机硬件失效)，它可能引起 SRECS 的危险失效；

注 1：对于机电子系统，应考虑制造商声明的工作周期数和工作循环(见 5.2.3)后进行失效概率估计。该信息应基于 B_{10} 值(即总体 10%的预计时间将失效)。也见 IEC 61810-2。

c) 子系统限制：

——应观察环境和工作条件，以保持评估的失效率的有效性，该失效率归因于随机硬件失效；

——不应超过子系统寿命，以保持评估的失效率的有效性，该失效率归因于随机硬件失效。

d) 任何试验和/或维护要求；

e) 诊断覆盖率和诊断测试的时间间隔(必要时，见注 2)；

注 2：e)项涉及子系统外部诊断功能。在 SRECS 可靠性模型中，子系统执行的诊断功能的行为需要信用保证时，才需要该信息。

f) 任何必要的附加信息(例如修理次数)，从而能够按照诊断学故障检测推算平均维修时间(MTTR)。

注 3：需要 b)～f)项以估计 SRCF 每小时失效概率。

g) 由于体系结构限制造成的 SILCL(见 6.7.6)或；

——能够推导出应用于 SRECS 的子系统的安全失效系数(SFF)所需的所有信息；和

注 4：要求的信息是子系统可能的失效模式。根据子系统失效模式，可以确定子系统失效是否引起 SRECS 安全或危险失效。

注 5：有关 SFF 评估的细节，见 6.7.7。

——子系统硬件失效容错；

h) 为避免系统失效应遵守对子系统应用上的任何限制；

i) 对使用子系统的 SRCF 可能具备的最高安全完整性等级依据下列因素：

——在子系统硬件、软件设计和执行期间用于预防系统故障而采用的措施和技术；

——预防系统故障的子系统容错设计特点。

注 6：需要 h)和 i)项以根据体系结构限制确定 SRCF 可能具有的最高安全完整性等级。而且，这些项目能够用于对 GB/T 16855.1 在故障检测和硬件容错两方面的安全类别要求提供链接(见表 4、表 5)。

j) 为了能够按照 6.11.3.2 对 SRECS 进行配置管理，需要识别子系统硬件、软件配置的所有信息；

k) 数字数据通信过程中危险传输错误概率(如适用)。

6.7.3 选择现有(预设计)子系统的要求

6.7.3.1 如供方为安全规范涉及的专用 SRCF 提供子系统，则可能选择这类预设计子系统而不用客户设计，只要它满足子系统的安全要求规范、6.4.3 和 6.7.3.2 或 6.7.3.3。

6.7.3.2 为了适合所要求的 SIL，包括复杂部件的子系统应遵照 GB/T 20438.2 和 IEC 61508-3。

例外：如子系统设计包括作为子系统元素的复杂部件，6.7.4.2.3 适用。

6.7.3.3 只包括低复杂性部件的子系统应遵照本标准的 6.7.4.4.1、6.7.6.2、6.7.6.3、6.7.7、6.7.8 和 6.8。

6.7.4 子系统设计和开发

6.7.4.1 目标

6.7.4.1.1 第一个目标是设计满足配置功能块安全要求的子系统。

6.7.4.1.2 第二个目标是按照以组合方式一起工作的子系统元素创建体系结构，以满足配置给子系统的所有功能块的功能和安全完整性要求。

6.7.4.2 一般要求

6.7.4.2.1 子系统应按照其安全要求规范设计。

6.7.4.2.2 子系统应符合下列 a)～c)的所有要求：

a) 硬件安全完整性的要求包括：

——硬件安全完整性的体系结构限制(见 6.7.6);

——危险随机硬件失效概率的要求(见 6.7.8)。

b) 系统安全完整性要求包括:

——避免失效的要求(见 6.7.9.1),和系统故障控制的要求(见 6.7.9.2);

——设备在使用中经验证的资料。如果这样,子系统应满足 GB/T 20438.2 的有关要求(见 GB/T 20438.2中 7.4.7.5～7.4.7.12)。

c) 故障检测时子系统行为的要求(故障反应)(见 6.3)。

6.7.4.2.3 包含复杂部件(作为子系统元素)的子系统设计时,且部件满足 GB/T 20438.2 和 IEC 61508-3的有关 SILCL 的所有相关要求,在子系统设计上下文中,它可以被看作低复杂部件,因为其相关失效模式、故障检测行为、失效率和其他安全相关信息均已知。这类部件应只能按照其规范和供方提供的相关使用信息使用。

6.7.4.3 子系统设计和开发过程

子系统设计和开发应遵循明确规定的程序,考虑图 4 所示程序包含的所有方面。

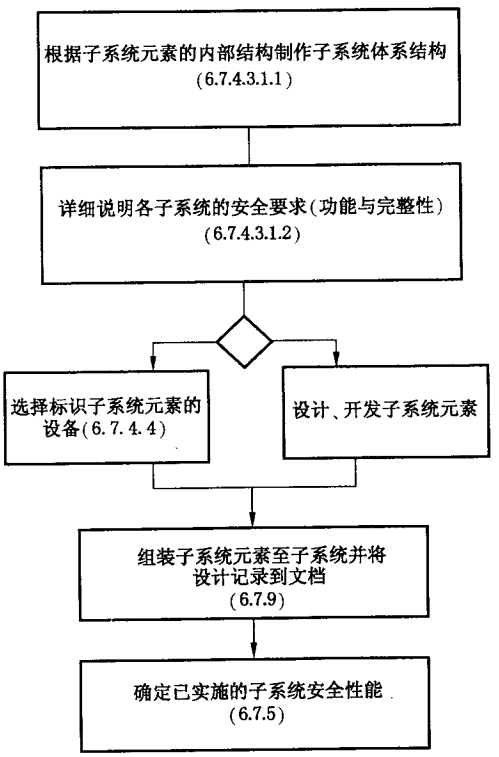


图 4 子系统设计和开发流程(见图 2 的 6B 框)

6.7.4.3.1 子系统体系结构设计

6.7.4.3.1.1 在子系统体系结构设计期间,分解过程应通向完全代表功能块的功能要求的功能块元素的结构。该过程应一直应用到配置给子系统元素的各功能块元素确定的功能要求容许的等级。(见图 5 示例)。

注:设计过程工作流程如图 4 所示。

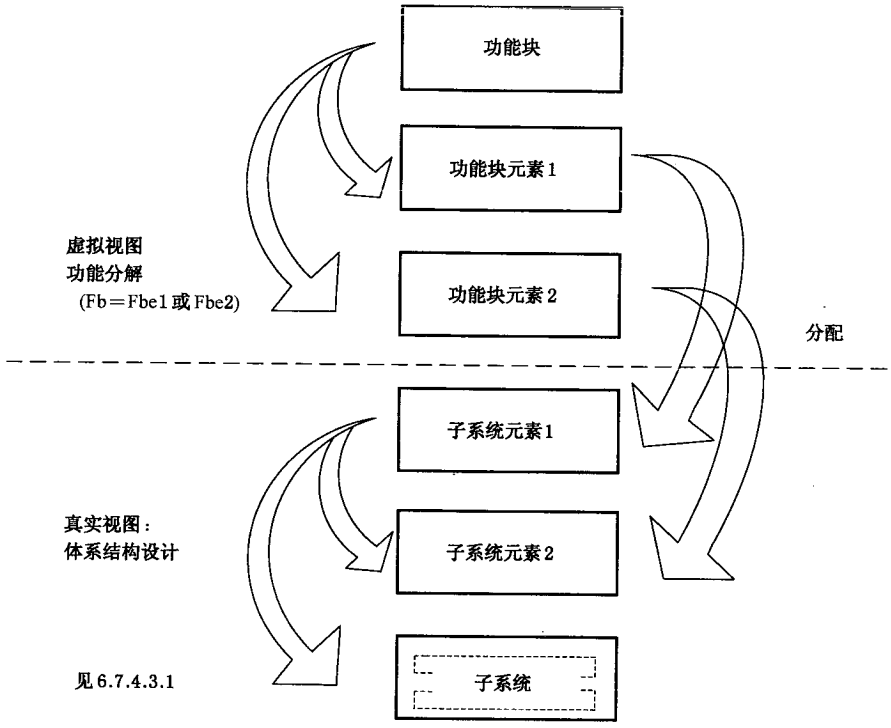


图 5　功能块分解成冗余功能块元素和其相关的子系统元素

6.7.4.3.1.2　子系统体系结构应根据其元素和相互关系形成文件。必要时，还应包括配置到子系统元素的功能块元素相关的信息。

6.7.4.4　子系统元素选择和设计要求

6.7.4.4.1　子系统元素应适合它们的预定用途，并应符合现有的相关国际标准。

6.7.4.4.2　各子系统元素应有下列信息：

a)　子系统元素功能规范；

b)　子系统元素界面规范(如电气特性)；

c)　每个失效模式及其发生概率(例如按照 6.7.4.2.3 使用的复杂部件)、诊断覆盖率和危险失效概率。

注：对于机电子系统，失效概率应考虑制造商公布的工作周期数和应用的工作循环(见 5.2.3)进行评估。该信息应基于 B_{10} 值(即总体 10%失效的预计时间)。见 IEC 61810-2。

d)　子系统元素的限制：

——为维护 c)项所提供的信息的有效性应遵守的环境和工作条件；

——为维护 c)项所提供的信息有效性不应超过子系统元素的寿命；

e)　任何周期验证试验和/或维护要求；

f)　有助于诊断的特点(例如机械连接的触点)；

g)　任何必须的附加信息(例如修理次数)，从而能够按照诊断学故障检测推算平均恢复时间(MTTR)；

h)　为避免系统失效应遵守的子系统元素应用方面的任何限制；

i)　硬件容错。

6.7.5 子系统安全性能确定

子系统的安全性能由其体系结构约束(6.7.6)所确定的 SILCL 来描述,而它的 SILCL 归因于系统完整性(6.7.9)和它的危险随机硬件失效率(6.7.8)。

注 1:子系统的 SILCL 为该子系统使用的安全相关控制功能所要求的最大安全完整性等级设置极限。

注 2:需要所有关于这 3 方面的信息,以确定由执行配置的 SRCF 的安全相关控制系统所实现的 SIL。

6.7.6 子系统硬件安全完整性的体系结构限制

6.7.6.1 联系硬件安全完整性的上下文,SRCF 可能要求的最高安全完整性等级受限于硬件容错和执行 SRCF 的子系统的安全失效系数。表 5 规定了 SRCF 可能要求的最高安全完整性等级,该 SRCF 使用的子系统考虑到硬件容错和安全失效系数。表 5 所示体系结构限制适用于各子系统。鉴于以下这些体系结构限制:

a) N 的硬件容错指 $N+1$ 个故障可能引起的 SRCF 丧失。确定硬件容错时,不考虑可能控制故障影响的其他措施,例如诊断;

b) 一个故障直接导致一个或多个相继故障的发生,这些应视为单一故障;

c) 确定硬件容错时,可以排除某些故障,只要其涉及子系统安全完整性要求的事物发生的可能性很低。任何这类故障的排除应证明是对的,并形成文档(也见 6.7.7)。

6.7.6.2 表 5 的体系结构限制应适用于执行 SRCF 功能块的各个子系统。

6.7.6.3 只包含单一子系统元素的子系统应满足表 5 的要求。特别是,对于硬件零容错(即 $N=0$)的子系统,99%以上的 SFF 应通过 SRECS 诊断功能来实现。

注:为了证明 SIL3 的 SILCL,该要求是必须的,以确保体系结构限制的适当形式应用于那些只包含单一子系统元素的子系统。

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

安全失效系数	硬件容错(见注 1)		
	0	1	2
<60%	不允许(见注 3)	SIL1	SIL2
60%~<90%	SIL1	SIL2	SIL3
90%~<99%	SIL2	SIL3	SIL3(见注 2)
≥99%	SIL3	SIL3(见注 2)	SIL3(见注 2)

注 1:N 的硬件容错指 $N+1$ 个故障可能失去安全相关控制功能。

注 2:本标准不考虑 SIL4 要求限度。有关 SIL4,见 GB/T 20438.1。

注 3:例外,见 6.7.7。

6.7.6.4 子系统根据 GB/T 16855.1 设计,并根据 GB/T 16855.2 确认,在体系结构限制上下文中的下述关系可以按照表 6 单独适用。

假设符合 GB/T 16855.1 的特别类别的子系统有表 6 所示的相关硬件容错和安全失效系数。

注:为达到要求的 SIL,还有必要按照危险失效概率和系统安全完整性来实现该要求。

表 6　体系结构限制：分类相关的 SILCL

类别	硬件容错	SFF	根据体系结构限制的最大 SIL 要求限度
	假设带所述类别的子系统具有以下特性		
1	0	<60%	见注 1
2	0	60%～90%	SIL1
3	1	<60%	SIL1
	1	60%～90%	SIL2
4	>1	60%～90%	SIL3(见注 3)
	1	>90%	SIL3(见注 4)

注 1：对于类别 1 和类别 2，当 SFF<60%时，认为与 GB/T 16855.1 原理范围内无关，按照 GB/T 16855.1 设计的子系统在实践中将达到 60%以上的 SFF。

注 2：对于类别 2，当在 SFF>90%时，假设通过 GB/T 16855.1 设计要求不能达到。

注 3：对于类别 4 子系统，当考虑到大于单一硬件容错(即累积故障)时，假设诊断覆盖率小于 90%。

注 4：当考虑单一硬件容错时，类别 4 要求 SFF 大于 90%，小于 99%。

注 5：与 GB/T 16855.1 一致的类别 B 不认为足以达到 SIL1。

6.7.7　安全失效系数评估(SFF)

6.7.7.1　由于体系结构限制需要确定 SILCL 时，应评估 SFF。

6.7.7.2　为了评估 SFF，应分析每个子系统(例如故障树分析，失效模式和效果分析)，以确定所有相关的故障以及它们相应的失效模式。无论失效是安全的或是危险的，都取决于 SRECS 和预期的安全相关控制功能，包括故障反应功能。各失效模式概率应以考虑预期用途相关故障概率为基础以及可从下列源点导出：

a)　由制造商从现场经验中收集和预期用途相关的可靠的失效率数据；

b)　来自认可的工业源(见附录 D)和预期用途相关的部件失效数据；

c)　附录 D 给出的失效模式数据；

d)　源自测试结果和分析的失效率数据。

例外：对于硬件容错为零的子系统，如果故障排除适用于可能导致危险失效的故障，那么由于子系统体系结构限制的 SILCL 其最大限制在 SIL2。

6.7.7.3　故障排除的使用应证明是正确的(例如通过分析)和形成文件。

注：排除故障允许按照 GB/T 16855.2 中 3.3 和表 D.5。

6.7.8　子系统危险随机硬件失效概率的要求

6.7.8.1　一般要求

6.7.8.1.1　危险随机硬件失效概率应等于或小于子系统安全要求规范(见 6.6.2.1.7)规定的目标失效值。

6.7.8.1.2　为执行配置的功能块，随机硬件失效导致的各子系统的危险失效概率应予评估，并考虑下列因素：

a)　考虑中的与配置功能块相关的子系统体系结构；

注 1：这涉及决定是否存在硬件容错。

b)　在可能导致子系统危险失效但能通过诊断试验检测的任何模式下，各子系统元素的失效率(见 6.3)；

c) 在可能导致子系统危险失效但不能通过诊断试验检测的任何模式下，各子系统元素的失效率（见 6.3）；

d) 子系统对共同原因失效的敏感度，可能引起子系统危险失效（见注 2 和注 3）；

注 2：故障检测使用冗余部件比较法时，当冗余部件在同一时间同一模式下失效时，故障检测手段可能失效。这是由于共同原因引起的，称之为共同原因失效（CCF），用贝它（β）因子表示。评估共同原因失效敏感度简单方法见 6.7.8.3。对于量化有关硬件共同原因失效的影响，见 GB/T 20438.6，附录 D。

e) 诊断试验的诊断覆盖率（见 3.2.38）以及相关诊断试验的时间间隔；

f) 为保持 b）和 c）项提供信息的有效性，在进行验证试验的时间间隔，揭示危险故障（由诊断试验未检测出的）和/或不应超过的子系统元素的任务时间；

g) 设计为在线修理的子系统已检测故障的修理次数。

注 3：最大修理时间将构成恢复时间的一部分（见 IEV 191-10-05），也包括检测故障时间和不可能修理的任何时间段（见 GB/T 20438.6，附录 B 有关如何使用恢复平均时间计算失效概率）。对于只能在特定时间段进行维修的情况，当机器关闭并处于安全状态时，全面考虑不能进行修理所占的时间段特别重要，尤其该时间段相对大时。

注 4：子系统危险随机硬件失效的概率评估的简化方法见 6.7.8.2。其他可行的方法和最恰当的方法将视情况而定。可用方法包括：

a) 故障树分析（见 GB/T 20438.7 的 B.6.6.5 和 GB/T 7829）；

b) 马尔可夫模型（见 GB/T 20438.7 的 C.6.4 和 IEC 61165-13）；

c) 可靠性方块图（见 GB/T 20438.7 的 C.6.5）。

注 5：由于共同原因影响和数据通信过程引发的失效可能由各种影响而产生，而不是实际的硬件部件失效（例如：电磁干扰、软件错误等）。见 6.7.9。

6.7.8.1.3 对于子系统或子系统元素，当所给的失效率与许多操作循环相关时，这些值应通过使用相关的 SRCF 规定的工作循环，转化为时间相关的值（见 5.2.3）。

6.7.8.1.4 硬件容错大于零的任何子系统诊断试验间隔应使子系统满足随机硬件失效概率要求（见 6.3.1）。

注：该诊断试验间隔应使故障在其后续故障出现前检测到，该后续故障会导致子系统危险失效和超出目标失效度的后续故障的发生。

6.7.8.1.5 任何硬件容错为零的子系统诊断试验间隔时间应符合 6.3.2 的要求。

6.7.8.1.6 当低复杂性子系统按照 GB/T 16855.1 设计和按照 GB/T 16855.2 确认，也满足体系结构限制（见 6.7.6）和系统安全完整性（见 6.7.9）的要求时，表 7 所示的危险失效概率（PFH_D）的阈值可用于评估硬件安全完整性（见 6.6.3.2）。

表 7 危险失效概率

分类	硬件容错	DC	子系统要求的 PFH_D 阈值（每小时）
	假设带有所述类别的子系统具有下列特性		PFH_D（MTTF 子系统测试、DC）（见注 1）
1	0	0%	由供方提供或使用通用数据（见附录 D）
2	0	60%～90%	$\geqslant 10^{-6}$
3	1	60%～90%	$\geqslant 2\times 10^{-7}$
4	>1	60%～90%	$\geqslant 3\times 10^{-8}$
	1	>90%	3×10^{-8}

注 1：PFH_D 阈值是子系统 MTTF 的函数（来源于子系统制造商或有关元件数据手册），试验/检查循环时间如同安全要求规范中规定的（该信息也是按照 GB/T 16855.2，3.5 子系统确认所要求的）以及本表所示的诊断覆盖率（这些数值以 GB/T 16855.1 描述的类别要求为基础）。

注 2：按照 GB/T 16855.1 的类别 B 不能认为足以达到 SIL1。

6.7.8.2 子系统危险随机硬件失效概率评估的简化方法

6.7.8.2.1 概述

该子项描述许多基本子系统体系结构的危险随机硬件失效概率评估的简化方法，提供可用于低复杂性子系统元素或复杂子系统元素组合的子系统公式。这些公式本身是可靠性分析理论的简化和预期提供侧重安全方面的评估。在本子项所给的所有公式有效性的前提是 $1 \gg \lambda \times T_1$，其中 T_1 为验证试验间隔时间或寿命的较小值。该子系统在“高要求或连续模式”下运行(见 3.2.27)。也见 6.8.6。

注 1：获得的结果表示子系统依据其危险随机硬件失效概率限制和不能接受时，可以采用更精确的建模技术(见 6.7.8.1.1)。

注 2：对于 6.7.8.2 所给的公式(1)～(5)，假设子系统元素失效率(λ)为常数和足够低($1 \gg \lambda \times T$)(这意指危险失效平均时间必须远大于子系统的验证试验间隔时间或寿命)。因此，可用下列基本等式：

$$\lambda = 1/\mathrm{MTTF}$$

对于机电设备，失效率用规定的 B_{10} 值和操作循环数 C(见 5.2.3)确定。

$$\lambda = 0.1 \times C/B_{10}$$

注 3：使用下列术语：

$\lambda = \lambda_S + \lambda_D$；其中 λ_S 为安全失效率，λ_D 为危险失效率。

$PFH_D = \lambda_D \times 1\mathrm{h}$；一小时内危险失效的平均概率。

T_1：验证试验时间间隔或寿命中的较小值。

6.7.8.2.2 基本子系统体系结构 A：无诊断功能的零容错

本体系结构，子系统元素的任何危险失效会引起 SRCF 失效。对于体系结构 A，子系统危险失效概率是所有子系统元素的危险失效概率的和：

$$\lambda_{DssA} = \lambda_{De1} + \cdots + \lambda_{Den} \qquad \cdots\cdots(1)$$

$$PFH_{DssA} = \lambda_{DssA} \times 1\mathrm{h}$$

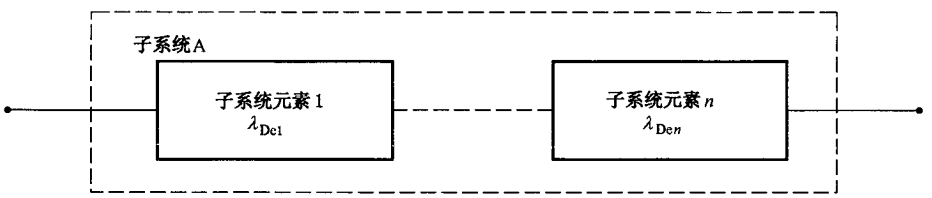


图 6 子系统 A 逻辑表示

注：图 6 为子系统 A 体系结构的逻辑表示，而不应该理解为其物理实现。

6.7.8.2.3 基本子系统体系结构 B：无诊断功能的单一容错

本结构为任何子系统元素的单一失效不会引起 SRCF 的丧失。因此在 SRCF 失效可能出现前，必定在一个以上的元素中有危险的失效。对于结构 B 来说，子系统危险失效概率为：

$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2 \qquad \cdots\cdots(2)$$

$$PFH_{DssB} = \lambda_{DssB} \times 1\mathrm{h}$$

式中：

T_1——验证实验时间间隔或寿命中的较小者。

β ——共同原因失效的敏感度。

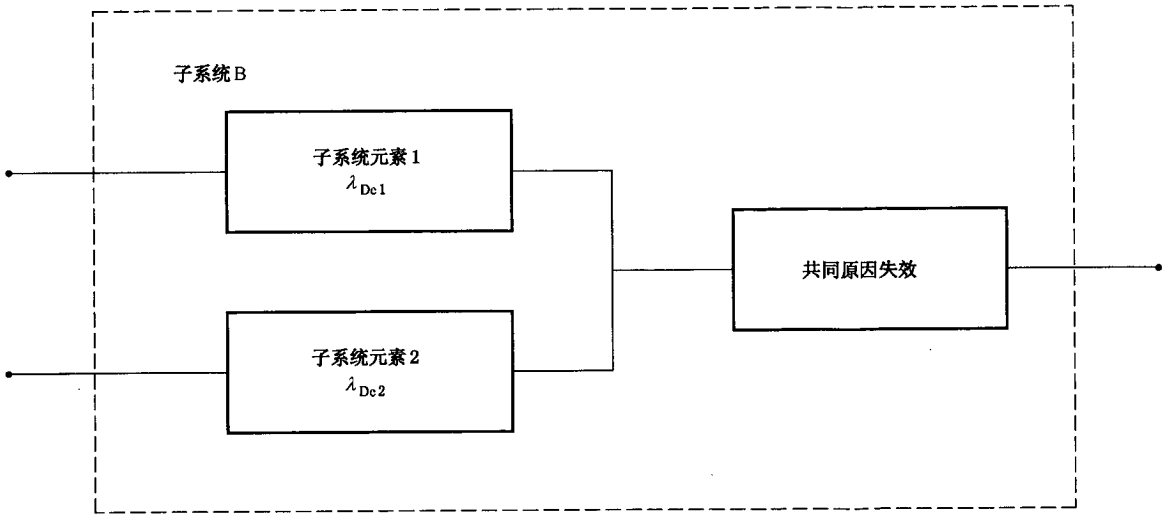


图 7　子系统 B 逻辑表示

注：图 7 为子系统 B 体系结构的逻辑表示，而不应该理解为其物理实现。

6.7.8.2.4　基本子系统体系结构 C：带诊断功能的零容错

子系统元素的任何没有检测出的危险故障会导致 SRCF 的危险失效。当子系统元素的故障被检测出时，诊断功能引发失效反应功能（见 6.3.2），对于结构 C，子系统的危险失效概率为：

$$\lambda_{DssC} = \lambda_{De1}(1 - DC_1) + \cdots + \lambda_{Den}(1 - DC_n) \quad \cdots\cdots (3)$$

$$PFH_{DssC} = \lambda_{DssC} \times 1\text{h}$$

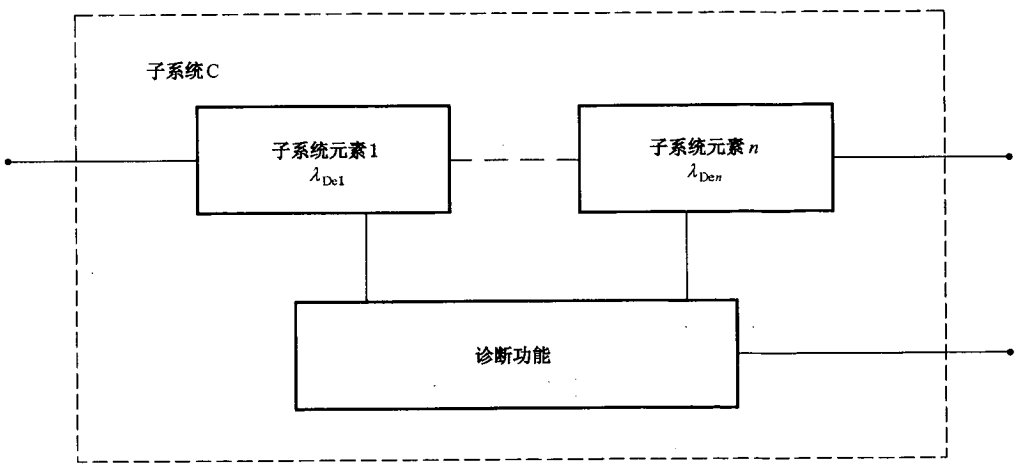


图 8　子系统 C 逻辑表示

注：图 8 是子系统 C 体系结构的逻辑表示，不应该理解为其物理实现。所示的诊断功能可能由下列因素执行：

——要求诊断的子系统；

——SRECS 的其他子系统；

——不执行安全相关控制功能的子系统。

6.7.8.2.5　基本子系统体系结构 D：带诊断功能的单一容错

本结构中，任何子系统元素的单一失效不引起 SRCF 的丧失，这里

T_2 是诊断试验时间间隔；

T_1 验证实验时间间隔或寿命中较小者。

β 是共同原因失效的敏感度；$\lambda_D=\lambda_{DD}+\lambda_{DU}$；这里，$\lambda_{DD}$ 是可检测的危险失效率，而 λ_{DU} 为不可检测的危险失效率。

$\lambda_{DD}=\lambda_D\times DC$

$\lambda_{DU}=\lambda_D\times(1-DC)$

对于不同设计的子系统元素：

λ_{De1} 为子系统元素 1 的危险失效率；

DC_1 为子系统元素 1 的诊断覆盖率；

λ_{De2} 为子系统元素 2 的危险失效率；

DC_2 为子系统元素 2 的诊断覆盖率。

$$\lambda_{DssD}=(1-\beta)^2\{[\lambda_{De1}\times\lambda_{De2}\times(DC_1+DC_2)]\times T_2/2+[\lambda_{De1}\times\lambda_{De2}\times(2-DC_1-DC_2)]\times T_1/2\}+\beta\times(\lambda_{De1}+\lambda_{De2})/2 \quad \cdots\cdots(4)$$

$$PFH_{DssD}=\lambda_{DssD}\times 1\text{h}$$

对于相同设计的子系统元素：

λ_{De} 为子系统元素 1 或 2 的危险失效率；

DC 为子系统元素 1 或 2 的诊断覆盖率。

$$\lambda_{DssD}=(1-\beta)^2\{[\lambda_{De}^2\times 2\times DC]\times T_2/2+[\lambda_{De}^2\times(1-DC)]\times T_1\}+\beta\times\lambda_{De} \quad \cdots\cdots(5)$$

$$PFH_{DssD}=\lambda_{DssD}\times 1\text{h}$$

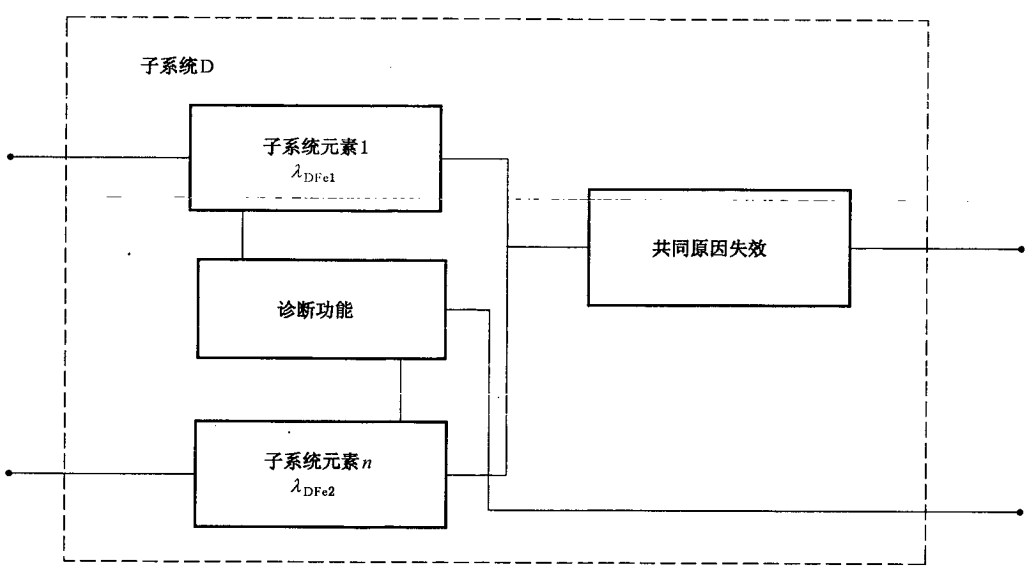


图 9　子系统 D 逻辑表示

注 1：图 9 是子系统 D 结构的逻辑表示，不应理解为其物理实现。所示诊断功能可能由下列因素执行：

——需要诊断的子系统；或

——SRECS 的其他子系统；或

——不执行安全相关控制功能的子系统。

注 2：假设本子系统的故障反应为 6.3.1 所要求的有关操作的中止。当在线修理成为设计一部分时，故障反应是报告故障而不是中止相关的操作，在第一个故障发生后，应为剩余结构确定子系统新的 PFH_D。

6.7.8.3 共同原因失效(CCF)评估的简化方法

6.7.8.3.1 为有助于子系统危险随机硬件失效概率的评估,对于 CCF 而言需要子系统失效敏感度的知识(见 6.7.8.1)。

6.7.8.3.2 为获得所需的子系统危险随机硬件失效概率而使用冗余结构和 CCF 可以消除冗余的影响时,以共同原因失效的发生为基础的危险随机硬件失效概率,应增加到以使用冗余结构为基础的子系统的危险随机硬件失效的概率中。

6.7.8.3.3 CCF 失效发生的概率通常将随技术、结构、应用和环境的组合而定。使用附录 F 将有效避免 CCF 的许多类型。

6.7.8.3.4 附录 F 包含有记分表和相应的方法,可用于评估在子系统设计中应用措施的有效性,以限制 CCF 的敏感度。

6.7.9 对子系统安全完整性的要求

当实现了 6.7.9.1 和 6.7.9.2 的要求,由子系统的系统安全完整性导致的 SILCL 达到 SIL3。

注:这些要求适用于子系统级,子系统元素互连以实现子系统。有关实现 SRECS 的其他要求见 6.4。

6.7.9.1 避免系统失效的要求

6.7.9.1.1 应采取下列措施:

a) 适当地选择、组合、安排、组装和安装元件,包括电缆连接、配线和任何互联:应用制造商的使用注意事项和良好工程实践;

b) 在制造商规范和安装说明书的范围内使用子系统和子系统元素;

c) 兼容性:使用具有兼容工作特性的元件;

d) 能承受规定的环境条件:子系统的设计应使其在所有的预期的环境和任何可以预见的不利条件下工作,例如温度、湿度、震动和电磁干扰(EMI)(见 GB/T 16855.2 中 D.1);

e) 按照适当标准使用元件并有其定义明确的失效模式:以降低使用有特定特性元件所引起的未被检测的故障风险;

f) 选择适宜的材料和适当的制造:材料、制造方法的选择和例如压力、耐久性、弹性、摩擦、耐磨性、腐蚀、温度、传导性、绝缘强度有关的处理;

g) 正确的尺寸和形状:考虑例如应力、张力、疲劳、温度、表面粗糙度、制造公差等的效果。

6.7.9.1.2 还有,考虑子系统的复杂性,应采取下列一项或多项措施:

a) 硬件设计审查(如检查或初排):通过审查来发现或分析规范和执行之间的差异:

注 1:为了找出规范和执行之间的差异,与产品实现、执行和使用有关的任何可能的弱点应写入文档,那么这些问题可以解决;考虑到:对于检查程序,作者是被动而检查人员主动;而对于初排程序,作者是主动而检查人员是被动。

b) 计算机辅助设计工具能够模拟或分析:系统地执行设计程序,包括适当的自动构造元素,这些元素已经可用并经试验过。

注 2:这些工具的完整性可以通过下列方式证明:具体测试或由广泛的令人满意的使用历史或由正在进行设计的具体子系统的输出独立验证。见 6.11.3.4。

c) 模拟:根据功能的性能和部件的合适大小,执行子系统设计的系统仿真。

注 3:子系统的功能可以在计算机上通过软件行为模型(见 6.11.3.4)仿真。电路的单独部件各有他们自己的仿真行为,而互相连接的子系统的响应,通过察看各元件的图例说明进行检查。

6.7.9.2 系统失效控制要求

6.7.9.2.1 应使用下列措施：

a) 控制绝缘击穿，电压变化和中断，过电压和欠电压影响的措施：对绝缘击穿，电压变化和中断，过电压或欠电压情况做出反应的子系统行为应预先确定，这样，子系统可以达到或保持SRECS的安全状态。

注1：也见GB 5226.1的有关要求，尤其：

——过电压应尽早被检测出来，以便断电程序将所有输出切换至安全状态或转接到第二个电源；和/或

——控制电路电压应被监视，如果电压不在规定的范围内，应引发断电，或转接到第二个电源，和/或

——过电压或欠电压应该尽早被检测出来，使其内部状态存储到非易失性储存(必要时)，以便断电程序会把所有输出置于安全状态，或转接至第二电源。

b) 控制或避免实际环境(例如：温度、湿度、水、震动、粉尘、腐蚀性物质、电磁干扰及其作用)影响的措施：对实际环境的影响做出反应的子系统行为应预先确定，以便SRECS可以达到或保持机器的安全状态。见GB 5226.1；

c) 温度变化时，控制或避免温度升高或降低影响的措施：子系统的设计应考虑，例如，在其操作超出规范前，过温即应检测出。

注2：详情见GB/T 20438.7，A.10。

6.7.9.2.2 另外，应用下列措施控制系统失效：

——在线失效检测；

——冗余硬件比较试验；

——相异硬件；

——主动操作模式(例如保护装置打开时，即按动限制开关)；

——面向失效模式；

——采用适当因素的过尺寸，这里制造商能证明减额将提高其可靠性。

注1：如果过尺寸合适，过尺寸系数至少应为1.5。

注2：详见GB/T 16855.2，D.3。

6.7.10 装配子系统

子系统元素应按照6.7.4.3.1.2组合成子系统和详细设计文档。

6.8 实现诊断功能

6.8.1 为了满足体系结构限制(6.7.6)和危险随机硬件失效概率(6.7.8)的要求，每个子系统应当具备有相应的诊断功能。

6.8.2 诊断功能被认为是单独的功能，与SRCF相比可能有不同的结构，可以由下列因素执行：

——要求诊断的相同子系统；或

——SRECS的其他子系统；或

——不执行SRCF的SRECS子系统。

注：也见6.6.2.1中注3。

6.8.3 诊断功能应满足下列要求，并适于其相关联的SRCF：

——避免系统失效要求(见6.7.9.1)；和

——系统失效的控制要求(见6.7.9.2)。

6.8.4 评估SRCF危险失效概率时，应考虑SRECS诊断功能的失效概率。

注1：也见6.6.2.1中注3。

注2：用于检测执行诊断功能的子系统的定时限制，可能与适合SRCFs的时间限制不同，一般来说，试验时间间隔

应满足硬件容错度为 1 的子系统的要求。

注 3：应检测诊断功能的失效，并做出适当的反应，以保证诊断功能有利于 SRCF 的安全完整性保持。诊断功能失效可以由在线测试，冗余硬件交叉检测等方式发现。

6.8.5 应提供 SRECS 诊断功能、诊断功能的失效检测/反应和诊断功能有助于相关 SRCFs 安全完整性的清晰描述。

6.8.6 为应用简化方法，适用于评估子系统(6.7.8.2)的危险随机硬件失效概率，应使用下列因素：

——为达到要求的危险随机硬件失效概率和子系统硬件容错为零而需要 SRECS 诊断功能时，则故障检测和规定的故障反应该在该故障导致危险之前执行，和

——SRECS 诊断功能应实施最小，以使随机硬件失效概率和系统安全完整性是相同的，如同相应 SRCF 所规定的；或

注 1：硬件安全完整性的体系结构限制不需要用于实现诊断功能。

——危险随机硬件失效概率是一个数量级大于 SRCF 规定的数量级时，应进行试验以确定诊断功能或诊断装置是否保持运行。假定，这样的诊断功能或诊断装置试验在子系统检验试验之间的间隔期间最少进行 10 次。

注 2：诊断功能试验尽可能 100%覆盖执行诊断功能的部件。

注 3：如果诊断功能由 SRECS 逻辑求解器实现，可能不需要单独进行诊断功能试验了，因为其失效能作为 SRCF 失效显示出来。

注 4：试验既可以由外部方法(例如试验设备)也可以由 SRECS 的内部动态检查(例如嵌入式的逻辑求解器)来完成。

6.9 SRECS 硬件实现

SRECS 应当按照 SRECS 设计文件实现。

6.9.1 SRECS 互联

6.9.1.1 SRECS 应互联以满足 SRECS 的安全要求规范的适当部分，而这些要求与 GB 5226.1 中的导体、电缆和配线有关。

6.9.1.2 避免和控制互联导体失效和电缆失效的措施应符合 6.4.1 和 6.4.2。

6.10 软件安全要求规范

6.10.1 概述

若实现安全相关控制功能的 SRECS 中任一部分使用软件，应开发软件安全要求规范，并撰写文档。

6.10.2 要求

6.10.2.1 在 SRECS 规范和结构的基础上，对于每个子系统应开发软件安全要求规范。

6.10.2.2 每个子系统的软件安全要求规范都应来自：

a) SRECS 规定的安全要求；

b) 产生于 SRECS 体系结构的要求，和

c) 功能安全计划(见 4.2)的任何要求。这些信息应提供给应用软件开发商。

6.10.2.3 应用软件安全要求规范应详细，使得 SRECS 的设计和执行达到要求的安全完整性，并允许验证。

6.10.2.4 应用软件开发人员应该检查规范中的信息，保证所有要求都有充分的规定。特别是软件开发人员应遵照本标准，包括下列信息：

SRCF；

——系统的配置或结构；

——容量和响应时间特性；

——设备和操作者界面；

——安全要求规范中所规定的机器操作所有相关的模式；

——外部装置诊断试验(例如：传感器和最终元件)。

6.10.2.5 规定的软件安全要求其表达和结构应能：

——清晰、可验证、可试验、可维修和可操作、有相称的安全完整性等级；

——可追溯到 SRECS 的安全要求规范；

——没有含糊术语和描述。

6.10.2.6 软件安全要求规范应表达要求的每个子系统的特性，要通过提供正确选择设备的信息。应规定下列基于软件的 SRCF 的要求：

——分配到每个子系统的所有功能块的逻辑(如功能性)；

——每个功能块的输入输出接口；

——输入输出数据的格式和数值范围以及其有关功能块；

——描述各功能块限制的相关数据，例如最大响应时间，真实性检查限制值；

——由子系统实现的 SRECS 范围内的其他装置(例如：传感器和最终元件)的诊断功能；

——能让机器达到或保持安全状态的功能；

——有关检测、通告和处理故障的功能；

——有关 SRCF 在线和离线的周期测试的功能；

——防止未经授权 SRECS 修改功能；

——非 SRCF 接口；和

——容量和响应时间性能。

注：接口包括在线和离线编程工具。

6.10.2.7 适当时，在文件中应使用半形式化方法，例如逻辑、功能模块及序列图表。

注：软件文档指导见 GB/T 19898、ISO/IEC 15910 和 ISO/IEC 9254。

6.11 软件设计和开发

6.11.1 嵌入式软件设计和开发

并入子系统的嵌入式软件应符合 IEC 61508-3，要求的 SIL 应适当。

注 1：也见 6.7.3.2。

注 2：附录 C 帮助 SRECS 中用于实现 SRCF 的嵌入式软件的设计和开发。

6.11.2 参数化软件

6.11.2.1 有关安全参数的软件参数化被认为是 SRECS 设计的有关安全方面，SRECS 设计在软件安全规范(见 6.10)中描述。参数化应使用 SRECS 或相关子系统的供方提供的专用工具进行。该工具应有属于自己的标识(名称、版本等)。参数化工具将防止未经授权的修改，例如：使用密码。

6.11.2.2 应保持用于参数化使用的所有数据的完整性。应采用下列措施实现：

——控制有效输入的范围；

——控制数据传输前的损坏；

——控制参数传输过程的错误影响；

——控制参数传输不完整的影响；和

——控制参数化所用工具的软件、硬件的故障和失效影响。

6.11.2.3 用于参数化的工具应满足下列要求：

——按照本标准对子系统所有相关要求，以确保正确的参数化；或

——应使用特别程序设置有关安全参数。该程序应包括通过下列途径确认 SRECS 的输入参数：

- 将已修改的参数再传给参数化工具；或
- 确认参数完整性的其他方法；

和随后的确认（例如，经合适的技术人员和参数化工具的自动检查）；

注：使用非专用装置（例如，个人计算机或同等设备）进行参数化时是特别重要的。

——在传送/再传过程中用于编码/译码的软件模块和用于用户安全相关参数的可视化软件模块，应在功能上作为最小使用的相异技术，以预防系统失效。

6.11.2.4 基于软件参数化的文档应指明使用的数据（例如：预定义的参数集）、需要识别与 SRECS 相关参数的信息和执行参数化的人员连同其相关信息例如参数化日期。

6.11.2.5 基于软件参数化应采用下列验证活动：

——验证正确设置每个安全相关参数（最小、最大和典型值）；

——验证安全相关参数合理性检查，例如：用无效值等检测；

——验证防止安全相关参数的未经授权修改；

——验证作为参数化数据/信号的产生和处理，故障不能导致 SRCF 损失。

注：使用非专用装置（例如：个人计算机或同等设备）进行参数化是特别重要的。

6.11.3 应用软件的设计和开发

注：本分条基于 IEC 61508-3。

6.11.3.1 一般要求

6.11.3.1.1 IEC 61508-3 的要求符合全可变语言类型（FVL）。下列要求适用于基于有限可变语言类型（LVL）的应用软件。

6.11.3.1.2 应用软件开发期间，执行活动的结果应在适当阶段进行验证。

6.11.3.1.3 为满足所需 SRCF 的 SIL，选择的设计方法和应用语言应具有下列便于应用的特征：

a) 抽象性、模块性及其他控制复杂性的特征；可能的话，软件应基于经过充分验证的逻辑功能，包括用户库功能和链接逻辑功能的良好定义规则；

b) 如下表述：

- 功能性，理想地作为逻辑描述或算法函数；
- 模块化元素之间的信息流；
- 顺序和有关时间的要求；
- 定时限制；
- 数据结构和其属性，包括数据类型、数据范围的有效性；

c) 由开发者和其他需要懂设计的人理解的，包括应用功能性的理解和 SRECS 技术限制的知识；

d) 验证和确认，包括应用软件的结构测试（白箱）、集成应用程序的功能测试（黑箱）、与 SRECS 交互的接口测试（灰箱）、和其应用特定的硬件体系结构；

e) 安全修正。

6.11.3.1.4 测试是用于应用软件的主要验证方法。试验计划应包括：

——软件和硬件集成的验证策略；

——试验实例和试验结果；

——执行的试验类型；

——试验设备，包括工具、支持软件和配置说明；

——试验准则，应对完成的试验进行判定；
——实际位置（例如工厂或现场）；
——外部功能性的依赖；
——必要的试验实例的数量；和
——相关功能或要求的完成情况。

6.11.3.1.5 应用软件要同时执行非安全和安全相关控制功能时，那么所有应用软件应作为安全相关处理，除非可以证明设计的功能之间有足够的独立性。

6.11.3.1.6 在应用层设计应包括数据完整性检查和合理性检查（例如通信链路检查、传感器输入边界检查、数据参数边界检查）。

6.11.3.1.7 应用软件设计应包括控制流和数据流的自监控，除非这类功能已经包括在嵌入式软件中。在失效检测方面，应采取恰当的行为，以达到或保持安全状态。

6.11.3.1.8 如果预先开发的软件库函数作为设计的一部分，应证明其满足软件安全要求规范的适合性。适合性应基于证明有类似功能性的类似应用中令人满意的操作，或预期任何新开发的安全相关软件应承受同一验证和确认程序。应评估来自先前软件环境（例如操作系统和编译器）的约束。

6.11.3.1.9 对应用软件的任何修改和变动应做影响分析，识别所有受影响的软件模块和必要的重新验证活动，以确定软件安全要求规范仍然被满足。

6.11.3.2 软件配置管理

6.11.3.2.1 功能安全计划应规定软件开发、集成、验证和确认的策略。

6.11.3.2.2 软件配置管理应：

——确保所有必要操作已执行，并证明达到了软件安全完整性要求。
——准确保持和唯一识别有关配置项目的所有文件，这是为保持 SRECS 的完整性所需要的。配置项目至少应包括：
- 安全分析和要求；
- 软件规范和设计文件；
- 软件源代码模块；
- 试验计划和结果；
- 将被并入 SRECS 的预存软件模块和软件包；
- 在应用软件上用于创建或试验、或执行任何动作的所有工具和开发环境。

——应用改变控制程序：
- 防止未经授权的修改；
- 文件修改请求；
- 分析提议的修改的冲突，通过或拒绝请求；
- 授权和所有批准的修改的详细文件；
- 软件开发中在适当点提供软件配置文件。

——为下述信息提供文件，允许随后的审计：版本状态，批准所有修改的理由和修改细节。
——正式应用软件的版本文件，软件和所有相关文件的原版拷贝应保存，允许维护和修改能够在发行软件的生命周期内完全有效。

6.11.3.3 软件体系结构要求

注 1：软件体系结构规定系统的主要元件及子系统和应用软件，他们如何并入、如何实现要求的属性。例如，应用软件模块包括整个机器的应用功能：机器输入/输出，超越和禁止元件、数据有效性检查和范围检查等。

注 2：软件体系结构也受由供方提供的子系统的基本体系结构的影响。

6.11.3.3.1 在SRECS系统结构限制和子系统设计范围内，软件体系结构设计应遵循SRECS的安全规范。

6.11.3.3.2 软件体系结构设计应：

a) 提供内部结构、SRECS操作及其部件的综合描述(见注释)；

b) 包括所有识别的软件部件规范，和识别的部件(软件与硬件)之间的连接和交互描述；

c) 包括内部设计和所有不是黑箱的识别的部件的的体系结构；

d) 识别SRECS中但未在任何安全相关操作模式中使用的软件模块。

注：体系结构文件及时更新，保持SRECS的完整性，这一点非常重要。

6.11.3.3.3 为满足规范要求，在应用软件设计期间的一套技术和措施应被描述和证明。这些技术和措施应确保SRECS行为的可预见性，并与SRECS文件中任何识别的限制一致。

6.11.3.3.4 应描述和证明用于保持所有数据完整的措施。这类数据可以包括机器的输入和输出数据、通信数据、操作接口数据、维修数据和内部数据库数据。

6.11.3.4 支持工具、用户手册和应用语言要求

6.11.3.4.1 应选择一组合适的工具，包括配置管理、模拟、和试验装备工具。应考虑合适工具的可用性(最初系统开发时不使用的工具)，以便在SRECS的生命周期内提供相关的服务。工具的适用性应说明和形成文件。

注：开发工具的选择取决于软件开发活动的性质，嵌入式软件和软件结构。可能需要验证和确认的工具，例如代码分析仪和模拟器。

6.11.3.4.2 必要时，应规定应用编程语言子集。

6.11.3.4.3 应用软件的设计应考虑限制，和在SRECS和子系统用户手册中包括的已知缺陷。

6.11.3.4.4 选择的应用语言应：

——使用翻译器/编译器处理的应评估以使其适应用途；

——定义完全和明确或仅限于明确定义的特征；

——对应于应用特征；

注：应用特征指，例如任何性能限制。

——便于检查编程错误的包含特征；和

——匹配设计方法的支持特征；

或，在软件体系结构设计描述中，使用语言的不足应形成文件，语言用途的适应性应说明，包括：识别的语言缺陷所需的附加措施。

6.11.3.4.5 应用语言使用程序应规定良好的配置实践，禁止非安全通用软件特征(例如：未定义语言特征、非结构化设计等)，识别检查能用于检测结构错误，规定应用程序的文件程序。至少，应用程序文件中应包含下列内容：

a) 合法实体(例如公司、作者等)；

b) 描述；

c) 应用功能要求的可追溯性；

d) 标准库函数的可追溯性；

e) 输入和输出；和

f) 结构管理。

6.11.3.5 应用软件设计要求

6.11.3.5.1 以下信息应在应用软件详细设计开始之前得到：

——软件安全要求规范；

——软件体系结构设计描述包括应用逻辑和故障容错功能识别，输入和输出数据表，通用软件模块，使用的支持工具和与可用材料一起配置应用软件的程序，以便为定义的 I/O 提供应用功能性。

——确认软件安全的计划。

6.11.3.5.2 应用软件应以结构的方法产生，以达到：

——应用功能以及 I/O 控制数据的模块性；

——功能（包括容错特征）和内部结构的易测性；

——安全修改的能力，通过规定适当的可追溯性和应用功能及相关限制说明实现。

6.11.3.5.3 在应用软件体系结构设计（见 6.11.3.5.1）的描述中，对于各主要部件/子系统，设计优化应基于：

——功能，是以循环方式使用于整个设计；

——应用软件模块的输入/输出信息映射；

——通用软件功能和 I/O 映射实现应用功能。

6.11.3.5.4 应规定各应用软件模块的设计和用于各应用软件模块结构的试验。

6.11.3.5.5 应规定适当软件和 SRECS 集成试验，以保证应用程序满足规定的应用软件安全要求。应考虑下列项目：

——应用软件分割成可管理的集成集；

——试验实例；

——执行的试验类型；

——试验环境、工具、配置和程序；

——试验准则，用来判断试验完成情况；和

——对试验失效，用于纠正行为的程序。

6.11.3.6 应用代码开发要求

6.11.3.6.1 应用软件应：

——可读、可理解、可测试；

——满足有关设计原则；

——满足安全计划中规定的相关要求。

6.11.3.6.2 应用软件应得到核对，以保证与指定设计、编码规则和安全规划要求一致。

注：应用软件评审包括这类技术，例如：软件检查或走查、编码分析或数学证明。这些技术应与测试和/或模拟结合使用，以保证应用软件满足其相关规范要求。

6.11.3.7 应用模块测试要求

注：应用软件能恰当满足其试验规范的测试是验证活动。它是编码审查和结构测试的结合，为应用软件模块满足其相关规范提供了保证。即：它得到了验证。

6.11.3.7.1 每个输入和输出点的配置应检查，凭借评审、测试、或模拟，以确认 I/O 数据映射到正确的应用逻辑。

6.11.3.7.2 每个软件模块应检查，凭借过程评审、模拟和测试，以确定预期功能被正确执行，而非预期功能不能执行。

6.11.3.7.3 试验应符合受试的特定模块，还应：

——保证任何应用软件模块的各分支经过练习；

——保证边界数据经过练习；

——保证正确执行顺序，包括有关同步条件。

6.11.3.7.4 应用软件模块测试结果应形成文件。

6.11.3.7.5 已经被评估的软件或大量的积极操作经验可用时，测试的数量可能会减少。

6.11.3.8 应用软件集成测试要求

注：软件被正确集成的测试是验证活动。

6.11.3.8.1 应用软件试验应验证所有应用软件模块和部件/子系统彼此正确交互，用基本的嵌入式软件执行预期功能，而不执行可能危害任何安全功能的非预期功能。

6.11.3.8.2 应用软件综合测试结果应形成文件，陈述：

——试验结果；和

——是否符合试验准则的目标。

6.11.3.8.3 如有失效，测试结果文档内应包括失效原因以及采取的纠正措施。

6.11.3.8.4 在应用软件集成期间，软件的任何修改或变更应按照安全影响分析进行，确定如下：

——受影响的所有软件模块；和

——所有必需重新验证和重新设计的活动。

6.12 安全相关电气控制系统集成和测试

注：SRECS 集成一般在安装前进行，但在有些情况下，SRECS 集成在安装后才能进行（例如：应用软件开发到安装结束后才定下来）。

6.12.1 一般要求

6.12.1.1 SRECS 应按规定的 SRECS 设计集成。作为所有子系统和子系统元素的一部分集成到 SERCS，应按照规定的集成试验进行 SRECS 试验。这些试验应验证所有模块正确交互，以执行他们的预期功能，不执行非预期功能。

6.12.1.2 安全相关应用软件集成到 SRECS 应包括在设计和开发阶段规定的试验，以保证应用软件和硬件及嵌入式软件平台的兼容性，从而满足功能和安全性能要求。

注 1：这不表示所有输入结合的测试。测试所有相等级别（见 GB/T 20438.7 中 B.5 和 C.5.7）已经足够。静态分析、动态分析或失效分析能降低测试案例数目至可接受的水平。使用结构化设计或半正式方法便于测试和验证。

注 2：用结构设计或半正式方法允许降低试验实例的深度和数量。

注 3：也可以使用统计证据降低试验实例的深度和数量。

6.12.1.3 应制作 SRECS 集成测试的恰当文件，表述试验结果，是否达到了设计开发阶段规定的目标和准则。如果有失效，失效的原因应该形成文件，并进行纠正行动和重新测试。

6.12.1.4 集成和测试期间，对 SRECS 的任何修改或变化应进行影响分析，并应识别所有受影响的部件和附加验证。

6.12.1.5 在 SRECS 集成测试期间，应形成下列文件：

a) 所用试验规范的版本；

b) 集成试验可接受的准则；

c) 受试的 SRECS 版本；

d) 使用的工具和设备连同校准数据；

e) 每次试验的结果；

f) 期望和实际结果之间的所有差异；

g) 在发生差异的地方，所做的分析和决定是否继续测试或提出改变要求。

6.12.2 SRECS 集成时，决定系统安全完整性试验

6.12.2.1 应用软件和硬件集成期间，暴露故障和避免失效的测试应使用。试验期间，应进行评审考虑

是否达到了规定的 SRECS 特性。

6.12.2.2 应进行下列试验：

a) 在充分表征操作的数据处，对 SRECS 应用功能试验。应观察输出，其响应与规范规定的进行比较。偏离规范和未完成规范的指示应形成文件；和

b) 在实际功能条件下，验证动态行为的动态试验和满足 SRECS 功能规范的显示失效，并评估 SRECS 的实用性和鲁棒性。

注：在规定的环境中和有规定的试验数据，执行系统或程序的功能。该试验数据根据已确定的准则，从 SRECS SRS 系统生成。这暴露了 SRECS 的行为，并允许与规范进行比较。目的是为了确定 SRECS 和/或其子系统是否正确执行了规范要求的所有功能。形成等值级别技术是用于黑箱试验数据的准则例子。依照规范，输入数据空间再分成特定的输入值范围(等值级别)。试验实例形成于：

——可允许范围的数据；

——不可允许范围的数据；

——范围限制数据；

——极限值；

——上述级别的结合。

在不同的试验活动(模块试验、集成试验和系统试验)中，为选择试验实例，其他准则可以是有效的。

6.13 SRECS 安装

6.13.1 目的

本条要求的目标是适合 SRECS 安装以保证其适合预期用途和为确认做准备。

6.13.2 要求

6.13.2.1 SRECS 应按照最终系统确认的功能安全计划进行安装(见 4.2.1 中 h))。

6.13.2.2 SRECS 的安装应做恰当记录，陈述任何试验结果。如果有失效，应记录失效原因。

7 SRECS 使用信息

7.1 目的

应提供 SRECS 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 SRECS 所要求的功能安全。

7.2 安装、使用与维护文件

注 1：见 GB/T 15706.2 第 6 章提供的一般信息，起草随机文件时应予以考虑。

注 2：分条文档中的一个或多个项目可能已经被开发出来了，为了满足本标准的其他方面。

文档应提供 SRECS 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) SRECS 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) 验证试验时间间隔或寿命。

g) SRECS 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，来保证 SRECS 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，程序验证），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 SRECS 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 SRECS 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) SRECS 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) 维护和重新试运转必需的工具和适用于维护工具和设备的程序；

5) 定期测试规范、预防维护和纠正维护规范。

注 3：定期试验是确认正确操作和检测故障必须的功能试验。

注 4：预防性维护是保持 SRECS 所需性能而采取的措施。

注 5：纠正维护包括将 SRECS 带回到设计状态的特定故障发生后采取的措施。

8 安全相关电气控制系统确认

注：SRECS 确认可能形成适用于全部机器设计的确认活动的一部分。

8.1 目的

本条规定用于 SRECS 的确认程序的要求，包括：检查和 SRECS 测试，以保证达到安全要求规范中陈述的要求。

8.2 一般要求

8.2.1

应按照预定计划执行 SRECS 确认（见 4.2）。

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 SRECS 确认由硬件、软件要求确认组成。软件确认要求包括在 6.11.3 中。

8.2.2 SRECS 要求规范（见 5.2）中规定的各 SRCF、所有 SRECS 操作和维护程序应通过试验和/或分析进行确认。

8.2.3 SRECS 安全确认的测试应形成恰当文件，对各 SRCF 应有下列陈述。

a) 安全确认计划使用的 SRECS 版本和试验的 SRECS 版本；

b) 在 SRCF 试验（或分析）中，在 SRECS 安全确认计划期间，和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。

8.2.4 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。

8.3 SRECS 系统安全完整性确认

8.3.1 下列要求应适用：

a) 在规范、设计和集成阶段暴露失效的功能测试，和在 SRECS 软件/硬件的确认期间应采用避免失效的功能测试。包括验证（例如通过检查或试验）以评估 SRECS 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。

注 1：也见 6.12.2.1。

b） 干扰抗扰度测试用以保证 SRECS 能够满足 5.2.3。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，在那儿，SRECS 对它的预期应用有足够的抗扰度，通过分析可以表现出来。

注 2：SRECS 只要可行，用典型应用程序装载，所有外围线路（所有数字、模拟和串行接口，以及总线连接、电源等）要遭受标准噪声信号。为了获得定量陈述，对接近限值应谨慎。

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

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

a） 静态和失效分析；

注 1：这种分析技术的结合只考虑适合 SRECS，用指定的 SIL，不超过 SIL2 来执行 SRCFs。

注 2：进一步的信息可以在 GB/T 20438.7 中 B.6.4 和 B.6.6 中找到。

b） 静态、动态和失效分析；

注 3：这种分析技术的结合并不推荐用于 SRECS，用指定的 SIL，低于 SIL2 来执行 SRCFs。

注 4：进一步的信息可以在 GB/T 20438.7 中 B.6.4，B.6.5 和 B.6.6 中找到。

c） 模拟和失效分析。

注 5：这种分析技术的结合只考虑适合 SRECS，用指定的 SIL，不超过 SIL2 来执行 SRCFs。

注 6：进一步的信息可以在 GB/T 20438.7 中 B.3.6 和 B.6.6 中找到。

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

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

注 1：也见 6.12.2.1。

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 SRECS 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（见 8.3.2）；

注 2：在最坏的情况下，对 SRECS 的操作能力及其元件的尺寸进行试验。环境条件变化到最高所能允许的边缘值。检查 SRECS 的最基本响应，并与安全要求规范进行比较。

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 SRECS 确认期间出现故障。

注 3：也见 6.12.2。

9 修改

9.1 目的

9.2 修改程序

在 SRECS 设计、集成和确认期间（例如，SRECS 安装和试运行时）当其修改时，本条规定的修改程序适用。

9.2.1 修改 SRECS 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 SRECS 的使用信息或说明书对其进行的干预(例如：调整、设置、修理)，本条不考虑修改。

9.2.2 要求修改 SRECS 的原因应生成文件。

9.2.3 要求的修改其影响应进行分析，以建立 SRECS 的功能安全效果。

9.2.4 修改的效果分析和其对 SRECS 功能安全影响的分析应形成文件。

9.2.5 对 SRECS 有影响的所有可接受的修改应开始返回到其硬件和/或其软件的适当设计阶段(例如规范、设计、集成、安装、试运行和确认)。所有后续阶段应按照本标准中的特定阶段所规定的程序执行。所有相关文件应修订、修改和再版。

9.2.6 以那些经过修订的文件为基础，在执行任何修改前应该准备一个完整的行动计划，并形成文件。

9.3 配置管理程序

9.3.1 配置管理程序应按照功能安全计划(见 4.2.1)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 SRECS 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：

- 识别可能受影响的危险；
- 改变要求(硬件和/或软件)的描述；
- 改变要求的原因(也见 9.2.1)；
- 做决定(和每个决定的授权)；
- 影响分析；
- 重新验证(对各阶段)和重新确定；
- 受改变要求活动影响的所有文件；
- 在改变过程中执行的所有活动，和负责这些活动的人/实体。

d) 下列信息的文件，允许随后审查：

- 配置状况；
- 版本状态；
- 所有修改和批准的理由；
- 修改的细节。

9.3.2 适当改变-控制-过程的程序应考虑下列要求：

a) 为每个 SRECS 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) 硬件和/或软件模块；
4) 试验计划和结果；
5) 验证和确认报告；
6) 已存在的软件部件，这些软件部件将并入 SRECS；
7) 创建和试验用的工具和开发环境；
8) 所有配置项有唯一标识的准确维护，这对保持 SRECS 的完整是必要的。
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，批准或拒绝该要求；

- 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（部分的）集成测试，该测试证明基线是正确的；
- 保证所有硬件或软件基线的构成和建造（包括以前的基线的再建造）。

10) 效果分析，应对每个改变要求进行评定。该分析也应包括合适的危险分析，和应考虑SRECS的所有其他修改活动。

11) 对SRECS有影响的所有可接受的修改，返回到SRECS的硬件和/或软件的适当设计阶段（例如，规范、设计、集成、安装、试运行和确认）。所有后续阶段应按照本标准执行。

12) 执行所有必要的操作，以证明已达到所要求的安全完整性。

13) 对执行必需的改变要求活动的授权应取决于影响分析的结果。

9.3.3 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) 决策过程和各有关SRECS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件（工作日志），包括：

- 识别可能受影响的危险；
- 改变要求（硬件和/或软件）的描述；
- 改变要求的原因（见9.2.1）；
- 做决定（和每个决定的授权）；
- 影响分析；
- 重新验证（对各阶段）和重新确认；
- 受改变要求活动影响的所有文件；
- 在改变过程中执行的所有活动，和负责这些活动的人/实体。

e) 下列信息的文件，允许随后审查：

- 配置状况；
- 发布状态；
- 所有修改和批准的理由；
- 修改的细节。

10 文件

10.1 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。

10.2 SRECS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。

10.3 文件应该有标题和名称，指明其内容范围。

10.4 文件应有修订索引（版本号），从而能够区别文件的不同版本。

注：有关文件管理所使用方法的进一步信息，参见IEC 82045-1:2001。

10.5 表8对可用信息及文件进行了总结。

表 8　SRECS 的信息和文件

必需的资料	子　目
功能安全计划	4.2.1
SRCF 的要求规范	5.2
SRCF 的功能安全要求规范	5.2.3
SRCF 的安全完整性要求规范	5.2.4
SRECS 设计	6.2.5
结构设计过程	6.6.1.2
SRECS 设计文件	6.6.1.8
功能块的结构	6.6.2.1.1
SRECS 体系结构	6.6.2.1.5
子系统安全要求规范	6.6.2.1.7
子系统实现	6.7.2.2
子系统体系结构(组成元素及其相互关系)	6.7.4.3.1.2
在估计容错/SFF 时的故障排他性要求	6.7.6.1c)/6.7.7.3
子系统装配	6.7.10
软件安全要求规范	6.10.1
基于软件的参数化	6.11.2.4
软件配置管理项目	6.11.3.2.2
软件开发工具的合适性	6.11.3.4.1
应用程序的文件	6.11.3.4.5
应用软件模块测试的结果	6.11.3.7.4
应用软件集成测试的结果	6.11.3.8.2
SRECS 集成测试的文件	6.12.1.3
SRECS 安装的文件	6.13.2.2
安装、使用和维护的文件	7.2
SRECS 确认测试的文件	8.2.4
SRECS 配置管理的文件	9.3.1

附 录 A
（资料性附录）
SIL 分配

A.1 概述

本附录提供了风险评估和 SIL 分配的定性方法的示例，可适用于机器的 SRCF。在 GB/T 20438.5 中有可用于 SIL 分配的其他技术的例子，并且将会在即将提出的 IEC TC44 技术规范中略述。

注 1：本附录所描述的方法论使用风险的定性评估，通常适用于对机器的 SRCF 的 SIL 分配。对特定的机器应用这种方法时所使用的风险参数（见图 A.2）和其具体的危险应与相关人员协议，以确保 SRECS 能够将风险降至足够低。

注 2：大量的机器特定标准（CEN 中的“C”类标准）中执行了风险评估，以按照 GB/T 16855.1 机器控制系统有关安全部件选择要求的类别，为简化，就是要注意下列常用的关系：要求的类别 1——要求的 SIL1、要求的类别 2——要求的 SIL1、要求的类别 3——要求的 SIL2 和要求的类别 4——要求的 SIL3。在 GB/T 16855.1 要求的类别和本标准所用要求的 SILs 之间更多映射的综合法在考虑中。

对于每一个特定危险，其安全完整性要求由 SRECS 执行的安全相关控制功能分别决定（见 5.2.4.2）。

对于 SRECS 功能，在导致评估 SIL 要求的具体危险时，图 A.1 是执行风险评价的实际方法的例子。对于每个风险应执行这种方法，这些风险会通过 SRECS 执行的安全相关控制功能而减少。图 A.1 应与本附录的指导信息结合使用。

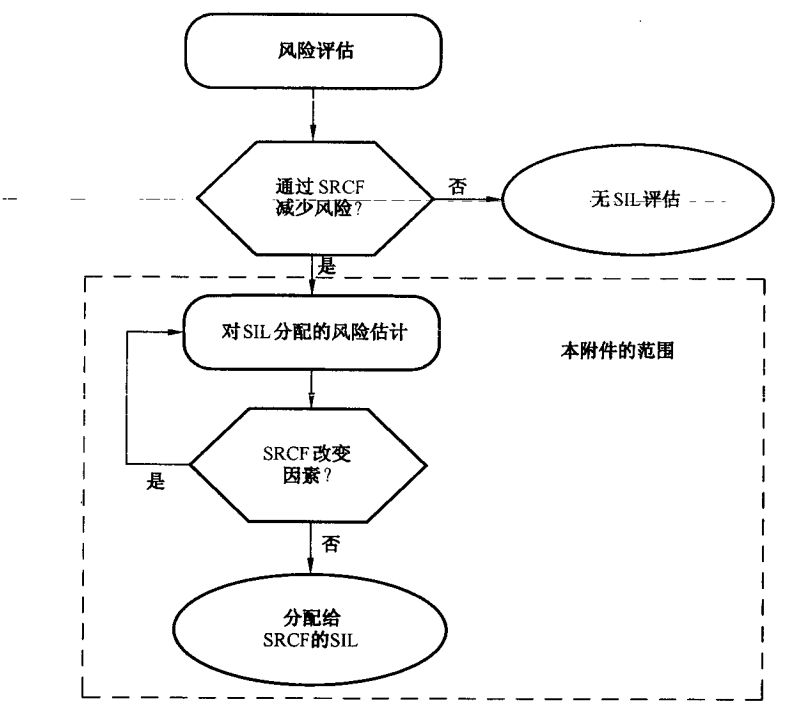


图 A.1 SIL 分配过程的工作流程

风险估计是一个迭代过程，这是指该过程需要不止一次地执行。

图 A.1 所示指向风险评估的反馈箭头。这是必需的，因为提供特殊保护措施来执行 SRCF 可能对风险参数有影响（例如，使用保护光帘可能会导致更大频率进入）。光帘失效将操作者暴露到比最初设

想的更大的风险。这要求应遵循相同的方法不断重复过程，但使用的是修改过的风险参数。

如图 A.1 所示在过程的结尾，经过评估的 SIL 就是安全相关控制功能要求的 SIL。

A.2 风险估计和 SIL 分配

A.2.1 危险识别/指示

指示危险，包括可预见的误用所引起的危险，通过执行 SRCF 减少风险。在表 A.5 中的“危险”列(栏)列出。

A.2.2 风险评估

应通过确定风险参数为每个危险进行风险评估。如图 A.2 所示，风险参数来源于下列要素：

——伤害严重程度，Se；和

——发生伤害的概率，它是下列因子的函数：

- 人们暴露在危险中的频率和持续时间，Fr；
- 危害事件发生的概率，Pr；
- 避免或者限制伤害的可能性，Av。

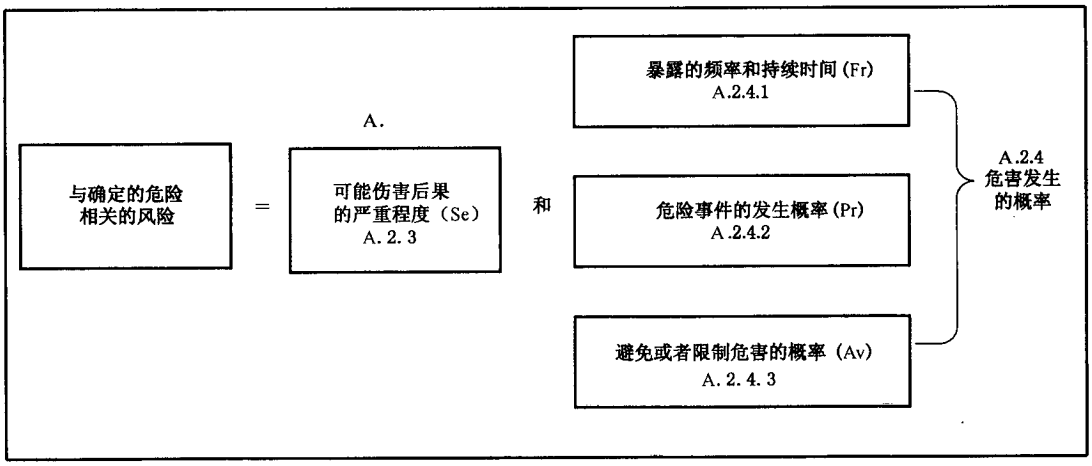


图 A.2 用于风险评估的参数

进入表 A.5 的评估通常是以对 SRCF 的最坏情况考虑为基础的。然而，在一种情况下，例如：有一个不能挽回的伤害可能发生，但是比可以挽回的伤害的发生概率要低很多，那么每一个的严重程度等级应在表格中占单独一行。可能每一行都执行不同的 SRCF。如果两行执行同一个 SRCF，那么应使用最高目标 SIL 要求。

A.2.3 严重程度(Se)

伤害或者损坏健康的严重程度能够通过考虑可以挽回的伤害、不可挽回的伤害和死亡来进行评估。根据伤害的后果从表 A.1 选择严重程度的适当值，其中：

4 代表致命的或者严重且不能挽回的伤害，在康复后难以进行相同的工作，即使有也极少；

3 代表严重或不能挽回的伤害，但在康复后存在可以继续从事相同工作的可能性。同时它还包括重大的但可以挽回的伤害，比如断肢；

2 代表可以挽回但需要专业医疗护理的伤害，包括严重的破口、刺伤及严重的撞伤；

1 代表需要急救护理的较小伤害，包括擦伤和较轻的撞伤。

对于伤害后果(Se)在表 A.1 选择适当的行。在表 A.5 的“Se”列填入适当数字。

表 A.1 严重程度(Se)分类

后　果	严重程度(Se)
无可挽回:死亡、失去眼睛或胳膊	4
无可挽回:断肢、断指	3
可挽回:要求医疗	2
可挽回:要求急救	1

A.2.4 伤害发生概率

危害发生概率的 3 个参数(即 Fr,Pr 和 Av)互相应独立地进行评估。每个参数需使用最坏情况的设想,从而确保 SRCF 没有被错误指定比必需的等级低的 SIL。通常,强烈建议使用基于任务分析的形式,以确保伤害发生概率的评估被给予适当的考虑。

A.2.4.1 暴露频率和持续时间

确定暴露的等级考虑如下述方面:

——在所有使用方式的基础上,需要进入危险区,例如,正常运行、维护;和

——进入的性质,例如,手工送料、设置。

那么应能评估暴露和进入的平均频率之间的时间间隔。

同样,可以预见暴露在危险中的持续时间,例如长于 10 min。

当持续时间短于 10 min 时,数值可能会减少到下一个等级。这并不适用于暴露频率≤1 h 的情况,当暴露频率≤1 h 时,任何时间都不会减少。

注:持续时间与在 SRCF 的保护下执行的活动的性能相关。GB 5226.1 和 ISO 14118 有关动力隔离和功率耗散的要求应适用于主要干预。

这个因素不包括 SRCF 的失效考虑。

对于暴露的频次和持续时间在表 A.2 中选择适当的行。在表 A.5 中“Fr”列填入适当的数字。

表 A.2 暴露的频率(Fr)和持续时间分级

暴露的频率(Fr)和持续时间	
暴露的频率	持续时间 >10 min
≤1 h	5
>1 h 至≤1 d	5
>1 d 至≤2 星期	4
>2 星期至≤1 a	3
>1 a	2

A.2.4.2 危险事件发生概率

伤害发生的概率应独立于其他相关参数 Fr 和 Av 进行评估。每个参数应作最坏情况的设想,以确保 SRCF 没有被错误指定比所需等级低的 SIL。为防止以上事件的发生,强烈建议使用基于任务分析

的形式，以确保伤害发生概率的评估被给予适当考虑。

参数评估应考率下述因素：

a) 在不同的使用方式(例如正常操作、维护、故障发现)，与危险有关的机器零部件行为的可预见性。

有必要仔细考虑控制系统，特别是与意外启动风险相关的控制系统。但是不要考虑任何SRECS的保护效应。如果SRECS失效，为了评估暴露的风险量这是必需的。概括来说，必须考虑机器或进行加工的材料是否有以外方式运作的倾向。

机器的行为将变化，从完全可以预见到无法预见，但是意外事件不能打折扣。

注1：可预见性经常与机器功能的复杂性相关。

b) 规定的或可预见的与相关危险的机器零部件间的交互作用有关的人类行为特性，以下列因素为特征：

——工作压力(例如，由于时间限制，工作任务，可感觉的损坏限制)；和/或

——缺乏危险相关的认识。这会受一些因素的影响，例如：技能、培训、经验、机器/加工的复杂性。

这些属性通常并不直接受SRECS设计者的影响，但是任务分析将暴露那些不能完全预见所有可能方面(包括不可预见的结果)的活动。

危险事件的发生概率“非常高”应选择反映正常生产限制和最坏情况的考虑。对于使用任何较低值，正确的原因(例如，良好定义的应用和用户高水平知识的能力)是必需的。

注2：任何所需的或假定的技能、知识等都应在使用信息中陈述。

对于危险事件发生概率(Pr)在表A.3中为选择的适当的行。在表A.5中Pr列标示适当的数字。

表A.3 概率(Pr)分类

发生概率	概率(Pr)
非常高	5
或许	4
可能	3
很少	2
可忽略	1

A.2.4.3 避免或限制伤害的概率(Av)

这个参数可以通过考虑机器设计和其预期应用方面来评估：预期应用有助于避免或限制来自危险的伤害。这些方面包括，例如：

——危险事件的发生是突发的，快速的，或是缓慢的；

——撤离危险的空间可能性；

——元件或系统的性质，例如，刀通常是锋利的，日常环境里的管道通常是热的，电虽然看不见，但其性质通常是危险的；和

——识别危险的可能性。例如电气危险：铜棒不因其是否带电压而改变它的外观；人们需要用仪器来确定电气设备是否通电；环境条件，例如高噪声级可能妨碍人们听到机器的启动。

对于避免或限制损害概率(Av)，从表A.4中选择适当的行。在表A.5中的Av列填入适当的数字。

表 A.4 避免或限制伤害的概率(Av)等级

避免或者限制伤害的概率(Av)	
不可能	5
极少发生	3
有可能	1

A.2.5 损害概率的级别(CI)

对每一种危险,如果适用,则对每一个严重等级,叠加在 Fr,Pr 和 Av 列的分数,然后在表 A.5 的 CI 列中输入总和。

表 A.5 用于决定伤害概率级别的参数(CI)

系列号	危险	Se	Fr	Pr	Av	CI
1						
2						
3						
4						

A.2.6 SIL 分配

用表 A.6,其中表示严重程度(Se)的行与有关的列(CI)相交,交叉点即表示是否需要采取措施。黑色区域表示 SIL 被指定为 SRCF 目标,浅阴影区域表示应使用其他措施的建议。

表 A.6 SIL 分配矩阵

严重程度(Se)	级别(CI)				
	3-4	5-7	8-10	11-13	14-15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2
1				(OM)	SIL1

例如:如果一个特定的危害的 Se 为 3,Fr 为 4,Pr 为 5,Av 为 5,则:

CI=Fr+Pr+Av=4+5+5=14

根据表 A.6,将会分配 SIL3 给 SRCF,从而减轻特定的危险。

图 A.3 显示使用本附录用于记录 SIL 分配练习结果的文件示例。

风险评价和安全措施

产品：_____

发布者：_____

日期：_____

黑色区域＝必要的安全措施

灰色区域＝所建议的安全措施

后果	严重程度，Se	级别 CI					频率和持续时间，Fr		危险事件概率，Pr		避免伤害概率，Av	
		3-4	5-7	8-10	11-13	14-15						
死亡，失明或者肢残	4	SIL2	SIL2	SIL2	SIL3	SIL3	≤1 h	5	很高	5		
永久性失去手指	3		OM	SIL1	SIL2	SIL3	>1 h ≤1 d	5	很可能	4		
可恢复，专业医疗	2			OM	SIL1	SIL2	>1 d ≤2 星期	4	可能	3	不可能	5
可恢复，急救	1				OM	SIL1	>2 星期 ≤1 年	3	很少	2	可能	3
							>1 年	2	可忽略	1	可能	1

序号	危害编号	危害	Se	Fr	Pr	Av	CI	安全措施	安全

说明

图 A.3　SIL 分配过程形式示例

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

B.1 概述

本标准使用的SRECS设计结构化方法，定义一套安全相关控制功能和安全完整性要求的方法，即功能细分成若干子功能。该过程用于实现进入机械部分的功能安全的技术框架，图B.1描述适用于每个等级的术语，在机器安装，当集成SRECS时，这些术语非常重要。

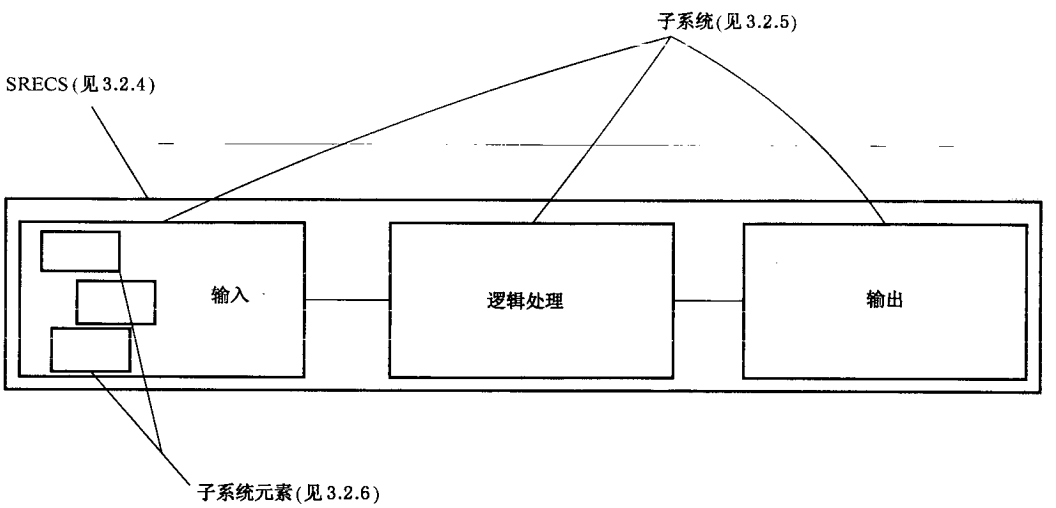
可以通过验证和确认过程使用本设计方法，以证明SRECS满足了条款5所描述的安全要求规范。

以下SRECS设计示例是为了阐明功能分解的原则和按照条款6的要求实现规定的安全相关控制功能。因此本示例是简单化的，不考虑在实践中可能要求的附加措施，例如“保持—运转”装置。

总体来说，图B.1显示的术语是为了将设计过程描述成两个关键阶段：

——SRECS设计可以由机器设计者或控制系统集成商执行；和

——子系统（和子系统元素）设计，适用于电气设备和控制设备（例如接触器，联锁开关，可编程逻辑控制器）的供应商和机器设计者或控制系统集成商。



图B.1 功能分解的术语

B.2 示例(见图 B.2)

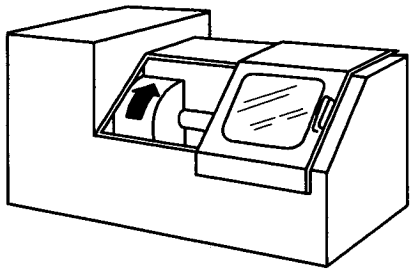


图 B.2 机器示例

本标准所使用的方法是基于自上而下的结构化设计,以实现安全相关控制功能规范和实现这些功能的 SRECS 设计。

步骤 1:SRCF 安全要求规范(条款 5)

由 SRCF 安全要求规范可以得出如图 B.3 信息。

图 B.3 SRCF 要求说明

步骤 2:SRECS 设计开发过程(见 6.6.2)

步骤 2.1:安全要求规范中所规定的安全相关控制功能被分解为功能块结构(见图 B.4)。

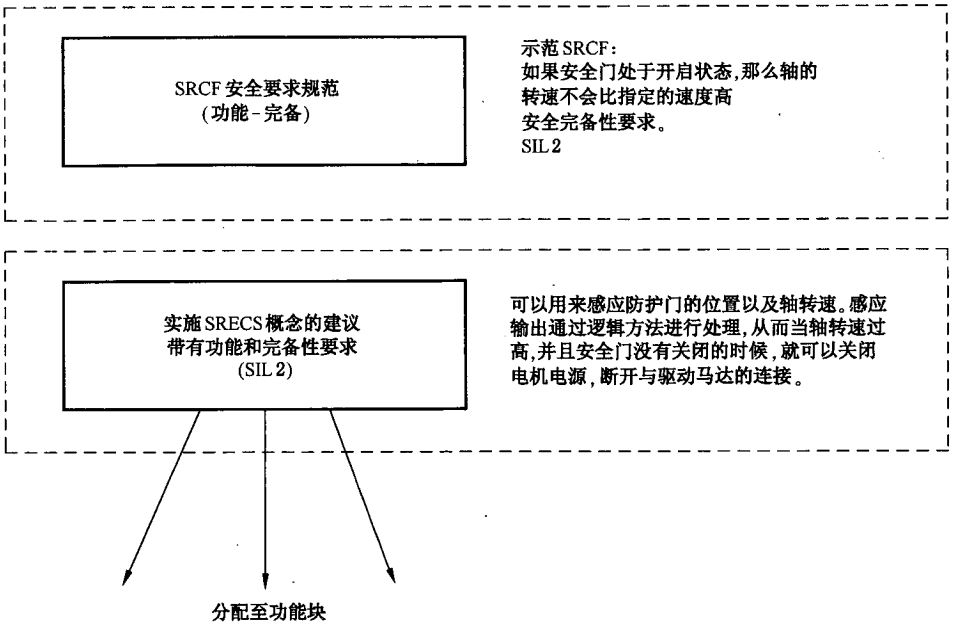


图 B.4 分解功能块结构

步骤 2.2:功能块结构为 SRECS 的结构提供一个初步概念。各功能块的安全要求来自相应的安全相关控制功能的安全要求规定。

实现各功能块的要素必须至少达到分配给 SRCF 的相同 SIL 能力。图 B.5 即表示 SIL2 能力(例如 FB1 SILCL2,等)。

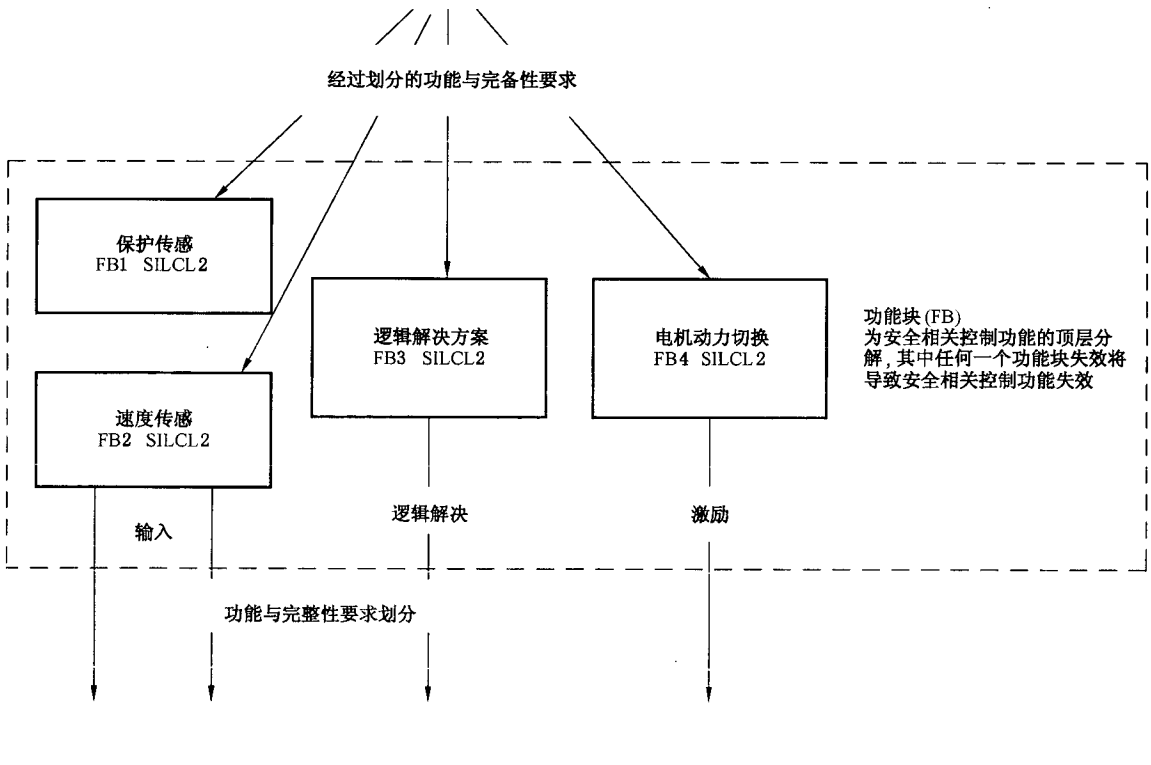


图 B.5 SRECS 的结构的初步概念

步骤 3:每个功能块被分配到 SRECS 结构内的子系统,各子系统都由子系统元素,需要时,和诊断功能构成,以确保能检测出故障,并采取适当行动(见 6.2)。

体系结构应以子系统的术语和子系统间的相互关系来描述 SRECS。就本例而言,有若干可供选择的方案可用于实现 SRECS 及其子系统结构。

示例 1:在此例中(见图 B.6),各子系统内嵌诊断功能。

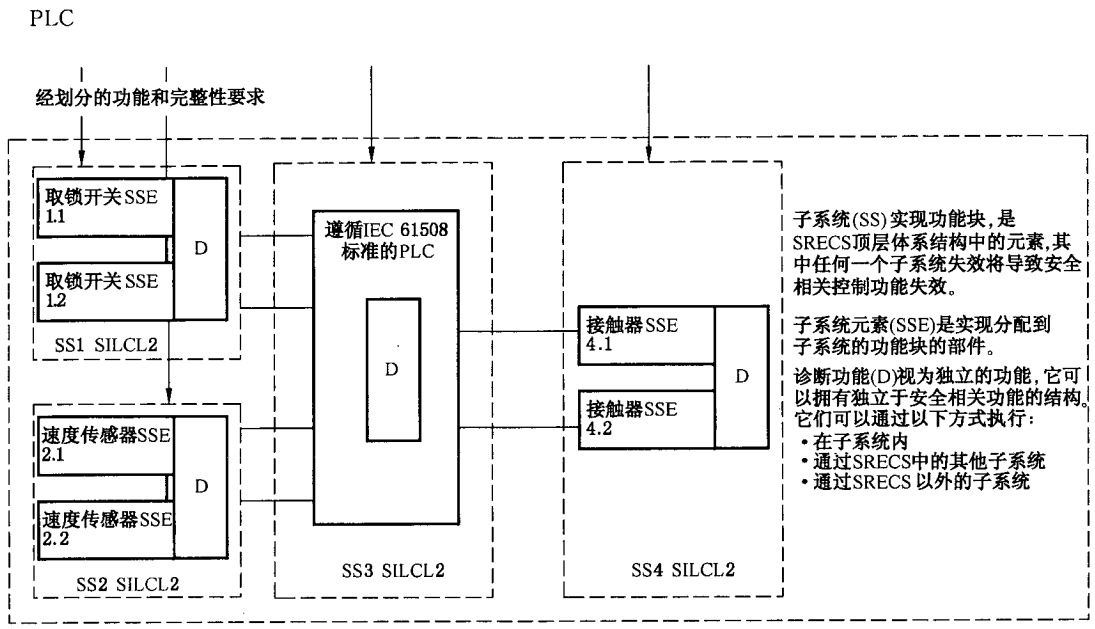


图 B.6　各子系统(SS1 到 SS4)内嵌诊断功能的 SRECS 体系结构

示例 2:在此例中(见图 B.7),诊断功能嵌入 SS3 的可编程逻辑控制器(PLC)中,PLC 满足 GB/T 20438 相关方面的要求。

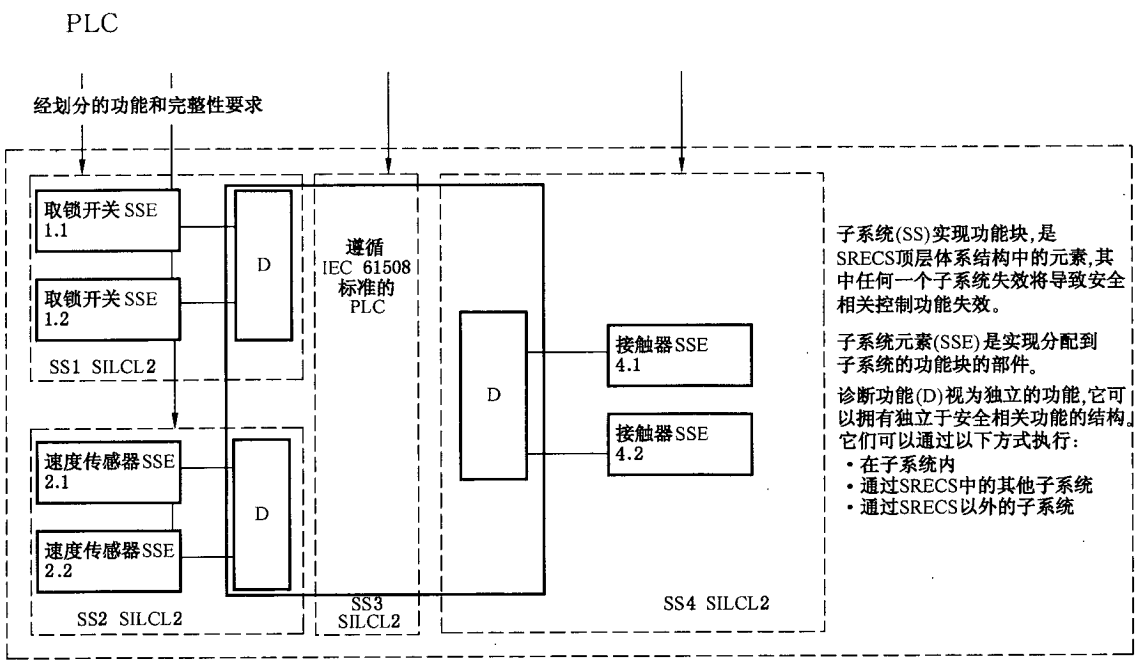


图 B.7　子系统 SS3 内嵌诊断功能的 SRECS 体系结构

步骤 4:由 SRECS 实现的 SIL 的评估(见 6.6.3)

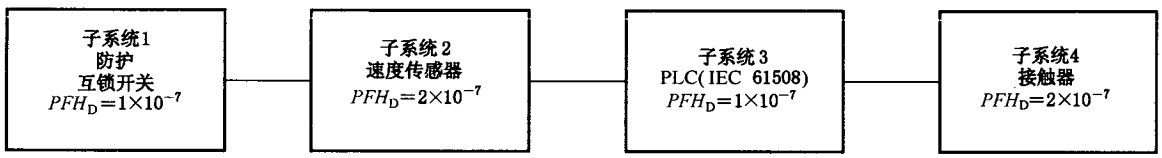
SRECS 要求 SIL 应小于或等于任何子系统的 SILCL 的最低值。SRECS 危险随机硬件失效概率(PFH_{DSRECS})是所有执行安全相关控制功能的子系统每小时危险失效的概率(PFH_{D1}～PFH_{Dn})的总和,在适当的场合还应包括数字数据通信过程中的危险传送错误概率(P_{TE}):

$$PFH_{DSRECS} = PFH_{D1} + \ldots + PFH_{Dn} + P_{TE}$$

对于此例,安全相关控制功能的目标失效值是 SIL2 和来自表 3(见 5.2.4.2),这相当于每小时危险

失效概率(PFH_D)≥10^{-7}到<10^{-6}的范围。因此,假设子系统每小时危险失效概率如下所示,那么所有子系统每小时危险失效概率的总和即可以评估,如图 B.8 所示。

因此,在此例中,可以表明在 SIL2,SRECS 的设计满足用以实现安全相关控制功能的所有要求。



$$PFH_{DSRECS}=(1\times10^{-7})+(2\times10^{-7})+(1\times10^{-7})+(2\times10^{-7})=6\times10^{-7}$$

图 B.8 对于 SRECS 的 PFHD 评估

附 录 C
（资料性附录）
嵌入式软件设计和开发指南

注：本附录用于说明为满足 IEC 61508-3 要求的基本方法。如果不采用进一步措施，它本身不提供与 IEC 61508-3 的一致性。

C.1 综述

本附录用于帮助人们设计和开发嵌入式软件以实现 SRECS 内的安全相关控制功能。

主要目标是进行总体指导，防止嵌入式软件失效和嵌入式软件的其他意外行为，而导致系统产生危险故障。

为达到这些目标，应考虑下列几点：

——SRECS 软件要素的主要特性的描述，应具备保证质量和安全性（软件要素指导）；

——对于那些涉及软件设计，确立所有相关的技术活动和软件开发有关的规定。在开发此类软件的制作期间，可用于指导设计者（软件开发过程指导）；

——软件评估的参考性框架。让软件设计人员和/或分析人员决定软件要素是否符合 SRECS 或要被分析的 SRECS 子系统的安全要求（软件验证指导）。

本附录提供一套基本指导，与 IEC 61508-3 一致，适用于微处理器的嵌入式软件。

C.2 软件要素指导

本条款表述指导方针，即 SRECS 或 SRECS 子系统的嵌入式软件要素应履行操作安全和高质量。为了获得这类软件要素，应确立若干活动、某些组织和若干原则。这些在开发周期应尽早进行。

C.2.1 系统结构界面

硬件结构对软件施加的限制应定义并形成文件。对于被监控的机器或系统的安全性，任何软件/硬件相互作用的结果应由设计者进行识别和评估，并在软件设计时考虑。

注：限制包括协议和格式、输入输出频率、上升沿和下降沿或电平、输入数据采用负逻辑等。列出这些限制可以使其在开发活动之初就纳入考虑范围，当软件安装在目标硬件时，应减少软件和硬件之间不兼容的风险。

C.2.2 软件规范

软件规范应考虑下列各项：

——安全相关控制功能具有对性能准则（精确度，准确度）和瞬时限制（响应时间）的定量描述，可能时，应考虑所有因素的容差或余量；

——系统配置或结构；

——说明有关硬件安全完整性（逻辑解算器，传感器，操动器等）；

——说明有关软件完整性；

——有关存储器容量和系统响应应时间的限制；

——操作者和设备界面；

——软件自我监控和由软件执行的硬件监控的说明；

——当系统运行时允许对所有安全相关控制功能进行验证的说明（例如，在线测试，快速信号的捕

获时间，与扫描频率一致）。

注 1：用于监控的说明，考虑开发的安全目标和操作限制（持续操作时间等），可能包括某些装置，例如看门狗，中央处理器（CPU）加载监控，输出反馈至输入实现软件自监控。对于硬件监控，CPU 和存储器监控等。安全相关控制功能验证的说明：例如，定期验证安全装置正确操作的可能性应包括在规范中。

对于各功能模式，应规定其功能要求。一种模式到另一种模式的模式切换也应规定。

注 2：功能模式可包括正常模式和一个或多个降级模式。目的是为了规定所有情况下的行为，以避免在非正常模式下的意外行为。

C.2.3 预存软件

术语“预存”软件是指还没有为现有系统具体开发并集成到软件其余部分中的源模块。包括先前项目设计人员开发的软件元素或商用软件（例如计算、数据排序算法模块）。

当处理这类软件时，特别是商用软件元素时，设计人员并不是总能访问用以满足预先要求所需的所有要素（例如，已经进行什么试验？设计文件是否可得到？）。因此，在早期需要与分析人员具体协调。

设计人员应向分析人员指示预存软件的使用。设计人员应证明预存软件具有和其他软件元素同样的水平。这类证明应做到：

a） 对预存软件采用与软件其他部分同样的验证活动；和/或

b） 在可比的执行环境中，预存软件有相比类似系统的作用时，通过实际经验证明（例如，可能需要评估编译程序更改或不同软件结构格式更改的后果）。

注 1：指示预存软件使用的目标是为了就该类软件可能导致的任何意外困难与分析人员尽早进行协商。如果预存源模块的开发不如软件其余部分严格，那么其集成可能会导致某些异常或不安全行为。

预存软件应采用与其他软件部分相同的配置管理和版本控制原则进行识别。

注 2：应行使对所有软件元件的配置管理和版本控制，不管其来源。

C.2.4 软件设计

软件设计的描述应包括下列描述：

——定义符合规范要求的结构的软件结构；

——所有构成软件结构的模块的输入和输出（例如，以内部和外部数据字典的形式）；

——中断；

——全局数据；

——各软件模块（输入/输出，算法，设计特性等）；

——使用的模块或数据文件库；

——使用的预存软件。

软件应以逻辑方式划分模块和编写，以便验证或维护：

——若可能，每一模块或模块组应对应规范中的某项功能；

——模块间的接口应尽量简化。

注：正确软件架构的总体特征可总结如下：模块应拥有高水准的功能内聚以及与所处环境的简单接口。

软件应：

——限制使用全局变量的数目或程度；

——在存储器中，数组的控制分布（避免数组溢出的风险）。

C.2.5 编码

源代码应：

——可读，可理解，和接受测试；

——满足软件模块的设计规范；

——遵循编码手册说明。

C.3 软件开发过程指导

C.3.1 开发过程:软件生命周期

适用于软件生命周期的如下指导目标旨在获取软件开发组织的正式化描述,特别是不同技术任务构成该开发。

软件开发生命周期应当详细规定和文件化(例如,在软件质量计划中)。生命周期应包括所有技术活动和必要阶段及足够的软件开发。

生命周期各阶段应分成不同基本任务和包括下述描述:

——输入(文件、标准等);

——输出(制作的文件、分析性报告等);

——执行的活动;

——进行的验证(分析、试验等)。

C.3.2 文件:文件管理

文件应符合本标准第10条的规定。

C.3.3 配置和软件修改管理

配置管理和版本管理是任何开发都不可或缺的部分。两者可能都需要进行批准。事实上,只有当提供的配置能够识别时,该批准才有效。配置管理包括配置识别活动,修改管理,建立参考点和软件元素归档,包括相关数据(文件、试验记录等)。贯穿整个项目生命周期,主要目标是提供:

——定义的和受控的软件配置,该配置保证物理归档和用于重新生成前后一致的可执行代码(考虑未来软件制作或修改);

——修改管理的参考基础;

——控制方法,使任何问题能进行正确分析,经批准的修改能正确执行。

有关修改,原因可来自,例如:

——功能安全低于规定的;

——系统故障经验;

——新的或修正的安全法规;

——对机器或其使用的修改;

——对总体安全要求的修改;

——操作和维护性能的分析,指示性能低于目标。

C.3.4 配置和归档管理

应规定配置管理和修改管理程序和文件。该程序至少应包括下列项目:

——由配置管理的各细项,至少包括软件规范、初步和详细的软件设计、源代码模块、计划、程序和确认试验的结果;

——识别规则(源模块、软件版本等);

——修改处理(要求记录等)。

配置的各项应能识别可能发生的任何更改和相关元素的版本。

注1:目的是为了能够追溯各项开发历史:进行过哪些修改,为什么进行修改和什么时候进行的修改。

软件配置管理应允许准确和唯一的软件版本识别。配置管理应关联所有需要证明功能安全的项目

(和其版本)。

软件配置中的所有项目应在试验或分析人员为最终软件版本评估前由配置管理程序覆盖。

注2:目的是为了确保对软件执行评估程序时,所有元素处于正确状态。任何后续更改可能是软件修订需要的,因此由分析人员可以识别。

应建立软件和相关数据的归档程序(备份和档案存储的方法)。

注3:这些备份和档案可用于软件功能生存期内维护和修改。

C.3.5 软件修改管理

任何对SRECS功能安全有影响的软件修改应服从为修改和配置管理建立的规则,以便在最高"上游"点在开发过程重新开始时需要考虑的修改,没有降低功能安全。

注:值得注意的是,文件也应更新,和执行所有需要的验证活动。这将保证软件在进行修改后能保持其所有的初始特性。

C.4 开发工具

与软件版本有关的文件(例如,在版本控制文件中),在开发程序期间使用的工具(编译程序、连接程序、试验等),应识别(名称、参照代号、版本等)。

注:工具的不同版本不一定得出相同的结果。因此,工具的准确识别可在版本发生修改时,直接证明生成可执行版本的过程的连续性。

C.5 复制,传播

C.5.1 可执行代码产生

软件产生期间,任何选项或更改应记录(例如,在版本表中),这样就可能说明软件是什么时间和怎样生成的。

C.5.2 软件安装和开发

使系统设计人员注意的与安全相关控制功能有关的所有失效应记录和分析。

注:这说明设计人员知道传达给他的任何安全相关失效,和采取适当行动(例如,对其他用户提出告警,软件修改等)。

C.6 软件验证和确认

验证活动的目的是为了证实,来自开发周期的特定阶段的软件元素符合先前阶段制定的规范和任何可应用标准或规则。验证活动也作为检测手段和说明在软件开发过程中可能引入的任何错误。

软件验证不是一系列简单的试验,对于本附录考虑的相对小型的软件元素,即使试验是主要的。其他活动(例如审查和分析)不管是否与这些试验有关,也认为是验证活动。在某些情况,它们可以代替一些试验(例如,试验不能进行的事件,因为试验可能导致硬件损坏)。

C.7 验证和确认总则

在软件开发的不同阶段,分析人员应通过实施审查或专门技能认定来评估软件的一致性。

软件生命周期的所有技术方面经受分析人员的评估。应允许分析人员查阅所有验证报告(试验,分

析等)和在软件开发期间使用的所有技术文件。

注 1：分析人员在规范阶段的介入优于后期介入，这样有可能限制任何决定所产生的影响。另一方面，项目的财务和人力方面与评估无关。

注 2：提供软件开发过程中所有活动的令人满意的证据，对申请人是有利的。

注 3：分析人员应该在其处理中，包含所有的必要元素，以便明确地表述其观点。

软件一致性的评估是对具体的、可参考的软件版本进行的。以前评估的软件的任何修改，对已得到分析人员最终意见认可的部分应指出，以便进行任何补充的评估活动来更新该意见。

注 4：任何修改可能更改软件行为；因此分析人员进行的评估只适用于准确的软件版本。

C.8 验证和确认复审

分析活动和软件设计验证应核实符合规范。

注 1：目的是为了确保软件规格和设计(详细设计和初步设计)是一致的。

外部确认复审(由分析人员执行)应在确认阶段结束时进行。

注 2：可用于确定元素是否符合规范。

复审结果应形成文件并归档，它应包括复审过程中确定的所有活动的列表，以及复审结论(决定是否进行下次活动)。复审中所规定的活动应进行监控和处理。

C.9 软件测试

C.9.1 一般确认

在填写第一张试验表前，在试验计划中建立试验策略是非常重要的。该策略应指出采取的方法，根据试验覆盖范围设定的目标，使用的环境和具体技术，应用的成功准则等。

试验目的应符合软件的类型和具体因素。这些准则决定承担的试验类型——功能试验、限制试验、非限制试验、性能试验、负载试验、外部设备失效试验、配置试验以及由试验覆盖的目标范围(功能模块试验、安全相关控制功能试验、规范中各元素试验等)。

新软件版本的验证应包括非回归试验。

注：非回归试验用于确保对软件的修改没有以任何意外方式修改软件的行为。

C.9.2 软件规格验证：确认测试

这些验证的目的是在目标系统环境中检测与软件有关的错误。该类型验证检测到的错误包括：处理中断的各种错误机制，运行时间要求的考虑不够，在瞬变模式(启动、输入流、降级模式中的切换等)中软件操作的错误响应，访问存储器中不同资源或组织问题的矛盾，不能检测故障的集成试验，软件/硬件接口错误和堆栈溢出。确认试验是软件规格验证的主要组成部分。

试验的覆盖范围应以可追溯矩阵详述并确保：

——确认试验应覆盖规范的各元素，包括安全机制；

——可验证任何操作模式下的软件实时行为。

此外，确认应在代表 SRECS 或 SRECS 子系统的操作条件下进行。

注 1：这保证软件在操作中如预期般的反应。它只适用于当试验条件可能破坏硬件的情况(例如，不能模拟的部件的物理故障)。重要的是，确认应在 RECS 或 SRECS 子系统的操作条件下进行(例如，软件和硬件的最终版本，和安装在目标系统上的软件)。任何其他组合可能会降低试验效率和其代表要求的分析。

确认结果应记录在确认报告中，至少包括下列方面：

——所确认的软件和系统版本；

——执行的确认试验的描述(输入、输出、测试程序)；

用于确认或评估结果的工具和设备；

——各确认试验是否成功的显示结果；

——确认评价：识别结果不符合，对安全的影响，是否接受确认的决定。

确认报告应适用于各已交付的软件版本，应与各交付软件元素的最终版本一致。

注2：此报告可用于提供试验的确实已执行的证明和结果是正确的（或包含可解释的偏离）。以后，对于未来的软件版本或其他项目，它也可用于改写试验。保证各交付的版本按最终形式已确认。另一方面，它不强求对现有代码的每次修改进行完整确认，某些情况，影响分析可以证明部分确认。

C.9.3 软件设计验证：软件集成试验

该验证注重软件模块的正确组装和软件部件间的相互关系。该验证可用于暴露下列类型的错误：变数和常数的不正确初始化，参数传递错误，数据变更，特别是全局数据，事件和操作的不正确排序。

软件集成试验试应能验证：

——软件执行的正确排序；

——模块间的数据交换；

——性能准则的考虑；

——全局数据的不变更。

试验覆盖范围应以可追溯矩阵明确表示，证明承担的试验和规定的试验目标间的一致性。

集成试验结果应记录在软件集成试验报告中，其中至少应包括下列方面：

——集成软件的版本；

——所执行试验的描述（输入、输出、程序）；

——集成试验结果及其评估。

C.9.4 详细设计验证：模块试验

模块试验注重软件模块及其与详细设计的一致性。对于大型复杂软件元素，该活动可能是不可缺少的，但是，对于这里所述的小型软件元素只是建议。该阶段的验证程序允许检测下列错误：

——不能产生符合软件规范的算法；

——错误循环操作；

——错误逻辑决定；

——不能正确运算输入数据的有效组合；

——对缺失或变更的输入数据的错误反应；

——阵列界线的破坏；

——错误计算顺序；

——精度不够；

——算法的准确性或性能；

采用输入数据，对各软件模块实施一系列试验以检验模块是否满足在详细设计阶段所规定的功能。

本试验覆盖范围应以可追溯矩阵提供，证明试验结果和规定试验的目标一致。

附 录 D
（资料性附录）
电气/电子部件的失效模式

SRECS及其子系统的最低操作环境应符合GB 5226.1的规定。但是，在实际操作中，许多子系统（例如AOPDs）应符合的产品标准可能规定更复杂的操作环境。

表D.1列举了来自参考源的电气/电子部件失效模式率。这些值可能与其他来源提供的信息不同。一般，采用的失效模式数据应反映部件的实际应用。

注1：下表并不是部件失效模式的详尽列表。

注2：失效率数据应由子系统制造商提供。

表D.1 电气/电子部件失效模式率示例

部 件	失效模式	标准失效模式率（%）
需求强制断开的开关，例如按钮，急停装置，位置开关，凸轮操作开关，选择开关	触头将不断开	20
	触头将不闭合	80
机电位置开关，限位开关，手动操作开关等（按要求不强制断开）	触头将不断开	50
	触头将不闭合	50
继电器	当线圈断电时，所有触头保持在通电位置	25
	当线圈通电时，所有触头保持在断电位置	25
	触头将不断开	10
	触头将不闭合	10
	切换触头的3个触头间同时短路	10
	常开和常闭触头的同时闭合	10
	两对触头间和/或触头与线圈端子间的短路	10
断路器，差分断路器，漏电保护器	当线圈断电时，所有触头保持在通电位置	25
	当线圈通电时，所有触头保持在断电位置	25
	触头将不断开	10
	触头将不闭合	10
	切换触头的3个触头间同时短路	10
	常开和常闭触头同时闭合	10
	两对触头间和/或触头与线圈端子间的短路	10
接触器	当线圈断电断电时，所有触头保持在通电位置	25
	当线圈通电时，所有触头保持在断电位置	25
	触头将不断开	10
	触头将不闭合	10

表 D.1（续）

部　　件	失 效 模 式	标准失效模式率（%）
	切换触头的 3 个触头间同时短路	10
	常开和常闭触头同时闭合	10
	两对触头间和/或触头与线圈端子间的短路	10
熔断器	断开失效（短路）	10
	开路	90
接近开关	输出时永久低阻	25
	输出时永久高阻	25
	电源中断	30
	机械失效引起的开关失效	10
	切换触头的 3 个端子间同时短路	10
温度开关	触头将不闭合	30
	触头将不断开	10
	相邻触头间的短路	10
	切换触头的 3 个端子间同时短路	10
	传感器故障	20
	检测或输出特性的改变	20
压力开关	触头将不闭合	30
	触头将不断开	10
	相邻触头间的短路	10
	切换触头的 3 个端子间同时短路	10
	传感器故障	20
	检测或输出特性的改变	20
电磁阀	未通电	5
	未断电	15
	切换时间的改变	5
	漏电	65
	其他失效模式（见注 4）	10
分立半导体	任意连接的开路	25
	任意两连接间的短路	25
	所有连接间的短路	25
	特性的变更	25
变压器	单独绕组的开路	70
	不同绕组间的短路	10

表 D.1（续）

部　件	失效模式	标准失效模式率（%）
	一个绕组的短路	10
	有效匝数比的改变	10
电感	开路	80
	短路	10
	值的随机变化	10
电阻器	开路	80
	短路	10
	值的随机变化	10
电阻器网络	开路	70
	短路	10
	任意连接间的短路	10
	值的随机变化	10
电位计	单独连接的开路	70
	所有连接间的短路	10
	任意两连接间的短路	10
	值的随机变化	10
电容器	开路	40
	短路	40
	值的随机变化	10
	变化值 $\tan\alpha$	10
	漏电	65
	其他失效模式（见注 4）	10
	特性的变更	25
不可编程的集成电路（非复杂，例如，少于 1 000 门和/或少于 24 个管脚，运算放大器，移位寄存器和混合模块）	任意连接的开路	20
	任意两连接间的短路	20
	固定故障	20
	输出的寄生振荡	20
	变化值（例如，模拟装置的输入/输出电压）	20
光耦合器	单个连接的开路	30
	任意两处输入连接间的短路	30
	任意两处输出连接间的短路	30
	任意两处输入和输出连接间的短路	10

表 D.1（续）

部　件	失效模式	标准失效模式率（%）
插头和插座，多管脚连接器	任意 2 个相邻管脚间的短路	10
	任意导体到外露可导电部件的短路	10
	单个连接器管脚的开路	80
接线盒	相邻端子间的短路	10
	单个端子开路	90

注 1：本数据出自一些工业来源，包括：

MIL-HDBK 217F（注 2）电子设备的可靠性预计（28-02-95），部件压力分析；

MIL-HDBK 217F（注 2）电子设备的可靠性预计（28-02-95），附录 A，部件计数可靠性预计；

SN 29500 第 7 部分，部件的失效率，继电器的期望值，1992 年 4 月；

SN 29500 第 11 部分，部件的失效率，接触器的期望值，1990 年 8 月。

SN 29500 系列的文件可公开得到，也可通过下列途径获取：

Siemens AG，CT SR SI；

Otto-Hahn-Ring 6；

D-81739 München。

注 2：电气失效模式取自 GB/T 16855.2 的表 D.5。机械失效模式（若适用）取自 GB/T 16855.2 的附录 A，附录 B 和附录 C。

注 3：对于电气/电子部件，例如电阻器和电容器，不同的设计可能会与表中所述的失效模式不同。

注 4：适用于电磁阀的其他失效模式包括：

——非切换（保持在结束或零位置）或不完全切换（保持在随意中间位置）；

——初始切换位置的自发变更（无输入信号）；

——长时间漏电流速的更改；

——阀门外壳的爆裂或移动部件的损坏以及安装或外壳螺丝的损坏/破裂；

——导致伺服系统和比例阀失控行为的气动/液压故障。

注 5：失效率数据和失效模式比率的其他来源信息包括：

——UTE C 80-810 RDF 2000：可靠性数据手册——电子部件，PCB 和设备可靠性预计的通用模式；

失效模式/机械交付 FMD-91，RAC 1991。

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

表 E.1 SRECS 的电磁现象（EM）和提高的抗扰度

端口 （见注 1）	现象	基本标准	SRECS 性能附加试验的增加值 （见 6.4.3）
外壳	静电放电（ESD）	GB/T 17626.2—2006	6 kV/8 kV 接触/空气放电（见注 2）
	电磁（EM）场	GB/T 17626.3—2006	20 V/m（80 MHz～1 GHz） 6 V/m（1,4 GHz～2 GHz） 3 V/m（2 GHz～2,7 GHz） （见表 E.2 和注 3）
	额定电源频率磁场	GB/T 17626.8—2006	30 A/m（见注 4 和注 5）
交流电源	电压暂降/短时中断	GB/T 17626.11—2008	0,5 周期 30%减少（见注 5）
	电压变化/中断	GB/T 17626.11—2008	250 周期 >95%减少（见注 5）
	脉冲群	GB/T 17626.4—2008	4 kV
	浪涌	GB/T 17626.5—2008	2 kV 线到线/4 kV 线到地 （见注 6）
	无线电传导频率 （RF）	GB/T 17626.6—2008	在给定的频率下 10 V（见表 E.3 和注 3）
直流电源（见注 7）	脉冲群	GB/T 17626.4—2008	4 kV
	浪涌	GB/T 17626.5—2008	1 kV 线到线/2 kV 线到地 （见注 6）
	传导 RF	GB/T 17626.6—2008	在给定的频率下 10 V （见表 E.3 和注 3）
I/O 信号/控制线路	脉冲群	GB/T 17626.4—2008	线路>3 m 2 kV
	浪涌	GB/T 17626.5—2008	2 kV 线到地（见注 8）
	传导 RF	GB/T 17626.6—2008	在给定的频率下 10 V（见表 E.3 和注 3）
功能接地	脉冲群	GB/T 17626.4—2008	2 kV

注 1：端口是 SRECS 与其带外部电磁环境的子系统的特别接口。

注 2：等级应按照 GB/T 17626.2—2006 中描述的环境条件应用。对部件，除了工作职员以外的其他人员也可能接触到的部件按照 ESD 控制规定的程序，但不是对设备，设备只限于受过适当培训的人员才能接近。

注 3：增长值应适用于移动数字无线电广播发射机使用的频率范围，除了采取可靠措施防止来自这类设备的电磁干扰。单个设备需考虑到 ISM 频率。

注 4：只对磁敏感设备。

注 5：增长的值不适用于无需考虑功能安全的现象。

注 6：允许外部保护装置达到抗扰度。

注 7：不连接到 D.C. 的配电网络的设备/系统部件间的直流连接可作为 I/O 信号/控制端口处理。

注 8：只在长距离线路的情况下。

注 9：参考 IEC 61326-3（准备中）。

注 10：在功能安全的情况下，产品标准（例如 GB/T 19436.1—2004）对于特定的 EMC 现象规定适用于 SRECS 子系统的不同的试验等级。

表 E.2 RF 场试验选择频率

系　统	频　率
GSM	(890～915)MHz
GSM	(1 710～1 785)MHz
GSM	1 890 MHz
UMTS	开发中
Walkie Talkie	开发中
ISM	(433.05～434.79)MHz
ISM	(83.996～84.004)MHz
ISM	(167.992～168.008)MHz
ISM	(886.000～906.000)MHz

表 E.3 传导 RF 场选择频率

系　统	频　率
ISM	(6.765～6.795)MHz
ISM	(13.553～13.567)MHz
ISM	(26.957～27.283)MHz
ISM	(40.66～40.70)MHz

附 录 F
（资料性附录）
共同原因失效(CCF)敏感度评估方法

F.1 概述

本资料性附录为适用于子系统设计的CCF评估提供简便的定性方法。

F.2 方法论

子系统的提议的设计应评价，从而建立有效措施，以防止出现共同原因失效(CCF)。表F.1中适用的项目应标识并给出总分，总分用于从表F.2中确定的共同原因失效系数(用百分值表示)。

表F.1 CCF评估准则

项 目	参考	分数
分离/分凝		
SRECS单通道信号电缆与其他通道的线路在所有位置是分开的或有充分的屏蔽吗?	1a	5
使用信息编码/译码时，能完全检测出信号传送错误吗?	1b	10
SRECS信号和电能动力电缆在所有位置都分开或有充分的屏蔽?	2	5
如果子系统元素对CCF影响，在其局部外壳中作为物理分离装置提供了吗?	3	5
相异性/冗余性		
子系统使用不同电气技术，例如电子或可编程电子和其他机电继电器?	4	8
子系统采用融合不同物理原理的元素(例如，在防护门采用机械和磁传感技术的敏感元件)?	5	10
在功能操作和/或失效模式上子系统采用了有时序差分的元素?	6	10
子系统元素有≤1分钟的诊断试验间隔?	7	10
复杂性/设计/应用		
除了用于诊断测试的目的，防止子系统通道间交叉连接了吗?	8	2
评价/分析		
相比建立共同原因失效源，失效模式和影响分析的结果已经检查了吗? 预定的共同原因失效源通过设计排除了吗?	9	9
电磁场失效是否已经进行分析，并反馈到设计中?	10	9
技能/培训		
子系统设计人员理解共同原因失效的原因和后果?	11	4
环境控制		
子系统元素可能总是在规定的温度、湿度、腐蚀、粉尘、振动等范围内运行，超过了范围已经过试验，没有使用外部环境控制?	12	9
子系统免除电磁干扰的有害影响，达到和包括附录E规定的极限值?	13	9
表F.1提供选择项(例如参考项1a和1b)，目的在于在最相关项目避免CCF。		

使用表 F.1，应增加认为影响子系统设计的那些项目，为即将执行的设计规定一个总分。通过采用特定设计方法（例如用光隔离装置而不是屏蔽电缆）的等效方法也可实现避免 CCF，因此可以声称相关分数被认为同样有助于避免 CCF。

根据表 F.2，总分可用于确定共同原因失效因素（β）。

表 F.2　CCF 因素（β）评估

总分	共同原因失效因素（β）
＜35	10%(0.1)
35～65	5%(0.05)
65～85	2%(0.02)
85～100	1%(0.01)

按照 6.7.8.1 的要求，得出的 β 值应用于评估危险失效概率。

GB 28526-2012

*
书号：155066・1-45582
定价：　66.00 元