



中华人民共和国国家标准

GB/T 16855.1—2025/ISO 13849-1:2023

代替 GB/T 16855.1—2018

机械安全 安全控制系统 第 1 部分：设计通则

Safety of machinery—Safety-related parts of control systems—
Part 1: General principles for design

(ISO 13849-1:2023, IDT)

2025-08-29 发布

2025-08-29 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

引言 V

1 范围 1

2 规范性引用文件 1

3 术语、定义、符号及缩略语 2

 3.1 术语和定义 2

 3.2 符号及缩略语 9

4 总体要求 11

 4.1 机器的风险评估和风险减小过程 11

 4.2 对风险减小的作用 13

 4.3 SRP/CS 的设计过程 13

 4.4 方法 15

 4.5 所需的信息 15

 4.6 采用子系统实现安全功能 15

5 安全功能规范 16

 5.1 安全功能识别和总体描述 16

 5.2 安全要求规范 16

 5.3 确定各安全功能的所需性能等级(PL_r) 21

 5.4 审查安全要求规范(SRS) 22

 5.5 将 SRP/CS 分解成子系统 22

6 设计考虑 24

 6.1 已达到性能等级的评估 24

 6.2 实现总的的功能性能等级的子系统组合 37

 6.3 基于软件的手动参数化 38

7 软件安全要求 40

 7.1 一般要求 40

 7.2 有限可变语言(LVL)及全可变语言(FVL) 41

 7.3 安全相关嵌入式软件(SRESW) 44

 7.4 安全相关应用软件(SRASW) 45

8 已达到性能等级的验证 47

9 人类工效学方面的设计 47

10 确认 47

 10.1 确认原则 47

 10.2 安全要求规范(SRS)的确认 51

 10.3 分析确认 51

10.4	测试确认	52
10.5	安全功能的确认	53
10.6	SRP/CS 安全完整性的确认	53
10.7	环境要求的确认	56
10.8	确认记录	56
10.9	维护要求的确认	56
11	SRP/CS 的可维护性	57
12	技术文件	57
13	使用信息	58
13.1	概述	58
13.2	SRP/CS 集成的信息	58
13.3	用户信息	58
附录 A (资料性)	所需性能等级(PL _r)确定指南	60
附录 B (资料性)	模块法和安全相关模块图	64
附录 C (资料性)	单个元件 MTTF _D 值的计算或评估	66
附录 D (资料性)	估算各通道 MTTF _D 的简化方法	72
附录 E (资料性)	功能和子系统诊断覆盖率(DC)的估计	74
附录 F (资料性)	防止共因失效(CCF)的措施的量化方法	77
附录 G (资料性)	系统性失效	80
附录 H (资料性)	多个子系统组合的示例	83
附录 I (资料性)	估算子系统 PL 的简化程序示例	85
附录 J (资料性)	软件	92
附录 K (资料性)	图 12 的数值表示	95
附录 L (资料性)	电磁干扰(EMI)抗扰度	98
附录 M (资料性)	安全要求规范(SRS)的更多信息	102
附录 N (资料性)	在软件设计中避免系统性失效	105
附录 O (资料性)	控制系统元件或部件的安全相关值	121
参考文献	124

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/T 16855《机械安全 安全控制系统》的第1部分。GB/T 16855 已经发布了以下部分：

- 第1部分：设计通则；
- 第2部分：确认。

本文件代替 GB/T 16855.1—2018《机械安全 控制系统安全相关部件 第1部分：设计通则》。与 GB/T 16855.1—2018 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 将术语“控制系统安全相关部件”更改为“安全控制系统”，并更改了其定义（见 3.1.1，2018 年版的 3.1.1）；
 - 增加了术语“安全要求规范”及其定义（见 3.1.3）；
 - 更改了术语“类别”的定义（见 3.1.4，2018 年版的 3.1.2）；
 - 增加了术语“故障排除”和“永久故障”及其定义（见 3.1.9 和 3.1.11）；
 - 将术语“抑制”更改为“默停”（见 3.1.15，2018 年版的 3.1.8）；
 - 增加了首选术语“风险减小措施”（见 3.1.22，2018 年版的 3.1.27）；
 - 增加了术语“子功能”“交叉监控”“平均失效间隔时间”和“危险失效比”及其定义（见 3.1.28、3.1.30、3.1.33、3.1.34）；
 - 将术语“要求率”更改为“需求率”（见 3.1.38，2018 年版的 3.1.30）；
 - 将术语“应用软件”更改为“安全相关应用软件”（见 3.1.41，2018 年版的 3.1.36）；
 - 将术语“嵌入式软件”更改为“安全相关嵌入式软件”（见 3.1.42，2018 年版的 3.1.37）；
 - 将术语“高要求或连续模式”更改为“高需求或连续模式”（见 3.1.43，2018 年版的 3.1.38）；
 - 增加了术语“低需求模式”“子系统”“子系统组件”“通道”“操作模式”“经验证的安全原则”“经验证的元件”“动态测试”“真实性检查”“验证”“确认”“熟练人员”“黑盒”“灰盒”和“每小时危险失效平均频率”及其定义（见 3.1.44～3.1.58）；
 - 删除了术语“手动复位”“维修率”和“经使用证明”及其定义（见 2018 年版的 3.1.9、3.1.31 和 3.1.39）；
 - 增加了总体要求（见第4章）；
 - 更改了安全功能规范（见第5章，2018 年版的 5.1）；
 - 更改了设计考虑（见第6章，2018 年版的第4章）；
 - 删除了类别及其与 DC_{avg} 、CCF 和每个通道 $MTTF_D$ 的关系并将技术内容整合到设计考虑中（见第6章，2018 年版的第6章）；
 - 增加了软件安全要求（见第7章）；
 - 更改了实现的性能等级的验证要求（见第8章，2018 年版的 4.7）；
 - 更改了人类工效学方面的设计要求（见第9章，2018 年版的 4.8）；
 - 更改了确认的要求（见第10章，2018 年版的第8章）。
- 本文件等同采用 ISO 13849-1:2023《机械安全 安全控制系统 第1部分：设计通则》。
- 本文件做了下列最小限度的编辑性改动：
- 将 10.6.5 第一列项中的“7.2”改为“6.2”。

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。

本文件由全国机械安全标准化技术委员会(SAC/TC 208)提出并归口。

本文件起草单位:皮尔磁电子(常州)有限公司、中机研标准技术研究院(北京)有限公司、上海辰竹仪表有限公司、立宏安全设备工程(上海)有限公司、莱茵技术—商检(青岛)有限公司、深圳市湾测技术有限公司、贝博华自动化(南京)有限公司、骑鲸瞰海(杭州)科技有限公司、济宁科力光电产业有限责任公司、山东莱恩光电科技股份有限公司、宁波纬诚科技股份有限公司、安士能电器(上海)有限公司、施迈赛工业开关制造(上海)有限公司、南京理工大学、苏州市质量和标准化院、深圳市意普兴科技有限公司、沃德检测(广东)有限公司、奥煌检测技术服务(上海)有限公司、南京优倍电气技术有限公司、泰瑞机器股份有限公司、深圳市多恩技术有限公司、岚图汽车科技有限公司、西门子(中国)有限公司、南京林业大学、四川蜀兴优创安全科技有限公司、济南铸锻所检验检测科技有限公司、格睿安(重庆)工业技术有限公司、斯凯孚(中国)有限公司、特斯拉(上海)有限公司、威凯检测技术有限公司、乐高玩具制造(嘉兴)有限公司、华中师范大学、中铁建大桥工程局集团电气化工程有限公司、东莞市三信精密机械有限公司、湖北高农科技股份有限公司、江苏中睿安全科技发展有限公司、北京控制工程研究所、南通维尔斯机械科技有限公司、中铁建大桥工程局集团建筑装配科技有限公司、深圳市睿达科技有限公司、武汉普迪真空科技有限公司、东莞市固达机械制造有限公司、南京轻机包装机械有限公司、南安市中机标准化研究院有限公司。

本文件主要起草人:徐凯、黄之炯、周婷、李立言、曹永梅、孟昭瑞、陈卓贤、许一、王振伟、邵光存、尹之尧、李海明、胡进芳、陆晓光、何俊、居里锴、李彦涛、戴闻杰、刘晓英、刘明汉、黄飞、王林、魏建鸿、于恒、陈国良、李佳、居荣华、秦培均、卢军、殷高俊、董行、刘志隆、钟锦铭、徐文超、周潮亮、曹高辉、姚天金、高雪刚、尤小阳、戴骁蒙、马荣胜、史传明、褚卫中、刘治永、张硕、孙帅华、陈能玉、朱斌、陈小全、谢炳勋、凌益民、张合庆、姜涛、周成、赵晓东、张传甲、杨景隆、傅燕敏、张晓飞、马艳、郑华婷、周焱文。

本文件于1997年首次发布,2005年第一次修订,2008年第二次修订,2018年第三次修订,本次为第四次修订。

引 言

机械领域安全标准体系由以下几类标准构成。

——A类标准(基础安全标准),给出适用于所有机械的基本概念、设计原则和一般特征。

——B类标准(通用安全标准),涉及机械的一种安全特征或使用范围较宽的一类安全装置:

- B1类,特定的安全特征(如安全距离、表面温度、噪声)标准;
- B2类,安全装置(如双手操纵装置、联锁装置、压敏装置、防护装置)标准。

——C类标准(机械产品安全标准),对一种特定的机器或一组机器规定出详细的安全要求的标准。

根据 GB/T 15706—2012,本文件属于 B1 类标准。

本文件尤其与下列与机械安全有关的利益相关方有关:

——机器制造商;

——健康与安全机构。

其他受到机械安全水平影响的利益相关方有:

——机器使用人员;

——机器所有者;

——服务提供人员;

——消费者(针对预定由消费者使用的机械)。

上述利益相关方均有可能参与本部分的起草。

此外,本文件预定用于起草 C 类标准的标准化机构。

本文件规定的要求可由 C 类标准补充或修改。

对于在 C 类标准的范围内,且已按照 C 类标准设计和制造的机器,优先采用 C 类标准中的要求。

注 1: 本文件的主要内容和示例绝大部分都是针对工厂内的固定式机器,但本文件并没有排除其他机器。本文件没有考虑某些机械(如移动式机械)是否有特殊要求,但本文件尽可能做到适用于跨行业使用,且作为 C 类标准制修订的基础。

安全控制系统是机器控制系统中执行安全功能的部分。GB/T 16855 旨在明确安全控制系统各项关键指标的要求,确保机器的安全功能,进而保障人员的安全,拟由两个部分构成。

——第 1 部分:设计通则。目的在于指导安全控制系统的设计,以及为 B2 或 C 类标准的制修订提供指导。

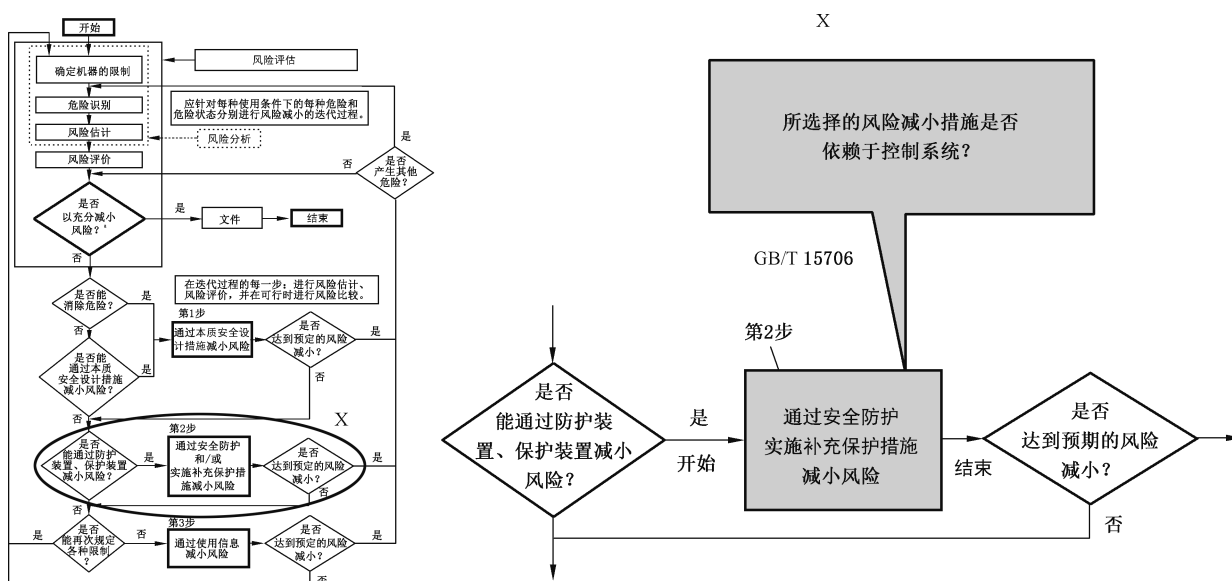
——第 2 部分:确认。目的在于指导安全控制系统的评估与验证。

按本质安全设计措施、安全防护和/或补充风险减小措施、使用信息的顺序采取风险减小措施,实现符合 GB/T 15706—2012 中的风险减小。设计者能够通过具备安全功能的风险减小措施减小风险。机器控制系统中分配用于提供安全功能的那一部分称之为安全控制系统(SRP/CS)。安全控制系统由硬件或硬件和软件的组合构成,既可独立于机器控制系统,也可以是机器控制系统的组成部分。除了实现安全功能以外,SRP/CS 也能实现操作功能。

GB/T 15706—2012 用于机器的风险评估。C 类标准中没有规定 SRP/CS 实现的安全功能的所需性能等级(PL_r)时,可根据附录 A 确定 PL_r 。依据 GB/T 15706—2012 进行风险评估后,确定需要采取依靠安全功能(如联锁防护装置)的风险减小措施时,可根据本文件采用安全控制系统执行安全功能。本文件预定用于 SRP/CS 的设计和评价。本文件的范围只包括安全相关控制系统。

图 1 给出了 GB/T 15706—2012 与本文件的关系。详细情况见图 2。

注 2: 更多信息,见 ISO/TR 22100-2:2013。



^a 基于 ISO/TR 22100-2:2013 中的图 2。

图 1 本文件(GB/T 16855.1)集成到 GB/T 15706—2012 的风险减小过程

注3: 图1给出了SRP/CS对GB/T 15706—2012的风险减小过程第2步的贡献。SRP/CS通过执行安全功能支持风险减小措施的组合。安全控制系统在预期条件下执行安全功能的能力分为5级,称为性能等级(PL)。具体安全功能(取决于所需的风险减小)的所需性能等级(PL_r)由风险估计确定。

本文件的资料性附录 A 给出了风险估计的方法,能够用于确定 SRP/CS 执行的安全功能的 PL_r。由于评价准则的主观性,不同的风险估计方法之间存在差异。与附录 A 相比, C 类标准能够针对特定机器给出更具体的风险估计方法。

安全功能危险失效的频率取决于几个因素,包括但不限于:软硬件结构、故障检测机制的范围[诊断覆盖率(DC)]、部件的可靠性[平均危险失效间隔时间(MTTF_D)、共因失效(CCF)]、设计过程、运行应力、环境条件和操作程序等。

为了便于 SRP/CS 的设计并评估所实现的 PL, 本文件采用了基于故障条件下特定设计准则(如 $MTTF_D$ 、 DC_{avg})和规定行为来进行架构分类的方法。这些架构分为 5 种类别: 类别 B、类别 1、类别 2、类别 3、类别 4。

功能安全考虑执行安全功能的组件/元件的失效特征。对于每种安全功能,其失效特征通过每小时危险失效的频率(PFH)来表示。

性能等级和类别适用于 SRP/CS, 例如:

- 控制单元(如控制功能、数据处理、监控等的逻辑单元);
- 电敏保护装置(如光幕)、压敏保护装置。

对于采用安全部件(元件)的 SRP/CS 的子系统,能够确定其性能等级和类别。安全部件(元件)的示例包括:

- 保护装置(如双手操纵装置、联锁装置);
- 动力控制组件(如继电器、阀);
- 传感器和人机交互组件(如位置传感器、使能开关)。

本文件涵盖从简单的机器(如小型厨房炊机具或自动门)到复杂的机器(如包装机械、印刷机械、压力机和集成制造系统等)。

本文件和 IEC 62061 均给出了机器安全控制系统的设计和实施要求。

机械安全 安全控制系统

第 1 部分：设计通则

1 范围

本文件规定了包括软件设计在内的执行安全功能的安全控制系统(SRP/CS)的设计和集成方法、相关要求、建议和指南。

本文件适用于包括子系统在内的用于高需求和连续操作模式的 SRP/CS,无论其采用何种技术和能量(如电气的、液压的、气动的、机械的)。本文件不适用于低需求操作模式。

注 1: 低需求操作模式见 3.1.44 和 IEC 61508(所有部分)。

本文件未规定特定应用的安全功能或所需性能等级(PL_r)。

注 2: 本文件规定 SRP/CS 设计方法时未考虑某些机械(如移动式机械)的特殊要求。此类特殊要求由 C 类标准考虑。

本文件未给出构建 SRP/CS 的产品/元件的具体设计要求。适用于某些 SRP/CS 元件设计的具体要求由适用的 ISO 和 IEC 标准涵盖。

本文件未给出物理安全、IT 安全和网络安全等方面的具体措施。

注 3: 物理安全、IT 安全和网络安全等问题可能会影响安全功能。更多信息见 ISO/TR 22100-4 和 IEC/TR 63074。

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/T 15706—2012 机械安全 设计通则 风险评估与风险减小(ISO 12100:2010,IDT)

GB/T 16855.2—2015 机械安全 控制系统安全相关部件 第 2 部分:确认(ISO 13849-2:2012,IDT)

GB/T 19876—2012 机械安全 与人体部位接近速度相关的安全防护装置的定位(ISO 13855:2010,IDT)

GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第 3 部分:软件要求(IEC 61508-3:2010,IDT)

GB/T 42598—2023 机械安全 使用说明书 起草通则(ISO 20607:2019,IDT)

IEC 61508(所有部分) 电气/电子/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)

IEC 62046:2018 机械安全 检测人体存在的保护设备应用(Safety of machinery—Application of protective equipment to detect the presence of persons)

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)

IEC/IEEE 82079-1:2019 产品使用信息准备(使用说明) 第 1 部分:原则和一般要求[Preparation of information for use (instructions for use) of products—Part 1: Principles and general requirements]

3 术语、定义、符号及缩略语

3.1 术语和定义

GB/T 15706—2012 界定的以及下列术语和定义适用于本文件。

3.1.1

安全控制系统 **safety-related part of a control system;SRP/CS**

控制系统中执行安全功能(3.1.27)的部分,从安全输入开始到产生安全输出。

注:执行安全功能的控制系统,以安全输入被触发为起始点(例如:位置开关的致动凸轮和滚轮等),以动力控制组件的输出为终止点(例如:接触器的主触点等)。

3.1.2

机器控制系统 **machine control system**

响应来自机器元件、操作者、外部控制设备或其组合的输入信号,并产生输出信号使机器按照预定方式工作的系统。

注:机器控制系统能使用任何技术或不同技术的组合(例如:电气/电子的、液压的、气动的、机械的等)。

3.1.3

安全要求规范 **safety requirements specifications;SRS**

包含安全控制系统从安全功能特征(功能要求)和所需性能等级(PL_r)(3.1.6)角度必须满足的安全功能(3.1.27)要求。

[来源:GB/T 20438.4—2017,3.5.11,有修改]

3.1.4

类别 **category**

子系统(3.1.45)按照通过部件结构布置、故障检测和/或部件可靠性实现的故障(3.1.8)抵抗能力以及故障条件下后续行为进行的分类。

3.1.5

性能等级 **performance level;PL**

用于规定安全控制系统(SRP/CS)(3.1.1)在预期条件下执行安全功能(3.1.27)的离散等级。

注:性能等级概述见 6.1。

3.1.6

所需性能等级 **required performance level**

PL_r

每种安全功能(3.1.27)为达到所需的风险(3.1.19)降低所要求的性能等级(3.1.5)。

注:更多信息见 5.3 和图 A.1。

3.1.7

安全完整性等级 **safety integrity level;SIL**

一种离散的等级(四种可能等级之一),用于规定分配给安全控制系统的安全功能(3.1.27)的安全完整性要求。其中,安全完整性等级 4 是最高的,安全完整性等级 1 是最低的。

注:本文件只考虑了 SIL1~SIL3。

[来源:GB/T 20438.4—2017,3.5.8,有修改]

3.1.8

故障 **fault**

可能造成功能单元执行能力下降或丧失的异常状态。

注 1:故障通常是产品自身失效(3.1.10)后引起的,但也可能在未先发生失效的情况下存在。

注 2：本文件中“故障”是指随机故障或系统性失效(3.1.14)造成的故障。

[来源:IEC 60050-192:2015,有修改]

3.1.9

故障排除 **fault exclusion**

如果故障(3.1.8)发生的概率能忽略不计,就能将其从安全控制系统中排除。

3.1.10

失效 **failure**

装置执行所要求功能的能力的终止。

注 1：失效后,装置有故障(3.1.8)。

注 2：“失效”与“故障”的区别在于,失效是事件,故障是状态。

注 3：本文件不包括只影响受控进程可用性的失效。

[来源:IEC 60050-192:2015,有修改]

3.1.11

永久故障 **permanent fault**

采取纠正性维护措施前一直持续存在的产品故障(3.1.8)。

[来源:IEC 60050-192:2015]

3.1.12

危险失效 **dangerous failure**

参与执行安全功能(3.1.27)的组件和/或子系统(3.1.45)和/或系统发生失效(3.1.10),以致:

- a) 阻止安全功能在需要时运行(需求模式)或者造成安全功能失效(连续模式),从而使机器/机械处于危险或潜在危险状态;或者
- b) 降低了安全功能在需要时正确运行的概率。

[来源:GB/T 20438.4—2017,3.6.7,有修改]

3.1.13

共因失效 **common cause failure; CCF**

由一个或多个事件引起的故障(3.1.10),造成多通道子系统(3.1.45)中两个或多个独立通道(3.1.47)同时失效,导致安全功能(3.1.27)失效。

注：共因失效与共模失效不同(见 GB/T 15706—2012,3.36)。

[来源:GB/T 20438.4—2017,3.6.10,有修改]

3.1.14

系统性失效 **systematic failure**

与某个原因必然有关的,只有通过修改设计或制造工艺、操作程序、文档或其他关联因素才能消除的失效(3.1.10)。

注 1：仅作修复性维修而无修改措施通常不会消除失效原因。

注 2：系统性失效能够通过模拟失效原因诱发。

注 3：以下情况中系统性失效的原因包括人为错误：

- 安全要求规范(SRS)(3.1.3)；
- 硬件的设计、制造、安装和操作；
- 软件的设计和实施；
- 未对环境条件作出充分规定。

[来源:IEC 60050-192:2015]

3.1.15

默停 muting

由 SRP/CS 实现的安全功能(3.1.27)临时性自动暂停。

[来源:ISO 61496-1:2020, 3.16]

3.1.16

伤害 harm

对健康产生的生理上的损伤或危害。

[来源:GB/T 15706—2012, 3.5]

3.1.17

危险 hazard

潜在的伤害(3.1.16)源。

注 1: “危险”一词能由其起源(例如:机械危险和电气危险),或其潜在伤害的性质(例如:电击危险、切割危险、中毒危险和火灾危险)进行限定。

注 2: 本定义中的危险包括以下两种情况:

——机器的预定使用期间始终存在的危险(例如:危险运动部件的运动、焊接过程中产生的电弧、不健康的姿势、噪声、高温);

——意外出现的危险(例如:爆炸、意外启动引起的挤压危险、破碎引起的抛射、加速/减速引起的坠落)。

[来源:GB/T 15706—2012, 3.6, 有修改]

3.1.18

危险状况 hazardous situation

人员暴露于至少具有一种危险(3.1.17)的环境。

注: 这类暴露可能立即或在一定时间之后对人员产生伤害(3.1.16)。

[来源:GB/T 15706—2012, 3.10]

3.1.19

风险 risk

伤害(3.1.16)发生的概率与伤害严重程度的组合。

[来源:GB/T 15706—2012, 3.12]

3.1.20

剩余风险 residual risk

采取风险减小措施(保护措施)(3.1.22)之后仍然存在的风险(3.1.19)。

注: 见图 3。

[来源:GB/T 15706—2012, 3.13, 有修改]

3.1.21

风险评估 risk assessment

包括风险分析(3.1.23)和风险评价(3.1.24)在内的全过程。

[来源:GB/T 15706—2012, 3.17]

3.1.22

风险减小措施 risk reduction measure

保护措施 protective measure

用于消除危险(3.1.17)或减小风险(3.1.19)的行为或方法。

示例: 本质安全设计、保护措施、个体防护装备、使用及安装信息、工作组织、培训、应用设备、监督。

[来源:ISO/IEC Guide 51:2014, 3.13]

3.1.23

风险分析 risk analysis

机器限制的确定、危险(3.1.17)识别和风险(3.1.19)估计的组合。

[来源:GB/T 15706—2012,3.15]

3.1.24

风险评价 risk evaluation

以风险分析(3.1.23)为基础,判断是否已达到减小风险的目标。

[来源:GB/T 15706—2012,3.16]

3.1.25

机器的预定使用 intended use of a machine

按照使用说明书提供的信息使用机器。

[来源:GB/T 15706—2012,3.23]

3.1.26

可合理预见的误用 reasonable foreseeable misuse

不以设计者预定的方法使用机器,而是按照常理能预见的人类习惯来使用机器。

[来源:GB/T 15706—2012,3.24]

3.1.27

安全功能 safety function

失效(3.1.10)后能立即造成风险(3.1.19)增加的机器功能。

注:安全功能是由控制系统安全相关部分实施的功能,是针对特定危险事件实现或保持机器安全状态所需要的功能。

[来源:GB/T 15706—2012,3.30,有修改]

3.1.28

子功能 sub-function

安全功能(3.1.27)的组成部分,失效(3.1.10)后会造成安全功能失效。

注:子功能由控制系统安全相关部分的子系统(3.1.45)实施。另见 IEC 61800-5-2:2016。

示例:IEC 61800-5-2:2016 规定的子功能包括安全转矩关断(STO)、安全停止 1(SS1)。见图 6。

3.1.29

监控 monitoring

检测状态并和预期值对比的诊断措施。

注:实现诊断的方法包括:真实性检查(3.1.52)、直接/间接/交叉监控(3.1.30)(见附录 E)、循环测试。

3.1.30

交叉监控 cross monitoring

对冗余子系统(3.1.45)两个通道(3.1.47)的冗余信号都进行真实性检查的诊断措施。

3.1.31

可编程电子系统 programmable electronic system; PE system

基于一个或多个可编程电子装置的控制、保护或监视系统(3.1.29),包括系统中所有的组件,如电源、传感器和其他输入装置、数据总线和其他通信路径,以及执行器及其他输出装置。

[来源:GB/T 20438.4—2017,3.3.1]

3.1.32

平均危险失效间隔时间 mean time to dangerous failure**MTTF_D**

平均危险失效间隔时间期望。

注：如果产品的无危险失效前运行时间呈指数分布（如恒定失效率），则 $MTTF_D$ 的数值等于危险失效率的倒数。

[来源：IEC 62061:2021, 3.2.38, 有修改]

3.1.33

平均失效间隔时间 **mean time between failures**

MTBF

连续两次失效（3.1.10）之间运行时间的期望值。

3.1.34

危险失效比 **ratio of dangerous failures**

RDF

组件总体失效（3.1.10）率中能造成危险失效（3.1.12）的占比。

3.1.35

诊断覆盖率 **diagnostic coverage**

DC

诊断有效性的量度，定义为检出危险失效（3.1.12）的失效（3.1.10）率与全部危险失效的失效率的比率。

注：诊断覆盖率的适用对象可能是整个安全相关系统或其部件。例如：诊断覆盖率能适用于传感器和/或逻辑系统和/或功率控制组件。

3.1.36

任务时间 **mission time**

T_M

SRP/CS 预定使用的时段。

3.1.37

测试率 **test rate**

r_t

SRP/CS 中检测故障（3.1.8）的测试频率。

注：测试率也用作诊断测试间隔时间的倒数。

3.1.38

需求率 **demand rate**

r_d

要求安全控制系统（SRP/CS）执行安全功能（3.1.27）的频率。

3.1.39

有限可变语言 **limited variability language; LVL**

通过组合预定义和专用的库函数来实现安全要求规范（SRS）（3.1.3）的语言类型。

注 1：LVL 提供了与实现应用所需功能之间的紧密功能对应关系。

注 2：IEC 61131-3 中给出了 LVL 的典型示例，包括梯形图、功能块图和顺序功能图。指令表和结构化文本不看作 LVL。

注 3：采用 LVL 的典型系统示例：配置用于机器控制的可编程控制器（PLC）。

[来源：IEC 62061:2021, 3.2.62]

3.1.40

全可变语言 **full variability language; FVL**

实现全面广泛的功能和应用的语言类型。

注 1：使用 FVL 的典型系统示例：通用计算机。

注 2：FVL 通常用于嵌入式软件，很少用于应用软件。

注 3: FVL 的示例包括: Ada、C、Pascal、指令表、汇编语言、C++、Java、SQL。

[来源: IEC 62061:2021, 3.2.61]

3.1.41

安全相关应用软件 safety-related application software; SRASW

面向应用的软件, 通常包括逻辑序列、范围、表达式, 用于满足安全控制系统(SRP/CS)要求所必需的输入、输出、计算和结果。

3.1.42

安全相关嵌入式软件 safety-related embedded software; SRESW

作为系统组成部分由制造商提供的软件, 最终用户无法对其进行修改访问。

注: 嵌入式软件也称作固件或系统软件。见全可变语言(FVL)(3.1.40)。

[来源: GB/T 21109.1—2022, 3.2.76.2]

3.1.43

高需求或连续模式 high demand or continuous mode

一种运行模式, 在该模式下, 要求安全控制系统(SRP/CS)执行其安全功能(3.1.27)的频率大于 1 次/年, 或者作为正常操作的一部分, 安全功能使机器保持在安全状态。

[来源: GB/T 20438.4—2017, 3.5.16, 有修改]

3.1.44

低需求模式 low demand mode

一种运行模式, 在该模式下, 要求安全控制机系统(SRP/CS)执行其安全功能(3.1.27)的频率不大于 1 次/年。

注: 本文件未讨论低需求模式。更多细节见第 1 章。

[来源: GB/T 20438.4—2017, 3.5.16, 有修改]

3.1.45

子系统 subsystem

SRP/CS 经一级分解后得到的实体, 其危险失效(3.1.12)会导致安全功能(3.1.27)的危险失效。

注 1: 子系统的规范包括其在安全功能中的作用以及与 SRP/CS 其他子系统的接口。

注 2: 一个子系统可能是一个或若干个 SRP/CS 的组成部分, 例如同一个接触器组合能够用于检测到危险区内有人时以及打开安全防护装置时给电动机断电。

3.1.46

子系统组件 subsystem element

子系统(3.1.45)的组成部件, 由单个或一组元件组成。

注 1: 子系统组件能是硬件或者硬件和软件的组合。本文件中, 只有软件的元件不视为子系统组件。

注 2: 控制系统元件或部件的安全相关值见附录 O。

3.1.47

通道 channel

独立执行一个安全功能(3.1.27)或部分安全功能的一个或一组组件。

注: 通道能是功能通道或测试通道。

[来源: GB/T 20438.4—2017, 3.3.6, 有修改]

3.1.48

操作模式 operating mode

机器的运行模式(如自动、手动、维护等), 用于选择事先确定的机器功能以及与此类功能相关的安全措施。

注 1: 针对每种特定的操作模式都实施了相关的安全功能(3.1.27)和/或风险减小措施(3.1.22)。

注 2：操作模式本身不是机器功能。归入某一操作模式的功能（包括安全功能）只有在该特定操作模式激活后才能使用。

3.1.49

经验证的安全原则 well-validated safety principle

已在以往安全控制系统的设计或集成中证明有效的原则，以避免或控制影响安全功能（3.1.27）性能的关键故障（3.1.8）或失效（3.1.10）。

注 1：对于新制定的安全原则，只有经过验证，证明其在安全相关应用中的适用性和可靠性后，才能视为经验证。

注 2：经验证的安全原则不仅对随机硬件失效有效，还对产品生命周期过程中逐渐产生的系统性失效（3.1.14）有效，如由于产品设计、集成、更改或劣化引起的故障。

注 3：GB/T 16855.2—2015 中的表 A.2、B.2、C.2 和 D.2 阐述了不同技术的经验证的安全原则。

3.1.50

经验证的元件 well-validated safety component

安全相关应用中成功使用过的元件。

注：具体要求见 6.1.11，公认的经验证元件清单见 GB/T 16855.2—2015。

3.1.51

动态测试 dynamic test

采用受控或系统性方式执行软件和/或操作硬件，以证明具备所要求的行为，同时无不需要的行为。

注 1：如果监控（3.1.29）未检测到预期变化，则测试失败。

注 2：测试脉冲是动态测试的常用技术，广泛用于检测短路、信号路径中断或故障。

3.1.52

真实性检查 plausibility check

监控（3.1.29）输入（输出）状态与系统或其他输入（输出）状态是否相符的诊断措施。

3.1.53

验证 verification

通过提供客观证据对规定的要求已得到满足的认定。

注 1：验证所需的客观证据能够是检验结果或以其他形式的确定结果，如变换方法进行计算或文件评审。

注 2：为验证所进行的活动有时被称为鉴定过程。

注 3：“已验证”一词用于表明相应的状态。

[来源：GB/T 19000—2016, 3.8.12]

3.1.54

确认 validation

通过检查和提供客观证据，证明满足某一具体预期用途的特定要求。

注 1：确认所需的客观证据能够是测试结果或以其他形式的确定结果，如变换方法进行计算或文件评审。

注 2：“已确认”一词用于表明相应的状态。

注 3：确认使用的条件能是真实的或模拟的。

[来源：GB/T 20438.4—2017, 3.8.2]

3.1.55

熟练人员 skilled person

经过相关教育培训或具备经验，能够觉察风险（3.1.19）并避免相关设备关联危险（3.1.17）的人员。

注：评价专业培训时能考虑在相关技术领域多年的实践。

[来源：GB/T 38943.1—2020, 3.5.4, 有修改]

3.1.56

黑盒 black box

仅能从其输入和输出可见的装置、系统或对象。

3.1.57

灰盒 grey box

有些内部功能已知的装置、系统或对象。

注：功能测试的第三种方法是采用所有内部功能已知的“白盒”。

3.1.58

每小时危险失效平均频率 average frequency of a dangerous failure per hour; PFH

安全控制系统(SRP/CS)(3.1.1)在一个给定的时间周期内执行规定安全功能时的平均危险失效频率。

[来源:GB/T 20438.4—2017,3.6.19,有修改]

3.2 符号及缩略语

表 1 给出的符号及缩略语适用于本文件。

表 1 符号及缩略语

符号或缩略语	描述	条款或章条号
a、b、c、d、e	性能等级的指标	表 K.1
AOPD	有源光电保护装置(如光幕)	附录 H
B、1、2、3、4	类别的指标	表 5
B_{10D}	直到有 10% 元件危险失效时的周期数(针对有机械磨损的元件)	附录 C
Cat.	类别	3.1.4
CC	换流器	附录 I
CCF	共因失效	3.1.13
DC	诊断覆盖率	3.1.35
DC_{avg}	平均诊断覆盖率	E.2
EMI	电磁干扰	F.3.6.1
ETA	事件树分析	10.3.2
F、F1、F2	暴露于危险的频率和/或时间	A.3.2
FB	功能模块/功能块	附录 J
FVL	全可变语言	3.1.40
FMEA	失效模式及影响分析	6.1.5
FMECA	失效模式、影响及危害性分析	10.3.2
FTA	故障树分析	10.3.2
$F_D(t)$	累积分布函数	C.4.3
HFT	硬件故障裕度	6.1
I、I1、I2	输入装置,例如:传感器	6.1

表 1 符号及缩略语 (续)

符号或缩略语	描述	条款或章条号
i, j	计算指数	附录 D
I/O	输入/输出	表 E.1
i_m	相互连接方式	图 7、图 8、图 9、图 10
K1A、K1B	接触器	附录 I
L、L1、L2	逻辑单元	6.1
LVL	有限可变语言	3.1.39
λ_D	元件危险失效率	附录 C
M	电动机	附录 I
MTTF	平均失效间隔时间	附录 C
MTTF _D	平均危险失效间隔时间	3.1.32
MTTR	平均恢复时间	附录 D
n, N, \tilde{N}	项目编号	6.2、D.1
N_{low}	子系统组合中,性能等级为 PL _{low} 的子系统的数量	6.2
n_{op}	年平均操作次数	附录 C
O、O1、O2、OTE	输出装置、测试设备输出,如:功率控制组件	6.1
P、P1、P2	避免或限制危险的概率	A.3.3
PE system	可编程电子系统	3.1.31、附录 H
PFH	每小时危险失效平均频率	3.1.58、表 2、表 K.1
PL	性能等级	3.1.5
PLC	可编程逻辑控制器	附录 I
PL _{low}	子系统组合中子系统的最低性能等级	6.2
PL _r	所需性能等级	3.1.6
r_d	要求率	3.1.38
r_t	测试率	3.1.37
RDF	危险失效比	3.1.34
RS	旋转传感器	附录 I
S、S1、S2	伤害的严重程度	A.3.1
SB	子系统	图 13、H.1、H.2
SOS	安全操作停止	5.2.2.2
SS2	安全停止 2	5.2.2.2
SW1A、SW1B、SW2	位置开关	附录 I
SIL	安全完整性等级	3.1.7、第 6 章
SLS	安全极限速度	表 3
SRASW	安全相关应用软件	3.1.41

表 1 符号及缩略语 (续)

符号或缩略语	描述	条款或章条号
SRESW	安全相关嵌入式软件	3.1.42
SRP/CS	安全控制系统	3.1.1
SRS	安全要求规范	3.1.3
STO	安全转矩关断	表 3、N.2
TE	测试设备	6.1
T_M	任务时间	3.1.36
T_{10D}	直到有 10% 元件危险失效时的平均时间	附录 C

4 总体要求

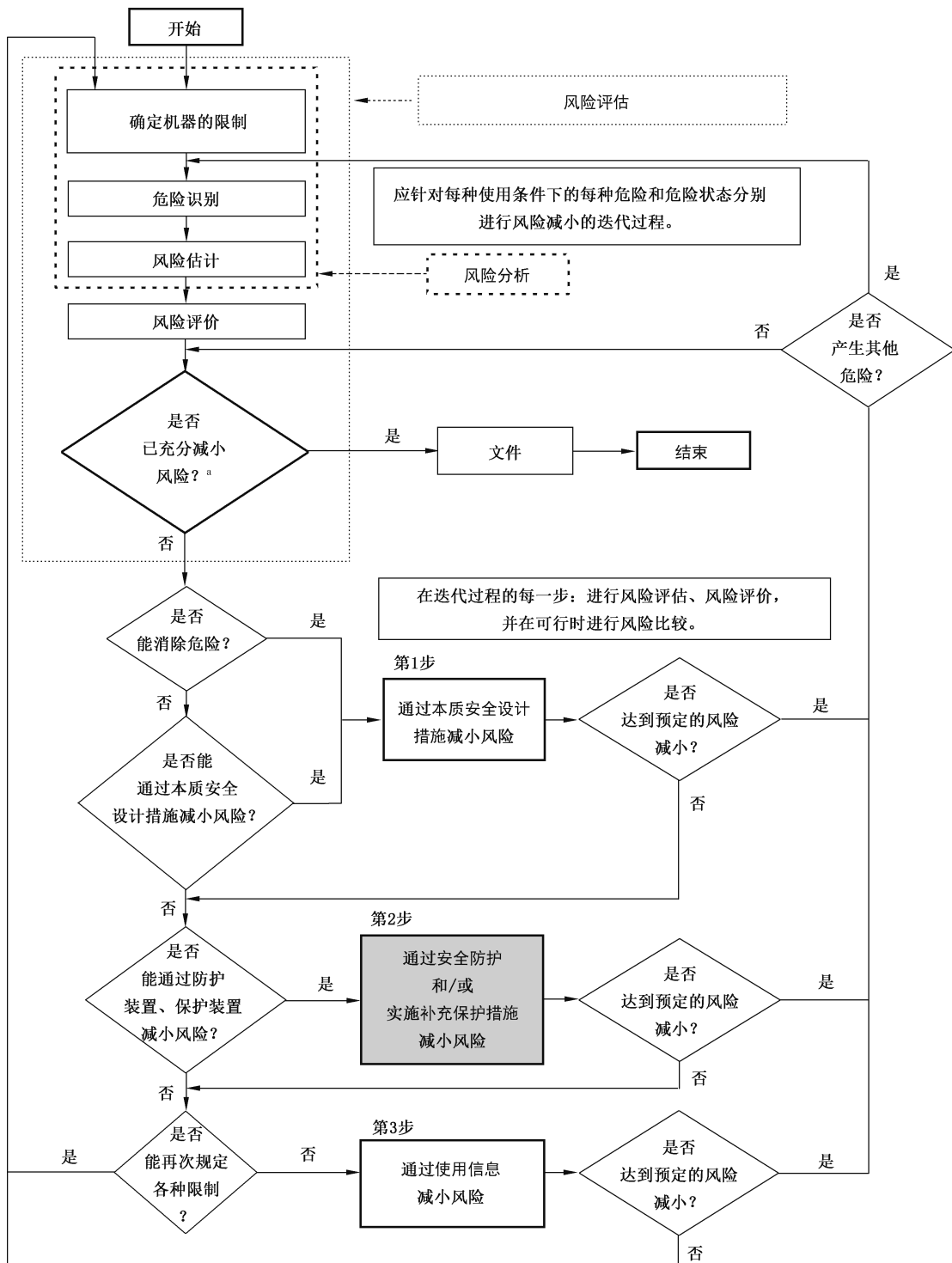
4.1 机器的风险评估和风险减小过程

GB/T 15706—2012 给出了风险评估和风险减小过程,见图 2。采用安全功能及相应的 SRP/CS 实现风险减小时,风险减小过程包括本文件的内容。

注 1: 更多信息,见 ISO/TR 22100-2:2013。

SRS 以及 SRP/CS 的设计应重视风险评估的结果,包括机器的预定用途和可合理预见的误用(见图 1 和图 2)。

注 2: 本文件不适用于机器的非 SRP/CS(见图 6)。



■ 通过安全防护减小风险可由执行安全功能的 SRP/CS 实现。这种情况下可适用本文件。

注：图为 GB/T 15706—2012 中的图 1。

^a 问题首次提出时，由初次风险评估结果回答。

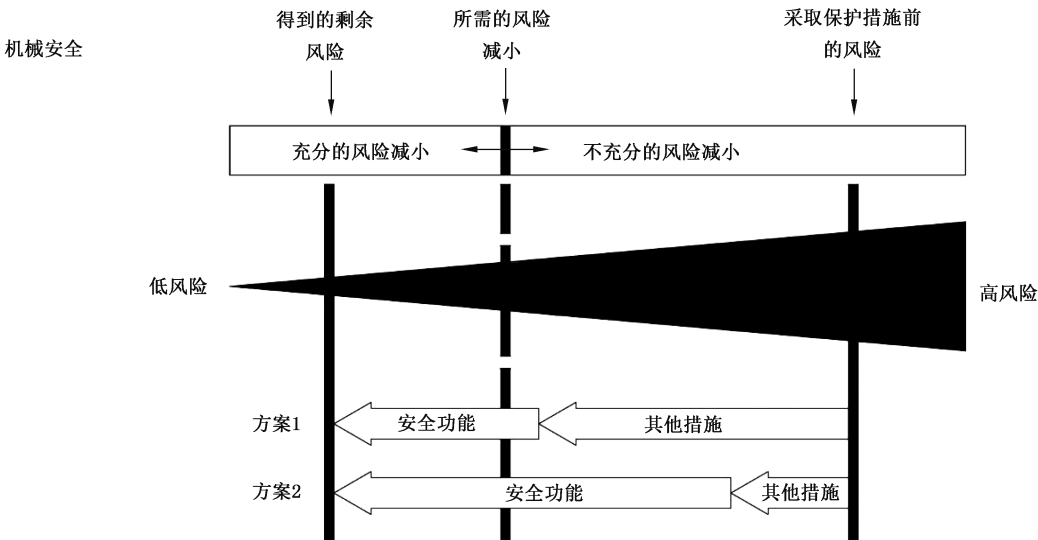
图 2 风险减小过程迭代三步法的图示

注 3：特殊情况下，本文件也适用于图 2 中的第 3 步。如显示和报警，见附录 M。

4.2 对风险减小的作用

从风险评估开始,设计者应确定需要由 SRP/CS 执行的每一种相关的安全功能对风险减小的作用。这一作用涵盖采用特定安全功能(见图 3)减小的那一部分风险,并不涵盖受控机器的全部风险。

示例:压力机上电敏保护装置触发的安全相关停止功能或清洗机门锁安全功能。



方案 1:绝大部分风险减小由安全功能之外的保护措施(如机械措施)实现,小部分由安全功能(如防护罩或联锁功能)实现。

方案 2:绝大部分风险减小由安全功能实现,小部分由安全功能之外的保护措施实现。

注:关于风险减小的更多信息见 GB/T 15706—2012。

图 3 每种危险状况的风险减小措施概况

4.3 SRP/CS 的设计过程

图 4 给出了 SRP/CS 的设计过程以及如何确定 SRP/CS 是否实现预定风险减小。

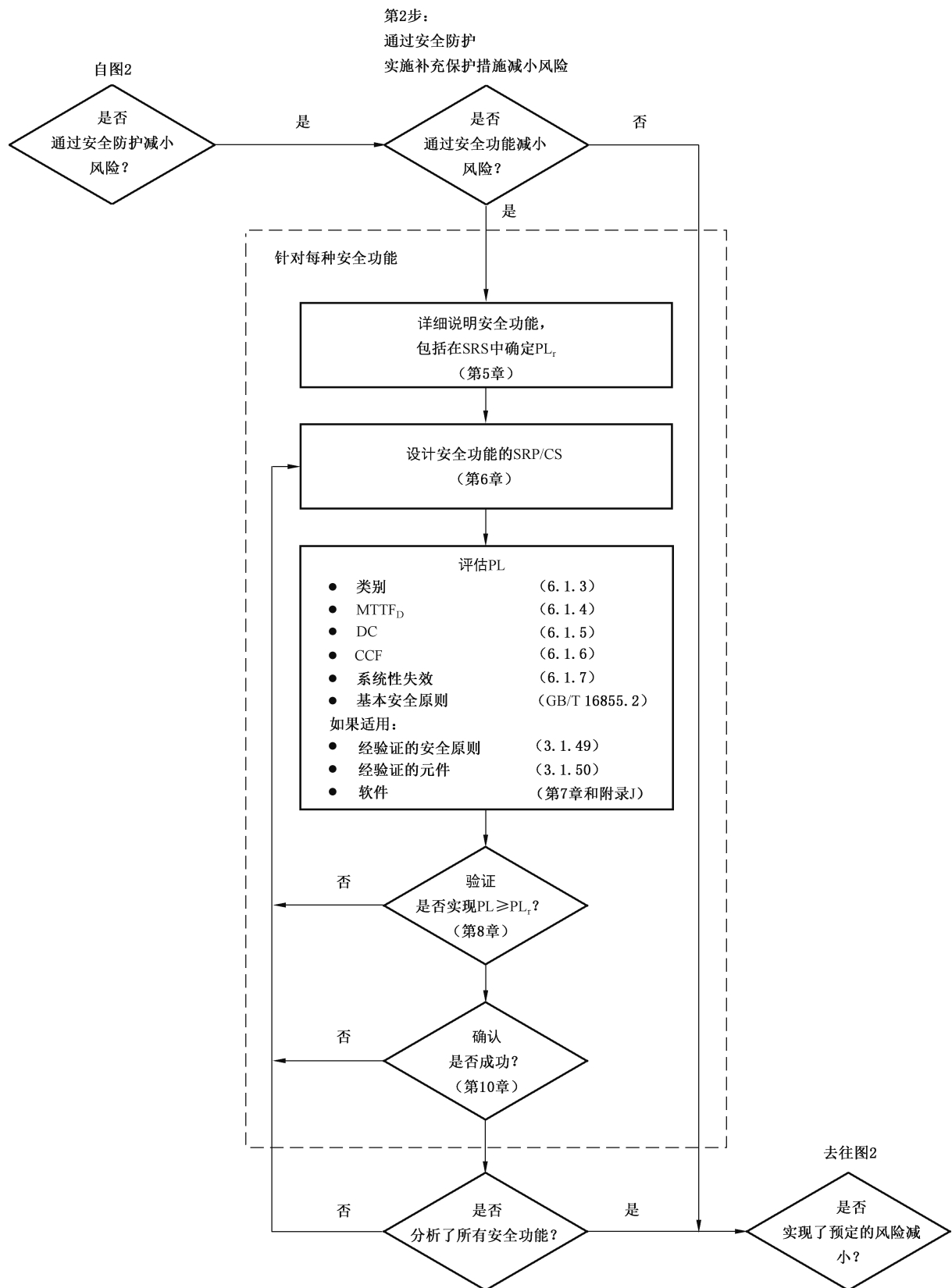


图4 安全控制系统(SRP/CS)的迭代设计过程

4.4 方法

本文件采用了以下方法。

- a) 安全功能规范(第 5 章)。
- b) 安全功能设计和技术实现,包括识别 SRP/CS 以及执行各安全功能的子系统。
 - 1) 设计考虑(第 6 章)。
 - 2) 软件安全要求(第 7 章)。
- c) 验证实现的 PL 是否满足 PL_r (第 8 章)。
- d) 人类工效学设计(第 9 章)。
- e) 确认(第 10 章或 GB/T 16855.2—2015)。
- f) 维护(第 11 章)。
- g) 技术文件(第 12 章)。
- h) 使用信息(第 13 章)。

所需性能等级(PL_r)对应需要由安全功能提供的风险减小。对风险减小的作用越大(取决于初始风险),所要求的安全性能应越高。安全功能的性能等级是以安全功能每小时危险失效平均频率来定义的。性能等级分为 5 级,PL a 对风险减小的作用最小,PL e 对风险减小的作用最大。各等级的每小时危险失效平均频率范围见表 2。

表 2 性能等级

PL	每小时危险失效平均频率(PFH) 1/h
a	$10^{-5} \leq PFH < 10^{-4}$
b	$3 \times 10^{-6} \leq PFH < 10^{-5}$
c	$10^{-6} \leq PFH < 3 \times 10^{-6}$
d	$10^{-7} \leq PFH < 10^{-6}$
e	$PFH < 10^{-7}$
注:此处的 PFH 值能与 IEC 62061:2021 和 IEC 61508(所有部分)规定的 PFH 相同。	

子系统(见 5.5)应采用 SRP/CS 相同的过程按照第 5 章~第 13 章进行评估。每一种安全功能所实现的性能等级应满足或超过所需性能等级(PL_r)。

4.5 所需的信息

按照本文件的要求,以下信息是必备的:

- 机器或其部件的风险评估结果;
- 已确定的每种危险风险减小过程必须的所有安全功能的信息(见第 5 章),包括:
 - 每种安全功能的详细描述,包括其对风险减小的作用(见 5.2);
 - 确定每种安全功能的所需性能等级(PL_r)(见 5.3)。

注:此信息由适用的 C 类标准中给出。

4.6 采用子系统实现安全功能

安全功能能通过以下方式实现:

- 采用以前已根据本文件、IEC 62061:2021、IEC 61508(所有部分)或其他有关的安全相关产品

- 标准[如 IEC 61496(所有部分)和 IEC 61800-5-2:2016]确认过的子系统；
- 根据本文件设计新的子系统；
- 上述两种方法的组合(见图 5 示例)。

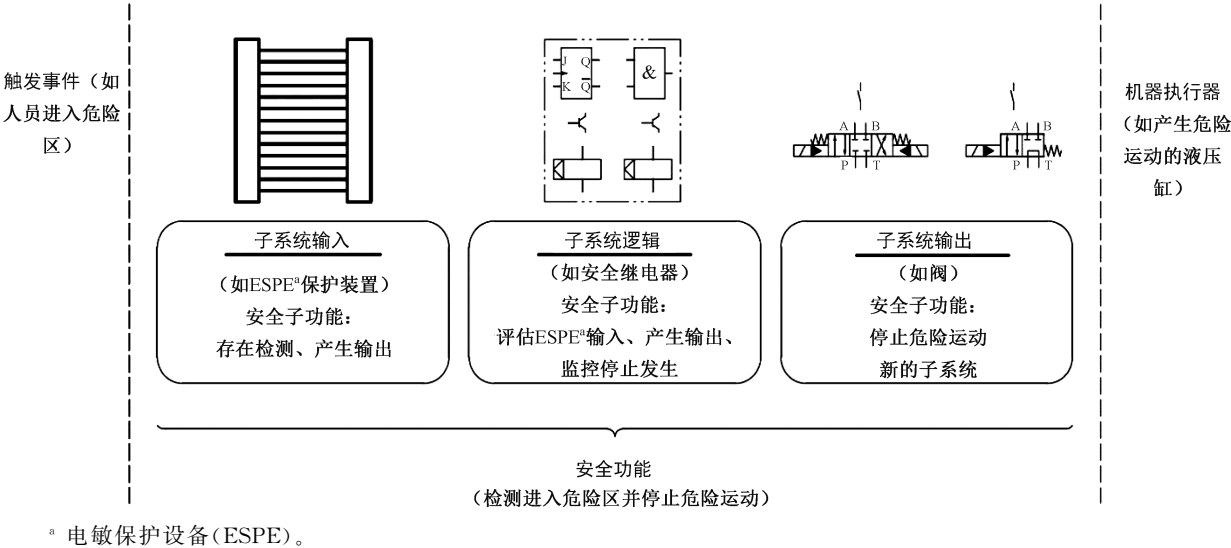


图 5 子系统组合示例

5 安全功能规范

5.1 安全功能识别和总体描述

应对安全功能进行总体描述,说明 SRP/CS 在风险减小中的作用。总体描述应联系风险评估识别的危险,并说明该功能如何工作,如何实现所要求的安全。编写安全功能规范需要按照 GB/T 15706—2012 进行风险评估得到的详细信息。

本条款的目的是给如何规定由 SRP/CS 实现的各安全功能的要求提供指南。

风险减小过程包括确定机器的安全功能,如防止意外启动。一个安全功能可以由一个子系统或者多个组合的子系统实现,多个安全功能也可共享一个或多个子系统,如逻辑单元、功率控制组件。

安全功能规范能按照 GB/T 15706—2012 中 6.2.11 的要求进行编写,然后根据本文件纳入 SRP/CS 的设计规范。

第 5 章涉及以下几个步骤:

- a) 安全功能总体描述(将安全功能与危险联系);
- b) 安全要求详细描述(见 5.2);
- c) 确定各安全功能的 PL_r(见 5.3);
- d) 审查 SRS(见 5.4)。

5.2 安全要求规范

5.2.1 通用要求


5.2.1.1 一般要求

SRS 是所有 SRP/CS 设计活动的基础,并应记录要实现的每个安全功能的详细情况。

SRS 提供了从按照 GB/T 15706—2012 进行的风险评估和风险减小过程向按照本文件进行的

SRP/CS 设计和评价过程过渡的必要信息,尤其是这两个过程由不同的人或机构实施的情况下(见表3)。

表3 从 GB/T 15706—2012 的风险评估与风险减小过程转化为本文件的 SRP/CS 设计和评估过程

编写 SRS 的必要信息(见 5.2.1.2)	转化	SRS 中安全功能规范示例(见 5.2.1.3)
—— 机器或其部件的风险评估结果,包括危险部件以及所要求的总体风险减小; —— 机器操作特性,如预定使用; —— 紧急操作; —— 描述不同工作过程和手动活动之间的相互作用,如修理; —— 人类工效学方面; —— 与环境条件相关的使用限制		所需的安全功能(示例) 1) 联锁功能 —— 操作模式(全部); —— 触发事件:打开活动式防护装置; —— 安全相关反应:所有运动安全转矩关断(STO); —— PL_{rd} ; —— 响应时间; —— 其他。 2) 安全极限速度(SLS) —— 操作模式(手动); —— 触发事件:速度高于规定限值; —— 安全相关反应:所有运动安全转矩关断(STO); —— PL_{rc} ; —— 响应时间; —— 其他

5.2.1.2 编写安全要求规范(SRS)的必要信息

注1: 以下信息用于编制技术文件。用户信息见 13.3。

应向安全控制系统设计者提供以下信息,以便编制 SRS。

- a) 风险减小措施依赖安全控制系统执行安全功能时,每种特定危险关联的机器或机器部件的风险评估结果。
- b) 机器的运行特征,包括:
 - 1) 机器的预定使用;
 - 2) 可合理预见的误用;
 - 3) 操作模式(例如:本地模式、自动模式、与机器区域或部件有关的模式);
 - 4) 期间安全功能激活的操作模式;
 - 5) 周期时间;
 - 6) 达到 GB/T 19876—2012 中 5.1 规定的安全状态的响应时间。

注2: 控制系统响应时间是机器总响应时间的一部分。所要求的机器总响应时间可能会影响安全相关部分的设计,如需要提供制动系统。

注3: 操作功能(如启动、正常停止)也可能是安全功能,但只有在对机器进行全面风险评估后才能确定。

- c) 紧急操作(IEC 60204-1:2016+AMD1:2021,附录 E)。
- d) 不同工作过程和手动活动(如修理、调整、清洗、故障查找、中止安全防护的操作模式)相互作用的描述。
- e) 人类工效学方面:最小化不正确操作或防止被废弃。
- f) 与环境条件相关的使用限制。

g) 叠加危险的影响(见 A.4)。

5.2.1.3 安全要求规范(SRS)中所有安全功能的规范

SRS 应包含各安全功能在特定应用中的以下信息:

- a) 安全功能的简述/名称;
- b) 触发安全功能的事件;
- c) 为达到预定安全状态安全功能输出要触发的反应;

示例 1: 停止危险运动。

- d) 所需性能等级 PL_r (见 5.3);
- e) 对安全功能提出要求后机器达到安全状态的响应时间,如 GB/T 19876—2012 规定的全系统停机性能(反应时间加停止时间);
- f) 安全功能活跃的操作模式;
- g) 安全功能与机器控制系统和其他安全功能的接口;
- h) 如果有需要,功能通道检测到故障如何使机器达到安全状态的程序,包括故障修复前如何保持安全状态;

示例 2: 如果功能通道发生故障时无法实现受控停机,那么能立即采用不受控停机触发故障反应。

- i) 失去动力时的机器行为(见 5.2.2.8);

示例 3: 可能有必要固定垂直轴的位置,防止因重力下坠。如果外力会影响功能安全,如承受重力作用的轴,可能有必要按照系统要求进行加固(如动力组件)。一种设计方案是在气缸上增加一个单向阀或增加机械制动。也能设计两个单独的安全功能:一个用于有动力,另一个用于无动力。

- j) 安全功能的要求率和/或 SRP/CS 的操作频率;
- k) 能够同时激活且能够造成冲突行为的安全功能的优先顺序;

示例 4: 紧急停止功能优先于所有其他功能。

示例 5: 安全速度限制(SLS)可能是“保持运行”安全功能的前提条件。

- l) 用于设计 SRP/CS 或子系统的 C 类标准的安全要求(ISO 23125:2015、ISO 16090-1);
- m) 安全功能激活后允许重新启动的条件。

注: 在采用持续人员检测防止危险状况发生的场合下,安全功能能自动复位。

典型安全功能及其特征和安全相关参数见 5.2.2 和附录 M。

5.2.2 特定安全功能的要求

5.2.2.1 概述

本条款给出了许多 SRP/CS 常用的一些特定安全功能的附加要求。

5.2.2.2 安全相关停止功能

安全相关的停止功能(例如:由安全防护装置触发)触发后,必要时应使机器尽快进入安全状态。这种安全相关停止功能应优先于所有相关启动和非安全相关停止。当一组机器协同工作时,应设置装置将停止状况信号发送至管理控制系统和/或其他机器。

根据风险评估结果,安全相关停止功能能够通过 IEC 60204-1:2016+AMD1:2021 中 9.2.2 规定的停止类别实现。

注: IEC 61800-5-2:2016 提供了关于安全相关动力传动系统的信息,包括对安全转矩关断(STO)、安全停止 1(SS1)、安全停止 2(SS2)以及安全操作停止(SOS)的描述。

安全功能触发停止指令后,停止状态应保持到具备重启的安全条件为止。另见附录 M 中表 M.1。

5.2.2.3 手动复位功能

通过复位安全防护装置重新恢复安全功能会解除停止指令。如果风险评估表明(有必要),解除此停止指令应由独立的审慎手动操作(手动复位)确认。

手动复位功能应:

- 由启动指令之外的一个独立的手动操作装置来提供;
- 只有所有安全功能和安全防护装置处于工作状态时才能实现;
- 自身不引起危险状况;
- 由审慎操作触发;
- 使控制系统能接受独立的启动指令;
- 只能通过受监控的信号变化接收,以防止可预见的误用。

要求“手动复位”功能为安全功能时(如防止意外启动),应确定所需性能等级(PL_r)。手动复位功能的 PL 与相关安全功能的 PL_r 不一定相同。

注:当安全功能(安全条件)仍然维持安全状态时,例如由人员无法进入的安全防护装置(防护罩)触发的安全功能,手动复位功能往往不是一个单独的附加安全功能。

复位触发装置应安装在危险区以外具备充分可见度的位置,以便检查是否有人处在危险区内。从危险区内应无法激活复位功能。如果危险区的可见度不充分,应采用特殊的复位顺序或对不可见区域进行监控。如果无法采用特殊复位顺序或无法对不可见区域进行监控,则应采用其他等效风险减小措施。

示例:一种解决方法是采用顺序复位。复位功能由位于危险区内的第一个装置结合位于危险区外(靠近安全防护装置)的第二个装置触发。该复位程序能在控制系统收到单独的启动指令前较短时间内完成。如果无法从复位位置观察到危险区内有人员存在,能采用存在检测装置监控危险区。

另见表 M.1。

5.2.2.4 重新启动功能

应只有安全条件得到保证的情况下,重新启动功能才能自动发生。特别是具有启动功能的联锁防护装置应符合 GB/T 15706—2012 中 6.3.3.2.5 的要求。

示例:机器自动运行时,传感器反馈给机器控制系统的信号通常用于控制流程。如果工件离开其位置,则流程停止。如果联锁防护装置的监控不能优先于自动流程控制,则操作者调整工件时可能存在机器意外重启的危险。因此,在防护装置再次关闭,且操作人员已离开危险区域之前,不宜允许自动重启。控制系统提供的防止意外启动的作用(见 GB/T 19670—2023)取决于风险评估的结果。

另见表 M.1。

5.2.2.5 本地控制功能

当机器通过便携式控制装置或悬挂式操纵装置等进行本地控制时,应满足以下要求:

- 用本地控制的设施位于危险区之外;
- 仅在风险评估确定的区域内才可以通过本地控制站触发指令,以避免危险状况;
- 本地控制和其他控制之间的切换不产生危险状况;
- 从多个控制站(本地或远程)触发指令不造成危险状况。选用本地控制站或触发某些指令时,有必要防止使用其他控制站。

另见表 M.1。

5.2.2.6 默停功能

默停是指由机器安全控制系统临时自动停止某项安全功能。该功能用于下列情况允许人员或物料

出入：

- 机器循环的非危险部分；或者
- 采用其他方式保持安全。

默停功能应自动触发并终止。这应通过恰当选型和定位的传感器或者来自机器控制系统的信号实现。如果信号、顺序或者默停传感器或信号的同步不正确，则不应允许默停。

执行默停功能的控制系统部件应具备相应的安全相关性能(PL 符合本文件或 IEC 62061:2021)并不应将保护功能的安全相关性能降低到该应用所需等级以下。

默停结束时，所有受影响的安全功能都应恢复并激活。

默停的实施应符合 IEC 62046:2018 的要求。另见表 M.1。

5.2.2.7 安全相关参数

当安全相关参数，例如：位置、速度、温度、时间、转矩或压力等偏离了预设的限值时，则安全控制系统应启动相应的措施。

如果可编程或可配置电子系统中安全相关数据手动输入错误能够导致危险状况，则应提供数据检查措施，如检查极限值的格式和/或逻辑输入值。更多要求见 6.3 和表 M.2。

5.2.2.8 能量源的波动、丧失和恢复

当能量水平的波动超出了设计工作范围时，包括能量供应丧失，SRP/CS 应连续提供或触发能使机器系统其他部件保持安全状态的输出信号。另见表 M.2。

5.2.2.9 操作模式选择要求

当操作模式的选择启用或禁用安全功能时，此选择属于安全功能。需要满足以下要求。

- a) 一次只能激活一种操作模式；每种选择的操作模式应清晰可识别或清晰显示。
- b) 模式选择本身不应触发机器运行。应要求另行触发启动控制。
- c) 从一种操作模式转换到另一种操作模式时，应激活所选择操作模式需要的安全功能和/或风险减小措施，且在转换过程中不损失任何预定风险减小。
- d) 选择操作模式的方法不应降低该模式下被激活的安全功能 PL 等级。

另见表 M.1。

5.2.2.10 用于维修任务的安全功能

机器的设计应分析在机器上执行的维修任务并为维修任务提供安全功能。安全功能规范应分析每项维修任务的风险评估结果。

注 1：维修任务可能包括，但不限于：

- 设定；
- 示教/编程；
- 过程/工具转换；
- 清洁整理；
- 消毒杀菌；
- 计划内或计划外的预防性或纠正性维护；
- 故障排查；
- 故障诊断。

有些维修任务要求将机器与动力源完全隔离，因此不依赖 SRP/CS。执行某些维修任务时，要求手动中止或超驰特定安全功能，而与此同时维修人员在危险区内，且需要动力和/或机器运行。这种情况下，应只有提供了适合的替代安全功能(如带速度限制的使能装置)时才允许此类操作。

示例：示教/编程、故障排查、过程微调等任务同时需要动力和机器运动。

以下是维修任务经常采用的单独或结合使用的安全功能示例：

- a) 保持运行；
- b) 使能控制；
- c) 速度、转矩、功率、位置、定位、温度、液位等监控或限制；
- d) 防止意外启动；
- e) 断开和能量耗散；
- f) 机械约束或抑制。

更多信息见附录 M。

SRP/CS 规范编制、设计和选型时，应分析机器维修过程中废弃或规避 SRP/CS 所提供风险减小措施的动机（见 5.2.3）。

SRP/CS 的设计还应分析预定操作者之外的其他执行任务的人员，如：

- 维修人员在危险区内时执行复位和重启功能的操作者；
- 预定保护单个人员的风险减小措施不适合多人使用。

维护模式下，SRP/CS 的设计应防止在未以适当方式通知或告知机器上或附近人员的情况下，允许远程访问（见 5.2.4）机器控制系统。

5.2.3 最小化废弃安全功能的动机

废弃或规避安全功能的动机取决于过程、机器（或其部分）的预定用途以及风险减小措施的设计细节。SRP/CS 的设计应最小化废弃安全功能的动机。

注 1：安全研究表明许多伤害都是由于废弃安全功能和/或安全防护装置造成的。更多信息见参考文献。

示例：设计风险减小措施和安全功能时，以下场景能引发废弃动机并加以考虑：

- 风险减小措施妨碍任务执行；
- 需要执行未经危险和风险识别和评估的任务；
- 风险减小措施影响生产速度或干扰了其他行为或用户偏好；
- 风险减小措施使用困难；
- 人员对风险减小措施和/或其关联风险没有认知；
- 不认可风险减小措施与其功能之间的适用性、必要性或恰当性；
- 未对执行安全功能的 SRP/CS 的硬件和软件访问权限加以限制。

注 2：提供方便执行任务措施的同时保护人员安全，减小废弃或规避安全功能和/或安全防护的动机。

注 3：ISO 14119 给出了如何最小化废弃联锁装置的可能性的方法和示例。

如果应用或管理不当，使用和访问可编程系统可能会增加废弃或规避安全功能的可能性。

5.2.4 远程访问

机器控制系统能被远程访问时，SRP/CS 仍应保持运行。使用信息给出了能远程访问的额外风险减小措施。

SRP/CS 的设计要求：只有已采取专门措施防止因未检测到机器内或附近人员而造成危险状况，才允许远程访问机器（例如，见 5.2.2.2）。

除非执行了本地安全功能确认，否则不应通过远程访问修改 SRP/CS 的安全相关软件。

注：远程启动对于机器上工作的人员来说属于意外启动，可能造成伤害。

5.3 确定各安全功能的所需性能等级(PL_r)

应确定和记录选取的每种安全功能的所需性能等级(PL_r)。所需性能等级的确定应以风险评估结

果为基础并与所需要的风险减小关联(见图 3)。附录 A 给出了确定安全功能 PL_r 的指南。定义安全功能时还应分析是否涉及叠加危险。进一步的指南见 A.3。

注 1: 也能采用其他方法确定 PL_r (例如 IEC 62061:2021 中附录 A 给出的方法)。

注 2: C 类标准通常会提供关于 PL_r 的信息。

注 3: 由于确定 PL_r 的方法包含主观估计, 因此允许与特定情况下的实际应用存在差异。

注 4: 安全功能的 PL_r 决定了执行安全功能并实现预定风险减小的控制系统所要求的可靠性。 PL_r 由若干风险因素决定。另见附录 A。

5.4 审查安全要求规范(SRS)

开始设计前应对照风险评估验证 SRS。审查应确保所有安全功能都有规范, 以实现机器预定的风险减小。SRS 的确认见 10.2。

应按照 10.1.1 的要求确认 SRS。

5.5 将 SRP/CS 分解成子系统

安全功能能够分解成子功能并分配给子系统。各子功能的描述应包括:

- 子功能的安全要求(功能要求和完整性要求);
- 各子功能的输入和输出。

SRP/CS 的构成可能包括:

- 一个或多个以前已确认的子系统;
- 一个或多个基于子系统组件的子系统;
- 以上两种的组合。

根据子系统的定义, 任何子系统的危险失效都会造成整个安全功能丧失。

示例: 图 6 给出了一个分解示例, 起始点为“触发事件”(如手动操动按钮、打开防护罩、遮断 AOPD 光束), 终止点为引发“机器执行器”(如电动机、气缸)安全响应的输出。

注 1: 安全功能 1 分解为子功能 1、子功能 2 和子功能 3。子功能 1 由子系统 1 执行。

注 2: 安全功能 2 分解为子功能 4 和子功能 5。子功能 4 由子系统 4 执行。

注 3: 安全功能 3 分解为子功能 6 和子功能 5。子功能 6 由子系统 6 执行。

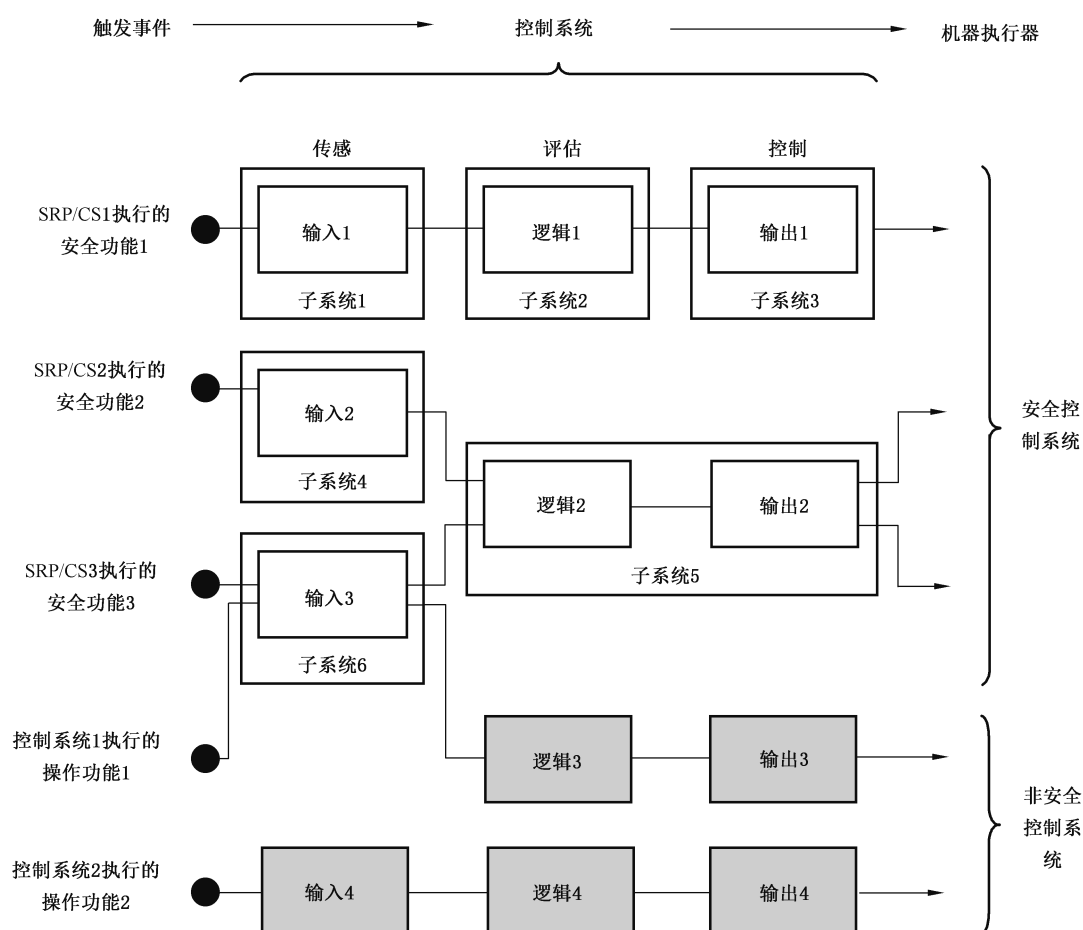


图 6 安全功能分解并分配给子系统示例

图 6 为子系统组合后用作以下 SRP/CS 的方框图：

- 触发事件(如打开防护罩、遮断 AOPD 光束)；
- 输入(如限位开关、传感器、AOPD)(子系统 1、子系统 4 和子系统 6)；
- 逻辑/处理(子系统 2 和子系统 5)；
- 输出/功率控制组件(如阀门、接触器、变流器、制动器)(子系统 3 和子系统 5)；
- 机器执行器(如电动机、气缸)；
- 互连方式(如电气、光学)。

图 6 所示 SRP/CS 分解为子系统为典型示例,但是整个 SRP/CS 也可以由单个或 3 个以上子系统实现。

注 4：SRP/CS 能由一个传感器、逻辑和功率控制组件构成的单个子系统实现。带一体式输出切换装置(如切断危险运动的继电器)的“智能”传感器单元(如光幕、激光扫描仪)就是由单个子系统实现的 SRP/CS 实例。

注 5：子系统或 SRP/CS 能够执行安全功能和标准控制功能。设计者能单独或组合使用任何可以获得的技术。SRP/CS 也能够提供操作功能(如将 AOPD 用于循环启动)。

已确认过的子系统设计者应按照 13.2 提供相关信息。

注 6：已确认过的子系统设计者可能是系统集成商、机器制造商或元件制造商。

6 设计考虑

6.1 已达到性能等级的评估

6.1.1 性能等级的一般要求

执行安全功能的能力是通过对性能等级的评估确定的。

应为执行安全功能的每个子系统和/或子系统组合确定性能等级。子系统的 PL 应通过对以下方面的估计确定。

- a) 架构(见 6.1.3);
 - 1) 指定子系统的类别;
 - 2) 评估是否符合该类别适用的定性(非量化)要求,包括:
 - 基本安全原则(GB/T 16855.2—2015 中表 A.1、表 B.1、表 C.1 和表 D.1);
 - 经验证的安全原则(GB/T 16855.2—2015 中表 A.2、表 B.2、表 C.2 和表 D.2);
 - 经验证的元件(GB/T 16855.2—2015 中表 A.3、表 D.3、附录 B 和附录 C)。
 - 3) 评估在故障条件下所需的行为是否得到满足。
- b) 单个元件的 MTTF_D 值(见 6.1.4,及附录 C 和附录 D)。
- c) DC(见 6.1.5 和附录 E)。
- d) CCF(见 6.1.6 和附录 F)。
- e) 安全相关软件设计对硬件运行的影响(见第 7 章和附录 J)。
- f) 针对系统性失效的措施的效果(见 6.1.7 和附录 G)。

注 1: 其他参数,例如操作方面、需求率、测试率,可能有特别的影响。

注 2: 控制系统元件或部件的安全相关参数值见附录 O。

这些方面能归纳为与评估过程相关的两种方法:

- 定量方面(单个元件的 MTTF_D 值、DC、CCF、架构);
- 影响子系统行为的定性方面(故障情况下的安全功能行为、安全相关软件、系统性失效、基本及经验证的安全原则的应用、经验证的元件的使用、环境条件及故障排除)。

注 3: 可靠性的作用(如 MTTF_D、架构)能够随着所使用的 SRP/CS 而变化。

注 4: 对于任何类型的系统(如复杂结构),有几种方法可以估计 PL 的定量方面,如马尔科夫模型、广义随机 petri 网(GSPN)、可靠性框图[见如 IEC 61508(所有部分)、IEC 61708、IEC 62021(所有部分)]。

本文件给出了 PL 评估的简化方法,该方法基于 5 种指定架构的定义,这些架构满足特定的设计准则以及故障条件下的行为(见 6.1.3)。

6.1 中给出了子系统的 PL 评估要求。6.1.8(图 12)和 6.1.9 给出了子系统 PL 评估的简化方法,该方法使用了附录 B~附录 H、附录 J、附录 K 和附录 L 中给出的流程。子系统组合的 PL 评估见 6.2。

应按照本文件的要求和指导实现 PL 的定性方面和避免系统性失效。系统性失效见 6.1.7 和附录 G。

如果产品的具体标准,如针对电敏感防护设备(ESPE)的 IEC 61496(所有部分)或针对压力敏感防护设备的 ISO 13856(所有部分),规定了避免或控制系统性或随机性失效的要求,则此类子系统除满足本文件规定的要求外,还应满足这些产品标准的要求。

应采取风险减小措施并应满足以下几点:

- 在组件层面上减小影响安全功能的失效概率。例如,通过选择经验证的组件或应用经验证的安全原则,或两者兼具,以最小化或排除致命故障或失效(见 GB/T 16855.2—2015)。
- 改进子系统的架构以避免故障的危险影响。有的故障可能需要检测,因此有必要采用冗余或

监控的架构,或两者兼具。

降低故障的概率和避免故障的危险影响能分开或结合使用。根据不同的技术,能通过以下方式实现:

- 选择可靠的组件并通过故障排除;
- 安全功能具有冗余或监控的架构系统,或两者兼具。

包括容错和故障检测在内的结构是决定 PL 的重要参数。架构约束限制了类别 B、类别 1 和类别 2 的最大可实现 PL。架构约束见 6.1.3.2.2~6.1.3.2.4。

应满足防止或避免 CCF 的要求。

制造商已提供 PL 或 SIL 和 PFH 值的子系统,无需再进行估计(如 DC、MTTF_D、CCF、SRESW 评估)。另见表 O.1。

6.1.2 性能等级(PL)和安全完整性等级(SIL)之间的关系

当使用一个或多个子系统设计安全功能时,每个子系统应根据本文件使用 PL,或根据 IEC 61508(所有部分)或 IEC 62061:2021 使用 SIL 进行设计。根据 IEC 61508(所有部分)或 IEC 62061:2021 设计的子系统可以使用,但应限于那些为使用路线 1_H(见 GB/T 20438.2—2017 中 7.4.4.2)的高需求或连续模式而设计的子系统。子系统应按 6.2 组合。PL 和 SIL 之间的关系见表 4。

表 4 性能等级(PL)与安全完整性等级(SIL)之间的关系

PL	SIL (见 IEC 61508-1) 高需求或连续模式
a	无对应
b	1
c	1
d	2
e	3
注 1: PL a 没有对应的 SIL 等级,主要用于减小轻微的、通常可逆的伤害的风险。 注 2: PL e 对应 SIL 3,通常是机械使用的最高等级。	

6.1.3 架构——类别及其与每个通道 MTTF_D、平均诊断覆盖率和共因失效(CCF)的关系

6.1.3.1 一般要求

根据本文件设计的子系统应符合 6.1.3.2 中规定的类别之一的要求。类别是实现特定 PL 的基础,描述了基于 6.1.1 中设计考虑的子系统在抵御故障方面的所需行为。

类别 B 是基本类别。故障的发生能够导致安全功能丧失。在类别 1 中,主要通过使用高质量的组件提高抗故障能力。在类别 2、类别 3 和类别 4 中,主要通过改善容错能力或诊断措施,或两者兼具,以改善性能。在类别 2 中,是通过定期检查指定的子功能是否被正确执行(无故障)实现的。在类别 3 和类别 4 中,是通过确保单一故障不会导致子功能的丧失实现的。在类别 4 中以及在类别 3 合理可行的情况下,这种故障被检测出来。类别 4 能够抵御故障累积。表 5 给出了子系统的类别、要求和子功能在故障情况下的行为概览。

当考虑部件的失效原因时,有可能排除某些故障(见 6.1.10.3)。

表 5 类别要求概述

类别	子系统要求摘要	子功能行为	用于实现安全的原则	每个功能通道的 MTTF _D	DC _{avg}	CCF
B (见 6.1.3.2.2)	子系统和/或其保护设备及元件都应根据相关标准进行设计、构造、选择、装配和组合,以使其能承受预期的影响。应使用基本安全原则	发生故障可导致子功能的丧失	主要特征是组件的选择	低~中	无	无关
1 (见 6.1.3.2.3)	应采用类别 B 的要求。应使用经验证的组件和经验证的安全原则	发生故障可导致子功能的丧失,但发生的概率低于类别 B 的概率	主要特征是组件的选择	高	无	无关
2 (见 6.1.3.2.4)	应采用类别 B 的要求和经验证的安全原则。 应在适当的时间间隔测试子系统	发生故障可导致两次测试之间子功能的丧失。 通过测试来检测子功能的丧失	主要特征是结构	低~高	低~中	见附录 F
3 (见 6.1.3.2.5)	应采用类别 B 的要求和经验证的安全原则。 安全相关部件的设计应使: ——这些部件中任何一个部件的单一故障都不会导致子功能的丧失; ——只要合理可行,单一故障都可被检测到	发生单一故障时,子功能总是执行。 会检测到某些故障但不是全部。 未检测到的故障累积可导致子功能丧失	主要特征是结构(冗余)	低~高	低~中	见附录 F
4 (见 6.1.3.2.6)	应采用类别 B 的要求和经验证的安全原则。 安全相关部件的设计应使: ——在这些部件中的任何一个部件的单一故障都不会导致子功能的丧失; ——单一故障在下次要求子功能时或之前检测到。 如果不可能,则未检测到的故障的积累不应导致子功能的丧失	发生单一故障时,子功能总是执行。 故障的累积的检测降低了子功能丧失的概率(高 DC)。 故障将被及时检测到,以防子功能丧失	主要特征是结构(冗余)	高	高(包括故障的累积)	见附录 F
注:全部要求见 6.1.3.2。						

子系统的类别选择主要取决于:

- 该子系统所贡献的安全功能所要实现的风险的减小;
- 所需性能等级(PL_r);
- 使用的技术;
- 子系统内的元件发生故障时产生的后果;
- 避免该子系统出现故障(系统性失效)的可能性;

- f) 平均危险失效间隔时间(MTTF_D)；
- g) 诊断覆盖率(DC)；
- h) 类别 2、类别 3、类别 4 情况下的 CCF。

6.1.3.2 指定的架构 —— 类别规范

6.1.3.2.1 一般要求

以下指定的架构满足相应类别的要求。

指定的架构显示了每个类别子系统结构的逻辑表示。

注 1：对于类别 3 和类别 4，并非所有的部件都需要物理冗余，但有冗余的措施能够保证单一故障不导致子功能的丧失。因此，技术实现(例如电路图)可能与架构的逻辑表示不同。

图 7~图 11 显示的不是示例，而是一般指定的架构。允许偏离这些架构，但均应通过适宜的分析工具进行论证，例如马尔可夫模型，故障树分析(FTA)，以使子系统满足所需性能等级(PL_r)。对于偏离指定架构的子系统，应提供详细的计算以证明 PL_r 的实现。

图 7~图 11 中的线条和箭头代表逻辑上的互连方式，并在适用时代表诊断方式。

注 2：子系统的结构是对 PL 有重大影响的关键特征。即使可能的结构种类很多，但基本概念往往是相似的。因此，机械领域中存在的大多数结构都能映射到其中一个类别。对于每一个类别，都能制作一个安全相关框图作为典型表示。这些典型的实现被称为指定架构，并在以下每个类别的说明中列出。

如果使用 6.1.8 的简化程序来估计 PL，子系统的架构应等同于声明的类别的指定架构。

6.1.3.2.2 类别 B

类别 B 子系统至少应根据相关标准进行设计、构造、选择、装配和组合，并将基本的安全原则(见 GB/T 16855.2—2015)用于具体应用，以耐受：

- 预期的运行应力，例如：与分断能力和频率有关的可靠性；
- 工艺物料的影响，例如：清洗机的洗涤剂，和；
- 其他相关的外部影响，例如：机械振动、电磁干扰(EMI)、动力源中断或扰动。

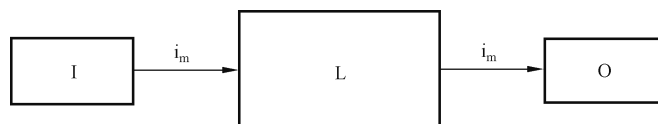
通道的 MTTF_D 应至少为低。

类别 B 可实现的 PL 最大值为 PL b。

注 1：类别 B 架构中没有平均诊断覆盖率(DC_{avg}=无)，CCF 分析是不相关的。

注 2：发生故障时可能会导致子功能的丧失。

对 EMI 的具体要求(抗扰度要求)可在相关产品或通用标准中找到。抗扰度要求与子系统尤其相关。包含有源电子组件的子系统应酌情满足基于环境的 EMI 抗扰度要求。实用指南见附录 L。



标引序号说明：

i_m —— 连接方式；

I —— 输入装置，如传感器；

L —— 逻辑；

O —— 输出装置，如主接触器；

图 7 类别 B 的指定架构

6.1.3.2.3 类别 1

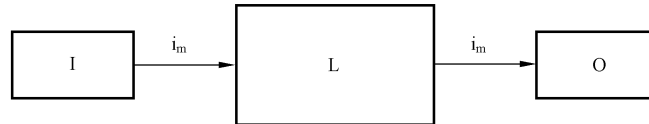
类别 1 除应满足与 6.1.3.2.2 对类别 B 的相同要求外，还满足以下要求。

类别 1 的子系统应采用符合 6.1.11 的经验证的组件和经验证的安全原则设计和构造(见 3.1.49 和 GB/T 16855.2—2015)。通道的 $MTTF_D$ 应为高。

注 1: 类别 1 架构中没有诊断覆盖率(DC_{avg} = 无)。在这种结构中(单通道架构),CCF 分析是不相关的。

类别 1 可实现的最大 PL 为 PL c。

注 2: 故障的发生能导致安全功能的丧失。然而,类别 1 中单个通道的 $MTTF_D$ 比类别 B 中的高。因此,安全功能丧失的可能性较小。



标引序号说明:

i_m ——连接方式;

I ——输入装置,如传感器;

L ——逻辑;

O ——输出装置,如主接触器。

图 8 类别 1 的指定架构

6.1.3.2.4 类别 2

类别 2 除应满足与 6.1.3.2.2 对类别 B 的相同要求外,还应遵循 3.1.49 和 GB/T 16855.2—2015 的“经验证的安全原则”。此外,还适用以下规定。

类别 2 的子系统设计应使其功能通道(I、L、O)在适当的时间间隔内得到测试。子功能的测试应先于任何危险情况,在要求安全功能之前或至少在要求之时进行,例如:

- a) 一个新循环开始之前;
- b) 其他运动开始之前;
- c) 要求安全功能时立即;
- d) 如果风险评估和操作类型表明有必要,运行期间定期进行。

测试本身不应导致危险状况(如由于响应时间的增加)。测试设备和提供安全功能的安全部件可以是一体的,也可以是分离的。

根据机器或部分机器的风险评估,该测试的启动可以是手动的。子功能的任何测试应做到:

——如果没有检测到故障,允许运行,或者

——如果检测到故障,产生触发适当控制动作的输出[测试设备的输出(OTE)]。

PL_r d 的输出(OTE)应触发一个安全状态,并保持到排除故障为止。

对于 PL_r c 及以下的 PL_r ,在可行的时候输出(OTE)应触发一个安全状态,并保持到故障清除为止。当不可行时(如最后的切换装置中的触点熔焊),OTE 发出警告即可。

DC_{avg} 的计算应只考虑功能通道的块(即图 9 中的 I、L 和 O),而不是测试通道的块。

类别 2 应采用以下规定:

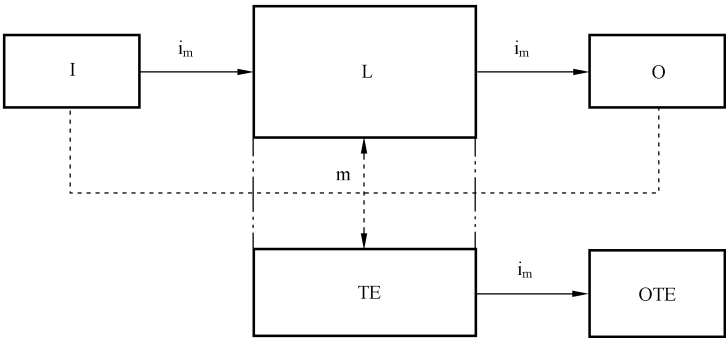
——要求率小于或等于测试率的 1%(见附录 K 中的注 1),或者一旦要求安全功能就立刻进行测试,并且检测故障和使机器处于非危险情况(通常为使机器停止)的总时间小于触及危险的时间(见 GB/T 19876—2012);

——测试通道(图 9 中 TE 和 OTE)的 $MTTF_D$ 大于功能通道 $MTTF_D$ 的一半。

所有功能通道(I、L、O)部件的诊断覆盖率(DC_{avg})应至少为低。功能通道的 $MTTF_D$ 应为低~高,取决于所需性能等级(PL_r)。应采取防止功能通道和测试通道 CCF 的措施(见 6.1.6 和附录 F)。

类别 2 可实现的最大 PL 为 PL d。

- 注 1: 对功能通道中的块的测试能通过监测等实现。
- 注 2: 类别 2 子系统行为特征为:
- 两次测试之间发生故障能导致子功能丧失,且;
 - 通过测试能检测到子功能丧失。
- 注 3: 类别 2 功能有效性的支持原理是所采用的技术措施,以及测试率的选择和测试设备的可靠性等,能够降低危险故障发生的概率。



标引序号说明:

i_m ——连接方式;

I ——输入装置,如传感器;

L ——逻辑;

m ——监控;

O ——输出装置,如主接触器;

TE ——测试设备;

OTE ——TE 的输出。

虚线代表合理可行的故障检测。

图 9 类别 2 的指定架构

6.1.3.2.5 类别 3

类别 3 除应满足与 6.1.3.2.2 对类别 B 的相同要求外,还应遵循 3.1.49 和 GB/T 16855.2—2015 的“经验证的安全原则”。此外,还适用以下要求。

类别 3 可实现的最大 PL 为 PL e。

类别 3 的子系统设计应确保单一故障不会导致子功能丧失。只要合理可行,单一故障应在下一次要求安全功能时或之前被检测出。

整个子系统的 DC 应至少为低。每个冗余通道的 $MTTF_D$ 应为低~高,取决于 PL_r 。应采取防止 CCF 的措施(见附录 F)。

- 注 1: 检测单一故障的要求并不意味着所有故障都被检测出。因此,未发现的故障的累积可能导致意外输出并使机器处于危险状况。用于故障检测的合理可行措施的典型示例,就是使用机械导向的继电器触点的反馈和冗余电气输出的监控(见附录 E)。
- 注 2: 如果有必要,由于技术和应用的原因,C 类标准的制定者能进一步给出故障检测的细节。
- 注 3: 类别 3 子系统行为特征为:
- 单一故障出现时子功能继续执行;
 - 检测到一些故障,但不是所有的故障;
 - 未检测到的故障的累积可能导致子功能丧失。

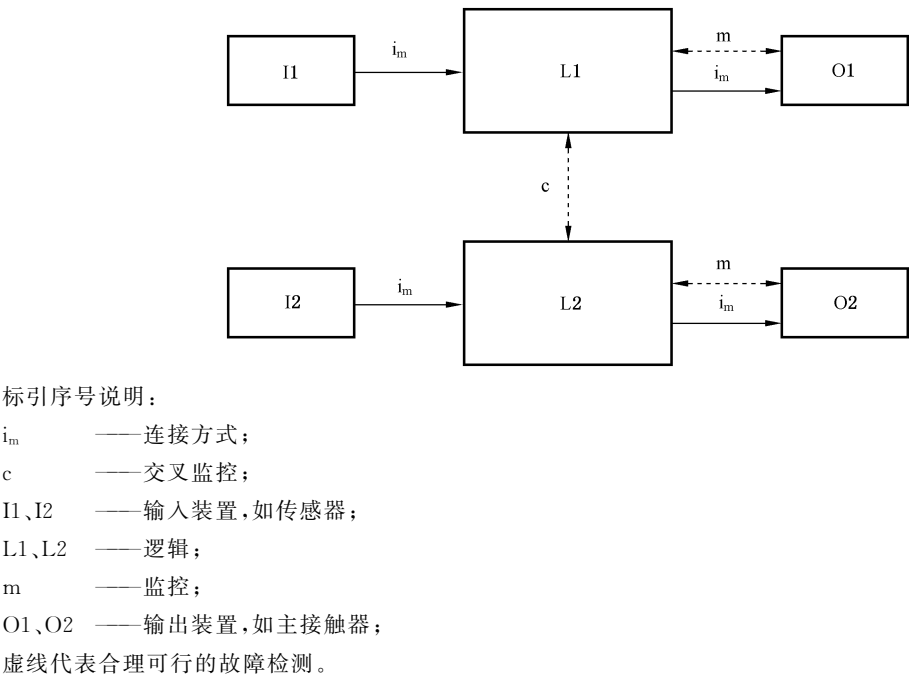


图 10 类别 3 的指定架构

6.1.3.2.6 类别 4

类别 4 除应满足与 6.1.3.2.2 对类别 B 的相同要求外，还应遵循 3.1.49 和 GB/T 16855.2—2015 的“经验证的安全原则”。此外，还适用以下要求。

类别 4 可实现的最大 PL 为 PL e。类别 4 的子系统设计应使得：

- 单一故障不会导致安全功能的丧失；
- 单一故障在下一次要求安全功能时或之前被检测到，例如：在开关接通时或机器工作循环结束时立即检测。但是如果无法进行这种检测，那么未发现的故障的累积也不应导致安全功能的丧失。

注 1：根据分析，例如 FEMA，概率很低的未检测到的故障，如果其被记录并验证，则无需考虑故障的累积。

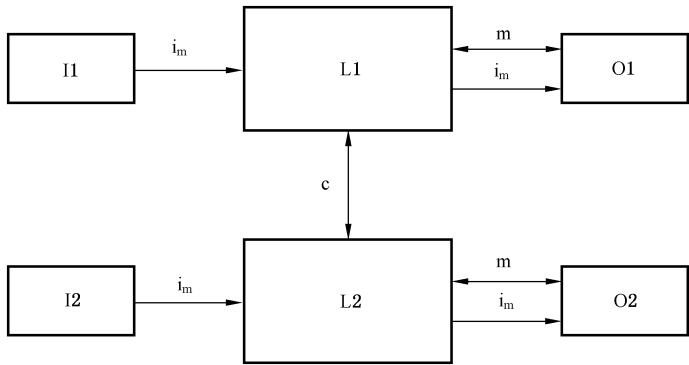
整个子系统的平均诊断覆盖率(DC_{avg})应为高。每个冗余通道的 $MTTF_D$ 应为高。应采取防止 CCF 的措施(见附录 F)。

注 2：类别 4 子系统行为特征为：

- 单一故障出现时安全功能继续执行；
- 及时检测到故障以防安全功能丧失；
- 考虑了未检测到的故障的累积。

注 3：类别 3 和类别 4 之间仅有的差别是类别 4 中的 DC_{avg} 更高，并且每个通道所需的 $MTTF_D$ 为“高”。

实际应用中，考虑两种故障的组合可能就足够了。



标引序号说明：

i_m ——连接方式；

c ——交叉监控；

I1、I2 ——输入装置，如传感器；

L1、L2 ——逻辑；

m ——监控；

O1、O2 ——输出装置，如主接触器；

用于监控的实线代表 DC，该 DC 大于类别 3 中指定架构的 DC。

图 11 类别 4 的指定架构

6.1.4 平均危险失效间隔时间(MTTF_D)

平均危险失效间隔时间(MTTF_D)是一个以时间为维度的量，用来表征所用部件的基本可靠性。对于恒定的危险失效率，MTTF_D 是危险失效率的倒数(例如，将 10⁹ h 内的失效次数换算为两次失效之间间隔的年数)。

估计组件 MTTF_D 的优先顺序为：

- a) 采用制造商的数据；
- 注 1：当组件(如机电组件)的 MTTF_D 数据由制造商提供时，需考虑制造商给出的操作次数。实际应用中的使用次数不高于制造商给出的操作次数。
- b) 使用附录 C 的方法；
- c) 在相当长的一段时间内，从相似环境中的相同部件应用中采集的失效率现场数据，前提是采集和分析方法能保证数据具有合理的置信区间；
- 注 2：关于现场数据的更多信息，见 GB/T 20438.7—2017 中 B.5.4。
- d) 选为 10 年。

附录 C 给出了如何计算或评估单个组件的 MTTF_D 值的实用指南。附录 D 描述了如何从中推导出每个通道的 MTTF_D，包括部件计数法和对称化。

对于表 5 的每个子系统，每个通道的最大 MTTF_D 值限制为 100 年。对于类别 4 的子系统，每个通道的最大 MTTF_D 值限制为 2 500 年。

注 3：更高的值是合理的，因为在类别 4 中，其他定量因素、结构及 DC 已达到最大值。这就允许将 3 个以上类别 4 的子系统串联，且根据 6.2 可实现 PL e。

每个通道的 MTTF_D 值分为 3 个等级(见表 6)，应单独考虑每个通道的值(例如单通道、冗余系统的每个通道)。

表 6 每个通道的平均危险失效间隔时间(MTTF_D)

MTTF _D	
每个通道的指标	每个通道的范围
低	3 年≤MTTF _D <10 年
中	10 年≤MTTF _D <30 年
高	30 年≤MTTF _D ≤100 年 ^a
<p>注 1：每个通道 MTTF_D 的范围的选择基于该领域内当前最先进水平的失效率，与 PL 对数标度形成对数匹配关系。现实中，子系统每个通道的 MTTF_D 值预期不小于 3 年，否则这意味着一年以后市场上 30% 的系统将不合格且需要更换。每个通道的 MTTF_D 值大于 100 年也不合适，因为用于高风险的子系统不宜只依靠组件的可靠性。为了加强子系统预防系统性和随机失效的能力，需要采用冗余和测试等附加方法。为了切实可行，范围的数量限制在 3 个内。执行安全功能的子系统的单个通道 MTTF_D 值最大限制为 100 年。单个组件的 MTTF_D 值可以更高(见表 D.1)。</p> <p>注 2：本表中给出的边界值可假定其精确度在 5% 范围内。</p>	
^a 对于类别 4，MTTF _D 的限制为 2 500 年。	

6.1.5 诊断覆盖率(DC)

诊断覆盖率(DC)是指检测出的危险失效率和总的危险失效率之间的比值。在类别 2、类别 3 和类别 4 中应分析 DC。

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \dots\dots\dots (1)$$

式中：

Σλ_{DD} ——所有检测到的危险失效的失效率之和；

Σλ_{Dtotal} ——全部危险失效的失效率之和。

DC 应基于失效模式和影响分析(FMEA)(见 IEC 60812:2018)，或通过使用基于 E.1 和表 E.1 的 DC 简化估计。E.2 描述了如何估计平均诊断覆盖率(DC_{avg})。

- 注 1：对于 DC 的估计，在大多数情况下，能使用 FMEA(见 IEC 60812 和 EN 50495:2010 的附录 B)或类似的方法来考虑所有相关的故障和/或失效模式。见 GB/T 16855.2—2015 的 E.5.3。
- 注 2：通常，逻辑单元负责输入和输出设备的诊断功能。
- 注 3：所使用的技术将影响实施故障检测的可能性。
- DC 的值分 4 级给出，见表 7。

表 7 诊断覆盖率(DC)

DC	
指标	范围
无	DC<60%
低	60%≤DC<90%
中	90%≤DC<99%
高	DC≥99%

表 7 诊断覆盖率(DC) (续)

DC	
指标	范围
<p>注 1: 对于包含几个部件的子系统,图 12、第 7 章和 E.2 中采用了 DC 的平均值 DC_{avg}。</p> <p>注 2: DC 范围的选择基于 3 个关键值:60%、90%和 99%,这也是在其他涉及测试 DC 的标准中确定的。研究表明,测试有效性的特征量度是$(1-DC)$而不是 DC 本身。$(1-DC)$的关键值 60%、90%和 99%形成一种适合对数 PL 标度的对数标度。小于 60%的 DC 值只能轻微影响被测系统的可靠性,因此称为“无”。复杂系统的 DC 值很难超过 99%。为了切实可行,范围的数量限制在 4 个。本表中给出的边界值认为精确度在 5%范围内。</p>	

6.1.6 共因失效(CCF)

对于类别 2、类别 3 和类别 4 的子系统,应分析具有共同原因的两个或多个独立故障的概率。在类别 2 中,CCF 指的是功能通道和测试通道中的共因失效。在类别 3 和类别 4 中,CCF 指的是两个功能通道中的共因失效。应采取足够的措施防止 CCF(见附录 F)。

6.1.7 系统性失效

系统性失效的发生有多种原因,其中包括:

- 错误的设计规格;
- 制造失败;
- 环境压力影响(例如,温度,振动及 EMI 抗扰度);
- 操作失败;
- SRS、硬件和软件设计中的人为错误。

为了建立足够等级的系统完整性,设计和实施安全功能的方法应是系统化的。

应编制功能安全计划记录为实现 SRP/CS 所要求的功能安全而必需进行的活动。编制功能安全计划的目的是为防止不正确的规范、实施或修改问题提供措施。

特别是在设计过程中,应实施系统性失效的控制和规避(见第 10 章和附录 G)。

6.1.8 估计子系统性能等级的简化程序

本条款描述了基于指定架构估计一个子系统 PL 的简化程序。其他架构可以被映射到这些指定的架构上进行 PL 估算(见 6.1.1)。

指定架构以模块图表示,并在 6.1.3.2 中的每个类别说明中列出。关于模块法和安全相关模块图的信息在 6.1.3.2 和附录 B 中给出。也可见 IEC 61708:2016。

每个子系统都分配一个指定的架构。如果 SRP/CS 由一个子系统组成,整个 SRP/CS 的指定架构将是相同的。如果 SRP/CS 由多个子系统组成,每个子系统均应分配一个指定架构,因此一个 SRP/CS 能包括多个架构。

简化方法基于:

- a) 任务时间(T_M)为 20 年(见 3.1.36);
- b) 任务时间内失效率恒定;
- c) 已采用足够措施防止 CCF(beta 系数为 2%),见附录 F 或 GB/T 20438.6—2017 中附录 D 的指南。

注:任务时间(T_M)假定为 20 年,此期间的组件可靠性能通过恒定的失效率来描述或估算。这普遍应用于电子子

系统中。当达到任务时间时,通过替换 SRP/CS 或采取等效措施以确保估计的 PL 仍然有效。

要声明 20 年的任务时间,应满足 6.1.3.2.2 对类别 B 的要求。如果使用磨损较快的部件或其他技术原因造成的实际的任务时间可能少于 20 年,宜予以记录。见 C.4。

该方法考虑把类别作为具有规定 DC_{avg} 的架构。每个子系统的 PL 取决于架构、每个通道的 $MTTF_D$ 以及 DC_{avg} 。

具有软件的子系统应满足第 7 章的要求。6.2 中考虑了几个子系统的组合。

图 12 显示了类别与每个通道 $MTTF_D$ 和 DC_{avg} 的组合能够实现的 PL。图 12 给出了类别与 DC_{avg} (水平轴)和每个通道 $MTTF_D$ (柱状图)可能的不同组合,用于估计 PL。柱状图中的阴影代表每个通道 $MTTF_D$ 的 3 个范围(低、中、高),能够选择用来实现所需的 PL。

在使用图 12 的简化方法(代表了基于 6.1.3 中指定架构的不同马尔可夫模型的结果)之前,应确定子系统的类别(见 6.1.3.2)、 DC_{avg} (见 6.1.5)和每个通道的 $MTTF_D$ (见 6.1.4)(见附录 C~附录 E)。对于类别 2、类别 3 和类别 4,应采取足够的措施防止 CCF(见 6.1.6 及附录 F)。考虑到这些参数,图 12 提供了一个确定子系统实现的 PL 的图形化方法。类别(包括 CCF)和 DC_{avg} 的组合决定了要选择图 12 的哪一行。根据每个通道的 $MTTF_D$,应在相关柱状图的 3 个不同阴影区域中选择 1 个。

图 12 中的垂直带显示了 $MTTF_D$ 、类别和 DC_{avg} 的每个组合所能期望的性能范围。在图 12 中的垂直带上找到这些变量的恰当范围,然后读到纵轴上,就会显示出用这种组合能够实现的 PL。根据每个通道的 $MTTF_D$ 的精确值对 PL 进行更精确的数字选择,见附录 K。

估计子系统性能等级的该简化程序的详细示例见附录 I。

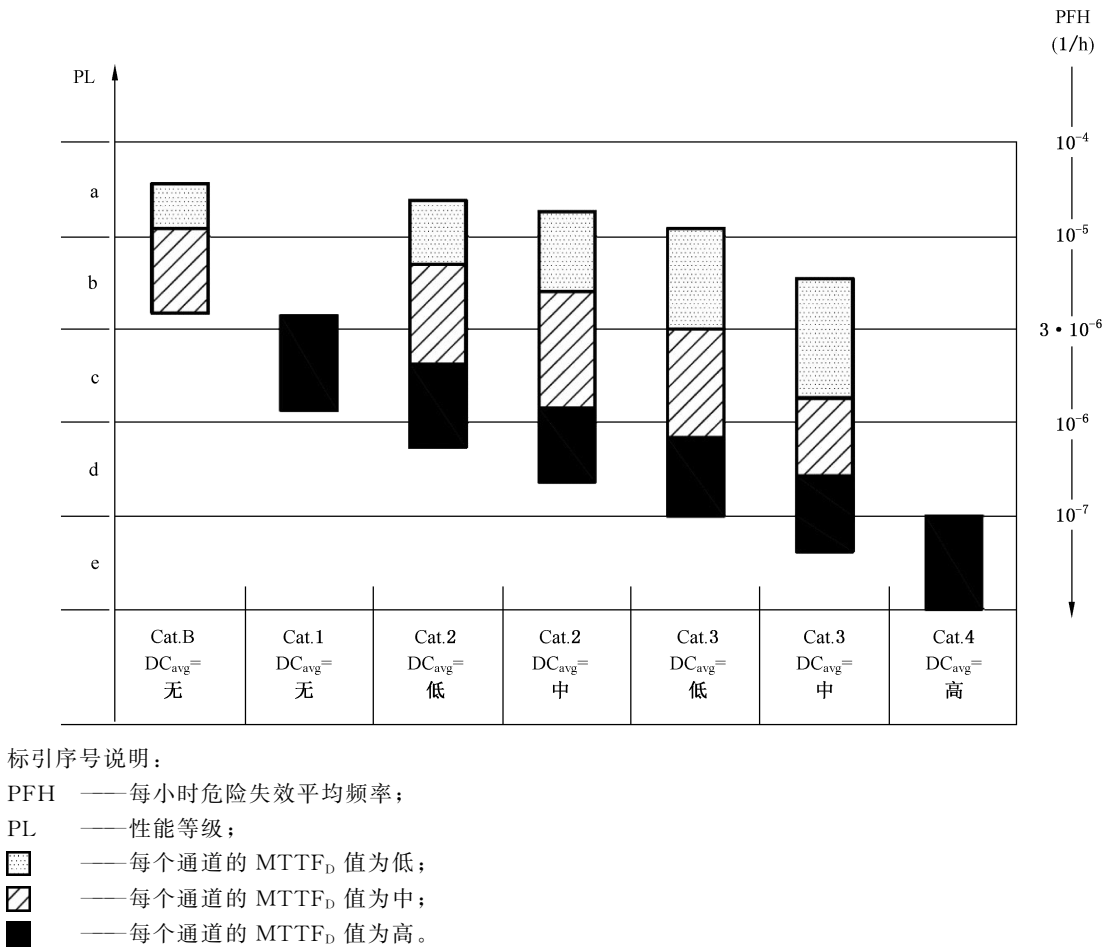


图 12 PL 与类别、 DC_{avg} 、每个通道的 $MTTF_D$ 的关系

6.1.9 无 $MTTF_D$ 时确定性能等级和 PFH 的替代程序

6.1.9.1 概述

在没有 $MTTF_D$ 的情况下,确定 PL 的替代程序只限于包含机械、液压、气动、电液压或电气动组件的子系统,这些子系统没有可靠性数据,也不能应用 C.2 中给出的良好工程实践方法。在这种情况下,机器制造商可以使用 6.1.9.2~6.1.9.4 中描述的替代程序来评估 PL,而无需进行任何 $MTTF_D$ 计算。

6.2 中考虑了多个子系统的组合。

6.1.9.2 前提条件

如果机械、液压或气动组件(或由混合技术组成的组件)无特定应用或组件制造商的可靠性数据,并且不能应用 C.2 的良好工程实践方法,机器制造商可以评估 PL 的可量化方面,而不进行任何 $MTTF_D$ 计算。在没有 $MTTF_D$ 数据的情况下,安全相关性能等级(PL)能够通过架构、DC 和针对 CCF 的措施来实现。

作为最坏的假设, T_{10D} 值限制为 10 年。对于经验证的组件,可以接受 T_{10D} 为 20 年的假设。在这个过程中,DC_{avg} 的计算被简化为子系统中所有单个组件 DC 值的算术平均值。

任务时间(T_M)假定为 20 年。对于类别 2,需要有足够的测试率(见 6.1.3.2.4)。应满足每个类别关于 DC_{avg} 和 CCF 以及系统性问题等(见 6.1.3)的要求。

6.1.9.3 输入或输出子系统

表 8 显示了可实现的 PL(对应于图 12)和类别之间的关系。如果遵循基本的安全原则,使用类别 B 能实现 PL a 和 PL b。如果使用经验证的组件、基本的和经验证的安全原则,使用类别 1 或类别 2 能实现 PL c。

如果使用经验证的组件、基本的和经验证的安全原则,使用类别 3 能够实现 PL d。使用类别 4 能够实现 PL e。

表 8 基于类别和组件选择的性能等级和 PFH 估计

类别 ^a	附加要求	估计的 PFH (1/h)	可实现的 PL ^b
B	—	5.0×10^{-6}	b
1	—	1.7×10^{-6}	c
2	仅使用经验证的组件	1.7×10^{-6}	c
3	仅使用经验证的组件	2.9×10^{-7}	d
4	仅使用经验证的组件	4.7×10^{-8}	e
^a 除 $MTTF_D$ 外,还应满足 6.1.3.2.2~6.1.3.2.6 中对相应类别的所有要求。 ^b 这里提到的可实现的 PL 只包括可量化的方面。还应满足非量化方面的附加要求,如系统性失效和软件(见 6.1.1)。			

6.1.9.4 逻辑子系统

在没有 $MTTF_D$ 数据的情况下,能采用估计 $MTTF_D$ 的保守方法。

——对于类别 B、类别 2 和类别 3,每个通道的 $MTTF_D$ 为 10 年。

——对于类别 1,如果使用经验证的组件,则能假定通道的 $MTTF_D$ 为 30 年(见 6.1.3.2.3)。

可能实现的最大 PL 为 PL c(见附录 K)。

对于类别 2 和类别 3,应分析共因失效和 DC。对于类别 2 和类别 3, DC_{avg} 应匹配至少 60%。

本方法不包括类别 4。

利用类别、 $MTTF_D$ 和 DC_{avg} ,能通过表 K.1 确定子系统的 PL 和 PFH。

6.1.10 故障考虑和故障排除

6.1.10.1 一般要求

在设计安全子系统时应评估故障及其影响。应考虑其故障可能导致子系统的某个功能通道中的安全功能失效的每个元件。设计者应列出一份可能发生在 SRP/CS 中的故障的清单。该清单应包括所有考虑到的故障在设计中是如何关注到这些故障的说明。如果提出排除故障,则给出排除的理由。对于组件制造商已确认的子系统,安全功能的设计者没有必要考虑组件的内部故障,只需考虑接口的故障。

注:执行安全功能不直接需要但起支持作用的元件(如滤波元件、过电压保护),通常不会影响通道的 $MTTF_D$ 。

6.1.10.2 故障考虑

GB/T 16855.2—2015 列出了各种技术的重要故障和失效。这些故障清单并不详尽,如有必要,应考虑并列出其他故障。在这种情况下,也应明确阐述评估方法。对于 GB/T 16855.2—2015 中未提及的组件,应采用一种方法来评估组件可能的故障或失效的影响,或两者兼具的影响,如 FMEA(见 IEC 60812),目的是识别这些组件考虑的故障。

一般来说,应考虑到以下故障准则:

——如果由于一个故障导致更多的组件故障,则第一个故障和所有后续故障应被视为单一故障;

——同时发生两个或更多不同原因的故障被认为极不可能,因此无需考虑。

具有共同原因的两个或多个独立故障应视为一个 CCF(见附录 F)。

6.1.10.3 故障排除

为了评估子系统,可能有必要排除故障。故障排除是技术安全要求和理论上发生故障的可能性之间的平衡。

故障排除能基于:

- a) 某些故障从技术角度考虑不太可能发生;
- b) 与具体应用无关的普遍接受的技术经验;以及
- c) 与具体应用和特定伤害有关的技术要求。

故障排除只适用于元件的某些故障,由设计者(制造商或集成商)根据设计和使用提出的限制证明相应故障的排除。只有根据已知的物理科学规律证明其不可能发生的情况下才能采用故障排除。任何这样的故障排除都应证明并记录。

对子系统内的某个元件的某些故障进行故障排除并不限制对系统性失效采取措施的必要性。

可能有些故障是由制造商排除的,有些是由子系统集成商排除的。

排除的每种故障类型都应有具体的特征描述。仅仅说明一个组件不会因磨损而断裂、变形或退化是不能接受的。有必要说明在何种直接影响下,该组件不会因磨损而断裂、变形或退化。例如,当受到来自 Y 方向的 X 牛顿的力时,该元件不会发生故障。

在所有预期的环境条件下,包括温度、压力、振动、污染、腐蚀性气氛,故障排除都应有依据。

PL e 不应仅依赖于故障排除。

注 1: 故障排除的信息见 GB/T 16855.2—2015 中的附录 A~附录 D。

注 2: 产品标准能提供更多信息。

6.1.11 经验证的组件

安全相关应用中的经验证的组件是指其符合以下情况之一:

a) 在过去被广泛使用,并在类似的应用中取得了成功的记录。

注: 见 GB/T 20438.2—2017 中 7.4.10“经使用证明”。

b) 列于 GB/T 16855.2—2015 中的附录 A~附录 D。

c) 根据相关的产品和应用标准,使用证明其对安全相关应用的适用性和可靠性的原则进行制作、验证和确认。

是否接受某个特定的组件是经验证的取决于应用,例如,由于环境影响。

复杂的组件(如 PLC、微处理器和专用集成电路)不应视为等同于经验证的组件。

6.2 实现总的安全功能性能等级的子系统组合

6.2.1 概述

SRP/CS 可以使用子系统的组合来实现,总的 PL 可以使用本条款中描述的方法实现。在这种情况下,需要将子系统的组合作为一个 SRP/CS 进行验证(见图 13)。这些子系统可以被赋予相同或不同的类别。

根据 6.1.3.2,多个子系统组合为 SRP/CS 时,组合起始于安全相关信号的触发点,终止于动力控制元件的输出。组合的子系统能由几个线性(串联)方式连接的部件组成。所有部件各自的性能等级(PL)都已算出时,为了避免对组合子系统实现的性能等级(PL)重新进行复杂的估算,以下是对子系统组合进行估算的方法。

如果使用依据 IEC 62061:2021 或 IEC 61508(所有部分)(SIL),采用路线 1_H(见 GB/T 20438.2—2017 的 7.4.4.2)的高需求或连续模式的先前已确认的子系统,使用 6.1.2 和 6.2.2 将 SIL 关联至 PL。根据 IEC 61508(所有部分)或 IEC 62061:2021 以及上述限制计算的 PFH 值,能作为本文件的 PFH 值。

类别不能总是推断出来,并且不需要按照 IEC 62061:2021 或 IEC 61508(所有部分)确认的子系统得出。

6.2.2 PFH 值已知

当组合已知 PFH 值的子系统时,假设有 n 个独立的子系统 SB_1 到 SB_n ,PFH 值能如下图所示进行组合。这些子系统以串联组合的方式运行,作为一个整体执行某个安全功能。每个 SB_i 都已经评估了 PL_i 。这种情况如图 13 所示(见图 5 和图 H.2)。

如果所有子系统的 PFH 值已知,那么组合 SRP/CS 的 PFH 为 n 个单个子系统全部 PFH 值的和。SRP/CS 的 PL 受到以下限制:

——参与执行安全功能的单个子系统的最低 PL 值,以及

——根据表 2 查出的与组合 SRP/CS 的 PFH 相对应的 PL。

注: 此方法的示例见附录 H。

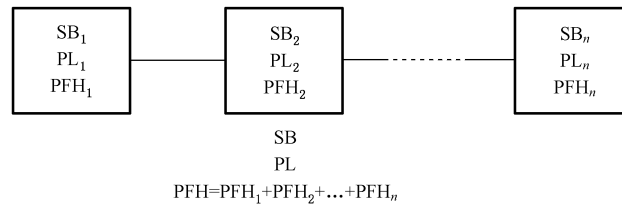


图 13 实现总的 PL 的子系统组合

6.2.3 PFH 值未知

如果所有单个 SB_i 的 PFH 值未知,那么作为 6.2.2 的替代方案,执行安全功能的 SRP/CS 的 PL 可以根据 6.1 确定,或使用表 9 计算如下:

- a) 识别所有子系统中最底的 PL:此为 PL_{low} ;
- b) 识别所有 PL_{low} 的子系统的数量:此为 N_{low} ;
- c) 在表 9 中查找 PL。

表 9 串联排列子系统 PL 的确定

PL_{low}	N_{low}	SRP/CS 的 PL
a	>3	无,不准许
	≤ 3	a
b	>2	a
	≤ 2	b
c	>2	b
	≤ 2	c
d	>3	c
	≤ 3	d
e	>3	d
	≤ 3	e

注:本表格基于和 PL 之间存在对数关系的 PFH 范围(见表 2)。

6.3 基于软件的手动参数化

6.3.1 概述

6.3 仅规定了基于软件的手动参数化,该参数化由授权人员执行和控制。见 5.2.2.6 和表 M.2。

某些安全相关子系统或 SRP/CS 需要对安全功能或子功能进行参数化。

示例:具有集成子功能的变频器能通过基于 PC 的配置工具进行参数化以设置速度限制参数。为了建立激光扫描仪的检测区域,能根据制造商的安全文件和机器风险评估配置角度和距离等参数。

基于软件的手动参数化要求的目的是保证安全功能或子功能指定的安全相关参数正确地传输到执行安全功能或子功能的硬件中。能采用不同的方法设置此类参数,如基于拨码开关的参数化或专用参数化软件(通常称为配置或参数化工具)。

注 1:本条款未考虑无人员交互自动进行的安全相关参数化,例如基于输入信号的参数化。

注 2：操作者对机器的直接控制不视为本条款所述的手动参数化，例如对叉车的速度控制。

如果配置或参数化工具是根据本文件或 IEC 61508(所有部分)预先设计的，如与其专用子系统一起使用时，则假定不会出现 6.3.2 中所列的影响或其他任何可合理预见的影响导致的危险失效。当使用预先设计的工具进行基于软件的手动参数化时，6.3.5 的要求适用。

如果安全相关子系统或 SRP/CS 不能通过基于软件的手动参数化功能进行参数化，则 6.3 不适用。

6.3.2 安全相关参数的影响因素

安全相关参数的设计应使其能承受相关的外部影响。在基于软件的手动参数化过程中，参数可能会受到以下影响：

- a) 参数化负责人的数据输入错误；
- b) 参数化工具软件的故障；
- c) 随参数化工具提供的其他软件和/或服务的故障；
- d) 参数化工具硬件的故障；
- e) 从参数化工具向 SRP/CS 或子系统传输参数期间出现的故障；
- f) SRP/CS 或子系统无法正确存储传输参数的故障；
- g) 参数化过程中的系统性干扰，例如电磁干扰或断电；
- h) 由于外部影响或因素造成的干扰，例如电磁干扰或(随机)断电。

如果不采取任何措施来抵消、避免或控制上述影响造成的潜在危险失效，可能导致以下后果及影响：

- 在没有通知参数化负责人的情况下，参数化过程中全部或部分参数没有更新；
- 全部或部分参数不正确；
- 参数被用于不匹配的设备，例如通过有线或无线网络进行参数传输时。

6.3.3 基于软件的手动参数化要求

基于软件的手动参数化应使用由 SRP/CS 或相关子系统的制造商或供应商提供的专用工具。SRP/CS 或相关子系统和参数化工具应具有防止未经授权修改的能力，例如通过使用专门的密码。

只有处在不会导致非安全状态的情况下，才允许在机器运行时进行参数化。

通过使用预先设计的子系统也可能满足要求。

使用预先设计的具备基于软件手动参数化能力的 SRP/CS 或子系统，目的是防止 6.3.2 中所列的影响或其他任何可合理预见的影响导致的危险失效。预先设计的子系统的确认应包括参数化。

根据本文件设计具备基于软件手动参数化能力的 SRP/CS 或子系统时，不应出现上述影响或其他任何可合理预见的影响而未能发现的危险失效，还应满足以下要求。

- a) 基于软件的手动参数化设计应被视为 SRS 中描述的 SRP/CS 设计中安全相关的一个方面。
- b) SRP/CS 或子系统应提供检查数据可信度的方法，例如检查数据的限制、格式和/或逻辑输入值。
- c) 应保持用于参数化的所有数据的完整性，并应通过以下措施实现：
 - 1) 通过有效性(范围)检查控制配置值范围；
 - 2) 控制传输前的数据损坏；
 - 3) 控制参数传输过程中的错误影响；
 - 4) 控制不完整参数传递的影响；
 - 5) 控制参数化硬件和软件的故障和失效的影响；
 - 6) 控制电源中断的影响。
- d) 参数化工具应满足本文件或 IEC 61508(所有部分)规定的 SRP/CS 的所有相关要求。

- e) 作为 d) 的替代方案,应使用一个特殊程序设置安全相关参数。该程序应包括通过以下方式确认输入到 SRP/CS 的参数:
- 通过修改参数重新传输给参数化工具的方式,或
 - 其他方式确认参数的完整性;
 - 以及随后的确认,例如,由合适的熟练人员和通过参数化工具自动检查。在确认更改之前,安全相关参数的新值不应用于安全相关的操作。

注:参数化软件工具使用非专用于此目的的设备(例如个人电脑或同等设备)时,这一点尤为重要。

传输/转发过程中用于编码/解码的软件模块,以及用于向用户显示安全相关参数的软件模块,至少应在功能中使用相异性技术,以避免系统性失效。

6.3.4 参数化工具的验证

参数化工具的基本功能应通过以下活动进行验证:

- 验证每个安全相关参数设置正确(最小、最大和代表值);
- 验证安全相关参数的合理性,例如通过无效值检测;
- 验证是否提供了防止未经授权修改安全相关参数的方法。

注:使用非专用于此目的的设备(例如个人电脑或同等设备)进行参数化时,验证尤为重要。

6.3.5 基于软件的手动参数化的文档

基于软件的手动参数化应使用 SRP/CS 或相关子系统的制造商或供应商提供的专用参数化工具,并应根据使用信息中的要求进行记录。该信息可能来自不同的相关方,见第 13 章(使用信息)。应采取保护措施防止未经授权的访问。

应记录初始参数化以及随后修改的信息,记录应包括:

- a) 初始参数化或变更的日期;
- b) 数据集的数据或版本号;
- c) 进行参数化的人员姓名;
- d) 所用数据的来源说明(例如预定义的参数集);
- e) 明确指明安全相关的参数;
- f) 对于可能或需要连续性修改的参数化工作的影响和界限;
- g) 明确指明用于特定参数化设定的 SRP/CS 或相关子系统。

7 软件安全要求

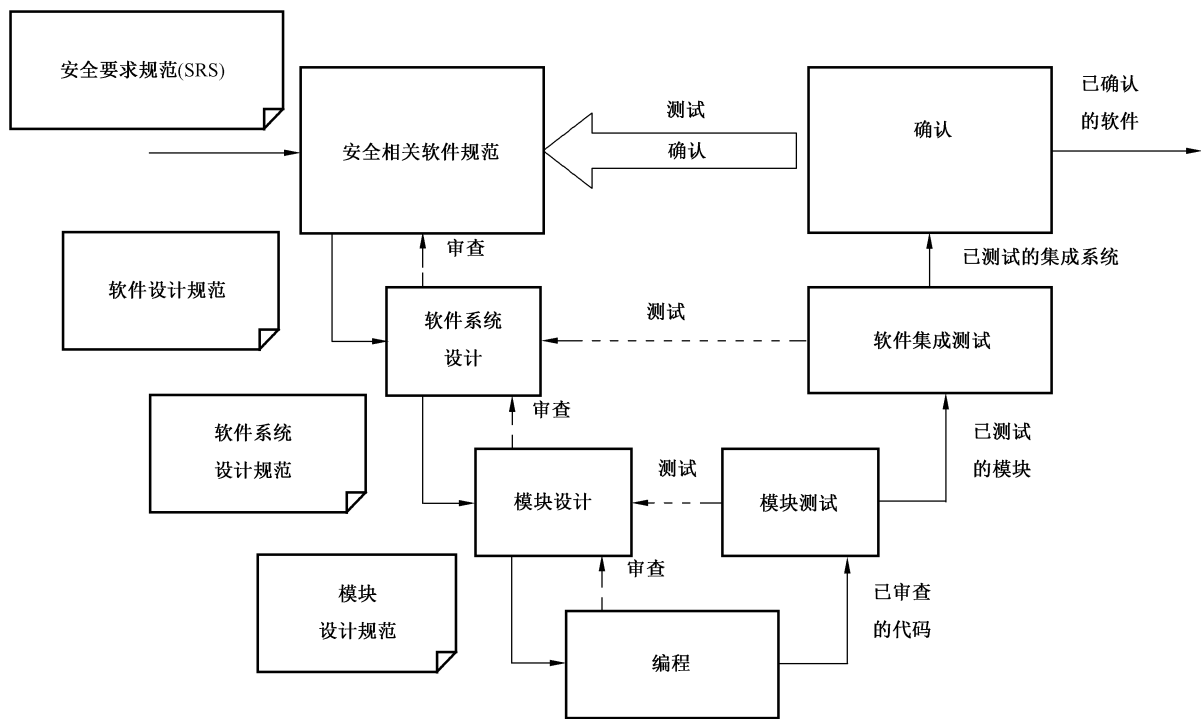
7.1 一般要求

尽管人工智能(AI)可能用于 SRP/CS,但本文件不涉及 AI 技术及其用于 SRP/CS 的额外具体要求。

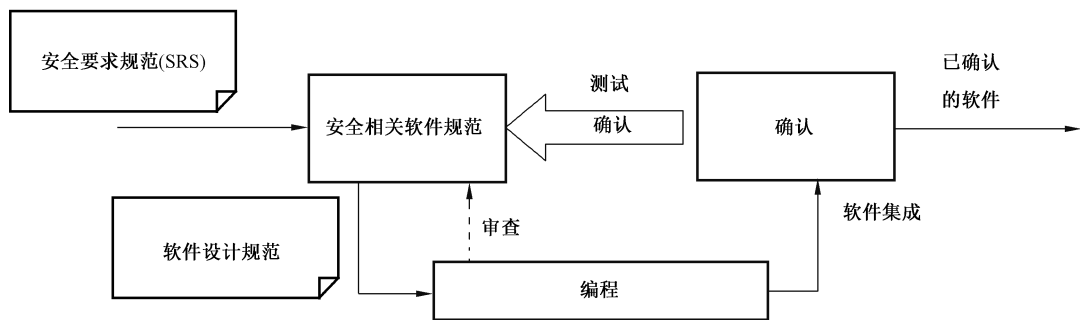
安全相关嵌入式软件或应用软件开发的相关活动应重点关注在软件生命周期[见图 14 a)]中避免故障。以下要求的主要目的是为了使软件可读、可理解、可测试和可维护。

注 1:附录 J 对生命周期活动给出了更详细的推荐。

注 2:附录 N 概述了使用 LVL 实现 SRASW 以及使用 FVL 实现 SRASW 或 SRESW 的方法。



a) 软件安全生命周期的简化 V 模型



b) 已预评估的安全相关硬件及软件模块与 LVL 结合使用时的软件简化 V 模型

标引序号说明：
—— 结果；
- - - 验证。

注：通常，如图 14 b) 所示的简化软件生命周期适用于在 LVL 中采用模块化编程，这种编程仅需配置简单的互连，其将输入和输出限制在一组预先定义的值，包括模块的组合。

图 14 简化 V 模型

已预评估的安全相关硬件及软件模块与 LVL 结合使用时，则适用图 14 b) 所示的简化软件生命周期。

当安全功能及非安全功能在同一硬件环境下实现时，应证明在正常及故障情况下，安全功能不受非安全功能的影响。例如安全响应的执行不应在任何时候被阻止或延迟等。

7.2 有限可变语言(LVL)及全可变语言(FVL)

7.2.1 有限可变语言(LVL)

LVL 是一种以文本和/或图形表达的软件编程语言。用于商业和工业可编程电子控制器，其能力

范围限于其应用范围(见 GB/T 20438.4—2017 中 3.2.14)。

LVL 的设计宜便于软件设计者理解,并宜重点聚焦于需要实现的应用。

以下是 LVL 的示例:

- a) 梯形图(见 GB/T 15969.3—2017 中 8.2):一种图形语言,由一系列输入符号(代表类似于常开和常闭触点等设备的行为)和输出符号(代表类似于继电器的行为)通过线条(表示流向)相互连接组成;
- b) 功能块图(见 GB/T 15969.3—2017 中 8.3):除了布尔运算符外,还允许使用更复杂的功能,如数据传输文件、块传输读/写、移位寄存器和顺序器指令;
- c) 顺序功能图(见 GB/T 15969.3—2017 中 6.7):顺序程序的图形化表示,由相互连接的步骤、动作以及带有转换条件的定向连接组成;
- d) 布尔代数:基于布尔运算符(如“与”“或”和“非”)的低级语言,具有一些添加助记符指令的能力。

7.2.2 全可变语言(FVL)

该类型语言是为计算机程序员设计的,提供了实现各种功能和应用的能力。该类型语言提供了所有可能的编程选项,能创建在如何构造逻辑方面具有完全灵活性的应用程序。

注:使用 FVL 的典型系统是通用计算机。

在机械领域,FVL 多用于嵌入式软件且很少用于应用软件。

示例:Ada、C、Pascal、指令表、汇编语言、C++、Java、MATLAB、Simulink、ST 及 SQL(没有使用限制且指令完全可变)。

7.2.3 使用有限可变语言(LVL)或者全可变语言(FVL)的决策

通常,软件能由 LVL 或 FVL 编写。SRP/CS 的设计者应根据图 15 决定编程语言采用 FVL 还是 LVL。

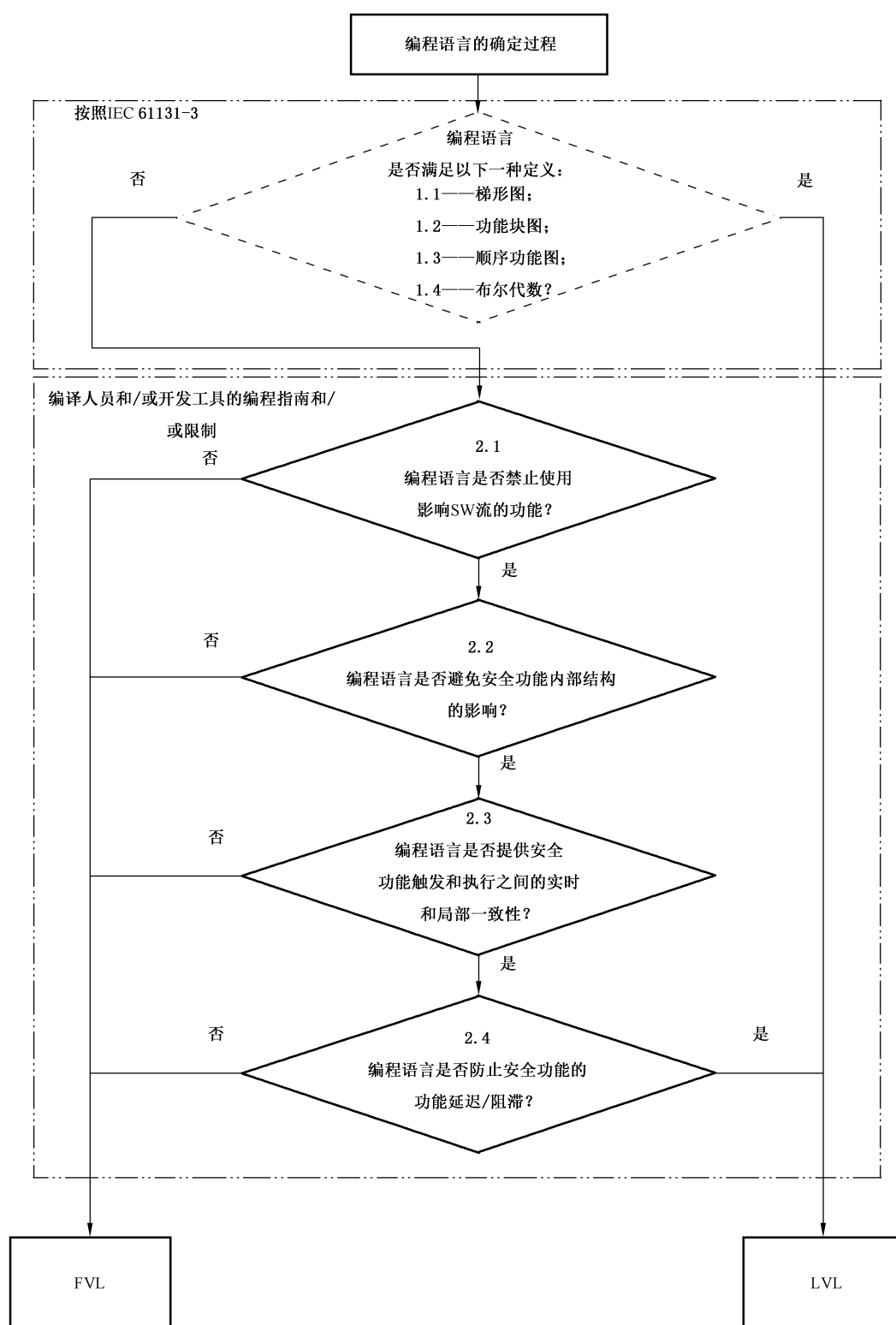


图 15 FVL 或 LVL 的决策指南

示例 1：如果使用 C 语言，即不符合 IEC 61131-3，且如果图 15 中问题 2.1～问题 2.4 任意一个回答为否，则结果为 FVL。

示例 2：如果使用了结构化文本或者有限的 C 语言子集，并在编译器和/或开发工具中加以限制，且满足 7.4 a) 和

7.4 b)的限制性编码准则,图 15 中问题 2.1~问题 2.4 所有回答为是,则结果为 LVL。

示例 3: 如果使用 Visual Basic 语言,即不符合 IEC 61131-3,且图 15 中问题 2.1~问题 2.4 任意一个回答为否,则结果为 FVL。

示例 4: 如果软件流程受编程语言影响,例如通过使用中断(图 15 中问题 2.1),则结果为 FVL。

示例 5: 如果功能块图使用了自我声明符合 IEC 61131-3 的结构化文本的功能块,且满足 7.4 a)和 7.4 b)限制,则结果为 LVL。

注 1: 附录 N 概述了使用 LVL 或 FVL 实现 SRASW 和 SRESW 的方法。

注 2: LVL 及 FVL 均能遵循技术文件,尤其是产品安全手册。通过编译器内部限制或者通过编码准则限制均能使用。

7.3 安全相关嵌入式软件(SRESW)

7.3.1 安全相关嵌入式软件(SRESW)设计

PL_r 为 a)~d)的元件的 SRESW 应采用以下基本措施:

- a) 软件安全生命周期具有验证及确认活动,例如审查及测试,见图 14 a);
- b) 编制规范及设计文件,例如软件设计规范、软件系统设计规范(SSDS)、模块设计规范(MDS)、包含注释的代码清单;
- c) 模块化和结构化的设计及编码,例如功能上的分层及限制、清晰的程序结构、接口定义、结构良好的调用图、避免中断、使用编码准则(见 GB/T 20438.7—2017 中 C.2.6.2);
- d) 控制系统性失效,例如程序顺序监控,数据通信过程中的错误控制(见 G.2);
- e) 使用基于软件的诊断措施控制随机硬件失效时,验证正确的实现,例如诊断措施的正确实现、RAM/ROM/CPU 测试、硬件测试、真实性检查;
- f) 功能测试,例如根据输入数据(有效、无效及边界值)验证正确输出数据的黑盒测试、接口兼容性、时序等;
- g) 软件修改后,适当的软件安全生命周期活动,例如影响分析;

PL_r 为 c 或 d 的元件的 SRESW 还应采用以下额外措施:

- h) 与 IEC 61508(所有部分)中如 workflow 定义、责任等具有可比性的项目管理和质量管理流程;
- i) 软件安全生命周期中所有相关活动的文件,例如审查、测试、确认及验证文件;
- j) 用于确定 SRESW 发布时所有相关配置项目及文件的配置管理,例如对代码清单、模块、设计文件、测试计划、发布控制、归档、不同版本软硬件和编程工具的系统兼容性进行版本控制;
- k) 含有安全要求的结构化规范及结构化设计;
- l) 采用合适的编程语言及计算机工具;
- m) 模块化及结构化编程、与非安全相关软件分开、受限的模块大小和充分定义的接口,例如使用设计及编码准则;
- n) 通过使用控制流分析的走查/审查进行代码验证,例如检查错误、注释质量、编码准则合规性、清晰度、可读性、完整性;
- o) 扩展功能测试,如灰盒测试、性能测试或仿真。例如通过使用未指定的输入数据、极端环境条件、满负荷、基于内部代码理解的测试。

对于类别 2 的测试通道,PL_r 降低一个性能等级。如果类别 3 或类别 4 的功能通道采用相异性技术,PL_r 降低一个性能等级。

PL_r 为 e 的元件的 SRESW 应符合 GB/T 20438.3—2017 中第 7 章,类同于 SIL3。在规范、设计及编码采用相异性技术时,对于类别 3 或类别 4 子系统的双通道,上述 PL_r 为 c 或 d 的额外措施能实现 PL_r e。

注: 采用多样化设计及编码的 SRESW,对于类别 3 或类别 4 的子系统,或者类别 2 测试通道中的元件,采取措施避

免系统性失效所涉及的工作可以减少。例如,仅通过考虑结构方面来审查软件的每一部分,而不是检查每一行的代码。附录 G 提供了执行这些方面的可用措施的指导。

7.3.2 嵌入式软件不可访问时的替代流程

当 SRP/CS 设计者无法访问嵌入式软件时,例如制造商未提供安全等级的 PLC,则 7.3.1 的 SRESW 要求无法满足。这些元件可以在下述替代条件下使用:

- 子系统限制在 PL a 或 b 且采用类别 B,类别 2 或类别 3;
- 子系统限制在类别 2 的 PL c 或类别 3 的 PL d,且需满足 CCF 的相异性要求,双通道采用相异性的技术、设计或物理原则;
- 应评估相关的硬件和 SRASW 的要求,特别是 CCF 的要求(见附录 F)。

7.4 安全相关应用软件(SRASW)

软件安全生命周期(见 7.1)同样适用于 SRASW。

采用 LVL 编写且符合以下要求的 SRASW 可以实现 PL a~PL e。若 SRASW 采用 FVL 编写,应采用 SRESW 的要求且可以实现 PL a~PL e。图 15 给出了决定采用 LVL 或 FVL 的指南。

如果一个元件中部分 SRASW(如因更改)会影响多个具有不同 PL 的安全功能,则应采用最高 PL 相关的要求。

PL_r 为 a~e 的元件的 SRASW 应采用以下基本措施。

- 具有验证及确认活动的开发生命周期,例如审查及测试。LVL 见图 14。
- 编制规范及设计文件。
- 模块化及结构化编程。
- 功能测试。
- 修改后的适当开发活动。

PL_r 为 c~e 的元件的 SRASW 采用以下有效性递增的额外措施(PL_r c 为低有效性,PL_r d 为中有效性,PL_r e 为高有效性)。

对于类别 2 结构的测试通道,PL_r 降低一个性能等级。如果类别 3 或类别 4 的功能通道采用相异性技术,PL_r 降低一个性能等级。

- a) 软件设计规范应经过审查(见附录 J)并提供给生命周期中涉及的人员,且应包含以下描述:
 - 1) 包含 PL_r 的安全功能及关联的操作模式;
 - 2) 性能参数,例如响应时间;
 - 3) 通信接口;
 - 4) 检测及控制硬件失效以达到所需的 DC 及故障响应。
- b) 工具、库、语言的选择。
 - 1) 工具应适合于应用。应采用能检测导致系统性错误情况(如数据类型不匹配、模糊的动态内存分配、不充分的接口调用、递归、指针运算)的技术特性。检查应主要在编译时间内执行而非仅在运行时间内执行。工具宜执行语言子集及编码准则,或者至少对使用它们的开发者进行监督或指导。若使用一个元件及其工具实现 PL e,该工具应符合适用的元件标准。如果使用两个具有不同工具的不同元件,采用以往项目的成功操作经验就能实现。
 - 2) 只要合理可行,宜使用经确认的功能块库——无论是由工具制造商提供的安全相关功能块库(强烈推荐用于 PL e),还是经应用验证且符合本文件的特殊功能块库。
 - 3) 宜使用适合于模块化方法的合理 LVL 子集(见 7.2.1),如符合 IEC 61131-3 的语言子集。
- c) 软件设计应具有以下特点:
 - 1) 采用半形式化方法描述数据及控制流,如状态图或程序流程图;

- 2) 模块化及结构化编程,主要应用经确认的安全相关功能块库或其他模块化结构衍生的功能块,以实现代码易读性及可测试性;
- 3) 限制功能块代码规模;
- 4) 功能块内代码执行只能有一个入口和一个出口;
- 5) 三阶段模型架构:输入⇒处理⇒输出(见图 16 及附录 J);
- 6) 仅在一个程序位置分配安全输出;
- 7) 使用检测和控制硬件失效的技术,并在触发进入安全状态的输入、处理和输出块内进行防御性编程技术。

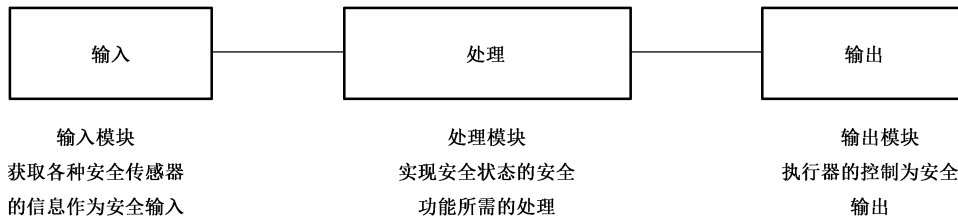


图 16 软件的一般架构模型

- d) 当 SRASW 和非 SRASW 组合在同一个元件内：
 - 1) SRASW 和非 SRASW 应在不同的具有明确定义接口的功能块中编码;
 - 2) 不应存在可能导致安全相关信号完整性降级的非安全相关数据和安全相关数据的逻辑组合,如将安全相关及非安全相关信号采用逻辑“或”组合的结果控制安全相关信号。
- e) 软件实现/编码：
 - 1) 代码应具有可读性、可理解性和可测试性,因此,宜使用符号变量(而不是显式的硬件地址);
 - 2) 应使用合理的或公认的编码准则(见附录 J);
 - 3) 宜使用应用层(防御性编程)提供的数据完整性和真实性检查(如范围检查);
 - 4) 代码宜通过仿真测试;
 - 5) 对于 PL d 或 PL e,宜通过控制流分析和数据流分析进行验证。
- f) 测试：
 - 1) 适当的确认方法是对功能行为和性能标准(如时序性能)进行黑盒测试;
 - 2) 对于 PL d 或 PL e,推荐使用边界值分析执行测试案例;
 - 3) 测试计划宜包含具有完成指标及所需工具的测试案例;
 - 4) I/O 测试应确保安全相关信号在 SRASW 内被正确使用。
- g) 文件：
 - 1) 所有的生命周期和修改活动都应被记录;
 - 2) 文件应完整、可用、可读及可理解;
 - 3) 源文本中的代码文件应包含带有法人实体名称的模块标题、功能和 I/O 描述、所用库功能块的版本以及网络/语句和声明行的充分注释。
- h) 验证：

验证应通过审查、检查、走查或其他适当的活动进行。

注：验证仅用于特定应用的代码,不用于经确认的库功能。
- i) 配置管理：

强烈推荐建立流程和数据备份,以确定和归档与特定 SRASW 版本相关的文件、软件模块、验证/确认结果和工具配置。

j) 修改:

对 SRASW 进行修改之前,应进行影响分析以确保与软件设计的一致性。修改后应进行适当的生命周期活动。应提供手段以防止对 SRASW 进行未经授权的修改,并应记录修改历史。

8 已达到性能等级的验证

对于单个安全功能,相关 SRP/CS 的 PL 应高于或等于 5.3 和 6.1.1 中确定的所需性能等级(PL_r)。否则需要采用图 4 中描述的迭代过程。

作为安全功能一部分,不同子系统的 PL 应高于或等于该安全功能所需性能等级(PL_r)(见 5.3 和 6.1.1)。

9 人类工效学方面的设计

操作者与 SRP/CS 之间的接口的设计和实现应最大限度地减少机器所有预定使用和可合理预见的误用过程中,由于忽视人类工效学原则而造成暴露于危险。

GB/T 15706—2012 中 6.2.8 给出了人类工效学原则的安全要求。

注:人类工效学原则旨在提高控制系统的易用性,以消除废弃动机或避免机器意外误用。人类工效学的指南见 ISO/TR 22100-3 和 ISO 9241—2010。

10 确认

10.1 确认原则

10.1.1 一般要求

确认过程的目的是确定 SRP/CS 满足按第 5 章和第 7 章要求创建的总体 SRS。

图 17 给出了确认过程概览。确认包括分析确认(见 10.3),以及按照确认计划在可预见的条件下进行的测试(见 10.4)。

注 1: SRP/CS 的确认保证安全功能实现预定的风险减小,并作为机械整体确认过程的一部分。

确认活动应保证确认计划中每个已被识别的设计活动的完整性和正确性。

SRP/CS 的确认包括对 SRP/CS 的检查(例如通过分析)和测试,以确保其达到 SRS 中规定的要求(根据第 5 章)。

确认应证明 SRP/CS 符合要求,特别是:

- a) SRS 提出的,由该部件所提供的安全功能的规定功能要求;
- b) 6.1.1 规定的 PL 的要求:
 - 1) 规定的类别要求;
 - 2) 控制和避免系统性失效(系统完整性)的措施;
 - 3) 软件的要求,如适用;
 - 4) 在预期环境条件下执行安全功能的能力;
- c) 操作界面的人类工效学设计、交互和定位。

确认过程宜由独立于 SRP/CS 设计的人员进行。

注 2: 独立人员是指不参与 SRP/CS 设计的人员,并不一定需要第三方。

分析宜尽可能早地启动,与设计过程并行。部分分析工作有必要推迟到设计完成后进行。

注 3: 在相对容易的时候尽早解决问题,即在“安全功能的设计和技术实现”和“评估 PL”这两步之间。

由于控制系统的规模、复杂性或者与(机器的)控制系统集成的效果,在必要时,宜作如下专门安排:

- 在集成前单独对子系统进行确认,包括模拟相应的输入和输出信号;
- 确认控制系统用于机器的情况下 SRP/CS 与控制系统其余部分的集成效果。

分析和测试之间的平衡取决于 SRP/CS 所采用的技术和所需的性能等级(PL_r)。对于类别 2、类别 3 和类别 4,安全功能的确认还应包括采用适当的故障插入测试,证明故障反应会被所执行的诊断功能触发。

图 17 中的“设计更改”是设计过程中的一部分。如果无法成功完成确认,则有必要改变设计。然后,还应对 SRP/CS 修改的部件重新进行确认。应重复此过程,直到每个安全功能的 SRP/CS 均已成功完成确认。

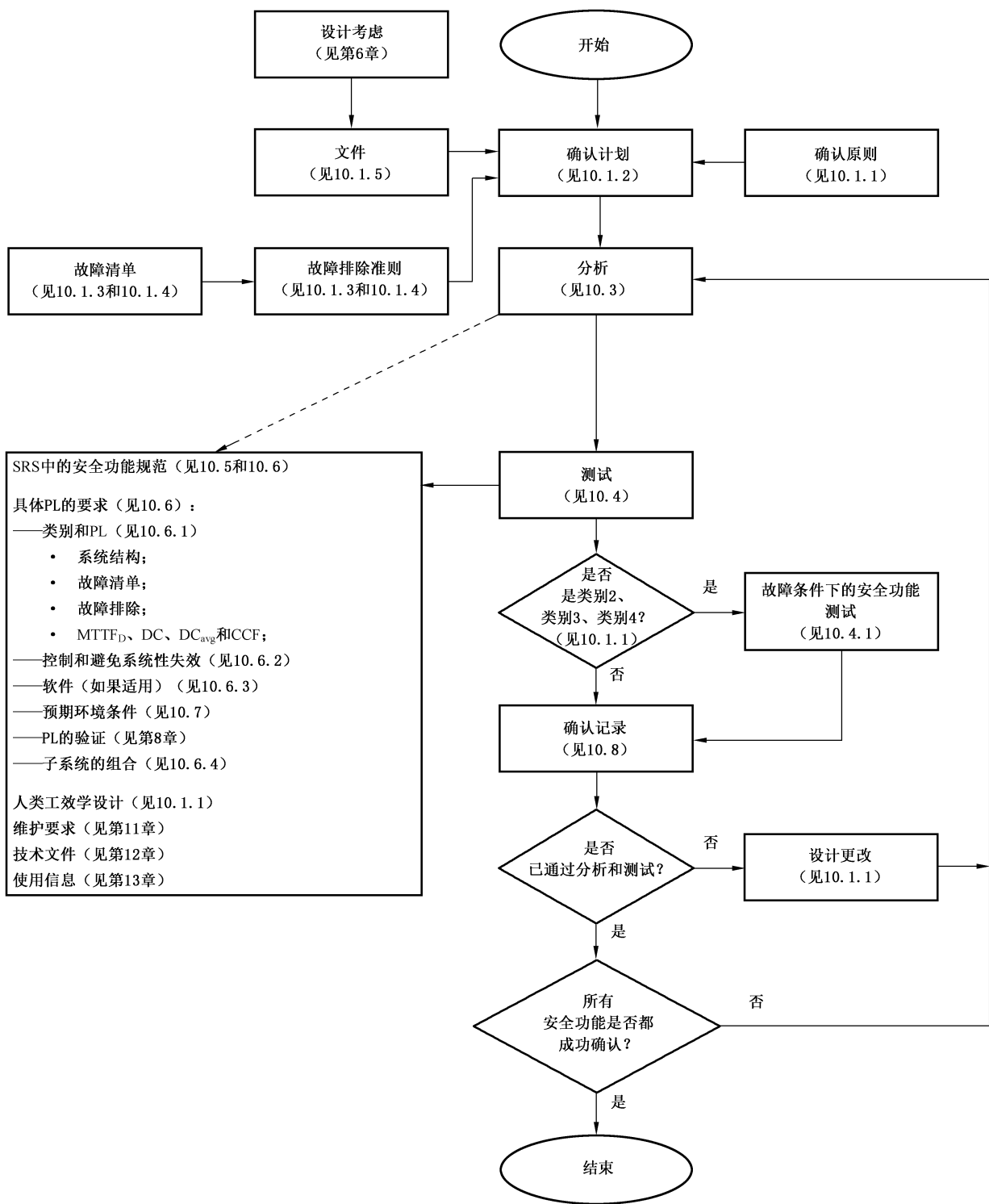


图 17 确认程序概览

10.1.2 确认计划

确认计划应识别和描述实施确认过程的要求,并应提供给确认过程相关的人员和单位。确认计划还应识别用于确认规定安全功能的方法。适当时,应识别:

- a) 技术规范文件；
- b) 测试过程中的操作和环境条件；
- c) 需要进行的分析和测试；
- d) 适用的测试标准；
- e) 确认过程各步骤的负责人或单位。

10.1.3 一般故障清单

确认包括考虑 SRP/CS 对所有要考虑的故障的行为。故障考虑的基础是 GB/T 16855.2—2015 中附录 A～附录 D 根据经验以表格形式给出的故障清单,其内容包括:

- 包含的元件/组件,如导线/电缆;
- 考虑的故障,如导体间短路;
- 允许的故障排除,考虑环境、操作和应用的因素;
- 备注栏,给出故障排除的理由。

故障清单仅考虑永久性故障。

10.1.4 特殊故障清单

如有必要,应创建一个特殊的产品相关故障清单,作为子系统或子系统组件确认过程的参考文件。此清单能够基于 GB/T 16855.2—2015 附录中的一般故障清单或通过产品观察发现的(重复出现的)故障。

对于基于一般故障清单的特定产品故障清单,应规定以下内容:

- a) 一般故障清单中列出的故障;
- b) 一般故障清单没有列出的其他相关故障(例如,共因失效);
- c) 一般故障清单中列出的,并且在满足一般故障清单中给出的准则的前提下可排除的故障;
- d) 特殊情况下,给出了排除的理由和原理的其他故障。

对于不是基于一般故障清单的特殊产品故障清单,设计者应给出故障排除的原理。

10.1.5 确认信息

确认所需要的信息因随着所采用的技术、待证实的类别和 PL、SRS 以及 SRP/CS 对风险减小的作用而异。确认中应包括含有以下足够信息的文件,以证明 SRP/CS 执行规定安全功能实现所需的 PL 和类别:

- a) SRS,包括每个安全功能所需的特性,例如:响应时间(根据 GB/T 19876—2012)、操作模式、PL、SRP/CS 子系统之间的接口、必要的各 SRP/CS 子系统类别的特性;
- b) 图样和技术文件,例如,机械、液压和气动部件、印刷线路板、装配面板、内部布线、外壳、材料和安装支架的图样和技术文件;
- c) 框图,并在需要澄清处提供模块的功能描述;
- d) 电路图,包括接口/连接;
- e) 澄清时需要的电路图的功能描述;
- f) 开关部件的时序图,安全相关的信号;
- g) 已确认元件相关特性的描述;
- h) 对于在 g)中没有列出的 SRP/CS,列出名称、额定值、允差、相关的工作应力、型号规格、失效率数据、元件制造商以及其他安全相关数据的元件清单;

注 1: 能够从 VDMA 66413 库提供数据。

- i) 符合 10.1.3 和 10.1.4 的所有相关故障的分析报告,如 GB/T 16855.2—2015 中附录 A～附录

D 的表格中列出的故障,包括所有已排除故障的理由;

j) 被加工材料影响的分析报告;

k) 使用信息、维护要求,例如安装和操作手册/说明手册。

如果软件与安全功能相关,则软件的文件应包括:

——清楚明确的技术规范;

——软件的设计能实现所需的 PL 的证据(见 10.6.3);

——用于证明实现了所需的 PL 而进行的测试细节(尤其是测试报告)。

应提供如何确定 PL 和 PFH 的信息,可量化因素的文件应包括:

——安全相关框图和符合 6.1.3.2 的指定架构;

—— $MTTF_D$, DC_{avg} 和 CCF 的确定;

——类别的确定。

注 2: 安全相关框图见附录 B。

需要提供防止 SRP/CS 系统失效措施的文件信息。

需要提供描述如何组合若干子系统来实现所需的 PL 的信息。

注 3: 若可行,允许对现有文件进行清晰、可追溯的引用。

10.2 安全要求规范(SRS)的确认

在确认提供安全功能的 SRP/CS 或子系统组合的设计之前,应先验证安全功能的安全要求规范,以确保其与预定用途的一致性和完整性(见 5.4)。

为了确认这些规范,应采用相应措施检测系统性失效(错误、疏漏或不一致)。

能够通过审查和检查 SRS 来完成确认,特别要考虑:

——预定应用的要求;

——风险评估;

——操作和环境条件;

——可合理预见的误用。

10.3 分析确认

10.3.1 一般要求

应通过分析对 SRP/CS 进行确认,分析的输入包括:

——安全功能及其特征,和符合 5.2 规定的安全完整性;

——符合 6.1.3.2 的系统结构(如指定架构);

——根据 6.1.4、6.1.5 和 6.1.6,通过确认与系统计算中使用的值的选择相关的假设和数据,确定的可量化指标($MTTF_D$ 、 DC_{avg} 和 CCF);

——影响系统性能的不可量化的定性指标(如适用,包括软件);

——确定性论据;

——故障清单;

——故障排除准则。

注: 确定性论据是基于定性指标(如制造质量、使用经验)的论据。这一方法取决于具体应用,确定性论据受到各种因素的影响。确定性论据与其他证据的区别在于,确定性论据表明所需的系统特征是根据系统模型进行逻辑推导得出的。此类论据能建立在简单易懂的概念基础上。

10.3.2 分析方法

分析能用如下两种基本方法。

- a) 自上而下(演绎)的方法,适合于确定能够导致顶事件的起始事件,并通过起始事件的概率计算顶事件的概率。该方法也能用于研究已知的多重故障的因果关系。

示例 1: FTA(见 IEC 61025)和 ETA(见 IEC 62502)。

- b) 自下而上(归纳)的方法,适合于研究已识别的单一故障的因果关系。

示例 2: FMEA(见 IEC 60812)和失效模式、影响与危害性分析(FMECA)(见 IEC 60812)。

10.4 测试确认

10.4.1 一般要求

确认应包含测试。对于类别 B 和类别 1,无需故障测试,可通过功能测试进行分析。

测试确认的计划和实施应遵循逻辑方法,尤其是:

- a) 在开始测试之前应制定测试计划,其内容应包括:

- 1) 测试规范;
- 2) 需要的符合性测试结果;
- 3) 如适用,测试的时间顺序。

- b) 应形成测试记录,其内容包括:

- 1) 测试人员的姓名;
- 2) 环境条件;
- 3) 测试程序和所使用设备;
- 4) 测试日期;
- 5) 测试结果。

- c) 应将测试记录和测试计划进行对比,以确保实现规定的功能和性能目标。

测试样品运行配置应尽可能接近最终运行配置,即连接上所有的外围装置和外罩。

测试可手动完成,也可自动完成,例如,通过计算机。

实际应用时,应向 SRP/CS 施加各种组合的输入信号完成安全功能的测试确认。应将输出端的最终响应与相应规定的输出结果进行比较。

宜系统地向控制系统和机器施加这些输入组合信号,例如:电源接通、启动、操作、方向改变、重新启动。为了观察 SRP/CS 在异常或不正常的情况下的响应,宜扩大输入数据的范围。此类输入数据的组合宜考虑可预见的误操作。

当分析确认没有结论时,应通过测试来完成确认。测试是对分析的补充,并且通常是必要的。

10.4.2 测量精度

通过测试进行确认的过程中,测量精度应与测试相适应。一般情况下,应保证温度的测量精度在 $\pm 5\text{ K}$ 以内,并保证以下参数的测量精度在 $\pm 5\%$ 以内:

- a) 时间;
- b) 压力;
- c) 力;
- d) 电气参数;
- e) 相对湿度;
- f) 线性。

如果与上述测量精度有偏差,应说明理由。

10.4.3 测试附加要求

如果对 SRP/CS 的要求比本文件规定的要求更严格,则应扩大测试范围,以包含这些更严格的

要求。

注：根据风险评估，如果控制系统不得不经受特别恶劣的工作条件时，如野蛮操作、湿度影响、羟基化反应、环境温度变化、化学试剂的影响、腐蚀、因靠近发射装置造成的高强度电磁场，则可能采用更严格的要求。

10.4.4 测试样品数量

除非另有规定，否则子系统的测试应采用单个产品样品进行。

不应修改测试过程中的子系统。

某些测试可能使某些元件的性能发生永久改变。如果元件的永久性改变使得安全相关部件无法满足后续测试的要求时，应采用新的样品进行后续测试。

如果某一特定测试为破坏性测试，且通过对 SRP/CS 的部件进行单独测试可得到相同的结果，则为了得到测试结果，可采用该 SRP/CS 部件的样品来代替整个 SRP/CS 进行测试。只有分析表明，对 SRP/CS 部件的测试已足以证明执行安全功能的整个 SRP/CS 的安全完整性，才应使用这种方法。

10.4.5 测试方法

根据应用，应使用不同的测试方法来确认 SRP/CS。在某些应用中，可能有必要把相连的 SRP/CS 分为几个功能组，并对这些功能组及其接口进行故障模拟测试。将故障插入到系统的准确时刻可能非常关键。应通过分析确定故障插入的最坏影响，并在此关键时刻插入故障。常见的测试方法如下。

- a) 发生故障时控制系统行为的模拟，例如通过硬件和/或软件模拟。
- b) 故障的软件模拟。
- c) 在机器所有操作模式下对安全功能进行功能测试，以确定其是否满足规定特征（见第 5 章）。功能测试应确保在整个范围内实现了所有安全相关的输出，并按照技术规范的要求响应安全相关输入。测试案例通常来源于技术规范，但某些案例也有可能来源于对原理或软件的分析。
- d) 扩展功能测试，以检查是否存在来自输入端的可预见的异常信号或信号组合，包括动力中断和恢复，以及不正确的操作。
- e) 在实际电路上进行故障插入测试，并对实际元件进行故障触发测试，尤其是失效分析结果存疑的系统部件。
- f) 对产品样品进行故障插入测试。
- g) 对硬件模型进行故障插入测试。
- h) 子系统失效测试（如动力源）。

10.5 安全功能的确认

安全功能的确认应证明提供安全功能的 SRP/CS 或子系统组合符合所规定的特征。

应采用以下列出的相应措施确认安全功能的规定特征：

- a) 原理图功能分析、软件审查（见 10.6.3）；

注：如果机器的安全功能很复杂或数量众多，分析能够减少所需功能测试的数量。

- b) 模拟；
- c) 检查安装在机器上的硬件元件，以及相关软件的详细资料，以确定其与文件的一致性（如制造商、类型、版本）；
- d) 功能测试（见 10.4.5）；
- e) 检查 SRP/CS 操作界面是否符合人类工效学原则。

10.6 SRP/CS 安全完整性的确认

10.6.1 子系统的确认

SRP/CS 的每个子系统的安全完整性应按照表 10 根据所使用的类别确定的要求进行确认。

表 10 类别确认的基本要求

要求	类别				
	B	1	2	3	4
基本安全原则	✓	✓	✓	✓	✓
预期工作应力	✓	✓	✓	✓	✓
被加工材料的影响	✓	✓	✓	✓	✓
受其他相关外部影响时的性能	✓	✓	✓	✓	✓
经验证的元件	—	✓	—	—	—
不基于 $MTTF_D$ 确定 PL 的经验证的元件	—	✓	✓	✓	✓
经验证的安全原则	—	✓	✓	✓	✓
各通道 $MTTF_D$	✓	✓	✓	✓	✓
可认知故障及相关诊断措施,包括故障反应	—	—	✓	✓	✓
检查间隔,如有规定	—	—	✓	✓	✓
DC_{avg}	—	—	✓	✓	✓
已识别的 CCF 及预防方法	—	—	✓	✓	✓
故障排除的理由	✓	✓	✓	✓	✓
每种故障条件下如何保持安全功能	—	—	—	✓	✓
每种组合故障条件下如何保持安全功能	—	—	—	—	✓
防止系统性失效的措施	✓	✓	✓	✓	✓
防止软件故障的措施	✓	—	✓	✓	✓
说明: ✓ ——需要; — ——不需要。 注:类别是指 6.1.3.2 中给出的类别。					

此外,SRP/CS 的每个子系统的安全完整性应通过确定以下内容进行确认:

- 危险的随机硬件失效率;
- 系统完整性(见附录 G、第 7 章、CCF)。

在这种情况下, $MTTF_D$ (包括 B_{10D} 、 T_{10D} 和 n_{op})、 DC_{avg} 和 CCF 的确认通常通过分析和目视检查来完成。

当故障排除声明表明特殊元件不影响通道 $MTTF_D$ 值时,则应检查故障排除的合理性。

注:故障排除意味着元件的 $MTTF_D$ 无限大;因此,该元件将不影响通道 $MTTF_D$ 的计算。

应检查子系统各通道 $MTTF_D$ 的计算是否正确,包括对不同冗余通道采用对称公式(见附录 D)计算得出的 $MTTF_D$ 。应确保在采用对称公式计算之前,单个通道的 $MTTF_D$ 已严格限制在不超过 100 年(对于类别 4,限制在不超过 2 500 年)。

应检查元件(子系统组件)和/或逻辑模块 DC 值的真实性(例如:是否违背附录 E 给出的措施)。应在典型的使用环境条件下,通过测试来确认是否正确实施检查和诊断(硬件和软件),包括相应的故障响应。

应确认是否采用了足够的措施来防止共因失效(例如,是否符合附录 F 的要求)。典型确认措施是

在环境条件下进行的静态硬件分析和功能性测试。

通常,对于电子元件 $MTTF_D$ 的计算,环境温度取 $40\text{ }^{\circ}\text{C}$ 作为基准。确认过程中,确保满足基准环境和功能条件(特别是温度)对于 $MTTF_D$ 非常重要。当设备或元件的工作温度明显高于(如超过 $10\text{ }^{\circ}\text{C}$)规定的 $40\text{ }^{\circ}\text{C}$ 时,则有必要采用较高环境温度的 $MTTF_D$ 值。

10.6.2 防止系统性失效措施的确认

防止系统性失效措施的确认通常能采用以下方式:

- a) 检查设计文件,以确定:
 - 1) 是否应用基本的和经验证的安全原则(见 GB/T 16855.2—2015 中附录 A~附录 D);
 - 2) 是否根据附录 G 的要求采取进一步措施避免系统性失效;
 - 3) 是否采取进一步措施控制系统性失效,如硬件相异性、防修改保护或失效断言编程;
- b) 失效分析(如 FMEA);
- c) 故障插入测试/故障触发;
- d) 如果使用了数据通信,则进行检查和测试;
- e) 检查质量管理体系是否能够在生产过程中避免系统性失效。

注:设计和集成阶段造成的错误(如对安全功能特征错误的理解、逻辑设计错误、硬件装配错误、软件代码输入错误等)可能导致系统性故障。部分错误在设计阶段暴露,其余错误或在确认过程暴露,或未被发现。此外,确认过程也可能犯错(如没有检查到某些特性)。

10.6.3 安全相关软件的确认

软件的确认应包含:

- 软件在目标硬件上执行时规定的功能动作和性能准则(如时序性能);
- 验证采用软件措施是否足以实现安全功能规定的 PL_r ;
- 通过检查记录证据,验证软件开发过程中为避免系统性软件故障所采取的保护措施和行动是否已被采用。

首先应检查是否对安全相关软件的技术规范和设计文件进行文件编制,并审查这些文件的完整性,且不存在错误理解、疏漏或矛盾。

一般来说,软件能看作是“黑盒”或“灰盒”(见第 7 章),并分别用黑盒或灰盒测试进行确认。

注 1:小型程序能利用软件的文件(控制流程图、模块或块的源代码、I/O 或变量分配表、对照表)通过控制流程或程序的审查或走查进行分析。

注 2:黑盒测试旨在检查真实功能条件下的动态动作,暴露不满足功能规范的失效,并评估效用和鲁棒性。灰盒测试与黑盒测试相似,但额外监控软件模块内部的相关测试参数。

根据 PL_r ,测试宜包括:

- 功能动作和性能(如时序性能)的黑盒或灰盒测试;
- 基于限值分析的附加延伸测试项目;推荐用于 PL_d 或 PL_e ;
- I/O 测试,以确保安全相关输入和输出信号的正确使用;
- 模拟事先通过分析方法确定的故障以及预期响应的测试项目,其目的是评价基于软件的失效控制措施是否充分。

注 3:示例见 N.2。

已确认过的单独软件功能无需再次确认,但是,如果针对具体项目而将多个此类安全功能块组合在一起时,则应确认最终的总体安全功能。

应检查针对软件实施、配置和变更管理所采取的符合第 7 章要求的措施是否得到正确实施,这些措施取决于需要实现的 PL 。

如果其后对安全相关软件进行了修改,应在相应的范围内进行再次确认。

10.6.4 子系统组合的确认

如果安全功能由两个或两个以上的子系统实现,则应通过分析和测试对该组合进行确认,确保该组合满足设计规定的安全完整性。可以考虑采用已有子系统的确认记录结果。应按以下步骤进行确认:

- 检查描述总体安全功能的设计文件;
- 检查根据每个单独子系统确定的子系统组合总体 PL(按照 6.2 要求)是否正确;
- 接口特性的考虑,如电压、电流、压力、信息的数据格式、信号电平;
- 与组合/集成相关的失效分析,如通过 FMEA;
- 子系统组合的测试;
- 针对冗余系统,组合/集成相关的故障插入测试。

10.6.5 安全完整性的总体确认

应进行以下步骤:

- 检查/验证根据子系统的 PFH 和 PL/SIL 评估得到的 PL 是否正确(见 6.2);
- 检查/验证根据类别、 DC_{avg} 、 $MTTF_D$ 、CCF 和防止系统性失效的措施评估得到的 PL 是否正确;
- 检查/验证 SRP/CS 实现的 PL 是否满足机器 SRS 中的 PL_r , 即: $PL \geq PL_r$ 。

10.7 环境要求的确认

设计中规定的 SRP/CS 性能应在控制系统规定的环境条件下进行确认。

确认应通过分析和测试来完成。分析和测试的范围取决于安全相关部件及其安装所在的系统、所采用的技术,以及需要确认的环境条件。采用系统或其元件的运行可靠性数据,或者确定是否符合相应的环境标准(如防水、防振),可能有助于确认过程。

适当时,确认应针对:

- 因冲击、振动、污染物进入产生的预期机械应力;
- 机械耐久性;
- 电气额定值以及动力源;
- 气候条件(温度和湿度);
- 电磁兼容性(抗扰度)。

当需要通过测试来确定是否符合环境要求时,则应遵循相关标准规定的,以及具体应用要求的程序进行。

通过测试完成确认之后,安全功能应仍然符合安全要求的技术规范,或者 SRP/CS 应提供安全状态的输出信号。

10.8 确认记录

应记录通过分析和测试进行的确认。记录应反映各项安全要求的确认过程。如果以前的确认记录有效,也可以引用。

对于确认过程中未通过确认的安全相关部件,确认记录应描述哪些组件没有通过分析/测试确认。应确保在修改后所有安全相关部件均已重新确认。

10.9 维护要求的确认

确认过程应证明已满足了维护要求。

维护要求的确认应包括：

- a) 使用信息的审查,以确认：
 - 1) 维护手册的内容是否完整[包括程序、需要的工具、检查的频率、更换易损元件的时间间隔(T_{10D})等],且容易理解；
 - 2) 适当时,是否存在只能由熟练维护人员完成维护的要求；
- b) 检查是否采用了便于维护的措施(如提供诊断工具辅助故障查找和修理)。

此外,适用时,还应包括以下措施：

- 防止维护过程中发生错误的措施(如通过真实性检查检测错误的输入数据)；
- 防止篡改的措施(如设置密码防止未经授权人员进入程序)。

11 SRP/CS 的可维护性

为了保持 SRP/CS 的规定性能,可能需要进行预防性或修复性维护。

注：超过规定的使用寿命或测试间隔,可能导致安全性能恶化甚至导致危险状况。

SRP/CS 的维护应考虑以下因素：

- 易接近性,考虑环境和人体尺寸,包括所用工作服和工具的尺寸；
- 易操作性,考虑人类工效学能力；
- 尽可能限制专用工具和设备的数量；
- 需要维护的指示(如振动增加),理想情况下自动生成警告信号(如寿命记录、自检、过程参数监测)；
- 要求的照明水平。

12 技术文件

根据本文件设计 SRP/CS 时,应至少对以下与安全相关部件有关的信息进行归档,以供内部使用：

- a) SRS(见 5.2.1)；
- b) 安全相关部件确切的起始点和终止点；
- c) 子系统分解(见 5.2.2),如适用；
- d) 环境条件(如 EMI 抗扰度、温度、振动)；
- e) 实现的性能等级和 PFH 值；
- f) 所选的类别(可不适用于先前验证的子系统)；
- g) 与可靠性有关的参数($MTTF_D$ 、DC、CCF 和 T_{10D})和任务时间；
- h) 防止系统性失效的措施；
- i) 所使用的技术；
- j) 考虑所有与安全有关的故障；
- k) 故障排除的理由(见 6.1.10.3 和 GB/T 16855.2—2015 的所有附录)；
- l) 软件文件,如适用；
- m) 防止可合理预见的误用的措施；
- n) 安全相关框图；
- o) 相关设计文件、测试、验证和确认记录,如适用。

注：通常,设计文档预期用于制造商内部,或在分包商(如外部系统设计师、认证机构)与制造商之间交换技术信息。

设计文件也是满足法律文件要求所必需的。设计文件无需分发给机器用户,但其部分内容与充分的使用信息的准备相关(见第 13 章)。

13 使用信息

13.1 概述

SRP/CS 的使用信息应符合 GB/T 42598—2023 或 IEC/IEEE 82079-1:2019, 包括预期目标群体的相关说明。本信息应涵盖涉及 SRP/CS 的机器的生命周期各个阶段。

13.2 SRP/CS 集成的信息

应向集成者提供正确集成 SRP/CS 的重要信息。这应包括, 但不限于下列信息。

- a) 所选 SRP/CS 安全相关部件的限制(如环境条件, 如 EMI 抗扰度、温度、振动)和适当的信息, 以保证故障排除持续合理。如改进、维护和维修的信息。
- b) SRP/CS 与保护装置的接口的明确阐述。
- c) 相关的响应时间(根据 GB/T 19876—2012)。
- d) 使用限制(如需求频率)。
- e) 指示和警报。
- f) 安全功能的默停和暂停。
- g) 控制模式和复位。
- h) 维护(见第 11 章)。
- i) 维护检查清单。
- j) 如何获得和更换 SRP/CS 的部件。
- k) 方便、安全的故障查找方式。
- l) 相关的测试间隔。
- m) 任务时间。

注: 集成者可以为制造商、集成商、工程公司或用户。

应提供各安全功能的类别和性能等级的如下具体信息(见 5.3):

- 构成 SRP/CS 的子系统类别(可能不适用于先前验证的子系统);
- 性能等级: a、b、c、d 或 e;
- 与安全功能相关的 SRP/CS 或每个相关子系统的 PFH。

13.3 用户信息

应向机器的用户(如操作者)提供正确使用 SRP/CS 的重要信息。

其内容包括但不限于 13.1 和 13.2 中的相关方面。还应提供安全功能测试的相关信息。SRP/CS 的设计者应提供用于描述 SRP/CS 必要维护任务的信息。

维护信息可能包括任务和应用, 例如:

- a) 设置;
- b) 示教/编程;
- c) 工艺/工具更换;
- d) 清洁;
- e) 预防性维护;
- f) 修复性维护;
- g) 故障排除/故障查找;
- h) 安全功能检查的性质和频率;
- i) 说明哪些维护操作要求技术知识和/或特殊技能, 宜仅由合格人员(如维护人员、专家)执行;

- j) 说明哪些维护操作(例如更换零件)不要求特定技能,可由机器用户(例如操作者)执行,宜提醒维护人员注意哪些零件对安全至关重要,只能更换为原始零件或满足相同安全要求的零件;
- k) 控制危险能量(手动措施/其他手段)的指南、标志和装置;
- l) 使维护人员能够执行其任务(特别是隔离故障条件的故障查找任务)的图纸/图表;
- m) 在任务时间周期结束时或之前更换部件的相关信息(气动、机械和机电部件见 C.4.2)。

注 1: 更多信息见 GB/T 42598—2023 和 IEC 60204-1:2016+AMD1:2021 中的 17.2 f)。

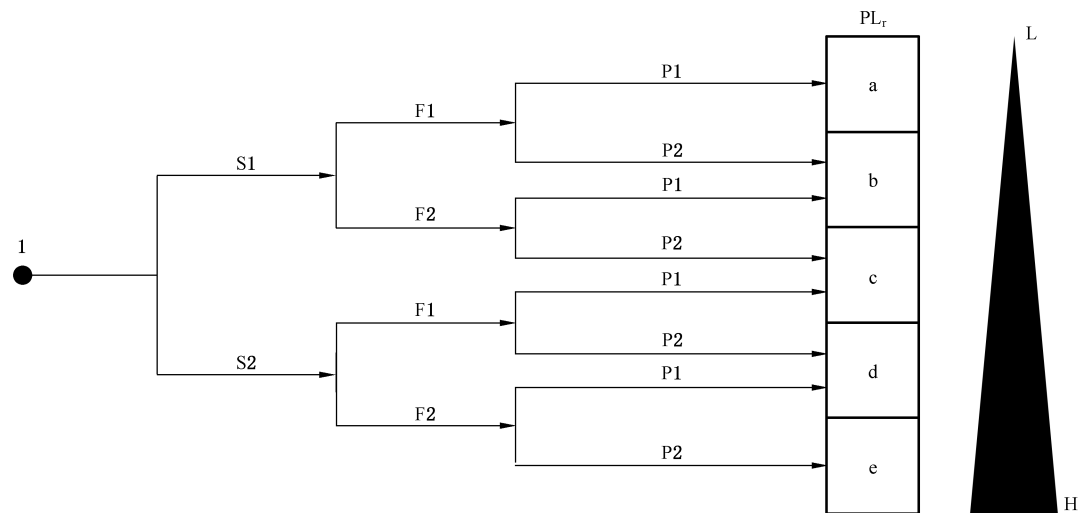
如有任何维护活动需要维修或修改 SRP/CS,则应重新进行包括功能测试的确认。

注 2: 相关的重新确认活动取决于原始元件和替换元件之间的差异程度。

附 录 A
(资料性)
所需性能等级(PL_r)确定指南

A.1 原则

图 A.1 给出了确定安全相关 PL_r 的指南。每种安全功能宜都考虑本图。



标引序号说明：

- 1 ——评估安全功能对风险减小的作用的起始点；
- L ——对风险减小的作用小；
- H ——对风险减小的作用大；
- PL_r——所需性能等级。

风险参数：

- S ——伤害的严重度；
- S1 ——轻微(通常是可恢复的伤害)；
- S2 ——严重(通常是不可恢复的伤害或死亡)；
- F ——暴露于危险的频率和/或持续时间；
- F1 ——很少~不常和/或暴露时间短；
- F2 ——频繁~连续和/或暴露时间长；
- P ——避免危险或限制伤害的可能性；
- P1 ——在特定条件下可能；
- P2 ——几乎不可能。

图 A.1 用于确定安全功能 PL_r 的风险图

A.2 PL_r 的选择

附录 A 是关于 SRP/CS 对风险减小的作用。本条款给出的方法建立在风险参数估计的基础上(与其他任何风险估计方法一样,本质上具有一定的主观性)。因此,该方法仅作为设计者和标准制定者估计 SRP/CS 执行的每种安全功能 PL_r 的指南。

这种 PL_r 估计方法不是强制性的。这是一种常规方法,假定发生危险事件的概率为 100%。如果

发生概率能够评估为低(此结论宜有依据并记录),则可能降低一个性能等级,否则发生概率按 100% 计算。在估计 PL_r 时可能适当使用其他特定类型机器的风险估计方法,并宜考虑处理类似机器/风险的成功经验。因此,C 类标准要求的 PL 可能偏离图 A.1 中给出的常规方法得出的结果。

图 A.1 是基于提供预期安全功能之前的情形(见 ISO/TR 22100-2:2013)。在确定预期安全功能的 PL_r 时,考虑了通过其他独立于控制系统的技术措施(例如:机械式防护装置)或附加安全功能实现风险减小。这种情况下,实施这些措施后再选取图 A.1 中的起始点(见图 3)。

确定 PL_r 采用的参数为:

- 伤害的严重程度(S);
- 暴露于危险的频率和/或时间(F);
- 避免或限制伤害的可能性(P)。

这些参数组合后能得出如图 A.1 所示的对风险减小作用由低到高的分级。

A.3 选择风险估计参数 S、F 和 P 的指南

A.3.1 伤害严重度 S1 和 S2

估计风险时,只考虑轻微伤害或严重伤害。

决定取 S1 还是 S2 时,宜考虑事故的通常后果以及正常的康复过程。例如:无并发症的擦伤和/或划伤可定为 S1,而断肢或死亡可定为 S2。

注:严重或轻微伤害评估指南见 ISO/TR 14121-2。

A.3.2 暴露于危险的频率和/或时间 F1 和 F2

参数 F1 或 F2 能选用的有效时长通常无法规定。但是,以下说明可能对决策过程有帮助。

如果人员频繁或连续暴露于危险,宜选 F2。这与是否为同一人或不同人连续暴露于危险无关,例如:使用电梯。频率参数宜根据接近危险的频率和持续时间来选择。

如果设计者已知对安全功能的需求,则能选择该需求对应的频率和持续时间,而不是接近危险的频率和持续时间。本文件中,假定对安全功能需求的频率大于 1 次/年。

暴露于危险的持续时间宜根据能预见的与设备使用总时间有关的平均值来估计。例如:循环运行期间,为了进给和移动工件,需要经常接近机器的刀具,宜选择 F2。

如果没有其他判定依据,当频率高于每 15 min 一次时,宜选择 F2。

如果累积暴露时间不超过总运行时间的 1/20 且频率不高于每 5 min 一次,宜选择 F1。

示例:机器每天总运行时间为 8 h,人员为了更换工件每小时暴露一次,暴露时间 2 min(估算的平均值),因此累积暴露时间为 16 min,除以 8×60 min,得出结果为 1/30。同时,由于频率为 1/h,能选择 F1。

A.3.3 避免或限制伤害的可能性 P1 和 P2

重要的是判定在导致伤害之前能否识别并避免危险事件。例如:能否通过物理特征直接识别危险暴露,还是只能通过技术手段(如指示器)来识别。影响选择参数 P 的其他重要因素包括但不限于:

- a) 危险状况发生的速度(例如:迅速或缓慢);
- b) 避开危险状况的可能性(例如:通过逃生);
- c) 与过程有关的实际安全经验;
- d) 是否由经过培训且合适的人员操作;
- e) 操作有无监管。

危险事件发生时,只有确实存在避免或显著减轻伤害的可能性才宜选择 P1,否则宜选择 P2。

以下为一种确定 P 的方法:

- 根据具体应用确定表 A.1 中各因素的字母(每个因素只有一种选择);

- 累计“A”“B”和“C”各自的数量；
- 根据表 A.2 确定参数 P 的对应值。

表 A.1 基于五个因素确定参数 P

因素	C	B	A
1. 机器的使用	—	非熟练人员 ^a	熟练人员 ^a
2. 能造成危险事件的机器部件的速度(取决于具体的机器以及逃离或避开危险状况的时间)	高速事件 如大于 1 000 mm/s,逃离危险的时间小于 1 s 和/或 没有或几乎没有逃生时间	中速事件 如 250 mm/s~1 000 mm/s,逃离危险的时间大于或等于 1 s 且小于 3 s 和/或 逃生时间有限	低速或极低速事件 如小于 250 mm/s,逃离危险的时间大于或等于 3 s 和/或 有足够的逃生时间
3. 空间上逃离危险的可能性	不可能	偶然/很少有可能 可能性小于 50%	很可能 可能性大于等于 50%
4. 认知/察觉危险的可能性(如高温/低温表面、非电离辐射等)	不可能 如需要依赖仪表、人的感知 无法察觉到危险、感知能力 被环境条件掩盖	偶然/很少认知危险 可能性小于 50%	容易认知危险 可能性大于等于 50%
5. 操作复杂程度(从交互角度而言的操作次数和/或操作可用时间)	—	复杂程度中至高 如故障排查、利用保持运行控制设定机器部件	复杂程度低 如调节工件夹具,或者 复杂程度极低/无交互 如将工件放入机器
注: 本表中给出的数据仅供参考,C 类标准或具体机器应用的数据可能不同。			
^a 本文件 3.1.55 定义了经过相关教育培训以及具备多年实践经验的“熟练人员”。			

表 A.2 参数 P1 或 P2 的选择

总得分	参数“P”
一个或以上“C”	■ ■ ■ ■ ■ P2
没有“C”,三个或以上“B”	■ ■ ■ ■ ■ P2
没有“C”、两个“B”、其余“A”	■ ■ ■ ■ ■ 根据具体情况选 P1 或 P2
没有“C”、一个或没有“B”、其余“A”	■ ■ ■ ■ ■ ■ ■ ■ ■ ■ P1

使用基于表 A.1 和表 A.2 的方法时,宜遵循:只有现实存在避免或显著减轻危险影响的可能性时才宜选择 P1,否则宜选择 P2。

A.4 叠加危险

使用本文件时,所有危险都作为一个特定危险或危险状况。因此每个危险均可能单独评估。如果明显存在直接关联危险的组合,且总是同时发生,则风险估计时宜将这些风险组合。进行机器风险评估时,宜考虑是否宜将危险单独考虑或组合考虑。

示例 1: 连续焊接的机器人可能产生多种同时存在的危险状况,比如由运动造成的挤压以及由于焊接过程导致的灼

伤。这可能作为一个直接关联危险的组合。

示例 2：不同的机器人在一个机器人站内工作，站内的每台机器人同一时间只能产生一种危险，每台机器人可能分别考虑。

示例 3：作为风险评估的结果，对带有夹持设备的旋转台，可能分别考虑每个夹持设备。

附录 B

(资料性)

模块法和安全相关模块图

B.1 模块法

该简化方法需要对子系统进行面向模块的逻辑表示。子系统宜根据以下要求分为少量的模块：

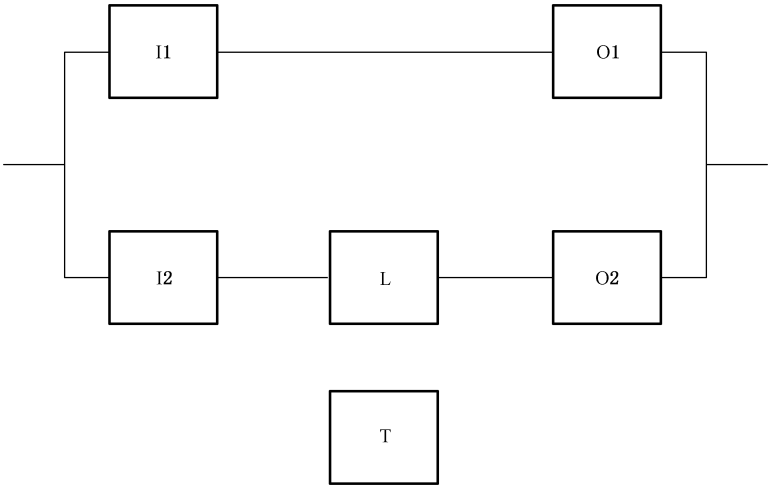
- a) 模块宜代表执行安全功能相关的子系统逻辑单元；
- b) 执行子功能的不同通道宜分为不同的模块；
- c) 如果一个模块不再执行其功能，不宜影响其他通道的模块执行子功能；
- d) 每个通道可由一个或多个模块组成——并不强制要求在指定架构中每个通道为 3 个模块(输入、逻辑单元和输出)，而只是每个通道内逻辑划分的示例；
- e) 子系统的每个硬件单元宜完全归属于一个模块，以便可以通过该模块各硬件单元的 $MTTF_D$ ，来计算该模块的 $MTTF_D$ (如：通过 FEMA 或部件计数法，见 D.1)。

B.2 安全相关的模块图

由模块法定义的模块可在安全相关的模块图中用图形方式表示子系统的逻辑结构。对于这种图形表示，下列内容能作为指南：

- 在串联模块中，一个模块的失效导致整个通道的失效(例如：如果子系统的一个通道的一个硬件单元发生危险失效，则整个通道也许就不再能执行子功能)；
- 在并联模块中，只有所有的通道发生危险失效才导致子功能丧失(例如：由几个通道执行的子功能只要有一个通道没有失效就可执行)；CCF 能够造成此类状况(见 6.1.6、附录 F 和附录 G)；
- 类别 3 或类别 4 的 SRP/CS 中仅用于测试目的且发生危险失效时不影响不同子功能执行的模块，可与不同通道的模块分离。

示例见图 B.1。



- 标引序号说明：
- I1、I2 —— 输入装置，例如：传感器；
 - L —— 逻辑单元；
 - O1、O2 —— 输出装置，例如：主接触器；
 - T —— 测试装置（仅用于测试）；
 - I1 和 O1 —— 构成了第一个通道（串联）；
 - I2、L 和 O2 —— 构成了第二个通道（串联），两个通道以冗余方式执行子功能（并联）。

图 B.1 安全相关功能模块图示例

附 录 C

(资料性)

单个元件 MTTF_D 值的计算或评估

C.1 概述

本附录给出了几种用于计算或评估单个元件 MTTF_D 值的方法；C.2 中给出的方法建立在不同种类元件的良好工程应用实践的基础上；C.3 中给出的方法适用于液压元件；C.4 给出了根据 B_{10} （见 C.4.1）计算气动元件、机械元件和机电元件的 MTTF_D 的方法；C.5 列出了电子元件的 MTTF_D 值。

C.2 良好工程实践方法

如果满足以下准则，则能根据表 C.1 估计用于元件的 MTTF_D 值和 B_{10D} 值：

- a) 元件是根据 GB/T 16855.2—2015 中基本安全原则和经验证的安全原则和相关的元件设计标准（见表 C.1）制造的（元件数据表中确认的）；

注：该信息能在元件制造商的数据表中找到。

- b) 元件制造商为 SRP/CS 的设计者规定了适当的应用和运行条件；
- c) SRP/CS 的设计满足 GB/T 16855.2—2015 中针对元件实施和运用的基本安全原则和经验证的安全原则。

表 C.1 元件 MTTF_D 或 B_{10D} 的相关标准

元件	符合 GB/T 16855.2—2015 的 基本的和经验证的安全原则	相关标准	典型值：MTTF _D （年） B_{10D} （周期）
机械元件	表 A.1 和表 A.2	—	MTTF _D = 150
$n_{op} \geq 1\,000\,000$ 次每年的液压元件 ^a	表 C.1 和表 C.2	ISO 4413	MTTF _D = 150
$1\,000\,000 > n_{op} \geq 500\,000$ 次 每年的液压元件 ^a	表 C.1 和表 C.2	ISO 4413	MTTF _D = 300
$500\,000 > n_{op} \geq 250\,000$ 次 每年的液压元件 ^a	表 C.1 和表 C.2	ISO 4413	MTTF _D = 600
$n_{op} < 250\,000$ 次每年的液压元件 ^a	表 C.1 和表 C.2	ISO 4413	MTTF _D = 1 200
气动元件	表 B.1 和表 B.2	ISO 4414	$B_{10D} = 20\,000\,000^c$
小载荷继电器和接触器式继电器	表 D.1 和表 D.2	IEC 61810-3 IEC 60947(所有部分)	$B_{10D} = 20\,000\,000$
额定载荷继电器和接触器式继电器	表 D.1 和表 D.2	IEC 61810-3 IEC 60947(所有部分)	$B_{10D} = 400\,000$
小载荷接近开关	表 D.1 和表 D.2	IEC 60947(所有部分) ISO 14119	$B_{10D} = 20\,000\,000$
额定载荷接近开关	表 D.1 和表 D.2	IEC 60947(所有部分) ISO 14119	$B_{10D} = 400\,000$

表 C.1 元件 MTTF_D 或 B_{10D} 的相关标准 (续)

元件	符合 GB/T 16855.2—2015 的 基本的和经验证的安全原则	相关标准	典型值:MTTF _D (年) B _{10D} (周期)
小载荷接触器 ^d	表 D.1 和表 D.2	IEC 60947(所有部分)	B _{10D} =20 000 000
额定载荷接触器 ^d	表 D.1 和表 D.2	IEC 60947(所有部分)	B _{10D} =1 300 000
位置开关 ^b	表 D.1 和表 D.2	IEC 60947(所有部分) ISO 14119	B _{10D} =20 000 000
位置开关(带有独立的 执行器,防护锁定) ^b	表 D.1 和表 D.2	IEC 60947(所有部分) ISO 14119	B _{10D} =2 000 000
急停装置 ^b	表 D.1 和表 D.2	IEC 60947(所有部分) ISO 13850	B _{10D} =100 000
按钮(例如:使能开关) ^b	表 D.1 和表 D.2	IEC 60947(所有部分)	B _{10D} =100 000
<p>注 1: B_{10D}的定义和用法见 C.4。</p> <p>注 2: 如果没有其他信息(如产品标准),则 B_{10D}估算为 B₁₀的二倍(50%的危险失效率)。</p> <p>注 3: 根据电气输出触点的数量以及后续 SRP/CS 的故障检测,符合 IEC 60947-5-5 和 ISO 13850 的急停装置以及符合 IEC 60947-5-8 的使能开关可以估计为一个类别 1、类别 3 或者类别 4 的子系统。每个触点组件(包括机械驱动)可能被考虑为一个具有各自 B_{10D}值的通道。对于符合 IEC 60947-5-8 的使能开关,意味着通过按压或者释放实现打开功能。有些情况下,考虑到装置的特定应用及环境条件,机器制造商能根据 GB/T 16855.2—2015 中表 D.8 进行故障排除。</p> <p>注 4: 开关周期的缩短可能导致开关元件卡在阀芯中的概率增加(见 ISO 4413)。</p> <p>注 5: 机械部件的 MTTF_D 仅指可做机械运动的元件/部件(不包括外壳)。</p>			
<p>^a 液压元件的 B_{10D} 计算不准许使用标准 MTTF_D 进行反向计算。</p> <p>^b 假如直接断开动作的排除故障是可能的。</p> <p>^c 通常,大多数气动元件,可以假定该值。但根据应用和类型,例如截止阀,该值可大幅降低。</p> <p>^d “额定载荷”或“小载荷”宜考虑 GB/T 16855.2—2015 中描述的安全原则,比如超过额定工作电流。“小载荷”的示例:额定载荷的 20%。</p>			

C.3 液压元件

如果满足以下准则,则单个液压元件(例如:阀)的 MTTF_D 值能估计为 150 年。如果全年的平均操作次数(n_{op})低于 1 000 000 次,其 MTTF_D 值能被估计得更高,如表 C.1 所示:

- a) 液压元件是根据 GB/T 16855.2—2015 中针对液压元件设计的表 C.1、表 C.2 和相关标准(见表 C.1)中基本安全原则和经验证的安全原则制造的(元件数据表中确认的);
- b) 液压元件制造商为 SRP/CS 的设计者规定了适当的应用和操作条件。SRP/CS 的设计者宜提供其职责相关的信息,以证明其针对液压元件的实施和运用符合 GB/T 16855.2—2015 中表 C.1和表 C.2 中基本安全原则和经验证的安全原则。

如果不能达到 a)或 b)的要求,制造商宜给出单个液压元件的 MTTF_D 值。如果制造商能提供数据,则针对气动、机械、机电以及液压元件的 MTTF_D,可采用 B_{10D}、B₁₀、T_{10D}、T₁₀ 的概念,而无需采用上述固定的 MTTF_D 值。

C.4 气动、机械和机电元件的 MTTF_D

C.4.1 概述

对于气动、机械和机电元件(气动阀、继电器、接触器、位置开关、位置开关的凸轮),可能难以计算出本文件所要求的、以年来表示的元件的 MTTF_D。多数时候,这类元件的制造商只给出直至 10% 的元件发生失效时的平均周期数(B_{10})或直至 10% 的元件发生危险失效时的平均周期数(B_{10D})。本条款给出了通过制造商给出的与操作次数密切相关的 B_{10D} 或 T (寿命)来计算元件 MTTF_D 的方法。

假如满足以下所有准则,则能根据 C.4.2 估计单个气动、机电或机械元件的 MTTF_D 值:

- a) 元件是根据 GB/T 16855.2—2015 中表 A.1、表 B.1 或表 D.1 的基本安全原则和经验证的安全原则设计及制造的;

注 1: 该信息能在元件制造商的数据表中找到。

- b) 用于类别 1、类别 2、类别 3 或类别 4 的元件是根据 GB/T 16855.2—2015 中表 A.2、表 B.2 或表 D.2 的基本安全原则和经验证的安全原则设计及制造的;

注 2: 该信息能在元件制造商的数据表中找到。

- c) 元件制造商为 SRP/CS 的设计者规定了适当的应用和工作条件。SRP/CS 的设计者宜提供相关信息,该信息用于证明其采用的元件符合 GB/T 16855.2—2015 中表 A.1、表 B.1 或表 D.1 的基本安全原则。对于类别 1、类别 2、类别 3 或类别 4,还宜告知使用者有责任确保实施和运用的元件满足 GB/T 16855.2—2015 中表 A.1、表 B.2 或表 D.2 经验证的安全原则。

C.4.2 根据 B_{10D} 计算元件的 MTTF_D

元件制造商宜根据相应的产品测试方法标准[如 ISO 19973(所有部分)、IEC 60947-4-1、IEC 60947-5-1、IEC 60947-5-5、IEC 61810-2-1]来确定 10% 的元件发生危险失效时的平均周期数(B_{10D})¹⁾。宜规定元件的危险失效模式,例如:在终端阻塞或切换时间改变。通过 B_{10D} 和年平均操作次数 n_{op} ,能计算出元件的 MTTF_D:

$$MTTF_D = \frac{B_{10D}}{0.1 \times n_{op}} \quad \dots\dots\dots (C.1)$$

式中:

$$n_{op} = \frac{d_{op} \times h_{op} \times 3\,600 \text{ s/h}}{t_{cycle}} \quad \dots\dots\dots (C.2)$$

式中:

h_{op} ——平均工作时间,单位为小时每天;

h_{op} ——平均工作时间,单位为天每年;

t_{cycle} ——元件两个相继周期起始点(例如:阀的切换)之间的平均操作时间,单位为秒每周期。

元件的工作寿命时间限制在 T_{10D} 内,10% 元件发生危险失效的平均时间为:

$$T_{10D} = \frac{B_{10D}}{n_{op}} \quad \dots\dots\dots (C.3)$$

如果制造商没有给出元件 B_{10D} 值,允许使用公式(C.4)来确定。

$$B_{10D} = \frac{B_{10}}{R_{DF}} \quad \dots\dots\dots (C.4)$$

如果元件制造商给出的危险故障比例(R_{DF})估计小于 50%,则 T_{10D} 被限制为 $T_{10} \times 2$ 。

当元件的 T_{10D} 小于任务时间(20 年或更少),负责集成提供安全功能的 SRP/CS 的制造商将在 T_{10D}

1) 如果没有给出 B_{10} 的危险分数(如由制造商给出),则可使用 B_{10} 的 50%,因此推荐采用 $B_{10D} = 2B_{10}$ 。

周期结束时或提前告知用户更换元件。将元件的使用时间限制在 T_{10D} 周期内,可以保持安全功能的预期性能等级。

C.4.3 公式说明

在本文件中,可靠性计算方法假定元件的失效为时间的指数分布: $F_D(t) = 1 - e^{-\lambda_D t}$ 。对于非电子元件,更有可能是威布尔分布。但如果元件的工作时间被限制在 10% 的元件发生危险失效的平均时间内(T_{10D}),则能把该工作时间内的恒定危险失效率(λ_D)估计为公式(C.5):

$$\lambda_D = \frac{0.1}{T_{10D}} = \frac{0.1 \times n_{op}}{B_{10D}} \quad \dots\dots\dots (C.5)$$

公式(C.6)考虑了在与 B_{10D} (周期)相对应的 T_{10D} (年)后有 10% 的元件在假设的应用中失效的恒定失效率。准确的说:

$$F_D(t) = 1 - e^{-\lambda_D T_{10D}} = 10\%, \text{ 即: } \lambda_D = \frac{\ln 0.9}{T_{10D}} = \frac{0.10536}{T_{10D}} \approx \frac{0.1}{T_{10D}} \quad \dots\dots\dots (C.6)$$

对于指数分布,由于 $MTTF_D = 1/\lambda_D$,代入后得到公式(C.7):

$$MTTF_D = \frac{T_{10D}}{0.1} = \frac{B_{10D}}{0.1 \times n_{op}} \quad \dots\dots\dots (C.7)$$

注:公式中的所有变量是以数值与测量单位乘积表示的物理量。正确使用公式(C.5)、公式(C.6)及 $MTTF_D = 1/\lambda_D$ 等公式可能需要使用 1 年等于 8 760 h 将单位“年”转换为单位“小时”。

C.4.4 示例

对于气动阀,制造商确定以 6×10^7 个周期的平均值作为 B_{10D} 。该阀在一年中工作 220 天,每天两班。该阀两次相继切换的起始点之间的平均时间估为 5 s。这就产生了以下的值:

- $d_{op} = 220$ 天每年;
- $h_{op} = 16$ 小时每天;
- $t_{cycle} = 5$ 秒每个周期;
- $B_{10D} = 6 \times 10^7$ 个周期。

把这些值代入下列方程式进行计算:

$$n_{op} = \frac{220 \times 16 \times 3\,600}{5 \text{ s}} = 2.53 \times 10^6 \text{ 周期/年} \quad \dots\dots\dots (C.8)$$

$$T_{10D} = \frac{60 \times 10^6}{2.53 \times 10^6} = 23.7 \text{ 年} \quad \dots\dots\dots (C.9)$$

$$MTTF_D = \frac{23.7}{0.1} = 237 \text{ 年} \quad \dots\dots\dots (C.10)$$

根据表 C.5 可给出该元件的 $MTTF_D$ 为“高”。对于该阀,上述假设在 23.7 年的限定操作时间内有效。

C.5 电子元件的 $MTTF_D$ 数据

C.5.1 概述

表 C.2~表 C.7 给出了电子元件 $MTTF_D$ 的某些典型平均值。这些数据来源于 SN 29500 (所有部分)数据库。所有数据均为普通类型。各种不同的数据库 (见参考文献列出的无穷清单) 可用于表示各种不同的电子元件的 $MTTF_D$ 值。如果 SRP/CS 的设计者具有所用元件的可靠的专用数据,则推荐采用专用数据。

表 C.2~表 C.7 中给出的值对于环境温度为 40℃ 时的电流和电压的额定载荷有效。当电子元件工

作于规定的温度或负载值范围之外时,宜使用 $MTTF_D$ 的校正系数[见 SN 29500(所有部分)]。

在这些表的 MTTF 栏中,来源于 SN 29500(所有部分)的值用于通用元件所有可能的失效模式,这些失效模式并不一定造成危险失效。在 $MTTF_D$ 栏中,典型的假设是:并不是所有的失效模式都会导致危险失效。这主要取决于实际应用。准确确定元件“典型” $MTTF_D$ 值的方法是进行失效模式及影响分析(FMEA)。某些元件,例如用作开关的晶体管,可能会遇到短路或断路而失效。这两种失效模式中只有一种可能是危险的;因此,在“备注”栏中假设危险失效的概率只有 50%,这就意味着元件的 $MTTF_D$ 是给出的 MTTF 值的 2 倍。

C.5.2 半导体

见表 C.2 和表 C.3。

表 C.2 晶体管(用作开关)

晶体管	示例	元件的 MTTF 年	元件的 $MTTF_D$ 年 典型值	备注
双极型	TO18、TO92、SOT23	38 052	76 104	危险失效概率 50%
双极型、低功率	TO5、TO39	5 708	11 416	危险失效概率 50%
双极型、功率	TO3、TO220、D-Pack	1 903	3 806	危险失效概率 50%
FET	MOS 交叉点	22 831	45 662	危险失效概率 50%
MOS、功率	TO3、TO220、D-Pack	1 903	3 806	危险失效概率 50%

表 C.3 二极管、功率半导体和集成电路

二极管	示例	元件的 MTTF 年	元件的 $MTTF_D$ 年 典型值	备注
一般用途	—	114 155	228 311	危险失效概率 50%
干扰抑制器	—	16 308	32 616	危险失效概率 50%
齐纳二极管 $P_{tot}<1W$	—	114 155	228 311	危险失效概率 50%
整流二极管	—	57 078	114 155	危险失效概率 50%
桥式整流器	—	11 415	22 831	危险失效概率 50%
闸流晶体管	—	2 283	4 566	危险失效概率 50%
双向可控硅、双向触发二极管	—	1 522	3 044	危险失效概率 50%
集成电路(可编程和不可编程)	采用制造商的数据			危险失效概率 50%

C.5.3 无源元件

见表 C.4~表 C.7。

表 C.4 电容

电容	示例	元件的 MTTF 年	元件的 MTTF _D 年 典型值	备注
标准无源电容	KS、KP、KC、KT、 MKT、MKC、MKP、 MKU、MP、MKV	57 078	114 155	危险失效概率 50%
陶瓷电容	—	22 831	45 662	危险失效概率 50%
铝电解质电容	非固态电解质	22 831	45 662	危险失效概率 50%
铝电解质电容	固态电解质	38 052	76 104	危险失效概率 50%
钽电解质电容	非固态电解质	11 415	22 831	危险失效概率 50%
钽电解质电容	固态电解质	114 155	228 311	危险失效概率 50%

表 C.5 电阻

电阻	示例	元件的 MTTF 年	元件的 MTTF _D 年 典型值	备注
碳膜	—	114 155	228 311	危险失效概率 50%
金属膜	—	570 776	1 141 552	危险失效概率 50%
金属氧化物和线绕电阻	—	22 831	45 662	危险失效概率 50%
可变电阻	—	3 805	7 610	危险失效概率 50%

表 C.6 感应器

感应器	示例	元件的 MTTF 年	元件的 MTTF _D 年 典型值	备注
MC 应用	—	38 052	76 104	危险失效概率 50%
低频感应器和变压器	—	22 831	45 662	危险失效概率 50%
主变压器、开关变压器 和电源变压器	—	11 415	22 831	危险失效概率 50%

表 C.7 光耦合器

光耦合器	示例	元件的 MTTF 年	元件的 MTTF _D 年 典型值	备注
双极输出	SFH 610	7 610	15 220	危险失效概率 50%
FET 输出	LH 1056	2 854	5 708	危险失效概率 50%

附 录 D

(资料性)

估算各通道 MTTF_D 的简化方法

D.1 部件计数法

“部件计数法”能用于分别估算每个通道的 MTTF_D。计算时要用到组成该通道的所有单个元件的 MTTF_D 值。

注：部件计数法是一种近似方法，取差总是朝向安全侧。

通用公式(D.1)为：

$$\frac{1}{MTTF_D} = \sum_{i=1}^N \frac{1}{MTTF_{Di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{Dj}} \dots\dots\dots (D.1)$$

式中：

- MTTF_D —— 整个通道的平均危险失效间隔时间；
- MTTF_{Di}、MTTF_{Dj} —— 组成子功能的每个元件的 MTTF_D；第一个和是每个独立元件的 MTTF_D 相加之和；第二个和是一个等效的简化形式，其中所有的 n_j 个具有相同 MTTF_{Dj} 的完全相同的元件被分类归集在一起。

表 D.1 中的示例给出了该通道的 MTTF_D 为 22.4 年，根据 6.1.4 和表 6，该示例中通道的 MTTF_D 为“中”。

表 D.1 电路板的元件表示例

<i>j</i>	元件	元件数 <i>n_j</i>	MTTF _{Di} 年 典型值	1/MTTF _{Dj} 1/年 典型值	<i>n</i> /MTTF _{Dj} 1/年 典型值
1	双极型低功率晶体管(见表 C.2)	2	11 416	0.000 087 6	0.000 175 2
2	碳膜电阻(见表 C.5)	5	228 311	0.000 004 4	0.000 021 9
3	标准无功率电容(见表 C.4)	4	114 115	0.000 008 8	0.000 035 0
4	数值由制造商给出的继电器($B_{10D}=20\ 000\ 000$ 周期、 $n_{op}=633\ 600$ 周期/年)	4	315.7	0.003 167 6	0.012 670 3
5	数值由制造商给出的接触器($B_{10D}=2\ 000\ 000$ 周期、 $n_{op}=633\ 600$ 周期/年)	1	31.6	0.031 645 6	0.031 645 6
$\Sigma(n_j/MTTF_{Dj})$		—	—	—	0.044 548 0
MTTF _D =1/ $\Sigma(n_j/MTTF_{Dj})$ (年)		22.4			

- 注 1：本方法建立在假设一个通道中任何元件的危险失效会导致该通道危险失效的基础上。表 D.1 中的 MTTF_D 计算就基于这个假设。
- 注 2：本示例中，主要影响来自接触器。本示例为 MTTF_D 和 B_{10D} 所选择的值建立在附录 C 的基础上。该示例应用中，假定 $d_{op}=220$ 天/年， $h_{op}=8$ 小时/天以及 $t_{cycle}=10$ 秒/周期，得出 $n_{op}=633\ 600$ 周期/年。通常，采用制造商提供的 MTTF_D 和 B_{10D} 值将会产生的更好的结果，即该通道的 MTTF_D 更高。
- 注 3：当 MTTR(平均恢复时间)忽略不计时，认为 MTTF 等于 MTBF。
- 注 4：如果只有 MTBF 能用，则通过 $MTTF_D \approx 2 \times MTBF$ 来完成其到 MTTF_D 的转换。

D.2 用于不同通道的 $MTTF_D$, 每个通道的 $MTTF_D$ 的对称化

6.1.3.2 中的指定架构假设: 对于冗余 SRP/CS 中的不同通道, 每个通道的 $MTTF_D$ 值是相同的。每个通道的 $MTTF_D$ 值宜输入到图 12 中。

如果这些通道的 $MTTF_D$ 不同, 则有两种可能:

——作为最坏假设, 宜采用较低的值;

——能用公式(D.2)估算一个值来代替每个通道的 $MTTF_D$:

$$MTTF_D = \frac{2}{3} \left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}} \right] \dots\dots\dots (D.2)$$

式中:

$MTTF_{DC1}$ 、 $MTTF_{DC2}$ 是两个不同的冗余通道的 $MTTF_D$ 值, 各限定为最大值 100 年(类别 B、类别 1、类别 2 和类别 3)或 2500 年(类别 4)。

示例: 一个通道的 $MTTF_{DC1} = 3$ 年, 另一个通道的 $MTTF_{DC2} = 100$ 年, 则每个通道最终的 $MTTF_D = 66$ 年。这就是说一个通道的 $MTTF_D$ 为 100 年, 另一个通道的 $MTTF_D$ 为 3 年的冗余系统等效于每个通道的 $MTTF_D$ 均为 66 年的系统。

根据上面的公式, 具有两个通道并且每个通道具有不同的 $MTTF_D$ 值的冗余系统, 可能由每个通道中具有相同 $MTTF_D$ 值的冗余系统来代替。这个过程是为了正确使用图 12。

注: 本方法假设采用独立的并联通路。

附 录 E
(资料性)
功能和子系统诊断覆盖率(DC)的估计

E.1 诊断覆盖率(DC)的示例

见表 E.1。

表 E.1 诊断覆盖率(DC)的估计

措施	DC ^{a,b}
输入装置	
由输入信号的动态变化激励的循环测试	90%
真实性检查,如使用常开和常闭的机械连接触点	99%
对输入信号交叉监控,无动态测试	取决于实际应用,如取决于应用中信号改变的频率(见注 4)
对输入信号交叉监控,有动态测试,无短路检测(用于多路 I/O)	90%
对逻辑(L)中的输入信号和中间结果进行交叉监控、对程序流进行临时和逻辑软件监控,以及静态故障和短路的检测(用于多路 I/O)	99%
间接监控(如通过压力开关进行监控,通过执行机构的电气位置进行监控)	90%~99%,取决于实际应用(见注 2)
直接监控(如控制阀的电气位置监控,通过机械连接的触点组件监控机电装置)	99%
通过过程进行故障检测	取决于实际应用;单用本措施达不到所需性能等级“e”(见注 2、注 3 和注 5)
监控传感器的某些特征参数(响应时间、模拟信号的范围,例如:电阻、电容)	60%
逻辑	
间接监控(例如:通过压力开关进行监控,通过执行机构的电气位置进行监控,最终结果的真实性检查)	90%~99%,取决于实际应用(见注 2)
直接监控(例如:控制阀的电气位置监控,通过机械连接的触点组件监控机电装置,中间结果的真实性检查)	99%
逻辑的简单暂时时间监控(例如:定时器用作看门狗,其触发点在逻辑程序内)	60%
由看门狗对逻辑进行时序和逻辑监控,由测试设备进行逻辑性能的真实性检查	90%
启动自检以检测逻辑中部件的潜在故障(例如:程序和数据存储器、输入/输出端口、接口)	60%~90%(见注 2)
在启动时,或在安全功能需要时,或在一个外部信号通过一个输入设备进行请求时,由主通道检查监测装置(如看门狗)的响应能力	90%
动态原则(要求安全功能时,逻辑的所有元件需要按 ON-OFF-ON 改变状态),如由继电器执行的联锁回路	99%

表 E.1 诊断覆盖率(DC)的估计 (续)

措施	DC ^{a, b}
逻辑	
不可变内存:单字的签名(单总线位宽)	90%
不可变内存:双字的签名(双总线位宽)	99%
可变内存:使用冗余数据进行 RAM 测试,例如:标记、标志、常量、定时器及这些数据的交叉比较	60%
可变内存:检查存储器单元数据的可读性和可写性	60%
可变内存:RAM 自检(例如:“galpat”码或“Abraham”码)或双 RAM 使用硬件或软件比较和读/写测试	99%
处理单元:通过软件自检(见 GB/T 20438.7 的 A.3)	60%~90%(见注 2)
处理单元:编码处理(见 GB/T 20438.7 的 A.3)	90%~99%(见注 2)
通过过程进行故障检测	取决于实际应用;单用本措施达不到所需性能等级“e”(见注 2、注 3 和注 5)
输出装置	
由一个通道对输出监控,无动态测试	取决于实际应用,例如:取决于应用中信号改变的频率(见注 4)
对输出信号交叉监控,无动态测试	取决于实际应用,例如:取决于应用中信号改变的频率(见注 4)
对输出信号交叉监控,有动态测试,无短路检测(用于多路 I/O)	90%
对逻辑(L)中输出信号和中间结果的交叉监控、对程序流进行临时和逻辑软件监控,以及对静态故障和短路的检测(用于多路 I/O)	99%
带有逻辑和测试设备监控的输出冗余关断路径,见 GB/T 16855.2—2015 的附录 E	99%
间接监控(如通过压力开关进行监控,通过执行器的电气位置进行监控)	90%~99%,取决于实际应用(见注 2)
通过过程进行故障检测	取决于实际应用;单用本措施达不到所需性能等级“e”(见注 2、注 3 和注 5)
直接监控(如控制阀的电气位置监控,通过机械接触点组件监控机电装置)	99%
<p>注 1: 对于 DC 的附加估计,见 GB/T 20438.2—2017 中 A.2~A.14 等。</p> <p>注 2: 对于给定 DC 范围的措施(例如通过过程进行故障检测),考虑所有的危险失效就能确定正确的 DC 值,然后决定对哪些危险失效需要通过 DC 措施进行检测。如仍不确定,宜根据 FMEA 估计 DC。</p> <p>注 3: 对于“通过过程进行故障检测”的 DC 措施,可将安全功能的要求率(r_d)和过程诊断(测试)率(r_t)与被测元件的有效 DC 限制一同考虑:</p> <p>——$r_t/r_d > 1$ 时,DC 限制为 60%;</p> <p>——$r_t/r_d > 10$ 时,DC 限制为 90%;</p> <p>——$r_t/r_d > 100$ 时,DC 限制为 99%。</p> <p>注 4: 对于“对输入或输出信号的交叉监控,无动态测试”的 DC 措施,测试率的影响可以与以下被测元件的有效 DC 限制结合:</p> <p>对于类别 3 和类别 4:</p> <p>——$r_t < 1$/年时,DC 限制为 0%;</p> <p>——$r_t \geq 1$/年时,DC 限制为 90%;</p> <p>——$r_t \geq 1$/月时,DC 限制为 99%。</p>	

表 E.1 诊断覆盖率(DC)的估计 (续)

措施	DC ^{a,b}
注 5: 当“通过过程进行故障检测”的 DC 措施与附录 E 中列出的其他 DC 措施相结合时,即使对于 PL _r e,该措施仍然可以包括在模块的 DC 估计中。	
^a DC 措施可以组合使用以实现更高的 DC。 ^b 如果逻辑要求 DC 为中或高,则应为每个变量存储器,常量存储器和处理单元采取至少一种措施,以使每部分 DC 至少为 60%。除此表中列出的措施外,还能使用其他措施。	

表 E.1 的应用示例如下。

示例 1: GB/T 16855.2—2015 的附录 E 给出了一个用于确认自动装配机故障行为和诊断方法的完整样例(非常详细)。

注: ISO/TR 24119 描述了如何采用渐进表格法评估串联的无电势触点联锁装置的诊断覆盖率。

示例 2: 可能只有在安全相关元件参与生产过程的情况下,例如:将标准 PLC 或标准传感器用于工件加工以及作为执行安全功能的两个通道之一,才能应用“通过过程进行故障检测”的 DC 措施。DC 水平是否合适取决于共用资源的重合度(逻辑、输入/输出),例如:如果印刷机上的旋转编码器的所有故障都会造成印刷过程显著中断,则用于检测安全极限速度的传感器的 DC 可估计为 90%~99%。

E.2 诊断覆盖率平均值的估计

很多系统用到了多种故障检测措施。这些措施能检查 SRP/CS 的不同部件且有不同的 DC。当根据 6.1.8 和图 12 来估计 PL 时,执行安全功能的整个 SRP/CS 只有一个平均 DC 适用。

DC 可确定为被检测到的危险失效的失效率与全部危险失效的失效率之间的比率。根据这个定义,用公式(E.1)来估计平均诊断覆盖率 DC_{avg}:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \quad \text{.....(E.1)}$$

所有未经故障排除的 SRP/CS 元件都宜考虑在内并求和。每个模块都考虑 MTTF_D 和 DC。公式(E.1)中的 DC 是指部件检测到的危险失效的失效率(不管用何种方法检测失效)与部件全部危险失效的失效率之间的比率。因此,DC 与被测试的元件有关,而与测试装置无关。无故障检测的元件(如未经测试的元件)其 DC=0,只改变 DC_{avg} 的分母。

附录 F
(资料性)

防止共因失效(CCF)的措施的量化方法

F.1 概述

每个对 SRP/CS 有影响的类别 2、类别 3 或类别 4 的子系统,均宜满足 F.2 和 F.3 中描述的防止 CCF 的措施的综合程序。

根据 GB/T 20438.6—2017 中附录 D,6.1.8 中的简化程序假设 β 系数为 2%。能通过满足 F.2 中的程序来实现。

宜记录 F.2 和 F.3 中描述的措施,以证实达到最低 65 分的分数。

F.2 防止 CCF 的措施的影响估计

宜考虑子系统每个部件的 CCF。

基于工程评定,表 F.1 中列出了各种措施对减小 CCF 的作用。

F.3 中详细描述了措施。对于每一项列出的措施,只有在措施得到充分实施的情况下,才能获得满分。如果只是部分满足某种措施,则宜假设得分为零。

每项措施都宜根据具体应用和 CCF 的相关原因进行评估(例如:对于电子系统,只有“防止 EMI”是相关的,而“流体介质的杂质”是不相关的)。

如果元件采用的内部措施未实现充分的过电压保护和环境影响保护,宜在系统级使用外部保护元件、滤波器和屏蔽层达到保护。

表 F.1 防止 CCF 的措施的评分过程及量化

序号	防止 CCF 的措施		得分
1	分离/隔离		15
2	相异		20
3	设计/应用/经验		—
3.1	防止过电压、过压力、过电流、过温等的保护		15
3.2	所用的元件是经验证的		5
4	评估/分析		5
5	培训		5
6	环境		—
6.1	防止 EMI 或流体介质的杂质		25
6.2	其他影响		10
—	合计		最高可得 100
总分		避免 CCF 的措施	
65 或 65 以上		满足要求	
小于 65		不合格⇒选择附加措施	

表 F.1 中列出的措施宜根据其有效性进行评估,以避免或控制冗余通道的 CCF。工程评定宜证实

已尽可能合理地减少了造成 CCF 的典型原因。

注 1: CCF 的计算通常在子系统级进行,因为特定子系统的措施不同(如输入、逻辑和输出)。

注 2: 本附录中的冗余通道是指类别 2 中的功能通道和测试通道,或类别 3 和类别 4 中的冗余功能通道。

注 3: 典型的 CCF 原因包括过电压、过压力、过电流、过温、湿度、冲击、振动、EMI、压力介质中的杂质。这些原因的适当程度是从 SRP/CS 的预期应用中推断出来的,包括可预见的故障(如冷却风扇故障)和可合理预见的误用。不同类别(类别 2 与类别 3 和类别 4)或 SRP/CS 的输入/逻辑/输出部分的措施可能有所不同。

F.3 表 F.1 中防止共因失效(CCF)的措施的说明

F.3.1 分离/隔离

冗余通道的信号路径之间的物理分离:

- a) 以配线方式分离(例如,导体之间具有适当绝缘的多条导线);
- b) 以管路方式分离(例如,避免液压管道因从另一个相邻管道释放的高压而损坏);
- c) 在线路中通过动态测试检测出短路或开路;
- d) 每个通道信号路径分别采用屏蔽;
- e) 独立印刷电路板上或独立外壳或机柜中的冗余通道;
- f) 印刷电路板上冗余通道之间足够的间隙和爬电距离,也考虑到例如锡须的存在(见 GB/T 16855.2—2015 中 D.2.2)。

F.3.2 相异

相异性考虑如下。

- a) 采用不同的技术/设计或物理原则,例如:
 - 第一个通道为电子的或可编程电子的,第二个通道为机电硬接线的;
 - 每个通道采用不同的安全功能启动方式(如位置、压力、温度);
 - 第一个通道的阀由橡胶密封,第二个通道的阀由金属密封;
 - 用两个位置开关来检测可移动防护装置(安全防护装置)的打开。第一个位置开关在安全防护装置打开时工作,使用符合 IEC 60947-5-1:2020 中附录 K 要求的直接断开的断开触点元件;第二个位置开关安全防护装置关闭时工作,使用闭合触点元件。
- b) 传感元件采用不同的测量原理(如数字和模拟)或物理原理(如距离、压力或温度)。
- c) 不同的元件,例如不同制造商的元件(非贴牌)。
- d) 不同的负载,例如:第一个通道中的触点/阀在没有负载的情况下切换,第二个通道中的触点/阀在有负载的情况下切换。

F.3.3 设计/应用/经验

过电压、过压力、过电流、过温的保护或控制,例如:

- a) 保护 SRP/CS 的输入和输出以及逻辑的电源,免受过电压和/或过电流的电位电平的影响(另见 IEC 60204-1);

注: SRP/CS 的部件能够承受和/或保护其免受过电压或过电流的电位电平的影响。SW 模式 PSU(开关模式电源)可能产生的最大过电压水平取决于应用的标准(例如,单个故障条件下的最大电压限制)。

重要的是要考虑使用标准 SW 模式 PSU 时可能产生的最大过电压水平,及其他操作条件(例如:过压等级,工作温度)。

- b) 如果故障情况下的基本压力永远不会超过 1.5 倍工作压力,防止过压的措施可为单通道系统。ISO 4414 规定了非预期压力防护(例如泄压阀)的要求。

仅使用了经验证的元件。见 6.1.11 和 GB/T 16855.2—2015。

F.3.4 评估/分析

为了避免 CCF,设计中对安全控制系统中每个部件进行了失效模式和影响分析或 FTA,以识别其潜在原因,并考虑其结果。

F.3.5 培训

设计者接受了培训(有培训文件,如培训证书),以了解 CCF 的原因和后果。

F.3.6 环境

F.3.6.1 防止 EMI 或压力介质杂质

对于电气/电子系统,根据适当的标准(如 IEC 61326-3-1、IEC 61000-6-7:2014、IEC 61000-1-2:2016、IEC 61800-5-2:2016)防止污染和电磁干扰,以防止 CCF。

注 1: 这些 EMI 标准通常比标准元件(如通用 PLC)的设计要求更严格。更多信息见 IEC 61800-3。

注 2: 附录 L 提供了有关 EMI 抗扰度的进一步指导。

对于流体系统,压力介质的过滤、污垢进入的防止、压缩空气的排出,均按照元件制造商关于压力介质纯度的要求执行(见 IEC 8537-1 指导)。

对于流体和电气组合系统,宜同时考虑这两个方面。

F.3.6.2 其他影响

SRP/CS 不受相关标准[如 IEC 60068(所有部分)]规定的所有相关环境的影响,如温度、冲击、机械应力、振动、湿度,同时考虑安全相关应用的增加要求。

F.4 防止共因失效(CCF)的措施和其他相关标准

对于某些 SRP/CS(子系统),并非表 F.1 中列出的所有防止 CCF 的措施都能适当减少 CCF 影响,因为这些 SRP/CS 所能提供的潜在风险减小也受到其系统能力(例如传感器的检测原理)的限制。

注: 某些标准[如 IEC 62024(所有部分)或 GB/T 18831—2017]可能包括与系统能力相关的应用限制。

整个 SRP/CS 的设计者采用这些标准中规定的措施,并遵守制造商提供的使用说明。

附 录 G
(资料性)
系统性失效

G.1 概述

本附录提供了设计和集成 SRP/CS 过程控制和避免系统性失效措施的指南。

G.2 系统性失效的控制措施

宜采用以下措施。

- a) 采用失能法(见 GB/T 16855.2—2015);安全控制系统(SRP/CS)的设计宜使其在动力供应丧失时可达到或保持安全状态(见 GB/T 16855.2—2015, IEC 60204-1:2016+AMD1:2021 中 7.5 和 IEC 62061)。
- b) 控制击穿电压、电压变化、过电压和电压不足的影响的措施;宜预先确定 SRP/CS 对击穿电压、电压变化、过电压和电压不足等条件的响应工况,使 SRP/CS 可实现或保持机器的安全状态(见 IEC 60204-1:2016+AMD1:2021 中第 7 章和 GB/T 20438.7—2017 中 A.8)。
- c) 控制或避免物理环境(例如:温度、湿度、水、振动、灰尘、腐蚀性物质、EMI 及其影响)影响的措施;宜预先确定 SRP/CS 对物理环境响应的工况,使 SRP/CS 能实现或保持机器的安全状态(见 IEC 60529 和 IEC 60204-1 等)。
- d) 为了检测有缺陷的程序顺序,包含软件的 SRP/CS 宜使用程序顺序监测;如果以错误的顺序或在错误的时间段内处理一个程序的独立组件(例如:软件模块、子程序或指令),或者如果处理器的时钟有故障,则存在有缺陷的程序顺序(见 GB/T 20438.7—2017 中 A.9)。
- e) 控制错误的影响或由任何数据通信过程引起的其他影响的措施(见 GB/T 20438.2—2017 中 7.4.11)。

另外,考虑到 SRP/CS 的复杂性及其 PL,还宜采用下列的一种或多种措施:

- 通过自动测试进行的失效检测;
- 通过冗余硬件进行的测试;
- 相异的硬件;
- 以直接模式操作;
- 机械连接的触点;
- 直接断开动作;
- 定向失效模式;
- 当制造商可证明裕量的增加能提高可靠性时,可通过适当的系数增加裕量。

注:增加裕量的例子见 GB/T 16855.2—2015 中 D.2。

G.3 SRP/CS 设计中避免系统性失效的措施

宜采用以下措施。

- a) 采用合适的原料和适当的制造工艺;
根据应力、耐用性、弹性、摩擦、磨损、腐蚀、温度、传导率、介电强度等选择材料、制造方法和处理方法。
- b) 正确的外形和尺寸;
应力、应变、疲劳、温度、表面粗糙度、公差和制造工艺等的考虑。

c) 元件的适当选择、组合、安排、装配和安装,包括布电缆、布线和其他连接等;
采用合适的标准和制造商应用说明,例如:目录单、安装手册、技术规范,并且使用好的工程实践。

d) 兼容性;
使用具有可兼容工作特征的元件。

注:液压或气动阀等元件可能需要循环切换,以避免开关故障或增加不可接受的开关次数。在这种情况下,定期测试是必要的。

e) 承受规定环境条件的能力;
SRP/CS 的设计应使其可在所有预期的环境和任何可预见的不利条件下工作,例如:温度、湿度、振动和 EMI(见 GB/T 16855.2—2015 中 D.2)。

f) 使用符合合适标准且有明确定义的失效模式的元件。
采用具有规定特征的元件减小未检测到的故障的风险(见 GB/T 20438.7—2017 中 B.3.3)。
另外,考虑到 SRP/CS 的复杂性及其 PL,宜采用下面的一种或多种措施。

- 复查硬件的设计(例如:通过检查或走查);
通过复查和分析技术规范和执行情况之间的差异进行查找。
- 有仿真或分析能力的计算机辅助设计工具;
系统地执行设计程序,并包括适当的可获得且已通过测试的自动构造组件。
- 仿真;
同时从功能特征和构成 SRP/CS 元件的正确尺寸两方面对 SRP/CS 的设计进行系统和完整的检查。

G.4 SRP/CS 集成过程中避免系统性失效的措施

SRP/CS 集成过程中宜采用以下措施:

- 功能性测试;
- 方案管理;
- 文档。

另外,考虑到 SRP/CS 的复杂性及其 PL,宜采用黑盒测试法。

G.5 功能安全管理

宜为每个 SRP/CS 设计项目制定和记录一个功能安全计划,并宜根据需要进行更新。功能安全计划旨在针对不正确的规范、实施或修改问题提供预防措施。

功能安全计划宜识别相关活动(见表 4),并宜根据项目进行调整。

注 1: 功能安全计划可能是其他设计文档的一部分。

注 2: 功能安全计划的内容视具体情况而定,包括:

- 项目规模;
- 复杂程度;
- 设计和技术的新颖程度;
- 设计特征的标准化程度;
- 失效所带来的可能后果。

功能安全计划宜包含:

- a) 确认 SRP/CS 设计过程中的相关活动(规范、设计、集成、分析、测试、验证、确认)以及这些活动宜何时发生的详细信息;
- b) 确认执行和审查每项活动时所需的角色和资源;
- c) 确认硬件和软件设计过程中同发布、配置、归档和修改相关的程序;

- d) 建立确认计划(见 10.1.2);
- e) 在进行任何修改之前确认相关活动。

注 3: 以下情况可能要求修改:

- SRS 变更;
- 实际使用工况;
- 事件/事故经历;
- 加工材料的变化;
- 弃用;
- 修改机器或其操作模式。

宜分析修改请求所带来的影响,以确定其对安全功能的影响。

所有对 SRP/CS 产生影响且被接受的修改宜返回到硬件和/或软件的相关设计阶段(例如规范、设计、集成、安装、调试和确认)。所有后续阶段和管理程序宜根据本文件中为特定阶段而指定的程序进行。所有相关文档宜进行修订、修正和重新发布。

附录 H

(资料性)

多个子系统组合的示例

图 H.1 是提供一种控制机器致动器功能的安全相关部件的示意图。这不是功能/工作图,且仅用于证明在这一种功能中类别和技术的组合原则。

控制过程由电子控制逻辑和液压方向阀提供。风险由 AOPD 减小,AOPD 通过检测接近危险状况并在光束被遮断时阻止流体致动器的启动来减小风险。

提供安全功能的 SRP/CS 子系统包括:AOPD、电子控制逻辑单元、液压方向阀和互连方式。

这些组合子系统提供停止功能作为安全功能。AOPD 被遮断时,输出把信号传递至电子控制逻辑单元,电子控制逻辑单元提供信号给液压方向阀来停止液压流作为 SRP/CS 的输出。在机器上,它就停止了致动器的危险运动。

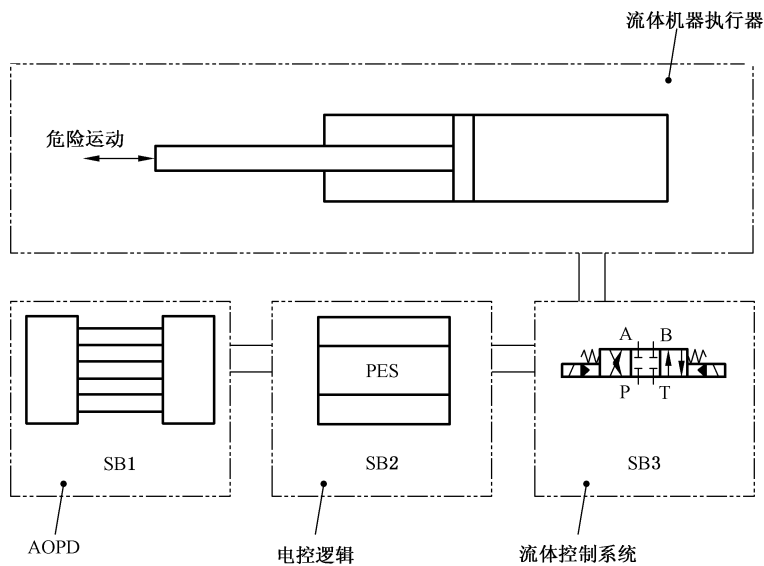
子系统的组合产生了一种安全功能,表现出符合第 6 章要求的不同类别和技术的组合。采用本文给出的原则,图 H.2 中的子系统能够作如下描述:

- 对于电敏保护装置(光幕):类别 2、PL c、PFH = 1.5×10^{-6} /h。为了减小故障发生的概率,该装置采用经验证的安全原则;
- 对于电子控制逻辑单元:类别 3、PL d、PFH = 2.0×10^{-7} /h。为了提高该电子控制逻辑单元的安全性能等级,子系统的结构采用冗余结构,并采用几种能检测大多数单一故障的故障检测方法;
- 对于液压方向阀:类别 1、PL c、PFH = 1.1×10^{-6} /h。经验证的状态主要取决于指具体应用。在本例中的阀可认为是经验证的。为了减小故障发生的概率,该装置由经验证的元件组成,采用经验证的安全原则,并考虑所有的应用条件(见 6.1.3.2.3)。

注 1: 还需考虑连接方式的位置、尺寸和布局。

本组合决定了总的 PFH = 2.8×10^{-6} /h,此值在 PL c 的范围内。连同 3 个子系统中最低的 PL 为 PL_{low} c,决定了总的性能等级为 PL c(见 6.2)。

注 2: 如果图 H.2 中类别 1 或类别 2 子系统发生一个故障,安全功能可能丧失。



标引序号说明：

AOPD —— 有源光电保护装置(如光幕)；

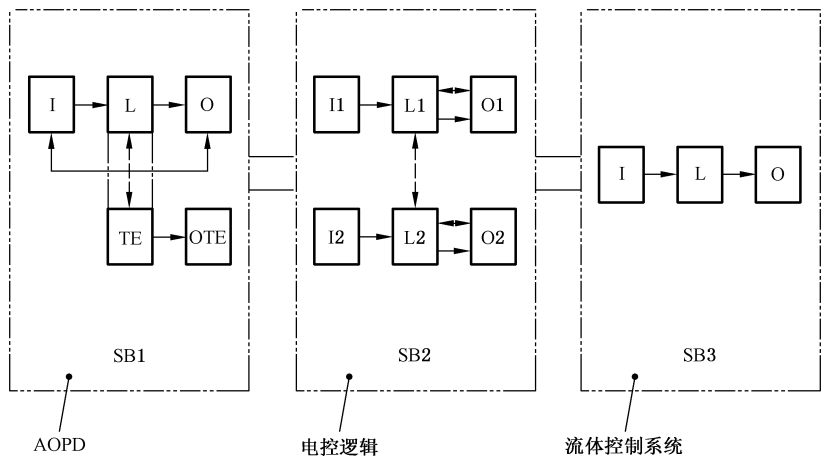
SB1 —— 类别 2(类型 2)、PL c；

SB2 —— 类别 3、PL d(电控逻辑)；

SB3 —— 类别 1、PL c(流体控制系统)；

PES —— 可编程电子系统。

图 H.1 示例——说明子系统组合的模块图



标引序号说明：

AOPD —— 有源光电保护装置(如光幕)；

I、I1、I2 —— 输入装置,例如:传感器；

L、L1、L2 —— 逻辑单元；

O、O1、O2、OTE —— 输出装置,例如:主接触器；

SB1 —— 类别 2(类型 2)、PL c；

SB2 —— 类别 3、PL d(电控逻辑)；

SB3 —— 类别 1、PL c(流体控制系统)；

TE —— 测试设备。

图 H.2 用指定架构替代图 H.1

附录 I

(资料性)

估算子系统 PL 的简化程序示例

I.1 概述

本附录说明了使用 6.1.8 给出的估算 PL 的简化程序,以及如何应用 6.1.8 和前面附录中给出的识别安全功能和确定 PL 的方法。本附录给出了两种控制回路的量化方式,迭代过程见图 4。

以下示例未考虑确保系统完整性、软件要求,以及正确应用基础和经经验证原则的措施。这些示例仅用于展示 $MTTF_D$ 、 DC_{avg} 、CCF、类别和对应 PL 的量化指标。

本附录分析了不同机器的控制回路的两个示例(A 和 B)(见图 I.1 和图 I.3)。两个示例都说明了防护门联锁的相同安全功能的性能,但由于用途不同, PL_r 也不同。第一个示例由 $MTTF_D$ 为中和高的机电元件组成一个通道,而第二个示例则由两个通道组成,一个为机电式,另一个为可编程电子式,由 $MTTF_D$ 为中和高的元件组成,并采用适当的诊断测试。

I.2 安全功能和所需性能等级(PL_r)

对于这两个示例,与防护门联锁相关的安全功能详细说明如下:

联锁防护门打开时,危险运动将停止(通过减速或切断电动机电源)。

注:对于示例 B,风险评估已确定由故障(SW2、CC 或 PLC)导致电动机减速失控是可接受的。

联锁防护和机器运动部件之间的最小距离根据机器停机性能按照 GB/T 19876—2012 确定。

对于示例 A,根据风险图法确定下列风险参数(见图 A.1):

——伤害的严重程度, $S=S2$,严重;

——暴露于危险的频率和/或时间, $F=F1$,很少和/或暴露时间短;

——避免危险的可能性, $P=P1$,特定条件下可能。

这些参数决定了所需性能等级为 PL_{rc} 。

首选类别的确定:通常, PL_c 可通过非常可靠的单通道系统(类别 1)、经测试的单通道系统(类别 2)或冗余架构(类别 3)实现(见图 12)。

对于示例 B,风险参数 $S2$ 和 $P1$ 与示例 A 相同,但暴露于危险的频率和/或时间, $F=F2$,频繁至连续和/或暴露时间长。

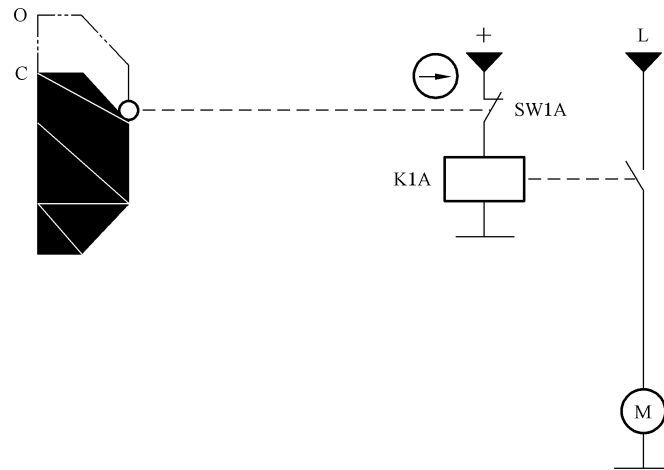
上述结论决定了所需性能等级为 PL_{rd} 。

首选类别的确定:通常, PL_d 可通过冗余架构(类别 2 或类别 3)实现(见图 12)。

I.3 示例 A——单通道系统

I.3.1 安全相关部分的识别

图 I.1 给出了影响联锁防护装置安全功能的所有部件。为了简化,省略了不影响安全功能的元件(例如启动和停止开关)。



标引序号说明：

- O —— 联锁防护装置打开；
- C —— 联锁防护装置未打开；
- M —— 电动机；
- K1A —— 接触器式继电器；
- SW1A —— 位置开关(NC)；
- L —— 电源；
- ⊕ —— 直接断开。

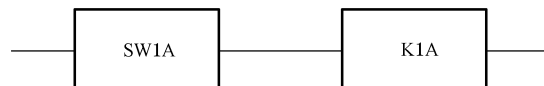
图 I.1 执行安全功能的控制回路 A

本示例中,采用直接断开动作并以强制致动模式工作的位置开关 SW1A,机械部件不能进行故障排除。位置开关连接到接触器式继电器 K1A,该接触器式继电器能切断电动机的电源。因此,这些 SRP/CS 的主要特征如下:

- 机电元件为单一通道；
- 位置开关 SW1A(NC)触点采用直接断开动作且 B_{10D} 为高；
- 接触器式继电器 K1A 的 B_{10D} 为高。

根据 GB/T 16855.2—2015,本例中的位置开关和接触器式继电器都是经验证的元件。

能由图 I.2 中的安全相关模块图来表示 SRP/CS。



标引序号说明：

- K1A —— 接触器式继电器；
- SW1A —— 位置开关。

图 I.2 识别示例 A 中安全相关部分的安全相关模块图

I.3.2 $MTTF_D$ 、 DC_{avg} 、防止共因失效的措施、类别以及 PL 的量化

假定 $MTTF_D$ 的值、 DC_{avg} 以及防止共因失效措施根据附录 C、附录 D、附录 E 和附录 F 来估计,或由制造商给出。类别根据 6.1.3 来估计。

—— $MTTF_D$

接触器式继电器 K1A 和位置开关 SW1A 对于单个通道的 $MTTF_D$ 有影响。假定制造商给出的值

为 $B_{10D,SW1A} = 20\,000\,000$ 次(位置开关不受负载影响)以及 $B_{10D,K1A} = 400\,000$ 个周期(接触器式继电器在最大负载下)。采用 C.4.2 的方法,取 220 天/年、每天工作 8 h 以及每次 60 min 的周期时间,得出 $MTTF_{D,SW1A} = 113\,636$ 年, $MTTF_{D,K1A} = 2\,273$ 年。根据 D.1 中的部件计数法,得出一个通道的 $MTTF_D$ 为:

$$\frac{1}{MTTF_D} = \frac{1}{MTTF_{D,SW1A}} + \frac{1}{MTTF_{D,SW1K}} = \frac{1}{113\,636 \text{ 年}} + \frac{1}{2\,273 \text{ 年}} = \frac{0.000\,45}{\text{年}} \quad \dots\dots (I.1)$$

由计算结果得出该通道的 $MTTF_D = 2\,222$ 年(限定为 100 年),或根据 6.1.4 中的表 5,该通道的 $MTTF_D$ 为高。

注:如果没有关于 SW1A 或 K1A 的 B_{10D} 信息,能根据 C.2 或 C.4 做出最坏情形的假设。

—— T_{10D}

C.4.2 给出的方法得出的 $T_{10D,SW1A}$ 为 11 364 年, $T_{10D,K1A}$ 为 227 年,两者均超出 20 年的任务时间,因此无需任何预防性更换。

——DC

控制回路 A 中未执行诊断测试,即 $DC=0$ 或“无”,同时仅使用一个通道,因此 DC 没有关联性。

——CCF

由于只使用了一个通道,因此不考虑 CCF 的防范措施。

——类别

满足类别 1 的特征(基本的和经验证的原则,经验证的元件),包括要求该通道的 $MTTF_D$ 为高。

图 12 中的输入数据:该通道的 $MTTF_D$ 为高(100 年), DC_{avg} 为无,类别为 1。

根据图 12,得出 PL_c 。

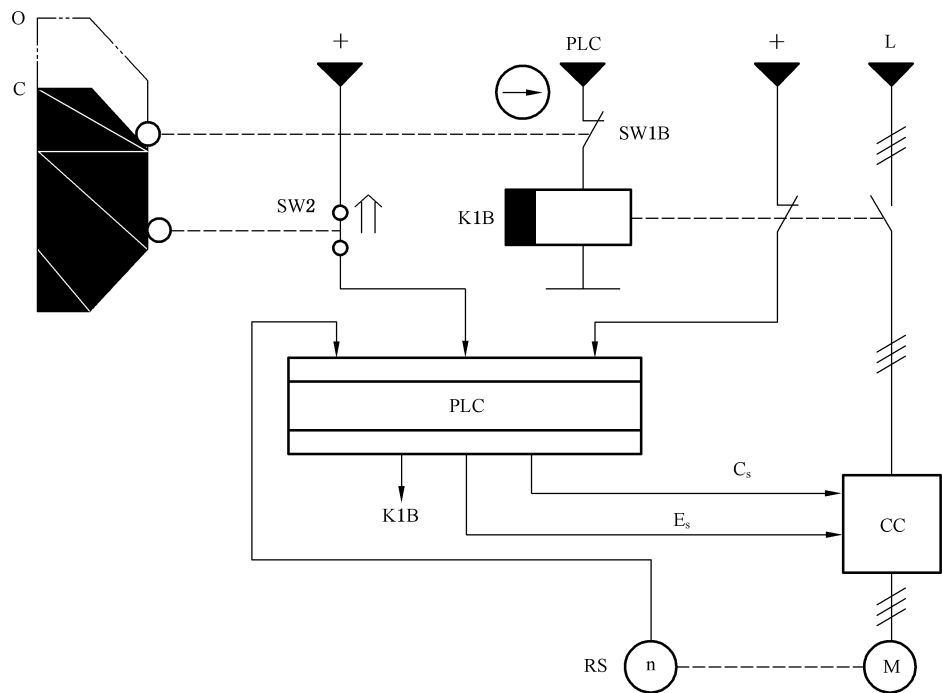
应用附录 K 得出 PFH 为 $1.14 \times 10^{-6}/h$ 和 PL_c 。

这个结果与 I.2 所需性能等级匹配。因此,控制电路 A 满足 I.2 应用示例 A 的风险减小要求,具体为 S2、F1、P1 和 PL_{rc} 。

I.4 示例 B——冗余系统

I.4.1 安全相关部分的识别

图 I.3 给出了所有影响联锁防护装置安全功能的部件。为了简化,省略了不影响安全功能的元件(例如启动和停止开关或 K1B 延时开关)。



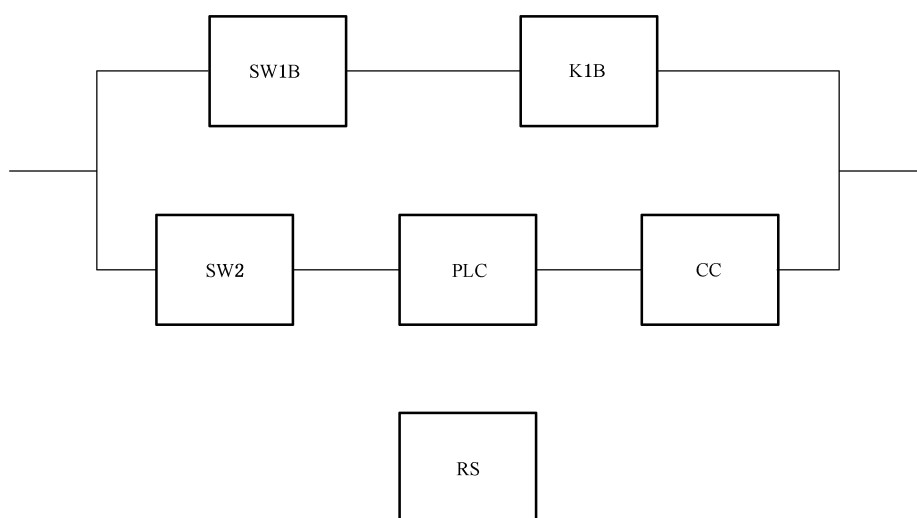
- 标引序号说明：
- | | | | |
|----------------|---------------|----------------|--------------|
| PLC | —— 可编程逻辑控制器； | E _s | —— 使能(标准的)； |
| CC | —— 换流器； | K1B | —— 接触器式继电器； |
| M | —— 电动机； | SW1B | —— 位置开关(NC)； |
| RS | —— 旋转传感器； | SW2 | —— 位置开关(NO)； |
| O | —— 联锁防护装置打开； | ⊖ | —— 直接断开； |
| C | —— 联锁防护装置未打开； | ↑↑ | —— 动作位置。 |
| L | —— 电源； | | |
| C _s | —— 停止功能(标准的)； | | |

图 I.3 执行安全功能的控制回路 B

在本示例中,采用双通道架构实现冗余。与示例 A 一样,第一个通道采用有直接断开动作的位置开关 SW1B,并以强制致动模式工作。这个位置开关与一个接触器式继电器 K1B 相连,该接触器式继电器可切断电动机的电源。第二个通道采用了可编程电子元件。第二个位置开关与可编程逻辑控制器相连接,能够控制换流器 CC 切断电动机电源。因此,这些 SRP/CS 的主要特征如下:

- 冗余通道,一个为机电元件通道,另一个为可编程电子元件通道;
- 只有位置开关 SW1B(NC)具有直接断开动作触点,但两个位置开关 SW1B 和 SW2 的 B_{10D} 均为高;
- 接触器式继电器 K1B 的 $MTTF_D$ 为高;
- 电子元件 PLC 和 CC 的 $MTTF_D$ 为中;
- PLC 的安全相关应用软件(SRASW),例如软件与监控输入信号 SW2、K1B、RS 以及去往换流器的输出指令相关的部分,均按 7.3 编制规范、设计和验证,实现 $PL_r d$ 。

SRP/CS 及其通道的划分可由图 I.4 中的安全相关功能模块图来表示。因此,第一个通道由 SW1B 和 K1B 组成,第二个通道由 SW2、PLC 和 CC 组成,而 RS 只用于测试换流器。



标引序号说明：

SW1B ——位置开关；

K1B ——接触器式继电器；

SW2 ——位置开关；

PLC ——可编程逻辑控制器；

CC ——换流器；

RS ——旋转传感器。

图 I.4 识别示例 B 中安全相关部分的模块图

I.4.2 每个通道 $MTTF_D$ 、 DC_{avg} 、防止共因失效的措施、类别以及 PL 的量化

假定每个通道 $MTTF_D$ 的值、 DC_{avg} 以及防止共因失效的措施根据附录 C、附录 D、附录 E 和附录 F 来估计，或由制造商给出。类别则根据 6.1.3 来估计。

开关 SW1B 具有直接断开动作并以强制致动模式工作，但机械部件未进行故障排除证明。

—— $MTTF_D$

位置开关 SW1B 和接触器式继电器 K1B 对于第一个通道的 $MTTF_{D,C1}$ 有影响。假定制造商给出的值为 $B_{10D,SW1B} = 20\,000\,000$ 次（位置开关不受负载影响）以及 $B_{10D,K1B} = 400\,000$ 次（接触器式继电器在最大负载下）。采用 C.4.2 的方法，取工作 300 天/年、每天工作 16 h 以及每次 4 min 的周期时间，得出 $MTTF_{D,SW1B} = 2\,778$ 年， $MTTF_{D,K1B} = 56$ 年。根据 D.1 中的部件计数法，得出第一个通道的 $MTTF_{D,C1}$ 为：

$$\frac{1}{MTTF_{D,C1}} = \frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} = \frac{1}{2\,778 \text{ 年}} + \frac{1}{56 \text{ 年}} = \frac{0.0182}{\text{年}} \quad \dots\dots (I.2)$$

由计算结果得出该通道的 $MTTF_D = 55$ 年，根据 6.1.4 中的表 6，该通道的 $MTTF_D$ 为高。

在第二个通道中，SW2、PLC 和 CC 对 $MTTF_{D,C2}$ 有影响。假设制造商给出的 $B_{10D,SW2}$ 为 1 000 000 个周期。与第一个通道相同，采用 C.4.2 的方法，得出的 $MTTF_{D,SW2}$ 为 139 年。假设制造商给出的 PLC 和 CC 的 $MTTF_D$ 为 20 年。采用 D.1 中的部件计数法得出第二个通道的 $MTTF_{D,C2}$ 为：

$$\frac{1}{MTTF_{D,C2}} = \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}} = \frac{1}{139 \text{ 年}} + \frac{1}{20 \text{ 年}} + \frac{1}{20 \text{ 年}} = \frac{0.1072}{\text{年}} \quad \dots\dots (I.3)$$

由计算结果导出该通道的 $MTTF_D = 9.3$ 年，根据 6.1.4 的表 6，该通道的 $MTTF_D$ 为低。

注：如果没有关于 SW1B、SW2 或 K1B 的 B_{10D} 信息，可根据 C.2 或 C.4 做出最坏情形的假设。

由于这两个通道具有不同的 $MTTF_D$ ，公式 D.2 可用来计算对称双通道系统的 $MTTF_D$ 的等效等同值。此公式计算出的 $MTTF_D = 37$ 年，或根据 6.1.4 中的表 6，通道的 $MTTF_D$ 为高。

—— T_{10D}

C.4.2 给出的方法得出的 $T_{10D,SW1B}$ 为 278 年、 $T_{10D,K1B}$ 为 5.5 年、 $T_{10D,SW2}$ 为 13.9 年,后两个低于 20 年的任务时间。因此,只有 K1B 在工作满 5.5 年之前更换,SW2 在工作满 13.9 年之前更换,PL 和 PFH 的估计才有效。

——DC

在控制电路 B 中,由 PLC 测试 5 个 SRP/CS;SW1、SW2 和 K1B 的测试由 PLC 读回,CC 的测试则由 PLC 经由 RS 读回,PLC 执行自检。每个被测部件相关的 DC 为:

- a) $DC_{SW1B} = DC_{SW2} = 99\%$,“高”,原因为真实性检查,见表 E.1(输入装置部分的第 2 行);
- b) $DC_{K1B} = 99\%$,“高”,原因为常开和常闭机械连接式触点,见表 E.1(输入装置部分的第 2 行);
- c) $DC_{PLC} = 30\%$,“无”,原因为自检效率低(该值由特定应用得出);
- d) $DC_{CC} = 90\%$,“中”,原因为由控制逻辑单元对致动器进行间接监测,见表 E.1(输出装置部分的第 6 行)——如果 PLC 监控到 CC 的失效,则可由使能装置(标准的)停止运动并断开接触器式继电器 K1B(额外的切断路径)。

对于 PL 的估计,需要一个按照公式(I.4)计算得出平均 DC 值(DC_{avg})作为图 12 中的输入:

$$DC_{avg} = \frac{\frac{DC_{SW1B}}{MTTF_{D,SW1B}} + \frac{DC_{K1B}}{MTTF_{D,K1B}} + \frac{DC_{SW2}}{MTTF_{D,SW2}} + \frac{DC_{PLC}}{MTTF_{D,PLC}} + \frac{DC_{CC}}{MTTF_{D,CC}}}{\frac{1}{MTTF_{D,SW1B}} + \frac{1}{MTTF_{D,K1B}} + \frac{1}{MTTF_{D,SW2}} + \frac{1}{MTTF_{D,PLC}} + \frac{1}{MTTF_{D,CC}}} =$$

$$\frac{\frac{0.99}{2\,778} + \frac{0.99}{56} + \frac{0.99}{139} + \frac{0.3}{20} + \frac{0.9}{20}}{\frac{1}{2\,778} + \frac{1}{56} + \frac{1}{139} + \frac{1}{20} + \frac{1}{20}} = \frac{0.99}{0.13} = 67.9\% \quad \dots\dots\dots (I.4)$$

因此,得出 DC_{avg} 为低。

——CCF

表 I.1 给出了根据 F.2 对控制电路 B 进行防止 CCF 措施估计的得分。

表 I.1 示例 B 中防止 CCF 方法的估计

编号	条目	实施方法	控制回路的得分	最大可能得分
1	分离/隔离			
—	信号路径之间的物理分离	——将 SW1B 和 SW2 单独接线到 PLC(信号线单独接线); ——将用以诊断测试的两个通道交叉连接	15	15
2	相异			
—	采用不同技术/设计或物理原则	——位置开关 SW1B 在安全防护装置打开时运行,并使用直接打开动作的断开触点元件,而位置开关 SW2 在安全防护装置关闭时运行,并使用闭合触点元件; ——一个功能通道使用机电元件,另一个功能通道使用可编程电子元件	20	20

表 I.1 示例 B 中防止 CCF 方法的估计 (续)

编号	条目	实施方法	控制回路的得分	最大可能得分
3	设计/应用/经验			
3.1	防止过电压、过压力、过电流、过温等的保护	——在需要时使用外部保护元件提供系统级的额外过电压和过电流保护。例如,二极管、输入和输出侧的保险丝以及继电器 K1B 上的续流二极管; ——PLC 中的过电压和欠电压检测	15	15
3.2	所用的元件是经验证的	开关 SW1B 和继电器 K1B 是经验证的组件	无(仅部分满足,见 F.2)	5
4	评估/分析			
—	为了避免共因失效,设计中对 SRP/CS 的每个部件进行了失效模式和影响分析并考虑其结果	未完全实现(以 CCF 为重点的 FMEA 已经实施,但没有以正式和完整记录的方式进行)	无	5
5	能力/培训			
—	设计者接受了培训,以理解共因失效的原因和结果	未完全实现	无	5
6	环境			
6.1	电气/电子系统:根据适当的标准(例如 IEC 61326-3-1),通过防止污染和 EMI 来防止 CCF	——使用外部保护元件对系统级电磁干扰提供额外保护。例如,所有输入和输出侧的二极管、保险丝、滤波器和屏蔽层(表 L.1 的适当措施以 CCF 为重点实施); ——信号线和电源线分开布线	25	25
6.2	其他影响:已考虑了对所有环境因素,例如温度、冲击、振动、湿度等(例如:相关标准中所规定的)的抗扰性要求	——选择两个位置开关以经受所有预期的环境影响,并充分考虑可能的 CCF 原因; ——K1B、PLC 和 CC 安装在具有温度控制功能的机柜中	10	10
总和			85	最大 100

足够防止 CCF 的措施要求最低得分为 65。在示例 B 中,85 分足以满足防止 CCF 的要求。

满足类别 3 的特征,因为:任何部件中的单一故障不会导致安全功能的丧失;只要合理可行,单一故障能够在下一次要求安全功能之时或之前被检测到;平均诊断覆盖率(DC_{avg})为 60%~90%;防止 CCF 的措施足够且每个通道的等效 $MTTF_D$ 为高。

图 12 中的输入数据为:通道的 $MTTF_D$ 为高(37 年), DC_{avg} 为低,类别为 3。

根据图 12,得出 PL d。

应用附录 K(用 36 年)得出 PFH 为 $5.16 \times 10^{-7}/h$ 和 PL d。

该结果与 I.2 中所需性能等级 PL_r d 匹配。因此,控制电路 B 满足 I.2 的应用示例 B 对风险减小的要求,具体为 S2、F2、P1 和 PL_r d。

附 录 J
(资料性)
软件

J.1 示例描述

本附录介绍了用于实现 PL_r d 的 SRP/CS 的 SRESW 的过程步骤。该 SRP/CS 与机器设备通过接口连接。它确保了：

- 获得各种传感器发出的信息；
- 用于操纵功率控制元件满足安全要求所需的处理；
- 功率控制元件的导向。

本应用中,功能块层级上的 SRESW 的设计如图 J.1 所示。

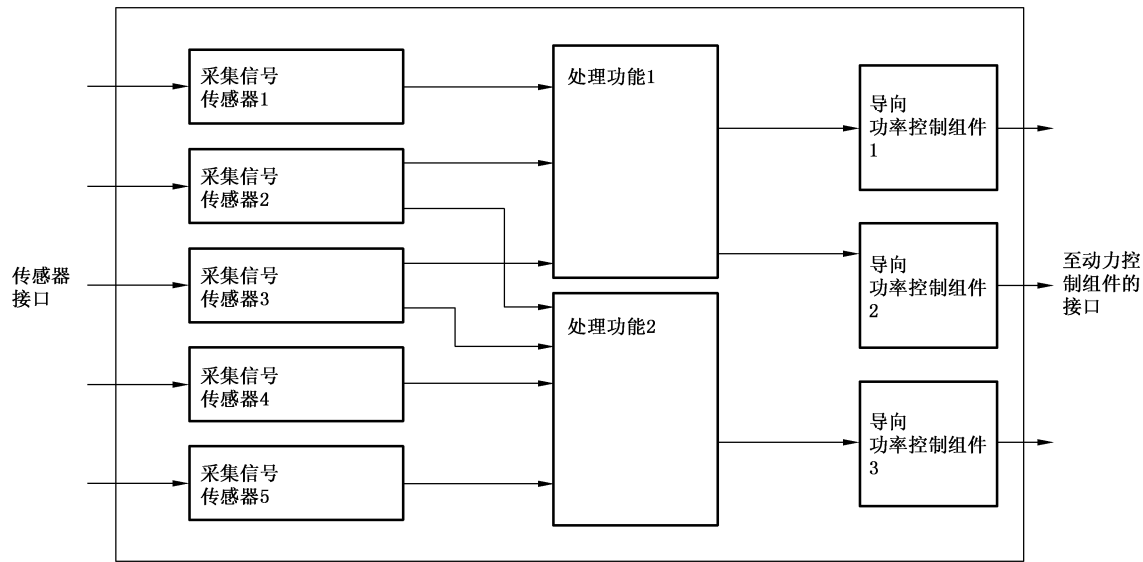


图 J.1 功能块层级的软件设计示例

J.2 软件安全生命周期 V 模型的应用

表 J.1 列出了开发活动及其相应的验证步骤,以及相关的文件。这些活动遵循图 14 a)中软件安全生命周期的 V 模型。

表 J.1 软件安全生命周期内的活动和文件

开发活动	验证活动	相关文件
机器方面(硬件及软件): ——识别涉及 SRP/CS 的功能	——识别安全相关功能	输出: ——安全要求规范(SRS)
架构方面(硬件及软件): ——确定带传感器和功率控制元件的控制架构	——所选元件安全特征的备注 ——计划 SRS 的测试	输出: ——控制架构的定义 ——SRS 的测试计划

表 J.1 软件安全生命周期内的活动和文件（续）

开发活动	验证活动	相关文件
软件规范方面： ——识别涉及 SRP/CS 的功能安全相关软件（SSRS）的要求规范，包括： ——将机器功能转换为软件功能	——对照 SRS 审查 SSRS 的描述（见 J.3） ——对照 SRS 计划 SSRS 的测试	输入： ——安全要求规范（SRS） 输出： ——包括软件描述的软件设计规范（SDS） ——SDS 的测试计划 ——审查活动的文件
软件架构方面： ——软件系统设计，包括将各种功能细分到功能块中	——对照 SDS 审查系统设计，包括确定关键模块，这些模块需要更多的审查和验证工作 ——计划软件系统设计的测试	输入： ——SDS 输出： ——包括功能块建模的软件系统设计规范（SSDS） ——SSDS 的测试计划 ——审查活动的文件
编码方面： 根据编程规则编写非已有软件模块代码（见 J.4）	——对照 MDS 审查代码 ——验证功能及合规性	输入： ——MDS 输出： ——包括代码中编码注释的经审查的代码 ——审查活动的文件
确认方面： ——模块测试	根据 MDS 测试计划，对照 MDS 测试软件模块，包括： ——验证测试覆盖范围 ——验证测试结果	输入： ——经审查的代码 ——MDS ——MDS 的测试计划 输出： ——经测试的软件模块 ——测试活动的文件
确认方面： ——软件集成测试	根据 SSDS 测试计划，对照 SSDS 测试集成的软件，包括： ——验证测试覆盖范围 ——验证测试结果 测试可能包括最终的硬件（如可能）	输入： ——经测试的软件模块 ——SSDS ——SSDS 的测试计划 输出： ——经测试的集成 ——测试活动的文件
确认方面： ——SRP/CS 确认 制作测试场景： ——功能运行方面 ——失效行为方面	根据 SDS 测试计划，对照 SDS 测试集成的软件和硬件（SRP/CS），包括： ——验证测试覆盖范围 ——验证测试结果 测试可能包括最终的硬件（如可能）	输入： ——SDS ——SDS 的测试计划 输出： ——经确认的（SRP/CS）软件 ——测试活动的文件
注：每个测试计划包括： ——交叉引用规范段落和测试的对照矩阵； ——包括测试场景和测试结果及备注的测试表。		

J.3 不同层面上软件规范的验证(即 SDS、SSDS、MDS)

根据图 14 a),作为软件安全生命周期的一部分,在软件规范的每个层面上包括阅读规范的验证活动,用于验证所有的敏感点都得到了正确的描述。在验证每种功能时,宜考虑以下方面:

- 限制软件规范错误解释的情况;
- 避免技术规范中出现导致 SPR/CS 产生预先未知行为的漏洞;
- 准确地规定用于激活和停用功能的条件;
- 明确保证所有可能的情况都已处理;
- 一致性测试;
- 不同的参数化情况;
- 失效后的反应。

J.4 编程规则示例

一般来说,宜能识别软件的版本。修改宜以作者、日期和修改类型的形式被记录。关于编程规则,能分为以下规则。

a) 程序结构层面上的编程规则

宜结构化编程,以显示一致和易懂的总体框架,便于定位不同的处理。这意味着:

- 1) 对典型程序或功能块使用模板;
- 2) 为了识别对应于“输入”“处理”和“输出”的主要组成部分,将程序分段;
- 3) 宜对源程序中的每段程序进行注释,以便于修改后更新注释;
- 4) 调用一个功能块时,描述该模块的作用;
- 5) 宜使用单一种类数据类型的存储地址,并以唯一的标签加以标识;
- 6) 工作顺序不宜依赖变量,例如:程序运行时计算出的跳转地址,经授权的条件跳转。

b) 关于使用变量的编程规则

- 1) 任何输出的激活或停用宜只发生一次(集中条件);
- 2) 程序宜结构化以使更新一个变量的等式集中化;
- 3) 每个全局变量、输入或输出宜具有一个显式助记符名称,并应在源程序中通过一个注释对其进行描述。

c) 功能块层的编程规则

- 1) 宜使用经 SRP/CS 供应商确认的功能块,宜检查这些经确认的模块假定工作条件是否符合程序的条件;
- 2) 代码块的大小宜限制在以下指导值:
 - 参数——最大 8 位数、2 个整形输入和 4 个输出;
 - 功能代码内——最大 10 个局部变量、最大 20 个布尔等式。
- 3) 功能块不宜修改全局变量;
- 4) 每个值都宜与预期的预先设定的基准进行比较,以确保其有效性;
- 5) 宜检查一个功能块的输入参数是否不一致;
- 6) 每个故障代码都宜是可查的,并能清楚地识别原始故障;
- 7) 宜通过注释来描述故障检测后的故障代码和模块状态;
- 8) 宜通过注释来描述模块的复位或正常状态的恢复。

附 录 K
(资料性)

图 12 的数值表示

图 12 的数值表示见表 K.1。

表 K.1 图 12 的数字表示

每个通道的 MTTF _D 年	每小时危险失效平均频率 PFH(1/h)及对应的性能等级 PL						
	Cat.B DC _{avg} = 无	Cat.1 DC _{avg} = 无	Cat.2 DC _{avg} = 低	Cat.2 DC _{avg} = 中	Cat.3 DC _{avg} = 低	Cat.3 DC _{avg} = 中	Cat.4 DC _{avg} = 高
3	3.80×10 ⁻⁵ a	—	2.58×10 ⁻⁵ a	1.99×10 ⁻⁵ a	1.26×10 ⁻⁵ a	6.09×10 ⁻⁶ b	—
3.3	3.46×10 ⁻⁵ a	—	2.33×10 ⁻⁵ a	1.79×10 ⁻⁵ a	1.13×10 ⁻⁵ a	5.41×10 ⁻⁶ b	—
3.6	3.17×10 ⁻⁵ a	—	2.13×10 ⁻⁵ a	1.62×10 ⁻⁵ a	1.03×10 ⁻⁵ a	4.86×10 ⁻⁶ b	—
3.9	2.93×10 ⁻⁵ a	—	1.95×10 ⁻⁵ a	1.48×10 ⁻⁵ a	9.37×10 ⁻⁶ b	4.40×10 ⁻⁶ b	—
4.3	2.65×10 ⁻⁵ a	—	1.76×10 ⁻⁵ a	1.33×10 ⁻⁵ a	8.39×10 ⁻⁶ b	3.89×10 ⁻⁶ b	—
4.7	2.43×10 ⁻⁵ a	—	1.60×10 ⁻⁵ a	1.20×10 ⁻⁵ a	7.58×10 ⁻⁶ b	3.48×10 ⁻⁶ b	—
5.1	2.24×10 ⁻⁵ a	—	1.47×10 ⁻⁵ a	1.10×10 ⁻⁵ a	6.91×10 ⁻⁶ b	3.15×10 ⁻⁶ b	—
5.6	2.04×10 ⁻⁵ a	—	1.33×10 ⁻⁵ a	9.87×10 ⁻⁶ b	6.21×10 ⁻⁶ b	2.80×10 ⁻⁶ c	—
6.2	1.84×10 ⁻⁵ a	—	1.19×10 ⁻⁵ a	8.80×10 ⁻⁶ b	5.53×10 ⁻⁶ b	2.47×10 ⁻⁶ c	—
6.8	1.68×10 ⁻⁵ a	—	1.08×10 ⁻⁵ a	7.93×10 ⁻⁶ b	4.98×10 ⁻⁶ b	2.20×10 ⁻⁶ c	—
7.5	1.52×10 ⁻⁵ a	—	9.75×10 ⁻⁶ b	7.10×10 ⁻⁶ b	4.45×10 ⁻⁶ b	1.95×10 ⁻⁶ c	—
8.2	1.39×10 ⁻⁵ a	—	8.87×10 ⁻⁶ b	6.43×10 ⁻⁶ b	4.02×10 ⁻⁶ b	1.74×10 ⁻⁶ c	—
9.1	1.25×10 ⁻⁵ a	—	7.94×10 ⁻⁶ b	5.71×10 ⁻⁶ b	3.57×10 ⁻⁶ b	1.53×10 ⁻⁶ c	—
10	1.14×10 ⁻⁵ a	—	7.18×10 ⁻⁶ b	5.14×10 ⁻⁶ b	3.21×10 ⁻⁶ b	1.36×10 ⁻⁶ c	—
11	1.04×10 ⁻⁵ a	—	6.44×10 ⁻⁶ b	4.53×10 ⁻⁶ b	2.81×10 ⁻⁶ c	1.18×10 ⁻⁶ c	—
12	9.51×10 ⁻⁶ b	—	5.84×10 ⁻⁶ b	4.04×10 ⁻⁶ b	2.49×10 ⁻⁶ c	1.04×10 ⁻⁶ c	—
13	8.78×10 ⁻⁶ b	—	5.33×10 ⁻⁶ b	3.64×10 ⁻⁶ b	2.23×10 ⁻⁶ c	9.21×10 ⁻⁷ d	—
15	7.61×10 ⁻⁶ b	—	4.53×10 ⁻⁶ b	3.01×10 ⁻⁶ b	1.82×10 ⁻⁶ c	7.44×10 ⁻⁷ d	—
16	7.13×10 ⁻⁶ b	—	4.21×10 ⁻⁶ b	2.77×10 ⁻⁶ c	1.67×10 ⁻⁶ c	6.76×10 ⁻⁷ d	—
18	6.34×10 ⁻⁶ b	—	3.68×10 ⁻⁶ b	2.37×10 ⁻⁶ c	1.41×10 ⁻⁶ c	5.67×10 ⁻⁷ d	—
20	5.71×10 ⁻⁶ b	—	3.26×10 ⁻⁶ b	2.06×10 ⁻⁶ c	1.22×10 ⁻⁶ c	4.85×10 ⁻⁷ d	—
22	5.19×10 ⁻⁶ b	—	2.93×10 ⁻⁶ c	1.82×10 ⁻⁶ c	1.07×10 ⁻⁶ c	4.21×10 ⁻⁷ d	—
24	4.76×10 ⁻⁶ b	—	2.65×10 ⁻⁶ c	1.62×10 ⁻⁶ c	9.47×10 ⁻⁷ d	3.70×10 ⁻⁷ d	—
27	4.23×10 ⁻⁶ b	—	2.32×10 ⁻⁶ c	1.39×10 ⁻⁶ c	8.04×10 ⁻⁷ d	3.10×10 ⁻⁷ d	—
30	—	3.80×10 ⁻⁶ b	2.06×10 ⁻⁶ c	1.21×10 ⁻⁶ c	6.94×10 ⁻⁷ d	2.65×10 ⁻⁷ d	9.54×10 ⁻⁸ e
33	—	3.46×10 ⁻⁶ b	1.85×10 ⁻⁶ c	1.06×10 ⁻⁶ c	5.94×10 ⁻⁷ d	2.30×10 ⁻⁷ d	8.57×10 ⁻⁸ e
36	—	3.17×10 ⁻⁶ b	1.67×10 ⁻⁶ c	9.39×10 ⁻⁷ d	5.16×10 ⁻⁷ d	2.01×10 ⁻⁷ d	7.77×10 ⁻⁸ e

表 K.1 图 12 的数字表示 (续)

每个通道的 MTTF _D 年	每小时危险失效平均频率 PFH(1/h) 及对应的性能等级 PL						
	Cat.B DC _{avg} = 无	Cat.1 DC _{avg} = 无	Cat.2 DC _{avg} = 低	Cat.2 DC _{avg} = 中	Cat.3 DC _{avg} = 低	Cat.3 DC _{avg} = 中	Cat.4 DC _{avg} = 高
39	—	2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43	—	2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47	—	2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51	—	2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56	—	2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62	—	1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68	—	1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75	—	1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82	—	1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91	—	1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.94×10^{-8} e	2.74×10^{-8} e
100	—	1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e
110							2.23×10^{-8} e
120							2.03×10^{-8} e
130							1.87×10^{-8} e
150							1.61×10^{-8} e
160							1.50×10^{-8} e
180							1.33×10^{-8} e
200							1.19×10^{-8} e
220	—	—	—	—	—	—	1.08×10^{-8} e
240							9.81×10^{-9} e
270							8.67×10^{-9} e
300							7.76×10^{-9} e
330							7.04×10^{-9} e
360							6.44×10^{-9} e
390							5.94×10^{-9} e
430							5.38×10^{-9} e
470							4.91×10^{-9} e
510							4.52×10^{-9} e
560							4.11×10^{-9} e
620							3.70×10^{-9} e
680							3.37×10^{-9} e
750							3.05×10^{-9} e

表 K.1 图 12 的数字表示 (续)

每个通道的 MTTF _D 年	每小时危险失效平均频率 PFH(1/h)及对应的性能等级 PL						
	Cat.B DC _{avg} = 无	Cat.1 DC _{avg} = 无	Cat.2 DC _{avg} = 低	Cat.2 DC _{avg} = 中	Cat.3 DC _{avg} = 低	Cat.3 DC _{avg} = 中	Cat.4 DC _{avg} = 高
820							2.79×10 ⁻⁹ e
910							2.51×10 ⁻⁹ e
1000							2.28×10 ⁻⁹ e
1100							2.07×10 ⁻⁹ e
1200							1.90×10 ⁻⁹ e
1300							1.75×10 ⁻⁹ e
1500	—	—	—	—	—	—	1.51×10 ⁻⁹ e
1600							1.42×10 ⁻⁹ e
1800							1.26×10 ⁻⁹ e
2000							1.13×10 ⁻⁹ e
2200							1.03×10 ⁻⁹ e
2300							9.85×10 ⁻¹⁰ e
2400							9.44×10 ⁻¹⁰ e
2500							9.06×10 ⁻¹⁰ e
<p>注 1: 如果类别 2 的要求率小于或等于测试率的 1/25(见 6.1.8), 则表 K.1 所述类别 2 的 PFH_D 值乘以 1.1 的系数用作最坏情况的估计值。</p> <p>注 2: 根据以下 DC_{avg} 计算 PFH_D 值:</p> <p>——DC_{avg} = 低, 用 60% 计算;</p> <p>——DC_{avg} = 中, 用 90% 计算;</p> <p>——DC_{avg} = 高, 用 99% 计算。</p>							

附 录 L
(资料性)
电磁干扰(EMI)抗扰度

以下途径为 SRP/CS 或子系统的 EMI 抗扰措施提供了指导(见图 L.1)。

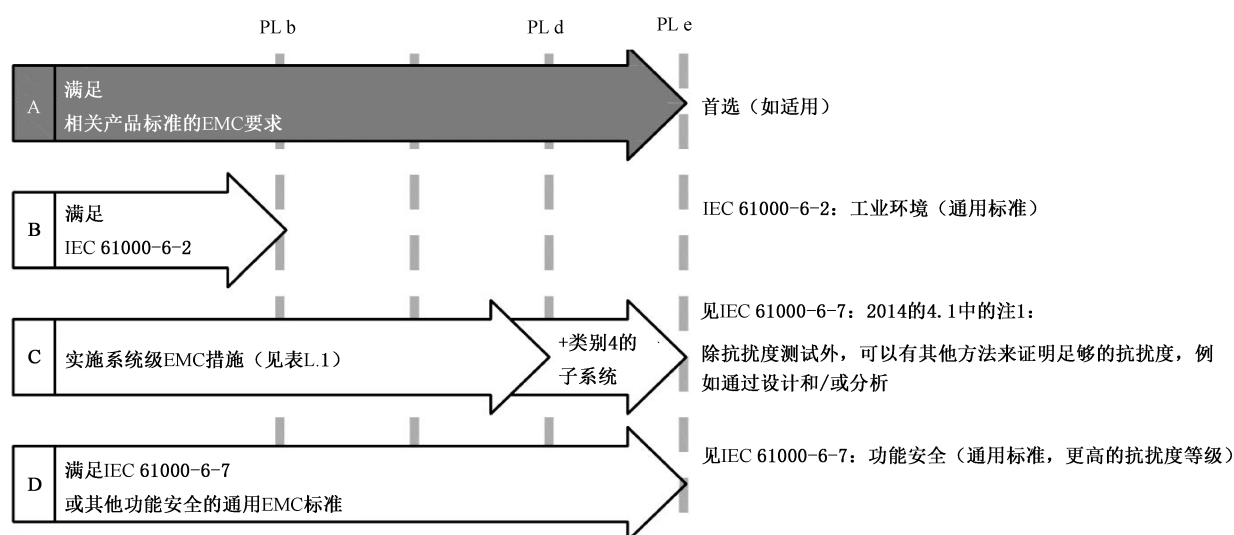


图 L.1 实现 EMI 措施的途径

宜至少选择一条或多条途径并完全应用：

- 途径 A: 满足相关产品标准的 EMI 要求(见 IEC 61000-6-7:2014 中 4.1 的第 1 句)。产品标准示例为 IEC 61800-5-2:2016；
- 途径 B: 对于 PL_r a 和 b, 满足 IEC 61000-6-2 的 EMI 要求；
- 途径 C: 根据表 L.1(见 IEC 61000-6-7:2014 中 4.1 的注 1), 对于任何 PL_r 实施 EMI 措施, 双通道子系统(类别 2、类别 3 和类别 4)最低得分为 280(最大可能得分为 390), 单通道子系统(类别 B 和类别 1)最低得分为 230。对于 PL_r e, 只有在额外满足类别 4 要求的情况下, 才能应用该途径；
- 途径 D: 满足 IEC 61000-6-7 或 IEC 61326-3-1 功能安全通用 EMI 标准的要求。

对于具有集成有源电子器件的机电部件, 宜分析 EMI 对执行安全功能的影响, 并宜采取相关措施实现 EMI。如果选择了途径 C, 宜根据其避免或控制 EMI 的有效性来评估表 L.1 中列出的措施。工程判断宜证明(例如使用 FMEA 技术)EMI 的典型原因已尽可能减少。宜清楚记录所选途径/措施, 并提供符合所选途径的充分证据。

如果用测试进行验证, 则宜确保安全功能得到执行, 并在 EMI 环境暴露足够的时间, 以证明其不敏感。

表 L.1 SRP/CS 或子系统实现 EMI 抗扰度的措施

实现 EMI 抗扰度的措施	得分 ^a
安全相关传感器及其线束	
IEC 60204-1:2016+AMD1:2021 中附录 H 和/或 IEC 61800-3 中所述措施的应用 [hr]	10

表 L.1 SRP/CS 或子系统实现 EMI 抗扰度的措施 (续)

实现 EMI 抗扰度的措施	得分 ^a
安全相关传感器及其线束	
模拟电压信号,角度编码器 传感器和安全相关输入/输出信号使用屏蔽且接地的和/或绞合的线缆(电缆屏蔽层在靠近元件处实现全方位且平滑的低阻抗接触)[hr]	20
元件之间的低压直流线束和接线采用双绞线	10
安全相关 I/O 系统(集中、分散或集成在 PLC 中)	
安装于屏蔽且等电位连接的机柜中或元件安装于屏蔽且等电位连接的外壳中 [hr]	20
控制系统和/或特定元件分区 ^b ,例如: a) 主电源和配电; b) 强干扰源,如电源滤波器、电源扼流圈、加热元件、大功率电源和电动机电缆; c) 敏感组件,如低压电源、PLC、数据总线、传感器和低压致动器。 [hr]	20
PLC 作为 SRP/CS 的一部分	
安装于屏蔽且等电位连接的机柜中或元件安装于屏蔽且等电位连接的外壳中	10
PL _r d 或 e,类别 3 或类别 4,同一外壳中的不同 PLC,按照制造商的安装说明间隔足够距离	10 ^{c,d}
PL _r d 或 e,类别 3 或类别 4,不同外壳中的冗余 PLC	20 ^{c,d}
PL _r d 或 e,类别 3 或类别 4,不同通道(例如 PLC 和离散逻辑)或使用安全 PLC	20 ^{c,d}
安全相关执行器及其线束	
IEC 60204-1;2016+AMD1:2021 中附录 H 中所述措施的应用和/或 IEC 61800-3 的使用 [hr]	20
具有相关干扰等级的其他部件和接线	
电动机和逆变器之间的电动机屏蔽等电位连接电缆或正弦波滤波器,或根据制造商的安装说明适当地采取等效措施 [hr]	20
根据制造商的安装说明适当地为安全相关输入信号提供射频滤波器、过压和瞬态保护(如滤波器、瞬态电压抑制二极管、光耦合器、铁氧体) [hr]	20
(根据制造商的安装说明或专门应用的)主电源的 EMI 滤波器(如过电压和瞬态保护)	20
IEC 60204-1;2016+AMD1:2021 中附录 H 所述措施的应用和/或 IEC 61800-3 的使用	10
工程、编程、培训、现场观察	
所有部件至少满足 EMI 通用标准 IEC 61000-6-2(制造商文件中提到)的要求[hr]	30
EMI 的风险分析(见表 L.2 中的示例)和风险评估的最终报告	20
不同的冗余通道(见注释)	20 ^e
EMI 源和敏感元件分离,例如: ——电源线和信号线的布线和位置分开; ——电力电子设备和低功率电子设备的金属柜分开; ——遵循制造商的说明;如果没有可用的说明,功率元件和敏感元件之间的距离 ≥ 20 cm,或在根据现场经验评估为低 EMI 影响的短距离内使用屏蔽和等电位连接元件	30

表 L.1 SRP/CS 或子系统实现 EMI 抗扰度的措施（续）

实现 EMI 抗扰度的措施		得分 ^a
工程、编程、培训、现场观察		
具有组件或系统级诊断功能的软件/固件,例如通过真实性检查、冗余情况下的数据交叉监控、自检		20
有经验或受过培训(具有培训文件,如培训证书),理解 EMI 的原因和后果的设计师		20
特定功能安全系统设计的再用,该设计曾用于类似的电磁环境,并具有高可靠性,没有已知的 EMI 问题		30
SRP/CS 的电源		
符合 IEC 61558-2-16 要求的隔离变压器产生的低压交流或直流电源,和/或符合 IEC 60950-1、IEC 62368-1 要求的 SELV 电源和/或符合 EN 50178 要求的 SELV 或 PELV 电源		20
SRP/CS 的通道 1/2 使用的冗余 PLC 采用独立的开关电源		10 ^c
总得分 390(单通道子系统为 320)	EMI 抗扰度措施 ^a	
280(单通道子系统为 230 或更高)	满足要求	
低于 280(单通道子系统为 230)	不合格⇒选择额外的措施或选择上述途径的一条或多条	
注:表 L.1 中的双通道是指类别 2 的功能通道和测试通道,或类别 3 和类别 4 的冗余功能通道。		
<p>^a 与技术措施无关时,在综合计算中可以考虑附加于本栏的分值。</p> <p>^b 分区可以位于一个机柜内,也可以分为多个机柜。</p> <p>^c 与单通道子系统无关的要求。</p> <p>^d PLC 作为 SRP/CS 的一部分,其分数只能在每个 SRP/CS 分配一次。</p> <p>[hr]——强烈建议采取此措施。如果该措施适用但未实现,则应提供详细的理由,说明如何以等效方式实现 EMI 抗扰度。</p>		

EMI 风险分析示例见表 L.2。

表 L.2 EMI 风险分析示例

干扰源	EMI-现象	—	敏感部件	风险后果	问题解决方案
电源	电感耦合 电容耦合	<20 cm	信号线 传感器线	错误测量值功能 失灵	较远的距离 屏蔽 滤波 屏蔽电缆
逆变器	电容耦合	<40 cm	所有电缆 所有传感器 可编程逻辑 模数转换器	偶发性故障 故障失灵 功能丧失	较远的距离 滤波 正弦滤波器 屏蔽电缆 铁氧体夹具
主电源	电导耦合 电容耦合 高功率瞬变	—	传感器 可编程逻辑 电动机驱动	扰动 故障失灵 损坏 未定义状态	电源滤波器 浪涌滤波器 双绞线滤波 瞬态保护

表 L.2 EMI 风险分析示例（续）

干扰源	EMI-现象	—	敏感部件	风险后果	问题解决方案
感性负载	电感耦合 电导耦合 电容耦合 高功率瞬变	—	所有电缆 所有传感器 可编程逻辑 模数转换器 电动机驱动	扰动 故障失灵 损坏 未定义状态	滤波 双绞线 瞬态保护
所有 EMI	所有耦合	—	所有有源电子器件	—	导向安全状态的 诊断系统

附 录 M

(资料性)

安全要求规范(SRS)的更多信息

表 M.1 和表 M.2 列出了典型的安全功能及其特征和安全相关参数,同时参考了其他要求与安全功能、特征或参数相关的文件。

表 M.1 和表 M.2 中提到的大多数安全功能与电气标准有关,当使用其他技术或能源(如液压、气动)时,需要调整适用的要求。

表 M.1 适用于典型机械安全功能的文件示例及其部分特性

安全功能/特性	要求		更多信息
	本文件(GB/T 16855.1)	GB/T 15706—2012	
安全相关停止功能	5.2.2.2	3.26、6.2.11.3	IEC 60204-1:2016+AMD1:2021 中 9.2.2、9.2.3.3、9.2.3.6 GB/T 18831—2017 GB/T 19876—2012 IEC 62046:2018 IEC 61800-5-2:2016
手动复位功能	5.2.2.3	—	IEC 62046:2018
启动/重启功能	5.2.2.4	5.2.11.3、5.2.11.4	IEC 60204-1:2016+AMD1:2021 中 9.2.3.2、9.2.3.3、9.2.3.10 IEC 62046:2018
本地控制功能	5.2.2.5	5.2.11.8、5.2.11.10	IEC 60204-1:2016+AMD1:2021 中 10.1.5
屏蔽功能	5.2.2.6	—	IEC 62046:2018 的 5.7
保持运行功能	—	5.2.11.8 b)	IEC 60204-1:2016+AMD1:2021 中 9.2.3.7
使能设备功能	—	—	IEC 60204-1:2016+AMD1:2021 中 9.2.3.9、10.9
防止意外启动	—	5.2.11.4	GB/T 19670—2023 IEC 60204-1:2016+AMD1:2021 中 5.4 IEC 61800-5-2:2016
受困人员逃生与营救	—	5.3.5.3	GB/T 18831—2017 的 5.7.5.2
断开及能量耗散功能	—	5.3.5.4	GB/T 19670—2023 IEC 60204-1:2016+AMD1:2021 中 5.3、6.3.1
操作模式选择	5.2.2.9	5.2.11.8、5.2.11.10	IEC 60204-1:2016+AMD1:2021 中 9.2.3.5

表 M.1 适用于典型机械安全功能的文件示例及其部分特性（续）

安全功能/特性	要求		更多信息
	本文件(GB/T 16855.1)	GB/T 15706—2012	
不同 SRP/CS 间交互	—	5.2.11.1(最后一句)	IEC 60204-1:2016+AMD1:2021 GB/T 16655—2008 GB/T 16754—2021
安全相关输入值 参数化的监控	7.3	—	—
操作模式选择	5.2.2.9	5.2.11.8、5.2.11.10	IEC 60204-1:2016+AMD1:2021 中 9.2.3.5
急停功能 ^a	—	5.3.5.2	GB/T 16754—2021 IEC 60204-1:2016+AMD1:2021 中 9.2.3.4.2 IEC 61800-5-2:2016
监控或限制速度、 转矩、功率、位置 (如位置限制设备)、 运动、动量、压力、 停止时间、停止距离	—	—	ISO 10218-1:2011 IEC 61800-5-2:2016 GB/T 36008—2018
安全制动控制	—	—	IEC 61800-5-2:2016
^a 对于补充性防护措施,见 GB/T 15706—2012。			

表 M.2 对部分安全功能和安全相关参数提出要求的文件示例

安全功能/特性	要求		更多信息
	本文件(GB/T 16855.1)	GB/T 15706—2012	
响应时间	5.2 13.2	—	GB/T 19876—2012 的 3.2、A.3、A.4 IEC 62046:2018 的 4.4.2.2 ISO 10218-1:2011 的附录 B
安全相关参数,如速度、 温度、压力、位置或转矩	5.2	5.2.11.7.3	IEC 60204-1:2016+AMD1:2021 中 7.1、9.3.2 IEC 61800-5-2:2016
电源的波动、丧失和恢复	5.2.2.8	5.2.11.4 5.2.11.5	IEC 60204-1:2016+AMD1:2021 中 4.3、7.1、7.5 GB/T 3766—2015 GB/T 7932—2017

表 M.2 对部分安全功能和安全相关参数提出要求的文件示例（续）

安全功能/特性	要求		更多信息
	本文件(GB/T 16855.1)	GB/T 15706—2012	
指示和报警	—	5.2.3.6 和 5.2.3.7	GB/T 1251.1—2008 GB/T 1251.2—2006 GB/T 1251.3—2008 IEC 61310-1:2007 IEC 60204-1:2016+AMD1:2021 中 10.3、10.4 GB/T 15969.3—2017 IEC 62061:2021

附 录 N

(资料性)

在软件设计中避免系统性失效

N.1 为安全相关软件的设计选择避错措施

下表为选择 SRESW 或 SRASW 的避错措施提供了指导。表 N.1 概述了选择措施的分组情况。表 N.2 宜用于 LVL 的 SRASW,表 N.3 宜用于 FVL 的 SRESW 和 SRASW。

表 N.1 为选择措施对案例分类

PL _r	类别	软件使用于	案例
a 和 b	B	功能通道	案例 1
a、b 和 c	2	测试通道	
a 和 b	2	功能通道	
a 和 b	3	预评估平台	
a 和 b	3	通道 1 和通道 2	
a、b 和 c	3	通道 1 或通道 2	
c	2	功能通道	案例 2
c	3	预评估平台	
c	3	通道 1 和通道 2	
d	2	测试通道	
d	3 和 4	通道 1 或通道 2	
d	2	功能通道	案例 3
d	3 和 4	预评估平台	
d	3 和 4	通道 1 和通道 2	
e	3 和 4	通道 1 或通道 2	
e	3 和 4	预评估平台	案例 4 ^a
e	3 和 4	通道 1 和通道 2	
说明： ——通道 1 和通道 2：类别 3 或类别 4 两个功能通道中均使用了 SRESW 或 SRASW。 ——通道 1 或通道 2：类别 3 或类别 4 两个功能通道中仅一个通道使用了 SRESW 或 SRASW。 ——预评估平台：硬件和内部软件（SRESW）是为安全应用而设计的，并已被评估为符合本文件或 IEC 61508（所有部分）或 IEC 62061：2021 规定的所需性能等级（PL _r ）。			
^a 案例 4 中两行的唯一区别是对工具选择的要求。			

示例 1: 对于一个 PL_r c 的类别 2 子系统,功能通道采用案例 2 且测试通道采用案例 1。

表 N.2 和表 N.3 中的 SRESW 和 SRASW 的避错措施根据类别及 PL 进行分级。

- a) PL a 和 PL b 通常使用类别 B 结构实现,在功能通道的逻辑块中使用软件;
- b) PL c 和 PL d 可以使用类别 2 结构实现,在功能通道的逻辑块或测试通道的测试设备块中使

用软件。对于测试通道,要求降低一个性能等级。

- c) PL d 和 PL e 可以使用类别 3 结构实现,在功能通道的逻辑块中使用软件。“通道 1 和通道 2”意味着在两个功能通道中均使用了软件。“通道 1 或通道 2”意味着两个功能通道中,仅一个通道使用了软件。
- d) PL d 和 PL e 中的 SRASW 也可以使用预评估平台(安全相关硬件与操作系统和编程工具相结合)实现。在这种情况下,两个功能通道仅使用一个应用软件。

表 N.2 为 LVL 的 SRASW 选择措施

序号	案例	案例 1	案例 2	案例 3	案例 4
1	宜采用以下基本措施：				
a)	具有验证及确认活动的开发生命周期,见图 14 a)及图 14 b)；	m	m	m	m
b)	技术规范及设计文件；				
c)	模块化及结构化编程；				
d)	功能测试(如黑盒测试)；				
e)	修改后的合适开发活动				
2	安全相关软件技术规范宜被审查(见附录 J)并提供给参与 V 模型生命周期的每一个人,且宜包含：				
a)	带有所需 PL 及相关操作模式的安全功能；	—	m	m	m
b)	性能参数,如响应时间；				
c)	带有外部信号接口的硬件架构；				
d)	硬件失效的检测及控制				
3	选择工具、库、语言：				
a)	工具宜适用于应用；	—	m	m	m
b)	对于实现 PL e 的一个元件及其工具,该工具宜符合适用的安全标准；		—	—	m ^a
c)	宜采用可以检测导致系统性错误情况(如数据类型不匹配、模糊的动态内存分配,不完整的接口调用、递归、指针运算)的技术特性；	—	m	m	m
d)	检查宜主要在编译时间内执行而非仅在运行时间内执行。工具宜强制执行语言子集及编码准则,或者至少对使用它们的开发者进行监督或指导；				
e)	只要合理可行,宜使用经确认的功能块(FB)库——无论是由工具制造商提供的安全相关功能块库,还是经应用确认且符合本文件的特殊功能块库；	—	r	r	r
f)	宜使用适合于模块化方法的合理 LVL 子集,如公认的 IEC 61131-3 语言子集				
4	软件设计宜具有以下特点：				
a)	采用半形式化方法描述数据及控制流,如状态图或程序流程图；	—	m	m	m
b)	模块化及结构化编程,主要应用安全相关经确认的功能块库或其他模块化结构衍生的功能块,以实现代码易读性及可测试性；				

表 N.2 为 LVL 的 SRASW 选择措施 (续)

序号	案例	案例 1	案例 2	案例 3	案例 4
4	软件设计宜具有以下特点：				
c)	限制功能块代码规模；	—	m	m	m
d)	宜在只有一个入口点及一个出口点的功能块内执行代码；				
e)	三阶段模型架构：输入⇒处理⇒输出（见图 16 附录 J）；				
f)	仅在一个位置赋值安全输出；				
g)	使用检测和控制硬件失效的技术，并在导致安全状态的输入、处理和输出块内进行防御性编程技术				
5	当 SRASW 和非 SRASW 组合在一个元件内：				
a)	SRASW 和非 SRASW 宜在不同的具有明确定义数据链接的功能块中编写代码；	—	m	m	m
b)	不宜存在可能导致安全相关信号完整性降级的非安全相关数据和安全相关数据的逻辑组合，如将安全相关及非安全相关信号采用逻辑“或”组合，其结果控制安全相关信号				
6	软件实现/编码：				
a)	代码宜具有可读性、可理解性和可测试性，因此，宜使用符号变量（而不是显示的硬件地址）；	—	m	m	m
b)	宜使用合理的或公认的编码准则（见附录 J）；				
c)	宜使用应用层（防御性编程）提供的数据完整性和真实性检查（如范围检查）；	—	r	r	r
d)	代码宜通过仿真测试；				
e)	对于 PL d 或 PL e，宜通过控制流分析和数据流分析进行验证	—	—	r	r
7	测试：				
a)	适当的验证方法是对功能行为和性能标准（如时序性能）进行黑盒测试；	—	m	m	m
b)	I/O 测试宜确保安全相关信号在 SRASW 内被正确使用；				
c)	测试计划宜包含具有完成指标及所需工具的测试案例；	—	r	r	r
d)	对于 PL d 或 PL e，推荐使用边界值分析执行测试案例	—	—	r	r
8	文件：				
a)	所有的生命周期和修改活动都宜被记录；	—	m	m	m
b)	文件宜完整、可用、可读及可理解；				
c)	源文本中的代码文件宜包含带有法人实体的模块标题、功能和 I/O 描述、所用库功能块的版本以及网络/语句和声明行的充分注释				
9	确认（仅用于特定应用的代码，不用于经确认的库功能）：				
	确认宜通过审查、检查、走查或其他适当的活动进行	—	m	m	m

表 N.2 为 LVL 的 SRASW 选择措施 (续)

序号	案例	案例 1	案例 2	案例 3	案例 4
10	配置管理:				
	强烈推荐建立流程和数据备份,以确定和归档与特定 SRASW 版本相关的文件、软件模块、验证/确认结果和工具配置	—	r ^b	r ^b	r ^b
11	修改:				
	SRASW 修改后宜进行影响分析以确保规范。修改后宜进行适当的生命周期活动。宜控制对修改的访问权,并宜记录修改历史。 注:修改不影响已投入使用的系统。	—	m	m	m
说明: ——r=推荐:措施宜被用于提高软件质量;不强制使用,但如果不使用,宜说明理由; ——m=强制(具有低、中或高效力,见 7.4):该措施宜始终被使用; ——“—”:不需要该措施。					
^a 如果使用了具有不同工具的两个不同元件,基于使用的信赖度或已足够(对于 PL e)。 ^b 强烈推荐。					

表 N.3 为 FVL 的 SRESW 和/或 SRASW 选择措施

序号	案例	案例 1	案例 2	案例 3	案例 4
1	宜采用以下基本措施:				
a)	具有验证及确认活动的软件安全生命周期,见图 14 a)	m	m	m	m
b)	技术规范及设计文件,例如软件设计规范,SSDS,MDS,包含注释的代码清单				
c)	模块化及结构化编程,例如功能上的分层及限制、清晰的程序结构、接口定义、结构良好的调用图、避免中断、使用编码准则				
d)	控制系统性失效,例如程序顺序监控,控制数据通信过程中的错误(见 G.2)				
e)	使用基于软件的诊断措施用于控制随机硬件失效时,验证正确的实现,例如诊断措施的正确实现、RAM/ROM/CPU 测试、硬件测试、真实性检查				
f)	功能测试,例如黑盒测试根据输入数据(有效、无效及边界值)验证正确输出数据、接口兼容性、时序				
g)	修改后的适当软件安全生命周期活动,例如影响分析				
2	宜采用以下额外措施:				
a)	与 IEC 61508(所有部分)等文件中的工作流定义、责任、配置管理、工具使用可比的项目管理和质量管理流程	—	m(见注)	m(见注)	m ^a
b)	软件安全生命周期中所有相关活动的文件,例如审查、测试、确认及验证文件				
c)	用于确定 SRESW 发布时所有相关配置项目及文件的配置管理,例如对代码清单、模块、设计文件、测试计划、发布控制、归档、不同版本软硬件和编程工具的系统兼容性进行版本控制				

表 N.3 为 FVL 的 SRESW 和/或 SRASW 选择措施 (续)

序号	案例	案例 1	案例 2	案例 3	案例 4
2	宜采用以下额外措施:				
d)	含有安全要求的结构化技术规范及设计	—	m(见注)	m(见注)	m ^a
e)	采用合适的编程语言及计算机工具,例如对程序员进行使用工具的培训				
f)	模块化及结构化编程、与非安全相关软件分开、受限的模块大小和充分定义的接口、使用设计及编码准则				
g)	通过使用控制流分析的走查/审查进行代码验证。例如检查错误、注释质量、编码准则合规性、清晰度、可读性、完整性				
h)	扩展功能测试,如灰盒测试、性能测试或仿真。例如通过使用未指定的输入数据、极端环境条件、满负荷、基于内部代码理解的测试				
i)	修改后的影响分析和适当的软件安全生命周期活动				
j)	PL _r e 元件的 SRESW 宜符合 GB/T 20438.3—2017 的第 7 章,适用于 SIL3	—	—	—	m ^a
<p>注:对于相异性设计及编码的 SRESW,对于类别 3 或类别 4,或者类别 2 测试通道中的元件,采取措施避免系统性失效所涉及的工作可能减少,例如,仅通过考虑结构方面来审查软件的一部分,而不是检查每一行的代码。</p> <p>说明:</p> <p>——m=强制(具有低、中或高效力,见 7.4);该措施宜始终被使用;</p> <p>——“—”:不需要该措施。</p>					
<p>^a 技术规范、设计及编码采用相异性时,对于类别 3 或类别 4 子系统的双通道,上述 PL_rc 或 d 的基本及额外措施能实现 PL_re。</p>					

N.2 软件确认示例

N.2.1 总则

确认的目的是确保软件符合总体软件要求(见 V 模型,图 14)。确认以检查(例如分析)和测试相结合的方式进行,且宜在生命周期的早期进行规划。

本示例中提出的确认基于预评估的软件模块。确认通过位于预评估软件模块的输入点测试案例来完成,以检查它们在整个应用软件背景下的使用。示例仅显示了基本测试案例。实际应用的测试案例数量可能需要增加。

测试需要计划,包括涵盖测试程序和所使用设备的测试规范。实际的测试结果需要与测试计划进行比较。

N.2.2 编码准则

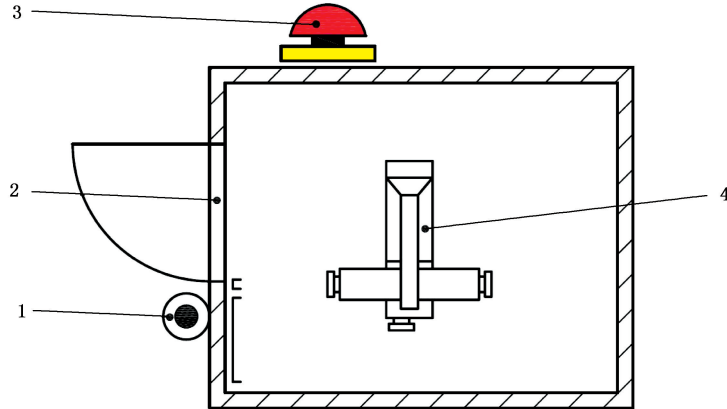
如果存在相关性,编码宜根据软件制造商所要求的编码准则来完成。或者宜根据“内部规范”编写代码,但不能与所使用的软件平台制造商要求的规范相抵触。

N.2.3 安全功能规范

安全功能及互补性操作如下(见图 N.1)。

- 如果联锁防护门 1(GD1)打开(可进入区域),则 M1 断开($PL_r = PL_d$)。GD1 的状态通过使用按钮 ACK1 确认。仅当 GD1 关闭时才可使用确认按钮 ACK1 复位。
- 按下急停按钮(ES1)则触发电动机 M1 的 STO($PL_r = PL_d$)。ES1 通过使用按钮 ACK1 确认。仅当 ES1 未锁持时才可进行确认。

注：对于复位按钮的要求,见 5.2.2.2 手动复位功能。



标引序号说明:

- 1——ACK1:联锁防护门 1(可进入区域)和急停 1 的确认按钮;
- 2——GD1:联锁防护门 1;
- 3——ES1:急停按钮 1;
- 4——M1:具有 STO(安全转矩关断)的电动机 1。

图 N.1 示例应用

N.2.4 从硬件设计规范输入信息

控制系统硬件设计的相关元件如下。

- 联锁防护门 GD1;
- 急停按钮 ES1;
- 确认按钮 ACK1;
- K1 的安全相关 CPU;
- K1 的安全相关 IO 板卡;
- 允许功能安全相关通信的现场总线[符合 IEC 61784(所有部分)];
- 安全相关变频器 T1(符合 IEC 61800-5-2:2016)用于电动机 M1。

如果满足所使用的安全 PLC(K1)制造商的所有安全相关要求,使用简化的 V 型模型便已足够,见图 14 b)。

图 N.2 中的元件代表了由元件制造商提供的预先设计的子系统。

变频器(驱动器 T1)根据 IEC 61800-5-2:2016 提供集成的安全相关子功能 STO(安全转矩关断)。

注：通常,变频器的参数化也在本文件和确认过程的范围内,但在本例中没有给出。

如果使用了安全 PLC(K1)制造商的所有安全相关要求,使用简化的 V 型模型便已足够,见图 14 b)。

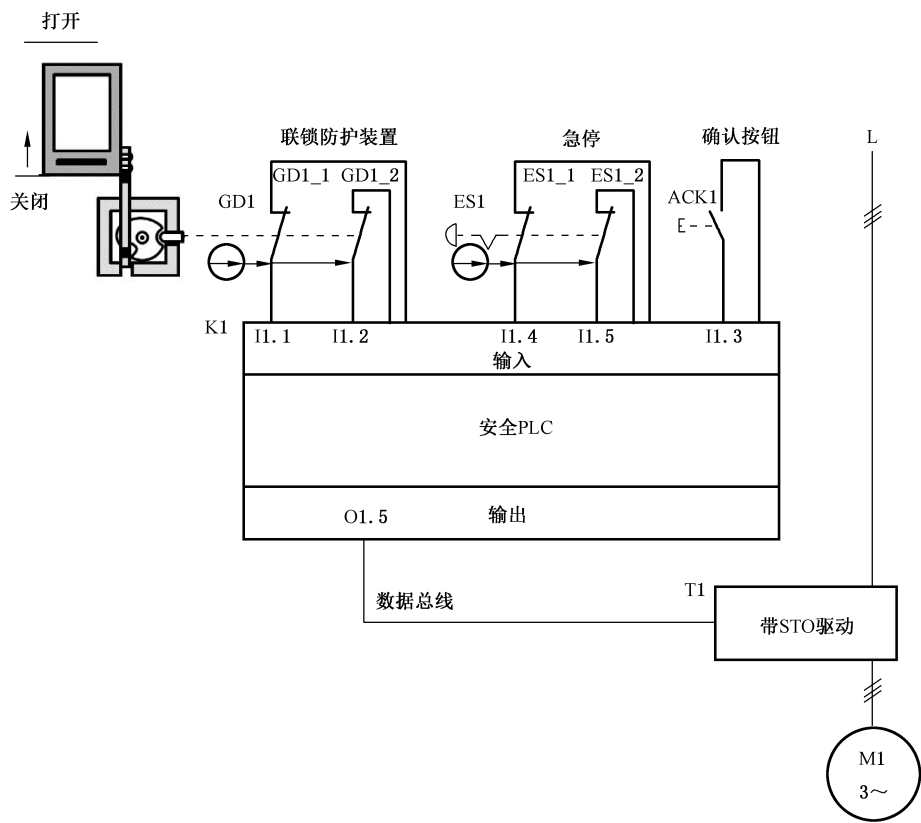
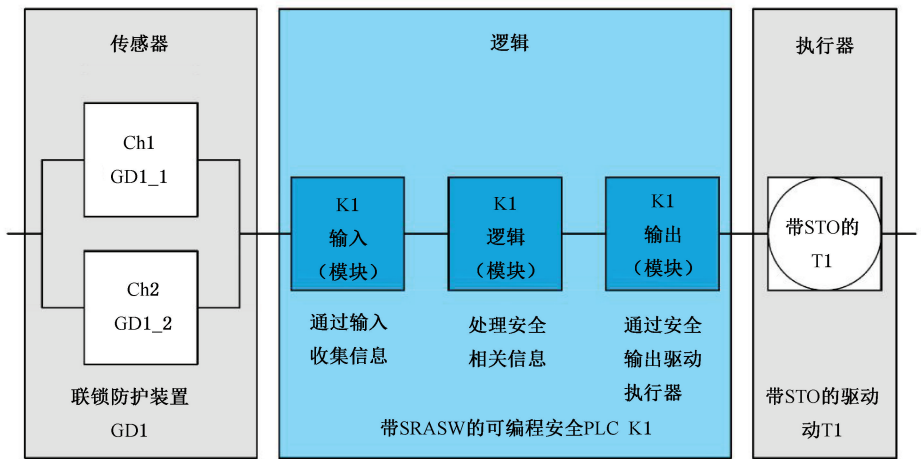


图 N.2 硬件概览

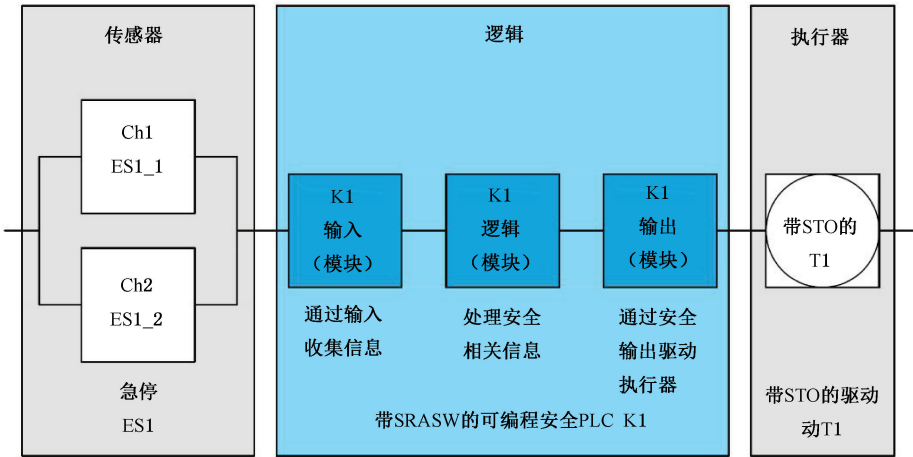
表 N.4 给出了执行安全功能和补充功能的相关信号,宜根据硬件接线和软件实现控制和测试这些功能。

图 N.3、图 N.4、图 N.5 给出了安全相关模块图。



SF1:如果联锁防护门 1 打开,则 M1 被变频器(驱动器 T1)切换至 STO。

图 N.3 SF1(联锁)



SF2:急停 ES1 通过变频器(驱动器 T1)触发电动机 M1 的 STO。

图 N.4 SF2(急停)

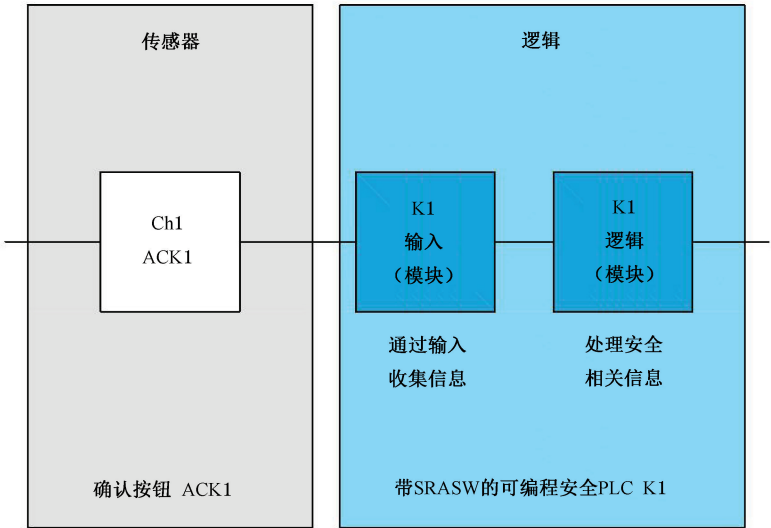


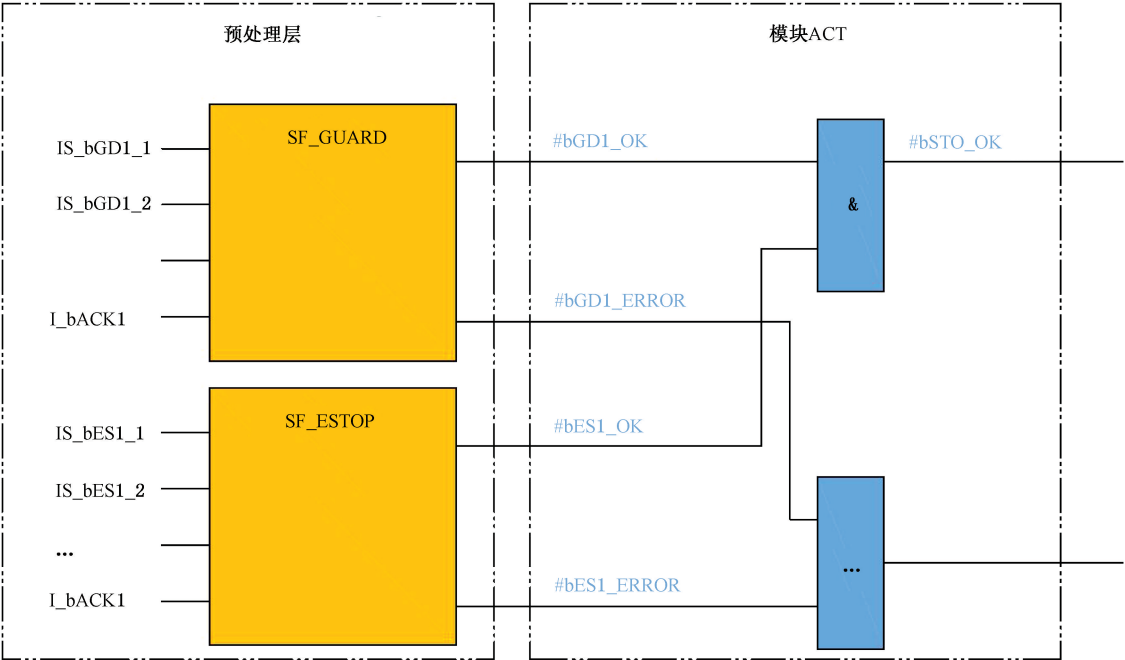
图 N.5 复位功能

表 N.4 确认接线及硬件输入/输出信号

输入信号列表			
描述(功能,信号)	变量(命名)	地址(命名)	接线及硬件地址是否正确?
GD1_1, 触点 1(NC)	IS_bGD1_1	I1.1	<input type="checkbox"/> 是 <input type="checkbox"/> 否
GD1_1, 触点 2(NC)	IS_bGD1_2	I1.2	<input type="checkbox"/> 是 <input type="checkbox"/> 否
ES1_1, 触点 1(NC)	IS_bES1_1	I1.4	<input type="checkbox"/> 是 <input type="checkbox"/> 否
ES1_1, 触点 2(NC)	IS_bES1_2	I1.5	<input type="checkbox"/> 是 <input type="checkbox"/> 否
ACK1, 知悉触点(NO)	I_bACK1	I1.3	<input type="checkbox"/> 是 <input type="checkbox"/> 否
输出信号列表			
M1,STO	QS_bM1_STO	O1.5	<input type="checkbox"/> 是 <input type="checkbox"/> 否

N.2.5 应用程序

图 N.6 给出了安全 PLC K1 中基于已预评估的软件模块(功能块)的应用程序(SRASW)。



标引序号说明：

■ —— 功能块。

注 1：#bSTO_OK 通过使用安全协议的现场总线传输给变频器(驱动器 1)。

注 2：指示及错误处理与特定应用相关,本示例未作考虑。

图 N.6 安全 PLC K1 中基于已预评估的软件模块(功能块)的应用程序(SRASW)

N.2.6 SRASW 的确认

N.2.6.1 原则

基于预评估的软件模块的确认可分为：

- a) 联锁安全防护的评估；
- b) 急停的评估；
- c) 电动机 M1 使能/切断的评估；
- d) 文件。

无需对已预评估的软件模块进行确认。此处给出的确认宜证明应用程序作为一个整体,满足其软件规范,包括参数化和预评估软件模块的配置。

N.2.6.2 联锁安全防护的评估

表 N.5 列出了执行 FMEA 的测试案例和联锁安全防护的测试。表 N.5 中的测试 1 是一个无故障插入的功能测试。测试 2 和测试 3 模拟了联锁防护相关触点上的常高电平信号。测试 4 和测试 5 模拟了这些触点中一个触点上的常低电平信号。测试 6 和测试 7 模拟了两个触点在设定的差异时间外的信号变化。测试 8 模拟了知悉触点的粘连故障(常高电平)。对于所有 8 个测试案例,确认了 #bGD1_OK 和 #bGD1_ERROR 的正确响应。

表 N.5 联锁安全防护的 FEMA 及测试

相关的输入				
信号	I/O	类型	信息	备注
GD1 Ch1; IS_bGD1_1 (安全门开关)	I1.1	布尔	通道 1 与通道 2 差异 时间 0.5 s	联锁防护 NC(直接断开动作)
GD1 Ch2; IS_bGD1_2 (安全门开关)	I1.2	布尔	通道 1 与通道 2 差异 时间 0.5 s	联锁防护 NC(直接断开动作)
ACK1; I_bACK1 (复位)	I1.3	布尔	无	连接至联锁防护 GD1 的共有知悉信号
相关的标志位				
信号		类型	信息	备注
内部标志位 # bGD1_OK		布尔	无	该释放标志位用于后续处理
内部标志位 # bGD1_ERROR		布尔	无	该错误标志位用于后续处理
使用的软件块				
名称	经预评估的 软件平台块	描述		软件块表示
SF_GUARD	是	联锁防护监控的预评估软件块。 比较两个 GD1 信号。评估后的 GD1 状态通过 # bGD1_OK 发出信号。当检测到故障时, # bGD1_ERROR 标志位变为高电平		
测试案例(失效模式影响分析)				
序号	测试或故障插入		预期结果 安全状态及故障反应	测试结果
1	无故障插入的功能测试且无预期故障反应: 当要求安全功能时(通过打开联锁防护), IS_bGD1_1=低电平且 IS_bGD1_2=低电平		# bGD1_OK=低电平且 # bGD1_ERROR=低电平。 只有在关闭 GD1 并按下 ACK1 后, # bGD1_OK 的高电平信号才会恢复	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 1: 无错误状态(初始情况/进行测试前的正常状态,联锁防护门已关闭)。				
2	IS_bGD1_1(I1.1)上为常高电平。 当要求安全功能时(通过打开联锁防护),仅 IS_bGD1_2 变为低电平		安全状态 # bGD1_OK=低电平且触发故障反应 # bGD1_ERROR = 低电平 变为 # bGD1_ERROR=高电平 SF_GUARD 块无法知晓 GD1 关闭后 SF_GUARD 块依然无法知晓。 只有在修复且 IS_bGD1_1 和 IS_bGD1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_GUARD	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 2: I1.1 报错。				

表 N.5 联锁安全防护的 FEMA 及测试 (续)

测试案例(失效模式影响分析)			
序号	测试或故障插入	预期结果 安全状态及故障反应	测试结果
3	IS_bGD1_2(I1.2)上为常高电平 当要求安全功能时(通过打开联锁防护),仅 IS_bGD1_1 变为低电平	安全状态 # bGD1_OK = 低电平且触发故障反应 # bGD1_ERROR = 低电平变为 # bGD1_ERROR = 高电平 SF_GUARD 块无法知晓 GD1 关闭后 SF_GUARD 块依然无法知晓。 只有在修复且 IS_bGD1_1 和 IS_bGD1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_GUARD	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 3: I1.2 报错。			
4	IS_bGD1_1(I1.1)上为低电平 GD1 关闭,因此 IS_bGD1_2 为高电平	安全状态 # bGD1_OK = 低电平且触发故障反应 # bGD1_ERROR = 低电平变为 # bGD1_ERROR = 高电平 即使 GD1 被打开后再被关闭,SF_GUARD 块仍无法知晓	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 4: I1.1 报错。			
5	IS_bGD1_2(I1.2)上为低电平 GD1 关闭,因此 IS_bGD1_1 为高电平	安全状态 # bGD1_OK = 低电平且触发故障反应 # bGD1_ERROR = 低电平变为 # bGD1_ERROR = 高电平 即使 GD1 被打开后再被关闭,SF_GUARD 块仍无法知晓	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 5: I1.2 报错。			
6	IS_bGD1_1 (I1.1)在同 IS_bGD1_2 设定的差异时间外改变信号状态	安全状态 # bGD1_OK = 低电平且触发故障反应 # bGD1_ERROR = 低电平变为 # bGD1_ERROR = 高电平 SF_GUARD 块无法知晓 GD1 关闭后 SF_GUARD 块依然无法知晓。 只有在修复且 IS_bGD1_1 和 IS_bGD1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_GUARD	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 6: 该诊断功能是为了防止被操纵。			
7	IS_bGD1_2 (I1.2)在同 IS_bGD1_1 设定的差异时间外改变信号状态	安全状态 # bGD1_OK = 低电平且触发故障反应 # bGD1_ERROR = 低电平变为 # bGD1_ERROR = 高电平 SF_GUARD 块无法知晓 GD1 关闭后 SF_GUARD 块依然无法被知晓。 只有在修复且 IS_bGD1_1 和 IS_bGD1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_GUARD	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 7: 该诊断功能是为了防止被操纵。			

表 N.5 联锁安全防护的 FEMA 及测试（续）

测试案例(失效模式影响分析)			
8	ACK1(I1.3)上为常高电平	安全状态 #bGD1_OK=低电平 无法知悉	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 8：知悉信号为边沿控制而非电平控制。该诊断功能是对操纵行为的一种预防措施。			

N.2.6.3 急停的评估

表 N.6 列出了执行 FMEA 的测试案例和急停的测试。表 N.6 中的测试 1 是一个无故障插入的功能测试。测试 2 和测试 3 模拟了急停相关一个触点上的常高电平信号。测试 4 和测试 5 模拟了这些触点中一个触点上的常低电平信号。测试 6 和测试 7 模拟了两个触点在设定的差异时间外的信号变化。测试 8 模拟了知悉触点的粘连故障(常高电平)。对于所有 8 个测试案例,确认了 #bES1_OK 和 #bES1_ERROR 的正确响应。

表 N.6 FEMA 及紧急停止测试

相关的输入				
信号	I/O	类型	信息	备注
ES1 Ch1: IS_bES1_1 (急停)	I1.4	布尔	通道 1 与通道 2 差异 时间 0.5 s	急停 NC(直接断开动作)
GD1 Ch2: IS_bES1_2 (急停)	I1.5	布尔	通道 1 与通道 2 差异 时间 0.5 s	急停 NC(直接断开动作)
ACK1: I_bACK1 (复位)	I1.3	布尔	无	连接至急停 ES1 的共有知悉信号
相关的输出/标志位				
信号		类型	信息	备注
#bES1_OK		布尔	无	该释放标志位用于后续处理
#bES1_ERROR		布尔	无	该错误标志位用于后续处理
使用的软件块				
名称	经预评估的 软件平台块	描述		软件块表示
SF_ESTOP	是	监控一个双通道信号的预评估 软件块。 比较两个 ES1 信号。评估后 的 ES1 状态通过 #bES1_OK 发出信号。当检测到故障 时, #bES1_ERROR 标志位变 为高电平		

表 N.6 FEMA 及紧急停止测试 (续)

测试案例(失效模式影响分析)			
序号	测试或故障插入	预期结果 安全状态及故障反应	测试结果
1	无故障插入的功能测试且无预期故障反应: 当急停被操动时,IS_bES1_1=低电平且 IS_bES1_2=低电平	# bES1_OK = 低电平 且 # bES1_ERROR = 低电平。 只有在解锁 ES1 并按下 ACK1 后, # bES1_OK 的高电平信号才会恢复	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 1: 无错误状态(初始情况/进行测试前的正常状态,未请求急停)。			
2	I IS_bES1_1(I1.4)上为常高电平 当急停被操动时,仅 IS_bES1_2 变为低电平	安全状态 # bES1_OK = 低电平 且 触发故障反应 # bES1_ERROR = 低电平 变为 # bES1_ERROR = 高电平 SF_ESTOP 块无法知晓 ES1 解锁后 SF_ESTOP 块依然无法知晓。 只有在修复且 IS_bES1_1 和 IS_bES1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_ESTOP	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 2: I1.4 报错。			
3	IS_bES1_2(I1.5)上为常高电平 当急停被操动时,仅 IS_bES1_1 变为低电平	安全状态 # bES1_OK = 低电平 且 触发故障反应 # bES1_ERROR = 低电平 变为 # bES1_ERROR = 高电平 SF_ESTOP 块无法知晓 ES1 解锁后 SF_ESTOP 块依然无法知晓。 只有在修复且 IS_bES1_1 和 IS_bES1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_ESTOP	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 3: I1.5 报错。			
4	IS_bES1_1(I1.4)上为低电平 ES1 被解锁,因此 IS_bES1_2 为高电平	安全状态 # bES1_OK = 低电平 且 触发故障反应 # bES1_ERROR = 低电平 变为 # bES1_ERROR = 高电平 即使 ES1 被操动后再被解锁,SF_ESTOP 块仍无法知晓	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 4: I1.4 报错。			
5	IS_bES1_2(I1.5)上为低电平 ES1 被解锁,因此 IS_bES1_1 为高电平	安全状态 # bES1_OK = 低电平 且 触发故障反应 # bES1_ERROR = 低电平 变为 # bES1_ERROR = 高电平 即使 ES1 被操动后再被解锁,SF_ESTOP 块仍无法知晓	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 5: I1.5 报错。			

表 N.6 FEMA 及紧急停止测试（续）

测试案例(失效模式影响分析)			
6	IS_bES1_1 (I1.4)在同 IS_bES1_2 设定的差异时间外改变信号状态	安全状态 # bES1_OK=低电平且发故障反应 # bES1_ERROR=低电平变为 # bES1_ERROR=高电平 SF_ESTOP 块无法知晓 ES1 解锁后 SF_ESTOP 块依然无法知晓。 只有在修复且 IS_bES1_1 和 IS_bES1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_ESTOP	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 6: 该诊断功能是为了防止被操纵。			
7	IS_bES1_2 (I1.5)在同 IS_bES1_1 设定的差异时间外改变信号状态	安全状态 # bES1_OK=低电平且 触发故障反应 # bES1_ERROR=低电平变为 # bES1_ERROR=高电平 SF_ESTOP 块无法知晓 ES1 解锁后 SF_ESTOP 块依然无法知晓。 只有在修复且 IS_bES1_1 和 IS_bES1_2 信号共同产生高-低-高电平变化后,通过 ACK1 的信号变化才能使能 SF_ESTOP	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 7: 该诊断功能是为了防止被操纵。			
8	ACK1(I1.3)上为常高电平	安全状态 # bES1_OK=低电平 无法知悉	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 8: 知悉信号为边沿控制而非电平控制。该诊断功能是对操纵行为的一种预防措施。			

N.2.6.4 带有电动机 M1 的安全联锁及急停的评估

表 N.7 列出了电动机 M1 使能/切断的 FEMA 及测试。

表 N.7 电动机 M1 使能/切断的 FEMA 及测试

相关的输入/相关的标志位			
信号	类型	信息	备注
# bGD1_OK (可变)	布尔	无	该释放标志位用于后续处理
# bES1_OK (可变)	布尔	无	该释放标志位用于后续处理
使用的软件块			
名称	经预评估的软件平台块	描述	软件块表示
模块 ACT	否	使用图 N.6 所示的与连接	见图 N.6 模块 ACT

表 N.7 电动机 M1 使能/切断的 FEMA 及测试 (续)

相关的输出/标志位				
描述	O	类型	信息	描述
# bSTO_OK	Q1.5	总线	根据 PL d 经过预评估	经由安全总线至变频器 (驱动器 1),激活 STO
测试案例(失效模式影响分析)				
序号	测试或故障插入		预期结果	测试结果
1	插入一个导致 # bGD1_ERROR=高电平的故障		应用特定的错误处理	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 1: 如果出现 # bGD1_ERROR 错误,则变频器(驱动器 1)也宜断开。				
2	插入一个导致 # bES1_ERROR=高电平的故障		应用特定的错误处理	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 2: 如果出现 # bES1_ERROR 错误,则变频器(驱动器 1)也宜断开。				
3	功能测试。 # bGD1_OK=高电平且 # bES1_OK=高电平		# bSTO_OK=高电平	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 3: 这是一个无错误状态。				
4	当 GD1 关闭时,通过操动 ES1 进行功能测试。 # bGD1_OK=高电平且 # bES1_OK=低电平		# bSTO_OK=低电平	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 4: 这是一个无错误状态。				
5	当 ES1 解锁时,通过打开 GD1 进行功能测试。 # bGD1_OK=低电平且 # bES1_OK=高电平		# bSTO_OK=低电平	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 5: 这是一个无错误状态。				
6	通过打开 GD1 并操动 ES1 进行功能测试。 # bGD1_OK=低电平且 bES1_OK=低电平		# bSTO_OK=低电平	<input type="checkbox"/> 是 <input type="checkbox"/> 否
注 6: 这是一个无错误状态。				
7	PLC K1 与变频器(驱动器 1)之间现场总线通信错误。 严重错误(在发生严重错误的情况下,宜重新启动控制器。)如果出现一个现场总线通讯错误,则变频器(驱动器 1)也宜断开		应用特定的错误处理	<input type="checkbox"/> 是 <input type="checkbox"/> 否

N.2.6.5 文件

该文件对确认设定了额外要求,例如软件规范、软件指南、表明软件的设计是为了实现 PL_r 的证明、表明软件支持所要求 DC 的证明、防止软件相关系统性失效的措施的文件。确认还包括对这些方面的分析。表 N.8 没有包括所有这些方面的细节,因此需要进一步的文件。

表 N.8 软件代码审查文件

项目	依据	修正
软件是否符合安全编程准则?	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
控制系统的设计是否与软件相符?	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
功能块的正确参数化	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
输入信号的正确参数化	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
输出信号的正确参数化	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
安全程序的架构是否符合技术规范	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
安全软件的规格说明是否对应安全功能的技术规范	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
防御性编程	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
没有通过“或”功能产生负面影响	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
没有通过“非”功能产生负面影响	见……	<input type="checkbox"/> 是 <input type="checkbox"/> 否
……		
日期:		
姓名:		
软件签名:		
硬件签名:		

附录 O

(资料性)

控制系统元件或部件的安全相关值

O.1 设备类型的定义

O.1.1 概述

设备在技术、应用、可用性及诊断机制和诊断信息的使用方面各不相同。因此,在此处将定义不同的设备类型。

注 1: 更多信息见 VDMA 66413。

设备通常能通过以下特征进行区分:

- 能直接作为 SRP/CS 或安全功能中的子系统组件使用的设备,因为制造商已经为这一特定应用开发了该设备(设备类型 1 和设备类型 4);
- 只通过用户的设计过程被定义和评估为 SRP/CS 或子系统组件的设备(设备类型 2 和设备类型 3)。

注 2: 安全功能通常使用多种设备类型。设备类型不能与如 ISO 14119 和 IEC 61496(所有部分)等的类型相混淆。

设备类型的特性值见表 O.1。

表 O.1 设备类型的特性值

特性值	设备类型				备注
	1	2	3	4	
PL	√	—	—	—	GB/T 16855.1(本文件)
SIL		—	—	—	IEC 62061:2021
PFH	√	—	—	—	GB/T 16855.1(本文件)和 IEC 62061:2021
类别	√	√	√	—	GB/T 16855.1(本文件)和 IEC 62061:2021 需要其中一个特性值
HFT	—			—	
MTTF _D	—	√	—	—	GB/T 16855.1(本文件)和 IEC 62061:2021 需要其中一个特性值
λ _D	—		—	—	
MTTF	—		—	—	
MTBF	—		—	—	
B _{10D}	—	—	√	—	GB/T 16855.1(本文件)和 IEC 62061:2021 需要其中一个特性值
B ₁₀	—			—	
RDF	—	O ^b	O ^b	—	GB/T 16855.1(本文件)
SFF	—			—	IEC 62061:2021 ^a

表 O.1 设备类型的特性值（续）

特性值	设备类型				备注
	1	2	3	4	
T_{10D}	√	—	—	√	GB/T 16855.1(本文件)和 IEC 62061:2021 需要其中一个特性值
T_M		—	—		
说明： √——强制的； O——可选的。					
^a SFF(安全失效分数)在 IEC 62061:2021 中 3.2.54 定义为子系统整体故障率中不会导致危险失效的部分。 ^b 如果供应商没有提供 MTTF _D 或 B_{10D} 数值。					

O.1.2 设备类型 1

设备类型 1 具有最高的集成水平。典型的是预设计的带有集成诊断功能的安全系统。该类型根据预期用途进行 SIL 或 PL 分类。设备的制造商指定了类别。

这种类型的设备是按照安全标准[如 IEC 61508(所有部分)]开发的。

示例：安全光幕、安全光栅、安全控制系统组件、集成安全功能的驱动器、安全继电器。

注：参数可能取决于其他特定应用的数据(例如最大切换频率的限制)。

O.1.3 设备类型 2

为了让用户评估安全功能,需要额外的应用数据(电路结构、DC 和 CCF 的考虑)。

这种类型的设备不一定是按照安全标准开发的。但是,符合本文件的应用不在排除范围内。

示例：运算放大器、接近开关、压力传感器、液压阀。

注：部分设备可能包括具有取决于操作次数的失效模式的元件以及其他几乎与操作次数无关的元件。由制造商决定是否将这种设备定义为类型 1、类型 2 或类型 3,以及向用户提供哪些特性值和应用限制。例如,将 MTTF_D 值与最大操作次数限制相结合,或者将 B_{10D} 值与用于公式(C.1)应用的最小 n_{op} 限制相结合。

O.1.4 设备类型 3

类型 3 的设备具有取决于操作次数的故障模式的元件。

为了让用户评估安全功能,需要额外的应用数据(操作次数、启动次数、电路结构、DC 和 CCF 的考虑)。

这种类型的设备不一定是按照安全标准开发的。但是,符合本文件的应用不在排除范围内。

示例：容易磨损的机电元件,如电源接触器、开关、气动阀、联锁装置、控制装置。

O.1.5 设备类型 4

设备类型 4 是设备类型 1 的特例。该类型具有导致危险故障的非随机性失效,这意味着发生危险故障的概率接近于 PFH=0。对于该类型的元件,每个潜在故障适用以下任何一种情况：

- 故障排除符合本文件的规定；
- 故障始终导致一个安全状态。

在架构要求或其他考虑因素对单独(单通道)使用施加了限制的情况下,应规定单通道使用的最大可实现 PL 和 SIL。

为了提供上述信息,设备应根据安全标准[例如 IEC 61508(所有部分)]进行评估。

O.2 其他信息

O.2.1 软件

如果在元件中使用软件,设备制造商宜提供与 PL 对应的软件的适用性信息。

O.2.2 基本安全原则

对于类别 B~类别 4 的元件,设备制造商宜提供该元件是否按照基本安全原则设计和制造的信息。

O.2.3 经验证的安全原则

对于类别 1~类别 4 的元件,设备制造商宜提供该元件是否按照经验证的安全原则设计和制造的信息。

参 考 文 献

- [1] GB/T 1251.1—2008 人类工效学 公共场所和工作区域的险情信号 险情听觉信号
- [2] GB/T 1251.2—2006 人类工效学 险情视觉信号 一般要求、设计和检验
- [3] GB/T 1251.3—2008 人类工效学 险情和信息的视听信号体系
- [4] GB/T 3766—2015 液压传动 系统及其元件的通用规则和安全要求
- [5] GB/T 7932—2017 气动 对系统及其元件的一般规则和安全要求
- [6] GB/T 15969.3—2017 可编程序控制器 第3部分:编程语言
- [7] GB/T 16655—2008 机械安全 集成制造系统 基本要求
- [8] GB/T 16754—2021 机械安全 急停功能 设计原则
- [9] GB/T 18831—2017 机械安全 与防护装置相关的联锁装置 设计和选择原则
- [10] GB/T 19000—2016 质量管理体系 基础和术语
- [11] GB/T 19670—2023 机械安全 防止意外启动
- [12] GB/T 20438.2—2017 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
- [13] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语
- [14] GB/T 20438.6—2017 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2和GB/T 20438.3的应用指南
- [15] GB/T 20438.7—2017 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述
- [16] GB/T 21109.1—2022 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、硬件和应用编程要求
- [17] GB/T 36008—2018 机器人与机器人装备 协作机器人
- [18] GB/T 38943.1—2020 土方机械 使用电力驱动的机械及其相关零件和系统的电安全 第1部分:一般要求
- [19] ISO/IEC Guide 51:2014 Safety aspects—Guidelines for their inclusion in standards
- [20] ISO 4413 Hydraulic fluid power—General rules and safety requirements for systems and their components
- [21] ISO 4414 Pneumatic fluid power—General rules and safety requirements for systems and their components
- [22] ISO 8573-1 Compressed air—Part 1: Contaminants and purity classes
- [23] ISO 9241-210 Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems
- [24] ISO 10218-1:2011 Robots and robotic devices—Safety requirements for industrial robots—Part 1: Robots
- [25] ISO 13850 Safety of machinery—Emergency stop function—Principles for design
- [26] ISO 13856 (all parts) Safety of machinery—Pressure-sensitive protective devices
- [27] ISO 14119 Safety of machinery—Interlocking devices associated with guards—Principles for design and selection
- [28] ISO/TR 14121-2 Safety of machinery—Risk assessment—Part 2: Practical guidance and examples of methods

- [29] ISO 16090-1 Machine tools safety—Machining centres, Milling machines, Transfer machines—Part 1: Safety requirements
- [30] ISO 19973 (all parts) Pneumatic fluid power—Assessment of component reliability by testing
- [31] ISO/TR 22100-2:2013 Safety of machinery—Relationship with ISO 12100—Part 2: How ISO 12100 relates to ISO 13849-1
- [32] ISO/TR 22100-3 Safety of machinery—Relationship with ISO 12100—Part 3: Implementation of ergonomic principles in safety standards
- [33] ISO/TR 22100-4 Safety of machinery—Relationship with ISO 12100—Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects
- [34] ISO 23125:2015 Machine tools—Safety—Turning machines
- [35] ISO/TR 24119 Safety of machinery—Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts
- [36] IEC 60050-192:2015 International electrotechnical vocabulary—Part 192: Dependability
- [37] IEC 60068 (all parts) Environmental testing
- [38] IEC 60204-1:2016+AMD1:2021 Safety of machinery—Electrical equipment of machines—Part 1: General requirements
- [39] IEC 60529 Degrees of protection provided by enclosures (IP code)
- [40] IEC 60812 Failure modes and effects analysis (FMEA and FMECA)
- [41] IEC 60947 (all parts) Low-voltage switchgear and controlgear
- [42] IEC 60950-1 Information technology equipment—Safety —Part 1: General requirements
- [43] IEC 61000-1-2:2016 Electromagnetic compatibility (EMC)—Part 1-2: General—Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena
- [44] IEC 61000-6-2 Electromagnetic compatibility (EMC)—Part 6-2: Generic standards—Immunity standard for industrial environments
- [45] IEC 61000-6-7:2014 Electromagnetic compatibility (EMC)—Part 6-7: Generic standards—Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations
- [46] IEC 61025 Fault tree analysis (FTA)
- [47] IEC 61131-3 Programmable controllers—Part 3: Programming languages
- [48] IEC 61310-1:2007 Safety of machinery—Indication, marking and actuation—Part 1: Requirements for visual, acoustic and tactile signals
- [49] IEC 61326-3-1 Electrical equipment for measurement, control and laboratory use—EMC requirements—Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—General industrial applications
- [50] IEC 61496 (all parts) Safety of machinery—Electro-sensitive protective equipment
- [51] IEC 61558-2-16 Safety of transformers, reactors, power supply units and combinations thereof —Part 2-16: Particular requirements and tests for switch mode power supply units and transformers for switch mode power supply units for general applications
- [52] IEC 61708:2016 Reliability block diagrams
- [53] IEC 61784 (all parts) Industrial communication networks—Profiles
- [54] IEC 61800-3 Adjustable speed electrical power drive systems—Part 3: EMC requirements and specific test methods for PDS and machine tools

- [55] IEC 61800-5-2:2016 Adjustable speed electrical power drive systems—Part 5-2: Safety requirements—Functional
 - [56] IEC 61810-2-1 Electromechanical elementary relays—Part 2-1: Reliability—Procedure for the verification of B_{10} values
 - [57] IEC 61810-3 Electromechanical elementary relays—Part 3: Relays with forcibly guided (mechanically linked) contacts
 - [58] IEC 62021 (all parts) Insulating liquids—Determination of acidity
 - [59] IEC 62024 (all parts) High frequency inductive components—Electrical characteristics and measuring methods
 - [60] IEC 62368-1 Audio/video, information and communication technology equipment—Part 1: Safety requirements
 - [61] IEC 62502 Analysis techniques for dependability—Event tree analysis (ETA)
 - [62] IEC/TR 63074 Safety of machinery—Security aspects related to functional safety of safety-related control systems
 - [63] EN 50178 Electronic equipment for use in power installations
 - [64] EN 50495:2010 Safety devices required for the safe functioning of equipment with respect to explosion risks
 - [65] SN 29500 (all parts) Failure rates of components, Edition 1999-11, Siemens AG 1999s
 - [66] VDMA 66413 Functional Safety—Universal data format for safety-related values of components or parts of control system
-