

国际标准

机械安全—控制系统的安全相关部件

—第1部分：一般设计原理

上部

(中文版)

2024年02月翻译

参考版本号：

ISO 13849-1:2023(E)

目录

前言.....	5
介绍.....	6
1 范围.....	8
2 规范性引用文件.....	8
3 术语、定义、符号和缩写.....	8
3.1 术语和定义.....	8
3.2 符号和缩略语.....	20
4 概述.....	21
4.1 机器的风险评估和风险降低过程.....	21
4.2 降低风险策略.....	23
4.3 SRP/CS的设计过程.....	23
4.4 方法论.....	24
4.5 所需信息.....	25
4.6 利用子系统实现安全功能.....	25
5 安全功能规范.....	26
5.1 安全功能的识别和一般描述.....	26
5.2 安全要求规范.....	26
5.2.1 一般要求.....	26
5.2.2 特定安全功能要求.....	28
5.2.3 最大限度地减少破坏安全功能的动机.....	31
5.2.4 远程访问.....	32
5.3 确定每个安全功能所需的效能等级 (PL _r)	32
5.4 审查安全要求规范 (SRS)	32
5.5 SRP/CS分解为子系统.....	33
6 设计注意事项.....	34
6.1 实现的绩效水平评估.....	34
6.1.1 绩效水平概述.....	34
6.1.2 效能等级 (PL) 和安全完整性水平 (SIL) 之间的相关性.....	35
6.1.3 体系结构—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.....	35
6.1.4 危险性失效平均时间 (MTTF _D)	41
6.1.5 诊断覆盖率 (DC)	42
6.1.6 常见原因失效 (CCFs)	43
6.1.7 系统性失效.....	43
6.1.8 评估子系统效能等级的简化程序.....	43
6.1.9 在没有MTTF _D 的情况下确定效能等级和PFH的替代程序.....	44
6.1.10 故障考虑和故障排除.....	46

6.1.11 . 久经考验的组件.....	47
6.2 . 实现安全功能整体效能等级的子系统组合.....	47
6.2.1 . 概述.....	47
6.2.2 . 已知PFH值.....	47
6.2.3 . 未知的PFH值.....	48
6.3 . 基于软件的手动参数化.....	48
6.3.1 . 概述.....	48
6.3.2 . 对安全相关参数的影响.....	49
6.3.3 . 基于软件的手动参数化要求.....	49
6.3.4 . 参数化工具的验证.....	50
6.3.5 . 基于软件的手动参数化文档.....	50
7 . 软件安全要求.....	50
7.1 . 概述.....	50
7.2 . 有限变异语言 (LVL) 和完全变异语言 (FVL)	52
7.2.1 . 有限变异性语言 (LVL)	52
7.2.2 . 全变率语言 (FVL)	52
7.2.3 有限变异语言 (LVL) 或完全变异语言 (FVL) 的决策.....	52
7.3 . 安全相关嵌入式软件 (SRESW)	54
7.3.1 . 安全相关嵌入式软件 (SRESW) 的设计.....	54
7.3.2 . 不可访问嵌入式软件的替代程序.....	55
7.4 . 安全相关应用软件 (SRASW)	55
8 . 验证实现的效能等级.....	57
9 . 设计的人机工程学方面.....	57
10 . 验证.....	57
10.1 . 验证原则.....	57
10.1.1 . 概述.....	57
10.1.2 . 验证计划.....	60
10.1.3 . 一般故障列表.....	60
10.1.4 . 具体故障清单.....	60
10.1.5 . 验证信息.....	60
10.2 . 安全要求规范 (SRS) 的验证.....	61
10.3 . 分析验证.....	61
10.3.1 . 概述.....	61
10.3.2 . 分析技术.....	62
10.4 . 通过测试进行验证.....	62
10.4.1 . 概述.....	62
10.4.2 . 测量精度.....	63
10.4.3 . 试验的附加要求.....	63

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/847163201165006105>