



中华人民共和国国家标准

GB/T 16855.1—2008/ISO 13849-1:2006
代替 GB/T 16855.1—2005

机械安全 控制系统有关安全部件 第 1 部分：设计通则

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

(ISO 13849-1:2006, IDT)

2008-08-25 发布

2009-04-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会

发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义、符号和缩写	1
4 设计方面的考虑	7
4.1 设计中的安全目标	7
4.2 风险减小策略	8
4.3 确定所需的性能等级(PL _r)	10
4.4 SRP/CS 的设计	10
4.5 所需的性能等级 PL 的估计及其与 SIL 的关系	11
4.6 软件的安全要求	15
4.7 检验达到的 PL 是否满足 PL _r	18
4.8 设计的人类功效学方面	18
5 安全功能	18
5.1 安全功能技术规范	18
5.2 安全功能详述	20
6 类别以及与 DC _{avg} 、CCF 和每个通道 MTTF _d 的关系	22
6.1 一般要求	22
6.2 类别规范	22
6.3 用于实现全部 PL 的 SRP/CS 组合	27
7 故障考虑和故障排除	28
7.1 概述	28
7.2 故障考虑	28
7.3 故障排除	28
8 确认	29
9 维护	29
10 技术文件	29
11 使用信息	29
附录 A (资料性附录) 要求的性能等级(PL _r)的确定	31
附录 B (资料性附录) 模块法和有关安全的模块图	33
附录 C (资料性附录) 单个元件 MTTF _d 值的计算或估计	34
附录 D (资料性附录) 估计每个通道 MTTF _d 的简化方法	40
附录 E (资料性附录) 对功能和模块的诊断覆盖率(DC)的估计	42
附录 F (资料性附录) 共因失效(CCF)的估计	44
附录 G (资料性附录) 系统性失效	46
附录 H (资料性附录) 控制系统有关安全部件组合的示例	48

附录 I (资料性附录) 示例	50
附录 J (资料性附录) 软件	55
附录 K (资料性附录) 图 5 的数值表示	57
参考文献	59