



中华人民共和国国家标准化指导性技术文件

GB/Z 162—2025/IEC TR 63161:2022

机械电气安全 安全完整性要求的分配 基本原理

Electrical safety of machinery—Assignment of safety integrity requirements—
Basic rationale

(IEC TR 63161:2022, Assignment of safety integrity requirements—
Basic rationale, IDT)

2025-12-03 发布

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
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 基于风险的定量方法	3
4.1 概述	3
4.2 功能安全分配中的步骤顺序	3
4.3 参考信息	5
5 功能安全分配的量化参数	6
5.1 概述	6
5.2 参数类型	7
5.3 伤害发生的概率	7
5.4 风险的量化	7
5.5 目标失效量	8
5.6 发生危险事件的概率 P_r	8
5.7 暴露参数 F_r	9
5.8 避免或限制伤害的可能性 A_v	9
5.9 要求类型和相关事件发生率	10
5.10 附加参数	13
6 安全功能分配的通用原则	15
6.1 基础	15
6.2 高要求或连续操作模式	16
6.3 低要求操作模式	16
7 要求模式分配	16
7.1 概述	16
7.2 分配准则	18
8 与 GB/T 15706 的关系	19
9 功能安全分配的工具	19
9.1 概述	19
9.2 选择独立参数	20
9.3 对数化参数	20
9.4 离散化参数	20
9.5 参数得分	21

9.6 严格意义上的评分方法	21
附录 A (资料性) SIL 分配工具数值分析的例子	23
A.1 概述	23
A.2 给参数项赋值	23
A.3 提取可容许的风险限度	23
A.4 IEC 62061 的风险矩阵	25
A.5 GB/T 16855.1 风险图	27
A.6 低要求操作模式的风险图	29
参考文献	32
图 1 功能安全分配中的步骤顺序	5
图 2 保护层、事件发生概率及其关系	12
图 3 根据亨利/熊本方程计算的危险发生率	17
图 4 根据 GB/T 15706 的风险要素	19
图 5 离散化参数	20
图 A.1 提取可容许的风险限度	24
图 A.2 基于 IEC 62061 的风险矩阵	25
图 A.3 最大容许 PFH 作为不同严重程度评分总和的函数	26
图 A.4 连续插值的表示	26
图 A.5 GB/T 16855.1 的风险图	28
图 A.6 每个严重程度级别的插值	29
图 A.7 低要求操作模式的风险图	30
图 A.8 低要求操作模式的风险图——来自 VDMA4315-1 ² 的图 7	31
表 1 参数概览	14
表 A.1 PFH 中 PLs 与范围的关系	29

前 言

本文件为规范类指导性技术文件。

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。

本文件等同采用 IEC TR 63161:2022《安全完整性要求的分配 基本原理》，文件类型由 IEC 的技术报告调整为我国的国家标准化指导性技术文件。

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。

本文件由中国机械工业联合会提出。

本文件由全国工业机械电气系统标准化技术委员会(SAC/TC 231)归口。

本文件起草单位：国家机床质量监督检验中心、中国科学院沈阳计算技术研究所有限公司、北京机床研究所有限公司、科德数控股份有限公司、上海电气集团股份有限公司中央研究院、西门子(中国)有限公司南京运动控制研发分公司、烟台金鹏矿业机械有限公司。

本文件主要起草人：张颖、薛瑞娟、吴怡然、张培森、高知国、吴翟、王楚婷、毕星瑞、刘贺强、尹震宇、王大伟、陈忠、姚坚、许庆砚。

机械电气安全 安全完整性要求的分配 基本原理

1 范围

本文件适用于已依据 GB/T 15706 对机械设备或流程工厂完成风险评估,并选定安全相关控制功能作为特定危险防护措施的场景。本文件描述了为选定功能分配安全完整性要求的基本逻辑原理示例。

该描述是通用的,并尽可能独立于可用于分配安全完整性要求的任何特定工具或方法。要求能表示为安全完整性等级(SIL)或性能等级(PL)。

本文件通过示例介绍了采用基于风险的定量方法时,这些工具和方法所体现的基本原理。

反之,本文件描述的逻辑能作为评估特定安全完整性分配方法或工具的参考依据,用以明确相应工具/方法在何种程度上遵循基于风险的定量方法,以及是否存在因其他考量而偏离该方法的情况。在实际应用中,基于风险的定量方法能因多种正当理由被修改或替代,此类理由的讨论与评估不在本文件范围内。通常,特定工具或方法会提供偏离定量逻辑的理由,以便在适当框架内进行讨论。

本文件以风险图和风险矩阵的形式提供了通用分配工具的分析示例。

本文件能用于安全相关控制功能的各种应用模式:连续模式、高要求模式和低要求模式。

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)

3 术语和定义

下列术语和定义适用于本文件。

ISO 和 IEC 维护的用于标准化的术语数据库网址如下:

IEC 电工百科:<http://www.electropedia.org/>

ISO 在线浏览平台:<http://www.iso.org/obp>

3.1

概率 probability

和一个随机事件相关的区间 $[0,1]$ 中的实数,用于定量地表示该事件出现的可能性。

注:更多信息见 5.2.2。

[来源:GB/T 2900.92—2015,103-08-02,有修改]

3.2

事件发生率 event rate

具有时间 t^{-1} 量纲的频率值,通常以 h^{-1} (每小时)或 a^{-1} (每年)为单位,用于表征随机事件的发生频次,以定量方式表示该事件在单位时间内预期发生的次数。