



中华人民共和国国家标准

GB/T 21562.2—2015

轨道交通 可靠性、可用性、 可维修性和安全性规范及示例 第 2 部分：安全性的应用指南

Railway applications—Specification and demonstration of
reliability, availability, maintainability and safety(RAMS)—
Part 2: Guide to the application for safety

2015-12-31 发布

2016-07-01 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	V
引言	VI
1 范围	1
2 规范性引用文件	2
3 术语、定义和缩略语	2
3.1 GB/T 21562—2008 中所用术语和定义解释	3
3.2 其他安全性术语	6
3.3 缩略语	8
4 相关机构/实体和系统层次与安全性概念指南	8
4.1 概述	8
4.2 系统中相关机构/实体	8
4.3 系统层次的概念	8
4.4 安全性概念	10
5 典型轨道交通系统的通用风险模型和通用功能危害检查表	13
5.1 概述	13
5.2 通用风险模型	13
5.3 风险评估流程	13
5.4 风险评估流程的应用	17
5.5 通用功能危害检查表	22
6 功能安全、功能安全要求、SI 目标、风险分配和 SILs 的应用指南	23
6.1 概述	23
6.2 功能安全和技术安全	23
6.3 风险分配的一般注意事项	25
6.4 SI 概念和 SIL 的应用	27
6.5 故障-安全系统指南	34
7 概率性方法和确定性方法相结合的安全举证指南	37
7.1 概述	37
7.2 安全举证	37
7.3 确定性方法	43
7.4 概率性方法	43
7.5 结合使用确定性方法和概率性方法	43
7.6 机械与混合(机电一体化)系统的方法	44
8 风险验收原理指南	44
8.1 概述	44
8.2 风险验收原理的应用	44
8.3 ALARP 原理	45

8.4 GAMAB(GAME)原理 46

8.5 MEM(最小内源性死亡率)安全原理(见 GB/T 21562—2008 中 D.3) 47

9 有关安全性证明文件(安全论据)的基本要素指南 48

9.1 概述 48

9.2 安全论据的用途 49

9.3 安全论据的范围 49

9.4 安全论据的层次 49

9.5 安全论据的阶段 50

9.6 安全论据结构 51

9.7 安全评估 54

9.8 与现有系统的接口 55

9.9 系统相互认可准则 56

附录 A (资料性附录) 风险评估流程的步骤 58

A.1 系统定义 58

A.2 危害识别 58

A.3 危害记录 61

A.4 后果分析 62

A.5 危害控制 62

A.6 风险评级 63

附录 B (资料性附录) 轨道交通系统层面的危害检查表 66

B.1 概述 66

B.2 基于受影响人员的危害分类示例 66

B.3 基于功能的危害分类示例 70

附录 C (资料性附录) 风险类别分类方法 74

C.1 功能细分方法(a) 74

C.2 系统(构成)分解方法(b) 74

C.3 危害细分方法(c) 75

C.4 基于危害原因的细分方法(d) 75

C.5 基于事故类型的细分方法(e) 76

附录 D (资料性附录) 英国铁路系统风险模型图解 77

D.1 构建风险模型 77

D.2 英国铁路风险模型的图解示例 77

附录 E (资料性附录) 技术和方法 81

E.1 概述 81

E.2 快速评级分析 82

E.3 结构化假设分析 82

E.4 HAZOP 83

E.5 状态转移图 83

E.6 消息序列图 83

E.7 失效模式影响与危害性分析-FMECA 85

E.8 事件树分析 85

E.9 故障树分析	86
E.10 风险图方法	87
E.11 其他分析技术	87
E.12 确定性方法和概率性方法指南	88
E.13 工具和选择	89
附录 F (资料性附录) 可用性概念的图形表示	91
附录 G (资料性附录) 建立风险验收准则的示例	92
G.1 ALARP 应用示例	92
G.2 哥本哈根地铁	94
附录 H (资料性附录) 安全论据概要示例	96
H.1 机车车辆	96
H.2 信号	97
H.3 基础设施	100
参考文献	102

前 言

GB/T 21562《轨道交通 可靠性、可用性、可维修性和安全性规范及示例》分为三个部分：

- 轨道交通 可靠性、可用性、可维修性和安全性规范及示例；
- 第 2 部分：安全性的应用指南；
- 第 3 部分：机车车辆 RAM 的应用指南。

本部分为 GB/T 21562 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本部分由国家铁路局提出。

本部分由全国牵引电气设备与系统标准化技术委员会(SAC/TC 278)归口。

本部分主要起草单位：株洲南车时代电气股份有限公司。

本部分参加起草单位：同济大学、铁道部标准计量研究所、中国铁道科学研究院机车车辆研究所、南车青岛四方机车车辆股份有限公司。

本部分主要起草人：王奇、邵志和。

本部分参加起草人：严云升、郭其一、孙超、王华胜、徐春华、罗君。

引 言

GB/T 21562—2008 列出了影响 RAMS 的因素,提出了有关安全性的风险管理方法,给出了一些风险验收原理的示例,并为整个轨道交通系统通用的生命周期的不同阶段定义了全面的任务。

GB/T 21562—2008 规定了轨道交通领域内的安全性和 RAM 特性。然而实际工作中不同主体在解释其安全性原理和/或需求时各不相同,并且 GB/T 21562—2008 在轨道交通系统及其子系统的具体应用中也存在差异。

本部分用于消除这些差异,并建立一致可行的方法来设定安全目标、评估风险、处理安全问题。本部分不规定任何特定的安全目标(安全目标由相关主管部门负责),只通过示例为特定条件下,设定目标、评估风险、形成安全要求和举证满意的安全等级等活动给出方法指南。目标设定方法的认可由轨道交通主管部门(RA)和安全主管部门(SRA)负责。

本部分涵盖整个轨道交通系统,并由 GB/T 21562—2008 涉及的所有用户组使用。用户组可为系统生命周期中从概念到处置各阶段的利益相关方(机构/实体)。

本部分仅涉及 GB/T 21562—2008 涵盖的问题,并对 GB/T 21562—2008 可能产生误解的地方进行澄清。

轨道交通 可靠性、可用性、 可维修性和安全性规范及示例

第 2 部分：安全性的应用指南

1 范围

1.1 GB/T 21562 的本部分对 GB/T 21562—2008 规定的轨道交通系统安全过程要求和系统生命周期各阶段安全活动所涉及的特定问题(见 1.3)给出指南。本部分适用于 GB/T 21562—2008 范围内涵盖的所有系统。本部分假设用户已熟悉安全问题,但在某些安全问题上 GB/T 21562—2008 缺乏详尽指导。

1.2 GB/T 21562—2008 是系统顶层的基本 RAMS 标准,本部分是对 GB/T 21562—2008 的补充说明,仅适用于 1.3 声明的安全问题。

1.3 本部分仅对 GB/T 21562—2008 范围内的下列问题给出指导:

- a) 轨道交通系统整体到其主要组成部分(如信号、机车车辆和基础设施等)的顶层通用风险模型的建立,模型组成部分及其相互作用的定义;
- b) 轨道交通系统(包括高速线路、轻轨和地铁等)通用功能危害检查表的建立;
- c) GB/T 21562—2008 中风险验收原理的应用;
- d) 轨道交通系统中功能安全性和容许风险定性评估的应用与示例;
- e) 功能安全要求和将安全目标分配给子系统(如轨道交通车辆、车门系统和制动系统等)的定义;
- f) 在系统生命周期中所有阶段,安全完整性等级的应用;
- g) 安全性举证的概率性方法和确定性方法应用;
- h) 安全证明文件(安全论据)的基本要素(包括维修和运营等)和典型结构。

1.4 表 1 说明了 GB/T 21562—2008 规定的生命周期各阶段安全活动的范围及其限制,并明确了主要参与者的角色/职责。宜结合本部分所有内容深入理解表 1。

表 1 特定生命周期阶段活动和本部分条款之间的对照

GB/T 21562—2008 的生命周期阶段	涉及的机构/实体	相关条款
1. 概念		—
2. 系统定义和应用条件	通常轨道交通主管部门(RA)负责轨道交通系统级,轨道交通支承工业(RSI)负责较低系统级	4.3 和 5.3.2.2
3. 风险分析	RA 或 RSI,取决于生命周期阶段	4.4、5.3 和 5.4
4. 系统需求	通常 RA 负责轨道交通系统级,RSI 负责较低系统级	5.3.2.2 和 6.2
5. 系统需求分配	负责设计所考虑系统的机构/实体	5.4.7、6.2、6.3 和第 8 章
6. 设计和实现	RSI	4.3、5.4 和第 6 章
7. 制造		—