

中华人民共和国铁道行业标准

TB/T 3133—2006

铁道机车车辆电子产品的可靠性、 可用性、可维修性和安全性(RAMS)

Reliability, Availability, Maintainability and Safety (RAMS) of
electronic products for railway rolling stock

2006-06-21 发布

2006-11-01 实施

中华人民共和国铁道部 发布



061120000050

目 次

前 言 II

1 范 围 1

2 规范性引用文件 1

3 术语和定义 1

4 电子产品的 RAMS 3

4.1 电子产品的 RAMS 与运行质量 3

4.2 产品 RAMS 的要素 3

4.3 影响 RAMS 的因素和 RAMS 失效分类 5

4.4 风 险 6

4.5 安全完整性 8

前 言

IEC 62278:2002《铁路应用 可靠性、可用性、可维修性和安全性规范及示例》标准是针对所有铁路应用的,它没有对特定铁路应用规定具体的 RAMS 指标、量值、要求和解决方案。本标准旨在针对铁道机车车辆的电子产品这个特定的应用范围,提出具体要求和量化,以便于 IEC 62278 规定的 RAMS 管理的实施。

本标准由中国南车集团株洲电力机车研究所提出并归口。

本标准由中国南车集团株洲电力机车研究所负责起草。

本标准主要起草人:严云升、言武、刘贵。

铁道机车车辆电子产品的可靠性、可用性、 可维修性和安全性(RAMS)

1 范 围

本标准定义了铁道机车车辆电子产品的可靠性、可用性、可维修性和安全性以及其相互作用;规定了电子产品的 RAMS 指标、量值、要求和解决方案。

本标准适用于铁道机车车辆上的各种电子产品。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

TB/T 3021—2001 铁道机车车辆电子装置

IEC 60050(191):1990 国际电工术语 第 191 章:可信性和服务质量

IEC 61508 电工/电子/可编程电子安全相关系统的功能安全性

IEC 62278:2002 铁路应用 可靠性、可用性、可维修性和安全性规范及示例

IEC 62279:2002 铁路应用 通信、信号和处理系统 铁路控制和防护系统软件

3 术语和定义

IEC 60050(191):1990 确立的以及下列术语和定义适用于本标准。

3.1

实际平均无故障时间 **actual mean time between failure(AMTBF)**

由现场统计得到的该产品平均故障间隔时间。

3.2

评估 **assessment**

为获得对产品适用性基于证据的评价所进行的调查工作。

3.3

评审 **audit**

用来决定一个产品是否符合设计方案、有效实施和是否适用于指定要求的系统化和独立的测试。

3.4

可用性 **availability**

在要求的外部资源得到保证的前提下,产品在规定的条件下和规定的时刻或时间区间内处于可执行规定功能状态的能力。

3.5

修复性维修 **corrective maintenance**

故障识别后,使产品恢复到能执行规定功能状态所实施的维修。

3.6

失效模式 **failure mode**

故障时与运行状况有关的指定项目失效原因的预计或观察结果。

3.7

失效率 failure rate

产品瞬间 T 失效并位于指定的时间区间 $(t, t + \Delta t)$ 内,其条件概率与时间间隔 Δt 的比例,当 Δt 趋近于 0(假设在该区间的起始时刻工作正常)时所得到的极限值(如果存在)。

注:在应用中,当走行距离或工作周期比时间对失效率更加相关时,时间单位可由相应的距离单位或周期的单位来替代。

3.8

故障模式 fault mode

对于规定的要求功能,故障项目的一种可能的状态。

3.9

隐患 hazard

潜在的对人或环境造成伤害的物理状态。

3.10

可维修性 maintainability

在规定的条件下,使用规定的程序和资源进行维修时,对于给定使用条件下的产品在规定的时间内,能完成指定的实际维修工作的能力。

3.11

维修 maintenance

为保持或恢复产品处于能执行规定功能的状态所进行的所有技术和管理工作,包括监督活动。

3.12

任务概要 mission profile

在生命周期的运行阶段内,任务中有关参数(次数、装载量、速度、距离、站台、隧道等)的预期范围和变化略图。

3.13

预防性维修 preventive maintenance

为了防止功能降级、减少故障发生概率而实施的定期或根据预定判据进行的维修。

3.14

铁路主管部门 railway authority

对运营铁路系统的管理者负有全部责任的机构。

注:对总系统或其部件和生命周期活动而言,铁路主管部门的责任有时分摊给一个或多个团体或组织。例如:

——系统的一个或多个部件拥有者或代理商;

——系统操作员;

——系统的某一部件或多个部件的维护者;

⋮

以上分配以法定文件或合同为依据,因此在系统生命周期的早期阶段,应明确规定这些责任。

3.15

铁路工业 railway support industry

表示整个铁路系统、子系统和组成部件的供应商的通用术语。

3.16

RAMS

Reliability, Availability, Maintainability 和 Safety 第一个字母的组合(前三者组合缩写为 RAM)。

3.17

可靠性 reliability

项目在规定条件下和规定时间区间(t_1, t_2)内,完成所需功能的能力。[IEC 60050(191):1990]

3.18

风险 risk

导致危害的隐患发生的概率及危害的严重等级。

3.19

安全性 safety

防止危害产生不容许的风险。

3.20

安全完整性 safety integrity

在所有规定的条件下系统于给定时间内满意地实现要求安全功能的可能性。

3.21

安全完整性级别(SIL) Safety integrity level

许多已规定的断续的数值之一,这些数值规定了分配给安全相关系统的安全功能的安全完整性级别。数值越大,安全完整性级别越高。

3.22

产品(系统)生命周期 Product(system) life cycle

从产品(系统)的构思开始到系统不能再使用被退役或淘汰的时间内所发生的活动。

3.23

系统失效 systematic failures

在某些特定的环境下或某些特定的输入组合情况下导致失效,在任何阶段的安全使用期内由于错误产生的故障。

3.24

容许风险 tolerable risk

铁路主管部门可以接受的产品的最大级别风险。

4 电子产品的 RAMS

4.1 电子产品的 RAMS 与运行质量

4.1.1 RAMS 是产品的长期工作特性,在产品的整个生命周期内,它可通过应用已建立的工程概念、方法、工具和技术而实现。产品的 RAMS 可用组成产品的各零部件的定性和定量指标来表示,以达到规定的要求、可用和安全,RAMS 是可靠性、可用性、可维修性和安全性的组合。

4.1.2 铁路系统的目的是为了在指定的时间内安全地达到轨道运输的规定水平。RAMS 说明了产品能保证达到此目标的置信度。产品的 RAMS 对交付给用户后的运行质量有明显影响。运行质量还受功能参数和性能参数的影响,如使用频度、运行规律及费用结构。其关系见图 1。



图 1 运行质量与产品 RAMS

4.2 产品 RAMS 的要素

4.2.1 安全性和可用性相互关联,对安全性要求和可用性之间的冲突的管理不善,会阻止获得可靠的产品。产品 RAMS 各要素(可靠性、可用性、可维修性和安全性)的相互关系见图 2。

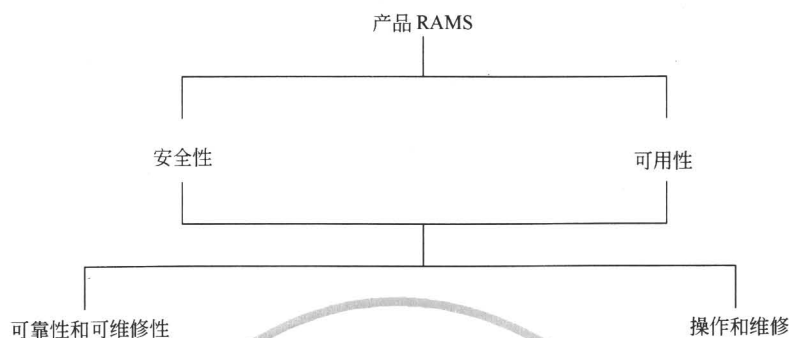


图2 产品 RAMS 各要素之间的关系

4.2.2 产品不仅需满足可靠性和可维修性要求,还需通过合适的操作和维修规则进行维修,才能达到运行期间的安全性和可用性目标。

4.2.3 安全防护,作为表示避免产品失效或不合理的操作行为造成危害的元素,是 RAMS 的更深层次上的要素,但安全防护需要考虑的事项不在本标准的范围之内。

4.2.4 可用性的技术概念以下述内容为基础:

a) 可靠性包括:

- 指定应用中所有可能的产品失效模式与周围环境;
- 每个失效发生的概率,或者每个失效发生的几率;
- 失效对系统性能的影响。

可靠性通常用平均无故障时间来衡量。

b) 可维修性包括:

- 执行计划维修的时间;
- 故障检测、识别及定位的时间;
- 失效系统的恢复时间(计划之外的维修);
- 如需专用工具,由制造厂提供专用工具。

可维修性用恢复到正常状态平均所需的时间来衡量。

c) 操作和维修包括:

- 产品生命周期内全部可能的工作模式和必要维修;
- 人为因素。

可用性用实际可用的时间对全运行时间的比率表示。计划以内的维修或日常的不需扣车的临修不影响可用性。

4.2.5 安全性的技术概念以下述内容为基础:

a) 在各种运行、维护和环境模式下系统中所有可能的隐患。

b) 每个隐患的性质,包括隐患结果的严重性。

c) 安全性/安全相关的失效包括:

- 导致隐患的全部系统失效模式(安全相关的失效模式),它是全部可靠性失效模式的子集(4.2.4a);
- 安全相关的每个系统失效模式的概率;
- 在应用中可能导致事故的事件的顺序和/或并发率、失效工作状态、环境条件等(即导致事故的隐患);
- 在运行中,每个事件发生的概率、故障、工作状态和环境条件等。

d) 系统安全相关的部件的可维修性包括:

- 与安全相关失效模式和隐患有关的部件及其组件维修的方便性;

- 安全相关部件在维修工作期间内发生错误的概率；
 - 系统恢复到安全状态的时间。
 - e) 系统操作及安全相关部件的维修包括：
 - 人为因素对系统安全相关部分的有效维修及系统安全操作的影响；
 - 用于系统安全相关部分的有效维修和系统安全操作的工具、设备和工序；
 - 有效的控制、处理隐患的措施并减轻隐患的后果。
- 4.2.6 系统内部失效与铁路应用环境的电磁干扰有关,所有系统失效都对系统可靠性产生负面影响,而只有其中的安全相关失效模式才对安全性产生负面影响,它们的联系见图 3。

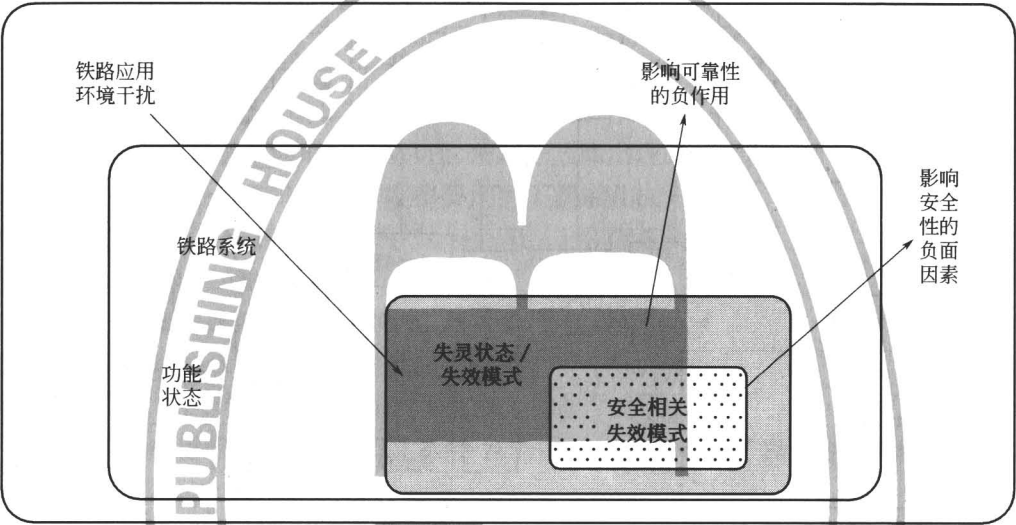


图 3 系统内部失效的影响

- 4.2.7 只有考虑了 RAMS 各要素的相互作用,并获得了优化的 RAMS 组合才能实现一个可靠的产品或系统。
- 4.3 影响 RAMS 的因素和 RAMS 失效分类
- 4.3.1 产品 RAMS 受来自 3 个方面因素的影响:产品生命周期中系统内部的失效(系统环境)、操作过程中强加给产品的失效(操作环境)和维修工作中强加给产品的失效(维修环境),这些失效源能够相互作用,其关系见图 4,详细情况见图 5。

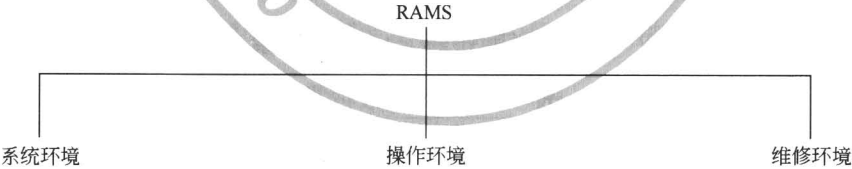


图 4 影响 RAMS 的因素

- 4.3.2 用于获得 RAMS 要求的方法基于采用预防措施,使在生命周期阶段由错误所引起的损伤概率最小。预防措施的组合包括：
- a) 预护:降低损伤发生的概率；
 - b) 防护:降低损伤后果的严重性。
- 4.3.3 表 1 规定了适用于铁路应用 RAM 的失效分类。

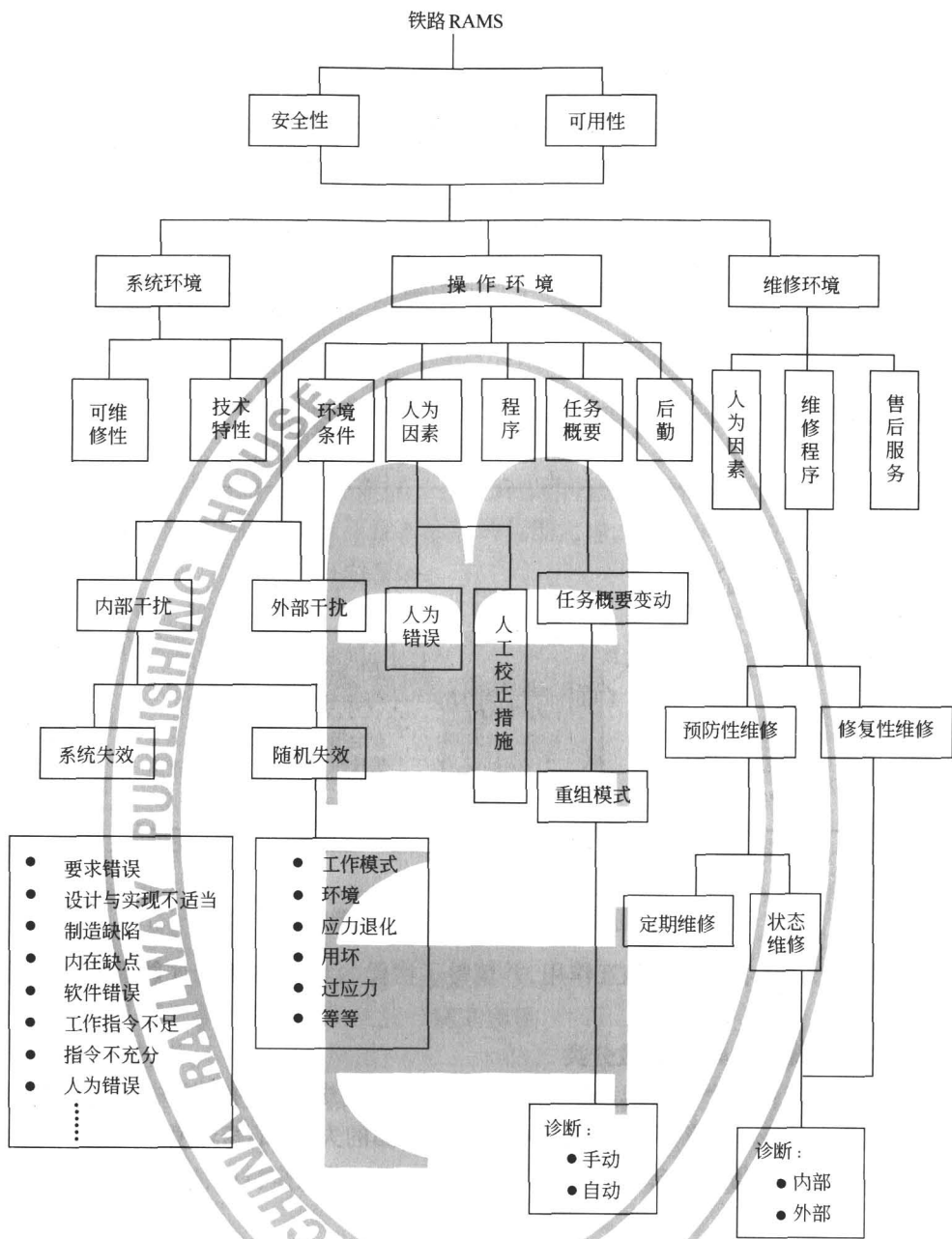


图 5 影响铁路 RAMS 的因素

表 1 RAM 失效种类

失效分类	定 义
重大(停车故障)	导致远大于规定时间的晚点、远远超出指定等级的费用、阻止列车运行及/或产生的故障
主要(运行故障)	系统为获得规定性能应整修的故障； 不导致晚点或不超出重大失效中规定的最小阈值费用的故障
次要	不阻止系统获得规定性能的故障； 不符合重大失效和主要失效标准的故障

4.4 风 险

4.4.1 风险概念由以下两个元素组成：

- a) 导致危害的事件发生或事件组合的概率，即这些事件发生的频繁程度；

b) 危害的后果。

4.4.2 铁路应用中,危害事件发生的概率或频度的典型分类见表2。

表2 危害事件出现的频度

分 类	定 义
频繁	频繁地出现,危害将一直存在
经常	发生多次,危害可以预期经常出现
有时	可能发生几次,危害预期有几次出现
很少	在系统生命周期的某个时期可能发生,危害能合理地预期出现
极少	不太可能发生但可能存在,可假定危害极少出现
几乎不可能	几乎不可能发生,可假定危害不会发生

4.4.3 对于机车车辆上的电子产品通常用更换一次重要元器件或一块插件作为一次故障来统计故障发生的次数。用实际平均无故障时间 AMTBF 来划分故障出现的频度。

频繁	AMTBF < 1 250 h(每季度都要发生 1 次或几次)
经常	2 500 h > AMTBF ≥ 1 250 h(一季度以上发生 1 次)
有时	5 000 h > AMTBF ≥ 2 500 h(半年以上发生 1 次)
很少	10 000 h > AMTBF ≥ 5 000 h(1 年以上发生 1 次)
极少	20 000 h > AMTBF ≥ 10 000 h(2 年以上发生 1 次)
几乎不可能	AMTBF ≥ 20 000 h(4 年以上发生 1 次)

4.4.4 表3描述了典型的危害严酷等级和所有铁路系统相关的每个严酷等级危害的结果。

表3 危害严酷等级

严酷等级	对环境或人的影响	运行结果	电子产品故障示例
特大	多人死亡,和/或是多方面的严重伤害,和/或对环境的较多伤害		可引发火灾、列车超速冒进信号
重大	一人死亡,和/或是单个严重伤害,和/或是对环境产生明显的伤害	主系统失效	机破、晚点超过 30 min
次要	较小的损伤和/或对环境的明显影响	重要的系统伤害	牵引力/制动力部分损失造成的列车少许晚点、客车电源故障、门失灵等
轻微	可能存在的较小的伤害	较小的系统损害	轻微:不造成列车晚点和影响舒适的临修和碎修
注:电子产品故障的后果有可能随具体运行情况而稍有变化。			

4.4.5 风险的评估

风险的评估应结合危害性事件发生的频度及其结果的严重性来进行,其频度-结果矩阵见表4。

表4 频度-结果矩阵

危害性事件的发生频度	风 险 等 级			
频繁				
经常				
有时				
很少				
极少				
几乎不可能				
	轻微	次要	重大	特大
	危害结果的严酷等级			

4.4.6 表 5 规定了定性的风险分类及应对每一类风险的措施。

表 5 定性的风险种类

风险种类	对每一类风险所采取的措施
不容许的	应该消除,不允许装车
不希望的	当风险减少不可行时,应经过铁路主管部门或安全规章主管部门同意后方可接受
容许的	采用充分控制并经铁路主管部门同意后可以接受
可忽略的	有或无铁路主管部门同意均可接受

4.4.7 风险的评估和验收见表 6。

表 6 风险评估和验收

危害性事件的发生频度	风 险 等 级			
频繁	不希望的	不容许的	不容许的	不容许的
经常	容许的	不希望的	不容许的	不容许的
有时	容许的	不希望的	不希望的	不容许的
很少	可忽略的	容许的	不希望的	不希望的
极少	可忽略的	可忽略的	容许的	容许的
几乎不可能	可忽略的	可忽略的	可忽略的	可忽略的
	轻微	次要	重大	特大
	危害结果的严酷等级			

4.4.8 不同电子产品故障时对列车造成的危害严重程度是不同的。各产品在设计阶段应根据本产品故障造成的危害程度知道所能允许的故障频度,从而采取各种避错和容错措施来达到规定的可靠性要求。或是适当采取冗余措施来降低故障造成的危害严酷等级,从而使产品风险评估达到可容许的等级。

4.4.9 产品风险评估后应按 4.4.7 条规定,决定该产品是否能装车或继续投入运行。

4.5 安全完整性

4.5.1 机车车辆上的电子主产品安全完整性应不低于 IEC 61508 中规定的低需要模式 SIL 3 级,执行所要求功能的平均失效率 $\lambda: 10^{-4} \leq \lambda < 10^{-3}$ 。系统功能的安全完整性的置信度可以通过有效地结合特定的系统结构、方法、工具和技术来得到。实现更高的安全要求功能则可能需要更加昂贵的费用。

4.5.2 安全完整性是定量元素(一般和硬件有关,如随机失效)和非定量元素(一般与软件技术条件、文件、程序等等的失效有关)的组合,为了达到预定的安全等级,除产品本身外还必须从外部环境以及系统来采取措施,以减少风险。

4.5.3 系统的安全功能应用其他相关标准规定的体系结构、方法、工具和技术来实现。例如 IEC 62279:2002 规定了开发软件系统的方法,TB/T 3021—2001 规定了电子产品的工作环境和电磁兼容性能及其试验方法。

4.5.4 故障诊断对缩小故障范围、减少故障的危害性及缩短维修时间是十分重要的。对 SIL 3 级别,图 3 中安全相关失效模式的诊断覆盖率应大于等于 90%。

4.5.5 产品及使用该产品的系统都应执行故障导向安全的原则,在所有失效模式下,及时采取相应措施来减少故障的危害性。

4.5.6 对于市场上现货供应的部件,应估计其对产品的规定环境及性能的限制和约束,它不应影响整个产品的安全完整性等级。

中 华 人 民 共 和 国
铁道行业标准
铁道机车车辆电子产品的可靠性、可用性、
可维修性和安全性(RAMS)

Reliability, Availability, Maintainability and Safety (RAMS) of
electronic products for railway rolling stock

TB/T 3133 — 2006

*

中国铁道出版社出版、发行
(100054,北京市宣武区右安门西街8号)
读者服务部电话:市电(010)51873174,路电(021)73174
北京市兴顺印刷厂印刷
版权专有 侵权必究

*

开本:880 mm×1 230 mm 1/16 印张:1 字数:15 千字
2006 年 10 月第 1 版 2006 年 10 月第 1 次印刷

*

统一书号:15113·2310 定价:8.00 元