ICS 45.060
S 39

# 中华人民共和国国家标准

GB/T 21562—2008/IEC 62278:2002

# 轨道交通　可靠性、可用性、可维修性和安全性规范及示例

**Railway applications—Specification and demonstration of reliability, availability, maintainability and safety(RAMS)**

(IEC 62278:2002,IDT)

2008-03-24 发布　　2008-11-01 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

中华人民共和国
国家标准
**轨道交通 可靠性、可用性、可维修性和安全性规范及示例**
GB/T 21562—2008/IEC 62278:2002
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.5 字数 101 千字
2008年7月第一版 2008年7月第一次印刷
*
书号:155066·1-32046 定价 36.00 元



GB/T 21562-2008

# 前　言

本标准等同采用 IEC 62278:2002《轨道交通　可靠性、可用性、可维修性和安全性(RAMS)规范及示例》(英文版)。

本标准等同翻译 IEC 62278:2002。

为便于使用,本标准做了下列编辑性修改:

a) “本国际标准”一词改为“本标准”;

b) 删除国际标准的前言。

本标准的附录 A、附录 B、附录 C、附录 D、附录 E 为资料性附录。

本标准由全国牵引电气设备与系统标准化技术委员会提出并归口。

本标准起草单位:株洲南车时代电气股份有限公司、南车四方机车车辆股份有限公司、中国南车集团株洲电力机车有限公司、中铁电气化勘测设计研究院、同济大学、铁道部标准计量研究所。

本标准主要起草人:严云升、范祚成、刘贵、郭立平、高道行、张志龙、苏光辉、程祖国、呼爱蝉。

# 引　言

本标准为轨道交通主管部门及其支承工业提供了一个流程，它使相应方法的实施达到对可靠性、可用性、可维修性和安全性(用 RAMS 表示)的管理。本标准以 RAMS 需求规范的流程及示例为基础，目的是促进共识和对 RAMS 的管理。

在轨道交通应用生命周期的所有阶段，轨道交通主管部门及其支承工业可以系统地应用本标准去开发特定的轨道交通应用 RAMS 需求并达到与之一致。本标准定义的系统分级方法有助于复杂轨道交通的各个要素间 RAMS 相互作用的评估。

在不同的采购策略中，本标准将促进轨道交通主管部门及其支承工业的相互合作，以获得最理想的轨道交通 RAMS 和费用的组合。

本标准规定的流程假定轨道交通主管部门及其支承工业有规定质量、性能和安全的行业政策。本标准中规定的方法应与 GB/T 19000 系列标准的质量管理内容保持一致。

# 目　次

# 轨道交通　可靠性、可用性、可维修性和安全性规范及示例

## 1　范围

本标准定义了RAMS各要素(可靠性、可用性、可维修性和安全性)及其相互作用,规定了一个以系统生命周期及其工作为基础、用于管理RAMS的流程,使RAMS各个要素间的矛盾得以有效地控制和管理。

本标准不规定轨道交通特定应用中的RAMS指标、量值、需求或解决方案,不指定保证系统安全的需求。这些应在各类特定应用的RAMS子标准中规定。

本标准适用于:

a)　所有轨道交通应用中和在此应用中各个不同层次的RAMS规范与说明;例如,从整个轨道线路到位于轨道线路上的主要系统以及到这些主要系统内独立的或综合的子系统及其部件,包括所含软件,特别是:

——新型系统;

——集成到在本标准制定前的既有系统中工作的新系统,尽管它一般不能应用于既有系统的其他方面;

——在本标准制定前的既有系统的更新,尽管它一般不能应用于此系统的其他方面。

b)　应用中生命周期所有相关的阶段。

c)　轨道交通主管部门及其支承工业的使用。

注:应用导则在本标准的要求中给出。

## 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。

GB/T 19001—2000　质量管理体系　要求(idt ISO 9001:2000)

GB/T 20438(所有部分)　电气/电子/可编程电子安全相关系统的功能安全[IEC 61508(所有部分),IDT]

IEC 60050(191):1990　国际电工术语　第191章:可信性和运行质量

IEC 62279　轨道交通　通信、信号和处理系统　轨道交通控制和防护系统软件

EN 50129:2003　轨道交通　信号用安全相关电子系统

## 3　术语和定义

下列术语和定义适用于本标准。

3.1

**分配　apportionment**

系统的RAMS要素在组成系统的各部分间进行分解的过程,以给各部分提出单独的目标。

3.2

**评估　assessment**

根据调查取证,对产品的适用性进行评价。

3.3

**评审 audit**

用来决定对一个产品的要求是否符合计划安排、有效实施和是否适用于指定目标的系统化和独立的考核。

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

**调试 commissioning**

在验证系统或产品满足规定要求之前拟采取的活动的总称。

3.6

**共因失效 common cause failure**

由一个事件引起两个或两个以上部件同时失效使系统不能执行规定功能的故障。

3.7

**一致性 compliance**

产品的特性或参数满足规定要求的证明。

3.8

**配置管理 configuration management**

用技术和管理来指挥和监控的一门学科，来证实一个项目配置的功能和物理特性，控制这些特性的改变、记录和汇报改变的过程、实现状态以及证实与特定的需求相一致。

3.9

**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。

3.10

**从属失效 dependent failure**

一组事件的失效，其概率不能用单个事件的无条件概率的简单乘积来表示。

3.11

**不可用时间 down time**

产品处于停机状态的时间间隔。

[IEC 60050(191)，修改过]

3.12

**失效原因 failure cause**

在设计、生产或使用期间导致失效的原因。

[IEC 60050(191)]

3.13

**失效模式 failure mode**

失效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。

3.14

**失效率 failure rate**

产品在瞬间 $T$ 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 $\Delta t$ 的比例，当 $\Delta t$ 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数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数来替代。

3.15

**故障模式　fault mode**

相对于给定的规定功能，故障产品的一种可能的状态。

[IEC 60050(191)]

3.16

**故障树分析　fault tree analysis**

以故障树的形式进行分析来确定故障模式的方法，它用于确定产品、子产品或外部事件或它们的组合可能导致产品的一种已给定的故障模式。

3.17

**危害　hazard**

对人造成潜在伤害或对环境造成潜在损害的物理状况。

3.18

**危害记录　hazard log**

所有安全管理活动、危害确定、作出的决定和解决方法的记录或参考文件，也可称为“安全记录”。

[EN 50129]

3.19

**后勤保障　logistic support**

在所需的生命周期费用下准备和组织用来操作和保持系统工作在规定可用性水平下的所有资源。

3.20

**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区间内，能完成指定的实际维修工作的能力。

[IEC 60050(191)]

3.21

**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。

[IEC 60050(191)]

3.22

**维修策略　maintenance policy**

用作某一产品的维修梯队、契约层和维修作业层之间的相互关系的说明。

[IEC 60050(191)]

3.23

**任务　mission**

系统执行的基本工作的目标说明。

3.24

**任务概要　mission profile**

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

3.25

**预防性维修　preventive maintenance**

为了防止功能降级、减少失效概率而实施的定期或根据预定判据进行的维修。

3.26

**轨道交通主管部门　railway authority**

对运营轨道交通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，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；
——等等。

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。

3.27

**轨道交通支承工业 railway support industry**

表示整个轨道交通系统、子系统和组成部件的供应商的通用术语。

3.28

**可靠性和可维修性规划 reliability and maintainability programme**

用书面形式写出的一组时间调度活动、资源和事件，适用于组织结构、责任、工序、运行情况、能力和资源的实现，它们一起保证达到规定合同或项目关于可靠性和可维修性的要求。

3.29

**RAMS**

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

3.30

**可靠性 reliability**

产品在规定条件下和规定时间区间（$t_1$，$t_2$）内完成规定功能的能力。

[IEC 60050(191)]

3.31

**可靠性增长 reliability growth**

产品持续地改进可靠性性能措施表征的一种状态。

[IEC 60050(191)]

3.32

**修理 repair**

修复性维修的一部分，是在该项目上实施的人工作业。

[IEC 60050(191)]

3.33

**恢复 restoration**

产品在故障发生后再次能执行规定功能的事件。

3.34

**风险 risk**

导致伤害的危害发生概率及伤害的严重等级。

3.35

**安全性 safety**

免除不可接受的风险影响的特性。

3.36

**安全论据 safety case**

产品符合规定安全要求的书面说明。

3.37

**安全完整性 safety integrity**

在所有规定的条件下系统在规定时间内实现所需安全功能的可能性。

3.38

**安全完整性等级（SIL）**

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要

求。数值越大,安全完整性等级越高。

3.39

**安全计划 safety plan**

一组适合于组织机构、责任、工序、活动、能力和资源实现的时间调度活动、资源和事件的文档,它们一起保证达到规定合同或工程关于安全性的要求。

3.40

**安全规章主管部门 safety regulatory authority**

通常是有责任规定或同意这些安全要求且保证轨道交通符合这些要求的国家政府机关。

3.41

**系统生命周期 system life cycle**

从系统的构思开始到系统不能再使用而退役或淘汰的时间内所发生的活动。

3.42

**系统性失效 systematic failures**

在某些特定的环境下或某些特定的输入组合情况下,在任何阶段的安全生命周期活动中由于错误产生的失效。

3.43

**容许风险 tolerable risk**

轨道交通主管部门可以接受的产品最大级别的风险。

3.44

**确认 validation**

用客观证据及检验来确定是否满足指定的预期用途的特定要求。

3.45

**验证 verification**

用客观证据及检验来确定是否满足规定要求。

注:关于验证(Verification)和确认(Validation)的说明见图 11 和 5.2.9。

## 4 轨道交通 RAMS

### 4.1 简介

4.1.1 本章提供了有关 RAMS 和 RAMS 工程的基本资料,其目的是使读者有足够的背景知识,从而使本标准有效地运用到轨道交通系统中。

4.1.2 轨道交通 RAMS 对轨道交通主管部门规定的运行质量起主要作用。轨道交通 RAMS 由几个分别起一种作用的要素组成。因此,本章结构如下:

a) 4.2 考查了轨道交通 RAMS 与运行质量之间的关系。

b) 4.3~4.8 考查了轨道交通 RAMS 的各个方面,即:

——RAMS 的要素;

——影响 RAMS 的因素和获得 RAMS 的方法;

——风险和安全完整性。

4.1.3 本章应尽可能使用已规定的国际术语以及本标准第 3 章定义的轨道交通行业形成的新术语或已经认可的术语。

4.1.4 本标准中“系统、子系统、部件”的顺序用来说明从任意完整应用到其组成部分的细目分类,每个术语(系统、子系统和部件)的精确界限取决于特定的应用。

4.1.5 系统可定义为用一定的方法组织起来获得特定功能的子系统和部件的集合。这些功能分配给系统中的子系统和部件,且系统的性能和状态随着子系统或部件功能的改变而改变。系统对输入作出

响应以产生指定的输出，同时与环境相互影响。

### 4.2 轨道交通 RAMS 和运行质量

4.2.1 本条介绍关于某项任务的 RAMS 和运行质量之间的关系。

4.2.2 RAMS 是系统的长期工作特性，在系统的整个生命周期内，它可通过应用已建立的工程概念、方法、工具和技术而实现。系统的 RAMS 可以用与系统或子系统或组成系统的部件有关的定性和定量指标来表示，且可保证达到规定的功能、可用和安全。本标准中系统 RAMS 是可靠性、可用性、可维修性以及安全性(RAMS)的组合。

4.2.3 轨道交通 RAMS 说明了系统能保证在指定的时间内安全地达到轨道运输规定水平的置信度。轨道交通 RAMS 对交付给用户的运行质量有明显的影响；运行质量还受有关功能和性能参数的其他特性影响，例如运行频度、运行规律性和费用结构。其关系见图 1。


图 1 运行质量和轨道交通 RAMS

### 4.3 轨道交通 RAMS 的要素

4.3.1 本条介绍了在轨道交通系统环境中，RAMS 各要素(可靠性、可用性、可维修性和安全性)之间的相互关系。

4.3.2 安全性和可用性相互关联，对安全性要求和可用性要求之间的冲突如果管理不善，会妨碍获得可信的系统。轨道交通 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。

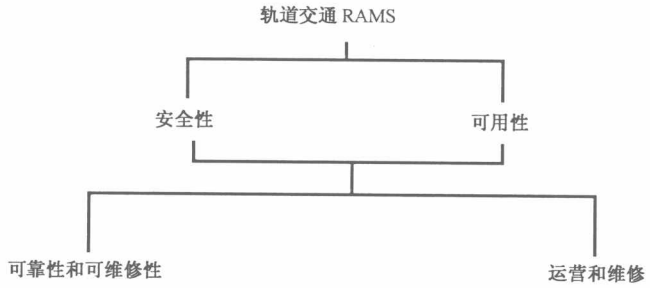


图 2 轨道交通 RAMS 各要素间的相互关系

4.3.3 满足了可靠性和可维修性所有要求，并控制正在进行的、长期的维修、运营活动及系统环境才能达到运行期间的安全性和可用性目标。

4.3.4 安全防护，作为表示轨道交通系统对抗故意破坏与不合理的人员行为的防御能力，是 RAMS 的更深层次上的要素。但是，安全防护需要考虑的事项不在本标准的范围之内。

4.3.5 可用性的技术概念以下述内容为基础：

a) 可靠性包括：
   ——规定应用及环境下所有可能的系统失效模式；
   ——每个失效发生的概率，或者每个失效出现的几率；
   ——失效对系统功能的影响。

b) 可维修性包含：
   ——执行计划维修的时间；
   ——故障检测、识别及定位的时间；
   ——失效系统的修复时间(计划之外的维修)。

c) 运营和维修包括：

——系统生命周期内全部可能的工作模式和必要维修；

——人为因素问题。

4.3.6 安全性的技术概念以下述内容为基础：

a) 在所有运行、维护和环境模式下系统中所有可能的危害。

b) 每个危害的特征，以危害后果的严重性表示。

c) 安全性/安全相关的失效包括：

——导致危害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[4.3.5.a)]；

——每个安全相关系统失效模式发生的概率；

——在应用中，可能导致事故的事件(即导致事故的危害)的顺序和/或并发率、失效、工作状态、环境条件等等；

——应用中，每个事件、失效、工作状态和环境条件等出现的概率。

d) 系统的安全相关部件的可维修性包括：

——与安全相关失效模式或危害有关的系统中子系统或其部件维修的方便性；

——系统安全有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) 系统操作与系统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运营的影响；

——用于系统安全有关部分的有效维修和系统安全运营的工具、设备和工序；

——有效的控制、处理危害并减轻危害后果的措施。

4.3.7 系统失效，它运行于应用与环境的范围之内，将对系统的性能产生某些影响。所有失效都对系统可靠性产生负面影响，在特定应用中，仅当某些特定失效才对安全性有负面影响。此外，外界环境也影响系统功能，进而影响轨道交通的安全性。它们的联系见图3。

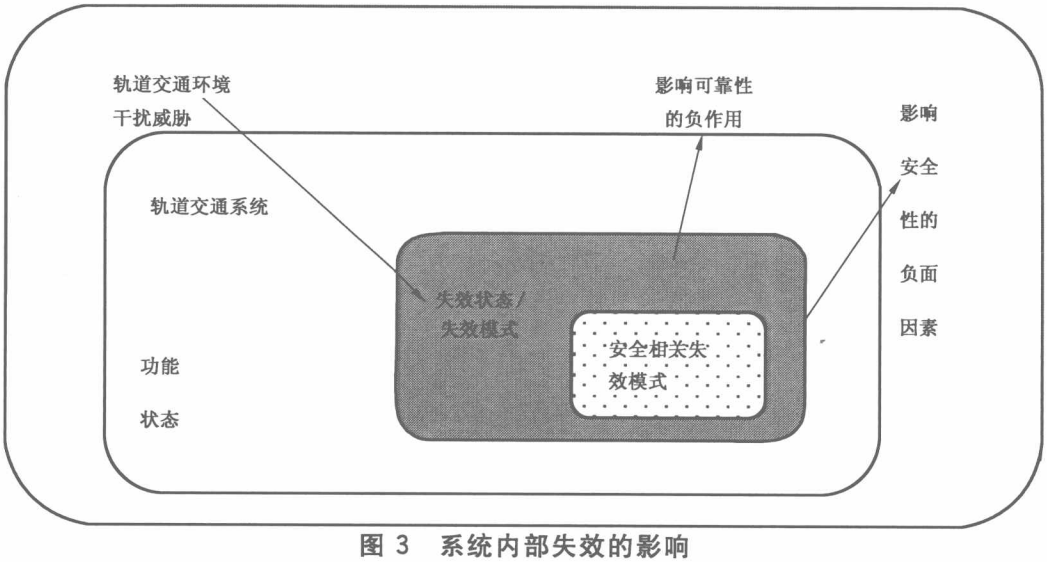


图3 系统内部失效的影响

4.3.8 只有考虑了系统中RAMS各要素的相互作用和本标准，并获得了系统优化的RAMS组合，才能实现一个可靠的轨道交通系统。

## 4.4 影响轨道交通RAMS的因素

### 4.4.1 总则

4.4.1.1 本条介绍和规定了一个流程，用于确定影响轨道交通系统RAMS的因素，尤其是对人为因素

影响的考虑。这些因素及其作用是系统 RAMS 需求规范的输入。

4.4.1.2 轨道交通系统 RAMS 受来自三个方面因素的影响：来源于在系统生命周期中任何阶段系统内部的失效(系统环境)、运营过程中强加给系统的失效(运营环境)和在系统维修工作中强加给系统的失效(维修环境)。这些失效源能够相互作用，其关系见图 4，详图见图 5。

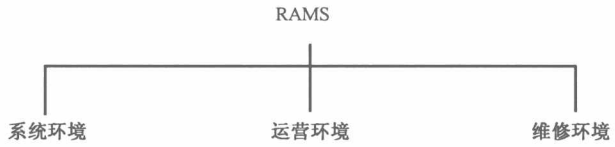


图 4 对 RAMS 的影响

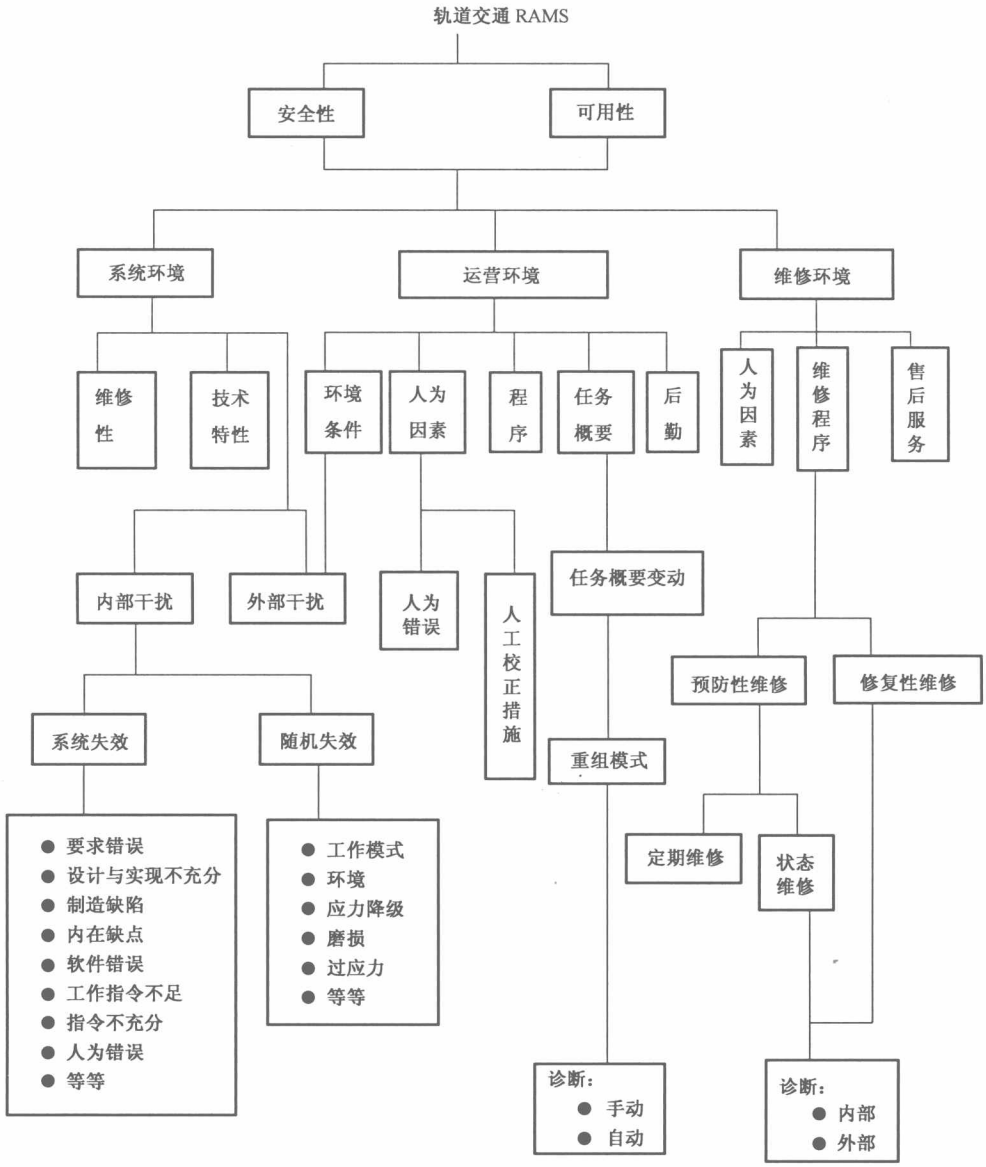


图 5 影响轨道交通 RAMS 的因素

4.4.1.3 为实现可靠的系统，需要确定影响系统 RAMS 的因素，估计其影响，并且在系统的生命周期内应用适当的控制来驾驭产生这些影响的原因，使系统性能得到优化。

4.4.2 **因素分类**

4.4.2.1 本条详细说明定义因素的流程，这些因素将影响系统成功地达到符合规定 RAMS 的要求。

4.4.2.2 工业应用中影响系统 RAMS 的因素是普遍存在的。图 5 包含影响轨道交通系统 RAMS 的一些普遍因素，还说明了这些因素之间的相互作用。为了确定影响轨道交通系统 RAMS 的具体因素，在指定的系统环境中应考虑每一个普通的影响因素。

4.4.2.3 关于人为因素对系统 RAMS 的影响，其分析在本标准要求的“系统途径”中是固有的。

4.4.2.4 人为因素可以规定为人的性格、期望和行为对系统的影响。这些因素涉及到人体解剖学、生理学和心理学等方面。在满足人的健康、安全和工作后，人为因素的这些思想指导人们有效率地工作。

4.4.2.5 典型的轨道交通包括很广的人群，从旅客、操作人员、维持轨道交通系统运营的人员到影响轨道交通运营的其他人员，例如平交道口的汽车司机。每人都用不同的方法反作用于轨道交通。显然，人类对轨道交通系统 RAMS 的潜在影响是很大的。因此，在整个系统生命周期内，与许多其他的工业应用相比，为达到轨道交通 RAMS 需求须更严格控制人为因素。

4.4.2.6 人可认为拥有有益于轨道交通系统 RAMS 的能力。为达到这一目标，在整个生命周期内，应确定和管理人为因素影响轨道交通 RAMS 的方式。在系统的设计和开发阶段内，分析应包括人为因素对轨道交通 RAMS 的潜在影响。

4.4.2.7 尽管通常在生命周期内需要涉及人为因素，但在所考虑的应用中应规定人为因素对 RAMS 的精确影响。

4.4.2.8 在所考虑轨道交通系统环境中，应复核普通因素，包括图 5 所含的内容。轨道交通主管部门在招标时应规定所有不可行因素。每一可行的普通因素应被评审，且详细的影响因素（与应用对应）应系统地导出。人为因素问题（整个 RAMS 管理程序的核心方面）在评审时应该说明。

4.4.2.9 源自具体影响因素的过程应可通过使用轨道交通特定因素（4.4.2.10）和人为因素（4.4.2.11）两个清单或如图 5 所示的替代图得到。

4.4.2.10 具体的轨道交通特定影响因素应包括对下述每一轨道交通特定因素的考虑，但不限于此。应注意下述列项是不详尽的，且应根据应用范围和目的进行调整。

a) 系统运营：
   ——系统应执行的工作和执行该工作的条件；
   ——在运营环境内旅客、货物、人员和系统的共存；
   ——系统生命需求，包括系统生命期望、运行密度和生命周期费用的要求。
b) 环境：
   ——物理环境；
   ——该环境内轨道交通系统集成的高水平；
   ——在轨道交通环境中测试整个系统的有限机会。
c) 应用条件：
   ——既有基本设施与系统对新系统的约束；
   ——在生命周期工作内轨道交通维修服务的需要。
d) 工作条件：
   ——轨道旁的设备工况；
   ——轨道旁的维修条件；
   ——在试运营和运营中已有系统和新型系统的集成。
e) 失效分类：
   ——分布式轨道交通系统内失效的影响。

4.4.2.11 详细的人为影响因素应包括对下述每一人为因素的考虑，但不只限于此。应注意下述列项是不详尽的，且应根据应用范围和目的进行调整。

a) 人机间系统功能的分配。
b) 系统内对人的行为的影响，包括：

——人/系统接口；
——环境，包括物理环境和人类工程学的要求；
——人类的工作方式；
——人的能力；
——人工工作的设计；
——人的互相配合；
——人工反馈流程；
——轨道交通组织机构；
——轨道交通文化；
——专业轨道交通术语；
——新技术引入出现的问题。

c) 源于下述内容的系统要求：
——人的能力；
——人的动机和志向支持；
——减轻人的行为变动的影响；
——运营安全装置；
——人的反应时间与间隔。

d) 源于人类信息处理能力的系统要求，包括：
——人机通信；
——信息传送密度；
——信息传送率；
——信息质量；
——人对异常情形的反作用；
——人员培训；
——支持人的决策形成过程；
——利于人应变的其他因素。

e) 系统中人和系统接口的影响，包括：
——人/系统接口的设计和操作；
——人为错误的影响；
——人类故意违反规则的影响；
——系统中人的干预和参与；
——人的系统监控和取代；
——人对风险的感知；
——在系统关键范围内人所牵连的事务；
——人预测系统问题的能力。

f) 系统设计与开发中的人为因素，包括：
——人的能力；
——设计中人的独立性；
——验证和确认中人所牵连的事务；
——人与自动化工具之间的接口；
——系统失效预防程序。

4.4.2.12 推荐使用图表法(如因果图)表示具体因素的来源。图 6 是一个简单的因果图。

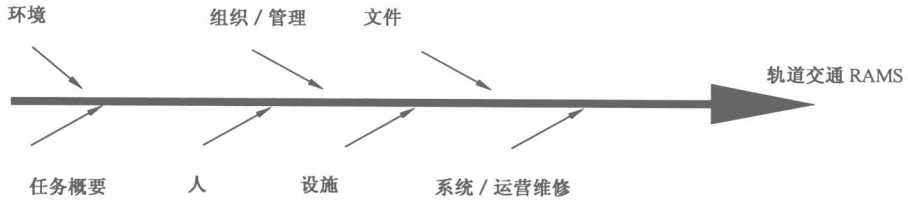


图 6 因果图示例

4.4.3 因素评估

对于所考核轨道交通系统的 RAMS 而言，每一影响因素的潜在影响应在适合于该考核系统的某一级别上进行评估，它包括在生命周期的每一阶段内各个因素影响的评估，且应在适合于考核系统的级别上。评估应该考虑有关影响因素的相互作用。对于人为因素来说，该评估应考虑彼此相关的每个因素的作用。

4.5 实现轨道交通 RAMS 需求的方法

4.5.1 总则

4.5.1.1 实现轨道交通 RAMS 需求的方法关系到整个系统生命内影响 RAMS 因素的控制。在系统的实现和维持中，有效控制要求制定机制和程序来防止误差源引入，这些防御措施需要考虑随机失效和系统失效。

4.5.1.2 用于实现轨道交通 RAMS 需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) 预防：降低损伤发生的概率；

b) 防护：降低损伤后果的严重性。

4.5.1.3 达到轨道交通系统 RAMS 需求的策略（包括预防和/或防护措施的使用）应被证明是正确的。

4.5.2 RAMS 规范

4.5.2.1 RAMS 需求的规范是一复杂的过程。在本标准详述的过程基础上，附录 A 举例提供 RAMS 需求规范的概要。基于本标准的要求，附录 B 提供了概述 RAMS 规划定义的步骤示例。这两个资料性附录仅起指导作用，并以机车车辆为例一起编译。附录 B 中还包含了适当的 RAMS 分析工具一览表。选择一个合适的工具取决于所考核的系统及因素，如其危险程度、新颖性、复杂程度等。

4.5.2.2 表 1 规定了适用于轨道交通 RAM 的失效种类。

表 1 RAM 失效种类

| 失效种类 | 定　　义 |
| --- | --- |
| 重大（停车故障） | 产生导致阻止列车运行、远大于规定时间的晚点、远远超出指定等级费用的失效 |
| 重要（运行故障） | ——系统为获得规定性能应整修的失效；<br>——不导致晚点或不超出重大失效中规定的最小阈值的费用的失效 |
| 次要 | ——不阻止系统获得规定性能的失效；<br>——不符合重大失效和重要失效标准的失效 |

4.5.2.3 附录 C 列出了表征轨道交通系统可靠性、可维修性、可用性、后勤保障和安全要求的适当参数，具体参数取决于所考核系统。所有的 RAMS 参数应通过轨道交通主管部门及其支承工业的协商。参数可以表示为不同量纲时，应提供它们之间的变换因数。

4.6 风险

4.6.1 风险概念

风险概念由以下两个元素组成：

——导致危害的事件或事件组合发生的概率或这些事件发生的频繁程度；

——危害后果。

4.6.2 风险分析

4.6.2.1 在系统生命周期的各个阶段，风险分析应由负责该阶段的主管部门来进行，并应形成文件。该文件至少应包括：

a) 分析方法；

b) 方法的假设、限制和判据；

c) 危害鉴定结果；

d) 风险估计结果和置信度水平；

e) 折衷选择的研究结果；

f) 数据及其来源与置信度水平；

g) 参考文件。

4.6.2.2 表2用定性的术语提供轨道交通系统中危害性事件发生概率或频度的典型分类，并对每类进行描述。这些类别及其数值、采用的数值定标应由轨道交通主管部门规定，与所考核的应用相适应。

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，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 |

4.6.2.3 后果分析应可用于估计可能的影响。表3对所有轨道交通系统描述了典型的危害严酷等级和每个严酷等级危害的后果。所应用的严酷等级数值和每个严酷等级的后果由轨道交通主管部门规定，应与所考核的应用相适应。

表3 危害严酷等级

| 严酷等级 | 对环境或人的影响 | 给运行带来的后果 |
|---|---|---|
| 特大 | 多人死亡，和/或是多方面的严重伤害，和/或对环境的较多损害 | |
| 重大 | 一人死亡，和/或是单个严重伤害，和/或对环境产生明显的损害 | 主系统失效 |
| 次要 | 较小的损伤和/或对环境的明显影响 | 严重的系统损害 |
| 轻微 | 可能存在的较小的伤害 | 较小的系统损害 |

4.6.3 风险评估和验收

4.6.3.1 本条论述了“频度-后果”矩阵的构成，它用于风险分析结果评估、风险分类、风险降低措施或不容许风险的消除和风险验收。

4.6.3.2 风险评估应结合危害性事件的发生频度及其后果的严重性(用于确定危害性事件产生的风险等级)来进行。“频度-后果”矩阵见表4所示。