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

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。

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 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。

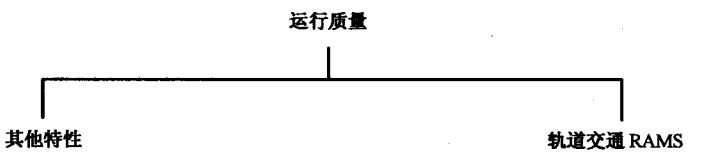


图 1 运行质量和轨道交通 RAMS

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。

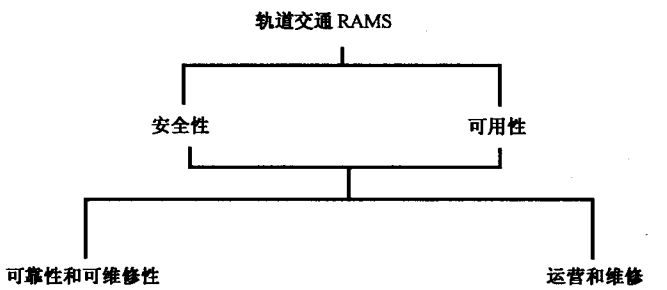


图 2 轨道交通 RAMS 各要素间的相互关系

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。

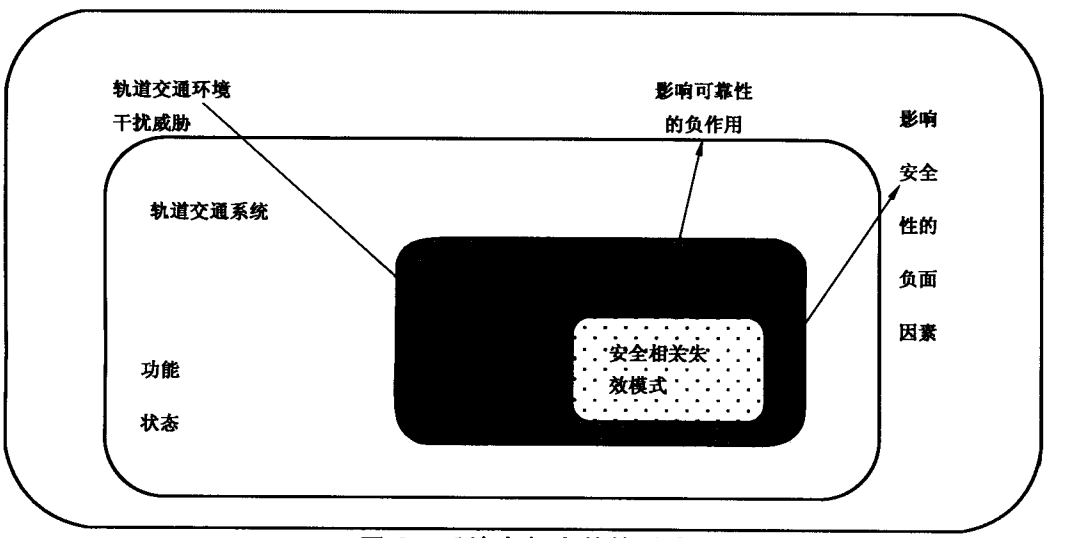


图3 系统内部失效的影响

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。

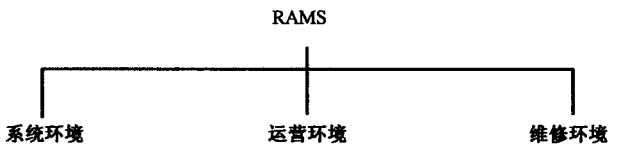


图 4 对 RAMS 的影响

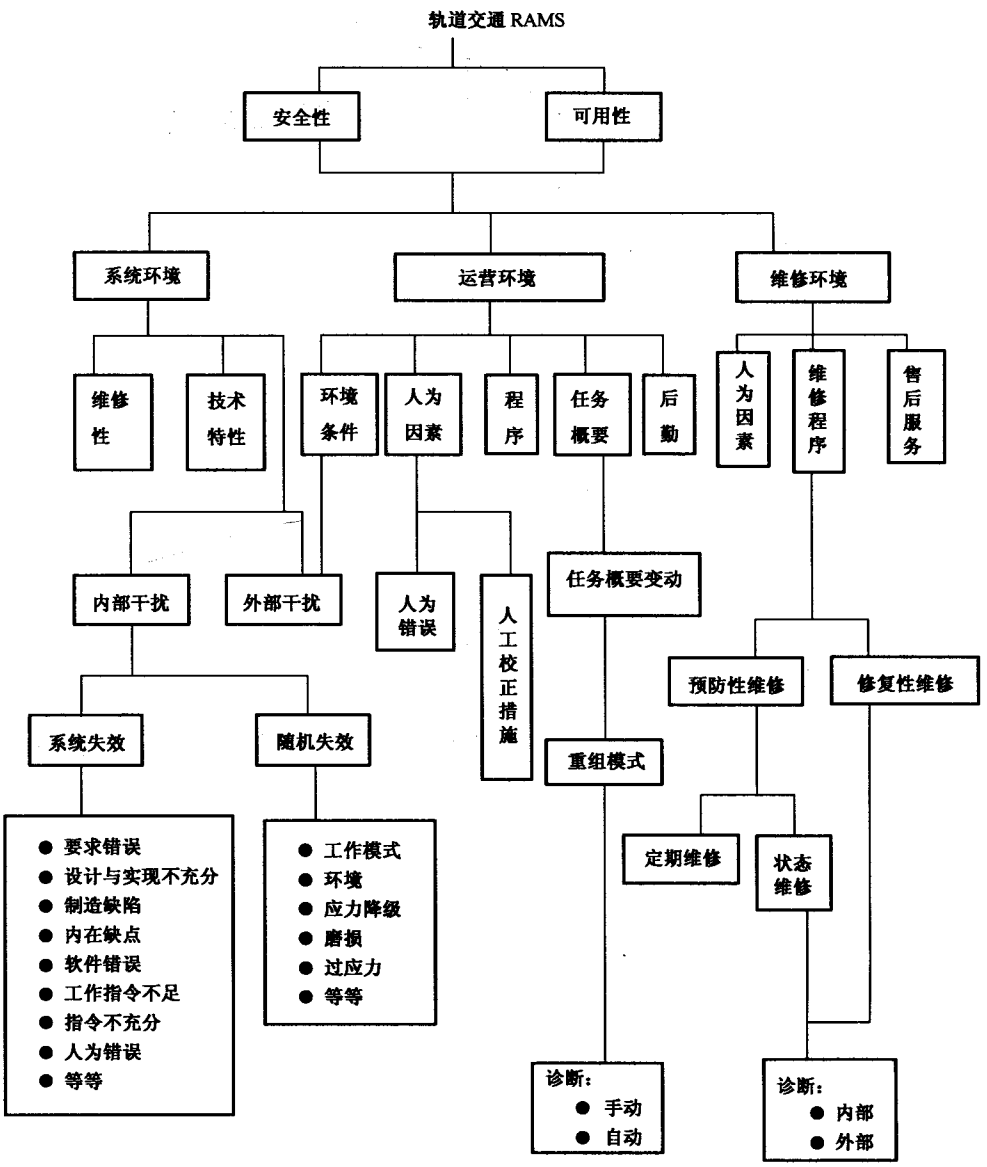


图 5 影响轨道交通 RAMS 的因素

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。

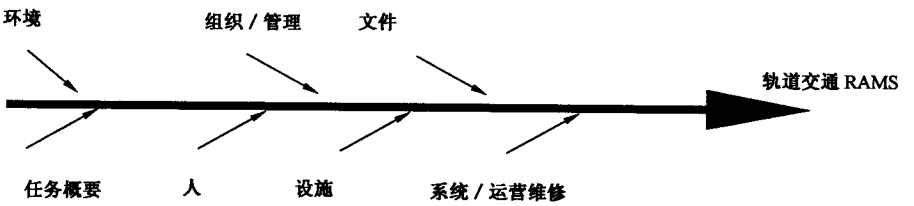


图 6 因果图示例

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； ——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； ——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。

表 4 频度-后果矩阵

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
	危害后果的严酷等级			

4.6.3.3 风险验收应以普遍公认的原理为基础。可以利用的原理有许多，如下面的几个例子(这些原理的更多信息参见附录 D)：

——ALARP(风险降到可行)原理(ALARP 原理在英国使用)。

——GAMAB(综合最优)原理(法国使用)。这个原理的完整表述是：

“所有新型的导向式运输系统应提供一个风险等级，此等级整体上至少与任何等效的现有系统所提供的等级一样好。”

——MEM(最小内源性死亡率)原理(MEM 原理在德国使用)。

表 5 规定了定性的风险等级及应对每一类风险的措施。轨道交通主管部门应负责规定所采用的原理、容许风险等级和可分成不同风险种类的标准。

表 5 定性的风险等级

风险等级	对各风险等级所采取的措施
不容许的	应该消除
不希望的	当风险降低不可行时，应经过轨道交通主管部门或安全规章主管部门同意后方可接受
容许的	经充分控制并经轨道交通主管部门同意后可以接受
可忽略的	有或无轨道交通主管部门同意均可接受

4.6.3.4 表 6 给出了风险评估和用于风险验收的风险降低/控制的例子。

表 6 风险评估和验收的典型例子

危害性事件的发生频度[a]	风险等级			
频繁		不容许的	不容许的	不容许的
经常	容许的		不容许的	不容许的
有时	容许的			不容许的
很少	可忽略的	容许的		
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
	危害后果的严酷等级			

[a] 危害性事件发生频度的定标取决于所考核的应用(4.6.2.2)。

4.7 安全完整性

4.7.1 在应用中已设定了安全等级并估计了必要的风险降低，以风险评审过程的结果为基础，应用中系统及部件的安全完整性要求可以得到。安全完整性可以认为是定量元素（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。为了达到安全性目标等级，降低风险的外部设施和系统降低风险设施应和系统要求的必要风险降低相匹配。

4.7.2 系统功能的安全完整性的置信度可以通过有效地组合特定的系统结构、方法、工具和技术来得到。安全完整性与获取要求的安全功能的失效概率相互关联。功能的安全完整性要求越高，则实现所需的费用越昂贵。对轨道交通系统本标准没有规定安全完整性和失效概率之间的相互关系，但应注意在 GB/T 20438 中规定了它们的一般关系，轨道应用中这个关系的定义是轨道交通主管部门的职责。虽然本标准规定的管理程序是通用的，并可适用于任何相互关系，但是，仍须经轨道交通主管部门同意。

4.7.3 系统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 规定了开发软件系统的方法、工具与技术，EN 50129 规定了轨道交通电子信号系统验收和批准的程序。

4.7.4 安全完整性基本上是为了安全功能规定的。安全功能应分配给安全系统和/或降低风险的外部设施。通过分配程序的反复进行，使整个系统的设计与费用最优化。

4.7.5 当安全计划与 RAM 规划有效实施后，它能给出最终系统获得符合 RAMS 需求的置信度。

4.7.6 应注意与产品安全完整性相关的以下几点：

a) 系统的安全性能和相应的安全完整性受系统使用环境的影响。

b) 当用与指定安全完整性相应的方法、工具和技术开发产品时，可声明该产品是安全完整性等级为“X”的产品。此声明表明产品在规定环境条件下、在某个完整性级别上具有指定的功能。

c) 图 7 表示商业“现货供应”产品在不同的应用中用途可以不同。例如产品 A 在系统 1 和系统 2 中实现不同的功能。因此，产品必需的安全完整性随应用的不同而改变。所以，为确保与系统的整体要求相一致，在一个系统中使用产品之前，应估计对产品的规定环境及功能的限制和约束。

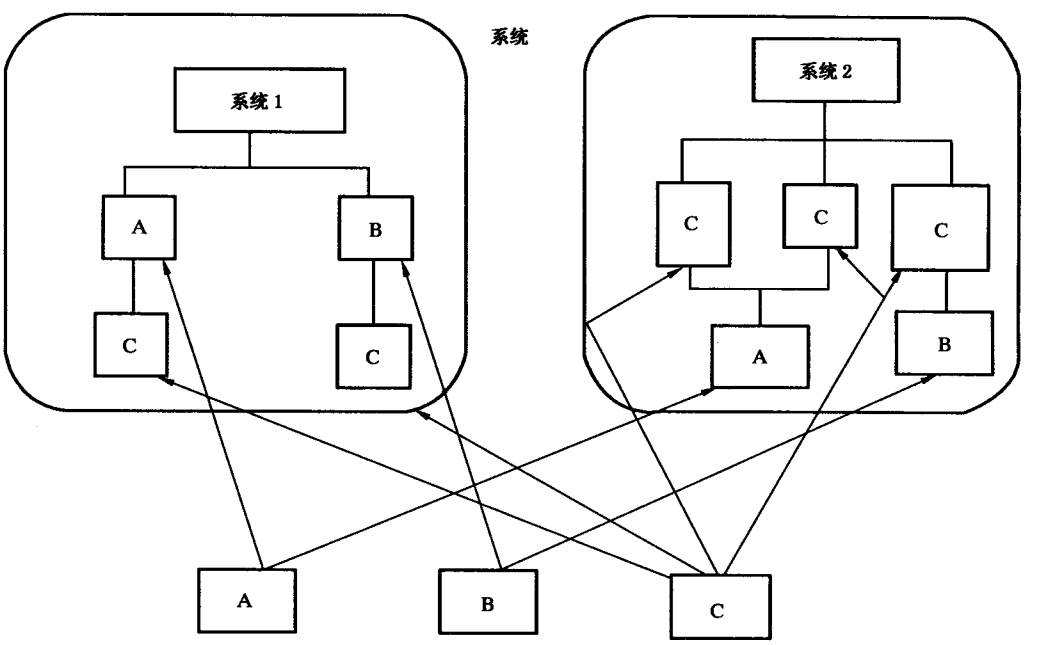


图 7 安全系统中被鉴定的产品

4.7.7 应用SIL概念之前，应该考虑以下要求：

a) 应由安全专家来确定所用的SIL是否适当，推荐使用不超过4个等级。

b) 一个“要素”应只分配一个SIL，“要素”指能实现一个或多个简单功能且可被一个实现相同功能的设备代替的独立设备。通常这个“要素”是最底层的设备，在第一级修复性维修工作中可以替换。

c) 对于所考核的系统，产品所在的环境是极其重要的，在与产品的安全要求比较时，应审查现货供应产品的已鉴定的SIL及鉴定方法是否满足全部条件。

d) 一个SIL只说明产品安全性置信度的一个期望等级。如本标准4.3所述，安全性要求和可用性要求在轨道运输范围内是相互关联的。SIL并没有考虑到系统的所有方面，因此只考虑SIL是不够的(如：降级运行模式和处于备用状态有不同的安全要求等等)。

4.8 故障安全概念

4.8.1 本标准采用广义的风险管理方法以获得安全性。此方法和故障安全概念一致，并经过轨道交通工程师的充分验证。

4.8.2 轨道交通使用初期，所使用的是故障安全的固有概念，它依赖于一系列的假设，以使用具有已充分证明的失效模式及其失效时安全状态的器件为基础。所有的器件均经过确定，以使这样构建的系统只有无失效时存在的容许状态。

4.8.3 通常，该概念的有效性以经验为基础，但用于商用微机的大型复杂系统的使用与开发时有局限性。使用这些部件时，考虑到失效组合数值的指数增长，通常意味着确定性的方法是不可行的。在这样复杂的系统中，可以有效地使用概率法。

4.8.4 此故障安全方法对系统部件是有效的，本标准中也不排除类似的其他确定性的方法。不管采用何种方法，都应与指定的系统RAMS要求相一致。

5 轨道交通RAMS管理

5.1 总则

5.1.1 本章规定了一个管理流程，它以系统生命周期为基础，能控制轨道交通中规定的RAMS因素。该流程包括：

——定义RAMS需求；

——评估与控制RAMS的影响；

——计划与实施RAMS工作；

——实现与RAMS需求一致性；

——监控生命周期内一直进行的一致性。

5.1.2 虽然轨道交通RAMS是本标准的核心内容，但只是整个轨道交通系统诸多方面中之一。本章规定了RAMS管理用系统化的流程，此流程是说明整个轨道交通系统的综合管理方法的一个组成部分。

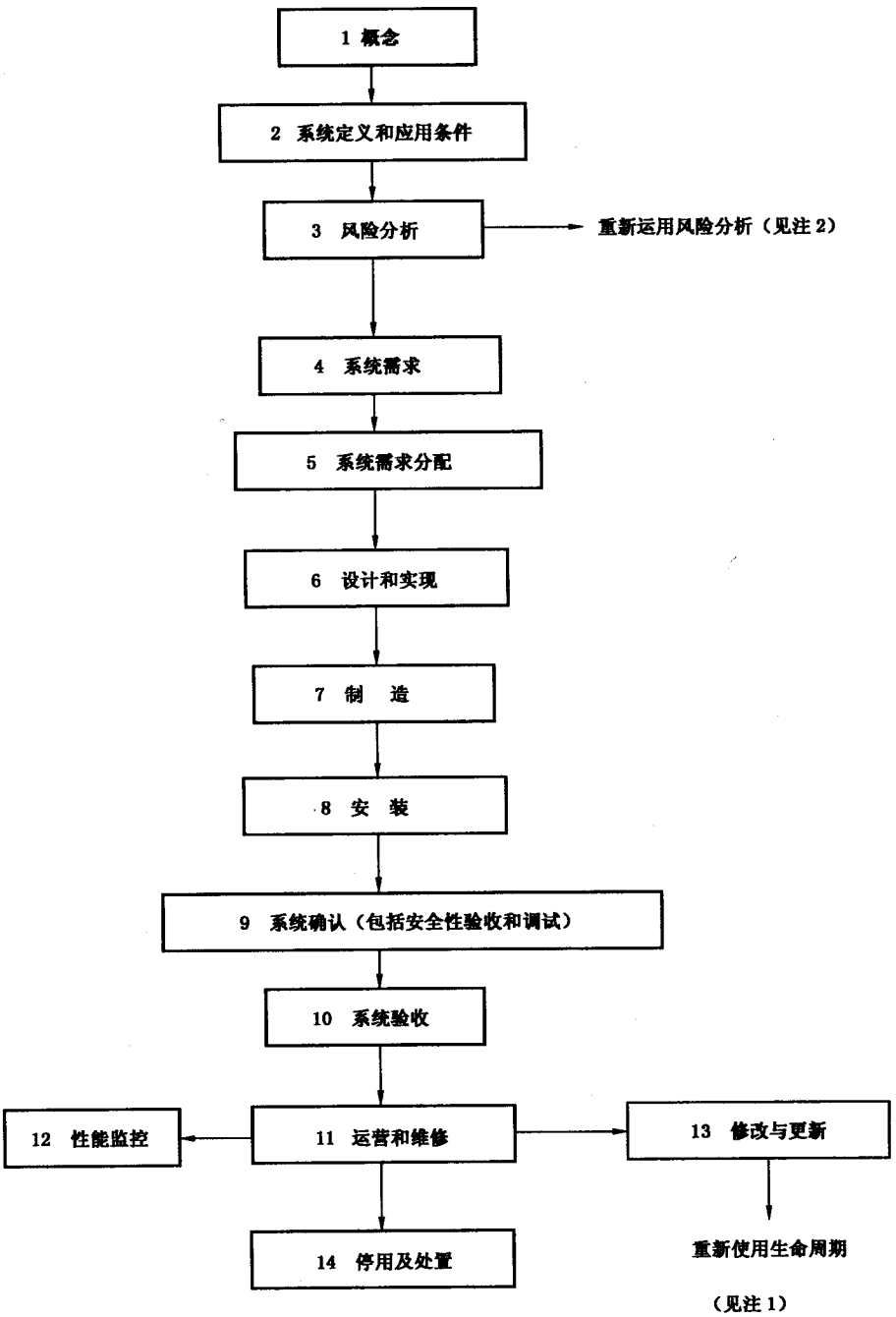
5.1.3 对于任何轨道交通主管部门，其轨道交通系统的容许安全风险取决于国家安全规章、主管部门或轨道交通主管部门自身(经安全规章主管部门同意)制定的安全标准。轨道交通主管部门的主要职责是评估风险、控制风险并使风险降至最小。有些情况下，制订法规需要提供正式的论证系统安全充分性的证据。

5.2 系统生命周期

5.2.1 系统生命周期是一个阶段序列(每一阶段均包含有工作)，包含从初始概念阶段到停用及处置阶段的整个生命周期。生命周期提供一个规划、管理、控制和监控系统所有方面(包括RAMS)的结构，且

在系统各阶段中不断完善，以便在协商的时间阶段内交付适当价格且正确的产品。生命周期概念是成功实施本标准的基础。

5.2.2 轨道交通范围内相应的系统生命周期见图 8。对于生命周期每个阶段的主要工作在图 9 中概述。此图表示作为一般工程工作组成的 RAMS 工作。这些一般工作不在本标准范围之内，却代表普通工业的实践。每个阶段中有助于一般工程工作的 RAMS 工作和 RAMS 工作的需求将在本标准随后的章节中详细说明。



注 1：修改进入生命周期的阶段取决于待修改的系统和所考虑的特定修改。

注 2：在生命周期的几个阶段中可能要重复进行风险分析[见 6.3.1 的 d)]。

图 8 系统生命周期

生命周期阶段	本阶段的一般工作	本阶段的 RAM 工作	本阶段的安全性工作
1. 概念	确定轨道交通项目的用途和范围 定义轨道交通项目概念 进行财务分析和可行性研究 设立管理机构	回顾先前达到的 RAM 业绩 考虑项目的 RAM 蕴涵	回顾先前达到的安全业绩 考虑项目的安全蕴涵 回顾安全规章和安全目标
2. 系统定义和应用条件	确定系统任务概要 拟定系统描述 确定运营和维修策略 确定运营环境 确定维修环境 验证现有基础设施约束的影响	评价 RAM 过去的经验数据 进行初步 RAM 分析 制定 RAM 方针 确定长期运营和维修环境 确定现有基础设施约束对 RAM 的影响	评价安全性过去的经验数据 进行初步危害分析 建立(整个的)安全计划 定义风险容许准则 确定现有基础设施约束对安全性的影响
3. 风险分析(见注 6)	开展项目相关的风险分析		完成系统危害性和安全性风险分析 建立危害记录 完成风险评估
4. 系统需求	开展需求分析 指定系统(所有的要求) 指定环境 定义系统论证和验收准则(所有的要求) 建立确认计划 确定管理、质量和组织需求 实施变更控制程序	规定(全面的)系统 RAM 要求 规定(全面的)RAM 验收准则 规定系统功能结构 建立 RAM 规划 建立 RAM 管理	指定系统(全面的)安全要求 定义安全(全面的)验收准则 定义安全相关的功能要求 建立安全管理
5. 系统需求分配	系统需求分配 ——明确子系统和部件要求 ——规定子系统和部件验收准则	系统 RAM 要求分配 ——指定子系统和部件 RAM 要求 ——规定子系统或部件 RAM 验收准则	系统安全目标和要求的分配 ——指定子系统或部件安全要求 ——规定子系统和部件安全验收准则 修改系统安全计划
6. 设计和实现	计划编制 设计和开发 设计分析和测试 设计验证 实施和确认 进行后勤保障资源设计	通过复核、分析、测试和数据评估来实施 RAM 规划,包括: ——可靠性和可用性 ——维修和可维修性 ——最佳维修策略 ——后勤保障 开展程序控制,包括: ——RAM 规划管理 ——分包商和供应商的控制	通过复核、分析、测试和数据评估来实施安全计划,涉及: ——危害记录 ——危害分析和风险评估 论证安全相关的设计决策 开展计划控制,包括: ——安全管理 ——分包商和供应商的控制 准备一般安全论据 准备(如合适)一般应用安全论据

图 9　项目各阶段的相关工作

生命周期阶段	本阶段的一般工作	本阶段的 RAM 工作	本阶段的安全性工作
7. 制造	编制生产计划 制造 零部件的制造和测试 准备文件 建立培训方案	完成环境应力筛选 进行 RAM 改进测试 着手运行失效报告分析和纠正措施系统(FRACAS)	通过复核、分析、测试和数据评审来实施安全计划 使用危害记录
8. 安装	组装系统 安装系统	开始维修人员培训 建立备件和工具供应方案	确定安装程序 实施安装程序
9. 系统确认(包括安全验收和调试)	调试 进行运营前的试运行 进行培训	完成 RAM 论证	建立调试程序 实施调试程序 准备应用特定的安全论据
10. 系统验收	以验收准则为基础实施验收程序 汇集验收证据 投入运行 继续试运行工作(如果适合)	评估 RAM 论证	评估应用特定的安全论据
11. 运营和维修	长期系统运营 进行计划内维修 执行计划内培训方案	备件和工具的计划内采购 进行计划内以可靠性为中心的维修后勤保障	进行计划内以安全为中心的维修 进行计划内的安全性能监控和危害记录维护
12. 性能监控	收集运营性能统计 获取、分析和评审数据	收集、分析、评估和使用性能及 RAM 统计	收集、分析、评估和使用性能及安全统计
13. 修改与更新	实施修改请求程序 实施修改与更新程序	考虑修改与更新 RAM 蕴涵	考虑修改与更新安全蕴涵
14. 停用及处置	停用和报废处置计划编制 执行停用 进行处置	无 RAM 工作	建立安全计划 进行危害分析和风险评估 实施安全计划

注 1：变更控制或结构管理活动适用于项目的所有阶段。

注 2：验证和确认活动可适用于大部分的生命周期阶段，见正文。

注 3：就 RAM 而言，“RAM 规划”是通用术语，并被本标准所采用。就安全性而言，“安全计划”是通用术语，并被本标准所采用。

注 4：注意本标准的范围只限于 RAMS，并不针对于系统的所有保证活动。但是，根据 RAMS 观点，应确保 RAMS 阶段和项目有关阶段同步，而且就通过一个阶段到另一个阶段的条件达成一致。

注 5：在第 9 阶段和第 10 阶段内的工作可以综合到一起，取决于所考核的应用。

注 6：在几个阶段中风险分析应重复使用[见 4.6.2 和 6.3.1 的 d)]。

图 9（续）

5.2.3 本标准承认系统 RAMS 性能和系统开发费用及所有权费用(即生命周期费用)之间的平衡。本标准要求考虑生命周期费用和系统 RAMS 的各个方面，但不在费用的基础之上来规定解决 RAMS 问题的方法，因为这是轨道交通主管部门的责任。

5.2.4 对每个生命周期阶段而言，第 6 章及其条款用一致的格式规定了整个项目范围内 RAMS 工作

的目标、要求、输入和可交付性。

5.2.5 此流程通过提供生命周期各个阶段内的综合工作序列来支持供货合同。在综合管理流程内，这是形成单个 RAMS 工作或工作组合的合同基础。进行这些工作的职责取决于所考核的系统和可行的合同条件。确定这些职责的一些一般导则见附录 E。

5.2.6 本标准按顺序表示了系统生命周期。这种表示法指出了单个的阶段及每个阶段之间的联系。其他的生命周期表示法(包括"V"模型在内)广泛应用于工业上。

5.2.7 本标准生命周期的"V"表示法见图 10。下行分支(左边的分支)一般称为设计与开发，这是一个精进过程，以系统的部件制造作为该分支的结束。上行分支(右边的分支)包括装配、安装、验收和整个系统的运营。

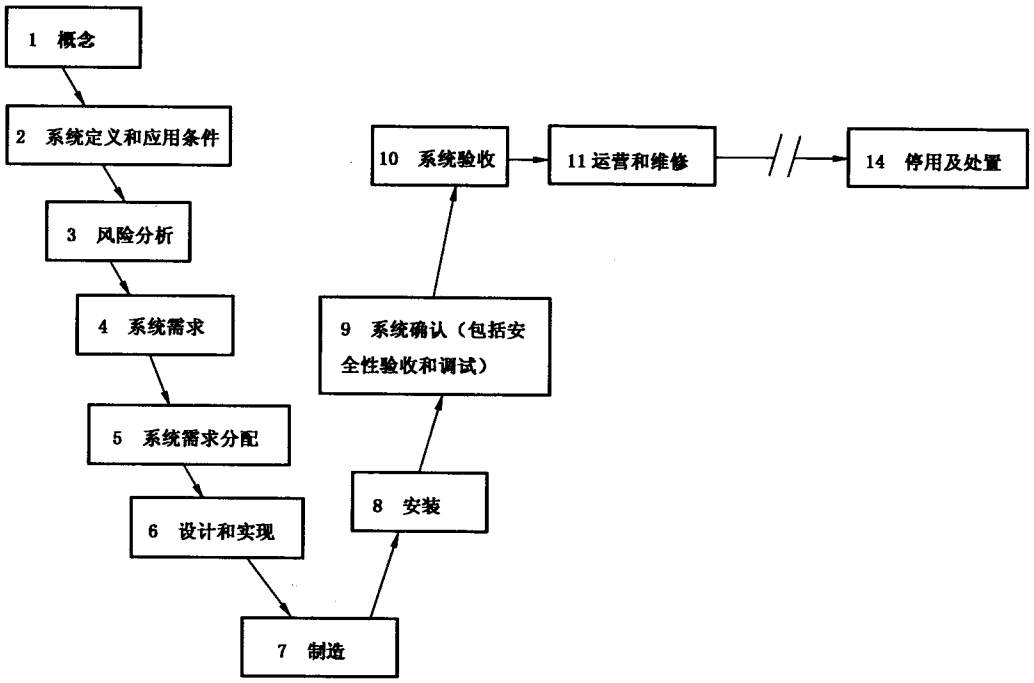


图 10 "V"表示法

5.2.8 由于实际开发的产品最终应按有关要求进行检查，"V"表示法假定验收活动与设计开发活动有固有联系，因此在系统各个阶段内，验收的确认活动以系统规范为基础，且应在较早的阶段中规划，即在相应的生命周期的设计开发阶段开始。这个联系见图 11。

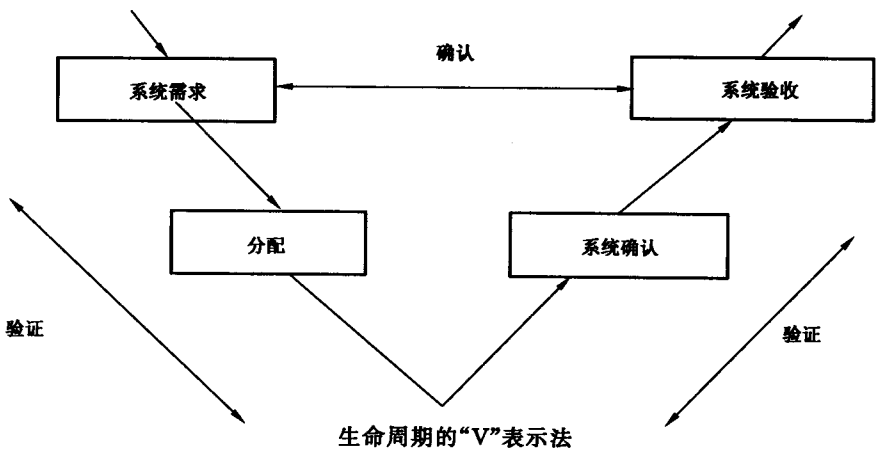
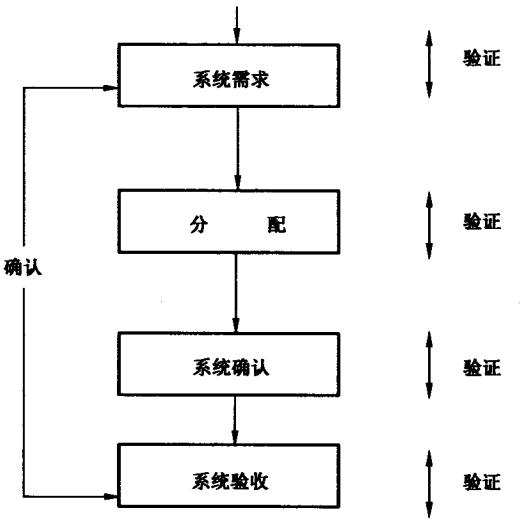


图 11 验证和确认



生命周期顺序表示法

注：5.2.9 提供关于验证和确认的附加信息。如图所示，确认包括系统验收框，因为某些确认工作包括在该阶段内（又见 6.9.1 和 6.10.1）。

图 11（续）

5.2.9　在生命周期内展示验证与确认工作时该表示法是有效的。验证的目的是为了证明在指定的输入下，每个阶段的交付性在所有方面满足本阶段的要求。确认的目的是为了证明所考核的系统在其开发的各阶段中及安装后满足该阶段各个方面的要求。

5.2.10　本标准中，生命周期的每个阶段都包括了验证工作。虽然本标准在 RAMS 章节涉及到系统保证，但是验证和确认（V&V）工作与全面的系统保证说明是一个整体。因此，RAMS V&V 有助于全面的系统保证 V&V。

5.3　本标准的应用

5.3.1　本条根据轨道交通系统的规模、复杂性和费用给出了要求以便灵活且有效应用本标准。

5.3.2　本标准规定的要求是通用的且可应用于轨道交通系统的所有类型。对所考核系统，轨道交通主管部门应规定本标准要求的应用。评估应以对特定系统要求的可行性为基础，在评估第 9 阶段（系统确认）和第 10 阶段（系统验收）内的工作序列时要特别注意。

5.3.3　在系统更新的情况下，既有系统和更新的系统混合运营或同时运营，常常会有“混合阶段”。在这种情况下，安全性研究应明确陈述既有系统与更新系统间可能的相互影响。

5.3.4　本标准的应用应适合于所考核系统的特定的要求。对所考核系统本标准应用的评估应包括：

a）　为实现所考核系统规定需要的生命周期阶段，为这些生命周期阶段提供正当的理由，论证在这些生命周期阶段所从事的工作是否与本标准要求的原理相一致。

b）　用图 9 和第 6 章相关阶段的相应信息为清单，规定所需的生命周期各阶段的强制性活动及要求，包括：

——与所考核系统相关的各个要求的范围；

——每个要求所需要的方法、工具和技术及其应用范围与深度；

——对于每个要求所需要的验证与确认活动及其应用范围；

——所有的支持文件。

c）　证明偏离本标准的要求与活动是正当的。

d）　证明所考核的应用选择的工作是充分的。

5.3.5 在本标准的所有应用中，下述要求是强制的：

a) 对所考核系统，在生命周期每个阶段所执行的全部 RAMS 工作的职责，包括关联工作之间的接口，应被规定并经过协商同意。

b) 所有对 RAMS 管理负责任的人员应有能力履行这些职责。

c) 在可信性系统的实现过程中 RAM 规划和安全计划的建立与实施是基本组成部分。虽然这些规划文件的内容是针对所考核系统的，对这些工作的约束可以不同，但很多 RAMS 工作将要求类似的分析工作。对以 RAM 为中心的工作来说，主要考虑的是费用，而在以安全性为中心的工作中，主要是防止意外的及相关联的事故发生。根据轨道交通主管部门的要求，与 RAMS 有关的经济结果可以不同，在这一意义上 RAMS 的要求可能有冲突。由于 RAMS 工作之间的分析活动的深度可以变化，对确定和管理 RAMS 冲突的认可及所有 RAMS 分析的详细资料应包括在 RAMS 的规划文件内。

d) 在企业活动过程中本标准的要求应被实现，它由符合 GB/T 19001—2000 要求、适用于所考核系统的质量管理体系(QMS)支持。

e) 应该建立和实施一个适当并有效的配置管理系统，它针对所有生命周期阶段的 RAMS 工作。配置管理的范围取决于所考核的系统，但通常应包括全部系统文件和所有其他系统的可交付性。

5.3.6 在系统生命周期规定的管理流程基础上，通过把每一个损伤的影响降到最小和控制第 4 章中讨论的因素，本标准的第 6 章详细讲述了保证达到 RAMS 要求的方法。设计可靠的系统所适用的方法、工具和技术在其他标准中列出(参见附录 B)。值得注意的是方法、工具、技术的选择及其应用的深度和范围以及文档的范围和深度应与所考核的系统需求相匹配。对于所考核系统，这些内容应通过轨道交通主管部门与供货商协商同意。这些与支持 RAMS 工程和管理的不同方面的方法总揽见图 12。

5.3.7 为了提供一个评审过程，本标准写出了一个详细的要求。对于所考核的系统，轨道交通主管部门及其支承工业应该同意和实施评审计划审查本标准要求的应用与系统相适应。

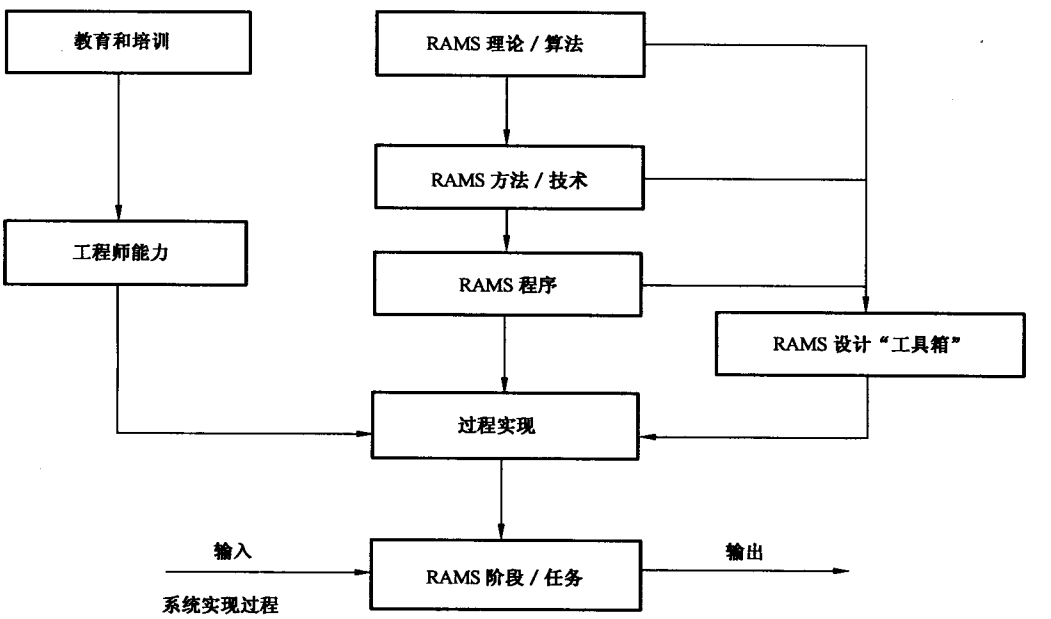


图 12 在系统实现过程中实施的 RAMS 设计和管理

6 RAMS 生命周期

本章详细说明了在生命周期的每个阶段内的目标、要求、交付性、所从事的验证和确认工作。这些

要求的应用和范围应通过评估并调整到满足所考核系统的特殊要求。关于该主题的更多信息见5.3。

6.1 第1阶段:概念

6.1.1 目标

本阶段的目标是理解系统达到某个层次,以使后续的RAMS生命周期工作能满意完成。

6.1.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据,如对项目的范围和目标说明。

6.1.3 要求

6.1.3.1 本阶段的第1个要求是获得对RAMS性能的来龙去脉的理解:

a) 系统的范围、背景和目标;

b) 系统环境包括:

——自然问题;

——潜在的系统接口问题;

——社会问题;

——政治问题;

——立法问题;

——经济问题;

c) 系统通用的RAMS蕴涵。

6.1.3.2 本阶段的第2个要求应是回顾:

a) 系统财务分析的RAMS蕴涵;

b) 系统可行性研究的RAMS蕴涵。

6.1.3.3 本阶段的第3个要求是确定影响系统RAMS性能的危害源,包括:

——与其他系统的相互作用;

——与人的相互作用。

6.1.3.4 本阶段的第4个要求包括获取以下信息:

a) 类似和/或相关系统中先前的RAMS要求和过去的RAMS性能;

b) 已确定的RAMS性能危害源;

c) 当前的轨道交通主管部门安全规章与目标;

d) 安全立法。

6.1.3.5 本阶段的第5个要求是为后续的系统生命周期RAMS工作规定管理要求的范围。

6.1.4 可交付性

6.1.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.1.4.2 可交付性应包括在生命周期第2、3和4阶段能充分实现RAMS要求的管理结构。

6.1.4.3 本阶段的可交付性是后续生命周期阶段的关键输入。

6.1.5 验证

本阶段应进行如下验证工作:

a) 评估本阶段内作为RAMS工作输入的信息、(合适时)数据与其他统计数据的充分性;

b) 评估第1个要求规定的系统环境的充分性;

c) 评估第3个要求列出的危害源的完整性;

d) 评估本阶段内使用的方法、工具和技术的适宜性;

e) 评估本阶段内从事工作的全体人员的能力。

6.2 第2阶段:系统定义和应用条件

6.2.1 目标

本阶段的目标是:

a) 规定系统任务概要；
b) 规定系统范围；
c) 确定影响系统特性的应用条件；
d) 规定系统危害分析的范围；
e) 确定系统 RAMS 方针；
f) 建立系统的安全计划。

只要它们影响潜在的系统 RAMS 性能，都要作出规定。

6.2.2 **输入**

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，包括在第 1 阶段的可交付性。

6.2.3 **要求**

6.2.3.1 本阶段的第 1 个要求是规定：

a) 系统任务概要：
——性能要求；
——RAMS 目标；
——长期运营策略和环境；
——长期维修策略和环境；
——系统生命考虑，包括生命周期费用问题；
——后勤考虑；
b) 系统范围，包括：
——与自然环境的接口；
——与其他技术系统的接口；
——与人的接口；
——与其他轨道交通主管部门的接口；
c) 影响系统的应用条件范围，包括：
——现有基础设施的约束；
——系统运营环境；
——系统维修环境；
——后勤保障因素；
——类似系统以往经验数据的复核；
d) 系统危害分析的范围，包括确定如下内容：
——受控过程中固有的危害；
——环境的危害；
——安全防护的危害；
——外部事件的影响；
——待分析系统的范围；
——现有基础设施约束对 RAMS 的影响。

6.2.3.2 本阶段的第 2 个要求是完成：

a) 支持目标的初步 RAM 分析；
b) 对下述内容的初步危害鉴定：
——确定与已识别的危害相关的子系统；
——确定待考核的初始事件的事故类型，包括部件失效、流程错误、人为误差和相关的失效机制；

——规定最初的风险容许准则。

6.2.3.3 本阶段的第3个要求是为系统建立通用RAMS方针，包括为解决可用性和安全性间冲突的轨道交通主管部门的方针与安全概念的要求。

6.2.3.4 本阶段的第4个要求为系统建立安全计划。对于所考核系统，安全计划应通过轨道交通主管部门及其支承工业同意，且应在系统的生命周期内实施、复核和维护，它包括：

a) 达到安全性的方针和策略；

b) 计划的范围；

c) 系统描述；

d) 生命周期内从事工作的团体之间的关系、责任、能力及所担任的角色的详细说明；

e) 系统生命周期与生命周期所从事的安全工作及其依赖性的描述；

f) 生命周期内使用的安全分析、设计和评估过程，包括以下的过程：

——在工作中保证人员相应的独立程度，确保和系统风险相匹配；

——危害确定和分析；

——风险评估和正在进行的风险管理；

——风险容许准则；

——安全要求充分性的确定与复核；

——系统设计；

——验证和确认；

——为获得系统要求与实现一致性进行的安全性评估；

——为获得管理程序与安全计划一致性进行的安全性审查；

——为获得子系统和系统安全分析一致性的安全性评估；

g) 生命周期中安全相关的可交付性的详细说明，包括：

——文件；

——硬件；

——软件；

h) 编写系统安全论据的过程；

i) 系统安全性批准过程；

j) 修改系统安全性的批准过程；

k) 分析运营与维修性能的流程以保证实现的安全与要求相符；

l) 安全相关文件维护的流程，包括危害记录；

m) 与其他相关规划和计划的接口；

n) 计划中的约束与假设；

o) 分包商的管理安排；

p) 贯穿生命周期且适合于所考核系统的与安全相关的周期性安全评审、安全性评估及安全性复核的要求，包括任何人员独立性的要求。

6.2.4 可交付性

6.2.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.2.4.2 可交付性应包括系统RAMS方针。

6.2.4.3 可交付性应包括安全计划。

6.2.4.4 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.2.5 验证

6.2.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据及其他统计数据的充分性；

b) 在第1阶段可交付性的基础上，应验证第2阶段的可交付性的各个方面，特别是评审RAMS方针与在第1阶段中规定的系统要求相一致；

c) 应对RAM分析的完整性和危害确定过程进行评估；

d) 安全计划充分性的评审，包括核查安全计划内所有数据源的充分性；

e) 评估本阶段内使用的方法、工具和技术的适宜性；

f) 评估本阶段内从事工作的全体人员的能力。

6.2.5.2 任何一个错误或不足都需要重复先前一个或多个生命周期阶段中的部分或全部工作。

6.3 第3阶段：风险分析

注：风险分析在生命周期的几个阶段需要重复[见6.3.1的d)]。

6.3.1 目标

本阶段的目标是：

a) 确定与系统有关的危害；

b) 确定导致危害的事件；

c) 确定与危害有关的风险；

d) 建立用于计划内风险管理的流程。

6.3.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第2阶段的可交付性。

6.3.3 要求

6.3.3.1 本阶段的第1个要求是：

a) 在系统应用环境中，系统地确定并区分所有有理由预见的系统危害的优先次序，包括由以下条件所产生的危害：

——系统正常运营；

——系统故障环境；

——系统紧急运营；

——系统误用；

——系统接口；

——系统功能；

——系统操作、维修和支持问题；

——系统处置所需要考虑的事项；

——人为因素；

——职业健康问题；

——机械环境；

——电气环境；

——包括雪、洪水、风暴、雨及滑坡等现象在内的自然环境。

b) 确定导致危害的事件的顺序。

c) 估计每个危害发生的频度(见表2)。

d) 估计每个危害后果可能的严酷性。

e) 估计每个危害产生的系统风险。

6.3.3.2 考虑了可用性与系统生命周期费用要求的冲突后，本阶段的第2个要求是确定与每个已识别危害有关的风险的可接受性，并对其进行分类。

6.3.3.3 本阶段的第3个要求是建立一个危害记录作为管理风险的基础。在生命周期中，只要已识别的危害发生改变或确定有新的危害，危害记录就应更新。危害记录包括下述详细情况：

a) 危害记录的目的和用途；
b) 每个危害性的事件和引起危害的部件；
c) 每个与危害有关的事件序列的可能结果及频度；
d) 每个危害的风险；
e) 应用中风险容许准则；
f) 降低风险至容许等级或消除每个危害事件的风险的方法；
g) 检查风险可接受性的流程；
h) 核查降低风险方法有效性的流程；
i) 日常的风险和事故汇报的流程；
j) 危害记录管理流程；
k) 已实施分析的极限；
l) 分析中所做的任何假设；
m) 分析所用数据的置信度限值；
n) 使用的方法、工具和技术；
o) 过程中有关的人员及其能力。

6.3.4 可交付性

6.3.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.3.4.2 风险分析的结果应记录在危害记录中。

6.3.4.3 本阶段的可交付性构成后续生命周期阶段的关键输入。

6.3.5 验证

6.3.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他统计数据的充分性；
b) 第3阶段的可交付性应比照第2阶段的可交付性进行检查；
c) 评审风险评估的完整性；
d) 评估风险可接受的类别；
e) 评审所考核系统危害记录流程的适宜性；
f) 评估本阶段内使用的方法、工具和技术的适宜性；
g) 评估本阶段内从事工作的全体人员的能力。

6.3.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段中的部分或全部工作。

6.4 第4阶段：系统需求

6.4.1 目标

本阶段的目标是：

a) 规定系统全面的RAMS要求；
b) 对系统RAMS，规定全面的论证与验收准则；
c) 为控制后续生命周期阶段的RAM工作建立RAM规划。

6.4.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第2、3阶段的可交付性。

6.4.3 要求

6.4.3.1 本阶段的第1个要求是规定整个系统的所有RAMS要求(参见6.2.3.1)。所考核系统的RAMS要求应包括：

——系统定义和界限；
——任务概要；

——功能要求和所支持的性能要求，对于每个安全功能，包括安全功能要求和安全完整性要求；
——后勤保障要求；
——接口关系；
——应用环境；
——已识别危害的容许风险等级；
——为达到要求所必需的外部测量；
——系统支持要求；
——分析限值的详细说明；
——所作假设的详细情况。

6.4.3.2 本阶段的第2个要求是规定与系统RAMS相一致的所有要求(参见6.2.3.3)，包括：
——所有RAMS要求的验收准则；
——系统RAMS确认计划推进的所有RAMS要求的论证和验收流程，包括：
- 系统描述；
- 系统采用的RAMS确认原理；
- 为进行确认所作的RAMS试验和分析，包括需要的环境、工具、设施等细节；
- 包括个人独立性要求在内的确认管理结构；
- 确认规划(顺序和进度表)的详细情况；
- 处理不一致性的程序。

6.4.3.3 本阶段的第3个要求是为余下的生命周期工作建立详细的RAM规划(参见6.2.3.3)。对于所考核系统，RAM规划应包括判定能最有效地达到RAM要求的工作。所考核系统的RAM规划应经过轨道交通主管部门及其支承工业的同意，并在整个系统生命周期内进行实施。RAM规划中，应考虑以下工作：

a) 管理，包括下列详细情况：
——获得RAM要求的方针和策略；
——规划范围；
——系统描述；
——系统生命周期、RAM工作和生命周期内采取的流程，特别是保证最有益于系统设计的RAM工作的顺序；
——生命周期内执行工作的组织的角色、责任、能力和关系；
——从生命周期的第7阶段，系统采用了失效报告分析和纠正措施系统(FRACAS)(适当时，由轨道交通主管部门及其支承工业同意)，记录包括如下内容：
- 系统的技术数据；
- 维修理由；
- 维修类别；
- 维修工时与用去的时间；
- 维修不可用时间；
- 人员的数量和其技能水平；
- 使用的备品；
- 消耗品的费用；
- 汇报和纠正措施；

——为保证单个RAM要素间的协调所作的安排；
——本生命周期内所有与RAM相关的可交付性的详细资料；
——RAM验收工作的详细资料；

——与其他相关规划和计划的接口；
——RAM 规划作出的约束和假设；
——分包商管理方案。

b) 可靠性包括：
——可靠性分析和预计包括：
- 功能分析和系统失效定义；
- 下行分析法，如故障树分析和方框图分析；
- 上行分析法，如失效模式影响分析(FMEA)；
- 共因失效或多路失效分析；
- 敏感度分析和折衷研究；
- 可靠性分配；
- 人机接口分析；
- 应力分析；
- “最坏情况”预计和容差分析；

——可靠性规划包括：
- 可靠性设计复核方案；
- 部件可靠性保证方案；
- 软件质量/可靠性保证方案；

——可靠性测试包括：
- 基于失效产生的可靠性增长测试；
- 基于预期失效模式的可靠性论证测试；
- 环境应力筛选；
- 部件的寿命测试；
- 早期运营期间的系统寿命测试；
- 可靠性数据获取和评估；
- 可靠性改进的数据分析。

c) 可维修性包括：
——可维修性分析和预计包括：
- 可维修性分析与验证；
- 维修工作分析；
- 易维修性研究和测试；
- 人为因素可维修性考虑；

——可维修性计划包括：
- 可维修性设计方案复核；
- 建立维修策略；
- 以可靠性为中心的维修选项的核查；
- 软件维修方案；

——后勤保障评估包括：
- 维修要求定义；
- 备件策略与支持资源的定义；
- 维修人员及设备；
- 人员安全预防措施；
- 系统支持要求；

- 培训方案要求；
- 系统运输、包装、搬运和贮存条件；

——可维修性数据获取和评估；

——可维修性改进的数据分析。

d) 可用性包括：

——可用性分析；

——敏感度分析和折衷研究；

——早期运营期间的可用性论证；

——可用性数据获取和评估；

——可用性改进和预计的数据分析。

6.4.3.4 本阶段第4个要求是修订安全计划以保证所有今后计划工作与系统的应急RAMS要求相一致。

6.4.4 可交付性

6.4.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.4.4.2 本阶段应产生一个更新的安全计划和验收计划。

6.4.4.3 本阶段的可交付性构成后续生命周期阶段的输入。

6.4.5 验证

6.4.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他统计数据的充分性；

b) 系统要求应在比照第2、3阶段产生的可交付性(包括生命周期费用)后验证；

c) 安全性要求应在比照轨道交通主管部门的安全目标和安全方针后验证；

d) RAM要求应对照轨道交通主管部门的RAM目标和RAM方针进行验证；

e) 评估验收计划和确认计划的充分性与完整性；

f) 评估RAM规划的充分性(包括复核所有使用的数据源的充分性)；

g) 评估本阶段内使用的方法、工具和技术的适宜性；

h) 评估本阶段内从事工作的全体人员的能力。

6.4.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段中的部分或全部工作。

6.5 第5阶段：系统需求分配

6.5.1 目标

本阶段的目标是：

a) 把系统的所有RAMS要求分配给所设计的子系统、部件和外部设施；

b) 为所设计的子系统、部件和外部设施规定RAMS验收准则。

6.5.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第4阶段产生的所有可交付性。

6.5.3 要求

6.5.3.1 本阶段的第1个要求是：

a) 给所设计的子系统、部件和外部设施分配功能要求；

b) 给所设计的子系统、部件和降低风险的外部设施分配安全要求；

c) 规定所设计的子系统、部件与外部设施达到全部的系统RAM要求，包括共因失效与多路失效的影响；

d) 复核RAM规划。

6.5.3.2 本阶段的第2个要求是规定符合子系统、部件和外部设施要求的一些要求，包括：

——子系统、部件和外部设施要求的验收准则；

——子系统、部件和外部设施要求的论证、验收过程与步骤。

6.5.3.3 本阶段的第3个要求是复核和更新安全计划并确认计划，确保计划的工作与分配后的系统要求相一致。包括人员独立性要求的关键区域和系统接口控制的安全功能，可折衷妥善处理。

6.5.4 可交付性

6.5.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.5.4.2 本阶段应产生更新的安全计划。

6.5.4.3 本阶段产生的文件应包括给所设计的子系统、部件和外部设施分配系统要求。

6.5.4.4 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.5.5 验证

6.5.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他的统计数据的充分性；

b) 对照第4阶段产生的可交付性，验证系统、子系统、部件和外部设施要求，包括对系统生命周期费用要求的复核；

c) 应验证所设计的子系统、部件和外部设备总的组成结构，确保与整个系统RAMS要求相一致；

d) 应验证子系统、部件和外部设施的RAMS要求，确保它们可追踪系统的RAMS要求；

e) 应验证子系统、部件和外部设施的RAMS要求，确保功能之间的完整性和一致性；

f) 修订后的安全计划和确认计划应经过验证以确保持续可用性；

g) 评估本阶段内使用的方法、工具和技术的适宜性；

h) 评估本阶段从事工作的全体人员的能力。

6.5.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段中的部分或全部工作。

6.6 第6阶段：设计和实现

6.6.1 目标

本阶段的目标：

a) 创建符合RAMS要求的子系统和部件；

b) 证明子系统和部件符合RAMS要求；

c) 为后续的生命周期工作(包括RAMS)建立计划。

6.6.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第5阶段的可交付性。

6.6.3 要求

6.6.3.1 本阶段的第1个要求是设计满足RAMS要求的子系统和部件的方案。

6.6.3.2 本阶段的第2个要求是完成满足RAMS要求的子系统和部件的施工设计。

6.6.3.3 本阶段的第3个要求是在RAMS范围内为今后的生命周期工作建立计划，包括：

——安装；

——调试；

——运营和维修，包括运营和维修程序的定义；

——运营中的数据获取和评估。

6.6.3.4 本阶段的第4个要求是定义、验证和建立能够生产已确认的RAMS的子系统和部件的制造工序，并考虑使用如下措施：

——环境应力筛选；

——RAM改进测试；

——对RAMS有关失效模式进行检查和测试；

——实施安全计划的第4个要求[见6.2.3.4中d)]。

6.6.3.5 本阶段的第5个要求是：

a) 为一已设计的并独立使用的系统准备一个一般安全论据，证明系统能满足安全性要求。该安全论据应通过轨道交通主管部门的正式批准，包括：

——系统概述；

——安全性要求的摘要或参考，包括安全功能SIL的论证；

——生命周期内采用的质量和安全管理控制摘要；

——安全性评估和安全性审查工作摘要；

——安全性分析工作摘要；

——系统所采用的安全工程技术综述；

——制造工序的验证；

——与安全性要求(包括系统的任何SIL要求)一致的充分性；

——应用到系统的限制与约束摘要；

——与本标准的普通要求相比，合同强加并认为是正当的任何特定的考核。

b) 如果在这个阶段合适，则为系统准备应用安全论据。该应用安全论据建立在一般安全论据的基础之上，用于证明对于特定类别的应用，系统设计及其物理实现(包括安装和试验阶段)满足安全性要求。该应用安全论据需经轨道交通主管部门的正式批准，且应包括：

——对于所考核应用的级别，证明系统安全性所必需的全部附加信息；

——系统应用有关的所有约束与限制。

6.6.4 **可交付性**

6.6.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.6.4.2 应记录本阶段内进行的RAMS确认工作。

6.6.4.3 应提出RAMS后续生命周期工作的详细计划。

6.6.4.4 运营与维修规程，包括所有提供备用部件的相关信息，特别是安全相关项目，应在本阶段内提出。

6.6.4.5 本阶段应出示一般安全论据。

6.6.4.6 本阶段可出示应用安全论据。

6.6.4.7 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.6.5 **验证**

6.6.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据与其他统计数据的充分性；

b) 通过分析和测试，验证子系统和部件的设计符合RAMS要求；

c) 通过分析和测试，验证子系统和部件的施工设计与设计方案一致；

d) 确认子系统和部件的实现，以保证与RAMS验收准则(包括生命周期要求)相一致；

e) 通过分析和测试，验证制造布局可生产已确认RAMS的子系统与部件；

f) 验证所有后续生命周期活动计划与系统RAMS要求(包括生命周期费用要求)相一致；

g) 评估一般安全论据与相应的应用安全论据的充分性和完整性；

h) 评估本阶段内使用的方法、工具和技术的适宜性；

i) 评估本阶段内从事工作的全体人员的能力；

j) 保证RAMS确认计划的持续适用性。

6.6.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段中的部分或全部工作。

6.7 **第7阶段：制造**

6.7.1 **目标**

本阶段的目标是：

a) 实施能生产出已确认 RAMS 的子系统和部件的制造工序；

b) 建立以 RAMS 为中心的工序确保计划；

c) 建立子系统和部件 RAMS 的支持计划。

6.7.2 **输入**

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第 6 阶段产生的可交付性。

6.7.3 **要求**

6.7.3.1 本阶段的第 1 个要求是验证和实现制造工序。

6.7.3.2 本阶段的第 2 个要求是建立子系统和部件支持计划，包括：

——子系统和部件 RAMS 支持文件的准备、验证和确认；

——RAMS 内容中运营和维修程序的准备、验证和确认；

——子系统和部件关于 RAMS 培训材料的准备、验证和确认。

上述文件、程序和培训材料应在所有后续阶段中复核。

6.7.3.3 本阶段的第 3 个要求(如果合适)是：

a) 安排满足要求的制造；

b) 实施满足要求的制造；

c) 实现 RAMS 流程保证，以避免潜在的 RAMS 相关失效模式。

6.7.4 **可交付性**

6.7.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.7.4.2 应继续记录本阶段内进行的 RAMS 确认工作。

6.7.4.3 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.7.5 **验证**

6.7.5.1 本阶段应执行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据及其他统计数据的充分性；

b) 验证 RAMS 支持文件是正确的、充分的，并与生命周期费用要求和系统规定的目标 RAMS 要求相一致；

c) 评估以确保正在生产的产品按系统要求制造；

d) 评估本阶段内使用的方法、工具和技术的适宜性；

e) 评估本阶段内从事工作的全体人员的能力。

6.7.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段的部分或全部工作。

6.8 **第 8 阶段：安装**

6.8.1 **目标**

本阶段的目标是：

a) 对形成完整系统所需要的子系统和部件进行组合装配与安装；

b) 启动系统支持计划。

6.8.2 **输入**

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第 6 阶段准备的安装计划，以及第 7 阶段制造的子系统和部件以及第 7 阶段准备的 RAMS 支持文件。

6.8.3 **要求**

6.8.3.1 本阶段的第 1 个要求是按照安装计划对形成完整系统所需要的子系统、部件和外部设施进行组合装配和安装。

6.8.3.2 本阶段的第 2 个要求是写出安装流程，包括：

——复核设计和实现阶段(6.6.3.3)第 3 个要求的计划；

——安装工作；

——用于解决失效和不兼容性的活动。

6.8.3.3 本阶段的第3个要求是在安装完成后复核和修改安全计划，确保记录了系统或工序发生的变化，并在后续的生命周期工作中有效管理。

6.8.3.4 本阶段的第4个要求是：

a) 开始人员培训；

b) 制订可用的支持步骤；

c) 建立备件供应；

d) 建立工具供应。

6.8.4 可交付性

6.8.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.8.4.2 应继续记录本阶段内所执行的所有RAMS确认工作，包括安装活动。

6.8.4.3 本阶段应更新安全计划。

6.8.4.4 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.8.5 验证

6.8.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(适当时)数据和其他统计数据的充分性；

b) 验证安装工作是按安装计划进行的；

c) 通过分析和测试，验证已安装的系统满足RAMS要求；

d) 评估安全计划以确保其持续适用性；

e) 评估系统支持计划的有效性和充分性；

f) 评估本阶段内使用的方法、工具和技术的适宜性；

g) 评估本阶段内从事工作的全体人员的能力。

6.8.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段的部分或全部工作。

6.9 第9阶段：系统确认(包括安全性验收和调试)

6.9.1 目标

6.9.1.1 本阶段的目标是：

a) 确认子系统、部件和降低风险的外部措施的总成与系统的RAMS要求一致；

b) 对子系统、部件和降低风险的外部措施的总成进行调试；

c) 准备和(合适时)验收系统的特定应用安全论据；

d) 提供获得的数据并评估。

6.9.1.2 关注第10阶段(系统验收)的要求是非常重要的，如果适合于所考核的系统，它可以是第9阶段要求的集成。如果是这样，在第9阶段实现后，本阶段的可交付性已证明第10阶段的要求得到了充分满足。

6.9.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是在第4阶段内产生的系统要求、验证和确认计划，还有第6阶段的调试计划及第7阶段准备的培训材料。

6.9.3 要求

6.9.3.1 本阶段的第1个要求是按照确认计划来确认子系统、部件和降低风险的外部措施的总成并记录确认流程，包括：

——RAMS确认工作对照验收准则的详细情况，包括RAM论证和安全性分析；

——确认工作采用的流程、工具、设备对照验收准则的详细情况；

——按所有验收准则进行确认工作的结果；

——应用于系统的所有限制与约束；

——解决各种失效和不兼容性的活动。

6.9.3.2 本阶段的第2个要求是：

a) 按照调试计划调试子系统、部件和降低风险的外部措施的总成并记录调试过程，包括：

——调试工作；

——失效报告与评估工作；

——解决各种失效和不兼容性的活动；

——任何约束与限制系统使用的详细情况。

b) 如果需要，采取试运营周期以解决正式运营时的系统问题。当采用作为系统验收一个部分的试运营周期时，在系统投入商业运营之前，应考虑证明系统的安全性。

6.9.3.3 本阶段第3个要求是，若在第6阶段还没有准备好[见6.6.3.5b)]，则应为系统准备一个应用安全论据，用它来证明该系统在特定的应用中符合系统安全性要求。该应用安全论据需经轨道交通主管部门的正式批准，并应包括：

——系统综述；

——安全性要求的参考或摘要(包括该应用的安全功能SIL合理性的考虑)；

——生命周期内采取的质量和安全管理控制摘要；

——安全评估及安全评审工作摘要；

——安全性分析工作摘要；

——系统所采用的安全工程技术概要；

——符合系统安全性要求的充分性，包括遵循在特定应用中的SIL要求(含其物理实现)的充分性；

——对本应用采取的限制与约束摘要。

6.9.3.4 本阶段的第4个要求是建立和实现一个流程，用于获取和评估运营数据，然后作为系统改进过程的输入。

6.9.4 可交付性

6.9.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.9.4.2 应继续记录本阶段内执行的所有RAMS确认工作，包括调试活动。

6.9.4.3 在本阶段内应为系统提供一个特定应用安全论据。

6.9.4.4 应继续记录本阶段内进行的所有验收工作。

6.9.4.5 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.9.5 验证

6.9.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他统计数据的充分性。

b) 通过分析和测试，验证并确认所安装系统满足RAMS要求。应注意在有些轨道交通系统中，特定应用安全论据的验收要求在安装和调试工作进行之前完成验收。

c) 验证调试活动是按调试计划实施的。

d) 评估运行数据采集系统的有效性和充分性。

e) 评估本阶段内使用的方法、工具和技术的适宜性。

f) 评估本阶段内从事工作的全体人员的能力。

6.9.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段的部分或全部工作。

6.10 第10阶段：系统验收

6.10.1 目标

本阶段的目标是：

a) 评估子系统、部件和降低风险的外部措施的总成符合完整系统的所有 RAMS 要求；

b) 验收投入运行的系统。

6.10.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是在第 4 阶段准备的系统要求、验证与确认计划和验收计划以及在第 9 阶段中准备的验证和确认工作的记录。

6.10.3 要求

6.10.3.1 本阶段的第 1 个要求是根据系统验收计划评估系统的所有验证和确认工作，特别是 RAM 验证和确认以及特定应用安全论据。

6.10.3.2 如果合适的话，本阶段的第 2 个要求是正式验收系统以便投入运行。

6.10.3.3 本阶段的第 3 个要求是复核和更新危害记录，记录系统确认或验收过程中确定的残留危害，并确保这些危害所造成的风险得以有效管理。

6.10.4 可交付性

6.10.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.10.4.2 应继续记录本阶段所执行的所有验收工作。

6.10.4.3 更新本阶段的危害记录。

6.10.4.4 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.10.5 验证

6.10.5.1 本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据与其他统计数据的充分性；

b) 通过分析和测试验收系统满足 RAMS 要求(包括生命周期费用要求)；

c) 验证验收工作是按验收计划执行的；

d) 评估修改过的安全计划的延续适用性；

e) 评估以确保任何残留的危害已得到有效地管理；

f) 评估特定应用安全论据的充分性和完整性；

g) 评估本阶段内使用的方法、工具和技术的适宜性；

h) 评估本阶段内从事工作的全体人员的能力。

6.10.5.2 任何一个错误或不足需要重复先前一个或多个生命周期阶段的部分或全部工作。

6.11 第 11 阶段：运营和维修

6.11.1 目标

本阶段的目标是运营(在规定限值内)、维修与支持子系统、部件和降低风险的外部措施的总成，使之继续符合系统 RAMS 要求。

6.11.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是第 6 阶段准备的运营和维修程序。

6.11.3 要求

6.11.3.1 本阶段的第 1 个要求是监控系统实现，实施运营和维修程序，特别是与系统性能和生命周期费用相关的程序。

6.11.3.2 本阶段的第 2 个要求是用下列方法确保整个阶段中符合系统 RAMS 要求：

a) 运营和维修程序的定期核查和更新；

b) 系统培训文件的定期核查；

c) 定期核查和更新危害记录与安全论据；

d) 有效的后勤保障，包括备品、工具、校正措施、胜任的人员和以 RAMS 为中心的维修；

e) 维护失效报告分析和纠正措施系统(FRACAS)。

6.11.4 可交付性

6.11.4.1 应继续记录在本阶段内所做的假设、论证及所有执行的 RAMS 工作。

6.11.4.2 在本阶段内应更新相应的系统文件。

6.11.4.3 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.11.5 验证

本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他统计数据的充分性；

b) 验证后勤计划的变动与系统 RAMS 要求和生命周期费用要求一致；

c) 评估本阶段内使用的方法、工具和技术的适宜性；

d) 评估本阶段内从事工作的全体人员的能力。

6.12 第 12 阶段：性能监控

6.12.1 目标

本阶段的目标是保持系统 RAMS 性能的置信度。

6.12.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据，特别是系统 RAMS 要求和系统支持数据。

6.12.3 要求

6.12.3.1 本阶段的第 1 个要求是建立、实施和定期核查以下流程：

——RAMS 和运营性能统计数据的收集；

——RAMS 和性能数据的获得、分析和评估；

——在安全论据中的假设保持有效的核查。

6.12.3.2 本阶段的第 2 个要求是分析影响下述内容的性能、RAM 数据以及统计数据：

——新的运营和维修程序；

——系统后勤保障的变动。

6.12.4 可交付性

6.12.4.1 应继续记录本阶段内所有性能监控工作、所作的假设与理由。

6.12.4.2 本阶段内可能更新的系统支持文件。

6.12.4.3 本阶段的可交付性构成后续生命周期阶段的一个关键输入。

6.12.5 验证

本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他统计数据的充分性；

b) 验证保障计划的变动与系统 RAMS 要求和生命周期费用要求相一致；

c) 评估本阶段内使用的方法、工具和技术的适宜性；

d) 评估本阶段内从事工作的全体人员的能力。

6.13 修改与更新

6.13.1 目标

本阶段的目标是控制系统修改与更新工作来保持系统 RAMS 的要求。

6.13.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据。

6.13.3 要求

6.13.3.1 本阶段的第 1 个要求是建立一个安全计划。

6.13.3.2 本阶段的第 2 个要求是在 RAMS 范围内建立、实现和定期核查控制系统修改与更新的流程，包括：

——通过强制采用一种合适的生命周期模型来控制全部修改与更新工作；
——在修改与更新之后要求建立一个验证、确认和验收系统 RAMS 性能的程序；
——要求分析变更的原因；
——要求进行变更 RAMS 的影响分析，包括对生命周期费用要求的影响；
——要求变更计划的实现及随后的验收；
——要求记录修改与更新工作；
——要求更新所有受影响的系统文件。

6.13.4 可交付性

6.13.4.1 本阶段的关键可交付性是确认修改过的系统。

6.13.4.2 本阶段的结果、作出的所有假设及理由应形成文件。

6.13.4.3 继续记录本阶段内进行的验证、确认和验收工作。

6.13.4.4 在本阶段内应更新危害记录。

6.13.4.5 在本阶段内应更新应用安全论据。

6.13.4.6 必需时，应复核及更新全部 RAM 相关的文件。

6.13.4.7 本阶段的可交付性构成后续生命周期阶段的关键输入。

6.13.5 验证

本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)数据和其他统计数据的充分性；
b) 验证和确认系统的任何变更或修改与系统 RAMS 要求和生命周期费用要求相一致；
c) 评估任何修改过的系统文件(特别是系统安全论据文件)的充分性和完整性；
d) 评估本阶段内使用的方法、工具和技术的适宜性；
e) 评估本阶段内从事工作的全体人员的能力。

6.14 停用及处置

6.14.1 目标

本阶段的目标是控制系统停用及处置工作。

6.14.2 输入

本阶段的输入应包括所有相关的信息和(合适时)满足本阶段要求所必需的数据。

6.14.3 要求

6.14.3.1 本阶段的第 1 个要求是：

a) 确定停用与处置对与待停用系统关联的任何系统和外部设施的影响；
b) 制订停用计划，包括确定以下内容的步骤：
——系统和相联外设的安全关闭；
——系统和相联外设的安全拆除；
——继续保证受停用系统影响的任何系统或外部设施的 RAMS 要求的一致性。

6.14.3.2 本阶段的第 2 个要求是提供包括生命周期费用在内的 RAMS 生命周期性能的分析，作为将来系统的输入。

6.14.4 可交付性

6.14.4.1 本阶段的结果、作出的所有假设及理由应形成文件。

6.14.4.2 继续记录本阶段执行的全部停用及处置工作。

6.14.4.3 在本阶段内应更新危害记录。

6.14.4.4 建立安全计划说明停用及处置工作和停用后要完成的工作。

6.14.4.5 本阶段可产生一个修订的应用安全论据。

6.14.4.6 在停用与处置工作期间，更新后的文件应包含仍然满足受影响的相关系统 RAMS 要求的一

致性。

6.14.5 验证

本阶段应进行如下验证工作：

a) 评估本阶段内作为工作输入的信息、(合适时)相应的数据和其他统计数据的充分性；

b) 评估被停用及处置工作影响的系统所有文件的充分性；

c) 评估本阶段内使用的方法、工具和技术的适宜性；

d) 评估本阶段内从事工作的全体人员的能力。

附 录 A
（资料性附录）
RAMS 规范概要（示例）

A.1 引言

为了促进本标准的应用，附录中列出了轨道交通系统 RAMS 规范的原理性概要。这个概要示例和本标准的图 8、图 9 有关，关于生命周期阶段相应的说明详见第 6 章，在此概要中提供以机车车辆作为示例的详细情况。

A.2 概要

RAMS 规范的基本结构和内容（完整系统要求的一部分）应和下面的概要一致。

1 立项

1.1 确定项目；

1.2 可交付性和最后期限；

1.3 项目组织和 RAMS 管理。

2 通用系统描述

2.1 系统的技术描述。

2.2 特定应用和运营：

例如对于机车车辆

——高速列车运营；

——列车编组；

——任务概要；

——地理位置；

——列车时刻表和容差；

——运营概要；

——安全性原理；

——人为因素考虑。

2.3 子系统的技术描述：

例如对于机车车辆

——能源供给系统；

——制动系统；

——牵引系统；

——通风系统；

——保护系统；

——控制系统；

——通信系统；

——采暖系统。

3 运营条件与环境条件

3.1 确定运营模式：

例如对于机车车辆

——日运营时间或里程；

——日待用时间；

——日停止运营时间。

3.2 期望寿命：

例如对于机车车辆

——系统预计使用的总时间(年)；

——年平均运营时间。

3.3 确定环境条件：

例如对于机车车辆

——遵循标准；

——温度范围；

——机车车辆内部的温度范围；

——运营中；

——停用状态；

——湿度范围；

——最高海拔。

4 可靠性

4.1 可靠性目标；

4.2 规定可靠性目标以满足特定应用所需的性能(见 2.2)；

4.3 系统失效模式和平均失效间隔时间(MTBF)：

例如对于机车车辆

失效种类	系统失效模式	对运行的影响	MTBF(.)[a]
特大	完全失效	不能运行	
重大	重大的功能失效	紧急运行 1	
次要	不重大的功能失效	紧急运行 2	
轻微	可忽略的功能失效	正常运行	
[a] MTBF(.)单位为小时、年或千米。			

深入了解见 4.5.2.2 表 1、附录 C 表 C.1。

4.4 对运营和性能的影响：

例如对于机车车辆

——对运行中完全失效、紧急运行 1、紧急运行 2 和对运营无影响的失效等各种技术和运营条件作出规定；

失效种类	对运行的影响[a]	性能			备注
		功率(%)	速度(%)	(.)	
特大	不能运行	0	0		
重大	紧急运行 1				
次要	紧急运行 2				
轻微	正常运行	100	100		简化信息显示
[a] 在应用中规定以下几个方面的技术与运行条件： ——完全失效； ——紧急运行 1； ——紧急运行 2； ——对运营没有影响的失效。					

5 维修和修理

5.1 预防性维修

维修制度和遇到的维修类型 R0～R3 的说明。

例如对于机车车辆

维修类型	MTBM(.)	MTTM(.)
R0		
R1		
R2		
R3		
MTBM：平均维修间隔时间(单位：小时、年或千米) MTTM：平均维修前时间(平均维修期限，单位：小时或天)		

详细说明见附录 C、表 C.2 和表 C.4

5.2 修理：

修理规章和必需的后勤保障描述。

- 规定系统平均恢复时间(MTTR)(单位：小时或天)。
- 规定包含在 MTTR 组成中的时间成分：
  ——调用/行车时间；
  ——进入时间；
  ——备件准备时间；
  ——修理/替换时间；
  ——测试/启动时间；
  ——数据接收时间；
  ——等待时间。
- 说明每个可修理部件的修理/替换时间(最大或平均修理/替换时间)及条件。
- 说明最小的备件供应和后勤保障条件。

例：

可修理部件	平均修理替换时间	修理地点(现场，修理车间)	必需的修理人数

6 安全性

6.1 安全目标：

- 说明安全目标和应用规章(见 2.2)。

6.2 危害情况：

- 识别和列出在应用中要考虑的危害；
- 指出危害的频度级别(见 4.6.2.2，表 2)。

6.3 安全相关的功能和失效：

- 识别和列出安全相关的功能或部件，如：制动或与制动相关的部件。
- 指出每个安全相关功能在应用中的安全相关失效(见 4.3.6 和 4.3.7)。

例如对于机车车辆

安全相关功能/部件	安全相关失效描述	MTBSF[a](年或千米)
制动		
车厢门		
[a] 参见附录 C,表 C.5。		

- 安全危害严重等级;

——规定应用的安全危害严酷等级(见 4.6.2.3,表 3)。

- 风险分类:

——规定风险的容许程度(见 4.6.3.2 和 4.6.3.3)。

7 可用性

系统的可用性 A 归因于下面的部分:

- 预料的不可用性(可维修性):$1-A_m$
- 没有预料到的不可用性(修理):$1-A_R$

$$A = 1-[(1-A_m)+(1-A_R)]$$

$$A = \mathrm{MUT}/[(\mathrm{MUT}+\mathrm{MDT})];0 \leqslant A \leqslant 1$$

式中:

MUT=平均可用时间;可用相应的 MTBF、MTBSF 等等代替。

MDT=平均不可用时间;可用相应的 MTTM、MTTR 等等代替。

对特定可用性 $A(.)$应规定 MUT 与 MDT。

如"安全系统"的可用性 As,(MUT= MTBSF)。

任务时间 T(如 1 年)内的不可用时间 $d(T)$的结果是:

$d(T)=(1-A)\times T$。

可用性规范:

- 说明系统可用性 A 是可维修性和修理要求的联合(见 A.2.5);
- 可维修性和修理规章是按期望一定的可用性 A 来规定的。

8 RAMS 性能的论证

第 9 阶段系统确认和第 10 阶段系统验收的 RAMS 性能的说明。

搜集的证据更加易于说明 RAMS 性能,如:

——RAMS 管理及组织;

——RAMS 资源的可用性;

——RAMS 需求规范;

——RAMS 计划和规划;

——RAMS 相关的核查报告;

——RAMS 分析报告;

——RAMS 测试记录(部件);

——失效数据获取(统计表);

——特定应用安全论据;

——系统确认和验收;

——在早期运营阶段 RAMS 性能监控;

——生命周期费用评估。

9 RAMS 规划

供应商应该建立 RAM 规划和安全计划,用以保证最有效地达到该项目的 RAMS 需求。

一个基本的 RAMS 规划的示例参见附录 B。

附 录 B
（资料性附录）
RAMS 规划

B.1 本附录给出一个关于基本 RAM 规划/安全计划的概要程序的示例，还列出一些关于 RAMS 管理和分析的方法和工具。

B.2 供应商应建立一个 RAMS 规划，它有助于满足所考虑应用的 RAMS 需求。类似项目的 RAMS 设计或供应商的系统要求可以提供一个“标准的 RAMS 规划”，它是一个公司的 RAMS 原始资料。

B.3 步骤

以下给出一个基本 RAMS 规划的简要示例步骤。

1 规定符合公司商业流程的合适生命周期。

结果：建立公司的生命周期或项目的各个阶段。

2 指定每个项目阶段及其相关的 RAM 和安全工作，这些应充分满足项目和系统指定的要求。

结果：确定生命周期内所有必需的 RAMS 工作。

3 规定在公司内执行每个 RAMS 工作的责任者。

结果：确定必需的 RAMS 资源和人员的责任。

4 规定每个 RAMS 工作必需的指令、工具和参考文件。

结果：文件化的 RAMS 管理。

5 在公司作业中执行的 RAMS 活动。

结果：集成 RAMS 管理规程（RAMS 原始资料）。

B.4 基本 RAMS 规划示例

表 B.1 给出基本 RAMS 规划的概要。这个概要由能够应用到特定项目中的一组工作的示例组成。

表 B.1 基本 RAMS 规划概要示例

项目—阶段	RAMS 工作	责任者	参考文件
预 计	——估计指定应用的 RAMS 目标		
可行性研究	——评估 RAMS 要求 ——评价 RAMS 过去的数据和经验 ——确定指定应用对安全性的影响 ——咨询用户关于 RAMS 的要求（必要时）		
邀请投标者	——进行初步的 RAMS 分析（最坏情况） ——系统 RAMS 要求的分配（子系统/设备、其他相关系统等） ——进行系统危害和安全风险的分析 ——进行 RAM 相关的风险分析 ——准备进一步的 RAMS 数据评审 ——逐条注释 RAMS		
合同协议	核查/修改初步的 RAMS 分析和 RAMS 分配		
指令作业： 规定系统要求	——确定项目具体的 RAMS 管理 ——规定系统 RAMS 需求（所有的） ——建立 RAM 规划（标准 RAMS 规划充分否?） ——分配 RAMS 要求给分包商、供应商 ——规定 RAM 验收准则（所有的）		

表 B.1（续）

项目—阶段	RAMS 工作	责任者	参考文件
指令作业：设计和实现	——可靠性分析(FMEA) ——安全性分析(FMECA)，如果可行的话 ——维护/修理分析；说明维护/修理策略 ——在维护/修理策略基础上作可用性分析 ——RAMS 核查 ——生命周期费用估计 ——RAMS 说明，一致性的证据 ——设计/制造 FMEA ——测试可靠性和可维修性，如果可行的话		
采购	提供给分包商/供应商的 RAMS 规范		
制造/测试	RAMS 相关的质量保证/工艺保证		
调试/验收	——完成 RAM 说明 ——准备特定应用安全论据 ——启动 RAMS 数据评估 ——早期运营的 RAM 测试、数据筛选和评估		
运营/维修	——临时的运营和维修(维修/修理策略) ——运营人员和维修人员的培训 ——RAMS 数据评估 ——生命周期费用评估 ——性能复核		

B.5 工具清单：

下面列出了一些实施和管理 RAMS 规划的合适的方法和工具。相关工具的选择取决于研究中的系统及系统的重要性、复杂性和新颖性等等。

1 RAMS 规范的概要形式：以保证所有的 RAMS 相关要求的评估(参见附录 A 的示例)。

2 正规设计核查程序：着重于 RAMS，使用某些普通的和应用指定的合适的检查清单，如：

IEC 61160 正规设计核查(第 1 次修订版)。

3 实施“从上到下”(推理法)和“从下到上”(归纳法)的程序，对简单和复杂功能的系统结构进行深入 RAM 分析和最坏情况的分析。通常对不同技术使用的 RAM 分析程序、方法、有利之处和不利之处、输入数据和其他要求的一般综述如下所示：

IEC 60300-3-1 可信性管理 第 3 部分：应用指南 第 1 节：可信性分析技术：方法指南

不同的 RAM 分析技术分别在不同的标准中描述，如：

IEC 60706-1 设备可维修性指南 第 1 部分 第 1、2、3 节：引言，要求和可维修性计划

IEC 60706-2 设备可维修性指南 第 2 部分 第 5 节：在设计阶段内进行可维修性研究

IEC 60706-3 设备可维修性指南 第 3 部分 第 6、7 节：数据的验证、收集、分析和表述

IEC 60706-4 设备可维修性指南 第 4 部分 第 8 节：维修及其保障规划

IEC 60706-5 设备可维修性指南 第 5 部分 第 4 节：诊断测试

IEC 60706-6 设备可维修性指南 第 6 部分 第 9 节：可维修性评估中的统计方法

IEC 60812 系统可靠性的分析技术 失效模式和影响分析(FMEA)程序

IEC 60863 可靠性、可用性和可维修性预测说明

IEC 61025 故障树分析(FTA)法

IEC 61078　可信性分析技术　可靠性框图法

IEC 61165　马尔可夫技术的应用

在设计中部件所统计的“RAM”数据的可用性是 RAM 分析的基础(特别是:失效率、修理率、维修数据、失效模式、事故率、数据和随机事件的分布状态等等),如:

IEC 61709(1996)　电子部件　可靠性　失效率和应力模型转化的参考条件

US MIL HDBK 217　电子系统的可靠性预计

许多关于系统 RAM 分析和统计数据分析的计算机程序也可利用。

4　实现危害和安全/风险分析程序:以下列出一些

US MIL HDBK 882D　系统安全设计要求

US MIL HDBK 764(MI)　对军事材料的系统安全工程、设计指南

上面的第 3 条关于 RAM 的基本技术和分析方法也可用于安全/风险分析。

GB/T 20438.1～20438.7《电气/电子/可编程电子安全相关系统的功能安全》由以下几部分组成:

第 1 部分:一般要求;

第 2 部分:电气/电子/可编程电子安全相关系统的要求;

第 3 部分:软件要求;

第 4 部分:定义和缩略语;

第 5 部分:确定安全完整性等级的方法示例;

第 6 部分:GB/T 20438.2 和 GB/T 20438.3 的应用指南;

第 7 部分:技术和措施概述。

5　RAM 测试计划和程序:目的是测试部件、装备和系统的长期运营性能是否与要求一致。更加深入的 RAMS 分析和测试结果是用来改进 RAMS 规划,如:

IEC 60300-3-5　可信性管理　第 3-5 部分:应用指南　可靠性测试条件和统计测试原理

IEC 60605-2　设备可靠性测试　第 2 部分:测试周期设计

IEC 60605-3-1　设备可靠性测试　第 3 部分:首选的测试环境　户内可移动的设备　粗模拟

IEC 60605-3-2　设备可靠性测试　第 3 部分:首选的测试环境　在气候保护的地方固定使用的设备　精模拟

IEC 60605-3-3　设备可靠性测试　第 3 部分:首选的测试环境　第 3 节:测试周期 3:在部分气候保护地方的固定使用的设备　粗模拟

IEC 60605-3-4　设备可靠性测试　第 3 部分:首选的测试环境　第 4 节:测试周期 4:便携的及非固定使用的设备　粗模拟

IEC 60605-4　设备可靠性测试　第 4 部分:成指数分布的统计步骤　点的判断、置信度间隔、预测间隔及容差间隔

IEC 60605-6　设备可靠性测试　第 6 部分:恒定失效率和恒定失效密度假设的有效性试验

IEC 61014　可靠性增长设计

IEC 61070　稳定状态可用性遵循的测试程序

IEC 61123　可靠性测试　成功率遵循的测试规划

现场的 RAMS 数据评估是很重要的(在运营中的 RAMS 测试),如:

IEC 60300-3-2　可信性管理　第 3 部分:应用指南　第 2 节:现场可靠性数据的收集

IEC 60319　电子部件可靠性数据的说明

B.6　执行 LCC(生命周期费用)分析的步骤/工具:LCC 分析可以利用各种各样的计算机程序。

附 录 C
（资料性附录）
轨道交通应用参数示例

适用于轨道交通的典型参数与符号示例列表如下：

C.1 可靠性参数

表 C.1 可靠性参数示例

参 数	符 号	量 纲
失效率	$Z(t)$,λ	失效数/(时间、距离、周期)
平均可用时间	MUT	时间、距离、周期
平均失效前时间 平均失效前距离 (对不可修理的项目而言)	MTTF MDTF	时间、距离、周期
平均失效间隔时间 平均失效间隔距离 (对可修理的项目而言)	MTBF MDBF	时间、距离、周期
故障发生概率	$F(t)$	无
可靠度(成功发生概率)	$R(t)$	无

C.2 可维修性参数

表 C.2 可维修性参数示例

参 数	符 号	量 纲
平均不可用时间	MDT	时间、距离、周期
平均维修间隔时间、距离	MTBM/MDBM	时间、距离、周期
平均修复性维修间隔时间、距离 平均预防性维修间隔时间、距离	MTBM(c)/MDBM(c) MTBM(p)/MDBM(p)	时间、距离、周期
平均维修前时间	MTTM	时间
平均修复性维修前时间 平均预防性维修前时间	MTTM(c) MTTM(p)	时间
平均恢复时间	MTTR	时间
错误报警率	FAR	时间的倒数

C.3 可用性参数

表 C.3 可用性参数示例

参　数	符　号	量　纲
可用性 ——固有的 ——达到的 ——运营的	$A(.)=MUT/(MUT+MDT)$ A_i A_a A_o	无
可用率	FA(=可用机车车辆/保有量)	无
准时率	SA	无

C.4 后勤保障参数

表 C.4 后勤保障参数示例

参　数	符　号	量　纲
运营和维修费用	O&MC	货币
维修费用	MC	货币
维修工时	MMH	时间(小时)
后勤和管理延期	LAD	时间
故障修复时间		时间
修理时间		时间
维修保障性		无
替换人员	EFR	无
需要时库存备件的概率	SPS	无

C.5 安全性参数

表 C.5 安全性能参数示例

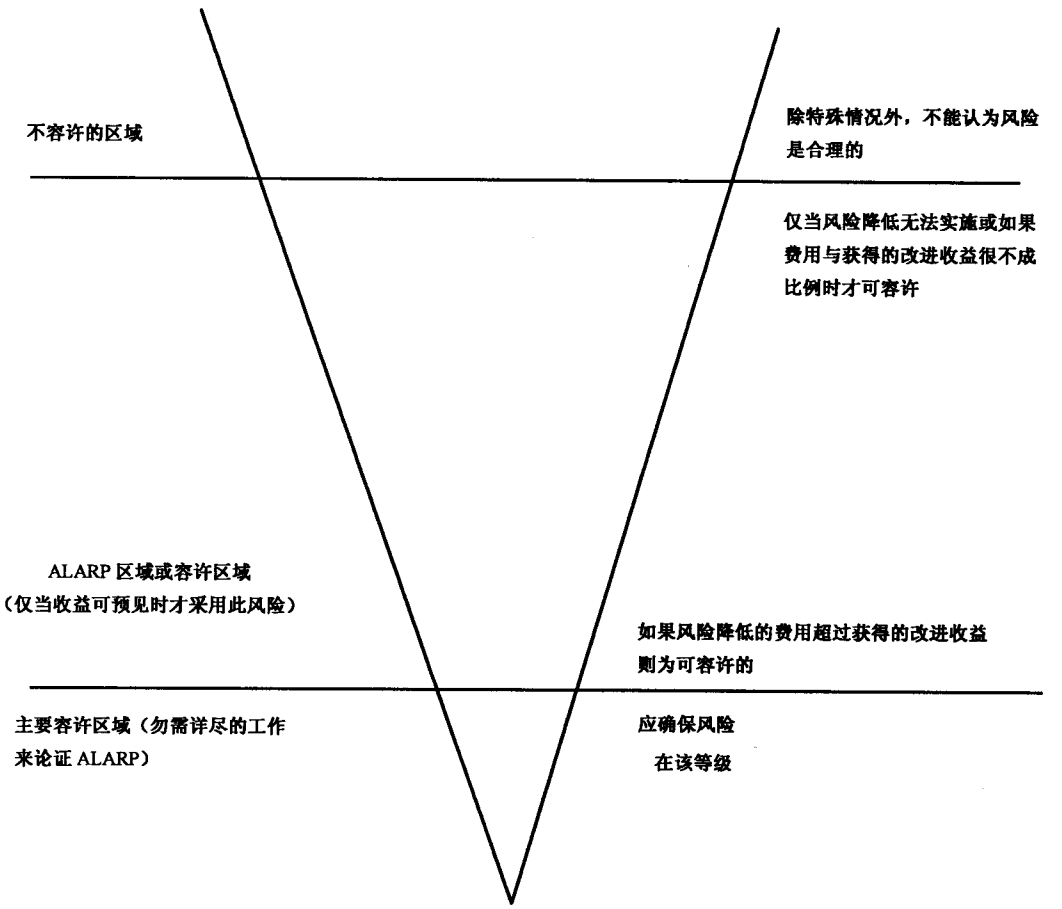
参　数	缩写符号	量　纲
平均无危害性失效时间	MTBF(H)	时间、距离、周期
安全系统平均无失效时间	MTBSF	时间、距离、周期
危害率	$H(t)$	故障数/时间、距离、周期
安全相关失效率	$F_s(t)$	无
安全功能概率	$S_s(t)$	无
恢复安全的时间	TTRS	时间

附 录 D
（资料性附录）
几种风险验收原理的例子

注：本附录中的值仅用来说明原理而不作其他用途。

D.1 ALARP(风险降到可行)原理(在英国实施)

本原理可以用下面的简图说明：



D.1.1 最上面的范围规定了不容许的风险等级。有些风险很大，且有些结果太不可接受，因此在任何场合它们都是不容许的，也不能认为它们是合理的。如果风险等级不能降低到此范围以下就不能投入运营。

D.1.2 该简图中的最下面范围规定为主要容许区域，该区域中风险都可认为很小不需要通过任何 ALARP 判据的证明。

D.1.3 上边界与下边界之间的区域称为 ALARP 区域。应强调的是所有在这个区域内的风险并不都是充分的，应使它们尽量低到可行。证明 ALARP 有很多方法。应充分表明采用目前可用的最佳标准和实践。对新的运营，或是当前标准或实践值得怀疑，要引入成本效益分析和使用期限的概念。

D.1.4 当可能有大量人员伤亡的灾难发生时，应检查社会风险。这些大型事故的厌恶度被称为“微分风险厌恶度”（DRA），可以在对数 F-N 曲线上用一条斜率为 -1 的直线来表示，F 表示每年发生频率（年$^{-1}$），N 表示发生一次事故的伤亡人员数。

D.2 GAMAB(综合最优)原理(在法国实施)

这个原理的完整表述如下:

"新的导向运输系统应提供一个风险等级,它整体上至少与现有的任何等效的系统一样好。"

D.2.1 根据要求"至少",此表述考虑现有制造的系统,并要求新系统有隐含的进步;根据要求"整体上",不需要考虑特定风险。轨道交通系统供应商可随意为系统固有的不同风险区分分配和采用相关的方法,即定性的和定量的方法。

D.2.2 采用定量方法时,可以用下述方法来解释:

1 $\tau_{c.ref}$(=死亡人数/旅客人数,死亡人数为两列列车相撞导致的死亡人数)表示在上一年运行中,轨道交通运输系统的经验数据。在同样的自然环境下,该分数应从现有系统的统计数据中提取,并作为同类新型系统的基准。

2 现在考查新的(更新的)系统。在此系统中规定:

C=一列车的载客量(乘客人数/车)

F=列车密度(列车/小时)

r=平均满员率(列车不全满)

n_c=新型系统中每次碰撞的死亡人数

D_m=吞吐量(旅客人数/小时)= $r\times C\times F$

因此,实际上每个旅客经历的碰撞次数应该是:

$\mathrm{col}=(\tau_{c.ref}/n_c)$(碰撞次数/旅客人数)

并且新型系统的碰撞率应小于现有系统的碰撞率:

因此,

$$\lambda_c \leqslant \mathrm{col}\times D_m$$
$$=(\tau_{c.ref}/n_c)\times D_m$$
$$=\tau_{c.ref}\times (r\times C/n_c)\times F \text{ (碰撞次数/小时)}$$

3 备注:

——对于现有系统和已设计系统而言,假定同一列车中死亡人数在旅客人数中所占的比例相同:即:$n_c/r\times C$=常量;

——对于较低的运行质量而言,λ_c 可以是难以实现的要求,特别是 F 值较小时(列车密度);

——改进由符号"≤"推进;

——设计者/供应商可在轨旁设备和车载设备之间自由分配 λ_c。

D.3 MEM(最小内源性死亡率)原理(在德国实施)

此原理由下述方法导出:

1 死亡有许多不同的原因。下列这样的原因被称为"技术因素"。如:

——娱乐和体育(冲浪、试用等);

——自助活动(割草等);

——工作机器;

——运输。

但不包括下述内容:

——疾病死亡;

——先天畸形死亡。

根据被考查的人口年龄的变化,每组导致一定的年龄死亡百分数也随之变化。此风险是指"内源性死亡率 R"。

2 在发达国家中，R 在 5 岁到 15 岁年龄段的值最小。内源性死亡率的最低等级称为“最小内源性死亡率”，用 R_m 表示，它由下式决定：

$$R_m = 2 \times 10^{-4} \text{ 死亡人数 /(人 × 年)}$$

3 综上所述，简要陈述下述规则：

“新型运输系统的危害应不使指标 R_m 明显增加”。

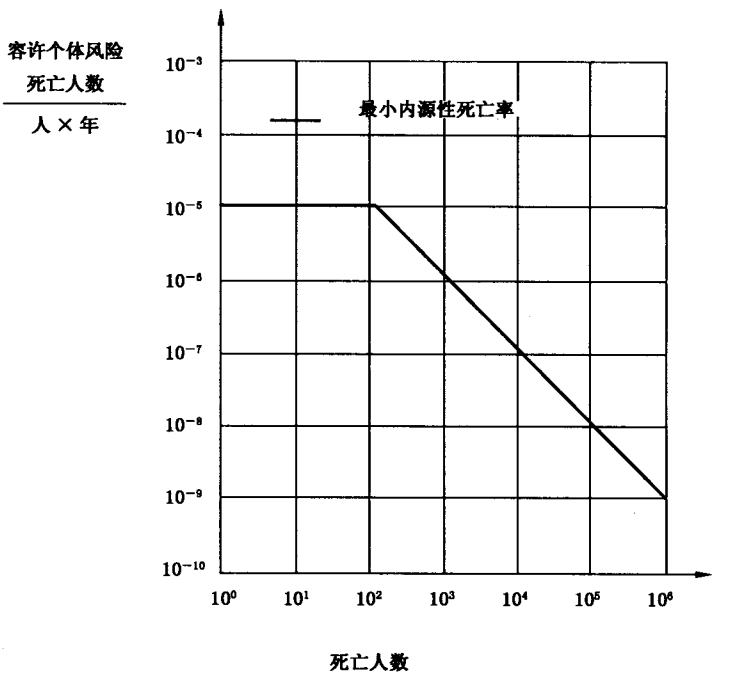
实际上可以使用下列数据：

$R_1 \leqslant 10^{-5}$ 死亡人数/(人×年)

$R_2 \leqslant 10^{-4}$ 重伤人数/(人×年)

$R_3 \leqslant 10^{-3}$ 轻伤人数/(人×年)

此观点在特大灾难或小型灾难的事实上，虽不能使受害者的家庭找到任何安慰，但就涉及到的实际运输方式(如火车、飞机等)而言，这是正确的。对于可能造成大量人员伤亡的事故，“微分风险厌恶度”(DRA)可以用下面的递减斜率曲线来介绍。



附 录 E
（资料性附录）
生命周期 RAMS 流程内的责任

作为一个典型轨道交通项目的一般导则，下列各条适用：

——通常，要求由用户或某个制定规章的（法定的）机构来制定；

——同样，批准和验收由用户或制定规章的机构来执行；

——解决方法及其效果与验证通常由承包商详细说明或执行；

——通常同时实施确认。

但此一般规则取决于有关各方的合同关系与法定关系。

然而，在每种情形下，本标准要求在生命周期各个阶段工作的责任都被规定且经过协商。下面的矩阵表举例说明典型安排的责任。

	用户/操作员	批准机构	（主要的）承包商	分包商	供货商
概念	×				
系统定义和应用条件	×				
风险分析	×		×		
系统需求	×	（×）			
系统需求分配	（×）		×		
设计和实现			×	（×）	
制造			×	×	×
安装			×	（×）	
系统确认	×	×	×	（×）	
系统验收	×	×			
运营和维修	×		（×）	（×）	
性能监控	×		（×）	（×）	
修改与更新	×		×	×	
停用及处置	×		（×）		

×＝全部责任并参与；

（×）＝特定的责任和/或部分参与（例如：分包商或备用要素的责任）。