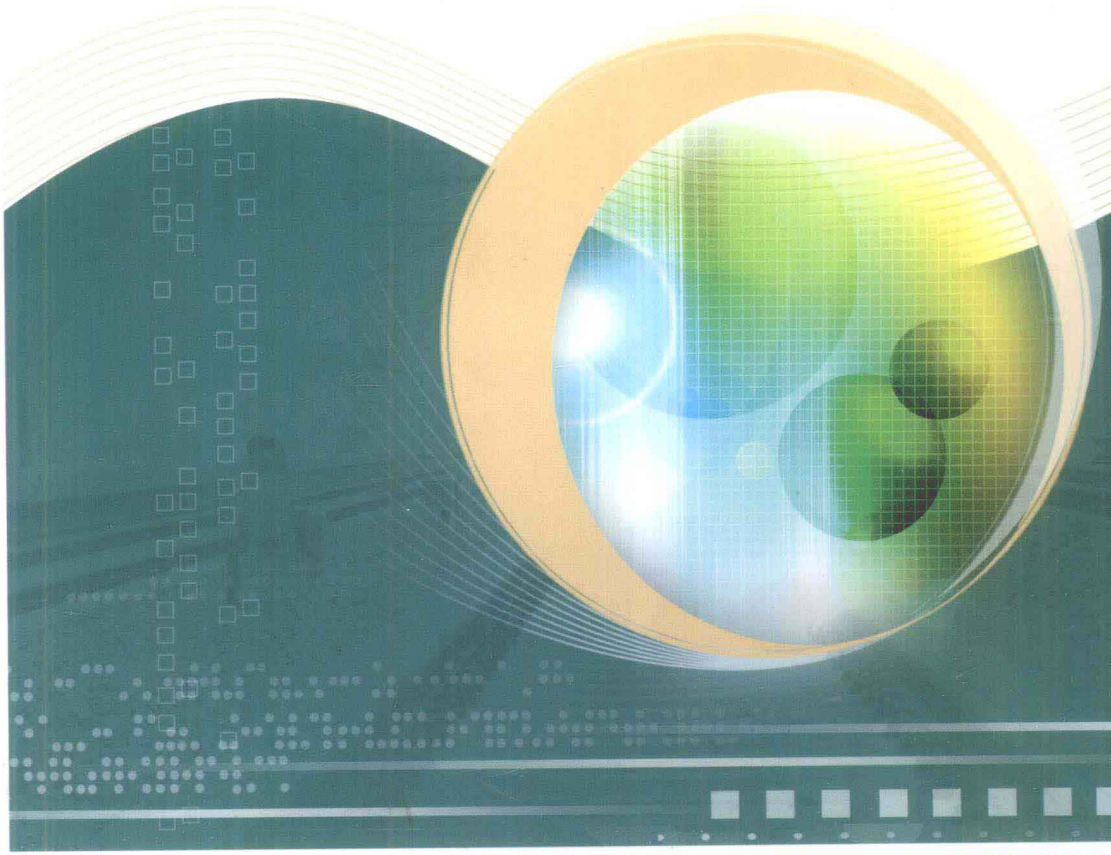
普通高等教育铁道部规划教材

铁路信号可靠性与安全性

程荫杭　主编　　穆建成　主审



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

普通高等教育铁道部规划教材

铁路信号可靠性与安全性

程荫杭　主　编
穆建成　主　审

中国铁道出版社
2010年·北　京

内 容 简 介

本书是普通高等教育铁道部规划教材。本书将可靠性、安全性联系在一起，注重铁路信号实际中的应用。本书共八章，主要介绍了可靠性理论、可靠性验证、安全管理和评估、可靠性分配和预计、可靠性和安全性分析、电子设备可靠性设计方法、故障—安全等内容。

本书可供铁道信号相关专业的本科生和研究生学习使用，也可供铁道信号工程技术人员学习和参考。

图书在版编目(CIP)数据

铁路信号可靠性与安全性/程荫杭主编．—北京：
中国铁道出版社，2010.2
ISBN 978-7-113-10858-8

Ⅰ.①铁… Ⅱ.①程… Ⅲ.①铁路信号-可靠性-高等学校-教材
②铁路信号-安全性-高等学校-教材 Ⅳ.①U284

中国版本图书馆 CIP 数据核字(2010)第 001481 号

书　　名：铁路信号可靠性与安全性
作　　者：程荫杭　主编

责任编辑：武亚雯　　**电话**：010 51873134　　**电子信箱**：zhumınjıe_0@163 com
编辑助理：朱敏洁
封面设计：崔丽芳
责任校对：张玉华
责任印制：陆　宁

出版发行：中国铁道出版社(100054，北京市宣武区右安门西街 8 号)
网　　址：http://www.tdpress.com
印　　刷：北京鑫正大印刷有限公司
版　　次：2010 年 3 月第 1 版　　2010 年 3 月第 1 次印刷
开　　本：787 mm×960 mm　1/16　**印张**：12　**字数**：251 千
印　　数：1～3 000 册
书　　号：ISBN 978-7-113-10858-8/TP・3697
定　　价：23.00 元

前　言

本书是普通高等教育铁道部规划教材，是由铁道部教材开发领导小组组织编写，并经铁道部相关业务部门审定，适用于高等院校铁路特色专业教学以及铁路专业技术人员使用。本书为铁道信号系列教材之一。

铁路信号是指示列车运行和调车作业的命令。保证命令正确和保证按命令执行，以保证列车运行和调车作业安全、提高运输效率的设备（系统）称为铁路信号设备（系统）。随着列车速度的提高、密度的加大和载重量的增加，铁路运输对铁路信号设备（系统）的依赖性也在不断增强，铁路信号在铁路运输中的作用越来越重要。而随着铁路信号系统功能的增加及复杂性程度的增大，铁路信号设备（系统）的可靠性和安全性问题倍受关注。

可靠性工程作为一门独立的工程学科，以 1957 年美国国防部电子设备可靠性咨询组 AGREE 发表研究报告为标志，至今已 50 余年。可靠性工程经历了形成、发展、成熟的过程。1965 年国际电工委员会（IEC）可靠性专业委员会的成立标志着国际可靠性标准化活动的开始。20 世纪 60 年代，我国在电子工业部门首先开始进行可靠性工程的工作。20 世纪 80 年代后我国颁布了一系列可靠性标准和管理规定，在武器装备的研制中全面地推行可靠性工程，并得到了迅速的发展，可靠性工程进入了规范化的轨道。1981 年 10 月中国铁道学会自动化委员会在南京召开了“铁路信号器材与可靠性学术会议”，会议宣读了有关继电器、电动转辙机等可靠性的论文，并专题讨论了铁路信号领域如何开展可靠性工作的问题。但是，由于铁路信号长期以来主要强调安全性，因此可靠性问题没有作为一个独立的问题明确出来。

在保证列车运行安全的前提下提高运输效率是铁路运输对铁路信号设备（系统）的要求，因此安全性对于铁路信号设备（系统）来说是第一位的。长期以来“故障—安全”原则作为铁路信号设备（系统）设计的原则，并依此原则对铁路信号设

备(系统)的安全性进行评估。随着微电子技术、计算机技术、通信技术、控制技术、网络技术在铁路信号设备(系统)中的应用,如何提高、保证和评估铁路信号设备安全性,特别是铁路信号系统的安全性成为摆在我国铁路信号工程技术人员面前的重要课题。

2003年我国铁路制定了中国列车运行控制系统CTCS(China Train Corltrol System)规范总则。为加快我国铁路列车运行控制系统的发展,制定了相关的技术规范和标准,在这些规范和标准中引用了国际上有关铁路的可靠性、可用性、维修性、安全性——RAMS(Reliability Availability Maintainability Safety)的标准,可靠性、安全性的问题更加引起我国铁路信号工程技术人员的关注。

近十年来,在铁路信号相关专业本科生的教学中,开设了可靠性基本理论、可靠性工程相关的课程,并编写了一些讲义,但并没有一本针对铁道信号专业本科生有关可靠性工程的教材。长期以来,在铁道信号专业本科生的教学中,"故障—安全"技术的内容分别被编写在各铁路信号专业课程的教材中,这已经不能适应铁路信号设备(系统)发展对安全性的要求。

可靠性问题研究的是如何减少故障的发生,安全性问题关心的是故障后果、研究的是如何防止故障发生后造成严重的后果和如何减少会造成严重后果的故障发生概率。可靠性和安全性既有联系又有区别。可靠性工程和安全性工程都是在同故障作斗争,它们在理论和方法上是相通的。因此,我们将可靠性和安全性放在一起,编写了本教材,以适应铁路信号发展和教学的需求。

可靠性工程与安全性工程是一门应用性很强的学科,它是人们在产品研制、生产、使用中总结出来的一般规律,它不是针对某一类产品的,但是有很强的实用性。读者学习中,在掌握基本概念和理论的基础上,要把握方法的实质和技术的核心,这样才能在铁路信号设备(系统)设计、生产、使用中应用这些理论、方法、技术,提高其可靠性、安全性;反过来通过实际的应用,才能加深对可靠性工程与安全性工程理论、方法、技术的理解和掌握。

本书与有关可靠性工程或安全性工程的书籍相比有两个特点:一是将可靠性和安全性联系在一起,突出了可靠性工程和安全性工程的共同点和不同点;二是突出了可靠性和安全性理论、方法、技术在铁路信号中的应用。

全书共八章,可划分为三部分内容。具体如下:

(1)第一部分(包括第一、二章)是可靠性、安全性的基本概念和理论。其中:

第一章分析了可靠性、安全性在铁路信号中的地位，介绍了可靠性、维修性、可用性、安全性、可靠性工程、安全性工程等基本概念；第二章介绍可靠性、维修性、可用性、安全性基本理论。

(2)第二部分(包括第三、四章)是可靠性的评估和验证、安全性管理和评估。其中：第三章介绍了可靠性数据收集、分析的目的和方法，可靠性验证的目的和方法，给出了铁路信号设备可靠性评估和验证的具体方法；第四章介绍了基于电气、电子器件和计算机的安全功能系统的安全性管理和评估。

(3)第三部分(包括第五、六、七、八章)是可靠性与安全性分析、设计方法和技术。其中：第五章介绍了可靠性分配和预计；第六章介绍了故障模式影响及危害性分析、故障树分析、事件树分析等可靠性和安全性(风险)分析方法，以铁路信号设备的示例介绍了分析方法的步骤；第七章介绍了元器件选择和控制、降额设计、冗余设计、环境设计和热设计等电子设备可靠性设计方法；第八章介绍了铁路信号"故障一安全"技术。

书名《铁路信号可靠性与安全性》中的"铁路信号"是泛指的"铁路信号设备(系统)"，本书中这两个术语没有严格区分，按照通用惯例使用。

本书可供铁道信号相关专业的本科生和研究生学习使用，也可供铁道信号工程技术人员学习和参考。

本书由北京交通大学程荫杭主编，铁道部科技司穆建成主审。其中程荫杭编写第一章、第三章、第八章第三节，赵林海编写第二章、第六章第一和第三节、第八章第一和第二节，燕飞编写第四章，刘中田编写第五章、第六章第二和第四节、第七章。

鉴于笔者水平，难免有不妥之处，欢迎读者指正。

编　者

2009 年 12 月

目　录

第一章
绪　论

第一节　可靠性、安全性在铁路信号中的地位

铁路运输是通过列车在钢轨线路上运行来完成的，为了保证列车运行安全（防止列车冲突、追尾、超速颠覆等事故的发生），列车必须根据行车命令运行。铁路信号就是指示列车运行和调车作业的命令。初期的铁路信号是由人骑马用手旗传递行车命令，随着列车速度的提高，进而采用音响、臂板、灯光显示信号，现在最常见的是地面的灯光显示、机车上的允许速度显示。为了保证列车运行安全、提高运输效率，作为列车运行的命令，一要保证给出的行车命令是正确的，防止人为的疏忽给出错误的行车命令；二要保证列车按照行车命令运行，防止司机误操作酿成行车事故；三要提高行车调度指挥的效率。而这些保证都是要通过各种设备、系统来实现的。保证给出的行车命令正确，保证列车按照行车命令运行和提高行车调度指挥效率的设备、系统，称之为铁路信号设备、系统。铁路信号的基础设备有信号机、道岔转换设备和线路占用检查设备等；按其功能划分铁路信号系统有区间闭塞（控制）系统、车站联锁（控制）系统、行（列）车调度指挥系统、列车运行控制系统、编组站调车控制系统和微机监测系统。

铁路信号的作用就是在保证列车运行安全的前提下提高运输效率。不断提高列车运行速度、列车运行密度和列车牵引重量是铁路运输发展的要求，而铁路运输的发展又对铁路信号不断提出新的要求。电子技术、计算机技术、通信技术、控制技术、网络技术等科学技术的发展为不断提高铁路信号的技术水平提供了有力的支撑。近十年来，我国铁路信号技术水平有了长足的发展，计算机联锁、分散自律式调度集中、列车运行控制系统、编组站综合自动化系统等已在我国推广和应用。随着铁路信号技术水平的不断提高，对铁路信号的要求也越来越高。如《既有线 CTCS-2 级列车运行控制系统技术规范（暂行）》要求“系统适应列车最高允许速度 250 km/h，正向运行时，动车组最小追踪间隔 5 min”。同时，随着列车速度的提高、密度的加大和载重量的增加，铁路运输对铁路信号的依赖性也在不断加大，也就是说铁路信号在铁路运输中的作用越来越重要。

铁路信号设备发生故障，系统将不能正常使用，会影响列车的正常运行，给铁路运输造成经济损失。以铁路部门统计的数据为例，2005 年 1～11 月，我国全国铁路共发生信

号故障(障碍)8 088 件,造成列车延误共 7 911 h 11 min,平均每次故障造成列车延误 59 min。

铁路信号的故障,不仅造成列车运行的延误,而且由于信号故障,失去了设备对列车运行安全的保障,列车运行安全要靠操作人员按照规章制度执行来保证,而一旦操作人员疏忽,违章作业,则可能酿成列车冲突、追尾、超速颠覆等重大事故,造成人员伤亡和重大经济损失。如 2006 年 4 月 11 日,由于铁路信号设备故障及维修人员处理不及时,而机车乘务员又违章作业,由青岛开往广州的 T159 次列车,行至京九线下行林水站至东水站间时,与武昌至汕头的 1017 次列车发生追尾,导致被撞列车 4 节车厢脱轨,2 名铁路职工当场死亡,18 名旅客受伤。具体原因是从 3 月 6 日到发生事故的 35 天当中,京九线下行林水站至东水站间 20679 号区间通过信号机共 6 次因轨道电路故障显示红灯,都未及时处理。事故当天,该通过信号机因轨道电路故障显示红灯,T159 次列车机车乘务员在开行过程中车站值班员通知 20679 号区间通过信号故障红灯,而 T159 次列车在通过该信号机时,刚好 1017 次列车占用该闭塞分区,而 T159 次机车乘务员的误认为是信号机故障显示红灯,并且违章没有按规定的 20 km/h 速度行驶,而以 48 km/h 的较快速度进入有车占用的闭塞分区,导致追尾事故。虽然事故最后的直接原因是机车乘务员违章操作,但铁路信号设备故障是事故的诱因。

铁路信号的故障,会造成列车运行的延误;或因铁路信号故障为诱因,使操作人员疏忽违章造成重大行车事故;更为严重的情况是,铁路信号故障后给出了错误的命令和操作。例如:本应该给出列车禁止运行的命令(信号机显示红灯),而由于铁路信号故障,错误地给出了允许列车运行的命令(信号机显示绿灯);本应该不允许给出道岔转动的操作,而由于铁路信号故障,给出道岔转动的操作;本应该给出列车减速的操作指令,而由于铁路信号故障,没有给出列车减速的操作指令。这些情况都会造成危及行车安全的后果,对于铁路信号设备或系统是绝对不允许这种情况存在的。也就是说,对于铁路信号设备或系统,绝对不允许其故障后会出现危及行车安全的后果,这就是铁路信号设备或系统设计时必须遵循的"故障—安全"原则。

铁路信号故障是可靠性问题,故障后的后果危及行车安全是安全性问题。铁路信号的作用和功能决定了可靠性和安全性在铁路信号中的重要性,而随着计算机技术、通信技术、网络技术在铁路信号中的应用,铁路信号功能的增加及系统复杂性程度的增大,铁路信号的可靠性和安全性问题越来越受到重视。

第二节　可靠性、可用性、维修性和安全性

可靠性的概念可以说在人类开始使用工具的同时就存在了,但是可靠性作为一门独立的学科,是 20 世纪 50 年代才确立的。1957 年 6 月美国国防部电子设备可靠性咨询组,简称

AGREE(Advisory Group on Reliability of Electronic Equipment)发表了《军用电子设备可靠性》的研究报告,该报告阐述了可靠性设计、试验及管理的程序和方法。该报告中把可靠度定义为"在规定的时间和规定的条件下,无故障完成规定功能的概率",将抽象的可靠性概念进行了定量的描述,从而确定了可靠性在科学中的位置。

作为一门学科,可靠性有明确的定义。在美国军用手册《MIL-HADB-338B(1998.10):DEPARTMENT OF DEFENSE HANDBOOK - ELECTRONIC RELIABILITY DESIGN》"电子设备可靠性设计手册"中 reliability 定义为:(1)The duration or probability of failure-free performance under stated conditions (2)The probability that an item can be perform its intended function for a specified interval under stated conditions. (For non-redundant items this is equivalent to definition (1). For redundant items this is equivalent to mission reliability.)

在欧洲标准 EN 50126《Railway applications-The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)》"铁路设备:可靠性、可用性、维修性和安全性(RAMS)的规范和说明"中 reliability 定义为:the probability that an item can perform a required function under given conditions and given time interval(t_1, t_2)(IEC60050(191)).

我国军用标准 GIB 451A—2005《可靠性维修性保障性术语》中,可靠性定义为:产品在规定的条件下和规定的时间内,完成规定功能的能力。可靠性的概率度量也称可靠度。

什么是可靠性呢?可靠性是产品所具有的功能反映到时间上的特性,反映了产品无故障持续时间的长短。可靠性具有两个特点:一是它是产品固有的特性,一旦产品设计并生产出来,那么它的可靠性也就被决定了;二是它与产品所处的环境条件密切相关。可靠性的特点说明产品的可靠性既与设计生产有关,又与使用有关。但是,我们必须清楚,产品的可靠性最终还是由产品的设计和生产决定的,因为产品生产的目的是使用,因此在设计产品时,必须充分了解并考虑产品使用的条件。同时,在选择产品时,必须充分考虑产品规定的使用条件,是否满足实际的应用条件。

产品按故障后能否修复并重复使用,可分为可修复产品和不修复产品。产品属于可修复产品还是属于不修复产品,主要取决于修复的可能性和修复的成本。

对于可修复的产品,人们总是希望产品故障后能尽快修复,这就涉及产品的维修性。因为绝大多数产品都是长期使用,并且故障修复后继续使用,因此维修性问题在研究可靠性的过程中受到人们的重视。

维修性同样有明确的定义。在《MIL-HADB-338B》中 maintainability 定义为:The relative ease and economy of time and resources with which an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of mainte-

nance and repair. Also, the probability that an item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

在 EN50126 中 maintainability 定义为：The probability that a given active maintenance action, for an item under given conditions of can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources(IEC60050(191)).

我国军用标准 GIB 451A—2005 中，维修性定义为：产品在规定的条件下和规定的时间内，按规定的程序和方法进行维修时，保持或恢复到规定状态的能力。维修性的概率度量也称维修度。

维修(maintenance)是为使产品保持或恢复到能执行规定的功能状态所进行的技术和管理，包括监督的活动。维修包括维护(servicing)、预防性维修(preventive maintenance)修复性维修(corrective maintenance)等类型。

维护是为使产品保持规定状态所采取的措施，如润滑、加燃料、加油、清洁等。维护也叫“保养”，有的人把维护作为一种预防性维修。

预防性维修是为降低产品故障的概率或防止功能退化，使其保持能执行规定的功能的状态，按预定时间间隔或按规定准则所采取的措施。它可以包括调整、润滑、检查和必要的修理等。

修复性维修是产品故障后为使产品恢复到规定的状态所采取的措施。它可以包括故障定位、故障隔离、分解、更换、再装、调准和检查等。

维修性是产品保持或恢复所具有的功能反映到时间和所需资源上的特性，反映了产品为保持或恢复其功能所需时间的长短和所需资源的多少(资源包括人力、财力和物力)。维修工作是由人进行的，维修时间的长短与维修人员的技术水平、精神状态密切相关。但是必须明确，产品的维修性同产品的可靠性一样，是产品固有的特性，产品的维修性是由产品的设计和生产决定的。在产品设计时，必须考虑产品的维修性。

可用性可以说是广义的可靠性，它既和产品的可靠性有关，又和产品的维修性有关。

可用性也有明确的定义。在《MIL-HADB-338B》中 availability 定义为：A measure of the degree to which an item is in an operable and committable state at start of mission is called for at an unknown (random) time. (item state at start of a mission includes the combined effects of the readiness -related system R & M parameters , but excludes time.)

在 EN50126 中 availability 定义为：The ability of product to be the in a state to perform a required function under given conditions at a given instant of time or over time interval assuming that the required external resources are provided.

我国军用标准 GIB 451A—2005 中，可用性定义为：产品在任一随机时刻需要和开始执行任务时，处于可工作或可使用状态的程度。可用性的概率度量称为可用度。

可用性是产品处于工作状态或可工作状态的能力，是产品可靠性和维修性的综合反映。

安全性涉及的范围很广，本书主要涉及设备和系统的安全性。

安全性也有明确地定义。在 EN50126 中，safety 定义为：freedom from unacceptable risk of harm.

在 GB/T 6583—94，ISO 8402—94《质量管理和质量保证术语》中，安全定义为：将伤害（对人）或损坏的风险降低到可接受水平的状态。

我国军用标准 GIB 1405—92《质量管理术语》中，安全性定义为：不导致人员伤亡，不危害健康及环境，不给设备或财产造成破坏或损伤的能力。

对系统而言，影响安全性的因素包括：设备故障、运行模式和人为因素。

单纯从设备角度而言，安全性也可以看作是一种有特殊要求的可靠性，即将产品故障造成的伤害和损失的风险限制在可接受的水平的能力。

第三节 可靠性工程和安全性工程

一、可靠性工程

研究可靠性的目的是要减少产品使用中的故障，提高产品的可靠性。可靠性工程是为了达到产品可靠性要求而进行的一套设计、研制、生产和试验工作。它与产品整个寿命周期的全部可靠性活动有关。从方案论证开始到产品报废为止的整个生命周期内，都要有计划的开展一系列的可靠性工作。整个寿命周期可以分为企划、设计、生产、验证、使用和维修等阶段。对于可靠性来说，最关键的阶段是设计阶段，是设计阶段所进行的可靠性工作。

可靠性要求是产品使用方从可靠性角度向承制方（或生产方）提出的研制目标，是进行可靠性设计分析、制造、试验和验收的依据，研制人员只有在透彻了解这些要求后才能在产品的设计生产过程中充分考虑可靠性问题，并按要求有计划地实施有关组织、监督、控制及验证工作。

可靠性要求可分为定量要求和定性要求。定量要求是规定产品的可靠性参数、指标和相应的验证方法，用定量方法进行设计分析、可靠性验证，从而保证产品的可靠性。定性要求是用一种非量化的形式设计、评价和保证产品的可靠性。

1. 可靠性定量要求

可靠性定量要求是确定产品的可靠性参数、指标以及验证时机和验证方法，以便在设计、生产、试验验证、使用过程中用量化的方法评价或验证产品的可靠性。

可靠性要求分为基本可靠性要求和任务可靠性要求。

任务可靠性——产品完成其规定功能的能力。

我们通常讲的产品可靠性一般指的是任务可靠性。在进行可靠性数据分析时，只统计影响产品功能的故障。

基本可靠性——产品无故障工作的能力。

采用冗余结构时，产品发生故障并没有影响产品功能的完成，但必须进行维修或更换，增加了维修的人力和备品备件的要求，在产品的实际应用中是必须考虑的。在进行可靠性数据分析时，不管是影响产品功能的故障，还是没有影响产品功能的故障，只要是故障都统计在内。

对于没有冗余结构的产品，其任务可靠性和基本可靠性的概念是相同的。

可靠性定量要求的应包括以下内容：

①可靠性参数和指标；

②环境和使用条件；

③故障判据；

④验证方法。

依产品的不同可选择不同的可靠性参数，如平均故障间隔时间（MTBF），可靠度$R(t)$等。

可靠性指标应根据产品的类型在制定合同和研制任务时提出规定值和最低可接受值，也可以只提最低可接受值。在确定可靠性指标时，一个重要的因素是可靠性指标在实际需要的期限内是可以实现的，还要与当前的设计技术水平相适应。否则，该可靠性指标要么是无法实现，要么实现起来要耗费大量的时间和金钱。

环境和使用条件会影响产品故障的概率，应以标准术语规定产品所处的使用环境和条件。

故障判据是判断故障的依据，应根据设备或系统的功能和性能参数明确故障判据，这些参数还必须采用在验证测试时可以测量的术语表示，以避免故障定义的主观解释。

验证方法是可靠性定量要求的重要内容，如果不明确验证方法或无法验证则失去了定量要求的意义。可靠性验证可采用试验验证和使用验证，应规定接收和拒收的判据。对于试验验证应规定试验条件、试验持续时间以及谁进行、何时进行、在哪进行试验等。

2. 可靠性定性要求

在定量化设计分析缺乏大量数据支持的情况下，产品的可靠性要求难于规定定量指标、验证方法时，提出定性的可靠性要求和验收准则就更为重要。可靠性定性要求一般可分为定性设计要求和定性分析要求。

可靠性定性设计要求一般是在产品研制过程中要求采取的可靠性设计措施，以保证提高产品可靠性。这些要求都是概要性的设计措施，在具体实施时，需要根据产品的实际情况而细

化。主要的定性设计要求见表1－1。

表1－1 可靠性定性设计要求项目表

序号	要求项目	目 的
1	制定和贯彻可靠性设计准则	将可靠性要求和使用中的边界条件转换为设计边界条件。给设计人员规定专门的技术要求和设计原则，以提高产品的可靠性
2	简化设计	减少产品的复杂性，提高其基本可靠性
3	冗余设计	用多于一种的途径完成规定的功能，以提高产品的任务可靠性和安全性
4	降额设计	降低元器件、零部件的故障率，提高产品的基本可靠性、任务可靠性和安全性
5	制定和实施元器件大纲	对元器件、零部件进行控制与管理、提高产品可靠性、降低保障费用
6	确定关键件和重要件	把有限的资源用于提高关键产品的可靠性
7	环境防护设计	选择能低消环境作用或影响的方案和材料，或提出一些改变环境的方案，或把环境应力控制在可接受的极限范围内
8	热设计	通过元器件筛选、电路设计、结构设计、布局来减少温度对产品可靠性的影响，使产品在较宽的温度范围内可靠的工作
9	软件可靠性设计	通过贯彻执行软件工程规范来提高软件的可靠性
10	包装、装卸、运输、储存等设计	通过对产品在包装、装卸、运输、储存期间性能变化的分析，确定应采取的保护措施以提高其可靠性

可靠性定性分析要求一般是在产品研制过程中要采取的可靠性分析工作，以保证提高产品的可靠性。这些可靠性分析工作要在产品研制的各个阶段根据产品的实际情况和分析方法的特点，具体组织实施。主要的定性分析要求见表1－2。

表1－2 可靠性定性分析要求项目表

序号	分析项目名称	分析方法特点	目 的
1	功能危险分析（FHA）	综合的、系统的演绎方法	检查系统功能故障，确定设计方案和可行性，发现设计中潜在的问题，提出改进措施
2	故障模式影响分析（FMEA）	系统的、自下而上的归纳分析法	分析产品各组单元的故障模式及其对产品功能的影响，确定其严酷程度，发现设计中的薄弱环节，提出改进措施
3	故障树分析（FTA）	系统的、自上而下的演绎分析法	分析造成产品某种故障状态（或事件）的各种因素，确定故障原因或原因的组合，发现设计中的薄弱环节，提出改进措施
4	事件树分析（ETA）	系统的演绎方法	分析一个给定的初因事件可能导致的各种事件序列结果的逻辑演绎方法

可靠性工程的目的是要尽可能防止可预知故障的发生，将不可预知的故障减少到最低的程度，使故障造成的损失最小。其实质就是同故障作斗争。就是发现故障、分析原因，进行改进，防止同样的故障发生。

可靠性数据即故障数据是可靠性工程的基础，没有可靠性数据，可靠性工程就成了无源之水。可靠性数据存在于可靠性试验、功能试验等试验中，即试验中出现的故障及其分析；对于大量长期使用的产品而言，可靠性数据大量存在于使用现场，即产品在现场使用中的故障及其分析。可靠性数据的收集与分析需要有计划有组织的管理，才能保证数据收集的完整性、准确性和分析工作的有效性。

可靠性设计和分析的目的就是挖掘和确定产品潜在的故障隐患和薄弱环节，通过设计预防和设计改进，有效地消除隐患和薄弱环节。可靠性设计和分析工作同样需要有计划有组织的管理，才能保证可靠性设计和分析的有效实施。

可以说可靠性工程中可靠性设计、可靠性试验、可靠性管理是最重要的工作。

二、安全性工程

安全性问题研究的目的是减少事故发生的概率和降低事故危害的程度。安全性用危险可能性和危险严重性，即风险来评价。安全性工程一般是针对系统而言，称为系统安全工程，即在系统的寿命周期的所有阶段，应用工程和管理的原则、准则和技术，以识别和消除危险、并降低风险，使系统获得最优的安全性。

系统的寿命周期包括：概念和定义阶段、设计和研制阶段、生产阶段、安装阶段、运行和维修阶段、处理阶段。

在概念和定义阶段，应制定安全性大纲。安全性大纲是包括安全性管理和系统安全性工程工作的文件，其目的是在系统寿命周期内，用及时、经济、有效的方法满足系统安全性要求。订购方应向承制方提出安全性大纲要求，包括：安全性定性、定量要求，试验项目要求和基本的工作项目要求，这些要求应纳入合同或任务书。承制方应根据合同要求，制定和实施安全性大纲，在制定安全性大纲时，一开始就与可靠性、维修性、人因工程等工作进行权衡和协商，以达到最佳的费用效益比。

系统安全性工作计划是实施安全性大纲最基本的文件，通常是承制方必须做的一项工作。为实现安全性大钢目标，承制方要通过计划来组织、指挥、协调、检查、监督和控制安全性的全部工作。

承制方制定系统安全性工作计划的作用是：有利于管理和实施安全性大纲；反映承制方在研制工作中对安全性工作重视的程度；便于订购方评价承制方为实施和控制安全性工作所规定的各项程序。

系统安全性工作计划包括：安全性工作项目（包括内容、要求、完成形式及检查）；安全性工作组织、人员及其资格与职责；安全性工作进度表；安全性评审点；安全性工作计划与其他如可靠性、维修性工作计划等的协调；安全性信息的管理及使用要求（包括提交的资料格式、内容与交付日期等）；安全培训等。

表 1—3 是根据 GJB 900—90《系统安全性通用大纲》列出的系统安全性工作项目。

表 1－3 概括了系统安全性工作的内容，包括：管理与控制、设计与分析、验证与评价、安全性培训和软件系统安全。

表 1－3 系统安全性工作项目

项目编号	工作项目	类型	项目编号	工作项目	类型
101	制定系统安全性工作计划	管理	208	订购方提供的设备和设施的安全性分析	工程
102	对转承制方的安全性综合管理	管理	301	安全性验证	工程
103	安全性大纲评审	管理	302	安全性评价	管理
104	对系统安全工作组的保障	管理	303	安全性符合有关规定的评价	管理
105	建立危险报告，分析、纠正措施跟踪系统	管理	401	系统安全性主管负责人的资格	管理
106	试验的安全性	管理	402	培训	管理
107	系统安全性进展报告	管理	501	软件需求危险性分析	工程
201	初步危险表	工程	502	概要设计危险分析	工程
202	初步危险分析	工程	503	详细设计危险分析	工程
203	分系统危险分析	工程	504	软件编程危险分析	工程
204	系统危险分析	工程	505	软件安全性测试	工程
205	使用和保障危险分析	工程	506	软件与用户接口分析	工程
206	职业健康危险分析	工程	507	软件更改危险分析	工程
207	工程更改建议的安全性评审	管理			

注：表中的项目编号引用自 GJB 900—90 中项目编号。

工作项目 103 安全性大纲评审是对系统研制工作从一个阶段转入另一个阶段的重要决策手段，大纲评审实际上包括两种性质的评审：①安全设计评审，主要评审安全性设计的可行性，以及系统的安全性是否达到合同规定的要求。②安全性工作评审，主要评审安全性工作项目的进展情况和关键问题。

工作项目 201～208 是安全性设计分析工作，承制方应尽早提出初步危险表，订购方可根据其结果决定后续危险分析（初步危险分析、分系统危险分析等）的范围。

工作项目 301 是安全性验证，对于合同文件中规定的安全性要求，许多需要通过分析、检查、演示或试验来验证。对研制中发现的危险，如果用分析或检查无法确定所采取的措施能否有效时，则应进行安全性试验以评价采取措施的有效性。

工作项目 302 是安全性评价，安全性评价的重要性在于使用户或试验人员了解所有不安全的设计或操作特性，安全评价应尽量进行残余风险的定量评价以确定控制措施、禁止事项或安全规程。

安全性工程和可靠性工程在理论和方法上是相通的。在定量分析中运用概率论和数理统