TIELU XINHAO
KEKAOXING ANQUANXING
LILUN JI ZHENGSHI

铁路信号可靠性安全性理论及证实

■ 编著　郦　萌　吴芳美
■ 审　　穆建成

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

铁路科技图书出版基金资助出版

铁路信号可靠性安全性理论及证实

郦　萌　吴芳美　编著
穆建成　　主审

中国铁道出版社
2008年·北京

内容简介

本书系统地介绍了与安全性相关的控制系统中可靠性和安全性的理论、技术以及证实、测试和评价等内容。

全书共分七章，除了可靠性和安全性的基本概念及它们的相互关系外，本书也涉及到了安全性的人文和社会属性，介绍了人因差错的起因和分类，讨论了社会对于安全性的可承受性。内容还包括可靠性、安全性论述所需的数理工具；可靠性、可维修性、可用性以及安全性的量化特征；可靠性和安全性技术与工程；安全信息传输技术；安全性证实及安全性相关产品的验收及安全性分析和安全性管理等。

本书的多数内容具有跨行业的普遍性。由于结合了铁路安全控制的背景，对从事铁路信号领域工作的工程和维护管理人员有较强的针对性，同时对从事铁路运输管理、机车车辆、工务工程工作，以及其他安全性相关领域的人员来说阅读本书也必定会有所裨益。

本书也可作为高等学校“交通信息工程与控制”、“安全性技术及工程”和“计算机应用技术”博士、硕士学位点的教学参考书。

图书在版编目(CIP)数据

铁路信号可靠性安全性理论及证实/郦萌，吴芳美编著．—北京：中国铁道出版社，2008.5

ISBN 978-7-113-07884-3

Ⅰ.铁… Ⅱ.①郦… ②吴… Ⅲ.①铁路信号-可靠性-研究 ②铁路信号-安全性-研究 Ⅳ.U284

中国版本图书馆 CIP 数据核字(2008)第 068599 号

书　　名：铁路信号可靠性安全性理论及证实

作　　者：郦　萌　吴芳美

策划编辑：魏京燕

责任编辑：魏京燕　崔忠文

电　　话：(010)51873115　　**电子信箱**：dianwu@vip.sina.com

封面设计：崔丽芳

责任印制：李佳

出版发行：中国铁道出版社(北京宣武区右安门西街 8 号　邮政编码：100054)

印　　刷：北京市彩桥印刷有限责任公司

版　　次：2008 年 6 月第 1 版　2008 年 6 月第 1 次印刷

开　　本：787 mm×960 mm　1/16　印张：17.5　字数：430 千

书　　号：ISBN 978-7-113-07884-3/TP·2307

定　　价：38.50 元

前　言

“可靠性”和“安全性”作为“关键词”在公众媒体上的出现越来越频繁，这是因为许多新的科学技术成果迅速被应用并伸展到了人类生活的深层，这些技术本身的可靠和应用上的安全直接影响到社会和每个人的生活。

这是一本向从事铁路信号及安全控制工程师和管理人员专门介绍可靠性和安全性知识的书籍。随着科学技术的发展，信息化和自动化的许多新技术被引入到铁路的运输管理、机车车辆、工务工程的安全防护控制系统中。虽然，依据铁路内部的职责分工，这些系统不属于铁路信号，但是保证安全运输的目标是一致的，可利用的手段和资源也是相近的。因此，阅读本书也必定会有所裨益。安全问题为整个社会所关注，不同领域的安全性技术也存在共性，所以即使是铁路行业以外的人员，只要是从事安全性技术或安全性管理的从业人员，相信也会从阅读本书中得到启发。

铁路自问世以来就极其重视安全，“没有安全就没有效率”。从这个传统意义来说，“安全性”是第一位的，但低效率下的安全性并不是社会进步和技术发展所期望的。由于计算机技术大举进入铁路各类安全防护和控制系统，使得可靠性和安全性两个原本被认为相制约的需求越来越显示出其相辅相成的一面。

可靠性和安全性两者之间的复杂和微妙关系并不是三言两语就能解释清楚的。有一种看法是安全性就是可靠性，这是忽略了两者在一定资源约束条件下的相互对立；也有人认为可靠性和安全性两者对立而不可调和，这是没有认识到安全防护系统如果本身不可靠也就谈不上安全，两者存在的“同一性”。对于许多安全防护与控制工程师来说，全面地、完整地、辨证地认识可靠性和安全性，对做好我们的工作是至关重要的。作者从长期的教学、科研经历中感到，由于近年来的技术发展，写一本新的、剖析可靠性和安全性关系，以及有关安全性证实、评价和测试方面的书是有价值的。

一方面，可靠性和安全性都是来源于生产实践和社会实践的命题，离开了实际背景，命题就变得没有意义；另一方面，可靠性和安全性涉及许多相关的学科知识，大而言之，至少与三方面学科相关——工程学、数学和社会学。更细一点还牵涉到心理学、生理学等等。现代关于社会问题、心理问题的研究都十分推崇数学建模，加之可靠性和安全性是“不可靠”或“不安全”事件发生之前的属性，不能简单测度，无论是通过认证、评估，还是测试、试验给出的可靠性和安全性评价，都是一种“预测”。因此，离不开像数理统计中的“统计推断”、“假设检验”之类数学工具。学科交叉为我们认识世界提供了新的空间，但是由于学科着眼点的不同，对事物认识会产生差异，工程师、管理者们追求的是问题

的实际解决，数学家们企望的是理论上的完备和表达上的优雅。在工程问题、社会问题模型化的时候，一些重要的细节被忽略是难免的。而当一个“普遍性”的数学模型被我们引用并返回到特定的工程应用时，如果忽视了建模过程中被简化了的条件而直接使用它的结果，根据这个结果得出的结论就可能缺失了某些指导实际问题的要素。

有一点工程经验的人都明白，在着手修复一个系统之初，必须花费一定的时间进行故障分析、定位和替换品的准备，然后才实施修理。因此，单位时间（如一小时）内修复的可能性——“修复率”应该是此前修理所经历时间的函数。在开始修理后的第一个小时，可能还在进行维修的准备工作，修复率应该较低。经过若干准备时间以后的“某一小时”中，被修复的可能性就较大，修复率应该较高，这是符合常理的。但是，我们仍然会不时见到将修复率假设为常数的论述（包括本书也不能避免）。在现实中，唯有那种“不分析故障、不作故障定位、不准备替换品，只用‘踢它一脚！’来修电视机”的修理方式，才比较符合修复率为常数的假设条件。将修复率假设为常数的唯一好处是对模型进行数学处理比较方便，可获得一个结构上比较规则的公式和从感性上对修复过程比较易于理解。如果我们不清楚这里的“奥妙”，真的把修理初期很低的修复概率估计为很高，最终得到的可维修度和可用度结果就非常“不安全（或说过于盲目乐观）”。只有我们比较深入地了解现实的要求和理想模型之间的区别，才能更好地利用数学领域里的成果来解决现实中希望解决的工程问题。

另一方面，随着我国市场经济的发育和完善，以及工业产品向国外市场的开拓，对产品质量必须有更科学的描述，安全性量化描述是一个不可回避的问题。因此，本书增加了验收与认证等有关的知识。

作为安全性的一个重要方面，人因差错诱发的可靠性和安全性问题也必须引起关注。本书为人因差错的分析和归类提供了一定的篇幅。这对于铁路运输的危害防范以及加强安全性管理应该有某些帮助。

虽然本书立意于可靠性和安全性知识的系统介绍，但内容上侧重于一些新概念的说明、引申和辨析。另外提供一个 按字母顺序排列的“英汉术语对照和索引”便于读者查阅。需要说明的是，本书在术语的使用上并不完全统一，诸如失效和故障、单元和成分之类。这是因为有些术语的形成和使用存在历史、行业等的不同背景，完全统一不仅困难，也会引出一些误解。因此随讨论的问题而定再补充做一些说明，本书尽量选择符合该术语原义的中文表达。

本书不是某些标准、规范和规章的解释性的书。如果在书中涉及一些具体的标准、规范和规章，它们仅仅是用来作为有利于说明概念的例子。书中的内容更不作为处理安全性问题的依据。

本书蒙铁路科技图书出版基金支持，谨此表示感谢。

作　者

2008 年 5 月

目　录

第一章　可靠性和安全性概念

第一节　对象——系统和设备

可靠性和安全性针对的都是工程上的问题，具体来说就是面向设备或系统而言的。

设备是指生产或生活上所需要的各种器械、用品。小到家庭中的豆浆机、洗衣机，大到一座炼钢炉都可以说是设备。设备能够完整地实现生产或生活上的某些特定的功能。设备由若干部件搭建而成，每个部件担当设备运行所必需的部分任务。如洗衣机中的电源部件、动力部件、变速部件等，都是实现洗衣功能所不可缺少的。

对一个企业来说，设备管理是企业管理的一项重要内容，设备往往是资产管理的基本单位。为加强和完善资产管理，通常每项设备都要建立自己的编号，有自己的历史档案。所以设备是一个独立存在的单元。

系统是指由若干相互关联、相互制约和相互作用的一些成分（也称为要素或单元）组成的具有特定功能的有机整体。英文中系统（system）一词来源于古希腊文 systēma，意思是由各成分组成的整体。系统具有整体性、结构性、层次性、历史性等特征。

整体性是系统最基本的特性。在一个系统中，系统整体的特性和功能在原则上不能归结为各成分特性和功能的总和。处在系统整体中组成成分的功能和特性，也异于它们处在孤立状态时的功能和特性。系统的组成成分是系统存在的基础，没有成分就没有系统。成分和成分之间既相互独立，又相互联系。各组成成分在系统中的地位、作用有差异，有的成分处于主导地位或支配地位，而有的成分只处于从属或被支配的地位。

结构性指系统中的组成成分必须按照一定的关系加以搭建，这种关系能够充分体现成分间的相互关联、相互制约和相互作用。

层次性反映的是系统和成分之间的辩证关系。一个系统在另一种环境条件下，它可能只是一个更高一层次系统的一个组成成分。而在一个系统中的组成成分，在低于它的环境中，或许就是一个系统。

系统有许多分类方法。按照系统的物质性可分为：实物系统和观念系统。按照形成原因可分为：自然系统和人工系统。另外还有物理系统和非物理系统（如社会系统和经济系统）；动态系统和静态系统；封闭系统和开放系统；线性系统和非线性系统；确定系统和不确定系统（如随机系统或模糊系统）；简单系统和巨系统等等划分方法。

设备由部件搭建，系统由成分（要素）组成，那么设备和系统在内涵上是否是完全

等价的呢？不是。

一项设备是否也可以称其为系统，主要根据它是否具有系统的所有特性来衡量。

一个系统的功能能否由一项设备来实现，主要根据系统各特征所体现的关系是否能用物理的方法来体现，以及系统本身能不能通过实物化的部件来搭建。

按照上述的系统分类，首先，设备不可能是自然系统，也不可能是观念系统或非物理系统。第二，同时具有简单、确定和静态系统属性的系统应该很容易通过实物化来加以实现，实物化的系统称其为设备可能更加妥当。第三，动态、开放、非线性、不确定或复杂的系统即使当它完全由实物化方法实现后，称其为系统或称其为设备都可以，但是，系统更偏于表述抽象的概念，而设备更着眼于具体实物，所以，可视待考察的问题而定称谓。

大多数铁路信号设备都由许多部件组成，一项设备是不是也可称其为系统并没有成文的规定。但是，应该说有一些是约定俗成的，如铁路编组站综合自动化系统、列车自动运行系统、运输信息系统等，很少被称为设备。相反，道岔转辙装置、轨道电路或计轴装置则很少被称为系统。这并不是说规模大的一定是系统，规模小的则是设备。设备和系统不是一种纯粹按规模的划分，而是要从系统应具有的特征来进行考察。同样是道岔转辙装置，在考察其功能时，转辙机的所有零件、锁闭部件以及控制电路的所有器件可视为各自功能的一种叠加。而当我们把考察问题的角度加以变换时，比如当我们要考察和分析道岔转辙装置的可靠性时，其各组成成分的可靠性除了作用、影响、制约整体的可靠性外，还相互影响和相互制约，符合系统的基本特征，这时就应该将道岔转辙装置作为一个系统来对待。

由于现在计算机大量被用于工业和交通领域，在考察铁路信号的问题时，有两点需要留意：一是计算机软件本身是一个逻辑系统，属于观念系统而不是实物系统。因此，只有当软件通过固化，或确认它的功能不能游离于它所搭载的宿主（host，也称主机）而直接对外发生作用时，才能将其看成设备的一个组成成分；二是有人参与工作的系统，人不是设备的组成成分，但人往往是系统的组成成分。

在铁路运输这个大系统中，包含许多和安全性相关的子系统，其中有一些并不是像具体信号设备那样的实物系统，但它们具有系统的属性，如安全管理的规章、制度等（制度和系统在英文中也是同一个词 system）。和其他系统一样，规章制度也有策划、设计（制订）、运行（实行）、维护（修订）直至报废（废止）这样的生命周期。因此，它们和其他系统或产品一样，需要遵循系统工程的某些规则。

在可靠性、安全性定义中经常将考查的对象表述为“产品”。产品是指通过设计、制造向社会提供的一种商品，它一般是元件、部件或设备、实物化的系统及固化在介质中的软件等。但是，当前很多服务项目也被称为产品，产品的概念就扩充了。

在本书中，使用设备、系统等概念时，基本遵循上述原则。但为了顾及所参考的文献，保持和它们尽可能的一致，在不会造成误解的前提下，有时也采取灵活的做法。

第二节 可 靠 性

1. 可靠和可靠性

所谓“可靠(reliable)”是作为“主体”的“我”对环境中“客体”——他人和他物的一种认识。这里的人不是所有的人,而只是那些你所倚仗的人。这里的物也不是所有的物,而是那些为你所用并试图借此实现某种意图(通俗地说“办成事”)的物,通常指装置、工具、材料或武器等。

我们常说某人“可靠”,通常指这个人“认真负责、恪守诚信”。相信依靠这个人能够把事办成,反过来“成事不足,败事有余”则用来形容一些“不可靠”的人。说某一个工具“可靠”,指其“用有实效而且坚固耐久”,常常能达到你所期望的要求。因此,不论客体为人或为物,能不能成功实现你的意图是衡量其“可靠”或“不可靠”的标准。

归结起来,“可靠”就是为实现某项使命对所仰仗的人或物给予信任程度所使用的一种评价。

问题在于“可靠与否”不是在“事成”或“事败”以后的“事后诸葛亮”,而是事前的推断。现实生活中,“能人”会“偶尔失手”,“瞎猫”会“碰上死耗子”,因此,事前推断的可靠与不可靠并不是绝对真实的。也就是说,在“绝对的可靠”与“绝对的不可靠”之间应该还有关于不同可靠程度的表达,例如“非常可靠”、“很可靠”、“可靠”、“不甚可靠”、“不可靠”、“很不可靠”这些分等级地描述关于可靠与否的性质。如果用“0”表示“绝对不可靠”,用“1”表示“绝对可靠”,那么,在0和1之间的自然数,例如0.75、0.999等可以用来连续地表达可靠的程度。

对可靠与否作为属性的系统性评价就是可靠性(reliability),对可靠性定量化度量称为可靠度。用可靠度这个“标尺”就能衡量各种为提高可靠性而采取技术措施的有效性。

所有为提高可靠性、评价可靠性而形成的理论、方法、技术等均纳入“可靠性工程学(reliability engineering)”范畴。可靠性工程学是一门起源于战争的学科。第二次世界大战中,纳粹德国开始用最原始的导弹袭击英伦三岛,但是很多导弹在飞行的途中失灵。“到底要施放多少枚导弹才有可能命中一个预定的目标”以及“每枚导弹的组成部件必须达到怎样的质量水平才能实现这个目标”等问题成为亟待研究的要点,但是这些问题还没有来得及解决,纳粹德国就瓦解了。不过,已经形成了“导弹正常飞行的成功概率可以用组成部件各自完好概率的乘积来加以估计”的概念,它是关于可靠性工程最早期的“成果”。在地球的另一边,忙于太平洋战争的美国人正在为军用通信器件的高故障率而发愁,由于这些产自美国本土的电子设备,先要运到不会被日本海军攻击的南太平洋某地储存,然后才被装上军舰,在北太平洋舰船及岛屿上使用,由于要两次

穿越炎热、潮湿的赤道海洋，设备故障频繁，促使了围绕可靠性问题的各种研究。而系统地开展可靠性研究，特别是电子产品可靠性的研究和成果的取得，已经是朝鲜战争开始以后了。

可靠性技术的发展大致分为四个阶段。

（1）调查研究阶段（1950—1957 年）：主要对以电子管为重点的电子元件、器件进行现场数据收集和分析；研究寿命试验方法并成立专门的可靠性组织。美国国防部电子设备可靠性顾问组 AGREE（advisory group on reliability of electronic equipment）在 1957 年公布关于电子器件可靠性规格的报告，奠定了可靠性工程的基础。

（2）统计试验阶段（1957—1962 年）：主要研制环境与可靠性试验设备；开展产品统计抽样寿命试验；制定电子产品可靠性标准和可靠性组织、管理规范；建立可靠性数据收集和交换系统。

（3）可靠性物理研究阶段（1962—1968 年）：主要分析元、器件失效机理；加强可靠性设计与工艺研究，建立高可靠元、器件生产线；研究加速寿命试验的方法。

（4）可靠性保证阶段（1968— ）：这个阶段的特点是建立保证产品可靠性的管理制度，形成质量保证体系；建立电子元、器件可靠性认证制度；发展可靠性试验技术和完善可靠性标准。

冷战时期，由于军备竞赛的白热化，可靠性工程的研究也不断发展。冷战以后的 20 世纪末期，大量科技成果进入民生领域，一项技术或一个设备可靠与否，直接关系到大众的生活，于是可靠性问题就成为了社会共同关注的问题。

最概括的可靠性定义就是你所依赖的对象完成你所期望任务的能力或可能性。对象过去多次完成过相同的任务，你就可以相信它（或他）完成本次任务的可能性大，据此给出比较“可靠”的估计，反之，失败的记录较多的，估计完成本次任务的可能性就小，可靠性也就较低。

再展开一点说，依靠同一个对象完成同样的任务，如果环境提供的条件不同，完成任务的可能性会不同，环境恶劣些，完成任务的可能性会低一些，这是很容易理解的。如果完成任务有时间上的限制，时间限制放宽一些，完成任务的可能性就会大一些。如果条件和限制时间相同，而你对任务的期望不同，完成的可能性当然也会不同。

因此，可靠性的更完整的定义是：对象在规定条件下、规定的时间内完成规定任务的能力或可能性。

按通常的表述方法，用 R 表示可靠性，用 c 表示条件，用 t 表示花费的时间，用 m 表示任务，则 $R = f(c,t,m)$，就是说可靠性是条件、时间和任务三者的函数。这里的 c、t、m 表示的是某特定的条件、时间和任务。在条件和任务确定的情况下，可靠性就是时间的函数，即 $R = f(t)$，这里的 f 表示函数，它和后面说到的概率密度不是一件事。它也表示为 $R(t)$，是可靠性时间函数最常见的表示形式。

可靠度是关于可靠性的一种测度。作为测度，它应该符合测度学（或称度量学）的

规则。在很多情况下可靠度被定义为一种概率(或然率,probability)。对电子、机械等批量生产的部件以及用这些部件构成的产品来说,由于通过产品试验能够提供足够用于统计推断的数据,作为概率的可靠度能够比较真实地反映可靠性。这时,可靠度是:"产品在规定的条件下从开始工作到规定的时间 t 内完成规定任务的概率"。换一种说法就是"完好的产品在规定的条件下开始工作(即从0时刻起)到时刻 t 不发生失效的概率"。作为概念的延伸也可以说是"产品在规定的条件下和规定的时间区间(t_1, t_2)内完成规定功能的概率"。

以概率形式提供的可靠性,必须有足够数量的试验作为基础,这时所做的估计才是可信的。例如,铁路的信号灯泡,它的平均寿命约为1 600 h,需要在规定的环境条件下进行数十万次(灯泡的个数×试验小时)试验后得到的数据来估计才能证实。如果离开统计试验要求很远,对可靠性所做出估计的可信程度(置信度,confidence level)就会降低。

有一些批量很小的产品不允许进行大量的试验,特别是进行大量破坏性的试验。这时,如果这个产品能够分解为许多独立的成分,而这些独立成分能够获得可信的统计数据,则可以通过系统综合的方法获得关于这个产品的可靠度。如果不能依赖统计,而是依赖经验或大部分依赖经验的途径来获得量化可靠性的话,这样的可靠性所表示的只是一种似然性(likelihood)意义上的可能性,而不是基于统计的概率。软件的失效源于人的种种失误,包括对评价对象设计需求的错误理解,程序设计中的疏忽,测试的不充分等等,评价软件可靠性的依据大多不是在相同或相近环境条件下进行试验所取得的,所以只能得到"似然"意味上的可靠性,和上述基于统计的可靠性存在着差别。

可靠度和可维修度(maintainability)、可用度(availability)等一起构成了广义可靠性指标体系。

在对产品进行可靠性研究时,还常常需要用到随机过程、排队论、数理规划等数学理论和方法,因此可靠性是一个综合的学科领域。

对于计算机产品,为提高可靠性,比较广泛地采用容错计算技术。通过冗余、自校验、重构、多版本、自恢复等实现计算机低故障或无故障运行。这种以容错技术为基础的广义可靠性技术也被称为可信性(dependability)或可信计算技术。

铁路信号既是运输安全的防范设备,也是提高运输效率的重要手段。在成本受到制约的时候,追求高安全性和追求高可靠性两个目标会存在一些矛盾。但是,在多数情况下高可靠性是高安全性的有力支撑。

可靠性工作基本内容见图1-1。

2. 不可靠事件的起因

每个人都遇到过设备发生故障的经历。一个完好的设备,不论是电视机还是洗衣机,使用了一段时间后,就会出现故障。请人来看一看,说是"故障啦,某某部件或零件

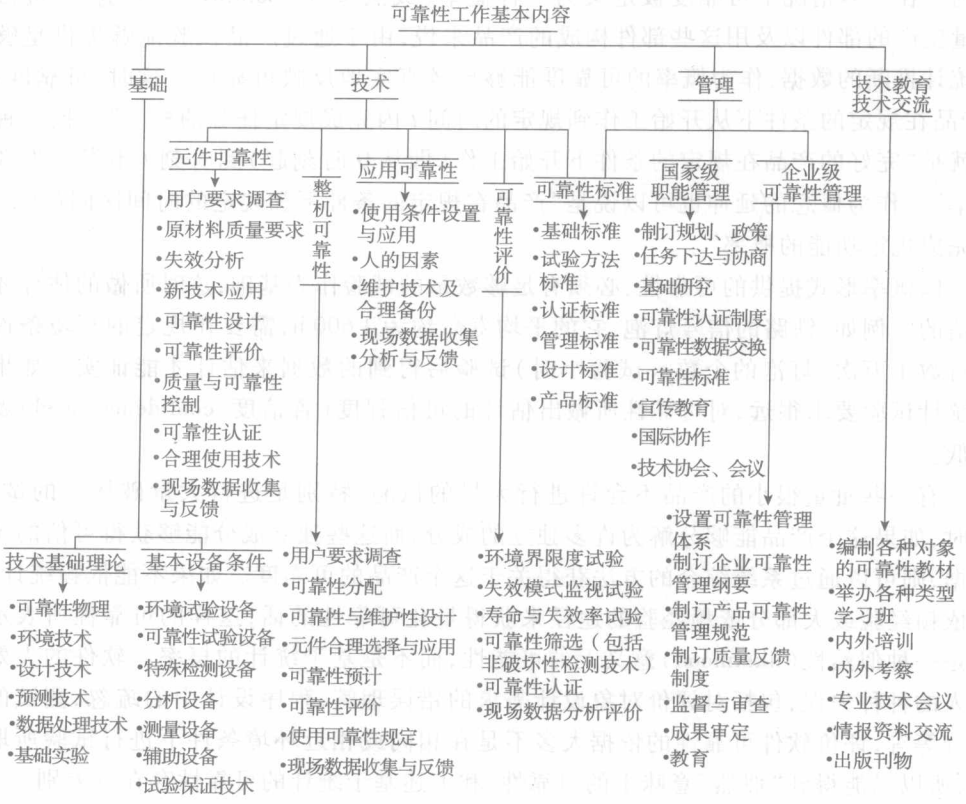

图 1－1　可靠性工作基本内容

性能变坏了”云云，换一个好的或调整一下，故障排除，设备又可以重新启用了。如果这个设备不时发生故障而经常不能使用，当然就成了一件不可靠的设备，究其原因，是设备出现了实物故障。

上面这个例子说的是由于设备中元、部件损坏或失效导致的故障。设备的故障还存在其他的原因。我们使用计算机，有时出现“死锁”而不能使用，这时只要关机重新启动，就可以继续使用了。如果这类计算机不时出现“死锁”而经常不能连续使用，当然也是一件不可靠的设备。而不可靠的原因并不是元部件的损坏或失效，而是出现了非实物的故障。

设备故障的成因“是”或“不是”元、部件失效，还只是第一层面上的问题。即使是元、部件失效造成的故障，还需要探究造成设备故障的元、部件失效的深层原因。是元部件本身质量不好，还是当初设计时根本就不应该选用这种元、部件，或者是选择该元、部件本身并无不当，但是和其他部件之间存在配合的问题等等。所以，对某一项设备不可靠原因的探究是一个综合的问题。

造成设备故障的原因很多，可归结为四个方面原因：需求说明的错误、技术实现上的失误、工艺制作上的失误、使用环境上的失误。工艺制作和环境造成的原因是最为表象的，通常是实物故障。而需求的原因却往往是深层次的和最为全局性的。

(1)需求说明的错误

需求说明是设备整体技术要求的体现。需求说明除了要阐明对象设备的整体要求以外，还必须指出该设备开发所应该遵循的各级技术的和非技术的标准。为什么说需求说明的差错是影响全局的、深层次的，因为以下各条中阐述的其他的故障起因，都可以通过提高需求说明工作的质量加以防范：

如果下述(2)中对于复杂的逻辑关系在需求说明中有更加严密的刻画、对部件间的适配性有细致描述，就可以减少由于设计造成的失误；

如果下述(4)中涉及的应用环境，在编制需求说明时做过周密的调查，提出选用更有效的环境防范措施和选用具有抗恶劣环境能力的元、部件的需求，同样可以减少设备故障的机会；

如果下述(3)中的制造工艺无法有效地监控，在需求说明中，至少可以对选用外部采购元、部件的检验提出更有针对性的特定要求。

(2)技术实现上的错误

技术实现上的错误除了因疏忽造成的缺陷外，较常见的还有两类：

一是存在复杂逻辑关系时设计上的错误。很多工业上的安全控制，包括铁路信号的控制都包含复杂的逻辑关系。在大量采用计算机来实现这种逻辑关系后，像车站计算机联锁的软件，涉及站场的不同布局和不同车站的作业特征，由于对布局和作业间逻辑关系理解上的偏差而导致故障。

二是设备各部件之间适配性设计的缺陷。尽可能采用通用部件是现代制造业面对全球化经济格局自然形成的一种普遍做法。互换性和可移植性(软件)等技术标准的形成，可以使企业集中精力开发设备中体现高科技特色的“卖点(指营销中竭力推介的亮点)”。但是由于适配性上的失误，导致设备故障的事件日见增多。例如，某成熟型号汽车的一个部件总成(组件)，当被一款新型车辆的设计采用时，如果存在个别参数失配，就可能在某种运行状态下出现车辆的故障。

(3)元、部件缺陷

元、部件的功能设计是正确的，但是工艺制作过程不完善，包括原材料检验环节、工艺过程的设计、工艺环境控制、产品质量检验环节存在问题而导致元、部件缺陷。有缺陷的元、部件在设备工作过程中因缺陷暴露而失效，造成设备故障。

说明：对属于消耗型的元、部件，或有确定磨损、耗散失效模式的元、部件，如电池、熔断器以及一些有机械磨损的零件等，它们的失效防范需要通过设备管理来实现。

(4)使用环境超限

设备组成的元、部件是无缺陷的，但是设备所处的使用环境，出现了超出或部分环

境条件超出额定的情况。使用的额定环境包括:温度、湿度、震动、电磁干扰、核辐射等方面的限制。在出现超限的条件下,元、部件失效,造成设备故障。

对许多设备故障的调查分析表明,需求说明的不完整性、模糊性是设备不可靠的根本原因。

对于任何设备的开发、运用都不可能是不计成本的。我们如果对元、部件进行检验,就必须支付检验工具、检验人员和检验时间上的开销;要求选用抗恶劣环境能力更强的部件,必定增加产品的造价;编制更加完善、周密的需求说明,更需要投入大量的人力和物力。由于成本的制约,设备的可靠性只能期望在某一个合适的高度。

设备故障的另一个重要的原因,是设备投入运行后的管理和维护。严格的管理和有效的维护是从另一个方面避免设备故障的有力手段。

3. 软件的可靠性问题

硬件和软件可靠性有某些相似点,但也有许多不同点,因此,既不要认为软件过于独特,但也不要将两者看得过于相似。软件可靠性与硬件可靠性两者可以用同样的方式加以定义,把它们结合起来就形成了系统可靠性。软件的故障来源是系统和程序的设计错误,硬件的故障来源一般是物理劣变。然而软件可靠性设计的某些概念也适用于硬件的设计活动。但是,由于磨耗和其他物理原因造成故障的可能性一般大于由于硬件设计问题所造成故障的可能性,硬件也没有软件复杂,减少硬件设计差错比较容易。所以"设计可靠性"的概念在硬件方面不常使用。

尽管硬件可靠性与软件可靠性有上述不同之处,但在研究软件可靠性时,仍可借鉴硬件可靠性的方法和理论。

应用软件的可靠性指在采用计算机控制的设备或系统中,在主机硬件及系统软件工作正常的条件下,应用软件满足规定功能要求的能力。软件可靠性作为一个技术领域,它还包括为提高软件制作质量所需技术上和管理上的努力,系统抗故障和误操作的努力,以及可靠性和安全性的评价等问题。

由于近些年计算机硬件质量迅速提高,运算速度不断加快,价格不断降低,功能日趋丰富,系统愈加复杂,一些应用软件的可靠性问题随之日显重要。

软件可靠性的研究对象是软件开发中的各类差错。和硬件可靠性问题有共同之处的是两者所研究的都是失效的"起因"和"结果"的关系。不同的是软件没有磨损、耗散、疲劳、断裂等导致硬件失效的机理。软件开发中引入的差错,在没有得到修改之前一直潜伏在软件中,当软件运行在某个特定的环境时,就会诱发系统出错,如果对错误没有一种纠正的机制,就会引起软件任务的一次失效(失败)。有差错的软件,如果没有碰到这个特定的环境,它的差错就不会暴露,软件也不会失效。失效只是软件运行未达到规定需求的一次记录,而不是该软件需要"废弃"的依据。软件差错从暴露到失效有个过程,内在的差错也称隐错(bug),相当于硬件的故障(fault),也称为软件故障(失