系统可靠性与安全性

胡启洲/主　编
李香红　陈新　刘英舜/副主编

西南交通大学出版社

图书在版编目（CIP）数据

系统可靠性与安全性 / 胡启洲主编. —成都：西南交通大学出版社，2019.10
ISBN 978-7-5643-7185-2

Ⅰ. ①系… Ⅱ. ①胡… Ⅲ. ①交通工程－系统可靠性－研究②交通工程－系统安全性－研究 Ⅳ. ①U491

中国版本图书馆 CIP 数据核字（2019）第 236076 号

Xitong Kekaoxing yu Anquanxing

系统可靠性与安全性

主编　胡启洲

责任编辑	孟秀芝
封面设计	曹天擎
出版发行	西南交通大学出版社 （四川省成都市金牛区二环路北一段 111 号 西南交通大学创新大厦 21 楼）
发行部电话	028-87600564　028-87600533
邮政编码	610031
网址	http://www.xnjdcbs.com
印刷	四川森林印务有限责任公司
成品尺寸	170 mm × 230 mm
印张	12.25
字数	193 千
版次	2019 年 10 月第 1 版
印次	2019 年 10 月第 1 次
书号	ISBN 978-7-5643-7185-2
定价	35.00 元

课件咨询电话：028-81435775
图书如有印装质量问题　本社负责退换
版权所有　盗版必究　举报电话：028-87600562

前　言

《系统可靠性与安全性》是交通工程专业开设的一门专业基础课。现代交通的发展，离不开科学技术的进步。而交通的快速发展，更离不开基础学科的大力推动。所以，掌握系统可靠性与安全性的基本知识，已经成为交通工程专业的学生及从业人员必须具备的条件。

本书从两个方面解读系统可靠性与安全性：一是“知其然，知其所以然”，即在界定可靠性的基础上，从系统角度研究可靠性的特征参数和计算方法；二是“理念创新，方法应用”，即在界定安全性基础上，从系统层面研究交通安全性的性能特征和量化方法，并结合交通学科特点来研究不同交通方式的系统安全性。最后，达到“从实践中来，到实践中去”的目的。

本书由南京理工大学胡启洲任主编，济南理工大学李香红，南京理工大学陈新、刘英舜任副主编，南京理工大学卞立、谈敏佳、林娟娟等博士研究生，岳民、周浩、李晓菡、曾爱然等硕士研究生也参与了编写。本书编写过程中也得到编辑部同仁的帮助，在此表示衷心感谢。本书参考了许多前人成果，在此表示感谢。

本书可作为科研工作者、工程技术人员、管理工作者、大专院校师生的读物。但由于时间和水平有限，书中难免有疏漏和不当之处，敬请广大读者赐教批评。

编　者

2019 年 7 月

此为试读，需要完整PDF请访问：www.ertongbook.com

目 录

第 1 章 系 统 ····· 1

1.1 系统的概念 ····· 1
1.2 系统工程 ····· 3
1.3 系统工程的实现途径 ····· 7

第 2 章 可靠性概论 ····· 9

2.1 可靠性的基本概念 ····· 9
2.2 可靠性的相关术语 ····· 16
2.3 可靠性的数学知识 ····· 26
2.4 可靠性参数体系 ····· 38

第 3 章 系统可靠性分析 ····· 41

3.1 系统可靠性概述 ····· 41
3.2 不可修复系统的可靠度计算方法 ····· 45
3.3 可修复系统的可靠性计算方法 ····· 65

第 4 章 系统可靠性的设计方法 ····· 75

4.1 可靠性设计的基本准则 ····· 75
4.2 系统可靠性的设计内容 ····· 76
4.3 系统可靠性的基本要求 ····· 77
4.4 系统可靠性的设计方法 ····· 78

第 5 章　系统可靠性的预计与分配……84

5.1　系统可靠性的预计方法 ……84
5.2　系统可靠性的分配方法 ……92
5.3　可靠性分配的注意事项 ……104

第 6 章　系统安全性 ……107

6.1　系统安全工程……107
6.2　系统安全性概述……108
6.3　交通系统的安全性……114

第 7 章　系统安全性的计算方法 ……125

7.1　系统安全性的分析方法 ……125
7.2　系统安全性的数学模型 ……146
7.3　系统安全性的评价方法 ……153
7.4　系统安全性的综合评价方法……160
7.5　系统安全性的粗糙集评估模型……179

附　录……183

参考文献……187

第 1 章　系　统

系统是指将零散的东西进行有序的整理、编排形成的具有整体性的整体。中国著名学者钱学森认为，系统是由相互作用、相互依赖的若干组成部分结合而成的，具有特定功能的有机整体，而且这个有机整体又是它从属的更大系统的组成部分。

由运动着的若干部分，在相互联系、相互作用之中形成的具有某种确定功能的整体，谓之系统。而系统工程是为了最好地实现系统的目的，对系统的组成要素、组织结构、信息流、控制机构等进行分析研究的科学方法。它运用各种组织管理技术，使系统的整体与局部之间的关系协调和相互配合，实现总体的最优运行。系统工程不同于一般的传统工程学，它所研究的对象不限于特定的工程物质对象，而是任何一种系统。它是在现代科学技术基础之上发展起来的一门跨学科的边缘学科。

1.1　系统的概念

“系统”一词源于英文 system 的音译，并对应其外文内涵加以丰富。系统就是由相互作用、相互依赖的若干组成部分结合而成的，具有特定功能的有机整体。而系统由部件组成，部件处于运动之中、部件间存在着联系、系统各部件和的贡献大于各部件贡献的和、系统的状态是可以转换和可以控制的。因此，系统概念含有五个基本要素：功能、组元（组成）、结构、运行与环境。

1. 系统的定义

系统（System）由相互作用、相互依赖而又相互区别的若干组成部分结合而成的，具有特定功能的有机整体。

（1）多元性（Multielement）。系统是由若干要素（部分）组成的。这些要素可能是一些个体、元件、零件，也可能其本身就是一个系统（或称之为子系统）。

（2）集体性（Collectivity）。系统有一定的结构。一个系统是其构成要素的集合，这些要素相互联系、相互制约。系统内部各要素之间相对稳定的联系方式、组织秩序及失控关系的内在表现形式，就是系统的结构。

（3）功能性（Functionality）。系统有一定的功能，或者说系统要有一定的目的性。系统的功能是指系统与外部环境在相互联系和相互作用中表现出来的性质、能力和功能。

因此，系统可以是机器、设备、部件和零件，单元也可以是机器、设备、部件和零件。系统和单元的含义是相对而言的，依研究的对象而定。系统可以分为可修复系统与不可修复系统两类。

2. 系统的分类

系统可以分为三类：自然系统、人工系统、复合系统。

（1）自然系统（Natural System）。系统内的个体按自然法则存在或演变，产生或形成一种群体的自然现象与特征。自然系统包括生态平衡系统、生命机体系统、天体系统、物质微观结构系统以及社会系统等。

（2）人工系统（Manual System）。系统内的个体根据人为的、预先编排好的规则或计划好的方向运作，以实现或完成系统内个体不能单独实现的功能、性能与结果。人工系统包括立体成像系统、生产系统、交通系统、电力系统、计算机系统、教育系统、医疗系统、企业管理系统等。

（3）复合系统（Composite System）。复合系统是自然系统和人工系统的组合。复合系统包括导航系统、交通管理系统和人—机系统等。

3. 系统的特性

系统的特性主要有：整体性、相关性、层次性、目的性、环境适应性。

（1）整体性（Integrity）：一个系统的完善与否主要取决于系统中各要素能否良好的组合，即是否能构成一个良好的实现某种功能的整体。即使并非每个要素都很完善，它们也可以综合、统一成为一个具有良好功能的系统，这就是一个较为完善的系统；反之，尽管每个要素是良好的，构成整体后却不具备某种良好的功能，这不能称之为完善的系统。

（2）相关性（Relativity）：系统内各要素之间是有机联系和相互作用的，要素之间具有相互依赖的特定关系，是互为相关的。

（3）目的性（Purposiveness）：所有系统为了实现某一特定的目标，没有目标就不能称之为系统。不仅如此，设计、制造和使用系统，最后总是希望完成特定的功能，而且要效果最好，这就是所谓最优计划、最优设计、最优控制、最优管理和使用等。

（4）层次性（Hierarchy）：系统有序性主要表现为系统空间结构的层次性和系统发展的时间顺序性。系统可分为若干子系统和更小的子系统，而该系统又是其所属系统的子系统。这种系统的分割形式表现为系统空间结构的层次性。

（5）环境适应性（Environmental Suitability）：任何一个系统都处于一定的物质环境之中，系统必须适应外部环境条件的变化，而且在研究和使用系统时，必须重视环境对系统的作用。

1.2 系统工程

系统工程（Systems Engineering）是以大型复杂系统为研究对象，按一定目的进行设计、开发、管理与控制，以期达到总体效果最优的理论与方法。所以，从系统观念出发，以最优化方法求得系统整体的最优的综合化的组织、管理、技术和方法的总称。因此，系统工程是组织管理系统的

规划、研究、设计、制造、试验和使用的科学方法，是一种对所有“系统”都具有普遍意义的科学方法。

1. 系统工程的定义

系统工程是为了研究由多个子系统构成的整体系统所具有的多种不同目标的相互协调，以期系统功能达到最优，并最大限度地发挥系统组成部分功能而发展起来的一门科学。

2. 系统工程的特点

系统工程的主要特点是：研究方法的整体性、应用学科的综合性、组织管理的科学化。

（1）整体性（Integrity）。把研究对象作为一个整体来分析，分析总体中各个部分之间的相互联系和相互制约，使总体中的各个部分相互协调配合，服从整体优化要求；在分析局部问题时，从整体协调的需要出发，选择优化方案，综合评价系统的效果。

（2）综合性（Comprehensiveness）。综合运用各种科学管理的技术和方法，将定性分析和定量分析相结合。

（3）科学化（Scientization）。对系统的外部环境和变化规律进行分析，分析它们对系统的影响，使系统适应外部环境的变化。

3. 系统工程案例

系统工程的典型案例有：美国阿波罗登月计划、苏联米格-25 战机、中国高速铁路工程。

（1）美国阿波罗登月计划（Apollo Program）。

阿波罗登月计划又称阿波罗工程，是美国 1961—1972 年组织实施的一系列载人登月飞行任务。其目的是实现载人登月飞行和人对月球的实地考察，为载人行星飞行和探测进行技术准备，它是世界航天史上具有划时代意义的一项成就。阿波罗计划是人类有史以来最庞大的工程之一，几十万名科学家和工程技术人员参与了这项工程。主要系统工程有：运载火箭

系统、导航定位系统、环境控制与生命保障系统、应急救生系统、人工控制系统、安全返回系统、高可靠性安全性系统。阿波罗登月计划的成功源于任何一个系统都要考虑与其他系统的衔接，如图 1.1 所示。

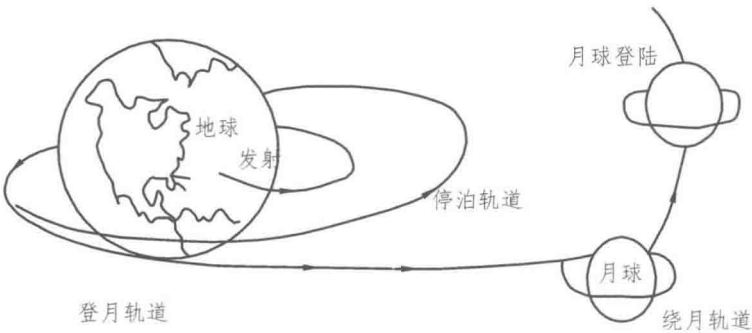

图 1.1 阿波罗登月系统工程

（2）苏联米格-25 战机（Mikoyan MiG-25 Program）。

米高扬米格-25（俄文：Микоян МиГ-25，英文：Mikoyan MiG-25，北约代号：Foxbat，译文：狐蝠）是高空高速截击战斗机，也是世界上第一种最大飞行速度超过 3 马赫的战斗机。米格-25 于 20 世纪 50 年代末开始设计，它的研制目的主要是对付美国研发的 XB-70“瓦尔基里”轰炸机与 A-12/SR-71“黑鸟”高空高速侦察机，这种侦察机的最高速度同样达到 3 马赫，普通的截击机根本无法追上。1961 年，米格-25 原型机在试验中创造了在 22 670 米的升限以 3 000 km/h 的速度飞行的世界纪录，当时世界上任何一架飞机都无法达到这一性能。“米格-25”是创造过“神话”的一代战机，打破和创造过 23 项世界纪录，其中 8 项飞行速度纪录、9 项飞行高度纪录、6 项爬高时间纪录。赋予“米格-25”高超本领的缘由，并不在于开拓了什么新的技术领域，也并非缘于采取了什么卓尔不群的技术成果，而是成功地利用了系统理论的整体功能原理，将并不是最先进的众多元件加以高效的有机组合，从而产生了惊人的系统效果，如图 1.2 所示。

此为试读，需要完整PDF请访问：www.ertongbook.com

图 1.2　米格战机系统工程

③ 中国高速铁路工程（China Railway High-Speed Program, CRHP）。

2005 年，我国铁路总营业里程为 7.5 万千米，我国人均占有铁路仅约 5.4 厘米，为美国的 1/3、日本的 1/7、德国的 1/15、英国的 1/10、法国的 1/8，当时我国并无高铁。从 2005 年开始，中国铁路客运专线及高速铁路网络建设进入实施阶段。到 2017 年，我国高铁运营里程为 2.5 千米（世界高铁里程 3.8 万千米），占世界 70%。中国已成为世界上高速铁路发展最快、系统技术最全、集成能力最强、运营里程最长、运营速度最高、在建规模最大的国家。通过“引进技术、消化、吸收、再创新”，特别是系统集成，完成高铁飞跃，中国用 5 ~ 10 年的时间，完成了其他国家 40 年走过的高铁历程。到 2020 年，世界逐步进入“高铁时代”，中国正站在世界铁路的前沿，共同应对全球性挑战，谋划未来，谱写高铁新篇章，如图 1.3 所示。

图 1.3 中国高铁铁路工程

1.3 系统工程的实现途径

系统工程不仅研究物质系统，还研究非物质系统，应用广泛；而一般工程技术以具体的物质系统为对象。系统工程也是一门高度综合性的管理工程技术，涉及应用数学、基础理论、系统技术科学以及经济学、管理学、社会学等各种学科。

1. 系统工程的实现内容

系统工程的主要任务是根据总体协调的需要，把自然科学和社会科学联系起来，应用现代数学和电子计算机等工具，对系统的构成要素、组织结构、信息交换和自动控制等功能进行分析研究，借以达到最优化设计、最优控制和最优管理的目标。系统工程的实现内容有：

（1）核心内容：一个“系统”，即以系统为研究对象。

（2）主要内容：两个“最优”，即总体效果最优、实现目标的具体方法或途径最优。

2. 系统工程的实现步骤

系统工程的基本方法是系统分析、系统设计与系统的综合评价（性能、费用和时间等）。系统工程的主要步骤有：

（1）系统规划（System Planning）：基于系统的概念、目的、目标、制约条件等要求，要进行综合分析研究，提出详细的规划方案。

（2）系统设计（System Design）：针对规划方案中相关内容，进行综合设计研究，设计效果要达到系统最优的效果。特别是在系统设计过程中，从可靠性工程出发，采取一系列设计措施以提高系统的可靠性和安全性水平，使其达到预定的性能指标。

（3）系统制造与运行（System Manufacturing and Operation）：根据设计，进行系统制造或运行，但也要达到实现方法最优的效果。

总之，通过系统可靠性指标的分配和设计，进行系统优化设计，使系统在现有条件下具有一定的可靠性。

重点与难点

重点：① 系统的定义；② 系统的特性；③ 系统工程的定义。

难点：系统工程的实现步骤。

思考与练习

（1）系统有哪些特性？

（2）系统工程的特点是什么？

（3）请你举出一些系统工程的案例。

（4）系统工程的实现内容有哪些？

（5）系统工程的实现步骤有哪些？

第 2 章　可靠性概论

可靠性（Reliability）是一门综合系统科学、管理科学、人机工程、计算机技术、信息技术、产品测试技术以及概率、统计、运筹、物理等多种学科的应用科学。它研究产品或者系统的故障发生原因、消除及预防措施。可靠性起源于 20 世纪 50 年代，60 年代得到迅速发展，70 年代进入成熟阶段，至今仍在发展。综观可靠性近半个多世纪的发展历程，它在实际应用中有着极其重要的作用。对于产品来说，可靠性问题和人身安全、经济效益密切相关。因此，对产品的可靠性问题进行研究，就显得非常重要与迫切。

随着科技的进步，系统或产品的规模越来越大，产品的复杂性日益增加。因此，研究可靠性意义重大：保证系统的可靠性与可用性，可以延长使用寿命、降低维修费用、极大提高系统的使用效益；可以防止或者预防故障和事故的发生，尤其避免灾难性的事故发生，从而保证人民的生命财产安全；可以减少停机时间，提高系统可用率；对于企业来讲，提高产品的可靠性可以改善企业信誉，增强竞争力，扩大产品销路，从而提高经济效益，还可以减少产品责任赔偿案件的发生，以及其他处理产品事故费用的支出，避免不必要的经济损失。

2.1　可靠性的基本概念

可靠性是“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”。把表示和衡量产品的可靠性的各种数量指标统称为可靠性特征量。可靠性特征量主要有：可靠度（Reliability）、失效（故障）概率密度（Failure Probability Density）、累积失效（故障）概率（Cumulative

Failure Probability）、失效（故障）率（Failure Rate）、平均寿命（Average Life）、可靠寿命（Reliable Life）、中位寿命（Median life）、特征寿命（Characteristics Life）等。可靠性按学科分类，一般可分为可靠性数学、可靠性工程、可靠性管理、可靠性物理等学科。

2.1.1 可靠性的定义

可靠性（Reliability）是一种表示元件、组件、部件、机器、设备或整个系统等产品，在正常使用条件下工作是否长期可靠、性能是否长期稳定的度量。可靠性除了有概率统计的概念外，还包含预期使用条件、工作的满意程度、正常工作时间的长短等内容。

1. 可靠性的基本定义

可靠性是系统在规定条件下和规定时间内，完成规定功能的能力。系统可靠性定义的要素有三个“规定”：

（1）条件。“规定条件”包括使用时的环境条件和工作条件。

（2）时间。“规定时间”是指系统规定了的任务时间。

（3）功能。“规定功能”是指系统规定了的必须具备的功能及其技术指标。

2. 可靠性的函数关系

可靠性就是系统在时间 t 内不失效的概率 $P(t)$。如果 T 为系统从开始工作到首次发生故障的时间，系统无故障工作的概率为

$$P(t)=P\ (T>t) \tag{2.1}$$

基于式（2.1），可靠性 $P(t)$ 具有以下三条性质：

性质一：$P(t)$ 为时间的递减函数；

性质二：$0\leqslant P(t)\leqslant 1$；

性质三：$P(t=0)=1,\ P(t=\infty)=0$。

因此，系统或设备的可靠性是一个与时间有密切关系的量，使用时间越长，系统越不可靠；使用时间越短，系统越可靠。

2.1.2　故障的定义

故障（Failure）是指系统或系统的一部分不能或将不能完成预定功能的事件或状态，即系统丧失了规定的功能。

1. 故障的相关概念

故障的相关概念主要有：失效、故障模式和故障机理。

（1）失效（Failure）：对于不可修的系统，其状态称作失效。

（2）故障模式（Failure Mode）：故障的表现形式，称作故障模式。

（3）故障机理（Failure Mechanism）：引起故障的物理化学变化等内在原因，称作故障机理。

2. 故障的分类

故障主要有三种分类方式：

（1）系统的故障按其故障规律分为两大类：偶然故障和渐变故障。

偶然故障（Random Failure）是指产品由于偶然因素引起的故障。

渐变故障（Gradual Failure）是指由于产品的规定性能随寿命单位数增加而逐渐变化引起的故障。

（2）系统的故障按其故障后果分为两大类：致命性故障和非致命性故障。

致命性故障（Critical Failure）是造成产品不能完成规定任务的或可能导致人或物发生重大损失的故障或故障组合；

非致命性故障（Uncritical Failure）是指不太可能导致人员伤亡、重要物件损伤或其他不可容忍后果的故障。

（3）系统的故障按其统计特性分为两大类：独立故障和从属故障。

独立故障（Independent Failure）是指不是由于另一产品故障而引起的故障。

从属故障（Dependent Failure）是指由于另一产品故障而引起的故障。

2.1.3　可靠度

可靠度（Reliability）是可靠性的度量，一般指的是产品在规定的条件下和规定的时间内，完成规定功能的概率。依定义可知，系统的可靠度是

时间的函数：

$$R(t)=P(\xi>t)$$

式中　$R(t)$——可靠度函数；

ξ——产品正常工作时间；

t——规定的时间。

事件$(\xi>t)$有三个含义：

（1）产品在 t 时间内完成规定的功能。

（2）产品在 t 时间内无障碍。

（3）产品的寿命 ξ 大于 t。

显然，规定的时间 t 越短，系统完成规定功能可能性越大；规定的时间 t 越长，系统完成规定功能的可能性就越小。

由可靠度的定义可知，$R(t)$描述了产品在$(0,t)$时间段内完好的概率，且

$$0\leqslant R(t)\leqslant 1,\quad R(0)=R(+\infty)=0$$

上述公式表明，开始使用时，所有的产品都是良好的，只要时间充分长，全部的产品都会失效。

如前所述，这个概率是真值，实际上是未知的。在实际应用中常用它的估值 $\hat{R}(t)$。

假如在 $t=0$ 时有 N_0 件产品开始工作，而到 t 时刻，有 $r(t)$ 个产品失效，仍有 $N_0-r(t)$ 个产品继续工作，则可靠度 $R(t)$ 的估计值：

$$\hat{R}(t)=\frac{N_0-r(t)}{N_0}=1-\frac{r(t)}{N_0}$$

式中：N_0——当 $t=0$ 时，在规定条件下进行工作的产品数；

$r(t)$——在 0 到 t 时刻工作时间内产品的累计故障数。

由可靠度的定义可知，$R(t)$ 描述了产品在 $(0,t)$ 时间内完好的概率，且 $R(0)=1$，$R(\infty)=0$。

2.1.4　累积故障概率

产品在规定条件下和规定时间内，丧失规定功能的概率称为累积故障概率（又叫不可靠度）。

此为试读，需要完整PDF请访问：www.ertongbook.com