复杂系统可靠性建模与分析

Complex System Reliability Modeling and Analysis

金光 著

国防工业出版社
National Defense Industry Press

复杂系统可靠性建模与分析

金光 著

国防工业出版社
·北京·

内 容 简 介

本书讨论复杂系统可靠性建模与分析问题，介绍了目前比较典型的模型和比较有效的分析方法。其中，主要包括基于 BDD 的复杂系统可靠性组合分析方法、基于 Petri 网的动态系统可靠性建模与分析方法、基于 Bayes 网络的不确定性系统可靠性建模与分析方法、高可靠度系统仿真方法，以及多模型集成的复杂系统可靠性建模与分析方法。书中通过典型案例对这些模型和方法进行了说明。本书所介绍的模型和分析方法，既具有较强的描述和解决问题的能力，又具有较好的扩展性和适用性，可以较好地满足现代复杂系统可靠性建模与分析的需求。

本书可供从事可靠性理论、概率论与随机过程、管理科学与工程以及系统工程等科研人员阅读，也可作为上述有关学科专业的研究生教材。

图书在版编目(CIP)数据

复杂系统可靠性建模与分析 / 金光著. —北京：国防工业出版社，2015.1

ISBN 978-7-118-09744-3

Ⅰ.①复... Ⅱ.①金... Ⅲ.①系统可靠性—系统建模 ②系统可靠性—系统分析 Ⅳ.①N945.1

中国版本图书馆 CIP 数据核字(2014)第 246281 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 19¼ **字数** 550 千字

2015 年 1 月第 1 版第 1 次印刷 **印数** 1-2000 册 **定价** 86.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

前　言

现代复杂系统具有多功能、多任务、多阶段、多状态、高可靠、长寿命、小子样以及复杂相关性和高度不确定性等特点，对这些系统的可靠性进行描述和定性定量分析越来越困难。传统的系统可靠性技术通过对复杂系统的结构和功能进行简化，根据所获得的近似的简单系统解决复杂系统的可靠性问题，有时会导致难以接受的误差甚至荒谬的结论。因此，根据复杂系统的特点，运用系统工程的方法，研究适用于现代复杂系统的可靠性设计、分析、制造、试验和使用等新技术、新方法，已经成为现代可靠性工程的迫切需求。

本书以现代复杂系统可靠性建模与分析问题为背景，介绍作者在相关研究领域的工作，以及近30年来国内外在复杂系统可靠性建模与分析领域的典型成果。在选材上，没有将可靠性建模与分析的经典方法，如故障树分析法、马尔可夫(Markov)过程建模与分析法等作为重点，而是针对现代复杂系统可靠性特点，介绍两种描述能力较强、理论研究成果比较丰富的系统级模型，包括Petri网模型和Bayes网络模型，前者主要解决复杂动态系统的可靠性建模与分析问题，后者主要针对不确定性系统的可靠性建模与分析问题。此外，从复杂系统故障模式分析的角度，重点介绍了基于BDD的系统可靠性组合分析方法，包括基本BDD方法及其扩展在非单调关联系统、多阶段系统、多状态系统、顺序相关失效系统、存在故障传播和波及效应的系统的可靠性分析中，实现的方式和典型的案例。针对复杂系统可靠性模型解析求解的困难，介绍了可靠性仿真方法，其中主要关注高可靠度系统仿真的抽样效率问题，介绍了限制抽样法、序贯抽样法、状态转移链法、重要性抽样法等。最后，本书介绍了如何将关于部件和系统可靠性的现有不同类型的模型和分析方法进行集成的方法，包括多模型集成的可靠性建模方法、解析分析方法和仿真方法，介绍了作者所开发的多模型集成的可靠性建模与分析软件工具MISER。书中对各有关的模型和方法，都通过案例进行了说明。

本书所介绍的模型和分析方法，是针对系统可靠性分析问题的特点提出的，即在系统可靠性分析中，人们不仅需要定量计算系统可靠性指标，同时也非常关注对故障模式、故障传播和波及效应、部件故障对系统影响的方式等的定性分析。为此，作者力求在模型描述能力及其对系统可靠性定性定量分析的支持之间获得平衡，以便较好地满足复杂系统可靠性建模与分析的需求。

本书内容主要来自作者本人及其合作者的科研工作的积累，他们是周经伦、周忠保、刘强、厉海涛、肖磊、赵炤、赵琰、周军等。本书的完成还得益于作者讲授“复杂系统可靠性技术”研究生课程过程中与学生的讨论交流，并参考了国内外代表性研究成果，对此作者亦表示感谢。

本书的完成得到国家自然科学基金“基于性能退化的可靠性理论方法研究”(编号：71071158)和“多阶段退化产品寿命预测理论方法研究”(编号:71371183)的资助。

由于作者水平有限，本书的选材和文字难免存在不当和疏漏之处，某些观点也可能需要进一步商榷，敬请读者不吝批评指正。

目　录

第1章 绪 论

1.1 可靠性工作的意义

在现代高技术局部战争中，为了赢得战争的胜利，必须发展高新技术武器装备。这些武器装备不仅必须具有精确打击能力和威慑能力，还必须具有良好的战备完好性和任务成功性，以及良好的机动性和快速反应能力。20 世纪 90 年代初发生的“海湾战争”和 1999 年历时 78 天的“盟军行动”等高技术局部战争表明，可靠性、维修性和保障性（R&M&S，包括测试性和安全性）已成为武器装备形成战斗力的前提条件，是保证武器装备战备完好性和出动强度的基础。21 世纪武器装备的性能和复杂性将会迅速提高，特别是信息技术、微电子技术和微机电技术的飞速发展，对 R&M&S 的发展将产生深刻影响，R&M&S 将面临新的挑战，同时也面对新的机遇。

具体到可靠性工作的意义，可以从以下几个方面理解：

1. 可靠性是装备的一项重要技术指标

可靠性是指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。“高附加值”产品的竞争实质上是可靠性的竞争。有人讲，“宁愿牺牲先进性，也要保证可靠性”[8]。只有掌握可靠性技术的工程师，才能设计和制造出有竞争力的产品。日本将可靠性作为企业的主要奋斗目标，美国认为世界产品竞争的焦点是可靠性，苏联曾将可靠性纳入 25 年发展计划。大型装备的可靠性是衡量一个企业、一个国家科技水平的重要标志。1969 年，美国“阿波罗”飞船登月成功，美国宇航局将可靠性工程列为三大技术成就之一。我国“神舟五号”飞船成功的关键是解决了可靠性问题，其可靠性指标达到 0.97，航天员安全性指标达到 0.997。而我国三峡工程大坝合龙时，使用的全部车辆为进口产品，也与当时国产车辆可靠性过低有关①。

2. 装备系统的大型复杂化，使可靠性问题越来越突出

21 世纪是空间时代，有人和无人的空间工程，如通信卫星、载人空间轨道实验室、宇宙飞船等都要求很高的可靠性。这些空间工程都是高科技产品，投资昂贵，产品结构复杂性极高，对可靠性的要求日益增高。这些大型复杂系统的可靠性不仅是企业的生命，而且与国家安全密切相关。

首先，工程系统结构的复杂性以及功能的相关性、涌现性、不确定性等，使得工程系统的行为越来越复杂[5]。1986 年，美国“挑战者”号航天飞机失事，就是由于助推火箭燃料箱密封装置在低温下失效所致。其次，某些工程系统使用环境的广泛性、严酷性，又要求系统具有很高的可靠性。丰田汽车公司油门踏板系统导致的召回危机，凸显了用计算机芯片和电子传感器替代软管和液压液的复杂系统的可靠性问题。最后，随着现代工业设备的容量、参数的日益提

① 例如，某越野车可靠性对比试验中，对 9 台国产车、3 台进口车进行试验，国产车无故障运行里程仅为 380～880km，进口车无故障运行里程则达到 28000km。

升，以及工业生产规模化、工艺流程连续化、设备运行高速化等特点，要求工程系统必须可靠。对于核电、化工等涉及安全性的领域，对可靠性要求更为突出，这些工程系统不可靠可能带来连锁反应，从元件故障扩散到整个系统，引发严重的经济和安全问题，可能给整个社会带来长期而严重的危害。1979 年的三哩岛核电站放射性物质泄漏事故、1986 年的切尔诺贝利核电站事故，都是这方面的典型案例。

3. 提高装备可靠性是减少装备寿命周期费用的重要途径

提高装备可靠性，有助于减少装备全寿命周期费用（LCC），特别是使用阶段的维修、保障人力和费用。据统计，美国使用与保障费用在装备全寿命周期费用中所占比例约为 60%，如图 1－1所示。美军部署一个 F－15A 战斗机中队，约需要 15～18 架 C－141B 运输机运载有关维修保障设备，需要 554 名维修人员；而由于其可靠性高，维修工时少，部署一个 F－22 战斗机中队仅需 6～8 架 C－141B，如表 1－1 和图 1－2 所示。美国 F－105 战斗机投资 2500 万美元，可靠度从 0.7263 提高到 0.8986，每年节省维修费用 5400 万美元。

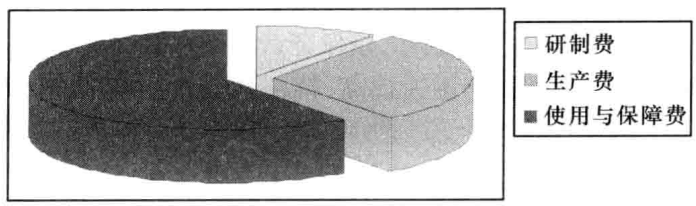

图 1－1　装备全寿命周期费用构成

表 1－1　美国战斗机维修规模

机型	服役年代	维修人员/中队	是否开展 R&M 工作
F－4E	20 世纪 60 年代	588	未开展
F－15A	20 世纪 70 年代	554	开展
F－22	20 世纪 90 年代末	277	开展

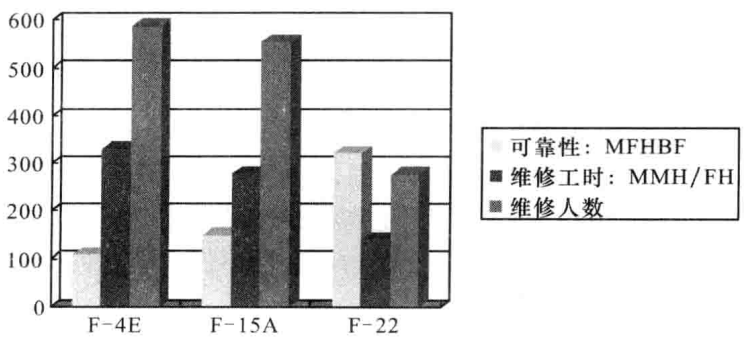

图 1－2　美国战斗机可靠性与维修性变化①

4. 提高装备可靠性，有助于提高装备效能

装备效能（Effectiveness）是衡量一个装备满足一组特定任务要求程度的度量。美国工业界武器装备效能咨询委员会（WSEIAC）的装备效能模型，是目前人们普遍接受的分析装备效能的经典模型。该模型指出，装备效能是装备可用性 A、可信性 D 和能力 C 的函数，具体表

① MFHBF：平均故障间隔飞行小时，Mean Fly Hour Between Failure。

示为

$$E = ADC$$

1986 年美军空袭利比亚时，从英国起飞 24 架 F－111 轰炸机，其中 6 架因故障中途返航，到达目标后 5 架因火控系统故障不能投弹，极大影响了装备作战效能的发挥。因此，可靠性（包括基本可靠性和任务可靠性）是影响装备效能的重要指标，也是提高武器装备战斗力的“倍增器”。21 世纪的可靠性技术将是提高武器装备战斗力的一种更加经济有效的工具，为更快、更好和更省地研制、生产、使用和保障满足 21 世纪军事需求的新一代武器装备提供强有力的技术支持。

1.2 可靠性工程的发展

可靠性起源于军用电子设备失效现象的研究。1941 年，R. Lusser 在德国 V－1 导弹测试过程中，采用串联系统可靠性乘积定律，计算 V－1 制导装置可靠度为 0.75，第一次定量表示产品可靠性。R. Lusser 也是第一个认识到可靠性工程应成为独立学科的人。第二次世界大战期间，美国 60% 的机载电子设备运到远东后不能使用，50% 的电子设备在存储期间失效，通信设备中 60% ～75% 的无线真空电子管失效，轰炸机的电子控制装置正常工作时间不超过 20h，美国空军飞机由于技术故障造成的事故高于战斗中被击落的损失。朝鲜战争前，美国 70% 的海军电控装置不能正常工作。1958 年，美国卫星发射成功率仅为 28%。大量军用电子设备频繁失效的现象，迫使人们思考失效现象背后的本质问题。从 1952 年美国国防部成立“军用电子设备可靠性咨询组”（Advisory Group of Reliability of Electronic Equipment，AGREE）以来，有组织、有计划地开展可靠性研究至今已有半个多世纪，可靠性工程不断成长、壮大，走过了工程化、标准化、制度化、CAD 化、智能化、一体化的发展历程，成为一门综合性基础工程学科。

20 世纪 50 年代是可靠性工程形成一门独立学科的兴起时期[3]，以美国为代表的工业发达国家，以军用电子设备（当时主要是电子管设备）可靠性为切入点，有组织、有计划、全面地开展可靠性研究，把可靠性技术运用到导弹和军用电子设备的研制中，取得了明显的效果。1953 年，兰德公司在美国空军资助下，系统总结了可靠性统计理论和技术。1954 年，IEEE、ASQC 和 IES 联合资助召开了美国第一个全国性的可靠性和质量控制会议。1956 年，McGraw－Hill 出版了 Keith Henney 编写的第一本关于可靠性的教材，美国无线电公司出版了第一份关于失效率和可靠性数据的报告。1957 年 1 月，美国空军公布了第一部军用可靠性规范 MIL－R－25717。1957 年 6 月，美国国防部发表的 AGREE 报告，奠定了可靠性工程的基础。

20 世纪 60 年代是可靠性工程全面发展的时期，制定出 MIL－HDBK－217《电子设备可靠性预计》（1962 年）、MIL－STD－781《可靠性鉴定试验及产品验收试验（指数分布）》（1965 年）、MIL－STD－785《系统与设备的可靠性大纲》（1965 年）、MIL－STD－1629《故障模式、影响及危害度分析程序》（1967 年）等军用标准，将可靠性正式列为军用产品质量指标。可靠性工程的研究从电子设备扩大到各种军用设备，开始研究机械可靠性问题。美国“阿波罗”计划大大推进了可靠性工程的全面发展，促进了元器件可靠性提高和可靠性设计技术进步。AGREE 的成果在“民兵”导弹及军用雷达等装备中得到应用。1960 年，美国海军研究生院成为第一个讲授可靠性工程的机构。1961 年，美国空军罗姆航空发展中心（RADC）推出失效物理

(PoF)计划,以研究解决军用设备复杂度增加和故障数上升的问题,并且在1962年召开了第一届电子设备失效物理年会,正式确定失效物理的概念。1962年,美国空军技术研究院成为第一个授予可靠性工程硕士学位的教育机构。到20世纪60年代后期,美国40%的大学都开设了可靠性工程方面的课程。

20世纪70年代,可靠性工程步入成熟阶段。随着洲际导弹、航空航天系统、原子能系统、电力系统、交通运输系统和武器装备系统的出现及性能提升,对可靠性提出了更高的要求,基于全寿命周期的可靠性设计、试验、分析、评估及可靠性控制的理念逐渐形成,并提出有效对策和措施。提出计算机辅助可靠性设计的概念,研究设备可靠性预计的软件包。研究非电子设备的可靠性设计与试验方法,1977年和1978年先后成立机械设备可靠性设计及可靠性试验研究组织,研究机械设备的可靠性,制定相应的设计程序和试验程序。在可靠性试验中采用综合环境应力试验,加强环境应力筛选,发展可靠性增长试验。1978年,颁布MIL-STD-1635《可靠性增长试验》。由于软件可靠性问题日益突出,1978年,美国成立三军软件可靠性技术协调组,负责国防部范围内的软件可靠性研究。1974年,美国原子能委员会利用故障树分析方法评价故障的工作引起世界各国重视。

20世纪80年代,可靠性工程向着更深、更广的方向发展。在管理上,加强集中统一管理,强调可靠性及维修性管理制度化,在技术上深入开展软件可靠性、机械可靠性研究,全面推广计算机辅助设计(CAD)技术,积极采用模块化、综合化、容错设计、光导纤维和超高速集成电路等新技术来提高武器系统可靠性。维修性工程得到军方重视,与可靠性工程的发展并驾齐驱。80年代初,美国国防部首次颁发指令DOD-D5000.40《可靠性及维修性》,把武器装备采办中的R&M管理以国防部指令的形式加以规定。80年代中期,美国空军制定R&M2000年行动计划,提出2000年要将空军装备可靠性水平"翻一番",将维修时间减少一半,通过提高R&M实现提高战斗力、降低战斗保障设施的易损性、减少运输要求、减少人力、降低费用等5项目标。

20世纪90年代以来,可靠性成为与性能、费用和时间同等重要的指标。计算机技术突飞猛进的发展,使得可靠性CAD技术与综合化得到广泛应用。可靠性的一些传统概念得到新的认识。例如,根据传统可靠性概念,设计原因引起的故障只要在允许范围之内,往往无需追溯到最终根源;制造过程导致的故障,只要仍低于许可的故障数也就不被追究。1995年传统可靠性定义受到质疑,随机失效无法避免的旧观念受到摒弃,(在欧洲)开始用无维修使用期(MFOP)取代平均故障间隔时间(MTBF)的概念,故障率浴盆曲线分布规律也被打破。国际上兴起在可靠工程中推行失效物理方法的新潮流,如马里兰大学(1990年)主张用PoF方法进行可靠性评价,美国陆军装备系统分析活动中心(AMSAA)(1993年)指出可用PoF方法解决MIL-HDBK-217的不足之处。1998年,美国国防部实施采办改革,推行军民融合以最大程度地利用民用产品和管理。采办改革唯一的可靠性要求是系统应该在研制项目结束时通过使用试验;可靠性增长试验和前端的设计可靠性工程不再作为最佳惯例加以要求;MIL-STD-785B被取消,但MIL-HDBK-189仍起作用。这些改革最终造成了一系列不良后果。

2000年以来,可靠性工程科学的理论基础、技术体系以及配套的管理和教育机构相继确立,并向更广义的方向发展,提出基于性能退化的可靠性技术、基于(可靠性与性能一体化的)功能的可靠性技术。失效物理技术得到深入,2008年,可靠性信息分析中心(RIAC)出版《微电子系统失效物理手册》,成为失效物理技术的重要里程碑。但在系统级失效物理分析仍存在很多挑战[23]。软件可靠性理论研究正在向工程应用过渡,人的失误及其可靠性的研究成为多学科交叉渗透、面向21世纪的重点研究领域,可靠性技术出现智能化、一体化趋势。鉴于防

务官员在武器系统寿命周期中对可靠性重视不够，致使越来越多的系统在关键的适用性试验中遭遇失败，2008 年 12 月 2 日，美国国防部负责采办、技术和后勤的国防部副部长约翰·杨批准了 DOD－D5000.2《防务采办系统的运行》的修订版本，其中将可靠性作为一项重大复兴工作，将国防部采办过程中“可靠性增长”和“可靠性最佳惯例”制度化。

我国的可靠性工程的发展主要分为起步阶段（20 世纪 60 年代）、兴起阶段（20 世纪 80 年代）和发展阶段（20 世纪 90 年代）。60 年代，可靠性技术首先在电子、航天、航空等领域兴起。80 年代，针对现役和在研装备所暴露出的具体可靠性问题，分别进行攻关突破，在装备的定寿延寿、维修改革等方面取得显著成绩，可靠性工程在“运七”飞机、“教八”飞机、“十号工程”、“东风”31 等航空航天项目的成功应用，带动了可靠性工程在军品其他领域的全面推行，但尚未形成能够指导可靠性工程的系统的理论体系及管理机制。随着 1985 年科六字 1325 号文《武器装备可靠性工程的若干规定》的发布，我国军品可靠性进入有法可依的阶段；1988 年，GJB 450—1988《武器装备可靠性通用大纲》以及后来一系列可靠性军标的强制推行，使我国军品可靠性逐步进入有章可循的阶段。90 年代，随着可靠性理论框架的建立及高层领导的重视，可靠性工程开始进入发展阶段。1991 年，原国防科工委发出了《关于进一步加强武器装备可靠性、维修性工作的通知》，强调各级领导必须转变观念，把 R&M&S 放到与性能同等重要的位置，树立以提高武器装备效能、降低寿命周期费用为目标的现代质量观。1993 年，原国防科工委发布了《武器装备可靠性维修性管理规定》。上述顶层文件从管理层次上极大地推动了装备 R&M&S 工作的开展，使我国装备研制中的 R&M&S 工作逐渐进入了系统化、规范化的全面发展时期。可靠性工作也是从“九五”期间开始进入预先研究计划的。相对于军品领域来说，我国民品领域的可靠性工程起步较晚，改革开放和市场经济给民品企业带来了新的机遇和挑战，残酷的市场竞争迫使各企业不得不在质量和可靠性方面增加人力和资源的投入，在借鉴军品可靠性工程经验的前提下，民品可靠性工程取得了长足的进步。

1.3 典型复杂系统可靠性建模与分析问题

现代科学技术的发展，以及大工程、大项目、大科研问题的出现，导致系统的复杂性不断增加，系统可靠性的描述和分析越来越困难。从可靠性工程角度，系统可靠性建模与分析问题的复杂性来自两个方面，即系统自身结构和失效机理的复杂性以及待解决的系统可靠性问题的复杂性，二者既有联系，也有区别。前者主要指系统可靠性行为特征描述的困难，如系统可靠性度量和系统可靠性建模困难。很多复杂系统具有多任务、多功能以及多阶段、多状态特点，而且常常遇到可靠性定量特征不明显、难以量化问题。在系统可靠性建模方面，相关失效、共因失效、负载分担、竞争失效、非单调性以及冗余（硬件、软件）、容错、重构、重组、覆盖性、恢复性等，是现代复杂系统的典型可靠性行为，经典的可靠性模型难以对这些行为进行有效描述和处理。待解决的系统可靠性问题的复杂性主要体现在如何满足客户对长寿命、高可靠的更高期望，如何适应新技术/新材料的变化，如何满足产品快速研制需求以及如何解决小子样、无失效情形下的可靠性建模、试验、分析和评估等问题。

下面通过一些案例，主要从系统自身结构和失效机理的复杂性角度，说明典型复杂系统可靠性建模与分析问题的特点。

1. 多功能多任务系统——可靠性指标体系问题

现代复杂系统的一个典型特点是具有多功能和多任务特性。对多功能多任务系统，系统

可靠性度量存在定量特征不明显、难以量化的困难。一般来说，需要根据系统功能和任务要求，建立系统可靠性指标体系，才能比较全面地度量系统的可靠性。

惯性约束聚变激光装置（ICF）[10]是典型的多功能、多任务系统，其可靠性指标体系的建立必须考虑试验类型、光束数量及其配置、光束入射角度和性能（能量、脉宽、功率、波长等）要求等问题。具体如我国的“神光”Ⅲ主机装置，需要进行间接驱动物理试验、平面靶物理试验和直接驱动物理试验等多种类型的试验，不同试验有不同的要求。有些试验（如器件试验）只需要1路光束，有些试验可能需要2路光束或全部光束（如聚变试验）；有些试验需要每束光的能量达到设计要求，有些试验只要求能量达到设计的50%或75%。此外，对打靶可靠度的概念进行限制，即将是否达到规定的性能参数要求和是否收集到诊断数据，修改为打靶前经过检测，确定是否能够达到规定的性能参数要求和是否能够收集到诊断数据，则又得到打靶可用度的概念。进一步地，对于ICF这样的多层次、多部件复杂系统，还可以在装置各系统、组件、模块、元器件层次定义类似的可靠性指标。

由此可见，在描述复杂系统多个方面的综合性能方面，经典可靠性概念显然是不够的。可信性和完成性等概念的提出[22]，为解决多功能、多任务系统可靠性指标体系问题提供了一条可行途径。可信性描述了与生存性（如质量、可靠性、维修性等）和安全性有关的一个或多个属性的综合。这些属性相互关联，并受到产品或系统的原材料、制造、技术、工艺、生产过程及其控制、使用方式等的影响。从可信性和成本效率两个方面考虑，可实现产品、系统或服务的部分优化设计。这是因为，此时产品、系统或服务的最优设计一般是在费用约束（有时也考虑其他技术经济约束）下对可信性进行优化；在产品或系统的最优设计或最优配置中，较少考虑材料和能源需求、废物产量、工艺流程以及可处置性等的影响。完成性是反映产品、系统或服务的所有性能的综合属性，包括可信性和可持续性两个方面。后者反映了现代工业生态的概念，用于描述非物质化、能源审计、废物最小化、重复使用和循环使用以及其他方面的环境考虑，关注于降低环境影响和可持续性发展。目前，完成性概念在卫生保健部门、结构工程、通信工程、计算系统（如网格计算）、故障容错系统、预测和健康监控、基础设施维护、电力系统重组、核电厂概率风险评估以及软件工程中，都具有明确需要并发挥了重要作用[26]。图1-3是文献[22]所描述的完成性概念体系，其中可信性是完成性的组成部分。

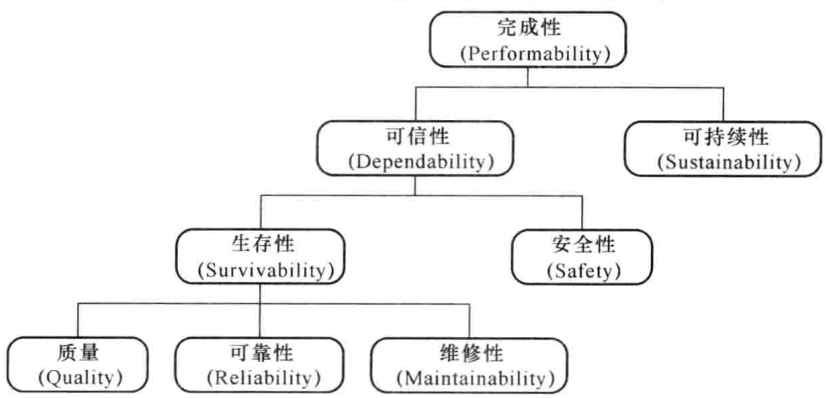

图1-3　完成性概念[22]

这里需要提及的一点是，完成性最初是包含在可信性概念范畴之中的。完成性的概念最早是1980年John Meyer为评价NASA所使用的航空器控制计算机的性能所提出的，当时主要用于反映可靠性以及其他有关属性，如可用性、维修性等的组合属性。目前计算机系统性能评

估仍然采用这一概念描述[27,28]，即认为完成性是描述系统失效－维修行为以及系统所能提供的性能的综合概念。本书将不对这些概念问题进行区分和规范，仅通过有关例子说明这些概念在系统可靠性评价中的具体应用及其求解方法。

2. 阶段任务系统——动态性和相关性问题

航天、核电及其他很多应用中，常常包含需要顺序完成的几种不同的任务或任务阶段。完成这些任务的系统称为阶段任务系统(Phased－Mission System，PMS)。一个典型的 PMS 的例子是飞行器的飞行任务，包括起飞、爬升、巡航、降落和着陆等几个阶段。在每个任务阶段，系统需要完成一个特定的任务，可能遭受不同的应力并满足不同的要求。因此，不同阶段系统配置、成功准则、部件失效行为可能发生变化。在可靠性分析中，分析这种动态行为通常需要为每个任务阶段定义不同的模型。使分析进一步复杂化的是，某些部件在不同阶段之间的失效具有统计相关性。例如，在不可修 PMS 中，一个部件的状态在新阶段开始时与其在前一阶段结束时的状态是相同的。这些动态行为和相关性对目前方法提出了独特的挑战。

下面以 TT&C 系统运行过程为例进一步说明 PMS 的特点[21]。由于卫星地面站的位置是固定不变的，航天器绕地球轨道运行，在地面站和航天器之间存在可见时间窗口约束。分布在不同区域的地面站具有不同的可见时间窗口，因此不同部件的任务开始和结束时间可能是不同的，这导致部件组合以及系统配置和逻辑在不同时间区间内的变化。图 1－4 是一个简单的 TT&C 任务过程，其中涉及 A、B、C 共 3 个部件。两个地面站 B 和 C 要求在其可见时间窗口 $[t_0,t_2]$ 和 $[t_1,t_3]$ 执行对航天器的 TT&C 任务，一个控制中心 A 要求在整个时间区间 $[t_0,t_3]$ 内运行，以便保证对数据的有效管理和处理。该 TT&C 可用故障树模型表示；根据图 1－4(a)所示可见时间窗口的时间点，该故障树模型被划分为 3 个时间连续、长度固定、不重叠的运行阶段。因此，此 TT&C 是一个阶段任务系统：整个任务的完成需要系统在所有阶段成功。在可靠性逻辑中，阶段 2 与阶段 1 和阶段 3 是平行的，因为它对应于地面站 B 和 C 的重叠的可见时间窗口。假设每个部件只有完好和失效两个状态，系统将处于以下几种状态之一：

(1) 所有部件完好，从而任务成功。

(2) 某个部件失效，但是不影响任务的执行，失效的部件将在随后修复。例如部件 C 在阶段 2 失效并在阶段 3 开始时修复。

(3) 一个或多个部件失效，并导致任务失败。

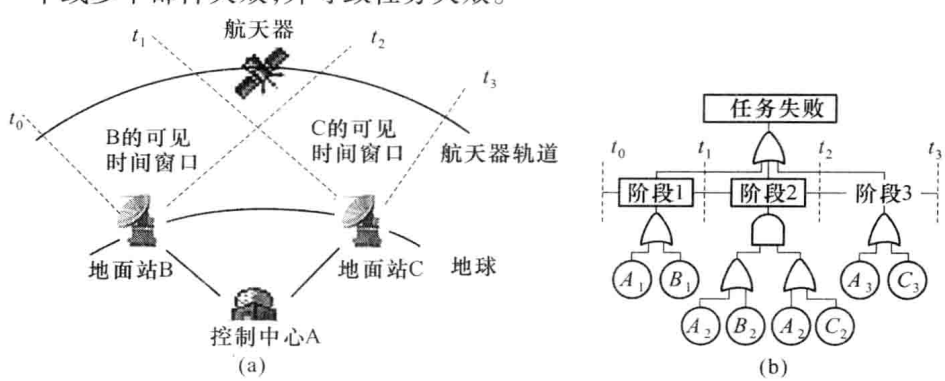

图 1－4　TT&C 任务过程[21]

说明：A_i，B_i，C_i 表示对应部件在阶段 i 失效

PMS 系统可能比较简单，如上述 TT&C 系统，也能非常复杂，包含维修、非单调、任务选择/组合等行为[22]。

3. 随机劣化系统——多状态问题

在传统可靠性分析中，系统及其部件一般假设只有两种状态：正常工作和完全失效。这一假设简化了可靠性模型和分析的方法，但是难以反映大多数系统的实际情况。现实世界的很多系统是由多状态部件构成的，即系统及其部件允许取两种以上的状态。这些部件具有不同的性能等级或多种故障模式。比如，计算机系统中处理器可分为完全工作、部分工作、部分故障和完全故障等几种性能等级；以美国陆军为首的一些部门和专家把地面武器装备的任务状态划分为能圆满完成任务、在规定时间内排除故障后能完成任务、能完成任务但性能降低、不能完成任务以及不能完成任务且失去机动能力等五种；网络中的继电器、弹头的保险系统、二极管电路、阀门等具有开路和短路两种失效模式，并且不同失效模式对系统整体性能的影响不同。这样的系统称为多状态系统（Multi - State System，MSS）。由于多状态之间的状态转移、互斥等，以及部件状态对系统的影响，MSS 的可靠性分析比两状态系统复杂得多。

以卫星系统为例，根据所获得的数据将卫星结构划分为姿态控制、传动杆/天线、控制处理器、机械系统/结构系统/热控系统、有效载荷/放大器/在轨数据/计算机/接收机、电源系统、遥感跟踪与控制等 13 个子系统[9,17]。一般来说，卫星在轨运行过程中不会突然完全丧失功能，因此卫星的性能或功能是逐渐退化的，根据性能损失程度将卫星状态划分为四种，运用多状态失效分析的结果可更加全面地反映卫星的可靠性：

（1）可运行状态：性能损失 0 ~ 5%。

（2）小幅退化：性能损失 5% ~ 35%。

（3）大幅退化：性能损失 35% ~ 85%。

（4）失效状态：性能损失 85% ~ 100%。

假设系统性能完全由其部件（或子系统）性能决定，即子系统功能/性能随时间的退化导致卫星功能和性能处于不同等级。根据对卫星的影响程度，对子系统发生的异常事件进行划分，可以归纳为四种水平的异常事件：

（1）Class Ⅰ：由于子系统失效引起卫星退役。

（2）Class Ⅱ：影响卫星或子系统运行的严重不可修失效。

（3）Class Ⅲ：对卫星或子系统运行造成备份损失的严重不可修失效。

（4）Class Ⅳ：小幅、暂时、可修的失效。

考虑到子系统还存在完全正常的状态，因此对子系统可定义五种状态，即状态 5（完全正常）、状态 4（发生 Class Ⅳ事件，部分失效）、状态 3（发生 Class Ⅲ事件，部分失效）、状态 2（发生 Class Ⅱ事件，部分失效）和状态 1（发生 Class Ⅰ事件，完全失效）。

用 Petri 网表示的子系统状态和状态转移规律如图 1 - 5 所示。其中，T_{ij}表示状态 i 到状态 j 的状态转移，通过历史数据获得子系统状态转移概率，就可以通过马尔可夫链或者随机 Petri 网模拟来分析子系统的多状态失效行为。

为分析卫星系统可靠性，根据观测数据和历史经验，可建立卫星状态与各个子系统状态之间的联系规则如下：

（1）所有子系统处于正常状态，则系统正常。

（2）有一个子系统发生 Class Ⅰ异常事件，则系统失效。

（3）子系统发生 Class Ⅲ、Ⅳ异常事件，对系统级的状态无直接影响。

（4）子系统出现 Class Ⅱ异常事件，则系统以一定概率出现小幅退化、大幅退化或失效。

据此可获得卫星的随机 Petri 网模型，如图 1 - 6 所示，其中引入一个中间层使模型更易理

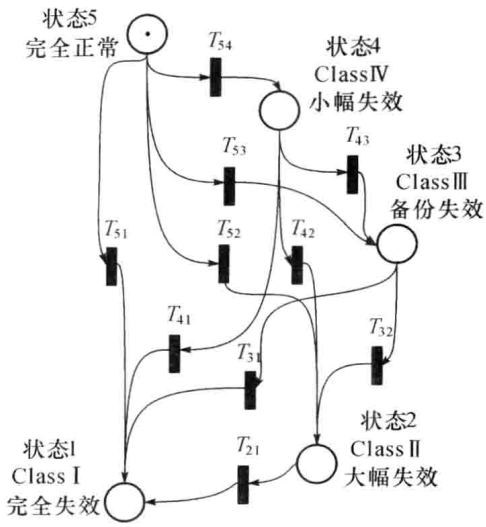

图 1-5　子系统五种状态和状态转移

解[17]，同时也是为了说明各子系统对整星影响程度的差异。例如，与卫星动力有关的系统一旦发生大幅退化，则整颗卫星就会完全失效；但是通信系统大幅退化则很可能不会导致卫星完全失效，这通过引入中间层的位置和转移来表现子系统对系统的影响程度。

4. 故障容错系统——高可靠性问题

计算机技术和体系结构技术的发展，以及不断增加的 VLSI 复制、大规模并行和网格化处理、大规模分布式系统，极大推进了故障容错设计的进步。故障容错的目标是保证在故障发生时系统仍能提供正确服务，即系统具有高可靠度。建立故障容错能力的基本思想是为系统提供冗余资源以便克服故障的影响。为了达到预期的可靠性，空间飞行器、核电厂等的操作系统、应用程序、控制系统、通信系统都大量采用冗余措施，因此都可以称之为故障容错系统（Fault Tolerant System，FTS）。

在故障容错系统中，一个系统通常提供一种以上水平的服务质量，故障可能导致服务质量的降低，不过服务仍然保持在满意的程度。这种退化也可能是由于额外的计算需求所致，如源自错误处理过程，或源自与故障有关的活动如系统重构或重组。这方面的一个例子是计算机集群中的节点失效导致性能下降甚至服务的暂时中断。重构是冗余系统的一个必然特征，如卫星姿态控制系统中飞轮运行模式的重新配置。此外，系统降级运行也涉及到系统结构和功能的重构。因此，故障容错系统一般具有多功能、多任务、多状态、可重构的特点。

故障容错可以通过硬件冗余或软件实现。典型的硬件冗余结构包括故障屏蔽和备份两种方式。故障屏蔽又称被动冗余，其中使用许多复制品实现对单个或多个故障的屏蔽，如三模块冗余（TMR）、N 模块冗余（NMR）、自净化冗余。其中，TMR 可以容错单个失效，且可同时提供对参与模块的“健康”预警。

波音 777 飞行控制系统[24]是一种电传系统（Fly - by - Wire，FBW），该系统所有硬件，包括计算（机）系统、电力系统、液压动力、通信路径等都采用三模块冗余。主飞行计算机（PFC）是 FBW 系统的中心计算部件，PFC 的体系结构也是基于 TMR 设计的，如图 1-7 所示。

备份又称动态冗余，通过一个主模块提供所需服务，另有一些在线或离线的备件提供备用服务。主模块失效后，第一个备用模块承担其任务并成为主模块，依次类推。失效模块不再发挥任何作用。为实现这种故障容错策略，基本的步骤包括故障检测、重构和恢复。在计算系统