国防科技工业质量与可靠性专业技术丛书

任立明 主编

潜在电路分析技术与应用

QIANZAI DIANLU FENXI JISHU YU YINGYONG

国防工业出版社
National Defense Industry Press

国防科技工业质量与可靠性专业技术丛书

潜在电路分析技术与应用

任立明　主编
张　亮　许　皓　张云中　副主编

国防工业出版社
·北京·

内 容 简 介

本书是《国防科技工业质量与可靠性专业技术丛书》之一，在介绍潜在电路分析技术的基本概念和原理及其国内外发展概况的基础上，重点讲述了规范的潜在电路分析方法，对其中的重要分析工具——网络树和线索表进行了详细的讲解。为体现全面性，本书还对此项技术涉及的软件潜在分析、IC 器件电路潜在分析、潜在电路分析软件工具和潜在电路分析项目的管理等方面进行了阐述，同时给出了潜在电路分析技术的工程应用案例，对读者起到了理解概念、掌握方法、工程化规范使用潜在电路分析技术的示范作用。

本书可为国防科技工程技术人员、质量与可靠性专业人员及各级管理人员开展潜在电路分析工作提供技术支持，也可作为该项技术的学习参考用书。

图书在版编目(CIP)数据

潜在电路分析技术与应用／任立明主编. —北京：国防工业出版社，2011.8
（国防科技工业质量与可靠性专业技术丛书）
ISBN 978-7-118-07449-9

Ⅰ.①潜… Ⅱ.①任… Ⅲ.①计算机辅助电路分析－研究 Ⅳ.①TN702

中国版本图书馆 CIP 数据核字(2011)第 172102 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）
北京嘉恒彩色印刷有限责任公司印刷
新华书店经售

*

开本 710×960　1/16　印张 12½　字数 212 千字
2011 年 8 月第 1 版第 1 次印刷　印数 1—5000 册　定价 36.00 元

国防书店：(010)68428422　　发行邮购：(010)68414474
发行传真：(010)68411535　　发行业务：(010)68472764

丛书前言

“质量是企业的生命”，是技术水平和管理水平的综合体现。提高产品质量水平，是加快转变经济发展方式的重要途径和必然要求。对于武器装备，质量关系型号成败，关系战争胜负，关系国家安危，“保质量就是保安全、保战斗力、保胜利。”

依靠先进技术和科学管理保证和提升质量，是我国国防科技工业质量工作的基本规律和有效经验。《武器装备质量管理条例》也明确规定，“国家鼓励采用先进的科学技术和管理方法提高武器装备质量”。特别是在武器装备机械化信息化复合式发展的新形势下，装备技术指标更高、系统更加复杂、软件更加密集、风险更难控制，对质量与可靠性技术的需求更大、要求更高。

为促进先进质量与可靠性技术方法在型号中的有效应用，在国防科技工业主管部门的指导和支持下，国防科技工业质量与可靠性研究中心牵头，在2003年编辑出版了包括统计过程控制，软件质量管理，危险分析与风险评价，故障模式、影响及危害性分析与故障树分析，元器件使用质量保证在内的《国防科技工业质量与可靠性专业技术丛书（第一批）》。为适应新形势和新任务的需求，又有针对性地遴选了潜在电路分析、概率风险评价、质量功能展开、六西格玛管理、健壮设计等五种技术方法，编辑形成了丛书的第二批书目。

新出版的这一批书目集中了五项行之有效的质量与可靠性技术方法，凝结了国防科技工业质量理论研究和工程实践的最新成果，对于促进先进技术推广应用、提高全员质量技能具有十分重要的意义，可为国防科技工业广大技术和管理人员开展质量工作提供技术支持，也可作为各类人员学习的参考用书。

考虑到丛书编写时间和资源有限，而且一些技术方法的研究和应用仍需继续深化，所以难免有不足和尚需完善的地方，欢迎广大读者提出宝贵意见。

《国防科技工业质量与可靠性专业技术丛书（第二批）》编委会

二〇一一年六月

《国防科技工业质量与可靠性专业技术丛书(第二批)》
编 委 会

前　言

潜在电路分析(Sneak Circuit Analysis,SCA)技术最早由美国波音公司提出。1967 年底,美国国家航空航天局(NASA)为了保障“阿波罗”飞船和“天空实验室”的电子电气设备无故障运行,确保机组人员的安全,首次提出了事先发现并纠正电子/电气系统中潜在电路的研究任务,并通过阿波罗工程的研究和应用突破了相关技术。在 20 世纪 80 年代后,该项技术被广泛应用于航天器、军用系统以及核设施。1980 年 SCA 被列为美军标 MIL-STD-785 的工作项目之一。目前,SCA 技术已扩展应用到液(气)管路系统以及计算机软件等领域。

SCA 技术是一种重要的系统级可靠性安全性分析技术,其突出特点是通过事先分析暴露系统中存在的潜在缺陷,这些缺陷与低层次部件或器件失效无关,而是一种系统设计方面的不足。这一类缺陷在复杂系统设计中具有普遍性,并且危害很大。

由于 SCA 技术的有效性,欧洲空间局(ESA)在 20 世纪 80 年代也起步开展了 SCA 技术的研究和工程实践。1997 年 ESA 出版了 SCA 方面的第一部技术标准 ECSS-Q-40-04A。

从 20 世纪 80 年代开始,国内一些科研院所、高校相继开展了 SCA 技术的研究工作,经过多年努力,取得了一些研究和应用成果,积累了宝贵的应用经验,完善了分析手段。1988 年 SCA 被列为国军标《装备研制与生产的可靠性通用大纲》的工作项目。2004 年该标准修订时保留了该工作项目,由原“潜在电路分析”扩展为“潜在分析”,包括“针对电路的潜在分析”、“针对软件的潜在分析”和“针对液(气)管路的潜在通路分析”。2005 年航天行业标准《潜在分析方法和程序》发布,成为国内关于 SCA 的第一部行业技术标准。

在 SCA 技术逐渐走出理论研究的象牙塔并在国内军工行业得到推广和应用的今天,本书总结了国内外相关研究与应用情况,试图以工程实用性、有效性为出发点,比较系统、全面地介绍 SCA 技术的原理、方法、流程、工具、项目管理以及工程应用案例。其目的是为读者开展潜在电路分析提供一本实用指南。

全书共 12 章。第 1 章介绍了潜在分析技术的背景与现状、潜在电路的表现形式与特点。第 2 章介绍了潜在分析技术的概念、原理、方法以及发展趋势。第

3章介绍了规范的潜在电路分析方法，包括数据收集、数据处理、元器件建模以及网络树生成的潜在电路分析方法。第4章介绍了网络树生成的基本技术方法。第5章介绍了潜在电路分析线索表的建立与应用。第6章介绍了简化的潜在电路分析方法，即功能节点识别、路径追踪以及综合线索表的路径分析方法。第7章给出了在基本电路、通用电路拓扑结构、功能电路、元器件以及航天行业专用电路等设计中避免潜在电路的指导性原则。第8章介绍了IC器件电路相关的潜在问题及其分析方法。第9章介绍了软件潜在分析技术发展的背景、基于功能节点识别和路径追踪的分析方法。第10章介绍了潜在电路分析项目管理有关考虑及工作流程，包括应用对象与任务承担方的选择，项目实施的时机与计划，项目的协调、监督与评估等。第11章介绍了潜在电路计算机辅助分析系统以及网络树的计算机辅助生成方法。第12章介绍了潜在电路分析技术工程应用案例。

书末附录A、B、C分别给出了潜在电路分析任务书、数据要求、分析报告简表的样式，供SCA工程应用实践中参考。

本书由任立明担任主编，并负责第1章、第2章的编写以及全书的策划和最终统稿工作。张亮和许皓编写第3章～第6章、第10章、第12章，张云中编写第7章、第8章，周新蕾编写第9章，胡冰编写第11章。张云中负责全书的校对工作。

本书编写过程中得到中国航天标准化与产品保证研究院卿寿松院长、顾长鸿副院长，以及航天领域严殿启、邵德生、邱邦清等专家的大力支持，可靠性研究所很多同志为本书的出版，在图表绘制、编辑、电子文档录入等方面做了大量工作，在此一并表示衷心感谢。

由于时间仓促，水平有限，本书存在疏漏和错误在所难免，恳请读者批评指正。

编　者

2011年4月

目　录

第1章　潜在电路的概念和特点

1.1　引　言

可靠性工程从其诞生开始就强调一个基本的因果关系，即：较低层次部件的失效会导致较高层次部件或系统的失效。以此进行反向逻辑思维，系统的失效或故障一般可以追溯到较低层次部件的故障。由此推论，发展了一系列“与低层部件的故障作斗争”的可靠性工程技术，例如可靠性预计、可靠性分配、故障模式及影响分析、故障树分析、失效分析等。可靠性预计是以低层次部件（例如元器件）的失效率预计产品的失效率；故障模式影响分析，是分析低层次部件故障对较高层次部件的影响；失效分析是以低层次部件（例如元器件、材料）的失效机理作为研究对象，试图揭示产品的失效规律。

但是，随着现代化的电气电子系统的技术和功能的复杂性越来越高，人们逐渐发现，复杂系统现场出现的故障在很多情况下很难追溯到低层次部件的失效或故障。根据对国内外运载火箭发射统计数据，运载火箭在发射场出现的现场故障只有不到10%可以明确归结到元器件或低层次部件的失效或故障，而由于非器件失效原因导致的系统故障一直居高不下，如设计不合理、接口故障、制造环节误差、环境条件超标、电磁兼容问题等，当然也包括很多设计人员所不熟悉的“潜通路”问题。在国外文献中，对这一大类由于未考虑到大系统功能和结构的复杂性特点而导致的系统故障，统统将其原因归结为“设计错误”或“设计缺陷”。

对于工程设计人员而言，往往难于认识到复杂系统的故障其背后的真正原因是“设计错误或缺陷”。在故障发生的第一时间、第一现场，人们总是习惯于寻找低层次部件失效这一“元凶”。作为系统的设计者，承认由于设计团队的失误或疏忽导致系统存在未曾认识到的“系统级故障模式”，不仅需要对系统故障机理认识观念上的转变，也需要一定的勇气。尽管这是系统的“复杂性”所导致的必然结果，但这并不意味着设计人员可以就此脱逃干系，因为复杂系统也是人设计的，对系统的复杂性进行充分的分析和识别，还是有可能预防或防范此类系统级故障发生的。

事实上，所有具有复杂功能和结构的系统较普遍地存在此类设计错误或缺陷。据统计，国外卫星型号从总装、集成和测试环节开始到卫星在轨运行的故障统计数据中，约有30%的系统级故障的最终原因为设计错误或缺陷。根据对世界上五个商业运行的核电站系统的数据调研，其安全事故记录中，约有25%的安全事故的最终原因是“设计错误或缺陷”，占第一位，其次的原因分别是：部件失效(18%)、操作失误(12%)、操作规程错误(10%)、不明或未记录的原因(12%)、生产环节错误(1%)等，见图1.1。可见“设计错误”问题，即由于设计人员考虑不周造成的系统故障问题，是复杂系统研制中必须予以重视的问题。

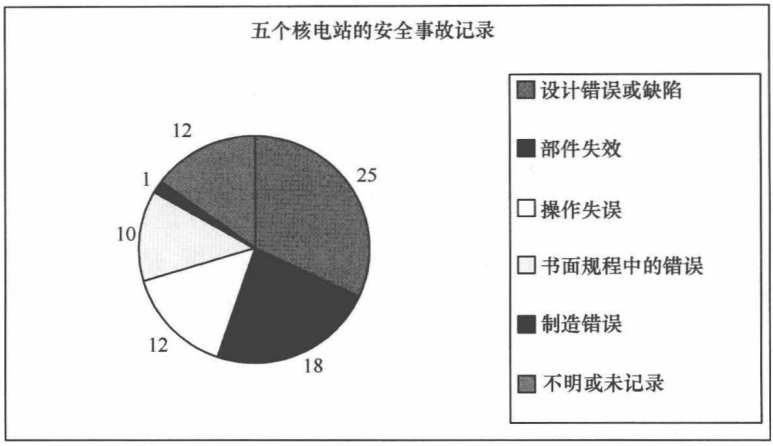

图1.1　导致核电站安全事故的原因分布

潜在电路(俗称潜通路)问题，就是上面所述的系统级故障模式的一种，是由于设计者对于系统的复杂性把握不够引入的一类设计错误或缺陷。由于潜在电路的存在，许多系统在没有低层次部件失效的情况下，出现了系统级的故障，系统不能正常运行。典型的表现是系统不能完成所期望的功能，或者激励了非期望的功能。在现代武器装备系统中，这样的问题可能产生危险的、甚至灾难性的后果。例如，由于未检测到的设计错误，在正常测试操作中可能导致导弹误发射。

这类非期望事件的主要起因是“潜在电路”，即在一定的条件下存在的一条非期望的路径或逻辑流，其出现会导致非期望的后果或者使期望的结果被抑制。潜在路径可以存在于硬件或软件中，存在于操作员操作中，或存在于这些元素的一些组合中。与系统中元器件发生物理失效的情况不同的是，这里是“没有故障”的情况，即虽然所有的部件都符合设计要求，但却产生了非期望的效果。

1.2 潜在电路案例

为讲清楚潜在电路的概念，我们首先从历史上一个著名的航天发射事故案例说起。

1960 年 11 月 21 日，美国著名的“红石”火箭在发射场整装待发，准备发射“水星”号无人飞船。发射指令下达后，火箭点火，但火箭刚离开发射台几英寸，发动机竟莫名其妙地熄火了。火箭落回发射台，“水星”号座舱被弹出，打开了降落伞。火箭虽然只受到轻微损伤，但这样一枚极易爆炸的火箭完全失控地竖立在发射台上，飘荡着的“水星”号座舱降落伞随时有把火箭撞倒的危险。在蓄电池耗尽、液氧完全蒸发之前的 28h 内，没有一个人敢靠近它。

事后对本次事故的调查发现，是由于控制插头比尾插头晚脱落 29ms，意外激发了一条潜在电流路径，使得“红石”火箭刚点火又立即关掉了发动机，导致发射失败。

图 1.2 为“红石”火箭助推器的点火控制电路图。该图画出了含有潜在路径的地面设备和火箭设备有关部分的电路。

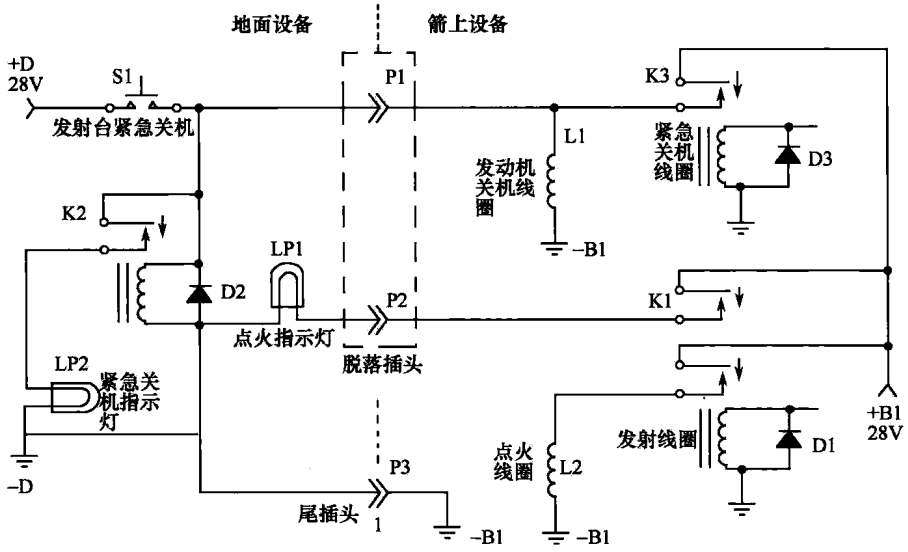

图 1.2 “红石”火箭助推器的点火控制电路简图

正常的发射顺序是：发射命令下达后，K1 触点闭合，使电池 +B1 给火箭点火线圈以及地面设备的“点火指示灯 LP1”供电。然而，如果发射过程中，连着接地返回点 -D 和 -B1 的“尾插头 P3”在“脱落插头 P1、P2”分离之前分离，则流

经“点火指示灯”的电流会继续流经二极管并且给“发动机关机线圈 L1”供电。而很不幸的是,在本次发射中,由于尾插头比脱落插头意外地早脱落 29ms,这个“如果”确实发生了。

为了更容易地暴露出其中的潜在电路,按“供电点在上、返回点在下”布图规则将图 1.2 的电路图重画成图 1.3 的“网络树”的形式。从图 1.3 中很容易看出:当“尾插头 P3”断开而“脱落插头”闭合的情况下,存在一条流经“K1”、“点火指示灯 LP1”、“D2”、“发动机关机线圈 L1”的电流路径。而正是由于这条路径的存在,激励了“发动机关机线圈 L1”,导致火箭刚起飞就关机的严重后果。

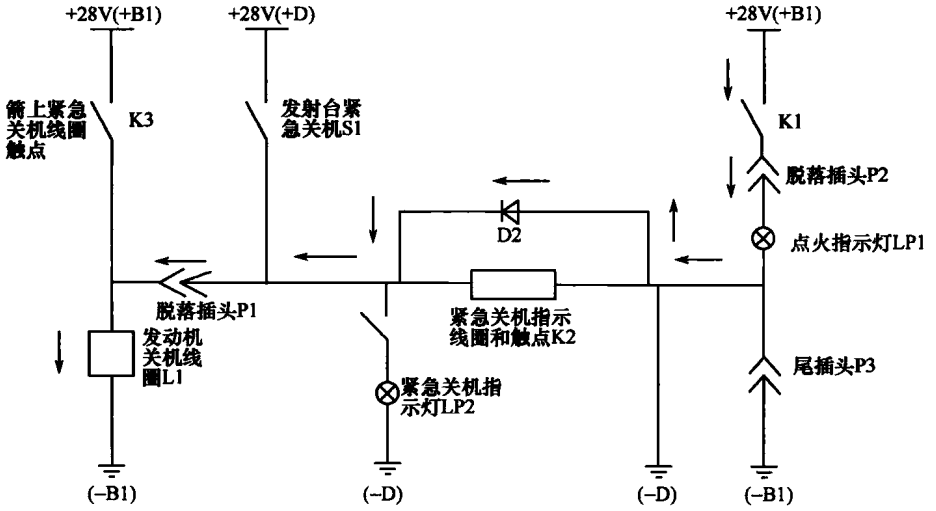

图 1.3 “红石”火箭助推器的点火控制电路的网络树图

从美国“红石”火箭事故之后,美国的航天专家们逐步认识到,这是一种完全不同于此前部件级故障或失效的系统级故障模式,并且较普遍地存在于功能和结构较复杂的电气电子系统中。其显著的特点是其“潜伏性”,因此命名为潜在电路(Sneak Circuit)。由于缺乏对其“潜伏性”的预见,一般对其发生没有任何防范措施。在“红石”事故中,正是由于根本没有预见到刚起飞发动机就可能关机这种后果,致使事故发生后无法采取任何补救措施(传递地面控制信号的 P3 插头已脱落)。在发射后的二十几个小时内,无法采取措施或派人靠近火箭处理事故,直至液氧液氢全部蒸发、箭上电池耗尽。这一案例充分说明了潜在电路的巨大危害性。

中外航天、航空、航海、核工业等领域由于潜在电路导致事故的案例不胜枚举,造成的后果大部分都很严重。

国外典型的案例包括：

（1）“阿波罗”四号飞船在紧急中断发射程序的过程中，由于激发了潜在电路，意外地点燃了宇航员使用的氧气而导致3名宇航员死亡；

（2）土耳其航空公司一架DC－10飞机，由于飞机舱门系统存在潜在指示，意外激发了一条潜在路径，导致飞机在法国伊门诺威尔上空坠毁；

（3）停在场坪上的B－52轰炸机意外地“激活”一枚导弹；

（4）核弹头被非期望地打开保险；

（5）飞行中执行勤务的喷气式飞机漏电，直至蓄电池耗尽也未向机组人员做任何告警。

国内航天领域近40年的导弹、运载火箭、卫星、飞船的研制、试验和发射过程中，也发生过由于潜在电路而导致的故障或事故案例，例如：

（1）某火箭发动机火工品误爆事故；

（2）某导弹平台飞转事故；

（3）某导弹不点火自毁事故；

（4）某运载火箭程序配电器误归零故障。

上述案例充分显示了潜在电路对军工产品的巨大危害。在低层次部件和元器件质量可靠性水平不断提高的今天，研制人员了解和掌握潜在电路分析技术，可以有效地发现此类与部件失效无关的系统级失效模式，工程应用需求十分迫切。针对实际设计和使用状态，对军工重点型号影响安全性和任务成败的系统进行潜在电路分析，具有重要的现实意义。

在非军工领域，也同样发生过由于潜在电路被激发而导致不良后果或隐患的案例，例如：

1）家用供电系统

在图1.4所示家用供电电路中，W_A、W_B、W_C分别是输配电变压器的次级线圈，各相相电压额定值是127V，线电压额定值是220V。设计采用三相供电，线电压为220V，各负载正常工作，三相二次线圈负载基本平衡。

当该电路中B相保险F_B烧断后，会出现如图1.4中虚线所示的潜在通路，导致的直接后果有两点：一是负载供电发生了改变，即负载L_{A-B}和L_{B-C}供电发生了变化，其两端电压将由设计的220V额定值，大幅下降，发生降压供电，负载不能正常工作；二是原先设计的输配电变压器次级线圈的平衡供电被打破，B相线圈空载，而A、C两相发生过载，可能直接导致变压器工作不正常或发热严重而烧毁。

2）汽车和拖挂车的灯系系统

汽车和拖挂车的灯系，也存在潜在电路问题，可能影响行车安全。图1.5给