第1章 绪论

1.1 可靠性概率风险评价的意义

可靠性技术的研究对于保障安全生产，推动产品结构优化和性能改进，提高系统的运行可靠性、安全性和可维护能力，促进制造科学发展具有重要的意义。在我国，由设备可靠性问题造成的安全事故不断发生，据各种不完全统计，制造行业中每年由于安全方面不完善所引起的人员伤亡事故就有上千起。在发生的各类事故中，处在前三位的是机械伤害(27.23%)、高处坠落(12.32%)和物体打击(10.67%)。除去由矿难所导致的人员伤害和财产损失外，由机械安全不完善引起的事故所造成的各种损失也开始受到人们的关注。

机械安全风险评价是一种最大限度地降低机械事故发生概率的方法。机械产品的安全不仅会影响人身和财产的安全，还可能造成各种贸易壁垒。由于国产机械设备在安全方面存在诸多问题，国内很多企业宁愿花大量资金去购买国外设备，同时国内机械产品也很难进入国际市场。从这些情况可以看出，我国机械行业需要对其制造的机械产品进行安全风险评价。

经过几十年的发展，我国装备制造业已经取得了令人瞩目的成就，形成了门类齐全、具有相当规模和水平的装备制造体系，装备制造业已然成为我国国民经济体系的重要支柱产业。目前我国装备制造业总产值已高于美国，远超日本，产业规模居世界第一。

虽然中国装备制造业已取得了令人瞩目的成就，成为世界瞩目的制造大国，但仍不是制造强国。目前，中国装备制造业要实现“由大到强”的转变仍面临许多问题和难题，如高端制造薄弱、自主化能力和水平不足、品牌知名度较低、关键核心技术仍未掌握、产业配套能力相对缺乏、缺乏一些具有国际竞争力的大企业以及产业可持续发展问题等。所以，中国装备制造业的发展任重道远。

2009年，工业和信息化部对我国装备制造业做出如下评述：近年来，工业产品重大质量安全事件仍然时有发生，产品质量不高已成为制约我国工业经济平稳较快发展的突出问题。此外还存在一个重要的问题就是一些企业产品质量的稳定性、可靠性较差，新产品技术成熟度不高，产品研发设计、生产制造、商品流通和售后服务阶段的质量保证能力还有较大差距。

2010年，中国工程院发布了《提高我国制造业产品质量途径的研究报告》，在装备制造

业产品质量重要特点中指出：我国装备制造业产品的性能指标优于可靠性指标，几十年来的发展，始终没有摆脱技术引进，模仿创新的模式，装备工业一直在“引进—落后—再引进”的怪圈中徘徊；与发达国家相比，还有相当大的差距。突出表现在：

(1) 产品一致性差。由于企业的设计与制造工艺不完善、监测手段不齐全、操作人员素质不高、质量监督管理不到位等原因，造成产品一致性差，这是我国装备产品的普遍性问题。

(2) 产品稳定性差。新产品研制技术水平很高，几乎所有新产品鉴定意见都写道：“主要技术性能达到国外先进水平”。可一旦批量生产，就达不到技术指标要求，严重影响用户使用和行业信誉。

(3) 产品可靠性差。在装备制造业领域，特别是高端制造业，可靠性是产品质量的核心和关键。多年来由于可靠性问题突出，产品早期故障频发，严重影响了我国产品在国内外市场中的竞争力。

盘点近三年来汽车工业由于发动机问题而召回的实例也足以证明以上观点：

(1) 大众汽车。由于燃油喷射系统密封不良，可能导致车内出现燃油异味，极端情况下，如遇火源可能导致车辆起火。大众汽车及保时捷汽车销售有限公司自 2015 年 3 月 20 日起召回大众、奥迪和保时捷等品牌汽车，共计 61046 辆。

(2) 福建奔驰。由于生产期间使用了不同材料的正时链条张紧器密封衬垫，可能导致随着发动机运行时间的增加，链条张紧器和发动机缸体之间的预张紧力下降，福建奔驰自 2015 年 1 月 27 日起，召回部分奔驰威霆 636 系列及凌特 900 系列汽车，共计 156 辆。

(3) 长安汽车。由于发动机舱保险盒电源线束端子存在装配问题，导致线束接触不良，可能引起发动机熄火或车辆无法启动，长安汽车召回 2012 年 8 月 14 日至 2013 年 6 月 5 日期间生产的长安 CS35 汽车，共计 27624 辆。

(4) 大发汽车。由于发动机传感器故障，可能导致发动机在车辆行驶当中突然停转，大发汽车公司自 2013 年 9 月 11 日起，召回 2005 年 11 月至 2010 年 6 月间生产的 892000 辆汽车。

(5) 宝马汽车。由于发动机可变气门正时机构外壳上的固定螺栓设计原因，可能松脱甚至断裂，导致发动机可变气门正时机构的密封性受到影响而发生异常或失效，宝马汽车有限公司自 2014 年 6 月 18 日起召回 232098 辆汽车。

(6) 东风汽车。由于发动机曲轴位置传感器在长期高温使用情况下，可能造成内部芯片焊点产生裂纹，东风汽车决定从 2012 年 8 月 22 日起，召回部分天籁轿车，涉及数量共计 11277 辆。

(7) 捷豹陆虎。因喷油器溢流油轨插口和喷油器溢流回油管接头之间的接合处可能泄漏柴油，捷豹陆虎公司召回 2013 年 8 月 12 日至 2014 年 8 月 31 日期间生产的陆虎神行者 2 和揽胜极光汽车共 8656 辆。

(8) 奇瑞汽车。由于发动机悬置整体设计的安全系数偏低，受到强外力冲击时，极端情况下可能会导致发动机悬置断裂，发动机下沉，奇瑞汽车自 2014 年 2 月 28 日起，召回 2009 年 9 月至 2013 年 3 月 20 日期间生产的瑞麒 X1 轿车，共计 31796 辆。

(9) 福特汽车。由于车辆油箱燃油输送模块接头长时间使用后可能会产生裂纹，存在严重安全隐患，福特公司召回 2013 年 7 月 15 日至 2014 年 6 月 30 日期间进口探险者汽车 409 辆。

在国家的若干发展战略报告及相关规划中，也对可靠性相关研究方向提出了要求。

(1) 国家自然科学基金委在2011—2020机械工程学科发展战略研究报告中：将复杂机电系统可靠性、失效评价、寿命预测、安全服役等列为重点发展和资助的领域之一。

(2) 国家“十二五”科学和技术发展规划中：将重大工程自然灾害灾变机理和风险研究，重大工程的减灾和安全设计，重大工程健康状态的检测、监测以及诊断和处置等方向列为制造与工程科学领域中的重大科学问题和研究方向。将复杂服役条件下材料的使用行为与失效列为材料科学领域中的重大科学问题和研究方向。

(3) 国家中长期科技发展规划纲要(2006—2020年)中：将重大产品和复杂系统的可靠性、安全性和寿命预测技术作为先进制造技术领域中的前沿技术之一，将复杂系统的灾变形成及其预测控制、材料服役与环境的相互作用、性能演变、失效机制及寿命预测原理列为面向国家重大战略需求的基础研究问题。

(4) 国家安全生产科技“十二五”规划中：始终坚持把安全生产基础理论研究立足于解决重点行业领域内的突出矛盾和突出问题上，放在安全生产发展战略的层面上，着力探索重大灾害事故致因机理及动力学演化过程、典型工业事故发生机理及动力学演化过程、生产事故应急救援等难题，着力破解安全生产社会实践中遇到的理论困惑，大力提升安全生产基础理论的水平。

(5) 高端装备制造业“十二五”发展规划中：指出高端装备制造业的可靠性低是制约行业发展的瓶颈之一。在智能制造装备产业“十二五”发展子规划中，把着力提升产品的安全性、可靠性、实用性作为主要任务之一，把突破部件和装备的健康维护诊断技术作为实现制造装备和制造过程的智能化技术支撑和重点发展方向之一。在轨道交通装备产业“十二五”发展子规划中，对轨道交通运营管理和设备的安全性、可靠性提出了更高、更苛刻的要求，要推动轨道交通装备向高安全性和可靠性、易维护方向发展，进一步提升轨道交通装备配套产品的技术水平、安全性和可靠性。

(6) 国务院关于工业转型升级规划(2011—2015年)中：提出要组织实施关键基础产品质量攻关计划，提升关键原材料、基础元器件性能的稳定性；组织实施重大装备可靠性增长计划，支持开展可靠性设计、试验与验证，提升重大装备的可靠性和一致性水平。

(7) 中国制造2025中：要统筹推进“四基”(即核心基础零部件、先进基础工艺、关键基础材料和产业技术基础)发展，提升基础产品的质量、可靠性和寿命。加强“四基”创新能力建设，强化前瞻性基础研究，着力解决影响核心基础零部件(元器件)产品性能和稳定性的关键共性技术。加快提升产品质量，实施工业产品质量提升行动计划，针对汽车、高档数控机床、轨道交通装备、大型成套技术装备、工程机械、特种设备、关键原材料、基础零部件、电子元器件等重点行业，组织攻克一批长期困扰产品质量提升的关键共性质量技术，加强可靠性设计、试验与验证技术开发应用，推广采用先进成型和加工方法、在线检测装置、智能化生产和物流系统及检测设备等，使重点实物产品的性能稳定性、质量可靠性、环境适应性、使用寿命等指标达到国际同类产品先进水平。大力提高国防装备质量可靠性，增强国防装备实战能力。

随着科学技术的高速发展以及新型复杂系统的建立，各种大型设备和系统日趋复杂，容量参数不断提高，环境条件更加严苛，其可靠性及由此带来的风险等问题日益突出。经过50多年的发展，常规二值状态可靠性理论已经比较成熟，在此基础上，突破传统“成功”和

“失效”两个状态的多状态可靠性理论应运而生。当前，多状态可靠性已成为可靠性领域发展的主要方向之一。由于大型机械装备系统直接影响国家安全和经济命脉以及行业经济效益，且越来越向着高可靠、长寿命和高有效性方向发展，具有诸如高成本、小批量、小样本、失效模糊性及状态不确定性等特征，使得如何评估这些系统及其部件的可靠性和安全性成为一个迫切需要解决的难题。因而，开展复杂系统可靠性概率风险评价理论与方法研究，建立和健全多状态系统的可靠性概率风险评价理论与方法体系，对其进行较为准确的可靠性概率风险评价，可以为复杂系统的可靠性评估、寿命预测和故障诊断与预防等提供新思路和新方法，成为可靠性设计领域研究的前沿和热点。

1.2 可靠性技术发展的现状与趋势

可靠性问题起于 20 世纪 40 年代，源于军工电子设备，始于美、德。经过几十年的发展，可靠性已经成为一门独立的新兴学科。国外可靠性技术的发展，是以需求为导向、以管理为中心、以工程为目的、以专业为推动的。20 世纪 40 年代和 50 年代是可靠性技术发展的摇篮期和奠基期，在这一阶段，一些工程技术人员和数学家们开始应用概率论和数理统计学对产品的可靠性问题进行定量研究。美国最先成立了可靠性咨询委员会，制订了军用规格、标准及可靠性标准体系，为世界范围可靠性研究的发展奠定了基础。从 20 世纪 60 年代开始，可靠性技术得到了全面的发展。70 年代可靠性发展步入成熟期，其主要特点是：建立了集中统一的可靠性管理机构，成立了国家可靠性数据网，对产品可靠性的分配、预计、可靠性设计、可靠性分析、可靠性试验和数据交换等进行系统化管理，形成了线条状的管理方式。进入 80 年代后，可靠性技术向更深、更广的方向发展，美国开始把可靠性放在与产品性能、成本和开发周期同等重要的位置，并颁发了一系列管理措施，推动可靠性技术的研究与应用。在管理上，加强集中统一管理，强调可靠性与维修性管理制度化；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技术在可靠性工程中的应用，并积极开展模块化设计、集成化设计、容错设计、防错设计和动态设计等可靠性设计方法。进入 90 年代以后，在可靠性研究方面，美国开始大力推行健壮设计、并行工程和集成产品与过程开发(integrated product and process development，IPPD)管理。

国外在进行可靠性研究过程中，十分重视可靠性技术的基础、应用和开发 3 个方面的协调发展。基础研究方面，加利福尼亚大学在可靠性数学、可靠性理论、寿命计算及数据分析、可靠性增长理论、贝叶斯方法等方面的研究，为美国可靠性定量分析和计算工作的开展奠定了基础；纽约理工大学在可靠性理论、软件可靠性定义、概念和建模技术的研究，锡拉丘兹大学在可靠性验收和抽样设计、可靠性贯序概率的试验方案设计方面的研究，麻省理工学院在加速试验模型及方法的研究，加拿大渥太华大学在人的可靠性方面的研究都取得了令人瞩目的成就；20 世纪 90 年代后期，以色列学者又开始了基于凸集模型的稳健可靠性概念及理论体系的研究。应用方面已开发出如 Relex、WQS、Realsoft Weibull++、Xfmea、RENO、RCM++、ALTA、BlockSim 等系列商用专业的可靠性软件，并得到了广泛的应用。

随着知识经济的快速发展，可靠性理论及其管理模式也从传统型向广义型发展。1995 年，欧洲开始对传统可靠性定义提出质疑，用无维修期(MFOP)取代原来的平均故障间隔时间(MTBF)，打破了故障率浴盆曲线分布规律，从而摈弃了随机失效无法避免的现象。国际

上开始推行在可靠性工程中开展失效物理方法的研究，旨在设计出不存在随机失效的产品。在可靠性管理模式上，先后经历了单点式管理、线条式管理、矩阵式管理，发展到今天的网络化管理。

经过50多年的发展，常规二值状态可靠性理论已经比较成熟，但是对于大型复杂系统，如重型柴油机、数控装备、大型工程机械、冶金转炉等，由于结构关系复杂，各个零部件的功能各异，可以呈现出多种工作状态、多种失效模式和不同的性能水平，对整个系统性能也产生各种不同的影响，某一元件的失效或者性能衰退会导致系统性能的下降，同时引起整个系统呈现出多个性能水平和多种失效模式，这样的系统称为多状态系统。这种情况下将系统粗略地描述为“成功”和“失效”两个状态显然不符合实际需要，多状态可靠性理论就是在这种背景下产生的。当前，多状态可靠性已成为可靠性领域发展的主要方向之一。

多状态系统的概念在20世纪70年代提出后，经过几十年的逐步发展，在Lisnianski(2003，2010，2012)、Zio(2003，2009)、Levitin(2005)、Zaitseva(2010，2012)、Kuo(2012)、Natvig(2011)、Xing(2009)、Zuo(1994)等国外学者及国内谢里阳、黄洪钟、康锐、崔利荣等众多教授的共同努力下，多状态系统可靠性理论研究已取得一定的成果。现有的多状态可靠性分析方法主要有：结构函数法、生成函数法和蒙特卡罗法等。结构函数法要求列举所有系统的状态，生成函数法适合于不可修串并联多状态系统，这两种方法只能用于规模较小的系统可靠性分析，蒙特卡罗方法适合于复杂系统的分析，但对于具有 n 个部件，每个部件具有 m 个状态的系统，蒙特卡罗法要求出其所有最小路割集是一件不易的事情。

国内早期对多状态系统可靠性的研究并不多，20世纪90年代后期多状态系统系统可靠性的研究又有上升，且取得了一定的成绩。

从国内外的研究现状来看，当前多状态可靠性研究主要在于将传统的二值状态系统中一些成熟有效的可性分析计算方法应用到多状态系统可靠性分析计算中去。但将这些方法扩展应用到多状态系统时遇到许多困难，需要解决，主要表现在：

(1) 多状态系统中系统以及元件都具有多种状态，容易产生状态数目爆炸问题，如何减轻计算负担成为研究的重点。

(2) 在多状态可靠性分析方法中，状态概率的计算也是主要需要解决的问题，状态概率的计算一般需通过结构函数进行，对多状态系统结构函数模型的建立并未提出一种普遍适用的方法。

(3) 多状态系统研究的一个重要方向就是寻求多状态系统优化算法，如何对系统及其部件的状态在可行状态空间中进行优化分配，目前这方面的研究还相当少。

1.3 可靠性风险评价的研究现状与发展趋势

风险评价，也称安全评价，是对系统发生事故的危险性进行定性或定量分析，依据现存的专业经验、评价标准和准则，对危害分析结果得出系统发生危险的可能性及其后果严重程度的评价。通过评价以寻求最低的事故率、最少的损失和最优的安全投资效益。风险评价包括风险分析和风险评定在内的全过程。

危险是客观存在、无法改变的，而风险却在很大程度上随着人们的意志而改变，亦即按照人们的意志可以改变危险出现或事故发生的概率，以及一旦出现危险，由于改进防范措施

从而改变损失的程度。

关于风险评价，主要有三种方法：一是概率风险评价，它是在事故发生前，预测某设施可能发生什么事故及其可能造成的环境（或健康）风险；二是实时（real time）后果评价，主要是在事故发生期间给出实时的有毒物质的迁移轨迹及实时浓度分布，以便做出正确的防护措施决策，减少事故的危害；三是事故后果（over-event 或 past accident）评价，主要研究事故停止后对环境（或健康）的影响。从这个意义上说，我们所研究的机械设备风险评价则偏重于概率风险评价。概率风险评价方法是根据零部件或子系统的事故发生概率，求取整个系统的事故发生概率。

概率风险评价（probability risk assessment，PRA），也称为定量风险分析，该技术源于可靠性学科。“二战”期间，由于科学技术的进步，国防工业和军事工业中的设备系统越来越复杂，产品的可用性直接决定于产品的可靠性和维修性，由此可靠性工程这一学科逐渐发展起来。至今，可靠性工程已经从调查研究、制定规范、统计试验发展到全面实现以可靠性为中心的质量管理阶段。

概率风险评价技术通过综合分析单个元件的设计和操作性能来估算整个系统发生事故的概率。自 20 世纪 60 年代末以来，主要服务于三个方面：

（1）提供某种技术的危险分析情况，用于制定政策，答复公众咨询，评价环境影响；

（2）提供危险定量分析值及减少危险的措施，帮助建立有关法律和操作程序；

（3）在工厂设计、运行、质量管理、改造及维修时提出安全改进措施。

概率风险评价最早运用于核工业。1972 年美国麻省理工学院拉姆森（Rasmussen）教授等 14 名专家用了两年的时间，耗资近 300 万美元，完成了核电站评估，并于 1975 年正式发表了《商用核电站轻水反应堆风险评价》报告，即著名的 WASH—1400 报告。该报告的目的是估计美国商用核电站的潜在事故对社会造成的风险，它第一次成功地运用了事件树和故障树的方法对核电站的风险作了定量分析，并与已经存在的社会风险作了比较，这在核能安全分析上是一个重要的里程碑。实践证明，概率风险评价技术有助于核电站的设计、运行和管理安全性的改进，它的作用在世界各国产生了广泛而深远的影响，同时也说明了概率风险评价是对系统进行风险评价的重要方法。

虽然第一个概率安全评估报告 WASH—1400 得到了专家小组的支持，但核工业对概率安全评估方法的实际应用仍持观望态度。1979 年 3 月，美国的三哩岛核电站 2 号机组发生了严重的事故，事故的进展过程正是 WASH—1400 中所预示的。三哩岛核电站事故使人们认识到，概率安全评估为全面了解核电站发生事故的可能性提供了最完整、最清晰的图像。美国核管理委员会（NRC）于 1981 年发布了《故障树手册》（NUREG—0492），大力推动了故障树在核电站概率安全评估中的应用。该手册经过多次修订之后，目前已成为核工业和航空航天工业重要的技术资料。三哩岛事故之后，概率安全评价得到了多个核电站的广泛关注。此后，巴西采用大事件树/小故障树方法研究了 ANGRAI 核电站的安全运行问题，并专门编制了能考虑不确定性传播的分析程序，对能引起堆芯熔化的 16 个主要事件序列进行了不确定性分析，找到了系统和人因方面的薄弱环节。日本采用小事件树/大故障树方法分析了钠冷快中子反应堆，得到了堆芯熔化的概率。到 1983 年为止，主要的核工业国家已对 22 个核电站进行了概率安全评估。

1985 年 3 月，国际原子能机构（IAEA）在英国召开了“概率安全评估含义”学术会议，会

议反映了各国概率安全评估的发展现状。从会议讨论的结果看出：许多国家已制定了规划，要求对核电站进行概率风险安全评估。一些国家已制定或即将制定法规，要求核电站同时进行确定论方法和概率安全评估方法的评审，并要求将评审结果作为发放许可证的必需工作。1989 年，世界核电站运营者协会(WANO)在莫斯科成立，该组织通过分享全世界核电站运行专家的经验结果来最大限度地提高核电站的安全性。到目前为止，几乎所有的核电站都加入了该组织。

现在，IAEA 的核安全评审组(OSART)经常性地检查各国核电站的运行和管理情况，定期到 WANO 的成员核电站进行运行安全评估。

由于概率安全评估在核领域取得了巨大的成功，加之 1986 年的“挑战者”号事故，美国宇航局(NASA)逐渐认识到采用定量方法对航天系统进行风险评估的重要性。在航空航天行业，1988 年 1 月，NASA 在《“挑战者”事故后航天飞机的安全性评估与管理》报告中指出：概率安全评估应尽早应用于航天飞机安全风险管理中去，航空系统的失效数据、飞行测试数据及相关的分析技术应系统化地应用于支撑概率安全评估、趋势分析及其他安全性定量分析。1993 年，NASA 开始采用概率安全评估方法对航天任务进行分析。1996 年 6 月，NASA 领导开发了定量风险评估系统(QRAS)，用来对航天飞机设计改进提供决策支持。

从“挑战者”号事故中得到警示，欧洲航天局(ESA)的安全评估也从定性转向定量，并开发了多目标决策支持系统来支持技术和计划的评估。而且 ESA 正在开发安全风险评估专家系统(ERES)，这些工作都是与欧洲有关部门通过签订合同展开的。目前，ESA 已经形成了专门的标准来指导航天系统概率安全评估。另外，在航天系统安全性评估方面，ESA 和 NASA 保持着非常紧密的合作关系。

20 世纪 70 年代我国开始进行有关系统安全性的研究。1982 年我国首次召开了安全系统工程讨论会，研讨了安全系统工程的发展方向，并对事件树、故障树分析技术进行了研究。1988 年，机械电子工业部颁布了《机械工厂安全评估方法》，并在机械行业中的 100 多个加工厂进行了推广。1990 年，贵州省完成了《工业企业安全评估——全面安全管理的事故隐患评价法》。1995 年，劳动部和北京理工大学合作完成了《易燃、易爆、有毒重大危险源的安全评估技术》。1998 年 5 月，中国海洋石油总公司完成了《海上油(气)生产设施安全风险分析》报告，该报告通过了评审验收并得到了专家的高度评价。1999 年 3 月，上海石化运用美国达信安全评估技术，对公司下属的多套装置和设备进行了安全评估并通过了专家的评议。近年来建设的陕京输气管道、西气东输干线等工程，都进行了定量安全评估。

1998 年，中科院系统科学研究所针对我国航天系统的现状，提出了中国概率风险评估(CPRA)方法，并将其应用于某型运载火箭安全性评估中。1999 年 6 月，深圳大亚湾核电站项目组完成了全部一级概率安全评估的修订工作，并与岭澳核电站项目组合作完成了岭澳核电站的概率安全评估报告。目前，大亚湾核电站和秦山核电站都已经正式启动了 10 年定期安全评估的计划。

“九五”期间，由国防科技大学完成的项目“计算机辅助安全性设计与分析技术”对危险与运行性(HAZOP)进行了较为深入的研究，并将其应用于某基地常规燃料加注系统的安全性分析中。

“十五”期间，由国防科技大学完成的项目“动态系统安全性分析技术”对现有的概率安全评估方法进行了较为系统的总结和完善，并开发了动态系统安全性分析平台(DSSAP)。

近年来，随着机械风险评价技术的不断发展，我国国内在概率风险评价方法的研究上也取得了显著的进步。

概率安全评价方法涉及许多系统可靠性分析方法，包括失效模式与影响分析（failure model and effect analysis，FMEA）、主逻辑图（master logic diagram，MLD）、事件序列图（event sequence diagram，ESD）、事件树（event tree，ET）、故障树（fault tree，FT）和可靠性方框图（reliability block diagram，RBD）等。

当前，静态概率安全评价（static probabilistic safety assessment，SPSA）方法经过 30 来年的完善和发展，理论已经比较成熟。对于大型复杂系统，如数控装备和冶金转炉等，传统的 SPSA 方法只是考虑各事件的组合对系统的影响，都是基于系统不变性发展起来的。但在实际应用中，机械装备系统都是由软件、硬件和操作控制人员组成，系统和组件状态往往处于动态变化的过程中。系统的运行往往是硬件、软件与操作控制人员相互交互、相互作用的动态过程，如在故障树中，各基本事件发生的顺序不同或同一基本事件发生的时间不同可能导致不同的顶事件；系统对软件、硬件和操作控制人员的响应以及基本事件间发生过程的关联性都存在一定的不确定性，使得传统的 SPSA 方法已经无法对系统做出较为精确的安全评价。

已有常用的静态安全分析方法有：贝叶斯分析、层次分析法、风险矩阵法、模糊评价法、概率安全评价、马尔可夫分析以及组合两种或多种安全评价方法的方法，如模糊层次分析法、模糊概率安全评价方法、模糊贝叶斯分析法、ET-FT、ESD-FT、ESD-FT-MC 以及 ESD-FT-BBN 等。静态风险评价方法在风险分析的发展中起了积极的作用，已经形成了比较完善的理论。然而，它只考虑各事件组合对系统的影响，在描述系统动态行为方面有着很大的局限性。

PRA 评价方法的核心技术是事件树分析（ETA）和故障树分析（FTA），二者的发展方向预示着 PRA 的发展趋势，尤其是 FTA。随着工程技术的快速发展，静态 FTA 已不能完全满足具有动态特性的系统风险分析，因而研究重点也转向动态事故树。

在进行系统安全评价时，需要综合考虑各事件发生的驻留时间、系统和组成系统的各部件的响应时间、同一事件发生的顺序、各事件发生的时间以及系统中各组件状态对系统状态的影响等一系列动态因素对系统安全性产生的影响。另一方面，由于大型复杂系统的结构复杂，部件繁多，在对其进行风险评价时需要获得充足的信息。但信息量越大，所建模型就会越复杂，计算过程就会越烦琐，甚至存在组合爆炸问题。如何评估大型复杂系统及其部件的可靠性以及如何解决动态概率安全评价（dynamic probabilistic safety assessment，DPSA）方法的组合爆炸问题都成为迫切需要解决的难题。当前，开展复杂系统的 DPSA 及系统的可靠性理论研究，对其进行较为准确的可靠性评价，以期为系统的可靠性评估、寿命预测和故障诊断与预防等提供新思路和新方法，是可靠性领域研究的前沿和热点之一。

目前，DPSA 方法在国外已经有了相应的应用。国内在这方面的研究起步较晚，相对滞后，严重影响我国机械装备的安全水平，阻碍了我国机械设备的发展。因此，对机械装备的 DPSA 方法进行深入研究，对于提高我国机械装备系统的可靠性、维修、诊断以及风险监控和管理，具有积极的现实意义。

常用的动态安全分析方法有以下三类：

（1）连续时间方法。如连续事件树方法（continuous event tree，CET），连续胞映射技术

(continuous cell-to-cell mapping,CCCM)。

(2) 离散时间方法。如动态逻辑分析法(dynamic logic analysis method,DYLAM)、动态事件树(dynamic event tree,DET)、离散动态事件树(discrete dynamic event tree,DDET)、事故动态模拟(accident dynamic simulation,ADS)、集成安全评估(integrated safety assessment,ISA)、结合离散动态事件树和马尔可夫过程的方法(Markov chain dynamic event tree,MCDET)、胞映射技术(cell-to-cell mapping,CCM)。

(3) 可视化界面的方法。如动态故障树(dynamic fault tree,DFT)、ESD、动态流程图方法(dynamic flow diagram,DFM)、Petri 网方法、GO-FLOW 方法等。

从国内外对概率风险评价方面的研究现状和应用情况来看,很多方法是对现有 SPSA 方法的扩展和完善,都存在不同程度的局限性。随着对系统安全评价要求的进一步提高,需要对现有的 SPSA 方法进一步进行扩展,使其能够应用于多态系统、动态系统和多态动态系统。另外,现有概率风险评价方法有各自的优势和缺陷,集合几种现有概率风险评价方法,以其中一种概率风险评价方法的优点去弥补另一种方法的缺点,既可以继承这几种概率风险方法的优点又能摒除这几种概率风险方法的不足。而且,对现有动态概率风险方法模型结构进行改进,简化现有模型,以提高计算效率、计算结果的准确性以及计算方法的稳健性。

现有概率风险评价方法存在的局限性主要表现在以下几个方面:

(1) 对于大型或复杂系统,特别是具有多状态的系统而言,由于构成其基本事件和最小割集的数量比较大,当应用传统的故障树/事件树分析方法对系统进行概率风险评价时,需要对一些地方进行必要的近似和截断,从而可能会导致对系统评估结果和组成系统的基本事件所对应的重要度存在较大偏差。

(2) 动态故障树/事件树的计算复杂度会随着构成系统的相关复杂度增长呈指数方式增长,从而可能会发生组合爆炸问题。

(3) 在现有概率风险评价方法的研究过程中,很少融合其他智能计算方法如模糊集理论、神经网络等,导致在整个风险评价过程中忽略了系统寿命周期理论,因此整个风险过程不太客观。

(4) 目前的方法很难准确与系统相关的运行信息、测试信息及专家经验进行融合,如果系统出现了新的风险信息,又需要对以前的系统进行重新建模,因而表现出来的问题是信息的可重用差以及不能快速和准确地对系统新出现的风险问题进行评价。

(5) 由于现代机械装备系统越来越复杂化、智能化和大型化,致使现有的动态研究方法需要综合考虑系统的响应时间、系统与组成该系统各部件状态的变化,以及系统各部件相互作用对系统可靠性与安全产生的影响。使用现有的动态概率风险评价方法在风险评价时需要得到充足的信息。但信息量越大模型就会越复杂,计算过程就会越烦琐和复杂。

(6) PRA 方法主要依赖的是 ET/FT 方法,ET/FT 方法目前应用较多的是基于二元决策图(BDD)的概率安全评价的方法。传统的方法是用 BDD 技术分析静态 ET/FT 模型,MC 技术分析动态 ET/FT 模型。但目前 BDD 技术只局限应用于二态系统,而实际应用时系统失效大都是多态的。因此,基于 BDD 的概率风险评价方法在多状态系统应用时有很大的局限性。

(7) 动态概率风险评价方法与其他技术结合的研究较少,如与重要度分析、共因失效分析、不确定分析、诊断分析、灵敏度分析等技术结合的研究相对较少。

另一方面，在可靠性工程中，系统在设计之前都旨在追求高可靠度和高质量。然而，如果所设计的组件不需要很高的要求，那么所做的设计就会存在着一定的资源浪费；再者，对运行中的设备进行检测时，如果只是定期做大量的预防维护和诊断维修，那这样的措施也是比较盲目的，没有针对性。因此，高效可行是可靠性分析技术所必须拥有的基本特点。重要度分析(importance measure，IM)就是这样一种极具针对性的方法，它衡量的是元部件故障(底事件发生)对系统故障(顶事件发生)的影响程度，是反映系统元部件重要性的数量指标。研制任何产品都必须考虑费用和效能两大关键因素，为了以最少的资源最大限度地提升可靠度以及获取最佳的经济效益，在对系统进行设计、可靠性优化以及采取维修措施时，只将重要度比较高的元部件的可靠性提高，就可以将整个系统的可靠性最大限度地提高，从而明显地使得设计成本和维修费用下降，进而获得最大的经济效益。

重要度分析是融合了危害度、灵敏度、风险性和重要性等多类知识的前沿和热点研究领域之一，是进行系统风险评价的一种重要手段。重要度量化了一个元部件在一个工程系统中的关键程度，说明同一个系统中元部件的关键性和重要程度是不尽相同的。因此，有必要找到重要度科学有效的计算方法，以确定影响系统可靠性变化较大的元部件是重要元部件还是关键性元部件。当前，重要度分析已广泛应用于核电站、生物信息、交通运输和轨道业、云计算中的数据存储管理、可靠性设计、网络开发、故障诊断与维修、风险分析等领域中。

重要度分析也是可靠性分析的关键部分，作为一种确定系统薄弱环节和优先提高系统可靠度的有力工具，对系统可靠性分析的意义体现在以下方面：

(1) 系统有很多个元部件，每一个元部件相对于系统的重要程度都不一样，只有准确分析每个元部件的重要程度才能高效地对相应元部件进行改善，从而有效地提高系统的可靠性。

(2) 对于多状态系统和元部件来说，每一个状态的灵敏度和关键程度也是分析的要点，可以根据状态属性的重要性来提出相应的保护或维修措施，使系统或元部件尽量减轻或避免某些危险状态，保持优良状态。

(3) 系统元部件的组合非常重要，并非高性能元部件就必定能组合成高性能系统，因此必须找出最优的组合状态，使系统性能状态达到最大。

(4) 重要度分析综合考虑了故障状态、安全因素、人为错误等方面，对可靠性分析的全面性较高、可操作性强。

1.4 本章小结

本章汇总了国内外文献对于复杂系统可靠性和风险评价的研究现状，对当前国内外在可靠性概率风险评价方面有待解决的问题进行了总结。从已有的文献资料可以看出，随着科学技术的高速发展以及新型复杂系统的建立，在已有研究工作的基础上，综合多种先进的理论与方法进行多状态系统可靠性概率风险评价理论与方法的研究，可以为提高重大产品和重大设施的运行可靠性、安全性和可维护性能力提供理论和技术支持，对于实现可靠性理论和方法的创新也有着十分积极的意义。