论文题目 复杂系统动态故障树分析的新方法及其应用研究

学 科 专 业 机械电子工程

学　　号 **200911080101**

作 者 姓 名 李彦锋

指 导 教 师 黄洪钟　教 授

分类号 _____ 密级 _____

UDC [注1] _____

学 位 论 文

复杂系统动态故障树分析的新方法及其应用研究

（题名和副题名）

李彦锋

（作者姓名）

指导教师 **黄洪钟** **教 授**

电子科技大学 **成 都**

（姓名、职称、单位名称）

申请学位级别 **博士** 学科专业 **机械电子工程**

提交论文日期 2013.10.22 论文答辩日期 2013.12.08

学位授予单位和日期 **电子科技大学** 2013 年 12 月 24 日

答辩委员会主席 _____

评阅人 _____

注 1：注明《国际十进分类法 UDC》的类号。

NEW METHODS OF DYNAMIC FAULT TREE ANALYSIS OF COMPLEX SYSTEM AND ITS APPLICATION

A Doctor Dissertation Submitted to

University of Electronic Science and Technology of China

Major: **Mechatronic Engineering**

Author: **Yanfeng Li**

Advisor: **Prof. Hong-Zhong Huang**

School: **School of Mechatronics Engineering**

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

作者签名：_____ 日期：　　年　　月　　日

论文使用授权

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权电子科技大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后应遵守此规定）

作者签名：_____ 导师签名：_____

日期：　　年　　月　　日

摘　要

随着现代工程系统的大型化、复杂化以及高新技术的引入，系统可靠性已经成为制约复杂系统发展的关键所在。可靠性分析技术作为实施系统可靠性工程的关键基础技术，目前正面临着复杂系统所带来的若干技术难点和应用挑战。针对复杂系统的可靠性分析技术已经成为可靠性工程领域的研究热点及难点问题之一。系统可靠性分析常规方法主要包括：可靠性框图法、故障模式影响及危害性分析法、故障树分析法、Petri 网方法以及蒙特卡洛数值仿真方法等。常规方法通常不考虑系统的动态失效特性，且多数建立在零部件故障相互独立和故障数据完备的基础之上。在实际复杂工程系统中，零部件失效之间通常并不是相互独立的，往往存在着多种复杂的关联关系和动态特性，比如部件失效的顺序关系。另一方面，由于成本、时间、管理和人因等多方面的原因导致零部件失效数据存在模糊不确定性。目前，在考虑动态失效特性的故障树分析方面已取得了一定成果。然而，在同时考虑模糊不确定性以及动态失效特性等情况下的故障树分析方面的研究工作还很缺乏，以致用常规方法分析所得结果与实际情况不符甚至相差甚远。因此，迫切需要开展考虑零部件动态失效特性和模糊不确定性的系统可靠性分析方法的研究。

针对上述问题，本文主要开展了以下研究工作：

（1）基于模糊马尔科夫模型的动态故障树分析方法。马尔科夫模型方法是一种状态空间分析方法，用该模型能够准确地描述失效分布与维修分布都服从指数分布的系统的失效及维修过程。本文在基于马尔科夫模型的基础上，考虑了零部件失效信息的模糊不确定性，研究了在模糊失效率下的动态故障树分析方法。通过建立系统的动态故障树模型，并运用三角模糊数来描述零部件和系统的失效率，通过已经得到的动态故障树模型建立系统失效过程的模糊马尔科夫模型。运用模糊理论中扩展原理的思想和 Laplace-Stieltjes 变换求解该模型，得到系统在给定时刻下的模糊失效概率和给定隶属度下的模糊可靠度曲线。最后应用该模糊马尔科夫模型对某数控加工中心液压系统进行可靠性建模与分析。研究结果表明，该方法能够有效地对具有动态失效特性和模糊不确定性的系统进行可靠性建模及定量评估。

（2）基于离散时间贝叶斯网络的动态故障树可靠性评估模型。研究了基于贝叶斯网络和动态故障树的系统可靠性建模和评估方法。通过把系统失效的动态故障树模型转化为贝叶斯网络模型，并运用贝叶斯网络的拓扑结构来表达系统中部

件失效之间的逻辑关系。针对基于马尔科夫模型的动态故障树求解方法中存在的状态爆炸问题，借助贝叶斯网络的条件独立性来降低模型求解的复杂度。在此基础上，建立了静态和动态故障树中各种逻辑门的条件概率分布的公式，以实现对系统失效过程及其动态特性进行建模和分析。以卫星太阳翼驱动机构为对象，建立了动态故障树模型和相应的贝叶斯网络模型，并运用联合树推理算法对该模型进行了双向概率推理。实例分析结果表明：该方法能够有效地解决具有动态失效特性的复杂系统的可靠性分析和评估问题。

（3）模糊数据下基于连续时间贝叶斯网络的动态故障树分析方法。研究了考虑模糊不确定性的基于连续时间贝叶斯网络的系统可靠性建模与分析方法。基于连续时间贝叶斯网络模型的方法能够直接得到系统的可靠度和失效概率的解析表达式。本文用三角模糊数描述零部件的失效率，并用其来构造零部件的模糊边缘失效密度函数及模糊失效分布函数。用单位阶跃函数和冲激函数来构造贝叶斯网络中非根节点失效事件的条件概率密度函数和分布函数。在此基础上，推导了在模糊失效率下的几种典型的故障树逻辑门输出事件发生的模糊边缘失效密度函数和模糊失效分布函数的表达式。最后，运用算例验证了该方法的正确性和有效性，并通过对大型矿用挖掘机电气系统整流回馈子系统的建模与分析阐述了该方法在实际工程系统中的应用。

（4）考虑共因失效的动态故障树分析方法。运用故障树分析方法对具有共因失效的系统进行了可靠性分析。阐述了当前共因失效研究中的一些经典模型和建模方法，运用显式建模方法与平方根模型对某动车组追尾事故进行了故障树分析。分别计算了考虑共因失效和假设部件失效独立两种情况下的系统失效概率。结果表明：不考虑共因失效因素的影响会对可靠性分析结果带来较大的误差，说明了共因失效对于交通工具这种重要设施的安全性影响非常重大，同时也表明了考虑共因失效的动态故障树分析方法可为列车安全性及可靠性评估提供基础。同时，本文还提出了各种备份条件下考虑共因失效的动态故障树及贝叶斯网络可靠性建模及评估方法。建立了考虑共因失效条件下，确定贝叶斯网络中各种备件门输出事件对应节点的条件概率分布表的方法。通过算例验证了该方法的有效性，并通过与蒙特卡洛数值仿真方法对比，验证表明该方法的计算精度能够满足实际要求。

关键词：系统可靠性分析、动态故障树分析、模糊马尔科夫模型、贝叶斯网络、模糊数、共因失效

ABSTRACT

Reliability and safety analysis and evaluation of complex systems have become one of the hot issues in reliability engineering. Reliability block diagram (RBD), failure modes, effects and criticality analysis (FMECA), fault tree analysis (FTA), petri nets method and Monte Carlo Simulation (MCS) method are the most commonly used tools for system reliability analysis. The traditional methods frequently do not consider the dynamic characteristics of system failure, such as the sequential dependency of component failure. However, in actual complex engineering systems, component failure events are mostly not independent to each other, but there are many interacting dynamic characteristics. On the other hand, due to the lack of data, the factors such as the update of product design, human factors, et al. will cause the uncertainty of components failure data. At present, the fault tree analysis considering the dynamic characteristics of failure has achieved fruitful results. However, the research of fault tree analysis which considering the influence in combination of fuzzy uncertainty and dynamic failure characters is still insufficient. Therefore, it is necessary to do some further exploratory researches on system reliability analysis on condition that component failures are not independent and considering fuzzy uncertainty of systems.

To solve the above problems, the following works are carried out in this dissertation:

(1) Dynamic fault tree analysis method based on fuzzy Markov model. Markov model is a state space method, which can be used for system failure and maintenance modeling where the failure and maintenance time is exponentially distributed. On the basis of Markov model and considering the influence of the fuzzy uncertainty of component failure parameters to system, a research on dynamic fault tree analysis method in the case of fuzzy failure rate is carried out in this dissertation. A dynamic fault tree model has been built. The triangular fuzzy numbers are used to express the failure rate of the components and system, after which the fuzzy Markov model has been established based on the dynamic fault tree model obtained before. The fuzzy Markov model can be solved using the expansion principle of fuzzy theory and Laplace-Stieltjes transformation. The fuzzy failure probability or fuzzy reliability curve on given degree of membership could be obtained. Finally, the fuzzy Markov model

based DFTA method is used for reliability modeling and analysis of hydraulic system of CNC machining center. The results show that this method can conduct reliability modeling and quantitative assessment effectively for systems which have dynamic failure characteristics and uncertainty of failure rate.

(2) Dynamic fault tree analysis method based on Discrete-Time Bayesian Network. The system reliability modeling and evaluation method based on Bayesian Network and dynamic fault tree is studied in this dissertation. In the Discrete-Time Bayesian Network model, the fault tree model of system failure in transformed into a Bayesian Network model, and the logical relationship between the failure components of system is expressed by the use of Bayesian Network topological structure. Taking advantage of the conditional independence of Bayesian Networks, the state space explosion problem for solving the Markov model corresponding to the dynamic fault tree model can be alleviated. Conditional probability distribution tables for various kinds of logic gates in both static and dynamic fault trees are created. A solar array drive assembly of satellite is used for case study. The dynamic fault tree model and corresponding Bayesian Network model is established, and the junction tree inference algorithm is used for bidirectional probabilistic reasoning for this model. The result shows that this method can solve the problem of dynamic complex system reliability analysis and evaluation effectively.

(3) Dynamic fault tree analysis under fuzzy data based on the Continuous-Time Bayesian Network. A system reliability modeling and analysis method based on continuous-time Bayesian network is introduced and the fuzzy uncertainty of the system is also taken into account. The analytical expression of reliability and failure probability can be obtained directly on the basis of Continuous-Time Bayesian Network. Triangular fuzzy number is used to describe the failure rate and construct the fuzzy marginal density function and fuzzy distribution function of failure distribution of components. The conditional probability density function and distribution function of non-root nodes failure events in Bayesian Networks are jointly constructed by the unit step function and impulse function. Expressions of fuzzy marginal density function and fuzzy distribution function for several typical logical gates of fault tree under the fuzzy failure rate data are derived. The results of a case study verified the feasibility and correctness of this method.

(4) Dynamic Fault tree analysis method considering common cause failure. The

reliability analysis of the instance system with common cause failure is carried out by using fault tree analysis method. Some classic models and modeling methods for common cause failure are introduced. The explicit modeling approach and the square root model are used for the fault tree analysis of train rear-end accident. The failure probabilities of the system with and without considering common cause failure are calculated, respectively. The result shows that, a large error will exists in reliability analysis result without considering the effect of common cause failure on system. This illustrates that common cause failure has very significant impact on the facility security of transport, and this also provide the foundation of train safety and reliability assessment. The dynamic fault tree and Bayesian Network reliability modeling and assessment method considering common cause failure are proposed. The equations for determining the conditional probability distribution of spare gate nodes under CCF are established. Finally, an example is given to validate the correctness of this method. The comparison with MCS shows that the result can meet the requirement of precision.

Keywords: system reliability analysis, dynamic fault tree analysis, fuzzy markov model, bayesian network, fuzzy number, common cause failure.

目 录

图目录

表目录

主要符号及缩略语

R	实数集
$P_r(\bullet)$	概率运算
$f(\bullet)$	概率密度函数（PDF）
$f_{\cdot\|\cdot}(t\|\bullet)$	条件概率密度函数（CPDF）
$\tilde{f}_{\cdot}(\bullet,t)$	模糊联合概率密度函数
$\tilde{f}_{\cdot}(\bullet)$	模糊边缘概率密度函数
$F(\bullet)$	累积分布函数（CDF）
$\tilde{F}_{\cdot}(t)$	模糊概率分布函数
X	随机变量
U	论域
$\tilde{A}$	模糊集合
$\mu_{\tilde{A}}$	模糊集 $\tilde{A}$ 的隶属函数
$\tilde{A}_{\alpha}$	模糊集 $\tilde{A}$ 的 α 水平截集
S	马尔科夫过程（模型）的状态空间
$\tilde{\lambda}_{i,j}$	状态 i 到状态 j 的模糊状态转移率
$\tilde{p}(\bullet)$	系统处于某个状态的模糊失效概率
$\tilde{\lambda}$	零部件的模糊失效率
$P(\bullet)$	事件（节点）的概率分布
$P(\bullet\|\bullet)$	事件（节点）的条件概率分布
Δ	时间子区间长度
$u(t-\tau)$	单位阶跃函数
$\delta(t-\tau)$	冲击函数
$\oplus$	模糊加法
$\ominus$	模糊减法
$\otimes$	模糊乘法
$\oslash$	模糊除法
$\tilde{F}_s^{\cdot}$	逻辑门的模糊算子
$\tilde{\lambda}_{\cdot}(\bullet)$	一定时间内事件模糊条件失效率
Q	系统失效概率
Q_k	任意 k 个部件同时失效的概率

β	共因因子
$P(A_F \bigcap B_F)$	A，B 两部件并联系统失效概率
Y_i^i	单元 i 单独故障不发生事件
$Y_{a_i b_i c_i d_i \cdots}^i$	包含单元 i 的若干个单元同时故障不发生事件
λ_i^i	单元单独故障的故障率
$R_s(t)$	系统可靠度
$P_n^m(t)$	n 单元系统，指定的 m 个单元同时正常概率
$\Phi(\bullet)$	故障树结构函数
FTA	故障树分析（Fault Tree Analysis）
MCS	蒙特卡洛仿真（Monte Carlo Simulation）
DFTA	动态故障树分析（Dynamic Fault Tree Analysis）
CSP	冷备份部件（Cold Spare Parts）
WSP	温备份部件（Warm Spare Parts）
HSP	热备份部件（Hot Spare Parts）
FDEP	功能相关门（Function Dependency Gate）
SEQ	顺序相关门（Sequence Enforcing Gate）
PAND	优先与门（Priority-AND Gate）
FWI	模糊加权指数（Fuzzy Weighted Index）
FFTA	模糊故障树分析（Fuzzy Fault Tree Analysis）
DFT	动态故障树（Dynamic Fault Tree）
FDFT	模糊动态故障树（Fuzzy Dynamic Fault Tree）
CNC	数控（Computerized Numerical Control）
CTMC	连续时间马尔科夫链（Continuous Time Markov Chain）
BDD	二元决策图（Binary Decision Diagram）
BN	贝叶斯网络（Bayesian Network）
DAG	有向无环图（Directed Acyclic Graph）
DTBN	离散时间贝叶斯网络（Discrete Time Bayesian Network）
MPD	边缘概率分布（Marginal Probability Distribution）
CPD	条件概率分布（Conditional Probability Distribution）
CTBN	连续时间贝叶斯网络（Continuous Time Bayesian Network）
SADA	卫星太阳翼驱动机构（Solar Array Drive Assembly）
CCF	共因失效（Common Cause Failure）
BP	基本参数模型（Basic Parameter Model）

MGL	多希腊字母模型（Multiple Greek Letters Model）
BFR	二项失效率模型（Binomial Failure Rate Model）

第一章 绪 论

系统可靠性建模与分析方法从系统的观点研究产品的失效行为及寿命特征，对提高产品的可靠性与安全性起着非常重要的作用。故障树分析方法作为系统可靠性分析的一种重要的工具，具有直观性、层次化、系统性等特征，这使得该方法在理论研究和工程应用等方面都取得了丰硕的成果。本章阐述故障树分析的研究背景及意义、国内外研究现状以及本文的研究内容。

1.1 选题背景及研究意义

随着现代设计、制造技术及计算机技术的飞速发展，系统的结构日益复杂，对性能的需求也越来越高。伴随着系统性能提高的同时，成本也在显著的增加，系统一旦发生故障或失效，无论是维修或报废都将会造成巨大的经济损失，有时甚至会造成人员伤亡。因此，复杂系统的可靠性和安全性问题越来越受到重视，复杂系统可靠性分析也成为目前国内外研究的热点及难点问题之一。常规的系统可靠性分析方法（如故障树分析方法）通常不考虑部件失效之间的先后顺序以及部件之间的功能相关性等特征，单纯地把系统失效作为某些零部件失效的组合，这对于现代复杂系统来说是不完全合理的。例如，故障树分析方法是系统可靠性分析方法中发展最为完善、应用最为广泛的分析方法，然而由于静态故障树分析方法不考虑部件失效的时间关系、顺序关系以及相关性等动态失效特性，使得在对具有动态失效特性的系统进行可靠性建模与分析时无法正确地建立系统的可靠性模型。另一方面，常规的故障树分析方法完全基于概率论与二值逻辑理论，通常把系统的状态以及失效分布视为确定性的，既不考虑状态的不确定性，也不考虑分布参数的不确定性。这也不符合现代实际工程系统的特点。因此，常规的故障树分析方法已经不能满足复杂系统的可靠性建模与分析的需求，迫切需要建立一系列新的建模与分析方法。

系统中零部件的失效行为往往具有一种或多种动态失效特性，如何正确地建立具有动态失效特性的子系统的可靠性模型是整个系统可靠性建模与分析的关键。Dugan 及其团队在故障树分析方面做了大量的开拓性研究，提出了动态故障树分析方法，并将其运用在系统可靠性建模与定量评估中[1,2]。在这些文献中，针对零部件的动态失效行为，Dugan 等定义了一组完善的动态逻辑门来描述零部件的动态失效特征，解决了具有时间相关性、功能相关性等特性的系统可靠性建模问题。

在定量评估方面，许多研究人员提出了不同的方法来求解复杂系统的动态故障树模型[3-5]。由于模型的规模随着系统的规模和复杂性的增长而呈指数增长，计算问题成了这类系统的可靠性定量评估工作的主要难点。基于马尔科夫模型[1]的求解方法是一种应用较为普遍的状态空间方法，但由于该模型是一种全局状态空间模型，其计算量会随系统规模的增长而发生状态爆炸，因此直接采用该方法是不可取的。Amari[3]提出一种基于复合梯形积分公式的数值积分方法，在不需把动态故障树转化成马尔科夫模型的条件下求解动态逻辑门。对于具有动态逻辑门以及重复基本事件的故障树，在已知基本事件的概率分布以及条件分布的情况下，该方法能够精确地对系统可靠性进行评估。Rao 等[5]提出一种基于蒙特卡洛的仿真方法，该方法可以用于失效分布及维修分布为非指数分布的情形，也能处理动态逻辑门级联的情况。Bobbio 等[6,7]提出一种基于贝叶斯网络的方法来简化动态故障树求解过程中的复杂性问题。然而，这几种故障树分析方法都没有考虑系统中的模糊不确定性问题。

在国家自然科学基金、国家 863 计划项目等的资助下，本文在现有动态故障树分析方法的基础上，基于贝叶斯网络及模糊数学理论，提出了新的动态系统可靠性分析方法，弥补了当前系统可靠性分析方法的不足，使得系统可靠性建模与分析理论体系更加完善，且更有利于系统可靠性方法在实际复杂工程系统中的应用。

1.2 故障树分析方法的国内外研究现状

1.2.1 常规故障树分析方法的发展现状

1961 年，美国贝尔实验室的 Watson[8]首次提出故障树分析方法，并将其成功地应用于民兵式导弹发射控制系统的分析设计中。随后，波音公司对故障树分析方法做了进一步研究并成功研制出故障树分析的计算机程序，为飞机的设计改进做出了重要贡献，同时使得故障树分析方法进入了以波音公司为中心的宇航领域。1965 年，在由华盛顿大学和波音公司联合主办的安全性研讨会上，发表了许多关于故障树的应用案例以及讨论该方法优越性的文章，标志着故障树分析方法作为一种复杂系统（如核反应堆等）安全性和可靠性分析的工具得到了广泛的关注和应用。1975 年，美国核管理委员会发表了关于核反应堆安全性研究的报告“商用轻水堆核电站事故危险性评价”。该文献用 1300 页阐述了 20 世纪 60 年代发展起来的事件树分析（Event Tree Analysis, ETA） 和故障树分析方法在核电站中的应用，详细分析了核电站可能发生的事故并给出了应对措施，保障了核电站的可靠

性和安全性[9,10]。此后，故障树分析方法逐渐由宇航领域和核工业领域渗透到其它工业领域，在机械、电子、化工、电力等领域得到了广泛的应用。故障树分析方法的研究主要集中在以下三个方面：

（1）故障树建模。Fussell[11]提出一种自动建树的方法：合成树模型（Synthetic Tree Model, STM）。他还提出针对电气系统故障树建模的计算机程序 DRAFT[12]。STM 方法的思想是先通过失效转移函数对系统中的各个部件进行建模，然后组合各个部件的转移函数得到系统的故障树。Power 和 Tompkins[13]针对化工系统提出一种故障树自动创建方法，该方法使用一种输入输出模型来描述系统中部件的变量及失效事件之间的局部因果关系。Salem 等[14,15]提出一种自动建树的计算机程序 CAT，该方法可用于核工业系统、机械系统、电气系统及液压系统等系统的故障树建模。Lapp 和 Powers[16]提出一种故障树合成方法（Fault Tree Synthesis），该方法首先采用图模型的方式来表达系统，然后采用故障树合成算法从图模型得到系统的故障树结构。

（2）故障树定性分析。Vesely 和 Narum[17]最早采用确定性方法开发出了故障树定性分析的计算机程序 PREP。Fussell 和 Vesely[18]在此基础上提出了不需要组合试验的替代算法，该算法的核心思想是对与门增加割集的容量，对或门增加割集的数量。Fussell 等[19]进一步运用上述算法开发出了计算机程序 MOCUS，该程序是一种自顶向下的方法，只能分析由与门和或门构成的故障树模型。Pande 等[20]开发出自底向上的计算机程序 MICSUP 来获取故障树模型的最小割集，该方法从最底层逻辑门开始逐层向上分析，直至得到顶事件的所有最小割集。

（3）故障树定量评估。顶事件失效概率的计算可以通过结构函数来获得，也可以用最小割集通过容斥原理等方法来计算。美国核管理委员会的 WASH-1400 报告采用了一种蒙特卡洛仿真程序 SAMPLE[9]，该程序运用一种简化的数学模型来计算系统的可靠性分布。Garrick[21]和 Kongsoe[22]分别提出一种基于蒙特卡洛仿真的计算机程序 SAFTE 和 REDIS 来计算系统的不可靠度。黄洪钟等[23]提出一种基于 BDD 的底事件排序方法，该方法除了考虑故障树中事件所在的层数对排序的影响之外，还考虑了重复事件、相邻事件以及逻辑门包含的事件数等因素，由上述四个指标共同决定底事件排序的优先级别。

上述故障树分析方法都是建立在不考虑系统动态失效特性和零部件失效的不确定性之上的常规故障树分析方法，其数学基础为布尔代数和概率论。这些方法在研究系统失效的各种直接和间接原因的基础上，建立事件之间的逻辑关系，通过定性分析得出全部最小割集，找出系统的薄弱环节，从而用最小割集的结构函数来描述系统故障的所有组合情况。同时在已知基本事件故障概率的情况下，运

用定量分析估计顶事件发生的概率并计算基本事件的重要度[24]。

由于受到失效机理认识水平、FTA 理论研究深度以及系统复杂性等因素的限制，早期的故障树分析方法相对简单，多数仅限于最小割集计算或定量分析等某一项分析功能。为了方便 FTA 在工程实际中的应用，在二十世纪 70 年代，基于 DOS 系统的 FTA 软件就已开发出来，但却存在诸多不足，使得 FTA 在实际运用上不够直观和形象[25]。

二十世纪 90 年代以来，FTA 与其它分析方法相结合，形成了许多复合技术，如故障模式影响分析（Failure Mode and Effects Analysis, FMEA）、故障模式影响与危害度分析（Fault Mode, Effects and Criticality Analysis, FMECA）、事件树分析等。二十世纪 80 年代以后，FTA 技术已经开始逐步应用于我国核工业、化工、电子、机械、交通和船舶等领域，并取得了较好的效果。随后，许多高校和科研机构陆续开发了 FTA 分析程序或软件[26]。

随着科学技术的迅猛发展，许多系统的复杂度不断提高，其失效模式与失效机理也越来越复杂，从而对系统的失效分析及可靠性评估变得越来越困难。由于客观世界中存在着各种不确定性因素，虽然传统故障树分析能很好解决随机不确定性问题，但在日益复杂的各种系统中普遍存在的模糊不确定性却很难精确量化，因此 FTA 正经历着由传统到模糊的发展过程。在日益复杂化、大型化的系统中，传统的二态假设已不能充分表达系统所处的状态，并且系统状态也不局限于静态，从而 FTA 逐步由二态发展为多态、由静态发展为动态。

1.2.2 模糊故障树分析方法的发展现状

传统故障树分析中，在评估顶事件失效概率时，往往把系统组成单元的失效概率看成确切的数值。但在很多系统中，由于系统环境的变化，通过部件的历史失效数据不能精确地获得其当前的失效率，同时那些无失效数据的单元失效率的确定也是值得研究的问题。因此 Tanaka 等[27]将模糊理论引入故障树分析中，采用模糊概率代替传统可靠性分析中的精确概率值，并根据模糊数学中的扩展原理，用梯形模糊数表示系统单元失效概率，并采用近似计算来实现模糊数之间的乘积运算。然而 Tanaka 的研究工作没有考虑故障树模型中事件之间的相关性等动态失效特性。

Furuta 等[28]基于模糊集合理论，运用隶属函数重新定义了顶事件的状态，并提出了基于模糊积分计算底事件重要度的方法，最后通过实例分析验证了该方法在结构失效分析中的有效性。Singer[29]对模糊故障树分析方法做了进一步研究。他运用 $L-R$ 型模糊数来描述底事件的发生概率，并定义了 $L-R$ 型模糊数的运算规

则，其中乘、除仍用近似的 $L-R$ 型模糊数表示，最后给出了一个工程应用实例。Sawyer 等[30]对机械系统进行了模糊故障树分析，他将底事件发生概率视为模糊数，并对模糊数取 λ 截集后进行运算。为了便于推导和计算，文中假设系统的组成单元是不可修和相互独立的，还假设底事件发生概率服从指数分布。Misra 等[31]针对多态系统提出了一种分析方法来计算顶事件发生的模糊概率。利用模糊概率向量建立多态部件的联合可能性分布，然后再利用扩展原理和非线性数学规划来估计顶事件发生的模糊概率。Geymayr 等[32]提出基于知识工程的模糊故障树分析方法来解决工业系统中可靠性、可用性、维修性和安全性的评估问题。Ferdous 等[33]提出一种基于模糊理论的计算机辅助故障树分析方法，这是一种进行故障树建模、最小割集确定以及顶事件发生概率分析的系统方法，它运用静态和动态结构分析和建模来实现模糊概率分析以及灵敏度分析。应用案例研究中模糊加权指数和割集重要度度量在敏感度分析（系统风险概率分析）以及改进设计中的作用进一步说明了此方法的有效性。Fujino 等[34]针对大多数决策分析中需要的是主观信息而不是故障树分析中的清晰的布尔表达式，通过运用布尔语言变量表达事件值，提出了一种模糊故障树方法。同时还提出了两种重要的逻辑门算子：模糊均值运算和逻辑求和运算。

Mentes 等[35]针对多点系泊系统提出一种模糊故障树分析方法，在模糊环境下针对操作失误以及人因失效对多点系泊系统配置的影响进行综合分析。风险辨识中的传统故障树分析不能有效地处理诸如人因失效的不精确事件，同时也没有考虑风险概率值的偏差。由于数据的缺乏，很难精确估计系统组件的失效率以及系统失效事件的概率值。Mentes 等针对这一问题提出了一种基于模糊集合理论的故障树分析方法，并应用到多点系泊系统中。同时基于模糊加权指数（Fuzzy Weighted Index, FWI）提出一种新的灵敏度分析法来度量基本事件对顶事件发生概率的影响程度。

Dong 等[36]运用模糊故障树方法研究了石油天然气传输管道的模糊概率估计问题。他把模糊集合理论与专家启发式语言相结合来评估顶事件发生的模糊概率。Shu 等[37]把模糊集合引入印刷电路板装配的故障树分析中，根据专家的知识和经验构造底事件失效可能性值，藉此提出直观的模糊故障树分析算法来计算系统部件的故障概率区间，找出关键部件为管理决策提供依据。何俐萍和黄洪钟等[38]基于模糊逻辑与可能性测度，提出了一种新的故障树分析方法来弥补统计数据不足的问题，定义了失效可能性，并以可能性理论来表达模糊变量，把故障树中用自然语言描述的子事件视作一组弹性约束的模糊变量。与以往的模糊故障树方法不同的是，该方法整合了可能性方法与基于推理的模糊逻辑，能够用于创建相应的专

家知识数据库。Song 等[39]基于 T-S 模型提出一种新颖的故障树分析方法（TS-FTA），该方法以模糊可能性及模糊变量表达事件发生的取值，以 T-S 模型导出的 T-S 模糊门表达上下层事件之间的失效逻辑关系。运用该方法能够处理失效机理以及部件故障概率无法精确获取的情形。Chang 等[40]对不同底事件失效的可能性分布给出故障隶属函数，运用故障树分析、模糊集合的 α-截集及区间运算来获得系统的故障概率的区间值和可靠度区间值，还改进了 Tanaka[27]等对模糊故障树的定义，并将其应用范围扩展到适合不同隶属函数下的模糊故障树分析。Cheng 等[41]运用直觉模糊集合理论对天然气终端的紧急关闭系统进行了故障树分析，构造了直觉模糊故障树的概率区间和可靠度区间，提出了一种算法来识别系统的关键部件并确定系统的最弱路径。Dokas 等[42]运用模糊专家系统、故障树分析以及互联网技术对填埋场运行管理进行了可靠性分析研究。

Zhao 等[43]运用模糊故障树分析法对盾构隧道段进行了失效风险分析。通过详细分析风险事故的潜在失效模式及其影响因素，提出了一些有效的控制措施。Abdelgawad 等[44]提出一种模糊可靠性分析器（Fuzzy Reliability Analyzer, FRA）来对故障树进行自动的定性和定量分析，该方法的主要特点是用专家语言代替精确值来评估基本事件的发生概率。Mao 等[45]运用模糊故障树分析方法对消防系统中的自动供水系统进行了可靠性分析。Deshpande 等[46]提出一种模糊故障树框架对氨水箱的分离器和储氨罐进行了可靠性分析。作者在文中还提出一种估计模糊事件可能性的方法，并通过应用研究验证了其有效性。Kumar 等[47]用基于 *L-R* 型三角模糊集的直观模糊故障树对计算机安全系统进行了可靠性分析。米金华、李彦锋和黄洪钟等[48]运用模糊故障树方法对数控加工中心液压系统进行了可靠性分析。基于模糊集合理论和证据理论，Ferdous 等[49]提出一种方法来对过程系统概率风险评估框架中的不确定性问题进行分析研究。Ferdous 等基于相关系数提出一种方法来表达事件树或者故障树中的事件及基本事件的相关性，并应用实例分析验证了该方法的有效性。Chen 等[50]运用基于梯形模糊数的故障树分析方法分析了飞机座舱压力调节系统的可靠性，计算了顶事件的发生概率及底事件的重要度。Kumar 等[51]运用实数编码遗传算法及模糊 Lambda Tau 方法对垃圾清理机械手进行了可靠性分析，运用遗传算法获得了平均故障间隔时间以及平均维修时间的最优值。Celik 等[52]提出了基于风险的故障树建模方法来提高船运事故调查的执行效率。Celik 等在联合风险评估框架下结合结构故障及船上技术系统失效等因素提出了一种模糊扩展故障树分析方法。实例研究表明，运用该方法能够帮助事故调查人员查明船运事故中技术失效、误操作以及操作规程短缺等事件发生的概率。杨建平和黄洪钟等[53]应用证据理论来量化故障树分析中存在的不确定信息。基于能双可

靠性理论，黄洪钟等[54]以可能性测度来表达事件的失效行为，定义了并联系统能双故障树的结构函数。

1.2.3 动态故障树分析方法的发展现状

现代复杂工程系统的失效过程通常伴随着与失效时间和失效顺序相关的复杂动态特征，Dugan[1,2]提出一种动态故障树分析方法（DFTA）来解决这类复杂系统的可靠性建模与评估问题。Dugan 定义了一组动态逻辑门来描述失效优先性、顺序相关性及功能相关性等动态失效特征，并提出用马尔科夫模型来求解由这些逻辑门组成的复杂故障树模型。为便于该建模框架及求解方法的实施，Dugan 等[55,56]还建立了动态故障树分析的软件平台 DIFtree 和 Galileo。这两个软件都能对包含有硬件故障、软件故障以及人因故障的系统进行可靠性建模与分析。Anand 和 Somani[57]利用分解的方法对具有失效相关性的系统提出一种层次故障树分析方法，首先检测故障树的独立子树，再分层求解。求解的过程中只需要对某些动态模块用马尔科夫模型来分析，而不用对整个故障树应用马尔科夫模型来分析。针对故障树模型中输出事件的发生依赖于输入事件发生顺序的情况，Long[58]等提出一种分析顺序失效逻辑的概率模型，并由该模型导出了具有任意输入个数时输出事件发生概率的多重积分公式。Cepin 和 Mavko[59]从概率风险分析和可用性分析的角度考虑时间因素，提出一种动态故障树分析方法。该方法能够提供一些安全告知程序，比如合理规划安全设备的停机，通过该方法的使用能够提高系统的可用度。针对具有相依底事件的故障树，Sun 和 Andrews[60]提出一种方法来识别故障树中相互独立的模块。Boudali 等[61]提出一种应用输入/输出交互式马尔科夫链来分析动态故障树模型的方法。该方法能在一定程度上缓解连续时间马尔科夫模型的状态空间爆炸问题，并且能够按照模块化的方式来实施建模。Bucci 等[62]结合马尔科夫建模方法与元胞映射技术来创建动态故障树模型，克服了常规故障树方法在动态系统可靠性建模中的一些不足。Merle 等[63]基于布尔代数提出一种新的动态故障树分析方法，该方法把事件作为时间变量来处理，并定义了 BEFORE 和 SIMULTANEOUS 时间算子。在具有多个优先动态门重叠及重复底事件的情况下，利用该方法能够导出顶事件的结构函数。在 DFTA 的求解方法中，解析法和模拟法具有较强的理论基础，得到了广泛的研究与应用。但是这些方法都具有相同的局限性：随着故障树规模的增长，求解过程会发生状态空间组合爆炸或者仿真时间过长的问题。针对这些问题，Chiacchio[64]提出一种基于威布尔分布的合成算法，该算法能够解决底事件不可修且服从任意失效分布的 DFT 的求解问题，并且该算法中包含传统的层次分析技术，通过对独立子树的模块化分析能够大大降低模型

求解时间。Wang 等[65]基于中心极限理论提出一种两态冷备份系统可靠性分析的近似模型，该模型能够高效地估计具有两态部件及任意失效时间分布的冷备份系统的可靠性，并通过一些不同失效分布的 k-out-of-n 冷备份系统验证了该方法的精度和效率。针对传统故障树在复杂系统可靠性分析时的不足，Lindhe[66]提出一种基于马尔科夫方法的近似 DFT 计算方法，这种近似 DFT 计算方法通过标准蒙特卡洛模拟实现，并且不需要对整个马尔科夫模型进行模拟，因此简化了模型建立和求解的过程。此外，他们还提出两种逻辑门来对系统的失效补偿能力进行建模分析。

动态系统失效行为的时间相关性使得其 DFT 分析非常复杂，为了有效地对这种系统进行可靠性定量分析，Zhang 等[67]提出一种应用于 DFT 的定量分析方法。他们首先提出扩展顺序割集的概念，顺序割集包含时间逻辑关系，与普通割集相比具有更强的建模能力。其次生成最小扩展顺序割集，并对每个割集中的基本事件做冲突检测、时间约束缩减以及拓扑排序。最后采用组合分析的方法来得到系统的可靠性。基于状态空间的动态故障树分析方法把系统模型视为连续时间马尔科夫链（Continuous-Time Markov Chain, CTMC）模型。这种方法不适合于求解存在多重语义解释的动态故障树模型。Boudali[68]引入一种动态故障树的严密语义解释，其中复合 DFT 的语义由各个部件的语义解释以直观透明的方式产生。这不仅使得故障树模块之间的相互影响更易理解，而且也能在一定程度上缓解模型求解时的状态爆炸问题。

1.3 本文的主要研究内容

针对上述系统可靠性及故障树分析方法中存在的问题，本文拟对存在动态失效特征及模糊不确定性的系统展开分析研究。主要研究内容如下：

（1）基于模糊马尔科夫模型的动态故障树分析方法研究。现有的动态故障树分析方法中，主要有基于马尔科夫模型的状态空间法、数值积分方法和蒙特卡洛仿真方法等。迄今当系统存在模糊不确定性时的研究还很缺乏。本文将基于马尔科夫模型，对零部件及系统的失效数据存在模糊不确定性时的动态故障树分析方法展开研究。

（2）基于离散时间贝叶斯网络的动态故障树可靠性评估模型。作为处理不确定性知识推理的强有力的工具，贝叶斯网络对随机不确定性知识的表达和推理具有很强的处理能力。针对基于马尔科夫模型的动态故障树求解方法中存在的状态爆炸问题，本文拟采用贝叶斯网络替代马尔科夫模型来求解动态故障树模型，对运用贝叶斯网络模型进行系统可靠性建模与概率推理展开研究。

（3）模糊数据下基于连续时间贝叶斯网络的动态故障树分析方法研究。贝叶

斯网络能够有效地解决动态故障树的模型转化及概率推理问题。当系统中存在模糊不确定性时，需要考虑如何应用贝叶斯网络来对事件发生的模糊概率进行表达与推理。本文将研究考虑模糊不确定性的基于贝叶斯网络的系统可靠性建模与定量评估方法。

（4）考虑共因失效的动态故障树分析方法研究。共因失效是现代复杂工程系统中普遍存在的现象。本文将对共因失效的建模方法展开研究，运用实例分析阐述共因失效对复杂关键系统可靠性所产生的重大影响。

本文共分六章，拟分别对上述问题中的可靠性建模及求解方法展开研究。其中，第二至第四章主要致力于解决复杂系统动态故障树的建模、模型转化及求解等问题。第五章对存在共因失效的复杂系统故障树分析问题展开理论研究与实例分析。论文各章主要内容如下：

第一章为绪论，主要介绍论文的研究背景、意义和研究现状，并概述本论文的主要研究内容。

第二章研究存在模糊不确定性下动态故障树模型的建立及其向马尔科夫模型转化的方法，并研究模糊失效概率及模糊可靠度的求解方法。

第三章研究基于离散时间贝叶斯网络的动态故障树分析方法。建立各种逻辑门的贝叶斯网络条件概率分布公式，并对实例系统展开动态故障树及贝叶斯网络建模与定量评估。

第四章研究用模糊数建立连续时间贝叶斯网络中节点的模糊失效密度函数及模糊分布函数，用参数规划方法求解系统节点的模糊失效密度函数及模糊分布函数，从而求得系统的可靠度函数。

第五章研究共因失效问题。用显式建模方法对某系统进行共因失效建模，并用平方根模型对共因失效的影响做定量分析。

第六章对本文的研究工作进行总结，在此基础上对未来的研究工作进行展望。

第二章 基于模糊马尔科夫模型的动态故障树分析

动态故障树分析方法对具有动态失效逻辑的系统具有较强的建模与分析能力，并且得到了较为广泛的应用。然而，对于一些实际的工程系统，由于系统模型复杂、失效数据缺乏等原因，很难获得零部件精确的失效率。本章基于马尔科夫模型和模糊数学理论，对动态故障树分析方法展开研究。

2.1 引言

故障树分析方法是一种逻辑性强、表达直观的系统可靠性分析方法。它被广泛用于复杂工程系统的定性和定量可靠性建模与分析中。故障树模型以一种图形化的表达方式，通过与门、或门、表决门等逻辑门描述了导致系统失效的部件失效事件及其组合，并由结构函数给出其数学描述[69,70]。在可靠性和安全性领域工作的众多学者先后提出了采用故障树对复杂系统进行可靠性建模和评估的多种方法[72-75]。

然而，传统故障树的建模能力具有很大的局限性。实际工程系统中的零部件之间的失效往往存在失效优先性、顺序相关性和功能相关性等动态失效特性，应用传统的静态故障树对这些系统建模会面临很大的困难。基于马尔科夫链模型的动态故障树分析方法扩展了静态故障树分析方法的功能，通过引入一组动态逻辑门来表达事件之间的这种复杂相关性，解决了动态失效特征的建模问题[1,2]。

上述基于状态的故障树分析方法能够处理复杂系统的可靠性建模与评估问题，并且通过这些方法能够获得顶事件失效概率的精确值。在系统可靠性分析过程中，零部件的正常工作或者失效状态都被视为确定的。也就是说，零部件要么处于工作状态，要么处于失效状态，而且零部件处于这两种状态的概率也是确定的。然而，在实际工程系统中并不总是这样的，系统和零部件的状态及其概率常常存在由各种因素导致的模糊性，具体原因如下：

（1）零部件或者系统的状态退化是随着时间的推移逐步进行的，因此失效事件的发生本质上来讲也不是在某一个时间点上瞬间发生的，而是随着系统服役时间的推移而逐步产生的。由于不精确测量或者人为原因等不确定性因素的影响，常常不能准确的辨别零部件或者系统的实际状态，由此产生了状态的模糊性。

（2）由于系统复杂度较高，冗余备份等关系复杂，将导致故障树建模过程发生误差。同时，由于失效分析过程中的主观判断等原因，也会导致所建的故障树

模型与实际系统不完全相符。这些原因将会导致故障树模型中失效逻辑的模糊性。

（3）零部件或者系统的失效行为的阶段性和复杂性，以及系统运行环境的动态性，导致很难精确获得基本事件的失效概率。对于一些复杂、昂贵的系统或设备，获取足够多的失效数据存在很大困难。对于零部件失效率极低的产品或者新产品而言尤其如此。因此，系统和零部件的失效概率存在数据的模糊性。

在这种由于个人主观判断或客观原因导致系统分析中存在模糊性的问题时，Zadeh 提出的模糊集合理论是处理这种问题的有效方法[77,78]。在把模糊集合理论引入故障树分析中进行系统可靠性分析方面业已发表了大量有价值的学术论文。Misra 和 Weber[79]，Liang 和 Wang[80]，在其论文中基于扩展原理描述了故障树中模糊算子的运算法则。为解决概率风险评估中的不确定性问题，Singer[29]，Lai[81]和 Sawyer 等[30]把模糊集合理论引入到安全性与可靠性建模过程中。基于 Posbist 可靠性理论，黄洪钟等[54]提出了一种 Posbist 故障树方法用于解决单调关联系统可靠性分析问题。在他们的方法中，事件失效行为用概率测度来表达，并定义了单调系统 Posbist 故障树的结构函数。刘宇和黄洪钟[86,87]基于模糊集理论与马尔科夫模型对多态系统进行了可靠性和维修性分析。

为同时解决系统中存在的动态失效特征及模糊不确定性这两个问题，本章提出一种基于模糊马尔科夫模型的动态故障树分析方法。用动态故障树建立系统的可靠性模型。用三角模糊数来描述底事件发生概率的模糊性，并同时描述马尔科夫模型中状态之间的转移率。使用模糊数的扩展原理及参数规划方法来计算故障树顶事件失效的模糊概率值的隶属函数。最后，通过算例验证该方法的正确性和有效性。

2.2 动态故障树分析方法

2.2.1 动态逻辑门

常规故障树分析方法的主要不足之一是不能对系统中的顺序相关性进行建模。为解决该问题，Dugan 等[1,2,76]提出一种新的可靠性分析方法——动态故障树方法。该方法引入一系列动态逻辑门来描述系统的时序规则和动态失效行为。主要包括优先与门（Priority-AND Gate, PAND）、功能相关门（Functional Dependency Gate, FDEP）、顺序相关门（Sequence Enforcing Gate, SEQ）和备件门（Spare, SP）等四种典型的动态逻辑门。下面主要从动态门的输入事件和失效机理两个方面来介绍这四种动态逻辑门。

（1）优先与门（PAND）

输入事件：假设优先与门有两个输入事件 A 与 B，这两个输入事件可以是基本事件或者其它逻辑门的输出事件。

失效机理：优先与门的失效机理定义为，当基本事件按照从左至右的顺序发生时，输出事件发生。例如，对于具有两输入的优先与门，当 A 先发生 B 后发生时，系统输出事件为失效状态。优先与门的图形符号如图 2-1 所示。

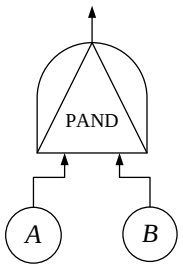


图 2-1 优先与门

（2）功能相关门（FDEP）

输入事件：功能相关门通常包含一个触发事件（为基本事件或者其它逻辑门的输出事件）和一个或者多个相关事件。相关事件在功能上依赖于触发事件的发生。

失效机理：当触发事件发生时，所有相关事件被强制发生。功能相关门的图形符号如图 2-2 所示。

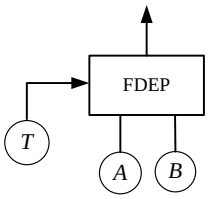


图 2-2 功能相关门

（3）顺序相关门（SEQ）

顺序相关门强制其输入事件按照特定的顺序发生，而不会按照其它的顺序发生失效。顺序相关门与优先与门类似，都表示基本事件的时序性，它们的区别在于：顺序相关门中的输入事件不能按照任意顺序失效；而优先与门可以以任意顺序失效，只有特定顺序的失效才会触发其输出事件的失效。

输入事件：顺序相关门的输入事件只能是基本事件，其它逻辑门的输出不能作为顺序门的输入事件，但顺序门的输出事件可以作为其它门的输入事件。

失效机理：如图 2-3 所示，顺序相关门有 n 个输入事件，只有当所有事件发生，

且按照从 1 到 n 的顺序依次发生时，输出事件才会发生。

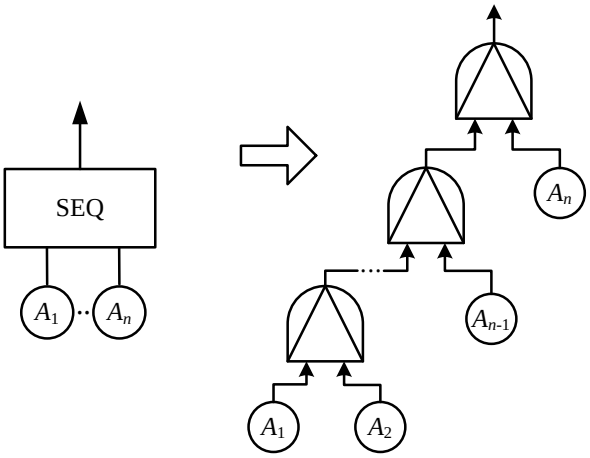


图 2-3 顺序相关门

（4）备件门

备件门通常有一个主输入部件和一个或多个备份部件，备件具有与主件相同的功能和失效率。备件按照失效机理的不同可以分为三类：冷备份部件（CSP），温备件（WSP）和热备件（HSP）。这三类备件对应于三类备件门，其图形符号如图 2-4 所示。

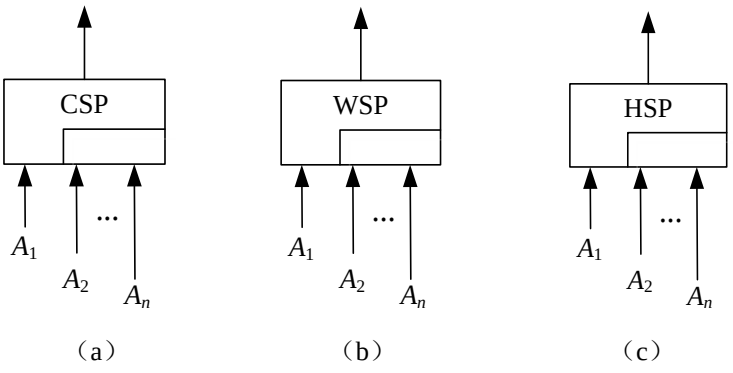


图 2-4 三种备件门

（a） 冷备件门；（b）温备件门；（c）热备件门

冷备件门有两种输入类型，基本输入和可选输入。基本输入在系统开始运作时就进入工作状态，而可选输入处于非工作状态；只有当基本输入产生故障后，可选输入（冷备件）继续接替工作，直至冷备件也完全失效。

温备件门不同于冷备件门的是，冷备件门在进入工作状态前视为无失效，而温备件却有可能失效，但其失效率与工作状态失效率不同，为贮备失效率。因此

系统具有两种失效过程：一是温备件保持贮备状态，当基本输入失效，备件转为工作状态；二是温备件先于基本输入失效，此时当基本输入失效，整个冗余系统就失效。

热备件门是在基本输入工作的同时，备件也处于工作状态。当基本输入失效时，备件立即转换为基本输入，以保证系统处于正常工作状态。

根据以上三种备件门的工作机理，假设部件的失效率为 λ，当作为备件使用时，其失效率可描述为 $\alpha\lambda$。分析可得：$\alpha=0$ 时，部件为冷备件；$\alpha=1$ 时，部件为热备件；$0<\alpha<1$ 时，部件为温备件。

2.2.2 马尔科夫模型

在动态故障树中，顺序割集的发生概率不仅与所包含的事件组合有关，而且与这些基本事件的发生顺序相关。因此，马尔科夫模型被用来建模动态系统的失效过程以及评价系统的可靠性。

假设 T 是无限实数集，若对每一个 $t\in T$，$X(t)$ 是一个随机变量，则称 $\{X(t),t\in T\}$ 为随机过程。当一个随机过程满足以下条件概率关系时，该随机过程被称为马尔科夫过程。

$$\begin{aligned}P\{X(t_n)=x_n\,|\,X(t_1)=x_1,X(t_2)=x_2,\cdots,X(t_{n-1})=x_{n-1}\}\\ =P\{X(t_n)=x_n\,|\,X(t_{n-1})=x_{n-1}\}\end{aligned}\tag{2-1}$$

这里 $x_i\in S$，S 是随机过程的状态空间，且

$$t_1<t_2<\cdots<t_{n-1}<t_n$$

式(2-1)体现了马尔科夫过程的无记忆性，这种无记忆性表明，随机过程在 t_i 时刻处于状态 x_i 的概率只依赖于 t_{i-1} 时刻的状态，而与之前时刻的状态无关。通常情况下，马尔科夫过程的状态空间和时间参数可以是离散或连续的，马尔科夫链就是时间离散状态空间离散的马尔科夫过程。

在动态系统中，系统的失效过程可以用马尔科夫过程来描述。

假定系统具有 n 个状态 $s_i(i=1,2,\cdots,n)$，则可以用马尔科夫过程

$$\{S(t),\ t\geq 0\}$$

来描述该系统的失效过程。其中，$s_i\in H$，H 是马尔科夫过程的状态空间。

以符号 $\lambda_{i,j}$ 表示由状态 i 到状态 j 的转移率，则系统的失效过程可以用图 2-5 所示的状态转移图来描述。

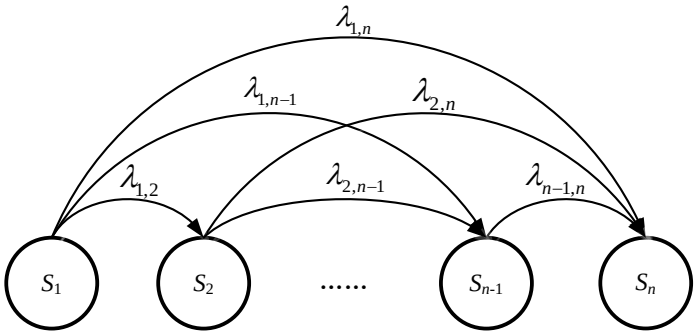


图 2-5 马尔科夫模型状态转移示意图

图 2-5 中，s_1 是系统完好状态，s_2 至 s_{n-1} 为系统中有零部件失效后的中间状态，s_n 为系统失效状态。

令 $p_i(t),\ i=1,2,\cdots,n$ 为时刻 t 系统处于各个状态 $s_i(i=1,2,\cdots,n)$ 的概率，上述马尔科夫模型对应的微分方程组如下：

$$\begin{cases} \dfrac{dp_1(t)}{dt} = -p_1(t)\sum\limits_{j=2}^{n}\lambda_{1,j} \\ \dfrac{dp_i(t)}{dt} = \sum\limits_{j=1}^{i-1}p_j(t)\lambda_{j,i} - \sum\limits_{j=i+1}^{n}p_i(t)\lambda_{i,j},\ 1<i<n,\ t\geq 0 \\ \dfrac{dp_n(t)}{dt} = \sum\limits_{j=1}^{n-1}p_j(t)\lambda_{j,n} \end{cases} \tag{2-2}$$

该模型的初始条件为：

$$\begin{cases} p_1(0)=1, \\ p_i(0)=0, i=2,\cdots,n \end{cases}$$

求解上述模型即可得到第 n 个状态的概率 $p_n(t)$，该值对应于故障树中顶事件的发生概率，即系统在 t 时刻的失效概率。

2.2.3 动态故障树向马尔科夫模型的转化

当故障树中具有一个或者多个动态逻辑门时，这种故障树就被称为动态故障树。针对马尔科夫模型的图解优势，将动态逻辑门转换为马尔科夫模型，能够有效解决动态逻辑门的求解问题。将动态逻辑门输入事件的状态组合作为马尔科夫模型的基本状态，同时马尔科夫模型的状态转移概率设置为输入事件的故障概率，这样就能够将动态逻辑门转换为马尔科夫模型。下面将介绍几种典型的动态逻辑门转换成的相对应的马尔科夫模型。本章假设零部件失效服从指数分布且为不可修的产品。

（1）优先与门（PAND）

两输入的优先与门转化为马尔科夫模型如图 2-6 所示。

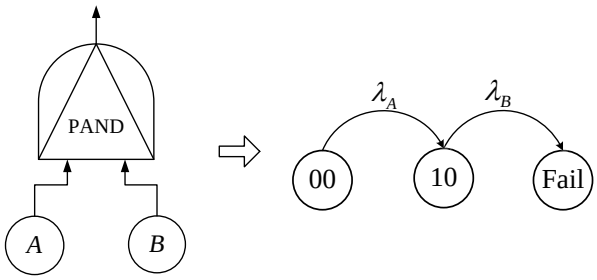


图 2-6 优先与门转换为马尔科夫模型

图 2-6 中，“00”代表两部件均正常工作的系统状态，“10”代表部件 A 失效而部件 B 工作的系统状态，“Fail”即指输出事件发生，系统失效的状态；λ_A 和 λ_B 分别表示部件 A 与 B 的失效率，分别对应图中的两个状态转移率。

（2）功能相关门（FDEP）

根据 2.2.1 节介绍的功能相关门的工作原理及失效机理，FDEP 向马尔科夫模型的转换如图 2-7 所示。其中 λ_A 和 λ_B 分别表示输入部件 A 与 B 的失效率，λ_T 为触发事件 T 的工作失效率。“000”为三个部件均工作的系统状态，“001”为只有部件 B 失效的系统状态，“010”为只有部件 A 失效的系统状态，“Fail”为系统失效状态。状态之间的转移如图 2-7 所示。

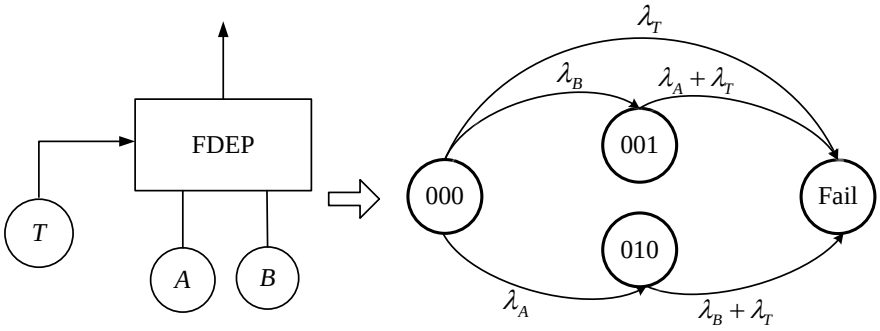


图 2-7 功能相关门转换为马尔科夫模型

（3）顺序相关门（SEQ）

与前两种动态逻辑门类似，用 λ_i 表示顺序输入事件 A_i 的失效率。将顺序相关门转换成马尔科夫模型的过程如图 2-8 所示。其中各个状态的含义与前面的马尔科夫模型中的状态类似。

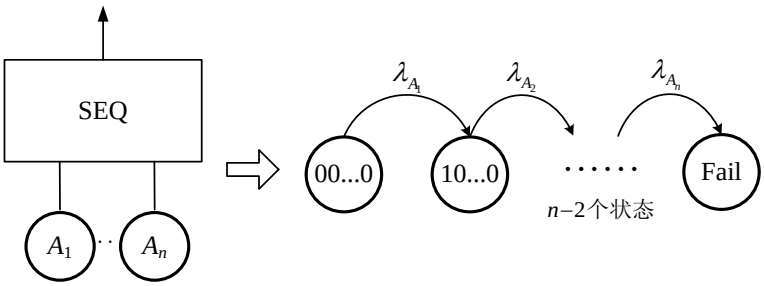


图 2-8 顺序相关门转换为马尔科夫模型

（4）备件门

如图 2-9, 2-10, 2-11 所示为冷备件、温备件和热备件门转换成相应形式的马尔科夫模型。其中 A 为基本输入，S 表示备件；λ_A 和 λ_s 分别表示 A 与 S 处于工作状态时的失效率。其中各个状态的含义与两输入优先与门的马尔科夫模型中的状态相同。根据三种门的失效机理可知，温备件门中备件在基本输入 A 失效前也具有一定失效率，将其表示为 λ_s'，此时 $\lambda_s' < \lambda_s$；当 A 失效时，S 转为全额工作，这时 $\lambda_s' = \lambda_s$。对于热备件门，备件 S 一直处于工作状态，所以其 $\lambda_s' = \lambda_s$。

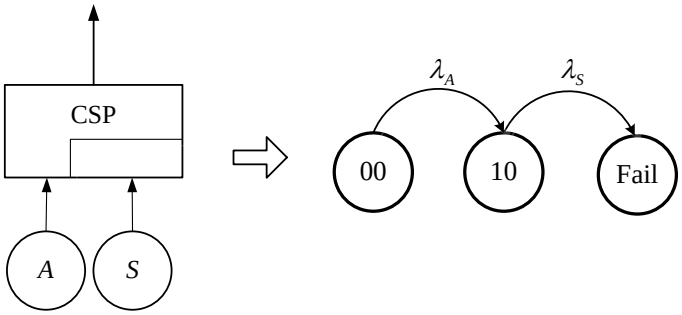


图 2-9 冷备件门转化为马尔科夫模型

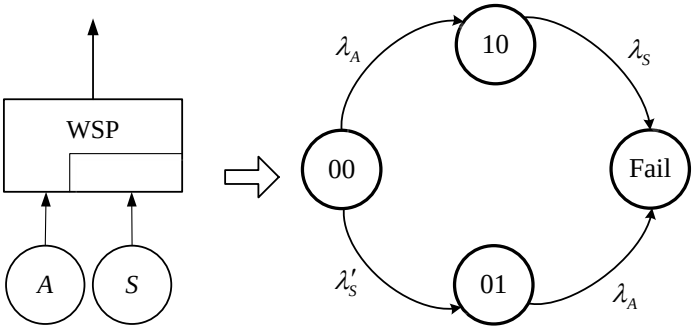


图 2-10 温备件门转化为马尔科夫模型

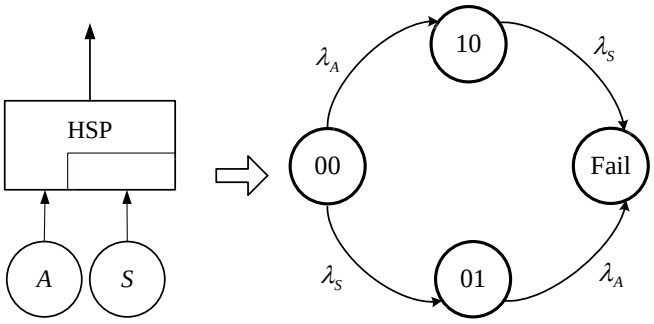


图 2-11 热备件门转化为马尔科夫模型

2.3 模糊集的基本概念及扩展原理

2.3.1 模糊集

在复杂工程系统可靠性评估中，存在着两种不确定性，随机不确定性和认知不确定性。Zadeh 提出一套系统的数学理论（模糊集合理论）来处理工程中常常存在的一类认知不确定性——模糊不确定性问题[77,78]。

给定论域 U 上的集合 $\tilde{A}$，对于任意 $u \in U$，存在一个与 u 对应的实数 $\mu_{\tilde{A}}(u) \in [0,1]$，该值确定了元素 u 对集合 $\tilde{A}$ 的隶属程度。集合 $\tilde{A}$ 叫做模糊集合，数值 $\mu_{\tilde{A}}(u)$ 叫做元素 u 对模糊集合 $\tilde{A}$ 的隶属度。该映射可以表示如下：

$$\mu_{\tilde{A}} : U \to [0,1]$$
$$u \mid \to \mu_{\tilde{A}}(u)$$

对于模糊集合 $\tilde{A}$，如果它是正规的凸模糊集，则称之为模糊数。三角模糊数、正态模糊数和梯形模糊数是最常用的几种模糊数。

典型的三角模糊数由其隶属函数定义，如式（2-3）所示：

$$\mu_{\tilde{A}} = \begin{cases} \dfrac{x-a}{b-a}, & a \le x < b \\ 1 \quad , & x = b \\ \dfrac{x-c}{b-c}, & b < x \le c \\ 0 \quad , & \text{其他} \end{cases} \tag{2-3}$$

典型的三角模糊数图形表达见图 2-12。

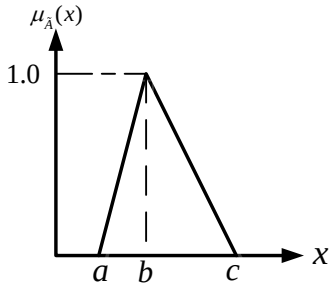


图 2-12 三角模糊数的隶属函数

2.3.2 扩展原理

Zadeh 提出模糊集合和模糊数的概念来表达和量化模糊信息。此外，Zadeh[77,78]还提出了扩展原理来定义模糊数之间的模糊运算法则。

给定论域 $R_i(i=1,2,\cdots,n)$中的一系列模糊数 $\tilde{X}_i(i=1,2,\cdots,n)$。$x_i \in R_i(i=1,2,\cdots,n)$是与论域 $R_i(i=1,2,\cdots,n)$及模糊数 $\tilde{X}_i(i=1,2,\cdots,n)$ 对应的变量。y 是实数域 R 中的变量。$f(x_1, x_2,\cdots,x_n)$是由变量 $x_i \in R_i(i=1,2,\cdots,n)$ 到变量 y 的映射。我们可以通过映射 $f(x_1, x_2,\cdots,x_n)$由模糊数 $\tilde{X}_i(i=1,2,\cdots,n)$ 诱导出一个新的模糊数 $\tilde{Y}$，通过扩展原理可以得到其隶属函数如下：

$$u_{\tilde{Y}}(y)=\sup_{\substack{x_i\in R_i\,(i=1,2,\cdots,n)\\ y=f(x_1,x_2,\cdots,x_n)}}\min(u_{\tilde{X}_1}(x_1),u_{\tilde{X}_2}(x_2),\cdots,u_{\tilde{X}_n}(x_n)) \tag{2-4}$$

根据扩展原理，模糊数 $\tilde{Y}$ 的 α 截集的区间如下：

$$\begin{aligned}\tilde{Y}_\alpha(y)&=[\min_{1\le i\le n} f(x;\mu_{\tilde{x}_i}(x_i)\ge\alpha),\max_{1\le i\le n} f(x;\mu_{\tilde{x}_i}(x_i)\ge\alpha)]\\&=[\tilde{Y}_\alpha^{\,L},\tilde{Y}_\alpha^{\,U}]\end{aligned} \tag{2-5}$$

于是，求解模糊数 $\tilde{Y}$ 的下界和上界问题可以转化为求解一组参数规划问题，参数规划构造如下：

$$\begin{aligned}&\tilde{Y}_\alpha^L=\min\ f(x_1,x_2,\cdots,x_n)\\&\text{subject to}\\&\tilde{x}_{1\alpha}^L\le x_1\le\tilde{x}_{1\alpha}^U\\&\tilde{x}_{2\alpha}^L\le x_2\le\tilde{x}_{2\alpha}^U\\&\qquad\vdots\\&\tilde{x}_{n\alpha}^L\le x_n\le\tilde{x}_{n\alpha}^U\end{aligned} \tag{2-6}$$

$$\begin{aligned}&\tilde{Y}_{\alpha}^{U}=\max\ f(x_1,x_2,\cdots,x_n)\\&\text{subject to}\\&\tilde{x}_{1\alpha}^{L}\le x_1\le\tilde{x}_{1\alpha}^{U}\\&\tilde{x}_{2\alpha}^{L}\le x_2\le\tilde{x}_{2\alpha}^{U}\\&\quad\vdots\\&\tilde{x}_{n\alpha}^{L}\le x_n\le\tilde{x}_{n\alpha}^{U}\end{aligned}\tag{2-7}$$

通过上述扩展原理可以很容易的获得模糊数在不同截集下的区间边界。

2.4 基于模糊马尔科夫模型的动态故障树（FDFT）

结合马尔科夫模型与模糊集合理论，提出一种新的可靠性分析方法——模糊动态故障树分析方法，来对同时具有与时间相关的动态失效特性和模糊不确定性的系统进行可靠性建模与分析。

在该方法中，首先根据系统的失效分析来建立系统的动态故障树模型，然后用马尔科夫模型来对具有 n 个状态的动态故障树作模型转化。在转化后的马尔科夫模型中，用模糊数来表示状态之间的转移率，从而使模型的状态转移率矩阵变为模糊状态转移率矩阵，形式如下：

$$\tilde{\mathbf{A}}=\left(\tilde{\lambda}_{i,j}\right)=\begin{pmatrix}\tilde{\lambda}_{1,1}&\tilde{\lambda}_{1,2}&\cdots&\tilde{\lambda}_{1,n}\\\tilde{\lambda}_{2,1}&\tilde{\lambda}_{2,2}&\cdots&\tilde{\lambda}_{2,n}\\\vdots&\vdots&\cdots&\vdots\\\tilde{\lambda}_{n,1}&\tilde{\lambda}_{n,2}&\cdots&\tilde{\lambda}_{n,n}\end{pmatrix}\tag{2-8}$$

模糊状态转移过程如图 2-13 所示。

图 2-13 中 S_1 表示系统完好运行状态，$S_i(i=2,\cdots,n-1)$ 表示系统中有零部件失效但系统仍能工作的中间状态，S_n 表示系统失效状态。

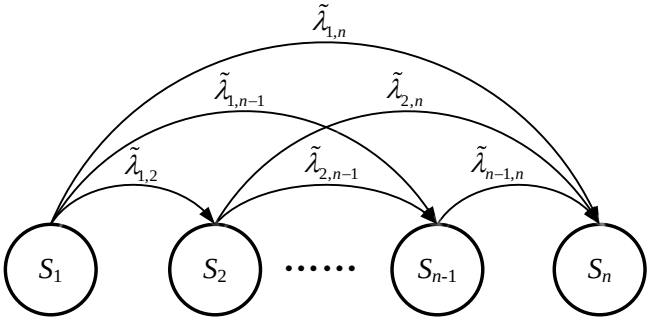


图 2-13 不可修系统的模糊状态转移图

于是，由模糊转移率构成的马尔科夫模型对应的微分方程如下：

$$\begin{cases} \dfrac{d\tilde{p}_1(t)}{dt} = -\tilde{p}_1(t)\sum\limits_{j=2}^{n}\tilde{\lambda}_{1,j} \\ \dfrac{d\tilde{p}_i(t)}{dt} = \sum\limits_{j=1}^{i-1}\tilde{p}_j(t)\tilde{\lambda}_{j,i} - \sum\limits_{j=i+1}^{n}\tilde{p}_i(t)\tilde{\lambda}_{i,j},\ 1<i<n,\ t\geq 0 \\ \dfrac{d\tilde{p}_n(t)}{dt} = \sum\limits_{j=1}^{n-1}\tilde{p}_j(t)\tilde{\lambda}_{j,n} \end{cases} \tag{2-9}$$

运用初始条件 $\tilde{p}_1(0)=1, \tilde{p}_i(0)=0(i\neq 1)$，对上述方程组采用 Laplace-Stieltjes 变换，得到线性方程组如下：

$$\begin{cases} s\tilde{p}_1(s)-1 = -\tilde{p}_1(s)\sum\limits_{i=2}^{n}\tilde{\lambda}_{1,i} \\ s\tilde{p}_i(s) = \sum\limits_{j=1}^{i-1}\tilde{p}_j(s)\tilde{\lambda}_{j,i} - \sum\limits_{j=i+1}^{n}\tilde{p}_i(s)\tilde{\lambda}_{i,j},\ 1<i<n \\ s\tilde{p}_n(s) = \sum\limits_{j=1}^{n-1}\tilde{p}_j(s)\tilde{\lambda}_{j,n} \end{cases} \tag{2-10}$$

求解上述方程组得到关于 s 的函数 $\tilde{p}_n(s)$，对其作 Laplace-Stieltjes 反变换，解得系统状态关于时间的概率分布 $\tilde{p}_n(t)$。由扩展原理即可求得该模糊数的上下限，即系统的模糊失效概率。

2.5 实例分析：数控加工中心主轴平衡回路可靠性分析

数控机床作为先进制造技术的基础装备，其技术水平是衡量一个国家工业现代化水平的重要标志。在数控机床中，加工中心占有特别重要的位置。加工中心一次装夹能集中完成多种工序，使得数控机床的切削利用率是普通机床的 3-4 倍，达 80%以上[82]。由于我国数控行业起步较晚，虽然国产数控机床在功能和性能方面一般能满足用户需要，但在产品质量稳定性方面存在诸多问题，如：故障频发、可靠性差、稳定性差、精度保持性差等[83]。液压技术作为实现现代传动与控制的关键基础技术之一，已成为机床等先进制造装备中不可缺少的重要基础技术。液压元件及其控制已发展成为综合的液压工程技术，液压传动与控制已成为现代机械工程的基本要素和工程控制的关键技术之一[84]。

2.5.1 数控加工中心液压系统简介

液压传动由于其结构紧凑、传动平稳、输出功率大且易于实现无级调速等优点，被广泛应用于各种机械设备中。虽然液压系统在整个机床中所占价值只有 5%-30%，并且其故障也只占机床故障的 14%左右，但由于液压传动往往用于实现

机床关键功能部件的转动和直线运动，是机床的重要组成部分，即使是液压系统一个小故障也会影响到整个机床的正常工作，因此机床液压系统能否可靠运行，对于机床的正常运行具有非常重要的作用[85]。

某型横梁移动龙门加工中心的液压系统主要由五部分组成：动力元件、控制元件、执行元件、辅助元件和液压油。本实例中所研究的液压系统由四个回路组成：主轴平衡回路、主轴松刀油路、C 轴夹紧与放松油路和 D 轴夹紧与放松油路。

该液压系统由一个 $N=2.2\text{kw}$，$n=1450\text{rpm}$ 的电机驱动一个流量为 $Q=8\text{L/min}$ 的定量泵同时对四个回路提供压力和流量。

这里选用主轴平衡油路来进行动态故障树及模糊马尔科夫模型建模与分析。

主轴回路的结构如图 2-14 所示。

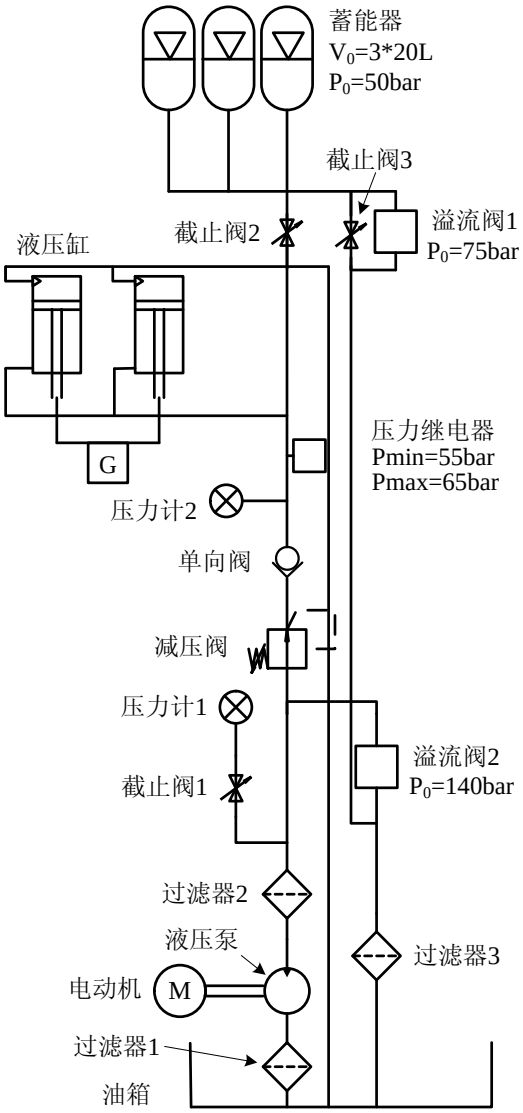


图 2-14 数控加工中心主轴平衡回路原理图

该主轴回路由 1 个油箱、1 个液压齿轮泵、3 个过滤器、3 个截止阀、1 个单向阀、1 个减压阀、2 个压力表、1 个压力继电器、2 个溢流阀、1 个气缸和蓄能器组成。

其工作原理简述如下：

液压油通过液压泵自油箱泵入主油路，当油路油压超过 140bar 时，经由溢流阀 2 流回油箱，使油压控制在 140bar 以下；减压阀使油路油压降低至 65bar；单向阀控制液压油的回流；液压继电器进一步控制油压在 55~65bar 之间，当油压超过 65bar 时，控制液压泵停止供油，低于 55bar 时启动液压泵供油；当油压超过 50bar 时，回路对蓄能器注入油液蓄压；当蓄能器回路油压高于 75bar 时，溢流阀 1 开始工作，使油液回流入油箱。

2.5.2 主轴平衡回路动态故障树建模

蓄能器除了作为辅助能源外，还起着补偿泄露、保持恒压、作紧急动力源的作用，因此在建模时把它作为串联单元来处理。选取“主轴回路压力不足”为顶事件。由于过滤器和压力表失效率很低，分析时不予考虑。其它事件如下：

X_1：压力继电器失效；X_2：液压泵故障；X_3：蓄能器故障；X_4：油箱故障；X_5：单向阀故障；X_6：液压缸故障；X_7：截止阀 2 故障；X_8：截止阀 3 故障；X_9：减压阀故障；X_{10}：溢流阀 1 故障；X_{11}：溢流阀 2 故障；M_1：供油故障；M_2：油路故障。

所建动态故障树如图 2-15 所示。

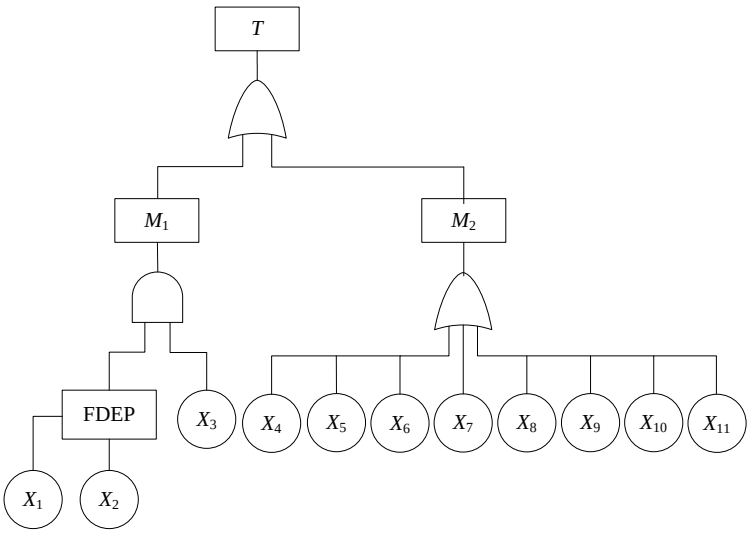


图 2-15 液压系统动态故障树

2.5.3 基于模糊马尔科夫模型的动态故障树定量评估

用三角模糊数表示基本事件的失效率，见表 2-1 所示。

表 2-1 三角模糊数表示基本事件的失效率数据

基本事件	模糊失效率 $\tilde{\lambda}$ ($\times 10^{-6}$/h)	基本事件	模糊失效率 $\tilde{\lambda}$ ($\times 10^{-6}$/h)
X_1	(0.0425,0.0500,0.0575)	X_7	(7.2250,8.5000,9.7750)
X_2	(11.4750,13.5000,15.5250)	X_8	(7.2250,8.5000,9.7750)
X_3	(6.1200,7.2000,8.2800)	X_9	(1.8190,2.1400,2.4610)
X_4	(1.2750,1.5000,1.7250)	X_{10}	(4.8450,5.7000,6.5550)
X_5	(4.2500,5.0000,5.7500)	X_{11}	(4.8450,5.7000,6.5550)
X_6	(0.0068,0.0080,0.0092)		

使用前述 FDFT 方法对图 2-15 的动态故障树模型进行可靠性分析。

首先把故障树模型转化为模糊马尔科夫模型，如图 2-16 所示。

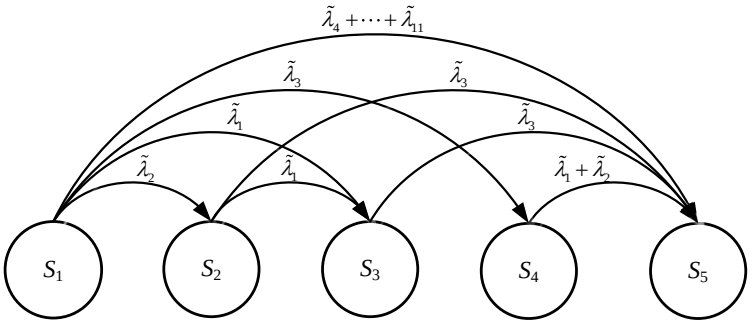


图 2-16 液压系统主轴平衡回路状态转移图

图 2-16 中，S_1：系统正常工作状态；S_2：液压泵故障导致供油系统部分故障状态；S_3：压力继电器故障导致供油系统部分故障状态；S_4：蓄能器故障导致供油系统部分故障状态；S_5：系统完全故障状态。

由状态转移图和各个基本事件的模糊失效率得模糊状态转移率矩阵如下：

$$\tilde{\mathbf{A}}=\begin{pmatrix} -\sum_{i=1}^{11}\tilde{\lambda}_i & \tilde{\lambda}_2 & \tilde{\lambda}_1 & \tilde{\lambda}_3 & \sum_{i=4}^{11}\tilde{\lambda}_i \\ 0 & -\tilde{\lambda}_1-\tilde{\lambda}_3 & \tilde{\lambda}_1 & 0 & \tilde{\lambda}_3 \\ 0 & 0 & -\tilde{\lambda}_3 & 0 & \tilde{\lambda}_3 \\ 0 & 0 & 0 & -\tilde{\lambda}_1-\tilde{\lambda}_2 & \tilde{\lambda}_1+\tilde{\lambda}_2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{2-11}$$

状态转移图对应的微分方程为：

$$\begin{cases} \dfrac{d\tilde{p}_1(t)}{dt} = -\tilde{p}_1(t)\sum_{i=1}^{11}\tilde{\lambda}_i \\ \dfrac{d\tilde{p}_2(t)}{dt} = \tilde{p}_1(t)\tilde{\lambda}_2 - \tilde{p}_2(t)(\tilde{\lambda}_1+\tilde{\lambda}_3) \\ \dfrac{d\tilde{p}_3(t)}{dt} = \tilde{p}_1(t)\tilde{\lambda}_1 + \tilde{p}_2(t)\tilde{\lambda}_1 - \tilde{p}_3(t)\tilde{\lambda}_3 \\ \dfrac{d\tilde{p}_4(t)}{dt} = \tilde{p}_1(t)\tilde{\lambda}_3 - \tilde{p}_4(t)(\tilde{\lambda}_1+\tilde{\lambda}_2) \\ \dfrac{d\tilde{p}_5(t)}{dt} = \tilde{p}_1(t)\sum_{i=4}^{11}\tilde{\lambda}_i + (\tilde{p}_2(t)+\tilde{p}_3(t))\tilde{\lambda}_3 + \tilde{p}_4(t)(\tilde{\lambda}_1+\tilde{\lambda}_2) \end{cases} \quad t \geq 0 \tag{2-12}$$

代入初始条件 $\tilde{p}_1(0)=1$ 及 $\tilde{p}_i(0)=0\,(1<i\leq 5)$，运用 Laplace-Stieltjes 变换，求解该微分方程得到线性方程组如下：

$$\begin{cases} s\tilde{p}_1(s)-1 = -\tilde{p}_1(s)\sum_{i=1}^{11}\tilde{\lambda}_i \\ s\tilde{p}_2(s) = \tilde{p}_1(s)\tilde{\lambda}_2 - \tilde{p}_2(s)(\tilde{\lambda}_1+\tilde{\lambda}_3) \\ s\tilde{p}_3(s) = \tilde{p}_1(s)\tilde{\lambda}_1 + \tilde{p}_2(s)\tilde{\lambda}_1 - \tilde{p}_3(s)\tilde{\lambda}_3 \\ s\tilde{p}_4(s) = \tilde{p}_1(s)\tilde{\lambda}_3 - \tilde{p}_4(s)(\tilde{\lambda}_1+\tilde{\lambda}_2) \\ s\tilde{p}_5(s) = \tilde{p}_1(s)\sum_{i=4}^{11}\tilde{\lambda}_i + (\tilde{p}_2(s)+\tilde{p}_3(s))\tilde{\lambda}_3 + \tilde{p}_4(s)(\tilde{\lambda}_1+\tilde{\lambda}_2) \end{cases} \tag{2-13}$$

由上述方程组解得 $\tilde{p}_5(s)$ 为：

$$\begin{aligned} \tilde{p}_5(s) = \frac{1}{s} &- \frac{\tilde{\lambda}_3}{(\tilde{\lambda}_3+\sum_{i=4}^{11}\tilde{\lambda}_i)\times(s+\tilde{\lambda}_1+\tilde{\lambda}_2)} \\ &- \frac{\tilde{\lambda}_1+\tilde{\lambda}_2}{(\tilde{\lambda}_1+\tilde{\lambda}_2+\sum_{i=4}^{11}\tilde{\lambda}_i)\times(s+\tilde{\lambda}_3)} \\ &+ \frac{(\tilde{\lambda}_1\times\tilde{\lambda}_3+\tilde{\lambda}_2\times\tilde{\lambda}_3-(\sum_{i=4}^{11}\tilde{\lambda}_i)^2)}{(\tilde{\lambda}_3+\sum_{i=4}^{11}\tilde{\lambda}_i)\times(\tilde{\lambda}_1+\tilde{\lambda}_2+\sum_{i=4}^{11}\tilde{\lambda}_i)\times(s+\sum_{i=1}^{11}\tilde{\lambda}_i)} \end{aligned} \tag{2-14}$$

对上述函数作 Laplace-Stieltjes 反变换可得系统处于状态 S_5 的概率关于时间 t 的函数，即系统的模糊失效概率函数为：

$$\tilde{p}_5(t)=1-\frac{\tilde{\lambda}_3}{\tilde{\lambda}_3+\sum_{i=4}^{11}\tilde{\lambda}_i}\times\exp(-(\tilde{\lambda}_1+\tilde{\lambda}_2)\times t)$$
$$-\frac{\tilde{\lambda}_1+\tilde{\lambda}_2}{\tilde{\lambda}_1+\tilde{\lambda}_2+\sum_{i=4}^{11}\tilde{\lambda}_i}\times\exp(-\tilde{\lambda}_3\times t) \tag{2-15}$$
$$+\frac{(\tilde{\lambda}_1\times\tilde{\lambda}_3+\tilde{\lambda}_2\times\tilde{\lambda}_3-(\sum_{i=4}^{11}\tilde{\lambda}_i)^2)\times\exp(-(\tilde{\lambda}_1+\tilde{\lambda}_2+\tilde{\lambda}_3+\sum_{i=4}^{11}\tilde{\lambda}_i)\times t)}{(\tilde{\lambda}_3+\sum_{i=4}^{11}\tilde{\lambda}_i)\times(\tilde{\lambda}_1+\tilde{\lambda}_2+\sum_{i=4}^{11}\tilde{\lambda}_i)}$$

给定任务时间 t，使用式（2-4）~（2-7）计算得系统处于状态 S_5 的模糊概率在不同 α 截集下的上下限，即为系统在该时刻 t 下的模糊失效概率的隶属函数。

在 t=5000h 时系统失效模糊概率的隶属函数如图 2-17 所示。

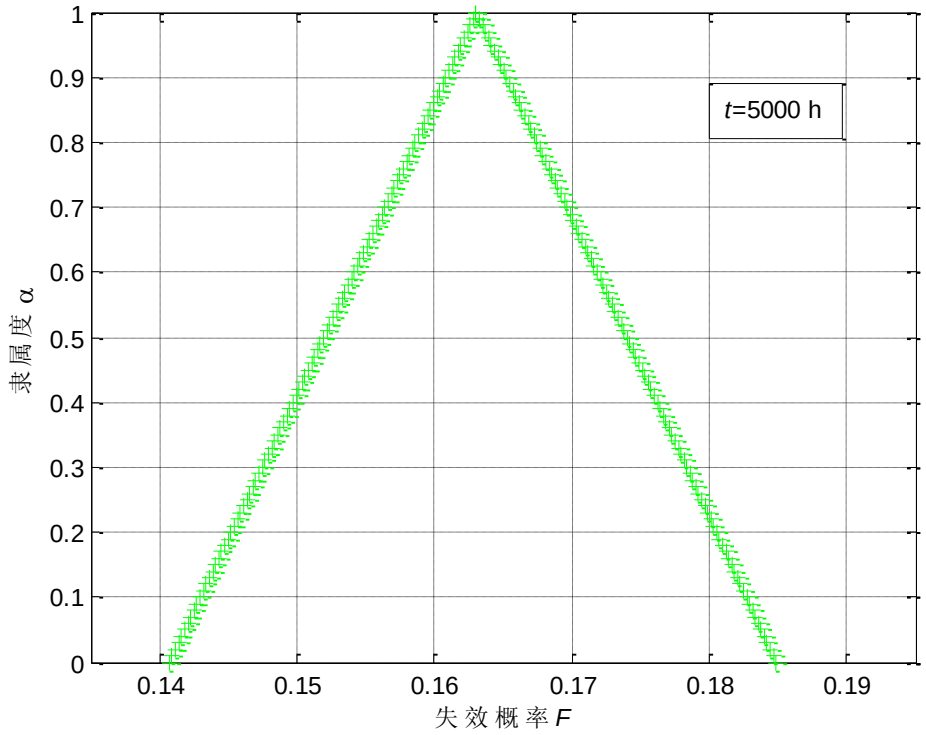


图 2-17 t=5000h 时，系统失效模糊概率的隶属函数

模糊概率的中值为 0.1631。该值表明系统运行至 5000h 的时候，失效概率的最大可能值为 0.1631。

系统在 t=10000h 时刻的失效模糊概率的隶属函数如图 2-18 所示，模糊概率的中值为 0.2892。

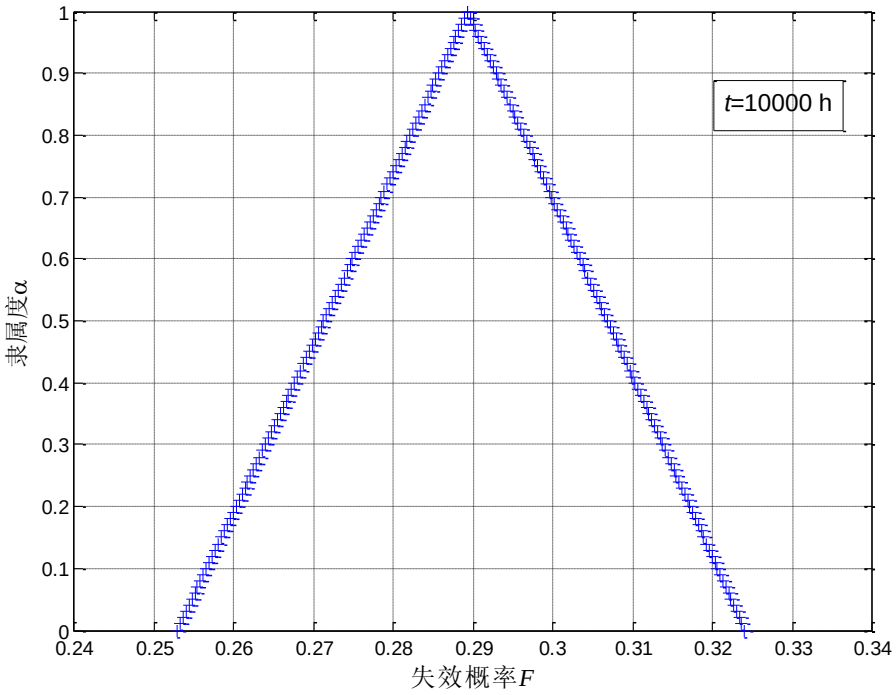


图 2-18 t=10000h 时，系统失效模糊概率的隶属函数

系统在 t=15000h 时刻的失效模糊概率的隶属函数如图 2-19 所示，模糊概率的中值为 0.3875。

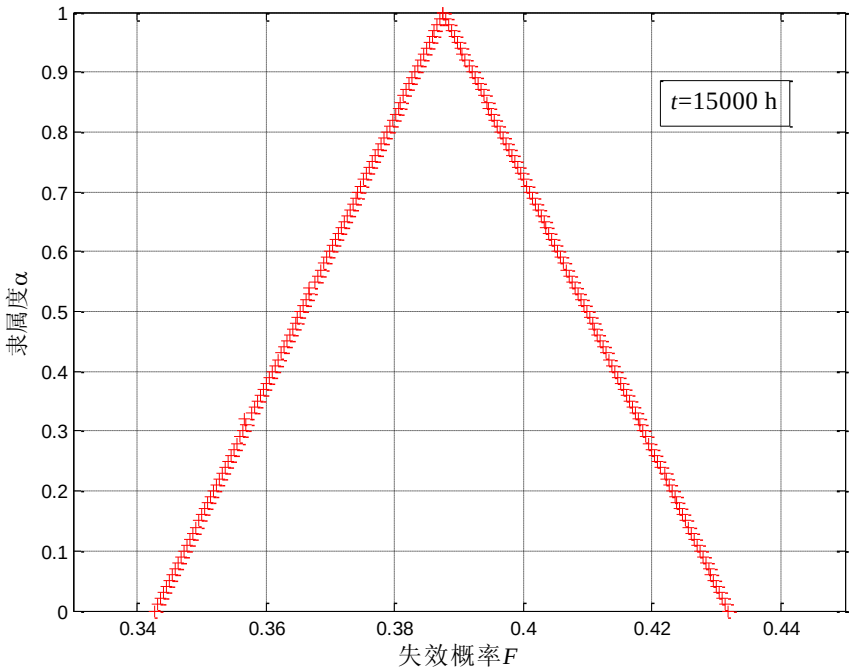


图 2-19 t=15000h 时，系统失效模糊概率的隶属函数

在固定水平截集下，系统可靠度曲线如图 2-20 所示。图中数据线分别表示在截集水平 α=1时系统的模糊可靠度曲线及在 α=0 时的模糊可靠度上下限的曲线。

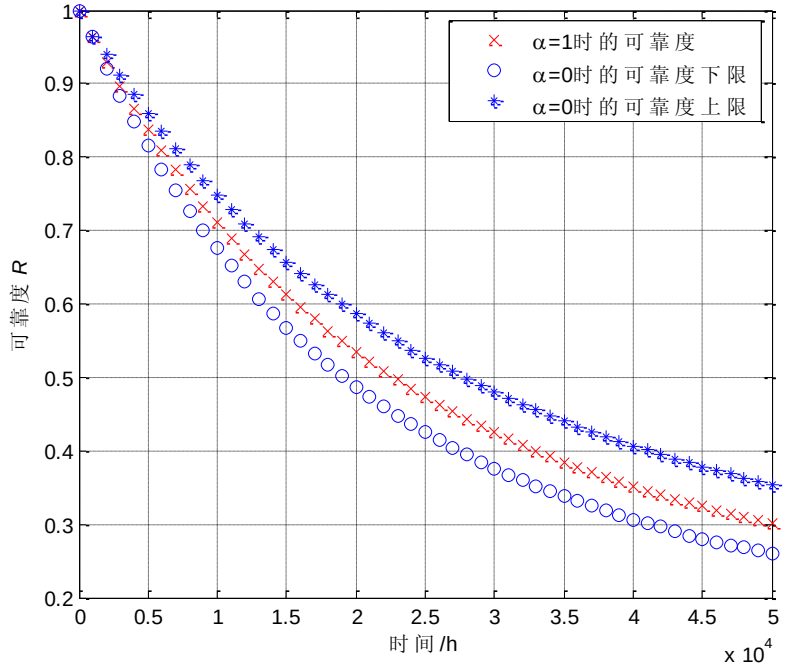


图 2-20 水平截集 α=0 及 α=1 时的系统模糊可靠度

2.6 本章小结

本章在基于马尔科夫模型的动态故障树分析方法的基础上，考虑了零部件失效率中的模糊不确定性，研究了在模糊失效率情况下的动态故障树分析方法。首先在系统结构分析和失效分析的基础上，建立系统的动态故障树模型。然后运用三角模糊数来描述零部件和系统的失效率，通过已经得到的动态故障树模型建立系统失效过程的模糊马尔科夫模型。再运用模糊理论中的扩展原理和 Laplace-Stieltjes 变换方法求解模型中的状态转移方程组，得到系统在给定时刻下的模糊可靠度和给定隶属度下的模糊可靠度曲线。最后应用该模糊马尔科夫模型对某数控加工中心液压系统进行可靠性建模与分析。实例分析表明，该方法是系统可靠性分析的一种有效的方法，能够准确地对具有动态失效特性和失效率具有不确定性的系统进行可靠性建模及定量评估。

第三章 基于离散时间贝叶斯网络的动态故障树可靠性评估模型

基于马尔科夫过程的动态故障树分析方法能够较好地解决具有动态失效特征的复杂系统的建模问题，然而在模型求解时该方法却要在全局状态空间中计算部件不同状态之间的转移。随着底事件以及逻辑门数量的增加，马尔科夫过程模型的计算量将呈指数增长，当不需要得到系统可靠度的解析解时，运用该方法进行可靠性分析就过于复杂。为了解决该问题，本章将贝叶斯网络与动态故障树分析方法相结合，利用贝叶斯网络的双向推理能力进行可靠性评估。最后通过算例和卫星太阳翼驱动机构的实例应用系统验证该方法的可行性。

3.1 引言

基于状态空间的马尔科夫模型能够对动态故障树模型进行建模和分析求解。然而，在马尔科夫模型中每一个节点都完整地描述了系统中所有变量的一个状态组合。也就是说，对于马尔科夫模型的状态空间中的每一个状态，其状态向量包含了系统中的所有变量，每个状态节点的向量长度都等于整个系统的变量个数。因此马尔科夫模型属于全局状态模型，这使得马尔科夫模型的求解复杂度随系统规模的增长而呈指数增长。

贝叶斯网络（Bayesian Network, BN）以图形化的方式来描述节点之间的连接关系，直观易懂，而且易于进行双向推理[88]。利用变量之间的条件独立关系，贝叶斯网络可降低非根节点的条件概率表的维数，从而大大降低推理环节的计算复杂度。随着不同证据的引入，可以通过贝叶斯网络进行向前的可靠性评估推理和向后的故障诊断和部件重要度评估。Boudali 等[89]提出了一种基于离散时间贝叶斯网络的可靠性建模与分析框架。

本章在上述文献和相关工作的基础上，系统研究贝叶斯网络模型在系统可靠性建模与分析中的应用。首先阐述贝叶斯网络模型及其概率推理的过程，然后建立几种典型的静态和动态逻辑门的条件概率分布的确定方法，以包含动态逻辑门的故障树为算例验证该方法的有效性，并阐述其双向推理方法在概率推理中的应用。最后，以卫星太阳翼驱动机构为实例详细阐述贝叶斯网络模型在复杂系统可靠性建模及评估中的应用；并对该系统进行双向推理，当存在证据的条件下运用其前向推理进行零部件重要度分析，运用反向推理进行故障诊断排序。

3.2 贝叶斯网络模型

3.2.1 贝叶斯网络简介及条件独立性

贝叶斯网络是一种有向无环图（Directed Acyclic Graph, DAG），其中节点代表随机变量，节点间的边代表变量之间的直接依赖关系[88]。贝叶斯网络中，如果节点 A 到节点 B 有一条 A 指向 B 的边，则节点 A 是 B 的父节点，同时 B 是 A 的子节点。没有输入边的节点，即没有父节点的节点称为根节点。根节点附有一个边缘概率分布表，描述了该节点在其对应状态空间中的概率分布。其它非根节点附有一个条件概率分布表，用以描述在已知其所有父节点的状态组合的条件下，该节点在状态空间中的条件概率分布情况。为表达方便起见，在本章将不区分事件、变量和节点。

考虑具有 n 个部件的两状态系统，分别以变量 X_i 表示各个部件。不考虑条件独立时，利用链规则，在这 n 个变量之间进行概率推理，其联合概率分布可以表示为如下式：

$$\begin{aligned} P(X_1, X_2, \cdots, X_n) &= P(X_1)P(X_2 \mid X_1)P(X_3 \mid X_1, X_2)\cdots P(X_n \mid X_1, X_2, \cdots, X_{n-1}) \\ &= \prod_{i=1}^{n} P\left(X_i \middle| X_1, X_2, \cdots, X_{i-1}\right) \end{aligned} \tag{3-1}$$

式中所需的独立参数个数为 $2^n - 1$ 个。

由于贝叶斯网络结构蕴含很强的条件独立关系，在给定某个节点的父节点时，除该节点的后代节点外，它与其它所有节点之间条件独立。即对任意 X_i，如果存在 $pa(X_i) \subseteq \{X_1, \cdots, X_{i-1}\}$，使得给定 $pa(X_i)$ 时，X_i 与 $\{X_1, \cdots, X_{i-1}\}$ 中的其它变量条件独立，即 $P(X_i \mid X_1, \cdots, X_{i-1}) = P(X_i \mid \delta(X_i))$。则利用贝叶斯网络的条件独立性，将联合概率分布分解成如下形式：

$$P(X_1, X_2, \cdots, X_n) = \prod_{i=1}^{n} P(X_i \mid pa(X_i)) \tag{3-2}$$

式中，$pa(X_i)$ 为节点 X_i 所有父节点的变量集合。

若假设任意 $pa(X_i)$ 最多包含 m 个变量，此时式（3-2）中所需的独立参数个数最多为 $n2^m$ 个，远远小于不考虑独立时确定联合分布所需的参数个数（2^n-1）。当变量数目 n 很大且 $m \ll n$ 时，采用贝叶斯网络的条件独立性可大大降低计算过程中的变量存储与运算的负担。

3.2.2 变量消元算法

变量消元算法（Variable Elimination, VE），也称为桶消元算法，是最简单的推理算法之一，可用来计算节点的后验概率 $P(Q|E=e)$ [88]。一般来讲，联合概率分布属于多变量函数，于是，变量消元算法可以推广到一般多元函数。

3.2.2.1 消元运算

设 $H(X_1,X_2,\cdots,X_n)$ 是变量 $\{X_1,X_2,\cdots,X_n\}$ 的一个函数，而 $\hbar=\{h_1,h_2,\cdots,h_m\}$ 是一组函数，其中每个 h_i 所相关的变量是 $\{X_1,X_2,\cdots,X_n\}$ 的一个子集。若

$$H=\prod_{i=1}^{m}h_i \tag{3-3}$$

则称 $\hbar$ 是 H 的一个分解（Factorization），$h_1,h_2,\cdots,h_m$ 称为此分解的因子。从 $H(X_1,X_2,\cdots,X_n)$ 出发，通过如下方式获得变量 $\{X_1,X_2,\cdots,X_{i-1},X_{i+1},\cdots,X_n\}$ 的一个函数：

$$F(X_1,X_2,\cdots,X_{i-1},X_{i+1},\cdots,X_n)=\sum_{X_i}H(X_1,X_2,\cdots,X_n) \tag{3-4}$$

这个过程称为消元（Elimination），即从函数 $H(X_1,X_2,\cdots,X_n)$ 中消去 X_i，得到函数 $F\left(X_1,X_2,\cdots,X_{i-1},X_{i+1},\cdots,X_n\right)$。从函数 H 中消去变量 X_i 的分解过程包括如下两步骤：

（1）从 $\hbar$ 中删去所有涉及 X_i 的函数；

（2）将新函数 $\sum_{X_i}\prod_{i=1}^{k}h_i$ 放回 $\hbar$ 中。

定理 4-1[88] 设 $\hbar$ 是函数 $H\left(X_1,X_2,\cdots,X_n\right)$ 的一个分解，设 $\hbar'$ 是从 $\hbar$ 中消去 X_i 后所得的一组函数；如果 $F\left(X_1,X_2,\cdots,X_{i-1},X_{i+1},\cdots,X_n\right)$ 是从 $H\left(X_1,X_2,\cdots,X_n\right)$ 中消去 X_i 后所得的函数，那么，$\hbar'$ 是 $F\left(X_1,X_2,\cdots,X_{i-1},X_{i+1},\cdots,X_n\right)$ 的一个分解。

3.2.2.2 算法描述

设 $f\left(X,Y\right)$ 为两组变量 X 和 Y 的函数，其中 $X\cap Y=\varnothing$，设 x 为 X 的取值。在 $f\left(X,Y\right)$ 中，将 X 设置为 x，得到一个关于 Y 的函数 $f_{X=x}\left(Y\right)$：

$$f_{X=x}\left(Y=y\right)=f\left(X=x,Y=y\right),\ \ \forall y\in\Omega_Y \tag{3-5}$$

有时为了方便，将 $f_{X=x}\left(Y\right)$ 记作 $f\left(X=x,Y\right)$。

设贝叶斯网络 N 中所有变量的集合为 X，$\hbar$ 是 N 中所有概率分布的集合。根据贝叶斯网络的定义可知，$\hbar$ 是 N 所表示的联合概率分布 $P\left(X\right)$ 的一个分解。假设

观测到证据 $E=e$。在 $\hbar$ 的因子中，将各证据变量设置为它们的观测值，得到一组新的函数，记为 $\hbar'$。称这一步为证据设置。从而，$\hbar'$ 是函数 $P(Y,E=e)$ 的一个分解，此时 $Y=X\setminus E$。

设 G 是 Y 的一个子集。从 $\hbar'$ 中逐个消去所有在 Y 中但不在 G 中的变量，得到另一个函数集合，记为 $\hbar''$。根据定理 4-1，$\hbar''$ 是 $P(G,E=e)$ 的一个分解。所以，将 $\hbar''$ 中的所有因子相乘，就可以得到 $P(G,E=e)$。按照条件概率的定义，进一步得到：

$$P(G|E=e)=\frac{P(G,E=e)}{P(E=e)} \tag{3-6}$$

式中，$P(E=e)=\sum_{G}P(G,E=e)$。上述过程即为消元算法，简称 VE 算法。此过程实际上给出了一个计算后验概率分布 $P(G|E=e)$ 的算法。

消元算法共有 5 个输入：

（1）贝叶斯网络 N，它为联合分布 $P(X)$ 的一个分解；

（2）证据变量（已知变量）的集合 E；

（3）证据变量的取值 e；

（4）查询变量（需要计算后验概率分布的变量）的集合 G；

（5）所有步骤 $G\cup E$ 中的变量的排序 ζ，称为消元顺序。

消元算法是通过首先设置证据，接着按照顺序 ζ 逐个消去不在 $G\cup E$ 中的所有变量；然后把所有 $\hbar$ 中因子相乘，得到 G 的一个函数 $\ell(G)$；最后将此函数归一化，得到后验概率分布 $P(G|E=e)$。

3.2.3 贝叶斯网络实例及双向推理

以图 3-1 所示的贝叶斯网络为例来阐述贝叶斯网络对概率分布的表达及推理能力。该网络中，X_1,X_2,X_3,X_4 称为根节点，M 称为中间节点，T 称为叶节点；其中，X_1,X_2,X_3 是 M 的父节点，M 及 X_4 又是 T 的父节点。每个根节点旁边列有一个边缘概率分布表（Marginal Probability Distribution, MPD），分别列出该节点的所有状态及其对应的概率。每个非根节点附有一个条件概率分布表（Conditional Probability Distribution, CPD），描述了该节点在给定其父节点的状态组合下的条件概率分布。下面运用贝叶斯网络的推理算法结合联合分布分解的链规则以及条件独立性对此网络进行概率推理。

运用贝叶斯网络联合树推理算法，在没有证据情况下叶节点 T 的概率分布为：

$$P(T=0)=0.9793,\ \ P(T=1)=0.0207$$

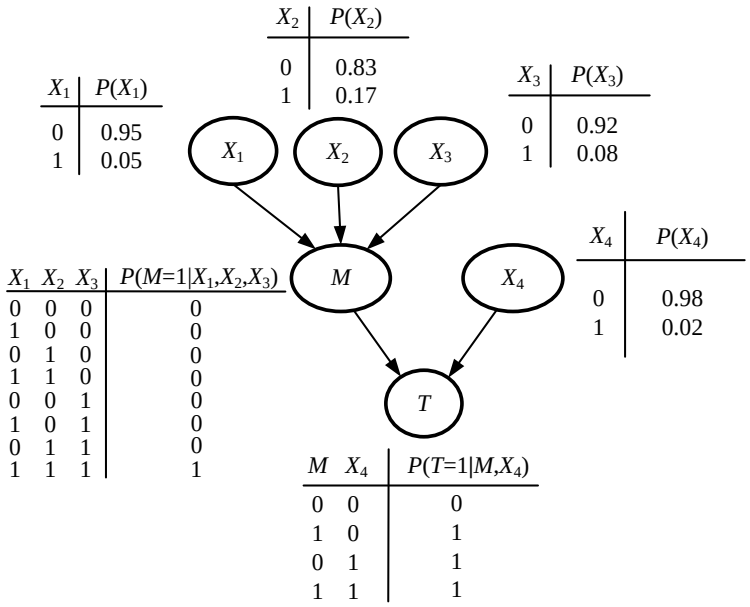


图 3-1 贝叶斯网络实例

分别假设各输入节点为 1，得到节点 T 的条件概率分布如表 3-1 所示。假设已知节点 T=1，则在加入该证据的情况下，各节点的条件概率分布如表 3-2 所示。

表 3-1 叶节点 T 的条件概率分布

X_i	$P(T=0\mid X_i=1)$	$P(T=1\mid X_i=1)$	X_i	$P(T=0\mid X_i=1)$	$P(T=1\mid X_i=1)$
X_1	0.9667	0.0333	X_3	0.9717	0.0283
X_2	0.9761	0.0239	X_4	0.0000	1.0000

表 3-2 根节点的条件概率分布

X_i	$P(X_i=0\mid T=1)$	$P(X_i=1\mid T=1)$	X_i	$P(X_i=0\mid T=1)$	$P(X_i=1\mid T=1)$
X_1	0.9194	0.0806	X_3	0.8903	0.1097
X_2	0.8032	0.1968	X_4	0.0322	0.9678

通过该实例可以得到如下结论：在没有证据的条件下，运用贝叶斯网络可以计算出叶节点（对应系统输出节点）的概率分布；在有证据输入的情况下，运用贝叶斯网络的双向推理，可以在网络的输入节点与输出节点之间进行条件概率推理，从而通过概率推理来实现可靠性分析和故障诊断。

3.3 基于动态故障树的离散时间贝叶斯网络可靠性评估模型

3.3.1 离散时间贝叶斯网络模型

离散时间贝叶斯网络（Discrete Time Bayesian Network, DTBN）与普通贝叶斯网络类似，是一个由代表变量的节点和连接这些节点的有向边构成的有向无环图。

基于动态故障树的离散时间贝叶斯网络可靠性评估过程包括以下步骤[89]：

（1）状态定义

把整个任务构成的时间区间$[0,t]$分成 n 个长度相等的子区间，每个子区间的长度为$\Delta = t/n$，则整个时间轴$[0,+\infty)$被划分成 n+1 个子区间。

网络中节点的状态定义如下：

当某节点 A 对应的零部件在任务时间 t 内第 i 个时间区间内发生失效时，即 A 在时间区间$[(i\text{-}1)\Delta, i\Delta]$内失效时，则称节点 A 处于状态 i。如果 A 在任务时间 t 内未失效，即 A 在$[t,\infty)$内失效，则称 A 处于状态 n+1。

通过以上的定义，得到贝叶斯网络中所有节点的状态空间为如下的时间区间：

$$[0,\Delta]，\ (\Delta,2\Delta]，\ \cdots，\ ((n-1)\Delta,n\Delta]，\ (n\Delta,+\infty)$$

简记为$\{1,2,\cdots,n+1\}$，系统以及部件的失效时间 X 总对应着 n+1 个区间中的某一个区间 i。系统处于前 n 个状态的概率之和即为该系统在任务时间 t 时的不可靠度，系统处于第 n+1 个状态的概率即为系统在任务时间 t 时的可靠度。

（2）动态故障树模型的建立

通过详细分析研究对象的结构功能和失效过程，并按照故障树建模的基本流程建立系统的动态故障树模型。该步骤是整个建模与分析过程的基础，需要准确合理地选择顶事件，确定系统中各个零部件之间的失效逻辑关系，以保证最终分析结果的正确性。

（3）模型映射

根据所建立的动态故障树模型，逐层将模型中的事件映射到贝叶斯网络模型的节点中。

（4）建立所有节点的概率分布

在正确建立贝叶斯网络模型之后，首先根据分析精度的要求大致选取任务时间 t 的区间划分数 n，也就是确定贝叶斯网络中节点的状态数。根据原故障树中底事件的失效概率确定各个底事件在 n+1 个状态的概率分布，该分布也可以称为根节点的边缘概率分布或先验概率分布。由原故障树中各个逻辑门的失效逻辑建立贝叶斯网络模型中对应节点的条件概率分布，该过程将在下一节详细讨论。

（5）模型的推理计算

根据贝叶斯网络的条件独立性可知，每个节点的条件概率分布可以表示为 $P\left(X_i \left| pa\left(X_i\right)\right.\right)$，用以表达节点与父节点之间的定量关系。在给定根节点的先验概率分布和非根节点的条件概率分布的条件下，可以得到包含所有节点的联合概率分布，进而对目标节点进行边缘化计算，得到其边缘概率分布。

包含 m 个节点的 DTBN 中，非叶节点用事件 U_i（$1 \le i \le m-1$）表示，U_i 的发生区间为 $\{[0,\Delta],(\Delta,2\Delta],\cdots,((n-1)\Delta,n\Delta],(T,+\infty)\}$。如果顶事件 U_T 在任务时间 T 内发生，则顶事件的发生时刻必定在 $[0,\Delta]$，$(\Delta,2\Delta]$，$\cdots$，$((n-1)\Delta,n\Delta]$，$(n\Delta,+\infty)$ 其中一个区间内。因此，U_T 在任务时间 T 内发生的概率可直接计算得到并表示为：

$$\begin{aligned} P(T) &= \sum_{0\le x\le n} P\left(U_T = \left((x-1)\Delta, x\Delta\right)\right) \\ &= \sum_{0\le x\le n} \sum_{U_1,\cdots,U_{m-1}} P\left(U_1 = u_1,\cdots,U_{m-1} = u_{m-1}, U_T = \left((x-1)\Delta, x\Delta\right)\right) \end{aligned} \tag{3-7}$$

式中，u_i 表示 U_i 的发生区间，u_i 属于 $\{[0,\Delta],(\Delta,2\Delta],\cdots,((n-1)\Delta,n\Delta],(T,+\infty)\}$。

3.3.2 逻辑门输出事件条件概率表的确定

基于贝叶斯网络的动态故障树可靠性建模与评估过程主要包括两个部分：定性分析和定量评估。定性分析部分包括状态定义、动态故障树模型建立和模型转化，定量评估部分包括节点 CPD 的确定以及概率推理的计算。定性部分的内容在前面已做了详细阐述，模型建立部分可参阅其它故障树建模方面的文献，这里不再赘述，下面重点讨论各种静态和动态逻辑门的条件概率表的确定。

3.3.2.1 与门

令 $\mathbf{X}=[X_1,X_2,\cdots,X_m]$，其中 m 为与门的输入事件个数，$X_i, i=1,2,\cdots,m$ 为输入事件的状态变量，其状态组合数为 $(n+1)^m$，n 为前面介绍的任务时间的区间划分数。令 Y 为与门输出的状态变量。所有变量的状态空间都为 $\{1,2,\cdots,n+1\}$。令 $k=\max(X_1,X_2,\cdots,X_m)$。与门的失效机理为所有输入事件发生则输出事件发生，则输出事件应处于所有输入事件的状态值的最大值，因此，在输入事件的任一状态组合下，Y 的条件概率分布为：

$$P(Y=j\mid\mathbf{X})=\begin{cases}1, & j=k\\ 0, & j\ne k\end{cases} \tag{3-8}$$

该分布表示在与门输出节点的 CPD 表中，元素的取值为 0 或为 1，且每一行中仅在输入事件状态最大值对应的列上的元素为 1，其它元素为 0。

3.3.2.2 或门

假设所有变量及其状态空间的符号及意义和与门相同。或门的失效机理为只要输入事件中有一个事件发生则输出事件发生，因此或门输出事件的状态与输入事件中状态的最小值相同。令 $r=\min(X_1,X_2,\cdots,X_m)$，则或门输出事件的条件概率分布为：

$$P(Y=j\mid \mathbf{X})=\begin{cases}1, & j=r\\ 0, & j\neq r\end{cases} \tag{3-9}$$

该分布同与门的形式一致，区别在于每一行中在输入事件状态的最小值对应的列上的元素为 1，其它元素为 0。

3.3.2.3 优先与门

设输入事件为 A、B，输出事件为 Y，状态取值分别为 a、b 和 y。优先与门的失效机理为，当 A 与 B 都失效，且 A 先于 B 失效时，输出事件 Y 发生，也就是说当 $a<b$ 时，输出事件 Y 处于状态 b；当 $a\geq b$ 时，输出事件 T 处于状态 n+1，即 Y 不失效。则 Y 的条件概率分布如下：

当 $a<b$ 时，

$$P(Y=i\mid\bullet)=\begin{cases}1, & i=b\\ 0, & \text{其他}\end{cases} \tag{3-10}$$

当 $a\geq b$ 时，

$$P(Y=i\mid\bullet)=\begin{cases}1, & i=n+1\\ 0, & \text{其他}\end{cases} \tag{3-11}$$

式（3-10）表明当输入事件满足优先失效条件时，输出事件处于输入事件 B 所在状态的概率为 1。式（3-11）表明当输入事件不满足优先失效条件时，输出事件 Y 处于状态 n+1 的概率为 1。

3.3.2.4 功能相关门

假设功能相关门只有一个相关输入事件 A，触发事件为 Tr，输出事件为 T。当 Tr 发生时其相关事件 A 发生，输出事件 T 发生；当 A 独立发生失效时，输出事件 T 也会发生。也就是说，事件 A 无论是独立失效还是相关失效，都会导致输出事件 T 的发生。为了更加直观和方便地确定节点的 CPD 表，我们在输入事件与输出事件之间增加一个中间节点 A' 来代表因 Tr 触发或者由 A 本身的独立失效所导致的 A

失效的总失效事件（如果不增加该节点，节点 A 的失效概率分布将不再是边缘分布，而是受 Tr 影响的条件概率分布）。该功能相关门的 FTA 模型以及增加节点 A' 后的 BN 模型见图 3-2 所示。

此时，节点 Tr 和节点 A 都有各自的边缘概率分布 MPD，节点 A' 为或门结构的条件概率分布。节点 T 只受节点 A' 的影响，与 A' 同时失效，其状态与 A' 相同。因此其条件概率分布表即为一个单位矩阵 E，其条件概率分布为：

$$P(T=j \mid A'=i)=\begin{cases}1, j=i\\ 0, j\neq i\end{cases} \quad i,j=1,2,\cdots,n+1 \tag{3-12}$$

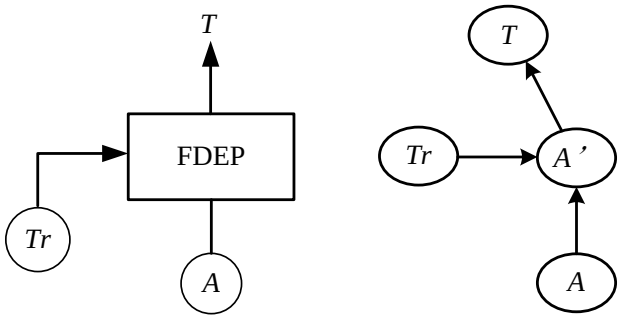


图 3-2 功能相关门 FTA 模型及对应 BN 模型

当功能相关门有两个及以上触发输入 $Tr_1, Tr_2, \cdots$ 时，在触发输入节点之后增加一个中间节点 Tr'，所有触发输入节点之间以或门逻辑关系影响节点 Tr'，而 Tr' 与其子节点之间的关系与单触发输入时相同。同理，当功能相关门具有两个及以上相关输入事件时，增加中间节点，各层节点之间的关系与多触发输入节点相同。

3.3.2.5 备件门

（1）冷备件门

备件条件概率分布的确定：

当系统具有零部件备份时，假设冷备件门具有主输入 A 与备份输入 B，输出为 T。当主输入 A 处于状态 x 时，根据 Boudali 等[89]给出的公式，可以得出备份 B 处于状态 y 的条件概率如式（3-13）所示。

输出事件条件概率分布的确定：

由于冷备份的特征，备件失效之前，输出是不会失效的，而一旦备件失效，输出就一定失效。因此，冷备件门输出事件的条件概率分布表为一个单位矩阵，其表达式与式（3-12）相同。

$$
\begin{aligned}
&P(B=y\mid A=x)\\
&=\begin{cases}
\dfrac{\int_{(x-1)\Delta}^{x\Delta}\int_{(y-1)\Delta}^{y\Delta}\lambda \mathrm{e}^{-\lambda(t-\tau)}\lambda \mathrm{e}^{-\lambda\tau}\mathrm{d}\tau\mathrm{d}t}{\int_{(x-1)\Delta}^{x\Delta}\lambda e^{-\lambda\tau}\mathrm{d}\tau}=\lambda\Delta \mathrm{e}^{\lambda x\Delta}\mathrm{e}^{-\lambda y\Delta}, & x<y<n+1\\
1-\sum_{i=x+1}^{n}P(B=i\mid A=x), & x<y=n+1\\
0, & x\geq y
\end{cases}
\end{aligned}
\tag{3-13}
$$

（2）热备件门

热备件门的备件的失效与主件无关，不管主件失效与否，备件均按照其失效率独立的产生随机失效，因此其失效概率分布为边缘概率分布 MPD。对于输出事件，虽然热备件门同与门的失效机理不同，但是从输出事件的概率评估角度看，热备件门同与门的输出事件具有相同的失效概率分布，这里不再赘述。

（3）温备件门

温备件门输出事件的 CPD 与热备件门的相同，如式（3-8）所示。其备件的 MPD 与热备件的 MPD 相似，区别在于其失效率需要乘上一个备份因子α，这里不再详细介绍。

3.4 模型验证与算例分析

本节以图 3-3 所示动态故障树模型为例，验证上述方法的正确性，并与蒙特卡洛仿真所得结果相比较，分析该方法的误差。

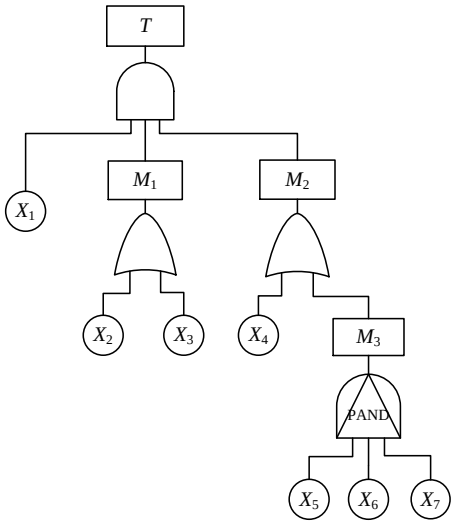


图 3-3 动态故障树模型

该动态故障树模型由三种逻辑门组成，分别是与门、或门和优先与门。首先把动态故障树模型的拓扑结构转化成贝叶斯网络模型的网络结构。再根据式（3-8）~（3-10）中的条件概率表构造方法，运用 Matlab 编制这几种逻辑门的条件概率表构造函数，再运用 BNT 工具箱及变量消元算法求解 BN 模型。

其贝叶斯网络模型如图 3-4 所示。图中各层节点与动态故障树中事件的对应关系分别如下所述：

第一层：节点 1、2、3 对应底事件 X_5、X_6、X_7；

第二层：节点 4 对应中间事件 M_3，节点 5、6、7 对应底事件 X_4、X_2、X_3；

第三层：节点 9 对应底事件 X_1；8、10 对应中间事件 M_2、M_1；

第四层：节点 11 对应顶事件 T。

假设动态故障树模型中各个底事件的失效率如表 3-4 所示。在区间划分数 n=6 时，运用变量消元算法及联合树推理算法，得到各个时间点上系统可靠度，如表 3-3 和图 3-5 所示。在此基础上，将蒙特卡洛仿真得到的系统可靠度与贝叶斯网络结果进行比较，结果如表 3-3 所示。从表中相对误差栏可知，两种方法得到的结果非常接近，从而验证了贝叶斯网络对此系统可靠性评估的有效性。

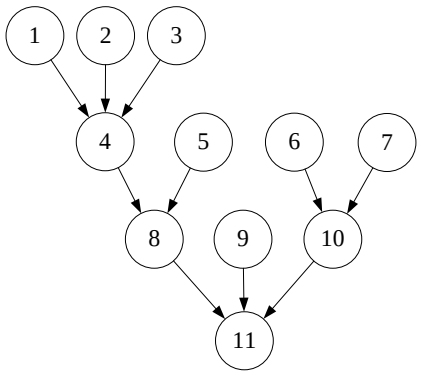


图 3-4 贝叶斯网络结构

表 3-3 BN 与 MC 仿真结果对比

时间（h）	BN 结果	MC 仿真结果	相对误差（%）
50	0.97932	0.97931	0.0018
100	0.90436	0.90491	0.0602
150	0.80153	0.80118	0.0448
200	0.69481	0.69438	0.0623
250	0.59532	0.59472	0.1009
300	0.50690	0.50611	0.1579

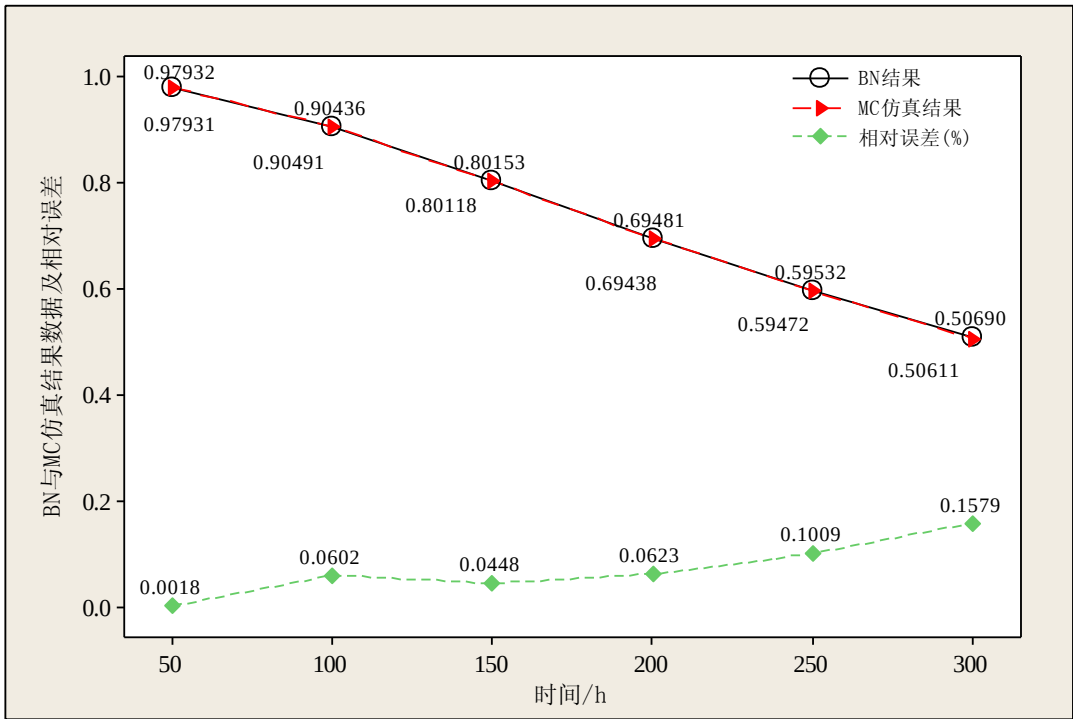
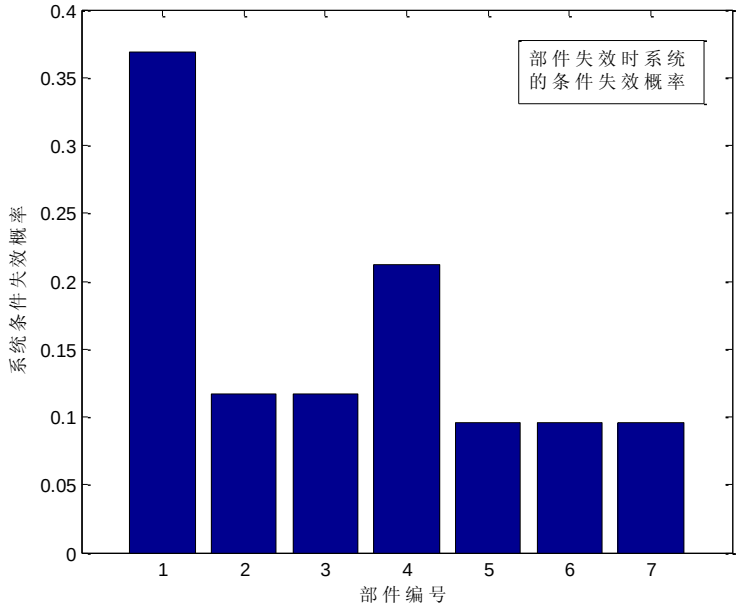


图 3-5 可靠度计算结果对比

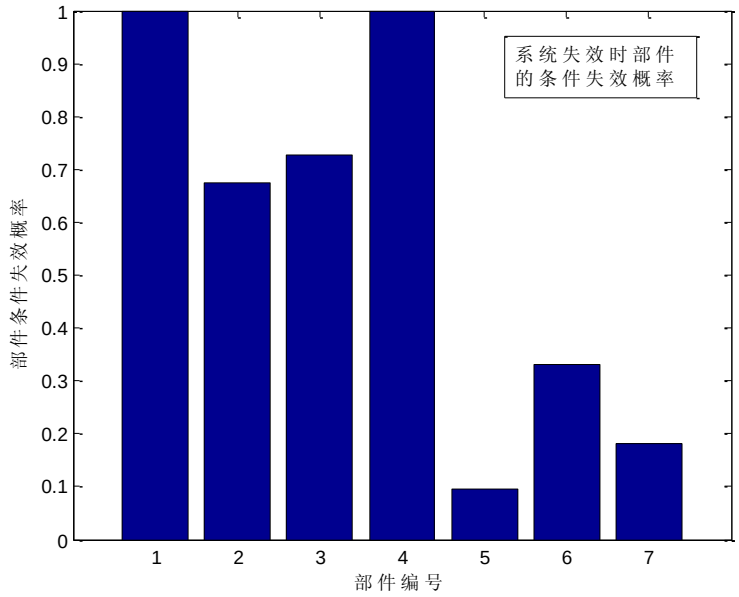
运用网络的正向推理，可以计算出当原故障树模型中各个底事件单独发生时顶事件发生的条件概率，即 $P(T=1|X_i=1)$。运用反向推理可以计算出当顶事件发生时，各个底事件发生的后验概率值，即 $P(X_i=1|T=1)$。本例中取任务时间 T=100h，正向推理结果如表 3-4 和图 3-6(a)所示，反向推理结果见表 3-4 和图 3-6 (b)所示。从图表的数据能够直接比较出每个部件失效对系统失效的影响程度的大小。

表 3-4 双向推理结果

部件编号	部件失效率（/h）	$P(T=1\|X_i=1)$	$P(X_i=1\|T=1)$
X_1	0.003	0.3690	1.0000
X_2	0.008	0.1170	0.6738
X_3	0.009	0.1170	0.7261
X_4	0.006	0.2118	0.9993
X_5	0.001	0.0962	0.0958
X_6	0.004	0.0958	0.3301
X_7	0.002	0.0959	0.1818



(a)



(b)

图 3-6 双向推理结果

(a)部件失效时系统失效的条件概率；(b)系统失效时部件失效的条件概率

3.5 实例分析：卫星太阳翼驱动机构可靠性建模与评估

3.5.1 太阳翼驱动机构动态故障树建模

随着现代大型军事卫星、气象卫星与商用广播通信卫星的结构和功能的日益

复杂化，人们对卫星系统的可靠性提出了新的要求，如要求系统长寿命、高可靠地在复杂环境中完成规定的功能。现代卫星普遍采用太阳能这一可持续利用的能源，以满足长寿命卫星对能源方面的需求。为了充分发挥太阳能电池的作用，产生足够多的能量，卫星上备有帆板来装载这些太阳能电池，并安置驱动装置以驱动帆板转动，从而控制其法线指向太阳光束的方向，达到尽可能多地吸收太阳能的目的。

卫星太阳翼驱动机构在卫星太阳翼对日定向功能中起着关键作用，因此有必要对卫星太阳翼驱动机构进行可靠性分析和评估，以保证其具有高的可靠性，从而保证整个卫星系统高可靠长时间地正常工作。本节采用动态故障树结合贝叶斯网络方法对某卫星的太阳翼驱动机构进行系统可靠性分析和评估。

某型号卫星的太阳翼驱动机构由太阳翼敏感器、星载计算机、导电环、太阳翼驱动线路和电机传动装置等组成，其工作原理如图 3-7 所示[91]。

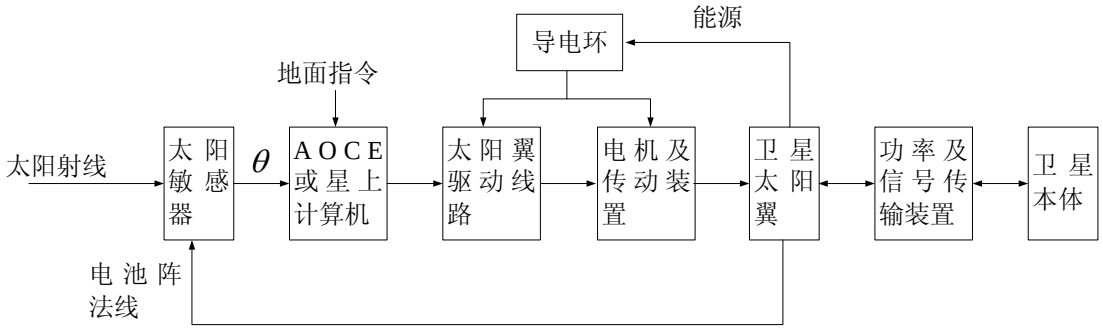


图 3-7 卫星太阳翼对日定向系统原理图

以“卫星太阳翼驱动机构失效”作为顶事件 T，从上向下逐级进行分析。设 A 代表太阳敏感器失效，B 代表星载计算机失效，C 代表谐波减速器失效，D 代表驱动电机失效，E 代表人为因素失效，F 代表电气系统失效，G 代表传动装置失效，H 代表导电环失效，I 代表位置传感器失效，S 代表绕组失效，K 代表电刷失效。设太阳敏感器、星载计算机、绕组、电气系统、位置传感器和电刷等的主、备份失效分别为 A_1、A_2、B_1、B_2、S_1、S_2、F_1、F_2、I_1、I_2、K_1 和 K_2。太阳敏感器、星载计算机、电机定子绕组和位置传感器采用冷备份。电气系统具有功能相关部件，采用功能相关门。导电环采用热备份。

假定除上述具有动态失效机理的部件以外，其它各部件之间的失效是相互独立的，结合所有模块的故障原因分析，最后得到整个驱动机构的故障树如图 3-8 所示。

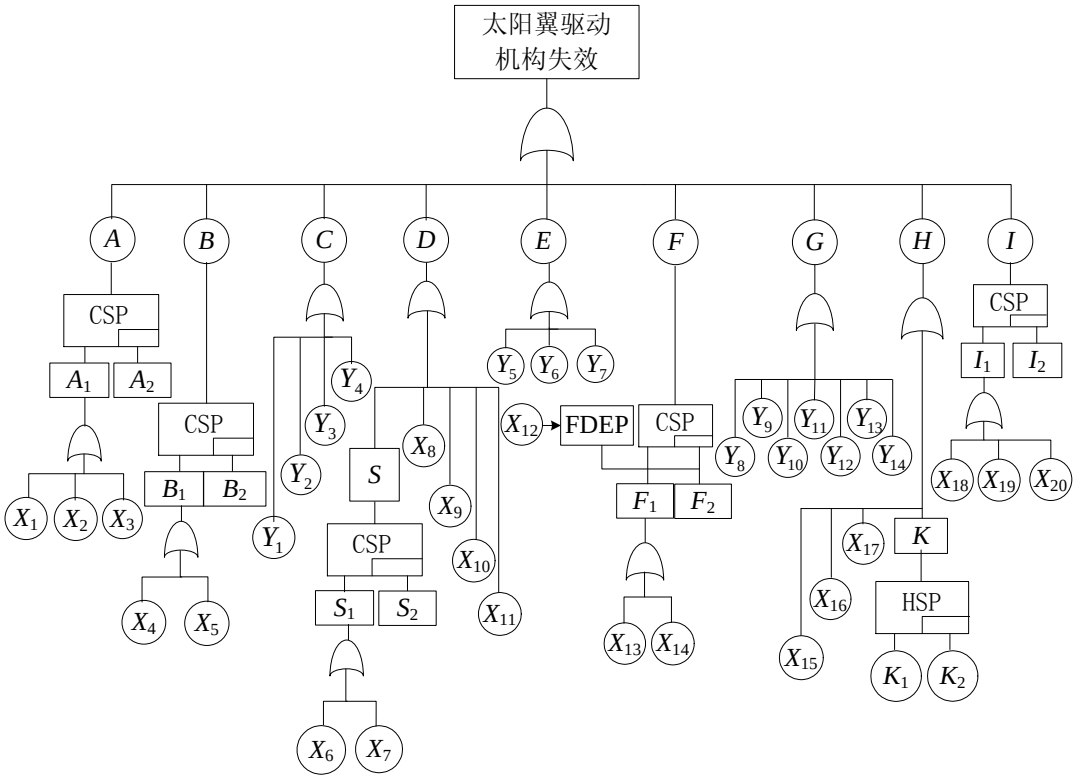


图 3-8 卫星太阳翼驱动机构故障树

3.5.2 太阳翼驱动机构贝叶斯网络模型

假定零部件与系统的工作状态仅取正常和失效两种状态，零部件失效服从指数分布，基本事件的失效率见表 3-5 所示。

按照前述方法，把故障树中的各级事件及其失效逻辑关系映射到贝叶斯网络中的各级节点上，最后得到相应的贝叶斯网络如图 3-9 所示。

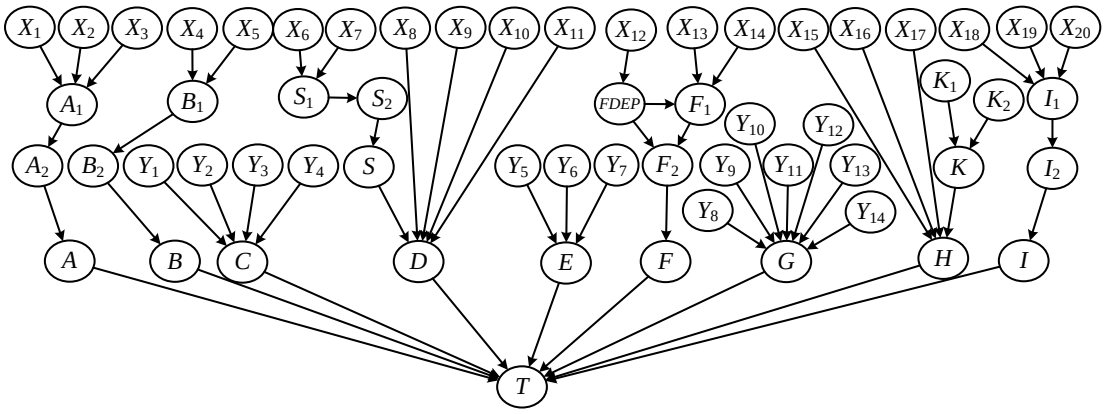


图 3-9 卫星太阳翼驱动机构贝叶斯网络模型

表 3-5 基本事件及其失效率

事件代号	事件名称	失效率 λ（$10^{-6}h^{-1}$）	事件代号	事件名称	失效率 λ（$10^{-6}h^{-1}$）
X_1	光学头部	0.500	X_{19}	发光二极管失效	0.500
X_2	传感器	0.600	X_{20}	检测电路失效	0.500
X_3	信号处理线路	0.120	Y_1	柔轮失效	0.100
X_4	星载计算机硬件故障	0.500	Y_2	齿轮磨损	0.600
X_5	星载计算机软件故障	0.250	Y_3	固体润滑膜失效	0.550
X_6	绕组疲劳	0.250	Y_4	润滑脂失效	0.500
X_7	绕组被烧毁	0.100	Y_5	指令走飞	0.500
X_8	驱动线路故障	0.120	Y_6	硬件设计错误	0.200
X_9	堵转	0.120	Y_7	软件设计错误	0.200
X_{10}	摩擦增大	0.100	Y_8	离合器故障	0.600
X_{11}	疲劳失效	0.100	Y_9	轴承卡死	0.500
X_{12}	接口故障	0.600	Y_{10}	键断裂	0.100
X_{13}	线路故障	0.125	Y_{11}	电位计旋转轴故障	0.500
X_{14}	晶体管故障	0.500	Y_{12}	齿轮故障	0.100
X_{15}	线路被放电烧毁	0.100	Y_{13}	外部故障	0.500
X_{16}	轴承润滑剂失效	0.100	Y_{14}	综合性故障	0.500
X_{17}	绝缘层失效	0.150	K_1	电刷主件	0.500
X_{18}	感光元件失效	0.500	K_2	电刷备件	0.500

3.5.3 太阳翼驱动机构贝叶斯网络可靠性分析

假设任务时间 t=50000h，当 n 分别取 2、3、4 时，即计算的时间间隔为 25000h、16667h、12500h 时，系统的可靠度随时间的变化曲线如图 3-10 所示。

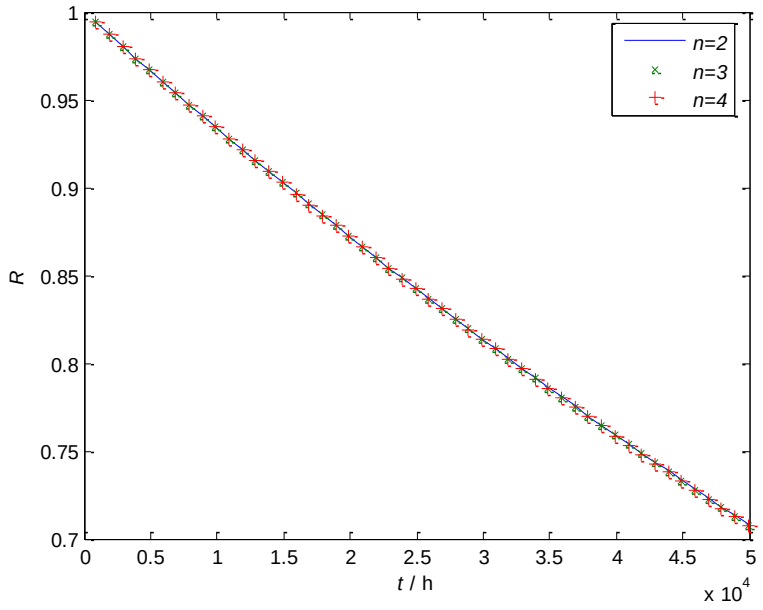


图 3-10 系统可靠度随时间的变化曲线

在[45000h，50000h]的任务时间中，当 n 分别取 2、3 和 4 时，每隔 100h 计算系统的可靠度，其结果如图 3-11 所示。

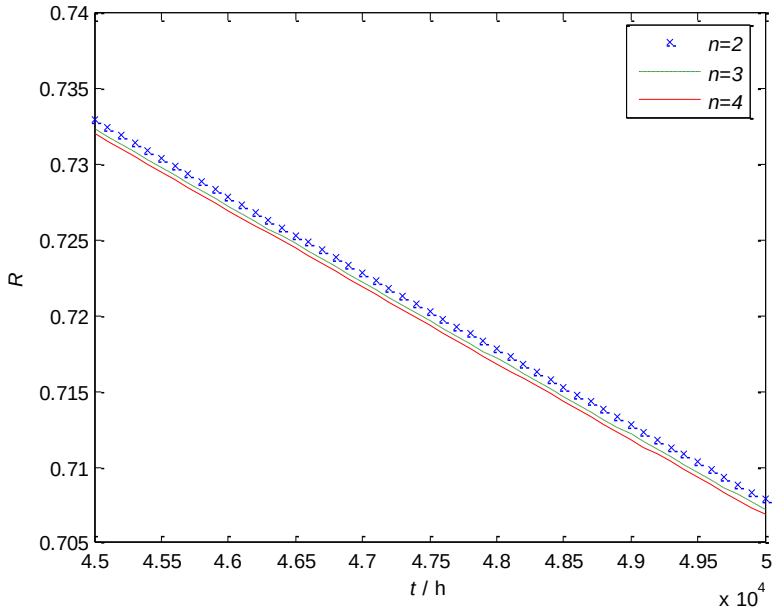


图 3-11 当 n 分别取不同值时系统可靠性的比较

由计算数据分析得到：在每个时间点上，第 2 组数据与第 1 组数据可靠度的最大差值比例为 0.0606%，而第 3 组数据与第 2 组数据可靠度的最大差值比例为 0.0305%；考虑到系统其它不确定性的存在，因此 n 取 4 时可靠度数据能够满足评估精度的要求。

当 t=50000h，n=4 时，顶事件 T 在 5 个时间区间上的概率分布如表 3-6 所示。

表 3-6 n=4 时顶事件的概率分布

$T=i$	1	2	3	4	5
$P(T=i)$	0.0820	0.0759	0.0703	0.0649	0.7069

顶事件在任务时间内发生的概率为 P=0.2931，系统的可靠度为 0.7069。

当系统故障时（叶节点 T 状态为 5），利用贝叶斯网络的反向推理，计算出各个底事件的失效概率如表 3-7 所示。由结果可知，X_7 失效的概率最小，而 X_{12}、Y_2 和 Y_8 失效的概率最大，则其对应的零部件是系统的薄弱环节。利用贝叶斯网络的前向推理，假定在各个根节点对应事件发生的条件下，得到对应顶事件失效的条件概率如表 3-8 所示。

表 3-7 系统故障时各个部件的失效概率

事件代号	失效概率	事件代号	失效概率	事件代号	失效概率
X_1	0.0260	X_{13}	0.0064	Y_5	0.0842
X_2	0.0311	X_{14}	0.0254	Y_6	0.0339
X_3	0.0063	X_{15}	0.0170	Y_7	0.0339
X_4	0.0255	X_{16}	0.0170	Y_8	0.1008
X_5	0.0128	X_{17}	0.0255	Y_9	0.0842
X_6	0.0126	X_{18}	0.0262	Y_{10}	0.0170
X_7	0.0051	X_{19}	0.0262	Y_{11}	0.0842
X_8	0.0204	X_{20}	0.0262	Y_{12}	0.0170
X_9	0.0204	Y_1	0.0170	Y_{13}	0.0842
X_{10}	0.0170	Y_2	0.1008	Y_{14}	0.0842
X_{11}	0.0170	Y_3	0.0925	K_1	0.0261
X_{12}	0.1008	Y_4	0.0842	K_2	0.0261

表 3-8 零部件故障时系统的失效概率

事件代号	失效概率	事件代号	失效概率	事件代号	失效概率
X_1	0.3083	X_{13}	0.3012	Y_5	1.0000
X_2	0.3083	X_{14}	0.3011	Y_6	1.0000
X_3	0.3084	X_{15}	1.0000	Y_7	1.0000
X_4	0.3027	X_{16}	1.0000	Y_8	1.0000
X_5	0.3027	X_{17}	1.0000	Y_9	1.0000
X_6	0.2977	X_{18}	0.3115	Y_{10}	1.0000
X_7	0.2977	X_{19}	0.3115	Y_{11}	1.0000
X_8	1.0000	X_{20}	0.3115	Y_{12}	1.0000
X_9	1.0000	Y_1	1.0000	Y_{13}	1.0000
X_{10}	1.0000	Y_2	1.0000	Y_{14}	1.0000
X_{11}	1.0000	Y_3	1.0000	K_1	0.3102
X_{12}	1.0000	Y_4	1.0000	K_2	0.3102

3.6 本章小结

本章研究了基于贝叶斯网络和动态故障树的系统可靠性建模和评估方法。作为处理不确定性知识推理的强有力的工具，贝叶斯网络对随机不确定性知识的表达和推理具有很强的处理能力。针对基于马尔科夫模型的动态故障树求解方法中存在的状态爆炸问题，通过运用贝叶斯网络替代马尔科夫模型来求解动态故障树模型。本章阐述了贝叶斯网络的条件独立属性降低模型推理和计算复杂性的机理，提出了静态和动态故障树中各种逻辑门所对应的贝叶斯网络模型中节点的条件概率分布的确定方法，建立了卫星太阳翼驱动机构的动态故障树模型和相应的贝叶斯网络模型，并应用联合树推理算法对该模型进行了双向推理，其结果可用于指导系统的故障诊断和预计。通过找出系统的薄弱环节并实施设计改进，能够有效地提高系统的可靠性。实例分析结果表明：该方法能够有效地解决具有动态失效特性的复杂系统的可靠性分析和评估问题。

第四章 模糊数据下基于连续时间贝叶斯网络的动态故障树分析

基于离散时间贝叶斯网络的可靠性分析方法在一定程度上缓解了马尔科夫方法的状态空间爆炸问题，弥补了常规动态故障树分析方法的不足。但该方法不能得到系统可靠度的解析解，同时没有考虑失效数据的模糊性问题。本章将研究考虑模糊不确定性的基于连续时间贝叶斯网络的动态故障树分析方法。主要包括模糊失效率下的动态逻辑门输出变量的概率分布确定、系统模糊失效概率计算等。

4.1 引言

贝叶斯网络模型由于考虑了变量之间的条件独立性，在给定变量的所有父节点的状态组合下，该变量与网络中的其它变量条件独立，其概率分布中只包含所有父节点的信息，因此属于局部状态模型。相对于马尔科夫模型，贝叶斯网络模型的求解复杂度要低很多。

基于连续时间贝叶斯网络模型的可靠性分析方法能够解决复杂系统动态故障树模型的转化和求解问题。动态故障树模型定义了一组特殊的动态逻辑门来表达系统的各种动态失效特征，并对这些动态失效特征进行建模和求解分析。同样，连续时间贝叶斯网络模型也定义了一组基本结构来描述与动态逻辑门相对应的部件动态故障机理；可分别对各种动态失效特征进行建模，得到对应的子模型，然后对各个子模型进行组合，求解得到系统的可靠度和失效概率等可靠性特征量。基于连续时间贝叶斯网络模型的分析方法能够对系统进行多种分析，包括系统可靠度分析、不确定性分析和灵敏度分析等。

另一方面，基于连续时间贝叶斯网络模型的分析方法未考虑在实际工程问题中普遍存在的不确定性问题。比如在定量分析过程中，该方法假设零部件的失效率为已知的正实数，各个逻辑门的输入输出逻辑关系也是确定的关系。而在实际工程中，由于诸多原因的影响，常常不能得到准确的零部件失效率，或者由于某些不确定性因素的影响，逻辑门输入输出事件之间的逻辑关系并不是确定的，这时采用传统的实变量函数来描述零部件的失效率以及系统的失效逻辑关系就不符合实际工程情况。

Li 等[93]研究了在人因可靠性分析中的不确定性问题，通过采用模糊贝叶斯网络方法研究了组织对人因可靠性分析的影响。Penz 等[94]应用贝叶斯网络和混合模糊贝叶斯网络来预计压缩机的性能。Ferreira 和 Borenstein[95] 基于影响图和模糊逻

辑提出了一种模糊贝叶斯模型来解决供应商选择的问题。

模糊数学作为处理认知不确定性的一种常用方法，能够有效地解决实际工程问题中的不确定性问题。本章在连续时间贝叶斯网络模型的基础上，通过用模糊数表达零部件的失效率，对模糊数据下基于贝叶斯网络的可靠性建模和分析方法进行研究。

4.2 连续时间贝叶斯网络模型

4.2.1 单位阶跃函数

在使用贝叶斯网络进行动态故障树模型转化及概率推理的过程中，需要构造中间节点的条件概率表或条件概率密度函数，也就是动态逻辑门的输出事件的条件分布。在构造动态逻辑门的输出事件的条件概率分布时，为了表达逻辑门不同输入事件的失效时间先后顺序对输出事件状态的影响，Boudali 等[90]提出用单位阶跃函数来构造逻辑门的输出分布。由于单位阶跃函数的输入变量可用来描述输入事件的失效时间，因此该函数能准确表达输出分布与各个输入分布的定量关系。

定义单位阶跃函数如下：

$$u(t-\tau)=\begin{cases}1, & t>\tau\\ \dfrac{1}{2}, & t=\tau\\ 0, & t<\tau\end{cases} \tag{4-1}$$

其图形如图 4-1 所示。

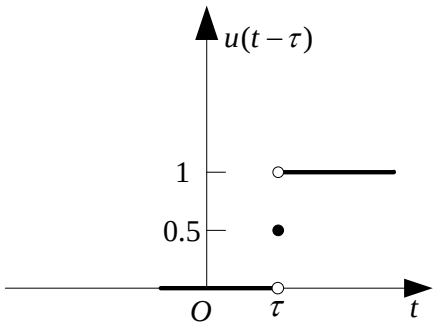


图 4-1 单位阶跃函数

4.2.2 冲激函数

在构造动态逻辑门的输出分布时，单位阶跃函数反映了不同输入的失效时间与输出的失效分布的关系，但此时输出分布还不具有密度函数的特征，因此，

Boudali 等[90]进一步引入冲激函数，利用冲激函数在整个实数轴的定积分为 1 的特点使得构造出的函数具有概率密度函数的特征。

冲激函数定义如下：

$$\delta(t-\tau)= \text{(}, \text{当} t \neq \tau \text{时} \tag{4-2}$$

该函数具有如下性质：

$$\int_{-\infty}^{\infty} \delta(t-\tau)dt = 1 \tag{4-3}$$

此处的积分变量为时间，取$(0,+\infty)$之间的正实数，因此式（4-3）可以改写为：

$$\int_{0}^{\infty} \delta(t-\tau)dt = 1 \tag{4-4}$$

冲激函数还具有如下重要性质：

$$\int_{0}^{\infty} f(t)\delta(t-\tau)dt = f(\tau) \tag{4-5}$$

4.2.3 L-R型模糊数及代数运算

1965 年，Zadeh 提出了模糊集合理论，将其用于处理不精确或模糊不确定性相关的问题[77]。其基本思想是把经典集合理论中元素对集合的绝对隶属关系模糊化，使得元素 x 对集合 A 的隶属程度不再局限于取 0 或 1，而是可以取从 0 到 1 的任何一个数值，这一数值反映了元素 x 隶属于集合 A 的程度。

定义 4-1：若 L 满足[96]：

（1）$L(x)=L(-x)$

（2）$L(0)=1$

（3）$L(x)$ 在$[0,+\infty]$上非增且逐段连续

则称 L 为模糊数的参照函数。

定义 4-2：设 L、R 为模糊数的参照函数，若

$$\mu_A(x)=\begin{cases} L[(m-x)/\alpha], & x \le m, \alpha > 0 \\ R[(x-m)/\beta], & x > m, \beta > 0 \end{cases} \tag{4-6}$$

则称模糊数为 $L-R$ 型模糊数，并记为 $\tilde{A}=(m,\alpha,\beta)_{LR}$。其中 m 为 $\tilde{A}$ 的均值，α,β 分别称为 $\tilde{A}$ 的置信上、下限。当 α,β 等于 0 时，$\tilde{A}$ 不是模糊数而是常规的清晰数。α,β 越大，$\tilde{A}$ 越模糊。

参照函数的形式有很多种，对应的 L-R 型模糊数的隶属函数也有多种形式。

常见的有三角型、正态型和尖型，如式（4-7）、（4-8）、（4-9）所示，其图形如图 4-2 所示。

三角模糊数的参照函数：

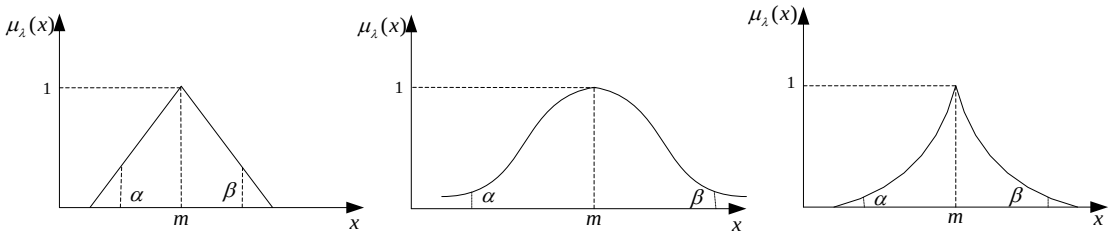
$$\begin{cases} L[(m-x)/\alpha] = \max\{0,1-(m-x/\alpha)\}, & x \le m, \alpha > 0 \\ R[(x-m)/\beta] = \max\{0,1-(x-m/\beta)\}, & x > m, \beta > 0 \end{cases} \tag{4-7}$$

正态模糊数的参照函数：

$$\begin{cases} L[(m-x)/\alpha] = \exp[-((m-x)/\alpha)^2], & x \le m, \alpha > 0 \\ R[(x-m)/\beta] = \exp[-((x-m)/\beta)^2], & x > m, \beta > 0 \end{cases} \tag{4-8}$$

尖型模糊数的参照函数：

$$\begin{cases} L[(m-x)/\alpha] = 1/[1+(m-x)/\alpha], & x \le m, \alpha > 0 \\ R[(x-m)/\beta] = 1/[1+(x-m)/\beta], & x > m, \beta > 0 \end{cases} \tag{4-9}$$



（a） （b） （c）

图 4-2 几种典型的模糊数

（a）三角模糊数；（b）正态型模糊数；（c）尖型模糊数

模糊数的代数运算法则如下[96]：

（1）加法⊕

$$(m,\alpha,\beta)_{LR} \oplus (n,\gamma,\delta)_{LR} = (m+n,\alpha+\gamma,\beta+\delta)_{LR} \tag{4-10}$$

（2）减法⊖

$$(m,\alpha,\beta)_{LR} \ominus (n,\gamma,\delta)_{LR} = (m-n,\alpha+\delta,\beta+\gamma)_{LR} \tag{4-11}$$

（3）乘法⊗

$$(m,\alpha,\beta)_{LR} \otimes (n,\gamma,\delta)_{LR} \simeq (mn, m\gamma+n\alpha, m\delta+n\beta)_{LR} \tag{4-12}$$

（4）除法⊘

$$(m,\alpha,\beta)_{LR} \oslash (n,\gamma,\delta)_{LR} \simeq (\frac{m}{n}, \frac{m\delta+n\alpha}{n^2}, \frac{m\gamma+n\beta}{n^2})_{LR} \tag{4-13}$$

4.2.4 故障树分析的模糊算子

传统故障树分析中顶事件的失效概率是利用逻辑门算子对基本事件发生的概率进行运算获得的。知道底事件的发生概率和结构函数就可以唯一确定系统顶事件的发生概率。而在模糊故障树分析过程中，采用模糊数 $\tilde{F}_i$ 来描述底事件发生的概率，同时用模糊门算子代替传统的逻辑门算子，从而得到顶事件发生概率的模糊数[97,98]。

故障树的与门结构和或门结构的模糊算子如下[97]：

（1）与门结构

$$\begin{aligned}\tilde{F}_s^{\text{and}} &= \prod_{i=1}^{\text{n}} \tilde{F}_i = \tilde{F}_1 \bullet \tilde{F}_2 \bullet \cdots \bullet \tilde{F}_n \\ &= (m_s, \alpha_s, \beta_s)_{LR} \\ &= (m_1, \alpha_1, \beta_1)_{LR} \bullet (m_2, \alpha_2, \beta_2)_{LR} \bullet \cdots \bullet (m_n, \alpha_n, \beta_n)_{LR} \\ &= (m_{s_{i-1}} m_i, m_{s_{i-1}} \alpha_i + m_i \alpha_{s_{i-1}}, m_{s_{i-1}} \beta_i + m_i \beta_{s_{i-1}})_{LR} \\ &= (m_{s_i}, \alpha_{s_i}, \beta_{s_i})_{LR}\end{aligned} \tag{4-14}$$

式中，$m_{s_i}, \alpha_{s_i}, \beta_{s_i} (i = 1, 2, \cdots, n)$ 分别为：

$$\begin{aligned}&m_{s_1} = m_1, m_{s_2} = m_1 m_2, m_{s_3} = m_{s_2} m_3, \cdots, \\ &m_{s_i} = m_{s_{i-1}} m_i \\ &\alpha_{s_1} = \alpha_1, \alpha_{s_2} = m_1 \alpha_2 + m_2 \alpha_1, \alpha_{s_3} = m_{s_2} \alpha_3 + m_3 \alpha_{s_2}, \cdots, \\ &\alpha_{s_i} = m_{s_{i-1}} \alpha_i + m_i \alpha_{s_{i-1}} \\ &\beta_{s_1} = \beta_1, \beta_{s_2} = m_1 \beta_2 + m_2 \beta_1, \beta_{s_3} = m_{s_2} \beta_3 + m_3 \beta_{s_2}, \cdots, \\ &\beta_{s_i} = m_{s_{i-1}} \beta_i + m_i \beta_{s_{i-1}}\end{aligned} \tag{4-15}$$

（2）或门结构

$$\begin{aligned}\tilde{F}_{\text{s}}^{or} &= 1 - \prod_{i=1}^{\text{n}} (1 - \tilde{F}_i) \\ &= (1,0,0)_{LR} - \{[(1,0,0)_{LR} - (m_1, \alpha_1, \beta_1)_{LR}] \\ &\bullet [(1,0,0)_{LR} - (m_2, \alpha_2, \beta_2)_{LR}] \\ &\bullet \cdots \bullet [(1,0,0)_{LR} - (m_n, \alpha_n, \beta_n)_{LR}]\}\end{aligned} \tag{4-16}$$

或者写成如下递归形式：

$$\begin{aligned}\tilde{F}_{\text{s}}^{or} &= (m_s, \alpha_s, \beta_s)_{LR} \\ &= (1,0,0)_{LR} - [m_{s_{i-1}}(1 - m_i), m_{s_{i-1}} \alpha_i + (1 - m_i) \alpha_{s_{i-1}} \\ &\quad m_{s_{i-1}} \beta_i + (1 - m_i) \beta_{s_{i-1}}]_{LR} \\ &= (1,0,0)_{LR} - (m_{s_i}, \alpha_{s_i}, \beta_{s_i})_{LR}\end{aligned} \tag{4-17}$$

式中，$m_{s_i},\alpha_{s_i},\beta_{s_i}(i=1,2,\cdots,n)$ 分别为：

$$\begin{aligned}
&m_{s_1}=m_1, m_{s_2}=(1-m_1)(1-m_2),\\
&m_{s_3}=m_{s_2}(1-m_3),\cdots,m_{s_i}=m_{s_{i-1}}(1-m_i)\\
&\alpha_{s_1}=\alpha_1,\alpha_{s_2}=(1-m_1)\alpha_2+(1-m_2)\alpha_1,\\
&\alpha_{s_3}=m_{s_2}\alpha_3+(1-m_3)\alpha_{s_2},\cdots,\alpha_{s_i}=m_{s_{i-1}}\alpha_i+(1-m_i)\alpha_{s_{i-1}}\\
&\beta_{s_1}=\beta_1,\beta_{s_2}=(1-m_1)\beta_2+(1-m_2)\beta_1,\\
&\beta_{s_3}=m_{s_2}\beta_3+(1-m_3)\beta_{s_2},\cdots,\beta_{s_i}=m_{s_{i-1}}\beta_i+(1-m_i)\beta_{s_{i-1}}
\end{aligned} \tag{4-18}$$

4.3 BN 模型中非根节点的概率分布问题

如前所述，贝叶斯网络的图形结构描述了系统中部件失效的定性关系，或者说是网络中节点之间的定性影响关系，各个节点的概率分布描述了节点与其所有父节点之间的概率依赖关系。本节讨论连续时间贝叶斯网络中非根节点的条件概率密度函数的构造问题。

由于本文中的 BN 模型是由故障树转化而来的，因此本节按照逻辑门类型来展开讨论。

4.3.1 与门输出事件的模糊概率分布函数

假设与门有两个输入事件，分别记为 *A*、*B*，输出事件记为 *T*。其故障树模型及相应的贝叶斯网络模型如图 4-3（a）与（b）所示。

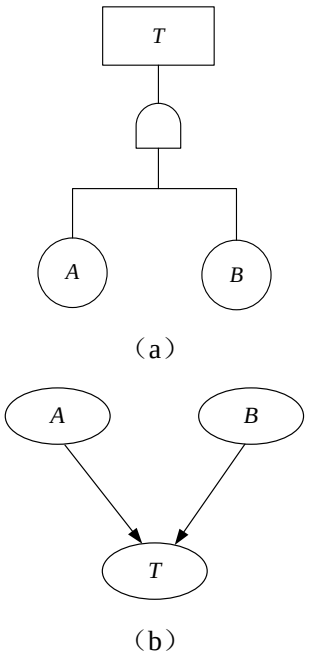


图 4-3 与门结构及等价的贝叶斯网络模型

（a）与门故障树模型；（b）与门贝叶斯网络模型

考虑模糊不确定性的影响，以模糊数 $\tilde{\lambda}_A$ 和 $\tilde{\lambda}_B$ 描述输入事件的失效率。在基本事件服从指数分布的假设下，输入事件的模糊边缘概率密度函数为：

$$\tilde{f}_A(a)=\tilde{\lambda}_A e^{-\tilde{\lambda}_A a} \tag{4-19}$$

$$\tilde{f}_B(b)=\tilde{\lambda}_B e^{-\tilde{\lambda}_B b} \tag{4-20}$$

根据与门的失效机理，由单位阶跃函数以及冲激函数构造出输出事件 T 的条件概率密度函数为：

$$f_{T|A,B}\left(t|a,b\right)=u\left(b-a\right)\delta\left(t-b\right)+u\left(a-b\right)\delta\left(t-a\right) \tag{4-21}$$

图 4-3（b）所示贝叶斯网络的模糊联合概率密度函数为：

$$\tilde{f}_{ABT}\left(a,b,t\right)=f_{T|A,B}\left(t|a,b\right)\tilde{f}_B\left(b\right)\tilde{f}_A\left(a\right) \tag{4-22}$$

对变量 a、b 积分，得到输出事件 T 的模糊边缘概率密度函数如下：

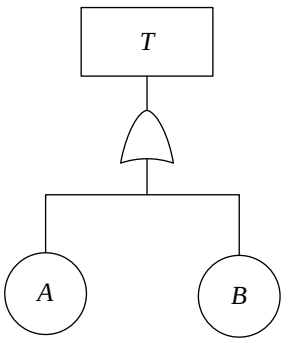
$$\begin{aligned}
\tilde{f}_T(t)&=\int_0^\infty\int_0^\infty u(b-a)\delta(t-b)\,\tilde{f}_B(b)\,\tilde{f}_A(a)dbda+\int_0^\infty\int_0^\infty u(a-b)\delta(t-a)\,\tilde{f}_B(b)\,\tilde{f}_A(a)dbda\\
&=\int_0^\infty\delta(t-b)\,\tilde{f}_B(b)\left[\int_0^\infty u(b-a)\,\tilde{f}_A(a)da\right]db+\int_0^\infty\delta(t-a)\,\tilde{f}_A(a)\left[\int_0^\infty u(a-b)\,\tilde{f}_B(b)db\right]da\\
&=\int_0^\infty\delta(t-b)\,\tilde{f}_B(b)\cdot\int_0^b\tilde{f}_A(a)dadb+\int_0^\infty\delta(t-a)\,\tilde{f}_A(a)\cdot\int_0^a\tilde{f}_B(b)dbda\\
&=\int_0^\infty\tilde{f}_B(b)\delta(t-b)\tilde{F}_A(b)db+\int_0^\infty\tilde{f}_A(a)\delta(t-a)\tilde{F}_B(a)da\\
&=\left[\tilde{F}_B(t)\tilde{F}_A(t)\right]'
\end{aligned} \tag{4-23}$$

则输出事件发生的模糊概率分布函数为：

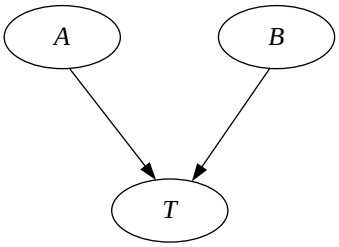
$$\tilde{F}_T(t)=\tilde{P}(T<t)=\int_0^t\tilde{f}_T(\tau)d\tau=\tilde{F}_B(t)\tilde{F}_A(t) \tag{4-24}$$

4.3.2 或门输出事件的模糊概率分布函数

与上述与门类似，假设或门具有两个输入事件 A、B，输出事件为 T。则根据或门的失效机理得到其故障树模型及相应的贝叶斯网络模型，如图 4-4 所示。



（a）



（b）

图 4-4 或门故障树模型及其相应的贝叶斯网络模型

（a）或门故障树模型；（b）或门贝叶斯网络模型

同理，以模糊数 $\tilde{\lambda}_A$ 和 $\tilde{\lambda}_B$ 描述输入事件 A 与 B 的失效率，以 $\tilde{f}_A(a)$ 及 $\tilde{f}_B(b)$ 表示 A 与 B 失效的模糊边缘概率密度函数。根据输出事件的失效特征，由单位阶跃函数及冲激函数构造出如下输出事件的条件概率密度函数：

$$f_{T|A,B}\left(t|a,b\right)=u\left(b\text{-}a\right)\delta\left(t\text{-}a\right)+u\left(a\text{-}b\right)\delta\left(t\text{-}b\right) \tag{4-25}$$

则上述或门的输入输出变量之间的模糊联合概率密度函数为：

$$\tilde{f}_{ABT}\left(a,b,t\right)=f_{T|A,B}\left(t|a,b\right)\tilde{f}_B\left(b\right)\tilde{f}_A\left(a\right) \tag{4-26}$$

对输入变量 a、b 积分，得到输出事件 T 在时刻 t 的模糊边缘概率密度函数如下：

$$\begin{aligned}
\tilde{f}_T\left(t\right)&=\int_0^\infty\int_0^\infty\tilde{f}_{T,A,B}\left(a,b,t\right)dbda\\
&=\int_0^\infty\int_0^\infty u\left(b-a\right)\delta\left(t-a\right)\tilde{f}_B\left(b\right)\tilde{f}_A\left(a\right)dbda+\int_0^\infty\int_0^\infty u\left(a-b\right)\delta\left(t-b\right)\tilde{f}_B\left(b\right)\tilde{f}_A\left(a\right)dbda\\
&=\int_0^\infty\delta\left(t-a\right)\tilde{f}_A\left(a\right)da\int_a^\infty\tilde{f}_B\left(b\right)db+\int_0^\infty\delta\left(t-b\right)\tilde{f}_B\left(b\right)db\int_b^\infty\tilde{f}_A\left(a\right)da\\
&=\int_0^\infty\delta\left(t-a\right)\tilde{f}_A\left(a\right)\{1-\tilde{F}_B(a)\}da+\int_0^\infty\delta\left(t-b\right)\tilde{f}_B\left(b\right)\{1-\tilde{F}_A(b)\}db\\
&=\tilde{f}_A(t)\{1-\tilde{F}_B(t)\}+\tilde{f}_B(t)\{1-\tilde{F}_A(t)\}\\
&=\tilde{f}_A(t)+\tilde{f}_B(t)-[\tilde{F}_A(t)\tilde{F}_B(t)]'
\end{aligned} \tag{4-27}$$

则输出事件 T 的模糊概率分布函数为：

$$\tilde{F}_T(t)=\tilde{P}(T<t)=\int_0^t\tilde{f}_T(\tau)d\tau=\tilde{F}_A(t)+\tilde{F}_B(t)-\tilde{F}_A(t)\tilde{F}_B(t) \tag{4-28}$$

4.3.3 备件门的模糊概率密度函数

假设备件门具有主输入 A 与备份输入 B，输出为 T。A 的失效率为 $\tilde{\lambda}_A$，B 的独立失效率为 $\tilde{\lambda}_{Bi}$，备用状态失效率为 $\alpha\bullet\tilde{\lambda}_{Bi}$，其中 α 为备份因子。其故障树模型及相应的贝叶斯网络模型如图 4-5 所示，这里 SP 指任意一种备件门。

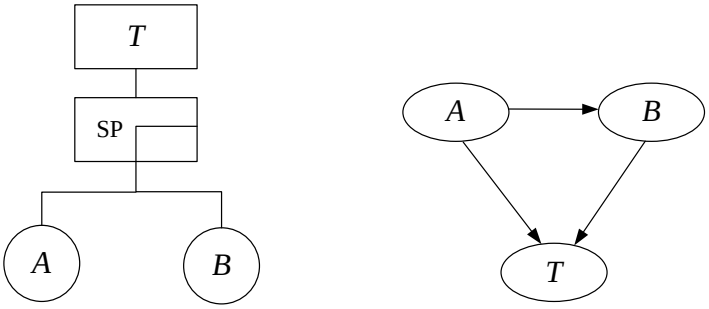


图 4-5 备件门及其等价的贝叶斯网络模型

（a）备件们故障树模型；（b）备件门贝叶斯网络模型

下面根据备份类型的不同，按照温备份、热备份以及冷备份的情况分别讨论备件的条件分布。备件门输出的边缘分布由主件 A 的边缘分布与备件 B 的条件分布按照与门连接关系得到，这里不再赘述。

（1）当逻辑门为温备份 WSP 时

当 A 在 a 时刻失效时，备件 B 在 b 时刻失效的条件失效率为：

$$\tilde{\lambda}_{B|A}(b\,|\,a)=u(a-b)\bullet\alpha\bullet\tilde{\lambda}_{Bi}(b)+u(b-a)\bullet\tilde{\lambda}_{Bi}(b) \tag{4-29}$$

设 B 的独立失效分布函数为 $\tilde{F}_{Bi}(b)$，则根据失效密度与失效率之间的关系式：

$$f(t)=\lambda(t)\bullet e^{-\int_0^t\lambda(\tau)d\tau}$$

可得 B 的模糊条件失效密度函数为：

$$\begin{aligned}\tilde{f}_{B|A}\left(b|a\right)&=\tilde{\lambda}_{B|A}\left(b|a\right)e^{-\int_0^b\tilde{\lambda}_{B|A}(t|a)dt}\\&=\left[u\left(a-b\right)\alpha\tilde{\lambda}_{Bi}\left(b\right)+u\left(b-a\right)\tilde{\lambda}_{Bi}\left(b\right)\right]e^{-\int_0^b\left[u(a-t)\alpha\tilde{\lambda}_{Bi}(t)+u(t-a)\tilde{\lambda}_{Bi}(t)\right]dt}\\&=u\left(a-b\right)\alpha\tilde{\lambda}_{Bi}\left(b\right)\times e^{-\int_0^b\alpha\tilde{\lambda}_{Bi}(t)dt}+u\left(b-a\right)\tilde{\lambda}_{Bi}\left(b\right)\times e^{-\int_0^a\alpha\tilde{\lambda}_{Bi}(t)dt}\times e^{-\int_a^b\tilde{\lambda}_{Bi}(t)dt}\\&=u\left(a-b\right)\alpha\tilde{\lambda}_{Bi}\left(b\right)\times\left[e^{-\int_0^b\tilde{\lambda}_{Bi}(t)dt}\right]^{\alpha}+u\left(b-a\right)\tilde{\lambda}_{Bi}\left(b\right)\times\left[\tilde{R}_{Bi}\left(a\right)\right]^{\alpha}\times\frac{e^{-\int_0^b\tilde{\lambda}_{Bi}(t)dt}}{e^{-\int_0^a\tilde{\lambda}_{Bi}(t)dt}}\\&=u\left(a-b\right)\alpha\,\hat{f}_{Bi}\left(b\right)\cdot\left[1-\tilde{F}_{Bi}\left(b\right)\right]^{\alpha-1}+u\left(b-a\right)\tilde{f}_{Bi}\left(b\right)\cdot\left[1-\tilde{F}_{Bi}\left(a\right)\right]^{\alpha-1}\end{aligned} \tag{4-30}$$

B 的模糊边缘概率密度函数为：

$$\begin{aligned}\tilde{f}_B(b)&=\int_0^{\infty}\tilde{f}_{B|A}(b\,|\,a)\tilde{f}_A(a)da\\&=\int_0^{\infty}\left\{u(a-b)\alpha\,\tilde{f}_{Bi}(b)\left[1-\tilde{F}_{Bi}(b)\right]^{\alpha-1}+u(b-a)\,\tilde{f}_{Bi}(b)\left[1-\tilde{F}_{Bi}(a)\right]^{\alpha-1}\right\}\tilde{f}_A(a)da\\&=\int_b^{\infty}\alpha\,\tilde{f}_{Bi}(b)\left[1-\tilde{F}_{Bi}(b)\right]^{\alpha-1}\tilde{f}_A(a)da+\int_0^{b}\tilde{f}_{Bi}(b)\left[1-\tilde{F}_{Bi}(a)\right]^{\alpha-1}\tilde{f}_A(a)da\\&=\alpha\,\tilde{f}_{Bi}(b)\left[1-\tilde{F}_{Bi}(b)\right]^{\alpha-1}\left[1-\tilde{F}_A(b)\right]+\int_0^{b}\tilde{f}_{Bi}(b)\left[1-\tilde{F}_{Bi}(a)\right]^{\alpha-1}\tilde{f}_A(a)da\end{aligned}\tag{4-31}$$

（2）当逻辑门为热备份 HSP 时

此时备份因子α=1，条件失效率变为：

$$\tilde{\lambda}(b|a)=\tilde{\lambda}_{Bi}(b)$$

式（4-30）退化为：

$$\begin{aligned}\tilde{f}_{B|A}(b|a)&=u(a-b)\,\tilde{f}_{Bi}(b)+u(b-a)\,\tilde{f}_{Bi}(b)\\&=\tilde{f}_{Bi}(b)\end{aligned}\tag{4-32}$$

模糊边缘概率密度函数为：

$$\begin{aligned}\tilde{f}_B(b)&=\int_0^{\infty}\tilde{f}_{B|A}(b\,|\,a)\tilde{f}_A(a)da\\&=\int_0^{\infty}\tilde{f}_{B_i}(b)\tilde{f}_A(a)da\\&=\tilde{f}_{B_i}(b)\int_0^{\infty}\tilde{f}_A(a)da\\&=\tilde{f}_{B_i}(b)\end{aligned}\tag{4-33}$$

（3）当逻辑门为冷备份 CSP 时

此时α=0，$\tilde{\lambda}_{B/A}(b|a)=u(b-a)\tilde{\lambda}_{Bi}(b-a)$，于是，条件失效密度函数为：

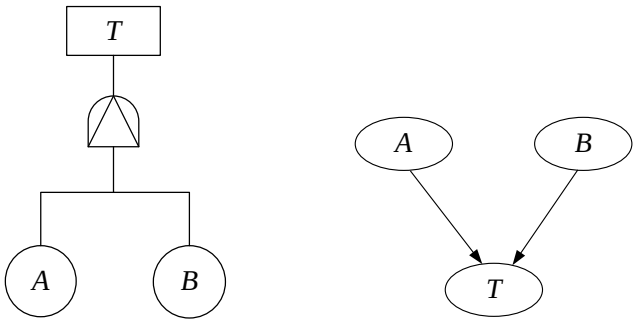
$$\begin{aligned}\tilde{f}_{B|A}(b|a)&=\tilde{\lambda}_{B|A}(b|a)e^{-\int_0^b\tilde{\lambda}_{B|A}(t|a)dt}\\&=u(b-a)\tilde{\lambda}_{Bi}(b-a)e^{-\int_a^b\tilde{\lambda}_{Bi}(t-a)dt}\\&=u(b-a)\tilde{\lambda}_{Bi}(b-a)e^{-\int_0^{b-a}\tilde{\lambda}_{Bi}(t)dt}\\&=u(b-a)\tilde{f}_{Bi}(b-a)\end{aligned}\tag{4-34}$$

则 B 的模糊边缘失效密度函数为：

$$\begin{aligned}\tilde{f}_B(b)&=\int_0^{\infty}\tilde{f}_{B|A}(b\,|\,a)\tilde{f}_A(a)da\\&=\int_0^{\infty}u(b-a)\,\tilde{f}_{B_i}(b-a)\tilde{f}_A(a)da\\&=\int_0^{b}\tilde{f}_{B_i}(b-a)\,\tilde{f}_A(a)da\end{aligned}\tag{4-35}$$

4.3.4 优先与门输出事件的模糊概率分布函数

假设优先与门只有两个输入事件 A，B（具有多个输入时，将其分解成多个优先与门的组合再依次进行求解），输出事件为 T。可得优先与门的故障树模型及相应的贝叶斯网络模型如图 4-6 所示。



（a）　　（b）

图 4-6 优先与门故障树模型及其贝叶斯网络模型

（a）优先与门故障树模型；（b）优先与门贝叶斯网络模型

优先与门的失效机理为：当 A 先失效、B 后失效时，输出事件与 B 同时发生；当 B 先失效而 A 后失效时，输出事件不发生，也即是说输出事件在 $t\to\infty$ 时发生。根据以上失效机理构造出优先与门输出事件发生的条件概率密度函数为：

$$f_{T|A,B}\left(t|a,b\right)=u\left(b\text{-}a\right)\delta\left(t\text{-}b\right)+u\left(a\text{-}b\right)\delta\left(t\text{-}\infty\right) \tag{4-36}$$

以模糊数 $\tilde{\lambda}_A$ 和 $\tilde{\lambda}_B$ 描述输入事件 A 与 B 的失效率，以 $\tilde{f}_A$(a) 及 $\tilde{f}_B$(b) 表示 A 与 B 失效的模糊边缘概率密度函数，则优先与门的模糊联合概率密度函数为：

$$\tilde{f}_{ABT}\left(a,b,t\right)=f_{T|A,B}\left(t|a,b\right)\tilde{f}_B\left(b\right)\tilde{f}_A\left(a\right) \tag{4-37}$$

上述联合概率密度函数对 a、b 积分，得到输出事件 T 的模糊边缘概率密度函数为：

$$\begin{aligned}
\tilde{f}_T\left(t\right)&=\int_0^\infty\int_0^\infty f_{T|A,B}(t\,|\,a,b)\tilde{f}_A(a)\,\tilde{f}_B(b)dbda\\
&=\int_0^\infty\int_0^\infty\{u\left(b-a\right)\delta\left(t-b\right)+u(a-b)\delta(t-\infty)\}\,\tilde{f}_A\left(a\right)\,\tilde{f}_B\left(b\right)dbda\\
&=\int_0^\infty\int_0^\infty u\left(b-a\right)\delta\left(t-b\right)\,\tilde{f}_B\left(b\right)\,\tilde{f}_A\left(a\right)dbda+\int_0^\infty\int_0^\infty u\left(a-b\right)\delta\left(t-\infty\right)\,\tilde{f}_B\left(b\right)\,\tilde{f}_A\left(a\right)dbda\\
&=\int_0^\infty\delta\left(t-b\right)\,\tilde{f}_B\left(b\right)db\int_0^b\,\tilde{f}_A\left(a\right)da+\delta\left(t-\infty\right)\int_0^\infty\,\tilde{f}_A\left(a\right)da\int_0^a\,\tilde{f}_B\left(b\right)db\\
&=\int_0^\infty\delta\left(t-b\right)\,\tilde{f}_B\left(b\right)\tilde{F}_A(b)db+\delta\left(t-\infty\right)\int_0^\infty\,\tilde{f}_A\left(a\right)\tilde{F}_B\left(a\right)da\\
&=\tilde{f}_B\left(t\right)\tilde{F}_A(t)+\delta\left(t-\infty\right)\int_0^\infty\,\tilde{f}_A\left(a\right)\tilde{F}_B\left(a\right)da
\end{aligned} \tag{4-38}$$

则输出事件的模糊概率分布函数为：

$$\begin{aligned}\tilde{P}(T \le t) &= \int_0^t \tilde{f}_T(\tau)d\tau \\ &= \int_0^t \tilde{f}_B(\tau)\tilde{F}_A(\tau)d\tau\end{aligned} \tag{4-39}$$

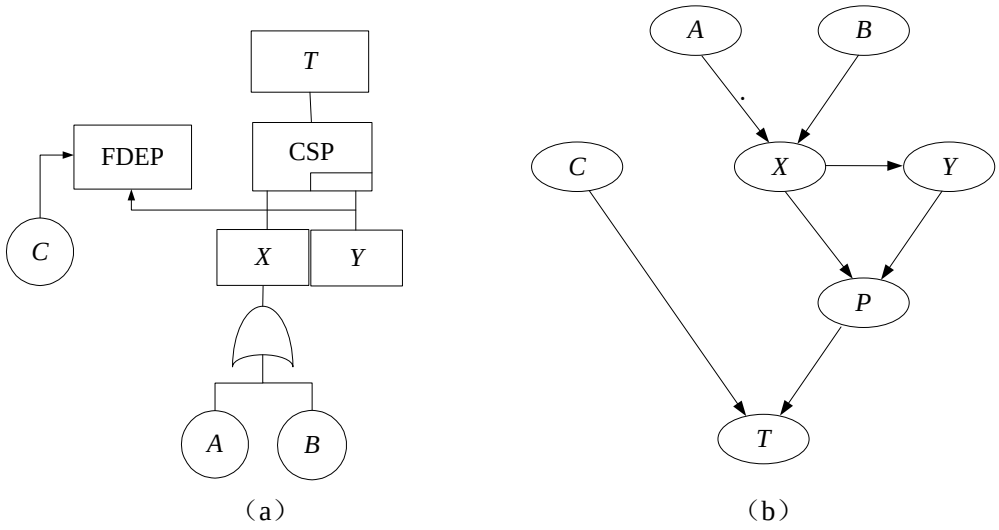
4.4 模型验证与算例分析

本节以图 4-7（a）所示动态故障树为算例，讨论本章所提出的方法的可行性。

该故障树由三个底事件 *A*、*B* 和 C，两个中间事件 *X*、*Y* 以及顶事件 *T* 组成。底事件 *A*、*B* 以或门连接，输出事件为 *X*；*Y* 是与 *X* 相同的子树，作为 *X* 的冷备份部件；*C* 为功能触发事件，当 *C* 失效时同时触发 *X* 与 *Y* 失效，也就是触发冷备件门 CSP 的输出事件发生。

按照故障树模型向贝叶斯网络模型转化的方法，把图 4-7（a）中的各级事件和逻辑门分别转化成贝叶斯网络的节点和有向弧，得到如图 4-7（b）所示的 BN 模型。因为功能相关门触发冷备件门的输出事件，而该输出事件直接导致顶事件的发生，也即是说功能相关门的输入事件 *C* 与 CSP 的输出以“或”的逻辑关系影响顶事件 *T* 的发生。因此在转化的 BN 模型中添加中间节点 *P* 作为 CSP 的输出节点，并与节点 *C* 同时指向子节点 *T*，且 *T* 的条件概率密度为或门的表达形式。

以三角模糊数 $\tilde{\lambda} = (m_1, m, m_2)$ 表示该故障树模型中各个底事件的模糊失效率，假设其失效率均值如表 4-1 中第三列所示。参照 Dubois 和 Prade[96]提出的模糊数左右分布的确定原则，取与均值相差 15%的值为其左右分布列于表 4-1 中。这里仍然假设 BN 模型中根节点服从指数分布。



（a） （b）

图 4-7 算例动态故障树及贝叶斯网络模型

（a）动态故障树模型；（b）贝叶斯网络模型

表 4-1 底事件失效数据（$10^{-5}h^{-1}$）

底事件代码	失效率下限 m_1	失效率均值 m	失效率上限 m_2
A	1.0650	1.2500	1.4370
B	0.7310	0.8600	0.9890
C	2.2100	2.6000	2.9900

按照层次法的思想逐层求解该 BN 模型。

第一步：首先求解最底层的输出节点 X 的分布。

分别以 $\tilde{\lambda}_A$ 与 $\tilde{\lambda}_B$ 、 $\tilde{f}_A(a)$ 与 $\tilde{f}_B(b)$ 以及 $\tilde{F}_A(x)$ 与 $\tilde{F}_B(x)$ 表示根节点 A 与 B 的模糊失效率、失效的模糊概率密度函数以及失效的模糊概率分布函数。把输入事件的密度函数及分布函数表达式代入 4.3 节中或门输出事件的模糊概率密度函数公式，得到节点 X 的边缘概率密度函数为：

$$\begin{aligned}\tilde{f}_X(x) &= \tilde{f}_A(x)+\tilde{f}_B(x)-[\tilde{F}_A(x)\tilde{F}_B(x)]' \\ &= \tilde{\lambda}_A e^{-\tilde{\lambda}_A x}+\tilde{\lambda}_B e^{-\tilde{\lambda}_B x}-[(1-e^{-\tilde{\lambda}_A x})(1-e^{-\tilde{\lambda}_B x})]' \\ &= (\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}\end{aligned} \tag{4-40}$$

第二步：推导备件门输出节点 P 的概率分布。

Y 为 X 的备件，因此 Y 的独立失效概率密度函数与 X 相同，即有：

$$\tilde{f}_{Yi}(y)=(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)y} \tag{4-41}$$

由式（4-32）得 Y 的条件概率密度函数为：

$$\begin{aligned}\tilde{f}_{Y|X}\left(y|x\right) &= u(y-x)\,\tilde{f}_{Yi}\left(y-x\right) \\ &= u(y-x)(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(y-x)}\end{aligned} \tag{4-42}$$

备件门输出节点 P 的条件密度函数与与门相同，因此有：

$$f_{P|X,Y}\left(p|x,y\right)=u\left(y\text{-}x\right)\delta\left(p\text{-}y\right)+u\left(x\text{-}y\right)\delta\left(p\text{-}x\right) \tag{4-43}$$

由上述节点 X、Y、P 的密度函数得节点 P 的模糊边缘密度函数为：

$$\begin{aligned}\tilde{f}_P(p) &= \int_0^\infty\int_0^\infty f_{P|X,Y}\left(p|x,y\right)\tilde{f}_{Y|X}\left(y|x\right)\tilde{f}_X(x)dydx \\ &= \int_0^\infty\int_0^\infty [u\left(y-x\right)\delta\left(p-y\right)+u\left(x-y\right)\delta\left(p-x\right)]u(y-x)(\tilde{\lambda}_A+\tilde{\lambda}_B) \\ &\quad \times e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(y-x)}(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dydx \\ &= \int_0^\infty\int_0^\infty u\left(y-x\right)\delta\left(p-y\right)u(y-x)(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(y-x)}(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dydx \\ &\quad +\int_0^\infty\int_0^\infty u\left(x-y\right)\delta\left(p-x\right)u(y-x)(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(y-x)}(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dydx\end{aligned} \tag{4-44}$$

利用式（4-4）分别求解上式的两项，第一项求解如下：

$$\begin{aligned}
&\int_0^\infty\int_0^\infty u(y-x)\delta(p-y)u(y-x)(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(y-x)}(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dydx\\
&=(\tilde{\lambda}_A+\tilde{\lambda}_B)^2\int_0^\infty u(p-x)u(p-x)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(p-x)}e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dx\\
&=(\tilde{\lambda}_A+\tilde{\lambda}_B)^2\int_0^\infty u(p-x)u(p-x)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}dx\\
&=(\tilde{\lambda}_A+\tilde{\lambda}_B)^2e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}\int_0^\infty u(p-x)u(p-x)dx\\
&=p(\tilde{\lambda}_A+\tilde{\lambda}_B)^2e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}
\end{aligned}\tag{4-45}$$

第二项求解如下：

$$\begin{aligned}
&\int_0^\infty\int_0^\infty u(x-y)\delta(p-x)u(y-x)(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(y-x)}(\tilde{\lambda}_A+\tilde{\lambda}_B)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dydx\\
&=(\tilde{\lambda}_A+\tilde{\lambda}_B)^2\int_0^\infty u(x-p)u(p-x)e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)(p-x)}e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)x}dx\\
&=(\tilde{\lambda}_A+\tilde{\lambda}_B)^2e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}\int_0^\infty u(x-p)u(p-x)dx
\end{aligned}\tag{4-46}$$

由阶跃函数的表达式可知，该积分值为零。

故最终得到 P 的概率密度函数为：

$$\tilde{f}_P(p)=p(\tilde{\lambda}_A+\tilde{\lambda}_B)^2e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}\tag{4-47}$$

节点 P 的概率分布函数为：

$$\begin{aligned}
\tilde{F}_P(p)&=\int_0^p\tilde{f}_P(p)dp\\
&=\int_0^p p(\tilde{\lambda}_A+\tilde{\lambda}_B)^2e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}dp\\
&=1-e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}-(\tilde{\lambda}_A+\tilde{\lambda}_B)p\cdot e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)p}
\end{aligned}\tag{4-48}$$

第三步：求解节点 T 的概率分布。

节点 C 的概率密度函数 $\tilde{f}_C(c)$ 为：

$$\tilde{f}_C(c)=\tilde{\lambda}_Ce^{-\tilde{\lambda}_Cc}\tag{4-49}$$

节点 C 的概率分布函数 $\tilde{F}_C(c)$ 为：

$$\begin{aligned}
\tilde{F}_C(c)&=\int_0^c\tilde{f}_C(c)dc\\
&=1-e^{-\tilde{\lambda}_Cc}
\end{aligned}\tag{4-50}$$

则节点 T 的边缘概率密度函数 $\tilde{f}_T(t)$ 为：

$$\tilde{f}_T(t)=\tilde{f}_P(t)+\tilde{f}_C(t)-[\tilde{F}_P(t)\tilde{F}_C(t)]'\tag{4-51}$$

最终得到叶节点 T 失效的模糊概率分布函数为：

$$\begin{aligned}\tilde{F}_T(t) &= \int_0^t \tilde{f}_T(t)dt \\ &= \int_0^t \{\tilde{f}_P(t) + \tilde{f}_C(t) - [\tilde{F}_P(t)\tilde{F}_C(t)]'\}dt \\ &= \tilde{F}_P(t) + \tilde{F}_C(t) - [\tilde{F}_P(t)\tilde{F}_C(t)] \\ &= [1 - e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)t} - (\tilde{\lambda}_A + \tilde{\lambda}_B)t \cdot e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)t}] + (1 - e^{-\tilde{\lambda}_C t}) \\ &\quad -[(1 - e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)t} - (\tilde{\lambda}_A + \tilde{\lambda}_B)t \cdot e^{-(\tilde{\lambda}_A+\tilde{\lambda}_B)t})(1 - e^{-\tilde{\lambda}_C t})]\end{aligned} \tag{4-52}$$

求解上述模糊失效概率函数，即可得到故障树对应的系统在给定时刻 t 时的模糊失效概率，也可以求解系统的模糊可靠度随时间变化的关系曲线。

图 4-8 为系统在 t=5000h 的模糊失效概率的隶属函数。

图 4-9 为系统在 t=10000h 的模糊失效概率的隶属函数。

图 4-10 为系统在隶属度 $\alpha = 1$ 及 $\alpha = 0$ 下，任务时间 $t = 100000\,\mathrm{h}$ 的模糊可靠度曲线。

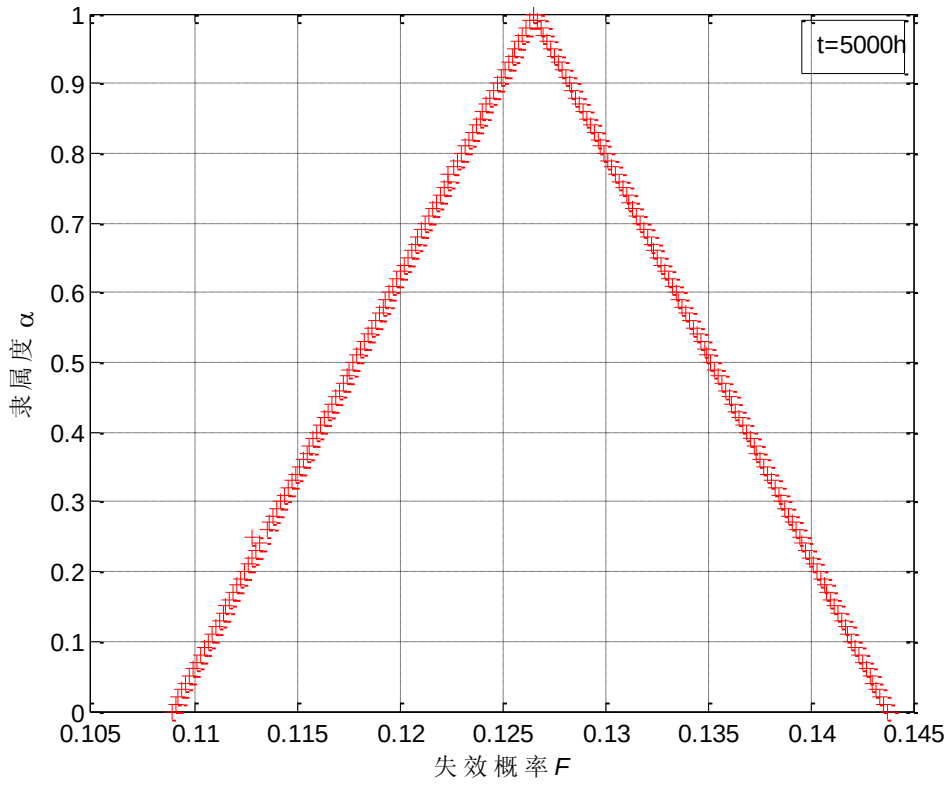


图 4-8 t=5000h 的失效概率隶属函数

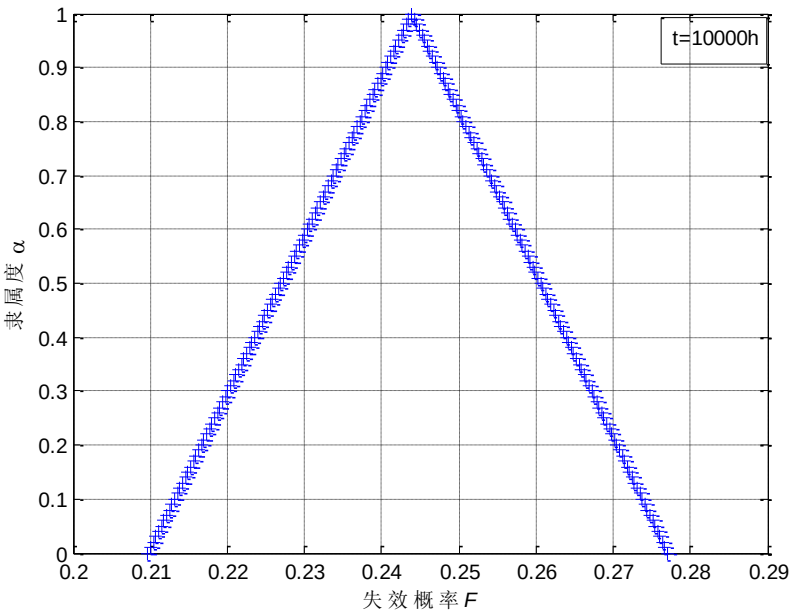


图 4-9 t=10000h 的失效概率隶属函数

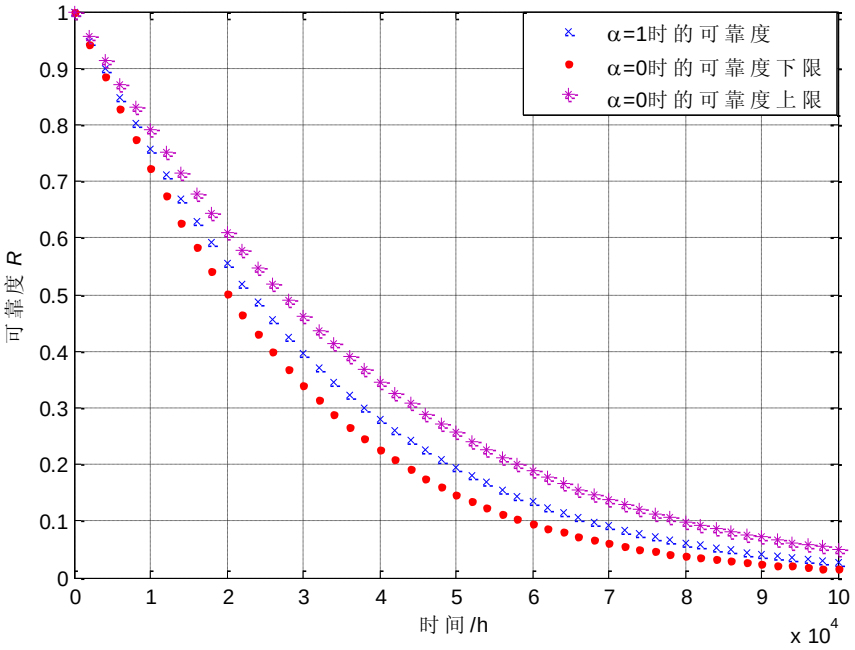


图 4-10 系统的模糊可靠度

4.5 实例分析：某大型矿用挖掘机整流回馈系统可靠性分析

4.5.1 某大型矿用挖掘机整流回馈系统动态故障树建模

大型矿用挖掘机是露天矿山采装作业的主要设备。某大型矿用挖掘机用于千

万吨级大型露天矿场的采装作业，其电气控制采用交流变频调速系统。该系统由上位综合监控系统、PLC 及基础变频传动系统组成三级控制系统。挖掘机行走、回转、推压、提升以及开斗等基础动作均由电气系统控制完成。

整流回馈系统的工作原理如下：供电系统电流经过主变压器二次侧，直接传入整流回馈系统。整流回馈系统由整流回馈单元、公用直流母线以及逆变单元组成。其中整流回馈单元将供电系统传输过来的交流电转换为电压稳定的直流电，使得即使在逆变器能量回馈到电网时，该电压在规定范围内仍保持恒定。整流回馈单元内部由两台容量相同的控制柜并联运行，其中一套为主装置，另一套为从装置；通过 SLB 板和光缆将 2 台控制柜连接起来。两套控制装置并联后的直流输出母线作为公用直流母线，为各机构逆变器提供直流电源[99-101]。逆变单元由直接挂接在直流母线上的各机构逆变器构成，用于将母线上的直流电转换为电压、频率可调的交流电，从而实现电机平滑调速。电涌保护箱用于限制系统中因雷电引起的过电压，以及因系统操作产生的过电压。

除了上段所述的内部工作原理外，整流回馈系统的工作还受 PLC 控制系统的控制。PLC 控制系统采用 PROFIBUS DP 现场总线通讯网络控制，通过挂接在总线上的整流控制器、各机构逆变器，获取整流回馈单元以及逆变单元运行状态、故障信息以及安全保护等，然后经逻辑与数据运算后经由相同的路径对整流回馈系统以及整个电气系统进行控制。其工作原理如图 4-11 所示。

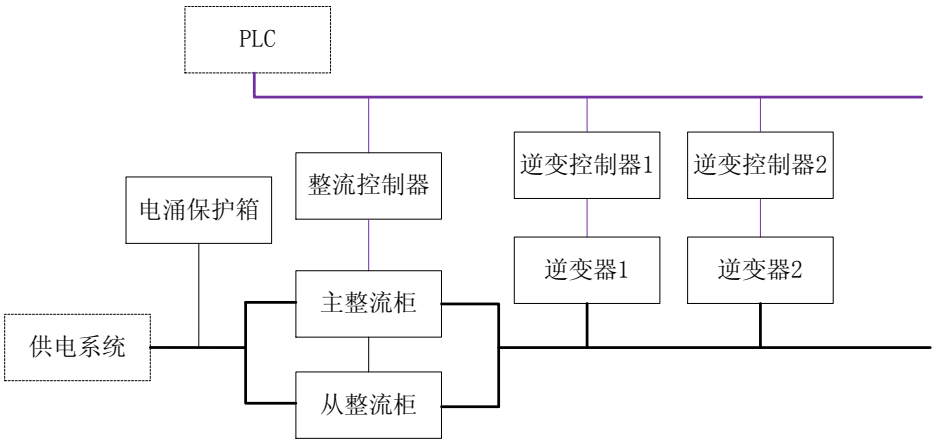


图 4-11 整流回馈系统工作原理图

系统中采用主从整流柜，将其失效逻辑视为热备份。另外，整流控制器对主从整流柜提供控制信号，其失效机理存在功能相关性。按照上述功能原理分析及失效分析，以“整流回馈系统故障”为顶事件，得到系统的动态故障树模型如图 4-12 所示。

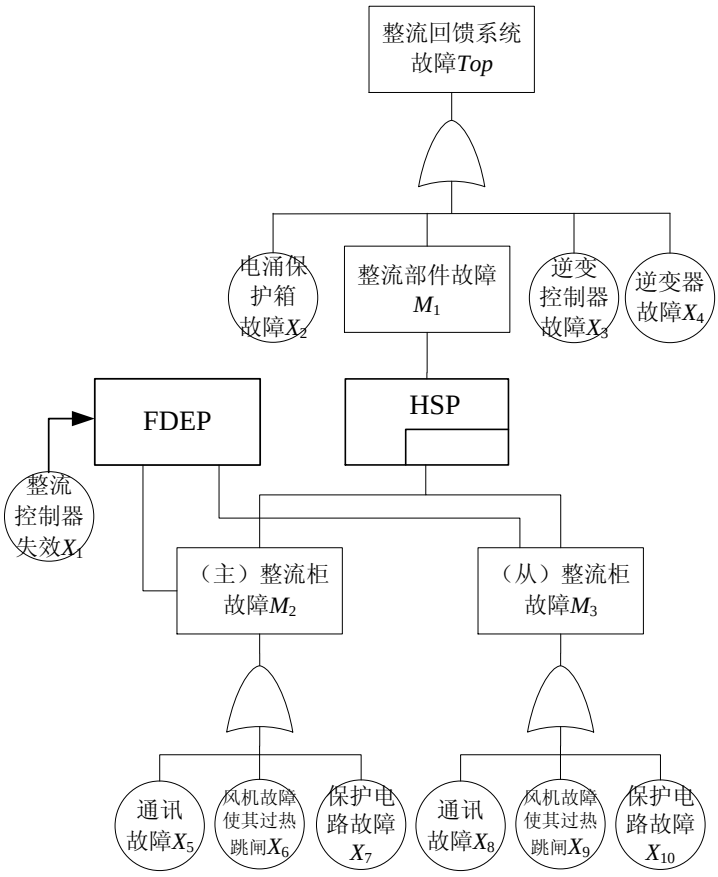


图 4-12 整流回馈系统动态故障树

4.5.2 某大型矿用挖掘机整流回馈系统贝叶斯网络模型

上述故障树模型包含或门、功能相关门和热备件门。按照模型映射方法，把图 4-12 所示动态故障树模型转化为对应的贝叶斯网络模型，如图 4-13 所示。

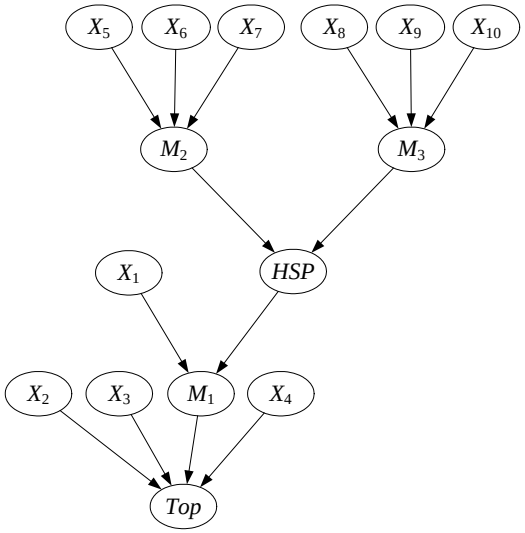


图 4-13 整流回馈系统贝叶斯网络模型

4.5.3 整流回馈系统贝叶斯网络可靠性分析

结合某公司 WK 系列大型矿用挖掘机的故障数据、《机械设计手册》、《电子设备可靠性预计手册》以及相关可靠性文献中的元器件通用失效率数据，对故障树模型中的底事件进行初步的概率估计。考虑到系统失效过程中存在的各种不确定性因素对系统可靠性的影响，本节采用三角模糊数描述故障树模型中底事件失效率的模糊不确定性，并分别以 $\tilde{\lambda}_i(i=1,\cdots,10)$ 表示各个底事件 $X_i(i=1,\cdots,10)$ 的模糊失效率。上述故障树模型中各个基本事件的信息如表 4-2 所示。

表 4-2 实例系统基本事件代码及失效率（$10^{-6}h^{-1}$）

事件代码	模糊失效率	事件代码	模糊失效率
X_1	[29.75,35.00,40.25]	X_6	[153.00,180.00,207.00]
X_2	[42.50,50.00,57.50]	X_7	[226.10,266.00,305.90]
X_3	[63.75,75.00,86.25]	X_8	[199.75,235.00,270.25]
X_4	[161.50,190.00,218.50]	X_9	[153.00,180.00,207.00]
X_5	[199.75,235.00,270.25]	X_{10}	[226.10,266.00,305.90]

同样按照层次法的思想逐层求解上述 BN 模型。

第一步：求解底层输出事件 M_2 及 M_3 的分布。

分别以 $\tilde{f}_{X_i}(x_i)(i=1,\cdots,10)$ 及 $\tilde{F}_{X_i}(x_i)(i=1,\cdots,10)$ 表示各个底事件发生的模糊边缘密度函数及模糊边缘分布函数。节点 M_2 为或门输出节点，并具有三个输入节点。按照或门输出节点的分布公式得该节点的模糊边缘概率密度函数为：

$$\tilde{f}_{M_2}(m_2)=(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)m_2} \tag{4-53}$$

节点 M_3 也为具有三个输入事件的或门输出节点，同时也是热备件门的备件节点。由式（4-33）得其模糊边缘概率密度函数为：

$$\tilde{f}_{M_3}(m_3)=(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})m_3} \tag{4-54}$$

第二步：推导节点 HSP 的分布。

热备件的条件分布考虑在了备件 M_3 中，因此其输出分布为与门的分布。由式（4-24）得节点 HSP（记为 H）的分布为：

$$\tilde{F}_H(h)=(1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)h})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})h}) \tag{4-55}$$

第三步：求解节点 M_1 的分布。

该节点为功能相关门对应的输出节点，其输入节点为 X_1 与 HSP。因此节点

M_1 的分布为：

$$\begin{aligned}\tilde{F}_{M_1}(m_1)=&(1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)m_1})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})m_1})+(1-e^{-\tilde{\lambda}_1 m_1})\\&-(1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)m_1})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})m_1})(1-e^{-\tilde{\lambda}_1 m_1})\end{aligned} \tag{4-56}$$

第四步：求解叶节点 TOP（记为 T）的分布。

该节点为或门节点，按照或门的分布公式得其分布为：

$$\begin{aligned}\tilde{F}_T(t)=&(1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)t})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})t})+(1-e^{-\tilde{\lambda}_1 t})\\&-(1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)t})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})t})(1-e^{-\tilde{\lambda}_1 t})\\&+(1-e^{-(\tilde{\lambda}_2+\tilde{\lambda}_3+\tilde{\lambda}_4)t})-((1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)t})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})t})+(1-e^{-\tilde{\lambda}_1 t})\\&-(1-e^{-(\tilde{\lambda}_5+\tilde{\lambda}_6+\tilde{\lambda}_7)t})(1-e^{-(\tilde{\lambda}_8+\tilde{\lambda}_9+\tilde{\lambda}_{10})t})(1-e^{-\tilde{\lambda}_1 t}))(1-e^{-(\tilde{\lambda}_2+\tilde{\lambda}_3+\tilde{\lambda}_4)t})\end{aligned} \tag{4-57}$$

求解上述模糊失效概率函数，即可得到故障树对应的系统在给定时刻 t 时的模糊失效概率，也可以求解系统的模糊可靠度随时间的变化关系曲线。

图 4-14 为系统在 t=10000h 时的模糊失效概率的隶属函数。

图 4-15 为系统在隶属度 $\alpha=1$ 及 $\alpha=0$ 下，任务时间 t 在 0~1000 h 以内的模糊可靠度曲线。

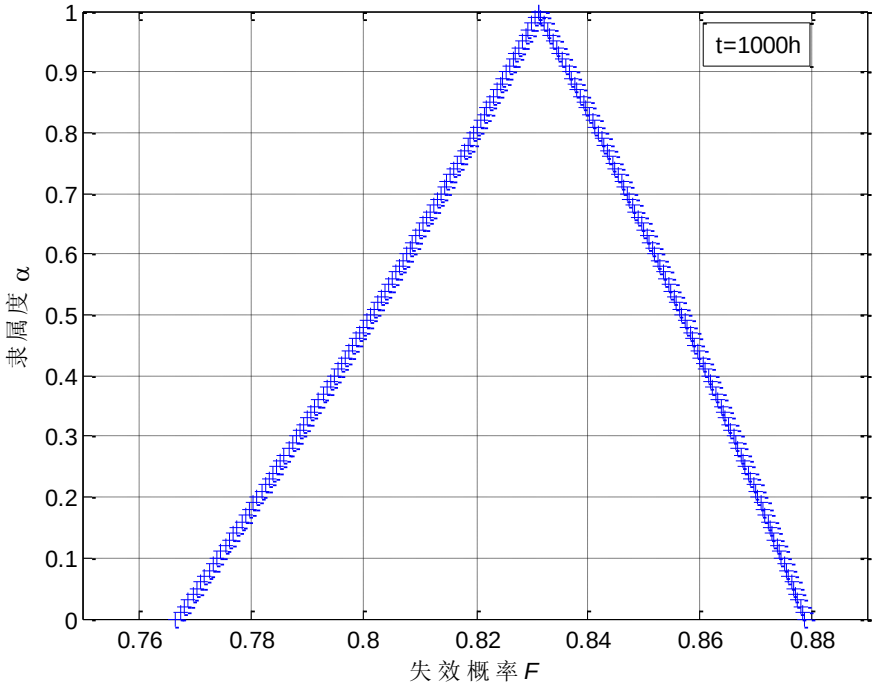


图 4-14 t=1000h 的模糊失效概率

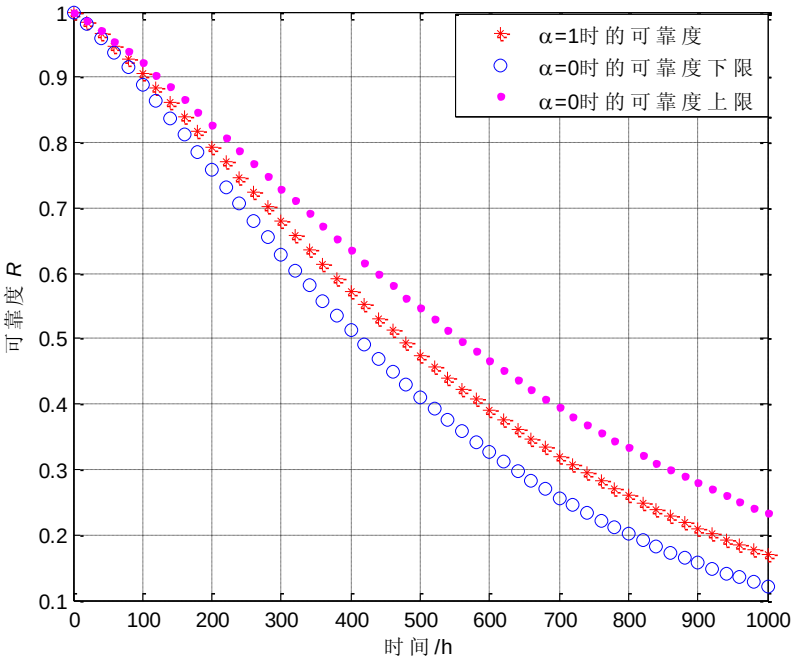


图 4-15 模糊可靠度曲线

4.6 本章小结

本章研究了考虑模糊不确定性下的基于连续时间贝叶斯网络的系统可靠性建模与分析方法。当系统中零部件失效之间具有顺序相关及功能相关等动态失效特性时，基于连续时间贝叶斯网络的可靠性建模与分析方法能准确地建立系统的贝叶斯网络模型，并进行可靠性分析和计算。本章考虑系统及零部件失效行为和数据的模糊不确定性，用三角模糊数描述其失效率值，并用模糊失效率构造零部件的模糊边缘失效密度函数。通过采用单位阶跃函数和冲激函数联合构造了贝叶斯网络中非根节点失效事件的模糊条件概率密度函数和分布函数。在此基础上，推导了在模糊失效率下几种典型的故障树逻辑门输出事件发生的模糊边缘失效密度函数和模糊失效分布函数的表达式。算例结果表明了该方法的可行性。最后，通过对大型矿用挖掘机电气系统整流回馈子系统的建模与分析阐述了该方法在实际工程系统中的应用。

第五章 考虑共因失效的动态故障树分析

现代工程系统正朝着大型化、复杂化方向发展，其应用环境也呈现出动态性、极端性等特征，系统的失效过程也逐渐呈现出零部件失效相关的特征，使得共因失效成为了系统失效过程中的一种普遍现象。在系统可靠性分析中忽略系统部件失效之间的相关性将导致分析结果偏差过大甚至得出错误的结果。本章针对共因失效的问题，介绍常用的 3 种共因失效模型和 2 种共因失效的建模方法。利用显式建模方法对甬温线动车组追尾事故进行故障树建模，并用平方根模型对其发生概率进行计算。建立考虑共因失效（Common Cause Failure, CCF）的基于离散时间贝叶斯网络的动态故障树分析方法，通过算例验证该方法的有效性，同时采用对比分析的方法进一步说明考虑共因失效与否对系统可靠性分析结果的影响。

5.1 引言

随着现代工程系统的日趋复杂和冗余度的增加，部件的独立失效对系统失效的贡献越来越小，而由于多个部件相关失效而引起的系统安全事故呈增长趋势。事实上，“相关”失效是系统失效的普遍特征。忽略系统各底事件发生的相关性，在各底事件相互独立的假设条件下进行故障树定量计算，往往会导致过大的偏差甚至得出错误的结论。

近几十年来，共因失效已成为可靠性分析中的一个重要问题，特别是在复杂系统的可靠性分析中，它往往是造成硬件随机故障的主要因素。如果一个系统中有两个或多个事件可能会由于相同的原因而失效，则称这种系统为共因失效系统。自二十世纪 70 年代以来，有关专家学者提出了许多描述共因失效的方法，如β-因子模型[102]、基本参数模型（BP）[103]、混合参数模型（MGL）[104]、α-因子模型[105]以及平方根模型[106]等。时至今日，共因失效问题仍然受到许多学者的广泛关注，并且目前依然没有找到一种适合处理共因失效问题的通用方法。在实际应用方面，这些模型已被用于处理控制系统、复杂计算机系统、运输系统等实际系统的故障分析和可靠性分析中[107-114]。

对于列车追尾事故，Das 等[115]运用遗传规划建模方法并考虑碰撞次数与伤害严重度等因素进行了列车安全性分析方法研究，该方法提供了一种在不限制数据分布类型时的建模方法。Milho 等[116]提出并验证了一种基于多体动力学的用于列车碰撞场景仿真和能量吸收模拟的程序。在该仿真模拟程序中，用一组刚体来描述车辆的运动部件，其相对运动由运动接头约束来限制。近年来，美国联邦铁路

局一直致力于客运铁路设备的防撞性研究[114,115]。客运铁路设备的防撞性研究工作主要集中在提高结构防撞性以及开发室内乘员保护策略两个方面，其研究成果已被用于制定铁路采购规程[119,120]及工业标准中[121,122]。Tyrell 等[123]进行了碰撞能量管理的全尺度列车冲击试验，并计算出了客运铁路采用防撞性保护设计策略后性能提高的程度。虽然有很多学者在结构防撞性和客运铁路防撞性的研究中做了大量的理论研究工作，但是要对实际铁路车辆的安全性和可靠性进行有效的分析和评估还需要进一步的探索研究。对列车的一些实际事故进行可靠性分析研究，既能验证上述理论方法的有效性又能促进其在实际工程中的应用。

在共因失效研究方面，Levitin 等[111]将多态系统可靠性分析中的 UGF 方法应用到考虑共因失效的系统可靠性评估中。Vaurio 等[124,125]针对串并联系统共因失效问题，提出一种量化共因事件观察、记录以及解释的不确定性方法，并通过文献[126]-[128]中的补充工作对此方法做了进一步深化。Kvam 和 Martz[129]为了预测未来电厂共因失效率，通过收集多种失效原因“混杂”的系统故障数据（包括设计上的缺陷、机器维修错误和其它类型共因失效），运用 Bayes 方法对系统可靠性进行了估计并求出了相应的共因失效概率。Mosleh 等[130]对共因失效进行了全面的研究，建立了一个共因失效识别、建模和量化的详细框架。该框架便于分析过程中逐步执行分析流程，并且可根据实际情况在每个任务中灵活选择可接受和替代的模型及相应的分析技术。为了分析高阶冗余系统中共因失效占主导的安全风险状况，Marseguerra 等[131]研究描述了环境对系统可靠性的影响以及在冗余系统设计中需要考虑的有关环境的若干问题。

本章结合故障树分析方法与共因失效分析模型来开展列车追尾事故的失效分析，尝试提供一种铁路交通工具安全性与可靠性分析的方法。综述目前共因失效模型的研究现状，介绍两类共因失效建模方法，并以列车追尾事故为例研究考虑共因失效的故障树分析方法。其次，提出一种考虑 CCF 下的基于贝叶斯网络的动态故障树分析方法，通过算例验证该方法的正确性和有效性。

5.2 共因失效参数模型简介

自二十世纪 70 年代以来，各界学者先后提出许多描述共因失效的模型与方法[132-135]，如β-因子模型、基本参数模型（BP）、MGL 模型、α-因子模型以及平方根模型等。下面以 3 部件并联系统为例，解释说明各种模型的使用方法。

5.2.1 基本参数模型（Basic Parameter Model）

假设系统是由 A，B，C 三个部件组成。部件 A 失效的概率包括部件 A 的独立

失效概率以及与 A 相关的共因部件 B 或 C 或 BC 同时发生失效时的多重失效概率。用 A_l、B_l、C_l 分别表示三个部件独立失效的概率，则有：

$$\begin{aligned} P(A) &= P(A_l) + P(AB) + P(AC) + P(ABC) \\ P(B) &= P(B_l) + P(AB) + P(BC) + P(ABC) \\ P(C) &= P(C_l) + P(AC) + P(BC) + P(ABC) \end{aligned} \tag{5-1}$$

那么三个部件组成的共因失效部件组中任意一个部件失效发生的概率（包括单独失效和共因失效）为：

$$Q_l = \sum_{k=1}^{3} C_{3-1}^{k-1} Q_k \tag{5-2}$$

式中，Q_k 表示任意 k 个部件同时失效的概率。

对于 m 个部件组成的系统，部件总的失效概率可以表示为[136]：

$$Q_l = \sum_{k=1}^{m} C_{m-1}^{k-1} Q_k \tag{5-3}$$

理想情况下，Q_k 的值能够通过数据计算出来，但通常情况下不能得到完整的数据，因此提出了一些其它的模型，这些模型利用更多的假设来解决不完备的数据问题。

5.2.2 β因子模型（Beta Factor Model）

β因子模型是目前最常用的共因失效模型之一，它最初由 Fleming 提出[102]。β因子模型最早是基于两单元并联系统提出来的，它假设所有失效中有一定百分比为共因失效，模型中用 β因子来量化共因失效对系统产生的影响。使用该模型进行计算时，只考虑两种失效情况：一种是单元本身独立的失效，一种是所有单元因为共同的原因同时失效。因此单元的失效概率由两部分组成，即单元的本身失效概率和共因失效概率，即

$$Q = Q_1 + Q_2$$

式中，Q_1 为单元本身的失效概率，Q_2 为共因失效概率，Q 为系统失效概率。

以符号 $\lambda_1,\lambda_2,\lambda$ 分别表示单元本身失效、共因失效以及整个系统失效的失效率。共因因子 β 的计算表达式为[136,137]：

$$\beta = \frac{Q_2}{Q} = \frac{Q_2}{Q_1 + Q_2} = \frac{1 - e^{-\lambda_2 \cdot t}}{1 - e^{-\lambda \cdot t}} = \frac{1 - e^{-\lambda_2 \cdot t}}{(1 - e^{-\lambda_1 \cdot t}) + (1 - e^{-\lambda_2 \cdot t})} \tag{5-4}$$

共因因子 β 的值可以通过计算在给定失效的条件下共因失效的条件概率得

到，如式（5-5）所示：

$$\beta = P\left(\text{CCF}\middle|\text{Failure}\right) \tag{5-5}$$

5.2.3 平方根模型（Square-Root Model）

平方根模型是一个简单的用来评估共因失效对系统影响的模型[106]。假设系统由 A 和 B 两个部件并联而成，则系统失效的概率为 $P(A_F \cap B_F)$，A_F 和 B_F 分别表示部件 A 和 B 失效，那么系统可靠性可以用下式表示：

$$P\left(A_F \cap B_F\right) \le P\left(A_F\right),\ P\left(A_F \cap B_F\right) \le P\left(B_F\right) \tag{5-6}$$

式（5-6）也可以表示为：

$$P(A_F \cap B_F) \le \min\ \{P(A_F), P(B_F)\}$$

A 和 B 正相关时，有：

$$P\left(A_F \cap B_F\right) = P\left(A_F\middle|B_F\right)P\left(B_F\right) \ge P\left(A_F\right)P\left(B_F\right) \tag{5-7}$$

令 $a = P(A_F)P(B_F)$，$b = \min\ \{P(A_F), P(B_F)\}$，平方根 CCF 模型可以用几何平均数 a 和 b 表示为：

$$P\left(A_F \cap B_F\right) = \sqrt{ab} \tag{5-8}$$

类似地，对于由 n 个单元组成的并联结构系统，不可靠度的上下限可以由下式得到：

$$a = \prod_{i=1}^{n} P\left(A_i\right),\ b = \min\left\{P\left(A_1\right), P\left(A_2\right), \cdots, P\left(A_n\right)\right\} \tag{5-9}$$

5.3 共因失效及其可靠性建模分析方法

系统中单元失效相关的情况主要有两种：共因失效和从属失效。造成系统故障的原因可能来自系统外部和系统内部。当造成系统若干个单元同时故障的各种冲击来自系统外部时，可认为各种故障冲击作用彼此相互独立，这也是大多数共因失效分析模型的基本假设[106]。存在共因失效时，系统的故障分析方法主要有两种：隐式方法和显式方法[138]。隐式分析方法首先不考虑共因失效，在独立失效条件下对系统各部分展开分析，再通过适当的方法将共因失效的影响引入分析模型中，最终得到考虑共因失效时系统的顶事件发生概率。显式方法在对系统各个部分进行分析时即考虑共因失效的影响，并通过相应的建模分析得到系统的顶事件发生概率。

5.3.1 存在共因失效时系统可靠性分析的基本假设

设 n 个单元组成的系统中，在$[0,t)$区间内，令Y_i^i表示单元 i 单独故障不发生的事件，$Y_{a_i b_i c_i d_i \cdots}^i$表示包含单元 i 的若干个单元同时故障不发生的事件。上述事件符号中$i=1,\cdots,n$，$a_i=1,2,\cdots,n$，$b_i=1,2,\cdots,n$，…，上标 i 表示故障单元为 i，下标$i,a_i,b_i,\cdots$表示共因部件组中的所有故障单元，单元单独故障时下标与上标相同。当两个或两个以上单元同时不发生故障时，如果下标组合相同，则表示相同事件。

进行系统共因失效分析时，作如下假设：

（1）导致单元故障的各种冲击是彼此相互独立的泊松过程。系统故障服从指数分布，单元单独故障的故障率为$\lambda_i^i,(i=1,2,\cdots,n)$，单独故障时与上标相同即都为$i$。

（2）采用相似模型[106]，如图 5-1 所示。相似模型是针对故障强度难以确定的情况下假设 n 个单元组成的单元群中，相同数目的单元同时故障的故障强度相同。由于相同分布单元承受相似共因失效冲击，则相同数目单元同时故障的故障率相同，也就是指定 j 个单元同时故障的故障率都为$\lambda_j,(j=1,2,\cdots,n)$。

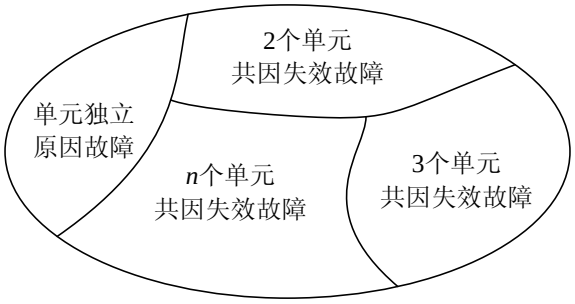


图 5-1 任意单元故障组成因素

5.3.2 存在共因失效时系统可靠性的隐式建模方法

考虑共因失效的系统可靠性隐式建模方法首先推导出不考虑共因失效时系统可靠度表达式，再利用指定 m 个单元同时正常工作的概率表达式替代该系统可靠度表达式中对应单元可靠度的 m 次方，将共因失效的影响引入其中，得到考虑共因失效时系统可靠度的表达式。

下面以三单元并联系统为例，假设系统单元服从相同分布、承受相似共因失效冲击，采用隐式替代方法，分析此系统的可靠性[106]。该系统的故障树模型如图 5-2 所示，其中 T 对应一个由 A、B、C 三个单元组成的并联系统，A_1、B_1、C_1 表示单元本身的失效，CCF 表示共因失效部分。

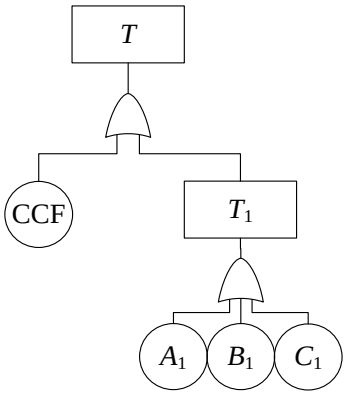


图 5-2 共因失效的隐式建模

根据典型系统可靠性分析知识，n 单元并联系统的可靠度为：

$$\begin{aligned} R_s(t) &= 1-\left[1-R(t)\right]^n \\ &= 1-\sum_{m=0}^{n}(-1)^m C_n^m R^m(t) \\ &= \sum_{m=1}^{n}(-1)^{m+1} C_n^m R^m(t) \end{aligned} \tag{5-10}$$

N 个单元组成的系统中，指定的 m 个单元同时正常概率为 $P_n^m(t)$，则

$$\begin{aligned} P_n^m(t) &= P_n^1(t)P_{n-1}^1(t)\cdots P_{n-m+1}^1(t) = \prod_{k=n-m+1}^{n} P_k^1(t) \\ &= \prod_{k=n-m+1}^{n} e^{-\left(\sum_{i=1}^{k} C_{k-1}^{i-1}\lambda_i\right)t} = e^{-\sum_{k=n-m+1}^{n}\left(\sum_{i=1}^{k} C_{k-1}^{i-1}\lambda_i\right)t} \end{aligned} \tag{5-11}$$

式中，$n \geq 2, m \geq 1$。

令 $R^m(t) = P_n^m(t)$，代入式（5-10），得考虑共因失效时并联系统可靠度完整表达式为：

$$\begin{aligned} R_s(t) &= \sum_{m=1}^{n}(-1)^{m+1} C_n^m R^m(t) \\ &= \sum_{m=1}^{n}(-1)^{m+1} C_n^m e^{-\sum_{k=n-m+1}^{n}\left(\sum_{i=1}^{k} C_{k-1}^{i-1}\lambda_i\right)t} \end{aligned} \tag{5-12}$$

单元同分布时，三个单元组成的并联系统的可靠度为：

$$R_s(t) = 3R(t) - 3R^2(t) + R^3(t) \tag{5-13}$$

令 $R^m(t) = P_3^m(t)$，得：

$$R_s(t) = 3P_3^1(t) - 3P_3^2(t) + P_3^3(t) \tag{5-14}$$

由式（5-11）得：

$$\begin{aligned} P_3^1(t) &= e^{-\left(\sum_{i=1}^{3} C_{3-1}^{i-1}\lambda_i\right)t} \\ &= e^{-\left(C_2^0\lambda_1+C_2^1\lambda_2+C_2^2\lambda_3\right)t} \\ &= e^{-(\lambda_1+2\lambda_2+\lambda_3)t} \end{aligned} \tag{5-15}$$

$$\begin{aligned} P_3^2(t) &= e^{-\left[\left(\sum_{i=1}^{3} C_{3-1}^{i-1}\lambda_i\right)+\left(\sum_{i=1}^{2} C_{3-2}^{i-1}\lambda_i\right)\right]t} \\ &= e^{-\left[\left(C_2^0\lambda_1+C_2^1\lambda_2+C_2^2\lambda_3\right)+\left(C_1^0\lambda_1+C_1^1\lambda_2\right)\right]t} \\ &= e^{-\left[(\lambda_1+2\lambda_2+\lambda_3)+(\lambda_1+\lambda_2)\right]t} \\ &= e^{-(2\lambda_1+3\lambda_2+\lambda_3)t} \end{aligned} \tag{5-16}$$

$$\begin{aligned} P_3^3(t) &= e^{-\left[\left(\sum_{i=1}^{3} C_{3-1}^{i-1}\lambda_i\right)+\left(\sum_{i=1}^{2} C_{3-2}^{i-1}\lambda_i\right)+\left(\sum_{i=1}^{1} C_{3-3}^{i-1}\lambda_i\right)\right]t} \\ &= e^{-\left[\left(C_2^0\lambda_1+C_2^1\lambda_2+C_2^2\lambda_3\right)+\left(C_1^0\lambda_1+C_1^1\lambda_2\right)+C_0^0\lambda_1\right]t} \\ &= e^{-\left[(\lambda_1+2\lambda_2+\lambda_3)+(\lambda_1+\lambda_2)+\lambda_1\right]t} \\ &= e^{-(3\lambda_1+3\lambda_2+\lambda_3)t} \end{aligned} \tag{5-17}$$

考虑共因失效时，三个单元组成的并联系统的可靠度为：

$$R_s(t) = 3e^{-(\lambda_1+2\lambda_2+\lambda_3)t} - 3e^{-(2\lambda_1+3\lambda_2+\lambda_3)t} + e^{-(3\lambda_1+3\lambda_2+\lambda_3)t} \tag{5-18}$$

5.3.3 存在共因失效时系统可靠性的显式分析方法

系统可靠性的显式分析方法可用于单元分布不相同并且承受多种共因失效冲击的情况。例如由三个单元组成的并联系统，每个单元服从相同的分布，承受相似共因失效冲击。对于并联系统，只要一个单元正常系统就正常[106]。令 X_i（i=1,2,3）表示包含单元 i 的所有失效事件都不发生的事件，$\overline{Y_i^i}$（i=1,2,3）表示单元 i 单独故障的事件，$\overline{Y_{i,j\ldots}^i}$（$i,j$=1,2,3）表示包含单元 i 的若干个单元同时故障的事件。通过显式建模方式得系统的故障树模型如图 5-3 所示。

系统正常事件为：

$$S = X_1 + X_2 + X_3$$

这里的 X_i 之间是相交的，由全概率公式可得：

$$P(X_1+X_2+X_3) = \sum_{i=1}^{3} P(X_i) - \sum_{\substack{i,j=1 \\ i\neq j}}^{3} P(X_iX_j) + \sum_{\substack{i,j,k=1 \\ i\neq j\neq k}}^{3} P(X_iX_jX_k) \tag{5-19}$$

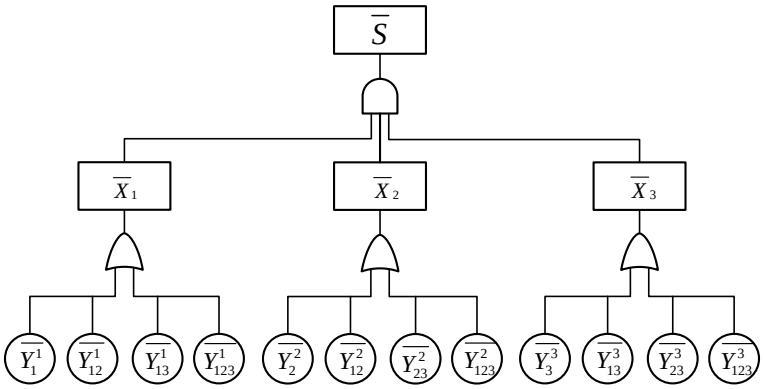


图 5-3 共因失效的显式建模

由于每个单元服从相同分布，承受类似共因失效冲击，因此，各个 $P\left(X_i\right)$，$P\left(X_iX_j\right)$，$P\left(X_iX_jX_k\right)$ 分别相同。

式（5-19）可以简化为：

$$\begin{aligned} P\left(X_1+X_2+X_3\right)&=C_3^1P\left(X_1\right)-C_3^2P\left(X_1X_2\right)+C_3^3P\left(X_1X_2X_3\right)\\ &=3P\left(X_1\right)\text{-}3P\left(X_1X_2\right)+P\left(X_1X_2X_3\right)\end{aligned} \tag{5-20}$$

由 $X_1=Y_1^1Y_{12}^1Y_{13}^1Y_{123}^1$ 可得：

$$\begin{aligned} P\left(X_1\right)&=P\left(Y_1^1Y_{12}^1Y_{13}^1Y_{123}^1\right)=P\left(Y_1^1\right)\underbrace{P\left(Y_{12}^1\right)}_{C_{3\text{-}1}^1}\underbrace{P\left(Y_{123}^1\right)}_{C_{3\text{-}1}^2}\\ &=\left(e^{-\lambda_1t}\right)^1\left(e^{-\lambda_2t}\right)^{C_{3\text{-}1}^1}\left(e^{-\lambda_3t}\right)^{C_{3\text{-}1}^2}=e^{-\left(\sum_{i=1}^{3}C_{3-1}^{i-1}\lambda_i\right)t}\\ &=e^{-(\lambda_1+2\lambda_2+\lambda_3)t}\end{aligned} \tag{5-21}$$

由 $X_1=Y_1^1Y_{12}^1Y_{13}^1Y_{123}^1$ 和 $X_2=Y_2^2Y_{12}^2Y_{23}^2Y_{123}^2$ 可得：

$$\begin{aligned} P\left(X_1X_2\right)&=P\left[\left(Y_1^1Y_{12}^1Y_{13}^1Y_{123}^1\right)\left(Y_2^2Y_{12}^2Y_{23}^2Y_{123}^2\right)\right]\\ &=P\left(Y_1^1\right)P\left(Y_2^2\right)\underbrace{P\left(Y_{12}^1Y_{12}^2\right)}_{C_{3-1}^1+C_{3-2}^1}\underbrace{P\left(Y_{123}^1Y_{123}^2\right)}_{C_{3-1}^2+C_{3-2}^2}\\ &=\left(e^{-\lambda_1t}\right)^2\left(e^{-\lambda_2t}\right)^{C_{3\text{-}1}^1+C_{3-2}^1}\left(e^{-\lambda_3t}\right)^{C_{3\text{-}1}^2+C_{3-2}^2}\\ &=e^{-\left(\sum_{i=1}^{3-1}\left(C_{3-1}^{i-1}+C_{3-2}^{i-1}\right)\lambda_i+C_{3-1}^{3-1}\lambda_3\right)t}\\ &=e^{-(2\lambda_1+3\lambda_2+\lambda_3)t}\end{aligned} \tag{5-22}$$

三个单元同时不发生故障时有：

$$\begin{aligned}P\left(X_1X_2X_3\right)&=P\left[\left(Y_1^1Y_{12}^1Y_{13}^1Y_{123}^1\right)\left(Y_2^2Y_{12}^2Y_{23}^2Y_{123}^2\right)\left(Y_3^3Y_{13}^3Y_{23}^3Y_{123}^3\right)\right]\\&=P\left(Y_1^1\right)P\left(Y_2^2\right)P\left(Y_3^3\right)\underbrace{P\left(Y_{12}^1Y_{12}^2Y_{13}^3\right)}_{C_{3-1}^1+C_{3-2}^1+C_{3-3}^1}\underbrace{P\left(Y_{123}^1Y_{123}^2Y_{123}^3\right)}_{C_{3-1}^2+C_{3-2}^2+C_{3-3}^2}\\&=\left(e^{-\lambda_1t}\right)^3\left(e^{-\lambda_2t}\right)^{C_{3-1}^1+C_{3-2}^1+C_{3-3}^1}\left(e^{-\lambda_3t}\right)^{C_{3-1}^2+C_{3-2}^2+C_{3-3}^2}\\&=e^{-\left(\sum_{i=1}^{3-2}\left(C_{3-1}^{i-1}+C_{3-2}^{i-1}+C_{3-3}^{i-1}\right)\lambda_i+\left(C_{3-1}^{3-2}+C_{3-1}^{3-1}\right)\lambda_2+C_{3-1}^{3-1}\lambda_3\right)t}\\&=e^{-(3\lambda_1+3\lambda_2+\lambda_3)t}\end{aligned}\tag{5-23}$$

整理后可得此并联系统的可靠度为：

$$\begin{aligned}R_s\left(t\right)&=3P\left(X_1\right)-3P\left(X_1X_2\right)+P\left(X_1X_2X_3\right)\\&=3e^{-(\lambda_1+2\lambda_2+\lambda_3)t}-3e^{-(2\lambda_1+3\lambda_2+\lambda_3)t}+e^{-(3\lambda_1+3\lambda_2+\lambda_3)t}\\&=\sum_{j=1}^{3}c_je^{-r_jt}\end{aligned}\tag{5-24}$$

式中，$c_j=\left(-1\right)^{j+1}C_3^j$，$r_j=\sum_{p=3-j+1}^{3}\sum_{i=1}^{p}C_{p-1}^{i-1}\lambda_i$，$1\le j\le3$。

5.4 实例分析：甬温线动车组追尾事故分析

5.4.1 甬温线动车组追尾事故的故障树建模

2011 年 7 月 23 日 20 时 30 分 05 秒，甬温线浙江省温州市境内，由北京南站开往福州站的 D301 次列车与杭州站开往福州南站的 D3115 次列车发生追尾事故，造成 40 人死亡、172 人受伤，中断行车 32 小时 35 分，直接经济损失 19371.65 万元。

本节对文献[139]中针对上述 7·23 甬温线特别重大铁路交通事故所建立的动车组追尾事故的故障树模型进行共因失效分析。

该故障树模型针对单向只有一条轨道的情形，并假设应用了信号灯控制系统、车辆距离控制系统、车辆状态通信与控制系统等列车防撞系统以及调度中心险情告警系统[139]。

动车组追尾事故的故障树模型如图 5-4~图 5-6 所示，各个事件的意义及代码见表 5-1 所示。

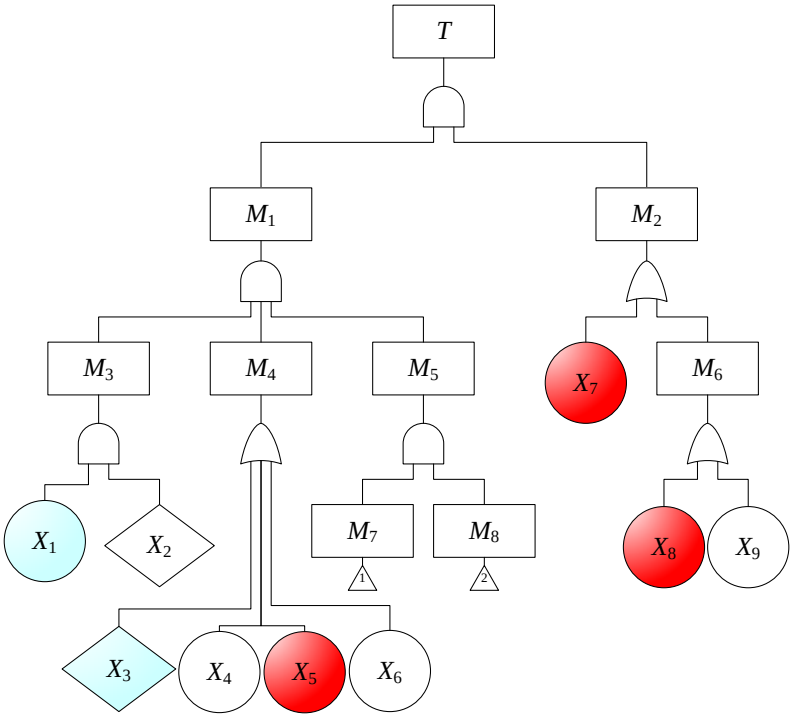


图 5-4 列车追尾事故的故障树

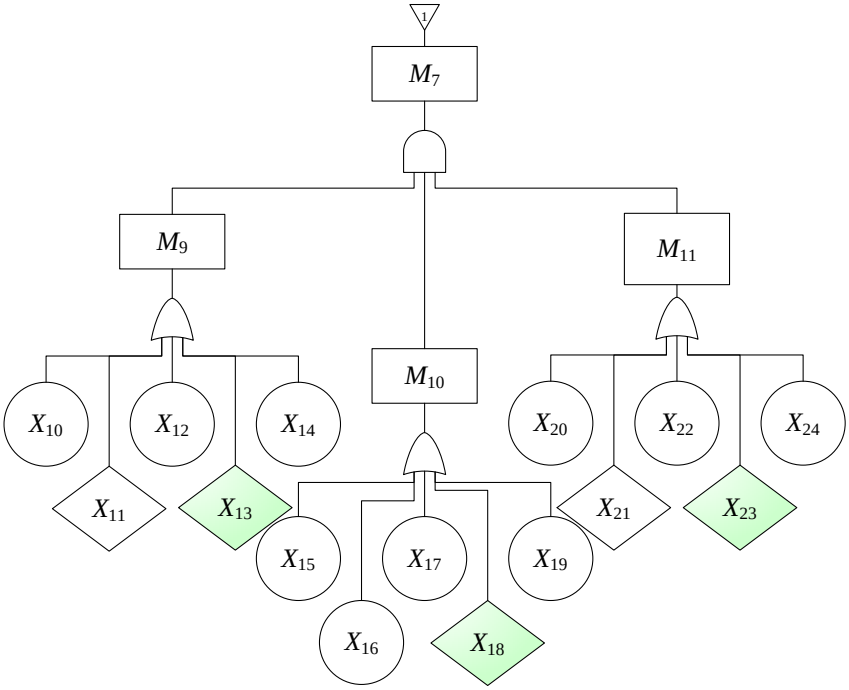


图 5-5 “防撞系统失效”事件的故障树

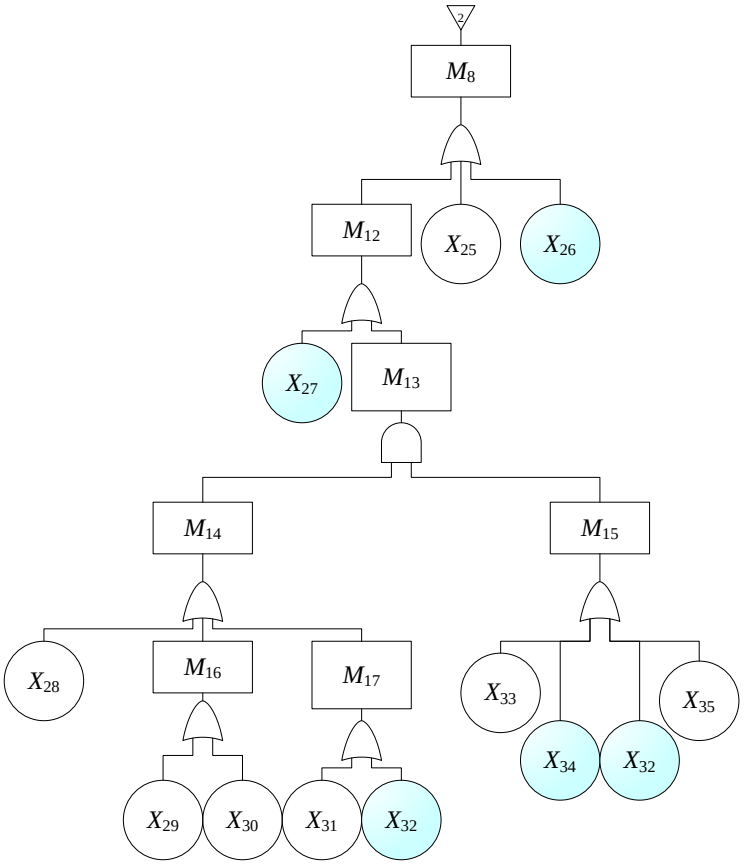


图 5-6 “人工介入措施失败”事件的故障树

5.4.2 定性分析

由图 5-4~图 5-6 可以得到甬温线动车组追尾事故故障树的结构函数如下：

$$\begin{aligned}\Phi(X)=&X_1\cdot X_2\cdot(X_3+X_4+X_5+X_6)\cdot(X_{10}+X_{11}+X_{12}+X_{13}+X_{14})\cdot\\&(X_{15}+X_{16}+X_{17}+X_{18}+X_{19})\cdot(X_{20}+X_{21}+X_{22}+X_{23}+X_{24})\cdot\\&((X_{28}+X_{29}+X_{30}+X_{31})\cdot(X_{33}+X_{34}+X_{35})+X_{32}+X_{25}+X_{26}+X_{27})\cdot\\&(X_7+X_8+X_9)\end{aligned}\tag{5-25}$$

根据结构函数可以看出，列车追尾事故共有：

$$1\times1\times4\times5\times5\times5\times\ (4\times3+4)\ \times3=24000$$

种发生模式，若不对防撞系统失效进行细分，则事故模式也有 192 种。

必须指出，从故障树分析得到的故障模式的数量与分析的详细程度有直接关系。

表 5-1 事件代号及名称

事件代号	事件名称	事件代号	事件名称
T	列车追尾事故	X_{10}	车辆位置数据采集错误
M_1	存在追尾条件	X_{11}	人为原因造成错误信号
M_2	司机未能通过制动阻止	X_{12}	数据处理逻辑错误
M_3	前后车在同一轨道上	X_{13}	环境原因造成错误信号
M_4	后车速度大于前车速度	X_{14}	信号输出出错
M_5	追赶区间内防撞系统失效	X_{15}	获取目标位置出错
M_6	司机制动失效	X_{16}	车辆控制指令未得到正确执行
M_7	防撞技术系统失效	X_{17}	距离计算错误
M_8	人工介入措施失效	X_{18}	环境原因造成距离控制错误
M_9	信号灯系统失效	X_{19}	后车距离决策与控制失效
M_{10}	车辆距离控制系统失效	X_{20}	前车状态信号遗失或有错
M_{11}	车辆状态通信与控制系统失效	X_{21}	人工决策与控制失效
M_{12}	调度员未注意到险情	X_{22}	后车未准确接收前车信号
M_{13}	调度员正常执勤未注意到险情	X_{23}	环境原因造成车辆状态通信与控制错误
M_{14}	险情告警技术措施失效	X_{24}	后车状态决策与控制失效
M_{15}	人工监视未发现险情	X_{25}	调度员来不及处理险情
M_{16}	险情告警系统未发现险情	X_{26}	调度员险情处理不当
M_{17}	险情告警系统告警未引起注意	X_{27}	调度员脱岗
X_1	前后车被派上同一铁路区间	X_{28}	险情告警系统被关闭
X_2	区间内同方向只有一条轨道	X_{29}	险情告警系统未获得准确数据
X_3	调度命令错误	X_{30}	险情识别软件缺陷
X_4	前车停车或慢行	X_{31}	险情告警方式不合理
X_5	司机违反指令	X_{32}	调度员分心
X_6	自动控制系统异常	X_{33}	信息过载、任务太复杂
X_7	司机未注意到险情	X_{34}	经验不足
X_8	目视距离内制动不及	X_{35}	人机界面不好
X_9	制动系统失效		

由结构函数可知，列车追尾事故的事故链较长，每种失效模式至少有八个事件同时发生才能引发事故。如果这些事件均相互独立，事故发生的概率极低。但由于存在多方面的共因失效，事故发生的概率并非那么低。其中，各方面的共因失效用不同的颜色予以标记，如图 5-4 所示。

5.4.3 定量计算

为了便于定量评估及比较分析，我们假设各个底事件的失效概率如表 5-2 所示。

表 5-2 底事件发生概率

编号	底事件名称	发生概率	编号	底事件名称	发生概率
X_{27}	调度员脱岗	0.020	X_{32}	调度员分心	0.020
X_{28}	险情告警系统被关闭	0.001	X_{33}	信息过载、任务太复杂	0.001
X_{29}	险情告警系统未获得准确数据	0.001	X_{34}	经验不足	0.020
X_{30}	险情识别软件缺陷	0.002	X_{35}	人机界面不好	0.001
X_{31}	险情告警方式不合理	0.005			

中间事件 M_{12}“调度员未注意到险情”的结构函数为：

$$\Phi(X)=\left(\left(X_{28}+X_{29}+X_{30}+X_{31}\right)\cdot\left(X_{33}+X_{34}+X_{35}\right)+X_{32}+X_{27}\right) \tag{5-26}$$

若按照各底事件相互独立的假设计算可得“调度员未注意到险情”的发生概率为：

$$P(M_{12})=0.0398 \tag{5-27}$$

通过仔细分析，我们不难发现“调度员分心”与“经验不足”存在共因关系，而“调度员脱岗”与“调度员正常执勤未注意到险情”互斥，“险情告警系统被关闭”、“险情告警系统未发现险情”与“险情告警系统告警未引起注意”两两互斥。因此，M_{12} 子树的结构函数可以表示如下：

$$\begin{aligned}P(M_{12})&=P\left(\left(X_{28}+X_{29}+X_{30}+X_{31}\right)\cdot\left(X_{33}+X_{34}+X_{35}\right)+X_{32}+X_{27}\right)\\&=P\left(\left(X_{28}+X_{29}+X_{30}+X_{31}\right)\cdot\left(X_{33}+X_{34}+X_{35}\right)+X_{32}\right)+P\left(X_{27}\right)\end{aligned} \tag{5-28}$$

令 X_a=X_{28}+X_{29}+X_{30}+X_{31}，X_b= X_{33}+X_{35}，则

$$\begin{aligned} P(X_a) &= P(X_{28}+X_{29}+X_{30}+X_{31}) \\ &= P(X_{28})+P(X_{29}+X_{30})+P(X_{31}) \\ &= 0.001+(1-(1-0.001)(1-0.002))+0.005 \\ &\approx 0.009 \end{aligned} \tag{5-29}$$

$$\begin{aligned} P(X_b) &= P(X_{33}+X_{35}) \\ &= 1-(1-0.001)(1-0.001) \\ &\approx 0.002 \end{aligned} \tag{5-30}$$

根据分析，式（5-28）可进一步简化如下：

$$\begin{aligned} P(M_{12}) &= P(X_aX_b+X_aX_{34}+X_{32})+P(X_{27}) \\ &= P(X_a)P(X_b)+P(X_a)P(X_{34})+P(X_{32})- \\ &\quad P(X_a)P(X_b)P(X_{34})-P(X_a)P(X_b)P(X_{32})- \\ &\quad P(X_a)P(X_{34}X_{32})+P(X_a)P(X_b)P(X_{34}X_{32})+P(X_{27}) \end{aligned} \tag{5-31}$$

根据平方根模型可得：

$$\begin{aligned} P(X_{34}X_{32}) &= \sqrt{ab} = \sqrt{P(X_{34})P(X_{32})\min\{P(X_{34}),P(X_{32})\}} \\ &= \sqrt{0.020\times 0.020\times \min\{0.020,0.020\}} = 0.0028 \end{aligned} \tag{5-32}$$

$$P(M_{12}) = 0.0402 \tag{5-33}$$

与不考虑 CCF 所得到的概率相比较，考虑共因失效的顶事件发生概率相对误差为：

$$\begin{aligned} \eta &= \frac{0.0402-0.0398}{0.0402}\times 100\% \\ &= 1.01\% \end{aligned} \tag{5-34}$$

由计算结果可以看出，对于动车这种可靠性和安全性至关重要的系统来说，若不考虑共因失效的因素得到的可靠性分析结果误差非常大。这说明了共因失效对列车追尾事故的发生具有显著的影响，如果在列车的设计、分析和运行中不考虑这种影响将会误判事故发生的概率，从而造成重大的人员伤亡和经济损失。

5.5 含共因事件的系统动态故障树分析方法

5.5.1 共因失效参数模型选择

一个系统往往承受多种共因失效的影响，如：功能相关失效、物理相关失效、环境相关失效、人因相关失效等。对于组件之间的相互作用引起的物理相关失效以及人因引起的共因失效，通常采用 β 因子模型进行建模分析。由文献[136]可知，

β因子由组件独立失效对系统贡献 Q_{ind} 和共因失效对系统贡献 Q_{com} 两部分决定。设共因失效和系统失效所对应的失效率分别为 λ_{com} 与 λ，根据 5.2.2 节可得：

$$\begin{aligned}\beta &= \frac{Q_{com}}{Q} \\ &= \frac{Q_{com}}{Q_{ind}+Q_{com}} \\ &= \frac{1-e^{-\lambda_{com}\cdot t}}{1-e^{-\lambda\cdot t}} \\ &\approx \frac{\lambda_{com}}{\lambda}\end{aligned} \tag{5-35}$$

β因子的确定方法包括以下几个步骤：

（1）确定组件整体失效率；

（2）分析失效模式，确定共因失效在组件失效中所占比重；

（3）计算与共因失效相关的失效率的百分比（β因子）；

（4）运用 β因子计算组件相关失效率和独立失效率。

通常 β因子的范围为 0~0.25，其中 0 表示没有对应的这种共因失效发生。在实际应用中 β因子的取值往往由专家经验获得。对于硬件失效，β因子一般在 0.1% 到 10%的范围内。组件对各种共因机理的敏感程度决定了 β因子的大小，对共因机理越敏感，β因子越大[136,137]。

5.5.2 两种考虑 CCF 的动态逻辑门显式建模

由 5.3.3 节可知，系统可靠性的显式分析方法可用于单元分布不相同，承受多种共因失效冲击的情况。在此基础上，可得考虑共因失效的功能相关门和冷备件门的动态故障树建模，如图 5-7 与图 5-8 所示。

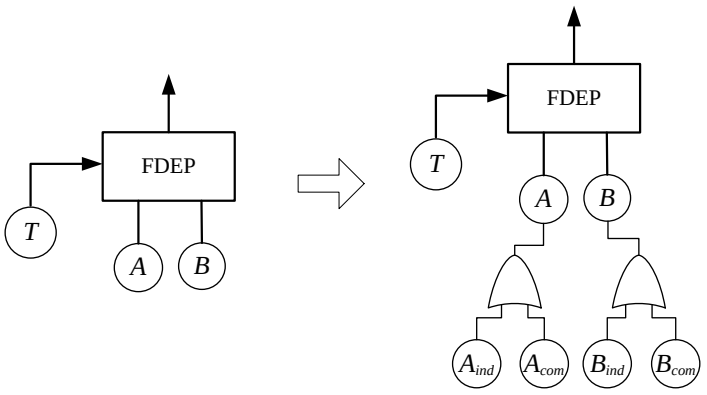


图 5-7 功能相关门共因失效的显式建模

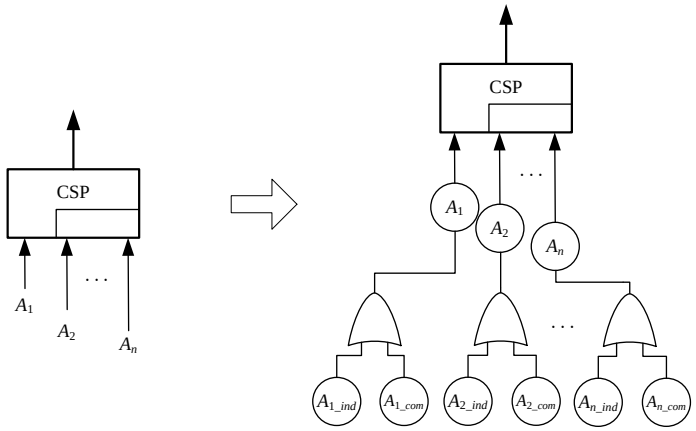


图 5-8 多部件冷备份共因失效的显式建模

5.5.3 包含共因失效的动态逻辑门求解

5.5.3.1 含冷备份的共因失效建模及分析

在系统可靠性设计中，冷备件用来对系统中的关键零部件进行备份，以提高整个系统的可靠性。在零部件失效独立的假设条件下，主件失效之前，相应的备件失效率为零，不会发生失效。考虑环境因素时，由于受共同的外部环境条件的影响，会存在主备件同时失效的情况，也就是主备件共因失效的发生。下面针对这种情况下的系统失效进行贝叶斯网络建模及求解。由于本节考虑了动态逻辑门，因此各个事件的状态划分与 3.3 节中一致，即任务时间被划分为 n 个状态，每个状态对应一个时间区间，某事件处于该状态表示该事件在这个时间区间内发生。

另外，本节的共因失效采用 β 因子模型，β 因子取值范围为 0~0.25。

（1）零部件级备份

当系统中存在零部件级备份时，加入共因失效节点 K，同时在输入事件 A_1、A_2 与输出事件 T 之间插入两个复合节点 B_1、B_2，按照 FT 模型向 BN 模型的转化规则，建立系统的贝叶斯网络模型如图 5-9 所示。

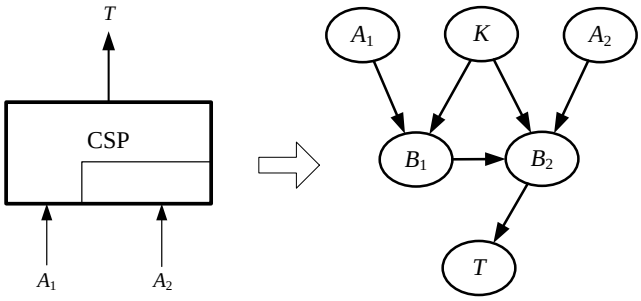


图 5-9 单部件冷备份系统 DFTA 模型转化为考虑 CCF 时的 BN 模型

其中各节点的意义如下：

A_1、A_2 分别代表主件 A_1、A_2 单独失效事件，K 代表共因失效事件，B_1、B_2 分别代表主备件总失效事件（包含各自独立失效和共因失效），T 代表 CSP 门的输出事件。下面讨论各个非根节点 CPD 的确定。

B_1 节点：该节点的父节点包含对应部件 A_1 独立失效事件 A_1 和共因失效事件 K 两个节点。独立失效和共因失效之间只要任意一个发生，该节点就失效，因此该节点的 CPD 与 OR 门的 CPD 相同，见 3.3.2.1 节。

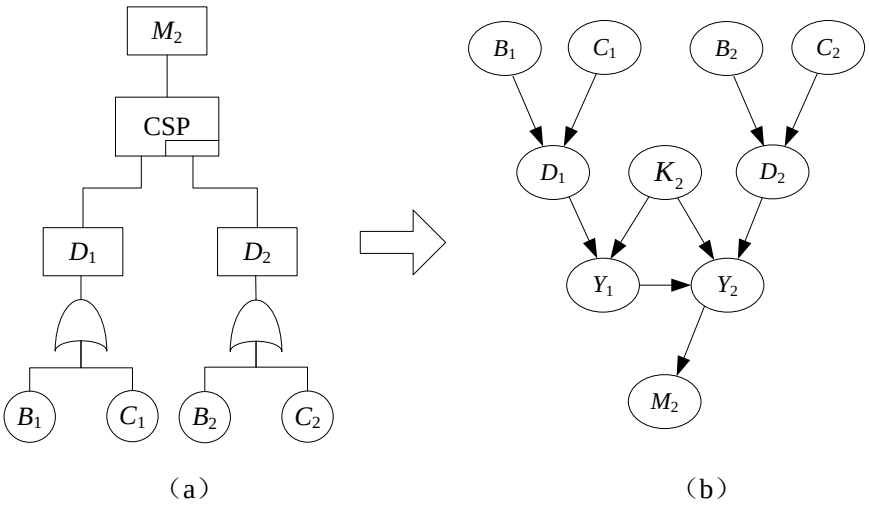
B_2 节点：该节点有三个父节点 K、A_2 与 B_1，假设其状态分别为 c，a，b，输出事件 T 的状态为 t。根据冷备件门的失效特征，考虑共因失效的影响，得到节点 B_2 的条件概率表如下：

$$f(t\mid a,b,c)=\begin{cases} c, & \mathrm{b}<\mathrm{c}\le\mathrm{a} \\ c, & b=c<a \\ a, & b<a<c \\ n+1, & \text{其它} \end{cases} \qquad (a,b,c,t=1,2,\cdots,n+1) \tag{5-36}$$

T 节点：由于把主件的影响考虑在备件中，节点 T 只含有备件这一个父节点，其 CPD 为一个单位矩阵，见 3.3 节所示。

（2）子系统级备份

在某些场合下，在系统设计过程中会对某个局部的子系统进行备份，以提高系统的可靠性。考虑双部件子系统备份的情况，其动态故障树模型如图 5-10（a）所示。考虑共因失效的影响后，其贝叶斯网络模型如图 5-10（b）所示。



（a） （b）

图 5-10 双部件冷备份子系统 DFTA 模型转化为考虑 CCF 时的 BN 模型

（a）子系统级备份系统 FTA 模型；（b）考虑 CCF 时的 BN 模型

在图 5-10（a）中，D_2 对 D_1 进行备份。考虑共因失效后，在图 5-10（b）中引入中间节点 Y_1、Y_2、K_2。D_2 表示 B_2 与 C_2 的输出事件，未考虑其冷备份的作用，而把冷备份失效机理转移到节点 Y_2 中来考虑。D_1、D_2 的 CPD 分别由其父节点 B_1 与 C_1、B_2 与 C_2 的逻辑关系来确定，而 Y_1、Y_2 的 CPD 与前述单部件备份相同。

当子系统中含有两个以上的部件时，修改网络中节点 D_1 及 D_2 的父节点数，同时增加其对应的 CPD 的维数，即可建立对应的贝叶斯网络模型。

5.5.3.2 含温备份及热备份的共因失效建模及分析

包含两个输入事件的温备份故障树模型及考虑 CCF 时的贝叶斯网络模型如图 5-11 所示，其中，A_1, A_2 分别为主、备件的独立失效事件，K_1 为共因事件，X_1, X_2 为考虑 CCF 后的主、备件失效事件，M_2 为输出事件。

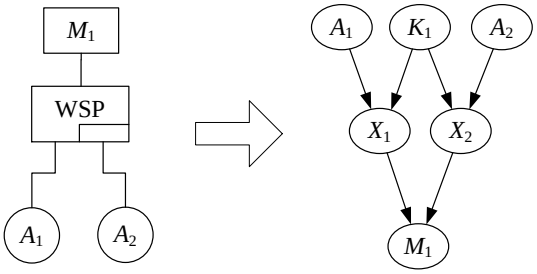


图 5-11 两输入热备份 DFTA 模型转化为考虑 CCF 时的 BN 模型

假设各个事件的状态分别为 $a_1, a_2, k_1, x_1, x_2, m_1$（在 1~$n$+1 之间取值），则根据失效机理可得输出事件的条件分布如下：

$$\begin{aligned} f(m_1 \mid a_1, a_2, k_1) &= \max(x_1, x_2) \\ &= \max(\min(a_1, k_1), \min(a_2, k_1)) \end{aligned} \tag{5-37}$$

根据以上规则，当输入事件为任意 n 个时，FTA 模型及 BN 模型如图 5-12 所示。

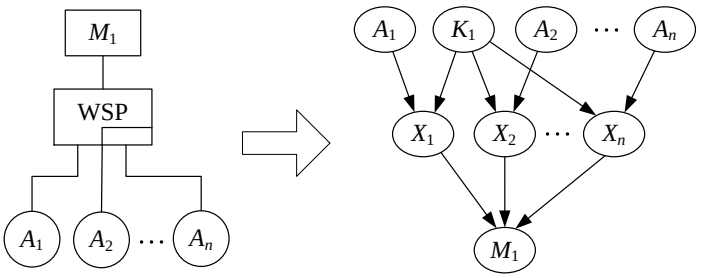


图 5-12 n 个输入事件的热备份 FTA 模型转化为考虑 CCF 时的 BN 模型

输出事件的条件概率分布为：

$$\begin{aligned} f(m_1 \mid a_1, a_2, \cdots a_n, k_1) &= \max(x_1, x_2, \cdots x_n) \\ &= \max(\min(a_1, k_1), \min(a_2, k_1), \cdots \min(a_n, k_1)) \end{aligned} \tag{5-38}$$

对于热备份的情况，由于备份因子$\alpha = 1$此时备件的概率分布与主件相同，各级输出事件的 CPD 都与或门的 CPD 相同。

5.6 实例分析：星载天线双轴定位机构控制系统的可靠性分析

5.6.1 系统描述及故障树建模

本节以星载天线双轴定位机构控制系统为例进行考虑共因失效的贝叶斯网络可靠性分析方法的实例分析验证。

双轴定位机构控制系统的主要功能是控制整个机构的运动，其结构组成主要包括：

（1）电源；

（2）控制线路；

（3）控制计算机。

为提高整个控制系统的可靠性，对其中的组件采用冗余备份[92]，其中电源组件采用热备份，控制线路和控制计算机采用冷备份。

双轴定位机构控制系统的故障树模型如图 5-13 所示，各个事件描述如表 5-3 所示。

表 5-3 系统事件描述

事件符号	事件名称	事件符号	事件名称
A_1	主电源故障	C_2	备用控制计算机故障
A_2	备用电源故障	D_1	主控制组件故障
A_3	备用电源故障	D_2	备用控制组件故障
B_1	主控制线路故障	M_1	电源组件故障
C_1	主控制计算机故障	M_2	控制线路与计算机组件故障
B_2	备用控制线路故障	T	控制系统故障

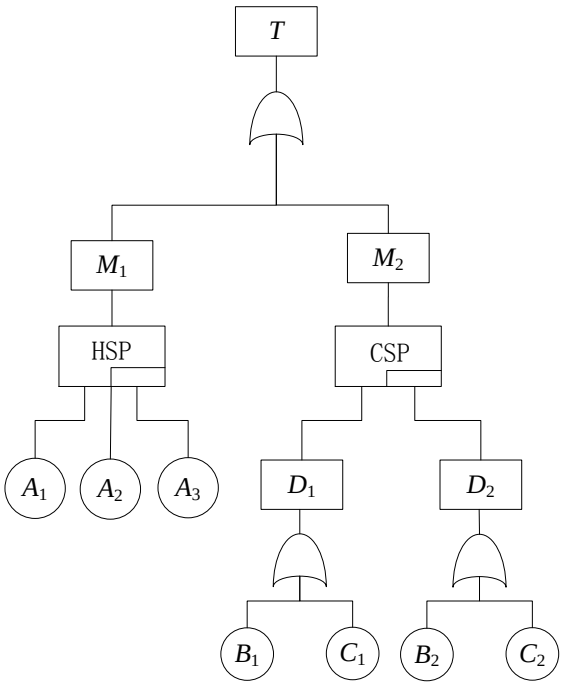


图 5-13 控制系统动态故障树

5.6.2 不考虑共因失效的贝叶斯网络可靠性分析

在不考虑共因失效的情况下，对图 5-13 所示的动态故障树进行可靠性分析。按照故障树模型向贝叶斯网络模型的转化原则，建立与图 5-13 所示故障树模型对应的贝叶斯网络模型如图 5-14 所示。

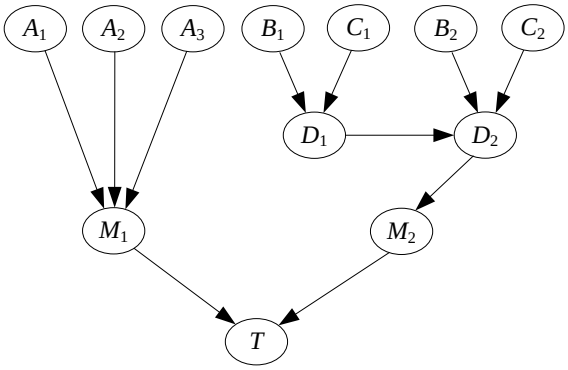


图 5-14 不考虑 CCF 时的控制系统 BN 模型

该 BN 模型的非根节点中包含热备份节点 M_1，或门节点 D_1，或门结合冷备份节点 D_2，节点 M_2 以及或门节点 T。假定各个基本事件的失效率如表 5-4 所示。利用第三章中的方法确定所有非根节点的 CPD 表，编制 Matlab 程序，对该 BN 模型进行分析计算。

表 5-4 不考虑 CCF 的基本事件失效率

基本事件	A_1	A_2	A_3	B_1	C_1	B_2	C_2
失效率（10^{-6}/h）	2.4	2.4	2.4	2.6	2.2	2.6	2.2

在状态划分数 n=10 的情况下运用 BN 方法对系统进行计算，同时在仿真次数取 500000 次的条件下作仿真计算，得到系统在给定时间点下的可靠度数据如表 5-5 和图 5-15 所示。

表 5-5 BN 方法与 MCS 方法的可靠度计算结果对比

时间（h）	BN1 结果	MC 仿真结果	相对误差（%）
5000	0.99975	0.99966	0.0089
10000	0.99899	0.99883	0.0046
15000	0.99779	0.99746	0.0321
20000	0.99613	0.99559	0.0493
25000	0.99405	0.99332	0.0731
30000	0.99158	0.99038	0.1257
35000	0.98872	0.98719	0.1551
40000	0.98552	0.98327	0.2394
45000	0.98197	0.97870	0.3337
50000	0.97811	0.97419	0.4041

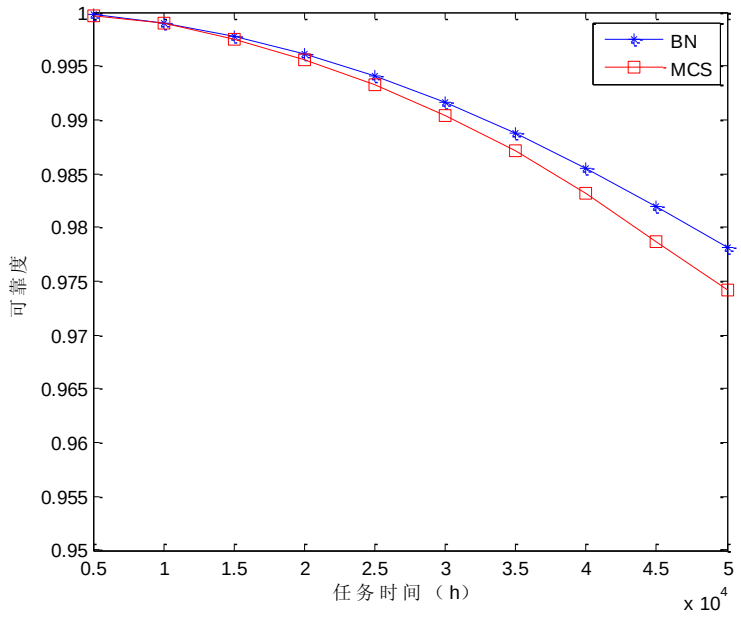


图 5-15 不考虑 CCF 的可靠度计算结果

5.6.3 考虑共因失效的贝叶斯网络可靠性分析

考虑共因失效后，按照 5.5.3 节中所述的方法增加相应的节点，再进行模型转化，得到如图 5-16 所示的贝叶斯网络模型。该模型中 K_1，K_2 分别为图 5-13 中热备份门输入事件的共因失效节点和冷备份门输入事件之间的共因失效节点，X_1、X_2、X_3 分别为热备份门各个输入事件与共因失效事件之间的复合事件，Y_1、Y_2 分别为冷备份门主备件的复合失效事件，M_1 为热备份的输出事件，M_2 为冷备份的输出事件，T 为系统输出事件。

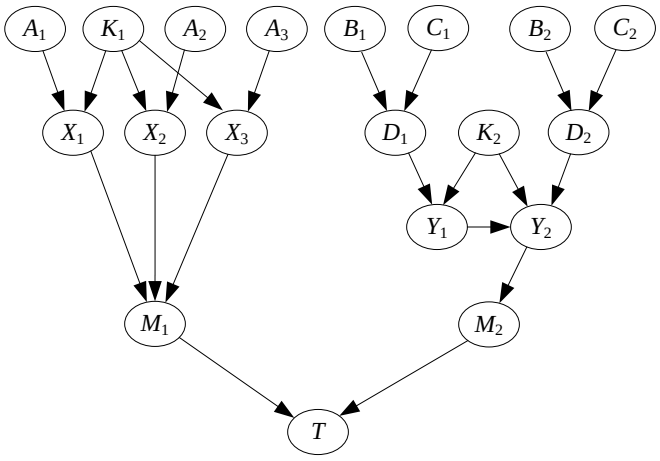


图 5-16 考虑 CCF 的控制系统 BN 模型

取共因因子 β=0.1，并假设各个基本事件的失效率数据如表 5-6 所示。

表 5-6 考虑 CCF 的基本事件失效率

基本事件	A_1	A_2	A_3	K_1	B_1	C_1	B_2	C_2	K_2
失效率（10^{-6}/h）	2.4	2.4	2.4	0.24	2.6	2.2	2.6	2.2	0.48

在状态划分数 n=10 时的情况下，运用 Matlab 的 BNT 工具箱对贝叶斯网络进行计算，同时在仿真次数取 500000 的条件下对系统作仿真计算，得到系统在给定时间点下的可靠度数据如表 5-7 和图 5-17 所示。

表 5-7 和图 5-17 中，BN1 为不考虑 CCF 时的 BN 计算结果，BN2 为考虑 CCF 时的 BN 计算结果，MCS 为考虑 CCF 时的仿真计算结果。

表 5-7 考虑 CCF 时 BN 方法与 MCS 方法的可靠度计算结果对比

时间	BN2 结果	MC 仿真结果	相对误差（%）
5000	0.99618	0.99608	0.0106
10000	0.99195	0.99155	0.0405
15000	0.98734	0.98661	0.0738
20000	0.98236	0.98153	0.0838
25000	0.97704	0.97554	0.1536
30000	0.97141	0.96892	0.2568
35000	0.96549	0.96216	0.3445
40000	0.95929	0.95536	0.4097
45000	0.95285	0.94749	0.5629
50000	0.94617	0.93998	0.6543

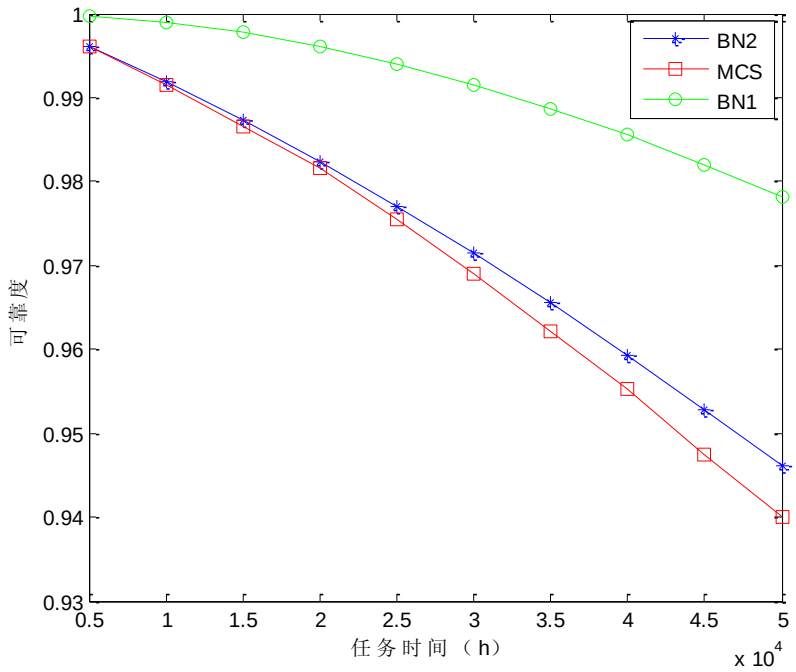


图 5-17 两种情况下的贝叶斯网络计算结果与 MCS 方法计算结果对比

由分析结果的对比可以得出，考虑 CCF 的基于时间区间划分的离散时间 BN 方法与 MCS 方法的计算结果比较吻合。前者由于是近似计算，减小了系统在任务时间内各个状态的概率，因此所得的可靠度（BN2）略高于 MCS 的计算结果。同

时也可以得出，在共因因子 β 取值仅为 0.1 的情况下，考虑 CCF 后的系统可靠度（BN2）远小于不考虑 CCF 时的系统可靠度（BN1）。由此可以得出，CCF 对系统的可靠度有着显著的影响。另外，与 5.6.2 节类似，由于我们取的 n 值是固定的，因此随着任务时间的增长，区间长度也会相应增长，误差会相应的增大。当任务时间大于 20000h 后，可以采取分段设定 n 值的办法，在前期设定较小的 n 值以降低计算成本，在后期适当增大 n 值以提高求解精度，使所得分析结果能满足计算效率和分析精度的要求。

5.7 本章小结

本章运用故障树方法对具有共因失效的实例系统进行了可靠性分析。首先介绍了当前共因失效研究中的一些经典模型和建模方法，运用共因失效的显式建模方法与平方根模型对列车追尾事故进行了故障树分析。通过对子树 M_{12}“调度员未注意到险情”的定量计算得出该事件发生的概率为 0.0402。并通过与底事件相互独立假设下的计算结果进行对比，结果表明不考虑共因失效因素的影响会对可靠性分析结果带来较大的误差。这说明了共因失效对列车追尾事故的发生具有重要的影响，同时这也为列车安全性及可靠性评估提供了参考。本章还提出了考虑共因失效的含备件门的动态故障树及贝叶斯网络可靠性建模与分析方法。通过算例分析及与蒙特卡洛仿真方法的对比分析，验证了该方法的有效性和准确性。

第六章 结　论

6.1 全文总结

随着现代设计、制造技术及计算机技术的飞速发展，系统的结构日益复杂，对性能的需求也越来越高。伴随着系统性能提高的同时，成本也在显著的增加，系统一旦发生故障或失效，无论是维修或报废都将会造成巨大的经济损失，有时甚至会造成人员伤亡。因此，复杂系统的可靠性和安全性问题越来越受到人们的广泛重视，复杂系统可靠性分析也成为目前国内外研究的热点及难点问题之一。故障树分析方法是系统可靠性分析方法中发展最为完善、应用最为广泛的方法。静态故障树分析方法不考虑部件失效的时间关系、顺序关系以及相关关系等动态失效特性。实际工程系统中零部件的失效行为往往具有一种或多种动态失效特性，如何正确地建立具有动态失效特性的子系统的可靠性模型是整个系统可靠性建模与分析的关键。

另一方面，不确定性广泛存在于实际工程系统中。零部件及系统的状态和失效行为等都存在大量的随机和模糊不确定性。同时，由于成本、时间、管理和人因等多方面的原因导致复杂系统可靠性分析的基础数据存在模糊不确定性。目前，在考虑模糊不确定性的动态故障树分析方面的研究还相对较少，一些最新的动态故障树分析方法还有待补充和完善。同时，复杂系统的失效往往伴随着大量的共因失效，在不考虑共因失效的条件下对系统进行可靠性分析，往往会带来较大的误差，进而会影响可靠性设计的准确性，使得复杂系统在实际服役过程中的失效概率远大于独立失效条件下的预计值，造成巨大的经济损失甚至是人员伤亡。因此，本文对考虑模糊不确定性、动态失效特性及共因失效的复杂系统可靠性建模与分析方法进行了深入的研究，其主要研究成果如下：

（1）建立了基于模糊马尔科夫模型的动态故障树分析方法。在基于马尔科夫模型的动态故障树分析方法的基础上，考虑了零部件失效的模糊不确定性，研究了在失效率存在模糊不确定性的情况下的动态故障树分析方法。首先在系统结构分析和失效分析的基础上，建立了系统的动态故障树模型。然后运用三角模糊数来描述零部件和系统的失效率，并将动态故障树模型转换为系统失效过程的模糊马尔科夫模型。再运用模糊理论中的扩展原理和 Laplace-Stieltjes 变换方法求解模型中的状态转移方程组，得到系统在给定时刻下的模糊可靠度和给定隶属度下的模糊可靠度曲线。最后应用该模糊马尔科夫模型对某数控加工中心液压系统进行

可靠性建模与分析。实例分析表明，该方法是系统可靠性分析的一种有效的方法，能够准确地对具有动态失效特性及模糊不确定性的系统进行可靠性建模及定量评估。

（2）建立了基于离散时间贝叶斯网络的动态故障树可靠性评估模型。研究了基于贝叶斯网络和动态故障树的系统可靠性建模和评估方法。作为处理不确定性知识推理的强有力的工具，贝叶斯网络对随机不确定性知识的表达和推理具有很强的处理能力。针对基于马尔科夫模型的动态故障树求解方法中存在的状态爆炸问题，运用贝叶斯网络替代马尔科夫模型来求解动态故障树模型。阐述了贝叶斯网络的条件独立属性降低模型推理和计算复杂性的机理，提出了静态和动态故障树中各种逻辑门所对应的贝叶斯网络模型中各个节点的条件概率分布的确定方法。建立了卫星太阳翼驱动机构的动态故障树模型和相应的贝叶斯网络模型，并运用联合树推理算法对该模型进行了双向推理，其结果可用于指导系统的故障诊断和预计，通过找出系统的薄弱环节并实施设计改进，能够有效地提高系统的可靠性。实例分析结果表明：该方法能够有效地解决具有动态失效特性的复杂系统的可靠性分析和评估问题。

（3）建立了模糊数据下基于连续时间贝叶斯网络的动态故障树分析方法。研究了考虑模糊不确定性下的基于贝叶斯网络的系统可靠性建模与分析方法。当系统中零部件失效之间具有顺序相关及功能相关等动态失效特性时，基于连续时间贝叶斯网络的可靠性建模与分析方法能准确地建立系统的贝叶斯网络模型，并进行可靠性分析和计算。考虑系统及零部件失效行为的模糊不确定性，用三角模糊数描述其失效率，并用模糊失效率构造零部件的模糊边缘失效密度函数。用单位阶跃函数和冲激函数联合构造了贝叶斯网络中非根节点失效事件的条件概率密度函数和分布函数。推导了在模糊失效率数据下的几种典型的故障树逻辑门输出事件发生的模糊边缘失效密度函数、模糊失效分布函数的表达式。算例及实例分析结果验证了该方法的可行性和正确性。

（4）提出了考虑共因失效的动态故障树及贝叶斯网络可靠性建模与分析方法。运用共因失效的显式建模方法与平方根模型对甬温线动车组追尾事故进行了故障树分析。结果表明不考虑共因失效因素的影响会对可靠性分析结果带来较大的误差。这说明了共因失效对列车追尾事故的发生具有重要的影响，同时也为列车安全性及可靠性评估提供了参考。提出了考虑共因失效的动态故障树及贝叶斯网络可靠性建模与分析方法，建立了考虑共因失效条件下确定各种备件门输出事件的条件概率分布的公式。通过算例验证了该方法的可行性，并通过与蒙特卡洛方法的计算结果对比分析，表明了该方法具有较高的求解精度，能够满足工程实

际的需求。

综上所述，本文在考虑动态失效特性、模糊不确定性及共因失效等因素下对动态故障树分析方法进行了深入的研究，在一定程度上完善了系统可靠性分析方法的理论基础并拓展了其应用范围。

6.2 后续工作展望

本文在考虑动态失效特性、模糊不确定性及共因失效等因素下对动态故障树分析方法开展了具有创新的研究工作，但所建立的体系和所取得的成果仍然需要进一步完善。作者今后将从以下几方面继续开展相关研究：

（1）多状态条件下基于贝叶斯网络的动态故障树分析。实际工程中系统的失效状态往往不是突发的，而是一个逐渐退化的过程，中间通常会经历部分功能丧失的性能退化状态。多状态条件下基于贝叶斯网络的静态故障树分析方法已经取得了较多的研究成果，但是在结合多状态和动态失效特性的贝叶斯网络建模与分析方面的研究还相当匮乏，有必要在这方面做进一步的研究。

（2）多种变量下的动态故障树分析方法研究。本文对非概率方面的探索性研究仅限于模糊变量，当系统或模型中需要引入其它类型的非随机变量来描述分布参数时，如何建立和求解此类动态故障树模型或者贝叶斯网络模型还有待继续展开研究。

（3）考虑共因失效及多状态条件下的动态故障树分析方法。实际工程系统中经常遇到共因失效、动态失效及多状态等特征同时存在的情况，对于这类系统的可靠性建模与分析方法的研究还相当匮乏，针对这种多状态、多失效特征和失效相关的复杂系统的理论分析模型与求解方法还很不完善。因此有必要对这些特征同时存在下的系统可靠性建模及分析做进一步的研究与探索。

致　谢

四年多的博士生涯即将结束，此时此刻，心中不免感慨万千。二十三年的漫漫求学路，包含了太多的艰辛与不易，承载了太多人的期望与关怀。在此，谨向在整个博士求学期间给予我指导、关心、帮助和支持的所有老师、同学、朋友和亲人们致以最诚挚的感谢！

首先，衷心感谢我的导师黄洪钟教授在我攻读博士学位期间给予我的指导与帮助。黄老师渊博的学识、严谨的治学态度和饱满的工作热情一直深深地影响着我。正是有了黄老师的悉心指导和深切关怀，我才能够顺利完成学业。黄老师肩负着整个可靠性工程团队的建设和管理任务，承担着学院繁重的行政管理工作，同时又主持多个科研项目的开展，但黄老师依然时刻关心着我的学习，时常关注我的科研进展情况。从论文选题、课题开展到学术论文及博士学位论文的撰写和修改，都倾注了黄老师大量的心血，他经常为了审阅、修改我的学术论文而工作至深夜。每次收到黄老师审阅论文后发回的邮件，看到遍布整个论文的修改痕迹，都让我的心灵受到涤荡和洗礼，提醒自己要不断的努力改进和完善自己。在此谨向尊敬的黄老师致以最衷心的感谢，向黄老师及家人致以最美好的祝福！

感谢美国 Rutgers University 的 Hae Chang Gea 教授。在我留学美国的一年时间里，Gea 教授在学术上和生活上都给予了我极大的指导与帮助。感谢 Rutgers University 的 W. Song 博士、P.N. Ge 博士、H.H. Qi 博士、X.K. Zhao 博士、B. Wang 博士在我留美期间给予我的关心和帮助。

感谢可靠性工程团队的何俐萍老师、许焕卫老师、李海庆老师、刘宇老师、汪忠来老师、张小玲老师、朱顺鹏老师、肖宁聪老师等给予我的帮助和鼓励。祝愿他们工作顺利，生活幸福！

感谢我的同学们，郭夙昌博士、张旭东博士、庞煜博士、甘露萍博士、孟德彪博士、杨圆鉴博士、彭卫文博士及孙健硕士等，感谢他们给予我的帮助。

感谢我的女友米金华对我的支持和鼓励，与她携手的日子充满了欢乐与幸福，祝愿她前程似锦、幸福快乐！

衷心的感谢我的父母，是他们默默的付出、一如既往的支持，才使我能够顺利的毕业。

最后，再次感谢所有给予我帮助、支持和关心的老师、同学、朋友和亲人们！

参考文献

[1] J. B. Dugan, S. J. Bavuso, M. A. Boyd. Dynamic fault-tree for fault-tolerant computer systems[J]. IEEE Transactions on Reliability, 1992, 41(3): 363-376.

[2] J. B. Dugan, K. J. Sullivan, D. Coppit. Developing a low cost high-quality software tool for dynamic fault-tree analysis[J]. IEEE Transactions on Reliability, 2000, 49(1): 49-59.

[3] S. Amari, G. Dill, E. Howald. A new approach to solve dynamic fault trees[C]. Proceedings of Annual IEEE Reliability and Maintainability symposium (RAMS 2003), Tampa, USA, 2003.

[4] T. Yuge, S. Yanagi. Quantitative analysis of a fault tree with priority AND gates[J]. Reliability Engineering & System Safety, 2008, 93(11): 1577-1583.

[5] K. D. Rao, V. Gopika, V. V. S. S. Rao, et al. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment[J]. Reliability Engineering & System Safety, 2009, 94(4): 872-883.

[6] A. Bobbio, C. R. Daniele. Parametric fault trees with dynamic gates and repair boxes[C]. Proceedings of the Annual IEEE Reliability and Maintainability Symposium (RAMS 2004), Los Angeles, USA, 2004.

[7] A. Bobbio, L. Portinale, M. Minichino, et al. Improving the analysis of dependable systems by mapping fault trees into bayesian networks[J]. Reliability Engineering & System Safety, 2001, 71(3): 249-260.

[8] W. S. Lee, D. L. Grosh, F. A. Tillman, et al. Fault tree analysis, methods, and applications-a review[J]. IEEE Transactions on Reliability, 1985, R-34(3): 194-203.

[9] N. Rasmussen. Reactor safety study-an assessment of accident risk in U.S. commercial nuclear power plants, WASH-1400[R]. US Nuclear Regulatory Commission, Washington DC, 1975.

[10] 朱继洲. 故障树原理和应用[M]. 西安: 西安交通大学出版社, 1989.

[11] J. B. Fussell. Synthetic tree model: A formal methodology for fault tree construction[R]. ANCR-1098, 1973.

[12] J. B. Fussell. A formal methodology for fault tree construction[J]. Nuclear Engineering and Design, 1973, 52: 337-360.

[13] G. J. Powers, F. C. Tompkins. Computer-aided synthesis of fault trees for complex processing systems[J]. AICHE Journal, 1974, 20: 376-387.

[14] S. L. Salem, G. E. Apostolakis, D. Okrent. A new methodology for the computer-aided construction of fault trees[J]. Annals of Nuclear Energy, 1977, 4(9-10): 417-433.

[15] S. L. Salem, J. S. Wu, G. E. Apostolakis. Decision table development and application to the construction of fault trees[J]. Nuclear Technology, 1979, 42(1): 51-64.

[16] S. A. Lapp, G. J. Powers. Update of lapp-powers fault tree synthesis algorithm[J]. IEEE Transactions on Reliability, 1979, R-28(1): 12-15.

[17] W. E. Vesely, R. E. Narum. PREP and KITT computer code for the automatic evaluation of a fault tree[R]. Idaho Nuclear Corporation, Idaho Falls, Idaho, IN-1349, 1970.

[18] J. B. Fussell, W. E. Vesely. New methodology for obtaining cut sets for fault trees[J]. Transactions of the American Nuclear Society, 1972, 15: 262-263.

[19] J. B. Fussell, E. B. Henry, N. H. Marshall. MOCUS-a computer program to obtain minimal sets from fault trees[R]. ANCR-1156, Aerojet Nuclear Company, Idaho Falls, Idaho, 1974.

[20] P. K. Pande, M. E. Spector, P. Chatterjee. Computerized fault tree analysis[R], TREEL AND MICSUP, ORC 75-3, Operation Research Center, University of California, Berkeley, 1975.

[21] B. J. Garrick. Principles of unified system safety analysis[J]. Nuclear Engineering and Design, 1970, 13: 245-321.

[22] H. E. Kongsoe. REDIS, a computer program for system reliability analysis by direct simulation[C], Intern. Symp. Reliability of Nuclear Power Plants, Innsbruck, Austria, 1975.

[23] H. Z. Huang, H. Zhang, Y. F. Li. A new ordering method of basic events in fault tree analysis[J]. Quality and Reliability Engineering International, 2012, 28(3): 297-305.

[24] 米金华, 李彦锋, 李海庆, 等. 基于模糊理论的数控机床液压系统故障树分析[J]. 制造技术与机床, 2011, (4): 114-119.

[25] 梅启智, 廖炯生, 孙慧中. 系统可靠性工程基础[M]. 北京: 科学出版社, 1987.

[26] 罗航. 故障树分析的若干关键问题研究[D]. 成都: 电子科技大学, 2010.

[27] H. Tanaka, L. T. Fan, F. S. Lai, et al. Fault-tree analysis by fuzzy probability[J]. IEEE Transactions on Reliability, 1983, R-32(5): 453-457.

[28] H. Furuta, H. Shiraishi. Fuzzy importance in fault tree analysis[J]. Fuzzy Sets and Systems, 1984, 12(3): 205-213.

[29] D. Singer. A fuzzy set approach to fault tree and reliability analysis[J]. Fuzzy Sets and Systems, 1990, 34(2): 145-155.

[30] J. P. Sawyer, S. S. Rao. Fault tree analysis of fuzzy mechanical system[J]. Microelectronics and Reliability, 1994, 34(4): 653-667.

[31] K. B. Misra, G. G. Weber. A new method for fuzzy fault tree analysis[J]. Microelectronics

and Reliability, 1989, 29(2): 195-216.

[32] J. A. B. Geymayr, N. F. F. Ebecken. Fault-tree analysis: a knowledge-engineering approach[J]. IEEE Transactions on Reliability, 1995, 44(1): 37-45.

[33] R, Ferdous, F. Khan, B. Veitch, et al. Methodology for computer aided fuzzy fault tree analysis[J]. Process Safety and Environmental Protection, 2009, 87(4): 217-226.

[34] T. Fujino, F. C. Hadipriono. New gate operations of fuzzy fault tree analysis[C]. IEEE World Congress on Computational Intelligence, 1994.

[35] A. Mentes, I. H. Helvacioglu. An application of fuzzy fault tree analysis for spread mooring systems[J]. Ocean Engineering, 2011, 38(2-3): 285-294.

[36] Y. Dong, D. Yu. Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis[J]. Journal of Loss Prevention in the Process Industries, 2005, 18(2): 83-88.

[37] M. H. Shu, C. H. Cheng, J. R. Chang. Using intuitionistic fuzzy sets for fault-tree analysis on printed circuit board assembly[J]. Microelectronics Reliability, 2006, 46(12): 2139-2148.

[38] L. He, H. Z. Huang, M. J. Zuo. Fault tree analysis based on fuzzy logic[C]. Proceedings of Annual IEEE Reliability and Maintainability Symposium (RAMS 2007), Orlando, USA, 2007.

[39] H. Song, H. Y. Zhang, C. W. Chan. Fuzzy fault tree analysis based on T-S model with application to INS/GPS navigation system[J]. Soft Computing, 2008, 13(1): 31-40.

[40] K. H. Chang, C. H. Cheng. A novel general approach to evaluating the PCBA for components with different membership function[J]. Applied Soft Computing, 2009, 9(3): 1044-1056.

[41] S. R. Cheng, B. Lin, B. M. Hsu, et al. Fault-tree analysis for liquefied natural gas terminal emergency shutdown system[J]. Expert Systems and Applications, 2009, 36(9): 11918-11924.

[42] I. M. Dokas, D. A. Karras, D. C. Panagiotakopoulos. Fault tree analysis and fuzzy expert systems: early warning and emergency response of landfill operations[J]. Environmental Modeling & Software, 2009, 24(1): 8-25.

[43] D. A. Zhao, J. J. Zheng, Y. W. Zheng. Risk analysis of shield tunnel segment failure based on fuzzy fault tree method[C]. International Conference on Natural Computation (ICNC 2010), Yantai, China, 2010.

[44] M. Abdelgawad, A. R. Fayek. Fuzzy reliability analyzer: quantitative assessment of risk events in the construction industry using fuzzy fault-tree analysis[J]. Journal of Construction Engineering and Management, 2010, 137(4): 294-302.

[45] G. Z. Mao, J. W. Tu, H. B. Du. Reliability evaluation based on fuzzy fault tree[C]. IEEE

International Conference on Industrial Engineering and Engineering Management (IE&EM 2010), Xiamen, China, 2010.

[46] A. Deshpande. Fuzzy fault tree analysis: revisited[J]. International Journal of System Assurance Engineering and Management, 2011, 2(1): 3-13.

[47] M. Kumar, S. P. Yadav, S. Kumar. Reliability analysis of computer security system based on intuitionistic fuzzy fault tree[J]. Advanced Materials Research, 2011, 403: 3495-3502.

[48] J. Mi, Y. F. Li, H. Li, et al. Reliability analysis of CNC hydraulic system based on fuzzy fault tree[C]. International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE 2011), Xi'an, China, 2011.

[49] R. Ferdous, F. Khan, R. Sadiq, et al. Fault and event tree analyses for process systems risk analysis: uncertainty handling formulations[J]. Risk Analysis, 2011, 31(1): 86-107.

[50] L. Chen. An approach of fault diagnosis for electronic system of aircraft based on trapezoid fuzzy fault tree[C]. International Conference on Artificial Intelligence, Management Science and Electronic Commerce, Zhengzhou, China, 2011.

[51] N. Kumar, J. H. Borm, A. Kumar. Reliability analysis of waste clean-up manipulator using genetic algorithms and fuzzy methodology[J]. Computers & Operations Research, 2012, 39(2): 310-319.

[52] M. Celik, S. M. Lavasani, J. Wang. A risk-based modelling approach to enhance shipping accident investigation[J]. Safety Science, 2012, 48(1): 18-27.

[53] J. P. Yang, H. Z. Huang, Y. Liu, et al. Evidential networks for fault tree analysis with imprecise knowledge[J]. International Journal of Turbo & Jet Engines, 2012, 29(2): 111-122.

[54] H. Z. Huang, X. Tong, M. J. Zuo. Posbist fault tree analysis of coherent systems[J]. Reliability Engineering & System Safety, 2004, 84(2): 141-148.

[55] J. B. Dugan, B. Venkataraman, R. Gulati. DIFtree: A software package for the analysis of dynamic fault tree models[C]. Proceedings of Annual IEEE Reliability and Maintainability symposium (RAMS 1997), Philadelphia, USA, 1997.

[56] J. B. Dugan, K. J. Sullivan, D. Coppit. Developing a low cost high-quality software tool for dynamic fault-tree analysis[J]. IEEE Transactions on Reliability, 2000, 49(1): 49-59.

[57] A. Anand, A. K. Somani. Hierarchical analysis of fault trees with dependencies, using decomposition[C]. Proceedings of Annual IEEE Reliability and Maintainability symposium (RAMS 1998), Anaheim, USA, 1998.

[58] W. Long, Y. Sato, M. Horigome. Quantification of sequential failure logic for fault tree analysis[J]. Reliability Engineering & System Safety, 2000, 67(3): 269-274.

[59] M. Cepin, B. Mavko. A dynamic fault tree[J]. Reliability Engineering & System Safety, 2002, 75(1): 83-91.

[60] H. Sun, J. D. Andrews. Identification of independent modules in fault trees which contain dependent basic events[J]. Reliability Engineering & System Safety, 2004, 86(3): 285-296.

[61] H. Boudali, P. Crouzen, M. Stoelinga. Dynamic fault tree analysis using input/output interactive markov chains[C]. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Edinburgh, England, 2007.

[62] P. Bucci, J. Kirschenbaum, L. A. Mangan. Construction of event-tree/fault-tree models from a markov approach to dynamic system reliability[J]. Reliability Engineering & System Safety, 2008, 93(11): 1616-1627.

[63] G. Merle, J. M. Roussel, J. J. Lesage, et al. Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events[J]. IEEE Transactions on Reliability, 2010, 59(1): 250-261.

[64] F. Chiacchio, M. Cacioppo, D. D' Urso, et al. A Weibull-based compositional approach for hierarchical dynamic fault trees[J]. Reliability Engineering & System Safety, 2013, 109: 45-52.

[65] C. Wang, L. Xing, S. V. Amari. A fast approximation method for reliability analysis of cold-standby systems[J]. Reliability Engineering & System Safety, 2012, 106: 119-126.

[66] A. Lindhe, T. Norberg, L. Rosen. Approximate dynamic fault tree calculations for modeling water supply risks[J]. Reliability Engineering & System Safety, 2012, 106: 61-71.

[67] H. L. Zhang, C. Y. Zhang, D. Liu, et al. A method of quantitative analysis for dynamic fault tree[J]. The Annual Reliability and Maintainability Symposium (RAMS 2011), Lake Buena Vista, USA, 2011.

[68] H. Boudali, P. Crouzen, M. Stoelinga. A rigorous, compositional, and extensible framework for dynamic fault tree analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(2): 128-143.

[69] W. E. Vesely. Fault tree handbook[M]. NUREG-0492. Washington D.C.: US Nuclear Regulatory Commission, 1981.

[70] International Electrotechnical Commission. IEC 61025. Fault tree analysis (Edition 2.0)[S]. Geneva: 2006.

[71] Bell Telephone Laboratories. Launch control safety study (Section VII) [M]. New Jersey: Murray Hill Press, 1961.

[72] K. K. Aggarwal. Comment on an efficient simple algorithm for fault tree automatic synthesis

from the reliability graph[J]. IEEE Transactions on Reliability, 1979, R-28(4): 309 - 315.

[73] R. N. Allan, I. L. Rondiris, D. M. Fryer. An efficient computational technique for evaluating the cut/tie sets and common-cause failures of complex systems[J]. IEEE Transactions on Reliability, 1981, R-30(2): 101-109.

[74] P. K. Andow. Difficulties in fault-tree synthesis for process plant[J]. IEEE Transactions on Reliability, 1980, R-29(1): 2-9.

[75] N. N. Bengiamin, B. A. Bowman, K. F. Schenk. An efficient algorithm for reducing the complexity of computation in fault tree analysis[J]. IEEE Transactions on Nuclear Science, 1976, 23(5): 1442-1446.

[76] L. Meshkat, J. B. Dugan, J. D. Andrews. Dependability analysis of systems with on - demand and active failure modes using dynamic fault trees[J]. IEEE Transactions on Reliability, 2002, 51(2): 240-251.

[77] L. A. Zadeh. Fuzzy sets[J]. Information and Control, 1965, 8(3): 338-353.

[78] Zadeh L A. Fuzzy set as a basis for a theory of possibility[J]. Fuzzy Sets and Systems, 1978, 1(1): 3-28.

[79] K. B. Misra, G. G. Weber. Use of fuzzy set theory for level-1 studies in probabilistic risk assessment[J]. Fuzzy Sets and Systems, 1990, 37(2): 139-160.

[80] G. Liang, J. M. Wang. Fuzzy fault tree analysis using failure possibility[J]. Microelectronics and Reliability, 1993, 33(4): 583-597.

[81] F. S. Lai, S. Shenoi, T. L. Fan. Fuzzy fault tree analysis: theory and applications[J]. Engineering Risk and Hazard Assessment, 1986, 2: 117-138.

[82] 田士业．也谈数控车床的发展及应用[J]. 机床, 1991, 11: 11-13.

[83] 文广．我国数控机床可靠性的现状及对策[J]．机械研究与应用, 2003, 6: 5-6.

[84] 立式组合机床液压系统 (http://www.lunwen250.com/html/lw/qita/8515.html).

[85] 凌智勇．机床液压系统及故障维修[M]. 北京: 化学工业出版社, 2008.

[86] Y. Liu, H. Z. Huang. Reliability assessment for fuzzy multi-state systems[J]. International Journal of Systems Science, 2010, 41(4): 365-379.

[87] Y. Liu, H. Z. Huang, G. Levitin. Reliability and performance assessment for fuzzy multi-state elements[J]. Journal of Risk and Reliability, 2008, 222(4): 675-686.

[88] 张连文，郭海鹏. 贝叶斯网引论[M]. 北京: 科学出版社, 2006.

[89] H. Boudali, J. B. Dugan. A discrete-time Bayesian network reliability modeling and analysis framework[J]. Reliability Engineering & System Safety, 2005, 87(3): 337-349.

[90] H. Boudali, J. B. Dugan. A coutinuous-time bayesian network reliability modeling, and

analysis framework[J]. IEEE Transactions on Reliability, 2006, 55(1): 86-97.

[91] 石磊. 太阳翼驱动机构的可靠性分析[D]. 成都: 电子科技大学, 2011.

[92] 张华. 星载天线双轴定位机构的系统可靠性分析[D]. 成都: 电子科技大学, 2011.

[93] P. C. Li, G. H. Chen, L. C. Dai, et al. A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks[J]. Safety Science, 2012, 50(7): 1569-1583.

[94] C. A. Penz, C. A. Flesch, S. M. Nassar, et al. Fuzzy-Bayesian network for refrigeration compressor performance prediction and test time reduction[J]. Expert Systems with Applications, 2012, 39(4): 4268-4273.

[95] L. Ferreira, D. Borenstein. A fuzzy-Bayesian model for supplier selection[J]. Expert Systems with Applications, 2012, 39(9): 7834-7844.

[96] D. Dubois, H. Prade. Fuzzy sets and systems: theory and application[M]. New York: Academic Press, 1980.

[97] 黄洪钟. 机械系统故障树分析的一种新的模糊方法[J]. 机械科学与技术, 1994, 1: 1-7

[98] 赵艳萍，贡文伟. 模糊故障树分析及其应用研究[J]. 中国安全科学学报，2001，12(6): 81-87.

[99] 苗根蝉. WK 系列大型矿用挖掘机的电气调速和控制系统[J]. 露天采矿技术，2012，(4): 34-38, 41.

[100] 苗根蝉，刘晓星. WK-35 电铲的电气故障类型与自诊断系统[J]. 机械工程与自动化, 2010, (6): 125-127.

[101] 马兵. 变频技术在 WK35 矿用挖掘机上的应用[J]. 建筑机械, 2010, (1): 80-83.

[102] K. N. Fleming. A reliability model for common cause failures in redundant safety systems[C]. Proceedings of the 6th Annual Pittsburgh Conference on Modeling and Simulation, Pittsburgh, USA, 1975.

[103] J. K. Vaurio. Availability of redundant safety systems with common mode and undetected failures[J]. Nuclear Engineering and Design, 1980, 58(3): 415-424.

[104] K. N. Fleming, A. Mosleh, A. P. Kelley. On the analysis of dependent failures in risk assessment and reliability evaluation[J]. Nuclear Safety, 1983, 24(5): 637-657.

[105] A. Mosleh, N. O. Siu. A multi-parameter event-based common-cause failure model[C]. Proceedings of the 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, 1987.

[106] 金星，洪延姬，杜红梅. 共因失效系统的可靠性分析方法[M]. 北京: 国防工业出版社, 2008.

[107] 曹山根, 常玉国, 吴刚. 考虑共因失效的某发控系统可靠性分析[J]. 四川兵工学报, 2009, 30(11): 78-80.

[108] 王家序, 周青华, 肖科, 等. 不完全共因失效系统动态故障树模型分析方法. 系统工程与电子技术, 2012, 34(5): 1062-1067.

[109] 王学敏. 考虑共因失效的系统可靠性新模型[D]. 沈阳: 东北大学, 2005.

[110] 周忠宝. 基于贝叶斯网络的概率安全评估方法及应用研究[D]. 长沙: 国防科学技术大学, 2006.

[111] G. Levitin. Incorporating common-cause failures into nonrepairable multistate series-parallel system analysis[J]. IEEE Transactions on Reliability, 2001, 50(4): 380-388.

[112] A. Volkanovski, M. Čepin, B. Mavko. Application of the fault tree analysis for assessment of power system reliability[J]. Reliability Engineering & System Safety, 2009, 94(6): 1116-1127.

[113] L. Xing, A. Shrestha, L. Meshkat, et al. Incorporating common-cause failures into the modular hierarchical systems analysis[J]. IEEE Transactions on Reliability, 2009, 58(1): 10-19.

[114] D. Kancev. Limitations of explicit modeling of common cause failures within fault trees[C]. Proceedings of Annual Reliability and Maintainability Symposium (RAMS 2012), Reno, USA 2012.

[115] A. Das, M. A. Abdel-Aty. A combined frequency severity approach for the analysis of rear-end crashes on urban arterials[J]. Safety Science, 2011, 49(8-9): 1156-1163.

[116] J. F. Milho, J. A. C. Ambrósio, M. F. O. S. Pereira. Validated multibody model for train crash analysis[J]. International Journal of Crashworthiness, 2003, 8(4): 339-352.

[117] U.S. Department of Transportation, Federal Railroad Administration. 49 CFR Part 216 et al., Passenger equipment safety standards; Final Rule[Z]. USA, 1999.

[118] D. Tyrell. US rail equipment crashworthiness standards[J]. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 2002, 216(2): 123-130.

[119] D. Tyrell, K. J. Severson, B. J. Marquis. Crashworthiness of passenger trains[Z]. U.S. Department of Transportation, DOT/FRA/ORD-97/10, 1998.

[120] D. Tyrell, E. Martinez, K. Jacobsen, et al. Overview of a crash energy management specification for passenger rail equipment[C]. Proceedings of the IEEE/ASME Joint Rail Conference, 2006.

[121] American Public Transportation Association, Member Services Department, Manual of Standards and Recommended Practices for Passenger Rail Equipment[M], Issue of May 1,

2004.

[122] Association of American Railroads, Technical Services Division, Mechanical Section-Manual of standards and recommended practices, locomotive crashworthiness requirements[M], Standard S-580, Adopted 1989, Revised 1994, Revised 2005.

[123] D. Tyrell, K. Jacobsen, E. Martinez, et al. A train-to-train impact test of crash energy management passenger rail equipment: structural results[C]. Proceedings of ASME International Mechanical Engineering Congress and Exposition, Chicago, Illinois, USA, 2006.

[124] J. K. Vaurio. The probabilistic modeling of external common cause failure shocks in redundant systems[J]. Reliability Engineering & System Safety, 1995, 50(1): 97-107.

[125] J. K. Vaurio. Extensions of the uncertainty quantification of common cause failure rates[J]. Reliability Engineering & System Safety, 2002, 78(1): 63-69.

[126] J. K. Vaurio. Treatment of general dependencies in fault tree and risk analysis[J]. IEEE Transactions on Reliability, 2002, 51(3): 278-287.

[127] J. K. Vaurio. Common cause failure probabilities in standby safety system fault tree analysis with testing-scheme and timing dependencies[J]. Reliability Engineering & System Safety, 2003, 79(1): 43-57.

[128] J. K. Vaurio. Uncertainties and quantifications of common cause failure rates and probabilities for system analyses[J]. Reliability Engineering & System Safety, 2005, 90(2-3): 186-195.

[129] P. H. Kvam, H. F. Martz. Bayesian inference in a discrete shock model using confounded common cause data[J]. Reliability Engineering & System Safety, 1995, 48(1): 19-25.

[130] A. Mosleh. Common cause failures: an analysis methodology and examples[J]. Reliability Engineering & System Safety, 1991, 34(3): 249-292.

[131] M. Marseguerra, E. Padovani, E. Zio. The impact of the operating environment on the design of redundant configurations[J]. Reliability Engineering & System Safety, 1999, 63(2): 155-160.

[132] P. Dorre. Basic aspects of stochastic reliability analysis for redundancy systems[J]. Reliability Engineering & System Safety, 1989, 24(4): 351-375.

[133] P. Dorre. An event-based multiple malfunction model[J]. Reliability Engineering, 1987, 17(1): 73- 80.

[134] Z. Pan, Y. Nonaka. A new approach for reliability estimation of system with complex common cause failures[J]. International Journal of Reliability, Quality and Safety Engineering,

1994, 1(2): 291- 298.

[135] E. E. Lewis. A load-capacity interference model for common mode failures in 1-out-of-2: G systems[J]. IEEE Transactions on Reliability, 2001, 50(1): 47-51.

[136] J. Börcsök, S. Schaefer. Estimation and evaluation of common cause failures[C]. Proceedings of the 2nd International Conference on Systems, Martinique, French, 2007.

[137] J. Mi, Y. F. Li, H. Z. Huang, et al. Reliability analysis of multi-state systems with common cause failure based on Bayesian networks[C]. International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE 2012), Chengdu, China, 2012.

[138] 周金宇，谢里阳. 多状态系统共因失效机理与定量分析[J]. 机械工程学报，2008，44(10): 77-81.

[139] 李志忠. 工业工程与管理[J]. 列车追尾事故的故障树分析兼谈复杂系统安全, 2011, 16(4): 1-8.

在学期间参与的项目研究

[1] 国家自然科学基金项目：复杂机械系统认知不确定性量化理论和可靠性分析方法研究，项目编号：51075061

[2] 国家自然科学基金项目：基于可能性和证据理论的机械系统可靠性分析和设计优化，项目编号：50775026

[3] 国家 863 计划项目：数据不足时的重大装备可靠性分析与设计技术，项目编号：2007AA04Z403

[4] 高档数控机床与基础制造装备国家科技重大专项课题“高速龙门五轴加工中心（AC 摆角），课题编号：2009ZX04002-013”子课题：高速龙门五轴加工中心整机可靠性研究。

[5] 国家国防科工局航天产品高可靠长寿命专题项目：长寿命 XX 机构可靠性量化设计技术研究，项目编号：4.1.3

[6] 国家 863 计划项目“75 立方米大型露天矿用挖掘机研制，课题编号：2012AA062001”子课题：大型矿用挖掘机可靠性分析及设计关键技术研究。

攻读博士学位期间取得的成果

[1] YF Li, HZ Huang, H Zhang, et al. Fuzzy sets method of reliability prediction and its application to a turbocharger of diesel engines[J]. Advances in Mechanical Engineering, 2013, Article ID 216192, 7 pages. (SCI 收录)

[2] YF Li, , HZ Huang, Y Liu, et al. A new fault tree analysis method: fuzzy dynamic fault tree analysis[J]. Maintenance and Reliability, 2012, 14(3): 208-214. (SCI 收录)

[3] YF Li, J Mi, HZ Huang, et al. System reliability modeling and assessment for solar array drive assembly based on bayesian networks[J]. Maintenance and Reliability, 2013, 15(2): 117-122. (SCI 收录)

[4] YF Li, HZ Huang, SP Zhu, et al. An application of fuzzy fault tree analysis to uncontained events of an areo-engine rotor[J]. International Journal of Turbo and Jet Engines, 2012, 29(4): 309-315. (SCI 收录)

[5] YF Li, J Mi, HZ Huang, et al. Fault tree analysis of train rear-end event considering common cause failure[J]. Maintenance and Reliability, 2013, 15(4): 312-318. (SCI 收录)

[6] YF Li, HZ Huang, Y Liu, et al. A novel dynamic fault tree analysis method[C]. International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE2013), Emeishan, China, 2013. (EI 收录)

[7] 李彦锋, 杜丽, 肖宁聪, 等. 汽车驱动桥系统模糊故障树分析研究[J]. 西安交通大学学报, 2009, 43(7): 110-114. (EI 收录)

[8] HZ Huang, YF Li, Y Liu, et al. Posbist reliability theory of k-out-of-n：G system[J]. Journal of Multiple-Valued Logic and Soft Computing, 2010, 16(1-2): 45-63. (SCI 收录)

[9] 黄洪钟, 李彦锋, 孙健, 等. 太阳翼驱动机构的模糊动态故障树分析. 机械工程学报, 2013, 49(19): 70-76. (EI 收录)

[10] Y Liu, YF Li, HZ Huang, et al. Optimal preventive maintenance policy under fuzzy Bayesian reliability assessment environments[J]. IIE Transactions, 2010, 42(10): 734-745. (SCI 收录)

[11] NC Xiao, YF Li, Z Wang, et al. Bayesian reliability estimation for deteriorating systems with limited samples using the maximum entropy approach. Entropy, 2013,

15(12): 5492-5509. (SCI 收录)

[12]J Mi, YF Li, HZ Huang, et al. Reliability analysis of multi-state system with common cause failure based on Bayesian networks[J]. Maintenance and Reliability, 2013, 15(2): 169-175. (SCI 检索)

[13]肖宁聪, 李彦锋, 黄洪钟. 卫星太阳翼展开机构的可靠性分析方法研究[J]. 宇航学报, 2009, 30(4):1704-1710. (EI 检索)

[14]黄洪钟, 李彦锋, 孙健, 等. 一种面向备份结构的故障树分析方法. 中国, 发明专利, 专利号: 201110458160.7

[15]李彦锋（9/15）. FMECA 和 FTA 中的若干新方法及其应用. 国防科技奖三等奖, 2012

[16]李彦锋（4/15）. 基于故障物理的航空发动机典型零部件寿命预测新方法. 四川省国防科工办鉴定成果, 2012