面向复杂工程系统的安全分析研究综述

王德琳 [1] 张 可 [1] 朱哲人 [2, 3] 陈小龙 [1] 陈志文 [4] 蒋朝辉 [4] 柴 毅 [1] 宋执环 [3]

摘 要 面向工程系统运行安全的分析技术对于提升风险感知、预防潜在安全事故发生、保障系统安全可靠运行具有重要意义. 然而, 随着工程系统功能与结构的复杂化、内部组件之间非线性相互作用的日益增强, 其运行过程中的安全分析往往面临着安全事件难以系统识别、评估指标难以准确选取、风险传播机制难以清晰刻画、安全边界难以有效量化等诸多挑战. 为此, 本文系统地梳理复杂工程系统运行过程中安全的定义及其内涵, 阐述安全分析的整体实施框架, 全面回顾和总结有关安全事件分析、评估指标选取、事故模型构建及安全区域刻画等方面的研究进展, 并对该领域未来的发展趋势与研究方向进行探讨.

关键词 运行安全; 安全分析; 复杂工程系统; 风险评估; 安全控制

引用格式 王德琳, 张可, 朱哲人, 陈小龙, 陈志文, 蒋朝辉, 柴毅, 宋执环. 面向复杂工程系统的安全分析研究综述. 自动化学报, 2026, **52**(4): 611−637

DOI 10.16383/j.aas.c250493 **CSTR** 32138.14.j.aas.c250493

An Overview of Safety Analysis for Complex Engineering Systems

WANG De-Lin[1] ZHANG Ke[1] ZHU Zhe-Ren[2, 3] CHEN Xiao-Long[1] CHEN Zhi-Wen[4]
JIANG Zhao-Hui[4] CHAI Yi[1] SONG Zhi-Huan[3]

Abstract Safety analysis plays a pivotal role in enhancing risk perception, preventing potential accidents, and assuring the reliability and safety of the entire engineering system. However, with the progressive increase in complexity and integration of modern engineering systems, the interactions within their components are inherently intensifying. The examination of risk accidents, selection of evaluation metrics, identification of risk transmissions, and characterization of safety boundaries for complex engineering systems all pose significant challenges. For these challenges, this paper presents an introductory overview on the development of safety analysis for complex engineering systems. The definition and connotation of safety are elucidated, along with the specific implementation process of quantitative assessment. Afterward, key references are provided for which interested readers can obtain more detailed information on risk analysis, metric determination, accident modeling, safety region representation, and so forth. Finally, some critical issues are discussed as open problems for future research directions in this emerging field.

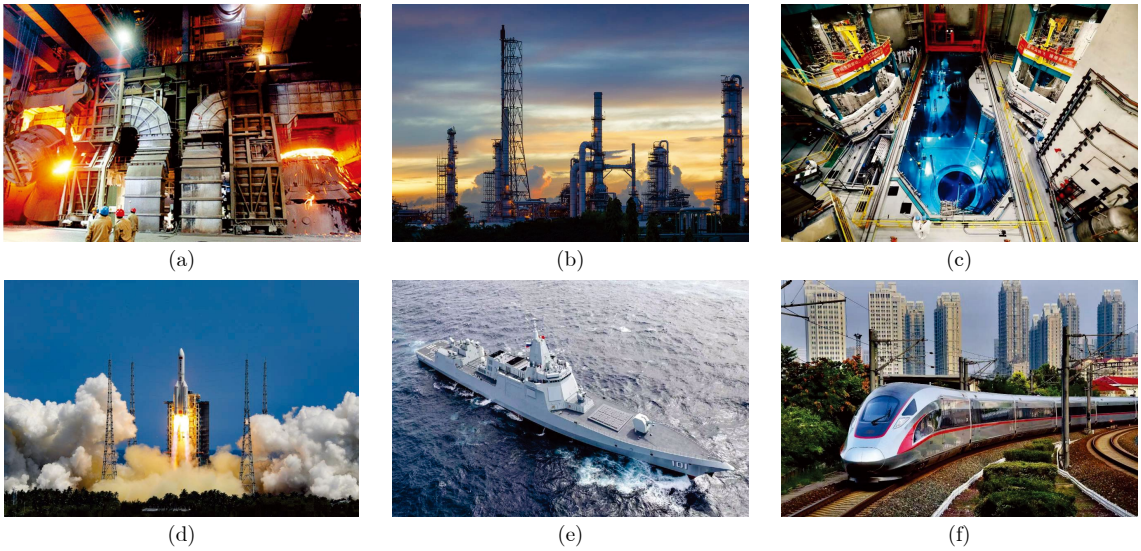
Keywords operational safety; safety analysis; complex engineering systems; risk assessment; safety control

Citation Wang De-Lin, Zhang Ke, Zhu Zhe-Ren, Chen Xiao-Long, Chen Zhi-Wen, Jiang Zhao-Hui, Chai Yi, Song Zhi-Huan. An overview of safety analysis for complex engineering systems. *Acta Automatica Sinica*, 2026, **52**(4): 611−637

收稿日期 2025-09-23 录用日期 2026-01-12
Manuscript received September 23, 2025; accepted January 12, 2026
国家自然科学基金 (62573072, 62403416, 62173349, U2034209, 61633005), 中央高校基本科研业务费 (2024CDJGF-022), 重庆市技术创新与应用发展专项项目 (CSTB2025TIAD-GPX0001) 资助
Supported by National Natural Science Foundation of China (62573072, 62403416, 62173349, U2034209, 61633005), Fundamental Research Funds for the Central Universities (2024CDJGF-022), and Chongqing Technological Innovation and Application Development Foundation (CSTB2025TIAD-GPX0001)
本文责任编委 刘毅
Recommended by Associate Editor LIU Yi
1. 重庆大学自动化学院 重庆 400044 2. 杭州师范大学数学学院 杭州 311121 3. 浙江大学控制科学与工程学院 杭州 310027 4. 中南大学自动化学院 长沙 410083
1. School of Automation, Chongqing University, Chongqing 400044 2. School of Mathematics, Hangzhou Normal University, Hangzhou 311121 3. College of Control Science and Engineering, Zhejiang University, Hangzhou 310027 4. School of Automation, Central South University, Changsha 410083

工程系统广泛存在于现代化工业体系中, 其范畴既涵盖冶金、化工、核电等大型工业过程, 也包括运载火箭、舰船、高速列车等典型装备系统, 如图 1 所示. 这些工程系统既是支撑国家关键基础设施的核心载体, 也是构筑国家支柱产业体系、推动国民经济发展的重要组成部分[1−3].

随着我国经济的快速发展, 工程系统在信息技术革命和工业自动化浪潮的推动下, 呈现出规模持续扩张、结构日益复杂、设备组件之间功能耦合不断紧密的发展趋势[4]. 复杂的逻辑结构和交互关系使工程系统在面临风险事件时稳定性急剧下降. 系统中任意功能单元的局部失效, 均可以通过紧密交织的信息或能量流动网络, 蔓延和扩散至其他与之关联的设备、单元乃至子系统. 这种层级式的失效



(a) (b) (c)

(d) (e) (f)

图 1 典型的复杂工程系统 ((a) 冶金系统; (b) 化工系统; (c) 核电系统; (d) 运载火箭; (e) 大型远洋舰船; (f) 高速列车)

Fig. 1 Typical complex engineering systems ((a) Metallurgical systems; (b) Chemical industry systems; (c) Nuclear power systems; (d) Rockets; (e) Large ocean-going vessels; (f) High-speed trains)

传播导致初始失效的后果不断累积、影响范围不断扩大, 并最终演变成引发系统运行中断且难以快速恢复的灾难性事故[5].

据 EW-DAT 数据库 2000—2024 年间全球 5855 起工业事故的统计分析显示, 复杂工程系统中的各类安全事故均造成不同程度的经济损失和人员伤亡, 如图 2 所示. 因此, 为避免事故发生并确保系统安全稳定运行, 安全分析作为能够实时评估系统状态、鉴别潜在风险与安全隐患的有效途径, 已成为当前的研究热点.

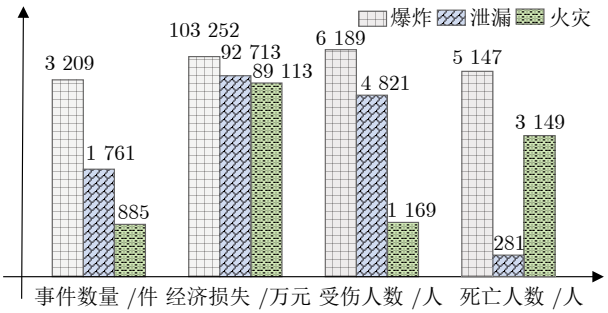


图 2 2000—2024 年的事故统计结果

Fig. 2 Statistical results of accidents from 2000 to 2024

为此, 本文面向复杂工程系统的安全分析研究展开综述. 首先, 对复杂工程系统运行安全的理论基础及其实施流程框架进行系统性分析与概述. 随后, 围绕实施流程框架, 对现有安全事件分析、评估指标选取的研究成果进行介绍, 对基于事故模型及安全域的安全量化评估方法进行分类梳理与归纳. 最后, 结合现有研究不足, 讨论复杂工程系统安全分析领域亟待解决的关键问题, 并展望未来的研究方向.

1 概述

本节对安全及其相关概念进行系统性的梳理与界定, 并给出适用于不同复杂工程系统的安全分析实施流程框架. 该框架从安全事件分析、测量指标选取及模型构建等环节出发, 为后续各节中所涉及的现有方法与研究进展综述提供明确的流程指引与结构性支撑.

1.1 安全和风险的定义

根据美国国防部颁布的第五代系统安全标准 (MIL-STD-882E), 安全被定义为免于导致死亡、伤害、职业疾病、设备损伤、财产损失及环境损害的状态[6]. 而参照国际电工委员会 (International Electrotechnical Commission, IEC) 和国际标准化组织 (International Organization for Standardization, ISO) 发布的 IEC 61508-1 和 ISO/IEC Guide 51:2019 标准, 安全被描述为系统、设备或过程在特定运行条件下运行时免于导致人员伤亡、设备损伤、环境破坏或资产损失的特性[7−8]. 此外, Leveson[9] 和 Hollnagel[10] 从系统防御的角度出发, 将安全视为系统通过预防性或防护性措施, 将系统风险控制在可接受水平, 并防止不期望事件或事故发生的能力. 由于系统安全与风险之间呈现显著的负相关关系, 风险常被视为安全的另一种度量或表征形式. 相应地, 风险评估也被视为安全分析的另一种重要途径

或核心手段.

如图 3 所示, 当系统面临的风险水平较低时, 这意味着其整体运行状态是较为安全的; 相反, 系统越不安全, 其所需要承担的潜在风险水平就越高[11]. 而在不同的研究领域及实际工程应用中, 研究者也从各自的角度出发, 对系统的风险进行多层次的理解与阐述, 并提出多种不同的定义方式, 如表 1 所示. 通常, 在风险评估中可以将其统一地表示为二元组 $R_q=(s_q,\ p_q)$ 或三元组 $R_q=(s_q,\ p_q,\ c_q)$ 的形式. 其中, s_q 表示可能发生的第 q 种安全事件; p_q 表示该事件可能发生的概率; c_q 表示该事件可能导致后果的严重程度; $q=1,\ 2,\ \cdots,\ Q$, Q 为安全事件的总数.

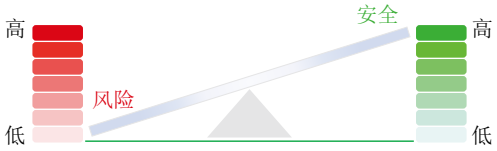


图 3　安全与风险之间的关系

Fig. 3　Relationship between safety and risk

为对风险发生的概率 p_q 与严重程度 c_q 进行定量计算, 文献 [12−13] 从外部环境、行为主体等 7 个不同的维度出发, 梳理影响风险发生概率和严重程度的主要因素, 如表 2 所示. 其中, “多层级的主体构成”、“跨层级决策的协调失衡”、“外部环境压力对运营决策的偏向性影响”等 3 类要素, 主要用于反映由政策制定、组织管理、市场竞争等社会管理机制所驱动的风险. 这些要素已被系统理论分析模型 (system theoretic accident modeling and process model, STAMP)[14]、AcciMap[15] 及系统理论过程分析 (system theoretic process analysis, STPA)[16] 等风险评估方法纳入至评估框架体系之内, 面向多层级组织及跨部门协调运营的复杂场景, 通过垂直整合不同社会层级和决策主体的交互机制, 分析并揭示不同要素对风险事件的影响[17].

与上述以社会管理机制为主导研究不同的是, 本文聚焦于复杂工程系统运行过程中, 与结构特征、组件耦合关系及状态演化机制等密切相关的系统性风险. 专注于与系统本体运行状态相关的 4 类风险要素, 即“风险的持续累积”、“多源风险因素的耦合效应”、“新型风险的持续涌现”及“安全防护机制的功能性退化”, 提出一种适用于不同复杂工程系统的安全分析框架.

1.2　实施流程框架

面向复杂工程系统的安全分析, 其核心步骤可以被归纳如下:

1) 安全事件分析. 安全事件是最能反映复杂工程系统安全特性的认知性依据, 通常指系统运行过程中突然发生的、对人员健康造成伤害、对设备设施造成破坏, 并可能导致运行暂时中断或永久终止的意外事件. 受系统功能属性、运行机制及所处环境差异的影响, 安全事件因工程系统的不同而各具特色. 针对安全事件进行识别与分析, 并深入剖析其中蕴含的关键因素, 是理解系统安全特性与风险机制的关键步骤.

2) 评估指标选取. 安全是一种具有主观性的抽象属性, 难以通过直接手段进行测量, 只能依托于一系列与系统密切相关的测量参数进行间接衡量. 类似于医学中的发热诊断, 医生无法直接测量到“发烧”这一主观生理状态, 但却可以通过体温等体征参数来对病人是否“发烧”加以判断. 因此, 面向不同的复杂工程系统, 针对不同安全事件的风险特性, 选取能够有效表征或衡量系统安全状态的评估指标, 也是安全分析中的重要步骤之一.

3) 安全量化评估. 根据不同的安全评估指标, 可进一步展开系统安全状态的量化评估. 针对复杂系统在安全状态表征方面的不同需求, 本文将现有的安全量化评估方法划分为基于事故模型的方法和基于安全域的方法. 其中, 基于事故模型的方法考虑了表 2 中所列的“风险的持续累积”、“多源风险因素的耦合效应”及“新型风险的持续涌现”等 3 类关键要素. 结合专家知识或历史运行数据, 建立评估指标与安全状态之间的映射关系, 形成能够对事故传播及其演化机制进行规律性表征的事故模型, 并展开相应的量化计算与评估分析. 由于基于事故模型的方法能够有效地捕捉复杂工程系统中事故的

表 1　风险的定义

Table 1　Definitions of risk

序号	定义	侧重	文献
1	风险为某种特定场景下可能产生的预期损失	侧重于从经济损失的角度对风险进行描述	[18]
2	风险是指在特定时期或特定情况下, 事件产生特定影响的可能性	侧重于描述风险发生的概率	[19]
3	风险是指与生命以及社会价值相关的不确定后果	侧重于描述风险所造成后果的严重程度	[20]
4	风险是衡量事故产生特定影响与后果的有效指标	侧重于描述风险发生概率与严重程度之间的共同作用	[21]

传播路径及阶段性演化特征, 因此适用于分析事故形成机理、识别长期风险累积, 并为其制定相应的预防性措施. 相比之下, 基于安全域的方法从“安全防护机制的功能性退化”角度出发, 通过系统评估指标的相关额定约束, 界定系统在不同标称工况下的状态边界与可行运行空间, 并进一步考虑随时间演变的轨迹约束, 描述维持安全运行的时变可行区域. 这类方法通过表征安全域, 对系统状态的可达范围与安全裕度进行明确, 能够为系统运行的可控范围提供准确的判断依据. 因此, 适用于需要进行即时决策或动态轨迹优化的应用场景.

在明确了安全分析的整体实施流程与系统框架后, 后续各节将围绕该框架的各个关键步骤, 对已有的研究方法与技术进展展开论述. 各节内容之间的逻辑关系如图 4 所示.

2 安全事件分析与评估指标选取现有方法与进展

目前, 安全事件的识别与分析在实际工程中仍主要依赖于行业专家长期积累的经验知识. 通过对系统结构、运行流程及历史安全事件的理解, 专家

表 2 风险的 7 项要素

Table 2 Seven elements of risk

序号	要素	描述	要素在风险评估中的指导准则
1	多层级的主体构成	风险的产生受到社会治理体系中多层级主体的共同影响. 例如, 制定国家政策的政治家、主导企业制度构建的公司经理及一线操作人员等	应识别与风险相关的所有行为主体, 而不仅仅局限于直接参与执行的操作人员
2	跨层级决策的协调失衡	不同层级主体在职责定位或利益诉求上的错位性差异, 极易引发决策过程中的协调失衡	应重视并促进各层级主体之间的信息共享与认知协同, 从而就潜在风险达成共识性理解
3	外部环境压力对运营决策的偏向性影响	激烈的市场竞争迫使公司决策者倾向于关注公司的短期运营表现, 而对系统安全等长期保障因素关注不足	应针对性地考虑可能干扰决策者判断的外部环境压力
4	风险的持续累积	在复杂工程系统长期运行过程中, 微小的风险因未能被及时排除而持续累积, 并最终在无显著外部扰动的情况下逼近或突破安全阈值	应准确鉴别系统内部的安全薄弱环节及其演化累积路径, 构建基于系统安全临界状态的早期预警机制与主动干预措施
5	多源风险因素的耦合效应	复杂工程系统中的风险通常源于系统内部多层级风险之间的非线性交互与动态耦合, 难以通过风险因素的线性叠加予以刻画	应全面考虑系统内部同一层级及跨层级组件之间潜在的风险因素及其耦合关系, 而非聚焦于单一的突发性风险或孤立的异常行为
6	新型风险的持续涌现	复杂工程系统在长期运行过程中可能涌现出未曾预见的新型风险	应尽可能地考虑和包含所有的风险, 并具备对未知风险的自适应感知与动态更新能力
7	安全防护机制的功能性退化	受设备老化、部件磨损、性能漂移及环境干扰等影响, 而出现的冗余设计失效、报警阈值下降及安全裕度持续收窄等防护机制退化现象	应针对系统的安全裕度变化进行分析与感知, 以识别系统安全防护机制的退化程度

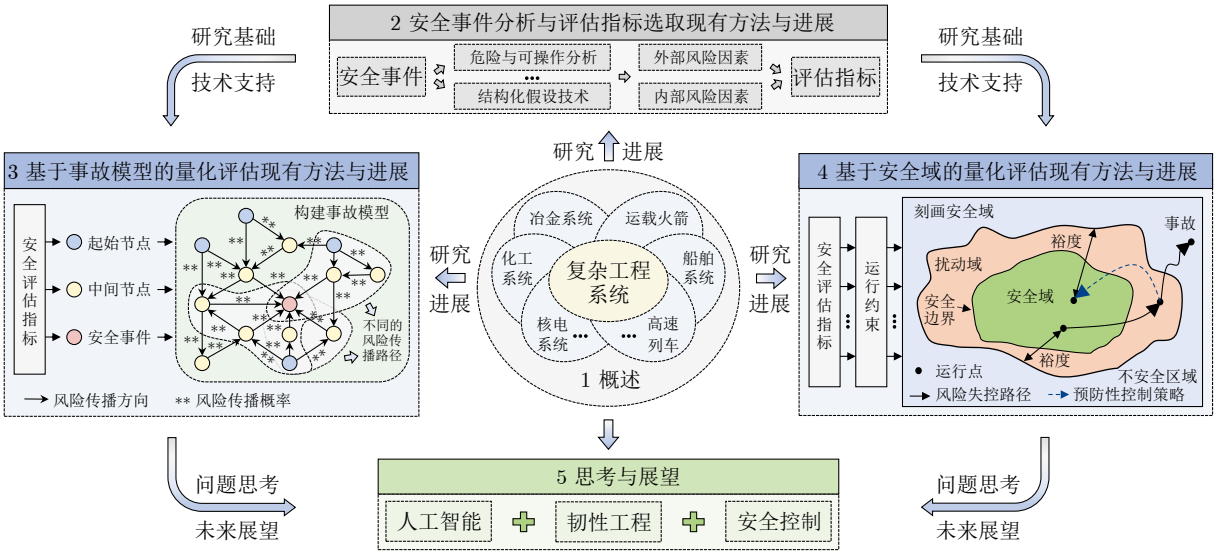


图 4 本综述各节之间的逻辑关系

Fig. 4 Interrelationships between each section of this overview

能够对系统所面临的潜在风险及其影响因素进行定性判断与归纳分析. 由此, 逐步衍生出一系列以专家知识为核心的安全事件分析方法, 如危险与可操作性分析 (hazard and operability analysis, HAZOP)、故障模式与影响分析 (failure mode and effect analysis, FMEA) 及结构化假设技术 (structured what-if technique, SWIFT) 等[22]. 其中, HAZOP 以一系列预设的引导词为基础, 围绕系统操作过程中可能出现的潜在偏差进行逐项分析, 并通过专家集体研讨的方式识别潜在的系统风险事件与诱因, 提炼出系统的安全事件[23]. FMEA 依托于专家对系统构成和功能层次的理解认识, 逐层识别可能的系统风险, 并结合风险发生严重性对系统风险进行优先级排序, 为确认与分析具有代表性的安全事件提供依据[24]. SWIFT 则通过“假如 $\cdots$ ”的形式化提问, 引导专家对系统运行过程中的不确定场景展开思考, 并据此梳理潜在的风险事件及其诱因, 形成包含潜在风险、风险成因及决策建议的清单[25].

针对不同类型的安全事件与潜在风险, 借助 HAZOP、FMEA 及 SWIFT 等方法识别的风险成因通常被归纳为两大类: 外部风险因素与内部风险因素. 其中, 外部风险因素主要指源自于系统所处运行环境且系统本身难以规避的影响因素, 通常包括系统运行时所处的极端天气、极端环境、执行任务的复杂性 (如超远距离航行或飞行任务) 以及与人为因素相关的操作偏差 (如操作人员疲劳、安全规章制度执行不力) 等. 因此, 其评估指标往往围绕环境感知与人因监测展开. 例如, 在船舶动力系统中, 常常采用水深声呐、风速计等环境感知设备获取外部运行环境的实时数据, 并引入船员的生理监测数据 (如心率、疲劳度及其反应时长等) 来对其精神状态及操作稳定性进行实时监测与反映.

另一方面, 内部风险因素主要源于系统自身的结构复杂性、子系统之间的高度耦合关系及关键设备部件的运行状态等. 例如, 高精度传动设备在长期高强度、高负荷工作条件下所展现出的性能退化及设备故障等, 均属于内部风险因素的范畴. 而针对系统内部风险因素的监测及其安全状态的感知, 则主要依赖于系统本体的传感器数据支持, 如设备部件对应的电流、电压、温度、振动和压力等. 表 3 归纳了典型复杂工程系统的各类安全事件, 并系统梳理了其对应的内/外部风险因素及相应的安全评估指标.

3 基于事故模型的量化评估现有方法与进展

基于事故模型的方法通过挖掘复杂工程系统同一层级及跨层级组件之间的依赖关系, 综合考虑一系列相互关联、相互影响的安全指标与风险因素, 构建出能够反映事故累积过程及其动态传播规律的结构化模型. 由于其构建的模型能够有效地表征复杂工程系统中事故演变的内部拓扑关系及其对外行为特征, 为后续系统风险的量化计算与评估分析提供科学依据. 因此, 近几十年来, 基于事故模型的安全量化评估方法得到了不同领域研究人员的广泛关注.

基于建模的不同形式与考虑, 该类方法可以被划分为传统的方法、基于级联失效故障的方法及基于图的方法. 在本节中, 将围绕 3 类方法的核心思想展开描述, 归纳现有研究进展, 并对其各自的实际应用场景进行深入讨论.

3.1 传统的方法

基于事故模型的传统方法包括故障树 (fault tree, FT)、事件树 (event tree, ET) 和领结分析 (bow-tie, BT). 这些方法依赖于专家对复杂工程系统结构、风险要素、潜在故障模式及失效逻辑关系的理解和认识, 通过形式化的逻辑表达构建事故模型. 得益于模型明确的逻辑性、可解释性及良好的工程适用性, 这些方法在当前不同复杂工程系统的安全量化评估中被广泛地使用.

3.1.1 故障树

故障树由贝尔实验室的 H. Watson 于 1961 年首次提出并应用于洲际导弹发射控制系统的安全评估. 作为一种自上而下的系统安全分析工具, 故障树从顶层失效事件出发, 通过布尔逻辑对其进行逐层拆解, 识别并分析出可能导致系统风险的多种底层风险因素, 形成包含不同风险路径的树形结构. 一个典型的故障树由顶层事件、中间事件、基本事件、逻辑门和连接路径组成, 如图 5 所示. 其中, 位于底层的基本事件反映系统运行过程中最基本的风险因素; 中间事件和顶层事件由基本事件通过逻辑门组合而成; 逻辑门用于描述事件之间的逻辑关系, 常见的逻辑门包括“与”门和“或”门, 分别表示当且仅当所有输入事件同时发生时才会触发输出事件, 以及只要任意一个输入事件发生即可导致输出事件的发生[26].

基于上述原理构建的传统故障树模型, 通常被称为静态故障树. 由于无法有效表征系统状态迁移和时序约束等动态行为, 静态故障树适用于耦合关系明确、运行条件稳定的静态系统安全分析, 即, 针对在整个生命周期中, 始终运行在单一标称工况下的系统进行分析. 而随着现代工程系统额定标称工

表 3 面向典型复杂工程系统的安全事件分析

Table 3 Safety events analysis for typical complex engineering systems

	安全事件	外部风险因素	内部风险因素	评估指标	文献
冶金系统	尾矿库溃坝、高温熔融金属泄漏爆炸、瓦斯爆炸、粉尘爆炸火灾、煤气中毒、机械伤害、高空坠落、钢包掉落、其他	环境因素: 自然灾害 (海啸、洪水、地震、泥石流、火山爆发等)、地下水位变化、雷暴与雷电等 人为因素: 第三方施工干扰、供应原料质量缺陷、维修保养不当、设备巡检不足、操作人员违规操作等	高炉缸侵蚀、高炉悬料、热风炉烧损、转炉/电炉故障、连铸系统故障、钢包运输系统机械损坏、轧制设备故障、热处理故障、通风系统故障、除尘系统故障等	可燃气体浓度 (煤气、硫化氢、甲烷等)、高炉炉壁厚度、高炉炉龄、炉温、炉压、铁水温度、煤气柜压力、粉尘浓度、烟气排放浓度、尾矿坝浸润线、操作人员日常行为记录、视频监控采集系统等	[27−29]
化工系统	火灾/爆炸、有毒气体泄漏、机械伤害、反应失控、其他	环境因素: 建筑环境恶劣、通风不良、自然灾害 (海啸、洪水、地震、泥石流、火山爆发等)、外部公用设施中断等 人为因素: 人员缺乏安全意识、缺乏专职安全管理人员、人员未经培训或不符合标准等	系统设计缺陷、未评估设备/工艺风险、化学品存储不当、反应釜过热或超压、阀门故障、离心机故障、管道腐蚀或泄漏、压力容器失效等	反应釜压力、反应釜温度、换热器压力、有毒气体浓度 (一氧化碳、氨气、氯气等)、泵轴承振动信号、离心机转子振动信号、粉体输送管道静电聚集强度、换热器内部腐蚀速率、工作人员操作日志等	[30−32]
核电系统	反应堆停堆、核反应失控、不同回路的冷却失效、核辐射暴露、放射性气体意外排放、机械伤害、蒸汽爆炸、其他	环境因素: 极端天气 (暴雪、干旱等)、自然灾害 (海啸、洪水、地震、泥石流、火山爆发等)、海平面上升、外部公用设施中断等 人为因素: 维护或检查疏忽、应急响应不力、应急处置能力差、人员培训不足等	系统设计缺陷、冷却系统故障、蒸汽发生系统故障、冷凝系统故障、汽轮机故障、稳压器故障、控制棒故障、辐射屏蔽失效等	冷却剂流量、冷却剂 (进/出口) 温度、蒸汽发生器水位、稳压器压力、控制棒插入深度、汽轮机转速、堆芯出口温度、燃料包壳温度、放射性气体浓度、堆芯损坏频率、运行日志等	[33−34]
运载火箭	高空解体、坠毁爆炸 (并造成弹片和毒气散逸)、载荷掉落、失控、发动机关机、部件损毁、卫星未入轨、其他	环境因素: 高空风、雷暴与雷电、强风、大雾、地磁暴、地震、太阳耀斑、低轨空间碎片等 人为因素: 操作失误、维修保养不当、空域管制延误、外部供应链质量缺陷、发射流程执行偏差等	地面发射设备故障、推进剂加注系统故障、测控与通信系统故障、内部结构材料疲劳老化、发动机设计缺陷、燃烧室压力波动、控制系统故障、传感器信号失真、热防护系统失效、焊接装配失误、软件系统故障等	冲击加速度、发动机推力、推进剂量、入轨精度 (轨道高度、倾角、偏心率)、姿控精度 (俯仰角、偏航角、滚转角等偏差)、地面安全半径影响范围、火箭结构系数、弹道偏差、工作人员操作日志等	[35−39]
船舶系统	船只碰撞、船只搁浅、船只触礁、船只沉没、火灾/爆炸、风灾、其他	环境因素: 航行海域、离港距离、极端天气 (气旋、寒潮、海雾、冰雹等)、风向、风速、浪高等 人为因素: 船舶人员配置不齐、海员严重疲劳、海员缺乏航海理论知识、海员航海经验欠缺等	船只类型、船只吨位、船体结构疲劳、推进系统故障、增压系统故障、起动系统故障、配气机构故障、汽轮机故障、光伏组件故障、活塞泵故障等	船体吃水深度、液压系统压力、燃油供给压力、螺旋桨轴系振动信号、螺旋桨推力、燃油温度、燃油喷射压力、液压油温度、航行效率、船体横倾度、船体纵倾度、船员生理监测数据等	[40−42]
高速列车	列车脱轨、列车碰撞、列车车体断裂、列车爆炸、其他	环境因素: 极端天气 (高温、暴雨、冻雨、沙尘暴、强横风、大雾等)、轨道结冰或积雪等 人为因素: 驾驶员疲劳或操作失误、维护检修不到位或失误、第三方施工干扰、信号调度错误、违规占用线路或道口等	焊接或连接件缺陷、车体结构疲劳、牵引变流器故障、牵引电机故障、闭锁结构故障、制动系统故障、转向架故障、供电系统故障、列车管理系统缺陷或通信丢包等	轨道温度、轨道几何参数、制动缸压力、制动响应时延、平均制动距离、转向架振动信号、牵引电机电流/扭矩、接触网电压、变流器温度、驾驶员生理监测数据、操作行为记录等	[43−45]

况的不断增多、运行参数显著的时变特性, 要求故障树从静态向动态进行转变. 于是, 研究者通过引入具有时序特征和依赖关系的动态逻辑门, 包括功能依赖门 (functional dependency, FDEP)、冷/热备用门 (spare component management, SPARE)、优先级与门 (priority-AND, PAND) 和顺序相关门 (sequence enforcing, SEQ) 等, 来增强动态故障树 (dynamic fault tree, DFT) 对系统时变行为的刻画能力[46]. 此外, 为进一步应对工程系统中广泛存在的空间相关性及多状态动态演化等复杂特性, 空间故障树 (space fault tree, SFT)[47]、状态事件故障树 (state event fault tree, SEFT)[48] 等变体被相继提出.

构建故障树之后, 研究者倾向于将最小割集 (minimal cut set, MCS) 与故障树相结合, 用于风险的量化计算与分析. 其基本思想是将故障树中复杂的树状逻辑结构转化成若干失效逻辑的组合, 进而识别导致系统顶层事件发生的最小基本事件集. 当基本事件相互独立时, 可通过计算最小割集内各基本事件发生概率的乘积, 得到该最小割集的发生

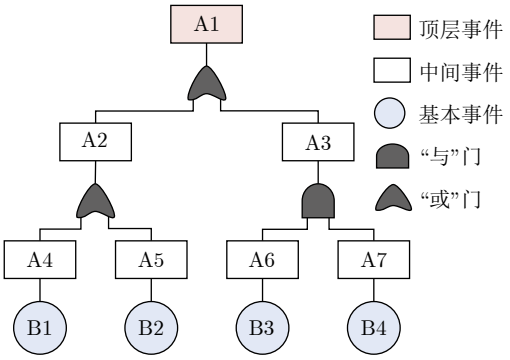


图 5　故障树示意图

Fig. 5　Schematic diagram of fault tree

概率. 随后, 基于包含–排除原理, 对所有最小割集的联合概率进行求解, 得到系统顶层事件的整体失效概率[49].

随着系统复杂性的提升, 割集数量的急剧增加使得最小割集的直接搜索与完全识别变得异常困难. 为应对这一挑战, Reay 等[50] 利用二元决策图 (binary decision diagram, BDD) 将故障树分解为若干结构独立的逻辑子树, 并基于子树进行最小割集的探寻, 有效避免了传统最小割集搜寻过程中的组合爆炸问题. Remenyte-Prescott 等[51] 在传统二元决策图 0-1 分支的结构基础上, 引入共识分支的概念, 提出名为三元决策图 (ternary decision diagram, TDD) 的方法. 该方法通过共识分支扩展节点的状态表述能力, 提升了故障树中最小子集的搜索效率. 与此同时, 二元决策图和三元决策图还能将故障树映射成一个有向无环图 (directed acyclic graph, DAG), 并结合变量排序和图节点共享, 将简化后的最优逻辑结构用于风险计算. 此外, 其他研究还致力于将故障树映射成等效的马尔科夫链[52–53]、Petri 网[54–55] 或贝叶斯网络[56–57] 等, 并根据其系统组件行为的指数或概率分布对其进行量化计算与评估.

总体而言, 基于故障树的方法因其建模过程直观、逻辑结构清晰及工程可操作性强, 已被广泛应用于航空航天、化工生产等复杂工程系统的安全分析当中. 然而, 故障树的评估有效性强烈依赖于逻辑门隐含的独立性假设以及对基本失效概率的准确估计. 对于复杂工程系统而言, 低频发生的安全事件及有限的运行数据使得统计方法在为故障树提供基本失效概率时存在较大的不确定性. 这种不确定性在故障树的推理分析过程中将被逐层放大, 并最终导致顶层风险评估结果偏离实际状况. 因此, 结合先进的联邦学习算法, 实现跨系统的数据共享与知识融合, 发展能够应对数据稀缺及参数不确定性的故障树模型, 并将其用于安全评估与分析, 是后续亟需研究的方向.

3.1.2　事件树

事件树是一种典型的归纳分析技术, 起源于 1975 年美国核安全研究项目 WASH 1400 期间. 事件树通常以明确的初始事件 (系统故障、设备失效及人员误操作等) 为起点, 按照时间或逻辑顺序, 依次分析各项安全防护措施在事故演化过程中的响应情况. 由于每项防护措施的响应均存在成功或失败两种状态, 事件树由此形成多条不同的分支路径. 沿分支路径逐步展开分析, 即可全面探寻并揭示初始事件在不同响应条件下的事故演化路径及其潜在后果. 以核电系统为例, 图 6 所示的事件树以小破口失水事故 (small break loss of coolant accident, SBLOCA) 为起点, 依次分析高压加注系统 (high pressure injection system, HPIS)、安注箱系统 (accumulator, ACC) 和低压加注系统 (lower pressure injection system, LPIS) 等 3 个关键安全系统的响应情况. 基于关键安全系统的响应情况, 形成相应的事件序列与逻辑分支, 反映了不同响应策略下系统所面临的事故后果[58].

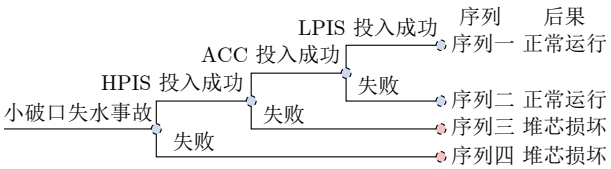


图 6　事件树示意图

Fig. 6　Schematic diagram of event tree

通常, 事件树可以被分为连续事件树 (continuous event tree, CET) 和离散事件树 (discrete event tree, DET). 其中, 连续事件树又可进一步细分为静态事件树 (static event tree, SET) 和动态事件树 (dynamic event tree, DyET). 静态事件树假设系统各项响应均为瞬时完成, 事件发生之间没有显著的时间延迟. 当初始事件发生之后, 系统各项安全防护措施将依据专家经验知识预设的顺序进行逐一评估, 从而推导事故发展的可能路径[59].

然而, 在实际工程实践中, 安全防护措施的响应过程往往受到多种不确定因素的影响, 系统状态也会随时间不断演变. 因此, 为克服静态事件树建模方法在时序依赖刻画上的不足, 动态事件树结合逻辑推理与动态仿真, 根据系统的实际状态来确认系统的分支条件与响应, 从而能够更加精确地捕捉系统状态随时间演变的特征[60–61].

与此同时, 研究人员倾向于将事件树与两类典型的安全分析方法相结合, 用于系统的量化评估,

即确定性安全分析 (deterministic safety analysis, DSA) 与概率性安全分析 (probabilistic safety analysis, PSA). 其中, DSA 以预设的事故场景为起点, 设定保守的工况参数, 分析系统在不同参数设定情况下的运行状态及其潜在风险; PSA 则基于事件树中的事件序列, 评估各类序列的发生概率及其后果. 由于两种分析方法各有侧重, 于是部分研究提出综合确定性和概率安全分析的方法 (integrated deterministic and probabilistic safety analysis, IDPSA). 该方法结合 DSA 和 PSA 的不同优势, 能够在统一的框架体系下捕捉和分析多序列组合之间的耦合关系, 并对事故建模过程中模型参数的认知不确定性 (epistemic uncertainty) 及事故演化过程中的随机不确定性 (stochastic uncertainty) 进行处理和量化[62].

最佳估计加不确定性 (best estimate plus uncertainty, BEPU) 作为综合确定性和概率安全分析方法的拓展. 通过计算每组事件序列中系统最佳估计响应与对应安全限值之间的距离, 并在考虑随机不确定性和认知不确定性的基础上, 构建该距离在不确定空间中的分布特征, 量化出系统在特定事故序列下的安全裕度, 如图 7 所示.

在 BEPU 的分析框架下, 由于不同事件序列对

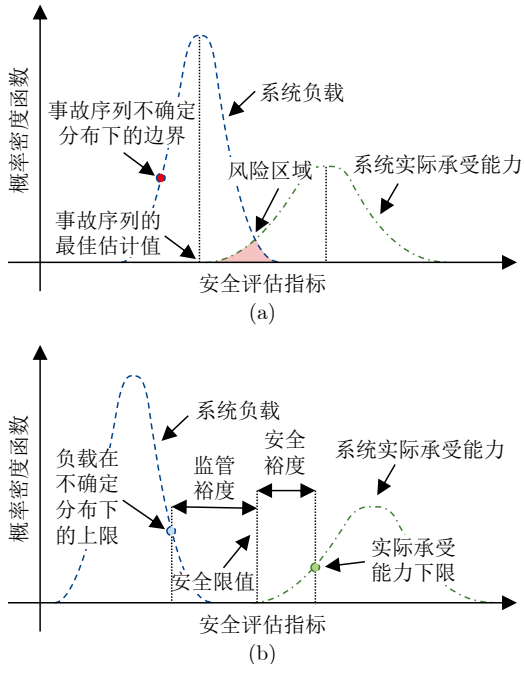


图 7 基于 BEPU 的风险与安全裕度示意图 ((a) 由实际负载与承受能力决定的风险; (b) 安全裕度)

Fig. 7 Schematic diagrams of risk and safety margin based on BEPU ((a) Risk determined by actual load and capacity; (b) Safety margin)

应着不同的系统响应路径和失效组合, 全面的安全量化评估往往需要对所有事故序列逐一建模和分析, 并结合其发生概率与安全限值展开裕度分析, 从而获得整体系统风险的定量结果. 这种基于全序列的计算方法虽然提高了安全分析的准确性, 但不可避免地带来了较高的计算复杂度和较低的计算效率. 为此, 研究者开发了多种基于事件序列的优化策略, 旨在确保安全评估精度的同时降低计算负担. 文献 [63] 引入混合粒子群优化算法 (hybrid particle swarm optimization, HPSO), 用于识别难以通过专家知识直接确定的复杂事故序列, 并通过设定截止频率合理简化用于 BEPU 的事故序列集合, 从而提升核电系统安全分析的整体效率. Liang 等[64] 提出概率显著序列 (probability significance sequence, PSS) 的概念. 通过分析和计算事故序列的发生概率及其对系统整体风险的贡献度, 将对系统最终风险具有显著影响的事件序列作为概率显著序列, 并将贡献度较低的次要序列予以剔除, 实现事件序列的降维优化. 文献 [65−66] 提出基于剪枝策略的优化算法, 在确保事故场景完整性的同时, 对冗余序列进行裁剪删除, 有效降低了 BEPU 安全评估过程中的计算复杂度. 此外, 文献 [67−70] 提出一种扩展的最佳不确定性估计 (extended best estimate plus uncertainty, EBEPU) 方法. 该方法利用多变量响应面及嵌套概率结构对多事件序列间的不确定性传播及其参数之间的非线性耦合效应进行捕捉, 实现了从单一事件序列分析到多序列协同评估的有效拓展. 因此, EBEPU 在进行安全分析时能够更真实地反映复杂工程系统中多源不确定性及多时间序列交互耦合的现实场景, 并具备对多风险并发及连锁演化导致潜在后果的识别与定量分析能力.

综上所述, 基于事件树的方法能够有效刻画系统在不同初始事件下的演化过程, 为事故后果评估与防控决策提供直观的分析框架. 然而, 事件树在模型构建过程中高度依赖专家知识, 缺乏数据驱动的建模范式. 这不仅导致构建事件树模型费时耗力, 也限制了构建所得模型在不同工程系统间的可迁移性与可扩展性. 未来, 随着与深度学习、实时优化及增量学习等技术的融合, 基于事件树的方法有望突破上述瓶颈, 从而在复杂工程系统的安全分析与评估中发挥更为重要的作用.

3.1.3 领结分析

领结分析是一种融合故障树和事件树、针对事件因果序列进行描述的风险评估方法. 其核心框架以顶层事件为中心, 将故障树放置在顶层事件的左侧, 用于逐层追溯导致顶层事件发生的各种潜在原

因; 事件树被放置在顶层事件的右侧, 基于时序逻辑推演顶层事件可能引发的后续事件序列, 量化和评估不同事件序列的后果严重程度. 领结分析在故障树和事件树的因果路径和事件路径上均部署和设置了不同的预防性安全屏障, 包括物理性安全措施及应急响应行动等, 如图 8 所示. 其中, 左侧因果路径上的安全屏障旨在预防或消除顶层事件的发生; 右侧事件路径上的安全屏障则侧重于缓解事故后果, 并协助系统从失控中恢复.

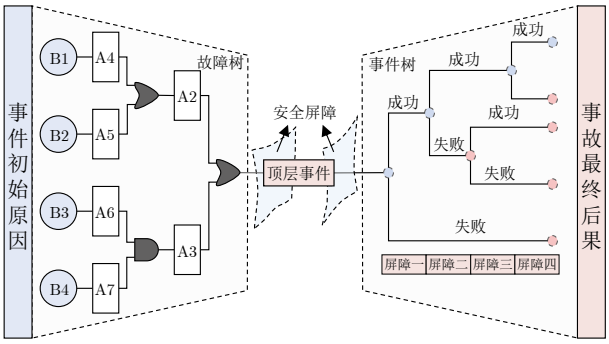


图 8　领结分析示意图

Fig. 8　Schematic diagram of bow-tie

目前, 领结分析已被广泛应用于不同复杂工程系统的安全评估中. 在化工领域, Pirbalouti 等[71] 面向高毒性石化加工装置的 9 种典型事故场景, 采用领结图结合概率分析的方法开展事故风险的定量计算; Khakzad 等[72] 利用物理可靠性模型 (physical reliability model, PRM) 拓展传统领结分析的功能, 将化工过程中的不同物理参数作为新观测, 结合贝叶斯网络实现风险概率的实时计算与动态更新; Yuan 等[73] 充分考虑领结建模、安全屏障识别、屏障维护间隔最优选取等问题, 提出考虑经济约束的领结分析安全屏障维护策略, 在降低安全屏障维护成本的同时, 将系统风险水平维持在可接受范围内. 在铁路运输领域, Huang 等[74] 和 Yang 等[75] 基于铁路风险事故资料库中的语义信息挖掘, 识别不同的安全因素及其因果关系, 并分别针对我国台湾花莲脱轨事故及北京市地铁火灾事故构建相应的领结图, 实现了顶层事件发生概率的定量计算. 在建筑施工领域, 文献 [76] 以接触尖锐物体 (contact with sharp object, CWSO) 作为安全事件, 提出一种新颖的混合领结模型 (hybrid bow-tie, H-BT), 该模型通过整合安全因素与安全屏障之间的关联信息, 能够有效识别与特定伤害类型相关的关键致因路径, 从而为建筑工程中的事故防护决策提供更具针对性的参考与支持. 在海洋工程领域, Slatnick 等[77] 针对海上浮式平台的典型风险 (如海上碰撞、浮动稳定性丧失等), 系统化地识别了风险的因果传播路径, 构建基于领结分析的风险模型, 并在此基础上优化风险的应对措施, 降低了风险事件对平台的影响; 此外, 针对海上钻井平台井喷、立管安全壳损失及海上疏散等风险事件, 基于领结分析的风险评估在各种来源的现有文献中均有涉及[78−80].

可见, 领结分析凭借其能够清晰地呈现事故因果关系、潜在后果及相应防护措施的图形化表达, 在多领域的风险识别及安全分析中展现出巨大的应用潜力. 然而, 由于领结分析本质上是故障树与事件树的组合, 其在面向复杂工程系统进行安全分析时, 不可避免地继承了两种方法的固有局限性. 例如, 建模过程中对专家知识的高度依赖及缺乏数据支撑所引发的认知不确定性, 会导致领结分析产生的评估结果存在显著的主观性偏差. 因此, 将模糊逻辑、敏感性分析及不确定性量化与领结分析相结合, 以提升其在知识不完备条件下的鲁棒性, 并使其能够在复杂工程系统的安全分析中更加可靠地评估系统风险及其关键薄弱环节, 是未来研究需要重点关注的方向.

3.2　基于级联失效故障的方法

复杂工程系统是由多个组件与子系统所构成、存在显著非线性相互作用的多层次工程系统. 在此类系统中, 若某一组件发生故障且未能得到及时的干预或处理, 故障可能会随着物理连接、信息或材料的流动在系统中传播、蔓延和扩散, 形成所谓的级联失效故障. 级联失效故障会触发系统内部的连锁反应, 并通过系统内部复杂的因果耦合非线性地放大初始故障的影响, 最终导致安全事故的发生. 因此, 级联失效故障可以描述为基于因果关系的链式反应, 即, 故障组件通过因果链条相互关联, 形成具有特定结构的级联故障传播路径. 通过集成和封装潜在的级联故障传播路径, 可构建用于表征系统事故发展路径与连续失效行为的评估模型 (如图 9 所示), 并实现复杂工程系统安全风险的量化分析.

近年来, 大量研究围绕级联失效故障的传播路径识别、事故模型构建与安全量化评估展开. 文献 [81] 对不同事故的相关安全指标进行识别, 并基于安全指标之间的相互作用刻画各类事故的因果链条, 建立面向铁路系统的风险监测模型. 文献 [82] 结合事件逻辑图和知识图谱, 识别铁路系统在极端天气条件下的关键节点和传播机制, 为铁路系统的安全评估和风险管理提供了有效的参考和指导. 文献 [83−84] 针对近地卫星系统的运行特性, 围绕 3 种典型失效场景构建相应的级联失效传播模型, 并

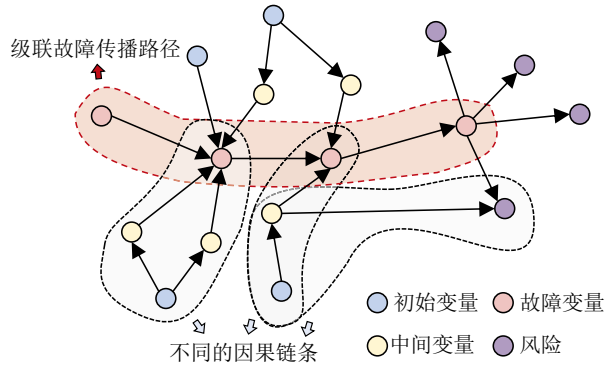


图 9 基于级联失效故障的事故模型

Fig. 9 Accident model established by cascading failures

对高负载工况下由卫星性能退化所引发的级联效应进行定量化表征与评估. 文献 [85] 基于尖峰时间依赖可塑性 (spike timing dependent plasticity, STDP), 设计具备自适应学习能力的动态事故模型. 该模型可根据时序序列中的特征动态识别因果关系, 从而精确刻画复杂工程系统事故演化过程中的非线性传播路径. 文献 [86] 基于大量事故调查报告, 系统地识别地下项目施工过程中的多类风险因素, 并采用关联规则对不同安全指标与事故发生之间的潜在逻辑关系进行挖掘, 建立反映级联失效传播的交互式风险模型用于评估.

与此同时, 研究者受到多米诺骨牌倒塌现象的启发. 将复杂工程系统中的多米诺效应 (domino effect) 定义为初始事件在单个设备内或邻近设备上同时或逐序传播的事件效应, 如图 10 所示. 目前, 该方法作为复杂工程系统中级联失效建模的类比工具, 广泛应用于火灾、爆炸等灾难性事件的演化分析中. 文献 [87] 将常压储罐的温度和强度作为结构安全指标, 评估多种火灾场景下常压储罐的多米诺效应, 并基于所描述的风险升级路径, 展开储罐系统在火灾诱发下的多层级风险量化. 文献 [88] 将火焰吞噬 (flame engulfment) 和热辐射 (heat radiation) 视为引发储油罐火灾的根本诱因. 通过考虑系统中的多米诺效应, 刻画了基于不同诱因的事故演化路径, 并结合阈值分析评估了各类火灾场景下常压储罐的动态失效概率.

在此背景下, 有研究在多米诺效应的基础上进一步引入了平行效应和协同效应的概念, 以探究多米诺效应在多路径、多源事故下的链式扩展规律[89−90]. 其中, 平行效应用于描述单一事故源通过不同传播路径同时导致多个设备失效的能力; 而协同效应则用于刻画多个事故源之间的相互作用对单一设备失效的联合影响. 基于以上定义, 文献 [91−92] 针对常压储罐的火灾场景, 综合考虑多米诺效应的平行演

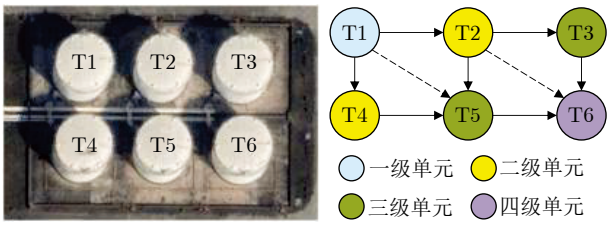


图 10 多米诺效应示意图[93] ((a) 储罐场的卫星地图; (b) 多米诺效应在储罐场中可能触发的传播路径)

Fig. 10 Schematic diagram of domino effect[93] ((a) Satellite map of the storage tank farm; (b) Probable domino accident propagation paths in the storage tank farm)

化过程和协同升级机制, 提出一种基于时空效应的风险事故模型, 用于识别多米诺传播中的关键节点, 并据此提出差异化的厂区安全防护策略, 以有效抑制火灾的级联扩散. 进一步地, 文献 [94] 聚焦于多米诺效应中不同层级事故源之间的时空交互特性, 将协同效应细分为同阶同类、同阶异类、跨阶同类和跨阶异类 4 种类型, 并在此基础上提出基于时序耦合的概率计算模型, 用于安全评估.

综上所述, 基于级联失效故障的方法通过多米诺效应的类比分析, 在复杂工程系统的安全分析与评估中展现出了广阔的应用前景. 然而, 复杂工程系统中潜在的因果依赖关系往往难以被有效地挖掘. 为此, 对不同领域的事故报告展开深度语义解析, 对多元时序序列中蕴含的关联特征进行分析, 从而全面地识别复杂工程系统中所包含的因果结构与关键路径, 是未来研究需要重点攻克的方向.

3.3 基于图的方法

图作为一种能够描述复杂工程系统全局结构特征及局部依赖关系的有效工具, 所构建的事故模型不仅能够从宏观层面辨识不同风险事件在模型拓扑结构中的共性特征与结构性差异, 还能够从微观层面揭示风险要素之间的因果联系. 因此, 近年来, 基于图的方法在复杂工程系统的安全量化评估中得到广泛应用.

3.3.1 基于传统图论的方法

现有大量基于传统图论的事故建模方法, 其核心主要是利用图的拓扑结构来对复杂工程系统中各类组件之间的相互关系及其传播路径进行刻画和表征. 通常, 构建所得的图模型, 也即事故模型 $\boldsymbol{G}$ 可表示为 $\boldsymbol{G}=(\boldsymbol{X}, \boldsymbol{E})$, 其中 $\boldsymbol{X}=\{x_1, x_2, \cdots, x_N\}$ 是包含 N 个节点的节点集, $\boldsymbol{E}=\{e_1, e_2, \cdots, e_M\}$ 是包含 M 条边的边集. 在复杂工程系统中, 不同的安全事件与关键安全指标 (如压力、温度等) 被抽象

为图模型的节点, 其间的因果关系则通过边来表示.

无向无权的图模型因其建模简单、计算高效的特点, 而广泛应用于大型密集型生命线网络的拓扑结构表达中, 如交通道路[95]、供水网络[96] 及电力系统[97] 等. 然而, 无向无权图难以充分刻画节点之间的属性差异及其交互关系. 因此, 研究者逐渐将建模思路拓展至加权图与有向图的构建中, 以便更为真实地反映节点间相互作用的因果强度及其方向. 例如, 文献 [98] 提出一种基于概率空间转换的加权图构建框架, 借助 Nataf 变换和 Cholesky 分解实现了边权重的计算与映射. 文献 [99] 采用卡方检验确定电梯系统中 67 个风险因素的显著相关性, 并以相关系数作为边权重构建了风险图模型, 完成了风险的定量评估. 此外, 文献 [100−101] 则分别聚焦于列车制动系统及高速铁路系统, 基于有向无权图刻画了安全指标之间的因果依赖关系及其方向特征, 为不同系统的风险路径传播分析提供更为清晰的结构化表征.

随着研究的深入, 兼具权重属性与方向特征的有向加权图被越来越多地应用于复杂工程系统的风险建模与量化评估中. 文献 [102] 以灾难因果链条为基础构建管道溢油事故的有向加权图模型, 并通过最大似然表达实现了事故传播的定量表征. 文献 [103] 针对深水钻井平台的井喷事故, 将有向加权图模型与风险熵理论相结合, 对事故发生最短路径上的风险概率与熵值进行量化. 文献 [104−105] 以管道重要性为权重, 对天然气管网的有向加权图模型进行构建, 并结合效用理论对天然气泄漏风险后果的严重性进行分析.

此外, 大量研究者将图的基本度量指标 (如表 4 所示) 引入至风险评估领域, 以此来对模型中的关键节点及传播路径展开识别与分析[106−107]. 文献 [108−109] 基于 2019 年的航空事故调查报告, 构建了有向加权的航空安全图模型. 以图模型为基础, 以节点度作为衡量指标, 对模型中不同节点的重要性进行评估, 并从整体上对航空系统的脆弱环节和潜在风险路径进行分析和描述. 文献 [110] 构建了包含 109 个节点和 260 条边的铁路事故因果图模

表 4　基本度量指标

Table 4　Basic metrics

序号	指标	描述	计算公式	该指标在安全分析中的作用	符号说明
1	度	节点 i 的度由连接到该节点的相关边数所定义	$k_i = \sum\limits_{i,\, j\in \boldsymbol{X},\, i\neq j} \lambda_{ij}$	度量节点在图中的连接能力, 用于识别风险传播过程中的关键节点	当 $\lambda_{ij}=0$ 时, 表示节点 i 到节点 j 不相连; 当 $\lambda_{ij}=1$ 时, 则表示节点 i 到节点 j 相连
2	平均度	所有节点度的平均值	$<k> = \dfrac{\sum\limits_{i\in \boldsymbol{X}} k_i}{N}$	用于衡量风险传播的总体潜在密度	节点集 $\boldsymbol{X}$ 中总共包含 N 个节点
3	最短路径	节点 i 到节点 j 所有路径集合中的最小值	$d_{ij} = \min\{\mathcal{P}_{ij}\}$	用于识别风险在节点间传播的最短路径	$\{\mathcal{P}_{ij}\}$表示从节点 i 到节点 j 所有路径的集合
4	最短路径长度	任意两个节点之间最短连接路径所包含的边数	$l = \lvert d_{ij}\rvert$	用于描述风险在节点间传播的最小距离	$\forall i,\ j\in \boldsymbol{X}$ 且 $i\neq j$
5	平均最短路径长度	所有最短路径长度的平均值	$<l> = \dfrac{\sum\limits_{i,\, j\in \boldsymbol{X},\, i\neq j} \lvert d_{ij}\rvert}{N(N-1)}$	用于反映整体的风险传播速度	—
6	直径	所有最短路径长度中的最大值	$d = \max\{\lvert d_{ij}\rvert\}$	衡量节点间最远的风险传播距离, 用于评估风险传播的整体波及范围	$\forall i,\ j\in \boldsymbol{X}$ 且 $i\neq j$
7	聚集系数	节点邻居间实际存在边数与最多可能边数的比例	$C = \dfrac{\sum\limits_{i\in \boldsymbol{X}} \dfrac{2\xi_i}{k_i(k_i-1)}}{N}$	用于反映节点周边的风险聚集效应	ξ_i表示节点 i 与邻居节点之间实际存在的边数
8	介数中心性	节点在最短路径中出现的频率	$\tilde{b}_i = \dfrac{\sum\limits_{i,\, j,\, k\in \boldsymbol{X},\, i\neq j\neq k} \dfrac{\zeta_{jk}(i)}{\zeta_{jk}}}{(N-1)(N-2)}$	反映节点在风险传播过程中的中介特性, 用于识别风险传播过程中的关键节点	ζ_{jk} 是节点 j 到节点 k 最短路径的条数; $\zeta_{jk}(i)$ 表示最短路径中通过节点 i 的条数
9	接近中心性	节点到图中其他所有节点平均最短路径长度的倒数	$cl_i = \dfrac{N-1}{\sum\limits_{i,\, j\in \boldsymbol{X},\, i\neq j} \lvert d_{ij}\rvert}$	用于衡量风险传播过程中节点快速到达其他节点的能力	$0 \leq cl_i \leq 1$
10	网络中心势	图中介数中心性的最高节点与其他节点之间中心性差异的平均程度	$Z_B = \dfrac{\sum\limits_{i\in \boldsymbol{X}} (\tilde{B}_{max} - \tilde{B}_i)}{N-1}$	用于评估图结构是否过度依赖少数关键节点	$\tilde{B}_{max}$ 为图中介数中心性的最大值; $\tilde{B}_i$ 区别于 $\tilde{b}_i$, 为节点 i 在全图中统一量化后的介数中心性数值

型, 并结合节点度、直径及介数中心性等多种度量指标, 识别与风险传播相关的若干关键节点, 深入分析铁路系统中风险传播的结构特征, 实现了面向铁路系统事故风险的精确判断与主动防控. 文献 [111] 将图拓扑衡量指标与输电线路过载、母线电路过载等电力系统实际运行特性相结合, 综合识别系统中具有高故障影响效力的关键部件, 有效遏制了级联故障对系统的整体性危害. 文献 [112] 通过事故报告分析, 构建涉及危险气体泄漏的事故演化图模型, 并通过聚合系数、平均路径长度及直径等指标对灾难性路径进行评估, 为积极预防和有效管理天然气泄漏提供了有效的见解与参考. 文献 [113] 将工程系统中的功能层、操作层和管理层中的不同组件抽象成具有层次结构的行为节点, 并通过节点度和网络异质性刻画了与风险传播相关的阈值和传播范围.

然而, 尽管图模型在不同领域的安全分析中已取得显著成果, 但在面对大规模复杂工程系统时, 仍面临诸多挑战. 组件间高度耦合且非线性的因果依赖关系使得构建准确的图模型成为一个尚未解决的难题. 同时, 大规模图模型的复杂性也导致其实时推理效率低下, 难以满足实际工程对于及时安全评估和决策支持的严格要求. 图神经网络 (graph neural network, GNN) 作为一种能够在图结构中进行端对端特征学习与高效推理的方法, 为突破传统图模型在可扩展性与实时性方面的局限提供了新的思路[114−116]. 因此, 利用图神经网络构建面向安全分析的图模型, 并借助图嵌入、注意力机制等技术手段[117], 以增强模型的结构表达能力并降低推理延迟, 将是未来实现复杂工程系统安全状态感知与评估的重要方向.

3.3.2 基于贝叶斯网络的方法

贝叶斯网络 (Bayesian network, BN) 是一种有向无环图, 其结构由节点集合 $\boldsymbol{X} = \{x_1, x_2, \cdots, x_N\}$ 与边集合 $\boldsymbol{E} = \{e_1, e_2, \cdots, e_M\}$ 共同定义. 其中, 每个节点表示一个关键安全指标, 节点之间的定向弧线 (有向边) 表示相连节点之间的条件依赖关系. 弧线的起始节点是父节点, 弧线所指向的节点是子节点. 没有父节点的节点是根节点, 而没有子节点的节点是叶子节点, 除根节点和叶子节点之外的其他节点是中间节点. 其中, 父节点与子节点之间的条件依赖形式及因果关系强度通过分配给子节点的条件概率来描述[118].

因此, 基于贝叶斯网络的安全评估方法是一种通过概率图模型描述安全事件之间因果联系, 并利用条件概率进行定量分析的方法. 采用贝叶斯网络进行安全分析与评估, 通常包含两个主要步骤, 如图 11 所示. 1) 事故模型构建: 首先, 需要明确安全指标之间因果依赖关系的网络拓扑结构, 形成对应的贝叶斯网络, 并对网络的参数进行学习和设定, 包括各节点在给定父节点下的条件概率等. 2) 安全量化评估: 利用贝叶斯网络的推理特性对复杂工程系统的安全性进行量化评估, 包括演绎推理 (即从已知风险推导后果) 和溯因分析 (即从观察结果反推潜在原因), 实现对潜在事故原因的诊断、关键风险因素的识别及系统安全的定量计算和有效评估.

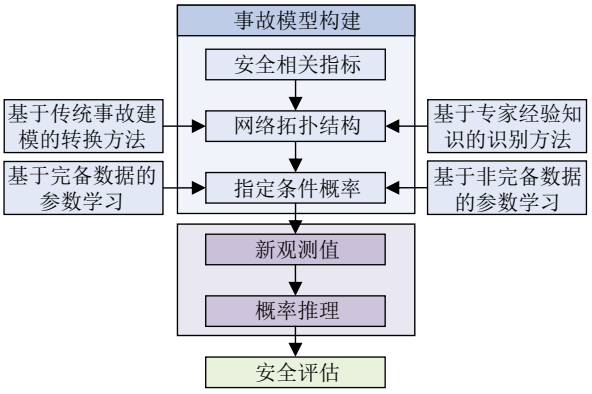


图 11 构建和使用贝叶斯网络进行安全量化评估的必要步骤

Fig. 11 Steps necessary to build and use the Bayesian network for safety quantification and assessment

1) 基于贝叶斯网络的事故模型构建

传统的事故建模方法, 如可靠性框图、故障树及事件树等, 可以有效地转换成贝叶斯网络, 并借助其图结构特性描述安全指标之间的因果依赖关系.

1998 年, Torres-Toledano 等[119] 首次提出将可靠性框图转换为贝叶斯网络的方法, 并将其用于系统的可靠性评估. 随后, Zhou 等[120] 和 Li 等[121] 分别从多状态建模及共因失效的角度对可靠性框图进行拓展, 并成功实现了向贝叶斯网络的映射转换. 文献 [122−123] 进一步探究了将故障树转化成贝叶斯网络的可行性, 并详细阐述了相应的转化步骤, 如图 12 所示. 其中, 故障树的顶层事件映射为贝叶斯网络的根节点, 中间事件映射为中间节点, 基本事件映射为叶子节点. 基本事件的故障概率直接决定了对应叶子节点的先验概率, 不同节点之间的条件概率则依据其对应的逻辑门功能进行定义. 由于逻辑门的结果具有确定性 (非真即假), 其对应取值通常为 0 或 1.

然而, 传统基于静态故障树的映射方法在工程实践中难以适应工业过程的动态变化. 为此, 研究者将动态故障树引入贝叶斯网络的映射构建中, 以

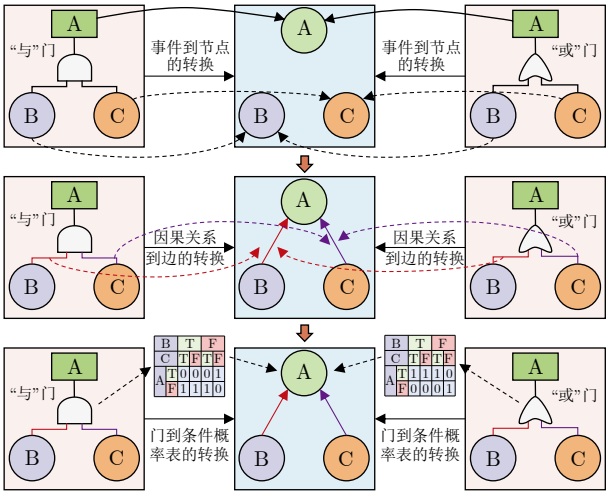


图 12　故障树到贝叶斯网络的转换过程

Fig. 12　Transformation process from fault tree to Bayesian network

详细刻画不同安全指标在时间维度上的动态交互特性与演化特征. 例如, 文献 [57, 124] 在充分考虑时序依赖、离散编码和离散间隔选取等问题的情况下, 提出将动态故障树转换成离散时间贝叶斯网络 (discrete time Bayesian network, DTBN) 的方法. 文献 [125] 通过引入没有明确时间演化的静态节点, 以连续时间马尔科夫过程为基础, 构建了连续时间贝叶斯网络 (continuous time Bayesian network, CTBN), 实现了对系统中各变量在任意时间点状态下的精确建模. 文献 [56, 126] 在无需时间离散化的前提下, 参考时间分量的演化过程, 对连续时间贝叶斯网络进行拓展, 提出将动态故障树映射成广义连续时间贝叶斯网络 (generalized continuous time Bayesian network, GCTBN) 的方法. 实际上, 在过去的二十几年里, 研究者持续地尝试将贝叶斯网络与其他经典的风险分析方法相结合, 以拓展贝叶斯网络的构建方式与适用场景, 如表 5 所示.

与此同时, 贝叶斯网络的结构可由人工基于经验知识进行构建. 如华中科技大学的研究团队依托于积累的工程经验和领域知识, 形成了用于地铁隧道渗漏风险评估的贝叶斯网络模型[150]. 文献 [151] 以大量的航空事故调查结果为基础, 将各类风险因素建模为网络节点, 其中的高频风险因素被设定为父节点, 飞机损坏程度与人员伤亡情况被设定为根节点, 建立了相应的贝叶斯网络模型. 文献 [152−153] 基于各国港口的监测数据, 对船舶不同缺陷之间的相互关系及缺陷对海上交通事故发生的影响机制进行总结, 构建了涵盖船龄、船只类型、船只缺陷及事故结果等要素的贝叶斯网络. 文献 [154] 创建了与海洋因素相关的贝叶斯网络, 用于预测北海航线 (northern sea route, NSR) 护航行动中船舶陷入冰中的概率.

表 5　不同模型向贝叶斯网络的转化

Table 5　Transformation of different models into Bayesian network

原始模型类型	文献
可靠性框图	[119−121, 127]
故障树	[122−123, 128−137]
动态故障树	[56−57, 124−126, 138−142]
领结分析	[71, 143−146]
故障模式与影响分析	[147−148]
AcciMap	[149]

综上所述, 基于传统事故建模转换的方法和基于专家知识的方法共同构成了贝叶斯网络建模的两种重要途径. 基于上述方法构建得到的贝叶斯网络, 实质上形成了一类能够全面描述复杂工程系统中安全指标因果依赖关系的事故模型. 依托于该模型, 可进一步结合实时观测数据开展下游概率推理, 实现面向复杂工程系统的安全风险定量化表征.

2) 基于贝叶斯网络的安全量化评估

基于贝叶斯网络的事故模型采用条件概率来表征各安全因素之间的因果关系, 以捕捉系统风险的概率结构. 安全量化评估则依托该模型, 计算安全指标集合的联合概率分布, 量化系统风险发生的概率, 并通过证据更新机制动态调整评估结果. 对于给定的安全指标集合 $\boldsymbol{X}=\{x_1,\ x_2,\ \cdots,\ x_N\}$, 贝叶斯网络的联合概率分布 $\Pr(\boldsymbol{X})$ 可表示为:

$$\Pr(\boldsymbol{X})=\prod_{i=1}^{N}\Pr(x_i|\pi(x_i)) \tag{1}$$

其中, x_i 表示贝叶斯网络中的第 i 个节点, 也即第 i 个安全指标; $\pi(x_i)$ 是 x_i 父节点的集合. 当引入新的证据或观测信息 $\boldsymbol{Z}$ 时, 贝叶斯网络会根据贝叶斯定理进行概率更新, 其对应的后验概率分布可写作:

$$\Pr(x_i|\boldsymbol{Z})=\frac{\Pr(x_i,\ \boldsymbol{Z})}{\Pr(\boldsymbol{Z})}=\frac{\sum\limits_{\boldsymbol{X}\setminus\{x_i,\ \boldsymbol{Z}\}}\Pr(\boldsymbol{X})}{\sum\limits_{\boldsymbol{X}\setminus\boldsymbol{Z}}\Pr(\boldsymbol{X})} \tag{2}$$

其中, $\Pr(x_i,\ \boldsymbol{Z})$ 表示 x_i 和 $\boldsymbol{Z}$ 的联合概率分布; $\boldsymbol{X}\setminus\boldsymbol{Z}$ 表示从 $\boldsymbol{X}$ 中去除 $\boldsymbol{Z}$ 之后的集合; $\boldsymbol{X}\setminus\{x_i,\ \boldsymbol{Z}\}$ 表示从 $\boldsymbol{X}$ 中去除节点 x_i 以及 $\boldsymbol{Z}$ 之后的集合.

贝叶斯网络通过条件概率的推理机制实现了节点间信息的高效传播与动态更新, 从而刻画了系统不确定性的变化, 并解释了系统状态潜在的风险变化趋势[155]. 基于这种不确定性推理和信息更新的特性,

贝叶斯网络在复杂工程系统的安全量化评估中展现出了独特的优势. 大量研究表明, 贝叶斯网络已广泛应用于船舶系统[128−129]、工程结构系统[130, 135, 137, 150]、航空系统[133] 及化工系统[156−157] 等多个领域的安全量化评估任务当中.

然而, 传统贝叶斯网络受限于其本身固有的静态结构, 在刻画复杂工程系统的动态演化方面存在显著局限. 基于此, 以隐马尔科夫模型 (hidden Markov model, HMM) 为拓展的动态贝叶斯网络 (dynamic Bayesian network, DBN) 应运而生. 动态贝叶斯网络通常以离散时间步的形式进行建模, 即, 在每个时刻, 一个节点不仅受到当前时刻父节点的影响, 还会受到先前 p $(p \geq 1)$ 个时刻父节点的影响. 在该种性质假设下, 动态贝叶斯网络的联合概率分布可表示为:

$$\begin{aligned}&\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{t-1},\ \boldsymbol{X}^{t-2},\ \cdots,\ \boldsymbol{X}^1)=\\&\quad\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{t-1},\ \boldsymbol{X}^{t-2},\ \cdots,\ \boldsymbol{X}^{t-p})=\\&\quad\prod_{i=1}^{N}\Pr(x_i^t|\pi(x_i^t))\end{aligned}\tag{3}$$

其中, $\boldsymbol{X}^t=\{x_1^t,\ x_2^t,\ \cdots,\ x_N^t\}$ 表示 t 时刻不同节点的状态集合; $\pi(x_i^t)$ 表示第 i 个节点包括当前时刻及过去 p 个时间步的父节点集合. 当新的证据或观测信息 $\boldsymbol{Z}$ 在时刻 t 出现时, 动态贝叶斯网络基于贝叶斯定理的更新形式表示为:

$$\begin{aligned}&\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{1:t-1},\ \boldsymbol{Z})=\frac{\Pr(\boldsymbol{X}^t,\ \boldsymbol{Z}|\boldsymbol{X}^{1:t-1})}{\Pr(\boldsymbol{Z}|\boldsymbol{X}^{1:t-1})}=\\&\quad\frac{\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{1:t-1})\Pr(\boldsymbol{Z}|\boldsymbol{X}^t)}{\sum\limits_{\boldsymbol{X}^t}\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{1:t-1})\Pr(\boldsymbol{Z}|\boldsymbol{X}^t)}\end{aligned}\tag{4}$$

其中, $\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{1:t-1})$ 是给定前 $t-1$ 时刻所有节点信息和证据 $\boldsymbol{Z}$ 下, 时刻 t 所有节点及证据的联合概率分布; $\Pr(\boldsymbol{Z}|\boldsymbol{X}^{1:t-1})$ 是证据 $\boldsymbol{Z}$ 在前 $t-1$ 时刻所有节点信息下的边际概率分布. 联合概率分布由所有节点信息的先验概率分布 $\Pr(\boldsymbol{X}^t|\boldsymbol{X}^{1:t-1})$ 和给定 t 时刻节点状态 $\boldsymbol{X}^t$ 下证据 $\boldsymbol{Z}$ 的条件概率分布计算得到.

文献 [158−159] 针对建筑、桥梁、管道等工程结构系统的应用研究, 对涉及动态贝叶斯网络的安全量化评估方法进行了全面的归纳和总结. 文献 [160] 开发了基于动态贝叶斯网络的概率风险评估与预测框架, 并在 5 种不同的交通事故场景下对其进行实验验证. 与此同时, 在电力系统、核电系统、化工系统及航空航天等复杂工程系统中, 动态贝叶斯网络由于其对于不同系统组件之间时间依赖性上的考虑, 以及能够通过最新观测更新组件安全状态的能力, 而被广泛地使用[161−163].

无论是传统的贝叶斯网络还是动态的贝叶斯网络, 其推理结果都在很大程度上依赖于网络初始设定的根节点概率. 这些概率值通常被要求以明确的数值形式给出, 作为后续贝叶斯推理计算的基础. 然而, 在现实的工业场景中, 认知信息的不足及数据的缺乏, 使得贝叶斯网络中根节点的先验概率往往难以精确获取[164].

在此背景下, 研究者开始在贝叶斯网络中引入模糊集理论 (fuzzy set theory, FST), 期望以模糊数或区间概率的形式来描述和量化工业场景下的认知不确定性. 在模糊贝叶斯网络中, 安全指标集合 $\boldsymbol{X}=\{x_1,\ x_2,\ \cdots,\ x_N\}$ 的联合概率分布 $\tilde{\Pr}(\boldsymbol{X})$ 可表示为:

$$\tilde{\Pr}(\boldsymbol{X})=\prod_{i=1}^{N}\tilde{\Pr}(x_i|\pi(x_i))\tag{5}$$

其中, $\tilde{\Pr}(x_i|\pi(x_i))$ 表示模糊条件概率. 在引入新的证据或观测信息 $\boldsymbol{Z}$ 后, 模糊贝叶斯推理可表示为:

$$\tilde{\Pr}(x_i|\boldsymbol{Z})=(\tilde{\Pr}(x_i)\otimes\tilde{\Pr}(\boldsymbol{Z}|x_i))\oslash\tilde{\Pr}(\boldsymbol{Z})\tag{6}$$

其中, $\otimes$ 和 $\oslash$ 分别是模糊集理论中定义的乘积算子和除法算子, 其具体形式取决于所选用的模糊隶属函数及其对应的模糊逻辑运算规则.

模糊贝叶斯网络能够对非精确、不完备的数据进行处理, 在存在显著不确定认知的复杂工业场景安全评估中具有较高的使用价值. 例如, 文献 [165] 提出一种基于模糊贝叶斯网络的安全评估方法. 如图 13 所示, 通过将低、中、高三种形式变量的模糊失效概率引入根节点作为先验输入, 进而对中间节点和叶子节点的条件模糊概率进行推理, 实现了面向整体系统风险水平的模糊计算和评估. 文献 [134] 使用模糊集理论刻画环氧乙烷 (ethylene oxide, EO) 系统数据中的不确定性, 并结合贝叶斯网络对事件

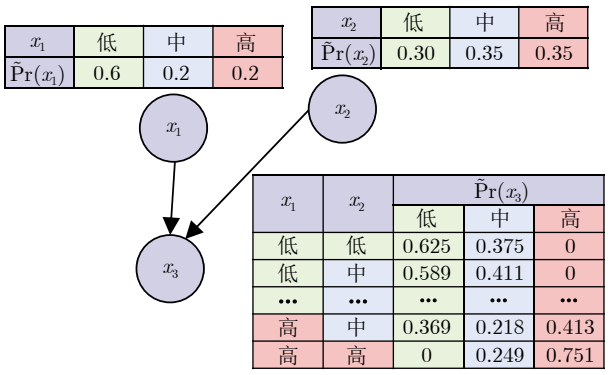


图 13 基于模糊贝叶斯网络的系统风险水平描述

Fig. 13 Description of system risk levels based on fuzzy Bayesian network

之间的概率依赖关系进行捕获和建模, 以获取系统层面的安全概率指标. 文献 [150] 将模糊贝叶斯网络应用于武汉长江隧道的结构安全分析中, 构建了以诱导损伤为风险事件的因果网络, 并通过模糊概率的方式完成了基于因果网络的失效概率计算.

此外, 针对工程系统中普遍存在的认知不确定性, 研究者还提出信息差距理论 (info-gap theory)[166]、随机集 (random set)[167] 及 P-box (probability-box)[168] 等方法. 近年来, 也有大量的研究致力于将这些方法与贝叶斯网络相结合, 用于复杂工程系统的安全量化评估[131, 142, 169–171].

综上所述, 基于贝叶斯网络的安全量化评估方法经历了从静态到动态、从简单到复杂的整体发展过程. 然而, 联合概率分布函数中涉及的高维积分与求和运算显著增加了该方法的计算复杂度, 影响其安全分析的效率. 因此, 进一步结合安全事件分析, 优化安全指标候选集的筛选方法, 减少网络节点及其计算负担, 是未来具有较高研究价值的方向.

4　基于安全域的量化评估现有方法与进展

基于事故模型的方法在评估理念上遵循“逐点”判定的逻辑, 即, 以一组描述系统状态的监测数据作为事故模型的输入, 并据此输出当前状态下系统是否处于安全状态的判别结果. 此类以“逐点”评估为核心的方法, 虽然能够反映系统在某一特定运行状态下的安全水平, 但当系统的运行状态发生变化时, 其安全水平则需要重新进行计算与判定. 此外, 其评估结果通常呈现“安全”与“不安全”的二元判断, 既缺乏与系统安全边界的关联性刻画, 也难以提供系统的剩余安全裕度, 即系统运行状态与安全边界之间的相对距离度量.

针对上述问题, 研究者提出安全域 (safety region, SR)[1] 的概念, 以弥补“逐点”法在安全量化评估方面的不足. 安全域从系统运行状态出发, 强调在多维安全指标状态空间中, 对系统安全运行区域的整体性描述. 换言之, 安全域不仅定义了涵盖系统运行状态全局信息的封闭区域, 还反映了系统运行状态与安全域边界之间的时空特征信息, 为系统剩余安全裕度的定量化表征提供了有效的参考依据[172].

目前, 在面向复杂工程系统的安全量化评估研究中, 安全域可以被大致分为静态安全域和动态安全域两种类型. 以下将对基于两类安全域的方法展开更为详细的介绍.

[1] 在一些英文文献中安全域也被称为 safety domain 或 security region

4.1　基于静态安全域的方法

静态安全域 (static safety region, SSR) 的概念最早由文献 [173] 提出, 旨在对无外部扰动且运行状态不随时间演变的系统边界进行理论刻画. 具体而言, 系统的安全必须严格遵循各类安全设备在设计阶段所确定的运行约束. 这些约束通常是设备在电气、热力及机械等多物理场下的性能极限, 是系统实际运行过程中不可逾越的边界. 为此, 针对不同设备的运行约束进行识别, 以不等式组的形式构建运行约束集合, 并最终将所有满足运行约束的系统状态空间子集, 也即系统在理想静态条件下保持安全稳定运行的区域, 界定为系统的静态安全域.

若运行约束中的各状态变量相互独立, 则由其共同定义的静态安全域在低维状态空间中通常呈现出轴对齐的超矩形结构. 其几何边界由各变量的上/下边界决定, 如图 14 所示. 以核电系统为例, 典型的安全相关设备包括反应堆、蒸发器及稳压器等[174]. 若将反应堆压力 P_{re} 与蒸发器温度 T_e 作为关键安全指标, 其运行约束可表示为:

$$\begin{cases} P_{re}^{m} \le P_{re} \le P_{re}^{M} \\ T_{e}^{m} \le T_{e} \le T_{e}^{M} \end{cases} \tag{7}$$

其中, P_{re}^{m} 和 P_{re}^{M} 分别表示反应堆压力的下限和上限; T_{e}^{m} 和 T_{e}^{M} 分别表示蒸发器温度的下限和上限. 基于上述运行约束, 核电系统在二维状态空间中的静态安全域, 即为所有满足该不等式组的运行状态集合[175], 其几何形态如图 14(a) 所示. 若进一步将稳压器压力 P_s 的约束条件引入:

$$P_{s}^{m} \le P_{s} \le P_{s}^{M} \tag{8}$$

其中, P_{s}^{m} 和 P_{s}^{M} 分别表示稳压器压力的下限和上限. 那么, 在三维状态空间中, 由三个运行约束共同限定得到的静态安全域如图 14(b) 所示.

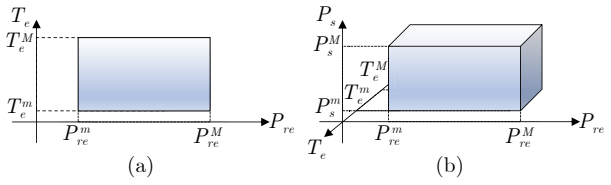


图 14　不同维度下的静态安全域示意图 ((a) 二维空间中的静态安全域; (b) 三维空间中的静态安全域)

Fig. 14　Schematic diagrams of SSR in different dimensions ((a) SSR in 2-dimensional space; (b) SSR in 3-dimensional space)

这类基于安全指标运行约束的静态安全域构建方法, 由于其直观的建模过程和较低的计算开销, 在早期的安全研究中得到了广泛的应用. 然而, 在

实际的复杂工程系统中, 各项安全指标往往并非相互独立, 而是受到系统物理规律、结构耦合及反馈控制的联合制约, 呈现出显著的相关特性及耦合特性[176]. 此时, 由多个耦合指标共同描述的静态安全域不再是简单的超矩形几何形态, 而是在状态空间中呈现出非线性及非轴对称的边界结构[177], 如图 15 所示.

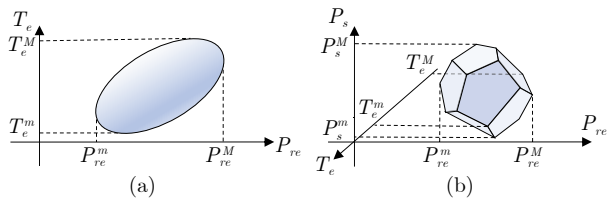


图 15 考虑变量耦合的静态安全域示意图 ((a) 二维空间中耦合的静态安全域; (b) 三维空间中耦合的静态安全域)

Fig. 15 Schematic diagrams of SSR considering variable coupling ((a) Coupled SSR in 2-dimensional space; (b) Coupled SSR in 3-dimensional space)

随着系统维度的进一步提升, 安全指标之间的耦合关系显著增强. 基于运行约束刻画的静态安全域难以再通过直观的几何形式进行呈现. 为此, 研究者致力于将静态安全域的构建问题转化为多重运行约束下求解特定目标函数的规划问题, 如图 16 所示. 相应地, 静态安全域被重新定义为目标函数在约束空间内所有可行解的集合[178]. 其边界和形态不再仅由运行约束本身的上/下限所决定, 而是由目标函数在多维状态空间中的变化规律及系统变量间的耦合关系共同决定.

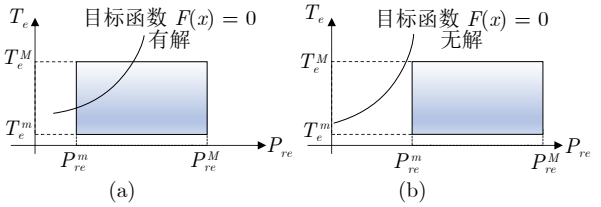


图 16 运行约束下的可行解 ((a) 有解; (b) 无解)

Fig. 16 Feasible solutions under operational constraints ((a) Have solutions; (b) No solution)

目前, 此类方法在复杂电力系统中已经有了较为成熟的应用. 假设电力系统网络包含 $n+1$ 个节点和 n_b 条线路. 其中, $G=\{0,\ 1,\ 2,\ \cdots,\ n_g\}$ 表示发电机节点集合 (节点 0 为参考节点); $L_g=\{n_g+1,\ n_g+2,\ \cdots,\ n\}$ 表示负荷节点集合; $N_g=\{0,\ 1,\ 2,\ \cdots,\ n\}$ 表示全部节点的集合; $B=\{1,\ 2,\ \cdots,\ n_b\}$ 表示线路集合. 发电机有功出力 P_i 与支路 r 的有功潮流 P_{lr} 被选作安全指标, 其运行约束作为求解目标函数的必要条件, 可表示为:

$$\begin{cases} P_i^m \le P_i \le P_i^M,\ \ \forall i \in G \\ P_{lr}^m \le P_{lr} \le P_{lr}^M,\ \forall r \in B \end{cases} \tag{9}$$

目标函数 $F(x)$ 被设定为电力系统稳态分析中的有功潮流方程[179]:

$$F(x) = P_i - V_i \sum_{j\in i} V_j \left(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}\right) = 0 \tag{10}$$

其中, V_i 表示节点 i 的电压幅值; $G_{ij}+jB_{ij}$ 为节点导纳矩阵中第 i 行第 j 列的元素, 对应节点 i 与节点 j 之间的支路电导和电纳; θ_{ij} 为对应节点 i 与节点 j 之间的电压相角差.

为降低计算复杂度, 在研究电力系统静态安全域时, 通常会引入两个合理的近似假设以简化有功潮流方程的表达形式: 1) 在系统运行稳定且支路电压相角差 $|\theta_{ij}|$ 足够小时, 可采用小角度近似, 令 $\cos\theta_{ij}\approx 1$ 及 $\sin\theta_{ij}\approx\theta_i-\theta_j=\theta_{ij}$; 2) 在支路电阻远小于支路电抗时, 可以忽略电阻对有功潮流的影响, 令支路电导 $G_{ij}=0$. 基于上述假设, 作为目标函数 $F(x)$ 的有功潮流方程可进一步简化为[180]:

$$F(x) = P_i - V_i \sum_{j\in i} V_j B_{ij}\theta_{ij} = 0 \tag{11}$$

针对式 (11), 需要求解的状态向量 $\boldsymbol{x}_\beta=\{\theta_0,\ V_0,\ P_1,\ P_2,\ \cdots,\ P_n,\ V_1,\ \cdots,\ V_{n_g}\}\in\mathbf{R}^{n+n_g+2}$. 其中, 包括参考节点的电压相角与幅值 ($\theta_0$ 和 V_0)、各发电机节点的有功出力 ($P_1,\ P_2,\ \cdots,\ P_n$) 及不同节点的电压幅值 ($V_1,\ V_2,\ \cdots,\ V_{n_g}$). 在满足目标函数与约束条件的前提下, 所有可行状态向量 $\boldsymbol{x}_\beta$ 所构成的集合即为电力系统的静态安全域, 如图 17 所示[2]. 为便于计算和分析, 通过节点的有功功率注入向量 $\boldsymbol{P}$ 对静态安全域进行等效刻画, 并最终将其定义为[181]:

$$\boldsymbol{\Omega}_s = \left\{ \boldsymbol{P}\in\mathbf{R}^n \left| \begin{array}{l} P_i^m \le P_i \le P_i^M,\ \forall i\in G \\ \left|\sum\limits_{i=1}^{n}\gamma_{r,\,i}P_i\right| \le 1,\ \forall r\in B \end{array} \right. \right\} \tag{12}$$

其中, $\gamma_{r,\,i}$ 是支路 r 上基于最大允许潮流幅值得到的边界权重系数.

上述方法基于对电力系统物理规律的显式表达及目标函数的推导求解, 完成了静态安全域相关的数学描述. 然而, 此类方法高度依赖于电力系统本身的运行机制和结构假设, 难以直接迁移至其他结构复杂、变量耦合强烈的复杂工程系统中进行应用.

[2] 图中的 $x_{\beta,\,1}$ 和 $x_{\beta,\,2}$ 表示从状态向量 $\boldsymbol{x}_\beta$ 中任意选取的两个互不相同的分量

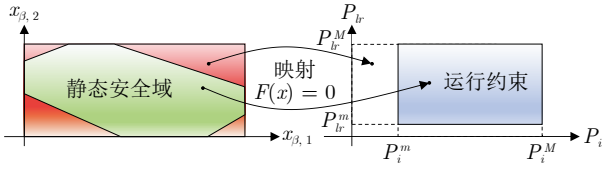


图 17　静态安全域与运行约束之间的关系[182]

Fig. 17　Relationship between SSR and operational constraints[182]

针对这一局限, 研究者提出一类更为通用的静态安全域刻画方法. 其核心思想是通过收集并分析系统在各项运行约束边界条件下产生的临界点数据, 借助线性或非线性方法近似拟合由临界点构成的安全边界, 形成不同的超平面, 进而刻画安全域的整体形状与结构, 如图 18 所示.

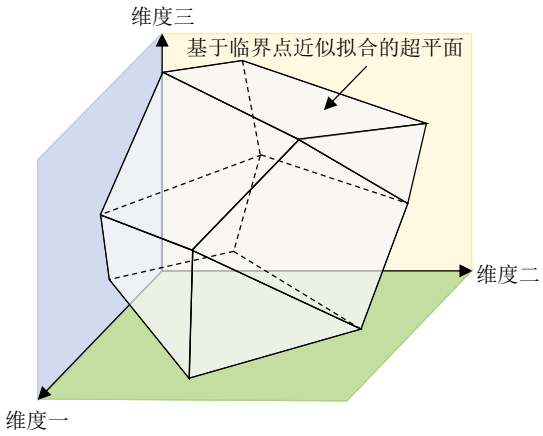


图 18　基于超平面构建的静态安全域

Fig. 18　SSR constructed by hyperplanes

在线性近似中, 王成山等[183] 在割集空间中对电压稳定区边界进行大规模临界采样, 并通过线性表达式对临界点进行拟合, 构建了能够整体逼近安全边界的线性超平面. 文献 [184] 采用最小二乘法, 针对割集空间中的临界点构建了近似的线性超平面, 进一步验证了线性近似方法在安全边界拟合中的适用性. 文献 [185] 先后结合多元线性模型与显著性指标, 对 $N-1$ 个热稳定约束下的电网安全边界进行建模与分析. 然而, 复杂工程系统的安全边界往往呈现出高度的非线性特征, 单纯的线性近似难以对其进行准确捕捉与刻画. 为此, 文献 [186−187] 提出一种基于分段线性的动态自适应差分进化算法, 用于动态逼近由若干线性超平面构成的非线性边界. 文献 [188] 将隐函数定理与二阶泰勒展开相结合, 通过刻画系统在局部邻域内的高阶变化特征, 实现了对非线性边界的精确逼近. 文献 [189] 进一步发展了结合泰勒展开与梯度投影的方法, 来对安全边界的非光滑分布特征进行实时监测与处理. Sun 等[190] 和 Gutierrez-Martinez 等[191] 通过人工神经网络从临界样本中学习输入与边界之间的非线性映射关系, 从而实现对复杂安全边界的拟合. 此外, 基于 Galerkin 的方法[192] 及多项式拟合[193] 也是较为常见的非线性近似拟合方法.

与此同时, 部分研究者开始从数据分布建模的角度出发, 将安全边界的刻画转化为对安全状态与不安全状态之间最优判别超平面的学习问题. 该方法不依赖于系统的显式模型与内部安全约束, 而是依托于已有的历史运行数据, 采用机器学习、深度学习等数据驱动技术, 在状态空间中构建出可区分不同运行状态的决策边界, 从而实现对复杂系统安全边界的自动判别与学习. 文献 [194] 将系统故障考虑为不安全状态, 并利用一类模糊 C 均值聚类算法 (type 1 fuzzy C-means algorithm, T1FCM) 对系统在正常和故障状态下的运行边界进行识别, 进而界定了轨道车辆的安全运行区域, 如图 19 所示. He 等[195−196] 以飞行系统的俯仰角 θ、攻角 α 和空速 v 作为安全指标, 利用深度神经网络 (deep neural network, DNN) 及深度循环残差神经网络 (deep recurrent residual neural network, DR-RNN) 对安全指标数据对应的非线性判别边界进行隐式建模, 并通过动态调整网络的权重分布来表征飞行系统在不同运行状态下的安全边界, 如图 20 所示.

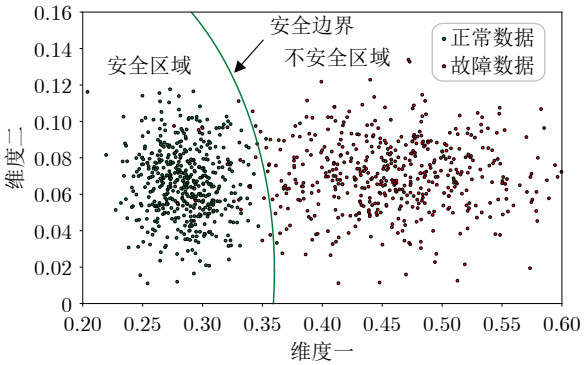


图 19　基于分类的安全边界识别[194]

Fig. 19　Safety boundaries identified by classification[194]

从已有的研究成果来看, 目前基于静态安全域的方法主要依托于系统的运行约束和采样临界点, 通过目标函数求解、超平面拟合及边界学习等手段对系统的安全运行范围进行刻画. 然而, 方法本身所依赖的静态假设, 使其所刻画的安全区域难以全面地覆盖工程系统在实际运行过程中由于外部扰动、工况切换等因素影响而改变的安全状态. 因此, 突破静态假设、发展能够反映系统时变行为特征的动态安全域, 已逐渐成为当前安全分析领域的重要研究方向.

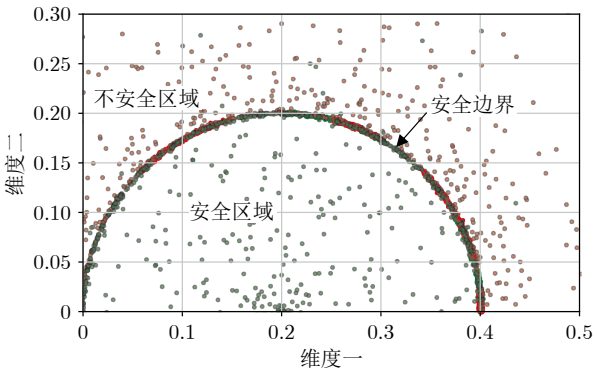


图 20 基于深度神经网络的安全边界识别[195]

Fig. 20 Safety boundaries identified by DNN[195]

4.2 基于动态安全域的方法

动态安全域 (dynamic safety region, DSR) 作为近年来过程安全领域的新概念, 目前尚无统一的定义. 不同的专家学者和研究组织针对动态安全域给出了不同形式的解读, 并随即衍生出了相应的一般性理论. Yu 等[197−199] 从电力系统的暂态稳定角度出发, 将动态安全域定义为事故前节点功率注入空间中, 所有能够在事故后保持系统暂态稳定的运行点集合. 具体而言, 在给定网络拓扑结构和预设事故场景下, 若某一特定的功率注入向量在系统遭受预设事故后仍能够保持暂态稳定, 则认为该运行点是动态安全的. 所有满足此条件的功率注入点构成了该事故场景下的动态安全域. 假设特定预想事故场景为 s_d, 事故前/后的网络结构分别为 $\boldsymbol{G}_i$ 和 $\boldsymbol{G}_j$, 则该情形下的动态安全域可定义为[200]:

$$\boldsymbol{\Omega}_d(\boldsymbol{G}_i,\ \boldsymbol{G}_j,\ s_d) = \{\boldsymbol{x}_\beta | \boldsymbol{x}_d(\boldsymbol{x}_\beta) \in A(\boldsymbol{x}_\beta)\} \tag{13}$$

其中, $\boldsymbol{x}_d(\boldsymbol{x}_\beta)$ 表示事故清除时刻由功率注入 $\boldsymbol{x}_\beta$ 所对应的系统状态; $A(\boldsymbol{x}_\beta)$ 是事故后系统状态空间内基于功率注入 $\boldsymbol{x}_\beta$ 所决定的暂态稳定域. 动态安全域 $\boldsymbol{\Omega}_d$ 则可以被视为事故前功率注入空间中所有能使事故后系统状态 $\boldsymbol{x}_d(\boldsymbol{x}_\beta)$ 收敛至对应暂态稳定域 $A(\boldsymbol{x}_\beta)$ 的运行点集合. 其中, 暂态稳定域 $A(\boldsymbol{x}_\beta)$ 和动态安全域 $\boldsymbol{\Omega}_d$ 的关系如图 21 所示.

在结合电力系统实际情况的基础上, 文献 [201] 研究了实用动态安全域 (practical dynamic security region, PDSR), 并指出其在有功注入空间中表现为一个超多面体, 由节点注入功率上/下限形成的超平面及暂态稳定临界超平面共同围成. 文献 [202] 利用微分拓扑理论, 证明了动态安全域边界面的无扭扩性 (不会打结)、紧致性 (可由有限子表面并集表示) 与稠密性 (内部无空洞). 值得注意的是, 该种定义以功率注入为出发点, 以系统在预设事故后能

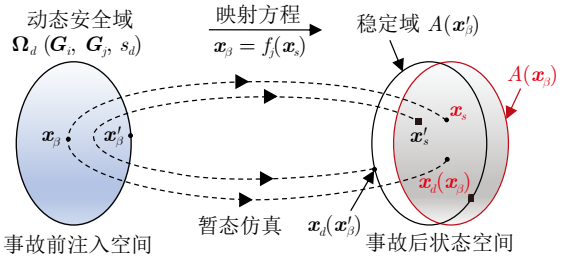


图 21 稳定域和动态安全域的区别与关联[200]

Fig. 21 Difference and relationship between stable region and DSR[200]

否实现动态收敛为判据, 构建了具有明确边界“稳定域”作为系统的动态安全域, 反映了系统在特定时刻和工况下承受预设事故并维持暂态稳定的能力. 然而, 复杂工程系统通常涉及多种运行工况, 各工况下的安全域可能存在显著的差异. 为此, 有研究进一步从系统运行状态的动态演化过程出发, 将动态安全域定义为随时间和标称工况变化而不断更新的安全域集合[203], 如图 22 所示.

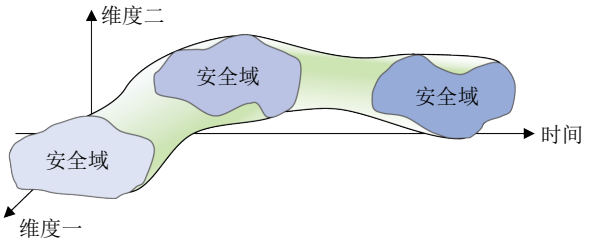


图 22 动态安全域示意图

Fig. 22 Schematic diagram of DSR

基于上述定义, 安全域被重新考虑为系统所处安全状态的概率性区域. 相应地, 安全域的动态演变被考虑为概率分布在多维时序空间中的迁移与重构. 因此, 能够有效刻画系统状态概率分布演化规律的方法被引入至动态安全域的研究当中. Li 等[204] 首先提出一种基于广义概率密度演化方程 (generalized probability density evolution equation, GDEE) 的概率密度演化方法, 并将其用于复杂系统概率密度演化的建模与分析, 如图 23 所示.

文献 [205] 对广义概率密度演化方程的初始条件进行了优化, 并引入平滑的 Dirac Delta 函数来增强动态安全域边界建模的适用性. 文献 [206] 提出基于物理信息神经网络 (physics informed neural network, PINN) 的概率密度演化框架, 通过转移概率密度函数计算高层木结构建筑整体的失效概率, 实现了建筑性能的动态安全分析. Lv 等[207] 和 Behrendt 等[208] 在确保概率守恒的前提下, 构建了面向多变量响应的联合概率密度函数, 揭示了系统

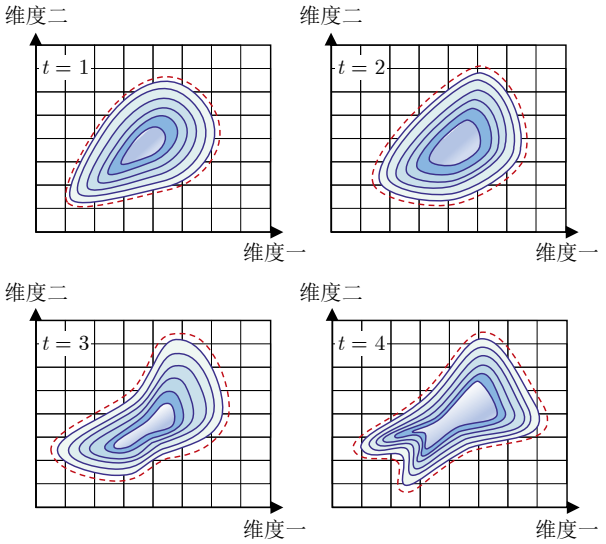


图 23　基于广义概率密度演化方程的概率密度演变过程

Fig. 23　Probability density evolution process based on GDEE

在不确定激励下的演化规律. 此外, 文献 [209] 提出一种基于耗散模型的吸引子理论, 将复杂动力系统视为在 N 维相空间中随时间演变并逐渐收缩至低维点集 (吸引子) 的耗散系统, 用于描述系统在不同初始条件下的演化结果. 受此启发, 文献 [210] 将吸引子理论引入至有限状态网络模型, 用于分析飞行系统在不同潜在风险模式下的动态演化过程及其状态收敛特性, 为动态安全域的求解与构建提供了新的可行思路.

总体而言, 尽管现有的研究在动态安全域的定义方式及其应用研究上各有侧重, 但随着研究的深入, 围绕复杂工程系统的动态安全域进行表征与刻画, 并据此展开安全分析与评估, 已逐渐成为当前安全领域的主流研究趋势. 然而, 无论是上述提到的静态安全域还是动态安全域, 都普遍忽略了外部扰动对系统安全状态的影响. 对于闭环控制系统来说, 微小、瞬时出现但又立即消失的扰动往往并不会导致系统进入单调发散或持续震荡的状态. 这种具有非持久性和可恢复性的系统状态即非绝对“安全”, 也不构成真正意义上的“不安全”, 更应被视为介于两者之间的过渡态[211]. 因此, 将系统扰动情况下的系统响应行为纳入至安全域的理论框架中, 并针对安全域的安全边界进行延展, 构建更具鲁棒性的扰动安全域[212], 是未来研究的一个可行方向.

5　思考与展望

对于复杂工程系统来说, 如何充分利用系统工程知识、历史运行数据及实时监测信息, 持续提升系统风险描述的全面性、安全表征的科学性、状态分析的准确性, 是确保其安全可靠运行的核心途径. 为此, 本文提出一种安全分析的实施流程框架, 从安全事件识别、评估指标选取、事故模型构建到安全区域刻画, 为复杂工程系统的安全评估与决策提供清晰的操作思路与方法支撑. 受制于当前技术的发展水平, 本节总结了一些重要但仍需解决的关键问题, 并给出未来值得深入探究的研究方向.

5.1　人工智能驱动下的安全分析

本文所提出的安全分析框架依赖于对所有潜在安全风险及其后果的显式枚举. 然而, 在结构高度复杂、风险耦合关系密集的工程系统中, 由于可穷举性不足及耦合关系难以准确建模等问题, 使得该框架在现实场景中的可适用性与可操作性受到了显著的制约.

近年来, 人工智能技术的快速发展为突破上述制约提供了新的思路与技术路径. 人工智能技术凭借其在数据挖掘、高维表征及非线性建模等方面的能力与优势, 能够对复杂高维的系统运行数据进行有效降维, 精确提取潜在耦合关系与关联特征, 并借助知识推理实现高效的风险认知与决策推导. 因此, 充分考虑不同工程系统的运行特性与安全需求, 结合机器学习与深度学习等人工智能技术, 进一步展开安全事件分析与风险指标选取, 构建从安全隐患到事故的风险模型, 并设计契合不同应用场景的安全分析框架[213], 是未来一个重要的研究方向.

5.2　结合韧性工程的安全分析

当前的安全分析框架以潜在安全风险为核心, 评估了风险发生的概率及其触发后果的严重程度, 并着重刻画了风险演化过程中对系统性能造成的累积性退化, 然而却普遍忽视了风险冲击后对系统动态恢复能力的综合性描述.

韧性这一概念被广泛应用于生态、能源以及经济等领域, 用于表征系统抵御灾害扰动、快速恢复正常运营的能力. 与传统安全分析主要关注风险发生的可能性及其后果严重程度不同的是, 韧性工程侧重于描述风险发生后系统性能的动态变化[214–215]. 因此, 在未来的研究中, 能否从韧性的角度去考虑复杂工程系统的动态性能恢复模式与规律, 明晰系统所处状态及其安全裕度, 从而实现复杂工程系统中风险事件的广义表征, 是一个有价值的研究方向.

5.3　从安全分析迈向安全控制的理论研究

目前安全分析框架给出的分析结果独立于系统的运行闭环之外, 缺乏与反馈控制及操作干预等机

制的有效融合. 这种安全分析与系统闭环控制分离的形式, 使得复杂工程系统的安全保障更多地停留在事后评估的层面, 难以及时响应系统状态及外部环境扰动所带来的动态影响, 从而在一定程度上制约了系统安全防护的实时性与主动性.

因此, 将安全视为一种可调控、可约束的系统特性, 并将其纳入至控制理论框架之内, 通过合理地设计控制输入并引入安全约束, 使系统在运行过程中能够自主地规避风险状态, 实现系统安全的主动调控, 将是未来一个重要的研究方向. 在此背景下, 研究者参考 Lyapunov 函数的基本思想, 提出名为障碍函数 (barrier function) 的分析方法. 该方法借助满足特定微分不等式的障碍函数, 将系统状态需始终维持在安全集合内的要求, 转化为判断控制输入是否满足障碍函数导数约束的判定问题, 并通过构造满足约束的控制律在理论上实现系统安全的主动控制[216]. 然而, 在高维、非线性的复杂工程系统上[217−218], 相关的分析方法仍有待进一步发展.

6 结论

本文面向复杂工程系统运行过程中日益凸显的安全需求, 首先概述安全及相关基础概念, 并从系统本体运行安全的角度出发, 给出安全分析的具体实施流程框架. 围绕实施框架中的关键环节, 系统回顾了现有研究在安全事件识别、评估指标选取、事故模型构建、安全区域刻画等方面的主要方法与进展, 进而凝练出其所面临的关键问题与核心挑战. 最后, 针对上述问题与挑战, 对复杂工程系统的安全分析研究进行思考与展望, 详细探讨了人工智能技术、韧性工程及控制理论在提升系统安全分析能力、优化安全决策与实现主动防护等方面的未来研究方向.

参考文献

1 Lu C, Li S, Xu K, Zhang Y. Research on data-driven coal mine environmental safety risk assessment system. *Safety Science*, 2025, **183**: Article No. 106727

2 Yang Chun-Hua, Sun Bei, Li Yong-Gang, Huang Ke-Ke, Gui Wei-Hua. Cooperative optimization and intelligent control of complex production processes. *Acta Automatica Sinica*, 2023, **49**(3): 528−539
(阳春华, 孙备, 李勇刚, 黄科科, 桂卫华. 复杂生产流程协同优化与智能控制. 自动化学报, 2023, **49**(3): 528−539)

3 Chu Fei, Hao Li-Li, Wang Fu-Li. Review and prospect of operation performance assessment methods for complex industrial processes. *Control and Decision*, 2024, **39**(3): 705−718
(褚菲, 郝莉莉, 王福利. 复杂工业过程运行状态评价方法回顾与展望. 控制与决策, 2024, **39**(3): 705−718)

4 Chai Yi, Zhang Ke, Mao Yong-Fang, Wei Shan-Bi. *Operational Safety Analysis Technology for Dynamic Systems*. Beijing: Chemical Industry Press, 2019.
(柴毅, 张可, 毛永芳, 魏善碧. 动态系统运行安全性分析与技术. 北京: 化学工业出版社, 2019.)

5 He Xiao, Liu Ze-Yi, Hu Song-Qiao, Liu Chang, Zhou Dong-Hua. Real-time safety assessment techniques of dynamic systems. *Acta Automatica Sinica*, 2025, **51**(2): 249−270
(何潇, 刘泽夷, 胡嵩乔, 刘畅, 周东华. 动态系统的实时安全性评估技术. 自动化学报, 2025, **51**(2): 249−270)

6 System Safety, MIL-STD-882E, 2012.

7 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems, IEC 61508-1, 2010.

8 Safety Aspects——Guidelines for Their Inclusion in Standards, ISO/IEC Guide 51:2019, 2019.

9 Leveson N G. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge: MIT Press, 2012.

10 Hollnagel E. *Barriers and Accident Prevention*. London: Routledge, 2004.

11 Khan F I, Amyotte P R, Amin M T. Advanced methods of risk assessment and management: An overview. *Methods in Chemical Process Safety*, 2020, **4**: 1−34

12 Rasmussen J. Risk management in a dynamic society: A modelling problem. *Safety Science*, 1997, **27**(2−3): 183−213

13 Dallat C, Salmon P M, Goode N. Risky systems versus risky people: To what extent do risk assessment methods consider the systems approach to accident causation? A review of the literature. *Safety Science*, 2019, **119**: 266−279

14 Rad M A, Lefsrud L M, Hendry M T. Application of systems thinking accident analysis methods: A review for railways. *Safety Science*, 2023, **160**: Article No. 106066

15 Yousefi A, Hernandez M R, Peña V L. Systemic accident analysis models: A comparison study between AcciMap, FRAM, and STAMP. *Process Safety Progress*, 2019, **38**(2): Article No. e12002

16 Yuan C H, Fu G, Wu Z R, Zhao J K, Han M, Ye S P. Theory and practice of solution strategies for unsafe acts based on accident causation models: A systematic review. *Journal of Loss Prevention in the Process Industries*, 2025, **95**: Article No. 105605

17 Wu Y L, Fu G, Han M, Jia Q S, Lv Q, Wang Y X, et al. Comparison of the theoretical elements and application characteristics of STAMP, FRAM, and 24Model: A major hazardous chemical explosion accident. *Journal of Loss Prevention in the Process Industries*, 2022, **80**: Article No. 104880

18 Amin M T, Khan F. Dynamic process safety assessment using adaptive Bayesian network with loss function. *Industrial & Engineering Chemistry Research*, 2022, **61**(45): 16799−16814

19 Hu Y W, Parhizkar T, Mosleh A. Guided simulation for dynamic probabilistic risk assessment of complex systems: Concept, method, and application. *Reliability Engineering & System Safety*, 2022, **217**: Article No. 108047

20 Aven T. The risk concept-historical and recent development trends. *Reliability Engineering & System Safety*, 2012, **99**: 33−44

21 Willis H H. Guiding resource allocations based on terrorism risk. *Risk Analysis*, 2007, **27**(3): 597−606

22 Leimeister M, Kolios A. A review of reliability-based methods for risk analysis and their application in the offshore wind industry. *Renewable and Sustainable Energy Reviews*, 2018, **91**: 1065−1076

23 Khan F, Rathnayaka S, Ahmed S. Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection*, 2015, **98**: 116−147

24 Bharatbhai M G. Failure mode and effect analysis of repower 5M wind turbine. *International Journal of Advance Research in Engineering, Science & Technology*, 2015, **2**(5): 7−14

25 Rausand M, Hoyland A. *System Reliability Theory: Models, Statistical Methods, and Applications* (Second edition).

Hoboken: John Wiley & Sons, 2003.

26 Han Y H, Li Q, Wang C, Zhao Q. A novel knowledge enhanced graph neural networks for fault diagnosis with application to blast furnace process safety. *Process Safety and Environmental Protection*, 2022, **166**: 143−157

27 Song T F, Zhang J L, Wang G W, Wang H Y, Xu R S. Influencing factors of the explosion characteristics of modified coal used for blast furnace injection. *Powder Technology*, 2019, **353**: 171−177

28 Jiang K, Jiang Z H, Jiang X D, Xie Y F, Gui W H. Reinforcement learning for blast furnace ironmaking operation with safety and partial observation considerations. *IEEE Transactions on Neural Networks and Learning Systems*, 2024, **35**(3): 3077−3090

29 Vuorio A, Stoop J, Johnson C. The need to establish consistent international safety investigation guidelines for the chemical industries. *Safety Science*, 2017, **95**: 62−74

30 Yang J F, Wang P C, Liu X Y, Bian M C, Chen L C, Lv S Y, et al. Analysis on causes of chemical industry accident from 2015 to 2020 in Chinese mainland: A complex network theory approach. *Journal of Loss Prevention in the Process Industries*, 2023, **83**: Article No. 105061

31 Soltanzadeh A, Yarandi M S, Jazari M D, Mahdinia M. Incidence investigation of accidents in chemical industries: A comprehensive study based on factor analysis. *Process Safety Progress*, 2022, **41**(3): 531−537

32 Zhou T T, Zhang L B, Hu J Q, Modarres M, Droguett E L. A critical review and benchmark study of dependency modeling for seismic probabilistic risk assessment in the nuclear power industry. *Reliability Engineering & System Safety*, 2024, **245**: Article No. 110009

33 Yao Y T, Han T, Yu J, Xie M. Uncertainty-aware deep learning for reliable health monitoring in safety-critical energy systems. *Energy*, 2024, **291**: Article No. 130419

34 Kuhn K D. Using structural topic modeling to identify latent topics and trends in aviation incident reports. *Transportation Research Part C: Emerging Technologies*, 2018, **87**: 105−122

35 Chai Yi, Mao Wan-Biao, Ren Hao, Qu Jian-Feng, Yin Hong-Peng, Yang Zhi-Min, et al. Research on operational safety assessment for spacecraft launch system: Progress and challenges. *Acta Automatica Sinica*, 2019, **45**(10): 1829−1845
(柴毅, 毛万标, 任浩, 屈剑锋, 尹宏鹏, 杨志敏, 等. 航天发射系统运行安全性评估研究进展与挑战. 自动化学报, 2019, **45**(10): 1829−1845)

36 Oster C V, Strong J S, Zorn C K. Analyzing aviation safety: Problems, challenges, opportunities. *Research in Transportation Economics*, 2013, **43**(1): 148−164

37 Rey M, Aloise D, Soumis F, Pieugueu R. A data-driven model for safety risk identification from flight data analysis. *Transportation Engineering*, 2021, **5**: Article No. 100087

38 Chai Yi. Intelligent space launch system and its key technology. *National Defense Science & Technology*, 2016, **37**(1): 7−9
(柴毅. 智能化航天发射系统及其关键技术研究. 国防科技, 2016, **37**(1): 7−9)

39 Rawson A, Brito M. A survey of the opportunities and challenges of supervised machine learning in maritime risk analysis. *Transport Reviews*, 2023, **43**(1): 108−130

40 Chen P F, Huang Y M, Mou J M, van Gelder P H A J M. Probabilistic risk analysis for ship-ship collision: State-of-the-art. *Safety Science*, 2019, **117**: 108−122

41 Jiang Shao-Qi, Chen Wei-Jiong, Xie Qi-Miao, Wang Jin-Hui, Zhang Pan-Fei. Identification of critical causes of marine accidents based on correlation analysis. *Navigation of China*, 2020, **43**(4): 33−38
(蒋少奇, 陈伟炯, 谢启苗, 汪金辉, 张盼飞. 基于关联分析的船舶事故关键致因识别. 中国航海, 2020, **43**(4): 33−38)

42 Tan Z, Gou H Y, Li W H, Bao Y. Effect of frost heave deformation of bridge foundation on operation safety of high-speed railway. *Structures*, 2023, **47**: 2099−2112

43 Wu X T, Lian W B, Zhou M, Bai W Q, Yang M K, Dong H R. Critical spatial-temporal node identification for a high-speed railway network: A cascading delay perspective. *IEEE Transactions on Network Science and Engineering*, 2024, **11**(1): 823−833

44 Zhang D N, Chen F, Zhu J Y, Wang C Z, Cheng J C, Zhang Y L, et al. Research on drivers′ hazard perception in plateau environment based on visual characteristics. *Accident Analysis & Prevention*, 2022, **166**: Article No. 106540

45 Bai X Y, Fan Y F, Hou J J. Reliability assessment method of wind power DC transmission system based on level fault tree analysis. *Energy*, 2025, **327**: Article No. 136426

46 Zhu C Y, Jiang Y J, Liu G Y, Zhang T Y. Integration frameworks and intelligent research in dynamic fault tree: A comprehensive review and future perspectives. *Quality and Reliability Engineering International*, 2023, **39**(7): 3157−3178

47 Cui Tie-Jun, Li Sha-Sha. Revision of the space fault tree and the space fault network system. *Journal of Safety and Environment*, 2019, **19**(2): 399−405
(崔铁军, 李莎莎. 空间故障树与空间故障网络理论综述. 安全与环境学报, 2019, **19**(2): 399−405)

48 Kaiser B, Gramlich C. State-event-fault-trees——A safety analysis model for software controlled systems. In: Proceedings of the 23rd International Conference on Computer Safety, Reliability and Security. Potsdam, Germany: Springer, 2004. 195−209

49 Huang Kun, Wang Hai-Tao, An Long-Kun. Probability assessment of safety risk occurrence based on minimum cut set fault tree analysis method. *Shipboard Electronic Countermeasure*, 2024, **47**(3): 45−50
(黄坤, 汪海涛, 安隆坤. 基于最小割集故障树分析的安全风险发生概率评估. 舰船电子对抗, 2024, **47**(3): 45−50)

50 Reay K A, Andrews J D. A fault tree analysis strategy using binary decision diagrams. *Reliability Engineering & System Safety*, 2002, **78**(1): 45−56

51 Remenyte-Prescott R, Andrews J. Analysis of non-coherent fault trees using ternary decision diagrams. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 2008, **222**(2): 127−138

52 Boudali H, Crouzen P, Stoelinga M. A compositional semantics for dynamic fault trees in terms of interactive Markov chains. In: Proceedings of the 5th International Symposium on Automated Technology for Verification and Analysis. Tokyo, Japan: Springer, 2007. 441−456

53 Yevkin O. An efficient approximate Markov chain method in dynamic fault tree analysis. *Quality and Reliability Engineering International*, 2016, **32**(4): 1509−1520

54 Kabir S, Walker M, Papadopoulos Y. Dynamic system safety analysis in HiP-HOPS with Petri nets and Bayesian networks. *Safety Science*, 2018, **105**: 55−70

55 Kabir S, Walker M, Papadopoulos Y. Quantitative evaluation of Pandora temporal fault trees via Petri nets. *IFAC-PapersOnLine*, 2015, **48**(21): 458−463

56 Codetta-Raiteri D, Portinale L. Approaching dynamic reliability with predictive and diagnostic purposes by exploiting dynamic Bayesian networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 2014, **228**(5): 488−503

57 Barua S, Gao X D, Pasman H, Mannan M S. Bayesian network based dynamic operational risk assessment. *Journal of Loss Prevention in the Process Industries*, 2016, **41**: 399−410

58 Sun D B, Li L, Tian Z F, Chen S J, Wang H, Chen G L, et al. An advanced probability safety margin analysis approach combined deterministic and probabilistic safety assessment. *Nuclear Engineering and Design*, 2021, **385**: Article No. 111514

59 Rahman S, Karanki D R, Epiney A, Wicaksono D, Zerkak O,

Dang V N. Deterministic sampling for propagating epistemic and aleatory uncertainty in dynamic event tree analysis. *Reliability Engineering & System Safety*, 2018, **175**: 62−78

60 Maidana R G, Parhizkar T, san Martin G, Utne I B. Dynamic probabilistic risk assessment with K-shortest-paths planning for generating discrete dynamic event trees. *Reliability Engineering & System Safety*, 2024, **242**: Article No. 109725

61 Baek S, Heo G. Development of dynamic integrated consequence evaluation (DICE) for dynamic event tree approaches: Numerical validation for a loss of coolant accident. *Reliability Engineering & System Safety*, 2023, **238**: Article No. 109425

62 Chi L X, Su H, Zio E, Zhang J J, Li X Y, Zhang L, et al. Integrated deterministic and probabilistic safety analysis of integrated energy systems with bi-directional conversion. *Energy*, 2020, **212**: Article No. 118685

63 Sun D B, Li L, Tian Z F, Wang H, Chen G L. Research on simplification of branches method of accident sequences based on expert knowledge and heuristic optimization algorithm. *Nuclear Engineering and Design*, 2023, **404**: Article No. 112198

64 Liang T H, Liang K S, Cheng C K, Pei B S, Patelli E. Risk-informed analysis of the large break loss of coolant accident and PCT margin evaluation with the RISMC methodology. *Nuclear Engineering and Design*, 2016, **308**: 214−221

65 Kaneko F, Yuzui T. Novel method of dynamic event tree keeping the number of simulations in risk analysis small. *Reliability Engineering & System Safety*, 2023, **231**: Article No. 109009

66 Martin N S, Denman M R, Wheeler T A. Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping, Technical Report SAND2016-5632C, Sandia National Laboratory, USA, 2016.

67 Queral C, Fernández-Cosials K, Zugazagoitia E, Paris C, Magan J, Mendizabal R, et al. Application of expanded event trees combined with uncertainty analysis methodologies. *Reliability Engineering & System Safety*, 2021, **205**: Article No. 107246

68 Yu S Z, Zhang J Z, Labeau P E. Safety margin quantification by integrating probabilistic and deterministic safety assessments: Application to design extension conditions. *Nuclear Engineering and Design*, 2024, **421**: Article No. 113121

69 Mazgaj P, Darnowski P, Kaszko A, Hortal J, Dusic M, Mendizábal R, et al. Demonstration of the E-BEPU methodology for SL-LOCA in a Gen-III PWR reactor. *Reliability Engineering & System Safety*, 2022, **226**: Article No. 108707

70 Martorell S, Sánchez-Sáez F, Villanueva J F, Carlos S. An extended BEPU approach integrating probabilistic assumptions on the availability of safety systems in deterministic safety analyses. *Reliability Engineering & System Safety*, 2017, **167**: 474−483

71 Pirbalouti R G, Behnam B, Dehkordi M K. A risk-based approach to identify safety-critical equipment in process industries. *Results in Engineering*, 2023, **20**: Article No. 101448

72 Khakzad N, Khan F, Amyotte P. Dynamic risk analysis using bow-tie approach. *Reliability Engineering & System Safety*, 2012, **104**: 36−44

73 Yuan S Q, Reniers G, Yang M, Bai Y P. Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm. *Process Safety and Environmental Protection*, 2023, **170**: 356−371

74 Huang Y J, Zhang Z P, Tao Y, Hu H. Quantitative risk assessment of railway intrusions with text mining and fuzzy rule-based bow-tie model. *Advanced Engineering Informatics*, 2022, **54**: Article No. 101726

75 Yang L, Li K P. Safety risk analysis of railway accident with text-based bow-tie model. In: Proceedings of the 3rd International Conference of Safe Production and Informatization (IICSPI). Chongqing, China: IEEE, 2020. 200−204

76 Kuzucuoğlu D, Koc K, Kazar G, Tokdemir O B. Prioritization of risk mitigation strategies for contact with sharp object accidents using hybrid bow-tie approach. *Safety Science*, 2023, **166**: Article No. 106248

77 Slatnick S, Angevine D, Cranefield J, Maddox C, Overstake M, Palmer L, et al. Bow-ties use for high-consequence marine risks of offshore structures. *Process Safety and Environmental Protection*, 2022, **165**: 396−407

78 Abimbola M, Khan F, Khakzad N. Dynamic safety risk analysis of offshore drilling. *Journal of Loss Prevention in the Process Industries*, 2014, **30**: 74−85

79 Olamigoke O, Odumade A A, Abhulimen K E, Ehinmowo A B, Orodu O D. Risk assessment of floating, production, storage and offloading (FPSO) risers using bow-tie methodology. In: Proceedings of the 18th International Health, Safety and Environment Biennial Conference on the Oil and Gas Industry (IHSEB). Lagos, Nigeria: Society of Petroleum Engineers, 2018. 1−13

80 Deacon T, Amyotte P R, Khan F I, MacKinnon S. A framework for human error analysis of offshore evacuations. *Safety Science*, 2013, **51**(1): 319−327

81 Li K P, Wang S S. A network accident causation model for monitoring railway safety. *Safety Science*, 2018, **109**: 398−402

82 Huang Y J, Zhang Z P, Hu H. Risk propagation mechanisms in railway systems under extreme weather: A knowledge graph-based unsupervised causation chain approach. *Reliability Engineering & System Safety*, 2025, **260**: Article No. 110976

83 Zhang L, Du Y, Li A. Rapid cascading risk assessment and vulnerable satellite identification schemes for LEO satellite networks. *Reliability Engineering & System Safety*, 2025, **256**: Article No. 110699

84 Zhang L, Du Y. Cascading failure model and resilience enhancement scheme of space information networks. *Reliability Engineering & System Safety*, 2023, **237**: Article No. 109379

85 Hu Y, Meng Z, Hu Y Z, Tian W J, Yang Y Y, Gao S L. Modelling of accident dynamic spreading based on spike timing dependent plasticity. *Process Safety and Environmental Protection*, 2022, **159**: 727−739

86 Han Y W, Shen J, Zhu X W, Bao X Y. Two-stage propagation analysis of safety risks in complex underground engineering: An integrated modeling framework. *Reliability Engineering & System Safety*, 2025, **261**: Article No. 111081

87 Amin M T, Scarponi G E, Cozzani V, Khan F. Dynamic domino effect assessment (D2EA) in tank farms using a machine learning-based approach. *Computers & Chemical Engineering*, 2024, **181**: Article No. 108556

88 Amin M T, Scarponi G E, Cozzani V, Khan F. Improved pool fire-initiated domino effect assessment in atmospheric tank farms using structural response. *Reliability Engineering & System Safety*, 2024, **242**: Article No. 109751

89 Zeng T, Chen G H, Yang Y F, Chen P Z, Reniers G. Developing an advanced dynamic risk analysis method for fire-related domino effects. *Process Safety and Environmental Protection*, 2020, **134**: 149−160

90 Li X F, Chen G H, Amyotte P, Khan F, Alauddin M. Vulnerability assessment of storage tanks exposed to simultaneous fire and explosion hazards. *Reliability Engineering & System Safety*, 2023, **230**: Article No. 108960

91 Huang K X, Chen G H, Khan F, Yang Y F. Dynamic analysis for fire-induced domino effects in chemical process industries. *Process Safety and Environmental Protection*, 2021, **148**: 686−697

92 Ding L, Khan F, Abbassi R, Ji J. FSEM: An approach to model contribution of synergistic effect of fires for domino effects. *Reliability Engineering & System Safety*, 2019, **189**: 271−278

93 Zeng T, Wei L J, Reniers G, Chen G H. A comprehensive study for probability prediction of domino effects considering synergistic effects. *Reliability Engineering & System Safety*,

2024, **251**: Article No. 110318

94 Li X F, Chen G H, Amyotte P, Alauddin M, Khan F. Modeling and analysis of domino effect in petrochemical storage tank farms under the synergistic effect of explosion and fire. *Process Safety and Environmental Protection*, 2023, **176**: 706−715

95 Luo Z Y, Li K P, Ma X, Zhou J. A new accident analysis method based on complex network and cascading failure. *Discrete Dynamics in Nature and Society*, **2013**: Article No. 437428

96 Xu Y F, Wang Z, Jiang Y, Yang Y X, Wang F. Small-world network analysis on fault propagation characteristics of water networks in eco-industrial parks. *Resources, Conservation and Recycling*, 2019, **149**: 343−351

97 Zhang Y L, Yang N D, Lall U. Modeling and simulation of the vulnerability of interdependent power-water infrastructure networks to cascading failures. *Journal of Systems Science and Systems Engineering*, 2016, **25**(1): 102−118

98 Lu Z H, Wang X W, Liu L, Zhang X Y, Li C Q. An efficient method for network connectivity reliability computation considering correlation of components. *Reliability Engineering & System Safety*, 2025, **257**: Article No. 110805

99 Liu M, Chong H Y, Liao P C, Xu L Y. Probabilistic-based cascading failure approach to assessing workplace hazards affecting human error. *Journal of Management in Engineering*, 2019, **35**(3): Article No. 04019006

100 Xing J D, Yang W, Yin X L, Zio E. An integrated method of resilience and risk assessment for maintenance strategy optimization of a train braking system. *Reliability Engineering & System Safety*, 2025, **260**: Article No. 110929

101 Zhou J, Xu W X, Guo X, Ma X. Railway faults spreading model based on dynamics of complex network. *International Journal of Modern Physics B*, 2015, **29**(6): Article No. 1550038

102 Kang J, Meng X X, Su T, Chang W C, Wang Z X, Wang H, et al. Research on leakage control of river oil and gas pipelines based on accident situation evolution model. *Journal of Loss Prevention in the Process Industries*, 2025, **96**: Article No. 105615

103 Meng X K, Li X H, Wang W G, Song G Z, Chen G M, Zhu J Y. A novel methodology to analyze accident path in deepwater drilling operation considering uncertain information. *Reliability Engineering & System Safety*, 2021, **205**: Article No. 107255

104 Wang W C, Zhang Y, Li Y X, Hu Q H, Liu C S, Liu C W. Vulnerability analysis method based on risk assessment for gas transmission capabilities of natural gas pipeline networks. *Reliability Engineering & System Safety*, 2022, **218**: Article No. 108150

105 Wang W C, Zhang Y, Li Y X, Liu C S, Han S Y. Vulnerability analysis of a natural gas pipeline network based on network flow. *International Journal of Pressure Vessels and Piping*, 2020, **188**: Article No. 104236

106 Ren T, Xu Y J, Wang P Y. Identifying influential spreaders in complex network based on the node′s weight and spreading probability. *International Journal of Modern Physics C*, 2024, **35**(11): Article No. 2450142

107 Nazempour R, Monfared M A S, Zio E. A complex network theory approach for optimizing contamination warning sensor location in water distribution networks. *International Journal of Disaster Risk Reduction*, 2018, **30**: 225−234

108 Zhang Han, Wang Qiang. Aviation safety accident risk identification and evaluation based on directed networks. *Systems Engineering and Electronics*, 2024, **46**(6): 1995−2001
(张晗, 王强. 基于有向网络的航空安全事故风险识别与评估. 系统工程与电子技术, 2024, **46**(6): 1995−2001)

109 Zhang Han, Wang Qiang, Min Gui-Long. Aviation safety risk early warning model based on mean field theory. *Systems Engineering and Electronics*, 2025, **47**(1): 210−216
(张晗, 王强, 闵桂龙. 基于平均场理论的航空安全风险预警模型. 系统工程与电子技术, 2025, **47**(1): 210−216)

110 Zhou J, Xu W X, Guo X, Ding J. A method for modeling and analysis of directed weighted accident causation network (DWACN). *Physica A: Statistical Mechanics and Its Applications*, 2015, **437**: 263−277

111 Wang Z Y, Hill D J, Chen G, Dong Z Y. Power system cascading risk assessment based on complex network theory. *Physica A: Statistical Mechanics and Its Applications*, 2017, **482**: 532−543

112 Ma X G, Tsai Y T, Shu C M, Yang Y. Risk evolution analysis of gas leakage accidents based on complex network. *Safety Science*, 2025, **182**: Article No. 106692

113 Feng J R, Zhao M K, Lu S X. Accident spread and risk propagation mechanism in complex industrial system network. *Reliability Engineering & System Safety*, 2024, **244**: Article No. 109940

114 Jia M W, Jiang L W, Guo B, Liu Y, Chen T. Physical-anchored graph learning for process key indicator prediction. *Control Engineering Practice*, 2025, **154**: Article No. 106167

115 Jia M W, Yao Y, Liu Y. Review on graph neural networks for process soft sensor development, fault diagnosis, and process monitoring. *Industrial & Engineering Chemistry Research*, 2025, **64**(17): 8543−8564

116 Jia M W, Yang C, Pan Z X, Liu Q, Liu Y. Adversarial relationship graph learning soft sensor via negative information exclusion. *Journal of Process Control*, 2025, **145**: Article No. 103354

117 Ma L, Zhao R H. AcciMap causal analysis of Chinese chemical industry accidents unraveled by graph neural networks. *Reliability Engineering & System Safety*, 2025, **264**: Article No. 111425

118 Zheng J H, Zhuo Y, Jiang X Y, Zeng L Q, Ge Z Q. Advances in Bayesian networks for industrial process analytics: Bridging data and mechanisms. *Expert System With Applications*, 2025, **271**: Article No. 126670

119 Torres-Toledano J G, Sucar L F. Bayesian networks for reliability analysis of complex systems. In: Proceedings of the 6th Ibero-American Congress on Artificial Intelligence (IBERAMIA). Lisbon, Portugal: Springer, 1998. 195−206

120 Zhou Z B, Jin G, Dong D D, Zhou J L. Reliability analysis of multistate systems based on Bayesian networks. In: Proceedings of the 13th Annual IEEE International Symposium and Workshop on Engineering of Computer-based Systems (ECBS). Potsdam, Germany: IEEE, 2006. 347−352

121 Li K J, Yi R, Ma Z. Reliability analysis of dynamic reliability blocks through conversion into dynamic Bayesian networks. In: Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). Bali, Indonesia: IEEE, 2016. 1330−1334

122 Portinale L, Bobbio A. Bayesian networks for dependability analysis: An application to digital control reliability. In: Proceedings of the 15th Conference on Uncertainty in Artificial Intelligence. Stockholm, Sweden: ACM, 2013. 551−558

123 Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering & System Safety*, 2001, **71**(3): 249−260

124 Khakzad N, Khan F, Amyotte P. Risk-based design of process systems using discrete-time Bayesian networks. *Reliability Engineering & System Safety*, 2013, **109**: 5−17

125 Boudali H, Dugan J B. A continuous-time Bayesian network reliability modeling, and analysis framework. *IEEE Transactions on Reliability*, 2006, **55**(1): 86−97

126 Codetta-Raiteri D, Portinale L. Generalized continuous time Bayesian networks as a modelling and analysis formalism for dependable systems. *Reliability Engineering & System Safety*, 2017, **167**: 639−651

127 Kim M C. Reliability block diagram with general gates and its application to system reliability analysis. *Annals of Nuclear Energy*, 2011, **38**(11): 2456−2461

128 Bobbio A, Ciancamerla E, Franceschinis G, Gaeta R, Minichino M, Portinale L. Sequential application of heterogeneous models for the safety analysis of a control system: A case study. *Reliability Engineering & System Safety*, 2003, **81**(3): 269−280

129 Martins M R, Maturana M C. Application of Bayesian belief networks to the human reliability analysis of an oil tanker operation focusing on collision accidents. *Reliability Engineering & System Safety*, 2013, **110**: 89−109

130 Simon C, Weber P, Levrat E. Bayesian networks and evidence theory to model complex systems reliability. *Journal of Computers*, 2007, **2**(1): 33−43

131 Simon C, Weber P, Evsukoff A. Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. *Reliability Engineering & System Safety*, 2008, **93**(7): 950−963

132 Yin X W. Common cause failure model of system reliability based on Bayesian networks. *International Journal of Performability Engineering*, 2010, **6**(3): 255−268

133 Yin Xiao-Wei, Qian Wen-Xue, Xie Li-Yang. A method for system reliabiltiy assessment based on Bayesian networks. *Acta Aeronautica et Astronautica Sinica*, 2008, **306**: 1482−1489
(尹晓伟, 钱文学, 谢里阳. 系统可靠性的贝叶斯网络评估方法. 航空学报, 2008, **306**: 1482−1489)

134 Yazdi M, Kabir S. A fuzzy Bayesian network approach for risk analysis in process industries. *Process Safety and Environmental Protection*, 2017, **111**: 507−519

135 Leu S S, Chang C M. Bayesian-network-based safety risk assessment for steel construction projects. *Accident Analysis & Prevention*, 2013, **54**: 122−133

136 Li H, Soares C G, Huang H Z. Reliability analysis of a floating offshore wind turbine using Bayesian networks. *Ocean Engineering*, 2020, **217**: Article No. 107827

137 Zheng Y, Zhao F, Wang Z. Fault diagnosis system of bridge crane equipment based on fault tree and Bayesian network. *The International Journal of Advanced Manufacturing Technology*, 2019, **105**(9): 3605−3618

138 Codetta-Raiteri D. Applying generalized continuous time Bayesian networks to a reliability case study. *IFAC-PapersOnLine*, 2015, **48**(21): 676−681

139 Codetta-Raiteri D, Portinale L. Dynamic Bayesian networks for fault detection, identification, and recovery in autonomous spacecraft. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2015, **45**(1): 13−24

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

141 Marquez D, Neil M, Fenton N. Improved reliability modeling using Bayesian networks and dynamic discretization. *Reliability Engineering & System Safety*, 2010, **95**(4): 412−425

142 Mi J H, Li Y P, Yang Y J, Peng W W, Huang H Z. Reliability assessment of complex electromechanical systems under epistemic uncertainty. *Reliability Engineering & System Safety*, 2016, **152**: 1−15

143 Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection*, 2013, **91**(1−2): 46−53

144 Abimbola M, Khan F, Khakzad N, Butt S. Safety and risk analysis of managed pressure drilling operation using Bayesian network. *Safety Science*, 2015, **76**: 133−144

145 Zarei E, Azadeh A, Khakzad N, Aliabadi M M, Mohammadfam I. Dynamic safety assessment of natural gas stations using Bayesian network. *Journal of Hazardous Materials*, 2017, **321**: 830−840

146 Zhou Q Y, Li B, Lu Y, Chen J, Shu C M, Bi M S. Dynamic risk analysis of oil depot storage tank failure using a fuzzy Bayesian network model. *Process Safety and Environmental Protection*, 2023, **173**: 800−811

147 Wang C S, Xie Y H. Applying Bayesian network to distribution system reliability analysis. In: Proceedings of the IEEE Region 10 Conference TENCON 2004. Chiang Mai, Thailand: IEEE, 2004. 562−565

148 Wang Cheng-Shan, Xie Ying-Hua. A new Bayesian network model for distribution system reliability evaluation based on dual isomorphic Bayesian network model. *Power System Technology*, 2005, **29**(7): 41−46
(王成山, 谢莹华. 基于双层同构贝叶斯网络模型的配电网可靠性评估. 电网技术, 2005, **29**(7): 41−46)

149 Fu S S, Yu Y R, Chen J H, Xi Y T, Zhang M Y. A framework for quantitative analysis of the causation of grounding accidents in arctic shipping. *Reliability Engineering & System Safety*, 2022, **226**: Article No. 108706

150 Zhang L M, Wu X G, Skibniewski M J, Zhong J B, Lu Y J. Bayesian-network-based safety risk analysis in construction projects. *Reliability Engineering & System Safety*, 2014, **131**: 29−39

151 Zhang X G, Mahadevan S. Bayesian network modeling of accident investigation reports for aviation safety assessment. *Reliability Engineering & System Safety*, 2021, **209**: Article No. 107371

152 Hünninen M, Kujala P. Bayesian network modeling of port state control inspection findings and ship accident involvement. *Expert Systems With Applications*, 2014, **41**(4): 1632−1646

153 Hossain N U I, el Amrani S, Jaradat R, Marufuzzaman M, Buchanan R, Rinaudo C, et al. Modeling and assessing interdependencies between critical infrastructures using Bayesian network: A case study of inland waterway port and surrounding supply chain network. *Reliability Engineering & System Safety*, 2020, **198**: Article No. 106898

154 Xu S, Kim E, Haugen S, Zhang M Y. A Bayesian network risk model for predicting ship besetting in ice during convoy operations along the northern sea route. *Reliability Engineering & System Safety*, 2022, **223**: Article No. 108475

155 Moradi R, Cofre-Martel S, Droguett E L, Modarres M, Groth K M. Integration of deep learning and Bayesian networks for condition and operation risk monitoring of complex engineering systems. *Reliability Engineering & System Safety*, 2022, **222**: Article No. 108433

156 Leoni L, BahooToroody A, de Carlo F, Paltrinieri N. Developing a risk-based maintenance model for a natural gas regulating and metering station using Bayesian network. *Journal of Loss Prevention in the Process Industries*, 2019, **57**: 17−24

157 Wu J S, Zhou R, Xu S D, Wu Z W. Probabilistic analysis of natural gas pipeline network accident based on Bayesian network. *Journal of Loss Prevention in the Process Industries*, 2017, **46**: 126−136

158 Wang Q A, Chen J, Ni Y Q, Xiao Y F, Liu N B, Liu S K, et al. Application of Bayesian networks in reliability assessment: A systematic literature review. *Structures*, 2025, **71**: Article No. 108098

159 Soomro A A, Mokhtar A A, Kurnia J C, Lashari N, Sarwar U, Jameel S M, et al. A review on Bayesian modeling approach to quantify failure risk assessment of oil and gas pipelines due to corrosion. *International Journal of Pressure Vessels and Piping*, 2022, **200**: Article No. 104841

160 Kammouh O, Gardoni P, Cimellaro G P. Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks. *Reliability Engineering & System Safety*, 2020, **198**: Article No. 106813

161 Luque J, Straub D. Reliability analysis and updating of deteriorating systems with dynamic Bayesian networks. *Structural Safety*, 2016, **62**: 34−46

162 Villa V, Paltrinieri N, Khan F, Cozzani V. Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety Science*, 2016, **89**: 77−93

163 Animah I. Application of Bayesian network in the maritime industry: Comprehensive literature review. *Ocean Engineering*, 2024, **302**: Article No. 117610

164 Figueroa-García J C, Neruda R, Hernandez-Perez G J. On cosine fuzzy sets and uncertainty quantification. *Engineering Applications of Artificial Intelligence*, 2024, **138**: Article No. 109241

165 Wang Y F, Xie M. Approach to integrate fuzzy fault tree with Bayesian network. *Procedia Engineering*, 2012, **45**: 131−138

166 Ben-Haim Y. Evidence and uncertainty: An info-gap analysis of uncertainty-augmenting evidence. *Risk Analysis*, 2024, **44**(11): 2649−2659

167 Deng J X, Deng Y, Yang J B. Random permutation set reasoning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2024, **46**(12): 10246−10258

168 Zhang H. Interval importance sampling method for finite element-based structural reliability assessment under parameter uncertainties. *Structural Safety*, 2012, **38**: 1−10

169 Jiang C, Bi R G, Lu G Y, Han X. Structural reliability analysis using non-probabilistic convex model. *Computer Methods in Applied Mechanics and Engineering*, 2013, **254**: 83−98

170 Tonon F. Using random set theory to propagate epistemic uncertainty through a mechanical system. *Reliability Engineering & System Safety*, 2004, **85**(1−3): 169−181

171 Yang X F, Liu Y S, Zhang Y S, Yue Z F. Hybrid reliability analysis with both random and probability-box variables. *Acta Mechanica*, 2015, **226**(5): 1341−1357

172 Zu G Q, Xiao J, Sun K. Mathematical base and deduction of security region for distribution systems with DER. *IEEE Transactions on Smart Grid*, 2019, **10**(3): 2892−2903

173 Wu F, Kumagai S. Steady-state security regions of power-systems. *IEEE Transactions on Circuits and Systems*, 1982, **29**(11): 703−711

174 di Maio F, Picoco C, Zio E, Rychkov V. Safety margin sensitivity analysis for model selection in nuclear power plant probabilistic safety assessment. *Reliability Engineering & System Safety*, 2017, **162**: 122−138

175 Alobaid F, Mertens N, Starkloff R, Lanz T, Heinze C, Epple B. Progress in dynamic simulation of thermal power plants. *Progress in Energy and Combustion Science*, 2017, **59**: 79−162

176 Lin W, Yang Z F, Yu J, Xie K G, Wang X B, Li W Y. Tie-line security region considering time coupling. *IEEE Transactions on Power Systems*, 2021, **36**(2): 1274−1284

177 Wang Y C, Ji Z Z, Cao Y, Yang S H. Safety critical variable analysis for process systems. *Industrial & Engineering Chemistry Research*, 2023, **62**(50): 21704−21720

178 Qin C, Yu Y X. Small signal stability region of power systems with DFIG in injection space. *Journal of Modern Power Systems and Clean Energy*, 2013, **1**(2): 127−133

179 Yang T K, Yu Y X. Steady-state security region-based voltage/var optimization considering power injection uncertainties in distribution grids. *IEEE Transactions on Smart Grid*, 2019, **10**(3): 2904−2911

180 Yu Y X, Qin C. Security region based security-constrained unit commitment. *Science China Technological Sciences*, 2013, **56**(11): 2732−2744

181 Yu Yi-Xin. Review of study on methodology of security regions of power system. *Journal of Tianjin University*, 2008, **41**(6): 635−646
(余贻鑫. 电力系统安全域方法研究述评. 天津大学学报, 2008, **41**(6): 635−646)

182 Ma X Y, Liang J W, Wan Y H, Gui Z S, Yuan Z H, Wang Y, et al. Small-signal stability region analysis of multi-time delay wind power system considering degenerate Hopf bifurcation. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2025, **72**(11): 7146−7159

183 Wang Cheng-Shan, Xu Xiao-Fei, Yu Yi-Xin, Wei Wei, Stephen T L, Zhang Pei. Visualization of power system static voltage stability region in cut-set space. *Proceedings of the CSEE*, 2004, **24**(9): 13−18
(王成山, 许晓菲, 余贻鑫, 魏炜, Stephen T L, Zhang Pei. 基于割集功率空间上的静态电压稳定域局部可视化方法. 中国电机工程学报, 2004, **24**(9): 13−18)

184 Li Hui-Ling, Yu Yi-Xin, Han Qi, Su Ji-Feng, Zhao Jin-Li, Lee S T, et al. Practical boundary of static voltage stability region in cut-set power space of power systems. *Automation of Electric Power Systems*, 2005, **29**(4): 18−23
(李慧玲, 余贻鑫, 韩琪, 宿吉锋, 赵金利, Lee S T, et al. 割集功率空间上静态电压稳定域的实用边界. 电力系统自动化, 2005, **29**(4): 18−23)

185 Jiang Tao, Jia Hong-Jie, Jiang Yi-Lang, Kong Xiang-Yu, Lu Ning. Approximating method of wide area thermal security region boundary in bulk power system. *Transactions of China Electrotechnical Society*, 2016, **31**(8): 134−146
(姜涛, 贾宏杰, 姜懿郎, 孔祥玉, 陆宁. 跨区互联电网热稳定安全域边界近似方法. 电工技术学报, 2016, **31**(8): 134−146)

186 Maihemuti S, Wang W Q, Wang H Y, Wu J H, Zhang X. Dynamic security and stability region under different renewable energy permeability in IENGS system. *IEEE Access*, 2021, **9**: 19800−19817

187 Wu D, Nie T T, Turitsyn K, Blumsack S. Estimating loadability region of natural gas system via monotone inner polytope sequence. *IEEE Transactions on Control of Network Systems*, 2020, **7**(2): 660−672

188 Perninge M, Söder L. Risk estimation of the distance to voltage instability using a second order approximation of the saddle-node bifurcation surface. *Electric Power Systems Research*, 2011, **81**(2): 625−635

189 Perninge M, Soder L. On the validity of local approximations of the power system loadability surface. *IEEE Transactions on Power Systems*, 2011, **26**(4): 2143−2153

190 Sun D W, Yu Y X. Accurate identification of critical boundary hyperplanes of practical steady-state security region in distribution grids. *IEEE Transactions on Smart Grid*, 2023, **14**(6): 4312−4321

191 Gutierrez-Martinez V J, Canizares C A, Fuerte-Esquivel C R, Pizano-Martinez A, Gu X P. Neural-network security-boundary constrained optimal power flow. *IEEE Transactions on Power Systems*, 2011, **26**(1): 63−72

192 Qiu Y W, Wu H, Song Y H, Wang J H. Global approximation of static voltage stability region boundaries considering generator reactive power limits. *IEEE Transactions on Power Systems*, 2018, **33**(5): 5682−5691

193 Qiu Y W, Wu H, Zhou Y Z, Song Y H. Global parametric polynomial approximation of static voltage stability region boundaries. *IEEE Transactions on Power Systems*, 2017, **32**(3): 2362−2371

194 Qin Y, Yu S, Zhang Y, Jia L M, Cheng X Q. An online quantified safety assessment method for train service state based on safety region estimation and hybrid intelligence technologies. *International Journal of Software Engineering and Knowledge Engineering*, 2015, **25**(3): 493−511

195 He Y N, Yu H F, Brat G, Davies M. Statistical learning framework for safety and failure analysis of a DNN-based autonomous aircraft system. In: Proceedings of the 20th International Conference on Machine Learning and Applications (ICMLA).

Pasadena, USA: IEEE, 2021. 1−6

196 He Y N, Schumann J. A framework for the analysis of deep neural networks in aerospace applications using Bayesian statistics. In: Proceedings of the 14th International Joint Conference on Neural Networks (IJCNN). Glasgow, UK: IEEE, 2020. 1−9

197 Yu Y X, Huang C H, Feng F. A study on reactive power steady-state security regions. *Electric Machines & Power Systems*, 1989, **17**(3): 155−166

198 Yu Y X, Liu Y L, Qin C, Yang T K. Theory and method of power system integrated security region irrelevant to operation states: An introduction. *Engineering*, 2020, **6**(7): 754−777

199 Yu Y X, Liu Y L, Yu D D. Smart grid innovations: Increasing resilience, security, and sustainability in the era of energy transition. *Engineering*, 2025, **51**: 1−2

200 Liu Y L, Jia R P. Space division and WGAN-GP based fast generation method of practical dynamic security region boundary. *Engineering*, 2025, **51**: 75−85

201 Zeng Yuan, Fan Ji-Chao, Yu Yi-Xin, Lu Fang, Huang Yao-Gui. Practical dynamic security regions of bulk power systems. *Automation of Electric Power Systems*, 2001, **25**(16): 6−10
(曾沅, 樊纪超, 余贻鑫, 卢放, 黄耀贵. 电力大系统实用动态安全域. 电力系统自动化, 2001, **25**(16): 6−10)

202 Yu Yi-Xin, Zeng Yuan, Feng Fei. Differential topological characteristics of the DSR on injection space of electrical power system. *Science in China Series E: Technological Science*, 2002, **32**(4): 503−509
(余贻鑫, 曾沅, 冯飞. 电力系统注入空间动态安全域的微分拓扑特性. 中国科学 E 辑: 技术科学, 2002, **32**(4): 503−509)

203 Wang Y C, Ji Z Z, Cao Y, Yang S H. Dynamic risk assessment for process operational safety based on reachability analysis. *Reliability Engineering & System Safety*, 2025, **253**: Article No. 110564

204 Li J, Chen J B. Probability density evolution method for dynamic response analysis of structures with uncertain parameters. *Computational Mechanics*, 2004, **34**(5): 400−409

205 Liu G, Gao K, Yang Q S, Tang W, Law S S. Improvement to the discretized initial condition of the generalized density evolution equation. *Reliability Engineering & System Safety*, 2021, **216**: Article No. 107999

206 Das S, Tesfamariam S. Reliability assessment of stochastic dynamical systems using physics informed neural network based PDEM. *Reliability Engineering & System Safety*, 2024, **243**: Article No. 109849

207 Lv M Z, Feng D C, Chen J B, Li J. A decoupled approach for determination of the joint probability density function of a high-dimensional nonlinear stochastic dynamical system via the probability density evolution method. *Computer Methods in Applied Mechanics and Engineering*, 2024, **418**: Article No. 116443

208 Behrendt M, Lv M Z, Luo Y B, Chen J, Beer M. Failure probability estimation of dynamic systems employing relaxed power spectral density functions with dependent frequency modeling and sampling. *Probabilistic Engineering Mechanics*, 2024, **75**: Article No. 103592

209 Kumar P, Merzouki R, Bouamama B O. Multilevel modeling of system of systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018, **48**(8): 1309−1320

210 Li M Z, She Z K, Xu D, Song X Y, Jia W. Complex state networks based safety analysis of complex engineering systems considering closed-loop feedback. *Reliability Engineering & System Safety*, 2025, **259**: Article No. 110931

211 Yazdi M, Kabir S, Walker M. Uncertainty handling in fault tree based risk assessment: State of the art and future perspectives. *Process Safety and Environmental Protection*, 2019, **131**: 89−104

212 Dai X H, Tu J H, Quan Q. Safety assessment approach to UAVs based on profust safety index and HIL simulation. *IEEE/ASME Transactions on Mechatronics*, 2024, **29**(5): 3336−3347

213 Arunthavanathan R, Sajid Z, Amin M T, Tian Y H, Khan F, Pistikopoulos E. Process safety 4.0: Artificial intelligence or intelligence augmentation for safer process operation? *AIChE Journal*, 2024, **70**(7): Article No. e18475

214 Li X X, Huang W C. Resilience quantification method of high-speed railway train diagram under operation section interference: Strategies and practices. *Reliability Engineering & System Safety*, 2025, **260**: Article No. 111020

215 Zhang L, Du Y. Resilience enhancement scheme for gateway placement in space information networks. *Computer Networks*, 2023, **222**: Article No. 109555

216 Zhu Z R, Huang P F, Zhang X M, Chai Y, Song Z H. First attempt of barrier functions for Caputo′s fractional-order nonlinear dynamical systems. *Science China Information Sciences*, 2023, **66**(7): Article No. 179205

217 Chen Zhong-Qiu, Liu Yong-Hua, Su Chun-Yi. Safe control of strict-feedback systems using filtered control barrier functions. *Acta Automatica Sinica*, 2024, **50**(12): 2474−2486
(陈仲秋, 刘勇华, 苏春翌. 基于滤波控制障碍函数的严格反馈系统安全控制. 自动化学报, 2024, **50**(12): 2474−2486)

218 Zhang Z Y, Zhao Q C, Sun K L. A learning-based method for computing control barrier functions of nonlinear systems with control constraints. *IEEE Robotics and Automation Letters*, 2023, **8**(7): 4259−4266

王德琳 重庆大学自动化学院博士研究生. 主要研究方向为复杂工程系统的安全分析与评估.
E-mail: wangdelin@stu.cqu.edu.cn
(**WANG De-Lin** Ph.D. candidate at the School of Automation, Chongqing University. Her research interests include safety analysis and assessment for complex engineering systems.)

张 可 重庆大学自动化学院教授. 主要研究方向为复杂工程系统的安全控制与故障诊断. 本文通信作者.
E-mail: zhangke@cqu.edu.cn
(**ZHANG Ke** Professor at the School of Automation, Chongqing University. His research interests include safety control and fault diagnosis for complex engineering systems. Corresponding author of this paper.)

朱哲人 杭州师范大学数学学院助理研究员. 主要研究方向为复杂工程系统的安全分析与控制.
E-mail: drzzr@hznu.edu.cn
(**ZHU Zhe-Ren** Assistant researcher at the School of Mathematics, Hangzhou Normal University. His research interests include safety analysis and control for complex engineering systems.)

陈小龙 重庆大学自动化学院讲师. 主要研究方向为复杂工程系统的软测量与故障诊断.
E-mail: xiaolong.chen@cqu.edu.cn
(**CHEN Xiao-Long** Lecturer at the School of Automation, Chongqing University. His research interests include soft sensing and fault diagnosis for complex engineering systems.)

陈志文 中南大学自动化学院教授. 主要研究方向为复杂工程系统的健康管理与故障诊断.
E-mail: zhiwen.chen@csu.edu.cn
(**CHEN Zhi-Wen** Professor at the School of Automation, Central South University. His research interests include health management and fault diagnosis for complex engineering systems.)

蒋朝辉 中南大学自动化学院教授. 主要研究方向为复杂工程系统的图像识别与智能监测.
E-mail: jzh0903@csu.edu.cn
(**JIANG Zhao-Hui** Professor at the School of Automation, Central South University. His research interests include image recognition and intelligent detection for complex engineering systems.)

柴 毅 重庆大学自动化学院教授. 主要研究方向为复杂工程系统的信息融合与安全控制.
E-mail: chaiyi@cqu.edu.cn
(**CHAI Yi** Professor at the School of Automation, Chongqing University. His research interests include information fusion and safety control for complex engineering systems.)

宋执环 浙江大学控制科学与工程学院教授. 主要研究方向为复杂工程系统的数据分析与故障诊断.
E-mail: songzhihuan@zju.edu.cn
(**SONG Zhi-Huan** Professor at the College of Control Science and Engineering, Zhejiang University. His research interests include data analysis and fault diagnosis for complex engineering systems.)