航天发射系统运行安全性评估研究进展与挑战

柴 毅 [1,2] 毛万标 [2,3] 任 浩 [1,2] 屈剑锋 [1,2] 尹宏鹏 [1,2]
杨志敏 [1,2] 冯 莉 [1,2] 张邦双 [3] 叶 欣 [3]

摘 要 航天发射作为人类太空活动最为基础和最为重要的环节之一, 是评判一个国家综合国力的重要指标, 而航天发射系统运行安全性评估作为现代航天发射控制指挥与决策系统的核心, 是保证航天发射安全运行的基础. 首先, 本文概述了现代航天发射系统, 简要回顾了系统安全性研究发展历程, 阐述了航天发射系统运行安全性评估的内涵. 其次, 通过综述航天发射系统运行故障检测与诊断、异常运行工况识别、运行过程安全分析与预测、安全性动态评估技术等方面的研究现状的基础上, 总结出了航天发射系统运行安全性评估面临着系统极度复杂、决策风险性极大、先验信息少以及评估结果要求高准确性与实时性等方面的挑战. 最后, 本文对航天发射系统运行安全性评估有待研究的基础前沿问题进行了思考.

关键词 航天发射系统, 运行安全性评估, 异常运行工况识别, 故障检测与诊断

引用格式 柴毅, 毛万标, 任浩, 屈剑锋, 尹宏鹏, 杨志敏, 冯莉, 张邦双, 叶欣. 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

DOI 10.16383/j.aas.c180135

Research on Operational Safety Assessment for Spacecraft Launch System: Progress and Challenges

CHAI Yi[1,2] MAO Wan-Biao[2,3] REN Hao[1,2] QU Jian-Feng[1,2] YIN Hong-Peng[1,2]
YANG Zhi-Min[1,2] FENG Li[1,2] ZHANG Bang-Shuang[3] YE Xin[3]

Abstract The spacecraft launch system is not only one of the most basic and the most important parts in human space activities but also an important indicator for judging a country′s overall national strength. The operational safety assessment of the spacecraft launch system can be considered as the core of modern spacecraft launch control command and decision system. It is the basis for ensuring the safe operation of spacecraft launches. The modern spacecraft launch system is outlined and the development of system safety research is briefly reviewed. The connotation of the operational safety assessment of the spacecraft launch system is explained. Secondly, it focuses on the research progress of operational fault detection and diagnosis, abnormal operational condition identification, operational processes safety analysis and prediction, safety dynamic evaluation technology. Additionally, the challenges on the operational safety assessment of spacecraft launch system are discussed, including extremely complexity in practical system, great risk in decision-marking, little prior information, high accuracy and real-time evaluation results. Finally, the basic and systemic issues of the future research for the operational safety assessment of spacecraft launch system are pondered.

Key words Spacecraft launch system, operational safety assessment, anomaly operational condition identification, fault detection and diagnosis

Citation Chai Yi, Mao Wan-Biao, Ren Hao, Qu Jian-Feng, Yin Hong-Peng, Yang Zhi-Min, Feng Li, Zhang Bang-Shuang, Ye Xin. Research on operational safety assessment for spacecraft launch system: progress and challenges. *Acta Automatica Sinica*, 2019, **45**(10): 1829−1845

21 世纪是人类进入探索太空和利用太空资源的时代, 低成本、安全、快速、高效的太空进入能力是保证人类太空活动取得成功的关键[1−4]. 航天发射是人类太空活动最为基础和最为重要的环节之一, 航天发射系统是实现航天器送上太空的航天工程设施系统, 也是一个典型的涉及多人、多机、多环境的大规模复杂工程系统, 其运行安全受到诸多边界条件的约束, 任何安全隐患、人员误操作以及系统故

收稿日期 2018-03-09 录用日期 2018-11-19
Manuscript received March 9, 2018; accepted November 19, 2018
国家自然科学基金项目 (61633005, 61773080), 重庆大学科研后备拔尖人才项目 (cqu2018CDHB1B04) 资助
Supported by National Natural Science Foundation of China (61633005, 61773080) and Scientific Reserve Talent Programs of Chongqing University (cqu2018CDHB1B04)
本文责任编委 潘泉
Recommended by Associate Editor PAN Quan
1. 重庆大学复杂系统安全与控制教育部重点实验室 重庆 400044 2. 重庆大学自动化学院 重庆 400044 3. 航天发射场可靠性技术重点实验室 海口 570100
1. Key Laboratory of Complex System Safety and Control, Ministry of Education, Chongqing University, Chongqing 400044 2. School of Automation, Chongqing University, Chongqing 400044 3. Key Laboratory of Space Launching Site Reliability Technology, Haikou 570100

障, 均会招致运行事故甚至灾难的发生[5−7]. 另外, 航天任务的探索性、试验性、危险性和社会性也决定了航天发射系统运行安全性评估的研究具有迫切性与现实性[1−3].

一般地, 航天发射安全性是指航天产品进场后直至火箭点火发射期间, 发射系统保证航天员、航天产品不受损害的综合性能, 即航天发射过程中不发生导致人员伤亡、健康恶化、设备财产损失以及环境污染等意外事件的能力[8−9]. 近年来, 为保证航天发射任务的顺利完成, 世界各国高度重视航天发射安全, 积极开展航天发射系统运行安全分析与评估技术的探索与研究[1−4, 8, 10−15]. 期望采用科学的系统运行安全性分析与评估手段, 提高航天发射过程的安全性以及避免重大事故的应急处置能力[1−4,10−12].

为此, 本文首先对现代航天发射系统进行了概述, 得出高准确性与高安全性是其区别于其他复杂系统的基本特征. 接着, 从系统安全性发展历程的角度出发, 对系统 (以下无特别说明时, 将 “航天发射系统” 简称为 “系统”) 运行安全评估的内涵进行了界定. 并综述了航天发射系统中运行故障检测与诊断、异常运行工况识别、安全分析与预测、运行安全性动态评估技术等方面的研究现状, 指出了航天发射系统运行安全动态评估研究中面临的挑战, 并以此为基础, 最后对其未来发展的基础前沿问题进行了思考, 以期推动航天发射系统运行安全动态评估技术的发展.

1 概述

1.1 现代航天发射系统概述

航天发射系统是指发射航天器的特定系统, 含有完整的试验设施和设备, 用以装配、储存、监测和发射航天器[3−4]. 航天器是按照天体力学的规律在天空运行, 执行探索、开发、利用太空和天体等特点任务的各类飞行器, 如我国的北斗卫星导航系统等, 美国的全球卫星定位系统等[3−4]. 运载火箭又称运载器, 是指把有效载荷从地面运送到太空预定位置、从太空某位置运回地面或运送到太空另一位置的运载工具的统称, 包括一次性使用运载火箭、部分重复使用运载器和完全重复使用运载器[3−4], 如中国的长征系列、美国的德尔塔系列、大力神系列等. 航天发射场是指发射航天器的场地[3−4], 如我国的酒泉、太原、西昌和文昌发射中心, 美国的肯尼迪航天中心、卡纳维拉尔角空军基地、范登堡空军基地、欧洲的圭亚那太空中心等. 如今, 为满足航天发射试验任务的需求, 提高航天发射的现代化水平, 航天发射场先后建立了航天发射控制指挥与决策监控系统 (C3I 系统, 即指挥、控制、通信与信息系统), 它是基地前线指挥所和发测站对航天发射实施指挥的自动化保障系统, 主要任务是保障航天试验产品各系统在发射场技术区和发射区测试发射组织指挥、管理和监控任务的完成, 其基本结构见图 1[5]. 由此可见, 航天器是发射活动的目的, 运载火箭是运载航天器的工具, 航天发射场是发射活动的场地, 航天发射系统是对整个发射活动的系统性总称, 航天发射控制指挥与决策监控系统是航天发射系统的 “灵魂”, 是整个发射系统的决策核心, 而实现该系统有效运行的关键环节是实现发射过程中的故障及时诊断与系统运行安全性的在线分析与评估等[3−4, 6, 8−9, 10, 13, 16].

由图 1 可知, 作为整个航天发射系统的决策核心, 航天发射控制指挥与决策系统的故障诊断环节主要体现在: 运载火箭起飞前后, 发射场各地面测试与遥测设备的故障与运行异常的检测、识别、诊断与定位, 及时修复各种故障与运行异常, 保障航天发射任务的准时准点完成[6−7]. 而系统运行安全性的在线分析与评估主要包括航天发射过程中的 3 大方面: 1) 实时分析影响航天发射运行安全性的各子系统的运行性能, 如射前燃料加注与补加、测试点火发射升空、射后废物燃料处置、射后飞行态势感知等, 2) 及时分析与识别异常运行工况, 评估运载火箭在发射前后的现场安全态势以及系统运行的安全性能, 3) 构建完善的组织救援体系和处置方案, 提高航天发射安全的应急保障能力[6−7].

航天工程虽然历经半个多世纪的太空探索, 取得了长足的发展, 但航天发射任务失败的案例仍时有发生, 如表 1 所示. 因射前加注出现安全问题, 导致发射任务失败就有 4 次之多, 而这仅仅只是众多安全性事故公开报道的一小部分. 另有在发射过程中面临的可能不止一次的故障、异常运行工况等, 甚至导致人员损伤、环境污染与发射任务数次推迟等安全事故[17−18]. 一般来说, 表 1 所列举的安全问题, 大致可以分为三类: 射前未发现问题而致使重大事故, 射前未发现故障而致使发射失败, 以及射前发现故障而推迟或中止发射. 无论是射前故障的发现与否, 都将会导致人员损伤、环境污染或发射任务中止或失败等问题. 射前故障的发现主要涉及异常运行工况的检测与识别、故障检测与诊断等, 而系统安全性分析与评估则是分析系统异常或故障发射时, 对于整个发射过程的人员、环境以及试验任务的影响. 需要说明是, 并不是所有的运载火箭导致卫星未能入轨等发射失败, 都属于航天发射问题, 例如航天器自身质量问题等.

因航天发射工程在国内外政治、国民经济、社

表 1　近年来部分航天发射场的安全问题统计

Table 1　The statistics on safety issues in some space launch sites in recent years

时间	后果	国别	原因
1960-10-24	160 多名专家死亡.	前苏联	异常抢修过程中, 第二级引擎意外点燃.
2003-08-22	VLS 火箭最后测试中爆炸, 21 人死亡.	巴西	火箭主体内一个发动机的点火装置出现故障.
2010-11-05	“发现” 号航天飞机第五次推迟发射.	美国	“发现” 号外部燃料箱加注液氢和液氧燃料两小时后, 外部燃料箱的一个通风孔出现了氢气泄漏.
2011-04-29	“奋进” 号航天飞机推迟至少 48 小时起飞.	美国	“奋进” 号航天飞机附属电力装置加热器出现技术故障, 5 次推迟后才成功.
2012-11-29	“罗老号” 运载火箭和发射台的连接部分故障, 第三次延期发射.	韩国	“罗老号” 第一段火箭的高压、超低温液态气体压力不足, 导致阀门异常开合.
2013-07-02	三颗格洛纳斯 M 导航卫星化为灰烬.	俄罗斯	发射几秒钟后, 质子 M 火箭失控并爆炸.
2013-08-27	日本新型火箭发射前 19 秒出现异常, 中止发射.	日本	地面计算机 “LCS (发射控制系统)” 向火箭上的计算机 “OBC (板载计算机)” 数据交换出现了 0.07 秒的时间差.
2014-11-26	载有欧洲通讯卫星 “Astra-G” 的运载火箭 “质子 -M” 推迟发射.	俄罗斯	俄罗斯航天局: 在检查助推器时查出指令系统故障, 更换故障仪器.
2015-01-06	猎鹰 9 号运载火箭在倒计时 1 分钟时, 发射任务紧急中止.	美国	由于火箭 “二级推力矢量控制驱动器发生漂移” 导致火箭在倒计时 1 分钟时发射任务紧急中止.
2017-11-28	未能将卫星载荷送入预定轨道, 发射失败.	俄罗斯	联盟 2.1b 运载火箭由于上面级火箭出现故障, 失败.

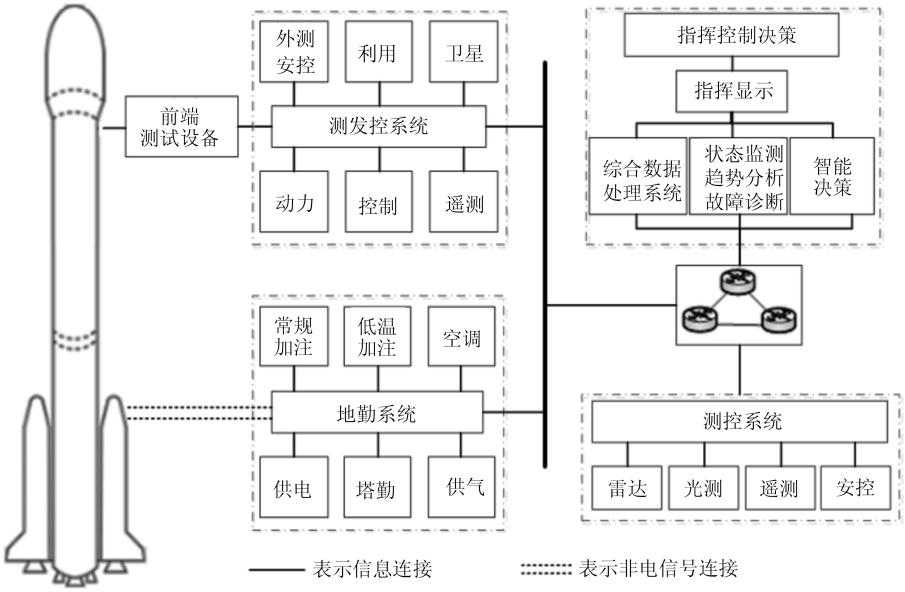


图 1　航天发射控制指挥与决策系统示意图

Fig. 1　The diagram of space launch control command and decision system

会影响等方面的特殊地位, 在线检测、识别、定位设备隐患、系统故障以及误操作等危险因素, 成为航天发射系统运行安全必不可少的工作, 即迫使现代航天发射系统必须具有保障高准确性与高安全性等的能力, 因而开展系统运行安全评估研究具有重大的理论价值与现实意义[3−4, 10−12].

1.2 系统安全性研究发展历程

系统安全的概念是美国学者于 20 世纪 40 年代提出的, 但并未采用系统工程分析的方法展开研究 (此处的 “系统”, 为一般意义上的 “系统”, 非特指 “航天发射系统”). 直到 50 年代, 美国开始尝试将故障模式、影响与危害分析方法 (Failure mode and effect analysis, FMEA) 应用于航天飞机发动机的设计与研制中, 并于 1962 年提出采用系统工程的理念对导弹系统安全性进行分析与研究[3−4,8]. 系统安全性评估分析理论诞生的标志性事件则是安全系统计划标准 MIL-STD-882 的制订, 使得系统安全性的相关概念和技术手段得以系统的阐述. 并在此标准的基础上, 美国结合系统安全工程的发展, 制订了一系列与系统安全性相关的标准手册, 推动了系统安全分析与评估工程的快速发展[3−4, 8].

20 世纪 60 年代开始, 前苏联、日、英、法等国相继开展安全性相关领域的研究, 主要集中于航空电子与电力电子领域; 80 年代开始, 系统安全研究在各领域逐步展开. 截止目前, 研究学者已提出了初步危险分析 (Preliminary hazard analysis, PHA)、故障树分析 (Fault tree analysis, FTA)、事件树分析 (Event tree analysis, ETA)、因果分析图法、运行危险分析 (Hazard and operability analysis, HAZOP)、安全检查表法、事故致因理论、安全行为理论、综合安全评价、安全管理评估等安全分析方法[3−4, 8]. 而随着研究的逐渐深入, 航空航天领域的有关安全性分析理论与方法体系得到不断的改进与发展, 并逐渐应用于保障航天发射任务顺利完成的航天发射系统中[9].

为保障发射过程的安全, 国外分别针对航天发射系统出台了一系列的工作方法和管理程序, 如《美国东西发射场安全要求》, 欧洲《圭亚那航天中心安全条例》等. 20 世纪 90 年代初, 我国参照美国相关安全性标准规范制订了《QJ2236 航天器和导弹武器系统安全性通用大纲》与《GJB900-90 系统安全性通用大纲》, 标志着我国航天工程系统安全性工作的研究进入了新阶段[19−21].

我国航天发射系统安全主要靠实践中积累形成的一些安全管理规章制度来保证, 发射安全工作从依靠经验过渡到安全标准体系, 可分为设计上和管理上两类. 设计上通过将系统设备和设施布置在相互安全的距离上, 合理地组织射前准备和发射操作过程. 管理上的安全措施, 包括制定严格的安全规章制度、严格执行操作规程和落实安全措施以及经常性的技术安全检查等. 这些文件明确了发射安全要求的基本原则, 有效地规范了发射安全管理工作. 遗憾地是, 航天发射系统并没有建立运行安全的分析理论和方法体系[3−4, 6−8, 13].

目前, 我国航天发射系统虽然处于较高的安全水平, 但以航天发射系统为特定研究对象的相关工作还比较少[3−4, 8]. 另外, 我国航天事业正处于快速发展阶段, 高密度的发射任务和新技术的试验也给航天发射系统的运行安全带来了新的挑战.

1.3 系统运行安全性评估内涵

随着传感器、计算机及通信技术的不断发展, 航天发射场也呈现向现代化、自动化和智能化等方向发展的趋势[3−6, 8−9, 12, 16, 22−24]. 国内外学者经过在航天发射系统安全性方面的多年研究, 逐渐形成了一个对航天发射 “运行安全” 都认可的概念, 即从数学角度讲, 系统运行安全性就是在整个航天发射过程中, 规避人员伤亡、系统运行性能劣化, 刻画评价由其产生的重大妨碍发射任务的危险因素等[8−9].

需要指出的是, 系统运行安全性不同于系统安全性, 其是指在整个发射系统运行过程中, 需要动态实时地发现系统中存在的异常、故障以及各种安全风险因素. 为此, 国内外学者在航天发射系统运行安全性评估方面主要集中在系统运行故障检测与诊断、系统运行异常工况识别、系统动态运行过程安全分析以及系统运行安全性动态评估等 4 个方面[3−4, 8−9], 其逻辑关系如图 2 所示.

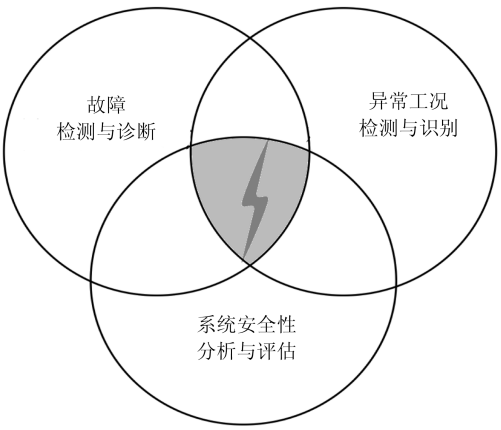


图 2 航天发射系统运行安全性分析与评估的内涵

Fig. 2 The connotation of operational safety analysis and assessment of spacecraft launch system

航天发射系统突出特点便是其庞杂的结构, 复杂程度极高 (达到 10^6 以上), 而各个子系统中的故障与运行异常并不一定会引起运行安全问题[18−26]. 因此, 由图 2 可知, 航天发射系统的运行安全性分析与评估并不包含故障检测与诊断、异常工况检测与识别的全部, 而是与航天发射运行安全有关的关键子系统的故障与运行异常才会引起安全问题, 如低温推进剂加注系统、液压系统等.

另外, 航天发射系统运行安全性与系统安全分析与评估也有一定的区别, 主要原因是不同的危险源在不同的运行条件下将会表现出截然相反的安全形态. 此外, 系统运行安全性与系统安全也有动态与静态之分. 因此, 不能将系统运行安全性与系统安全等同起来, 而是系统运行安全性来源于系统安全性, 前者考察系统的动态运行过程, 后者考察系统几乎所有的安全风险因素, 两者相辅相成[27−30].

就目前来看, 航天发射流程极为复杂、状态变化多端, 检测的关键参数多, 需要诊断的故障模式多, 给测发控指挥人员带来了很大的故障在线检测与诊断负担、异常运行工况发现与识别负担, 以及运行安全分析与评估负担, 进而增加了流程决策的压力[27−30]. 因此, 开展航天发射系统运行安全性分析与评估研究, 构建现代化、自动化、智能化地航天发射系统, 将测发控指挥人员从繁重的数据判读与故障判断中解放出来, 并为其提供有效的辅助决策的信息, 完善航天发射系统运行安全性评估体系建设, 将是航天发射系统未来发展的一个方向.

2　研究现状

为完善航天发射系统运行安全性评估体系建设, 综合考虑影响和制约航天发射系统运行安全的诸多因素. 通过依据航天发射系统机理模型与数据监测信息, 突破仅限于状态监测与故障诊断领域的技术层次, 构建针对现代大型运载火箭的一种全面化、体系化、深入化、精准化的系统运行安全性实时评估的解决方案, 从而更有效地提升航天发射系统的安全性. 就目前有限的相关报道而言, 航天发射系统运行安全性评估研究主要包括系统运行故障检测与诊断、系统异常运行工况识别、系统动态运行过程安全分析、系统运行安全性动态评估技术等.

2.1　系统运行故障检测与诊断研究现状

航天发射是一项探索性和试验性的活动, 具有短期运行和长期停用的间歇运行特点, 区别于飞机、舰船、车辆的频繁投运, 参与航天发射的对象和发射设施, 年发射次数不超过几次至十几次, 每发任务几乎都有新的实验目的和技术状态, 产品研发时所进行的检查、测试次数也都有限. 而且, 在航天发射系统运行高安全性的需求下, 及时对系统运行故障进行分析、诊断和预测, 确定故障性质、类别、程度、原因及部位, 预测发展趋势及可能造成的后果[15, 31], 有助于在紧急情况下迅速排除故障, 及时避免或减少事故的发生.

就现有在航天发射系统的故障检测、诊断与传播分析等方面的研究而言, 国内外对此方面的研究报道很少, 且主要集中在数据驱动和知识驱动的故障诊断方法[32−34], 而基于模型的故障检测与诊断方法极为少见, 主要原因是系统的数学模型很难建立, 且运行数据与理论值相差较大, 难以构建有效的数学模型, 动态描述系统的运行工况. 此外, 如前所述, 航天发射系统是一个极为复杂的系统, 其涉及的子系统众多, 主要集中在燃料加注系统、电液一体化系统、空调制冷系统等[35−42].

就燃料加注系统而言, 国内外已有很多学者展开了有关研究, Datta 等[35] 综述了实际加注工程中的管道泄漏和堵塞等故障检测方面的研究, 对各种管道故障检测方法进行了简要讨论, 包括振动分析、脉冲回波法、声学技术、负压波检漏技术、基于支持向量机、基于干涉光纤传感器以及基于滤波对角化等管道检漏方法, 并讨论了各方法的优缺点, 这些方法已应用于石油、天然气、水等流体输送领域, 适用于直管、曲管、长管等不同类型的管道, 在各种故障检测方法中, 声反射法因其能准确识别管径 1 % 的堵塞和泄漏而被认为是最适合的故障检测方法. 就航天加注系统而言, Ren 等[17] 针对航天加注系统中储罐挤压压力骤降、冷凝器故障、管道泄漏、传感器和执行器故障等, 提出了一种基于深度置信网络和多模型相结合的数据驱动的方法实现了航天复杂加注系统的故障检测. Xu 等[25] 针对管道泄漏问题, 以不确定性、不同类型的信息为基础, 描述了更复杂的因果关系, 构建基于信念规则的专家系统, 实现了加注管道的泄漏检测. 马昕晖等[43] 则针对液氢输送需要在极低温度下进行, 出现漏热故障将十分危险, 发生漏热后的液氢会迅速产生气液两相流, 其对加注系统中的器件造成很大冲击与危害, 造成加注系统损坏等事故, 重点研究了液氢加注系统中过滤器漏热故障. 总结这些文献中涉及的方法, 主要为数据驱动的深度置信网络[17], 知识驱动的专家系统[25] 以及对加注机理知识[43] 等方面的研究, 缺乏其他各种不同有效地检测技术研究, 如基于声反射技术的管道泄漏检测.

在电液一体化系统中, 诸如电液比例阀和电液伺服阀等元件对于液压油污染极其敏感, 极易使系统出现各种故障, 且故障模式多种多样, 难以检测和诊断. 目前来看, 实现电液一体化系统的运行故障检测与诊断方法可以分为两类: 专家知识驱动的故障诊断与数据驱动的故障诊断[42−54]. 专家知识驱动的故障诊断主要是利用先验知识对系统进行主观判断, 存在很多问题, 如难以对液压元件失效机理进行判断, 且诊断效率低、时间长以及准确性低等问题; 数据驱动的诊断方法则是利用其他仪器设备对系统的压力、流量和温度等参数识别系统的运行状态, 主要采用多传感器信息融合技术、人工智能以及机器学习等方法实现. 航天发射系统的电液一体化系统也

不例外, 如 Kordestani 等[36] 针对空间运载火箭推进系统中的关键部分 (液压控制阀) 展开研究, 介绍了一种新颖模块化的基于多传感器数据信息降维的故障诊断与预测方法, 该方法主要包括故障检测和诊断模块、故障参数估计模块和剩余使用寿命估计模块三大部分, 主要考虑液压控制阀系统中的活塞泄漏、排液堵塞和过滤器故障三种故障, 这对于液压阀的健康监测以及航天发射的安全性和可靠性至关重要.

航天发射系统还有另一重要的空调制冷系统, 其故障主要是由于日常操作不当和维护不良造成的. 一般来说, 即使是大型商业建筑中使用的标准设备, 空调制冷系统往往也是定制的, 缺乏高度的系统集成, 导致系统硬件和控制器故障频发. 针对此系统的故障检测与诊断方法主要分为三类: 分析方法、知识驱动的方法和数据驱动的方法. 基于分析的方法主要利用被测对象的实测数据与模型过程 (数学模型) 的残差来检测和诊断故障, 包括参数估计和输出残差两大类. 对于大规模系统, 尤其是对航天发射系统的大型空气制冷系统来说, 如果与数学模型有关的信息不可用或成本太高且耗时时, 基于知识的方法便是解决这些问题, 进行故障诊断的主流方法, 主要包括专家系统、因果建模以及模式分类等方法. 还有一种是在建模过程中, 使用监测数据和故障模式之间关联关系构建数据驱动模型, 这些方法主要优势在于将高维监测数据映射为低维特征, 包括模式识别以及基于信号的特征提取方法, 非常适合超大型设备系统的故障诊断[55−57].

近年来, 已有复杂工程系统的故障检测、诊断与传播方法的研究成果来看, 航天发射系统所涉及的众多子系统均在民用工业系统中得到了深入的研究, 如空调制冷系统与加注系统等, 而其所涉及的理论方法是否可以应用于航天发射系统中, 则是一个有待继续深入探讨的课题. 此外, 航天发射系统因其极大的复杂性, 往往涌现出所有单独个体或子系统均不具有的整体行为特性, 这也对故障诊断带来极大的挑战. 就目前来看, 现有的相关理论方法不能准确地描述系统外部变化和人为误操作等导致的系统内部运行性能的变化, 而航天发射场地处寒冷、风沙或者是高盐、高湿、高温等环境, 系统运行过程中易受环境变化、设备磨损和人为误操作等诸多因素的影响, 目前缺乏对航天发射系统运行故障传播演化的有效刻画. 因此, 对航天发射系统运行故障进行建模、检测、诊断等仍是一个极具挑战的研究, 也是极少有国内外学者涉足的研究领域.

2.2 系统异常运行工况识别研究现状

航天发射系统运行工况描述了系统在运行过程中的状况、工艺条件或设备在和其动作有直接关系条件下的工作状态. 航天发射系统运行过程中出现的异常工况, 若发现和处置得不及时、过程安全管理不到位会造成发射任务延误或推迟, 甚至导致发射失败、人员伤亡和设备损坏等安全事故. 例如, 由于航天发射系统所服务对象的特殊性, 任何系统的微小异常, 在高盐、高湿、高温, 甚至是运行环境的极端切换等, 都会将其放大为一起重大发射事故, 这与普通工业生产设备系统有着极大的区别.

异常是指监测数据由因不同机制产生的一种与其他观察结果不同的偏差. 就现有文献来看, 异常检测是一项从监测到的数据集中挖掘异常或异常数据, 即识别测试数据在某些方面与训练期间可用数据间差异性, 也称为新颖性检测、偏差检测和异常挖掘等. 由于众多重大罕见的事故是由微小异常的事件造成的, 因而异常工况检测得到了众多研究学者的关注. 异常检测的难点主要表现在数据不均衡性, 即有大量的 “正常” 运行工况的数据, 而没有足够的数据来描述 “异常”, 使得模型的训练具有极大的挑战性[44−51, 58].

异常检测在涉及从关键系统获取的大型数据集的应用领域中获得了很多研究关注, 包括复杂工业系统中的故障、结构损伤的检测, 电子安全系统中的入侵检测等. 现代高度集成的复杂系统使理解所获得的各种系统组件间的关联关系极为有限, 不可避免地存在大量可能的 “异常” 模式, 其中有相当一部分是无先验知识的, 极难匹配与识别. 如 Pimentel 等[59] 总结现有文献方法来看, 主要包括频域方法、贝叶斯网络法、信息论、极值统计、支持向量机、神经网络以及其他核方法, 依据各种方法的原理, 将其分类以下 5 类: 1) 基于概率的; 2) 基于距离的; 3) 基于重构的; 4) 基于值域的; 以及 5) 信息论[47].

基于概率方法的异常检测, 通常涉及 “正常” 类的密度估计问题, 即假设训练集中的低密度区域为大概率监测到的 “异常工况”; 基于距离方法的异常检测概念, 包括最近邻和聚类分析思想, 即假设 “正常” 数据紧密聚集, 而 “异常” 数据远离其最近邻类; 基于重构方法异常检测概念, 是采用训练集实现回归模型的训练, 当采用训练后的模型映射 “异常” 数据时, 回归目标与实际观察值间的重构误差较大, 进而实现异常工况检测; 基于值域方法的异常检测通常是指试图通过定义 “正常” 类的边界来描述 “正常” 数据域, 探索 “正常” 数据所服从的某种值域, 以实现异常检测; 基于信息论方法异常检测就是通过计算训练数据中的信息, 以此达到信息的提取、表征与识别, 如熵、谱系数等[47]. 如 Wu 等[45] 提出了一种数据驱动的异常运行工况识别方法, 其根据当前跟踪误差以及当前波动的速率和持续时间

提取识别规则, 并基于规则的推理识别异常工况, 以解决过程工业中, 因进料组分变化而未及时适当调节设定点而出现的异常工况. Zeng 等[46] 构建基于 Kullback-Leibler 差异性的异常工况检测模型, 该模型通过比较当前过程工况的估计密度和参考密度函数来检测系统的异常工况.

这些方法在现有关于航天发射系统异常工况在线识别与预警的研究报道还比较少, 但也已初现端倪. 龚学兵等[60] 针对航天总检查飞控系统早期故障征兆在闭环系统下难以被检测、数学模型难以精确建立的问题, 提出了一种基于数据关联性分析的系统异常监测方法. Riasi 等[61] 研究了加注管道中因加注水锤现象引起的非定常湍流管道的能量耗散和湍动能的产生及耗散, 以进行异常工况的识别. Do 等[44] 讨论了一种基于状态的主动维护技术, 该方法考虑到 "完美" 维护的高成本问题, 研究了 "不完美" 维护对系统运行的影响, 以发掘每次检查的最佳维护行为. Lutz 等[48] 则研究异常运行工况与安全关键指标间的演化关系, 主要关注异常操作对安全需求的动态影响, 结果却发现许多先前的错误规范致使了很多异常运行工况, 结果也表明需要增加对系统维护活动影响研究, 以提供技术支持. Matthews 等[49] 则针对运载火箭中关键部件 (流量控制阀) 的运行异常展开研究, 该流量控制阀的异常极易导致灾难性的气态氢泄漏, 为此, 提出了联合虚拟传感器的监督学习方法和感应监测系统的无监督学习方法实现主推进系统中流量控制阀相关异常的检测.

航天发射系统测量变量众多且彼此相互关联、耦合, 同时动态运行过程中存在不可预知的突变干扰以及其他众多不确定性因素, 在航天发射 "零窗口"、高可靠、高安全和高实时性的要求下, 对航天发射系统运行工况的特征提取、分析和识别显得尤为重要. 且就已有少量的报道文献中, 除未考虑外界环境、扰动变化和参数漂移等因素对工况的影响, 也未考虑航天发射系统变工况运行下的异常识别与预警问题. 开展基于数据分析与处理技术的挖掘隐含在航天发射系统运行数据中工况与过程变量的关联关系, 研究异常工况识别与预警技术具有重要的科学价值和工程意义.

2.3 系统运行过程安全分析研究现状

国标 GB-T20438.1-2006/IEC61508-1 中利用伤害、危险 (危险情况与危险事件)、风险 (允许风险和残余风险)、安全 (功能安全与安全状态) 及合理的可预见的误用等术语对电气/电子/可编程电子安全相关系统的功能安全进行刻画件的问题 (如传感器、控制器、执行器等), 而且要考虑构成组合安全相关系统的所有相关系统的安全[62]. 标准中进一步指出, 为保证系统安全不仅要考虑各系统中元器件的问题 (如传感器、控制器、执行器等), 而且要考虑构成组合安全相关系统的所有相关系统的安全[62−65]. 因此, 在系统设计或运行过程阶段, 综合利用各种现代分析方法研究系统运行过程中潜在的安全问题和危险因素, 是保证现代航天发射系统运行过程固有安全性的重要研究内容[63, 66−68].

目前, 多数工业过程常用的安全分析方法[15] 是基于静态的安全分析, 很大程度上不能反映系统实际的运行情况. 如 Chandra 等[31] 中电力系统静态安全分析方法, 只考虑事故后稳定运行情况的安全性, 没有考虑从当前的运行状态向事故后稳定状态的动态转移过程. Saeh 等[69] 提出采用径向基神经网络实现电力系统静态安全分析, 且与人工智能分类器进行了比较, 以检验电力系统是否在稳态运行条件下得到保护. 但也有一些学者尝试设计一种实时的安全性分析方法, 如 Gholami 等[70] 提出了一种新颖的智能分层结构的分类算法, 与传统方法相比, 具有更小的计算复杂度, 适用于不同情境间的实时安全性分析. 风险评估分析是化工过程工业常见的安全分析方法, 如 Arunraj 等[71] 使用模糊集理论和蒙特卡罗模拟方法改进了适用于工业安全风险评估方法, 对风险评估过程中的不确定性进行了建模, 与传统方法不同, 该方法提供了比现有方法更好的不确定性度量, 将信息的可变性和不确定性考虑到风险计算中, 而不是单一风险, 提供了一种以区间形式表征的风险计算值.

而针对航天发射系统的整体运行安全性分析与预测方法还没有形成体系化的研究理论, 相关研究还处于起步阶段. Watson 等[72] 认为航天工程系统是集成和平衡许多不同的系统而构建的有效体系, 通过分析运载火箭的热力学性质, 识别集成系统的运行性能, 调整许多不同配置, 确定最有效的设计以及从系统角度指导设计活动. 航天发射过程中, 运载火箭以及相关设备常常需要经历其他工业系统不常见的高强振动问题, Kolaini 等[73] 讨论了完全组装好的飞行航天器振动测试方面的益处以及存在的潜在问题, 包括航天器筛选测试、发动机动力学环境的工艺问题、力和力矩限制振动测试等, 使用振动测试结构频率数据实现潜在问题的识别. Luo 等[74] 考虑了导航偏差和控制误差的航天器交汇轨迹定量安全性能指标, 主要包括追踪车 3σ 椭球与目标车控制区间的最小距离以及两者间的最大瞬时碰撞概率, 提供了安全性能指标的详细定义和简化的计算方法.

国内学者崔豹等[75] 针对发射场地面设备的薄弱环节、潜在风险及其原因, 从风险分析的角度研究设计了一种基于概率风险评价 (PRA) 的发射场风险分析系统. 苏永芝等[76] 探讨了我国航天发射场地

面设施设备可靠性分析的研究现状及相关问题. 美国宇航局艾姆斯研究中心 (NASA′s Ames Research Center)[77] 针对发射过程中碎片数量及速度变化趋势对航天员安全影响, 通过结合物理机理与经验知识建立与时间相关的碎片场概率风险模型实现发射过程的风险预测. Chen 等[78] 构建了航天器装配风险评估分析模型, 来研究和分析该装配过程安全问题. 该文中[78] 还介绍了航天器装配的安全性和可靠性的国内外研究, 在此基础上, 进一步讨论了系统安全性和可靠性的关系和区别, 并强调航天器装备的安全评估与分析的内容不仅仅局限于人为故障、系统设计和环境而引起的系统功能损失, 提出了航天器装配系统安全分析和定量风险评估模型, 包括 4 个步骤: 1) 工作程序和任务分解; 2) 为每项任务开发安全分析图; 3) 航天器装配风险识别和事故预测数据库系统的发展; 4) 航天器装配的安全评估指标体系.

然而, 航天发射过程运行安全分析与预测的实现仍存在层次多、因素多和类型多等问题. 针对过程/设备出现故障、工艺指标出现异常 (如液体燃料加注的温度、压力、流量异常)、以及操作中突然发生人为因素的差错 (如误动开关、操作截止阀开度小或开度大、操作顺序错误等) 等情况, 研究带有时序特性的故障、事故与隐患的演化机制对实现系统动态安全分析, 及时进行系统运行安全的评估, 避免可能导致的事故发生.

2.4 系统运行安全性动态评估研究现状

航天发射运行安全实时评估的结果直接关系到发射任务是否按计划进行, 甚至直接关系到避免事故的发生, 可见系统运行安全评估在航天发射过程中的重要地位.

目前, 各类复杂工程系统运行安全的评估理论和方法主要分为三种类别[60, 63, 66−68, 79−82]: 1) 基于定性分析的运行安全评估方法, 主要是将静态安全分析方法应用于动态运行过程中, 方法的实时性有待进一步深入研究; 2) 基于定量的运行安全评估方法, 定量表示与计算各种危险因素、后果以及发生的可能性等, 采用包括事件树法、马尔科夫法、事件序列图法、逻辑分析方法、模拟仿真方法等实现系统运行安全的评估; 3) 综合评估方法, 包括风险协调评审和概率风险评估方法等. 如 Chen 等[83] 提出了一种利用事故后稳态安全距离指数 (Post-contingency steady-state security distance, PCSSD) 的安全评估方法, 该模型是一种大规模的非线性优化模型, 可有效地识别事故后稳态安全域的有效边界, 如若 PCSSD 计算的工作点到应急后稳态安全区域边界距离最短, 则系统在意外事件后是安全的. 在动态运行风险评估模型中, 组件修复时间是表征组件状态和后续系统状态的重要参数, 特别适合于工业系统的部件修复时间评估, 用作系统状态轨迹的蒙特卡罗模型的输入, 如 Yang 等[84] 应用统计分析技术来表征相关参数数据的分布模型的不确定性和敏感性, 并以分布模型选择参数的分配, 以研究动态运行风险评估模型的输出, 以达到确定组件修复时间的分布.

航天发射是依靠发射场的设备、设施系统实现加注推进剂、射前总检查、点火发射等全部工作和程序的实施过程, 相关学者从设备性能、系统可靠性等不同层次对航天发射系统运行安全评估展开了研究. Dong 等[10] 研究了航天发射系统的运行安全性, 定义了系统中补偿性和不可替代性因子, 在分析了空间因素和系统组织安全性的基础上, 构建了航天发射系统的整体组织安全性模型, 并采用灰色关联分析技术对影响系统安全的因素进行评估. Kadzhaev 等[16] 讨论了运载火箭发射准备阶段的可靠性与安全水平的准则, 描述了系统无故障运行的概率、后验可靠性和安全屏障等. Gee 等[77] 则重点关注了运载火箭在上升飞行过程中因故障而中止发射, 且要实现机组人员与运载工具安全分开, 以便机组人员安全返回地球, 其构造了一个物理模型以描述和评估发射失败环境下的安全风险的演化过程. 崔豹等[75] 实现了安全评估过程的 “定性分析、定量计算、定标评价”.

另一方面, 航天发射系统为满足日趋复杂的航天器和运载器, 且发射任务日益多样化, 迫切需要解决任务过程趋于密集动态化、设备组成趋于系统网络化、故障因素趋于多元关联化等背景下的航天发射系统动态安全性评估理论与方法[28−29, 75−76, 81−82, 84−88]. 徐克俊等在文献 [8] 中系统地介绍了航天发射场可靠性与安全性的评估方法, 对相关定性和定量评估方法的优缺点进行了总结. Nield 等[85] 则对美国商业载人空间飞行运行安全的标准进行了介绍, 重点分析了基于安全查表法的运行安全评估. 宋建军等[28] 针对航天发射场加注系统风险评估过程中主观随意性较大的问题, 提出了基于综合云的多属性风险评估方法计算得到加注系统各风险源的权重, 使得风险源权重的确定更具客观性和合理性.

定性安全评估方法虽然可以快速高效地进行危险辨识、后果分析, 但大多偏重于设计阶段的静态分析且只针对单一故障, 而航天发射系统具有多工况间歇运行的特点, 不同工况下故障模式多样且设备之间不是简单的一一对应关系. 因而基于定性分析的安全评估难以建立对象多因素作用下的系统级动态安全评估模型, 也难以给出安全风险事件的重要

度排序及其不确定影响和系统的累加风险值[85]. 定量安全评估方法以航天发射系统发生事故的概率或性能分析为基础, 虽然能够求出风险率, 以风险率的大小衡量系统危险性大小及安全度, 但由于航天系统设施设备类型多、服役时间长、短期运行和长期停用、使用环境恶劣等特点, 使得定量分析法难以准确地评估系统的运行安全[8]. 综合安全评估方法尽管对复杂系统的特性有全面深刻的了解, 能够找出系统的薄弱环节提高系统的安全性, 为风险决策提供有价值的定量信息[79], 但尚未从航天发射系统实时运行状态、间歇运行多工况等方面系统深入地研究航天发射系统的动态安全性.

从航天发射系统实时运行状态、间歇运行多工况等方面深入研究航天发射系统的动态运行安全性, 研究如何根据航天发射系统异常运行工况、运行故障等方面的分析结果, 构建系统运行安全性评价指标体系, 是保障我国航天事业安全快速发展需要解决的关键问题.

3 航天发射系统运行安全评估面临的挑战

航天发射是实现航天器送上太空活动的统称, 是评判一个国家综合国力的重要指标, 是航天工程最为基础和最为重要的环节之一, 具有成本高昂、技术难度大、过程复杂, 其组织规模、复杂程度远远超过一般工程系统, 也给航天发射系统运行安全动态评估带来了一系列挑战.

就我国现有的航天发射系统来看, 系统运行安全性评估所具有的挑战性问题主要表现在以下几方面[3−12]:

1) 系统极度复杂. 现代航天发射系统是包含设施设备、人员、材料等在内的复杂系统, 具有试验设备类型繁多、技术复杂、集成度高、投资大、使用周期长、环境影响大、涉及部门人员众多以及指挥操作流程复杂等特点, 存在层次多、因素多和类型多等问题. 因而其结构和规模的复杂性是其区别于传统复杂系统的基本特点, 涉及专业数量, 系统关联耦合程度, 以及安全性要求都远远超过一般的复杂工程系统[51−57].

2) 决策风险性极大. 高风险是航天发射场的突出特点, 且其由很多具有不同功能和物理机制并在行为上相互耦合、强烈相关的子系统组成, 任何一个设备或系统的异常或故障, 甚至微小的失误和缺陷就可能导致安全事故, 导致航天工程系统具有许多其他复杂系统不常见的风险性, 使得其安全裕度的可操作区间极其有限, 极易引发安全事故. 因而对航天发射系统故障与异常工况的误检、误判和错误处理, 往往孕育着巨大的安全风险, 甚至给国民经济, 国家的整个航天计划带来极大的影响[4, 8−9, 11−13, 16, 19, 89−91].

3) 先验知识信息少. 航天发射系统本身是一种间歇使用、长期维护的系统, 且每次任务都有新研制的试验产品 (卫星、飞船、空间站等, 以及运载火箭和发射设施) 被应用在各航天发射任务中, 常出现新的异常与故障, 使得航天工程具有明显的探索性、试验性等特点, 表现出单台次、小批量、使用环境恶劣等特点, 故障与异常运行工况先验知识信息很少[4, 8−9, 11−13, 16, 19, 37−39, 92].

4) 高准确性与实时性. 在现代航天工程中, 发射窗口精度要求极高, 最长不到 2 小时, 最短 20 ∼ 30 秒 (“零窗口”). 需要在航天发射过程中尽早发现故障与异常, 尽快诊断故障与识别异常, 及时决策处置, 要达到这一要求, 就要求系统对运行过程做到早发现、早辨识、早规避、早解决. 再者, 航天发射系统故障危害巨大, 对安全性、可靠性有着苛刻的要求, 需要研究系统运行安全性的变化趋势, 实时辨识系统运行中的异常工况与故障, 以采取高效准确的维修策略[3, 10, 29, 88, 93−99]. 因此, 高准确性与实时性的客观要求也给航天发射系统运行安全性的实时评估带来了巨大的挑战.

随着我国航天发射活动越来越密集, 试验任务交叉并行, 发射系统设施设备任务状态变化大, 技术状态转换快, 检测维护时间紧张, 系统运行安全性问题越来越突出.

4 思考与展望

虽然我国一直在不断跟进国外航天发射系统技术的发展, 并开展了若干项航天发射安全分析与评估等关键技术的预研和技术验证工作, 但与国外主要机构相比, 存在着较大的差距. 本文认为, 在从航天大国迈向航天强国的过程中, 应在系统运行事故演化、系统异常运行工况识别、系统动态运行过程安全分析与评估等方面展开深入研究, 以提高我国的安全、快速地空间进入能力[28−30, 100].

1) 系统运行事故的演化规律与机理建模研究方面

航天发射系统在运行过程中, 某些危险因素在连续的时间内的多次出现是事故发生的主要原因. 在系统/设备的工艺参数超限、故障以及误操作等危险因素的影响下, 系统的大规模和子系统间的强耦合使得系统运行事故的发生机理和演化规律呈现出复杂性和不确定性. 因此, 在系统运行事故的演化规律和机理建模等方面的研究, 由于系统中任何一个运行异常或故障都可能通过耦合的子系统、设备进行传播和扩散, 变得愈发重要, 主要包括系统 “危险因素 − 事故” 演化机理建模、系统运行工况与危险因素关联关系建模以及系统运行事故演化的动态仿真

技术研究[17, 25, 35−43, 55−57].

系统 “危险因素 – 事故” 演化机理建模主要是考虑到安全事故的发生与发展往往是由于系统中各种危险因素与系统相互作用与耦合的复杂动力学演化过程, 应从能量变化角度和系统控制角度建立安全事故演化的机理模型. 从能量变化角度, 分析发射过程中的危险事故以及事故发生的能量变化过程, 构建能量变化模型; 分析子系统事故能量传递特性, 研究基于能量守恒和突变拓扑空间的运行安全事故分析模型. 从系统控制角度, 针对运行过程中出现的工艺参数超限、故障以及误操作等危险因素, 分析危险因素在系统运行中 “发生 – 扩散 – 事故” 的参数和状态行为的特征变化, 通过航天发射系统运行监测参数和子系统机理模型, 研究运行安全事故的演化机理和演化条件, 建立描述系统性能和工艺指标劣化、误操作、异常工况和系统故障的多时空多尺度事故演化模型[93, 101−105].

系统运行工况与危险因素关联关系建模主要是通过系统事故演化状态模型与实际运行下的系统状态模型相关联, 分析系统运行各种工况的安全性. 将航天发射系统所包含的机械系统、电气系统以及过程系统等多个子系统, 根据所研究的安全性事故演化过程, 分析误操作、设备故障作用下子系统的系统动态行为及其状态转移规律, 得到事故演化状态. 针对系统物理参数的变化而引起的不确定性, 发射场恶劣运行环境和试验过程中引发的未知干扰, 在信息传输过程中由于受到物理设备限制而引起测量信号发生变化等问题, 通过建立自适应状态观测器或状态最优估计器, 对系统状态进行重构或最优估计. 通过利用系统运行监测数据, 量化航天发射系统各阶段的工况特征变量与系统状态的关联关系, 建立工况特征变量和系统状态映射模型[106−108]. 设计危险因素/故障的事故演化状态与系统状态的残差滤波器, 通过残差信息描述系统运行工况与危险因素/故障的关联关系.

系统运行事故演化的动态仿真技术研究主要是基于系统组成结构和物理特性, 结合实测数据重点对加注系统和射前飞行控制模拟 (总检查) 建立半实物数值仿真模型. 从理论分析、实验研究和数值模拟研究各子系统在 “故障”、“误操作” 下的事故演化过程. 对于物理机理已知的系统, 分析系统的 “危险因素”、“故障” 对参数的影响; 对于已知测试数据和典型故障特性的模块, 应用机器学习和函数逼近的方法模拟系统模块的 “黑盒子” 特性. 通过对子系统传递函数、功能原理的分析, 建立功能模块之间的关系模型, 动态仿真航天发射系统中典型系统的 “危险因素 – 事故” 传播与演变过程[109−111].

2) 数据驱动的系统异常工况在线识别方面

航天发射系统运行工况描述了系统在运行过程中的状况、工艺条件或设备在和其动作有直接关系的条件下的工作状态. 通过分析以加注系统、发射塔架液压系统等航天发射过程系统的工作状况, 以及发射控制设备在某一时刻的运行状况, 对航天发射系统的异常工况进行识别. 因此, 从航天发射系统物理机理分析模型和数据实时处理与分析的角度出发, 挖掘数据描述下的运行工况与过程变量的关联关系, 构建运行工况过程多变量高维工作区模型, 研究基于工作区动态阈值的异常工况在线识别, 为航天发射系统运行安全实时评估奠定必要的基础[44−51, 58−61, 112].

运行工况与过程变量的关联关系挖掘主要是针对系统运行监测数据量大和多源异构特性, 研究基于增量式算法和多维关联规则的相关关系挖掘算法, 分析数据间以及数据与工况间的相关关系. 针对过程变量与运行工况的关系复杂、时变、难以精确表达等问题, 结合序列模式分析、空间模式挖掘和结构挖掘等海量数据分析方法研究表征运行工况的过程变量间时序关联规则, 构建过程变量与工况指标的动态关联矩阵, 提取航天发射系统多工况过程的特征变量[113].

运行工况的多特征变量高维空间模型主要是考虑到发射任务多阶段、多过程的运行工况与多个特征变量关联的特点, 结合发射任务技术状态与子系统单元操作模式, 分析特征变量参数间的关联函数, 研究基于关联函数的参数聚类算法. 针对航天发射系统过程监控数据与运行工况的非线性关联问题, 依据发射系统先验知识和发射任务流程, 结合工况特征变量与运行工况的关联关系, 建立系统典型工况下多个特征变量共同表征的高维工作区模型, 分析历史关键变量和运行特征变量之间的差异与趋势, 优化更新当前工作区域模型[30, 114−116].

运行工况工作区模型的动态阈值设计主要内容是基于运行工况的高维工作区模型和运行工况表示模型, 以航天发射系统运行工序的工艺指标与性能指标为基础, 研究特征变量工作范围与运行工况关联下的动态阈值设计方法. 以误报率、漏报率和检测延迟为指标, 结合非参数统计和贝叶斯决策理论, 建立异常工况阈值的目标函数, 研究过程在参数死区和延迟等因素下的阈值优化技术与方法[116].

3) 危险因素下动态运行过程安全分析方法研究方面

航天发射系统具有短期运行和长期停用、服役时间长、使用环境恶劣等特点, 使得系统在运行中伴随着众多的安全隐患, 需要及时进行系统运行安全的分析、评价、诊断, 预测系统的运行安全和设备状况, 避免可能导致的事故发生. 因此, 需要研究

高安全性要求下的航天发射系统实时运行安全分析方法, 主要包括变工况下过程工艺参数超限运行安全分析、数据驱动的系统运行故障诊断与安全分析以及人在回路的误操作辨识与运行安全分析三大方面[15, 31, 55−57, 62−71, 77−78, 80].

变工况下过程工艺参数超限运行安全预测分析主要是因为航天发射系统本质上是非线性动力学系统, 其结构之间相互耦合, 运行工况在阶段性变化下, 使其过程变量 (温度、流量、液位和压力) 具有复杂的动态特性和时变性, 需要针对系统在运行过程中工艺参数超过设计指标, 通过状态估计将超限信息转化为状态信息, 结合事故演化机理, 建立过程工艺参数超限的系统状态和事故演化状态之间的映射模型, 提取事故演化状态的系统安全特征, 分析其变化趋势和分布特性, 最后通过聚类和分类方法识别系统状态, 根据不同系统状态之间的转移概率, 建立基于状态转移的系统运行安全预测模型[117].

数据驱动的系统运行故障诊断与安全分析主要是根据实测数据、历史运行数据、专家知识等信息, 提取系统安全运行的特征参数, 研究基于数据驱动的系统运行安全分析方法. 结合系统性能退化特性, 发现故障在控制系统中的传播过程, 预判故障的发展趋势及事故的演化进程. 从监测信息的智能感知与系统内部结构特性的分析角度出发, 研究基于深度学习、流形学习等非线性学习的系统故障特征集构建方法. 结合历史运行数据和专家知识, 构建具有复杂动态推理能力的基于数据信息的故障诊断方法. 针对故障下的运行安全性预测, 结合 “故障−事故” 演化模型和 “工况−故障” 关联模型, 利用定性和定量相结合的方法, 提取表征系统安全运行的关键参数. 结合系统运行故障的传播特性、时间特性和子系统间的故障耦合作用, 研究故障下系统运行安全性的预测方法[118−119].

人在回路的误操作辨识与运行安全分析是指航天发射系统运行过程中, 按照发射流程涉及大量的手动操作, 而人在回路中的误操作将会导致系统运行状态的变化, 进而影响整个系统的运行性能, 甚至造成安全事故. 应用运行工况工作区模型和预警技术分析系统在误操作下的工况特征变量并预警异常工况, 在线实时辨识和定位系统发生的误操作类型和相应子系统. 结合 “误操作−事故” 演化模型和运行工况与危险因素关联模型, 判断误操作下的运行安全问题. 针对人在回路系统误操作和运行状态的混杂特性, 应用符号有向图描述误操作下系统过程变量间的作用过程以及发射系统能量和物质的传播路径, 结合 Petri 网描述系统误操作事件的离散特性和在耦合子系统的各层次、各阶段的传播趋势, 建立误操作下系统运行安全性分析和趋势预测模型[120−123].

4) 系统运行安全性实时评估体系与方法研究方面

现代航天工程中, 在有限发射窗口的需求下, 由发射系统、运载器和航天器所构成的庞大系统存在着大量的未知规律, 从燃料加注到点火起飞过程中, 误操作、运行参数超限和系统故障等危险因素具有很大的不确定性, 系统失效模式相当复杂、影响安全性的诱因多. 准确的故障风险分析和发射系统运行安全性评估对航天发射任务显得尤为迫切, 亟待建立以发射安全为目标的安全性评估指标体系, 实时对各种危险因素做出分析和评估, 保证完成发射任务和保障系统运行安全[8, 28−29, 60−61, 66−68, 75−77, 79−88].

系统运行安全实时评价指标体系的构建是在分析误操作、故障传播和事故演化对系统行为影响的基础上, 确定系统中的危险因素和危险过程, 由系统中的故障、误操作、异常工况和参数超限等构成系统安全的评价要素集. 通过系统运行监测数据, 分析数据和安全要素之间的相关关系, 选取系统运行过程中可表征运行安全的相关参数/过程变量, 得出安全指标变量集, 建立运行工况下的航天发射系统安全性实时评估量化指标. 利用系统或设备的额定参数指标, 通过所研究的事故演化机理, 分析安全评价要素与额定参数之间的映射关系, 构建安全事故演化机理下的安全性评价指标. 根据《GJB900-90 系统安全性通用大纲》和《QJ2236 航天器和导弹武器系统安全性通用大纲》等提取出航天发射安全性要求的定性、半定量和定量评价指标. 综合以上三类安全性评价指标, 通过功能聚合和相关性聚合, 针对现场设备层安全评估、过程/子系统层安全评估和系统运行层安全评估, 从工艺参数超限、额定指标超限、异常工况、故障、误操作等出发, 建立运行安全综合评价指标体系[124−126].

系统运行安全性实时评估计算模型是指分析航天发射系统在各个危险过程中存在的安全事故类型, 针对不同事故类型如设备损坏以及引发的二次事故等, 应用模糊分析等计算事故的严重程度, 建立系统基于运行事故严重程度的安全性评估等级. 针对工况异常和危险因素如故障、误操作等, 筛选指标体系中相同层级的评价指标并进行聚合处理. 结合误操作、设备故障和工艺参数异常下安全性预测技术, 应用层次分析量化各指标的相对重要程度, 应用统计分析建立各指标的重要性区间和相应的置信度分布, 从而构建系统运行安全性实时评估计算模型[127−129].

基于危险因素和指标体系的安全性实时评估考虑航天发射系统的危险运行阶段中, 出现的物质、能

量密集流动的特点, 利用系统运行工况的安全关键参数, 建立危险指标集和相应的指标范围, 对危险过程运行安全性的实时预警. 针对系统故障和误操作下系统异常运行, 结合运行事故演化模型以及运行工况与危险因素关联模型, 实时识别系统运行过程中发生的危险因素. 基于运行工况异常区间模型, 实时计算系统当前危险因素下各指标的重要区间的置信度和系统安全性等级. 以系统运行监测的海量数据出发, 研究系统异常工况的识别与预警、运行安全性的在线分析和运行安全性实时评估的理论和方法, 提高系统的安全性[130−133].

5 结束语

航天发射系统运行安全性实时评估是现代航天发射控制指挥与决策系统的重要组成部分, 综合利用各种现代分析方法发现发射过程中潜在的安全问题和危险因素, 是保障我国航天事业安全快速发展迫切需要关注的研究领域.

为此, 本文首先概述了现代航天发射系统, 指出其运行安全性实时评估技术是现代航天发射控制指挥与决策监控系统的重要组成部分. 此后, 回顾了航天发射系统运行安全性的发展历程, 概述了系统运行安全性实时评估的研究内容, 主要包括系统运行故障检测与诊断、异常运行工况识别、运行过程安全分析与预测、安全性动态评估技术等方面, 并对这 4 方面的研究现状进行的总结. 接着, 依据航天发射系统的运行特性, 总结出了航天发射系统运行安全性方面的挑战. 最后, 随着航天任务的多样化, 在运行监测的海量数据下, 对航天发射系统运行安全性分析与评估的未来研究进行了思考.

References

1 Stamatelatos M. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. Washington, D. C., USA: NASA, 2011.

2 Morio J, Balesdent M. *Estimation of Rare Event Probabilities in Complex Aerospace and Other Systems*. Waltham: Woodhead Publishing Limited, 2015.

3 Chai Yi, Li Shang-Fu. *Intelligent Testing, Control and Decision-Making for Space Launch*. Beijing: National Defense Industry Press, 2013.
(柴毅, 李尚福. 航天智能发射技术–测试、控制与决策. 北京: 国防工业出版社, 2013.)

4 Chai Y, Li S F. *Intelligent Testing, Control and Decision-Making for Space Launch*. New York: John Wiley & Sons, 2015.

5 Wang Jia-Wu, Shen Huai-Rong, Tang Li-Wen. The research of C3I system on modern spacecraft launching fields. *Journal of Institute of Command and Technology*, 2001, **12**(1): 52−56
(王家伍, 沈怀荣, 唐立文. 现代航天发射场 C3I 系统探讨. 指挥技术学院学报, 2001, **12**(1): 52−56)

6 Chai Yi. Intelligent space launch system and its key technology. *National Defense Science and Technology*, 2016, **37**(1): 7−9, 13
(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, 13)

7 Zhang Peng, Zhang Zhi-Yong, Yin Yu-Shu. The study of aerospace launch sites integration command decision system architecture. *Computer and Information Technology*, 2016, **24**(2): 12−15
(张鹏, 张志勇, 尹玉曙. 航天发射场一体化指挥决策系统体系架构研究. 电脑与信息技术, 2016, **24**(2): 12−15)

8 Xu Ke-Jun, Jin Xing, Zheng Yong-Huang. *The Reliability and Safety Assessment of Spacecraft Launch Site*. Beijing: National Defense Industry Press, 2006.
(徐克俊, 金星, 郑永煌. 航天发射场可靠性安全性评估与分析技术. 北京: 国防工业出版社, 2006.)

9 Mashchenko A, Fedyakin A. Space launch system safety estimation models. *Acta Astronautica*, 2009, **64**(1): 9−13

10 Dong X J, Chen Y W, Li M, Zhang Y X. A spacecraft launch organizational reliability model based on CSF. *Quality and Reliability Engineering International*, 2013, **29**(7): 1041−1054

11 USA, Department of Defense. Handbook test requirements for launch, upper-stage, and space vehicles, Vol I: baselines and Vol II: applications guidelines. MIL-HDBK, 1999.

12 Murtazin R, Petrov N, Ulybyshev Y. Launch strategy for manned spacecraft: improving safety or increasing of launch mass? *Acta Astronautica*, 2011, **69**(7−8): 644−649

13 Luo Gui-Hua. The Optimization of Planning, Scheduling and Allocation of Human Resources on Space Launching Project [Master thesis], Zhejiang University, China, 2010
(罗桂华. 航天发射场的最优运行研究 [硕士学位论文], 浙江大学, 中国, 2010)

14 Satellite Earth Stations and Systems (SES), European Cooperation for Space Standardization (ECSS), Satellite Software Data Handling Interfaces (SSDHI), European Standard ETSI-EN-301-927, 2003.

15 Jones R T, Handsfield L, Read P W, Wilson D D, Van Ausdal R, Schlesinger D J, et al. Safety and feasibility of STAT RAD: improvement of a novel rapid tomotherapy-based radiation therapy workflow by failure mode and effects analysis. *Practical Radiation Oncology*, 2015, **5**(2): 106−112

16 Kadzhaev V, Barmin I, Denoyers J Y, Ragot A. Ensuring an acceptable reliability and safety level for a launch complex. *Acta Astronautica*, 2011, **68**(7−8): 1079−1085

17 Ren H, Chai Y, Qu J F, Ye X, Tang Q. A novel adaptive fault detection methodology for complex system using deep belief networks and multiple models: a case study on cryogenic propellant loading system. *Neurocomputing*, 2018, **275**: 2111−2125

18 Liu Hai-Fei, Chen Hong, Wang Tian-Xiang, Lei Gang. Study on the transient flow characteristics of the filling pipe of liquid hydrogen/liquid oxygen cryogenic propellants. *Journal of Hydrodynamics*, 2014, **29**(6): 642−648
(刘海飞, 陈虹, 王天祥, 雷刚. 液氢和液氧低温推进剂加注系统中的管路瞬变特性研究. 水动力学研究与进展, 2014, **29**(6): 642−648)

19 Békési B. System Safety Program Requirements, NASAMIL-STD-882D, 2000.

20 国防科学技术工业委员会. QJ2236 航天器和导弹武器系统安全性通用大纲, 1996.

21 国防科学技术工业委员会. GJB900-90 系统安全性通用大纲, 1996.

22 der Kiureghian A. Risk assessment of satellite launch with reusable launch vehicle. *Reliability Engineering and System Safety*, 2001, **74**(3): 353−360

23 Keller S, Collopy P. Value Modeling for a Space Launch System. *Procedia Computer Science*, 2013, **16**: 1152−1160

24 Gee K, Lawrence S L. *Sensitivity Analysis of Launch Vehicle Debris Risk Model*. Washington, D. C., USA: NASA, 2010.

25 Xu D L, Liu J, Yang J B, Liu G P, Wang J, Jenkinson I, et al. Inference and learning methodology of belief-rule-based expert system for pipeline leak detection. *Expert Systems with Applications*, 2007, **32**(1): 103−113

26 Zhang Ke, Zhou Dong-Hua, Chai Yi. Review of multiple fault diagnosis methods. *Control Theory and Applications*, 2015, **32**(9): 1143−1157
(张可, 周东华, 柴毅. 复合故障诊断技术综述. 控制理论与应用, 2015, **32**(9): 1143−1157)

27 Harland D M, Lorenz R. *Space Systems Failures: Disasters and Rescues of Satellites, Rocket and Space Probes*. Chichester: Praxis, 2005.

28 Song Jian-Jun, Du Xiao-Ping, Zhao Ji-Guang. Research on risk evaluation in filling system of space launch site. *Aerospace Control*, 2012, **30**(1): 76−80
(宋建军, 杜小平, 赵继广. 航天发射场加注系统风险评估技术研究. 航天控制, 2012, **30**(1): 76−80)

29 Song Zheng-Yu. The survey of launch vehicle long distance fault diagnosis technique. *Journal of Astronautics*, 2016, **37**(2): 135−144
(宋征宇. 运载火箭远程故障诊断技术综述. 宇航学报, 2016, **37**(2): 135−144)

30 Zhang Su-Ming, An Xue-Yan, Yan Ting-Gui, Yan Xaio-Tao. Analysis and discussion of health management technology for large launch vehicle. *Missiles and Space Vehicles*, 2013, (6): 33−38
(张素明, 安雪岩, 颜廷贵, 阎小涛. 大型运载火箭的健康管理技术应用分析与探讨. 导弹与航天运载技术, 2013, (6): 33−38)

31 Chandra S, Mehta D, Chakrabortty A. Equilibria analysis of power systems using a numerical homotopy method. In: Proceeding of the 2015 IEEE Power and Energy Society General Meeting. Denver, USA: IEEE, 2015. 1−5

32 Yin S, Xiao B, Ding S X, Zhou D H. A review on recent development of spacecraft attitude fault tolerant control system. *IEEE Transactions on Industrial Electronics*, 2016, **63**(5): 3311−3320

33 Marzat J, Piet-Lahanier H, Damongeot F, Walter E. Model-based fault diagnosis for aerospace systems: a survey. *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, 2012, **226**(10): 1329−1360

34 Kang X, Pi D C. A data-driven method of health monitoring for spacecraft. *Aircraft Engineering and Aerospace Technology*, 2018, **90**(2): 435−451

35 Datta S, Sarkar S. A review on different pipeline fault detection methods. *Journal of Loss Prevention in the Process Industries*, 2016, **41**: 97−106

36 Kordestani M, Zanj A, Orchard M E, Saif M. A modular fault diagnosis and prognosis method for hydro-control valve system based on redundancy in multisensor data information. *IEEE Transactions on Reliability*, 2019, **68**(1): 330−341

37 Carvajal-Godinez J, Guo J, Gill E. Agent-based algorithm for fault detection and recovery of gyroscope′s drift in small satellite missions. *Acta Astronautica*, 2017, **139**: 181−188

38 Yang E F, Xiang H J, Gu D B, Zhang Z P. A comparative study of genetic algorithm parameters for the inverse problem-based fault diagnosis of liquid rocket propulsion systems. *International Journal of Automation and Computing*, 2007, **4**(3): 255−261

39 Moore R C. Autonomous safeing and fault protection for the New Horizons mission to Pluto. *Acta Astronautica*, 2007, **61**(1−6): 398−405

40 Yu J, Rashid M M. A novel dynamic Bayesian network-based networked process monitoring approach for fault detection, propagation identification, and root cause diagnosis. *AIChE Journal*, 2013, **59**(7): 2348−2365

41 Pandit J K, Mahapatra D R, Pandiyan R. Modal analysis of power electronics module of spacecraft and its health monitoring-an approach. *Procedia Engineering*, 2016, **144**: 283−288

42 Yin Mao-Jun. Research and Implementation of Launch Vehicle Fault Diagnosis System [Master thesis], University of Electronic Science and Technology of China, China, 2011
(尹茂君. 运载火箭故障诊断系统研究与实现 [硕士学位论文], 电子科技大学, 中国, 2011)

43 Ma Xin-Hui, Luan Xiao, Chen Jing-Peng, Sun Ke. Hot-Leakage fault simulation and analysis of filter in liquid hydrogen filling system. *Cryogenics*, 2012, **40**(7): 17−21
(马昕晖, 栾骁, 陈景鹏, 孙克. 液氢加注系统中过滤器漏热故障仿真与分析. 低温技术, 2012, **40**(7): 17−21)

44 Do P, Voisin A, Levrat E, Iung B. A proactive condition-based maintenance strategy with both perfect and imperfect maintenance actions. *Reliability Engineering and System Safety*, 2015, **133**: 22−32

45 Wu Z W, Wu Y J, Chai T Y, Sun J. Data-driven abnormal condition identification and self-healing control system for fused magnesium furnace. *IEEE Transactions on Industrial Electronics*, 2015, **62**(3): 1703−1715

46 Zeng J S, Kruger U, Geluk J, Wang X, Xie L. Detecting abnormal situations using the Kullback-Leibler divergence. *Automatica*, 2014, **50**(11): 2777−2786

47 Greensmith J, Aickelin U, Tedesco G. Information fusion for anomaly detection with the dendritic cell algorithm. *Information Fusion*, 2010, **11**(1): 21−34

48 Lutz R R, Mikulski I C. Operational anomalies as a cause of safety-critical requirements evolution. *Journal of Systems and Software*, 2003, **65**(2): 155−161

49 Matthews B L, Srivastava A N, Iverson D, Beil B, Lane B. Space shuttle main propulsion system anomaly detection: a case study. *IEEE Aerospace and Electronic Systems Magazine*, 2011, **26**(9): 4−13

50 Karanki D R, Kim T W, Dang V N. A dynamic event tree informed approach to probabilistic accident sequence modeling: dynamics and variabilities in medium LOCA. *Reliability Engineering and System Safety*, 2015, **142**: 78−91

51 John A, Yang Z L, Riahi R, Wang J. A risk assessment approach to improve the resilience of a seaport system using Bayesian networks. *Ocean Engineering*, 2016, **111**: 136−147

52 Rahman F A, Varuttamaseni A, Kintner-Meyer M, Lee J C. Application of fault tree analysis for customer reliability assessment of a distribution power system. *Reliability Engineering and System Safety*, 2013, **111**: 76−85

53 Higdon K P, Klaus D M. Characterizing human spacecraft safety and operability through a minimum functionality design methodology. *Journal of Spacecraft and Rockets*, 2013, **50**(3): 591−602

54 Sharifi S, Tivay A, Rezaei S M, Zareinejad M, Mollaei-Dariani B. Leakage fault detection in Electro-Hydraulic Servo Systems using a nonlinear representation learning approach. *ISA Transactions*, 2018, **73**: 154−164

55 Yu Y B, Woradechjumroen D, Yu D H. A review of fault detection and diagnosis methodologies on air-handling units. *Energy and Buildings*, 2014, **82**: 550−562

56 Okochi G S, Yao Y. A review of recent developments and technological advancements of variable-air-volume (VAV) air-conditioning systems. *Renewable and Sustainable Energy Reviews*, 2016, **59**: 784−817

57 Bruton K, Raftery P, Kennedy B, Keane M M, O′Sullivan D T J. Review of automated fault detection and diagnostic tools in air handling units. *Energy Efficiency*, 2014, **7**(2): 335−351

58 Ahmed M, Naser Mahmood A, Hu J K. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 2016, **60**: 19−31

59 Pimentel M A F, Clifton D A, Clifton L, Tarassenko L. A review of novelty detection. *Signal Processing*, 2014, **99**: 215−249

60 Gong Xue-Bing, Wang Ri-Xin, Xu Min-Qiang. Abnormality detection for flywheels based on data association analysis. *Acta Aeronautica et Astronautica Sinica*, 2015, **36**(3): 898−906
(龚学兵, 王日新, 徐敏强. 基于数据关联性分析的飞轮异常检测. 航空学报, 2015, **36**(3): 898−906)

61 Riasi A, Nourbakhsh A, Raises M. Energy dissipation in unsteady turbulent pipe flows caused by water hammer. *Computers and Fluids*, 2013, **73**: 124−133

62 中华人民共和国国家标准化管理委员会. 电气/电子/可编程电子安全相关系统的功能安全, GB-T 20438, 2007.

63 Oktem U G, Seider W D, Soroush M, Pariyani A. Improve process safety with near-miss analysis. *Chemical Engineering Progress*, 2013, **109**(5): 20−27

64 Weiss K A, Dulac N, Chiesi S, Daouk M, Zipkin D, Leveson N. Engineering spacecraft mission software using a model-based and safety-driven design methodology. *Journal of Aerospace Computing Information and Communication*, 2006, **3**(11): 562−586

65 Kadzhaev V, Barmin I, Denoyers J Y, Ragot A. Ensuring an acceptable reliability and safety level for a launch complex. *Acta Astronautica*, 2011, **68**(7−8): 1079−1085

66 van Staalduinen M A, Khan F, Gadag V, Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliability Engineering and System Safety*, 2017, **157**: 23−34

67 Wang S P, Zhang Z Z, Ning J M, Ren G X, Yan S H, Wan X C. Back propagation-artificial neural network model for prediction of the quality of tea shoots through selection of relevant near infrared spectral data via synergy interval partial least squares. *Analytical Letters*, 2013, **46**(1): 184−195

68 Meng H Y, Bianchi-Berthouze N, Deng Y D, Cheng J K, Cosmas J P. Time-delay neural network for continuous emotional dimension prediction from facial expression sequences. *IEEE Transactions on Cybernetics*, 2016, **46**(4): 916−929

69 Saeh I S, Wustafa M W. Performance evaluation of deregulated power system static security assessment using RBF-NN technique. *Jurnal Teknologi*, 2013, **64**(1): 109−116

70 Gholami M, Gharehpetian G B, Mohammadi M. Intelligent hierarchical structure of classifiers to assess static security of power system. *Journal of Intelligent and Fuzzy Systems*, 2015, **28**(6): 2875−2880

71 Arunraj N S, Mandal S, Maiti J. Modeling uncertainty in risk assessment: an integrated approach with fuzzy set theory and Monte Carlo simulation. *Accident Analysis and Prevention*, 2013, **55**(3): 242−255

72 Watson M D. System Exergy: system integrating physics of launch vehicles and spacecraft. *Journal of Spacecraft and Rockets*, 2018, **55**(2): 451−461

73 Kolaini A R, Tsuha W, Fernandez J P. Spacecraft vibration testing: benefits and potential issues. *Advances in Aircraft and Spacecraft Science*, 2018, **5**(2): 165−175

74 Luo Y Z, Liang L B, Wang H, Tang G J. Quantitative performance for spacecraft rendezvous trajectory safety. *Journal of Guidance, Control, and Dynamics*, 2011, **34**(4): 1264−1269

75 Cui Bao, Zhao Ji-Guang, Chen Jing-Peng, Zhang Yang. Research of the risk analysis system of space launch site. *Safety and Environmental Engineering*, 2014, **21**(4): 152−158
(崔豹, 赵继广, 陈景鹏, 张杨. 航天发射场风险分析系统研究. 安全与环境工程, 2014, **21**(4): 152−158)

76 Su Yong-Zhi, Chen Jing-Peng. Research on the reliability of spaceflight launch site′s facilities and equipment. *Journal of Equipment Academy*, 2014, **25**(2): 56−59
(苏永芝, 陈景鹏. 航天发射场地面设施设备可靠性工作研究. 装备学院学报, 2014, **25**(2): 56−59)

77 Gee K, Lawrence S L. Launch vehicle debris models and crew vehicle ascent abort risk. In: Proceedings Annual Reliability and Maintainability Symposium. Orlando, FL, USA: IEEE, 2013. 1−5

78 Chen W Y, Chen W Y, Wan B L, Sun G. Safety analysis and research on risk assessment model of spacecraft assembly. In: Proceedings of the 9th International Conference on Reliability, Maintainability and Safety. Guiyang, China: IEEE, 2011. 454−459

79 Collong S, Kouta R. Fault tree analysis of proton exchange membrane fuel cell system safety. *International Journal of Hydrogen Energy*, 2015, **40**(25): 8248−8260

80 Li Run-Qiu, Shi Shi-Liang, Wu Ai-You. EEMD-PSR-Elman modeling method for safety prediction and its application. *China Safety Science Journal*, 2015, **25**(6): 105−110
(李润求, 施式亮, 伍爱友. 安全预测的 EEMD-PSR-Elman 建模方法及应用. 中国安全科学学报, 2015, **25**(6): 105−110)

81 Falcoz A, Henry D, Zolghadri A. Robust fault diagnosis for atmospheric reentry vehicles: a case study. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2010, **40**(5): 886−899

82 Dulac N, Nancy L, David Z, et al. A framework for dynamic safety and risk management modeling in complex engineering systems. In: Proceedings of the 2005 Winter Simulation Conference. Orlando, USA, 2007.

83 Chen S J, Chen Q X, Xia Q, Zhong H W, Kang C Q. N-1 security assessment approach based on the steady-state security distance. *IET Generation, Transmission and Distribution*, 2015, **9**(15): 2419−2426

84 Yang X L, Sam Mannan M. An uncertainty and sensitivity analysis of dynamic operational risk assessment model: a case study. *Journal of Loss Prevention in the Process Industries*, 2010, **23**(2): 300−307

85 Nield G C, Sloan J, Gerlach D. Establishing recommended practices for commercial human space flight occupant safety. *New Space*, 2015, **3**(3): 147−153

86 Iverson D L, Martin R, Schwabacher M, Spirkovska L, Taylor W, Mackey R, et al. General purpose data-driven monitoring for space operations. *Journal of Aerospace Computing, Information, and Communication*, 2009, **9**(2): 26−44

87 Osipov V V, Muratov C B. Dynamic condensation blocking in cryogenic refueling. *Applied Physics Letters*, 2008, **93**(22): 224105

88 Filatyev A S, Buzuluk V, Yanova O, Ryabukha N, Petrov A. Advanced aviation technology for reusable launch vehicle improvement. *Acta Astronautica*, 2014, **100**: 11−21

89 Mueller G E, Kohrs D, Bailey R, Lai G. Autonomous safety and reliability features of the K-1 avionics system. *Acta Astronautica*, 2004, **54**(5): 363−370

90 Wu F W, Ji Z D, Yang C F. Construction monitoring of cable-stayed bridges based on gray prediction model. *Open Civil Engineering Journal*, 2015, **9**(1): 736−742

91 Ciancone M L, Johnson G W. Safety considerations in design of spacecraft hatches. In: Proceedings of the 4th IAASS Conference-Making Safety Matter. Huntsville, AL, USA: ADS, 2010.

92 Chen J, Kumar R. Stochastic failure prognosability of discrete event systems. *IEEE Transactions on Automatic Control*, 2015, **60**(6): 1570−1581

93 Palerm S, Bonhomme C, Petitot S, Chopinet J N. CNES Future preparation for liquid propulsion. In: Proceedings of the 51st AIAA/SAE/ASEE Joint Propulsion Conference. Orlando, USA: AIAA, 2013. 1−7

94 Yan H, Gong Q, Park C D, Ross I M, D′Souza C N. High-accuracy trajectory optimization for a trans-earth lunar mission. *Journal of Guidance, Control, and Dynamics*, 2011, **34**(4): 1219−1227

95 Li J Y, Gong S P, Wang X, Li J X. Launch window for manned Moon-to-Earth trajectories. *Aircraft Engineering and Aerospace Technology*, 2012, **84**(5): 344−356

96 Fazelzadeh S A, Varzandian G A. Minimum-time Earth-Moon and Moon-Earth orbital maneuvers using time-domain finite element method. *Acta Astronautica*, 2010, **66**(3−4): 528−538

97 Palerm S, Bonhomme C, Guelou Y, Chopinet J N, Danous P. The future of cryogenic propulsion. *Acta Astronautica*, 2015, **112**: 166−173

98 Jia Chi-Qian, Feng Dong-Qin. Industrial control system devices security assessment with multi-objective decision. *Acta Automatica Sinica*, 2016, **42**(5): 706−714
(贾驰千, 冯冬芹. 基于多目标决策的工控系统设备安全评估方法研究. 自动化学报, 2016, **42**(5): 706−714)

99 Wurzelbacher S J, Bertke S J, Lampl M P, Bushnell P T, Meyers A R, Robins D C, et al. The effectiveness of insurer-supported safety and health engineering controls in reducing workers' compensation claims and costs. *American Journal of Industrial Medicine*, 2014, **57**(12): 1398−1412

100 Long Le-Hao, Wang Xiao-Jun, Guo Lin-Li. The present situation and prospect of China′s space-entering capacity. *Engineering Science*, 2006, **8**(11): 25−28, 32
(龙乐豪, 王小军, 果琳丽. 中国进入空间能力的现状与展望. 中国工程科学, 2006, **8**(11): 25−28, 32)

101 Osipov V V, Daigle M J, Muratov C B, Foygel M, Smelyanskiy V, Watson M D. Dynamical model of rocket propellant loading with liquid hydrogen. *Journal of Spacecraft and Rockets*, 2011, **48**(6): 987−998

102 Bao Wei-Min. Present situation and development tendency of aerospace control techniques. *Acta Automatica Sinica*, 2013, **39**(6): 697−702
(包为民. 航天飞行器控制技术研究现状与发展趋势. 自动化学报, 2013, **39**(6): 697−702)

103 Bandyopadhyay A, Majumdar A. Network flow simulation of fluid transients in rocket propulsion systems. *Journal of Propulsion and Power*, 2014, **30**(6): 1646−1653

104 Mazzetti A, Merotto L, Pinarello G. Paraffin-based hybrid rocket engines applications: a review and a market perspective. *Acta Astronautica*, 2016, **126**: 286−297

105 Hassan R, Crossley W. Spacecraft reliability-based design optimization under uncertainty including discrete variables. *Journal of Spacecraft and Rockets*, 2008, **45**(2): 394−405

106 Launay S, Sartre V, Bonjour J. Analytical model for characterization of loop heat pipes. *Journal of Thermophysics and Heat Transfer*, 2008, **22**(4): 623−631

107 Liu Qiang, Qin S J. Perspectives on big data modeling of process industries. *Acta Automatica Sinica*, 2016, **42**(2): 161−171
(刘强, 秦泗钊. 过程工业大数据建模研究展望. 自动化学报, 2016, **42**(2): 161−171)

108 Faure J M, Oloveira J M, Chintalapati S, Gutierrez H M, Kirk D R. Effect of isogrid-type obstructions on thermal stratification in upper-stage rocket propellant tanks. *Journal of Spacecraft and Rockets*, 2014, **51**(5): 1587−1602

109 Chen Jun, Zhao Ji-Guang, Xia Lu-Rui. Simulation analysis for filter of liquid hydrogen filling equipment in launch center. *Machine Tool and Hydraulics*, 2012, **40**(7): 149−151, 155
(陈俊, 赵继广, 夏鲁瑞. 发射场液氢加注管路过滤器仿真分析研究. 机床与液压, 2012, **40**(7): 149−151, 155)

110 Su Yong-Zhi, Liu Dang-Hui, Zhang Zhen-Wei. Optimization technology of 3D model for space launch site based on MultiGen Creator. *Journal of System Simulation*, 2013, **25**(8): 1816−1819
(苏永芝, 刘党辉, 张振伟. 基于 MultiGen Creator 的航天发射场三维模型优化技术. 系统仿真学报, 2013, **25**(8): 1816−1819)

111 Chen Shi-Chao, Huang Fu-You, Ding Peng-Fei, Tang Qiang, He Yi. Simulation research of the liquid oxygen filling system. *Cryogenics*, 2016, **44**(6): 10−13
(陈世超, 黄福友, 丁鹏飞, 唐强, 何烨. 液氧加注系统仿真研究. 低温与超导, 2016, **44**(6): 10−13)

112 Gao Zhi-Yong, Huo Wei-Han, Gao Jian-Ming, Jiang Hong-Quan. Diffusion mapping and abnormal recognition algorithm for mass data of chemical system. *Computer Integrated Manufacturing Systems*, 2014, **20**(12): 3091−3096
(高智勇, 霍伟汉, 高建民, 姜洪权. 化工系统海量数据的扩散映射和异常辨识. 计算机集成制造系统, 2014, **20**(12): 3091−3096)

113 Chabridon V, Balesdent M, Bourinet J M, Morio J, Gayton N. Evaluation of failure probability under parameter epistemic uncertainty: application to aerospace system reliability assessment. *Aerospace Science and Technology*, 2017, **69**: 526−537

114 Yang Yong. Study on roadmap of Chinese reusable launch vehicle. *Missiles and Space Vehicles*, 2006, (4): 1−4
(杨勇. 我国重复使用运载器发展思路探讨. 导弹与航天运载技术, 2006, (4): 1−4)

115 Cong H, Yang Y L, Jiang P C, Feng F Z, Zhang H X, Li Y K, et al. Optimization strategy for air handling units in spacecraft launching site. *Applied Thermal Engineering*, 2016, **109**: 678−684

116 Yang Y L, Jiang P C, Cong H, Feng F Z, Zhang H X. Research on the route optimization for fresh air processing of air handling unit in spacecraft launching site. *Applied Thermal Engineering*, 2015, **86**: 292−300

117 Nagano S. Space systems verification program and management process. *Systems Engineering*, 2008, **11**(1): 27−38

118 Hedayat A, Cartagena W, Majumdar A K, LeClair A C. Modeling and analysis of chill and fill processes for the cryogenic storage and transfer engineering development unit tank. *Cryogenics*, 2016, **74**: 106−112

119 Zio E. Reliability engineering: old problems and new challenges. *Reliability Engineering and System Safety*, 2009, **94**(2): 125−141

120 Daigle M, Goebel K. Model-based prognostics under limited sensing. In: Proceedings of the 2010 IEEE Aerospace Conference. Big Sky, MT, USA: IEEE, 2010. 1−12

121 Čepin M. Comparison of methods for dependency determination between human failure events within human reliability analysis. In: Proceedings of the International Conference Nuclear Energy for New Europe. Portorož, Slovenia, 2007. 302.1−302.8

122 French S, Bedford T, Pollard S J T, Soane E. Human reliability analysis: a critique and review for managers. *Safety Science*, 2011, **49**(6): 753−763

123 Dong Xue-Jun, Chen Ying-Wu. Method of human reliability analysis based on CSICF. *Systems Engineering- Theory and Practice*, 2012, **32**(9): 2087−2096
(董学军, 陈英武. 基于补偿和不可替代因素合成的人因可靠性分析方法. 系统工程理论与实践, 2012, **32**(9): 2087−2096)

124 Su X Y, Mahadevan S, Xu P D, Deng Y. Inclusion of task dependence in human reliability analysis. *Reliability Engineering and System Safety*, 2014, **128**(4): 41−55

125 Collopy P. Aerospace system value models: a survey and observations. In: Proceedings of AIAA SPACE 2009 Conference and Exposition. Pasadena, California, USA: AIAA, 2009.

126 Zhi Wen-Shu, Ma Xin-Hui, Zhao Ji-Guang, Chen Jing-Peng. Risk assessment of low temperature filling system based on AHP method. *Cryogenics*, 2013, (6): 31−35
(智文书, 马昕晖, 赵继广, 陈景鹏. 基于层次分析法的低温加注系统安全风险评估. 低温工程, 2013, (6): 31−35)

127 Geng F, Herd R, Tien A, Saleh J H. Beyond cost tools: spacecraft net present value and the hosted payload paradigm. In: Proceedings of the 2015 IEEE Aerospace Conference. Big Sky, MT, USA: IEEE, 2015. 1−19

128 Doherty M P, Gaby J D, Salerno L J, Sutherlin S G. Cryogenic fluid management technology for moon and mars missions. In: Proceedings of AIAA SPACE 2009 Conference and Exposition. Pasadena, USA: AIAA, 2010.

129 Ma Xin-Hui, Chen Jing-Peng, Xu La-Ping, Zhi Wen-Shu, Sun Jian. Risk assessment research of geysering phenomenon in cryogenic liquid hydrogen loading system. *Cryogenics*, 2013, (4): 54−59
(马昕晖, 陈景鹏, 徐腊萍, 智文书, 孙建. 低温液氢加注系统间歇泉现象风险评估研究. 低温工程, 2013, (4): 54−59)

130 Snelgrove K B, Saleh J H. Toward a new spacecraft optimal design lifetime? Impact of marginal cost of durability and reduced launch price. *Acta Astronautica*, 2016, **127**: 271−282

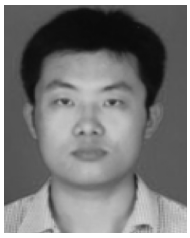
131 Saffers J B, Molkov V V. Hydrogen safety engineering framework and elementary design safety tools. *International Journal of Hydrogen Energy*, 2014, **39**(11): 6268−6285

132 Flachbart R H, Hedayat A, Holt K A, Sims J, Johnson E F, Hastings L J, et al. Large-Scale Liquid Hydrogen Tank Rapid Chill and Fill Testing for the Advanced Shuttle Upper Stage Concept, Technical Report NASA/TP-2013-217482, NASA, Washington, D. C., USA, 2013.

133 Xie Fu-Shou, Lei Gang, Wang Lei, Xing Ke-Wei, Li Yan-Zhong. Performance advantages and application prospects of subcooled cryogenic propellants. *Journal of Xi'an Jiaotong University*, 2015, **49**(5): 16−23, 127
(谢福寿, 雷刚, 王磊, 邢科伟, 厉彦忠. 过冷低温推进剂的性能优势及其应用前景. 西安交通大学学报, 2015, **49**(5): 16−23, 127)

柴 毅 重庆大学自动化学院教授. 2001 年获得重庆大学博士学位. 主要研究方向为信息融合, 故障诊断, 智能控制系统. 本文通信作者.
E-mail: chaiyi@cqu.edu.cn
(**CHAI Yi** Professor at the College of Automation, Chongqing University. He received his Ph. D. degree from Chongqing University in 2001. His research interest covers information fusion, fault diagnosis, intelligent control system. Corresponding author of this paper.)

毛万标 西昌卫星发射中心高级工程师. 主要研究方向为故障诊断, 发射场安全性分析评估.
E-mail: rocketmwb@126.com
(**MAO Wan-Biao** Senior engineer of Xichang Satellite Launch Center. His research interest covers fault diagnosis, launch site safety analysis and assessment.)

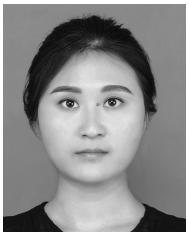


任 浩 重庆大学自动化学院博士研究生. 主要研究方向为智能系统, 故障诊断和深度学习.
E-mail: renhao@cqu.edu.cn
(**REN Hao** Ph. D. candidate at the College of Automation, Chongqing University. His research interest covers intelligent control system, fault diagnosis, and deep learning.)

屈剑锋 重庆大学自动化学院副教授. 2009 年获得重庆大学博士学位. 主要研究方向为故障诊断, 信号分析与处理.
E-mail: qujianfeng@cqu.edu.cn
(**QU Jian-Feng** Associate professor at the College of Automation, Chongqing University. He received his Ph. D. degree from Chongqing University in 2009. His research interest covers fault diagnosis, signal analysis and processing.)

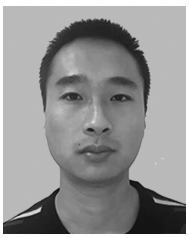
尹宏鹏 重庆大学自动化学院教授. 2009 年获得重庆大学博士学位. 主要研究方向为模式识别与智能系统, 故障诊断与健康管理.
E-mail: yinhongpeng@gmail.com
(**YIN Hong-Peng** Professor at the College of Automation, Chongqing University. He received his Ph. D. degree from Chongqing University in 2009. His research interest covers pattern recognition and intelligent systems, fault diagnosis and health management.)

杨志敏 重庆大学自动化学院博士研究生. 主要研究方向为故障诊断和容错控制. E-mail: zmyoung@yeah.net
(**YANG Zhi-Min** Ph. D. candidate at the College of Automation, Chongqing University. His research interest covers fault diagnosis and fault tolerance control.)



冯 莉 重庆交通大学交通运输学院讲师. 2017 年获得重庆大学博士学位. 主要研究方向为故障诊断和故障估计.
E-mail: fengli_cqu@126.com
(**FENG Li** Lecturer at the College of Traffic and Transportation, Chongqing Jiaotong University. She received her Ph. D. degree from Chongqing University in 2017. Her research interest covers fault diagnosis and fault estimation.)

张邦双 西昌卫星发射中心高级工程师. 主要研究方向为设备设施可靠性, 装备环境适应性.
E-mail: zhangbangshuang@163.com
(**ZHANG Bang-Shuang** Senior engineer at Xichang Satellite Launch Center. His research interest covers equipment facility reliability and equipment environment adaptability.)



叶 欣 西昌卫星发射中心工程师. 主要研究方向为低温推进剂管道输送, 发射场可靠性分析评估, 数字图像处理.
E-mail: nanjingyexin@163.com
(**YE Xin** Engineer at Xichang Satellite Launch Center. His research interest covers low temperature propellant pipeline transportation, reliability analysis and evaluation of launch site, and digital image processing.)