基于 PRA 的组合体航天器风险评估模型

周昊澄,杨 宏,夏侨丽
(中国空间技术研究院载人航天总体部,北京 100094)

摘 要:针对组合体航天器高可靠性、小子样的特性,以组合体航天器控推系统为例对多舱融合性设计方案建立了基于 PRA(Probabilistic Risk Assessment,概率风险评估)的风险评估模型。通过对比使用融合性设计和未使用融合性设计两种方案的故障树和相对比差,以验证融合性设计对系统可靠性的贡献为目标,从定性和定量的角度验证了融合性设计可以大幅降低组合体航天器控推系统重大风险的发生概率。通过分析重大风险的重要度权重,得到了组合体航天器控推系统重大风险的重要度排序,从风险的角度为决策者提供了应用融合性设计的建议。

关键词:组合体航天器;概率风险评估;故障树;融合性设计
中图分类号:V475 **文献标识码**:A **文章编号**:1672 - 9374(2019)01 - 0059 - 07

Risk assessment model of combined spacecraft based on PRA

ZHOU Haocheng, YANG Hong, XIA Qiaoli
(Institute of Manned Space Engineering, China Academy of Space Technology, Beijing 100094, China)

Abstract: For the characteristics of high reliability and small sample of combined spacecraft, this paper takes the control and propulsion system of combined spacecraft as an example to establish a PRA-based risk assessment model for multi-cabin integrated design scheme. By comparing the fault tree and the relative difference between the two schemes using and not using integrated design, in order to verify the contribution of integrated design to the reliability of the system, it is verified qualitatively and quantitatively that integrated design can significantly reduce the probability of major risks of the combined spacecraft thrust control system. By analyzing the importance weight of the major risk, the importance ranking of the major risk of the combined spacecraft thrust control system is obtained. From the risk point of view, some suggestions for decision makers to apply the integrated design are also provided.

Keywords: combined spacecraft; PRA; fault tree; integrated design

0 引言

我国空间站的建设是载人航天工程三步走的第三步,是我国从航天大国迈向航天强国的重要标志。空间站是典型的组合体航天器,本文将借鉴空间站的设计方法构建具有载人航天特色的组合体航天器风险评估模型。

组合体航天器由多舱段在轨组装建造而成,本

收稿日期:2018-11-29;**修回日期**:2018-12-30
基金项目:国家自然科学青年基金(11802015)
作者简介:周昊澄(1989—),男,博士,研究领域为航天器总体设计

文构建的组合体航天器由核心舱、实验舱、载人飞船和货运飞船 4 个飞行器组成,如图 1 所示。核心舱主要承担组合体的管理和控制功能,是组合体航天器的大脑。实验舱主要承担舱内和舱外空间科学实验和技术实验,根据实际需求组合体航天器可以允许一个或多个实验舱同时存在。载人飞船和货运飞船也称天地往返运输器,是接送航天员和必要物资往返组合体航天器的运输器。

国际空间站(ISS)也是典型的组合体航天器,在组合体形态下由美国段进行控制,各舱段间仅在变轨期间有简单的协调工作能力,即俄罗斯段和货运飞船在组合体变轨时可以根据美国段的指令开关轨控发动机完成组合体变轨。此类设计属于最初级的融合性设计,长期在轨运营期间如果美国段出现故障,整个组合体则失去正常运营能力。

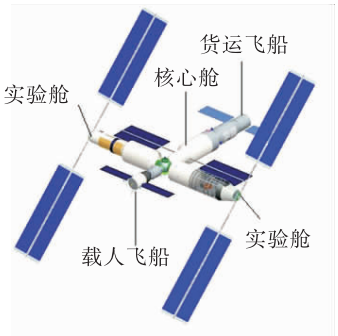

图 1 组合体航天器结构示意图

Fig. 1 Structural sketch of combined spacecraft

组合体航天器各舱段都应具备独立飞行 3 年以上和组合体运营 10 年以上的能力。如果可以合理地利用各舱段的独立飞行能力,在核心舱对组合体航天器失去控制能力时由其他舱段进行控制将大幅提升组合体航天器长期在轨运营的可靠性。本研究将对组合体航天器双舱控推系统建立 PRA(概率风险评估)模型,对比组合体航天器应用多舱融合性设计和未应用多舱融合性设计可靠性的不同。

1 PRA 建模意义

PRA 是多种安全性分析技术的综合集成,是一种全面的、结构化的、逻辑的分析方法,是对复杂系统进行风险评估的一种重要工具[1],在航空航天、核电及石化等众多领域得到了广泛应用。早在 1960 年的“阿波罗登月计划”中,NASA 就曾用定量分析方法对航天系统成功完成飞行任务的概率进行了计算[2],后续在航天飞机、国际空间站及探月飞船等项目中也均采用 PRA 进行了定量风险评估[3-8]。2002 年,NASA 公布了“概率风险评估过程指南”,该指南总结了 NASA 历年来的概率风险评估经验,综合集成了 NASA 在航天项目中的概率风险评估方法,具有重要的理论和应用价值[9-10]。NASA 于 2002 年公布了 V1.1 版本的“航天应用的故障树手册”[11],标志着 PRA 模型正式成为航天系统可靠性分析的标准规范之一。

应用 PRA 可以帮助设计师更加直观、深入地了解复杂系统并对其风险进行评估。PRA 方法不仅考虑后果事件的严重度,还会给出其发生可能性的大小[12]。PRA 技术可以基于事故场景有效识别系统设计当中存在的薄弱环节及未来长期运营可能发生的潜在风险,并对其进行定性和定量分析,区分出不同影响因素对风险影响的重要程度排序,为系统决策者提供真实可靠的风险信息。

2 航天器风险评估故障建模与应用

2.1 确定目标及后果状态

确定目标及后果状态步骤:

1)通过主逻辑图识别初因事件;

2)使用 PRA 方法对比使用多舱融合性设计和未使用多舱融合性设计系统的风险;

3)分析评估结果,提出开展融合性设计的应用建议。

按照《航天器产品故障模式及影响分析指南》中关于故障严酷度等级的规定,结合控制与推进系统功能特点,定义故障严重等级大致分为 4 个等级[13-14],如表 1 所示。本文只考虑Ⅰ类和Ⅱ类故障。

2.2 通过主逻辑图识别初因事件

主逻辑图(MLD)是一种自上而下分层次梳理的树状图,可以分为顶事件、中间事件和底事件。顶事件是最不希望发生的事件,对于大系统而言一般为机毁人亡或航天员伤亡,中间事件一般为具有独立功能的子系统,底事件就是建立主逻辑图的主要研究对象初因事件。本文针对的是组合体航天器的控推系统,对于控推系统而言最不希望发生的事件是控推系统故障。图 2 为组合体航天器控推系统主逻辑图。

表 1　故障等级定义

Tab. 1　Definition of fault level

等级	程度	定义
Ⅰ	灾难的	造成航天员伤亡或整个组合体航天器丧失,包括: 1)核心舱独立飞行时,失去使用发动机进行姿控的能力 2)组合体航天器失去使用发动机进行姿控的能力
Ⅱ	严重的	造成航天员严重受伤或核心舱严重受损,任务不能完成,包括: 1)核心舱独立飞行时,失去自身轨控功能,但具备发动机姿控功能 2)组合体航天器失去自身轨控功能,但具备发动机姿控功能 3)组合体航天器短时失去发动机姿控功能,但可以通过切备机使用 4)组合体航天器短时失去发动机轨控功能,但可以通过切备机使用
Ⅲ	轻度的	航天员轻度伤害,系统轻度损坏或任务部分失败,包括: 1)控制系统的设备存在故障,冗余度下降 2)控推系统设备地面发指令切换冷备设备前,系统存在控制问题 3)推进系统的姿轨控发动机存在故障,可用配置减少,冗余度下降
Ⅳ	轻微的	轻于 III 类的人员伤害或轻于Ⅲ类的系统损坏,不影响任务完成,包括: 1)平台设备没有受损或受损后仍能执行正常功能 2)航天员受轻微伤害,不需治疗即可恢复

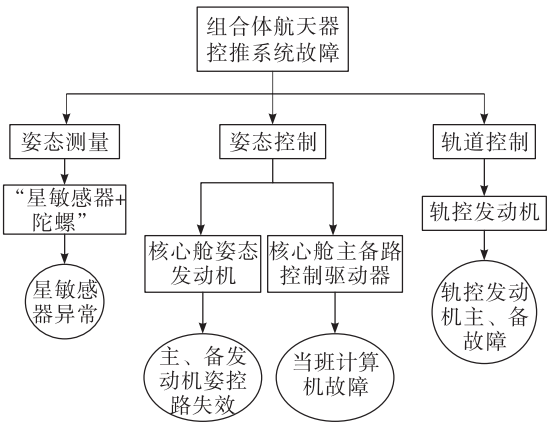

图 2　组合体航天器控推系统主逻辑图

Fig. 2　MLD of control and propulsion system for combined spacecraft

由图 2 可以看出,核心舱单飞状态主事件是控推系统,中间事件是姿态测量、姿态控制和轨道控制。导致中间事件发生的事件称为底事件,也称初因事件。当顶事件为Ⅰ,Ⅱ类故障时,其对应的初因事件是导致Ⅰ,Ⅱ类故障发生的底事件,如表 2 所示。

初因事件的识别是事件链建模的基础,如果不考虑初因事件便不能充分理解系统扰动和后果状态及基本事件之间的关系。

表 2　初因事件列表

Tab. 2　Initial event list

序号	描述
1	核心舱“星敏感器 + 陀螺”姿态测量异常
2	核心舱主、备路姿控发动机工作提供姿控力矩功能异常
3	核心舱主、备路控制驱动器内部当班计算机故障
4	核心舱轨控发动机主、备故障

2.3　构建组合体故障树

PRA 分析首先要定义系统的分析范围,组合体航天器各舱段都具有独立飞行能力并配有一整套完整的控推系统,故对控推系统进行风险评估是极具代表性的。从表 1 可以看出,Ⅲ,Ⅳ类故障对系统的危害极小,而且组合体航天器为了满足长期在轨运营的需求还具备维修性的特点,大多数Ⅲ,Ⅳ类故障也都可以通过维修性解决,因此风险评估的重点应当放到Ⅰ,Ⅱ类故障上。即本次风险评估模型

的范围是:组合体航天器控推系统Ⅰ,Ⅱ类故障。

本次分析在识别底事件时用到了主逻辑图,根据定义范围自上而下对控推系统所有的中间事件和底事件进行了筛选,将仅对航天员产生轻度伤害及系统轻度损坏或任务部分失败的故障筛除,保留了可以导致机毁人亡、造成航天员严重受伤或核心舱严重受损、任务不能完成的故障进行分析,如表 2 所示。

PRA 采用事件树和故障树相结合的分析方法[15]。分别建立应用融合性设计和未应用融合性设计的事件树和故障树对比融合性设计对系统可靠性的贡献。

对系统建造故障树时,首先要把系统的故障或失效状态作为故障树的顶事件,然后找出导致顶事件发生的中间事件和导致中间事件发生的所有可能的直接因素,即所有的故障模式。故障树通常用来建立事件的层次,可以更清晰地展示出初因事件导致系统故障的逻辑关系,并提供更多的细节以帮助量化。由于归纳过程和演示过程的互补性,事件树和故障树经常一起使用,表示从初因事件到故障状态的系统响应。二者结合使用比只使用其中一种更能够完全、精确、清晰地构造和记录事件链[16-17]。图 3 为应用融合性设计的故障树。

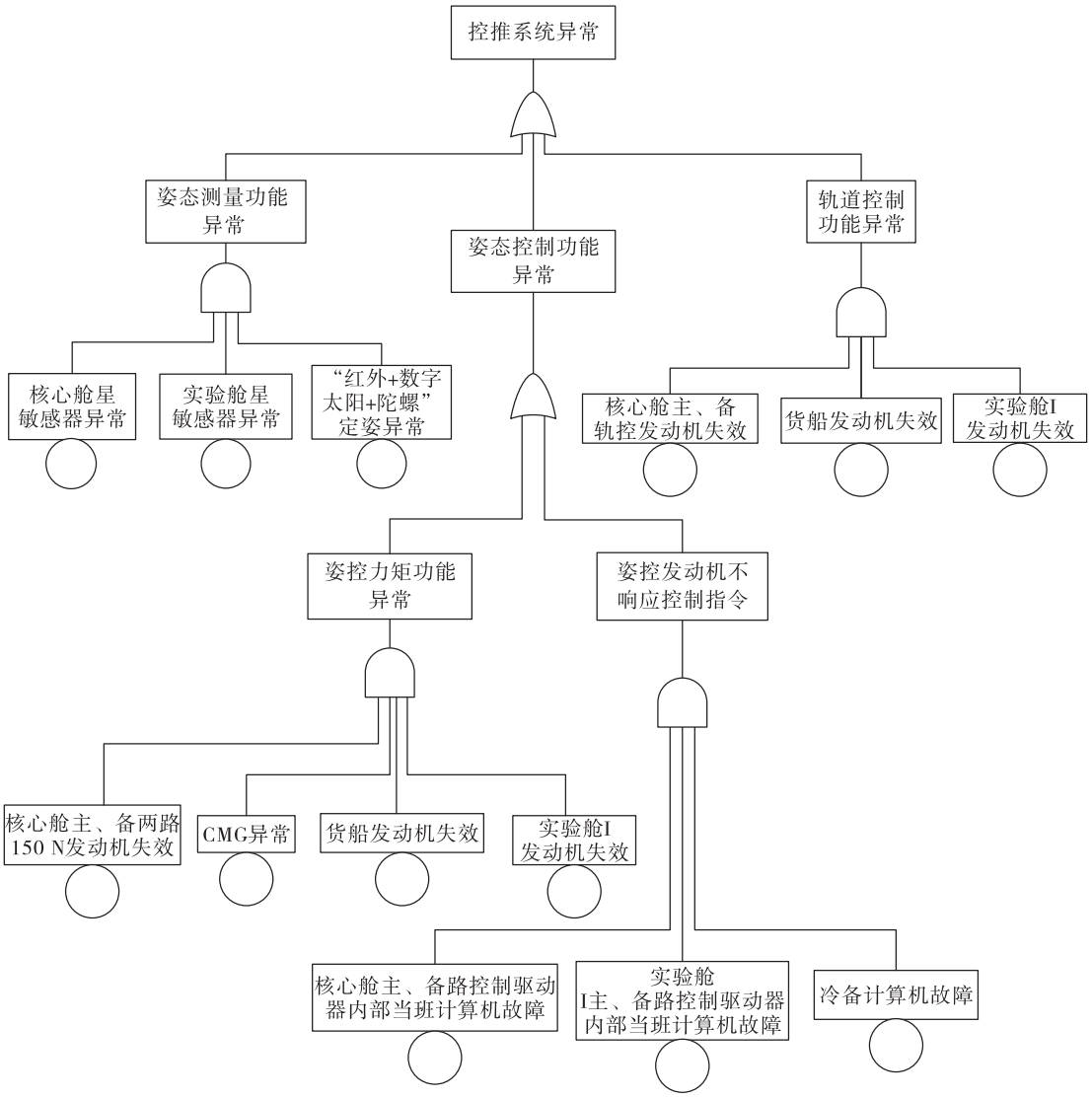

图 3 应用融合性设计的故障树

Fig. 3 Fault tree based on integrated design

姿态测量功能的Ⅰ,Ⅱ类故障有一个:核心舱“星敏感器 + 陀螺”姿态测量异常。组合体航天器星敏感器姿态测量需星敏感器正常工作,核心舱和实验舱星敏设备备份。当星敏无法满足使用条件时,组合体航天器无法按照两舱长期飞行姿态 - 惯性飞行姿态在轨飞行,需转入三轴稳定对地定向姿态在轨飞行,推进剂消耗增加。

姿态控制功能的Ⅰ,Ⅱ类故障有两个:姿控发动机工作提供姿控力矩功能异常和姿控发动机不响应控制指令。核心舱为保证姿控力矩功能的可靠性,其姿控发动机采取主、备份设计。当货运飞船停靠时可以优先选用货运飞船发动机对组合体进行控制,无货运飞船停靠时优先选用实验舱发动机进行控制。

为保证姿态控制发动机可以响应控制指令,本模型在核心舱和实验舱都采用双机备份的情况下,在核心舱又添加了一台冷备计算机。如果核心舱主、备路控制驱动器内部当班计算机均出现故障,则启用实验舱的控制驱动器接替核心舱工作,此时可以保证组合体姿控发动机及时响应控制指令。如核心舱和实验舱控制驱动器主、备份均出现故障,则启用核心舱冷备份计算机执行任务,此时姿控功能冗余度下降,需要进行单机维修并在必要时将元器件降额使用。

轨道控制功能的Ⅰ,Ⅱ类故障有一个:核心舱轨控发动机主、备故障。核心舱轨控发动机为确保轨道控制功能正常,轨控发动机采取主、备份设计。当核心舱主、备两路轨控发动机均失效,在货船停靠时优先使用货船轨控发动机,在货船未停靠且实验舱剩余足够推进剂时选用实验舱轨控发动机。图 4 为未应用融合性设计的故障树。

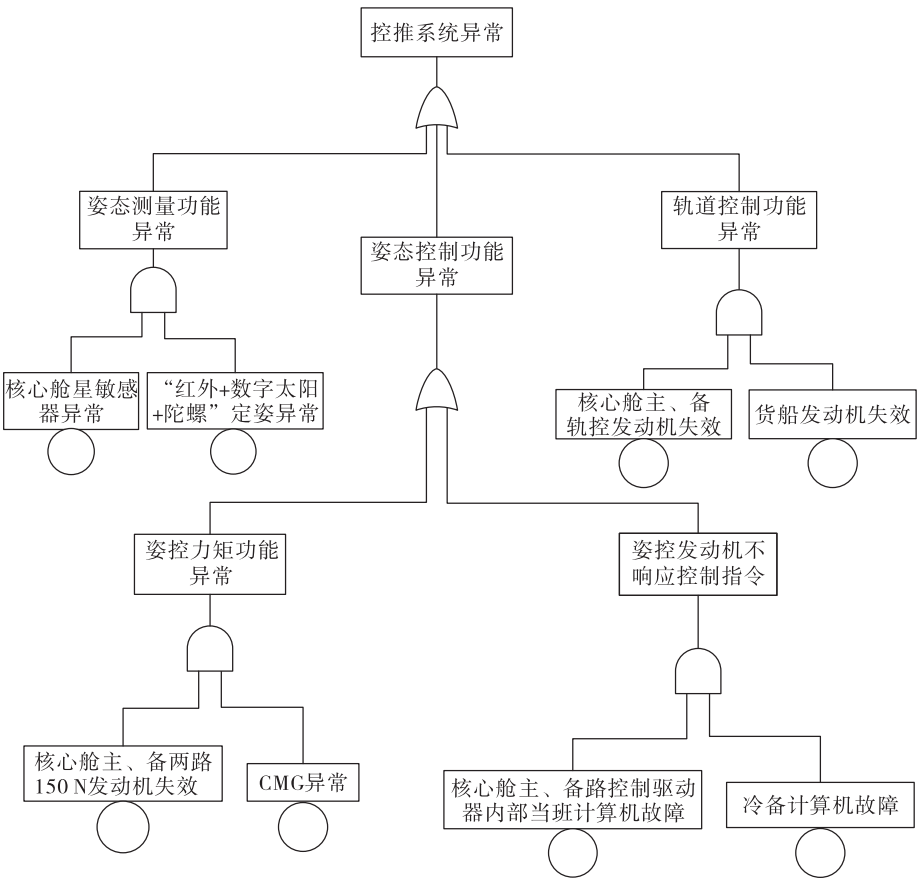

图 4　未应用融合性设计的故障树

Fig. 4　Fault tree without integrated design

从图 3 和图 4 可以清晰地看出应用融合性设计和未应用融合性设计的差别。未应用融合性设计

的组合体航天器在发生故障时只能采取启动冷备份或者降级使用的应对策略;而应用了融合性设计的组合体航天器则可以通过实验舱和货运飞船接替核心舱控制的方法,在不影响组合体航天器正常工作的情况下应对突发故障,大大提升了组合体航天器的可靠性,并且为航天员和地面工作人员对核心舱进行维修提供了充足时间。

3 风险评估结果分析

本研究的重点是对比组合体航天器应用融合性设计和未应用融合性设计两种方案在可靠性上的差别。设 R_1 为未应用融合性设计的风险,R_2 为应用融合性设计的风险,δR_{21} 为相对风险率,则 $\delta R_{21} = (R_2 - R_1)/R_2$。评价指标的权重作为综合评价的关键,其权重的取值将直接影响评估结果[18]。设组合体航天器控推系统异常为比对准则,第一层准则定义出系统的主要功能,第二层准则按照故障树将第一层准则细分。通过权重计算对控推系统功能进行重要度排序依次为:姿控力矩功能,轨道控制功能,姿控发动机指令控制功能,姿态测量功能。表 3 为重要性权重示例。

表 3 重要性权重示例

Tab. 3 Example of importance weight

目标层	权重	第一层	权重	第二层
控推系统异常	0.166	姿态测量功能	0.599	核心舱星敏感器(C_{11})
			0.275	实验舱星敏感器(C_{12})
			0.126	“红外 + 数字太阳 + 陀螺”定姿(C_{13})
	0.333	姿控力矩功能	0.528	核心舱主、备路姿控发动机(C_{21})
			0.181	CMG 功能(C_{22})
			0.169	货船姿控发动机(C_{23})
			0.122	实验舱姿控发动机(C_{24})
	0.249	姿控发动机指令控制功能	0.528	核心舱主、备路当班计算机(C_{31})
			0.171	实验舱主、备路当班计算机(C_{32})
			0.301	核心舱冷备计算机(C_{33})
	0.252	轨道控制功能	0.645	核心舱主、备路轨控发动机(C_{41})
			0.206	货船轨控发动机(C_{42})
			0.149	实验舱轨控发动机(C_{43})

设未应用融合性设计且所有底事件均发生,即:C_{11},C_{13},C_{21},C_{22},C_{31},C_{33},C_{41},C_{42}同时发生为“设计 1”。设应用融合性设计且所有底事件均发生为“设计 2”。设计 1 与设计 2 具有相同的功能设计,设计 1 为参考设计方案,其风险贡献量的比率设为 1。表 4 为参考设计与可选设计方案之间的相对差比。相对差比强调设计差别,其计算式为 $\frac{C_i^{(2)} - C_i^{(1)}}{C_i^{(1)}} - 1$,式中 $C_i^{(1)}$ 和 $C_i^{(2)}$ 分别为设计方案 1 和设计方案 2 的影响因素的影响量。

表 4 设计方案的相对差比

Tab. 4 Relative difference ratio of design scheme

第一层	设计 1	设计 2
姿态测量功能	0	-0.903
姿控力矩功能	0	-0.974
姿控发动机指令控制功能	0	-0.993
轨道控制功能	0	-0.896

从表 4 可以看出,组合体航天器控推系统的 4 种Ⅰ类和Ⅱ类故障通过融合性设计改进后其相对差比均为负。所得相对风险评估结果为:控推系统Ⅰ,Ⅱ类故障发生概率相对减少 21.1%,融合性设

计使组合体航天器控推系统的可靠性明显提升。再结合表 3 中第一层和第二层准则的权重,充分利用权重蕴含的潜在信息[19],给出系统应用融合性设计建议:建议控推系统大范围应用融合性设计,如果不能大范围应用则应该以姿控力矩功能、轨道控制功能、姿控发动机指令控制功能和姿态测量功能的顺序应用。

4　结束语

为验证组合体航天器融合性设计对可靠性的贡献,选取了组合体航天器的控推系统为研究对象,以Ⅰ,Ⅱ类故障作为底事件,分别对应用融合性设计和未应用融合性设计的系统构建故障树模型。然后,根据组合体航天器的特性分析了控推系统的权重和两种设计方案的相对差比,采用相对风险评估方法,得到应用融合性设计控推系统Ⅰ,Ⅱ类故障发生概率降低 21.1% 和控推系统各功能的重要度排序。从风险的角度建议决策者全系统或根据重要度排序逐步应用融合性设计。所采取的两种设计方案相比对的分析方法在工作量与完备性之间有较好的平衡,未来的工作中应进一步完善评估方法并将其通用化。

参考文献:

[1] 任培,周经纶,郑龙. 基于 PRA 方法风险评估系统的设计与研究[J]. 计算机应用研究, 2007,24(6):91-93.

[2] PAT-COMELL E, DILLON R. Probabilistic risk analysis for the NASA space shuttle: a brief history and current work [J]. Reliability Engineering and System Safety, 2001, 74: 345-352.

[3] MAGGIO G. Space shuttle probabilistic risk assessment: methodology & application [C]//Annual Reliability and Maintainability Symposium. Las Vegas: IEEE,1996.

[4] HAMLIN T L, CANGA M A, BOYER R L, et al. 2009 space shuttle probabilistic risk assessment overview[C]// 10th International Probabilistic Safety Assessment and Management Conference. Seattle:ESRA,2010.

[5] BIGLER M, CANGA M A, DUNCAN G. Extravehicular activity probabilistic risk assessment overview for thermal protection system repair on the Hubble space telescope servicing mission [C]// 10th International Probabilistic Safety Assessment and Management Conference. Seattle: ESRA,2010.

[6] SMITH C A. Probabilistic risk assessment for the international space station [C]//Joint ESA-NASA Space-flight Safety Conference. New York: ESA-NASA, 2002.

[7] PERERA J, HOLSOMBACK J. Use of probabilistic risk assessments for the space station program conference [C]// 2004 IEEE Aerospace Conference. Gaithersburg: IEEE, 2004.

[8] PRASSIONS P G, STAMATELATOS M G, YOUNG J, et al. Constellation probabilistic risk assessment (PRA): design consideration for the CEV [R]. Washington: NASA, 2006.

[9] STAMATELATOS M. Probabilistic risk assessment procedures guide for NASA managers and practitioner [R]. Washington: NASA, 2002.

[10] 李健,栾家辉,刘春雷. 我国空间站过程量化风险评估工作探讨[J]. 载人航天,2014,20(3):249-255.

[11] MICHAEL S, WILLIAM V, DUGAN J B, et a1. Fault tree handbook with aerospace applications(Version 1.1) [R]. Washington: NASA, 2002.

[12] 节永师,王伟,王功,等. 载人航天概率风险评价工程事件及其在空间应用中的前景分析[J]. 载人航天,2017,23(1):98-113.

[13] 刘瑛,李敏强,陈富赞. 飞行器机动动作风险定量评估模型[J]. 系统工程与电子技术,2014,36(3):469-475.

[14] 王一枫,汤伟,刘路登,等. 电网运营风险评估与定级体系的构建及应用[J]. 电力系统自动化,2015,39(8):141-148.

[15] 丁明,肖瑶,张晶晶,等. 基于事故链及动态故障树的电网连锁故障风险评估模型[J]. 中国电机工程学报,2015,35(4):821-829.

[16] 周海京,遇今,郑恒. 概率风险评价技术及应用[J]. 质量与可靠性,2007(6):6-8.

[17] 遇今,张海龙. 航天器研制风险管理过程及实施[J]. 质量与可靠性,2011(1):20-26.

[18] 沈阳武,彭晓涛,施通勤,等. 基于最优组合权重的电能质量灰色综合评价方法[J]. 电力系统自动化,2015,36(10):67-73.

[19] 张春晓,严爱军,王普. 一种改进的案例推理分类方法研究[J]. 自动化学报,2014,40(9):2015-2021.

(编辑:马　杰)