载人飞船安全性评估方法研究

宫　颖　程　卓
（中国空间技术研究院总体部）

摘　要　安全性评估是安全性验证的一种形式，是在产品转阶段或出厂前对产品安全性水平做出量化的综合评估，并为下一步的管理决策提供依据。结合我国载人飞船可靠性安全性工作，研究提出载人飞船安全性定量评估方法。介绍并分析近几年发射的载人飞船进行安全性评估所采用的“安全性评估方法Ⅰ、Ⅱ”和国际上安全性定量评价应用较为广泛的“PRA 方法”，简述“安全性评估方法Ⅰ、Ⅱ”在载人飞船上的应用情况，提出载人航天器后续安全性评估工作建议。

关键词　载人飞船　安全性　评估

1 概论

1.1 飞船安全性工作概况

为了保证航天员在飞行期间的正常工作和生活，除了要求其高可靠之外，载人飞船的安全性工作也显得尤为重要。

安全性是指将伤害（对人）或损坏的风险限制在可接受水平状态。飞船的安全性特指航天员安全性，即在载人航天活动全过程中，保障航天员健康生活、正常工作并安全返回、不发生伤亡事故的能力。

载人飞船的安全性工作就是为了保证航天员安全性而开展的工作，一般包括安全性管理、设计、分析和验证等内容，安全性定量评估是安全性验证的一项重要工作。

载人飞船的安全性管理主要包括明确安全性组织和职责、策划并制定安全性大纲、处理安全性工作与其它工作之间的关系、组织安全性评审、组织安全性培训以及做好安全性信息管理与事故报告与调查工作等。飞船系统所达到的安全程度，决定于系统在设计、制造、试验和使用过程中对安全性管理完善的程度，管理的不完善是引起意外事故的根本原因。

安全性设计是通过各种设计活动来消除和控制各种危险，防止系统在使用中发生导致人员伤亡或系统损坏的各种意外事故，进行安全性设计也是危险控制的过程，因此在进行系统功能设计时必须遵循安全性设计准则。安全性设计主要采用最小危险设计、故障容限设计、故障安全设计、环境适应性设计、冗余隔离等设计方法和手段。

安全性分析是以系统迭代的方式，对系统设计和使用的安全性进行全面分析，以识别潜在的危险和产生危险的原因，分析危险可能造成的后果，提出消除或控制危险措施并验证，最终确定危险风险能否接受，支持管理决策。飞船系统具体的安全性分析工作主要包括危险源识别、危险分析、残余危险分析、故障树分析（FTA）、安全性关键项目确定与控制以及偏离、超差等对系统安全性影响分析等。

安全性验证是为了保证安全性已集成到各级产品中去，它包括定性验证和定量评估。定性验证的范畴包括检查安全性大纲实施情况、故障树分析情况、残余危险分析情况、应急状态分析情况、最坏情况分析、偏离和超差对系统安全性影响分析、重大事故的调查和分析等。安全性定量评估与定性验证所对应，是在产品研制阶段或出厂前，对产品安全性做出量化的综合评估，为进一步的管理决策提供依据。飞船系统所做的定量评估是利用采集到的可靠性、安全性信息和已建立的可靠性、安全性模型来进行具体的安全性指标验证。

1.2 飞船安全性评估概况

作为一个载人航天器，仅仅对其进行安全性的定性验证是不够的，在其转阶段或发射之前需要对其安全性水平进行定量评估，从国外航天机构的相关研究资料可以看出，进行载人航天器安全性定量评估的方法主要包括“安全性评估方法Ⅰ”、“安全性评估方法Ⅱ”和目前国际上较为流行的“PRA 方法”。

从我国实施载人航天工程初期，飞船系统内部就开始对载人飞船安全性定量评估的方法进行研究，系统总体一方面借鉴国外的成功经验，一方面结合自己的工程实践，虽然在国内开创性的开展了安全性评估工作，陆续在几艘载人飞船的研制中使用了“安全性评估方法Ⅰ”和“安全性评估方法Ⅱ”，但这两种方法在应用上还都存在一定的局限性，需要开展进一步的研究。通过介绍载人飞船安全性评估的几种方法及其应用情况，可以针对存在的问题进行一定的分析。

2 载人飞船安全性定量评估方法

2.1 安全性评估方法Ⅰ

我国载人飞船工程前期都采用了“安全性评估方法Ⅰ”进行安全性定量评估，对涉及航天员安全的事件进行量化分析。该方法的主要思想是将整个任务划分为几个阶段来分别计算它们的安全性指标，用这种方法进行飞船安全性评估时，把全任务阶段分为待发段、发射段、运行段、返回段和着陆后五个任务阶段来分段计算各段的安全概率，与公式(1)的评估方法相比，用经典方法计算整个系统在全任务阶段的安全性指标时不易操作，前者也是在该方法的基础上改进所得到的。

该评估方法也对危及航天员安全的各种危险事件(X_{ij})的发生概率，以及尽可能采取的安全措施成功实现的事件(Y_{ij})的概率做出定量分析化的估计，从而给出不同阶段的安全概率点估计值：

$$S_i=1-\sum_{i=1}^{m}\sum_{j=1}^{n}P(X_{ij})[1-R(Y_{ij})] \qquad (1)$$

式中：　S_i——第 i 个阶段的安全概率估计值；

X_{ij}——在飞行任务的第 i 个阶段，系统可能出现的第 j 个危险事件（i=1,2，…,m 时段；j=1,2，…,n 个危险事件，互不相容）；

Y_{ij}——对应事件 X_{ij} 的安全措施成功实现的事件；

$P(X_{ij})$、$R(Y_{ij})$——事件 X_{ij}、Y_{ij} 发生的概率。

2.2 安全性评估方法Ⅱ

我国载人飞船工程后期进行安全性评估的方法采用了“安全性评估方法Ⅱ”。该方法是在方法Ⅰ的基础上考虑到整个飞行阶段的成功概率，在完成可靠性评估的基础上开展安全性评估，将飞船各阶段的可靠性指标作为安全性评估的输入条件，其思想是将前一阶段任务的成功作为后一阶段成功的条件概率，并将应急救生作为设备发生故障时拯救航天员的措施，航天员在飞船舱内安全概率的设计评估取决于全任务周期内设备的故障。

进行发射段概率计算时，因为在发射段运载火箭有故障时，飞船可以配合逃逸塔开展逃逸救生措施，因此不但要考虑飞船的任务成功概率同时还要考虑到运载火箭的可靠性指标。具体评估按以下公式进行计算：

$$P=\prod_{k=1}^{N}P(k)+q(1)P_{cn}(1)+\sum_{k=2}^{N}\sum_{i=1}^{M}q(i,k)P_{cn}(i,k)\prod_{l=1}^{k-1}P(l) \qquad (2)$$

其中：$P(k)$——圆满完成飞行大纲第 k 阶段的概率；

$q(1)$——载人飞船在飞行大纲第一阶段(发射段)发生故障的概率；

$P_{cn}(1)$——载人飞船在飞行大纲第一阶段(发射段)发生故障时拯救航天员的概率；

$P(i,k)$——飞行第 k 阶段，第 i 分系统无故障工作概率；

$q(i,k)$——第 k 阶段第 i 分系统，在其它分系统正常工作的条件下，发生故障的概率；

而：　$q(i,k)=1-P_{cn}(i,k)$ (3)

$P_{cn}(i,k)$——当第 k 阶段，第 i 分系统发生故障时，启动应急程序，使航天员顺利返回地面的概率；

$P(1)$——圆满完成飞行大纲第 l 阶段的概率；

N——正常飞行大纲的阶段数；

M——在该飞行阶段工作的分系统数。

2.3 PRA 方法

概率风险评估（Probabilistic risk assessment，PRA)是一种系统安全性风险的定量评估方法。近年来，随着 PRA 方法在国外各研究领域的广泛应用，以 NASA 为代表的各国航空航天部门对 PRA 的重视程度越来越高，PRA 在我国的核电工业也取得了有效的成绩。

该方法是将特定的系统事故的风险用其发生的可能性来量化，航天员安全性风险也就可以用出现航天员伤亡的可能性来量化。为计算系统事故风险(概率)而建立的模型称为概率风险模型，常用的概率风险模型是“故障树＋事件树”的因果图模型。事件树模型构成了 PRA 模型的基本框架，用于对事故序列进行建模与分析。故障树模型用于进行安全系统分析，目的在于确定事故序列中需要发挥功能的系统的平均失效概率，对于飞船系统主要就是 FTA 法，建立以系统事故(如载人飞船的船毁人亡)为顶事件，以引发该事故的所有潜在危险为底事件的故障树，通过搜集各底事件的发生概率，利用故障树逻辑结构得到系统的安全性评价指标。进行 PRA 包括初始事件的分析、事故序列的模型化、定量化分析，主逻辑图建立、数据分析、人因分析的要求等，PRA 的具体实施步骤见图 1。

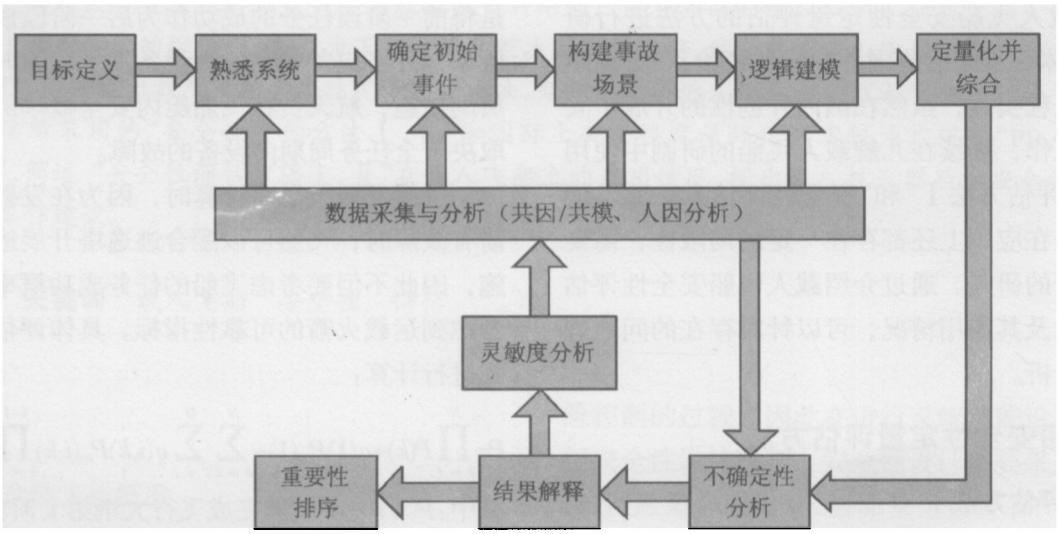

图 1　PRA 实施步骤

2.4 三种方法的对比

“安全性评估方法Ⅰ”是根据系统划分的任务阶段，对系统的安全性进行分段评估，它不能给出一个载人航天器全任务阶段安全性评估指标。而“安全性评估方法Ⅱ”能够给出一个全任务的安全性评估值，比方法Ⅰ更具有广泛的适用性。

但“安全性评估方法Ⅰ、Ⅱ”在实际操作中因“危险事件”都是以飞船出现故障的状态来描述，也就是用系统的不可靠度来表述，因此这两种方法的安全性评估都是以产品的可靠性评估结果作为安全性评估的基础数据，是以产品的高可靠性来保证高安全，体现了“可靠性是安全性的基础”的理念。但是“可靠不一定就安全”，可靠性评估数据一方面并不能反映产品一些潜在的安全隐患，另一方面系统的微小故障而表现出来的不可靠也不一定能危及飞船及航天员的安全。再有就是这两种方法一般只用于整船的安全性评估，而对于分系统级评估因数据采集等原因还不易实施。因此这两种方法虽然在一定程度上能够反映飞船的安全性水平，但因其局限性，还需在后续的工作中对评估公式和数据采集方法进行进一步的研究和优化。

PRA 方法与前两种方法不同，它是基于系统事件的逻辑关系以及事故的传播途径，量化每个事件和事故的发生概率，利用构建的事件树、故障树模型和基层数据来对系统的安全性进行评估，这样评估的结果较为真实，并且可以实现各级产品的安全性评估，但难点是事件量化指标的实现以及大量相关数据的采集，是一个涉及人力物力较多、较为庞大繁琐的工程，因此我国航天领域对 PRA 的研究还只是处于起步阶段，目前只能探索性的用 PRA 方法进行评估。

3 载人飞船安全性评估的应用

在我国近年发射飞船的安全性评估中，根据“安全性评估方法Ⅱ”，将该飞船各任务阶段的可靠性指标分别代入公式(2)，通过计算可以得到该型号安全性评估值也就是载人飞船航天员安全性保证概率的值。

由于前一艘载人飞船安全性评估采用的是“安全性评估方法Ⅰ”,也就是按公式(1)的方法进行计算，计算时只是按划分的任务阶段计算了每一段的安全性指标,没有一个全任务的量化评估值。因此，为了便于比较近一艘飞船在开展了一系列可靠性安全性工作后可靠性数据积累和部分设计改进后整船达到的安全性水平,特采用“安全性评估方法Ⅱ”重新对前一艘船的相关数据进行计算，得到前一艘船整船全任务阶段的安全性评估值。

在计算时，为了突出两艘飞船设计和生产等状态的直接比较而将计算用到的运载火箭的数据进行统一化处理，即将后一艘飞船计算用到的发射段运载火箭的相关可靠性数据直接用于前一艘飞船的安全性评估中,按照公式(2)的的计算步骤也就可以得到前一艘船航天员安全性保证概率的值。

对两艘船用同一种方法计算的结果进行比较可以看出，两艘船的安全性保证概率都在 0.9 以上,而近一艘飞船的安全性定量评估结果比前一艘船的评估结果高出 0.016,从而也从一定程度上表明在前一艘船发射之后，对后一艘飞船所做的一系列可靠性安全性工作是有成效的。

4 结论

我国发射载人飞船“多人多天”飞行的圆满成功,说明其可靠性安全性设计是合理的、成功的,满足工程总体的要求，同时也说明可靠性安全性的验证充分、验证方法和验证结果的正确性。因为其它航天型号都不涉及人的问题，所以我国载人飞船的安全性定量评估工作是开创性的，也较其它航天型号更全面深入,效果更好。

但是，同时也要认识到并且在后续的工作中做好两个方面的工作：

(1) 虽然目前使用的安全性评估方法Ⅱ从很大程度上合理地评价了飞船的安全性水平，但它还存在一定的局限性，需要在后续的研制工作中对其开展进一步的研究,对其数据采集方法等进行优化,同时还要深入开展对 PRA 方法的研究；

(2) 用“安全性评估方法Ⅱ”在评估过程中所用到的可靠性评估数据的准确性直接影响到安全性评估的结果,要想使安全性评估准确可信,就要提高可靠性评估的准确性，而进行可靠性评估所用到的产品可靠性预计和试验信息以及我们评估所用的软件都将直接影响评估的精度。因此在载人飞船后续工作中，要使安全性评估更能准确地反映系统的安全性水平,必须从搜集基础数据信息开始,严格把关,努力使安全性工作能真正起到应有的作用。 ◇

参 考 文 献

[1] 别烈高澳依,亚罗波洛夫.俄罗斯.《航天安全指南》.

[2] Office of safety and Mission Assurance.NASA Headquarters.《PRA procedures guide for NASA managers and practitioners》

(上接第 10 页)

不长的时间内可以达到稳态平衡状态。该稳态平衡温度随着压力的降低而增大。随着导线过载电流的增大,导线绝缘层的温度增大,微小的过载电流变化对单根导线的影响不明显,但排线的影响是明显的。在微重力排线内部的温度变化比排线表面发射的辐射温度要大。 ◇

参 考 文 献

[1] Friedman R. Testing and selection of fire-resistant materials for spacecraft use. NASA TM-209773 , 2000

[2] Friedman R. Risks and issues in fire safety on the space station. NASA TM-106430, 1994

[3] Friedman R. Fire safety in extraterrestrial environments. NASA TM-207417, 1998

[4] Friedman R, Gokoglu S A, Urban D L. Microgravity combustion research: 1999 program and results. NASA TM-209198, 1999

[5] Limero T, Wilson S, Perlot S, James J. The role of environmental health system air quality monitors in spacestation contingency operations. SAE Transactions, 1992, 101: 1521-1526

[6] Greenberg P S, Sacksteder K R, Kashiwagi T. Wire insulation flammability experiment: USML-1 1 year post mission summary. In: Proceedings of the Joint Launch Plus One Year Science Review of USML- and USMP-1 with the Microgravity Measurement Group, NASA CP 3272 2: 1994. 631-655.

[7] Greenberg PS, Sacksteder K R, Kashiwagi T. Wire insulation flammability. 3rd International Microgravity CombustionWorkshop, NASA CP 10174: 1995. 25-30.

[8] Kikuchi M, Fujita O, Ito K, Sato A, Sakuraya T. Experimental study on flame spread over wire insulation in microgravity. Proc. Combust. Inst., 1998, 27: 2507-2514.

[9] Kikuchi M, Fujita O, Ito K, Sato A, Sakuraya, T. Flame spread over polymeric wire insulation in microgravity. Space Forum, 2000, 6: 245-251