doi: 10.7690/bgzdh.2014.09.025

航天发射试验安全评估软件体系架构

尚晨[1]，马昕晖[2]，陈景鹏[2]，吉雯龙[1]
（1. 装备学院研究生管理大队，北京 101416；2. 装备学院航天装备系，北京 101416）

摘要：针对目前航天发射事故安全分析软件大多采用通用的建模仿真分析软件的问题，提出一种将“指标体系评估”、“概率风险评估”和“危害度及危害区域评估”三者相结合建立航天发射试验安全评估软件体系架构。依据航天事故的特点，结合现有的评估方法和我国航天任务的需要，通过指标体系优化评价对事故进行危害等级的评估，用概率风险评价进行事故发生概率的计算，将危害度及危害区域评价进行事故后果分析，得到航天发射试验安全评估“三步走”方法。分析结果证明：该软件可对航天发射试验进行全面的安全预测和危害后果分析，将为航天发射试验场的建立和发射任务的实施提供重要的数据及安全保障。

关键词：航天发射试验；指标体系；概率风险评估；安全评估；软件架构
中图分类号：TJ86　　**文献标志码：**A

Security Assessment Software System Architecture for Space Launch Test

Shang Chen[1], Ma Xinhui[2], Chen Jingpeng[2], Ji Wenlong[1]
(1. *Administrant Brigade of Postgraduate*, *Academy of Equipment*, *Beijing* 101416, *China*;
2. *Department of Spaceflight Equipment*, *Academy of Equipment*, *Beijing* 101416, *China*)

Abstract: For the current the space launch accident safety analysis software had used the common modeling and simulation software to analyze problems, the security assessment software system architecture combined “index system assessment”, “probabilistic risk assessment” and “criticality and hazard area assessment” for the space launch test is given. Based on the characteristics of aerospace accidents the existing assessment methods and the needs of our space missions, the accident hazard rating through using the evaluation index system optimization is assessed. The probabilistic risk assessment the probability of an accident is calculated. The accident consequence by criticality and hazard area assessment is analyzed. Finally, the space launch test safety assessment “three-step” approach is got. The Analysis results show that: this software can provide not only a thorough analysis for security predictions and hazardous consequence of the space launch test but also be the important data reference and security for the building of space launch testing ground and the implementation of the launching test.

Keywords: space launch test; index system; probabilistic risk assessment (PRA); security assessment; software architecture

0 引言

航天发射试验的安全性历来是世界各国关注的焦点。一旦发生航天事故，将会给人员财产带来极大的损失。1967 年 1 月，阿波罗 1 号飞船在实验台上起火，3 名航天员被烧死在舱内，原因是飞船的设计和生产错误。1986 年 1 月，美国挑战者号航天飞机起飞 73 s 后爆炸，机毁人亡。1996 年，长征三号乙运载火箭首次飞行发射国际卫星 708 号失利，造成 8 死 57 伤[1]。因此航天发射试验中的安全评估显得极为重要。

目前针对安全评估主要是进行安全预测和危害后果分析，安全预测可提供危害等级评估和危害发生概率评估，而危害后果分析主要是进行危害发生后的仿真评估。国内外针对航天发射事故的安全分析用到的软件大多数是通用的建模仿真分析软件。笔者结合航天发射试验特点构建航天发射试验安全评估软件体系架构，采用将危害等级评估、概率安全评估(probabilistic risk assessment，PRA)和危害后果评估相结合的方式，对航天发射事故进行安全预测和危害后果分析。

1 需求分析

1.1 航天发射试验安全现状分析

航天发射试验的安全历来是各国关注的重点。航天发射器在设计、生产、安装、试验、测试、维修、保养和使用过程中出现任何的故障或失败都将带来极大地损失。不管是美国国家航空航天局(national aeronautics and space administration，NASA)还是欧洲宇航局(european space agency，ESA)都投入了大量的物力人力进行安全评估的研究，但是航天事故仍然层出不穷。

收稿日期：2014-03-21；修回日期：2014-04-21
作者简介：尚晨(1965—)，男，陕西人，在读硕士，从事航天系统安全性与可靠性研究。

据公开信息统计，自 1973 年以来我国火箭发射中至少有过 21 次失败[2]；从 1959 年 8 月 21 日美国发射的水星号模型/小兵飞行器开始，直到 1995 年底，在美国、前苏联/俄罗斯进行的 249 次载人航天发射飞行中，故障总数为 166 次。带来的经济和人员损失极为严重，因此，提前进行安全评估，对航天发射极为重要。

针对航天试验安全评估的方法各国也进行了大量的研究。1986 年的“挑战者”号事故使得 NASA 认识到建立故障模式及其危害性分析(FMEA)/关键相关项目表(CIL)方法的重要性，至此 NASA 开始用 PRA 对航天发射试验中的各个阶段进行详细的分析，到目前为止 PRA 已经在 NASA 广泛使用[3]。ESA 对 NASA 的概率风险管理方法进行了吸收和分析，现已开发了多目标决策支持系统来支持风险分析。而我国目前的安全评估方面才刚起步，还停留在基础的定性阶段，缺乏评估的体系和系统性[4]。

1.2 现有安全评估软件分析

目前航天发射试验中用到的安全评估软件主要有 2 大类，即安全预测软件和危害后果分析软件。安全预测软件主要是进行概率风险评估，即通过风险模型的建立，之后进行定量化分析的一个过程。如 NASA 开发的大型定量风险评估系统(quantitative risk assessment system，QRAS)，解决了多阶段任务风险建模、任务进度阶段的风险分析和评估问题，该软件利用概率进行风险评价，用到顺序图、事件树分析、故障树分析等方法对风险、系统安全性进行定量分析和评估[5]；ABSG 公司于 20 世纪 80 年代前期开发的 RISKMAN 软件是基于概率风险评价技术的定量风险分析与评价软件，它使用事故链的模拟方法、综合使用事件树和故障树、方便了用户自有数据和外带数据库的整合、考虑了事故链之间的相关性、事故链可以直接和外部事件模型连接和用户可以选择单点计算或概率分布[6]；我国的 FDS 团队开发了名为 RiskA 的软件可进行概率安全/可靠性分析，并故障树和事件树的分析、重要度和敏感度分析、不确定性分析等。

危害后果分析软件用到的都是通用的仿真软件，以计算机模拟仿真计算的数字化评价技术为基础，即通过数字计算方法，在计算机上模拟仿真事故发生的过程，对其影响范围和危害程度做出综合分析和评价。英国 SHELL 公司开发的 SHELL FRED 针对过程泄漏、储槽泄漏、运输设备泄漏等过程进行模拟，也可以针对泄漏扩散引起的火灾、爆炸进行后果仿真[7]；DNV 公司自主开发了后果模拟软件 PHAST，该软件通过对发生事故时的真实场景输入，包括设备类型、物质种类、存储参数、泄漏方式、周围环境(大气温度、湿度、稳定度、风速)等设置，建立事故后果模型，即可模拟评价石油化工装置可能发生的毒性云团、火灾和爆炸事故的影响范围及程度[8]。

1.3 对安全评估的需求

通过对市面上现有的安全预测软件和危害后果分析软件的总结归纳可知，目前存在的软件大都属于通用安全分析软件，与航天发射试验的结合不紧密，并不能满足航天发射试验的安全评估，总结起来有以下缺点：

1) 危害后果分析软件种类繁多，功能单一。航天发射试验中涉及到的安全隐患很多，有冲击波、热辐射、毒气泄漏等，单一的软件不能满足所有航天发射任务中的安全危害评估。

2) 集成性不高。在航天发射试验中，不同安全隐患需用到的评估方法不尽相同，但却未检索到将概率安全评估和危害后果评估集成在一起的软件。

3) 与航天发射结合不够紧密。航天发射试验任务中涉及到的很多特有的数据在软件中都无法查询或直接使用。

综上所述，不管是国内还是国外，在航天发射试验危害评估过程中都要用到多种软件，且不能充分满足评估需要。因此笔者提出了关于航天发射试验安全评估软件平台建设的关键点包括：

1) 紧密结合航天发射试验的特点。将搜集获取的各类数据与软件进行有针对性的结合，建立航天发射试验数据库，进行数据的归类、提取和入库，为航天发射试验提供数据。

2) 集成 3 种主要模块功能。即将危害等级评估、概率安全评估和危害后果分析 3 种重要的评估模块集成在本软件中。

3) 满足各种航天发射试验中的危害后果分析，对爆炸冲击波、热辐射、毒气扩散等航天发射中涉及到的危害都能进行分析。

2 软件总体设计

依据国内外软件的现状和我国航天任务的需要，笔者提出航天发射试验安全评估平台体系架构。平台针对航天事故的特点，结合现有的评估方法，首先通过指标体系优化评价对事故进行危害等级的

评估，接着用概率风险评价进行事故发生概率的计算，最后再用危害度及危害区域评价进行事故后果分析，提出航天发射试验安全评估“三步走”方法。3 种评估平台各有侧重点，既可针对同一系统依次进行，又可独立工作，能够更好地对航天事故进行评估。软件总体架构框图如图 1。

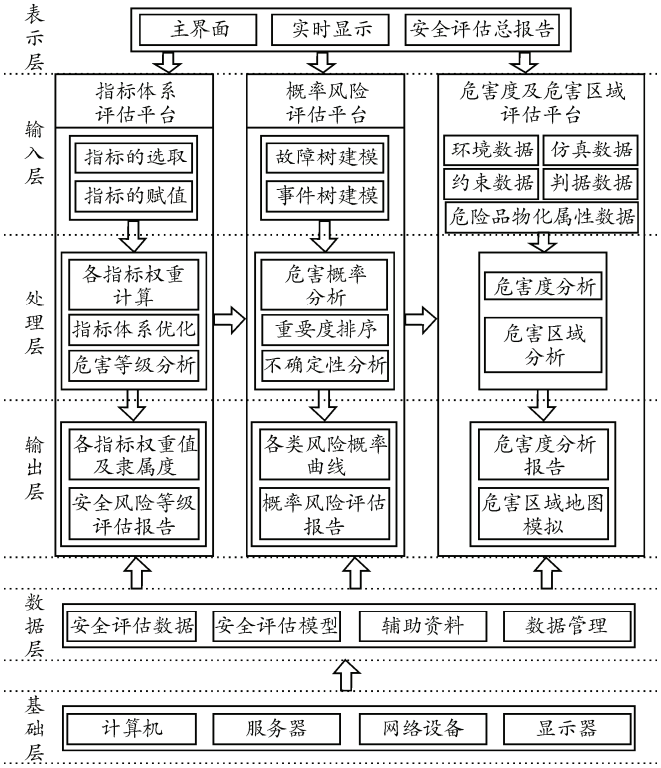

图 1　软件总体架构

该航天发射安全分析软件框架中，各层协同工作：表示层可以实时显示各层的处理运算情况；输入层主要进行各评估平台的初始数据输入；处理层采用高速计算引擎对数据进行处理并实现了软件的主要 3 大功能；输出层得出 3 种评估的最终结果；数据层进行所有数据结果存储工作；处于基础层的硬件设备提供软件的硬件基础。

3　指标体系评估平台

3.1　总体介绍

指标体系评估平台在没有完备数据的情况下，通过分析航天发射试验系统特点，得出影响系统安全的风险因素。步骤为：初步建立评估指标体系，然后对指标体系中各指标进行量化，基于量化的数据，采用指标体系优化方法对初步建立的指标体系进行优化，得出可用于安全评估的指标体系，最后选取评估方法进行评估，得出系统的安全风险等级。

3.2　功能模块介绍

该平台主要分为指标体系建立模块、指标量化模块、指标体系优化模块和系统评估模块，如图 2 所示。指标体系建立模块主要完成指标的选取及指标体系的建立，可通过从指标集中选取与手工输入实现指标的导入；指标量化可根据需求的不同，选取不同的方法进行量化，得出各指标的权重值；指标体系优化模块首先进行有效性、重要性、相关性以及指标体系的可靠性检验，利用量化的数据，对指标体系进行分析；评估模块主要根据优化后的指标体系，根据各指标的权重值及隶属度，计算得出系统的安全风险等级。

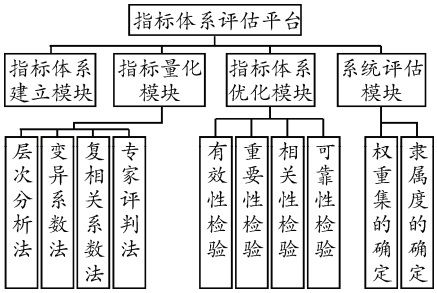

图 2　指标体系评估平台结构

3.3　涉及到的关键技术

指标量化过程中用到了层析分析法、变异系数法 4 种方法，指标的优化过程中有 4 类检验，如何处理多种方法和检验的程序化是需要重点考虑的。

4　概率风险评估平台

4.1　总体介绍

概率风险评估是一个综合的过程，其主要工作分为 2 个部分：风险模型的建立与模型的定量化分析。前者主要指描述和构建危险事件发生、发展的逻辑模型，后者主要是计算基本事件、危险事件的发生概率，在概率的意义上区分各种不同因素对风险影响的重要程度。

4.2　功能模块介绍

概率风险评估平台可对航天发射试验事故进行概率评价，得出该事故发生可能性的大小，平台构成如图 3 所示。任务规划模块是用户根据风险特点，采用网络图进行任务阶段(系统)的划分，任务规划结果作为事件树和故障树建模基础，每个网络节点对应相应的故障树和事件树模型。事件树故障树建模模块可针对任意复杂系统进行主逻辑图、事件序列图、故障树和事件树人机交互建模，建模中可实现共因失效事件、人为和环境因素的建模，可支持多用户协同建模。风险分析与计算模块是以发射任

务阶段(系统)为节点，分别计算各任务阶段内系统主要故障的风险概率，最后形成准备阶段风险、发射阶段风险和飞行阶段风险概率值。风险分析与计算模块可综合故障树和事件树分析任务阶段(系统)风险概率、重要度及敏感度等。风险曲线生成模块可生成故障树、事件树顶事件、各任务阶段以及总任务的风险概率曲线，包括 PDF 曲线、CDF 曲线、风险不确定性、置信区间等数据信息。

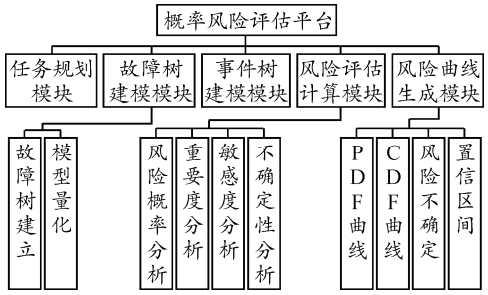

图 3 概率风险评估平台结构

4.3 涉及到的关键技术

1) 以事件链为基础的建模技术和以不确定性分析为核心的数据分析技术将是该平台设计编写中的关键。

2) 故障建模技术。事件树的建立过程以初因事件为起点，按照事件发生的逻辑顺序逐步建立事件树模型，最后形成所有事件序列。故障树建模采用反向逆推方法，详细列出可能导致顶事件的所有直接和间接因素，按照层次化建模手段逐步细化，最终形成完整故障树模型[4]。

5 危害度及危害区域评估平台

5.1 总体介绍

危害度及危害区域评估平台主要是通过软件中的数学模型模拟和预测航天发射试验过程中所产生的安全事故的危险后果和影响，计算安全区域及进行危害结果生成显示。针对航天发射试验的危害模式，通过危害度计算，可为安全分析人员提供精确的危害度数学计算模型，实现危害快速计算与评估，并为航天发射任务风险快速决策和安全防护提供理论和技术层面支持。通过危害区域生成，可为航天发射场的选址以及各建筑物之间的安全距离设计提供理论和方法支持。

5.2 功能模块介绍

该平台主要由危害模式选择模块、模型选择模块、参数初始化模块、危害度及危害区域计算模块组成，结构如图 4 所示。

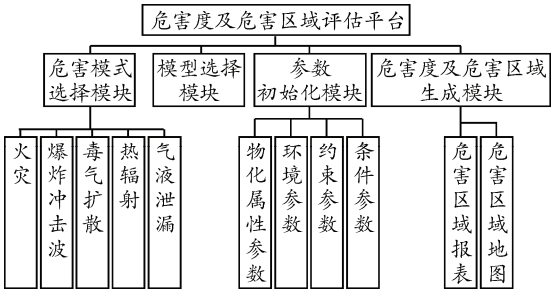

图 4 危害度及危害区域评估平台结构

危害模式选择模块：该模块可进行危害模式的选取，危害模式包括火灾危害、冲击波危害、热辐射危害、毒气扩散危害和气/液泄漏模块。

模型选择模块：针对某种危害模式，有多种计算模型。火灾计算模型包含池火模型、火球模型和喷火模型；爆炸冲击波计算模型包含 TNT 模型、TNO 模型、Bake-Strehlow 模型和 BLEVE 模型；毒气扩散计算模型包含非重气云扩散模型和高斯模型；气/液泄漏计算模型包含容器/管道源模型、液体泄漏模型、气体泄漏模型和两相流泄漏模型。该模块可进行模型的选取。

参数初始化模块：参数初始化模块针对具体的危害模式，利用向导快速选取数据库中推荐的参数，也可自行手工设置相关参数，形成危害度计算的初始参数。可进行物化属性参数、环境参数、约束参数和条件参数的设定，并可进行首区和航区的人口及建筑密度设定。

危害度及危害区域计算模块：该模块可进行各类参数计算、安全距离计算和危害程度计算。针对危害区域可在导入地图中进行实时危害区域生成。

5.3 涉及到的关键技术

1) 危害度计算模型生成技术。针对传统危害性计算模型难以精确计算发射场危害性计算，采取在传统计算模型的基础上将发射场的相关约束条件和数据代入传统计算模型，经过大量仿真分析计算，形成发射场危害度计算模型，并经国内外数据对比验证逐步修正，最终形成航天发射场危害度模型数值计算模型。

2) 危害区域生成技术是本平台的关键，平台中涉及到的模型很多，且要通过地图的导入来模拟危害区域的形成，如何更好的实现是关键。

6 数据管理平台

因为航天发射试验安全分析系统建设过程中所

涉及的参数、属性等数据非常大，数据库构建过程中要充分考虑各种因素，包括数据的分类、查询和数据库的可扩展性等。

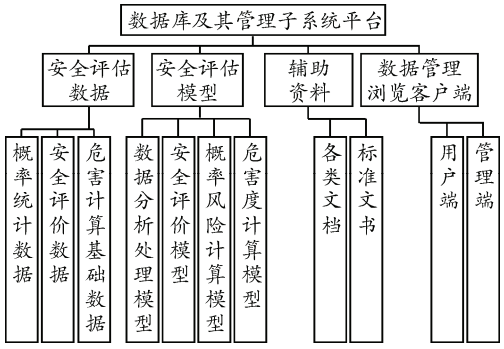

图 5　数据库及其管理子系统平台结构

数据库完成数据的分类、查询、备份和数据的扩展功能。数据库包括安全评估数据、安全评估模型、辅助资料和数据管理浏览客户端 4 个模块，如图 5 所示。安全评估数据为软件平台调用、生成和结果类数据，包括概率统计数据、危害计算基础数据和安全评价数据。安全评估模型为软件平台进行安全分析与评估过程中需要用到的各种计算模型，包括数据分析处理模型、概率风险计算模型、危害度计算模型、安全评价模型。辅助资料是研究安全问题所涉及的各类学习和参考资料。数据管理浏览客户端即进行管理和授权用户的使用权限。数据库及其管理子系统采用 Visual C++和 SQL Server 软件构建，建立数据库充分考虑数据库的各项指标，建成一个可扩展的数据库系统。

7　结论

笔者在详细分析航天发射试验安全需求的基础上，提出了适用于航天发射试验的软件架构，分为指标体系评估平台、概率风险评估平台和危害度及危害区域评估平台。该架构将实现对航天任务事故进行危害等级评估、事故发生概率评估和危害度及危害区域评估，可全方位地预测事故和进行事故的后果分析，并能够与底层数据库相接，对各类数据模型和分析结果进行管理。该平台的建立，将为航天发射试验场的规划与设计提供安全可靠的技术支持，也可为发射任务的规划和实施提供技术参考。

参考文献：

[1] 张宗美. 航天故障手册[M]. 北京: 宇航出版社, 1994: 4-6.

[2] 伍科. 中国历年发射卫星统计表: 1970.4—1995.3[J]. 航天返回与遥感, 1995, 16(2): 71-72.

[3] 张莉敏. NASA 风险管理初探[J]. 中国航天, 2012(3): 50-53.

[4] 郑恒, 周海京. 概率风险评价[M]. 北京: 国防工业出版社, 2011: 4-16.

[5] Weinstock R M, Smidts C S, Mosleh A, et al. Quantitative risk assessment system (QRAS): U.S. Patent 6,223,143[P]. 2001-4-24.

[6] Carter B, Hancock T, Morin J M, et al. Introducing RISKMAN methodology: the European project risk management methodology[M]. HM Stationery Office, 1996: 58-61.

[7] 姚雁. 石油化工危险系统安全评价的软件开发[D]. 大连: 大连理工大学, 2005.

[8] 朱伯龄. 气体泄漏扩散过程及影响因素研究[J]. 石油与天然气化工, 2009, 38(4): 354-358.

****

（上接第 71 页）

[2] Chen T H C, McGillem C D. Target motion compensation in synthetic aperture radar[J]. Aerospace and Electronic Systems Magazine, 1991, 6(2): 14-18.

[3] Son J S, Flores B C. Phase difference method for target motion compensation of stepped-frequency ISAR signature[M]. SPIE, 1996: 163-174.

[4] Young R W, Kingsbury N G. Frequency-domain motion estimation using a complex lapped transform[J]. IEEE Trans. on Image Process., 1993, 2(1): 2-17.

[5] Vetro A, Sun H, Bao J, Poon T. Frequency domain down-conversion of HDTV using adaptive motion compensation[C]//Image Processing International Conference, 1997(1): 763-766.

[6] Ding H, Li X, Huang X T, et al. Velocity compensation based Ultra-Wide bandwidth wireless moving target localization[C]//Wireless Communications & Signal Process., 2009: 1-4.

[7] Sun Y J, Fu Y, Cheng Z, et al. Wideband echo simulation and velocity compensation of midcourse ballistic target[C]//Signal Process., 2012(3): 1944-1948.

[8] Shi B P, Jia X, Cang Z P, et al. LFMCW bistatic ISAR space target velocity compensation based on IPD method[C]//Radar Conference, 2013: 1-4.

[9] Qiao W, Xiao P D, Zhong H Z. Velocity compensation based range-doppler decoupling method for FMCW radar[C]//Engineering and Technology (S-CET), 2012: 1-4.

[10] Zhang K F, Feng Z H, Ma D B. Study on a method of compensation for the range profile of high velocity spatial targets[C]//Image Analysis and Signal Processing, 2010: 450-453.

[11] Arii M. Efficient motion compensation of a moving object on SAR imagery based on velocity correlation function[J]. IEEE Transactions on Geoscience and Remote Sensing, 2013(99): 1.

[12] Nagano T, Iwamoto T, Hara T, et al. Range migration compensation for moving targets with unknown constant velocity in chirp radars[C]//Radar Conference (EuRAD), 2011: 125-128.

[13] Yi M L, Hua D M, Gang L, et al. Velocity estimation and range shift compensation for high range resolution profiling in stepped-frequency radar[J]. IEEE Geoscience and Remote Sensing Letters, 2010, 7(4): 791-795.