文章编号:1674-8190(2016)03-369-05

基于模型的安全性分析技术研究

车程,刘轶斐
(中国航空工业集团公司 第一飞机设计研究院,西安 710089)

摘 要:基于模型的安全性分析技术(MBSA)经过十余年发展,其理论基础和工程应用技术已日趋成熟。首先阐述了传统的安全性分析技术存在的不足,分析了 MBSA 的技术优势;然后结合传统系统安全性分析流程,初步构建了基于模型的安全性建模与分析流程,最后给出了 MBSA 分析技术在飞机研制过程中的安全性评估案例。结果表明:MBSA 可以解决传统安全性分析中飞机级安全性评估不足以及安全性分析结果正确性得不到客观保证的问题。

关键词:基于模型的安全性分析技术;安全性;功能危险分析;特殊风险分析;初步系统安全性评估
中图分类号:V37 **文献标识码**:A **DOI**:10.16615/j.cnki.1674-8190.2016.03.016

Research on Model Based Safety Analysis

Che Cheng, Liu Yifei
(The First Aircraft Design and Research Institute, Aviation Industry Corporation of China, Xi'an 710089, China)

Abstract: After more than 10 years of development on model based safety analysis(MBSA), its theoretical basis and engineering application technology has been mature. At first, the shortcoming of safety analysis is set forth. The application and advantage of MBSA are introduced. Then, combined with the process of safety analysis, the process of safety modeling and analysis are preliminary established. Finally aircraft safety assessment case based on MBSA is provided. The result shows that MBSA could solve the problem of evaluation deficiency of aircraft safety during the traditional safety analysis and unsureness of safety analysis result.

Key words: model based safety analysis; safety; functional hazard assessment; particular risk analysis; preliminary system safety assessment

0 引 言

随着航空技术的不断发展和革新,飞机机载系统复杂化和综合化程度越来越高,机载系统内部的复杂交联和系统之间的高度耦合给系统安全性分析工作带来了巨大挑战。

基于上述系统安全性分析难题,国外学者在基于模型的系统工程(Model Based System Engineering,简称 MBSE)的基础上,提出了基于模型的系统安全性分析技术(Model Based Safety Analysis,简称 MBSA)[1],该技术通过飞机系统研制过程与安全性分析过程的自动化集成,克服了传统安全性分析技术的不足[2],保证了安全性设计与飞机系统设计的同步和协调。利用其研究成果,空客公司开发了基于模型的安全性评估软件(Simfia)[3]。Simfia 不仅完成了传统安全性分析项目,还依据已构建的模型实现了系统动态仿真、安全序列生成、动态 FMEA 等分析,突破了传统静态分析工具的局限,扩充了安全性分析内容。Simfia 软件在军民用飞机中的应用情况如表 1 所示。

在国内,吴海桥等[4]和邢逆舟[5]通过对 MBSA 技术的持续理论研究,取得了一定成果,但上述研究成果还未在飞机型号研制中进行工程应用。

本文通过对 MBSA 的技术优势分析,给出了 MBSA 建模流程,并结合型号应用案例进行评估,以期为 MBSA 技术在飞机研制中的成功应用提供

收稿日期:2016-04-06; **修回日期**:2016-04-21
通信作者:车程,66610662@qq.com

一定参考价值。

表1 Simfia软件在军民用飞机中的应用

Table 1 Simfia application in military and civil aircraft

公司名称	MBSA应用描述
空客公司	A320、A330、A340、A350、A380、A400M的系统安全性分析
利勃海尔宇航公司	A400M、B747-800的空调系统和气源系统安全性分析
泰利斯航空电子公司	A350驾驶舱显示系统安全性分析
法国索加玛航空维修中心	A380座椅安全性分析
拉泰科雷公司	ERJ170、ERJ190舱门系统安全性分析
霍尼韦尔公司	NII90空调系统安全性分析
法国航空工业公司	KC135军用飞机燃油系统安全性分析

1 传统安全性分析方法不足

传统的安全性分析技术具有操作简单、工程实施难度低、生成分析结果快的优点，然而随着复杂系统表现出的高度集成和耦合特点与日俱增，受人类认知能力的限制，难以深入了解和预测飞机系统的所有可能行为[4]，尤其在军用飞机研制周期相对较短，留给安全性评估的时间有限的情况下，设计人员需要花费大量精力将物理模型转换成故障树模型。型号实践表明，这种方式不仅对分析人员要求很高，还存在评估准确性不高、容易遗漏、评估过程核查困难等缺点，从而影响安全性评估工作的效率。难以完全依靠手工描述系统的交联关系和构型变化来完成系统安全性评估。传统安全性分析技术的不足主要表现在以下四个方面：

①安全性评估通常滞后于设计，容易搞成“两张皮”

开展安全性评估需系统设计进展到一定阶段才能进行，不能实现设计与评估的有机融合和同步进行。尤其系统设计迭代更新带来的安全性分析工作周期较长，不能及时为系统构型变化提供建议。

②对设计人员经验水平依赖性强，不能保证结果的正确性和完整性

目前安全性分析主要依赖于设计人员经验，不同工程师对系统的安全性信息理解不同，导致分析结果存在一定差异。

③对系统界面安全性分析不足

各专业更关注本系统安全性分析，对于系统界面分析工作容易遗漏，虽然飞机安全性评估一定程度可以弥补不足，但开展时机较晚、协调工作量大，通常达不到预期效果。

④分析基本靠手工完成，效率较低

目前安全性分析除了故障树分析可以借助软件完成外，其他分析全部依靠设计人员手工完成，不仅效率低下，还增加了犯错的概率。

2 基于模型的安全性分析技术(MBSA)介绍

MBSA理论研究始于欧盟，MBSA是基于模型的安全性分析技术是一种通过将安全性分析工作项目转化为模型，充分借助于计算机的智能化分析，自动产生分析结果的分析技术。2001～2003年欧盟开展了复杂系统增强安全性评估，通过将计算机系统的模型检验方法引入到航空航天领域，构建了基于航空航天系统架构的动态故障传播验证模型。2004～2007年欧盟进行了航空复杂系统安全行为改进项目，通过对航空系统的多角度(功能、人为因素、几何学)研究，形成了系统安全性模型测试方法与工具。基于模型的安全性分析技术优势主要表现在以下四个方面：

①实现了安全性分析与系统研制的有机融合

通过系统设计模型和安全性分析模型的同一化，将系统设计工程师和安全性工程师紧密结合，在研发的迭代过程中可以随时了解和掌握系统参数和设备可靠性数据变化和系统设计架构变化对系统或整机的安全性影响，从而做出更为准确的设计决策，确保安全性分析与系统设计同步开展，及时将安全性分析结果反馈至系统设计。

②自动化安全性分析，从而降低工作量、保证分析结果客观、完整

设计人员构建安全性分析模型只需客观反映系统原理、架构、技术参数等信息，根据模型可以自动生成安全性分析结果，省略将系统信息转化为安全性结果的人工分析的过程，从而降低工作量，也避免了设计人员安全性分析的主观差异性和犯错的概率，保证了分析结果的完整性和客观一致性。

③仿真模型运行，扩充安全性分析内容

借助软件模拟系统运行，实现对模型的仿真分析，辅助设计人员发现设计薄弱环节。

④为四性一体化设计提供技术支撑

通过一次构建模型,可以同时产生四性分析结果,提高工作效率,可为实现四性一体化设计提供技术保证。

3　MBSA 应用研究

为了确保 MBSA 在飞机安全性分析工作中顺利开展,首先必须构建与传统安全性分析流程有机融合的建模与分析方法,力求模型统一,有效集成和规范化分析,确保能够及时评估型号阶段性研制结果并反馈设计;其次需研发具有较高成熟度的安全性建模与分析软件,这是保证智能化安全性分析得以实现的基础技术支撑。

3.1　MBSA 流程

MBSA 流程基本可以分为两条主线,涉及飞机研制的三个层级:

① 以功能为主线,建立飞机/系统/设备的功能模型,分析不同飞行阶段/工作状态可能产生的各种功能失效状态、失效影响等安全性信息,生成功能危险分析结果;

② 以物理架构为主线,建立飞机/系统/设备级物理模型,分析架构合理性,分解和验证安全性指标,生成 PSSA(Preliminary System Safety Assessment)/SSA (System Safety Assessment)结果。

在针对外部事件的特殊风险分析中(鸟撞、轮胎爆裂、发动机高能转子非包容失效),应首先确定特殊事件对飞机的影响范围(可借助 CATIA 模型),然后结合飞机各系统布置模型,提出飞机各系统\设备的隔离、分离建议。MBSA 流程如图 1 所示。

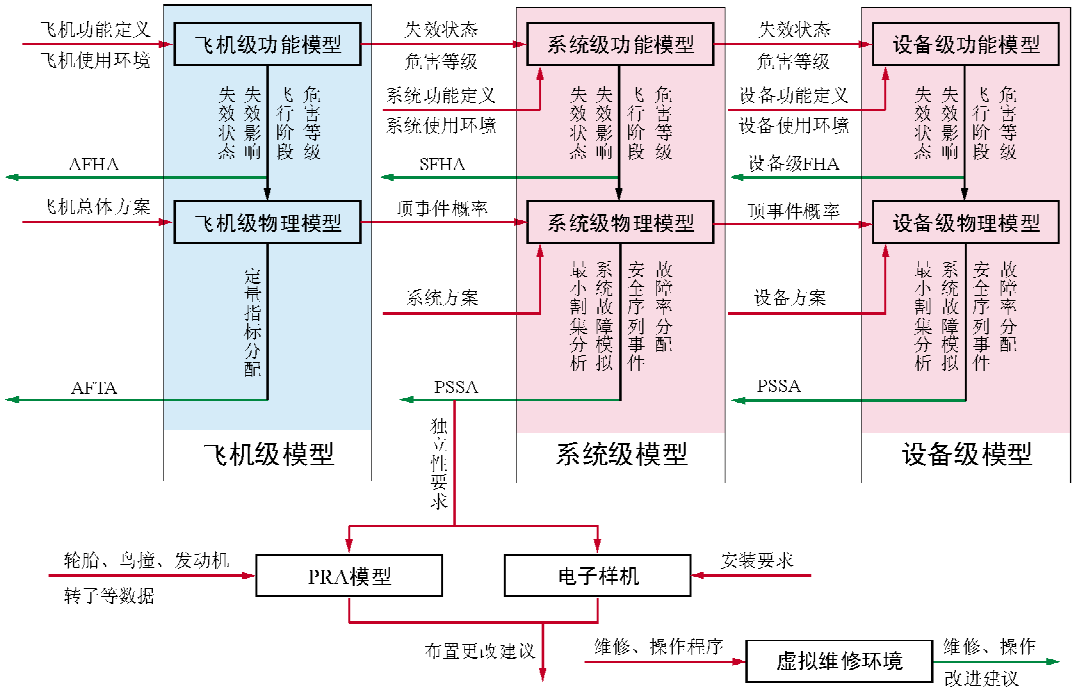

图 1　基于模型的系统安全性建模与分析流程

Fig. 1　Modeling and analysis process based on MBSA

3.2　型号安全性建模与分析

3.2.1　飞机级建模与分析

在方案阶段,以飞机功能和使用环境为输入,构建飞机级功能模型,识别飞机在不同的飞行阶段可能产生的各种功能失效状态、失效影响、以及飞行阶段等安全性信息,生成飞机级功能危险分析结果;以飞机系统架构为输入,构建飞机级物理模型,分解飞机级顶层安全性指标,生成飞机级故障树分析结果;在设计定型阶段,采集系统级模型产生的数据,开展飞机级安全性评估[6]。采用 Simfia 软件构建的飞机级功能模型如图 2 所示。

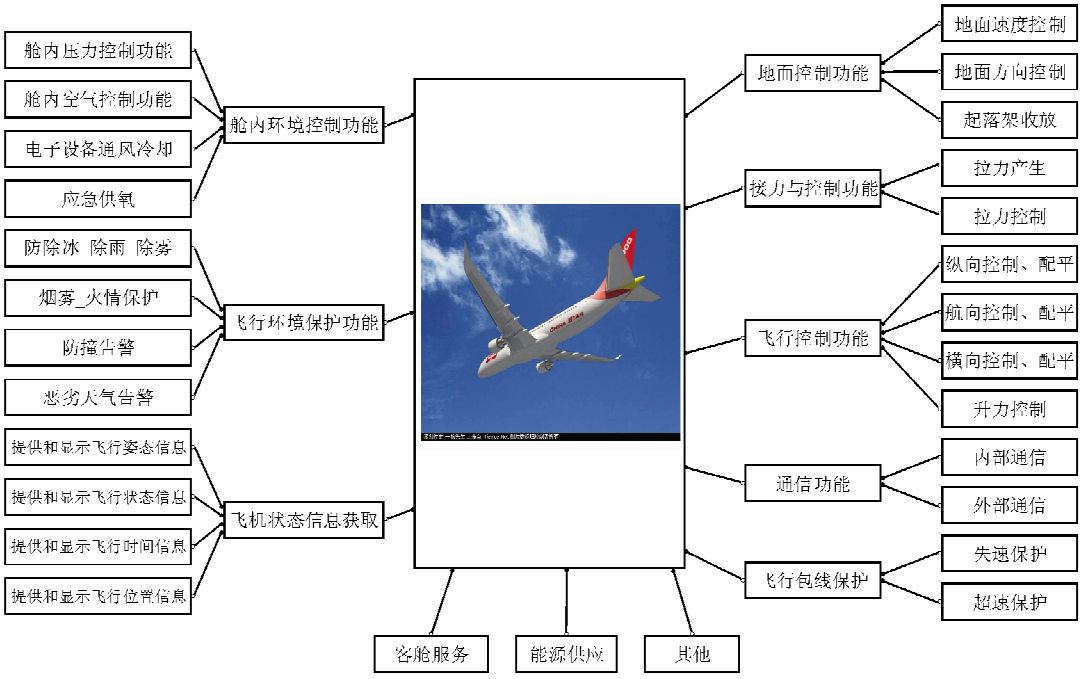

图 2 飞机级功能模型

Fig. 2 The aircraft function model

3.2.2 系统级建模与分析

物理模型需要真实反映系统内部架构以及与其他系统的交联关系，模型中每个模块表示一个设备或子系统，输出端表示设备的故障模式或系统功能失效状态(如图 3 所示)。通过模型可以自动生成故障树实现故障率分配、最小割集分析，另外通过故障模拟注入，系统安全序列分析还可以发现系统架构的薄弱环节。设备级建模与分析与系统级类似，本文不再阐述。

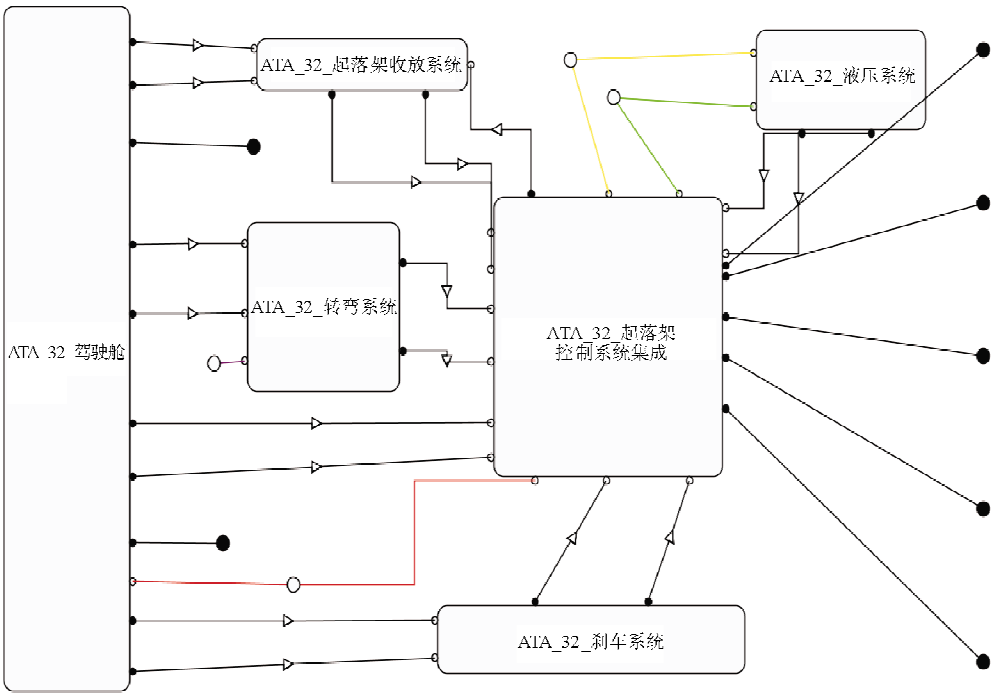

图 3 起落架系统物理模型

Fig. 3 The landing gear system physical model

3.2.3　特殊风险分析与建模

建立鸟撞、轮胎爆破、发动机高能转子非包容失效破坏模型,仿真特殊事件对飞机结构和系统损坏情况,结合飞机级/系统级物理模型,分析设备失效对系统及飞机的最终影响,进而提出设备布置建议和防护措施,并结合模型验证措施的有效性[7-8]。

4　结束语

通过在飞机系统研制过程中应用 MBSA 技术开展安全性分析与评估,可以解决传统安全性分析中飞机级安全性评估不足以及安全性分析结果正确性得不到客观保证的问题。借助 Simfia 软件特有功能,扩充了安全性分析工作内容,在传统安全性分析工作的基础上增加了飞机级模型的集成分析,实现了产品故障率自动化分配和故障模拟仿真分析,充分发挥了安全性评估对系统设计的约束作用。MBSA 代表了系统安全性分析技术的发展趋势,随着研究工作的进一步深入,相信其技术支撑亦会日趋完善,逐步实现系统安全性分析的智能化。

参考文献

[1] Adriano Gomes, Alexandre Mota, Augusto Sampaio, et al. Systematic model-based safety assessment via probabilistic model checking[EB/OL]. [2016-04-21]. http://www.di.ufpe.br/~acm/repConf/conf31.pdf.

[2] M Güdemann, F Ortmeier. Probabilistic model-based safety analysis[J]. Electronic Proceedings in Theoretical Computer Science, 2010(8): 114-128.

[3] 冯臻. 一种新兴的基于模型的民机安全性分析方法[J]. 科技创新导报, 2012(27): 44-45.
Feng Zhen. A new method about MBSA[J]. Science and Technology Innovation Herald, 2012(27): 44-45. (in Chinese)

[4] 吴海桥, 刘超, 葛红娟, 等. 基于模型检验的飞机系统安全性分析方法研究[J]. 中国民航大学学报, 2012, 30(2): 17-20.
Wu Haiqiao, Liu Chao, Ge Hongjuan, et al. Rssearch for aircraft system safety analysis method based on model checking[J]. Journal of Civil Aviation University of China, 2012, 30(2): 17-20. (in Chinese)

[5] 邢逆舟. 基于模型的综合化航电系统资源配置安全性分析与研究[D]. 南京: 南京航空航天大学, 2015.
Xing Nizhou. Safety analysis and research on model based for resource configuration in integrated modular avionics system[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2015. (in Chinese)

[6] SAE. SAE ARP 4754A Guidelines for development of civil aircraft and systems[S]. USA: SAE, 2010.

[7] 郭博智, 王敏芹, 阮宏泽. 民用飞机安全性设计与验证技术[M]. 北京: 航空工业出版社, 2015.
Guo Bozhi, Wang Minqin, Ruan Hongze. Civil safety design and verification[M]. Beijing: Aviation Industry Press, 2015. (in Chinese)

[8] 成伟. 飞机系统安全性设计与评估[J]. 北京: 适航参考资料, 2007(59): 3-8.
Cheng Wei. The aircraft system safety design and assessment[J]. Beijing: Airworthiness Resources, 2007(59): 3-8. (in Chinese)

作者简介:

车　程(1980—),男,硕士,工程师。主要研究方向:军民机适航、系统安全性。

刘轶斐(1981—),男,硕士,高级工程师。主要研究方向:适航与系统安全性分析技术。

(编辑:赵毓梅)