http://myfj.cnjournals.com myfj_sadri@163.com (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2024.01.019

基于模型的民机运营阶段失效评估方法研究

马思思* 郑勇乐 马 彪

(上海飞机设计研究院,上海 201210)

摘 要: 基于模型的安全性分析(model-based safety analysis,简称 MBSA)方法自提出至今,已经日益成熟,更适用于复杂的民机系统。在当前研究和 ARP4761A 草案的基础上,运用 MBSA 方法开展民机在运营阶段的失效评估方法研究,其相较传统方法,将运营数据、功能失效和设备故障集合进同一个模型中,更便于开展运行失效评估。首先,定义运行失效评估模型基本元素,梳理模型构建流程,基于 Simulink 建立包含失效模块的设备级、系统级和飞机级模型。之后,选择某型号飞机外部照明子系统构建模型,利用某机队运营阶段的运行数据开展算例分析。结果表明,基于模型的失效评估与故障树计算结果误差在可接受范围内,同时开展失效模式与影响分析(failure mode and effect analysis,简称 FMEA),利用运行数据计算和仿真得到丧失着陆照明功能危险的发生概率,30 次仿真结果表明基于运行数据的发生概率在设计值附近波动,整体略大于设计值,但仍满足安全性要求。

关键词: 基于模型的安全性分析;运行失效评估;Simulink;飞机系统;外部照明子系统

中图分类号: V37 **文献标识码**: A **OSID**:

0 引言

随着科学技术的进步,民用飞机系统的复杂度不断提高,传统的失效分析方法,如故障树分析(fault tree analysis,简称 FTA)、失效模式与影响分析(failure mode and effect analysis,简称 FMEA)等已难以满足复杂系统开展完整且高效的安全性分析[1]。为满足民机复杂系统安全性分析需求,在传统安全性分析方法的基础上,增强分析能力和分析效率,减少人力和经济投入,实现自动或半自动化的安全性分析,Gomes 等在基于模型的系统工程(model-based system engineering,简称 MBSE)的基础上,提出了基于模型的安全性分析(model-based safety analysis,简称 MBSA)[2],MBSA 将飞机系统研制过程与安全性分析过程自动化集成在同一个模型上,通过加入故障模型及一定比例的可控物理系统,对安全性进行自动化处理[3]。目前,国际航空领域已经有部分制造商及其产品使用 MBSA 进行安全性分析,如达索猎鹰 7x 和 380[4-5]。国内目前关于民机复杂系统的安全性分析主要停留在理论研究阶段,吴海桥等[6]提出了一种基于模型检验的安全性分析方法,利用模型检验工具 NuSMV 对机轮刹车系统安全性进行了分析;车程等[7]初步构建了基于模型的安全性建模与分析流程,采用 Simfia 软件构建飞机级功能模型;董力[8]以飞控系统为例,基于 Simulink 建立系统故障模型,并开展了系统安全性分析。综合上述研究以及 SAE ARP4761A《民用飞机机载系统与设备安全性评估过程的指南和方法》(草案)在标准附录中对 MBSA 方法进行的详细描述[9],本文首先介绍 MBSA 基本情况,之后在飞机级、系统级和设备级仿真模型中扩展失效模式模块,并对模型组成元素进行定义,其次总结建模步骤,给出模型示例。最后,选择某型号飞机外部照明子系统开展算例分析,建立 Simulink 仿真模型,通过对比故障树和基于模型的计算结果证明仿真模型的正确性和有效性,并基于该型号某机队飞机历史运营数据计算设备失效率,开展运营阶段的失效评估,通过对比多次仿真计算结果与设计值的偏

* 通信作者. E-mail: masisi@comac.cc

引用格式: 马思思,郑勇乐,马彪. 基于模型的民机运营阶段失效评估方法研究[J]. 民用飞机设计与研究,2024(1):121-127.
MA S S,ZHENG Y L,MA B. Model-based failure assessment method of civil aircraft operation phase[J]. Civil Aircraft Design and Research,2024(1):121-127(in Chinese).

离情况,评估该型号机队运营阶段的外部照明子系统是否满足安全性要求。

1　MBSA 概述

MBSA 是在传统安全性分析的基础上引入模型的理念,其核心在于通过计算机实现一部分重复性的安全性分析工作。在基于模型的安全性分析过程中,仿真、验证和测试等活动可以依赖于该模型开展各种分析工作。常用的 MBSA 方法有两种,一是扩充系统模型,在研制过程中使用建模语言捕获系统在正常运行条件下的物理架构和功能结构,即无故障的名义模型,针对安全性分析需求,在该模型的基础上引入失效模式模块和其他额外数据进行扩充;二是直接构建安全性模型,在安全性分析过程中使用建模语言捕获系统架构、失效模式、安全性相关行为及其他额外数据,具体组成模块取决于安全性分析需求。

两种方法均依赖失效的产生和传播过程,基于模型开展安全性分析。其中,失效的产生主要依据 FMEA 和 FMES。失效传播过程如图 1 所示,当组件 1 的输入存在偏差或内部发生故障后,会产生输出偏差,并将偏差传递给组件 2,这种输出偏差也会基于系统架构传播至子系统和系统之外。因此,MBSA 中不仅需要考虑组件内部故障,还需考虑失效的传播。

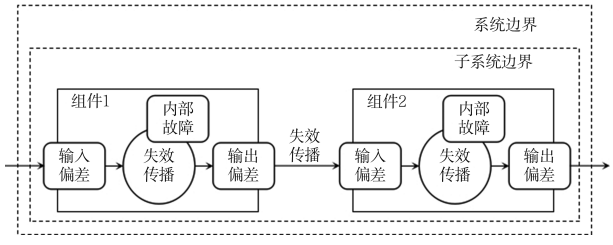

图 1　失效传播过程示意图

参考 SAE ARP4761A 中组件模块示意图,如图 2 所示,MBSA 中组件模块的基本组成元素包括输入、输出、组件内部事件、状态和传递函数。

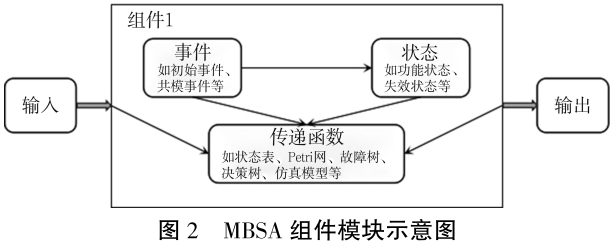

图 2　MBSA 组件模块示意图

综上,基于模型开展安全性工作存在以下优势:(1)安全性模型更接近于真实系统的功能架构和物理结构,从而能够保证系统模型与安全性模型的一致性;(2)基于模型的安全性分析通常采用高级建模语言,比故障树或可靠性框图等布尔形式更有表达力,能够描述备用冗余和共享组件等现象;(3)高级建模支持层级化建模与组件复用,更适合于描述大规模复杂系统;(4)对于带有功能循环和嵌套迭代的复杂系统,因其系统内部包含循环回路,传统的安全性分析方法无法分析,基于建模的安全性分析可以补足该需求[10]。

2　运行失效评估模型定义

1)架构。按照飞机级、系统级和设备级三个层级分别梳理各层级内系统、子系统和设备之间的连接和传递关系,逐层分解,形成模型结构,如图 3 所示。

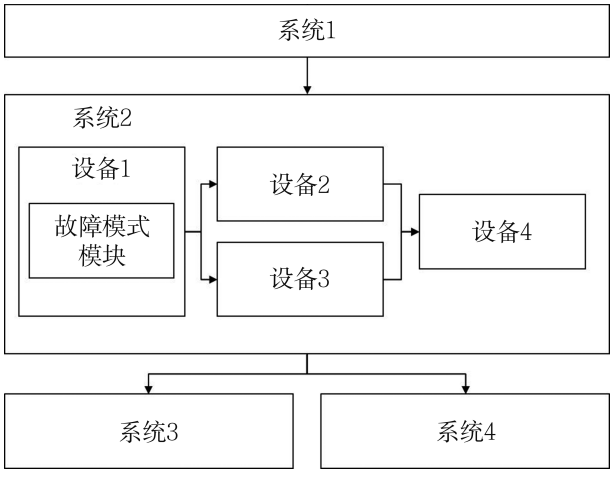

图 3　物理架构示意图

2)组件。运行失效评估模型按总体架构分层管理,可开展独立分析的最小层级为设备级模型。MBSA 基本建模步骤是在状态完好的系统模型中,构建确定故障模式的扩展模型[10]。因此,在设备级模型中设置故障模式模块,对设备的故障模式、故障发生概率以及故障模式对设备动态行为的影响进行分析。

3)接口。接口即连接不同模块的信号线两端的输入和输出接口。在运行失效评估模型中,为了将故障模式模块与设备的功能和性能有机结合,通过接口及其连接关系在模型组件之间传递逻辑值。

4)参数。参数包括两部分:一是模型参数,使仿真模型更接近真实情况的参数设置,如某设备的失效概率。失效概率通过统计分析运营阶段飞机运行数据获得,其余模型参数在系统设计时已经确

定。二是计算参数,便于快速准确地求解计算设置的参数,如仿真步长。计算参数不表征任何系统、设备的特性。

5）模型集成。系统级模型是由设备级模型及故障模块组成的,该系统级模型包含的设备级模型应按系统中各个设备的连接关系相连。同理,飞机级模型由系统级模型连接组成。

3　运行失效评估模型构建

步骤一:参考民用飞机系统的物理组成和功能架构,按层级梳理组成该系统的设备及设备间的连接和传递关系,确定模型的组件和接口。

步骤二:在设备级模型中引入故障模式模块,可根据分析精度要求,对模型的组件进行筛选,如只选择危害等级较高、影响较大的设备引入故障模式模块。

步骤三:选择功能完善、成熟度高的 Simulink 建立运行失效评估模型,按层级分别建模,模型样例如图 4 至图 6 所示。

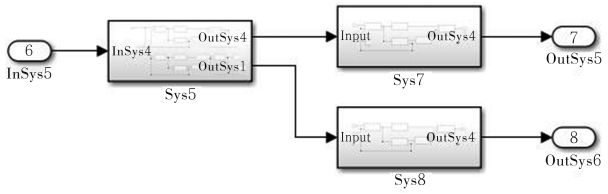

图 4　飞机级模型

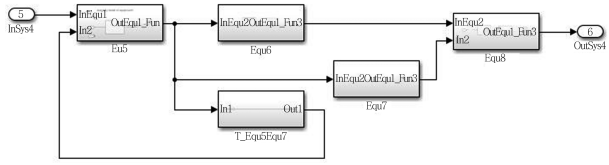

图 5　系统级模型

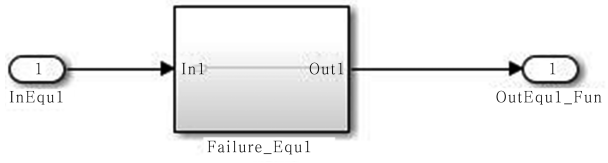

图 6　设备级模型

步骤四:在模型中引入参数,可以依据民机系统设计资料直接给定设计参数,也可以用等效替代的方式模拟参数的含义。对于故障模式模型,基于失效概率参数,采用随机模型等效模拟失效发生,具体方法如下:

记某设备的运行状态和该运行状态的发生概率分别为 FM 和 P,假设随机数 R ~ U[0,1/PR],R ∈Z。对于失效模式 i,有对应的 FMi 和 Pi,则可以假设 Ri ~ U[0,1/Pi],Ri ∈ Z。当 Ri = 0 时,认为该设备所处的运行状态为 FMi;当 Ri > 0 时,可以继续假设 Ri' ~ U[0,1/Pi'],Ri' ∈Z;当 Ri' = 0 时,认为该设备所处的运行状态为 Fmi';当 Ri' > 0 时,依次假设新增随机模块,直至描述了该设备的所有运行状态。假设某个设备存在两种运行模式:正常运行和故障,其故障模式模块如图 7 所示。

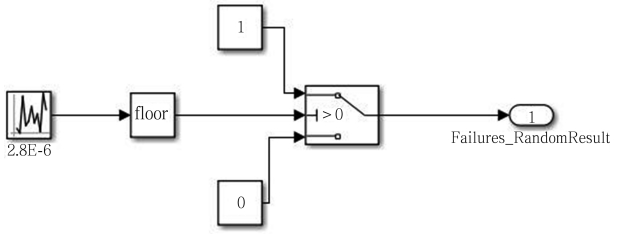

图 7　故障模式模块

步骤五:对模型进行验证,以检验其正确性和可信性。通过与目前较为成熟的故障树等方法进行比较,验证模型计算得到的系统失效发生概率是否正确、误差是否可接受。

步骤六:收集和处理某型号飞机机队在运行中产生的数据集,计算得到设备的各个故障模式发生概率等指标,并将这些指标的计算结果作为参数传入模型中,求解得到系统级和飞机级的指标,并与设计指标进行对比分析,对该型号机队的运行情况进行综合评估。验证时,可以进行多次仿真计算,防止出现偶然误差。

4　算例分析

选取某型飞机外部照明子系统作为典型对象,每个照明灯模块可以归为电源、断路器、继电器、控制器断路器、开关、电源盒和灯这七类组件,连接关系如图 8 所示。

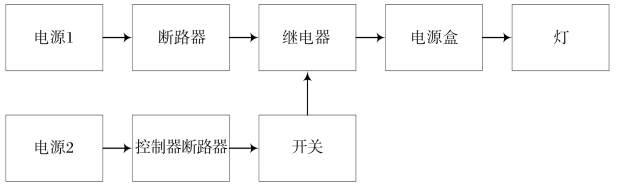

图 8　照明组件连接关系

对外部照明子系统中危害等级在Ⅲ类及以上的设备进行建模分析，包括前起落架着陆灯、前起落架滑行灯、左/右翼根着陆灯和左/右机翼探冰灯等六类组件。按照物理架构和功能架构梳理连接关系和层级关系，并基于 Simulink 搭建仿真模型，如图 9 至图 11 所示。

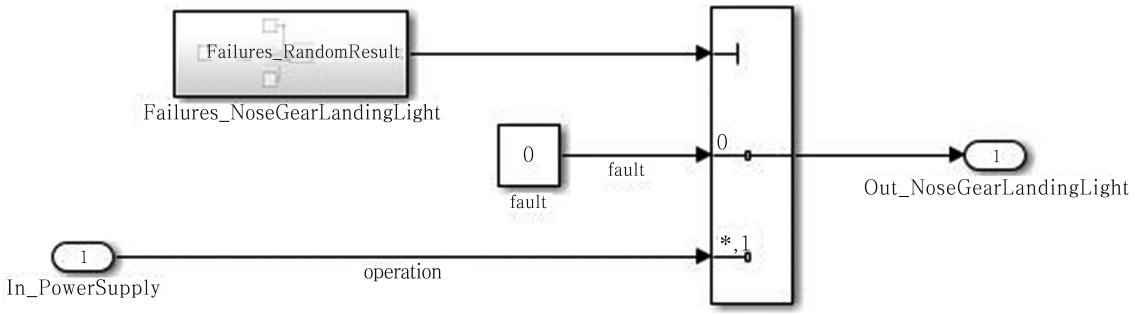

图 9　前起落架着陆灯模型

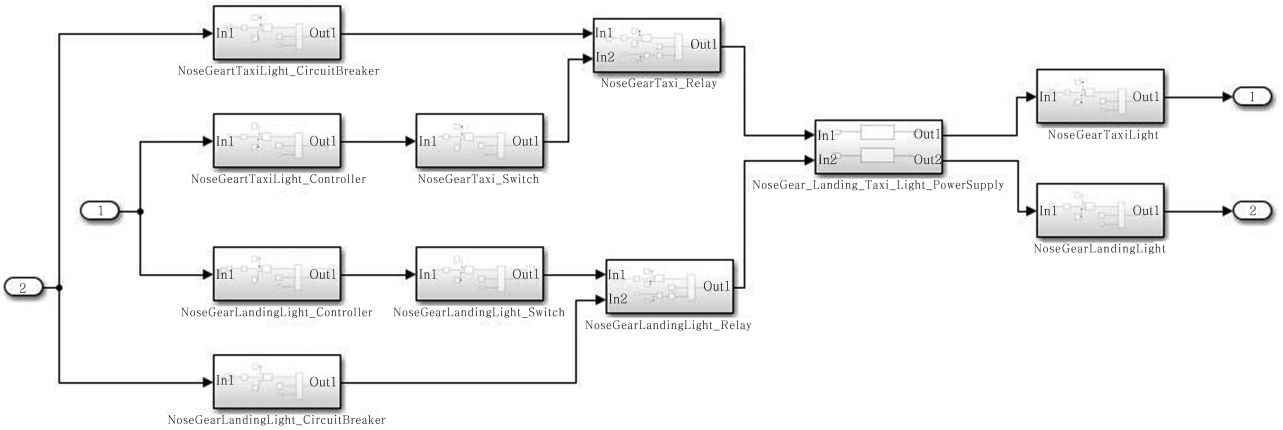

图 10　前起落架降落滑行照明模型

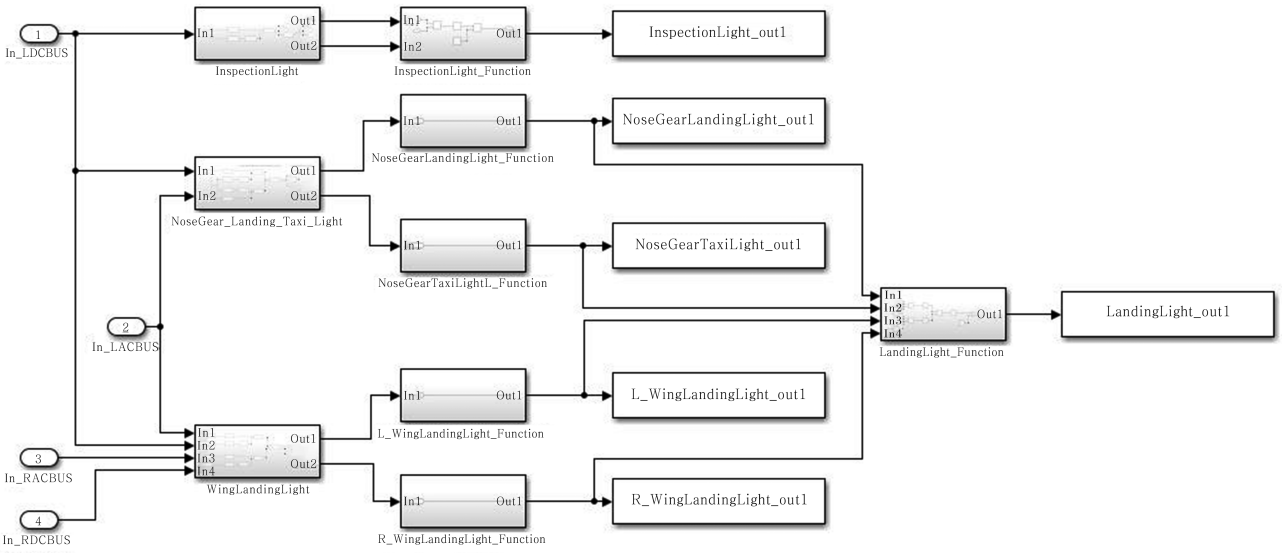

图 11　外部照明子系统模型

考虑到上述模型中 L/R AC BUS 和 L/R DC BUS 组件属于 ATA24 章节电源系统,其余组件为外部照明子系统,属于 ATA33 章节照明系统,为保证模型的完整性,将上述组件分别打包至两个独立的系统模型,如图 12 所示。

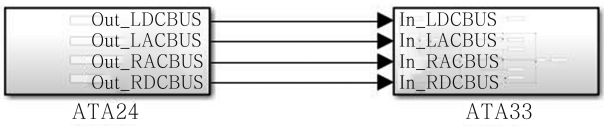

图 12　飞机级模型(ATA24&ATA33)

1) 模型验证

如表 1 所示,外部照明子系统中故障树顶事件包括丧失着陆照明功能和丧失机翼探冰照明功能,发生概率分别为 0.118 9 和 0.251 7(算例中失效发生概率数据量级均为 1×10^{-6},已对数据进行归一化处理)。设置模型求解步长为 0.01 s,仿真时间为 10 000 s,计算丧失着陆照明功能和丧失机翼探冰照明功能的发生概率分别为 0.125 0 和 0.260 7,误差分别为 5.13% 和 3.57%,在可接受的范围。

表 1　基于设计数据的外部照明子系统顶事件发生概率对比(1×10^{-6})

顶事件	发生概率(FTA)	发生概率(simulink)
丧失着陆照明功能	0.118 9	0.125 0
丧失机翼探冰照明功能	0.251 7	0.260 7

2) 运行安全性评估

基于该型号飞机某机队运营阶段飞机运行数据开展算例分析。分析结果如下:

处理和分析该机队运营阶段飞机运行数据,开展外部照明子系统运营阶段 FMEA 分析,得到各设备失效率,如表 2 所示。

表 2　外部照明子系统运行故障模式失效率(1×10^{-6}/h)

故障设备名称	故障模式名称	失效率
前起落架滑行灯	前起落架滑行灯坏灯泡内部故障	0.643 9
左着陆灯	左着陆灯坏灯泡内部故障	0.270 7
右着陆灯	右着陆灯坏灯泡故障	0.270 7

表2(续)

故障设备名称	故障模式名称	失效率
着陆滑行灯电源盒	着陆滑行灯电源盒通道失效电源盒内部故障	0.151 4

依据表 2 中外部照明子系统各设备运营阶段 FMEA 故障模式失效率,取暴露时间为 1.3 h,更新模型中各设备的失效模式及其发生概率。设置步长为 0.01 s,仿真时间为 10 000 s,进行 30 次仿真,得到结果如图 13 和图 14 所示。结果表明,仿真得到的运营阶段外部照明子系统丧失着陆照明功能发生概率约为 0.10~0.18,丧失机翼探冰照明功能发生概率约为 0.23~0.28。总体而言,丧失着陆照明功能发生概率仿真结果略大于设计值,丧失机翼探冰照明功能发生概率仿真结果基本在设计值附近上下波动,均满足安全性要求。

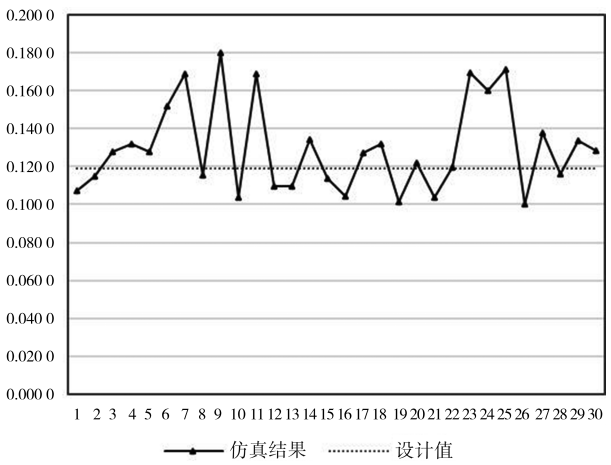

图 13　丧失着陆照明功能发生概率仿真结果

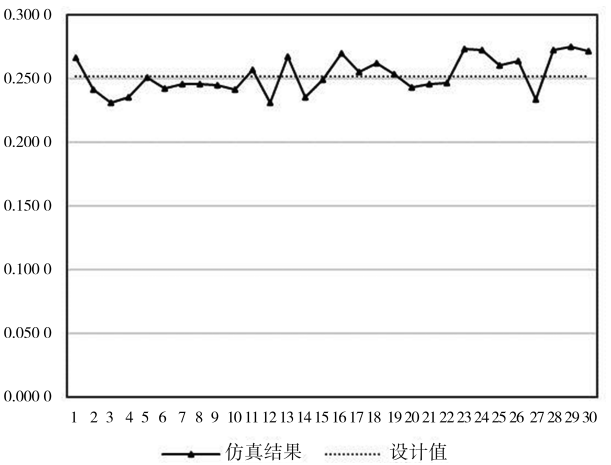

图 14　丧失机翼探冰照明功能发生概率仿真结果

5 结论

MBSA 方法相较传统安全性分析方法更适用于复杂系统。基于 Simulink 开展设备级、系统级和飞机级建模,可以将安全性分析与系统架构结合起来,更加客观和准确地开展安全性分析工作。将故障模式作为单独模块引入设备级模型中,在工程实际中有利于利用已有的安全性分析成果,将故障模式与系统模型重新整合,开展民用飞机运营阶段的失效评估。本文主要基于外部照明子系统开展算例分析,未引入飞控和航电等软件与硬件同时存在、系统架构和设备故障模式更为复杂的建模,后续将重点开展相关方面的研究。

参考文献:

[1] 陈磊, 焦健, 赵延弟. 基于模型的复杂系统安全分析综述[J]. 系统工程与电子技术, 2017, 39(6): 1287-1291.

[2] GOMES A, MOTA A, SAMPAIO A, et al. Systematic model-based safety assessment via probabilistic model checking[C/OL]//MAGARIA T, STEFFEN B. ISoLA 2010: Part I, LNCS 6415. Berlin, Heidelberg: Springer-Verlag, 2010. [2022-04-20]. https://link.springer.com/chapter/10.1007/978-3-642-16558-0_50.

[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.

[4] LISAGOR O, KELLY T, NIU R. Model-based safety assessment: review of the discipline and its challenges[C]//Proceeding Of the 9th international conference on reliability, maintainability and safety. [S. l.: s. n.], 2011: 625-632.

[5] LI Y, GONG Q, SU D. Model-based system safety assessment of aircraft power plant[C]// Proc. Of the 3rd international symposium on aircraft airworthiness: Procedia Engineering, 2014, 80: 85-92.

[6] 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.

[7] 车程, 刘轶斐. 基于模型的安全性分析技术研究[J]. 航空工程进展, 2016, 7(3): 369-373.

[8] 董力. 基于模型的飞行控制系统安全性分析方法研究[D]. 南京: 南京航空航天大学, 2020.

[9] Society of Automotive Engineers International. Guidelines and methods for conducting the safety assessment process on civil airborne systems andequipment: ARP 4761[S]. U. S.: SAE International, 1996.

[10] 徐小杰, 宫綦, 吴洋, 等. 基于模型的初步飞机安全性分析方法研究[J]. 航空科学技术, 2021, 32(11): 64-69.

[11] JOSHI A, HEIMDAHL M P E. Model-based safety analysis of Simulink models using SCADE design verifier[C]//International Conference on Computer Safety. Berlin, Heidelberg: Springer, 2005.

作者简介

马思思 女, 硕士, 工程师。主要研究方向: 航空器运行数据管理。E-mail: masisi@comac.cc

郑勇乐 男, 硕士, 工程师。主要研究方向: 安全性可靠性设计与数据管理。E-mail: zhengyongle@comac.cc

马 彪 男, 硕士, 高级工程师。主要研究方向: 安全性可靠性设计与数据管理。E-mail: mabiao@comac.cc

Model-based failure assessment method of civil aircraft operation phase

MA Sisi *　ZHENG Yongle　MA Biao

(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: The model-based safety analysis (MBSA) has become increasingly mature since its inception and is more suitable for complex civil aircraft systems. On the basis of current research and ARP4761A draft, the MBSA method is used to study the failure assessment method of civil aircraft during the operation phase. Compared to traditional methods, integrating operational data, functional failures, and equipment failures into the same model is more convenient for conducting operational failure assessment. Firstly, this paper defines the basic elements of the operational failure assessment model and sorts out the model construction process, and establishes equipment level, system level, and aircraft level models containing failure modules based on Simulink. The external lighting sub-system of a certain aircraft model was taken as an example to build the model, and a numerical analysis was conducted on the operational data of a certain fleet. The results show that the the error between MBSA and FTA results is within an acceptable range. At the same time, the FMEA analysis was performed, and the probability of loss of landing lighting function hazard was calculated and simulated using operational data. 30 simulation results indicate that the probability of occurrence based on operational data fluctuates around the design value, slightly exceeding the overall design value, but still meeting the safety requirements.

Keywords: MBSA; operational failure; simulink; aircraft system; external lighting subsystem

* Corresponding author. E-mail: masisi@comac.cc