民用飞机系统安全性分析中EWIS部件的考虑

Safety Analysis of EWIS System for Civil Aircraft

郑建／中国商飞上海飞机设计研究院

摘 要：通过对适航规章25.1709的分析，结合AC 25.1701，提出了民用飞机系统安全性分析中需考虑EWIS部件的一些方面，并初步研究了具体的分析方法。

Abstract：Based on the analysis of airworthiness regulation 25.1709 and AC 25.1701, this paper provides the considerations of EWIS components in the system safety analysis of civil aircraft, and preliminarily researches the analysis method.

关键词：电气线路互联系统；系统安全性；适航规章；符合性验证

Keywords：EWIS；system safety；airworthiness regulation；compliance verification

0 引言

电气线路互联系统(EWIS)是指任何导线、线路装置，或者其组合，包括端点装置，安装于飞机的任何部位用于两个或多个端点之间传输电能(包括数据和信号)。

美国联邦航空局(FAA)在2007年发布的运输类飞机适航规章(FAR 25部)123号修正案[1]中，正式提出了EWIS的概念及相应的规章要求。中国民用航空局(CAAC)在2011年发布的中国民用航空规章第25部运输类适航标准(CCAR25部)R4版[2]中，也提出了EWIS相关的规章要求。

系统安全性分析作为民用飞机研制和适航审定过程中的一项重要工作，为了满足EWIS相关的适航规章要求，需要对分析方法进行一定的调整。

1 适航规章要求及解析

CCAR25.1709和FAR 25.1709均要求每个EWIS的设计和安装必须使得灾难级失效状态是极不可能的且不会因单个失效而引起，并且每个危险失效状态是极微小的。

咨询通告AC 25.1701[3]对25.1709规章的制定背景进行了进一步的解析。制定25.1709规章，一是因为25.1309规章主要覆盖系统和设备，没有考虑EWIS部件的影响；二是因为EWIS设计的集成特性和EWIS部件失效的严重性，如导线的电弧故障可能会导致着火，需要采用比表明对25.1309规章要

的昏暗度数据，图中虚线为设定的烟雾探测器报警触发的昏暗度极限值。

表1为FDS5模拟得到的4个烟雾探测器报警触发的时间。

模拟结果显示，距离火源较近的烟雾探测器2和烟雾探测器3在13.7s和15s先后触发报警。距离火源较远的烟雾探测器1和烟雾探测器4在39.2s和37.6s也先后触发报警。根据烟雾探测系统的设计，有两个烟雾探测器报警触发时系统认为出现烟雾状况，即在烟雾探测器2和烟雾探测器3报警触发后，飞机烟雾探测系统即判定货舱出现烟雾并通知飞行员执行关闭货舱通风和货舱灭火操作，此时距离烟雾开始出现的时间约为16s左右，满足FAA适航规章中的1min内报警的要求。 AST

参考文献

[1] 李萍.火灾动态模拟器FDS软件介绍[J].高性能计算发展与应用.2009，(1)：63－66.

[2] Ezgi Öztekin. Smoke transport in a cargo compartment[R] .Koeln, Germany: International Aircraft Systems Fire Protection Working Group, 2011.

[3] Fire Dynamics Simulator (Version 5) User's Guide[K]. National Institute of Standards and Technology, 2010.

作者简介

程书山，硕士研究生，助理工程师，研究方向为大型客机防火系统。

表1 失效状态对应的安全性要求

危害等级	灾难级	危险级	较大的	较小的	无安全性影响
定量安全性要求	小于10^{-9}每飞行小时	小于10^{-7}每飞行小时	小于10^{-5}每飞行小时	小于10^{-3}每飞行小时	无
定性安全性要求	极不可能：在同机型所有飞机的整个运营寿命周期内不可能发生	极微小的：在飞机的整个寿命内、在单架飞机上非预期发生，但当考虑这一机型所有飞机的总的运营寿命时，可能会发生很少几次	微小的：在飞机的整个寿命内、在单架飞机上不太可能发生的，但当考虑这一机型中一定数量的飞机的总的运营寿命时，可能会发生几次	可能的：预期在单架飞机的整个使用寿命内发生一次或者几次	无

求符合性的传统安全性分析方法更为结构化的分析方法。

25.1709规章的具体要求与25.1309规章保持了一致性，不同等级的失效状态对应的定性和定量安全性要求如表1所示。

2 系统中EWIS（部件）的安全性分析

AC 25.1709建议从物理失效和功能失效两个方面进行EWIS的安全性分析。

物理失效分析中，主要分析带电的EWIS部件故障，并结合考虑其周围燃油、氧气、液压油等因素的情况下，产生的着火、冒烟或有毒气体对周围系统、结构或者人员的影响。需考虑飞机上所有系统的EWIS部件。EWIS的物理失效分析主要以飞机级功能危险性评估为输入，在飞机级层面开展。

功能失效分析中，主要分析EWIS部件的功能失效对所属系统安全性水平的影响。由于EWIS部件通常不独立具备系统级功能，并且在CCAR25部和FAR25部中均要求系统在进行符合性验证的过程中，需考虑与系统相关的EWIS部件的影响。因此，对EWIS部件的功能失效分析，宜作为所属系统安全性评估的一部分来开展。

3 系统安全性分析流程和方法

系统的安全性分析，贯穿于整个系统研制过程，通常划分为安全性要求定义、系统架构检查和安全性要求分配，以及安全性要求验证等三个阶段，其中涉及到EWIS部件的主要为后两个阶段。图1所示为系统安全性评估流程与系统研制流程的关系。

系统安全性评估过程中应用的分析和评估工具、方法主要包括：功能危险性评估(FHA)、初步系统安全性评估(PSSA)、共因分析(CCA)、系统安全性评估(SSA)、失效模式影响分析(FMEA)和故障树分析(FTA)等，这些工具和方法的详细描述可参见SAE ARP 4761[4]。

3.1 安全性要求定义

系统的安全性要求定义，以系统FHA的形式开展，FHA中检查和分析系统功能，确定系统的潜在功能失效，并根据功能失效对飞机、机组和乘员的影响进行分类，进而得出系统级的安全性要求。

3.2 系统架构检查和安全性要求分配

系统架构检查和安全性要求分配阶段，通过进行PSSA对建议的系统架构进行检查，评估系统架构设计能否满足FHA中定义的安全性要求，并将系统级安全性

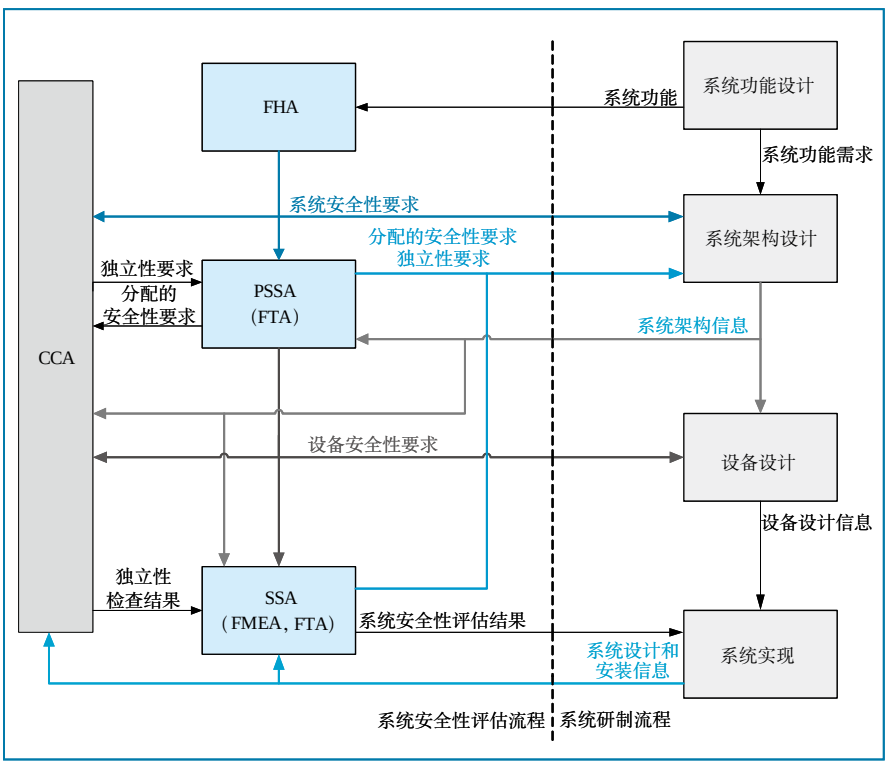

图1 系统安全性评估流程与研制流程的关系

要求分配到子系统级和设备级。PSSA过程中主要应用FTA这一分析工具。

在PSSA中应考虑系统中EWIS部件的影响，具体来说，应将EWIS部件的失效加入故障树分析中，检查系统架构设计能否满足定义的安全性要求。由于飞机EWIS设计通常滞后于系统设计，在这一阶段EWIS设计通常还处于电气原理图设计阶段，而EWIS部件的失效概率与部件本身、安装方式及工作环境均有一定的关系，因而在这一阶段还无法分析出每个EWIS部件的准确失效概率。

为此，可以基于相似机型的经验数据，初步确定EWIS部件失效概率的假设值，并加入系统故障树分析中。假设值应随着系统EWIS设计的深入，随系统PSSA文件的换版而进行迭代更新，以更准确地评估EWIS部件功能失效对系统安全性水平的影响，并在必要时对系统设计和EWIS设计进行优化。选取假设值时，可基于EWIS部件在端点之间传输电能、数据和信号这一功能进行失效概率的假设，而不是关注每个具体的EWIS部件。例如，在设备A和设备B之间传输某个信号，至少需经过设备A连接器、设备B连接器和连接导线等三个EWIS部件，如果对这三个部件分别假设概率值，容易带来假设值偏差大、故障树分析中底事件过多的问题。针对这种情况，可以设定“EWIS部件故障导致设备A和设备B之间某个信号传输失效”的失效概率假设值，该失效概率可以包含所有用于支持该信号传输的EWIS部件的故障，以简化分析。失效概率假设值的选取，应略为保守，以避免因为没有充分考虑EWIS部件的失效影响，在后期发现系统设计不能满足安全性要求而带来的系统设计更改。

在这一阶段还需进行系统共因分析(CCA)，得出系统内的冗余通道，及通道所属设备、部件（包括EWIS部件）的相互隔离要求。

3.3 安全性要求验证

安全性要求验证阶段，通过进行系统安全性评估和共因分析，对系统设计和安装进行全面检查，评估系统设计和安装能否满足系统安全性要求和相关适航规章要求。

SSA中应用的分析工具主要包括FMEA和FTA，此外，系统共因分析的结论也要作为SSA结论的一部分，用于支持系统的安全性要求验证。

系统FMEA是对系统中的设备和部件进行分析，分析其各种故障模式的影响、指示以及发生概率。为了满足25.1709规章的要求，FMEA中应考虑系统EWIS部件的失效模式，检查是否存在可能导致灾难级失效状态的单点故障。

系统FTA是对系统的组合故障进行分析，计算得出FHA中定义的失效状态（主要针对灾难的、危险的和较大的失效状态）的发生概率，并将其与规定的定量概率要求进行对比，判断是否满足定量概率要求。为了满足25.1709规章的要求，FTA中应考虑系统中所有EWIS部件的失效模式影响，将其作为故障树底事件进行分析。

系统共因分析(CCA)包括共模分析(CMA)、区域安全性分析(ZSA)和特定风险分析(PRA)等三方面的内容。

CMA用于证明“系统架构检查和安全性要求分配”阶段分配的独立性和冗余要求在系统设计中得到了贯彻，从而表明系统故障树分析中“与门”间独立性的真实存在，进而支持系统安全性评估。CMA中需要考虑系统共用的连接器、共用的接插件、共用的接地点等EWIS共用器件，分析这些共用器件失效的影响。

ZSA根据飞机区域划分，逐个区域分析潜在危险源对系统设备和部件（包括EWIS部件）的影响，以证明系统的设备和部件安装可以满足相关安全性要求。

PRA则是分析一些特定风险项，如非包容性发动机转子爆破、鸟撞等对系统设备和部件（包括EWIS部件）的影响，以证明系统的设备和部件安装可以满足相关安全性要求。通过CCA应能证明在考虑了全部系统设备和部件（包括EWIS部件），以及系统的内外部风险后，不存在可能导致灾难级失效的单点故障，并且可能导致危险级失效状态的故障的发生风险也处于可接受的范围。

4 结论

EWIS部件的失效对系统安全性的影响越来越受到公众、适航审查方以及飞机制造方的关注。本文初步研究了如何在系统安全性评估中考虑EWIS部件的影响，探讨了如何表明系统中EWIS部件的设计对25.1709规章的符合性。

AST

参考文献

[1] FAA. FAR Part 25 airworthiness standards: transport category airplanes [S].

[2] 中国民用航空局.中国民用航空规章第25部：运输类飞机适航标准[S].

[3] FAA. AC25.1701−1 certification of electrical wiring interconnection systems on transport category airplanes [Z].

[4] SAE. SAEARP 4761 guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment [S]. 1996.

作者简介

郑建，硕士，工程师，主要研究方向为民用飞机电源系统设计、系统安全性评估和适航符合性验证。