

初探民用飞机EWIS安全评估

Preliminary Study on Civil Aircraft EWIS Safety Assessment

柳丛 / 上海飞机设计研究院

摘要: 结合EWIS自身的特征, 提供安全评估的基本思路, 着重对EWIS安全性适航条款 § 25.1709进行分析与理解, 介绍了目前常用的五种安全评估分析方法, 并简要介绍了EWIS安全分析中输入数据常用的获取途径。

关键词: EWIS; 适航条款; 安全评估; 评估方法

Keywords: EWIS; airworthiness standards; safety assessment; assessment methods

0 引言

20世纪, 电气线路互联系统(EWIS)在航空安全中的重要性被逐渐认识, 但是一直没有就如何在航空安全评估中对EWIS进行分析达成一致看法。众所周之, 线路物理上的故障不但会引起飞机系统的损坏, 还可能引燃线路附近的可燃性材料, 甚至导致飞行终止、偏航、诱发航空灾难。随着飞机逐步向多电和全电飞机方向发展, 布线对于飞机各个系统来讲显得非常重要。鉴于由电气布线引起的飞行安全问题越来越多, 为了弥补适航条款 § 25.1309关于系统设计与分析在布线系统安全性方面的不足, 美国联邦航空局(FAA)颁布了新的条款, 将EWIS作为新的系统予以要求。2007年11月8日, FAA正式将EWIS列入25部并成立一个新的H分部, 强调了运输类飞机电气线路的设计、安装和维护的各个方面, 旨在使航空公司远离导线失效、烟雾和火灾引起的风险。H分部的条款极大地增强了已有和在研民用飞机电气布线设计、安装和维护方面的安全性要求。

1 EWIS安全评估思路

老龄飞机系统法制咨询委员会

(ATSRAC)通过调查发现, 典型的EWIS故障模式主要表现在导线或线束的磨损、未指明的短路、导线损坏和连接器故障等几方面, 如图1所示, 其中导线或线束的磨损是EWIS最普遍的故障形式。显而易见, 机龄越老, EWIS发生故障的可能性就越大。

§ 25.1701中定义, 任何EWIS元器件或组件存在缺陷或发生损坏, 在外部环境和人为因素的影响下, 有可能并不影响系统或飞机的正常工作, 也有可能也会导致某种元器件级或系统级的故障。故障发生后, 如果外部环境和人为因素不断减弱, 故障有可能仍然不会影响到系统或飞机的持续正常运行; 如果外部环境和人为因素不断加重, 有可能导致系统或子系统的功能

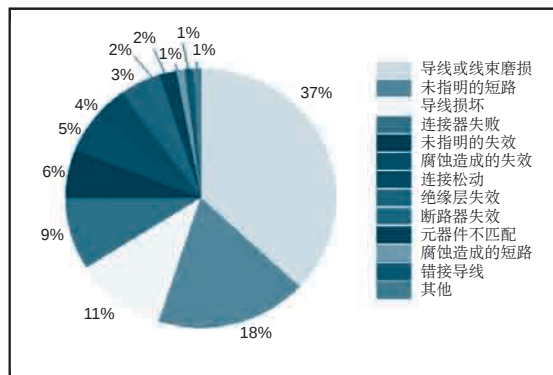


图1 EWIS的典型故障模式

失效, 甚至直接导致较小的、重大的、危险的/极其重大的以及灾难性的等四种后果。这一安全评估分析过程如图2所示。以导线绝缘层开裂损坏为例, 在干燥、无腐蚀性的环境下, 即使线路对地产生火花使系统工作不正常, 也不一定影响系统安全和飞机安全; 但在腐蚀和潮湿的环境下线路对地产生火花, 有可能导致飞机出现四种不同程度的后果。

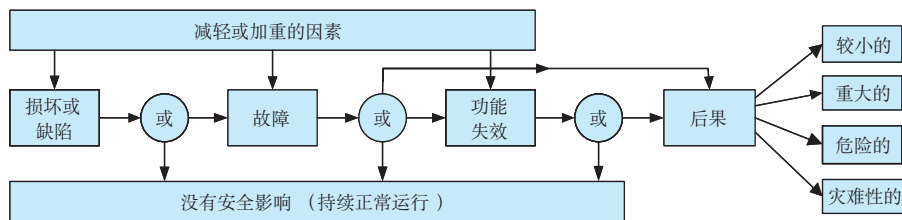


图2 EWIS安全评估基本思路

2 § 25.1709适航条款分析与理解

在FAR 25部 § 25.1309条款的要求下,系统安全性评估(SSA)和功能危险性评估(FHA)没有脱离系统而对机载关键系统的导线(或线束)独立进行评估。因此,SSA和FHA并不适用于EWIS及其相关的元器件。而且,该条款基于整个飞机级的定量安全性指标每飞行小时 1×10^{-9} 灾难级的失效。实际中,安全目标的实现是通过确定性要求如单故障准则、故障-安全设计以及应用于某一系统或某种功能的定量可靠性要求的组合来实现的,如假设单个系统可靠性低于指标值,那么实现关键功能的系统必须是冗余的。

虽然 § 25.1309条款已经对设备、系统及安装提出了安全性方面的要求,但是其要求并不能确保所有影响飞机安全的EWIS失效状态得到分析,这是因为 § 25.1309(a)只覆盖子章节中的系统和设备,对于未提及的系统布线有时会被忽略。 § 25.1309(b)和(d)条所覆盖的系统,其安全分析要求也并不总适用于相关系统的导线。传统观念认为,既然条款

对于某些非关键系统如机载娱乐系统并未限制和要求,因此它们提供的功能对于飞机安全就不是必要的,该系统的线路也没有必要进行安全分析。事实上,即使是一根传输电能或信号的导线失效,无论该导线是否与系统相连,都可能引起飞机严重的物理和功能损害,导致危险性甚至是灾难性失效状态。例如,导线短路的电弧会切断或损害飞控电缆;电弧发生但是断路器未跳闸,有可能导致线路失效甚至是火灾。因此, § 25.1709就是在 § 25.1309概念的基础上,对飞机布线及其标准件提供一个更全面和更结构化的分析,弥补 § 25.1309在EWIS安全评估方面的不足。

§ 25.1709条款(a)对灾难性失效状态予以强调说明,提出了明确的概率要求,即极度不可能出现灾难性失效状态;而且强调单个失效对飞机造成的影响有限。失效是影响某一元器件、零件或元素运行,使其无法按照预定目的(包括功能丧失和功能不正常)工作的事件。对于EWIS而言,物理失效考虑的因素包括不同线路的间距、隔离等,功能失效考虑的因素如导线的电磁干扰

和线路的冗余设计等,这些因素都必须在设计中予以考虑。 § 25.1709条款(b)提到了另一种失效状态“危险”,并对其提出了明确的概率要求,即极小。

根据 § 25.1709的条款要求和AC 25.1709的说明,失效状态按照严重性程度可分为没有安全影响、较小的、重大的、危险的/极其重大的和灾难性的影响。这五种失效状态对飞机、机组人员、乘客和客舱乘务人员的影响以及它们的定性、定量概率如表1所示。

3 安全评估分析方法介绍

3.1 失效模式与影响分析(FMEA)

基于可靠性理论,所有元器件都有其固有的失效模式。采用FMEA这种定性/定量分析工具,评估每一个元器件失效模式的影响,从而确定其对系统安全性的影响,其分析过程如图3所示。对于EWIS而言,可从线路和互联器件两大方面进行考虑,根据机械、电气和化学方面对失效的影响进行分类,列出每一种失效模式的影响及其可能产生后果的严重性,再将每一失效的发生率与检测到的发生率相乘,计算出风险优

表1 失效状态严重性分类

失效状态严重性分类 影响方面		没有安全影响 No Safety Effect	较小的 Minor	重大的 Major	危险的/及其重大的 Hazardous	灾难性的 Catastrophic
失效状态影响	飞机	无安全影响	轻微降低安全余度和功能	明显降低安全余度和功能	大幅降低安全余度和功能	机体受到损害
	机组人员	无影响	轻微增加工作量,例如日常飞行计划变更	明显增加机组人员工作量,或严重影响机组人员的工作效率	身体上痛苦和过度的工作量使机组人员无法精确和完整地完成任务	致命
	乘客或客舱乘务人员	无影响	身体不适	身体痛苦,甚至受伤	相对少部分人产生严重或致命的伤害	大多数致命
概率要求		无要求	可能 Probable	不可能 Improbable		
				较小可能的 Remote	极小可能的 Extremely Remote	极不可能的 Extremely Improbable
定性概率描述		无要求	在每架飞机的全寿命期内会发生一次或几次	很多飞机的全寿命期内会发生几次	在单架飞机的全寿命期内预计不会发生,但是对于同类型所有飞机的全寿命期而言会发生数次	在某种类型所有飞机的总运行寿命期内预计都不会发生
定量概率		无要求	$< 10^{-3}$	$< 10^{-5}$	$< 10^{-7}$	$< 10^{-9}$

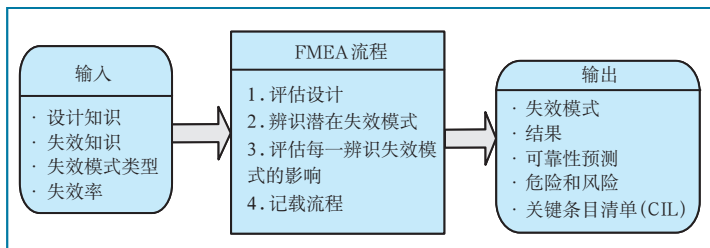


图3 FMEA分析过程

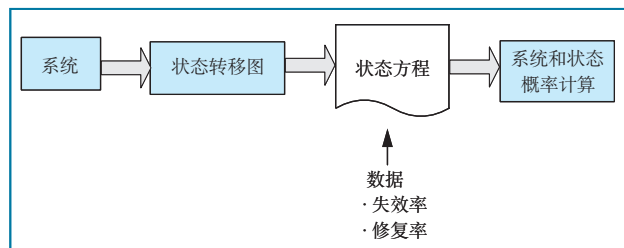


图4 MA分析过程

先发生次数(RPN),最后考虑在失效模式对子系统和系统产生安全影响前,通过采取何种措施或方法将失效的影响减至最低或避免。

3.2 共因分析(CCA)

1) 区域安全性分析(ZSA)

ZSA是对飞机上人为划定的每一区域,考虑系统或设备安全、维修失误、外部环境变化、系统运行等情况而进行的安全性分析。飞机上的区域一般根据其用途、压力、温度范围,是否属于暴露区和风险区来划分,不同区域的设备安装要求不同。ZSA不仅包括对设备安装是否满足安装规范的验证,也包含设备间导线、电缆和管路是否满足隔离要求的验证。

2) 特定风险分析(PRA)

特定风险是指处于所分析的系统或产品之外,但可能破坏该系统功能或引起故障的独立性事件或影响,如火灾、鸟撞、轮胎爆破、闪电、高强度辐射场等。特定风险可能同时对若干区域造成影响,而ZSA只分别针对每一个区域进行。因此在全机线路主通道设计阶段就应考虑PRA项目及其影响范围。

3) 共模分析(CMA)

共模分析主要针对具有相同模式的元器件失效的分析。共模失效的原因可分为五大类,包括外部正常环境如温度、湿度;设备设计缺陷;运行和维护差错,如粗心或违规操作;外部自然因素如地震、海啸;功能缺陷等。通过分类,安全性或可靠性工程师能够以系统的

方式着重分析同种模式失效的可能性并思考某一时间其发生的潜在诱因。

3.3 故障树分析(FTA)

故障树分析是一种识别、建模和评估可导致失效、不希望事件或状态以及意外事件或状态的独特事件内部关系的方法。该方法自顶向下通过布尔代数将一系列低级别事件或状态组合,分析失效或事件对于复杂系统的影响。与FMEA的不同在于,FMEA是自底向上分析单个元器件或功能失效对于设备或子系统影响的方法。FTA不善于找出所有可能的初始故障,FMEA却善于将初始故障归类,并识别出其在当时的影响,但却不善于检查多个失效及这些失效对某一系统级的影响。民用航空领域通常将失效模式影响总结(FMES)作为FMEA与FTA的接口。

3.4 马尔可夫分析(MA)

马尔可夫分析是一种描述系统状态转移并计算模型中到达各种系统状态概率的分析方法。这种工具用于复杂系统的设计中,包括用时、序列、修复、冗余和故障容差等,提供图形和数学(概率)系统的模型。图4描述了整个MA过程,已知某个系统,观察系统状态变化得到该系统的状态转移图,根据状态转移图和失效率、修复率数据列出状态方程,它的解可通过任一状态包括最终故障状态的时间概率得到。MA比FTA更为复杂,对于失效率/修复率依赖状态的系统、可修复系统以及其他潜在的失效都能够进行考虑和分析。

3.5 关联图分析(DD)

关联图分析方法是一种进行概率分析的故障组合的图形表示。FTA和DD的根本区别在于,DD没有额外的逻辑符号,它通过连续的或并行的方框布局来表示逻辑性,且不显示作为FTA中逻辑符号输出描述的中间事件。DD的分析类似于FTA,因此二者在安全评估分析中的角色也类似。

3.6 评估方法的输入数据

任何评估方法都离不开数据的支持,目前广泛运用的获取数据的方法有视觉检查、推荐措施或维修手册、实验室测试、通过仪器检查等。对于EWIS而言,一般视觉检查(GVI)、区域检查(ZI)和细节检查(DI)三种方法值得推荐。

GVI是对飞机内部或外部区域、安装或组件进行检查,以发现明显的损坏、失效和不规律现象。这一级的检查通常在正常光源下进行,如自然光、手电筒等。为了便于接近检查区域,有时需要移动或打开口盖或盖板,梯子、升降台等也是必不可少的。这种方法还允许使用反射镜,以便检查所有需要检查的表面。

ZI是针对飞机上每一区域(由可达难易程度和位置来划分区域)进行的GVI和视觉校对,从安全角度对系统和电源设备的安装和结构进行检查。

DI是对特定条目、安装或组件损坏、失效和不规律现象进行的深度检查,所需光源应除正常光源外,还需一种直接的具有一定亮度的光源辅助,可

民用飞机EWIS隔离设计

EWIS Separation of Civil Aircraft

王怡华 / 上海飞机设计研究院

摘要:通过对适航规章的分析,提出了民用飞机EWIS部件,尤其是电线电缆的隔离原则,制定了隔离方案并介绍了常用的隔离保护物,以达到保护EWIS部件,使其稳定长期地工作,从而保证飞行安全的目的。

关键词: 电气线路互联系统; 隔离; 防护; 适航; 安全性

Keywords: EWIS; separation; protection; airworthiness; safety

0 引言

民用飞机电气线路互联系统(EWIS)是否能安全地传输电能,关乎飞机的持续安全运行。发生EWIS故障时,EWIS部件与其他EWIS部件、系统或结构之间的分离对确保将故障后果降低至可接受水平至关重要。

能还需要反射镜、放大镜或其他方法进行辅助检查,有时需要检查表面清洁,且检查步骤精细。DI与GVI最大的不同是允许触觉检查。

4 结论

EWIS是一个复杂的系统,它高度集中,使用多种大量的元器件,是飞机上最后一个被综合的系统,具有高度的构型项,在生产方面也有高峰期。针对如此复杂的系统,如何深入理解适航条款对EWIS安全的要求,用何种安全评估方法可以更全面和准确地对EWIS失效模式进行评估并获得所需数据,是今后我国民用飞机EWIS设计与安全分析中值得研究和深入探讨的方向。

AST

参考文献

[1] Clifton A Ericson II. Hazard

1 EWIS隔离的规章要求

CCAR-25R4的§ 25.1707条款对EWIS的隔离提出了适航要求^[1]。其中,25.1707(a)款是EWIS设计、安装的通用规范要求,定义了系统分离的目的和方法。

纵观25.1707条款要求,EWIS系统隔离按对象可分为与其他系统部件的

隔离以及EWIS系统内部线束之间的隔离,按性质可分为功能隔离和物理损害隔离,按方法可分为通过距离分离和通过等效距离保护隔离。

25.1707(e)、(f)、(g)、(h)、(i)、(j)和(l)款提出了EWIS与其他系统之间的具体隔离要求。需要考虑的系统包括:燃油

analysis techniques for system safety[M]. John Wiley & Sons, Inc.,2005.

[2] Gangloff W C. Common mode failure analysis[J]. Power apparatus and systems, IEEE Transactions on ,1975, 94 (1):27-30.

[3] Press V L, Bruning A M. Advanced Risk Assessment Methods for Aircraft EWIS[C]. 6th Joint FAA/DoD/NASA Conference on Aging Aircraft, 2002.

[4] SAE ARP 4761 Guidelines & Methods for conducting the safety assessment process on civil airborne systems and equipment[Z].1996.

[5] Moffat B G, Abraham E, Desmullies M P Y, Koltsov D, Richardson A. Failure mechanisms of legacy aircraft wiring and interconnects[J]. IEEE Transactions on Dielectrics and Electrical

Insulation, 2008, 15(3):808-822.

[6] SAE ARP 4754 guidelines for development of civil aircraft and systems[Z]. 1996.

[7] FAR Part 25 Airworthiness Standards[S]. Transport Category Airplanes, FAA.

[8] Development of an Electrical Wire Interconnect System Risk Assessment Tool[Z]. FAA. 2006.

[9] AC 25.1309-1A system design and analysis[Z].

[10] AC 25.1701-1 Certification of Electrical Wiring Interconnection Systems on Transport Category Airplane[Z].

作者简介

柳丛,硕士,助理工程师,设计员,主要研究方向为EWIS系统架构和系统安全分析。