

民用飞机飞控电子设备托架风扇安全性需求分析

田亮*, 张新慧

中航飞机股份有限公司研发中心, 陕西 西安 710089

摘 要: 针对某民用飞机飞控电子设备通风方式, 结合其飞控系统架构, 从系统安全性角度出发对托架风扇的故障组合进行全面考虑和功能安全性评估。通过建立故障树的形式分别对 I 类和 II 类事件进行定量分析, 并将对应的安全性设计目标转化为托架风扇的安全性设计需求, 给出了托架风扇的平均故障间隔时间, 同时基于 ARP4761 对托架风扇的安全性进行共模考虑和分析, 解决了托架风扇的共模问题。

关键词: 托架风扇; 安全性需求; 故障树; 共模故障

中图分类号: V249.12 文献标识码: A 文章编号: 1007-5453 (2016) 12-0034-04

某型飞机总体规定左右电子设备柜中的电子设备应采用 ARINC600^[1] 设计标准, 使其能在有限空间内实现紧凑布置。根据 ARINC600 设计标准, 对于 SMCU 的电子设备, 若其热功耗超过 17W 时应进行强迫通风, 而该飞机飞控电子设备热功耗均在 70W 以上, 因此, 应对飞控系统电子设备进行强迫通风设计。

目前, 国内外民用飞机电子设备强迫通风方式主要是在电子设备托架底部安装风管, 在电子设备的下面设计通风孔进行强迫通风, 如 B787、A380 及 C919 等飞机均采用该形式。但由于某型飞机电子设备柜空间比较紧张, 设备安装紧密, 无法在飞控电子设备托架底部安装风管进行强迫通风。经评估和决策, 最终确定采用托架带风扇的形式对其进行强迫通风。

风扇的设计涉及诸多因素, 如风扇接口形式、送风温度需求、风流量需求、电子设备流阻特性、维修性需求、安全性需求等, 其中最关键的参数则是安全性需求。

当风扇发生故障时, 系统无法感知, 是一隐性故障, 只能在 A 检或 C 检中发现。此外, 飞控电子设备在风扇发生故障时不会立即失效, 它能在 55~70℃ 环境温度中工作

30min, 当环境温度超过 70℃ 时会立即发生故障而停止工作。因此, 风扇故障最终导致电子设备因过热而失效, 而电子设备发生故障则导致系统功能丧失从而对飞机产生不利影响。

为了避免电子设备因过热而发生故障, 有必要对其托架风扇的安全性需求进行分析, 以确保飞控系统、飞机舵面正常工作。

1 飞控系统架构

对于方案设计阶段, 为明确托架风扇的安全性需求, 通常采用的方法主要是初步系统安全性评估^[2] (PSSA)。初步系统安全性评估则是在系统功能危害评估 (FHA) 和系统架构基础上进行。

某型飞机驾驶舱左右电子设备柜中布置有 4 台飞控电子设备, 每台电子设备各有一个风扇对其强迫通风, 电子设备具体尺寸和热功耗如表 1 所示, 飞控系统 (FCS) 架构如图 1 所示。其中每台飞控计算机 (FCC) 将飞行控制模块 (FCM) 和作动器控制模块 (ACM) 集成在同一机箱内。

收稿日期: 2016-05-25; 退修日期: 2016-07-19; 录用日期: 2016-07-20

* 通讯作者. Tel.: 029-86832428 E-mail: crackhooker@163.com

引用格式: TIAN Liang, ZHANG Xinhui. Safety requirements analysis for tray fan used for civil aircraft flight control electronic equipment [J]. Aeronautical Science & Technology, 2016, 27 (12): 34-37. 田亮, 张新慧. 民用飞机飞控电子设备托架风扇安全性需求分析 [J]. 航空科学技术, 2016, 27 (12): 34-37.

表 1 飞控系统电子设备信息
Table 1 FCS electronic equipments information

安装位置	设备名称	数量	尺寸 /MCU	热功耗 /W
左电子设备柜	作动器控制器 1 (ACE1)	1	5	70
	飞控计算机 1 (FCC1)	1	5	85
右电子设备柜	作动器控制器 2 (ACE2)	1	5	70
	飞控计算机 2 (FCC2)	1	5	85

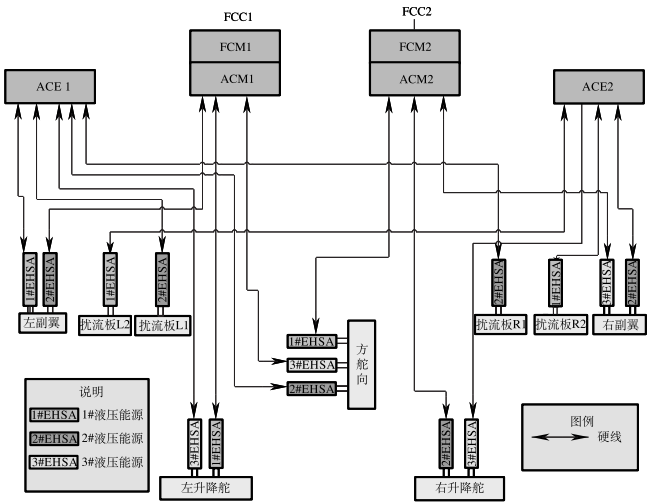


图 1 飞控系统架构图
Fig.1 Flight control system architecture

2 托架风扇故障组合及安全性分析

每台飞控电子设备各由一台风扇对其进行通风,因此需分别考虑和评估飞行中单台风扇故障、两台风扇故障和三台风扇故障最终对飞控系统和飞机产生的安全性影响。

2.1 单台风扇故障

单台风扇故障可以是其中任意一台风扇发生故障,但该故障情形最严重的事件是 FCC1 或 FCC2 的风扇发生故障,因为其将飞行控制模块 (FCM) 和作动器控制模块 (ACM) 集成在同一机箱内,若其风扇发生故障最终会导致其中的 FCM 和 ACM 功能同时丧失。此时,若 FCC1 或 FCC2 发生故障时,但飞控系统仍处于正常模式,系统依然能对所有操纵面进行正常操纵,它对飞机的安全性影响等级是微小的 (Minor)。根据该安全性影响等级评估得出,单台风扇的失效率 λ 应小于 $10^{-3}/\text{FH}$ 。

2.2 两台风扇故障

两台风扇同时故障的情形有 6 种组合,但只有 3 种类

别,分别是 2 台 FCC 的风扇故障或单侧电子设备柜中的 2 台电子设备风扇同时故障 (ACE 和 FCC) 或 2 台 ACE 的风扇同时故障。

第 1 类: 若 2 台 FCC 的风扇同时故障,则系统进入直接模式,剩余 2 台 ACE 可用。此时可用操纵面有 2 块副翼、2 块升降舵、1 块方向舵 (降级)、2 对扰流板,满足总体最小可接受操纵 (MAC) 要求。

第 2 类: 若单侧电子设备柜中的 ACE 和 FCC 风扇同时故障,则系统进入直接模式,剩余另一侧的 ACE 和 FCC 可用。此时可用操纵面有 1 块副翼、1 块升降舵、1 块方向舵 (降级)、1 对外侧扰流板,满足总体最小可接受操纵要求。

第 3 类: 若 2 台 ACE 的风扇同时故障,则系统进入直接模式,剩余 2 台 FCC 可用。此时可用操纵面有 2 块副翼、2 块升降舵、1 块方向舵,满足总体最小可接受操纵要求。

以上 3 类故障组合的安全性影响均满足 MAC 要求。但前两类的故障情形相对严重些,除了出现 MAC 操纵外,还同时出现方向舵降级,这对飞机产生的安全性影响是危险的 (Hazardous),是一个 II 类事件,对应的安全性设计目标是应小于 $10^{-7}/\text{FH}$ 。通过初步安全性评估对其设计目标进行分配,其故障树 (FTA) 分析如图 2 所示。

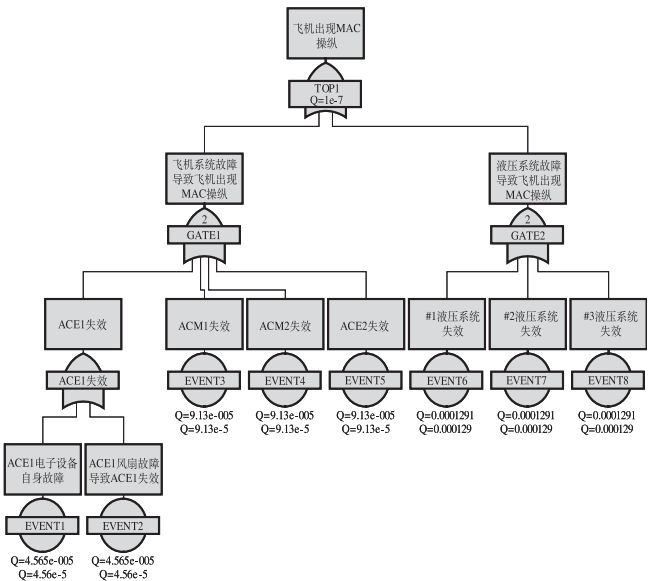


图 2 2 台托架风扇故障 FTA 分析
Fig.2 FTA analysis for the failure of 2-tray fans

(1) 故障树分析

根据飞控系统架构及总体定义的最小可接受操纵面组合要求,当任意 2 台作动器控制器失效或任意 2 套液压源失

效时均会导致飞机出现 MAC 操纵。而作动器控制器的失效可能是自身故障或由于风扇故障导致其温度过高而丧失相应功能。为降低指标计算复杂度,安全性指标的分配采用均分原则。

(2) 失效率 λ 及平均故障间隔时间 (MTBF) 计算

保守设计,认为风扇故障立即导致 ACE 失效,则其风险暴露时间为 1 个飞机轮挡时间 T ($T=1.37\text{h}$),其失效率 λ 为:

$$\lambda=Q/T=4.456 \times 10^{-5}/1.37=3.332 \times 10^{-5}, Q \text{ 表示 FTA 对托架}$$

风扇的安全性要求。此时风扇的 $\text{MTBF}=1/\lambda=30012\text{FH}$ 。

如果考虑风扇失效后,ACE 依然有 0.5h 的生存能力,则风险暴露时间为 0.87h,其失效率 λ 为: $\lambda=Q/T=4.456 \times 10^{-5}/0.87=5.247 \times 10^{-5}$,此时风扇的 $\text{MTBF}=1/\lambda=19059\text{FH}$ 。

2.3 三台风扇故障

三台风扇同时故障有 3 种组合,但无论哪种组合均会导致飞机发生灾难性事件,其安全性影响是灾难性的 (Catastrophic),是一个 I 类事件,对应的安全性设计目标是应小于 $10^{-10}/\text{FH}$ 。该事件的 FTA 分析如图 3 所示,事件中应认为风扇故障是独立事件。

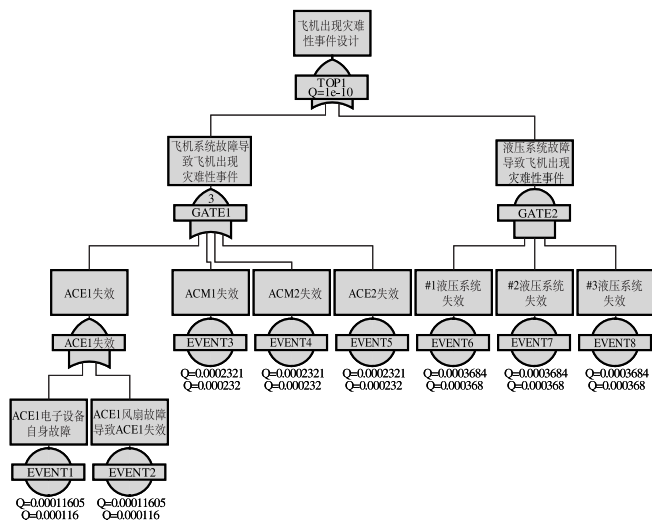


图 3 3 台托架风扇故障 FTA 分析

Fig.3 FTA analysis for the failure of 3-tray fans

该事件中托架风扇失效率 λ 计算如下:

保守设计,认为风扇故障立即导致 ACE 失效,则其风险暴露时间为 1 个飞机轮挡时间 T ,其失效率 λ 为:

$$\lambda=Q/T=1.1605 \times 10^{-4}/1.37=8.471 \times 10^{-4}, Q \text{ 表示图 3 FTA 对托架}$$

风扇的安全性要求。此时风扇的 $\text{MTBF}=1/\lambda=11805\text{FH}$ 。

如果考虑风扇失效后,ACE 依然有 0.5h 的生存能力,则风险暴露时间为 0.87h,其失效率 λ 为: $\lambda=Q/T=1.1605 \times 10^{-4}/0.87=1.334 \times 10^{-4}$,此时风扇的 $\text{MTBF}=1/\lambda=7497\text{FH}$ 。

2.4 托架风扇隐性故障

由于托架风扇无故障检测装置,为此需考虑在上一航班结束时,若单个风扇发生故障但对应的 ACE 没有受到影响,因而飞控系统在自检时无法检测出该隐性故障,若在之后的飞行中出现 1 台或 2 台风扇故障对飞控系统 & 飞机产生的安全性影响。这种故障模式应分 2 种故障情形:第 1 种情形是在下一次航班中其他风扇均正常工作。由于上一航班已出现单台风扇故障,故对应的 FCC 由于其环境温度过热导致其失效,此时系统可检测到该 FCC 的故障,因此在地面维护检查时可检测出风扇故障。这种情形对飞机的安全性影响是微小的 (Minor),是可以接受;第 2 种情形是在下一次航班中,同时又发生 1 台或 2 台风扇故障,这种情形按照条件概率进行考虑,其结果与以上讨论情形一样。更为安全的解决措施是应结合托架风扇的基本可靠性设置合适的维修间隔对风扇进行定期检查。

综合以上各种故障组合,托架风扇应选择最严酷的安全性指标要求,故其 MTBF 值应是 30012FH。

3 托架风扇共模故障分析

由于增加了托架风扇,从而会对飞控系统带来潜在风险。因此,不应仅仅从功能可用性的角度对托架风扇进行分析,还应从共模故障角度进行考虑,评估其是否会对飞控系统产生不利影响。

ARP4761^[2] 定义共模故障分析 (CCA) 是为了验证故障树 (FTA)、关联图 (DD) 及马尔科夫分析 (MA) 中的与门事件是否真正独立,同时它强调的是该与门事件的顶事件应是 I 类或 II 类事件,它可以应用在设备级、系统级和飞机级安全性分析过程中。从上述故障情形分析中可知,当 3/4 台风扇同时发生故障时,最终会导致灾难性事件发生,因此需对托架风扇进行共模考虑。

ARP4761 关于共模分析建议考虑的因素包括软 / 硬件设计错误、硬件故障、产品缺陷、环境影响、需求错误、安装错误、维修性错误、共用外部能源等。由于托架风扇不是复杂的电子硬件 / 软件而是简单的电气设备,同时又安装在电磁屏蔽和气密增压的驾驶舱电子设备柜中,因此其共模考虑主要是产品自身故障和共用外部源等因素。

此外,由于托架风扇的所有故障模式是已知且可验证,因此不需要采用非相似设计来避免共模故障。但如果 4 台风扇仅由同一汇流条进行供电,则该汇流条就是其共模考虑因素,因为由于该汇流条失效必然导致 4 台风扇同时失效,

从而导致灾难性事件发生。为解决该共模故障,应至少采用 2 路独立汇流条对风扇进行供电,建议采用 3 路独立汇流条进行供电更为合适,此时对各路汇流条的失效率要求是应小于 $10^{-4}/\text{FH}$ 。

4 结束语

通过对托架风扇的各种故障情形及故障组进行初步安全性评估,确定其安全性影响等级,并通过故障树分析将相应的安全性设计目标分配到飞控电子设备托架风扇,明确了飞控电子设备托架风扇的安全性需求。根据 ARP4761 的共模故障要求,通过对托架风扇的共模故障分析可知托架风扇选择同一类型即可,但其供电电源应由 3 路独立汇流条进行供电,各路汇流条的失效率应小于 $10^{-4}/\text{FH}$ 。

AST

参考文献

- [1] AEEC. ARINC600-16: Air Transport avionics equipment interfaces[S]. Airlines Electronic Engineering Committee, 2006.
- [2] Society of Automobile Engineers Inc. SAE ARP 4761: Guidelines and methods for conducting the safety assessment process on civil airborne system [S]. Society of Automobile Engineers Inc, 1996.

作者简介

田亮(1988—) 男,工程师。主要研究方向:飞控系统顶层设计及系统需求分析。

Tel: 029-86832428 E-mail: crackhooker@163.com

张新慧(1982—) 男,高级工程师。主要研究方向:飞控系统总体设计。

Safety Requirements Analysis for Tray Fan Used for Civil Aircraft Flight Control Electronic Equipments

TIAN Liang*, ZHANG Xinhui

AVIC Aircraft CO., Ltd. R&D Center, Xi'an 710089, China

Abstract: Focusing on the civil aircraft flight control electronic equipments' cooling method and combining with flight control system architecture, the functional hazardous assessment for the failure of the tray-type fans was conducted. By building the tree of FTA, a quantitative analysis for category I and II events was performed, and the safety target into safety requirements for the tray fans was carried out, the mean time between failures of tray fan was given. Additionally, a common mode for the safety of the tray fans was discussed and analyzed based on ARP4761, and the problems of the common mode failure of the tray fans were solved.

Key Words: tray fan; safety requirement; FTA; common mode failure

Received: 2016-05-25; Revised: 2016-07-19; Accepted: 2016-07-20

*Corresponding author. Tel. : 029-86832428 E-mail: crackhooker@163.com