# 基于功能危险性评估的民用飞机驾驶舱门设计探讨

# The Design and Discussion of Civil Aircraft Flight Deck Door Based on Function Hazard Assessment

安琳琳　汪　洋 / An Linlin　Wang Yang
（上海飞机设计研究院，上海 201210）
（Shanghai Aircraft Design and Research Institute，Shanghai 201210，China）

**摘　要：**
FAA 分别于 2002 年和 2008 年颁布 25-106 及 25-127 修正案，增加驾驶舱门安保事项以提高驾驶舱的安全水平。修正案要求加固驾驶舱门，驾驶舱门必须设计成可以阻止未被授权人员进入驾驶舱并且阻碍危险物体射入以保证机组人员的安全。驾驶舱门必须能检测驾驶舱失压并可以释放门或者卸压板平衡压力差，还应有措施使飞机机组成员在该舱门卡住的情况下能直接从驾驶舱进入客舱。因此，在驾驶舱门上设有一个可以快速释放的紧急出口。根据飞机驾驶舱门结构及功能的主要特点，对驾驶舱门功能故障进行探讨，同时对功能故障引发的危险性等级进行划分，以确定安全指标，进而辅助驾驶舱门设计工作。

**关键词：**民用飞机；驾驶舱门设计；功能危险性评估
**中图分类号：**V223$^{+}$.1　　**文献标识码：**A

[**Abstract**] FAA published 25-106 and 25-127 amendment in 2002 and 2008, in order to enhance the safety property via adding security considerations for flight deck door. The amendment demand that the flight deck door should be enhanced. The FDD (Flight Deck Door) should be designed to resist forcible intrusion into cockpit by unauthorized persons and resist penetration by small arms fire and fragmentation devices to ensure safety for crew. FDD system can detect the decompression of cockpit and release the door panel to equal the pressure and must be provided to enable flight crewmembers to directly enter the passenger compartment from the pilot compartment if the cockpit door becomes jammed. There is a emergency access in the door. This article will discuss the function failure and identify hazard according to FDD feature of structure and function. The safety target which is defined based on the hazard assessment will assist the designing of FDD.

[**Key words**] civil aircraft; flight deck door(FDD) design; function hazard assessment

## 0　引言

“9.11”恐怖事件后，民用航空运输安全性备受关注。2002 年 1 月 15 日，FAA 发布了《运输类飞机驾驶舱门设计的安保事项》的最终法则，公布了 FAR 25-106 修正案，该修正案采纳了 ICAO 标准中关于保护驾驶舱的要求，修订了 FAR 25 部 §25.772 条款（驾驶舱舱门），增加 §25.795 条（安保事项），要求加固驾驶舱门提高驾驶舱的安全水平。因此驾驶舱门功能发生转折。

2008 年 10 月 28 日，FAA 发布了《运输类飞机设计和运行的安保相关事项》的最终法则，颁布了 FAR25-127 修正案，修订 FAR25 适航规章，其中对驾驶舱抵御轻型武器装备火力的内部特征设计等几个方面提出了要求，以进一步加强运输类飞机的安保措施，提高飞机的安全水平。驾驶舱安全性大幅提升。

本文将根据飞机驾驶舱门结构及功能的主要特点，对驾驶舱门功能故障进行探讨，同时对功能故障引发的危险性等级进行划分，并根据功能危险

性等级确定安全设计指标,进而辅助驾驶舱门设计工作。

## 1 驾驶舱门设计目标

飞机驾驶舱门系统用于飞行员进入驾驶舱,同时阻隔驾驶舱和客舱。

根据 CCAR25 部要求,驾驶舱门必须满足 CCAR25.795(a)要求,即驾驶舱门必须设计成可以阻止未被授权人员进入驾驶舱并且阻碍危险物体射入以保证机组人员的安全。

同时驾驶舱门必须满足 CCAR25.365(e)中对增压情况的要求,因此要求驾驶舱门系统必须有措施来检测驾驶舱失压并且可以释放卸压板来平衡压力。

根据 CCAR25.772 要求,驾驶舱门必须有措施使飞机机组成员在该舱门卡住的情况下能直接从驾驶舱进入客舱。驾驶舱门必须可以提供一个可快速释放的紧急出口。[1-2]

### 1.1 驾驶舱门组成

驾驶舱门通常由以下部分组成,结构如图 1 所示。

(1)门结构组件(门板,卸压板,铰链,门框);

(2)门锁(门电磁锁,卸压感应锁);

(3)控制等电气组件(控制面板,电气控制盒,密码输入板,指示灯和警告灯,扩音器等)。

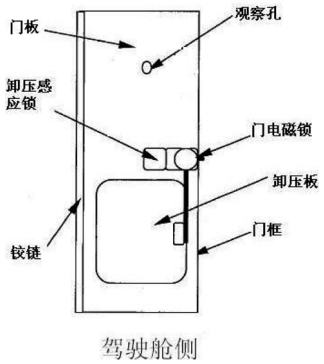


图 1 驾驶舱门结构组件示意图

驾驶舱门系统构架如图 2 所示。

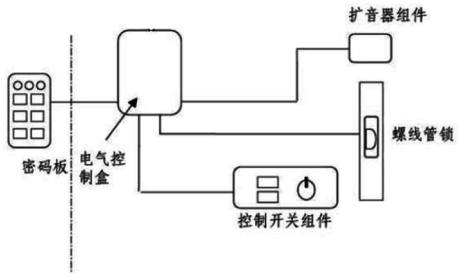


图 2 控制系统构架

### 1.2 驾驶舱门系统功能描述

依据驾驶舱门设计目标,要求其系统应有以下五个主要功能:

(1)供机组正常出入驾驶舱;

(2)驾驶舱失压时快速卸压(卸压板,压力感应锁);

(3)为驾驶舱门提供控制功能(电气控制系统);

(4)锁定驾驶舱门(电磁锁);

(5)为驾驶员提供开启或关闭状态显示(指示灯和警告灯)。

驾驶舱门的主要操作程序包括:

(1)正常进入驾驶舱程序(由密码板,电磁锁和控制面板实现);

(2)拒绝进入程序(由密码板,电磁锁和控制面板实现);

(3)在飞行员丧失行动能力时,紧急救援程序(由密码板,电磁锁实现);

(4)应急着陆时作为紧急出口(由机械卸压装置控制卸压板打开);

(5)驾驶舱出现失压时,快速卸压(由机械卸压装置控制卸压板打开)。

## 2 驾驶舱门系统危险性评估的必要性

危险性评估目的是确定驾驶舱门每个组件的设计和操作风险。CAAR25.1309(b)(c)[1]条款中作了详细说明,并且给出了构建安全系统的描述。主要包括以下内容:

(1)25.1309 (b)

飞机系统与有关部件的设计,在单独考虑以及与其它系统一同考虑的情况下,必须符合下列规定:

(i) 发生任何妨碍飞机继续安全飞行与着陆的失效状态的概率极不可能;

(ii) 发生任何降低飞机能力或机组处理不利运行条件能力的其它失效状态的概率不大可能。

(2)25.1309 (c)

必须提供警告信息,向机组指出系统的不安全工作情况并能使机组采取适当的纠正动作。系统、控制器件和有关的监控与警告装置的设计必须尽量减少可能增加危险的机组失误。

功能危险评估(FHA)是一种定性的分析方法,它是进行系统安全性分析的基础。通过功能危险

分析,可以评价系统各种功能故障危险,为安全性设计提供准则。证明驾驶舱舱门满足设计要求。

## 3 术语

### 3.1 影响等级

1)无安全性影响:失效状态不产生任何类似于妨碍飞机营运能力或增加机组工作负担的安全性影响。

2)较小的(Ⅳ):失效状态不会明显地降低飞机安全,机组的操作仍在其能力范围内。较小的失效状态可能包括轻微地降低安全裕度或功能能力,轻微地增加机组成员工作负担譬如常规飞行计划的更改,或个别乘客或客舱机组成员身体略有不舒适。

3)较大的(Ⅲ):失效状态会降低飞机的能力或机组处理不利操作情况的能力,包括明显地降低安全裕度或功能力,明显地增加机组成员工作负担或增加机组效率削弱的情况,使飞行机组成员身体不舒适,或使乘客或客舱机组成员身体不适甚至受到轻微伤害。

4)危险的(Ⅱ):失效状态会降低飞机的能力或机组处理不利操作情况的能力,包括:

(1)极大地降低安全裕度或功能能力;

(2)身体不适或过分的工作负担导致飞行机组成员不能准确地或完全地完成其任务;

(3)除了飞行机组成员以外可能个别乘员会遭受严重伤害或死亡。

5)灾难的(Ⅰ):失效状态会妨碍持续安全飞行和着陆,可导致机毁人亡的灾难性事故。

### 3.2 定性概率术语

1)可能的失效状态是那些在每架飞机的整个使用寿命内预期发生一次或多次的失效状态;

2)极少的失效状态是那些在飞机的整个寿命内、在每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营运寿命时,可能会发生几次的失效状态;

3)极端少的失效状态是那些在飞机的整个寿命内、在每架飞机上非预期发生的,但当考虑这一机型所有的飞机的总的营运寿命时,可能会发生很少几次的失效状态;

4)极不可能的失效状态是那些在某一机型所有的飞机的整个的营运寿命中非预期发生的不太可能的失效状态。

### 3.3 定量概率术语

1)可能的失效状态是那些每飞行小时平均概率高于$1\times10^{-5}$的失效状态;

2)极少的失效状态是那些每飞行小时平均概率低于$1\times10^{-5}$但高于$1\times10^{-7}$的失效状态;

3)极端少的失效状态是那些每飞行小时平均概率低于$1\times10^{-7}$但高于$1\times10^{-9}$的失效状态;

4)极不可能的失效状态是那些每飞行小时平均概率低于$1\times10^{-9}$的失效状态。

## 4 驾驶舱门系统功能危险性评估

对驾驶舱门进行功能危险性评估目的是确定所有的设备和组件的性能、性能退化、功能故障所导致的相关故障情况,即确定驾驶舱门系统各种功能故障危险,并确定每个飞行小时发生故障的概率。[3]

### 4.1 功能危险性评估(FHA)

根据驾驶舱门的设计目标,设计主要是满足基本的机械和电动系统要求,同时还满足防子弹穿透,防入侵及驾驶舱舱门的结构安装,阻燃性和软件的要求。

此系统主要涉及驾驶舱门系统机械/电磁锁定解锁功能失效,电的失效会导致热/火和电磁干扰保护系统的失效。

综合以上因素,驾驶舱门功能危险性评估将主要针对以下失效情况。

1)单个失去行动能力的驾驶员在驾驶舱,另一个驾驶员由于门的失效而被拒绝进入(灾难性的);

2)驾驶舱快速卸压时因释压面板打不开而无法完成卸压(灾难性的);

3)驾驶舱被侵入:即不法分子企图进入时电磁锁锁定失败,驾驶舱门无法关闭(灾难性的);

4)“LOCK FAIL”(对锁定失败)出错或缺失,“AUTOLOCK”(对应急出口),或驾驶舱门警示灯指示可见或有警报声(较小的)。

通过对驾驶舱门潜在危险评估后,对四种危险性进行比较深入的故障树分析(FTA)。

FTA 的研究综合了所有可能产生危险性的失效模式。确定的或不确定的功能被用作成为危险性的可能性。确定的失效需要两种情况都发生;他们发生的可能性是叠加的。可能的失效模式意味着任何在该程度的失效都属于危险性;这些失效概率是叠加的,因此得出事件发生的概率。

表 1 是系统级驾驶舱门系统的功能危险分析。共有 4 项功能故障,其中 3 项Ⅰ级功能故障, 1 项Ⅳ

级功能故障。对于Ⅰ类(灾难性)故障条件,要求在设计系统构架时考虑避免Ⅰ类故障条件发生,当故障条件由系统构架考虑不可避免时,应使其发生概率低于$10^{-9}$每飞行小时。

**表 1　系统级驾驶舱门系统的功能危险分析**

| 功能 | 危险说明 | 危险对飞机或人员的影响 | 影响等级 |
|---|---|---|---|
| 供机组出入驾驶舱 | 单个失去行动能力的驾驶员在驾驶舱,另外一个驾驶员由于门的失效而被拒绝进入(即电磁锁打开失败,舱门无法打开) | 飞机:飞机失去控制可能发生坠撞<br>机组:无法对飞机执行操作<br>乘客:可能全部遇难 | Ⅰ |
| 快速失压时卸压 | 驾驶舱快速卸压时卸压板打开失败 | 飞机:驾驶舱内失压,飞机可能由于驾驶舱门和机身结构的变形引起飞行控制的失效而发生坠撞<br>机组:机组人员失去行动能力<br>乘客:可能全部遇难 | Ⅰ |
| 驾驶舱防侵入 | 驾驶舱被侵入,即不法分子企图进入时,电磁锁锁定失败(由于门锁或者压力感应失效引起的门开启) | 飞机:在非正常的进入请求时,将导致不法分子进入,飞机可能被劫持并失去控制。可能发生坠撞<br>机组:机组人员被劫持<br>乘客:可能全部遇难 | Ⅰ |
| 为驾驶舱门锁定状态提供指示或警示 | 驾驶舱门警示灯和指示灯的可见指示错误或者失效 | 机组:飞行员和服务员工作量增加 | Ⅳ |

## 4.2　故障树分析(FTA)

1)基础数据

对 4.1 节提到的影响等级为Ⅰ的三种危险性进行故障树分析。用到的理论、试验和统计的数据如下。

若假设民机每次平均飞行时间为 3h,每天飞行 4 次,则每天总的飞行时间为 12h。

驾驶舱门操作:40 次操作/天

民机的飞行小时 :12 小时/ 天

航线每天都要检查驾驶舱门系统的完整性,尤其是在第一次飞行前。检查主要包括驾驶舱门电气系统的组件功能。

2)故障树分析

每一个飞行小时飞行员失去行动能力,快速失压和未被授权者试图进入发生的频率都来源于 FAA 国家民用航空安全数据分析中心和飞行安全航线劫机数据库。

(1) 飞行员丧失行动能力的概率

波音 747、波音 767 等飞机经验数据,假定驾驶员失去行动能力的概率是低于 1.92E-8/飞行小时。则每次飞行中失去行动能力的概率为 5.76E-08。

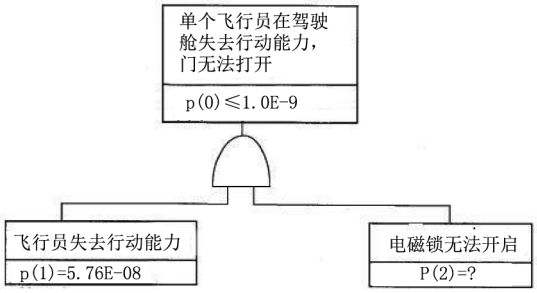


**图 3　飞行员丧失行动能力时门无法打开的 FTA 分析**

据图 3 得出:电磁锁无法开启的概率应≤1.72E-2。

(2)卸压事件概率

根据美国 FAR121 支线飞机 10 年的飞行小时中和 NTSB(美国运输安全委员会)/FAA 的卸压报告,卸压事件的概率假定是 1.4E-07/ 每飞行小时。

总的飞行小时:135h,737h,515h

总的卸压事件报道:19

因此卸压事件概率为:1.4E-07/ 飞行小时。每次飞行中卸压事件概率为 4.2E-07。

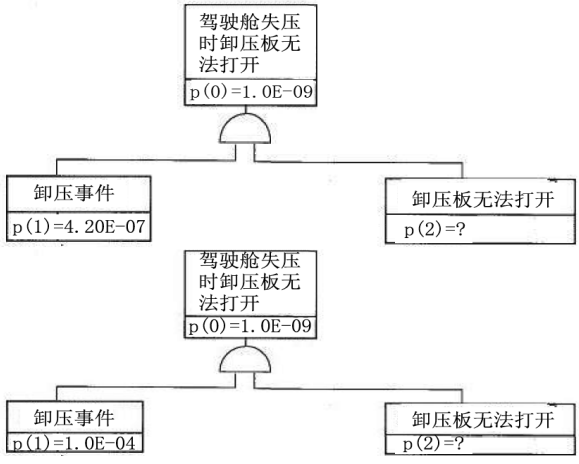


**图 4　驾驶舱失压卸压板无法打开 FTA 分析**

据图 4 得出:当选取卸压发生概率 4.2E-07,卸压板无法打开的概率应≤2.38E-3。假定为机械式卸压,则卸压板无法打开情况有如下两种:①卸压感应机构失效;②释放锁失效。保守情况下,卸压锁失效概率≤2.38E-3 即可满足设计要求。根据 FAA 备忘录 01-115-11,指出飞机发生卸压的概率≤1.0E-04,因此对卸压板锁提出了更高的设计要

求,其失效概率应设计成≤1.0E-05。在驾驶舱门设计中应对卸压感应机构和释放锁进行耐久性试验进行验证。

(3)未被授权人尝试进入的发生

未被授权的人员试图进入基本上都是劫机者或者难驾驭的乘客。

这种情况的危险性等级是“灾难性的”取决于有自杀企图的人员闯入的可能性。

在劫机事故中,“飞行安全航线网劫机数据库”提供了在波音 747、波音 767 等飞机平均每飞行小时的发生概率是 1.22E-7。考虑到驾驶舱门的目的,在 FTA 中每飞行小时采用保守数据即两倍的概率 2.44E-07 每飞行小时。每次飞行中失效概率为 7.32E-07,如图 5 所示。

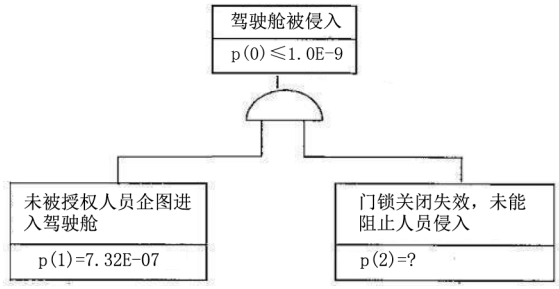


图 5　驾驶舱被侵入的 FTA 分析

由以上分析可知门组件平均故障间隔时间(MTBF),如表 2 所示,为组件设计提供参考。

表 2　门组件 MTBF

| 组件 | 失效概率 | MTBF |
|---|---|---|
| 门锁 | ≤1.72E-2 | ≥5.76E1 |
| 卸压锁 | ≤1.0 E-5 | ≥1.0E5 |

MTBF=组件寿命/失效率或每小时进入次数

组件寿命=MTBF×(失效率或每小时进入次数)

门锁寿命=MTBF×(40/12)

卸压锁寿命= MTBF×(1.0e-4)

根据4.2 2)由表 2 可知主要组件的寿命必须满足表 3 所示数据。

表 3　门组件使用寿命

| 组件 | 寿命 |
|---|---|
| 门锁 | ≥1.73E2 |
| 卸压锁 | ≥1.0E1 |

驾驶舱门设计过程中通常对组件寿命限定如下:

门锁系统:4.5E5 次循环;

卸压锁:1.0E3 次循环;

以上数值满足表 3 要求,则可满足驾驶舱门系统安全性要求。

为验证驾驶舱门功能安全性,同时应对驾驶舱门进行试验验证,如表 4 所示。

表 4　系统功能安全性符合性验证

| 功能 | 危险说明 | 影响等级 | 每飞行小时发生失效的概率 | 符合性验证方法 |
|---|---|---|---|---|
| 驾驶舱出口 | 单个失去行动能力的驾驶员在驾驶舱,另外一个驾驶员由于门的失效而被拒绝进入 | I | ≤1.0E-9 | (1)静载荷试验<br>(2)耐久性试验<br>(3)救援试验 |
| 快速失压时卸压 | 驾驶舱快速卸压时卸压板打开失败 | I | ≤1.0E-9 | (1)耐久性试验<br>(2)卸压分析<br>(3)紧急撤退试验 |
| 锁定驾驶舱门 | 门未能阻止暴力侵入 | I | ≤1.0E-9 | (1)防侵入试验<br>(2)防穿透试验<br>(3)静载荷试验<br>(4)耐久性试验 |

## 5　结论

功能危险评估(FHA)是进行系统安全性分析的基础。本文结合驾驶舱门的结构功能,对四种可能出现的主要失效模式进行分析,得出单个失去行动能力的驾驶员在驾驶舱,另一个驾驶员由于门锁的开启失效而被拒绝进入驾驶舱/快速卸压时释压面板打不开无法完成卸压/驾驶舱被侵入时电磁锁锁定失败导致的驾驶舱门无法关闭三种失效模式将引起灾难性事故。通过此三种失效模式的失效概率,计算得出驾驶舱门主要结构组件的寿命,为驾驶舱门系统参数设计提供指导。

参考文献:

[1] 中国民航局. CCAR25-R4 中国民用航空规章第 25 部:运输类飞机适航标准[S]. 北京:中国民用航空局,2011.

[2]《飞机设计手册》总编委会编. 飞机设计手册第 10 册:结构设计[M]. 北京:航空工业出版社,2000.

[3]《飞机设计手册》总编委会编. 飞机设计手册第 20 册:可靠性、维修性设计[M]. 北京:航空工业出版社,1999.