共模分析方法及其在民机设计中的应用研究

Methodology of Common Mode Analysis and Utilization in Civil Aircraft Design

王萌萌　孙　帆 / Wang Mengmeng　Sun Fan
（中航沈飞民用飞机有限责任公司，沈阳 201412）
（AVIC SAC Commercial Aircraft Company Limited, Shenyang 201412, China）

摘　要：
安全性是民机设计中最重要的考虑要素之一。作为安全性评估的重要手段，共模分析是通过对元件或事件之间的独立性进行分析，来保证设计对象的安全性。对共模分析的工作流程进行了说明，详细列出了需要考虑的共模失效源及失效模式。介绍了共模分析的与门方法和割集方法，并通过某型民用飞机舱门设计实例说明了在机械系统中如何通过这两种方法进行共模分析，同时给出了相关结论。

关键词：民机设计；安全性评估；共模分析；独立性要求
中图分类号：V21　　**文献标识码：**A

[**Abstract**] Safety is one of the most significant considerations in the civil aircraft design. Based on analysis of the independence between elements or events, Common Mode Analysis is also used to guarantee the safety of the design object. The procedure of Common Mode Analysis is introduced in this paper, listing the common failure sources and its failure modes in detail. Furthermore, the "AND-GATE" method and "SHORT-CUT" method of the Common Mode Analysis are presented. By an real example of a pressurized compartment door, two methods are analyzed in a mechanism system, which were used for Common Mode Analysis. And the relevant conclusions are given.

[**Key words**] civil aircraft design; safety assessment; common mode analysis; independence requirement

0　引言

飞机潜在风险的严酷度等级及其发生的概率，是安全性分析的重要组成部分，也是安全性分析的主要工作[1]。在飞机设计中，必须保障产品功能、系统或元件之间的独立性，才能满足安全性要求。确保独立性得到满足，或非独立性处于可接受的范围之内，是安全性工作的重要组成部分。在设计过程中，这些工作内容通常通过共模分析（Common Mode Analysis，简称 CMA）来实现。

CMA 是共因分析（Common Cause Analysis，简称 CCA）的一部分，设计中假定相互独立的失效之间是否确实相互独立可通过这种方法来证明[2]。但它并不是一种独立的分析工具，必须在完善的整机安全性分析（Aircraft Safety Analysis，简称 ASA）/系统安全性分析（System Safety Analysis，简称 SSA）中使用。具体地说，CMA 是用来验证 ASA/SSA 中的失效事件在实际情况中是相互独立的。这个过程中，无论是研发、制造、安装、维护和机组人员操作失误所造成的影响，还是可能影响系统独立性的失效，都应该逐一加以分析。同时还应注意功能与其相应的监控设备之间的独立性。

本文主要讨论 CMA 的分析方法，并通过某货舱门设计实例说明 CMA 的主要作用和最终分析结果。

1　CMA 分析内容及流程

在具体分析中，CMA 通常用来验证故障树分析（Fault Tree Analysis，简称 FTA）或其他分析手

段中所有的“与”事件在实际情况中是否互相独立。在整机分析中,可以从以下几方面来考虑共模失效的可能性[2]:

(1)硬件错误;
(2)软件错误;
(3)硬件失效;
(4)制造/维修流程;
(5)环境应力(温度、湿度、振动等);
(6)安装错误;
(7)要求错误;
(8)环境因素;
(9)串联;
(10)共同外源性故障。

根据分析的系统不同,CMA 工作需要考虑的重点内容也不同,应该具体分析。系统级 CMA 分析工作的流程可参考图 1[3]。

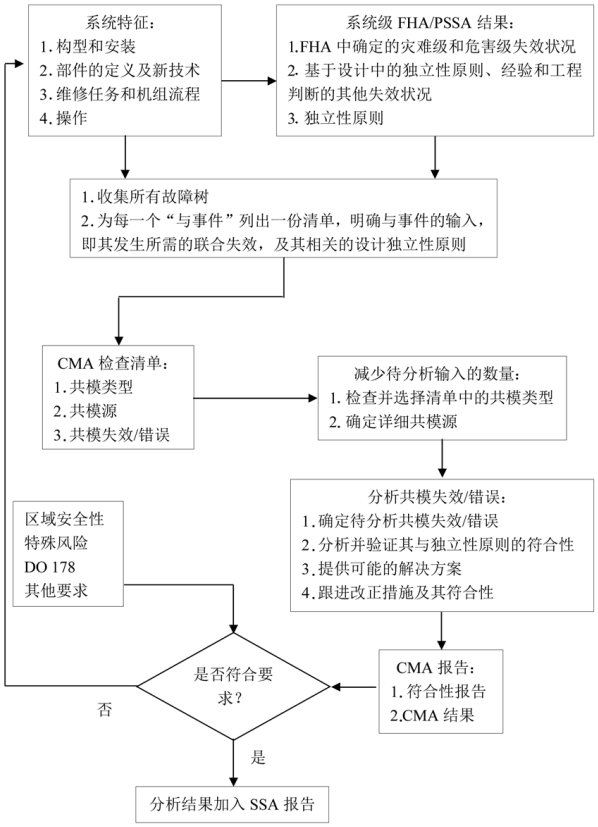

图 1　系统级 CMA 分析步骤

2　CMA 分析方法

CMA 分析一般分为与门方法和割集方法。实际工作中,往往根据系统复杂程度及其与机上其他系统的互联程度,结合其他通过安全性评估(在本文中特指 FTA)得到的细节信息,来选择通过与门方法或最小割集方法进行共模分析。这两种分析方法中都应考虑来自系统或整机的共同外源性影响。

CMA 工作主要从表 1 所示的几个方面开展。

表 1　共模类型、来源及失效检查单

编号	共模类型	共模子类型	共模失效/错误
1	概念设计方面	设计构型	物理独立性不足
			功能独立性不足
			软件编码错误
		失效后载荷重新分配	维持正常工作的元件不能承受附加载荷
		技术、材料	设计区别不足
		其他	纠正措施不足
2	制造方面	制造	人为错误
		流程	纠正措施不足
		工艺	工艺不成熟
3	安装/集成	装配	人为错误
		流程	纠正措施不足
		位置	同区域中的设计错误
		流程安排	独立的设计错误,应力安装
4	操作方面	操作人员	人为错误
		流程	纠正措施不足
5	维护方面	维修人员	人为错误
		流程	纠正措施不足,维修频率高
6	测试方面	测试人员	工作人员缺乏培训,缺少经验
		流程	纠正措施不足
7	环境方面	机械	振动、火山灰、尘土、加速度、摩擦、过度压缩、压强过大、液体聚集
		热	高温/低温、红外辐射、冷却不足
		电	雷击、电源、电压
		辐射	高强度辐射场、UV、X 射线、伽马射线、太阳辐射、臭氧、无线电
		化学方面	湿度、水分、腐蚀、电腐蚀、化学物聚集

2.1　与门方法

设计过程中,在通过故障树进行安全性评估时,如果以设计构型为基础建立故障树,将同时可

能引发“事件”的失效模式逻辑性地结合在一起，那么这种类型的故障树可以通过与门方法进行共模分析。与门方法通常用于机械系统或隐藏失效元件的分析以及外部风险导致后续影响的分析中。

与门方法分析的是最重要的系统要素之间的联合失效，并主观考察具有两个或三个输入的与事件（当输入超过三个时，由于其发生概率过低而不列入考虑范围）。

2.2 割集方法

对于复杂的重要电气系统，由于输入信号和状态信号的相互作用较复杂，因此故障树的建立通常是按照系统图纸和软件逻辑（如监控系统、自动控制等）中定义的信号路径来建立。这种情况下，故障树可能十分复杂，在故障树主要分支下的低层次树形图中还包括很多与门。仅评估这种故障树的与门已经无法明确设计是否满足 CMA 要求，这时应罗列出故障树的所有割集（使用 FTA 软件自动生成），并对割集进行评估。

由于割集列表中包含了所有可能的联合失效模式，导致割集的数量很多。在实际分析过程中，通常需进行简化，去掉一些小量（如超过 3 个元素的割集）。另外，如果割集中的元素是系统/子系统/功能之间已知或已证实相互独立的，则也应从列表中排除（如割集是由机构元素和电气元素，或控制频道和动力分配系统等构成）。

在机械系统中，割集分析通常用于考察单一失效能否引起不可接受的失效状况。

3 CMA 方法在民机设计中的应用

以某型民机货舱门为例，说明机械系统中如何开展 CMA 工作，并对 CMA 结果进行分析。

3.1 货舱门简介

某型民机货舱门为半堵塞式舱门，承受增压载荷。货舱门位于机身水线以下，因此还需承受水上迫降时的水负压。舱门的初始运动方向为向内、向上，飞行中解闩将导致危害性后果。舱门可从机身外侧通过操作手柄打开，达到提升位置后，舱门向外翻开，外翻的动力来自于电作动筒，其操作开关在舱门外侧。舱门完全打开后，作动筒还起到保持舱门打开状态的作用。货舱门构型如图 2 所示。

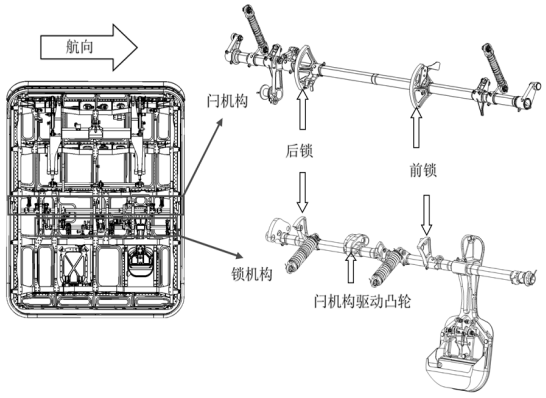

图 2 货舱门构型

3.2 与门分析

以图 2 中货舱门为例，对其故障树分析中的一个与门事件进行详细分析。该故障树阐述的失效状况（即故障树中的顶事件，故障树编号为 52-30-21-03）是：非增压飞行中货舱门解闩。其中与门 G204 为：手柄和舱门的位置正确，但舱门未完全关闭。该与门的输入有 3 个，分别为：前锁丧失功能、后锁丧失功能以及闩轴驱动机构故障，上述三个失效状况同时出现时，与门失效状况发生。该与门在故障树中的形式如图 3 所示。

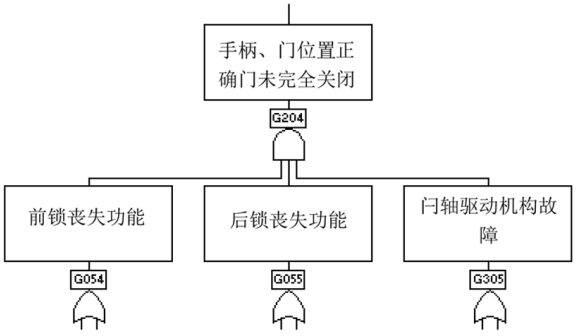

图 3 G204 图示

对该与门进行分析得到的结果为：

1）概念设计方面

锁机构和闩机构是由手柄通过锁轴和闩操作机构进行驱动的，在上锁情况下，锁机构通过锁轴上的锁头和闩轴上的配合锁头能够将闩机构位置锁定。

在打开过程中，如果闩操作机构上的零件失效，锁头和配合锁头能够产生约束，导致舱门打不开，飞行结束后门操作人员会发现这一状况。

闩锁机构已设计为能够承受限制手柄力和极限手柄力：在两对锁头和配合锁头都能正常工作时，锁机构能承受 200lbs 手柄力（限制载荷）和

300lbs 手柄力(极限载荷);如果一对锁头和配合锁头失效,仅余一对能够正常工作时,锁机构也能承受 200lbs 手柄力(限制载荷)和 300lbs 手柄力(极限载荷)。

2) 制造、安装/集成、维护方面

不正确的组装和调整将会降低货舱门在飞行中保持关闭状态的能力,为尽量减少这方面的错误,进行了如下设计:

(1) 每个闩过中弹簧都进行了标记,且均可互换;

(2) 每个锁都进行了标记,且均可互换;

(3) 闩过中弹簧及其附加零件(舱门上的重要机构件)都进行了集成式设计,避免出现操作过程中不能发现的安装错误;

(4) 锁机构的所有零件(舱门上的重要机构件)都进行了集成式设计,避免出现操作过程中不能发现的安装错误;

(5) 闩过中弹簧机构中,无需进行调整。

3) 环境方面

在环境方面,主要考虑的内容有:

(1) 温度

飞行状况下,舱门机构的环境温度较低,温度效应对金属结构许用值的影响微弱。舱门的功能不会受到低温的影响。

地面停机状况下,舱门机构的环境温度为不会超过整机包线中定义的最高温度。舱门名义载荷(手柄力 30 lbs)远小于限制载荷(200 lbs)和极限载荷(300 lbs)。这之间的安全裕度可以满足金属结构所受的温度影响。在地面停机时,舱门打开和关闭的功能不会受到温度的影响。因此,设计中未考虑舱门机构金属材料的温度效应。

(2) 腐蚀

航空工业目前使用的表面处理、涂层、内饰和恰当的材料能够保护舱门机构,避免使其受到由水分引起的腐蚀和电化学腐蚀。另外,舱门结构上布置的排水孔也能避免水分在舱门结构内聚集。因此,该与门符合独立性要求。

与此类似,对故障树中所有与门进行分析,均符合独立性要求。

3.3 割集分析

与电/电子系统不同,机械系统的割集分析通常用于考察单一失效引起失效状况的程度。仍以上述故障树为例,通过 FTA 软件得到表 2 结果。

表 2 52-30-21-03 割集分布状况

割集元素数量	割集数量
1	0
2	186

通过表 2 可以看出,割集元素数量为 1 的割集不存在(数量为 0),也就是说,由于 1 个元件失效不会导致 52-30-21-03 事件的发生。这就证明了单一失效不会导致故障树的顶事件发生。

4 结论

上文所述的与门方法讨论了设计本身、设计的执行过程及其在实际情况下受到的环境影响,分析得出这些内容不会导致共模失效。而通过割集方法,得出了无单一失效导致事件发生的结论。这些结论与适航条例中相关要求相符[4]。

该货舱门的设计充分考虑到了各种影响,分析结果能够满足要求。而在某些特殊情况下,设计并不能满足独立性要求,这种情况下,设计人员还应进行设计更改,或限制更加严格的使用环境,来满足元件之间独立性的要求(如图 1 所示),并再次进行新一轮 CMA 分析。

CMA 能够分析设计中假设为相互独立的事件是否具有潜在的共性,这些共性是否可能在飞机投入使用后导致共模失效。进行 CMA 分析可以使安全性评估更为完善。

参考文献:

[1] FAA. FAA System Safety Handbook, Chapter 2: System Safety Policy and Process[S]. US:FAA, 2000.

[2] Methodology for the Common Mode Analysis Zdzislaw H. Klim Marek Balazinski Bombardier Aerospace école Polytechnique de Montréal Published 2007-09-17.

[3] 赵廷弟. 安全性设计分析与验证[M]. 第 1 版. 北京:国防工业出版社 ,2011.

[4] SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment[S]. Issued 1996.

[5] 中国民用航空局. CCAR 25 中国民用航空规章第 25 部:运输类飞机适航标准[S]. 中国:中国民用航空局,2011.