

DOI: 10.19416/j.cnki.1674-9804.2019.01.017

# 基于工况/场景的飞机系统试验验证方法

## Method of Aircraft System Verification Test Based on Scenarios

袁闻起 / YUAN Wenqi

(上海飞机设计研究院, 上海 201210)

(Shanghai Aircraft Design And Research Institute, Shanghai 201210, China)

### 摘要:

描述了一种飞机系统在试验室系统综合或全机级环境下进行设计验证的方法和过程。首先定义系统需求所在工况/场景,然后根据功能基线,确定工况发生的阶段以及完成此工况需参与的系统范围和构型,从而形成具体的试验步骤,进而通过试验来判断系统的响应是否满足上一级需求。

关键词: 飞机系统; 试验验证; 系统需求

中图分类号: V416.6

文献标识码: A

OSID:



[Abstract] This paper describes a method and process of design verification for aircraft system on the integrated system or aircraft test level in the lab. Firstly we will define the scene of system requirement. According to the function baseline, we will determine the flight phase, the test system range and the configuration in order to form test procedure. Finally, we will judge whether the response of the system could satisfy the requirement by the test.

[Keywords] aircraft systems; verification test ; system requirement

## 0 引言

在现代民机研制过程中,机载系统特别是飞行控制和航电系统,其高度综合和复杂的特点给试验验证工作带来巨大的挑战。在工程发展阶段,需通过试验室试验尽早尽快地找出飞机系统存在的问题,减少系统设计迭代更改,从而加快研制流程。同时,通过试验验证证明产品设计符合设计需求,减少机上试验工作量,节省成本。

结合型号试验实践,该文给出了一种基于工况/场景的飞机系统试验验证方法,在系统综合级联试中通过定义各种飞机在正常和故障状态下的工况,来确定试验过程,从而达到验证的目的。

## 1 工况/场景的来源

在民机系统研制按照 SAE ARP4754A<sup>[1]</sup> 双“V”过程的前提下,飞机级、系统级和项目级都提出,继承(捕获)、分解或定义了各自的需求和功能,并对之进行确认和验证,上一级设计决策形成的结果会

成为下一级的设计输入。基于需求所对应的工况/场景的验证方法一般不适用于较低级别的需求验证,譬如项目(元件)级的验证还是要根据上一级分解和捕获来的功能和需求直接进行试验测试,从而判断该项目(元件)是否满足各项设计需求,譬如性能指标、功能、重量、环境要求和接口定义要求等,如图1所示。

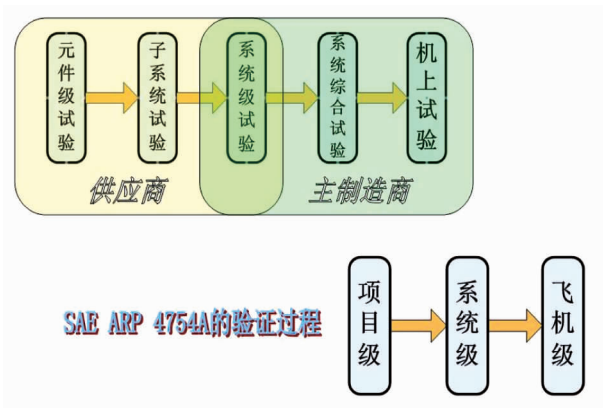


图1 飞机系统研制过程分级

飞机系统根据飞机级的需求进行的研制工作,会形成一系列设计结果,如设计图纸、系统描述文件 SDD(system description document)、功能接口定义 FICD(functional interface control document)、机械接口定义 MICD(mechanical interface control document)、电气接口定义 EICD(electrical interface control document)和一系列安全性分析报告等。传统的做法是对系统按照上述一系列定义进行测试,看系统表现出来的响应是否满足文件定义要求,以此为判据评判飞机系统是否通过。但用系统设计的结论和定义来作为系统设计是否满足上级需求的判据很难从根本上全面发现飞机系统的设计问题,或者证明设计没有问题。

对于飞机系统而言,进行基于需求所存在的工况/场景的验证就显得尤为重要了。就系统综合级或飞机级的试验来说,应该通过模拟飞机的各种工况/场景,来判定系统在这些情形下的响应是否满足最初的需求,从而发现设计问题。简单来说就是最终飞机产品打算怎么用及用到什么程度,那么试验就怎么试,所有的工况都试了没问题,产品设计也就成功了。

## 2 工况/场景的分类和定义

试验室试验工况的定义在条件允许的情况下应尽可能地覆盖设计需求,即使在系统需求和功能定义还不是很完善的情况下,通过识别飞机存在的各种工况,也能够较完整地覆盖被验证的飞机系统,从而提高系统在试验室试验中的问题发现率。

表1 飞机系统工况/场景分类

序号	工况	分类
1	正常工况	牵引、滑行/滑跑、起飞、爬升、返场、巡航、进近、复飞、着陆
2	地面维护工况	
3	人为操作失误	飞行员操作失误、地面维护人员操作失误
4	故障工况	系统自身失效、其他系统失效、系统无指令动作

如表1所示,首先对系统在机上的工况进行分类,包括正常工况、地面维护工况、人为操作失误和故障工况。民机的正常工况一般可分为从牵引滑行到着陆九个阶段,同时从系统维修维护需求考虑,地

面维护工况也是必不可少的。其次人为因素导致的错误操作也作为单独一类,分为飞行员/机组操作失误和地面维护人员/机务操作失误。系统故障作为系统验证中较多的一种工况被单独分为一类,故障包括失效和无指令动作,及其他系统带来的故障。

对于飞机系统来说,工况/场景化的验证实际上属于“黑匣”验证,即不需要知道系统内部架构、具体逻辑、线性关系和信号链路,只要在设定的工况下系统地响应符合预期就可以判定合格。工况可以是一个点,比如爬升阶段收上起落架或襟缝翼,也可以是一段过程,譬如整个正常飞行剖面。但“黑匣”也是相对的,具体工况还是要根据被试系统的功能和需求来设定,特别是在设定人为操作时的工况,还要了解系统的操作界面。飞机起落架控制系统试验验证工况的初步分类和定义如图2所示。

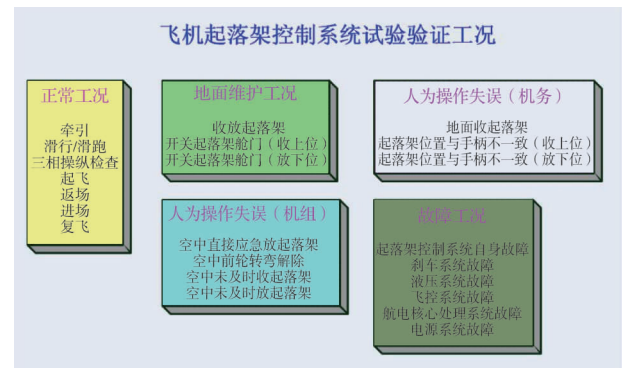


图2 起落架控制系统工况分类

## 3 故障工况

首先要确定故障点,譬如某个系统设备、某条线路等。一般先想到的是根据系统的功能危险性评估 FHA(functional hazard assessment)、系统安全性评估 SSA(system safety assessment)特别是根据故障树分析 FTA(fault tree analysis)来确定系统自身的故障源。但系统危险性评估只针对影响飞机飞行安全的系统功能进行分析,按照功能、子功能最后到元件级逐级分解并不能覆盖全部的系统故障工况,同时对于其他系统带来的故障也考虑不够。

所以对于系统自身故障,考虑试验室试验的实际情况,在不造成系统损坏和保障试验人员安全的前提下,按照系统的组成,每一种可以实现的故障都要纳入试验范畴,做到地毯式排查没有遗漏,即使是相同件的故障也都要模拟。在注入失效故障的同时

考虑其是否存在无指令动作故障,如有,则也需要进行试验。

对于外系统带来的故障工况,通过对系统交联和外系统的架构,找出从外系统元件到连接线缆到信号链路上一系列会影响到自身系统的各个环节的外系统故障,都需模拟。即使各系统重复了,可在试验实施阶段再合并同类项,以避免重复试验。

其次是在故障发生时刻,可定义在系统正工作时故障,也可以在系统工作前注入故障,系统在某个正常工况下运行并记录故障发生后的系统响应、告警和维护记录,同时对飞机运行影响进行评估,看其是否满足设计需求。一般要求“一次故障正常、二次故障安全”,同时有相对应的合适的告警和维护记录。对于二次故障的选择,不可能也没有必要在一个系统内进行排列组合式的穷举,还是要根据具体的系统架构进行故障叠加,来评估影响。再有就是要考虑区域性故障和针对电子软硬件的共模故障。

最后是故障的恢复,民机一般要求故障解除后解除告警,所以恢复也作为故障工况的一项内容,一般的故障工况发生过程可分为“故障发生”“系统动作”和“故障恢复”三个阶段,都定义清楚了,完整的试验程序也就确定了。表 2 以起落架控制系统为例,列举了系统自身及其他系统带来的故障工况。

表 2 起落架控制系统故障工况

序号	工况内容	故障发生阶段	故障恢复	故障类型
1	单个起落架收上故障	T03-Climb	N/A	系统自身失效
2	单个起落架放下故障	Approach	N/A	系统自身失效
3	单个舱门打开故障	T03-Climb	N/A	系统自身失效
4	单个舱门关闭故障	T03-Climb	N/A	系统自身失效
5	单个上位锁接近传感器失效	T03-Climb	起落架放下后	系统自身失效
6	单个下位锁接近传感器失效	T03-Climb	起落架放下后	系统自身失效
7	单个地空信号接近传感器失效	T03-Climb	着陆滑行后	系统自身失效
8	单个舱门打开接近传感器失效	T03-Climb	起落架放下后	系统自身失效
9	单个舱门关闭接近传感器失效	T03-Climb	起落架放下后	系统自身失效

序号	工况内容	故障发生阶段	故障恢复	故障类型
10	起落架控制手柄失效	T03-Climb	起落架放下后	系统自身失效
11	单个起落架控制阀线圈失效	T03-Climb	起落架放下后	系统自身失效
12	单个起落架控制阀线圈失效	Maintenance	舱门关闭后	系统自身失效
13	转弯控制阀失效	Approach	着陆滑行后	系统自身失效
14	单个转弯反馈传感器失效	Approach	着陆滑行后	系统自身失效
15	单个转弯手轮失效	Approach	着陆滑行后	系统自身失效
16	单个起落架控制盒失效	T03-Climb	起落架放下后	系统自身失效
17	起落架舱门地面维护开关失效	Taxi-out	故障后	系统自身失效
18	起落架舱门地面维护开关失效	Approach	故障后	系统自身失效
19	起落架控制盒内部通讯失效	T03-Climb	起落架放下后	系统自身失效
20	两个上位锁接近传感器失效	Approach	起落架收上后	系统自身失效
21	两个下位锁接近传感器失效	Approach	起落架放下后	系统自身失效
22	两个地空信号接近传感器失效	Approach	着陆滑行后	系统自身失效
23	起落架控制阀失效	Approach	起落架放下后	系统自身失效
24	转弯过度	Towing	N/A	系统自身失效
25	液压系统压力传感器失效	Taxi-in	着陆滑行后	其他系统故障
26	发动机驱动泵失效	T03-Climb	着陆滑行后	其他系统故障
27	液压系统控制盒失效	Taxi-in	着陆滑行后	其他系统故障
28	脚蹬传感器失效	Taxi-in	着陆滑行后	其他系统故障
29	单个主飞控计算机失效	Taxi-in	着陆滑行后	其他系统故障
30	轮速传感器失效	Taxi-out	着陆滑行后	其他系统故障
31	刹车压力传感器失效	Towing	N/A	其他系统故障
32	数据转换单元失效	T03-Climb	着陆滑行后	其他系统故障
33	左右整流模块失效	T03-Climb	着陆滑行后	其他系统故障
34	滑行时舱门意外开启	Taxi-out	N/A	无指令动作
35	飞行中舱门意外开启	Cruise	N/A	无指令动作

## 4 试验构型和过程

一个完整而清晰的试验必须有明确的构型定义(包括参试系统的范围、软硬件的版本和被试系统当前的功能基线),详尽的可重复的试验步骤以及准确的试验记录(测试数据等)。在研发过程中试验件特别是电子软硬件在不同的阶段其成熟度不尽相同,功能完整性也是逐步到位的。那么在进行试验前必须确认当前软硬件构型下系统的功能,如图3所示。

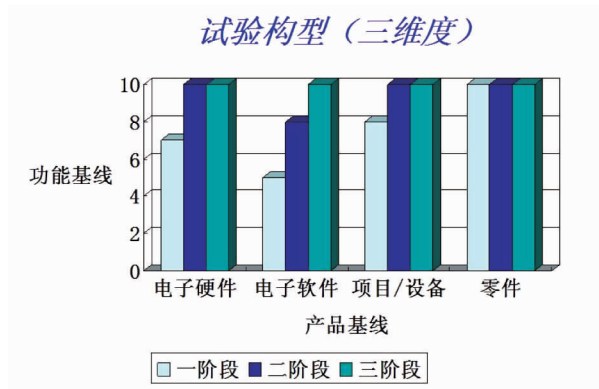


图3 试验构型

对于系统综合级试验验证,可以根据前一级譬如系统级的试验结果来确定被试系统当前的功能,或通过产品或系统的验收试验 ATP(acceptance test procedures),来确定其当前拥有的功能,从而确定在当前功能基线下可进行的工况试验。需要澄清的是

产品验收试验是产品的制造符合性验证过程,即所生产的产品是否与设计图纸或设计文档一致,属于“白盒验证”。有时在验收试验时也能发现设计缺陷,但大部分是低层次问题或设计上的低级错误。

在明确当前被试系统的各项功能后,需根据对应的工况来设定各个参试系统的状态,操作参试系统进行某个状态点或者某段过程的试验,并通过系统的各种响应来进行评判。有时在飞机级的试验中需要对飞机状态或飞行品质进行评估,那就需要建立飞机飞行仿真模型来满足验证要求。

## 5 结论

本文定义了一种飞机系统在试验室系统综合或全机级环境下进行设计验证的方法和过程。通过对工况/场景的定义,根据功能基线,确定工况发生的阶段,确定完成此工况需参与的系统范围和构型,从而形成具体的试验步骤,进而通过系统响应来判断系统的设计是否满足上一级需求。

### 参考文献:

- [1] SAE International. Guidelines for development of civil aircraft and systems: ARP 4754A[S]. SAE Aerospace Recommended Practice, 2010.

### 作者简介

袁闻起 男,高级工程师。主要研究方向:飞机液压、起落架系统全机地面模拟试验。E-mail: yuanwenqi@comac.cc