基于独立性的民用飞机研制保证等级分配方法分析

Analysis on Development Assurance Level Assignment Based on Independence for Civil Aircraft

李亚男　金平 / 中国商飞上海飞机设计研究院

摘　要：介绍了为民用飞机/系统功能和软硬件分配研制保证等级的基本原则和降级原则，确定了实施研制保证过程严格度的方法，分析了功能独立性和项目研制独立性对研制保证等级分配的影响，给出了基于独立性的研制保证等级分配方法。举例说明了该方法的实施步骤和有效性。

Abstract：Present general and degraded principles for development assurance level assignment of civil aircraft/system functions and software/hardware. Determine the rigorous method for performing development assurance process. Analyze the impact of the functional independence and item development independence on the development assurance process. Provide a method for assigning development assurance level based on independence. Take an example to show implementation procedures of the method and demonstrate its validity.

关键词：研制保证等级；功能独立性；项目研制独立性

Keywords：development assurance level；functional independence；item development independence

0 引言

高度综合复杂的系统在现代民用飞机上的广泛应用增加了民机研制过程中出现研制错误和非预期影响的可能性。在工业实践中，采用有限的测试表明这类系统在设计和研制过程中不存在研制错误是不实用的，也是不可能的。所以，为了确定这类系统能够满足安全性目标，航空业通过实施研制保证过程，以确保系统研制已经以一个十分规范的方式完成，并且产生影响飞机安全性的研制错误的可能性已经被限制[1]。研制保证过程的严格程度则通过研制保证等级度量。失效状态等级越严重，其对应的用于减轻失效状态所需的研制保证等级越高，研制保证等级越高，研制成本就越高，研制周期就越长。

本文首先给出了与研制保证等级相关的定义，其次说明了研制保证等级分配的基本原则和降级分配原则，然后给出了考虑功能独立性和项目研制独立性时研制保证等级的分配方法，实现了合理降低研制保证等级，最后通过实例说明了考虑独立性的研制保证等级分配的实施方法。

1 研制保证的相关定义

1) 项目：具有界限和明确定义接口的软件或硬件。

2) 功能失效集（FFS）：会导致顶层失效状态的单个成员或被认为相互之间独立的某一组成员。一个FFS相当于故障树的最小割集。

3) 功能研制保证等级（FDAL）和项目研制保证等级（IDAL）：功能研制保证等级定义了产生功能需求过程的严格程度。项目研制保证等级指对项目实施的研制保证任务的严重程度等级。

4) 功能独立性和项目研制独立性：功能独立性是一种属性，也就是在功能不同的情况下，保证了功能需求不会受到一个公共错误的影响。项目研制独立性也是一种属性，是指在项目不同的情况下，使发生各自研制项目间的共模错误的可能性降到最低程度[2]。

2 研制保证等级分配的基本原则和降级分配原则

采用功能失效集（FFS）的概念作为分配研制保证等级的系统性方法。

1) 对于灾难性的失效状态

a. 如果是由单个成员组成的功能失效集，即一个飞机/系统功能或项目的一个可能的研制错误导致，则该成

员的研制保证过程被分配为A级。

b. 如果是由多成员组成的功能失效集，即两个或多个独立研制的飞机/系统功能或项目可能的研制错误组合共同导致，则其中任一个研制保证过程被分配为A级，或者其中两个研制保证过程至少被分配为B级。其他独立研制的飞机/系统功能或项目的研制过程等级不低于C级。用以确保两个或多个独立研制的飞机/系统功能或项目独立性的研制保证过程仍应是A级。

2) 对于危险性的失效状态

a. 如果是由单个成员组成的功能失效集，即一个功能或项目的一个可能的研制错误导致，则该成员的研制保证过程至少被分配为B级。

b. 如果是由多成员组成的功能失效集，即两个或多个独立研制的飞机/系统功能或项目可能的研制错误组合共同导致，则其中任一个研制保证过程至少被分配为B级，或者其中两个研制保证过程至少被分配为C级。其他的独立研制的飞机/系统功能或项目的研制保证等级不低于D级。用以确保两个或多个独立研制的飞机/系统功能或项目独立性的研制保证过程仍应是B级。

3) 对于较大的失效状态

a. 如果是由单个成员组成的功能失效集，即一个功能或项目的一个可能的研制错误导致，则该成员的研制保证过程至少被分配为C级。

b. 如果由多成员的功能失效集，即两个或多个独立研制的飞机/系统功能或项目可能的研制错误组合共同导致，则其中任一个研制保证过程至少被分配为C级，或者其中两个研制保证过程至少被分配为D级。用以确保两个或多个独立研制的飞机/系统功能或项目独立性的研制保证过程仍应是C级。

4) 对于较小的失效状态

a. 如果是由单个成员组成的功能失效集，即一个功能或项目的一个可能的研制错误导致，则该成员的研制保证过程至少被分配为D级。

b. 如果是由多成员组成的功能失效集，即两个或多个独立研制的功能或项目的研制错误组合共同造成，则其中一个研制保证过程至少被分配为D级。

3 研制保证等级分配流程

3.1 FDAL和IDAL的分配概述

如图1所示，FDAL和IDAL的分配是一个自上而下的过程。首先，在初步飞机安全性评估（PASA）/初步系统安全性评估（PSSA）中根据功能危害性评估（FHA）的失效状态严重等级分配顶层FDAL。将顶层功能分解成多个子功能后，结合系统架构和独立性，分配子功能的FDAL。将每一个子功能进一步分解或分配给项目，并分配项目的IDAL。

如果不考虑系统的架构和独立性，支持顶层功能的所有子功能的FDAL及其架构中所有项目的IDAL的等级都与顶层功能的FDAL相同。该方法是最严格的研制保证等级分配方法。

3.2 基于系统架构和独立性的研制保证等级分配

如果初步安全性评估表明系统架构对于设计错误所产生的影响提供了包容性，那么研制保证活动能够在降低的严格度下进行，在将顶层功能分配成两个或多个独立子功能的过程中，可能会出现分配给至少一个子功能的FDAL比顶层功能的FDAL低的情况。在IDAL分配时，项目本身不包括用于减少潜在研制错误的架构特性。

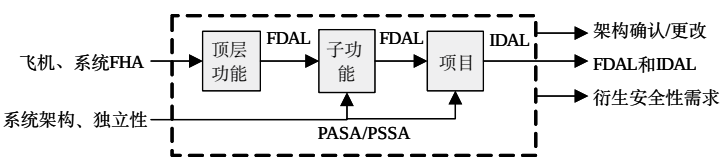

图1 FDAL和IDAL分配过程概述

考虑系统架构和独立性的研制保证等级分配步骤如下。

1) 确定顶层失效状态，为顶层功能分配研制保证等级。将飞机和/或系统FHA中的失效状态确定为顶层失效状态。顶层失效状态所对应的功能为顶层功能，顶层功能的FDAL等级为顶层失效状态最严重的等级。其中，灾难性失效状态为A级，危险性失效状态为B级，较大的失效状态为C级，较小的失效状态为D级，无安全影响的失效状态为E级[3]。E级顶层失效状态不用进一步分析。

2) 确定顶层失效状态的所有功能失效集。对每个顶层失效状态执行故障树分析，故障树的最小割集相当于FFS。只要FFS成员满足功能独立性，可以对给定的FFS成员分配低于顶层失效状态严重等级的FDAL。

3) 独立性判断和研制保证等级分配

a. 当功能和项目研制都具有独立性时，使用研制保证等级分配中与顶层失效状态类型相对应的降级原则分配FDAL，然后以上层研制保证等级为基准，用相同方法分配IDAL。

b. 当功能独立、项目研制不独立时，如果使用非独立的项目（或者部分项目是不独立的）实现独立的功能，并且非独立项目的研制错误可以导致某些或所有功能间的共模错误，则需要将“共同”的非独立项目的IDAL分配为最高的顶层功能FDAL等级。对于以相同设计实现的各个功能应进行隔离，以确定FDAL分配所要求的功能独立性，并避免一个功能研制过程

中的错误影响其他相同设计的功能。隔离功能的研制保证等级应分配为与研制中影响最严重的错误相对应的FDAL。如果没有采用隔离或者不能证明这些功能间的独立性，则相同设计的IDAL可以强制将设计中所实现功能的FDAL重新分配为该相同设计的IDAL。

c.当功能不独立、项目研制不独立时，FDAL和IDAL相同且都等于顶层功能的FDAL。

d. 当功能不独立、项目研制独立时，顶层功能由一个系统功能实现，该功能由多个相互独立的项目组成。根据基本原则对系统功能FDAL分配顶层功能FDAL。用与顶层失效状态类型相对应的研制保证等级降级分配原则分配项目IDAL。

4 应用实例

以图2所示的故障树为例，说明基于独立性的研制保证等级分配方法的实施过程。顶层功能失效状态FC2为灾难性失效状态，由F1功能失效和F2功能失效组合导致。F1和 F2具有功能独立性，项目2的研制错误能够导致F1功能和F2功能同时失效，从而导致顶层失效状态发生。

具体系统架构和独立性的研制保证等级分配步骤如下。

1) 确定顶层失效状态，为顶层功能分配研制保证等级

FC2为灾难性顶层失效状态，根据研制保证等级分配的基本原则，FC2的FDAL被分配为A级。

2) 确定顶层失效状态的所有功能失效集

根据图2的故障树，得到该故障树的6个最小割集，即功能失效集，分别为F1和F2，F1和I2，F1和I3，F2和I1，F2和I2，I2。

3) 独立性判断和研制保证等级分配

F1功能和F2功能独立，根据研制保证等级的降级分配原则，F1和F2的研制保证等级有三种分配方法，如表1所示。

将F1和F2的FDAL分配给项目。由于项目2研制中的错误能够同时引起F1和F2功能失效，根据3.2节中的3)b，I2的IDAL应该被分配为最高的顶层功能FDAL等级A级。根据表1中三种F1和F2的FDAL分配结果和第2节中的研制保证等级的降级分配原则1b，为I1和I3分配IDAL，结果如表2所示。

表1 F1和F2的研制保证等级分配

FDAL分配	
F1	F2
A	C
C	A
B	B

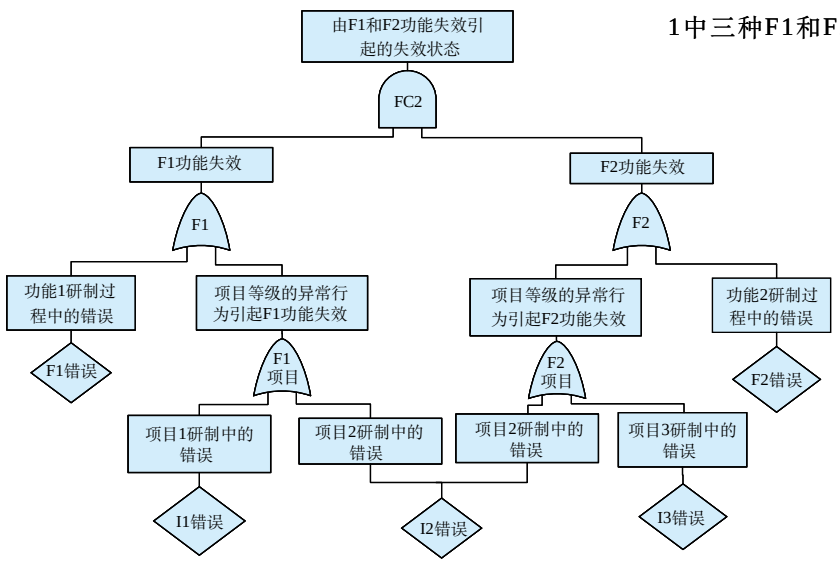

图2 基于独立性的研制保证等级分配故障树实例

表2 项目研制保证等级分配

FDAL分配		IDAL分配		
F1	F2	I1	I2	I3
A	C	A	A	C
C	A	C	A	A
B	B	B	A	B

5 结论

在民用飞机高度综合复杂系统的研制过程中，通过实施具有合适严格度的研制保证过程能够将研制错误减至最少，从而满足安全性目标。根据导致顶层失效状态的功能失效集中各成员间的功能独立性和项目研制独立性，可以在安全性可接受范围内，根据研制保证等级的降级分配原则将分配给飞机/系统功能和项目的研制保证等级适当的降级，从而能够节约研制成本，缩短研制周期。 AST

参考文献

[1] SAE ARP 4754. Certification Consideration for Highly–Integrated or Complex Aircraft Systems [S]. U.S.A: SAE International, 1996–11.

[2] SAE ARP 4754A. Guidelines for Development of Civil Aircraft and Systems [S] . U.S.A: SAE International, 2010–12.

[3] SAE ARP 4761. Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne System and Equipment [S]. SAE,1996–12.

作者简介

李亚男，工程师，硕士，研究方向为飞行操纵系统的安全性和可靠性。

金平，工程师，硕士，研究方向为电传飞控系统电子硬件与软件。