

DOI:10.19452/j.issn1007-5453.2017.02.049

研制保证等级分配原则及应用研究

华铭*, 景玉国, 王思静

中航飞机股份有限公司研发中心, 陕西 西安 710089

摘 要: 研制保证等级是有效降低现代民用飞机研制错误的重要技术。本文通过对ARP 4754A的研究, 介绍了研制保证等级的基本概念和分配原则。同时, 结合某民用飞机型号研制保证等级分配的实际工程经验, 对设计中所遇到的问题进行了探讨和总结, 为飞机设计提供参考。

关键词: 民用飞机; 研制保证等级分配; ARP 4754A; 独立性; 适航

中图分类号: V268.7 **文献标识码:** A **文章编号:** 1007-5453 (2017) 02-0049-04

随着现代飞机系统复杂度与集成度的不断提高, 研制过程中产生错误的可能性也在增大。与元器件自身的随机失效一样, 研制过程中产生的错误也会最终影响飞机/系统的表现。但不同于随机失效可以通过计算发生概率来定量的评估, 研制错误无法通过计算概率的方法来评估其发生的可能性。因此, 针对研制错误, 应当建立一种类似于质量管理程序的方法以确保研制错误被降低至可接受水平。执行这一程序的严格程度被称作为研制保证等级 (Development Assurance Level, DAL)。针对研制对象的不同, 研制保证等级又分为功能研制保证等级 (FDAL) 和项目研制保证等级 (IDAL)。

对于民用飞机型号研制过程, 不同的DAL规定了不同数量的保证活动, 以及完成的严格程度、详细程度和独立性组织体系要求, 这些都与飞机的研制成本密切相关。因此, 设计者总是希望在满足安全性要求的前提下, 为功能和项目分配尽可能低的DAL。为实现这一目标, 行业内一直在不断研究探索。SAE ARP 4754A^[1]虽然给出了较为详细的DAL分配方法和流程, 但在实际型号应用时还是存在诸多问题。本文通过对ARP 4754A的深入研究, 对DAL分配的基本原则进行进一步的解读, 并结合某民用飞机型号实际应用经验, 给出了作者的有关见解和思考。

1 基于ARP 4754A的DAL分配原则

与原版ARP 4754^[2]基于典型系统架构的分配方法不同, ARP 4754A强调DAL的确定和分配是建立在严格的安全性分析基础上。首先, 功能危险评估 (FHA) 所识别的失效状态及其严酷度等级是整个DAL分配的前提。初步飞机/系统安全性分析 (PASA/PSSA) 中所建立的故障树模型以及分析得到的最小割集, 是DAL至上而下分配的依据。DAL主要有以下3种分配原则:

(1) 直接对应分配原则

该原则是指按照与功能或项目关联的最严酷失效状态类别来为其分配对应的研制保证等级。表1给出了与不同的失效状态严酷度类别直接对应的DAL等级。例如, 当一个功能的研制错误可能导致的最严重后果是危险的, 那么为该功能分配DAL B级。该分配原则适用于确定顶层功能的FDAL, 以及不考虑架构独立性或独立性不存在时底层功能或项目的DAL分配。

(2) 基于独立性的分配原则

显然, 单纯地按照直接分配原则得到的等级并不是工程上的最优结果。架构中独立性的存在可以有效降低单一研制错误对于顶层失效状态的贡献。因此, 当功能失效集合^[1] (FFS) 中多成员之间存在独立性时, 可按照表2中的选项1或

收稿日期: 2016-10-31; 退修日期: 2017-01-17; 录用日期: 2017-01-18

*通讯作者: Tel.: 029-86832314 E-mail: huaming0922@163.com

引用格式: HUA Ming, JING Yuguo, WANG Sijing. Research on development assurance level allocation principles and applications [J]. Aeronautical Science & Technology, 2017, 28(02): 49-52. 华铭, 景玉国, 王思静. 研制保证等级分配原则及应用研究 [J]. 航空科学技术, 2017, 28(02): 49-52.

选项2进行降级分配。其中,功能失效集合相当于故障树分析所产生的最小割集^[3],但是其成员代表潜在的研制错误而不是失效。

表1 对应失效状态严酷度类别的DAL分配原则

Table 1 DAL assignment based on failure condition severity classification

失效状态严酷度类别	相应的DAL
灾难的	A
危险的	B
较大的	C
较小的	D
无安全影响的	E

表2 失效集合独立成员的研制保证等级分配原则

Table 2 DAL assignment to independent members of a failure set

序号	顶层失效状态类别	选项1	选项2
①	灾难的	其中一个成员设为A级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于C级。	其中两个成员设为B级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于C级。
②	危险的	其中一个成员设为B级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于D级。	其中两个成员设为C级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于D级。
③	较大的	其中一个成员设为C级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于E级。	其中两个成员设为D级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于E级。
④	较小的	其中一个成员设为D级;其他成员设为其研制错误可能单独导致的最严酷影响相对应的等级,但不能低于E级。	
⑤	无安全性影响	DAL E	

例如,假设一个灾难的顶层失效状态存在一个二阶最小割集(F1,F2)。当F1和F2满足独立性要求,按照表2中的选项1可产生的分配结果为(A,A),(A,B),(A,C),(B,A),(C,A);按照表2中的选项2可产生的分配结果为(B,B)。

(3)考虑外部事件的分配原则

当顶层失效状态是由单一功能组合外部事件所导致,针对这种情况上述表1和表2中的原则都无法适用。显然,外部事件发生频率的高低会影响到与之相关功能单独失效所造成影响的大小。因此,依据外部事件发生概率的不同,得到如下表3所示的分配原则。

表3 基于外部事件发生概率的DAL分配原则

Table 3 DAL assignment based on probability of external events

顶层失效状态类别	外部事件发生概率	相关功能的FDAL
灾难的	$P > 10^{-5}$	A
	$10^{-7} < P \leq 10^{-5}$	B
	$P \leq 10^{-7}$	C
危险的	$P > 10^{-4}$	B
	$P \leq 10^{-4}$	C

2 DAL分配在民用飞机型号中的应用

按照ARP 4754A要求,对某在研民用涡桨支线客机开展了基于需求的研制保证体系建设。其中,DAL分配工作分为飞机级和系统级两部分。飞机级工作包括飞机级顶层功能FDAL的确定以及向系统级功能的分配;系统级工作包括将系统的FDAL分配至底层项目,并由此确定相关软硬件的IDAL。DAL分配层次以及对应的飞机研制流程如表4所示。

表4 DAL分配层次和工作内容

Table 4 DAL assignment layer and job content

安全性工作阶段	对应的系统研制流程	DAL分配工作
飞机级	飞机功能研制	按照表1原则确定飞机级(顶层)功能的FDAL。
	将飞机级功能分配到系统	根据PASA中故障树模型,按照表2、表3原则将顶层FDAL分配至相关系统功能的FDAL。(衍生系统功能的FDAL按照表1原则进行分配)
	系统构架研制	根据PSSA中故障树模型,按照表2、表3原则将系统FDAL分配至相关底层项目的FDAL。
系统级	将系统需求分配到项目	根据项目FDAL确定软件和硬件的IDAL。
	项目开发	按照DO-178C ^[4] 和DO-254 ^[5] 中与软硬件等级相对应的要求和流程来进行研制和验证。

3 相关问题的探究和思考

按照上述方法进行DAL分配过程中不断地遇到了各类问题,主要集中在如何准确理解标准中的关键概念以及如何合理使用分配策略。下面以3个典型示例并结合ARP 4754A标准以及工程实践,给出了对于这些问题的探究和思考。

3.1 独立性声明的问题

独立性作为能否进行降级分配的判据,在研制保证等级的分配过程中扮演着十分重要的角色。因此,为了获得正确的DAL分配结果,首先应当对于独立性有更深入的理解。根据不同的分配对象,独立性又被分为功能独立性和项目独立性。

功能独立性是指对应于不同需求集合的不同功能。如飞机地面减速功能,可以通过机轮刹车和发动机反推两种方式实现,从功能和需求的角度看,两者不存在任何交集。这表明研制过程中机轮刹车需求集合中的错误,或者对其需求解读产生的错误,只会对飞机实施机轮刹车产生影响,并不会影响飞机使用发动机反推。由此说明二者之间具有功能独立性。

项目独立性是指对应于不同设计的项目。设计上的不同包括硬软件架构、编译语言、平台及开发工具等。例如,相关重要飞行参数分别采用液晶显示器和机电伺服仪表显示,这2种方式采用了不同的技术,因此,可以认为是相互独立的。如果全部使用液晶显示方式,由于使用了相同技术,可能出现由同一个技术开发错误导致使用时同时失效情况。

因此,独立性的关键在于保证目标对象之间存在不同,但随之而来的问题是多大程度的不同可以被认为是相互独立。实际工程中很难给出一个恒定的量值作为衡量独立性的标准。针对不同的情况,差异性要求也会不同。过分追求完全不同也会造成研制成本增加。所以为了向适航局方表明功能/设备独立性,设计者应当更加注重构型状态、需求集合等部分的不同,而尽量避免采用物理冗余、不同团队等不能有效增加独立性的方式。

3.2 针对简单部件的分配问题

DAL分配的重点在于确定底层软件和复杂电子硬件的等级,对于其他简单部件(包括机械组件、机电设备、伺服阀等)在分配过程中如何处理是一个被时常提及的问题。ARP 4754A中提到对于简单部件,如果能够完全通过试验和分析来保证,则可以认为它们具有与DAL A等效的置信度水平^[1]。基于该准则给出下述处理方法建议。

首先,为保持分配流程的完整性和可追溯性,应当对于DAL分配模型中的所有成员按照正确的原则进行等级分配。以失效状态“丧失座舱余压释放功能”为例,在着陆阶段发生的影响等级为Major。通过故障树分析(如图1所示)可知该失效由压调系统和舱门系统共同导致,故在满足独立性的条件下,可以给压调系统和舱门系统均分配DAL D级,并将作为顶层输入分别传递给两个系统的设计人员。由于舱门系统只包含简单机械部件(如图2所示,只包含泄压阀门、连杆、密封条、传感器等),设计人员可不按照ARP 4754A研制流程进行研制和验证,但必须通过充分的试验和分析表明研制过程中的错误已被完全消除,从而相当于满足了DAL A级的要求,自然也满足顶层分配下来DAL D级的目标。

3.3 多次分配降级的问题

针对本文表2分配原则,需特别注意在每次分配过程中

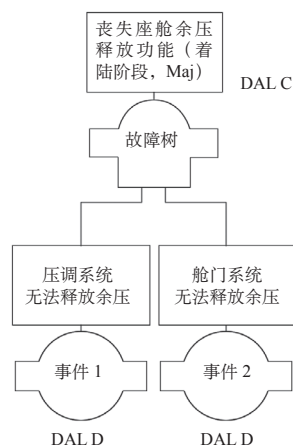


图1 DAL分配示例

Fig. 1 An example of DAL assignment

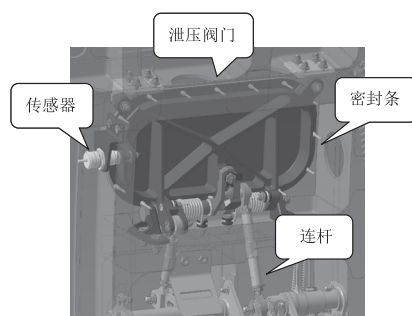


图2 舱门余压释放机构示例

Fig. 2 An example of pressure release device on the door

使用时,都应当使用顶层失效状态所对应行原则^[1]。例如,当顶层失效状态为灾难性时,往下的每一层分配,都应当使用表2中的原则①。即至少包含一个DAL A成员或者两个DAL B成员,其他成员至少是C级,不允许出现D级的分配结果。

图3给出了两种违背这一条准则的典型错误。示例(a)

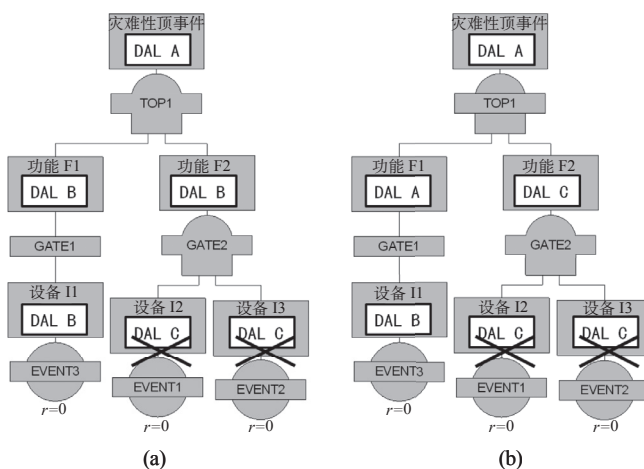


图3 研制保证等级分配中的多次降级错误示例

Fig. 3 Examples of repetitious reduction errors of DAL assignment

中,在第三层的分配结果中出现了一个成员为DAL B级,两个成员为DAL C级。这是因为没有继续使用表2中的原则①,而是错误的使用原则②造成的。同理,示例(b)同样在第三层分配时候未能保持与顶层失效状态使用相同的分配原则,从而出现了DAL D级的错误分配结果。在实际工程中应当避免此类分配错误的发生。

4 结束语

研制保证技术的使用已成为满足安全性需求和适航审定要求的有效方法。在满足安全性和适航要求的前提下,采用合理的分配策略可以降低研制成本。本文立足于对标准规范的研究和理解,同时结合某民用飞机型号实际应用经验,梳理出适用的分配方法和流程。另外,总结了与DAL分配过程相关的典型问题,给出了探究过程和相关见解。

AST

参考文献

- [1] Society of Automation Engineering. SAE ARP 4754A; Guidelines for development of civil aircraft and systems[S]. USA; Society of Automation Engineering S-18 Committee, 2010: 37-45.
- [2] Society of Automation Engineering. SAE ARP 4754;

Certification considerations for high-Integrated or complex aircraft systems[S]. USA; Society of Automation Engineering S-18 Committee, 1996.

- [3] Society of Automation Engineering. SAE ARP 4761; Guidelines and methods for conducting the safety assessment process on civil airborne system and equipment[S]. USA; Society of Automation Engineering S-18 Committee, 1996.
- [4] Radio Technical Commission for Aeronautics. RTCA DO-178C: Software considerations in airborne systems and equipment certification[S]. USA; Radio Technical Commission for Aeronautics SC-167 Committee, 2011.
- [5] Radio Technical Commission for Aeronautics. RTCA DO-254; Design assurance guidance for airborne electronic hardware, appendix B [S]. USA; Radio Technical Commission for Aeronautics SC-180 Committee, 2000.

作者简介

华铭(1989—) 男,硕士,助理工程师。主要研究方向:系统安全性评估

Tel: 029-86832314

E-mail: huaming0922@163.com

Research on Development Assurance Level Allocation Principles and Applications

HUA Ming*, JING Yuguo, WANG Sijing

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

Abstract: Development assurance level is an important technique to effectively reduce the development errors of current civil aircraft. Through the research of ARP 4754A, the basic concepts and assignment principles about development assurance level was introduced. Meanwhile, based on the actual engineering experience in a civil aircraft program, some problems encountered during the design were discussed and summarized as a reference.

Key Words: civil aircraft; development assurance level assignment; ARP 4754A; independence; airworthiness

Received: 2016-10-31; Revised: 2017-01-17; Accepted: 2017-01-18

*Corresponding author. Tel. : 029-86832314 E-mail: huaming0922@163.com