空客A380飞机可靠性工程中的确认和检验方法

Validation and Verification Methodologies in A380 Aircraft Reliability Program

杨宇航　刘钡钡／总参谋部陆航研究所

摘　要：叙述了空客A380飞机可靠性工程中的确认和检验过程的方法论，并就具体案例进行了分析，介绍了发动机联盟如何将确认和检验过程应用于GP7200发动机的设计中以满足安全性和可靠性的要求。

关键词：部件；格式化；确认和检验；飞机系统安全；可靠性；A380
Keywords：component；formatting；validation and verification；aircraft system safety；reliability；A380

0 引言

空客A380超大型飞机(VLA)可运载的旅客超过500名，最大起飞重量(MTOW)大约为560吨，不仅是有史以来建造的最大的民航客机，而且是拥有先进技术的飞机。先进技术带来运营经济性增长的同时，也改善了飞机的维修性能。可以说，A380创建了航空业的新标准，也开创了商用飞机可靠性和维修性工程(R&M)的新纪元。

维修工作的首要目标是获得最高水平的适航性，但这却与在最小实际成本的前提下获得较高的飞机可用性相矛盾。A380设定的关键可靠性目标是在服役两年内达到99%的使用可靠性，比空客A340系列的使用可靠性高出许多。

在飞机变得更大，航程更远的同时，如何满足运营经济性的要求变得更有挑战性。因此，R&M在A380的设计中占有举足轻重的地位。部件的可靠性必须与维修成本的目标相一致，这就给A380的设备供应商提出了富有挑战性的目标。为了在设计早期就达到技术的成熟，系统和部件的可靠性成为非常关键的因素。一般通过两种途径来确保飞机成熟，即设计的可靠性确认和检验(V&V)过程以及引入密集、加速的可靠性试验。

在嵌入式系统的发展过程中，V&V过程能够判断系统是否符合计划书的要求、输出是否正确。空客公司在A380飞机和供应商层面的安全评定过程中都运用了V&V过程，这是飞机层面安全评定首次用于大型的商用飞机中。该过程定义了飞机层面的功能和相关的故障条件，并分配至各个系统，进而对从事系统和设备开发各个层面的供应商提出要求。V&V过程的结论显示其结果是所有关键工程决策的基础。为了确保飞机在投入使用前能够达到设定的可靠性目标要求，空客公司已经在美国联邦航空局(FAA)的安全要求体系下对A380进行了更多的试验。

本文在对公开发表的相关文献研究的基础上，论述了包括目标和构架的V&V过程的基本知识和方法论，结合与A380安全性过程相关的各种分析细节，搜集并讨论了V&V方法在A380安全性过程中的应用。最后，列举了发动机联盟如何在GP7200的设计中运用V&V过程的案例。

1 用于A380的R&M设计的确认和检验方法论

空客公司为飞机的使用可靠性制定了最高水平的要求(TLAR)，并将可靠性要求分配至各系统、子系统和部件，这种要求是一个伴随着体系结构演化的反复迭代的过程。为了取得最优化的结果，在各设计过程中都采用了仿真方法。关键工程设计基于的是复杂数学理论的预测，为了判断数学模型的稳定性和安全性，空客公司对所有预测都运用了V&V过程。

美国机械工程师协会(ASME)定义了V&V过程的目标，并为评定模型和计算科学中仿真的正确性和可靠性制定了一系列标准。

确认过程判断数学模型是否能够

足够好地描述实际情况，以便做出决策。确认包括需求确认和产品确认。需求确认的目的在于确保产品的需求是充分正确和完整的，以便在项目限制条件（如成本、进度表）下，满足安全性和顾客的需要。产品确认是检查产品是否满足顾客提出的明确的需要。

检验过程判断的是计算模型与执行结果是否充分、准确，检验过程保证系统的执行满足检验的要求。设计检验的目的在于证明设计是符合需求的。设计检验还是一些决策的关键性输入，这些决策包括设计方案的选择以及项目是否推进至下一阶段的判定。空客A380飞机设计的V&V过程如图1所示。

2 适航性确认过程的V&V方法论

适航性确认过程的主要目标是确保飞机服从适当的适航性要求。为了适应多数调整的指导方针，飞机制造商必须创建一个安全性的实例，以此来证明系统的安全性。该安全性实例是一个系统整个生命期内相关的所有安全性活动的记录，如图2所示，确认和检验是系统安全性证明过程的组成部分。

安全性实例是一个用于支持确认的重要文件，包括一系列论点，支持论点的论据是有关设计安全性的分析证据和试验证据。在安全性实例中，调整的权限关注的是所有潜在的故障均被定义，且采取妥善措施进行了处理。而且，安全性实例还必须说明采用并正确执行了合适的研发方法。安全性需求的说明书、危险和风险分析的结果、检验和确认策略以及所有确认和检验活动的结果等条目都应该包含在安全性实例中。

确认和检验是由进行设计、开发和执行的厂家来进行的，但有时也由一家独立的测试公司来完成。目前已经被认可的测试包括一批在室内进行的静态和动态测试技术的步骤。

3 确认和检验过程

V&V过程主要通过与测量数据进行对比来实现，前提是假设测量是正确的、有价值的，能够作为参考。但实际测量可能存在各种问题，因此必须对假设进行仔细的论证。另一方面，一些测量特征并不能作为数值计算正确性的论据。

连续的确认和检验过程可以按照文献来实现：

1） 结合论证和经验，使出现错误结果的可能性最小；

2） 如果条件允许，运用其他方法和工具进行核查；

3） 仔细遵照使用方法的原则和限制条件；

4） 持续与可用的（可靠的）测量结果进行比照。

图3列出了ASME确认和检验委员会的包含检验和确认的数学模型流程，左侧为试验，右侧为计算模型。

对设计仿真结果进行测试和检查非常重要，不能简单地自动承认设计仿真结果。图4所示为确认金字塔，图5的架构说明了反复迭代的V&V过程。

金字塔的最底层为简单的校准试验。它们中的一部分被称为鉴定合格（验证）试验，是证明符合调整需求的基础。试验数据和计算数据的对照是基于一个特有的度量（如何测量差异）和拒绝准则的。度量和准则必须与预测及在预测基础

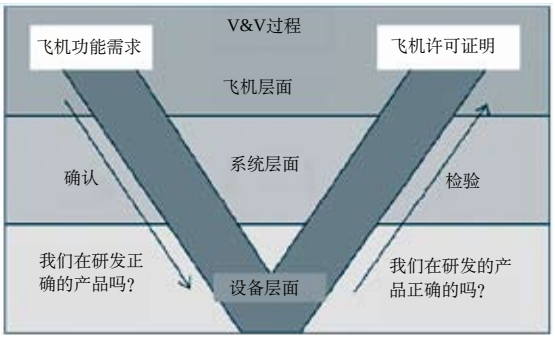

图1 空客A380飞机设计的V&V过程

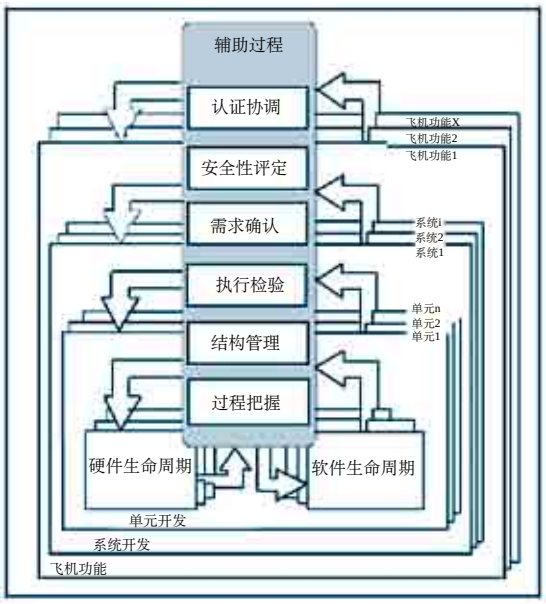

图2 飞机实际运用执行流程的安全性实例

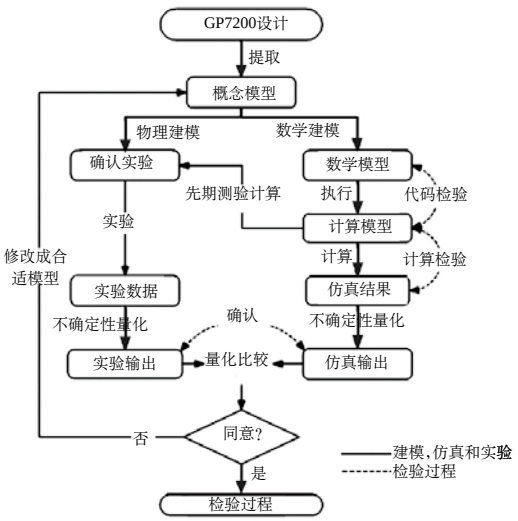

图3 ASEM的关于V&V在数学模型过程中的相互配合的详细说明图

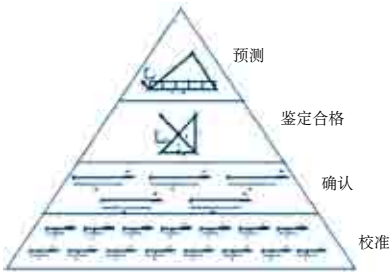

图4 确认金字塔

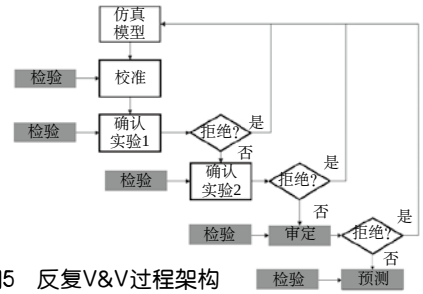

图5 反复V&V过程架构

表1 在各层面实施的安全性分析

飞机层面	系统层面	设备层面
功能危险分析(FHA) 区域安全性分析(ZSA) 特定危险分析(PRA) 共同模式分析(CMA) 人因危害分析(HHA)	FHA 初步系统安全性分析(PSSA) 内在危害分析(IHA) 环境条件危害评定(ECHA) 系统安全性分析(SSA) 结构件危害评定(RASP) CMA 主要最低的设备清单(MMEL)/构造偏离清单(CDL)	故障模式及影响分析(FMEA) 故障模式及影响摘要(FMES) 安全性评定 可靠性预测 IHA+ECHA 设备CMAs

上所做出的决策直接相关。如果判断的标准大于给定的偏差,将影响一些门槛条件,则模型应被拒绝。如果模型在确认金字塔的某一层面被拒绝,则模型必须进行修改,并通过所有的比该层面低的层面的测试,这可能需要更多的试验。如果模型在确认金字塔的某一确定层面没有被拒绝,则进行更高层面的判定。

4 A380安全系统评定过程

系统评定过程经常出现在概念设计过程和设计过程中,包括需求的产生和需求的检验,它们支持着飞机的研发活动,确保在飞机的功能和系统中列出可能的关联危险。

V&V过程在A380安全系统评定过程中扮演着非常重要的角色,空客公司进行了飞机层面的飞机安全性过程,它是反复迭代的V&V过程。空客公司在飞机、系统和设备三个层面上进行了安全性和可靠性分析。表1列出了飞机和系统层面的安全性过程的分析详情。图6展示了A380飞机的安全性分析流程模型。

4.1 功能危险分析(FHA)

这是空客公司第一次在飞机层面上进行FHA,也是第一次由一家飞机制造商来进行飞机层面的FHA。空客公司在飞机系统研发的初始阶段就进行了这项分析,这项工作是在飞机功能描述的基础上进行的,然后,按照飞机各系统的功能分配,对每个子系统实施了FHA。这两个层面的FHA实施都是基于相同的准则的。

FHA是一种预测技术,致力于探索一个系统各个部分的功能故障的影响。实施FHA的目标在于清晰地确定危险功能故障的条件。FHA的实施步骤包括:

1) 定义飞机功能(如地面减速);

2) 对功能相关的潜在故障进行分类;

3) 对各故障条件相关的危害进行分类;

4) 确认各个功能相关的目标;

5) 为每个后续的层面生成安全性需求;

6) 生成系统层面的安全性活动的输入(FHA、PSSAs等);

7) 联系各个功能,基于系统层面的危险程度,决定DAL。

FHA的创建取决于设计团队总体的知识和经验,可能需要众多专家的协商。表2的示例展示了功能及需要考虑的相关的故障条件。

通过FHA和故障树,故障条件也可向下分解。例如,对于不能控制飞行路径的故障条件,可以向下分为(人员,燃料等)丧失准备、疏忽、液压动力丧失、飞行控制丧失和飞行控制失效。影响安全的故障条件最终应该与目标以及建议的措施一起提出来。

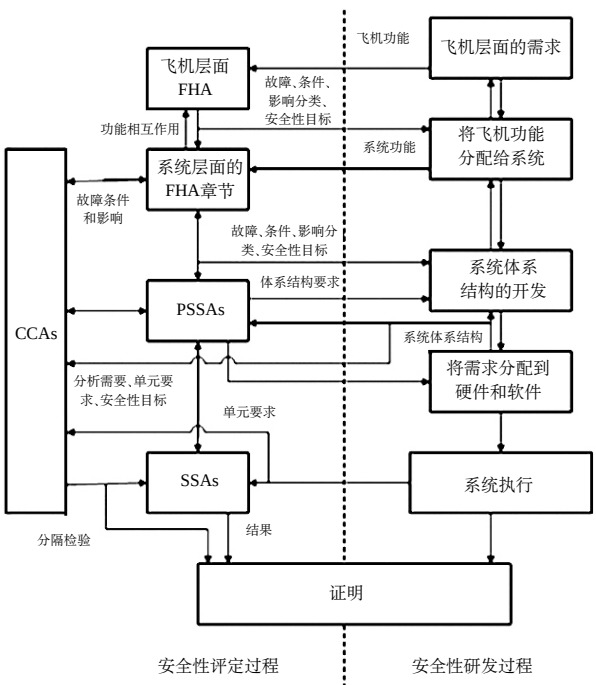

图6 A380飞机的安全性分析流程模型

表2 功能及故障条件示例

功能	故障条件
控制航线	无法控制航线
控制着陆和滑出	无法控制着陆和滑出
控制推力	无法控制推力
控制舱内环境	无法控制舱内环境
火灾防护	失去火灾防护

虽然FHA是预测飞机功能故障和故障影响的有效工具，但是要在飞机层面运用FHA还是困难的。对于相互独立的功能而言，往往能很好地实施FHA，但是大多数飞机的各项功能是由高度整合的系统来完成的，与独立性的要求相去甚远。当飞机层面的各项功能与其他系统整合时，就应该重新评估FHA，定义并区分出与多个功能相关的故障条件。如果FHA由面向系统的模块来构建，就需要描述飞机层面和系统层面之间的危险和故障。

4.2 初步系统安全性分析(PSSA)

PSSA用于检验系统体系结构，测定故障条件的完整性，并从FHA中提取S/R需求，也被用于确认从FHA提取出的S/R需求。PSSA是伴随整个系统开发的迭代分析。通过FTA，空客公司的PSSA说明偶然故障模型的组合可以再现故障产生的环境条件。故障产生的环境条件也可以通过独立图表、Markov分析或其他分析方法确定出来。

A380在PSSA中采用了内在危害分析(IHA)和环境条件危害评定(ECHA)两种分析方法。

4.3 经常性原因分析(CCA)

早期的研发过程中，执行评定可能会引入共因，用于解释多重飞机故障条件或伴随失效而来的系统间的联系。为了确定系统共因缺陷的位置，CCA是必需的。在飞机系统中使用自动防故障装置设计至关重要，通过添加冗余系统，进而提高可靠性来实现上述目标。CCA打破界线来处理共因缺陷，制定要运用的缺陷抑制策略，并提供理性的故障覆盖率。

对于A380飞机而言，空客公司为便于评定，将CCA细分为4类。

1) 区域安全性分析(ZSA)：在飞机上进行，以保证区域以内和区域之间的安全。迭代分为三个阶段，数学实体模型的建立、典型实体模型的重构以及飞机上的分析。

2) 特定危险分析(PRA)：针对特定的对飞机层面有潜在影响的危险进行分析。每个分析过程都包括确定一个验证过的危险模型，对模型的响应进行研究。A380共有22个PRA。

3) 共同模式分析(CMA)：为判定假设独立的功能以及故障模式是精确独立的提供证据。通过使用FTA，定义CMA需求，设计分析了安全性和设计过程文档的结果和反馈。

4) 人因危害分析(HHA)：在系统脆弱性的增长是与人相关的假定下，用于分析设备的可靠性。空客公司采用FMEA来确定由人工错误导致的设备故障的影响，后续的分析将确定错误的层面。

4.4 系统安全性分析(SSA)

SSA的分析过程与PSSA非常类似，但是它们的目的不同。PSSA用于获取系统和单元安全性的需求，而SSA证实使用的设计满足安全性的需求。SSA用于对PSSA的结果以及在PSSA中要求的任何添加的测试进行整合。SSA分析方法包括FTA、FMEA、Markov分析和独立图表。

4.5 检验过程

检验是判断一个计算模型是否准确反映了底层的数学模型及其求解方法的过程，检验的目的是查明每个层面的运行是否满足其特定的需求。

检验过程保证系统的运行满足经过确认的需求。检验活动主要在计算代码开发循环的前期进行，当代码在后续进行了修改或加强时，必须重复这些确认活动。检验包括检查、回顾、分析、测试和按照检验计划进行的服务体验。FHA故障条件的检验在PSSA、ICMA和SSA评定的结果中反映。图7描述了检验过程，该过程比较了代码中的数值解决方法与各种高精度解决方案。

4.6 确认过程

确认过程的目的在于确保需求的正确性和完整性，从而保证飞机满足适航性需求。如AIAA指导中所论述的，确认是从模型计划的用途出发，确定模型反映真实世界的程度，通过对计算结果与实验数据的比较来进行评定。

系统需求的缺陷主要来自歧义、不正确的描述，或者不完整(省略)的描述三方面因素。确认过程充分涵盖了所有潜在的不足之处。需求检查可以确保需求必要而且充分，是确认的重要方面。确认过程的进一步目标是限制系统中的非设计功能与接口系统中的非设计功能出现的可能性。

需求和假定应该针对每个层面进行验证，也应该涉及所有有意义的技术学科，包括在飞机功能层面、系统层面、零部件层面的需求确认和FHA确认。一般高层面的需求和假定确认是低层面确认的基础。通过比较模型预测结果与确认实验结果来作出评定，如果比较的结果符合要求，则模型被视为通过确认，模型拥有计划中的作用。图8对确认过程进行了描述，该过程比较了模型的计算结果与实验数据的仿真结果，实验数据是通过各种渠道获得的。

5 A380结构设计中的V&V过程

计算刚体力学在飞机结构设计中扮演着重要的角色，包括数值预测和仿真，

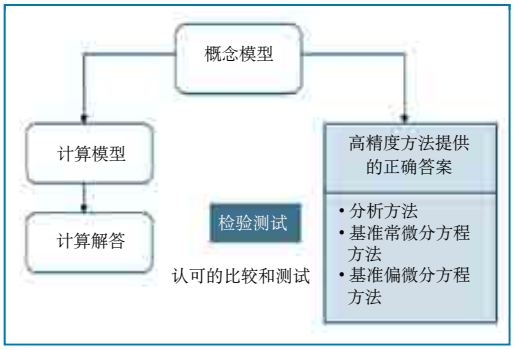

图7 检验过程

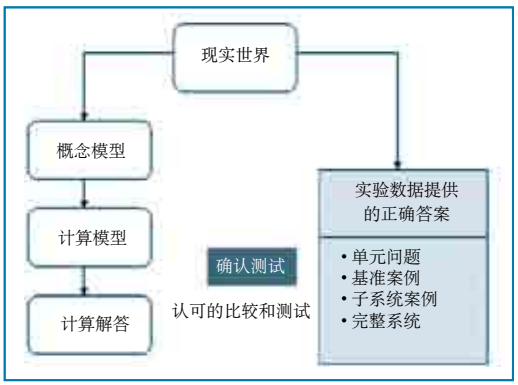

图8 确认过程

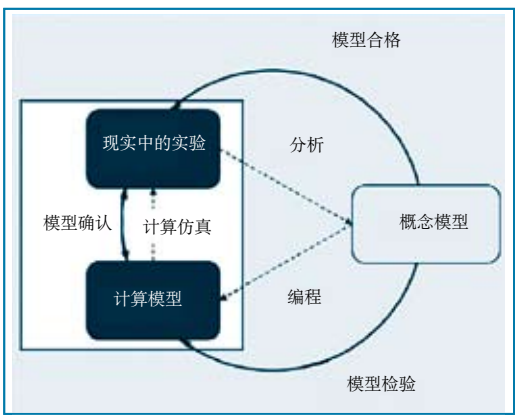

图9 建模和仿真流程

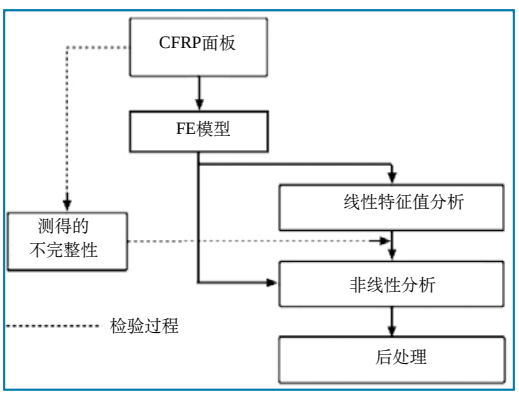

图10 分析流程

其中的V&V过程被用于提供和量化数学建模以及相应的仿真结果的可信性确认。检验通过比较数值方法和分析或高精度基准方法来确定和移除模型中的错误。而确认通过比较数值方法和实验数据来量化模型的准确性。简而言之，检验处理的是与模型相关的数学问题，而确认处理的是与模型相关的物理学问题。

下面介绍A380复合材料V&V过程的案例，该案例基于空客公司的研究和科技出版物。

A380结构设计中，重量是最重要的因素。在不损害成本和结构寿命的前提下，减少飞机结构的重量是A380设计的关键。空客公司通过在飞机的主要部件上使用更多的复合材料来达到这一要求。例如，机身结构中使用的CFRP材料，在压缩情况下损坏后，由薄壁梁加强的CFRP面板的许可承载能力受到其弯曲载荷的限制。研究人员建议通过扩展新的稳定性设计方案，从而允许在极限负载下材料的后挫曲。

这个设计过程引入了仿真技术来确定CFRP面板的弯曲特性，V&V方法用于提供仿真结果的可信性。

图9展示的萨金特圆用于演示与模型和仿真工作相关的确认和检验内容。在上述案例中，通过FEM来控制引导模型的建立活动，由FEM导出了数学模型。通过考量真实世界需要描述的部分，提取了数学模型。案例使用了不同种类的控制步长的牛顿迭代方法。通过编程，将数学模型演化为引入初始条件、边界条件、材料特性和计算模型几何形式描述的数值计算。检验活动是用于运行计算模型从而确信数学模型已被转换为正确的计算模型的检查和抽样问题。整个过程可以简略地用图10来描述。

在运用计算模型之前，确认是确保选择的方程组能够合适地描述复杂结构的活动。为了确保模型的正确，将仿真结果与实验结果进行了比较，如图11所示。

6 GP7200发动机的V&V过程

飞机投入使用时具有成熟的可靠性，是世界主要航空公司对制造商的要求之一。发动机联盟在设计过程中就遵从V&V过程，使发动机在使用前达到了要求的可靠性。

在详细设计阶段或如图12所示的阶段0，GP7200发动机中的设计分析包括任务/推进循环仿真、空气动力学建模、结构评估以及控制建模和评估等。在这个过程中，要进行代码的检验和计算的检验，并在仿真输出结果中总结。另一方面，为了确信计算模型是合适的，要进行实验测试。而将计算模型的

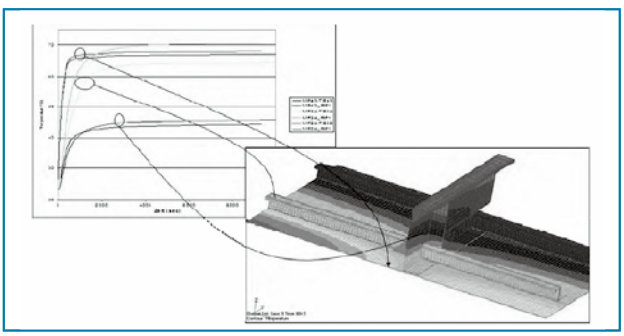

图11 实验和计算的对比

阶段 0 详细设计	阶段 1 发动机证明	阶段 2 使用准备	阶段 3 使用和保障
 数学模型和计算模型间的代码检验 计算模型和仿真输出的计算检验	• 发动机确认测试 • 747飞行测试台 • 耐力 • 风扇叶片甩出 • FAA 鸟类撞击测试 • FAA 阻塞物忍耐力测试 • LP 应力等 	FAA证书 A380/GP7200首飞	GP7200 进入使用

图12　GP7200设计和制造流程

预测与实物测试的结果进行对比则是确认活动。确认和鉴定测试用于说明产品符合说明书和飞行安全原则。这是客户最终认可的基础。

图13显示了确认金字塔。从飞机到独立零部件的各个层面，都实施了GP7200的确认过程。发动机联盟在GP7200组件的实验台测试中进行了大量的投入，这些测试是可靠性策略的一部分，目的是通过不断进行的测试来完善技术。

在飞机层面上，发动机联盟通过在双发飞机延伸航程运行性能标准（ETOPS）上进行飞行测试来考量GP7200的耐久力。通过使用波音747的飞行测试台，来评估发动机节流阀的响应和高空重新点燃特性，进而优化余量操纵图表。在发动机层面，GP7200进行了风洞测试，以此测量发动机部件的机械应力水平和振动水平等。对发动机的主要组件也进行了密集的测试，如风扇测试、核心发动机测试、高压压缩机和高压涡轮机测试等。最后，在测试实验室中进行了独立零部件的确认，以分析材料和结构应力状况。

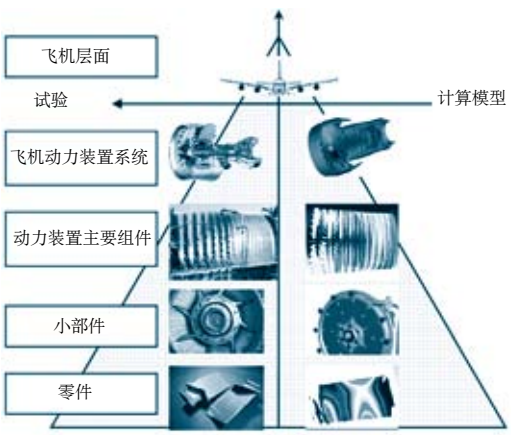

图13　发动机确认金字塔

7 总结

本文综述了空客A380项目的确认和检验方法。在V&V方法中，针对安全性和可靠性，进行了大量的分析，包括数学模型、计算模型的建模过程，伴随功能危害分析和系统安全性分析的仿真技术，以及所有其他的确认实验和测试。

可靠性评价也包括Markov分析、FMEA、FTA、独立表格和其他种类的分析。通过在设计的前期阶段实施V&V过程，可以明显缩短飞机的研发周期，使可靠性预测更加可信。V&V方法是贯穿飞机服务生命期的迭代的延续过程。文中列举了发动机联盟在GP7200上实施的V&V方法，这些方法的实施，使GP7200在进入使用之前的可靠性就超越了FAA的预期要求。

随着A380的投入运营，在安全性和可靠性工程中实施确认和检验方法被证明是卓有成效的。第一次在商用飞机的飞机层面上实施V&V过程，不仅证明对A380是有效的，而且也为新飞机的研发提供了参考。该方法也可能被运用于其他航空航天系统的设计或需要高安全性的产业当中。 AST

参考文献

[1] Arthasartsri Supanee, He Ren. Validation and verification methodologies in A380 aircraft reliability program[C]. The Proceedings of 2009 8th International Conference on Reliability, Maintainability and Safety(Vol. Ⅱ). Australia: 2009.

[2] Fendt M.A380 – reliability, maintainability, supportability – on target?[J]. Aircraft Technology Engineering & Maintenance. 2006(2/3).

[3] Cutler D,et al. A380 maintenance status report[J]. Airbus World FAST Magazine, Vol.28.

[4] AIAA. guide for the verification and validation of computational fluiddynamics simulations[Z]. American Institute of Aeronautics and Astronautics.Reston, VA:1998.

[5] Dohrmann F. A380 kabinetechnologie,integration & test [R]. Hamburg: Airbus, 2006.

作者简介

杨宇航，总参谋部陆航研究所可靠性研究室主任，高级工程师，博士后。