第 1 章　系统安全性分析概述

1.1　研究背景

安全性是指不导致人员伤亡、不危害健康及环境、不给设备或财产造成破坏或损伤的能力，也可定义为系统在特定环境、条件和规定时间内，以可接受的风险执行规定功能的能力。

系统安全性是指通过采用系统分析的方法、管理原则和工程工具，分析、识别和控制系统的失效影响，提高系统的安全性，最终使系统具有最佳安全性的工作。

系统安全性分析（System Safety Assessment，SSA）是制定安全设计标准、分析系统对这些标准的符合性、指导设计纠正措施和为符合标准所做的改进、验证所完成设计的系统与标准的符合性。

飞机的设计研制是反复迭代的过程，设计过程是通过反复更改而逐步完善的，因此安全性分析也是反复迭代的过程。安全性分析产生安全设计需求，系统设计考虑并满足这些需求。如果系统进行了更改，新的设计都需要进行重新分析；如果分析结果不满足要求设计就需要进行重新更改然后再进行分析。系统的研制与安全性分析如此反复进行，直到设计满足所有的安全性需求为止。

对于民机而言，安全性是其首要考虑的问题，贯穿于飞机从研制、生产、运营到退役的整个生命周期。同时安全性也是民机能否通过适航审查及进入市场并获得公众信任的前提条件。在民用飞机机载系统中，尤其是发动机的 FADEC 系统属于高度综合的复杂系统，在设计过程中运用机载系统安全性设计与分析技术是减少其事故发生概率的有效手段。民用飞机系统安全性分析是对所实施的民用飞机系统的安全性进行系统性的综合评价，以表明其满足相关的安全性需求。随着航空技术的发展，航空发动机 FADEC 系统功能的增加，系统设计也越来越复杂，给系统安全性分析工作带来了挑战。

中国民用航空规章（CCAR）第 33 部《航空发动机适航规定》中第 28 条“发动机控制系统”以及第 75 条“安全分析”等适航条款规定，FADEC 系统安全

性分析已经成为安装 FADEC 系统的发动机以及安装此类发动机的飞机开展型号合格审定、获取型号合格证必须进行的一项符合性验证工作。

适航法规 FAR/CS/CCAR25.1309 条款对飞机安全性目标提出了明确的要求——确保安装飞机上的设备和系统有一个可接受的安全水平。飞机系统安全性分析过程的主要目的就是通过一种科学、有效的分析方法表明飞机系统对安全性适航条款的符合性。

1.2　安全性问题的出现

系统安全性理念早在 20 世纪初就应用于航空业，追求完整性是第一个关于飞机系统安全性的设计方法，并且设计原则是尽量做出好的零件和完整的系统功能。由于发生许多未曾预计到的单点故障，进而引起了太多的事故；然后逐渐在完整性加上有限的设计特征上选择冗余，对飞机的发动机、无线电台、空速表等系统采取了冗余设计，同时计算单点故障的故障率。因飞机安全性不够，这个时期的飞机还不能赢得公众信任，其在飞行操纵失效、螺旋桨失控、发动机失火、有害的环境条件等方面仍存在问题。

在 1945—1955 年期间飞机安全性前进一大步。工业界和美国政府部门一起于 1945 年开会并制定了“ 单点故障概念 ”，即假设每次飞行期间至少发生一个故障，而不管其概率大小。这个概念对减少单点故障型事故产生了重要影响。虽然这个时期的安全性显著改进，公众信心增加，但事故仍然发生，并且发生的往往是一个以上故障组合的结果。1955 年开始出现了故障安全设计理念，以新运输类飞机的合格审定规则的形式，为涡轮动力的飞机引入了下列概念：必须考虑任一单点故障加上任一可预知故障的组合。这时，故障安全设计的基本原理是，任何一次飞行期间，单点故障或可预知的组合故障不会阻止飞机的继续安全飞行和着陆。在应用该理念设计的第一、二、三代商用喷气式飞机上，显著降低了事故发生率，相关系统的事故率出现实质性降低，并且导致这些机型出现事故的主要原因存在于其他领域，而非机载系统的故障上，例如操作者的错误、维修差错、对预期故障情况的非预期驾驶员反应等。

1.3　安全性分析发展历程与现状

20 世纪 20 年代以来随着军事航空活动的增多，美、英军方开始调查、记录飞行事故，统计飞机的飞行事故率。1937 年英国成立航空事故调查组，1944 年成立空军飞行安全机构负责军用飞机事故调查。1943 年美国陆军航空兵正式实施飞行安全大纲，加强事故调查与分析。

40 年代，美英空军把工作重点从事故记录和调查转向事故预防。而且开始强调在飞机和系统的设计和制造中考虑安全性问题。事故预防主要是加强飞行安全研究和技术检查工作，制定各种安全规章和条例，开展安全培训并推行标准化。

60 年代中期，“ 系统安全 ”的观念逐渐形成，许多先进国家对系统安全性分析开始有一定的研究，美国采用“ 数量风险 ”来计算有关项目或工业投资的各种可能发生的危险及危害，利用统计与计算方法，并参考已经发生的意外事故来加以总结。随着安全性工作的日益专业化，国外还出现了一些专门的系统安全性分析的机构，如英国安全分析服务有限公司。这一时期在航空航天领域也开始广泛使用“ 系统安全 ”概念，认为重大事故的主要原因是设备或系统在设计阶段缺乏系统的安全性分析与设计，要求在系统的初步设计阶段就着手进行安全性分析和危险控制，并一直延续到随后的设计、生产、试验和使用各阶段中。系统安全工作主要包括制定系统安全大纲、确定安全性设计要求、进行系统安全培训等。美国国防部把系统安全工作项目划分为系统安全管理和系统安全工程两大类。NASA 在航天飞机的安全性、可靠性、维修性上开展了许多研究工作。欧洲吸收了美国在系统安全方面的经验，制定了航天飞机的安全性设计分析和管理程序。民用航空领域开始吸取军用系统安全性分析的经验，进行民用飞机安全性评定，以满足适航局提出的要求。

20 世纪 80 年代至今，航空业界进一步加强了安全性分析、设计和验证工作，运用软件安全性、风险管理和定量风险分析等技术来预防事故发生，从飞机和系统的故障与操作人员的人为因素、设备的硬件与软件、安全性设计与风险管理、定性分析与定量风险分析等各个方面对安全性进行保证。

在适航安全性方面，美国航空管理局（Federal Aviation Administration，FAA）发布的联邦航空法 FAR25.1309 中规定了安全性设计的原则。随后 FAA 发布的一系列修正案和咨询通告（Advisory Circular，AC）中，进一步细化了安全性设计原则。适航当局制定的规章条例是商用飞机安全的最低限度要求，构成了航空系统安全性分析的主要内容，但没有完整的对安全性分析过程的说明。后来，美国汽车工程师协会（Society of Automotive Engineers，SAE）制定了《关于高

度综合或复杂的飞机系统的合格审定指南》（ARP4754）和《对民用机载系统和设备进行安全性分析过程的指南和方法》（APR4761）。其中 ARP4754 对飞机系统的基本开发和认证进行说明，APR4761 对机载系统和设备安全性分析的方法进行说明。由于法规和咨询通告都只是大系统级别的要求，美国航空无线电技术委员会（Radio Technology Commission for Aeronautics，RTCA）和欧洲民航设备组织（European Organisation for Civil Aviation Equipment，EUROCAE）联合制定了《机载电子硬件的设计保证指南》（DO-254）和《机载系统和设备认证的软件考虑》（DO-178），分别对机载电子硬件设计的安全性和机载软件开发中如何确保安全性进行具体说明。欧洲在 2003 年之前有联合民航局（Joint Aviation Agency，JAA）管理民航安全，2003 年成立了欧洲航空安全局（European Aviation Safety Agency，EASA）取代 JAA，以便更好地制定和实施法规，保证欧洲的航空安全。

我国民用航空局于 20 世纪 70 年代末成立工程司，开始着手适航审定管理。从 1985 年到 1992 年参照 FAR 逐步制定了 CCAR 第 21 部、第 23 部、第 25 部、第 27 部、第 29 部、第 33 部、第 35 部等，基本建立了与 FAR 相当的适航审定规章体系，其中与航空安全性直接相关的是 1985 年 12 月发布的中国民用航空条例 CCAR25.1309。经过近 40 年发展，我国民用航空安全性分析取得了一定进步，ARJ21 飞机于 2006 年完成部件系统安全性分析内容。

2009 年 1 月中航商用飞机发动机有限公司（中航商发）在上海成立，承担大型飞机发动机的研制，并确立了对商用发动机“五性”要求，即确保安全性、突出经济性、提高可靠性、改善舒适性、强调环保性。其中安全性要求对商用发动机至关重要。FAA、EASA 等制定颁布了一系列联邦航空法（Federal Aviation Regulation，FAR）和 AC、SAE 发布了一系列与 FAR 相符合的标准和规范，我国也参照 FAR 制定了自己的航空法规（CCAR），对民用涡扇发动机数控系统的安全性分析有相关性说明。但是，在具体的安全性分析中无法直接使用这些规章、标准和规范中的安全性分析内容，因为它们并没有针对发动机数控系统具体安全性分析过程。此外，这些规则、标准和规范多用于适航审定程序，如何具体在发动机数控系统研制过程中，进行安全性分析过程，以及在这个过程中会出现的问题，都需要进一步的研究。

要成功实现我国自主研发民用航空发动机，保证大飞机及以后我国民用飞机的“心脏”的健康，并顺利通过适航认证，进入世界民用航空发动机市场，在发动机的研制中，系统安全性分析过程是必不可少的。由于我国商用发动机系统研制的诸多领域得不到外国技术，要通过 FAA 或 EASA 适航当局的审定，

就需要尽早在发动机数控系统的研制过程中进行安全性分析与设计，甚至要在设计和测试过程中采用逆向工程，以确保安全性顺利符合 FAA/EASA 适航标准要求。因此，对发动机控制系统进行安全性分析研究有重要的工程实用价值。

商用航空发动机数控系统作为发动机的一个子系统，是发动机安全性分析的一部分。FAA 颁布的联邦航空规章 FAR33 为航空发动机适航标准，其中 FAR33.28 是关于发动机电气和电子控制系统的相关标准。为了进一步适用 FAR33.28 内容，FAA 在 2001 年 6 月 29 日发布了 AC33.28-1 和 AC33.28-2 的咨询通告，用以提供符合适航要求的指导和方法，以指导申请者证实开发的系统对 FAR33.28 内容要求的符合性。AC33.28-1 就控制系统的一般性定义、供电、数据失效、动力失效、完整发动机控制定义、环境说明及要求和软件要求等给出了一般性的指导。

国内外高校也开展了有关航空发动机数控系统安全性分析的相关研究，如美国麻省理工学院（MIT）初步开展了航空发动机数控系统安全性研究，将 MIT 开发的系统理论化事故建模和处理方法（Systems-Theoretic Accident Modeling and Processes，STAMP）等安全性分析方法用于航空发动机 FADEC 的安全性研究中，结论是现有的航空安全性分析方法不能有效分析设计中的错误，而 MIT 开发的需求完整性标准可以覆盖大部分错误。因此，美国某发动机公司的 FADEC 不完全使用 ARP4761 的方法进行安全性分析，甚至完全没有采用其中提供的共因分析（Common Cause Analysis，CCA）的方法。英国约克大学与罗罗公司合作对发动机数控系统的功能危险性分析做了研究，对数控系统功能进行了分类，指出了高度集成的 FADEC 复杂系统所造成的功能交叉问题。在国内，中国民航大学对 FADEC 的安全可靠性分析做了初步研究，北京航空航天大学对涡扇发动机 FADEC 的功能危险性分析进行了研究，提出了危险识别和多重失效分析的高效率方法。

1.4　系统安全性分析概述

安全性分析过程包括需求的产生和检验，后者支持飞机研制工作，该过程提供一个方法论来评价飞机的功能以及为实现这些功能而设计的系统，以确定相关的危险已经得到合理的处理。安全性分析过程是定性的也可以是定量的。安全性分析过程应该被计划提供一个必要的保证，保证所有相应的故障状态已经被确定，以及所有由这些被考虑到的故障状态导致的关键故障组合。集成系

统的安全性分析过程应当考虑所有由基层导致的附加复杂性和相互依赖性。在包括集成系统，安全性分析过程的所有案例中基本的重点是建立适当的系统安全性目标，并确定设备能满足这些目标要求。

一个安全性分析（包括功能危险分析、初步系统安全性分析、系统安全性分析）的顶层视图，如图 1.1 所示，而且还描述了安全性分析手段如何与该过程联系。研发过程是自然而然的迭代。安全性分析过程是该过程的固有部分，开始于概念设计并推出相应的安全性需求。随着设计的开展就会发生更改，修正后的设计必须再次分析。这个再分析可能产生新的衍生设计需求。这些新需求可能导致进一步的设计更改。安全性分析过程结束于设计满足安全性需求的检验。典型的开发周期时间线（见图 1.2）说明了安全性过程和研发过程的时间关系，在设计过程中有联系的安全性分析过程在如图 1.1 所示方框中被分组，以突出它们之间的关系。

功能危险分析（Functional Hazard Assessment，FHA）在飞机或系统开发周期的初期实施。它应当确定并给所有的飞机功能以及功能组合相关的故障分级。这些故障分级建立安全区目标。

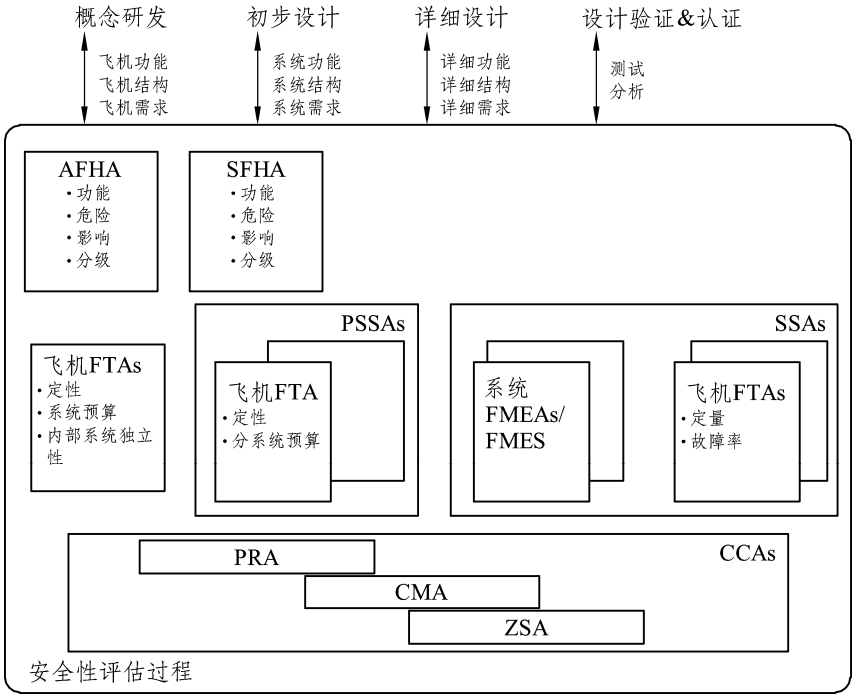

图 1.1　安全性分析过程

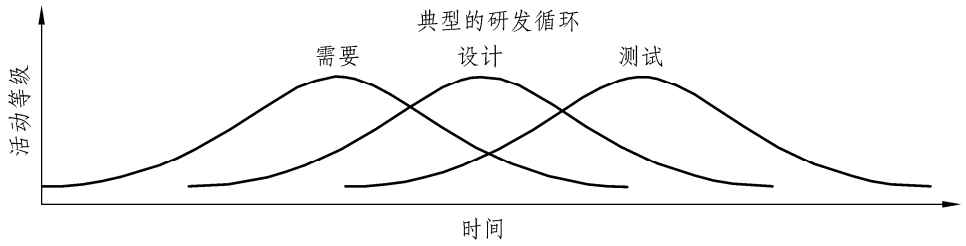

图 1.2　典型的开发周期时间

实施 FHA 的目的是用基本原理来清楚地确定每一个故障以便分级。通过设计过程将所有飞机的功能分配给各系统后，每一个综合了多种飞机功能的系统都应当通过 FHA 过程再次检查。FHA 更新以便考虑每个功能或者飞机功能结合的故障。FHA 的输出结果用作实施初步系统安全性分析（PSSA）的起始点。

PSSA 是对目标系统结构的系统化检查以确定故障为何能引起由 FHA 鉴定的功能性危险。PSSA 的目标是建立系统的安全性需求并确定推荐系统可以合理地满足由 FHA 鉴定的安全性目标要求。PSSA 与设计定义是一个互相作用的过程。PSSA 可以在系统研发的多个阶段（包括系统项目和硬件/软件的设计定义）中实施。在最底层级中，PSSA 确定硬件与软件的安全性相关设计需求。PSSA 通常采取 FTA（DD 或 MA 也可以用）的形式，并且包括共因分析。

系统安全性分析一个对实现系统进行系统化全面的评价，以表明 FHA 的安全性目标和 PSSA 的安全性需求被满足。SSA 通常以 PSSA、FTA（DD 或 MA 也可用）为基础，使用来自故障模式和影响汇总（FMES）。SSA 应该检验所有在 FMES 中确定的都被考虑的重大影响，并作为 FTA 的初始条件，FMES 是对由 FMEA 鉴定的故障的汇总，FMEA 是基于故障影响进行分组的。每个系统结构建立结构和特定系统中执行的界限，共因分析应该支持特定系统结构的研发以及相关系统，通过对所有结构进行共因事件的敏感性分析。这些共因事件执行如下分析方法：特殊分析、风险分析、区域安全性分析和共同模式分析。飞机层级的共因原因分析结果可用于每个系统的 PSSA 和 SSA。

当实施 FTA 时，不管是 PSSA 或者 SSA，在分析中用到的维修任务指定的故障检测方法和相应的暴露时间必须与飞机维修计划中使用的维修任务和暴露时间是一致的。在很多案例中故障检测方法由飞行平台提供或在系统中固有（如由自测设备提供、加电测试等）。DD 本质上等价于 FTA，选择哪个方法取决于分析员的个人偏好。马尔可夫分析技术通常在处理延迟的维修情况时有用。

1979 年 SAE 颁布了 SAE APR926A《零件失效模式及其影响分析和故障树分析》，并于 1986 年颁布了 SAE APR1834《数字系统的故障和故障分析》。然而

从目前的需求来看，SAE ARP926A 和 SAE ARP1834 已经明显不能适应新技术的发展，其存在着诸如为安全性目标所做的指南不完善、强调可靠性/维修性，以及内容过时（例如，不适合 DO-178B、没有强调飞机级分析，没有充分地覆盖共模分析、没有 PSSA）等缺陷。目前，SAE ARP926A 和 SAE ARP1834 已经被 SAE ARP4761（民用机载系统和设备安全性分析过程的指南和方法）替代。然而，AC23.1309-1C 允许在某些环境下对小飞机进行的系统安全性分析继续延用 SAE ARP926A 和 SAE ARP1834 规定的方法。

SAE ARP4761 中提出的新概念如下：

（1）更加正式地说明共因分析：区域安全分析、特定风险分析、共模分析。

（2）飞机级功能危险性分析：失效状态、危险等级、支持材料等。

（3）初步系统安全性分析：提供一个在设计过程的早期阶段更加系统化地分析安全性的方法，并且减少了研发计划即将结束时出现的不期望结果。

（4）故障树分析：基于每飞行小时的故障条件概率的计算；对于特定型飞机，用计算概率的结果除以平均飞行时间来确定每飞行小时的概率；解决潜在故障的暴露时间和受监控故障的其他情况（对带有监控故障的考虑）。

通过定性分析和定量分析，SAE ARP4761 发表了多数人的观点，其中的技术尚未被制造商全部采用，需要随着时间推移逐步被采纳。如果满足了安全性分析的目的要求，在对有关内容进行附加分析（合理性分析、保守性分析和可追溯性分析）后，旧的方法或其他方法也是可接受的。

可靠性是指产品在规定时间内、规定条件下完成规定功能的能力，也定义为系统及其组成部分在无故障、无退化或不要求保障系统的情况下执行其功能的能力。可靠性分析和安全性分析是互补的，可以互相提供有效信息。安全性首先定性地分析风险，找到危险的原因，确定危险的危险性等级，进而确定设计保证要求级别，系统研制来满足这个要求。可靠性基本是对零部件定量的失效率计算。可靠不一定安全，安全也不一定可靠，安全性首先偏重自上而下的定性危险分析，而可靠性首先偏重自下而上的元器件的定量的失效概率计算与预计。可靠性的故障树分析技术偏重于系统历史经验所得顶事件的分析，而安全性的故障树的顶事件来源于较为完善的功能危险性分析的结果。各自分析的来源和输出有所不同，但其中使用的 FTA、MA 等概率方法是相同的。安全性更关注的是系统输出的正确性。例如数控系统中一些非安全关键的传感器故障导致的输入信号错误，是不符合可靠性要求的，但如果控制通道能够诊断并隔离这个错误，那么就仍然是符合安全性要求的。

1.5　安全性分析过程概述

安全性分析过程开始于概念设计并推出相应的安全性需求。随着设计的开展，就会发生更改，修正后的设计必须再次分析。这个再分析可能产生新的衍生设计需求。这些新需求可能需要进一步的设计更改。安全性分析过程结束于设计满足安全性需求的检验。

安全性分析主要通过功能危险性分析、初步系统安全性分析、系统安全性分析等的分析方法/流程而实施。在飞机/系统研制周期的初始要进行一次 FHA，藉此查明与飞机功能及功能组合相关联的失效状态并对其进行等级分类。FHA 是对飞机和系统功能进行检查，确认潜在的功能失效，并对与特定失效相关的危害程度进行分类。在研制过程早期进行 FHA 工作，并且随着新功能或者失效情况的确认进行更新。进行 FHA 的目的是表明每一种失效状态及其分类的原理，随着设计过程中飞机的功能被分配到各个系统，应当对每一个综合了多项功能的系统再进行 FHA 检查，此时的 FHA 应调整为考虑分配到该系统的单个功能或其组合。最后 FHA 的输出将作为 PSSA 的起始点。

PSSA 是对所提出的构架进行系统性检查以确定失效如何导致 FHA 中所确定的失效状态。同时，PSSA 是对飞机/系统精心研制保证等级的分配。PSSA 的目标是完善飞机系统或设备的安全性需求，并确认所提出的构架能够合理地满足安全性需求，PSSA 可以确定保护性措施。SSA 及其他文件应该以 PSSA 的输出作为其输入，包括但不限于系统需求、软件需求及硬件需求。PSSA 是与设计定义相关的反复迭代的过程。PSSA 在系统研制的多个阶段进行，在最低层级 PSSA 确定了与软件安全性相关的设计需求。

SSA 是对所实现的飞机和系统的一种系统性和综合性评价，以表明其满足相关的安全性需求。PSSA 和 SSA 的区别在于 PSSA 是评价所提出的构建已经生成系统设备安全性需求的方法，而 SSA 是验证所实施的设计满足 PSSA 定义的安全性需求的方法。SSA 综合各种分析的结果，以验证整个飞机/系统的安全性，并具体考虑了 PSSA 所确定安全性方面的问题。SSA 通常建立在 PSSA 中 FTA 的基础上，并且要用到 FMES 所获得的定量数据。通过 SSA 应当确认 FMES 列出的所有重要的故障影响都被作为主事件在 FTA 中加以考虑。FMES 是对 FMEA 列出的故障的一个概括，其中根据故障影响对其进行了分组。另外，共因分析结论也必须包含在 SSA 中。在 PSSA 和 SSA 中进行故障树分析，分别有定性和

定量分析。