功能危险性分析在推进系统中的应用

The Application of Functional Hazard Assessment in Propulsion System

魏利军　李高民 / Wei Lijun　Li Gaomin
（中航商用航空发动机有限责任公司，上海 200241）
（AVIC Commercial Aircraft Engine CO. LTD. ，Shanghai 200241，China）

摘　要：
针对民用航空发动机研制过程中的安全性评估过程，结合系统工程思想以及工程实际，提出了在系统级开展功能危险性分析常遇到的问题，并结合在推进系统功能危险性分析中的实践，提出了解决这些问题的原则和方法。

关键词：安全性评估；功能危险性分析；推进系统
中图分类号：V23　　**文献标识码：**A

[**Abstract**] Combined with system engineering ideas and a real engineering example，this paper presents the common problems in functional hazard assessment for the safety assessment process of aeroengine development. And some good methods and principles were presented by the practice of propulsion system functional hazard assessment.

[**Key words**] safety assessment；functional hazard assessment；propulsion system

0　引言

对于飞机这种高度集成、高度复杂的系统，传统的设计过程中难免会引入设计错误或不足，从而产生非预期的危险后果。而适航作为民用航空器最低安全性标准，是民用飞机及系统研制最基本的准入标准，要求在产品寿命周期内将潜在的危险消除或使其在寿命周期内得以控制[1]。为了在设计过程中发现潜在的危险，并在设计中对其进行消除或控制，一般在研制过程中采用安全性评估技术，以保证系统满足安全性要求。

功能危险性分析（funcomal hazard assessment，简称 FHA）是安全性评估过程的起点，是在系统研制初期，对定义系统进行的高层次的、定性的评估。通过 FHA 识别与系统功能相关的失效状态并对其进行分类，确定系统研制的安全性目标。FHA 输出结果是分配低层级安全性要求的基础，可通过故障树分析（FTA）衍生出低层级安全性要求，FHA 中确定的失效状态也是研制保证等级分配的输入，FHA 识别的危险失效状态是在系统研制过程中应消除或控制的目标。

我国民用航空发动机安全性评估技术尚属起步阶段，几乎未在工程研制中得到应用，本文结合工程实践，从功能危险性评估原理出发，对安全性评估过程中的功能危险性分析过程及方法进行研究，给出了适用于推进系统的功能危险性分析和验证方法，并通过实例验证了其在推进系统中的应用，表明了该方法的有效性及其在推进系统工程设计中的应用。

1　功能危险性评估原理

功能危险性分析（FHA）是安全性评估过程的起点，是其他安全性分析工作的基础，是在系统研制初期对被分析系统功能进行系统地、综合地检查。功能危险性分析首先在飞机级进行，然后将飞机功能分配至飞机系统，再对每个系统进行功能危险性分析[1]。推进系统在进行功能危险性分析时，应首先收集飞机级 FHA 的功能分配，然后进行推进系统级 FHA，并分配功能至推进系统的系统，推进系统安全性与开发过程关系如图 1 所示[1]。

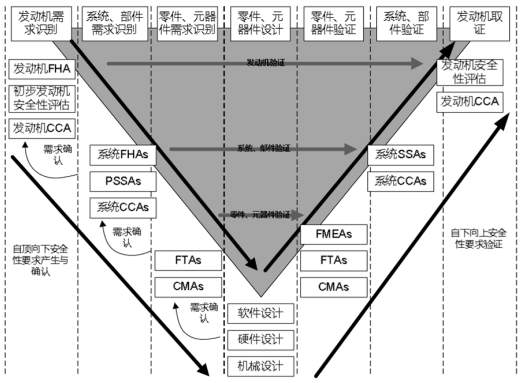

图 1　发动机安全性与开发过程的联系

功能危险性分析是一种探索系统部件功能失效影响的预测技术，其主要目的是识别危险的功能失效状态，以便在产品的整个寿命周期内消除或使其得到控制[1-2]。功能危险性分析方法简要描述如下：

(1)依次选择功能，并对功能进行恰当的描述；

(2)确定功能的目的和特性；

(3)考虑假设的失效模式，如：功能丧失，功能非指令提供，功能错误运行(高、低等)；

(4)确定影响；

(5)确定并记录相关的风险要素(严重度、预计概率)。

功能危险性分析结果通常用表 1 所示表格记录。功能危险性分析确定的功能失效的影响及严重度分类，是系统研制的安全性目标，功能失效状态影响、分类及其对应的定量概率要求之间的关系[2]如表 2 所示。

表 1　功能危险性分析表格式样

功能	失效状态	工作阶段	影响	分类	验证方法

表 2　功能失效状态影响、分类及定量概率要求

功能失效状态分类	失效影响	定量要求
灾难性的Ⅰ	妨碍继续安全飞行或着陆	不大于 1.0×10^{-9}
危险性的Ⅱ	极大降低飞机运行能力或安全裕度；极大的工作负荷或身体不适，使机组丧失或不能准确的执行任务	不大于 1.0×10^{-7}
重大的Ⅲ	较大降低飞机运行能力或安全裕度；较大增加工作负荷或身体不适，影响机组效率	不大于 1.0×10^{-5}
较小的Ⅳ	轻微较小安全裕度；轻微增加机组工作负荷	不大于 1.0×10^{-3}
无安全性影响的Ⅴ	无影响	无

2　系统级功能危险性分析常出现的问题

功能危险性分析(FHA)是一种自上而下的方法，用于识别功能失效状态并评估其影响。FHA 以功能为基础，可在系统设计之前仅知道系统要做什么时进行，它可用于任何能够识别功能的目标，是对给定对象功能失效影响的系统评估与分类。

功能危险性分析原理和方法在 SAE ARP4761 中有描述，然而在实际分析中常出现以下问题：

(1)功能定义

难以在恰当的层级定义功能，特别是在实现细节中分离出功能。而功能的表述过于细节将导致 FHA 过程过长，产生过多信息，使得将 FHA 变成了自下向上的设计活动。

(2)确定影响

对于发动机及发动机的系统与环境边界分隔了几个分析层，确定失效状态的影响较难，如分析发动机系统的功能失效时必须能先确定对发动机的影响，再确定单发对推进系统的影响(对于多发飞机)，最后确定推进系统对飞机的影响。

为了解决以上问题，总结工程实践中的应用，对功能危险性分析过程各环节提出了以下要求。

3　功能危险性分析

3.1　识别分析目标功能要求

在进行功能危险性分析时，首先应识别与给定对象相关的全部功能，包括内部功能和交互功能，并建立功能清单。在识别功能时应遵循以下原则：

(1)应包含分析目标执行的所有功能；

(2)应包含分析目标可能影响的所有功能；

(3)不包含分析目标的任何子功能；

(4)不包含任何设计细节或所列功能的实现。

为了在恰当的层级定义功能，确定的分析层功能应满足以下条件：

(1)功能是上一分析层要求提供的功能；

(2)功能是分析目标运行必须的功能；

(3)功能是对分析目标工作状态的监视；

(4)功能是保证分析目标安全运转必须的功能；

(5)功能失效将导致分析目标不能正常工作或直接对上一分析层产生影响。

3.2 识别每项功能的失效状态要求

在失效状态的识别过程中应建立环境条件以及应急状态清单。分析时应确定系统各项功能在此环境或应急/非正常情况下的失效状态及其影响。推进系统安全性分析中,环境条件包括天气、高能辐射场等,应急状态包括中断起飞、丧失液压系统、丧失发动机滑油系统、丧失电气系统等。

在建立失效状态清单时,应根据失效类型对建立的功能清单、环境条件及应急状态清单等进行分析检查,理解系统组成及系统内部设备之间的交互关系,确定单一和多重失效状态清单。功能失效类型包括:(1)功能丧失;(2)功能异常。

在进行失效状态识别时,应注意:

(1)一项功能至少有一个功能丧失和一个或多个异常的失效状态;

(2)如果较大的部分功能丧失情况在分析目标之外能够看出,则可能存在多重功能丧失状态;

(3)简单功能的故障状态较少;

(4)在获取失效状态时,特别是在已知设计的情况下,通常犯的一个错误是关注于分析目标内部。

为保证失效状态清单的完整、正确,可制定失效状态检查单对识别的功能失效状态清单进行检查,检查项应包含:

(1)是否覆盖功能的全部丧失;

(2)是否有部分丧失的情况,如果有,是否覆盖;

(3)是否有:非指令性工作、延迟工作、误导、误强化故障的情况,如果有,是否覆盖;

(4)失效情况是否根据影响客观描述(非其潜在原因)。

3.3 确定各失效状态的影响要求

在对已识别的功能失效状态清单中的各失效状态进行影响分析时,对每一失效状态必须确定其最终影响,影响的确定需考虑失效发生在飞行包线内任何可能发生的状态。失效的最终影响包括对飞机、机组人员及乘客的影响。

在分析对飞机的影响时,需考虑失效状态如何影响飞机的能力,包括:(1)能力可用/不可用;(2)飞机的性能;(3)结构完整性。

在分析对机组人员的影响时,需考虑机组人员如何识别失效状态及如何反应,包括:

1)失效的识别

(1)是否有机组告警信息或警报;

(2)能否认识到飞机的飞行状态;

(3)机组是否没有察觉到该失效状态。

2)机组操作及结果

(1)基本的飞行技术(直觉反应);

(2)应急措施(如认识到失效)。

为了确定功能失效影响,在实际工作中发现,通过建立功能模型可以较好地解决失效影响难以确定的问题,如图 2 所示,举例说明了发动机起动功能的功能模型,该功能模型中体现了功能的交互、存在的反馈循环以及可监测影响的点。通过该模型可以推测出失效的可监测和反馈的影响。

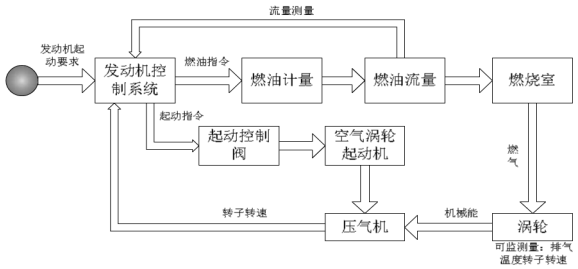

图 2 起动功能模型

3.4 FHA 验证

在 FHA 中,对所有灾难性的、危险性的和重要的这三类危险等级,都需要展开进一步的验证。对于每种确定的危险情况,通过相应的验证方法可判断设计是否能够满足相应的概率要求。对于“无安全性影响的”和“轻微的”失效状态,只需通过设计及安装评估说明该失效状态是轻微的即可。对于“重要的”、“危险性的”和“灾难性的”失效状态,如果设计属性与现有所属的,已取证的系统相似,只需证明相似性就能够证明其满足要求。否则,对于简单的或者常规的系统,要运用 FMEA(故障模式及影响分析)、FTA、DD(相关图)等方法进行验证;对于复杂系统,则要通过 FMEA、FTA、CCA(共因分析)、DD、MA(马尔可夫分析)等方法进行验证。验证方法决策[2]如图 3 所示。

4 实例分析

本例将以由推进系统支持的飞机功能(提供推力、提供电源和液压源、提供主要飞行信息、飞机减速与停止、提供着火保护)为例,识别了推进系统功能,并以部分功能为例进行了功能危险性分析。

4.1 功能分析与识别

本例通过对推进系统支持的飞机功能的分析

并考虑适航规章中对飞机安全的相关要求，确定了推进系统功能，见表3。

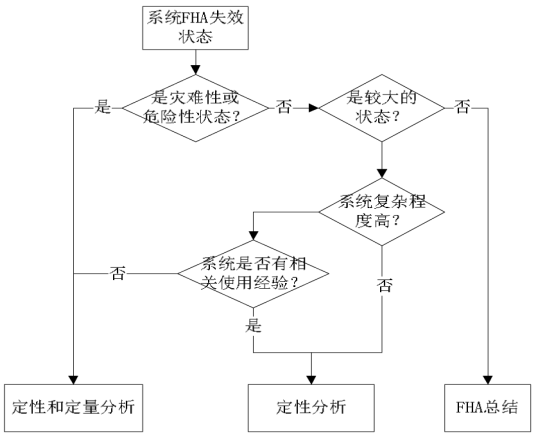

图3　FHA验证方法决策图

表3　推进系统系统功能

编号	功能	备注
1	提供(向前)推力	飞机功能相关
2	提供反向推力	飞机功能相关
3	提供发动机(主要参数)指示	飞机功能相关
4	驱动发电机和液压泵	飞机功能相关
5	提供飞机引气	飞机功能相关
6	提供发动机停车能力	飞机安全相关
7	提供发动机点火能力	飞机功能相关
8	提供发动机起动能力	飞机功能相关
9	提供发动机超转保护	飞机安全相关
10	提供发动机防冰	飞机功能相关
11	提供发动机着火保护	飞机功能相关

下面本文将以表3中确定的推进系统功能中的提供反向推力和提供发动机(主要参数)指示为例确定失效状态清单、影响分析等(其失效状态包含了功能丧失、功能部分丧失、功能故障(非指令工作、误导)等典型失效状态)。

4.2　典型飞行过程

推进系统功能与飞机飞行状态密切相关，功能危险性分析应急用于飞机飞行过程，典型的飞行过程包括滑行(地面慢车)、起飞(起飞滑跑、起飞、起飞爬升)、爬升、巡航、进场、着陆(着陆和着陆滑跑)等飞行阶段。

4.3　确定失效状态清单

下面将根据第2节中的要求，对表3中确定的推进系统系统功能清单中的2、3两项功能进行失效状态识别，获得的失效状态清单见表4。

表4　失效状态清单

功能	失效状态
P2 提供反向推力	P2.1 反推意外打开
	P2.2 发出指令时不能提供最大反推力
	P2.3 完全丧失反推力
P3 提供发动机(主要参数)指示	P3.1 发动机主要参数(N_1，N_2，涡轮级间温度)错误显示或误导显示
	P3.2 发动机主要参数(N_1，N_2，涡轮级间温度)不能显示

4.4　失效状态影响分析

对表4中识别的实效状态清单进行失效影响分析及分类见表5。

4.5　FHA分析结果的验证

在推进系统设计过程最终需要对FHA确定的安全性目标进行验证，表明设计满足安全性要求，通常采用的验证方法包括FTA(或DD/MA)、CCA、FMEA。FTA(或DD/MA)用于确定可能引起每个失效状态的低层单个失效或失效组合，FMEA用于确定FTA(或DD/MA)基本事件的失效率，CCA用于验证功能、系统之间的独立性要求。

5　结论

在高度集成、高度复杂的系统研制过程中，系统功能复杂且交互作用，合理地确定系统研制安全性目标直接影响系统研制的进度和研制成本，在系统研制之初应予以确定。本文基于系统工程思想，给出了推进系统设计之初，根据推进系统相关的飞机功能及安全目标，通过功能危险性评估识别并确定推进系统功能及其安全性设计目标的方法和流程，确定合理的安全性设计目标，将危险控制在可接受的范围内，从而降低系统研制成本。

参考文献：

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

[2] SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment [S]. U. S. A: SAE International, 1996-12.

表 5　失效状态分析

失效状态	阶段	影响	分类
P2.1	起飞(滑跑 v1 后)至着陆	对飞机:推力不对称、偏航及其引起的滚转、阻力增加。 对机组:飞行员通过机组报警系统信息和飞机表现、偏航力矩、滚转和速度降低察觉到反推打开。推力性能因阻力增加而降低,妨碍安全飞行,影响飞机的可控性。 对乘客:严重受伤或生命危险。	Ⅰ
P2.2	放弃起飞(湿跑道或污染跑道)	对飞机:一台发动机失效或反推装置完全打开后意外收起都会导致推力不对称和产生偏航力矩。若一台发动机反推装置不能按指令打开,FADEC 将两台发动机设置至慢车推力,使反推装置均不可用。 对机组:飞行员通过发动机指示和机组告警系统指示和飞机状态,如偏航力矩等,获知发动机失效或反推装置意外收起。此时飞行员可使用或停止使用依然可用的反推装置,同时操作方向舵和飞机前轮方向来控制飞机。如果反推装置未打开,飞行员通过发动机指示和机组告警系统指示和飞机未减速的状态获知。在这种情况下,飞行员停止使用反推装置,使用常规刹车来使飞机停止。 对乘客:可能会因使用反推对飞机制动而受到有不利影响。	Ⅱ
P2.3	着陆、放弃起飞(干跑道或干净跑道)	对飞机:功能和安全裕度轻微减小,在干燥无污染跑道上使用反推装置停止飞机对着陆性能无影响。 对机组:轻微增加工作负担。如果反推装置不能打开,飞行员可通过发动机指示和机组告警系统指示和飞机未减速的状态获知。在这种情况下,飞行员停止使用反推装置,使用常规刹车来使飞机停止。 对乘客:无安全影响。	Ⅳ
P3.1	起飞、复飞	对飞机:飞机仍具有完全控制能力和性能,飞机校正高度、空速和姿态依然有效。 对机组:飞行员认识到这种情况并在所有目视气象条件/仪表气象条件(VMC/IMC)情况下控制飞机。飞行员通过其他方法监视飞机性能,如姿态、速度误差和速度方向矢量。仅在高推力飞行阶段,如起飞、复飞,在可能出现发动机参数显示溢出的情况下,飞行员需决定降低推力设置至起飞复飞(TOGA)以下。即使在这些情况下,可用推力将超过单发失效状态。飞行员负担有较大增加,飞行员可能不能及时采取应急措施。 对乘客:可能处于不利状态,潜在的生命危险。	Ⅰ
P3.2	全阶段	对飞机:发动机和飞机均完全可控。发动机推力可手动控制或通过自动油门杆控制以维持飞行状态需要,飞机校正高度、空速和姿态依然有效。 对机组:飞行员很快认识到这种情况并在所有目视气象条件/仪表气象条件(VMC/IMC)情况下控制飞机。飞行员通过其他方法监视飞机性能,如姿态、速度误差和速度方向矢量。仅在高推力飞行阶段,如起飞、复飞,飞行员需决定降低推力设置以防止可能出现的发动机参数溢出。飞行员负担有较大增加。 对乘客:可能处于不利状态。	Ⅱ

(上接第 69 页)

飞机构型发生更改、维修类手册发生更改或技术管理等问题可能会导致设备/工具发生增减或修改。设备/工具清单通常需要评审、修改多次,才能定稿。当飞机交付后,也会根据客户的实际需要,再次完善。

5　结论

民机结构、系统复杂,研制周期长,对技术和管理层面的工作均是一个长期的考验。地面支援设备/工具清单的编制工作贯穿民机研制始终,是一个多次更迭完善的过程。编制工作必须基于维修工程分析结果,基于对设备/工具生产厂家与产品的调研,基于与供应商的多次协调,基于对航空公司、MRO 的充分调研。编制人员应以能顺利完成飞机维修手册规定的各项任务、降低主制造商和航空公司成本、顺利完成设备/工具采购为目标,有序开展清单编制工作。在工作中积累经验,向飞机设计人员输入明确的、可执行信息,使得机型在前期设计时能够更多兼顾后期设备/工具的使用性、通用性,是地面设备专业人员的愿景。

参考文献:

[1]德里克·怀特,贾丽岩. 用成本效益选购地面支援设备和工具[J]. 航空维修与工程,2002,1:31-33.

[2]左洪福,蔡景,吴昊,等. 航空维修工程学[M]:北京:科学出版社,2011.

[3]张宏. 地面支援设备在民机设计中的重要性及其相关研制程序[J]. 民用飞机设计与研究,2011,3:65-69.

[4]王燕玲. 民用飞机通用地面支援设备选型程序浅析[J]. 民用飞机设计与研究,2014,1:58-62.