http://myfj.cnjournals.com myfj_sadri@comac.cc (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2021.01.014

民用航空发动机顶层故障事件的概率计算研究

连 超*

(中国航发商用航空发动机有限责任公司,上海 200241)

摘 要: 为满足民用航空发动机的安全性目标,发动机顶层故障事件(顶事件)的风险应被控制至可接受状态。针对顶事件的风险控制要求,细化为顶事件的预期发生概率应被控制至可接受值以下。基于顶事件的预期发生概率要求,提出了从上到下分析导致顶事件发生的潜在原因并逐级建造故障树的方法,阐述了故障树分析的开展时机及作用。然后,对顶事件发生概率的计算进行了研究,通过考虑顶事件的飞行阶段影响因素、故障树最小割集及其概率、底事件失效率及其风险时间,提出了顶事件发生概率的计算模型。同时,结合示例对顶事件发生概率的计算模型进行了应用,以验证顶事件概率计算方法的可行性。提出顶事件概率计算模型,为发动机顶层故障事件风险控制要求提供有力的技术支撑。

关键词: 发动机;故障事件;概率;风险时间

中图分类号: V263.6 **文献标识码:** A **OSID:**

0 引言

飞行安全是民用飞机的永恒主题。为了保证民用飞机的飞行安全,新研发动机应具备要求的安全性水平。

安全性是通过设计赋予民用航空发动机的重要特性,旨在将影响飞机安全性的发动机顶层故障事件的概率降低至可接受状态,即影响后果越严重的发动机顶层故障事件应该越不可能发生[1-2]。为了确保发动机的安全性达到飞机安全性设计要求和适航要求,首先需要识别发动机顶层故障事件(顶事件),分析导致顶事件发生的潜在原因及其途径,从上到下建造导致顶事件发生的故障树。然后,从定性与定量角度对故障树进行分析,确定发动机关键组件和各个组件的失效率要求,通过设计解决措施将顶事件的发生概率降低至可接受状态。

目前,国内在顶事件概率计算方面的研究主要集中在通过故障树最小割集计算顶事件发生概率[3-6],国外相关文献[7-9]提到了顶事件概率计算方法,但是均未研究仅在特定飞行阶段内顶事件发生才会导致考虑的故障影响后果。

因此,为了保证运算精度使顶事件概率更接近真实值,在计算顶事件发生概率时,除了运用故障树最小割集外,有必要深入考虑顶事件的特定飞行阶段、底事件失效率及其风险时间等影响因素。本文结合实际工程经验,对发动机顶层故障事件的概率计算方法和过程进行研究。

1 故障树的建造方法

分析人员从一个不希望发生的发动机顶层故障事件(顶事件)开始,逐层向下分析确定引起顶事件发生的原因,从上到下逐级建造故障树。下面简要说明故障树的组成要素及其建造过程。

1.1 故障树的组成要素

故障树的组成要素包括两类符号:事件符号和门符号[8]。事件符号表示故障树中各种故障状态

* 通信作者. E-mail: lianchaoyouss@163.com

引用格式: 连超. 民用航空发动机顶层故障事件的概率计算研究[J]. 民用飞机设计与研究,2021(1):92-97. LIAN C. Research on probability calculation of top level failure event for civil aviation engine[J]. Civil Aircraft Design and Research,2021(1):92-97(in Chinese).

或不正常情况。门符号用于描述故障树中各种事件之间的逻辑关系，门符号在故障树中不应直接相连，其输入和输出都应该是事件。故障树组成要素的简要说明如图 1 所示。

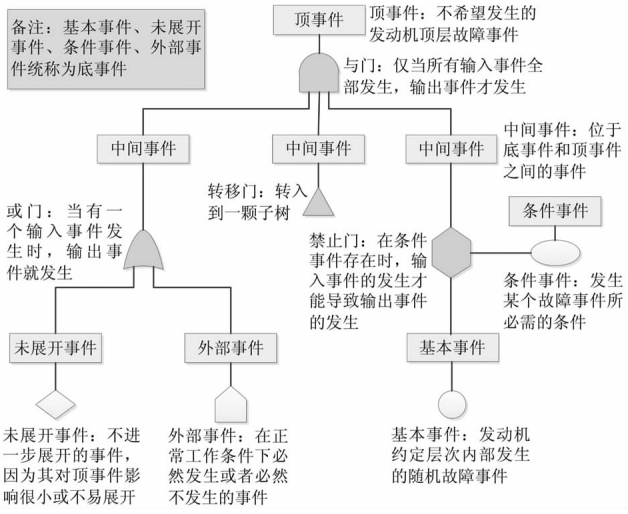

图 1　故障树组成要素示例图

1.2 故障树的建造过程

以一个不希望发生的发动机顶层故障事件（顶事件）作为对象，分析导致顶事件发生的直接原因（中间事件），使用逻辑门将识别出的中间事件与顶事件进行连接。以此类推，向下演绎分析导致中间事件发生的直接原因，直至分析至约定层次或者无需继续向下展开为止，此时的事件为故障树底事件，使用逻辑门将识别出的底事件与中间事件进行连接。根据上述过程，可以建造一颗以顶事件为“根”、中间事件为“节”、底事件为“叶”，使用逻辑门连接“根、节、叶”的倒置树。

2　故障树分析的开展时机及作用

根据航空工业界认可的行业标准，安全性评估过程主要包括：功能危险性评估、初步系统安全性评估和系统安全性评估[8]。其中，初步系统安全性评估过程和系统安全性评估过程都应开展故障树分析，在以上两个过程中故障树分析的作用分别为：

1）在初步设计阶段[10]，初步系统安全性评估过程中的故障树分析以顶事件（功能危险性评估识别出的功能失效状态）概率要求（即发动机安全性目标）为对象，对顶事件概率要求逐级向下分配，得到发动机系统/部件/组件失效概率预算值，作为系统/部件/组件的安全性设计要求；

2）在详细设计阶段和试制与验证阶段[10]，系统安全性评估过程中的故障树分析（可用设计细节可能会引起初步系统安全性评估中的故障树发生更改）对顶事件概率要求进行符合性分析，将来自故障模式影响分析的失效率数据输入至故障树底事件，计算得出故障树顶事件的发生概率，用于证明发动机设计符合功能危险性评估中功能失效状态的安全性目标。

3　发动机顶层故障事件的概率计算模型

为了得到发动机顶层故障事件（顶事件）的发生概率，需要确定引发顶事件的底事件组合（即最小割集），然后考虑所有最小割集的概率、顶事件的飞行阶段影响因素来计算顶事件的发生概率。

3.1 计算顶事件的发生概率

通过发动机功能危险性评估识别出功能失效状态（发动机顶层故障事件），在特定飞行阶段内功能失效状态的发生才会产生所考虑的失效状态影响。如果功能失效状态发生在特定阶段之外，则失效状态影响不会发生。为了考虑功能失效状态的飞行阶段影响因素，将功能失效状态所在特定飞行阶段影响因素定义为条件事件，故障树示例如图 2 所示。

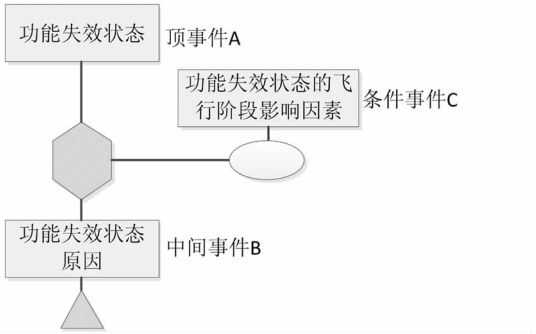

图 2　考虑功能失效状态飞行阶段影响因素的故障树示例

根据图 1 中禁止门的定义，功能失效状态（顶事件 A）发生概率的计算式如下：

$$P(A) = P(B) \times F(C) \qquad (1)$$

式中：

$P(A)$ 是功能失效状态（顶事件 A）的发生概率；

$P(B)$ 是功能失效状态原因（中间事件 B）的发生概率；

$F(C)$ 是功能失效状态的飞行阶段影响因素（条件事件 C），计算方法为功能失效影响所在特定飞行阶段时间占整个飞行阶段时间的比例。

为了计算功能失效状态原因(中间事件 B)的发生概率,需要使用导致中间事件 B 发生的底事件组合(即中间事件 B 的最小割集)及其概率。对于中间事件 B 的发生概率,计算式为:

$$P(B) = P(G_1 + G_2 + \cdots + G_n) = \sum_{i=1}^{n} P(G_i) + \cdots + (-1)^{n-1} P(G_1 G_2 \cdots G_n) \quad (2)$$

式中:

$P(G_i)$是第 i 个最小割集 G_i 的概率,$G_1, \cdots, G_n$ 是导致中间事件 B 发生的所有最小割集。

最小割集中底事件类型不同,最小割集的概率计算方法也不同。按照故障影响后果,可将底事件分为两类,即显性故障和隐蔽故障:

1)显性故障:可被飞行机组或维修人员察觉的故障。也就是,通过其故障影响后果,在下一个航班前显性故障的发生可被探测到;

2)隐蔽故障:发生时未被检测或未通告的故障。通常,隐蔽故障使保护性机理丧失作用,当被保护功能异常时,隐蔽故障的发生才可被探测到。

3.1.1 最小割集中底事件全是显性故障

对于最小割集中底事件全是显性故障的情况,在飞行开始前,底事件对应组件/部件/系统都正常运行,同一次飞行中最小割集中底事件(显性故障)全部发生而引发中间事件 B。对于最小割集 G_i 中各底事件发生概率进行相乘运算,就可以得到每次飞行中最小割集 G_i 的概率,计算式为:

$$P(G_i) = \prod_{j=1}^{m} P(D_j) \quad (3)$$

式中:

$P(G_i)$是第 i 个最小割集 G_i 的概率;

$P(D_j)$是最小割集 G_i 中底事件 D_j 的发生概率,$D_1, \cdots, D_m$ 是最小割集 G_i 中所有底事件。

3.1.2 最小割集中包含隐蔽故障底事件

对于包含隐蔽故障底事件的情况而言,隐蔽故障可在检查间隔时间内的任何一次飞行中发生。因此,分别考虑隐蔽故障发生在检查间隔时间内任何一次飞行中,求出每种情况下最小割集的概率值,并将各概率值求和,再除以检查间隔时间内飞行次数得到每次飞行中最小割集的概率。考虑最小割集中包含显性故障底事件、隐蔽故障底事件且有顺序要求的情形[8],在该情形下,底事件 D_j(隐蔽故障)须在底事件 D_k(显性故障)之前发生,否则不会引发顶事件,该情形下最小割集概率的计算式为:

$$P(G_i) = \frac{1}{2} \times (D_j) \times P(D_k) \quad (4)$$

式中,

$P(G_i)$是第 i 个最小割集 G_i 的概率;

$P(D_j)$是最小割集 G_i 中底事件 D_j 的发生概率;

$P(D_k)$是最小割集 G_i 中底事件 D_k 的发生概率。

3.2 计算底事件的发生概率

为了符合适航规章对顶事件的安全性定量要求,需要计算每飞行小时平均概率[3]。在计算过程中涉及的单个组件/部件/系统假定处于正常使用阶段,其失效率特征符合浴盆曲线中的偶然失效阶段。也就是,组件/部件/系统的失效率近似为常数,其寿命服从指数分布,底事件(组件/部件/系统的失效)的发生概率仅和组件/部件/系统使用时间的长短有关,其发生概率为:

$$P(D_j) = 1 - e^{-\lambda_j t_j} \quad (5)$$

式中:

$P(D_j)$是底事件 D_j 的发生概率;

e 是自然常数;

λ_j 是底事件 D_j 对应组件/部件/系统的恒定失效率;

t_j 是底事件 D_j 的风险时间。

3.2.1 确定底事件的失效率

对于初步系统安全性评估过程中的故障树分析,底事件的失效率可以参照已投入使用的相似设备的统计数据进行初步分析。对于系统安全性评估过程中的故障树分析,底事件的失效率应与故障模式影响分析中的失效率对应,底事件失效率的来源可以是航线统计数据、试验数据、其它广泛使用的工业标准和手册。

3.2.2 确定底事件的风险时间

显性故障底事件和隐蔽故障底事件分别具有不同的风险时间[8],下面分别说明:

1)显性故障底事件的风险时间

对于显性故障底事件而言,其风险时间与对应组件/部件/系统的使用情况有关:

(1)如果显性故障底事件对应组件/部件/系统在整个飞行过程中都使用,则该底事件的风险时间等于估计的平均飞行时间;

(2)如果显性故障底事件对应组件/部件/系统仅在特定飞行阶段使用,并且已知使用之前它可正常工作,则该底事件的风险时间等于从功能检查到特定飞行阶段结束所耗用的时间;否则该底事件的风险时间等于从起飞到特定飞行阶段结束所耗用的时间。

2)隐蔽故障底事件的风险时间

对于隐蔽故障底事件而言,其风险时间为对应组件/部件/系统上次检查其正常工作与再次检查其正常工作之间的时间段,即该底事件的风险时间为对应组件/部件/系统的检查间隔时间。

4　示例

为了缩短飞机着陆后的滑跑距离,大型民用客机发动机上通常设有反推力装置,通过阻挡涵道气流使之反向,以形成反向推力,使飞机高效地减速。

按照 CCAR-33R2 第 33.75 条的要求,“与驾驶员命令的推力方向相反的较大的推力”是危害性发动机后果,申请人必须表明,危害性发动机后果的预期发生概率不超过定义的极小可能概率(概率范围是 10^{-7} ~ 10^{-9}次/发动机飞行小时)[11]。造成“与驾驶员命令的推力方向相反的较大的推力”的发动机失效与飞行阶段有关,会导致与飞机操纵有关的危险情况,“要求反推力时却出现较大的前进推力”可以被归类为危害性发动机后果[1-2]。也就是,发动机顶层故障事件“要求反推力时却出现较大的前进推力”是危害性发动机后果,其发生概率应不超过定义的极小可能概率。

根据故障树建造过程,逐层向下分析导致发动机顶层故障事件“要求反推力时却出现较大的前进推力”发生的原因。首先,在飞机着陆时需要反向推力使飞机减速,“要求反推力时却出现较大的前进推力”事件在飞机着陆阶段才会造成危害性发动机后果。其次,可从以下两方面分析其发生的直接原因:

1)反推着陆时未展开;

2)出现非指令的较大前进推力。

根据上述分析,得到“要求反推力时却出现较大的前进推力”的故障树如图 3 所示。

顶事件 A 的影响阶段为飞机着陆阶段,中间事件 B 的最小割集是底事件 D_1 和底事件 D_2。根据发动机顶层故障事件的概率计算方法,使用顶事件的飞行阶段影响因素和最小割集概率计算顶事件 A 的发生概率为 $P(A)=P(B)\times F(C)=[(1-e)^{-\lambda t_0}]\times\beta$,其中 β 为飞机着陆阶段时间占整个飞行阶段时间的比例。

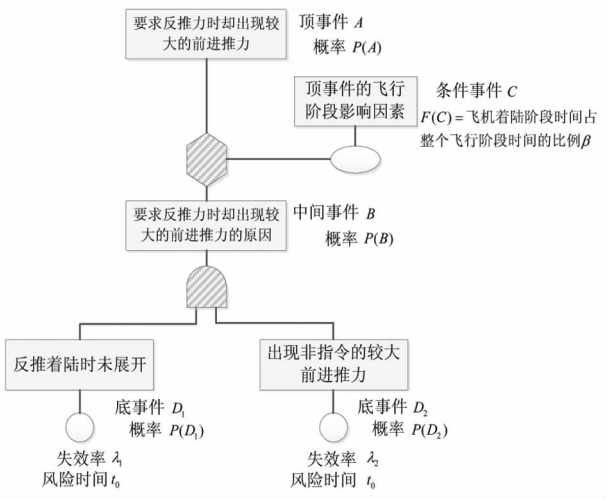

图 3　“要求反推力时却出现较大的前进推力”的故障树

5　结论

本文面向民用航空发动机的安全性设计,从安全性要求出发,使用故障树对发动机顶层故障事件的潜在原因及其途径进行建模,给出了故障树分析的开展时机及作用。然后,考虑顶事件的飞行阶段影响因素和故障树最小割集的概率,给出了顶事件发生概率的计算模型,并结合示例对该计算方法进行应用。

此外,本文仅给出发动机顶层故障事件的概率计算模型,未说明降低顶事件概率的措施。为了将顶事件发生概率降低至可接受状态,可从提高发动机组件可靠性、采取冗余设计、消除底事件等方面开展进一步研究。

参考文献:

[1] FAA. Guidance material for 14 CFR § 33.75, safety analysis: AC 33.75-1A[S]. U.S.: Federal Aviation Administration, 2015: 4-13.

[2] EASA. Certification specifications and acceptable means of compliance for engines: CS-E[S]. European Aviation Safety Agency, 2015: 121-124.

[3] 郭博智, 王敏芹, 阮宏泽. 民用飞机安全性设计与验证技术[M]. 北京:航空工业出版社, 2015: 188-

200.
[4] 张光炯, 孙军帅. 民用飞机高升力系统设计中安全性评估方案研究[J]. 航空工程进展, 2020, 11(2): 286-292.
[5] 董力, 吴雨婷, 韩冰, 等. 基于 FTA 的某型航空发动机电子控制系统安全性分析[J]. 电子技术与软件工程, 2019(17): 100-102.
[6] 朱自伟, 冯兴乐, 徐锦涛, 等. 基于故障树的电能表顶事件发生概率计算分析[J]. 计算机与数字工程, 2020(4): 767-772.
[7] FAA. System design and analysis: Arsenal version of AC 25.1309[S]. U.S.: Federal Aviation Administration, 2002: appendix 3: 34.
[8] SAE. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: ARP4761[S]. Warrendale: SAE, 1996: 12-22, appendix D: 50-55, 90-91.
[9] YUGE T, TAGAMI K, YANAGI S. Calculating top event probability of a fault tree with many repeated events [J]. Journal of Quality in Maintenance Engineering, 2006: 12(4): 364-372.
[10] 中华人民共和国工业和信息化部. 民用飞机研制程序: HB 8525-2017[S]. 北京: 中华人民共和国工业和信息化部, 2017: 5-13.
[11] 中国民用航空局. 航空发动机适航规定: CCAR-33R2[S]. 北京: 中国民用航空局, 2012: 40-43.

作者简介

连　超　男, 硕士, 工程师。主要研究方向: 民用航空发动机安全性设计与评估。E-mail: lianchaoyouss@163.com

Research on probability calculation of top level failure event for civil aviation engine

LIAN Chao *

(AECC Commercial Aircraft Engine Co., Ltd., Shanghai 200241, China)

Abstract: To satisfy the safety requirement of civil aircraft engine, it is required that the risk of top level engine failure event shall be controlled to an acceptable level. According to the risk control requirements of top event, the expected probability of top level event shall be controlled below the acceptable value. Based on the predicted probability requirement of top level event, this paper provides a "top-down" fault tree analysis method to analyze the potential causes of top level event and build fault tree step by step, and explains the role of fault tree analysis Then the calculation of top level event probability is studied. By considering the influence factors of flight phase of top level event, the minimal cut set of fault tree and its probability, the failure rate of basic event and its risk time, the calculation model of top level event occurrence probability is provided. Meanwhile, the calculation model of top event probability is applied with an example to verify the feasibility of the calculation method of top event probability. The top event probability calculation model proposed in this paper can provide strong technical support for the risk control requirements of engine top-level fault events.

Keywords: engine; failure event; probability; risk time

* Corresponding author. E-mail: lianchaoyouss@163.com