http：//myfj. cnjournals. com　myfj_sadri@163. com　(021)20866796

DOI：10. 19416/j. cnki. 1674-9804. 2024. 03. 020

航空发动机 FADEC 系统限时派遣(TLD)适航安全性分析方法研究

闫　锋*　张彦昌　徐文韬

(中国民用航空飞行学院航空工程学院,广汉 618307)

摘　要：限时派遣(time-limited dispatch,简称 TLD)技术既是满足民用航空在安全性基础上保证可盈利性的民航业现实需求,也是重要的航空发动机适航验证环节。对 TLD 分析的来源和基础做了简要介绍,同时基于某型发动机 FADEC 系统可靠性模型,用理论方程和数值解析的方式,对单故障状态下和多故障状态下使用马尔可夫模型(Markov modeling,简称 MM)、蒙特卡罗(Monte Carlo,简称 MC)方法进行分析推导系统平均丧失推力控制(loss of thrust control,简称 LOTC)率公式,通过对比分析双故障状态下两种方法的误差,确定在多故障条件下 MC 方法在可接受误差范围内可有效解决 MM 方法中高维状态空间爆炸问题,确定了仿真分析方法在 TLD 适航的应用流程,验证了 MC 方法在多故障下的合理性和适用性。在仿真分析基础上通过系统可靠性分配分析讨论了可靠性模型优化迭代时带给系统的影响,保证系统能在安全可靠的环境下运行。

关键词：适航;FADEC 系统;安全性分析;TLD

中图分类号：TB3　　**文献标识码**：A　　**OSID**：

0　引言

民用航空公司运营民航飞机的经济性问题一直是民航领域的关键问题,经济问题在满足安全需求的基础上结合系统可靠性得到一定程度解决,在各行业都在提出降本增效的同时[1],民航总局也对航空公司运行效率出台了相关规定[2]。因此,在民用航空中,基于安全性这一根本前提,降低综合运营成本关系到承运人的民航竞争力,而安全性则直接关系到机上人员人身安全。

限时派遣(time limited dispatch,简称 TLD)适航分析指机载系统的冗余单元故障时,在满足适航安全性要求的条件下,无需检修,允许系统带故障运行规定长度的时间[3]。限时派遣分析是商用飞机及航空发动机系统安全性分析和适航审定的重要组成部分,美国联邦航空管理局(FAA)颁布了法规 33 部作为航空发动机的适航审定基础,规定了运输类航空发动机全权限数字电子式控制系统的平均完整性水平必须好于或等于每十万飞行小时发生一次丧失推力控制(loss of thrust control,简称 LOTC)事件[4-5],并且根据 FAR 25. 1309 的规定,即使发动机制造商不申请 TLD 适航运行,也要提交一份表明制造商设计的发动机控制系统满足系统完整性要求的安全分析报告[6]。美国汽车工程师协会(SAE)在 1997 年出版了第一版发动机电子控制系统限时派遣分析指导原则航空推荐规范 ARP5107A。

现代航空运输飞机的发动机控制系统主要是

* **通信作者**. E-mail：yfcafuc@163. com

基金项目：J2023-030 中央高校基本科研业务费专项资金资助;XKJ2022-7 中国民用航空飞行学院研究生教育教学研究项目;GAMRC2021ZD04 四川省通用航空器维修工程技术研究中心重点项目;No. 2022NSFSC1885 四川省自然科学基金。

引用格式：闫锋,张彦昌,徐文韬. 航空发动机 FADEC 系统限时派遣(TLD)适航安全性分析方法研究[J]. 民用飞机设计与研究,2024(3):128-136. YAN F,ZHANG Y C, XU W T. Research on airworthiness safety assessment method of time-limited dispatch (TLD) for the FADEC system of aero-engine[J]. Civil Aircraft Design and Research,2024(3):128-136(in Chinese).

全权限数字电子式控制系统(full authority digital engine control,简称 FADEC)并采用双通道冗余架构,控制系统可以实现智能健康功能管理下的自我故障隔离,并在停场时间内提供故障信息。本文利用先进的 FADEC 系统可靠性模型计算出适合的系统带故障派遣时间,从而提高航班的正点率。

1　TLD 适航流程分析

根据 SAE5107C、CCAR33、FAA33.28 部相关规定对 FADEC 系统进行 TLD 安全性分析,结合可靠性系统架构、采样系统故障信息,在充分评估故障危险性影响的基础上形成技术文件支持的 TLD 分析策略[1]。

1.1　TLD 派遣决策分析

TLD 适航分析的目的就是在简化模型(如图 1 所示)上建立控制系统,可派遣性可划分为如下两个类别:

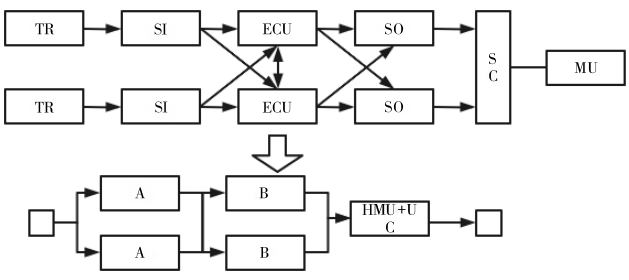

图 1　FADEC 系统可靠性简化模型

1) 基于 SAE 指南证明机队 FADEC 控制系统平均可靠性,保证故障发生时系统危险等级在适航法规限制之下:

$$F_{\mathrm{LOTC}} \leqslant 10^{-5} \tag{1}$$

2) 证明所有给定的建议派遣配置好于 FAA 要求的降级控制系统状态的瞬时丧失推力控制(loss of thrust control,简称 LOTC)率、机队范围平均可靠性标准或“平均 LOTC 率”,包含系统全勤状态、降级系统状态和未覆盖故障[2]。

(a) 不可派遣(no dispatch,简称 ND)

降级配置引起估算的 LOTC 发生率高于 100 次每百万飞行小时;不管计算的 LOTC 率如何,关键资源或者关键功能完全丧失;不管计算的 LOTC 率如何,不能管理发动机超速或者关键限制保护功能[2];

(b) 短时派遣(short time dispatch,简称 ST)

计算的 LOTC 发生率高于 75 次每百万飞行小时,但少于 100 次每百万飞行小时;不管计算的 LOTC 率多少,故障发生导致 FADEC 系统恢复到基本的单通道操作。

(c) 长时派遣(long time dispatch,简称 LT)

不会陷入短时或者不能派遣类别,LOTC 率小于 75 次每百万飞行小时。

1.2　FADEC 系统故障分析

故障状态的定性分析是故障树分析(fault tree-analysis,简称 FTA)方法的关键步骤,也是对故障影响程度定量分析的基础。FTA 方法的目的就是对要分析的目标寻找导致顶事件发生的所有故障模式,确定故障树的全部最小割集,从而计算出顶事件的故障概率和基本事件重要度,TLD 分析通常与失效模式和后果分析(failure mode and effects analysis,简称 FMEA)结合确定故障定量影响层级和导致 LOTC 事件发生的直接原因[3]。

在适航符合性验证分析中,以控制系统发生 LOTC 事件作为系统 FTA 的最终的顶事件,将系统划分为 21 个次级事件组成相对独立的故障识别体系,以此为基础性 FMEA 元素完成相关系统的安全约束[4]。

2　TLD 马尔可夫方法分析

实际承运人运营过程中采用的飞行报告(pilot report,简称 PIR)、最低设备清单(minimum equipment list,简称 MEL)、维修策略都会导致时间序列下故障过程难以分析,无法精准表达系统全修复特性,马尔可夫对高维状态空间虽然也存在难以表述等问题,但 TLD 分析只会涉及两个故障的状态空间[5]。

2.1　单故障马尔可夫模型分析

单故障马尔可夫模型仅考虑单故障发生后发生继发故障进入控制系统的 LOTC 状态,多重故障由于系统高可靠性可作为少数情况计算系统从全勤向 LOTC 状态转移的概率[6]。

单故障 FADEC 状态下闭环马尔可夫如图 2 所示,系统从全勤状态向 LOTC 状态转移路径。

图 2 中各符号的物理含义如下:λ_{ST}、λ_{LT}、$\lambda_{\mathrm{L.LOTC}}$、$\lambda_{\mathrm{S.LOTC}}$ 表示组件故障率;μ_{ST}、μ_{LT} 表示组件或系统修复率,其中 μ_{FB} 系统进入 LOTC 状态全修复后恢复到全勤状态,理想值设置为 1.0;$\lambda_{\mathrm{HM+UC}}$ 表示系统发生执行机构机械故障或者是未覆盖故障导致系统直接进入 LOTC 状态,系统在执行维修措施

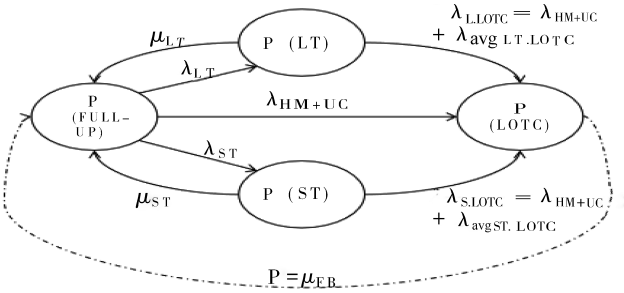

图 2　单故障闭环马尔可夫转移图

之前不能签派[7]。

系统状态变化率方程：

$$\begin{cases} \mu_{LT} = \dfrac{1}{T_{LT-RE}}, \lambda_{LOTC} = \dfrac{P_{in-LOTC}(LOTC)}{1-P(LOTC)} \\ \dfrac{dP_{FU}}{dt} = \mu_{LT} \times P_{LT} + \mu_{ST} \times P_{ST} - (\lambda_{LT} + \lambda_{ST} + \lambda_{HM+UC}) \times P_{LT} \\ \dfrac{dP_{LT}}{dt} = \lambda_{LT} \times P_{FU} - (\lambda_{L.LOTC} + \mu_{LT}) \times P_{LT} \\ \dfrac{dP_{ST}}{dt} = \lambda_{ST} \times P_{FU} - (\lambda_{S.LOTC} + \mu_{ST}) \times P_{ST} \\ P_{LT} + P_{ST} + P_{FU} + P_{LOTC} = 1 \end{cases} \tag{2}$$

其中，P_{LOTC} 的微分方程为：

$$\frac{dP_{LOTC}}{dt} = \lambda_{HM+UC} \times (P_{LT} + P_{ST} + P_{FU}) + \lambda_{L.LOTC} \times P_{LT} + \lambda_{S.LOTC} \times P_{ST} - \mu_{FB} \times P_{LOTC} \tag{3}$$

基于该模型求在极限概率下的稳态解，即设置条件概率 $dP/dt=0$，对稳态时方程求解：

$$\begin{cases} 0 = \mu_{LT} \times P_{LT} + \mu_{ST} \times P_{ST} - (\lambda_{LT} + \lambda_{ST} + \lambda_{HM+UC}) \times P_{LT} \\ 0 = \lambda_{LT} \times P_{FU} - (\lambda_{L.LOTC} + \mu_{LT}) \times P_{LT} \\ 0 = \lambda_{ST} \times P_{FU} - (\lambda_{S.LOTC} + \mu_{ST}) \times P_{ST} \\ 0 = \lambda_{HM+UC} \times (P_{LT} + P_{ST} + P_{FU}) + \lambda_{L.LOTC} \times P_{LT} + \lambda_{S.LOTC} \times P_{ST} - \mu_{FB} \times P_{LOTC} \\ P_{LT} + P_{ST} + P_{FU} + P_{LOTC} = 1 \end{cases} \tag{4}$$

综合上述公式求解 λ_{LOTC}，得出系统 LOTC 为：

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} \times P_{FU} + \lambda_{L.LOTC} \times P_{LT} + \lambda_{S.LOTC} \times P_{ST}}{1 - P(LOTC)} \tag{5}$$

将状态概率拆解得到以失效率和修复率为基础的系统失效率方程：

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} + \dfrac{\lambda_{LT} \times \lambda_{L.LOTC}}{\mu_{LT} + \lambda_{L.LOTC}} + \dfrac{\lambda_{ST} \times \lambda_{S.LOTC}}{\mu_{ST} + \lambda_{S.LOTC}}}{1 + \dfrac{\lambda_{LT}}{\mu_{LT} + \lambda_{L.LOTC}} + \dfrac{\lambda_{ST}}{\mu_{ST} + \lambda_{S.LOTC}}} \tag{6}$$

2.2　多故障 TLD 马尔可夫计算

在 FADEC 系统可靠性分析中，大多涉及双故障的组合故障状态，对三个或三个以上的组合故障依据适航规定直接判定系统为“ND”状态[8]，因此在法规约束下可创建系统双故障状态下马尔可夫模型如图 3 所示。基于图 3 模型计算系统 LOTC 率的状态转移概率矩阵：

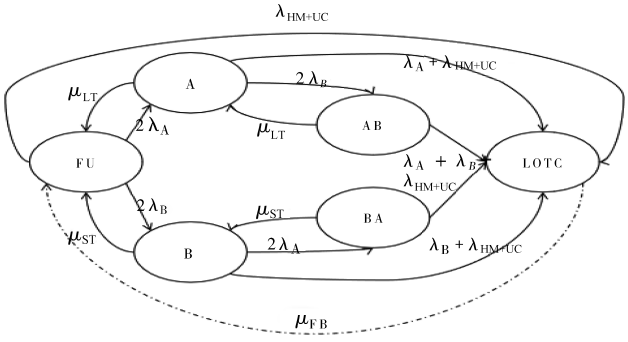

图 3　双故障转移状态 MM 模型

$$P = \begin{bmatrix} P_{11} & 2\lambda_A & 2\lambda_B & 0 & 0 & \lambda_{HM+UC} \\ \mu_A & P22 & 0 & 2\lambda_B & 0 & \lambda_B + \lambda_{HM+UC} \\ \mu_B & 0 & P33 & 0 & 2\lambda_A & \lambda_A + \lambda_{HM+UC} \\ 0 & \mu_A & 0 & P44 & 0 & \lambda_A + \lambda_B + \lambda_{HM+UC} \\ 0 & 0 & \mu_B & 0 & P55 & \lambda_A + \lambda_B + \lambda_{HM+UC} \\ \mu_{FB} & 0 & 0 & 0 & 0 & P66 \end{bmatrix} \tag{7}$$

当系统到达稳态时，得到系统 LOTC 率为：

$$\lambda_{LOTC} = [\lambda_{HM+UC} \times P_{FU} + (\lambda_B + \lambda_A + \lambda_{HM+UC}) \times (P_{AB} + P_{BA}) + (\lambda_A + \lambda_{HM+UC}) \times P_A + (\lambda_B + \lambda_{HM+UC}) \times P_B] / [1 - P(LOTC)] \tag{8}$$

代入系统可靠率守恒方程得：

$$\lambda_{LOTC} = [\lambda_{HM+UC} \times P_{FU} + (\lambda_B + \lambda_A + \lambda_{HM+UC}) \times (P_{AB} + P_{BA}) + (\lambda_A + \lambda_{HM+UC}) \times P_A + (\lambda_B + \lambda_{HM+UC}) \times P_B] / (P_{AB} + P_{BA} + P_{FU} + P_A + P_B) \tag{9}$$

将全勤概率 P_{FU}、故障率 λ 和修复率 μ 表示中间状态概率可得，其中 U 是状态概率之和。

$$U = P_{AB} + P_{BA} + P_A + P_B + P_{FU}$$

$$\lambda_{LOTC} = P_{FU} + \frac{2\lambda_B + \mu_{ST}}{\mu_{ST} + 2\lambda_A + \lambda_B + \lambda_{HM+UC}} \times P_{FU} + \frac{2\lambda_A + \mu_{LT}}{\mu_{LT} + 2\lambda_B + \lambda_A + \lambda_{HM+UC}} \times P_{FU} + \left(\frac{2\lambda_B}{\mu_{LT} + \lambda_B + \lambda_A + \lambda_{HM+UC}} + \frac{2\lambda_A}{\mu_{ST} + \lambda_B + \lambda_A + \lambda_{HM+UC}} \right) \times P_{FU}$$

$$\lambda_{LOTC} = \frac{\lambda_{HM+UC} \times P_{FU}}{U} + \frac{(\lambda_A + \lambda_{HM+UC}) \times \dfrac{2\lambda_A + \mu_{LT}}{\mu_{LT} + 2\lambda_B + \lambda_A + \lambda_{HM+UC}} \times P_{FU}}{U}$$

$$+\frac{(\lambda_B+\lambda_{HM+UC})\times\dfrac{2\lambda_B+\mu_{ST}}{\mu_{ST}+2\lambda_A+\lambda_B+\lambda_{HM+UC}}\times P_{FU}}{U}$$

$$+\frac{(\lambda_A+\lambda_B+\lambda_{HM+UC})\times P_{FU}\times\left(\dfrac{2\lambda_B}{\mu_{LT}+\lambda_B+\lambda_A+\lambda_{HM+UC}}+\dfrac{2\lambda_A}{\mu_{ST}+\lambda_B+\lambda_A+\lambda_{HM+UC}}\right)}{U} \tag{10}$$

经过适航审定的民用航空大涵道比涡扇发动机所搭载的第三代 FADEC 系统,冗余部件的失效率一般控制在 10^{-5} 到 10^{-8} 之间,双故障的同时失效已经是小概率事件,更多元器件同时失效是极小概率事件,可不做考虑[9]。系统修复原则一般遵循基于全修复的维修策略,系统修复率一般为 10^{-3}。

3　基于蒙特卡罗模拟的 FADEC 系统安全性评估

蒙特卡罗方法基于大数定律来解决随机事件问题。它通过在系统状态空间的随机游走来模拟随机过程,从而能够解决马尔可夫方法在高维空间所存在的空间爆炸问题。通过随机抽样生成大量随机值,蒙特卡罗方法能近似模拟并比较多次迭代的算数平均值。在复杂系统可靠性工程中,蒙特卡罗方法能很好地解决多维度、多状态问题[10]。

3.1　TLD 蒙特卡罗仿真分析

1) 维修决策过程分析

单故障或者多故障的维修决策都是基于定期维修原则或者按最低设备清单维修,核心主要是维修时机的选择,航空公司在平衡系统安全性问题和运营经济性问题时可自行选择最佳的维修策略,多故障派遣下维修决策有更丰富的选择性[11],也可能影响计算系统 LOTC 率的派遣间隔维修策略方式,如图 4 所示。

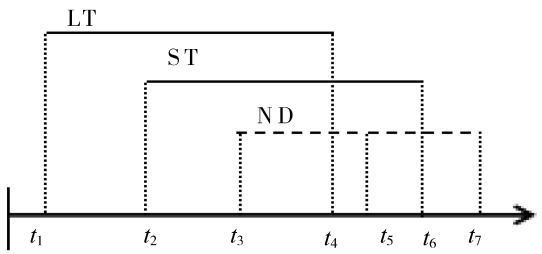

图 4　维修策略方式图

(1) 多故障状态下,TLD 派遣下维修策略的选择可能出现派遣间隔结束后存在多个故障需要维护,根据每个故障派遣间隔不同可选择的维修方案也不同,ST 故障派遣间隔 t_2-t_6,LT 派遣间隔 t_1-t_4。当存在故障 i 发生后优先修复 $\lambda_{i.\,LOTC}(t)$ 较大的故障,保证派遣时间小于 T_{LT}、T_{ST}。如果存在 ND 级别故障,则在 t_3 时刻立即修复故障,多余存在的故障可随之一并修复或调整派遣间隔从 t_3 调整到 t_6、t_7。对于三个或三个以上故障则立即修复故障到可容错降级派遣级别,调整派遣间隔从 t_4 到 t_6。航空公司往往在维修周期平均修理时间(mean time to repair,简称 MTTR)内选择一次性修复系统存在的所有故障,缩短系统全生命周期内 MTTR,提高控制系统平均故障时间(mean time to failure,简称 MTTF)数值,保证系统安全性,维修时间的减少意味着每个维修工时的投入变大,对航司的维修能力提出了更高要求[12]。

(2) 选择维修策略时执行依据系统监控的故障信息只维修需要修复的故障组,如 LT、ND 故障同时发生时,在 t_3 到 t_5 时刻只修复 ND 故障,修复完后继续派遣降级系统到 t_7;同理 ST、ND 故障同时发生时,修复系统后派遣到 t_6 时刻;LT、ST 故障发生时,首先保证系统可派遣时间 T_{LOTC} 在 600 Fh 以上,否则立即修复 ST 故障,再对 LT 故障派遣到 t_5。这种维修策略对于维修人员较易操作和执行,对维修能力要求并不高,在周期维护中就能完成故障修复,是维修成本较小的一种维修策略,也是在模拟派遣环境中较易计算的决策方式[13]。

(3) 蒙特卡罗方法的模拟仿真思路:基于 FADEC 系统组件失效率生成系统,从初始状态到寿命终点中的故障时间随机数,即从已知的组件故障率分布生成随机变量实现 MC 模拟过程。从原始的概率分布中抽样产生 N 个数据点,模拟过程产生的方程如式(11)所示。依据服从大数定理和单元寿命的随机值,当故障改变系统状态到达 LOTC 时,这段时间称为 T_{LOTC}[14]。系统多次循环模拟得到 $F(\mathrm{LOTC})$。

$p(z/x)$ 随机采样

$$z^{(1)},z^{(2)},z^{(3)},z^{(4)},z^{(5)},\cdots\cdots,z^{(N)}\sim p(z/x)$$

$$\frac{1}{N}\sum_{i=1}^{N}f(z^{(i)})\approx\int_z p(z/x)f(z)\,dz \tag{11}$$

$$F(\mathrm{LOTC})=f(T_{ST},T_{LT})$$

在难以采样的情况下,蒙特卡罗对复杂分布的概率密度函数会执行在辅助建议分布基础上对复杂函数进行 Acceptance-Rejection 过程,从而产生可接受的样本 U。

2）TLD 的蒙特卡罗仿真流程步骤如下：

（1）对需要分析的 FADEC 系统可靠性模型建立合适的参数模型，包含组件故障率（λ_A，λ_B，λ_{HM+UC} 等）、基于技术文件给定系统可派遣的长时派遣间隔（LT=600 Fh）和短时派遣间隔（ST=150 Fh）。

依据系统可靠度函数判定组件状态：

$$\begin{cases} R_S(t)=f(R(t));R_i(t)=e^{-\lambda_i t}; \\ R(t)=\ [R_1(t)\quad R_2(t)\quad \cdots\cdots\quad R_n(t)] \end{cases} \tag{12}$$

（2）初始化 T（时间）和 S（部件状态），定义模拟次数，令次数 $N=0$ 进入第一次模拟，其中可靠性模型瞬时 LOTC 可表示为：

$$\begin{cases} T=[t_1\quad t_2\quad \cdots\cdots\quad t_n]; \\ S=[S_1\quad S_2\quad \cdots\cdots\quad S_n]; \\ \Lambda=[\lambda_1\quad \lambda_2\quad \cdots\cdots\quad \lambda_n]; \\ \lambda_S(t)=f(\Lambda,S(t)) \end{cases} \tag{13}$$

（3）依据技术文件对 T_{error} 取值（如 $\Omega=0.0001$），依据下面公式判断系统平均 LOTC 率是否收敛，如果条件满足则输出结果宣布实验结束，不满足条件则进行下一步。（$F_{ave\text{-}LOTC}$ 表示系统平均 LOTC 率）

$$\begin{aligned} F_{ave-LOTC}(N)&=\frac{N}{\sum_{i=1}^{N}T_{LOTC}(i)}; \\ T_{error}(N)&=\left|\frac{F_{ave-LOTC}(N)-F_{ave-LOTC}(N-1)}{F_{ave-LOTC}(N)}\right| \end{aligned} \tag{14}$$

（4）模拟随机生成组件故障 T_i 并记录在时间表中。

（5）判断故障时刻各组件的状态，替换 $R(t)$ 和组件状态 S。（$\min T_i=t_n$）

a）若 $n=0$，模拟系统终止，进入步骤 10；

b）若 $n\neq 0$，基于组件状态选择执行步骤。

当 $S_n(t)=0$，表明组件 n 处于故障状态，更新组件状态 S；$S_n=1$，执行第 6 步；$S_n(t)=1$，表明组件 n 进入维修间隔 MTTR，更新组件状态 S；$S_n=0$，执行第 8 步。

（6）系统是否进入 LOTC 状态，由 $R(t)$ 和系统可靠度函数公式判断并计算 $R_S(t)$。如果 $R_S(t)=0$，则控制系统进入 LOTC 状态，$N=N+1$，执行第 9 步，判定为否则执行第七步。

（7）确定派遣级别，根据瞬时系统 LOTC 判断，ND、ST 类更新 S、T，LT 类更新 T，$t_n=t_n+t_{rand}$。返回第 5 步。

（8）模拟修复故障组件，更新 T，$t_n=t_n+t_{rand}$。返回第 5 步。

（9）全修复控制系统组件到 Full-Up 状态，更新 S、T。

$\forall i\in[1,n]\wedge S_i=1\Rightarrow S_i=0, t_i=t_i+t_{rand}$，$R_n(t)=e^{-\lambda_n t}$，返回第 5 步。

（10）统计 N 次模拟时间 $T_{sim}(N)$ 和 $F_{ave\text{-}LOTC}$。

3.2　多故障蒙特卡罗仿真分析

为了尽可能模拟真实环境，结合技术文件提供的适航论证参数说明，建立了 3 000 Fh 的模拟仿真。

在前文的马尔可夫仿真基础上以及相同的系统限制条件下，对比说明蒙特卡罗方法在 TLD 安全性中的合理性。将多故障马尔可夫、蒙特卡罗方法进行比较，表 1 阐述了在标准短时派遣 $T_{ST}=150$ Fh 条件下，两种不同方法在以 T_{LT} 为自变量时的变化规律。

表 1　马尔可夫方法和蒙特卡罗方法下 TLD 对比

LT/Fh	多故障 MM	多故障 MC	多故障 MM	多故障 MC
250	$2.800\,8\times10^{-6}$	2.078×10^{-6}	2.801×10^{-6}	2.447×10^{-6}
500	$3.124\,9\times10^{-6}$	2.592×10^{-6}	3.125×10^{-6}	2.867×10^{-6}
750	$3.442\,1\times10^{-6}$	3.105×10^{-6}	3.442×10^{-6}	3.239×10^{-6}
1 000	$3.752\,7\times10^{-6}$	3.569×10^{-6}	3.753×10^{-6}	3.644×10^{-6}
1 250	$4.056\,8\times10^{-6}$	4.028×10^{-6}	4.057×10^{-6}	4.020×10^{-6}
1 500	$4.354\,7\times10^{-6}$	4.475×10^{-6}	4.355×10^{-6}	4.399×10^{-6}
1 750	$4.646\,4\times10^{-6}$	4.923×10^{-6}	4.646×10^{-6}	4.713×10^{-6}
2 000	$4.932\,2\times10^{-6}$	5.346×10^{-6}	4.932×10^{-6}	5.060×10^{-6}
2 250	$5.212\,1\times10^{-6}$	5.774×10^{-6}	5.212×10^{-6}	5.394×10^{-6}
2 500	$5.486\,4\times10^{-6}$	6.180×10^{-6}	5.486×10^{-6}	5.700×10^{-6}
2 750	$5.755\,2\times10^{-6}$	6.525×10^{-6}	5.755×10^{-6}	6.044×10^{-6}
3 000	$6.018\,6\times10^{-6}$	6.922×10^{-6}	6.019×10^{-6}	6.352×10^{-6}

将表中数据制成曲线比对 FADEC 系统 LOTC 率的变化趋势，TLD 仿真结果如图 5 所示。由于蒙特卡罗方法是对理想系统的预测仿真，预测结果误差在可接受范围内，故仿真结果对于控制系统安全性是可接受的。

蒙特卡罗方法是由随机抽样算法下形成的点的聚合组成的曲线，对蒙特卡罗输出的图形进行线性回归以及拟合，其结果如表 2 所示。

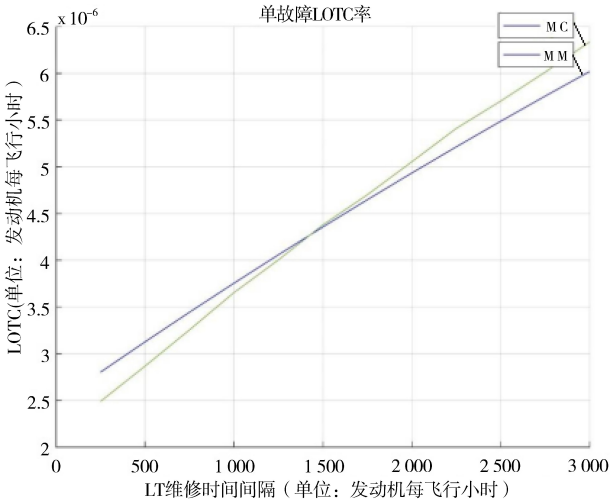

图 5　多故障状态下系统 LOTC 变化对比图

表 2　拟合优度分析结果

拟合优度	线性回归	2 次多项式	3 次多项式
SSE	4.691×10^{-14}	$2.699\ 1\times10^{-15}$	$2.453\ 4\times10^{-15}$
R-square	0.997 3	0.999 8	0.999 9
Adj-R	0.997 1	0.999 8	0.999 8
RMSE	$6.849\ 1\times10^{-8}$	$1.731\ 8\times10^{-8}$	$1.751\ 2\times10^{-8}$

根据其中一组蒙特卡罗方法得出的拟合曲线可以看出二次多项式就能建立可信的拟合最优曲线表达式,其中 R 值不断逼近最优值,根据常规表达式建立在 $T_{ST}=150$ Fh 时的函数表达式为:

$$F(\mathrm{LOTC}) = -5.755\times10^{-9}\times\mathrm{LT}^2 + 4.256\times10^{-7}\times\mathrm{LT} + 2.029\times10^{-6} \quad (15)$$

表 3　蒙特卡罗方法和马尔可夫方法对比误差数据

LT/Fh	250	500	750	1 000	1 250	1 500	1 750	2 000	2 250	2 500	2 750	3 000
R%	0.025	0.012	0.001	0.012	0.018	0.031	0.04	0.045	0.056	0.062	0.068	0.075

通过不同方法的多故障状态预测对比图,建立以系统丧失推力事件 10^{-5} 为限制的误差分析图,马尔可夫、蒙特卡罗方法的误差来源可能是故障维修方法的不同导致在控制系统生命周期中系统 LOTC 率出现误差[16]。

根据表 3 的误差数据可得 1 500 Fh 下两种方法误差控制在 0.05 以下符合 SAE5107 文件对模型预测数据误差在 5% 以内的要求[15]。在 0~3 000 Fh 的裕度要求中平均误差值 0.037 1,符合 SAE5107 文件对模型预测数据平均误差值在 5% 以内的要求[15]。TLD 分析误差来源可能是系统未覆盖故障和机械组件故障引起仿真模拟中计算误差,图 6 为蒙特卡罗方法和马尔可夫方法对比误差图。

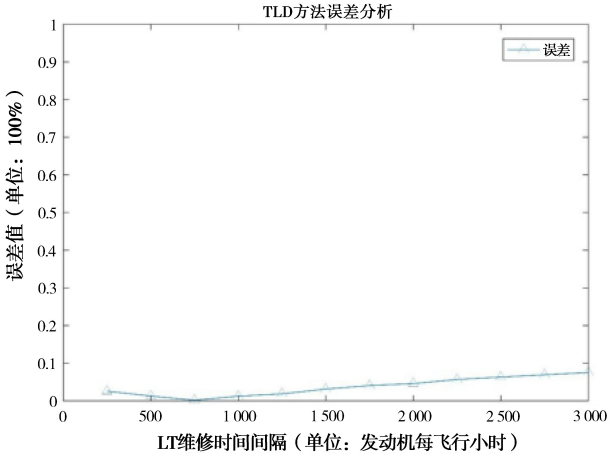

图 6　蒙特卡罗方法和马尔可夫方法结果误差对比图

4　系统可靠性模型优化仿真分析

4.1　部件重要度

把系统的可靠度指标直接分配给各个单元,计算比较复杂。将每组并联单元适当组合成单个单元,并将此单个单元看成是串联系统中的一个等效单元,用串联系统可靠度分配方法,将系统的容许失效率或失效概率分配给各个串联单元和等效单元;再确定并联部分中每个单元的容许失效率或失效概率 λ_i。

FUSSELL-VESELY 重要度在 n 个组件构成的系统 $N=(1,2,3,\cdots\cdots,n)$ 中,组件处于失效或者运行状态,系统状态只取决于组件状态。令 $X=(X_1, X_2, X_3,\cdots\cdots,X_n)$ 表示组件在给定连续时间状态下的随机向量,其中 $X_n=1$ 或 $X_n=0$ 表示元件 n 处于运行或失效状态,令 $\phi(X)$ 为控制系统的结构函数。系统组件瞬时重要度能表示为:

$$\begin{aligned} I'_B(t) &= E[\phi(0_i,X(t)) - \phi(1_i,X(t))] \\ &= 1\times P[\phi(1_i,X(t)) - \phi(0_i,X(t)) = 1] \\ &\quad + 0\times P[\phi(1_i,X(t)) - \phi(0_i,X(t)) = 0] \\ &= P[\phi(0_i,X(t)) - \phi(1_i,X(t)) = 1] \end{aligned} \quad (16)$$

组件 i 的 FUSSELL-VESELY 重要度值 $I^i_{\mathrm{FV}}(t)$ 表

明系统失效的概率与包含组件 i 在内的一个割集的失效一致,重要度为:

$$I_{FV}^{i}(t)=\frac{G_i(q(t))}{G(q(t))} \tag{17}$$

基于 AGREE 分配法,系统从飞机设计阶段分配设计可靠性需求到各子系统,由系统可靠性指标值确定各装置相应的可靠性指标值。第 i 个组件的重要度为:

$$\omega_i=\frac{n_i}{N_i} \tag{18}$$

将控制系统分割为等效串联系统的子集,则系统的可靠度 R 表示为:

$$\begin{aligned} R_S&=\prod_{i=1}^{n}R'_i \\ R'_i&=1-\omega_i F_i \end{aligned} \tag{19}$$

对于电子元器件寿命分布函数 $f=e^{-x}$,当 $x<<1$ 时,有 $e^{-x}\approx 1-x$,

$$\begin{aligned} &R_S\approx\prod_{i=1}^{k}(1-\omega_i\lambda_i t_i)\approx\prod_{i=1}^{k}e^{-\omega_i\lambda_i t_i}; \\ &R'_i=(R_S)^{\frac{1}{k}}=e^{-\omega_i\lambda_i t_i}; \\ &\ln R'_i=\ln(R_S)^{\frac{1}{k}}=\ln e^{-\omega_i\lambda_i t_i}\Rightarrow\frac{1}{k}\ln R_S=\omega_i\lambda_i t; \end{aligned} \tag{20}$$

在考虑装置复杂度影响因素后:

$$\lambda_i^{*}=n_i(-\ln R_S^{*})/(N\omega_i t_i) \tag{21}$$

FADEC 控制系统的零部件重要度不仅取决于它在系统可靠性模型中的位置和失效模式,还取决于它随时间的功能退化程度,这对设计和选择 TLD 派遣下的维修策略十分重要。当某些组件可被高级模型计算值代替时属于可靠性增长试验(RGT)的一种,可为控制系统可靠性提供不断改进的可能性,通过试验结果验证系统达到预期可靠性目标[16]。

4.2　系统安全性模型分析

建立如图 7 所示的可靠性融合模型,融合模型的建立可有效提高发动机和飞机的可靠性,对于在可靠性模型中移除的硬件问题,将在闭环马尔可夫模型中给这些元器件设置零故障率。此外,减少导致 LOTC 事件的组件可以使系统未覆盖故障率 λ_{UC} 略微下降,这也使控制系统可靠度上升。

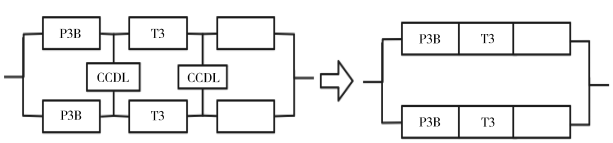

图 7　T3、P3B 可靠性模型演变

依据技术文件,压力传感器 P3B 组件的失效率 $\lambda_F=2.98\times10^{-6}$,温度传感器 T3 的失效率 $\lambda_F=3.22\times10^{-6}$,设置 ST = 150 Fh,遵循可靠性分配原则,在改变可靠性分配等级的条件下保证系统安全性和 TLD 派遣的合理性。

$$\begin{aligned} &\lambda_i^{*}=n_i(-\ln R_S^{*})/(N\omega_i t_i) \\ &I_{FV}^{i}(t)=\frac{G_i(q(t))}{G(q(t))}=\frac{n_i(-\ln R_S^{*})/(N\omega_i t_i)}{\sum_{i=1}^{n}\lambda_i+\lambda_{UC+HM}} \\ &I_{FV}^{i}(t)\approx I_{FV}(t) \end{aligned} \tag{22}$$

在实际计算过程中,系统未覆盖故障的变化很小:

$$\begin{aligned} &\lambda'_{UC}=\frac{1.93\times10^{-6}-2.87\times10^{-7}-1.08\times10^{-7}}{1.93\times10^{-6}}=0.204\,66 \\ &\because F_{LOTC}=\frac{\lambda'_{UC}}{\Lambda_{FADEC}}=2\%,\theta=2\%\times0.204\,66=0.004\,093\,2 \\ &\therefore\lambda'_{UC}\approx\lambda_{UC} \end{aligned} \tag{23}$$

在保证其他系统组件同等可靠性水平下:

$$\begin{aligned} &\theta=\frac{(\lambda_{T3+P3B}^{*}+\lambda_i^{*})/\left(\sum_{i=1}^{n}\lambda_i+\lambda_{UC}\right)}{\lambda'_i/\lambda'}=0.104\,28 \\ &\lambda'=(2.98\times10^{-6}+3.22\times10^{-6})\times\theta=0.646\,539\times10^{-6} \end{aligned} \tag{24}$$

系统依据分配原则,将组件失效率依据参数调整,满足可靠性安全标准形成的系统组件失效率如表 4 所示。

表 4　系统失效率分配表

模型	类型		
	T3	P3B	分配后
初始模型	3.22×10^{-6}	2.98×10^{-6}	4.49×10^{-6}
融合模型	0	0	$5.136\,539\times10^{-6}$

1) 依据图 8 的输出结果可以判断,融合模型在单故障控制系统可靠性模型中,LOTC 值为 $0.665\,39\times10^{-6}$,对某组件失效率改变后仍旧满足 1 500 Fh 的发动机系统的可靠性要求,依据图形数据导出融合模型对系统可靠性的改变值为 0.015 22,对于系统要求的 TLD 派遣间隔时间可以满足。另一方面,元器件在可靠性模型中的减少可

以切实提高系统可靠性,降低系统因未覆盖故障进入 LOTC 状态的概率,因此在此条件下,可靠性模型迭代优化可有效满足安全性需求[17]。

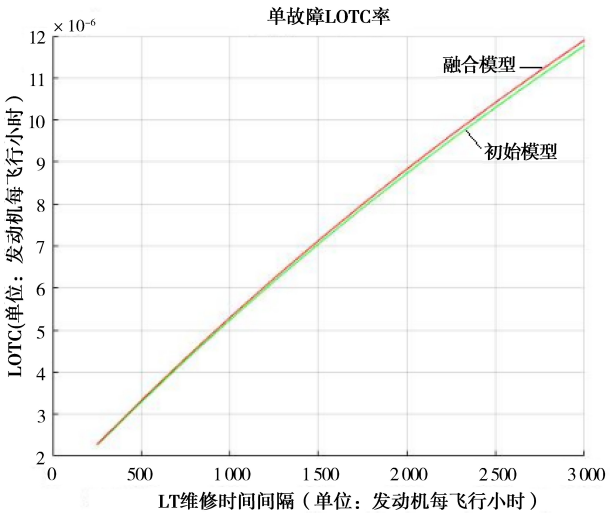

图 8　融合模型前后对比图

2）极限状态下融合模型对比分析:极限状态下设置系统融合模型组件失效率要求提高到10. 69×10^{-6},严格的可靠性安全标准对比如图 9 所示。

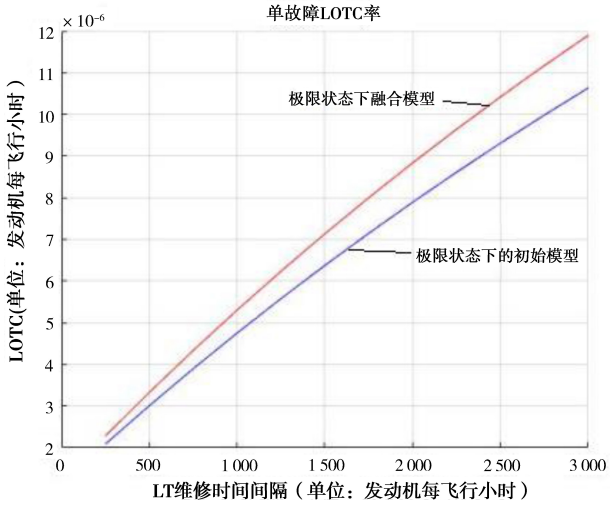

图 9　极限可靠性要求下对比图

从图中可知极限状态概率下,控制在 10^{-5} 时的系统派遣间隔时间达到 2 757 Fh,与原始模型 TLD 的长时派遣间隔 2 366 Fh 都能满足 FAA 对长时派遣间隔的时间要求,从图中对比得出极限状态下失效率改变引起系统可靠性改变可能达到 0. 103 9,因此,即使在极限状态下,系统可靠性水平依旧满足。

5　结论

民用航空公司运营民航飞机的经济性问题一直是民航领域的关键问题,经济问题依托于满足安全需求的基础上结合系统可靠性得到一定程度解决。本文建立了控制系统可靠性结构图和系统故障信息,结合某型航空发动机 FADEC 系统,利用闭环马尔可夫方法和蒙特卡罗方法给出 TLD 安全性模型和计算结果,然后根据动态控制系统对结构调整后的 TLD 安全性和可靠性分配问题做出了解释,为民用航空发动机的技术应用与适航审定提供一点借鉴与参考,对满足国产大飞机的运行需求、促进航空发动机国际化适航审定能力的提升做出一点贡献。

参考文献:

[1] 于蒙蒙. 腾讯持续推进降本增效[N]. 中国证券报, 2022-08-18(A05).

[2] 中国民用航空局. 关于把控运行总量调整航班结构提升航班正点率的若干政策措施[EB/OL]. (2017-09-22)[2023-03-20]. http://www.caac.gov.cn/XXGK/XXGK/ZCFBJD/201709/t20170922_46883.html.

[3] PRESCOTT D R, ANDREWS J D. A comparison of modelling approaches for the time-limited dispatch (TLD) of aircraft[J]. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2006, 220(1): 9-20.

[4] PRESSCOTT D R, ANDREWS J D. Modeling and specification of time-limited dispatch categories for commercial aircraft[J]. ASME Journal of Dynamic Systems, Measurement and Control, 2008, 130(2): 021004-1-021004-10.

[5] SAE International. Guidelines for time-limited dispatch (TLD) analysis for electronic engine control systems: ARP5107C[S]. Warrendale: SAE International, 2018: 8-58.

[6] 民航管理. 民航局发布《2018 年民航行业发展统计公报》[J]. 民航管理,2019(5):77.

[7] 闫锋. 民用航空发动机控制系统时间限制派遣方法[J]. 科学技术与工程, 2014,14(28): 148-152,158.

[8] 中华人民共和国中央人民政府. 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要[N]. 人民日报,2021-03-13(001).

[9] 中国航发商用航空发动机有限责任公司. 一种航空发动机传感器故障容错方法及其容错系统: 202010986491. 7[P]. 2022-04-05.

[10] 白杰,赵平,王伟. FADEC 系统 TLD 的维修策略[J]. 航空维修与工程,2012(6):35-37.
[11] 孙杨慧,杨坤,侯乃先,等. FADEC 系统限时派遣及维修性分析[J]. 系统工程,2017,35(6):152-158.
[12] 中国民用航空局. 航空发动机适航规定:CCAR-33-R2[S]. 北京:中国民用航空局,2011.
[13] 乔磊,李艳军,曹愈远,等. 航空发动机 CCAR33-R2.75 条款适航符合性验证方法[J]. 航空发动机,2016,42(1):99-102.
[14] 李昊燃,雷延生,龚昊伟. 民用航空发动机 ETOPS 型号设计和符合性验证方法研究[J]. 航空工程进展,2022,13(2):129-135.
[15] SAE International. Guidelines for time-limited dispatch (TLD) analysis for electronic engine control systems: ARP5107B[S]. Warrendale: SAE International, 2006.
[16] 蔡景,胡维,陈曦. 全修复策略下 FADEC 系统多故障 TLD 仿真分析[J]. 航空动力学报, 2020,35(4):823-831.
[17] 中国民用航空局. 运输类飞机适航标准:CCAR-25-R4[S]. 北京:中国民用航空局,2011.

作者简介

闫 锋 男,教授,硕士研究生导师。主要研究方向:民用航空器系统工程与可靠性。E-mail: yfcafuc@163.com

张彦昌 男,硕士。研究方向为:航空器系统工程。E-mail: zhang15136674499@163.com

徐文韬 男,硕士。主要研究方向:航空器数字系统可靠性与安全性分析。E-mail:1228607509@qq.com

Research on airworthiness safety assessment method of time-limited dispatch (TLD) for the FADEC system of aero-engine

YAN Feng* ZHANG Yanchang XU Wentao

(School of Aeronautical Engineering, Civil Aviation Flight University of China, Guanghan 618307, China)

Abstract: Time-limited dispatch technology (TLD) is not only to meet the practical needs of civil aviation to ensure profitability on the basis of safety, but also an important airworthiness verification link of aviation engines. The source and basis of TLD analysis are briefly introduced. At the same time, based on the reliability model of FADEC system of a certain engine, MM and MC methods are used to analyze and derive the average LOTC formula of the system under single fault state and multiple fault state by means of theoretical equation and numerical analysis. By comparing and analyzing the error determination of the two methods under the condition of double fault, the MC method can effectively solve the high-dimensional state space explosion problem in the MM method within the acceptable error range under the condition of multiple faults, the application flow of the simulation analysis method in TLD is determined, and the rationality and applicability of the MC method under the condition of multiple faults is verified. On the basis of simulation analysis, the influence of reliability model optimization iteration on the system is discussed through system reliability distribution analysis, so as to ensure that the system can run in a safe and reliable environment.

Keywords: airworthiness; FADEC system; safety analysis; TLD

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