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

DOI: 10.19416/j.cnki.1674-9804.2020.04.002

隐蔽失效适航要求符合性验证分析

刘会星*

(上海飞机设计研究院,上海 201210)

摘 要: 隐蔽失效的适航符合性验证对飞机系统安全性水平会产生重大影响。经过十余年论证,EASA 在 CS/AMC 25.1309 中新增了隐蔽失效的要求。例如要求尽可能消除重大隐蔽失效;为了防止再发生一个失效即导致灾难性失效状态的情况,对由两个失效导致的每个灾难性失效状态,其中任一个在大于单次飞行中是隐蔽失效,要求从隐蔽限制方面限制运行时间,并且从剩余概率限制方面假定一个隐蔽失效已发生时限制所有单个显性失效组合的平均概率。针对系统安全性条款 CS 25.1309(b)新增的隐蔽失效相关要求,分析条款的符合性方法,通过典型故障树分析及其最小割集的示例,说明隐蔽限制和剩余概率限制准则的应用方法。从工程角度说明了条款的应用范围,给出了隐蔽失效的概率和限制暴露时间的计算方法,提升型号系统安全性水平。

关键词: 隐蔽失效;系统安全性;特殊风险;最小割集

中图分类号: V221.91 **文献标识码**: A **OSID**:

0 引言

传统的系统安全性评估采用定量平均概率的方法,以限制机队全生命周期的风险,而在特定飞行中可能存在失效高于平均概率的特殊风险,例如隐蔽失效。隐蔽失效是一种在飞行机组或维修人员发觉前一直保持隐藏状态的失效[1]。隐蔽失效与一个或多个特定失效或事件组合,可能导致灾难性或危险的失效状态,这种隐蔽失效称为重大隐蔽失效。

2010 年 FAA 航空规章制定咨询委员会(ARAC)飞机级安全性分析工作组(ASAWG)发布了特殊风险报告[2],目的是在所有飞机系统、不同的适航当局之间建立协调一致的特殊风险准则。2014 年 EASA 发布修订建议通告[3],建议将隐蔽失效纳入 CS 25.1309(b)条款中。根据工业界意见[4],2020 年 EASA 在 CS 25.1309(b)(第 24 次修订)[5]中正式纳入隐蔽失效的要求。

国内外对运输类飞机隐蔽失效也有一些研究,主要聚焦于计算模型和检查间隔的确定等方面。例如马赞等[6]分析了隐蔽失效计算模型的审定关注点,指出了其中的安全性问题。L. Ozirkovskyy[7]等提出一种包含隐蔽失效的最小割集的平均概率评估方法。戴顺安等[8]结合 SAE ARP 5150 的风险评估理念,利用实际运行维修数据确定故障规律,建立定量风险评估方法。贾宝惠等[9]提出一种平均不可靠度和成本率函数优化检查及恢复间隔的模型。

本文对隐蔽失效的适航要求及其符合性方法进行分析,以典型故障树分析示例说明隐蔽限制和剩余概率限制准则的应用方法,说明条款的工程应用范围、隐蔽失效的概率和限制暴露时间的计算方法,以供型号的系统安全性设计参考。

1 隐蔽失效的适航要求

1.1 CS 25.1309 的变更

CS 25.1309(第 24 次修订)中(b)款新增两项要求,即:

(4) 任何重大隐蔽失效尽可能地消除;如果无法消除,则减小重大隐蔽失效的隐蔽性;

* 通信作者. E-mail: liuhuixing888@163.com

引用格式: 刘会星. 隐蔽失效适航要求符合性验证分析[J]. 民用飞机设计与研究,2020(4):6-11. LIU H X. Compliance verification analysis on latent failure airworthiness requirement[J]. Civil Aircraft Design and Research,2020(4):6-11(in Chinese).

（5）对由两个失效导致的每个灾难性失效状态，其中任一个在大于单次飞行中是隐蔽失效，必须同时证明：

（ⅰ）提供附加的冗余是不切实际的；

（ⅱ）假设在一次给定飞行中发生了单个隐蔽失效时，则失效状态是微小的；

（ⅲ）与每个显性失效组合的隐蔽失效的概率之和不超过 1/1 000。

此外，CS 25.1309（e）款（第 20 次修订）中还新增了审定维修要求的内容：必须制定审定维修要求以防止 CS25.1309（b）条款中所述失效状态的发展，且必须包含于 CS 25.1529 所要求的持续适航文件中的适航限制章节中。另外，EASA 还提议将研制保证等级作为安全性目标之一纳入 AMC 25.1309[10]，但由于 DAL 分配不仅与失效状态影响等级相关，还与系统架构密切相关，利益相关方对此持争议态度，因此该建议被撤回[11]。

1.2 对 CS 25.1309（b）款第（4）条的符合性

对 CS 25.1309（b）款第（4）条的符合性应按照以下系统化的方法：

首先必须采用当前最先进的技术，例如实施的、可靠的失效监测和飞行机组指示系统，以探测那些在大于一次飞行中可能的隐蔽失效，从而尽最大可能地消除重大隐蔽失效。AMC 25-19 第 8 节“重大隐蔽失效相关的设计考虑”提供了附加的指南。

对于每个无法合理消除的重大隐蔽失效，必须通过采用当前最先进的技术以减少暴露时间，而不是依赖间隔漫长的计划维修任务，即，执行飞行员发起的检测或自发的检测（例如，日检的第一次飞行、上电自检测或其他的系统自动化检测）。

当依赖于计划维修任务时，需要开展定量和定性评估以限制隐蔽性。AMC 25-19 第 10 节“CCMR 的识别”提供了附加的指南。

1.3 对 CS 25.1309（b）款第（5）条的符合性

当一个灾难性失效状态涉及两个失效，其中一个在大于一次飞行中是隐蔽失效且无法合理地消除时，要求符合 CS 25.1309（b）款第（5）条。当应用了 CS 25.1309（b）（4）后，涉及多个重大隐蔽失效的失效状态是不太可能预计的，因此重大隐蔽失效的剩余关注点就是 CS 25.1309（b）款第（5）条针对的双重失效。

应尽早确定出重大隐蔽失效，在设计方案中重点明确此类重大隐蔽失效的设计与验证方法。系统安全性评估应解释无法避免的原因，并提供可接受的支撑材料。支撑材料应基于当前最先进技术的设计、过去的经验、良好的工程判断或其他材料，证明不采用其他可能的避免措施的决策（例如，消除重大隐蔽失效或增加冗余）。

25.1309（b）款第（5）条中执行两个准则：隐蔽限制和剩余概率限制。隐蔽限制是为了再发生一个显性失效就导致灾难性失效状态时限制运行时间。这通过要求与每个显性失效组合的隐蔽失效的概率之和不超过 1/1 000 来实现。以一个灾难性失效状态为例：

1）在关注的一个双重失效组合中，一个显性失效仅被组合一次时，单个隐蔽失效的概率需要符合 1/1 000 的准则；

2）在关注的多个双重失效组合中，一个显性失效被组合多次时，隐蔽失效的组合概率需要符合 1/1 000 的准则；

剩余概率限制是为了在单个隐蔽失效发生时限制失效状态的（每飞行小时）平均概率。这通过定义剩余概率为微小的（remote，1E-5）来实现。剩余概率是假设已发生单个隐蔽失效时，再发生单个显性失效就导致灾难性失效状态，所有这些显性失效组合的（每飞行小时）平均概率。

这些要求作为 CS 25.1309（b）（1）的附加，要求灾难性失效状态被证明是极不可能的且不会由单个失效造成。对于符合 1/1 000 的准则，所关注隐蔽失效的概率应从最坏飞行情况的概率中产生，即，在计划维修检查前最后一次飞行中显性失效发生的概率，而隐蔽失效可能发生于两次连续的计划维修检查之间的任何一次飞行。在处理恒定失效率时，如果隐蔽失效的概率小于等于 0.1，则该值应从隐蔽失效可能发生的最大时间与其失效率的乘积计算得到。

2　条款符合性示例

以下示例解释了隐蔽限制和剩余概率限制分析的应用方法，说明了如何与 CS 25.1309（b）（1）一起实施 CS 25.1309（b）（5）的定量要求。以下方法是基于图 2 中识别的普通系统级故障树的灾难性顶事件相关联的最小割集。“最小割集”是指足以导致系统失效或所关注失效状态发生的基本事件的最小集合。

1）最小割集的清单应按割集的阶数展示。这将对所有二阶割集或失效组合进行分组。图 1 故障树的最小割集的完整清单见表 1。

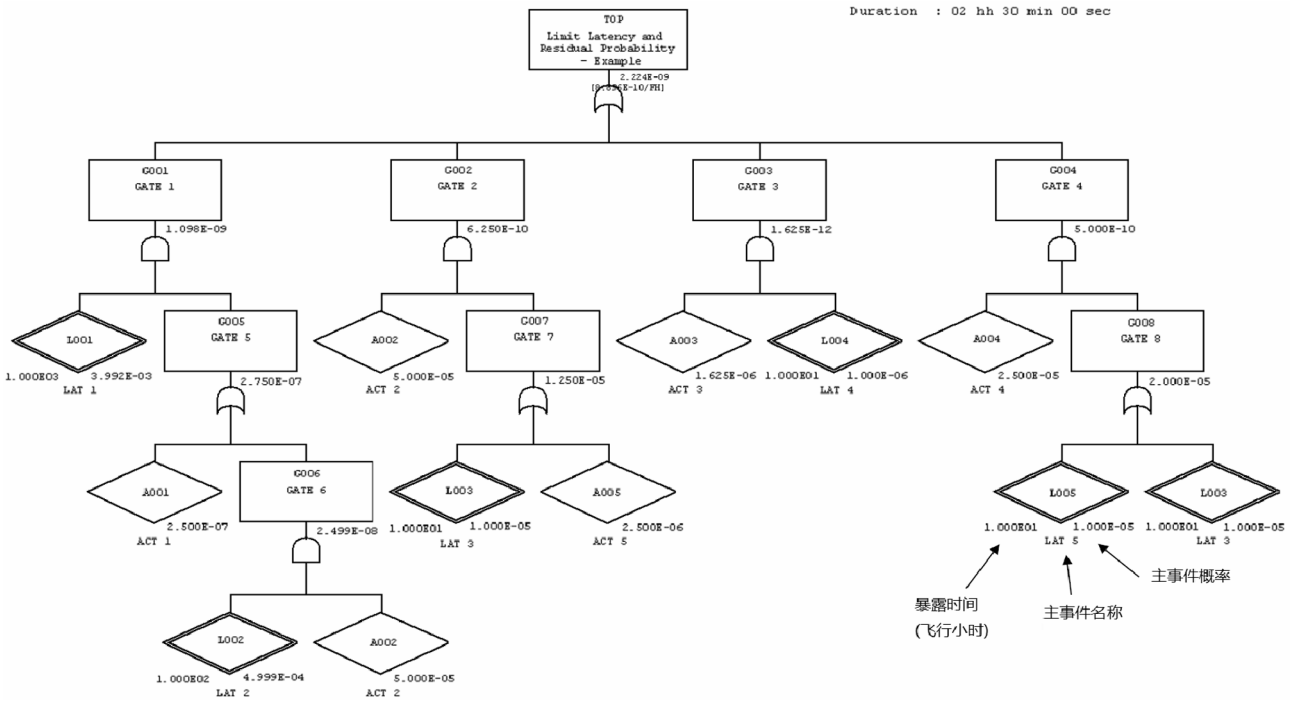

图 1　隐蔽限制和剩余概率限制的故障树示例

表 1　图 1 故障树的最小割集完整清单

序号	概率(每飞行小时)	事件名称	事件描述	失效率	暴露时间(小时)	事件概率(每次飞行)	CS 25.1309(b)(5)适用性和符合性
1	3.992E-10	A001	ACT 1	1.000E-07	2.5	2.500E-07	不符合隐蔽限制的准则(L001 的概率超过了 1.0E-03)
		L001	LAT 1	4.000E-06	1 000.0	3.992E-03	
2	2.000E-10	A002	ACT 2	2.000E-05	2.5	5.000E-05	不符合剩余概率限制的准则(A002 的每飞行小时概率(2.0E-05/FH)超过了 1.0E-05)
		L003	LAT 3	1.000E-06	10.0	1.000E-05	
3	1.000E-10	A004	ACT 4	1.000E-05	2.5	2.500E-05	不符合剩余概率限制的准则(虽然 A004 的每飞行小时概率等于 1.0E-05/FH, A004 和 A002 每飞行小时的组合概率(1.0E-05 + 2.0E-05/FH)超过了 1.0E-05
		L003	LAT 3	1.000E-06	10.0	1.000E-05	注:二阶最小割集#2 和#3 被分组在一起,因为相同的事件 L003 出现在 G002 和 G004 下面
4	1.000E-10	A004	ACT 4	1.000E-05	2.5	2.500E-05	同时符合隐蔽限制和剩余概率限制(A004 的每飞行小时概率等于 1.0E-05/FH, L005 和 L003 的组合概率(1.0E-05 + 1.0E-05)小于 1.0E-03)
		L005	LAT 5	1.000E-06	10.0	1.000E-05	
5	2.000E-11	A002	ACT 2	2.000E-05	2.5	5.000E-05	此二阶最小割集不包含任何在大于单次飞行中是隐蔽失效的基本事件,因此 CS 25.1309(b)(5)不适用此最小割集
		A005	ACT 5	1.000E-06	2.5	2.500E-06	
6	6.500E-13	A003	ACT 3	6.500E-07	2.5	1.625E-06	同时符合隐蔽限制和剩余概率限制(A003 的每飞行小时的概率 6.5E-07/FH 小于 1.0E-5, L004 的概率 1.0E-06 小于 1.0E-03)
		L004	LAT 4	1.000E-07	10.0	1.000E-06	
7	3.991E-11	A002	ACT 2	2.000E-05	2.5	5.000E-05	此最小割集为 3 个失效的组合,因此 CS 25.1309(b)(5)不适用此最小割集
		L001	LAT 1	4.000E-06	1 000.0	3.992E-03	
		L002	LAT 2	5.000E-06	100.0	4.999E-04	

注:飞行时间 = 2.5 小时

P[LAT i] ≈ 失效率 * 暴露时间

2）表 1 识别了包含一个在大于单次飞行中是隐蔽失效的初级事件的二阶最小割集。

3）然后对二阶最小割集进行分组：

（a）包含相同的显性初级事件。对每个分组，将剩余隐蔽失效的概率相加。对每个分组，隐蔽初级事件概率之和应小于 1/1 000。

（b）包含相同的隐蔽初级事件。对每个分组，假设隐蔽初级事件已失效，将剩余显性初级事件的概率相加。对每个分组，初级事件概率之和应小于 1×10^{-5}/FH。

4）所有最小割集之和应在 1×10^{-9}/FH 量级上。

另一种执行步骤(3)(b)的方法是，假设一个不同的隐蔽初级事件已经发生，重新计算每个模型，重新计算故障树概率，然后验证顶事件的每飞行小时平均概率在 1×10^{-5}/FH 量级上或更小。运输类飞机通常有约 100 个灾难性失效状态，需对每个灾难性失效状态识别出包含隐蔽失效的二阶割集并进行上述分析。

3　工程应用分析

3.1 条款应用范围分析

此次隐蔽失效的条款要求仅适用于新的 TC 或 STC，已取证飞机不再适用。由于被 CS 25.1309(b)(1)(ii)所覆盖，CS 25.1309(b)(4)不适用于与运行和环境条件组合导致灾难性影响的单个失效。由于 CS 25.1309(b)(5)包含“每个”灾难性失效状态的描述，因此对于同一个隐蔽失效导致多个灾难性失效状态的情况，剩余概率限制的要求不适用。为了限制条款符合性所需的分析工作量，设置 1E-12/FH 的截断准则，即概率小于 1E-12/FH 的组合失效（一个显性失效与一个或多个隐蔽失效组合）不适用，且 CS 25.1309(b)(5)仅适用于二阶割集。

3.2 隐蔽失效的概率计算方法

型号设计中通常采用国内外商用可靠性软件进行故障树计算。这些软件将隐蔽失效的部件在两次检查间隔之间近似为不可修复系统。当 $\lambda t<0.1$ 时，失效概率 $P=\lambda t/2$，该方法仅考虑了隐蔽失效自身的平均失效率，没有考虑与显性失效的组合、失效顺序等因素。如图 2 所示，对于隐蔽失效与显性失效组合，在 $t<T$ 时，隐蔽失效概率远小于显性失效的概率；而在 $t=T$ 时，隐蔽失效概率远大于显性失效的概率。工程上通常采用保守的最大概率进行概率计算。

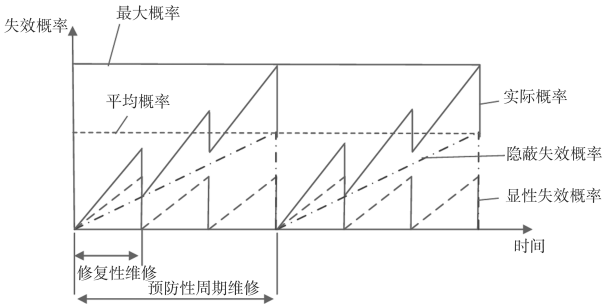

图 2　隐蔽失效与显性失效组合的失效概率

对于一个隐蔽失效与一个显性失效组合造成顶事件发生[6]，假设事件 1 存在隐蔽失效，维修间隔为 T_1，事件 2 处于风险的时间为 T_0，设 $T_1=nT_0$，则事件 1 的暴露时间为 T_1，则平均每次飞行的失效概率为：

$$P_f=\frac{1}{2}\lambda_1\lambda_2T_0(T_1+T_0) \tag{1}$$

此外，隐蔽失效的计算模型还与失效概率分布函数、失效概率简化的假设条件、风险时间/暴露时间、底事件失效率等因素相关。如何准确计算隐蔽失效与显性失效组合的平均概率，对系统安全性评估结果具有重大影响。因此，需对全机灾难性的和危险的失效相关的隐蔽失效进行统一管理，尤其应关注导致灾难性失效的二阶最小割集中隐蔽失效相关的失效率、失效率因子、暴露时间和检查间隔等因素。

从初始适航的角度，在 PSSA 分析过程中，可通过分配的安全性目标计算隐蔽失效最大风险暴露时间，所采用的检查间隔应小于该值。对于灾难性和危险的失效状态中的隐蔽失效，其检查间隔应被记录在 CCMR 和维修大纲中。

3.3 隐蔽失效限制暴露时间的计算方法

从持续运行安全的角度，应确定暴露时间以限制飞机的运行时间并纠正隐蔽失效[12-13]。当发生某个失效后，其风险越高，所需采取纠正措施的时间越短。当前，公众可接受的灾难性失效概率是 1×10^{-7}/飞行小时。假设 1/4 的飞机带故障运行，历史数据表明，单个飞机在生命周期中可能发生 10 次需要在灾难性失效状态下带故障运行。则每个灾难性失效的风险限制为：

$$R_l=10^{-7}\times\frac{1}{4}\times T_f\times\frac{1}{10} \tag{2}$$

式中 R_l是灾难性风险限制，T_f是设计生命周期，典型飞机的生命周期为 60 000 h（20 年，年利用率 3 000 h）。

计算失效的限制暴露时间 T_p即可用于制定纠正措施的时间：

$$T_p = \frac{R_l}{P} \tag{3}$$

式中 P 为灾难性失效的概率。图 3 描述了灾难性失效状态的概率和限制暴露时间的关系。当失效概率大于 2×10^{-6}时，飞机应停飞（除了转场至主基地之外）。当失效概率在 2×10^{-6}和 1×10^{-9}之间时，应在相应的限制暴露时间内采取纠正措施。

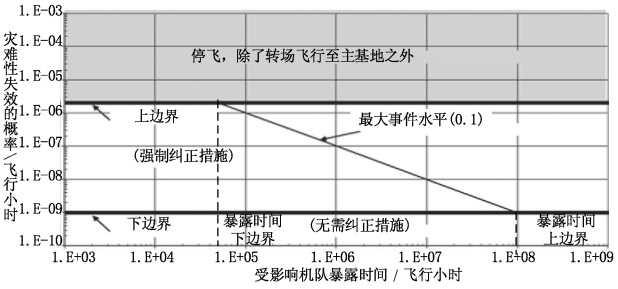

图 3　失效概率与暴露时间的关系

4　结论

为了协调不同适航当局、不同系统之间的隐蔽失效适航标准，CS 25.1309 新增了隐蔽失效的定性和定量要求。本文分析了 CS 25.1309（b）（4）和（b）（5）条款及其符合性方法，以典型 FTA 示例说明了隐蔽限制和剩余概率限制准则的工程应用方法，说明了条款的应用范围、隐蔽失效的概率和限制暴露时间的计算方法，可有效指导隐蔽失效的设计和符合性验证工作。

参考文献：

[1] European Aviation Safety Agency. AMC 25.1309 Amendment 24: System Design and Analysis[S]. Europe: EASA, 2020.

[2] Federal Aviation Administration. Specific Risk Tasking: ARAC ASAWG Report[R]. U.S.: FAA, 2010.

[3] European Aviation Safety Agency. Notice of Proposed Amendment 2014-02: Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems[S]. Europe: EASA, 2014.

[4] European Aviation Safety Agency. Comment Response Document (CRD to NPA 2014-02): Specific risk and standardised criteria for conducting aeroplane-level safety assessments of critical systems—Specifications for flight control systems and aeroelastic stability[S]. Europe: EASA, 2018.

[5] European Aviation Safety Agency. CS 25.1309 Amendment 24: System Design and Analysis[S]. Europe: EASA, 2020.

[6] 马赞，王鹏，赵长啸，等. 隐蔽故障计算模型审定要求分析[J]. 电光与控制，2019，26(7)：51-55.

[7] OZIRKOVSKYY L, VOLOCHIY B. Adequacy increase of assessment of minimal cut sets considering latent failures[J]. Central European Researchers Journal, 2019, 5(2): 58-66.

[8] 戴顺安，王烨，蔡景. 民用飞机隐蔽故障风险的定量评估方法研究[J]. 兵器装备工程学报，2016，37(6)：162-165.

[9] 贾宝惠，刘涛，杨杭，等. 民机隐蔽故障维修间隔优化方法研究[J]. 航空制造技术，2015(S1)：20-23；32.

[10] European Aviation Safety Agency. Notice of Proposed Amendment 2016-07: Regular update of CS-25[S]. Europe: EASA, 2016.

[11] European Aviation Safety Agency. CS-25 amendment 19: Explanatory Note to Decision 2017/015/R [S]. Europe: EASA, 2017.

[12] 郭博智，阮宏泽，刘会星. 飞机系统安全性——初始适航合格审定评估[M]，北京：航空工业出版社，2019：302-304.

[13] GUO Y Y, SUN Y C, LI L B. Residual Risk Assessment of Civil Aircraft for Airworthiness Requirements [C]// Proceedings of the 18th International Conference on MMESE, Singapore: Springer, 2019: 611-617.

作者简介

刘会星　男，博士，高级工程师。主要研究方向：飞机系统安全性。E-mail: liuhuixing888@163.com

Compliance verification analysis on latent failure airworthiness requirement

LIU Huixing *

(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: The compliance verification of latent failure has significant impact on the system safety level of aircraft. After a decade argument, EASA added new requirements of latent failure in CS/AMC 25.1309. For example, any significant latent failure is eliminated as far as possible. In order to prevent the aircraft from one failure away from catastrophe, for each catastrophic failure condition that results from two failures, either one of which is latent for more than one flight, the time of operating is required to be limited from the latency point, meanwhile the combined average probability of all the single active failures is required to be limited from the residual probability point, assuming one single latent failure has occurred. In view of new requirement of latent failure in CS 25.1309(b), its methods of compliance are analyzed. Two criteria limit latency and limit residual probability, are illustrated by minimal cut set of typical Fault Tree Analysis example. The application scope is analyzed from the engineering point of view, and the calculation methods of probability and exposure time limit of latent failure are illustrated, to promote system safety level of aircraft.

Keywords: latent failure; system safety; specific risk; minimal cut set

* Corresponding author. E-mail: liuhuixing888@163.com