中国民用航空局航空器适航

审定司

咨 询 通 告

编　　号：AC-21-AA-2021-XX

颁发日期：2021 年 XX 月 XX 日

民用无人驾驶航空器系统
安全性分析指南（征求意见稿）

目录

1. 目的 1

2. 适用范围 1

3. 相关文件 1

4. 参考文件 1

5. 缩略语 1

6. 定义 1

7. 民用无人驾驶航空器系统的运行风险类别 3

7.1. 严重性 3

7.2. 可能性 4

7.3. 运行风险类别 4

8. 民用无人驾驶航空器系统的安全性分析 6

8.1. 失效状态分类 6

8.2. 安全性目标 8

8.3. 失效状态评估 12

8.4. 失效概率计算 15

8.5. 系统安全性分析的工作要点 17

1. 目的

本指南为申请人和局方在民用无人驾驶航空器系统设计批准审定过程中，如何开展系统安全性分析提供指导，并就如何对民用无人驾驶航空器系统的运行风险进行分类以支持确定可接受的安全性水平予以说明。

2. 适用范围

本指南提供的系统安全性分析指导内容和民用无人驾驶航空器系统的运行风险分类方法，适用于按照国家有关规定纳入适航管理的民用无人驾驶航空器系统的设计批准审定。

3. 相关文件

《民用无人驾驶航空器系统适航审定管理程序》（AP-21-XX）

4. 参考文件

ARP 4761 民用机载系统和设备安全性评估过程的指南和方法

5. 缩略语

FHA 功能危害性评估

PSSA 初步系统安全性评估

FMEA 故障模式及影响分析

FTA 故障树分析

SSA 系统安全性评估

6. 定义

(一) 民用无人驾驶航空器系统：指民用无人驾驶航空器以及与其有关的控制站（台）、控制链路等组成的完整系统。

注：后文出现的子系统，是上述完整的民用无人驾驶航空器系统的组成部分，如机械系统、飞控系统、链路系统等。

(二) 风险：某种特定的危险事件发生的可能性与其产生的后果的组合。

(三) 不利影响：导致民用无人驾驶航空器系统或其子系统出现不良运行状态的系统响应。

(四) 不利的运行条件：民用无人驾驶航空器系统的环境或运行状况的组合，伴随着导致地面机组工作负荷显著增加的失效或其他紧急情况。

(五) 继续安全飞行与着陆：不需要超出常规的飞行技巧和力量的情况下，民用无人驾驶航空器系统能够持续受控飞行和着陆，可能会使用应急程序。着陆时，可能由于某个失效状态导致民用无人驾驶航空器的某些损伤。

(六) 失效：一种影响组件、部件或单元工作，使其不能完成预期功能的事件，包括功能的丧失和异常。

注：错误可能导致失效，但错误本身不被考虑为失效。

(七) 失效状态：考虑飞行阶段及相关的不利操作、环境条件或外部事件的情况下，由一个或多个失效或错误引起或促成，对民用无人驾驶航空器系统、机组操作、地面人员、空中其他航空器或上述组合产生直接或间接影响的状态。

(八) 功能危害性评估：是对民用无人驾驶航空器系统及其子系统的功能进行的一种系统、全面的检查，用于识别可能由功能失效或

异常导致的潜在的失效状态（灾难性的、危险的、重大的、轻微的、无安全影响的）。

(九) 定性分析：是用客观的、非量化的方式评估民用无人驾驶航空器系统及其子系统安全性的分析过程。

(十) 定量分析：是用量化的方法评估民用无人驾驶航空器系统及其子系统的安全性的分析过程。

(十一) 每飞行小时的平均概率：是一个数字表征，通过某个失效状态在一个型号的所有民用无人驾驶航空器系统整个运行寿命内预计可能发生的次数，除以该型号所有民用无人驾驶航空器系统预计的整个运行小时数得到。

7. 民用无人驾驶航空器系统的运行风险类别

民用无人驾驶航空器系统的运行场景不同，其可接受的安全性水平不同。划分民用无人驾驶航空器系统的运行风险类别，目的是区分其安全性水平的差异，进而为明确不同类别民用无人驾驶航空器系统的可接受的安全性水平提供支持。划分民用无人驾驶航空器系统的运行风险类别，主要从民用无人驾驶航空器系统运行过程中潜在的危害性影响出发，综合危害的严重性和可能性两个要素判断。

7.1. 危害的严重性

民用无人驾驶航空器系统潜在危害的严重性以其航空器的最大审定起飞重量作为基准，并结合最大限制速度计算出的动能，划分为如下四个级别：

Ⅰ级：5700 公斤（固定翼）或 3180 公斤（旋翼类）以上；

II级：750公斤～5700公斤（固定翼）或3180公斤（旋翼类）；150～750公斤且动能大于800千焦；

III级：150～750公斤且动能不大于800千焦；25～150公斤且动能大于100千焦；

IV级：25～150公斤，且动能不大于100千焦。

7.2. 可能性

民用无人驾驶航空器系统潜在危害的可能性与申请开展的运行种类相关，如载人飞行可能造成对机上乘员的危害，融合空域飞行可能造成对空中其他航空器的危害，还包括对地面人员等危害的可能性。

对地面人员等的危害，基于撞击地面人员等的可能，可分为人员稀疏区域和人员稠密区域上空飞行两种情况考虑。对空中其他航空器的危害，基于发生空中碰撞的可能，可分为融合飞行和隔离飞行两种情况考虑。

对机上乘员的危害，主要适用于载人的民用无人驾驶航空器系统，可以按机上所载乘员数量评估，分为1～2人、3～6人、7～9人、10～19人、19人以上五个级别。

7.3. 运行风险类别

综合造成危害的严重性和可能性，区分不载人飞行、载人飞行两种情况，分别划分民用无人驾驶航空器系统的运行风险类别。

对于不载人且不进入融合空域飞行的民用无人驾驶航空器系统，主要从不同级别民用无人驾驶航空器系统对地面人员等的影响出发，划分民用无人驾驶航空器系统的运行风险类别，如表1所示。其中，

对于II级民用无人驾驶航空器系统，进一步以2720公斤为界限划分运行风险类别。对于不载人但进入融合空域飞行的正常类、运输类民用无人驾驶航空器系统，运行风险类别应不低于E类。

表 1 不载人民用无人驾驶航空器系统隔离飞行的运行风险分类

严重性等级	隔离飞行	
	稀疏区	稠密区
I	C	A
II	D	B
	E	C
III	F	D
IV	G	E

对于载人飞行的情况，主要从对机上乘员的影响出发，划分民用无人驾驶航空器系统的运行风险类别，如表2所示。

表 2 载人民用无人驾驶航空器系统的运行风险分类

严重性等级	乘员数量				
	1~2人	3~6人	7~9人	10~19人	19人以上
I	A				
II	D	C	B	A	
III	D				
IV					

综上，评估民用无人驾驶航空器系统的运行风险，可以划分为A、B、C、D、E、F、G七类。民用无人驾驶航空器系统的运行风险类别不同，其可接受的安全性水平不同。局方根据民用无人驾驶航空器系统的运行风险类别，确定其可接受的安全性目标，以及适用的适航标准。

8. 民用无人驾驶航空器系统的安全性分析

本节在民用无人驾驶航空器系统的安全性分析工作基本完整的前提下，重点对相比有人驾驶航空器的系统安全性分析有所区别的内容进行介绍，并以最大审定起飞重量不超过 5700 公斤的限用类民用无人驾驶航空器系统为例说明，对系统安全性分析的一般方法不予重复。需要指出的是，控制站（台）作为民用无人驾驶航空器系统必不可少的一部分，同样应当纳入系统安全性分析的工作范围。

8.1. 失效状态分类

由于民用无人驾驶航空器系统具备无机上驾驶员直接操纵的特点，其失效状态影响与有人驾驶航空器存在较大差别。明确民用无人驾驶航空器系统的失效状态影响，是民用无人驾驶航空器系统安全性分析的首要问题。

民用无人驾驶航空器系统的失效状态影响，应考虑系统功能失效后，对空中其他航空器和（或）地面人员等的影响。由于民用无人驾驶航空器系统与有人驾驶航空器现阶段尚未融合飞行，本指南定义的失效状态影响主要针对隔离飞行的情况，即主要针对民用无人驾驶航空器系统的功能失效后对地面人员等的影响。相应的，失效状态影响的严重程度分类如下:

1. 灾难性的: 机组完全丧失对民用无人驾驶航空器系统的操纵能力，民用无人驾驶航空器系统完全丧失控制，在限制空域(含安全区）内或飞出限制空域（含安全区）坠毁，导致一人或多人死亡。

2. 危险的: 极大降低民用无人驾驶航空器系统的功能特性或机组应对不利操作情况的能力，如极大增加机组操作负担，影响机组操作的完整性及准确性；不会造成地面人员死亡，但会对人员安全产生危害，如重伤。

3. 重大的: 明显降低民用无人驾驶航空器系统的功能特性或安全裕度，或增加机组操作负担、影响机组操作效率。

4. 轻微的: 轻微降低民用无人驾驶航空器系统的功能特性或安全裕度，或增加机组操作负担，如改变飞行计划。

5. 无安全性影响: 不会对民用无人驾驶航空器系统安全飞行以及机组操作能力和工作负担产生影响。

由上可见，民用无人驾驶航空器系统是否可控是其能否造成危害的关键，分析失效状态影响的严重程度应以此为出发点，如下图所示。

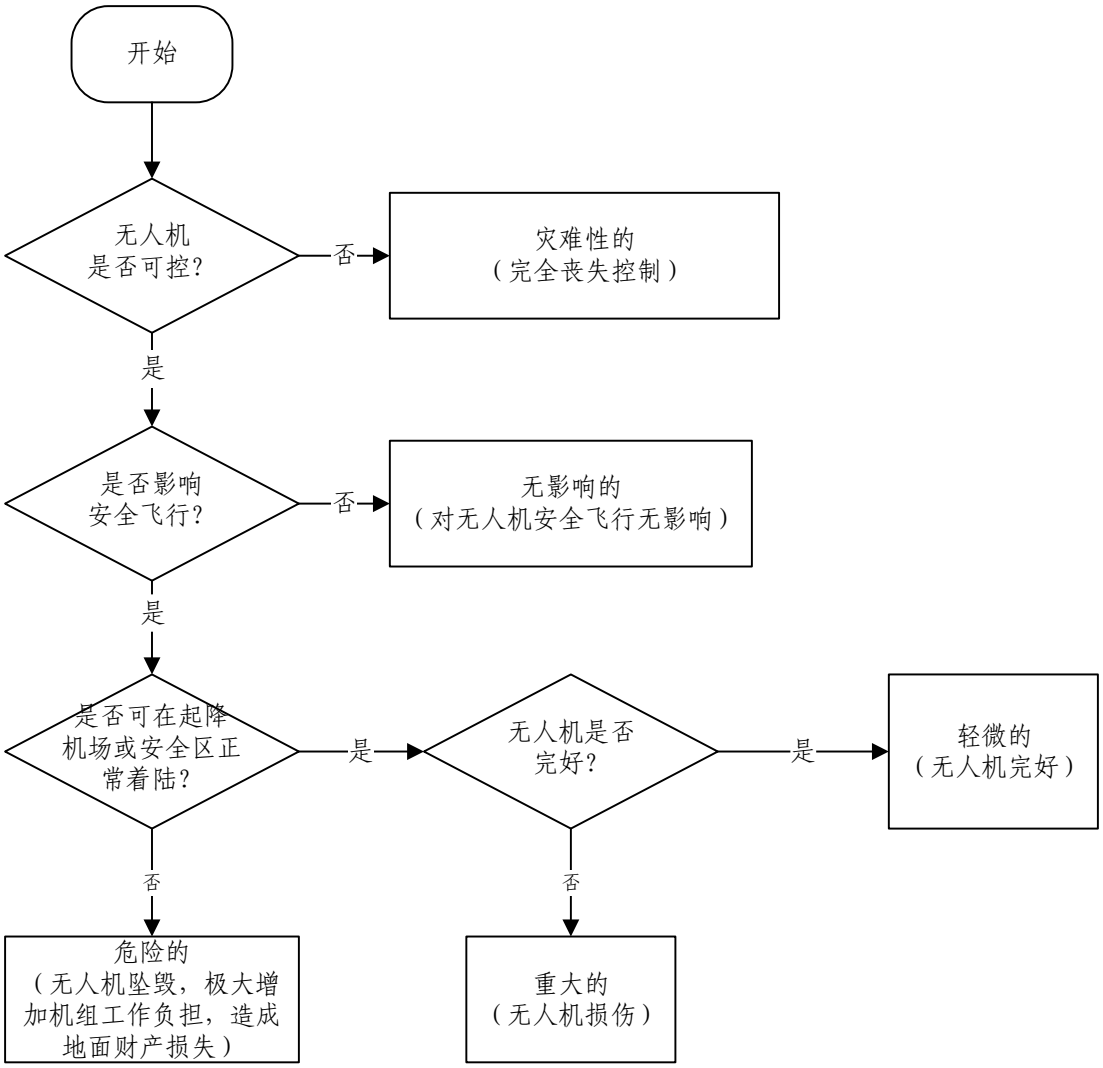

图 1 民用无人驾驶航空器系统失效状态的分类

8.2. 安全性目标

不同运行风险类别的民用无人驾驶航空器系统应当满足的安全性目标不同。对于正常类、运输类民用无人驾驶航空器系统，确定其安全性目标，应以未来能够和有人驾驶航空器融合飞行为出发点，保证其加入空域飞行后不降低总体的航空安全水平，即不增加对空域内其他航空器及地面人员、财产等的安全风险。因此，正常类、运输类民用无人驾驶航空器系统的安全性水平应当不低于同级别有人驾驶航空器的安全性水平。

对于限用类民用无人驾驶航空器系统，参考上述原则，同时针对其不用于载人飞行、不进入融合空域飞行且不在稠密区域上方飞行的特点，相应的危害主要是对稀疏区域的影响，确定适用的安全性目标。

特别地，对表 1 中最大审定起飞重量不超过 5700 公斤的 D 类限用类民用无人驾驶航空器系统，结合国内型号的研制情况、使用经验、飞行数据，获知因操作和设计原因造成失事的概率约为 1×10^{-4} 每飞行小时。同时考虑民用用途对安全性的需求，保守起见，对于新设计的民用无人驾驶航空器系统，要求其由于系统失效导致的失事不超过失事总数的 10%，则所有可能由系统导致失事的失效状态的发生概率不超过 1×10^{-5} 每飞行小时。考虑到限用类民用无人驾驶航空器系统复杂程度通常低于同类型有人驾驶航空器，假定限用类民用无人驾驶航空器系统有 10 个潜在的失效状态可以导致灾难性后果，则每个灾难性失效状态的发生概率不能超过 1×10^{-6} 每飞行小时，即对于 D 类限用类民用无人驾驶航空器系统，其灾难性失效状态应满足的发生概率上限为 1×10^{-6} 每飞行小时。表 1 中 E 类限用类民用无人驾驶航空器系统的灾难性失效状态的发生概率应满足的上限为 1×10^{-5} 每飞行小时。

失效状态的发生概率和影响严重程度之间应建立以下反比关系：

1. 无安全影响的失效状态没有发生概率要求；

2. 轻微的失效状态的发生概率是可能的；

3. 重大的失效状态的发生概率是微小的；

4. 危险的失效状态的发生概率是极小的，即对于每架民用无人驾驶航空器系统而言，这些失效状态在其整个寿命周期内预期不会发生，

但对于这个型号的全部民用无人驾驶航空器系统而言，在整个运行生命周期内可能会发生几次。

5. 灾难性的失效状态的发生概率是极不可能的，即这类失效状态在一个型号所有民用无人驾驶航空器系统的整个运行寿命期内预期不会发生。

下表 3 给出了失效状态分类及其描述，以及对应的概率要求。

表 3 最大审定起飞重量不超过 5700 公斤的 D 类限用类民用无人驾驶航空器系统的失效状态分类及概率要求

	灾难性的	危险的	重大的	轻微的	无影响的
对民用无人驾驶航空器系统的影响	完全丧失控制，在限制空域(含安全区）内或飞出限制空域（含安全区）坠毁。	极大降低民用无人驾驶航空器系统的功能特性及安全裕度。例如，民用无人驾驶航空器系统飞行轨迹可控，中止执行迫降，进而导致无人机坠毁。	显著降低民用无人驾驶航空器系统的功能特性及安全裕度。例如，民用无人驾驶航空器系统终止继续飞行，在机场或安全区应急着陆，可能导致无人机损伤。	民用无人驾驶航空器系统的功能特性或安全裕度轻微降低。例如，民用无人驾驶航空器系统继续飞行的安全裕度降低，但仍可飞行至着陆机场或安全区执行正常着陆程序，民用无人驾驶航空器系统完好。	对民用无人驾驶航空器系统安全飞行无影响。
对机组的影响	机组完全丧失对民用无人驾驶航空器系统的操纵能力。	极大增加机组工作负担，可能影响机组执行任务的完整性和准确性。	明显增加机组工作负担。	轻微增加机组工作负担。	无影响
对地面人员影响	可能导致地面一人或多人死亡。	对人员的健康、安全造成极大威胁，可能导致人员重伤。	可能导致人员受伤。	无影响	无影响
允许的定性概率	极不可能的	极小的	微小的	可能的	无概率要求
允许的定量概率（每飞行小时平均失效概率）	$<10^{-6}$	$<10^{-5}$	$<10^{-4}$	$<10^{-3}$	无概率要求

8.3. 失效状态评估

不同等级分类的失效状态评估方法不同:

（一）无安全影响的失效状态。常见的设计习惯是对安全运行所必须的部件进行物理隔离和功能隔离。如果申请人选择不进行功能危害性评估（FHA），则安全影响可以通过申请人完成的设计和安装评估获得。

（二）轻微的失效状态。需要分析系统失效对其他系统或功能的影响。对于此类失效状态的安全评估来说，必须建立与其他系统相独立的、带有设计和安装评估的 FHA。常见的设计习惯是对安全运行所须的部件进行物理隔离和功能隔离。如果申请人选择不进行 FHA，则安全影响可以通过申请人完成的设计和安装评估获得。

（三）重大的失效状态。可通过下面几种方法进行定性的工程评估:

1. 相似性分析。允许通过比较类似已审定的系统需求表明需求的符合性。相似性论断的充分性随着系统使用经验的时间增加。如果某个系统与用于其它无人机型号的系统的相关属性类似，同时其功能和失效影响相同的话，则可以接受以当前设备或相似设计设备的设计和安装评估以及令人满意的使用记录表明符合性。提供可接受的、已批准的数据和与之前安装的相似性的任何声明是申请人的责任。

2. 对于不能通过相似性表明符合性的非复杂系统，可以通过定性的评估来表明安装该系统后，系统的重大失效状态与 FHA 一致（如冗余系统）。

3. 对于高度复杂的无冗余系统(如一个带有自监视功能的微处理器)，要表明其故障发生的概率是微小的，有时需要进行由失效概率数据和失效检测分析支持的定性的功能故障模式及影响分析（FMEA）或故障树分析（FTA）。

4. 对于冗余系统的分析要表明冗余系统通道之间的隔离性，且每个通道都有令人满意的可靠性。对于需要功能冗余的复杂系统，可能需要定性的 FMEA 和 FTA 来确定冗余是真实存在的（例如不存在影响全部功能通道的单点故障）。

（四）危险的及灾难性的失效状态。对于 FHA 中识别的每个危险的及灾难性的失效状态都必须完成完整的、详细的安全性分析。这种分析通常包括定性的和定量的设计评估，及其适当组合。

1. 对于简单和传统的安装（即低复杂度且相关属性类似），可在丰富工程经验判断的基础上，通过定性分析的方法来评估极小的或极其不可能的危险的和灾难性的失效状态。这是建立在冗余度、通道间的独立性和隔离性以及相关技术的可靠性记录的基础上的。在系统设计和运行环境极其相似的情况下，用于多数无人机型号的类似系统的令人满意的服务经验也是可以接受的。

2. 对于复杂系统，如果可以严格确定包括安装属性在内各种相关属性的相似性，也可以使用根据工程经验判断的定性分析来表明一个危险的和灾难性的失效，其发生的概率是极小的和极其不可能的。这种情况下，设计和应用的相似度都要非常的高。

3. 系统的单个组件、部件或元件的失效不应导致灾难性失效状态。应通过丰富的工程经验判断和使用记录，表明单点故障引发灾难性失效状态在实际中是不可能的。评估过程中使用的逻辑和推理应能够直观明显的表明，除非其与一个不相关的、本身就是灾难性的失效状态联系起来，否则失效模式根本不会发生。

不同等级失效状态评估方法见下图 2。

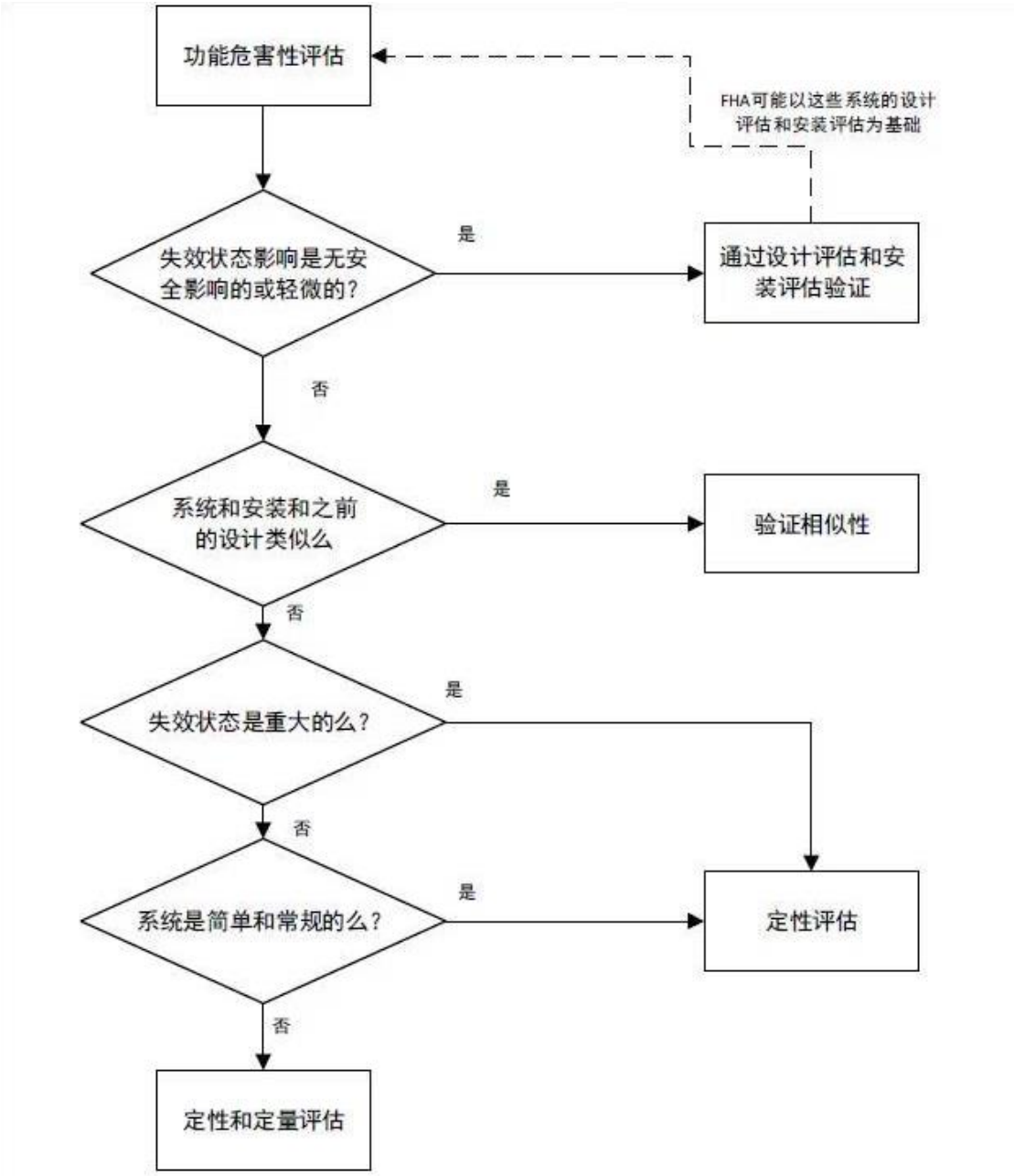

图 2 失效状态评估深度

8.4. 失效概率计算

申请人应尽早与审查组就失效状态分类，以及每一个重大的、危险的、灾难性的失效状态的失效概率达成一致。失效概率是指在一次飞行中，正常的飞行时间内一个失效状态发生的概率，即“每飞行小时平均概率”。

失效状态的概率评估可以是定性的，也可以是定量的；可以是一份用来解释试验结果或比较两个相似系统的简单报告，也可以是包括估计的概率数值或不包括估计的概率数值的详细分析。分析的深度和广度依赖于系统所要完成的功能、失效状态的严重程度以及系统是否复杂。定量分析往往作为基于工程和运行经验判断的定性分析方法的补充，而非替代。对于一个复杂的、缺少充分的使用经验表明安全性或带有与传统系统有显著差异属性的系统，该系统有可能导致灾难性的或危险的失效状态时，通常需要进行定量分析。

失效概率可以通过故障率和暴露时间确定。故障率数据来自相同或相似项目的服役经验、制造商的加速试验，或可接受的工业标准。 暴露时间与民用无人驾驶航空器系统的飞行时间相关。

进行失效概率计算时应考虑以下方面:

1. 平均飞行持续时间和平均飞行剖面需要审定;

2. 导致失效状态的全部的失效和事件的组合;

3. 如果一个失效状态是由一系列事件导致的，则要考虑条件概率;

4. 如果一个事件与某一飞行阶段相关联，则需要考虑相关的“风险”时间;

5. 如果失效持续发生在多次飞行中，则需要考虑平均暴露时间。

计算每个失效概率时，应为不确定因素留出适当余量。如使用已经证明的数据或来自服役经验和试验的数据进行分析，通常情况下不需要余量。但当相关数据有限的情况下，需要根据有效的判断保留余量。

8.5. 系统安全性分析的工作要点

(一) 功能危害性评估（FHA）

FHA 是系统安全性分析的重点，需经审查组批准。申请人要全面识别对民用无人驾驶航空器系统及其子系统的功能，据此考虑各种功能失效以及子系统间组合失效对民用无人驾驶航空器系统造成的影响，并评估影响等级。FHA 应随系统设计不断迭代更新。申请人开展 FHA 工作应重点关注以下内容:

1. 民用无人驾驶航空器系统及其子系统的功能清单;

2. 功能失效影响的描述及影响等级划分;

3. 安全性的定性/定量要求;

4. 失效状态分析。失效状态分析应全面，从功能全部/部分丧失、对称/不对称丧失、有通告/无通告/误通告、非指令性、失效组合等方面综合考虑。

5. 影响等级确定。确定影响等级应从功能失效对民用无人驾驶航空器系统、地面机组操作负担、地面其他人员等的影响考虑。对于特殊情况如森林防火、危险物品运载等，需考虑坠毁后造成的环境影响。

(二) 初步系统安全性评估（PSSA）

对于新研民用无人驾驶航空器系统，PSSA 也是审查组关注的工作项目。PSSA 用来证明系统如何满足 FHA 中确定的定性或定量的安全性要求，并确定衍生的安全性需求。PSSA 是随着系统设计需要反复迭代分析的一项工作。申请人开展 PSSA 工作需注意:

1. 故障树架构;

2. 外部事件发生概率;

3. 对系统、设备的提出的安装要求、安全性要求、机组操作要求、故障检测要求等。

(三) 故障模式影响分析（FMEA）

申请人要确保对民用无人驾驶航空器系统的所有航线可更换单元级组件均开展了 FMEA，并且要分析到所有的故障模式，同时确保每个故障模式的故障率真实有效，才能保证自下而上的系统安全性评估全面可靠。

(四) 系统安全性评估（SSA）

SSA 是对已实施的系统进行系统性、综合性评估的方法，用来证实已满足相关的安全性要求。SSA 与 PSSA 相似，不同点在于 PSSA 是提出安全性要求的方法，SSA 是确认要求已被满足的证明。SSA 是审查组重点关注的工作项目，申请人的 SSA 工作应当注意并确保:

1. 提出的安全性要求的验证过程及结果;

2. 故障树底事件故障率的来源及真实性。