



U.S. Department
of Transportation
**Federal Aviation
Administration**

Advisory Circular

Subject: Guidance Material for 14 CFR § 33.75,
Safety Analysis.

Date:

Initiated By: ANE-110

AC No: 33.75-1

[DRAFT]

Change:

1. **PURPOSE.** This advisory circular (AC) describes guidance and acceptable methods, but not the only methods, for demonstrating compliance with the safety analysis requirements of Title 14 of the Code of Federal Regulations (14 CFR) § 33.75. The information provided in this AC replaces the guidance in Paragraph 52 (Section 33.75, Safety Analysis) of AC 33-2B, Aircraft Engine Type Certification Handbook.

2. **APPLICABILITY.**

a. The guidance provided in this document is directed to engine manufacturers, modifiers, foreign regulatory authorities, and Federal Aviation Administration (FAA) engine type certification engineers and their designees.

b. This material is neither mandatory nor regulatory in nature and does not constitute a regulation. It describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations. The FAA will consider other methods of demonstrating compliance that an applicant may elect to present. Terms such as “should,” “shall,” “may,” and “must” are used only in the sense of ensuring applicability of this particular method of compliance when the acceptable method of compliance in this document is used. While these guidelines are not mandatory, they are derived from extensive FAA and industry experience in determining compliance with the relevant regulations. On the other hand, if the FAA becomes aware of circumstances that convince us that following this AC would not result in compliance with the applicable regulations, we will not be bound by the terms of this AC, and we may require additional substantiation as the basis for finding compliance.

c. This material does not change, create any additional, authorize changes in, or permit deviations from existing regulatory requirements.

DRAFT FOR PUBLIC COMMENTS

3. RELATED READING MATERIAL.

a. FAA Documents.

- (1) AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes, dated March 12, 1999.
- (2) AC 25.1309-1A, System Design Analysis, dated June 21, 1988.
- (3) AC 27-1B, Certification of Normal Category Rotorcraft, dated February 12, 2003.
- (4) AC 29-2C, Certification of Transport Category Rotorcraft, dated February 12, 2003.
- (5) Significant Airworthiness Information Bulletin (SAIB) NE-00-12 on multi-engine maintenance issued February 1, 2000.

b. Joint Aviation Authorities Documents.

- (1) JAR-E 510 Safety Analysis (EASA CS-E 510)
- (2) ACJ-E 510, Safety Analysis, dated May 1, 2003 (EASA AMC CS-E 510)

c. Industry Documents.

- (1) Society of Automotive Engineers (SAE), Document No. ARP 926B, Fault/Failure Analysis Procedure, issued June 1997.
- (2) SAE Document No. ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, issued November 1996.
- (3) SAE Document No. ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, issued December 1996.
- (4) Carter, A.D.S., Mechanical Reliability (2nd ed.). Macmillan, 1986.
- (5) Systematic Safety Assessment (CAA Leaflet AD/IL/0092/1-7) draft 4, issue 2; July 9, 1970, paper #484.

4. DEFINITIONS. For the purposes of this AC, the following definitions apply:

a. Analysis. Analysis refers to a specific and detailed qualitative or quantitative evaluation of the engine relative to the requirements of § 33.75. Examples include: Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA) and Markov Analysis.

b. Assessment. Assessment refers to a more general or broad evaluation of the engine that may include the results of the analysis completed, as well as any other information, to support compliance with § 33.75.

c. Check. Check refers to an examination, inspection or test to determine the physical integrity or the functional capability of an item.

d. Effect. An effect is the outcome or result of an event, failure or malfunction. There are four effects specified within § 33.75: fire, burst, excess mount loads, and inability to shutdown.

1. Hazardous Engine Effect. The most severe engine effects are termed hazardous engine effects (see paragraph 8.b. of this AC).

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

2. Major Engine Effect. Effects that are less severe than hazardous engine effects, but are still serious, are termed major engine effects (see paragraph 8.b. of this AC).

e. Error. An error is an omission or incorrect action by a crew member or person in charge of the maintenance or a mistake in requirements, design, or implementation. An error may result in a failure but is not considered a failure in and of itself.

f. External Event. An external event is an occurrence that originates apart from the engine or aircraft (for example, icing or bird strikes).

g. Failure Condition. A failure condition is a condition with a direct, consequential engine-level effect, caused or contributed to by one or more failures. Examples include limitation of thrust to idle or oil exhaustion.

h. Failure Mode. Failure mode refers to the cause of the failure or the manner in which an item or function can fail. Examples include failures due to corrosion or fatigue or failure in jammed open position.

i. Redundancy. Redundancy refers to multiple independent methods incorporated to accomplish a given function, each one of which is sufficient to accomplish the function.

j. System. System refers to a combination of inter-related items arranged to perform a specific function(s).

5. BACKGROUND.

a. This AC offers guidance on acceptable methods to show compliance with § 33.75 by offering guidance on the terms analysis, probable, single failure, and multiple failure, and sub paragraphs (a) through (d) of the regulation. This guidance is being updated to reflect current FAA and industry practices concerning safety analyses. Much of this AC reflects the work accomplished by the Aviation Rulemaking Advisory Council (ARAC), which recently completed an effort to harmonize the Safety/Failure Analysis requirements of 14 CFR part 33 (§ 33.75) and Joint Aviation Requirements (JAR) Engine (Section E-510). That effort resulted in a common rule and advisory material that will be processed by FAA in the future when rulemaking resources are available. Until then, this guidance, which draws on the extensive work accomplished by ARAC, provides a source for updated information.

6. § 33.75 TEXT. The regulation in § 33.75 reads as follows: “It must be shown by analysis that any probable malfunction or any probable single or multiple failure, or any probable improper operation of the engine will not cause the engine to:

- (a) Catch fire;
- (b) Burst (release hazardous fragments through the engine case);
- (c) Generate loads greater than those ultimate loads specified in § 33.23(a); or
- (d) Lose the capability of being shut down.

7. GUIDANCE FOR ‘ANALYSIS’.

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

a. Compliance with § 33.75 may be shown by a safety analysis substantiated, when necessary, by appropriate testing, comparable service experience, or both. A substantiated safety analysis could consist of a simple report that offers descriptive details associated with a failure condition, an interpretation of test results, a comparison of two similar components or assemblies, other qualitative information, or a detailed safety analysis. Guidance for the acceptable depth and scope of the analysis is given in paragraph 7.c..

b. The analysis should consider the range of expected operations. Certain failure conditions only exist in certain aspects of operation or in certain missions; an analysis of the probability of their occurrence should consider the probability of that aspect or mission, combined with the subsequent probability of failure.

c. The depth and scope of an acceptable safety analysis depend on the following:

(1) The complexity and criticality of the functions performed by the system(s), components, or assemblies under consideration;

(2) The severity of related failure conditions;

(3) The uniqueness of the design and extent of relevant service experience;

(4) The number and complexity of the identified failures; and

(5) The detectability of contributing failures.

d. Prediction of the likely progression of some engine failures may rely extensively upon engineering judgment and is not susceptible to absolute proof. If some question of the validity of such engineering judgment exists, to the extent that the conclusions of the analysis could be invalid, additional substantiation may be required. Additional substantiation may consist of reference to previous relevant service experience, engineering analysis, material, component, rig or engine test, or a combination of these. If significant doubt over the validity of the substantiation exists, additional testing or other validation may be required.

e. If the assumptions or provisions of the safety analysis rely on specific instrumentation not required elsewhere, the analysis should state that information.

f. If the safety analysis depends on maintenance actions being carried out at specific intervals, such an assumption should be identified in the analysis and appropriately substantiated by reference to the appropriate manuals or other documentation.

g. If applicable to the effects described in the regulation, the safety analysis should also include, but not be limited to, investigation of the following:

(1) Indicating equipment;

(2) Manual and automatic controls;

(3) Compressor bleed systems;

(4) Refrigerant injection systems;

(5) Gas temperature control systems;

(6) Engine speed, power, or thrust governors and fuel control systems;

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

- (7) Engine overspeed, overtemperature, or topping limiters;
- (8) Propeller control systems; and
- (9) Engine or propeller thrust reversal systems.

8. GUIDANCE FOR ‘PROBABLE’.

a. The ultimate objective of a safety analysis is to ensure that the risk to the aircraft from all engine failure conditions is acceptably low. The basis is the concept that an acceptable total engine design risk is achievable by managing the individual engine risks to acceptable levels. This concept emphasizes reducing the likelihood or probability of an event proportionally with the severity of its effects.

b. The regulation states that the specified effects be not ‘probable’; that is, be unlikely to occur. The FAA has established that the associated numerical probability for ‘unlikely to occur’ should consider the severity of the effect under consideration. The most severe engine effects (termed ‘hazardous engine effects’ as defined within this AC) should be extremely remote (10^{-7} per engine flight hour, or less) and less severe, but still serious, engine effects (‘major engine effects’) should be remote (10^{-5} per engine flight hour, or less). To apply this guidance, the effects specified within § 33.75 should generally be regarded as hazardous engine effects. This AC provides guidance in the paragraphs below as to the hazardous and major engine aspects of each of the four specific effects specified within § 33.75.

c. The occurrence rate applies to each of the four specific effects individually. That is, the summation of the probabilities of individual failure modes or combinations of failures that could result in hazardous engine effects should be 10^{-7} or less per engine flight hour for each of the four specific effects. For example, the total rate of occurrence of uncontrolled fires, obtained by adding up the individual failure modes and combination of failures leading to an uncontrolled fire, should not exceed 10^{-7} per engine flight hour. The primary failure of critical components such as disks, hubs, and spacers need not be included in the summation for each of the four specific effects.

d. If each individual failure mode or combination of failures can be demonstrated to be less than 10^{-8} per engine flight hour, summation for the hazardous engine effect is not necessary. In other words, compliance may be shown by demonstrating that either:

1. each individual way of causing the particular hazardous engine effect is less than 10^{-8} per engine flight hour, or
2. all ways combined of causing the individual hazardous engine effect sum to less than 10^{-7} per engine flight hour.

e. In dealing with probabilities of this low order of magnitude, absolute proof is not possible, and compliance may be shown by reliance on engineering judgment and previous experience combined with sound design and test philosophies.

f. For those effects that may also result in a major engine effect, the individual failure modes or combinations of failures resulting in major engine effects should have probabilities not greater

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

than 10^{-5} per engine flight hour. No summation of the individual failure modes or combinations of failure modes is necessary for the major engine effects.

g. The possible latency period of failures should be included in the assessment of failure probabilities.

h. Section 33.75 defines engine-level effects, and this guidance applies to engine severity levels. The severity classifications of aircraft-level failure effects do not apply directly to engine safety assessments because the aircraft may have features that could reduce or increase the consequences of an engine failure condition. Additionally, the same type-certificated engine may be used in a variety of installations, each with its own aircraft-level severity classification of the same failure effect.

i. Aircraft-level requirements for individual failure conditions may be more severe than the engine-level requirements. Therefore, the engine manufacturer and the aircraft manufacturer should coordinate with each other, as well as with the relevant FAA certification offices, to ensure that the engine may be installed in the aircraft. The FAA strives to ensure that the engine applicant is aware of the possibility of more restrictive regulations in the installed condition.

j. Assumptions of typical aircraft devices and procedures, such as fire-extinguishing equipment, annunciation devices, etc., may be included in the analysis. These assumptions should be clearly stated in the analysis and included in the installation instructions under § 33.5(a) or (b), as appropriate. Regulations within the aircraft parts of 14 CFR (parts 23, 25, 27, and 29) contain aircraft-level device requirements. These regulations include xx.1305, Powerplant instruments.

9. GUIDANCE FOR ‘SINGLE FAILURE’.

a. There is inherent difficulty in demonstrating very low failure probabilities for the primary failure of single components or parts – for example, the primary structural failure of a disk. This failure condition, which likely results directly in uncontained hazardous fragments, should be extremely remote. However, the specific numerical probability cannot be reasonably estimated or demonstrated. If the primary failure of critical single components or parts (disks, hubs, impellers, large rotating seals, and other similar large rotating components) is likely to result in effects described within § 33.75, the applicant should rely on meeting the prescribed integrity requirements, such as those in §§ 33.14, 33.15 and 33.27. These requirements are considered to support a design goal, among others, that primary low-cycle fatigue (LCF) failure of the component should be extremely remote (10^{-7} per engine hour, or less) throughout its operational life.

10. GUIDANCE FOR ‘MULTIPLE FAILURE’.

a. ‘Multiple failure’ refers to several components failing or malfunctioning independently or in a cascading fashion. The safety analysis should address multiple failure considerations.

b. If the safety analysis relies on a safety system to prevent a failure from progressing to the effects defined within § 33.75, the possibility of a safety system failure in combination with a basic engine failure should be included in the analysis. Such a safety system may include safety

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

devices, instrumentation, early warning devices, maintenance checks, and other similar equipment or procedures. If items of a safety system are outside the control of the engine manufacturer, the assumptions of the safety analysis with respect to the reliability of these parts should be clearly stated in the analysis.

c. The safety system failure may be present as a latent failure or may occur simultaneously with, or subsequent to, basic engine failure.

11. GUIDANCE FOR ‘CATCH FIRE’.

a. Engine fire has both hazardous engine effect and major engine effect aspects. Extensive or persistent fires that are not effectively confined to a designated fire zone or that cannot be extinguished by using any aircraft means that may be identified in the assumptions of the safety analysis represent a hazardous engine effect.

b. Fires that are contained within the fire zone and are readily extinguished by using aircraft means represent a major engine effect.

c. Provision for flammable fluid drainage, fire containment, fire detection, and fire extinguishing may be taken into account when assessing the severity of the effects of a fire.

12. GUIDANCE FOR ‘BURST (RELEASE HAZARDOUS FRAGMENTS...)’.

a. Uncontained fragments cover a large spectrum of energy levels due to the various sizes and velocities of parts released by the engine. The engine has a containment structure that is designed to contain the release of a single blade and its consequences; it is also often adequate to contain additional released blades and static parts. The engine containment structure is not expected to contain major rotating parts if they fracture. Disks, hubs, impellers, large rotating seals, and other similar large rotating components should therefore always be considered to represent high-energy fragments. The failure of these items should be considered a hazardous engine effect.

b. Uncontained blades from a multiple blade release are typically considered low-energy fragments because their energy has been significantly reduced in defeating the containment structure. These events may typically be considered as major engine effects. However, the release of significant numbers of blades (for example, corn-cobbed rotors) will likely include fragments exiting with high energy, and would therefore be a hazardous engine effect.

c. Fan blades may have significant residual energy after defeating the containment structure, depending on the specifics of engine size, bypass ratio, and other design elements. The applicant should carefully consider whether fan blade uncontainment would result in high-energy fragments (and thus be a hazardous engine effect).

d. The engine casings generally serve as the engine containment structure, as well as pressure vessels. Thus, the rupture of engine casing due to pressure loads is inherently not contained. Service experience has shown that the rupture of the highest-pressure casings (compressor delivery pressure) can generate high-energy fragments; it should therefore be treated as a hazardous engine effect.

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

13. GUIDANCE FOR ‘GENERATE LOADS GREATER THAN...ULTIMATE’. The generation of loads greater than the ultimate loads specified in § 33.23(a) could result in the failure of the engine mount system leading to engine separation. The concern is the potential for the separated engine to then impact the aircraft and destroy critical systems or structure in flight. Service experience has shown that this may occur during separations at high engine thrust levels. This condition should be treated as a hazardous engine effect.

14. GUIDANCE FOR ‘LOSE THE CAPABILITY OF BEING SHUT DOWN’.

a. Inability to shut down the engine is included within § 33.75 due to the potential circumstances in which continued running of the engine, even at low thrust or power, represents a hazard. These circumstances include the inhibition of safe evacuation of passengers and crew, directional control problems during landing due to the inability to eliminate thrust or power, and the inability to ensure safe shut down when required following a failure.

b. Allowing for aircraft-supplied equipment (fuel cutoff means, etc.) to protect against the inability to shut down the engine is acceptable. A time delay of several minutes, but not more than 5 minutes, is acceptable between initiation of the shutdown and termination of the combustion cycle. Note that certain aircraft installations, especially rotorcraft, may require quicker shutdown to allow for safe evacuation.

c. The inclusion of “complete inability to shut the engine down” within § 33.75 does not preclude hardware or software intended to protect against inadvertent engine shutdown, including aircraft logic to mitigate against the inadvertent shutdown of all engines.

15. GUIDANCE FOR ‘IMPROPER OPERATION’.

a. Errors in operation of the engine have resulted in hazardous or catastrophic effects at the aircraft level that otherwise would have been less serious. The safety analysis should therefore address reasonably-expected instances of improper engine operation. The applicant should consider mitigating the effects of improper operation or providing operating instructions that reduce the likelihood of improper operation. In particular, abnormal engine symptoms and the desired response or appropriate procedures for trouble-shooting for these symptoms should be communicated to the installer (reference § 33.5).

16. LESSONS LEARNED.

a. Maintenance. Maintenance errors have contributed to hazardous or catastrophic effects at the aircraft level. Many of these events have arisen due to similar maintenance actions being performed on multiple engines during the same maintenance availability by one maintenance crew and are therefore primarily an aircraft-level concern. If appropriate, the applicant should consider communicating strategies against performing maintenance of multiple engines installed on the same aircraft as part of the same maintenance action (see, for example, SAIB NE-00-12 on multi-engine maintenance, Extended Range Operation with Two-Engine Airplanes (ETOPS) requirements). The applicant should also consider mitigating the effects of maintenance errors in the design phase. Components undergoing frequent maintenance should be designed to facilitate

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

the maintenance and correct re-assembly of the component. However, completely eliminating sources of maintenance error during design is not possible.

b. The following list of multiple engine maintenance errors was constructed from situations that have repeatedly occurred in service and have caused one or more serious events:

(1) Failure to restore oil system or borescope access integrity after routine maintenance (oil chip detector or filter check). Similar consideration should be given to other systems.

(2) Incorrect installation of O-rings.

(3) Servicing with incorrect fluids.

c. Improper maintenance on parts such as disks, hubs, and spacers has led to failures resulting in hazardous effects. Examples of this type of improper maintenance that have occurred in service are overlooking existing cracks or damage during inspection and failure to apply or incorrect application of protective coatings (for example, anti-gallant or anti-corrosive).

d. Mount system failure. Though the regulation addresses only engine mount system failure due to high loads likely associated with severe engine damage, other instances of mount separation have resulted from mount system failure due to fatigue originating from handling damage, or from corrosion or inadequate strength associated with manufacturing or maintenance error.

17. ANALYTICAL TECHNIQUES.

a. The depth and scope of an acceptable safety analysis depends on the complexity and criticality of the functions performed by the system(s), components, or assemblies under consideration, the severity of related failure conditions, the uniqueness of the design and extent of relevant service experience, the number and complexity of the identified causal failure scenarios, and the detectability of contributing failures.

b. There are various techniques for performing a safety analysis; the ones listed below represent two of the most commonly used methods. An applicant may propose other comparable techniques, and variations or combinations of these techniques are also acceptable. For derivative engines, limiting the scope of the analysis to modified components or operating conditions and their effects on the rest of the engine is acceptable. The applicant and the engine certification office should agree early in the certification program on the scope and methods of assessment to be used.

c. Various methods for assessing the causes, severity levels, and likelihood of potential failure conditions are available to support experienced engineering judgment. The various types of analyses are based on either inductive or deductive approaches. Brief descriptions of typical methods are provided below; more detailed descriptions of analytical techniques may be found in the documents referenced in paragraph 3 of this AC.

(1) Failure Modes and Effects Analysis (FMEA). An FMEA is a structured, inductive, bottom-up analysis that is used to evaluate the effects on the engine system of each possible element or component failure. When properly formatted, an FMEA will aid in identifying latent failures and the possible causes of each failure mode.

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.

DRAFT FOR PUBLIC COMMENTS

(2) Fault Tree or Dependence Diagram (Reliability Block Diagram) Analyses. These analyses are structured, deductive, top-down analyses that are used to identify the conditions, failures, and events that cause each defined failure condition. These analyses are graphical methods of identifying the logical relationship between each particular failure condition and the primary element or component failures, other events, or their combinations that can cause the failure condition. A Fault Tree Analysis is failure-oriented and is conducted from the perspective of which failures must occur to cause a defined failure condition. A Dependence Diagram Analysis is success-oriented and is conducted from the perspective of which failures must not occur to preclude a defined failure condition.

DRAFT--This document does not represent final agency action on this matter and should not be viewed as a guarantee that any final action will follow in this or any other form.