2. If the engine ice protection system does not require a flight crew action to operate it (i.e. the system is automatic, or it functions permanently), unless all of the following conditions are met:

— The engine thrust/torque and aeroplane performance are not significantly affected by the engine ice protection system switching on/off;

— There is no significant effect of the engine ice protection system switching on/off on the flight deck instruments, controls (such as the throttle lever) and the flight deck environment (such as noise);

— The engine ice protection system failures are indicated to the flight crew; and

— The indication of the functioning of the engine ice protection system is not used to indicate to the flight crew that the aircraft is operating in an icing environment, requiring, for example, the flight crew to apply an AFM procedure to protect the engine against the effects of the icing environment.

[Amdt 25/21]

AMC 25.1305(d)(1) Powerplant instruments

ED Decision 2003/2/RM

The following are examples of parameters, which are considered to be directly related to thrust; fan RPM(N_1), integrated engine pressure ratio (IEPR) and engine pressure ratio (EPR), depending on engine type.

CS 25.1307 Miscellaneous equipment

ED Decision 2003/2/RM

The following is required miscellaneous equipment:

(a) Reserved

(b) Two or more independent sources of electrical energy.

(c) Electrical protective devices, as prescribed in this CS-25.

(d) Two systems for two-way radio communications, with controls for each accessible from each pilot station, designed and installed so that failure of one system will not preclude operation of the other system. The use of a common antenna system is acceptable if adequate reliability is shown.

(e) Two systems for radio navigation, with controls for each accessible from each pilot station, designed and installed so that failure of one system will not preclude operation of the other system. The use of a common antenna system is acceptable if adequate reliability is shown.

CS 25.1309 Equipment, systems and installations

ED Decision 2020/001/R

(See AMC 25.1309)

The requirements of this paragraph, except as identified below, are applicable, in addition to specific design requirements of CS-25, to any equipment or system as installed in the aeroplane. Although this paragraph does not apply to the performance and flight characteristic requirements of Subpart B and the structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is dependent. Jams of flight control surfaces or pilot controls covered by CS 25.671(c)(3) are excepted from the requirements of CS 25.1309(b)(1)(ii). Certain single failures covered by CS 25.735(b) are excepted from the requirements of CS 25.1309(b). The failure conditions covered by CS 25.810 and CS 25.812 are excepted from the requirements of CS 25.1309(b). The requirements of CS 25.1309(b) apply to powerplant installations as specified in CS 25.901(c).

(a) The aeroplane equipment and systems must be designed and installed so that:

(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the aeroplane operating and environmental conditions.

(2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a)(1) of this paragraph.

(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any catastrophic failure condition

(i) is extremely improbable; and

(ii) does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote; and

(4) Any significant latent failure is eliminated as far as practical, or, if not practical to eliminate, the latency of the significant latent failure is minimised; and

(5) For each catastrophic failure condition that results from two failures, either one of which is latent for more than one flight, it must be shown that:

(i) it is impractical to provide additional redundancy; and

(ii) given that a single latent failure has occurred on a given flight, the failure condition is remote; and

(iii) the sum of the probabilities of the latent failures which are combined with each evident failure does not exceed 1/1 000.

(c) Information concerning unsafe system operating conditions must be provided to the flight crew to enable them to take appropriate corrective action in a timely manner. Installed systems and equipment for use by the flight crew, including flight deck controls and information, must be designed to minimise flight crew errors which could create additional hazards.

(d) Electrical wiring interconnection systems must be assessed in accordance with the requirements of CS 25.1709.

(e) Certification Maintenance Requirements must be established to prevent the development of the failure conditions described in CS 25.1309(b), and must be included in the Airworthiness Limitations Section of the Instructions for Continued Airworthiness required by CS 25.1529.

[Amdt 25/5]
[Amdt 25/6]
[Amdt 25/19]
[Amdt 25/20]
[Amdt 25/24]

AMC 25.1309 System design and analysis

ED Decision 2021/015/R

Table of Contents

1. PURPOSE.

a. This AMC describes acceptable means for showing compliance with the requirements of CS 25.1309. These means are intended to provide guidance to supplement the engineering and operational judgement that must form the basis of any compliance demonstration.

b. The extent to which the more structured methods and guidelines contained in this AMC should be applied is a function of systems complexity and systems failure consequence. In general, the extent and structure of the analyses required to show compliance with CS 25.1309 will be greater when the system is more complex and the effects of the Failure Conditions are more severe. This AMC is not intended to require that the more structured techniques introduced in this revision be applied where traditional techniques have been shown to be acceptable for more traditional systems designs. The means described in this AMC are not mandatory. Other means may be used if they show compliance with CS 25.1309.

2. RESERVED.

3. RELATED DOCUMENTS.

The following guidance and advisory materials are referenced herein:

a. *Advisory Circulars, Acceptable Means of Compliance.*

(1) AMC 25.1322 Alerting Systems.

(2) AC 25.19/AMC 25.19 Certification Maintenance Requirements.

(3) AMC 20-115 Software Considerations for Airborne Systems and Equipment Certification

(4) AMC 25.901(c) Safety Assessment of Powerplant Installations.

b. *Industry documents.*

(1) RTCA, Inc., Document No. DO-160D/EUROCAE ED-14G, Environmental Conditions and Test Procedures for Airborne Equipment.

(2) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A/EUROCAE ED-79A, Guidelines for development of civil aircraft and systems.

(3) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

4. APPLICABILITY OF CS 25.1309.

Paragraph 25.1309 is intended as a general requirement that should be applied to any equipment or system as installed, in addition to specific systems requirements, except as indicated below.

a. While CS 25.1309 does not apply to the performance and flight characteristics of Subpart B and structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is based. For example, it does not apply to an aeroplane's inherent stall characteristics or their evaluation, but it does apply to a stall warning system used to enable compliance with CS 25.207.

b. Jams of flight control surfaces or pilot controls that are covered by CS 25.671(c)(3) are excepted from the requirements of CS 25.1309(b)(1)(ii).

c. Certain single failures covered by CS 25.735(b)(1) are excepted from the requirements of CS 25.1309(b). The reason concerns the brake system requirement that limits the effect of a single failure to doubling the brake roll stopping distance. This requirement has been shown to provide a satisfactory level of safety without the need to analyse the particular circumstances and conditions under which the single failure occurs.

d. The failure conditions covered by CS 25.810 and CS 25.812 are excepted from the requirements of CS 25.1309(b). These failure conditions related to loss of function are associated with varied evacuation scenarios for which the probability cannot be determined. It has not been proven possible to define appropriate scenarios under which compliance with CS 25.1309(b) can be demonstrated. It is therefore considered more practical to require particular design features or specific reliability demonstrations as described in CS 25.810 and CS 25.812. Traditionally, this approach has been found to be acceptable.

e. The requirements of CS 25.1309 are generally applicable to engine, propeller, and propulsion system installations. The specific applicability and exceptions are stated in CS 25.901(c).

f. Some systems and some functions already receive an evaluation to show compliance with specific requirements for specific failure conditions and, therefore, meet the intent of CS 25.1309 without the need for additional analysis for those specific failure conditions.

g. The safety assessment process should consider all phases during flight and on ground when the aeroplane is in service. While this includes the conditions associated with the pre-flight preparation, embarkation and disembarkation, taxi phase, etc., it, therefore, does not include periods of shop maintenance, storage, or other out-of-service activities.

Where relevant, the effects on persons other than the aeroplane occupants should be taken into account when assessing failure conditions in compliance with CS 25.1309.

5. DEFINITIONS.

The following definitions apply to the system design and analysis requirements of CS 25.1309 and the guidance material provided in this AMC. They should not be assumed to apply to the same or similar terms used in other regulations or AMCs. Terms for which standard dictionary definitions apply are not defined herein.

a. *Analysis.* The terms "analysis" and "assessment" are used throughout. Each has a broad definition and the two terms are to some extent interchangeable. However, the term analysis generally implies a more specific, more detailed evaluation, while the term assessment may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application, e.g., fault tree analysis, Markov analysis, Preliminary System Safety Assessment, etc.

b. *Assessment.* See the definition of analysis above.

c. *At-Risk Time.* The period of time during which an item must fail in order to cause the failure effect in question. This is usually associated with the final fault in a fault sequence leading to a specific failure condition.

d. *Average Probability Per Flight Hour.* For the purpose of this AMC, is a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all aeroplanes of the type divided by the anticipated total operating hours of all aeroplanes of that type (Note: The Average Probability Per Flight Hour is normally calculated as the probability of a Failure Condition occurring during a typical flight of mean duration divided by that mean duration).

e. *Candidate Certification Maintenance Requirements (CCMR).* A periodic maintenance or flight crew check may be used in a safety analysis to help demonstrate compliance with CS 25.1309(b) for hazardous and catastrophic failure conditions. Where such checks cannot be accepted as basic servicing or airmanship they become Candidate Certification Maintenance Requirements (CCMRs). AMC 25.19 defines a method by which Certification Maintenance Requirements (CMRs) are identified from the candidates. A CMR becomes a required periodic maintenance check identified as an operating limitation of the type certificate for the aeroplane.

f. *Check.* An examination (e.g., an inspection or test) to determine the physical integrity and/or functional capability of an item.

g. *Complex.* A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.

h. *Complexity*. An attribute of functions, systems or items, which makes their operation, failure modes, or failure effects difficult to comprehend without the aid of analytical methods.

i. *Conventional.* A system is considered to be Conventional if its functionality, the technological means used to implement its functionality, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly-used.

j. *Design Appraisal.* This is a qualitative appraisal of the integrity and safety of the system design.

k. *Development Assurance.* All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.

l. Development Error. A mistake in requirements, design, or implementation.

m. *Error*. An omission or incorrect action by a crewmember or maintenance personnel, or a development error (e.g. mistake in requirements determination, design, or implementation).

n. *Event.* An occurrence which has its origin distinct from the aeroplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

o. *Exposure Time.* The period of time between the time when an item was last known to be operating properly and the time when it will be known to be operating properly again.

p. *Failure.* An occurrence, which affects the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Note: Errors may cause Failures, but are not considered to be Failures.

q. *Failure Condition.* A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

r. *Installation Appraisal.* This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

s. Item. A hardware or software element having bounded and well-defined interfaces.

t. *Latent Failure.* A failure is latent until it is made known to the flight crew or maintenance personnel.

u. *Qualitative.* Those analytical processes that assess system and aeroplane safety in an objective, nonnumerical manner.

v. *Quantitative.* Those analytical processes that apply mathematical methods to assess system and aeroplane safety.

w. *Redundancy.* The presence of more than one independent means for accomplishing a given function or flight operation.

x. *Significant Latent Failure.* A latent failure that would, in combination with one or more specific failure(s) or event(s), result in a hazardous or catastrophic failure condition.

y. *System*. A combination of interrelated items arranged to perform one or more specific functions.

6. BACKGROUND

a. *General*

For a number of years aeroplane systems were evaluated to specific requirements, to the ~~"~~'single fault'~~"~~ criterion, or to the fail-safe design concept. As later-generation aeroplanes developed, more safety-critical functions were required to be performed, which generally resulted in an increase in the complexity of the systems designed to perform these functions. The potential hazards to the aeroplane and its occupants which could arise in the event of loss of one or more functions provided by a system or that system's malfunction had to be considered, as also did the interaction between systems performing different functions. This has led to the general principle that an inverse relationship should exist between the probability of a failure condition and its effect on the aeroplane and/or its occupants (see Figure 1). In assessing the acceptability of a design it was recognised that rational probability values would have to be established. Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 % of the total were attributed to failure conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is reasonable to expect that the probability of a serious accident from all such failure conditions be not greater than one per ten million flight hours or 1×10^{-7} per flight hour for a newly designed aeroplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. For this reason it was assumed, arbitrarily, that there are about one hundred potential failure conditions in an aeroplane, which could be ~~C~~catastrophic. The target allowable average probability per flight hour of 1×10^{-7} was thus apportioned equally among these failure conditions, resulting in an allocation of not greater than 1×10^{-9} to each. The upper limit for the average probability per flight hour for catastrophic failure conditions would be 1×10^{-9}, which establishes an approximate probability value for the term 'extremely improbable'. Failure conditions having less severe effects could be relatively more likely to occur.

b. *Fail-Safe Design Concept.*

The CS-25 airworthiness standards are based on, and incorporate, the objectives and principles or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

(1) The following basic objectives pertaining to failures apply:

(i) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.

(ii) Subsequent failures of related systems during the same flight, whether detected or latent, and combinations thereof, should also be considered.

(2) The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e. to ensure that major failure conditions are remote, hazardous failure conditions are extremely remote, and catastrophic failure conditions are extremely improbable:

(i) *Designed Integrity and Quality,* including *Life Limits*, to ensure intended function and prevent failures.

(ii) *Redundancy* or *Backup Systems* to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.

(iii) *Isolation and/or Segregation of Systems, Components, and Elements* so that the failure of one does not cause the failure of another.

(iv) *Proven Reliability* so that multiple, independent failures are unlikely to occur during the same flight.

(v) *Failure Warning or Indication* to provide detection.

(vi) *Flight crew Procedures* specifying corrective action for use after failure detection.

(vii) *Checkability:* the capability to check a component's condition.

(viii) *Designed Failure Effect Limits*, including the capability to sustain damage, to limit the safety impact or effects of a failure.

(ix) *Designed Failure Path* to control and direct the effects of a failure in a way that limits its safety impact.

(x) *Margins or Factors of Safety* to allow for any undefined or unforeseeable adverse conditions.

(xi) *Error-Tolerance* that considers adverse effects of foreseeable errors during the aeroplane's design, test, manufacture, operation, and maintenance.

c. Development of Aeroplane and System Functions.

(1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of aeroplane and systems functions implemented through the use of electronic technology and software-based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for these aeroplane and system functions. Thus, other assurance techniques, such as development assurance utilising a combination of integral processes (e.g. process assurance, configuration management, requirement validation and implementation verification), or structured analysis or assessment techniques applied at the aeroplane level and across integrated or interacting systems, have been requested. Their systematic use increases confidence that development errors and integration or interaction effects have been adequately identified and corrected.

(2) Considering the above developments, as well as revisions made to the CS 25.1309, this AMC was revised to include new approaches, both qualitative and quantitative, which may be used to assist in determining safety requirements and

establishing compliance with these requirements, and to reflect revisions in the rule, considering the whole aeroplane and its systems. It also provides guidance for determining when, or if, particular analyses or development assurance actions should be conducted in the frame of the development and safety assessment processes. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative methods of analysis. The analytical tools used in determining numerical values are intended to supplement, but not replace, qualitative methods based on engineering and operational judgement.

7. FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS

a. Classifications.

Failure conditions may be classified according to the severity of their effects as follows:

(1) *No Safety Effect*: Failure conditions that would have no effect on safety; for example, failure conditions that would not affect the operational capability of the aeroplane or increase crew workload.

(2) *Minor*: Failure conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.

(3) *Major*: Failure conditions which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.

(4) *Hazardous*: Failure conditions~~,~~ which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating~~,~~ conditions to the extent that there would be:

(i) A large reduction in safety margins or functional capabilities;

(ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or

(iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

(5) *Catastrophic*: Failure conditions~~,~~ which would result in multiple fatalities, usually with the loss of the aeroplane.

(Note: A failure condition which would prevent continued safe flight and landing should be classified catastrophic unless otherwise defined in other specific AMCs. For flight control systems, continued safe flight and landing is defined in AMC 25.671, paragraphs 4 and 7.)

b. Qualitative Probability Terms.

When using qualitative analyses to determine compliance with CS 25.1309(b), the following descriptions of the probability terms used in CS 25.1309 and this AMC have become commonly accepted as aids to engineering judgement: