U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: System Design and Analysis

Date: 08/30/2024

AC No: 25.1309-1B

Initiated By: AIR-600

This advisory circular (AC) describes acceptable means, but not the only means, for showing compliance with the requirements of Title 14, Code of Federal Regulations (14 CFR) 25.1309, *Equipment, systems, and installations*. These means are intended to provide guidance to supplement the engineering and operational judgment that form the basis of any showing of compliance.

If you have suggestions for improving this AC, you may use the Advisory Circular Feedback Form at the end of this AC.

DANIEL J. ELGAS
Digitally signed by DANIEL J. ELGAS
Date: 2024.08.30 14:57:01 -04'00'

Daniel Elgas
Director, Policy and Standards Division
Aircraft Certification Service

CONTENTS

Paragraph **Page**

CONTENTS (CONTINUED)

CONTENTS

Paragraph **Page**

CONTENTS (CONTINUED)

FIGURES

TABLES

CHAPTER 1. GENERAL INFORMATION

1.1 Purpose.

1.1.1 This AC describes acceptable means, but not the only means, for showing compliance with 14 CFR 25.1309, *Equipment, systems, and installations*. These means are intended to provide guidance to supplement the engineering and operational judgment that form the basis of any showing of compliance. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

1.1.2 Revision B of this AC contains guidance based on rule changes to § 25.1309. This revision also improves upon the materials published in AC 25.1309-1A by providing more substantive guidance on safety analysis methods. It also implements Congressional instruction[1] to emphasize clear applicant documentation of certain technical details and failure modes, and pilot response times to them.

1.2 Applicability.

1.2.1 Applicability of this AC.

1.2.1.1 The guidance in this AC is for airplane manufacturers, modifiers, foreign regulatory authorities, and Federal Aviation Administration (FAA) Aircraft Certification Service engineers and the Administrator's designees.

1.2.1.2 Using this guidance as a means of compliance with § 25.1309 is voluntary only and not using it will not affect rights and obligations under existing statutes and regulations. The FAA will consider other methods of showing compliance that an applicant may elect to present. Terms such as "should," "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. If the FAA becomes aware of circumstances in which following this AC would not result in compliance with the applicable regulations, the agency may require additional substantiation as the basis for finding compliance.

1.2.2 Applicability of § 25.1309.

1.2.2.1 Section 25.1309 is intended as a general requirement to be applied to any equipment or system as installed on the airplane, be it for type certification, operating rules, or optional, in addition to specific systems requirements, except as indicated below.

[1] Section 115 of the Aircraft Certification, Safety, and Accountability Act of 2020.

1.2.2.2 Although the applicant does not need to account for § 25.1309 when showing compliance with the performance and flight characteristics requirements of part 25, subpart B, and the structural requirements of part 25, subparts C and D, § 25.1309 does apply to any system on which compliance with any of those requirements is based. For example, § 25.1309 does not apply to an airplane's inherent stall characteristics or their evaluation, but it does apply to a stall warning system used for compliance with § 25.207.

1.2.2.3 Some systems and functions already receive an evaluation to show compliance with specific requirements for specific failure conditions. Such evaluations may also be used to show compliance with § 25.1309 without additional or duplicative analysis for those specific failure conditions. The applicant provides substantiation that the evaluation is an acceptable means of compliance to § 25.1309 and documents it in the certification plans for approval by the certification office.

1.2.2.4 Jams of flight control surfaces or pilot controls covered by § 25.671(c)(3) are excepted from the requirements of § 25.1309(b).

1.2.2.5 Single failures covered by § 25.735(b)(1) are excepted from the requirements of § 25.1309(b) because § 25.735(b)(1) limits the effect of a single failure in the brake system to doubling the brake roll stopping distance. This requirement provides a satisfactory level of safety without the need to analyze the particular circumstances and conditions under which the single failure occurs. In addition, the diverse circumstances under which such a failure could occur make any structured determination of its outcome or frequency indeterminate. However, § 25.1309(b) does apply to failures in the brake systems that are not related to the intended braked roll stopping distance or if the failures affect functions other than braking. For example, if a hydraulic brake line failure in the brake system also affects ground spoiler deployment, then § 25.1309(b) applies to that failure.

1.2.2.6 The failure effects covered by §§ 25.810(a)(1)(v) and 25.812 are excepted from the requirements of § 25.1309(b). The failure conditions associated with these cabin safety equipment installations are associated with varied evacuation scenarios for which the probability cannot be determined due to the multitude of factors that can lead to an evacuation. For these types of equipment, the FAA has not been able to define appropriate scenarios under which an applicant could demonstrate compliance with § 25.1309(b). Therefore, the FAA considers it acceptable in terms of safety to require particular design features or specific reliability demonstrations for these types of equipment, and to exclude these equipment items from the requirements of § 25.1309(b). Traditionally, the FAA has found this approach acceptable.

1.2.2.7 The requirements of § 25.1309 are applicable to powerplant installations. The specific applicability and exceptions are stated in § 25.901(c). Section 25.901(c) states that § 25.1309(b) does not apply to propeller debris release failures; those failures are addressed by § 25.905(d) and 14 CFR part 35. Section 25.1309(b) does not apply to uncontained engine rotor failure, engine case rupture, or engine case burn-through failures addressed by §§ 25.903(d)(1) and 25.1193 and 14 CFR part 33.

1.2.2.8 In accordance with § 25.901(d), the requirements of § 25.901(c) and hence § 25.1309 are applicable to auxiliary power unit installations.

1.2.2.9 The fuel system is part of the powerplant installation and therefore must comply with § 25.1309. In addition, fuel systems must comply with § 25.954, *Fuel system lightning protection*, and § 25.981, *Fuel tank explosion prevention*. Section 25.954 provides a standard for lightning protection of both fuel tank structure and fuel tank systems. Refer to AC 25.954-1, *Transport Airplane Fuel System Lightning Protection*, for guidance on the safety assessment of fuel tank lightning protection. Section 25.981 provides standards for the prevention of ignition sources, other than lightning, within the fuel tanks of transport category airplanes. Refer to AC 25.981-1D, *Fuel Tank Ignition Source Prevention Guidelines*, for guidance on the safety assessment of fuel system ignition sources, other than lightning.

1.2.2.10 Section 25.1309, including the no-single-failure requirement, applies to structural elements in systems, even though those structural elements may also be required to meet the fatigue and damage tolerance criteria of § 25.571. For structural elements in systems, (with the exception of the main structural elements in landing gear, the horizontal stabilizer surface, and other control surfaces, including high lift surfaces), meeting the damage tolerance requirement of § 25.571 by itself is not sufficient to justify the assumption that a single failure will not occur. This is because single failure of structural elements can occur due to causes other than those addressed by § 25.571. For specific guidance related to structural elements in flight control systems, refer to Policy Statement No. PS-ANM-25-12 or the most recent FAA policy.

1.2.2.11 Section 25.1309 requirements are applicable to the electrical and electronic systems covered under § 25.1316, *Electrical and electronic system lightning protection*, and § 25.1317, *High-Intensity Radiated Fields (HIRF) Protection*. Sections 25.1316 and 25.1317 provide standards for those systems that are considered critical for continued safe flight and landing. Refer to AC 20-136, *Aircraft Electrical and Electronic System Lightning Protection*, and AC 20-158, *The Certification of Aircraft Electrical and Electronic Systems for Operation in the HIRF Environment*, for guidance on the safety assessment of electrical and electronic systems for lightning and HIRF environments, respectively.

However, these ACs may not provide complete guidance for compliance with § 25.1309.

1.2.2.12 Although § 25.1309 is always applicable to approved operating conditions (on ground and in flight) of the airplane or system, it is only applicable to ground operating conditions when the airplane is in service. While ground operating conditions include conditions associated with line maintenance, dispatch determinations, embarkation and disembarkation, taxi, and the like, they do not include periods of shop maintenance, storage, or other out-of-service activities.

1.2.2.13 Where relevant, applicants should also account for risks to persons other than airplane occupants, such as ground crew, when assessing systems failure conditions for compliance with § 25.1309. For this assessment, ground crew persons are aircraft handling, maintenance, or servicing personnel adjacent to the aircraft while it is in a ground operating condition. The risks include threats to people on the ground or adjacent to the airplane during ground operations, electric shock threats to mechanics, atmospheric threats to mechanics, unwanted door or thrust reverser movement, and other similar situations.

1.3 Cancellation.

This AC cancels AC 25.1309-1A, dated June 21, 1988.

1.4 Related Documents.

The following regulatory and advisory materials are related to this AC:

1.4.1 Related Regulations.

The following 14 CFR part 25 regulations are related to this AC. You can download the full text of these regulations from the Federal Register website at Electronic Code of Federal Regulations, jointly administered by the Office of the Federal Register (OFR) of the National Archives and Records Administration (NARA) and the U.S. Government Publishing Office (GPO). You can order a paper copy from the U.S. Superintendent of Documents, U.S. Government Publishing Office, Washington, D.C. 20401; at Government Publishing Office, by calling telephone number (202) 512-1800; or by sending a fax to (202) 512-2250.

- Section 25.4, *Definitions.*
- Section 25.302, *Interaction of systems and structures.*
- Section 25.305, *Strength and deformation.*
- Section 25.365, *Pressurized compartment loads.*
- Section 25.571, *Damage-tolerance and fatigue evaluation of structure.*
- Section 25.629, *Aeroelastic stability requirements.*

- Section 25.671, *Control Systems—General.*
- Section 25.735, *Brakes and braking systems.*
- Section 25.773, *Pilot compartment view.*
- Section 25.783, *Fuselage doors.*
- Section 25.810, *Emergency egress assist means and escape routes.*
- Section 25.812, *Emergency lighting.*
- Section 25.841, *Pressurized cabins.*
- Section 25.863, *Flammable fluid fire protection.*
- Section 25.901, *Installation.*
- Section 25.933, *Reversing systems.*
- Section 25.981, *Fuel tank explosion prevention.*
- Section 25.1301, *Function and installation.*
- Section 25.1302, *Installed systems and equipment for use by the flightcrew.*
- Section 25.1322, *Flightcrew alerting.*
- Section 25.1329, *Flight guidance system.*
- Section 25.1333, *Instrument systems*.
- Section 25.1351, *Electrical Systems and Equipment—General.*
- Section 25.1365, *Electrical appliances, motors, and transformers*.
- Section 25.1431, *Electronic equipment*.
- Section 25.1447, *Equipment standards for oxygen dispensing units*.
- Section 25.1529, *Instructions for Continued Airworthiness.*
- Section 25.1585, *Operating Procedures.*
- Section 25.1709, *System safety: EWIS.*
- Section H25.4, *Airworthiness limitations Section,* of Appendix H, *Instructions for Continued Airworthiness.*
- Section I25.3, *Performance and system reliability requirements*, of Appendix I, *Installation of an Automatic Takeoff Thrust Control System (ATTCS)*.
- Section K25.1, *Design requirements*, of Appendix K, *Extended Operations (ETOPS)*.
- Section M25.3, *Reliability indications and maintenance access,* of Appendix M*, Fuel Tank System Flammability Reduction Means*.
- Section M25.4, *Airworthiness limitations and procedures,* of Appendix M*, Fuel Tank System Flammability Reduction Means*.

1.4.2 Advisory Circulars.

The following ACs are related to the guidance in this AC. Please see the latest version of each AC referenced in this document; they are available on the FAA website at FAA Regulations and Policies and in the Dynamic Regulatory System (DRS).

- AC 20-115D, *Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178.*
- AC 20-136B, *Aircraft Electrical and Electronic System Lightning Protection.*
- AC 20-152A, *RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware*.
- AC 20-170, *Integrated Modular Avionics Development*.
- AC 20-174, *Development of Civil Aircraft and Systems*.
- AC 20-189, *Management of Open Problem Reports (OPRs)*.
- AC 21-16G, *RTCA Document DO-160 versions D, E and F, "Environmental Conditions and Test Procedures for Airborne Equipment*."
- AC 25-11B, *Electronic Flight Displays*.
- AC 25-19A, *Certification Maintenance Requirements*.
- AC 25-22, *Certification of Transport Airplane Mechanical Systems*.
- AC 25-28, *Compliance of Transport Category Airplanes with Certification Requirements for Flight in Icing Conditions*.
- AC 25.671-1, *Control Systems—General*.
- AC 25.783-1A, *Fuselage Doors and Hatches*.
- AC 25.901-1, *Safety Assessment of Powerplant Installations*.
- AC 25.933-1, *Unwanted In-flight Thrust Reversal of Turbojet Thrust Reversers*.
- AC 25.954-1, *Transport Airplane Fuel System Lightning Protection*.
- AC 25.981-1D, *Fuel Tank Ignition Source Prevention Guidelines*.
- AC 25.1302-1, *Installed Systems and Equipment for Use by the Flightcrew*.
- AC 25.1322-1, *Flightcrew Alerting*.
- AC 25.1329-1C, *Approval of Flight Guidance Systems*.
- AC 25.1701-1, *Certification of Electrical Wiring Interconnection Systems on Transport Category Airplanes*.
- AC 120-28D, *Criteria for Approval of Category III Weather Minima for Takeoff, Landing, and Rollout*.

1.4.3 Policy Statements.

The following policy statements are available on the FAA website at FAA Regulations and Policies and in the Dynamic Regulatory System (DRS).

- PS-ANM-25-11, *Guidance for Hazard Classifications of Failure Conditions that Lead to Runway Excursions*.
- PS-ANM-25-12, *Certification of Structural Elements in Flight Control Systems*.
- PS-AIR-21.15-01, *Submission of Outline of New and Changed Systems at the Beginning of the Type Certificate Amendment Process for Transport Category Aircraft*.

1.4.4 FAA-sponsored research Netherlands Aerospace Centre (NLR) reports.

These reports support AC 25.1309 accepted probabilities. Copies of the referenced Netherlands Aerospace Centre reports can be obtained by sending an email to: '9-AVS-AIR-SSADocs@faa.gov'.

- NLR-CR-2002-601, November 2002. Assessment of standard probabilities in support of FAA AC 25.1309, Phase one.
- NLR-CR-2003-554, September 2003. Assessment of standard probabilities in support of FAA AC 25.1309, Phase two.
- NLR-CR-2005-015, January 2005. Assessment of standard probabilities in support of FAA AC 25.1309, Phase three.
- NLR-CR-2016-601, February 2017. Update of standard probabilities in support of FAA AC 25.1309.

1.4.5 Industry Documents.

The following RTCA documents are available from RTCA Inc., 1150 18th Street NW, Suite 910, Washington, DC 20036; by completing the Document Order Form and faxing it to (202) 833-9434; or at RTCA. The following SAE International Aerospace Recommended Practice (ARP) documents are available from SAE Customer Service, 400 Commonwealth Drive, Warrendale, PA, 15096; or at SAE. Please use the latest version of the referenced document.

- RTCA, Inc., Document DO-160, *Environmental Conditions and Test Procedures for Airborne Equipment*.
- RTCA, Inc., Document DO-178, *Software Considerations in Airborne Systems and Equipment Certification*.
- RTCA, Inc., Document DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*.
- RTCA, Inc., Document DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations.*
- RTCA, Inc., Document DO-326, *Airworthiness Security Process Specification.*
- RTCA, Inc., Document DO-355, *Information Security Guidance for Continued Airworthiness Global Specification.*

- RTCA, Inc., Document DO-356, *Airworthiness Security Methods and Considerations.*
- SAE ARP 4754, *Guidelines for Development of Civil Aircraft and Systems*.
- SAE ARP 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*.

1.5 **Definitions.**

The following definitions apply to the system design and analysis requirements of § 25.1309 and the guidance material in this AC. See also § 25.4 for common term definitions used in part 25. Some of the following definitions are specific to the system design and analysis requirements of § 25.1309 and the guidance material in this AC. Some of the following definitions may have a different meaning when they are used in other regulations or ACs. There are no defined terms within this section for which standard dictionary definitions apply.

1.5.1 Analysis.

The terms "analysis" and "assessment" are used throughout this AC. The two terms are to some extent interchangeable. However, "analysis" generally implies a more specific, more detailed evaluation, while "assessment" may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning of each term comes from the specific application, for example, fault tree analysis, Markov analysis, preliminary system safety assessment (PSSA), and so forth.

1.5.2 At Risk Time.

The period of time during which the aircraft may be subject to the failure effect under analysis.

1.5.3 Assessment.

See the definition of "analysis" above.

1.5.4 Average Probability per Flight Hour.

For the purpose of this AC, this term is the quotient of the number of times the subject failure condition is predicted to occur during the entire operating life of all airplanes of the type divided by the anticipated total operating hours of all airplanes of that type. Please note that 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.

1.5.5 Catastrophic Single Latent Failure Plus One (CSL+1).

A catastrophic failure condition that results from a combination of two failures, either of which could be latent for more than one flight.

1.5.6 Certification Maintenance Requirement (CMR).

A required scheduled maintenance task established during the design certification of the airplane systems as an airworthiness limitation of the type certificate or supplemental type certificate. This term is defined in § 25.4 Definitions.

Note: The CMRs are a subset of the Instructions for Continued Airworthiness (ICA) identified during the certification process.

1.5.7 Complex.

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

1.5.8 Conventional.

A system is 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.

1.5.9 Design Appraisal.

A qualitative appraisal of the integrity and safety of the system design.

1.5.10 Development Assurance.

All 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 so that the system satisfies the applicable safety objectives.

1.5.11 Equipment.

A physical object that can be installed and removed from the aircraft and performs one or more specific functions. Equipment contains one or more items.

1.5.12 Error.

An omission or incorrect action by a flightcrew member or maintenance personnel, or a development error (for example, a mistake in requirements, design, or implementation).

1.5.13 Event.

An occurrence or condition that affects airplane safety.

1.5.14 External Event.

An occurrence that has its origin distinct from the airplane, such as atmospheric conditions (e.g., gusts, temperature variations, icing, and lightning strikes); runway conditions; conditions of communication, navigation, and surveillance services; bird-strike; and cabin and baggage fires (not initiated by features installed on the airplane); etc. The term does not cover sabotage or other similar intentional acts.

1.5.15 Exposure Time.

The time between when an item is known to be operating properly and when it will be known to be operating properly again.

1.5.16 Failure.

An occurrence that affects the operation of a component, part, or element such that it no longer functions as intended. This includes both loss of function and malfunction.

Note: Errors may cause failures or influence their effects but are not considered to be failures.

1.5.17 Failure Condition.

A condition, caused or contributed to by one or more failures or errors, that has either a direct or consequential effect on the airplane, its occupants, or other persons, accounting for—

- Flight phase,
- Relevant adverse operational or environmental conditions, and
- External events.

1.5.18 Failure Mode.

A specific way in which a system, equipment, hardware item, or piece-part may fail.

1.5.19 Ground Crew.

For the purposes of a system safety assessment, ground crew includes aircraft handling, maintenance or servicing personnel operating in or within the vicinity of the aircraft while it is in a ground operating condition.

1.5.20 Installation Appraisal.

This is a qualitative appraisal of the integrity and safety of the installation including the evaluation of any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, especially in the case of modifications made after entry into service.

1.5.21 Latent Failure.

A failure that is not detected or annunciated when it occurs.

1.5.22 Qualitative analytical process.

Those analytical processes that assess system and airplane safety in a non-numerical manner. Engineering judgment or an acceptable rough-order estimate may be used in this process.

1.5.23 Quantitative analytical process.

Those analytical processes that apply numerical methods and statistical analyses to assess system and airplane safety.

1.5.24 Redundancy.

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

1.5.25 Safety Requirement.

A requirement that is necessary to achieve either a safety objective or satisfy a constraint established by the system safety process.

1.5.26 Significant Latent Failure (SLF).

A latent failure that, in combination with one or more specific failures or events, would result in a hazardous or catastrophic failure condition. This term is defined in § 25.4 Definitions.

1.5.27 Single Failure.

Any failure or set of failures that cannot be shown to be independent from each other (e.g., failures due to a common cause).

1.5.28 System.

A defined combination of subsystems, equipment, items, or elements that perform one or more functions.

CHAPTER 2. BACKGROUND

2.1 General.

2.1.1 The FAA is issuing this revision 1B concurrently with a number of rule changes that address system safety, such as §§ 25.302, 25.629, 25.671, 25.901, 25.933, 25.1309, and others. The agency developed these rule changes, and corresponding advisory material, based on recommendations from several working groups under the Aviation Rulemaking Advisory Committee (ARAC).

2.1.2 In 2010, the ARAC Airplane-Level Safety Analysis Working Group (ASAWG) provided recommendations for changes to §§ 25.1301 and 25.1309. The ASAWG also recommended changes to the corresponding advisory material, and the FAA used these recommendations to develop this AC.

2.1.3 In the early years of aviation, airplane systems were evaluated to specific requirements: to the "single fault" criterion or to the fail-safe design concept, which are explained below. As later-generation airplanes developed, their designers added more safety-critical functions, which generally resulted in an increase in the complexity of the systems designed to perform these functions. A safety-critical function was a function whose failure when required would result in a catastrophic condition. The potential hazards to the airplane and its occupants, in the event of failure of one or more functions provided by a system, had to be considered, as did the interaction between systems performing different functions. To assess the safety of a complex system—and the adequacy of system redundancy to meet the fail-safe criterion—the FAA began assigning statistical probabilities to system failures in AC 25.1309-1, dated September 7, 1982. The agency's primary objective was to ensure that the proliferation of safety-critical systems would not increase the probability of a catastrophic accident. The FAA assigned numerical values to the qualitative probabilistic terms in the requirements, for use in those cases where the impact of system failures is examined by quantitative methods of analysis. However, numerical values were intended to supplement, not replace, qualitative methods based on engineering and operational judgment. See appendix A for a historical perspective of the use of statistical probabilities in system safety assessment.

2.2 Fail-Safe Design Concept.

The part 25 airworthiness standards for installations of systems and equipment are based on, and incorporate, the objectives, principles, and techniques of the fail-safe design concept, which instructs the applicant to assume that single failures will happen, and to consider the effects of those failures and combinations of failures in defining an acceptable safe design.

2.2.1 In fail-safe design, the following basic objectives pertaining to failures apply:

2.2.1.1 In any system or subsystem, the failure of any single element, component, or connection during any one flight must be assumed, regardless of its probability. Such single failures must not be catastrophic. See definition of "catastrophic" in paragraph 3.1.5 of this AC.

2.2.1.2 Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be considered.

2.2.2 The fail-safe design concept uses the following design principles or techniques in order to ensure an acceptable 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, in other words, to ensure that major failure conditions are remote, hazardous failure conditions are extremely remote, and catastrophic failure conditions are extremely improbable.

2.2.2.1 Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures.

2.2.2.2 Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s), for example, two or more engines, hydraulic systems, and so forth.

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

2.2.2.4 Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.

2.2.2.5 Failure Annunciation or Indication to provide awareness in case of detected failures.

2.2.2.6 Flightcrew Procedures specifying corrective action for use after failure detection.

2.2.2.7 Checkability, which is the capability to check a component's condition.

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

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

2.2.2.10 Margins or Factors of Safety to allow for any undefined or unforeseeable adverse conditions.

2.2.2.11 Error Tolerance that considers adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation, and maintenance.

2.3 Highly Integrated Systems.

In 1998, the ARAC System Design and Analysis Working Group raised a concern regarding the efficiency and coverage of the techniques used for assessing safety aspects of highly integrated systems that perform complex and interrelated functions, particularly through the use of electronic technology and software-based techniques. The concern was that design and analysis techniques applied to deterministic risks or to conventional, non-complex systems might not provide adequate safety coverage for more complex systems. Thus, other assurance techniques have also been applied by the FAA and applicants to these more complex systems. These techniques included development assurance using a combination of process assurance; validation and implementation verification techniques; and structured analysis or assessment techniques conducted at the airplane level if necessary or across integrated or interacting systems. The systematic use of these techniques increases confidence that errors in requirements, designs, or implementation, and integration or interaction effects have been adequately identified and corrected. Applicants should continue to emphasize the fail-safe design concept discussed in paragraph 2.2 of this AC in the development and assurance of highly integrated systems.

2.4 Use of Both Qualitative and Quantitative Methods.

Considering the above developments, as well as revisions made to § 25.1309, this AC includes additional approaches, both qualitative and quantitative, which may be used to assist applicants in their 14 CFR 21.20 obligations to show compliance with system safety regulations, considering the whole airplane and its systems. This AC also provides guidance to assist applicants in determining when, or if, particular analyses or development assurance activities should be conducted in the frame of the development and safety assessment processes. See AC 20-174 and the industry documents listed in paragraph 1.4.5 of this AC for additional guidance. In summary, both qualitative and quantitative methods are used in practice, and both may be necessary to some degree to support a compliance finding. The analytical tools used in determining numerical values are intended to complement, but not replace, qualitative methods based on engineering and operational judgment. See appendix B of this AC for guidance on available qualitative and quantitative methods for assessment of failure conditions.

CHAPTER 3. FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS

3.1 **Classifications.**

The FAA classifies failure conditions according to the severity of their effects as defined in paragraphs 3.1.1 through 3.1.5 below.

Note: The description of the terms provided for major, hazardous, and catastrophic failure conditions are the same as those found in § 25.4.

3.1.1 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 airplane or increase flightcrew workload but may cause inconvenience to passengers or cabin crew.

3.1.2 Minor.

A failure condition that would not significantly reduce airplane safety and would only involve flightcrew actions that are well within their capabilities. Minor failure conditions may result in, for example—

- A slight reduction in safety margins or functional capabilities,
- A slight increase in flightcrew workload, such as routine flight plan changes,
- Some physical discomfort to passengers or cabin crew, or
- An effect of similar severity.

3.1.3 Major.

A failure condition that would reduce the capability of the airplane or the ability of the flightcrew to cope with adverse operating conditions, to the extent that there would be:

- A significant reduction in safety margins or functional capabilities,
- A physical discomfort or significant increase in flightcrew workload or in conditions impairing the efficiency of the flightcrew,
- Physical distress to passengers or cabin crew, possibly including injuries, or
- An effect of similar severity.

3.1.4 Hazardous.

A failure condition that would reduce the capability of the airplane or the ability of the flightcrew to cope with adverse operating conditions, to the extent that there would be:

- A large reduction in safety margins or functional capabilities,
- Physical distress or excessive workload such that the flightcrew cannot be relied upon to perform their tasks accurately or completely, or
- Serious or fatal injuries to a relatively small number of persons other than the flightcrew.

3.1.5 Catastrophic.

A failure condition that would result in multiple fatalities, usually with the loss of the airplane.

Note 1: A failure condition that would prevent continued safe flight and landing should be classified as catastrophic unless otherwise defined in other specific ACs.

Note 2: For the purpose of performing a safety assessment, "multiple fatalities" means two or more fatalities.

3.2 **Qualitative Probability Terms.**

The probability terms used in § 25.1309 and in this AC are defined in paragraphs 3.2.1 through 3.2.4 below. These terms and definitions have become commonly accepted as aids to engineering judgment when using qualitative analyses to determine compliance with § 25.1309(b).

Note: The definitions provided for probable, remote, extremely remote, and extremely improbable failure conditions are the same as those found in § 25.4.

3.2.1 Probable Failure Condition.

A failure condition that is anticipated to occur one or more times during the entire operational life of each airplane of a given type.

3.2.2 Remote Failure Condition.

A failure condition that is not anticipated to occur to each airplane of a given type during its entire operational life, but which may occur several times during the total operational life of a number of airplanes of a given type.

3.2.3 Extremely Remote Failure Condition.

A failure condition that is not anticipated to occur to each airplane of a given type during its entire operational life, but which may occur a few times during the total operational life of all airplanes of a given type.

3.2.4 Extremely Improbable Failure Condition.

A failure condition that is not anticipated to occur during the total operational life of all airplanes of a given type.

3.2.4.1 **Intent of the Term "Extremely Improbable."**

3.2.4.1.1 The FAA's objective of using this term in the system safety regulations has been to describe a condition (usually a failure condition) that has a probability of occurrence so low that it is not anticipated to occur in service on any transport category airplane to which the standard applies. However, while a rule sets a minimum standard for all the airplanes to which it applies, the FAA's compliance determinations are limited to applications for individual type certificates. Consequently, in practice, the applicant should provide a sufficiently conservative showing that a condition is not anticipated to occur in service during the entire operational life of all airplanes under a type certificate application being assessed.

3.2.4.1.2 The means of showing that the occurrence of a failure condition is extremely improbable varies widely, depending on the type of system, component, or element that must be assessed. The FAA does not consider failure conditions arising from a single failure to be extremely improbable, unless the operational or environmental conditions under which the failure must occur to produce a catastrophic event are in and of themselves extremely remote, or the physics of a theoretical failure is so implausible that the FAA can agree it is not anticipated to ever actually occur. (See paragraph 7.3.2.) Thus, probability assessments for catastrophic outcomes normally involve conditions arising from multiple failures. Both qualitative and quantitative assessments are used in practice, and both are often necessary, to some degree, to support a conclusion that a failure condition is extremely improbable. Generally, performing only a quantitative analysis to show that a failure condition is extremely improbable is insufficient, due to the variability and uncertainty in the analytical process. Any analysis used as evidence that a failure condition is extremely improbable should include justification of any assumptions made, data sources, and analytical techniques to account for the variability and uncertainty in the analytical process.

3.2.4.1.3 Wherever part 25 requires that a condition be extremely improbable, the compliance method—whether qualitative, quantitative, or a combination of the two—along with engineering judgment, should provide convincing evidence that the condition is not anticipated to occur in service when the airplane is produced in accordance with the approved type design, is operated in accordance with approved operating procedures, and is maintained in accordance with approved maintenance procedures.

3.3 Quantitative Probability Terms.

3.3.1 When using quantitative analyses to help determine compliance with § 25.1309(b), the following descriptions of the probability terms used in this requirement and AC have become commonly accepted as aids to engineering judgment. They are expressed in terms of acceptable ranges for the average probability per flight hour. Those probability terms and ranges are as follows:

3.3.1.1 **Probable Failure Condition.**

A failure condition having an average probability per flight hour on the order of 1×10^{-3} or less, but greater than the order of 1×10^{-5}.

3.3.1.2 **Remote Failure Condition.**

A failure condition having an average probability per flight hour on the order of 1×10^{-5} or less, but greater than the order of 1×10^{-7}.

3.3.1.3 **Extremely Remote Failure Condition.**

A failure condition having an average probability per flight hour on the order of 1×10^{-7} or less, but greater than the order of 1×10^{-9}.

3.3.1.4 **Extremely Improbable Failure Condition.**

A failure condition having an average probability per flight hour on the order of 1×10^{-9} or less.

In a quantitative assessment of a remote failure condition a factor of two could be considered as ‘on the order of’ to show compliance. For an extremely remote or extremely improbable failure condition, a factor of three could be considered as ‘on the order of’ to show compliance. Note that at the low end of the probability value, there may be many factors in the analysis methods that influence the top undesired event probability calculations, therefore a higher factor may be acceptable on a case-by-case basis. (See paragraph 7.6.4 of this AC.)

Note: When using quantitative analysis to show compliance with § 25.1309(b), a calculated probability lower than the specified range in this section is considered as compliant.

3.3.2 The above numerical values associated with the probabilistic terms in § 25.1309(b) are guidelines for acceptable risk when applicants use quantitative probability methods of analysis to examine the effect of system failures. A design that meets these guidelines provides some, but not necessarily sufficient, evidence to support a finding by the FAA as to whether the design complies with the rule.

CHAPTER 4. SAFETY OBJECTIVE

4.1 **Objectives of § 25.1309(b).**

The objective of § 25.1309(b)(1), (b)(2), and (b)(3) is graphically presented in figure 4-1 as an inverse relationship between the probability and the severity of failure condition effects, such that:

4.1.1 Failure conditions with no safety effect have no probability requirement.

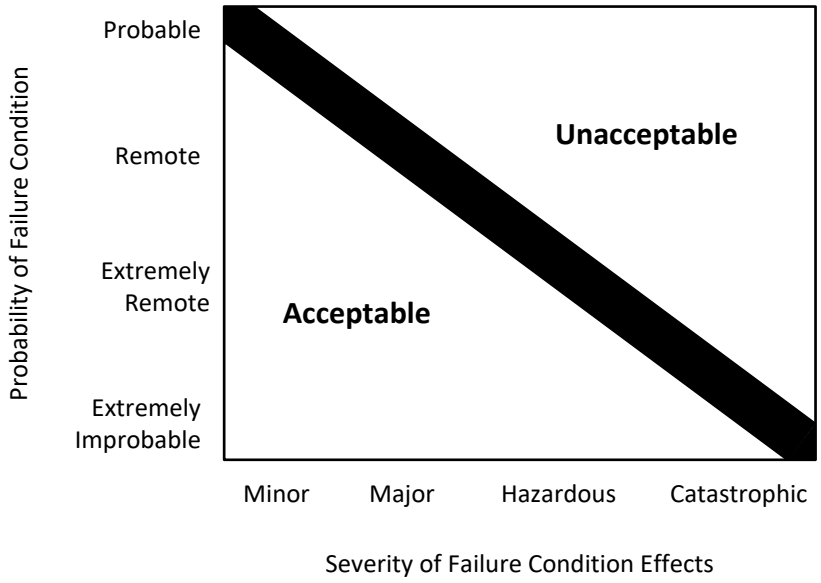
4.1.2 Minor failure conditions may be probable.

4.1.3 Major failure conditions must be no more frequent than remote.

4.1.4 Hazardous failure conditions must be no more frequent than extremely remote.

4.1.5 Catastrophic failure conditions must be extremely improbable.

Figure 4-1. Relationship between Probability and Severity of Failure Condition Effects



4.2 **Relationship between Probability and Severity of Failure Conditions.**

The relationship between probability and severity of the effects associated with failure conditions are described in table 4-1.

TABLE 4-1. RELATIONSHIP BETWEEN PROBABILITY AND SEVERITY OF FAILURE CONDITIONS

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in safety margins or functional capabilities	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants or Other Persons Excluding Flightcrew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of persons other than the flightcrew	Multiple fatalities
Effect on Flightcrew	No effect on flightcrew workload	Slight increase in workload	A physical discomfort or significant increase in workload or in conditions impairing the efficiency of the flightcrew	Physical distress or excessive workload such that flightcrew cannot be relied upon to perform their tasks accurately or completely	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	Probable	Remote	Extremely remote	Extremely improbable
Allowable Quantitative Probability range: Values shown are Average Probability per Flight Hour:	No Probability Requirement	⟷ On the order of 10^{-3} or less, but greater than the order of 10^{-5} *	⟷ On the order of 10^{-5} or less, but greater than the order of 10^{-7}	⟷ On the order of 10^{-7} or less, but greater than the order of 10^{-9}	On the order of 10^{-9} or less

* An allowable probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such analysis that this numerical criterion has been met for minor failure conditions. Current transport category airplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.

4.3 **Safety Objectives for Catastrophic Failure Conditions.**

The safety objectives associated with catastrophic failure conditions are satisfied by showing that:

4.3.1 No single failure results in a catastrophic failure condition;

4.3.2 Each catastrophic failure condition is extremely improbable; and

4.3.3 Significant latent failures are addressed in accordance with § 25.1309(b)(4) and § 25.1309(b)(5).

CHAPTER 5. COMPLIANCE WITH § 25.1309

5.1 Overview.

This chapter describes specific means of compliance with § 25.1309. The applicant would benefit from obtaining early agreement from the FAA on its chosen means of compliance.

5.2 Compliance with § 25.1309(a).

5.2.1 Equipment, systems, and installations regulated by § 25.1309(a)(1) must be shown to function properly when installed. The "airplane operating and environmental conditions" that must be considered under that regulation include the full normal operating envelope of the airplane found in the airplane flight manual (AFM) together with any modification to that envelope associated with abnormal or emergency procedures. External environmental conditions that the airplane is reasonably expected to encounter should be considered, such as atmospheric turbulence, high-intensity radiated fields, lightning, and precipitation. The severity of the external environmental conditions that should be considered is limited to those established by certification standards and precedence.

5.2.2 In addition to the external operating and environmental conditions, the effect of the operating and environmental conditions within the airplane should be considered. Examples of these effects include the following: vibration and acceleration loads, variations in fluid pressure and electrical power, fluid or vapor contamination due to either the normal environment or accidental leaks or spillage and handling by personnel, heat radiated from nearby equipment, and electromagnetic emission from installed equipment. AC 21-16 recognizes RTCA Document DO-160, which defines a series of standard environmental test conditions and procedures that may be used to support compliance. Environmental test procedures contained in technical standard orders (TSOs), or other environmental test standards approved for equipment qualifications, can be used to support compliance. The conditions under which the installed equipment will be operated should be equal to or less severe than the environment for which the equipment is qualified.

5.2.3 The applicant may substantiate the proper functioning of equipment, systems, and installations under the operating and environmental conditions approved for the airplane by test and/or analysis, or reference to comparable service experience on other airplanes if shown to be valid for the proposed installation. For the equipment, systems, and installations covered by § 25.1309(a)(1), the compliance demonstration should also confirm that their normal functioning does not adversely affect the proper functioning of other equipment, systems, or installations covered by § 25.1309(a)(1).

5.2.4 The equipment, systems, and installations addressed by § 25.1309(a)(2) are not required to meet § 25.1309(a)(1). These equipment, systems, and installations are those associated with miscellaneous systems intended for convenience, such as passenger

amenities, passenger entertainment systems, in-flight telephones, and so forth, whose failure or improper functioning should not affect the safety of the airplane. In other words, the types of systems addressed by § 25.1309(a)(2) should be designed so that the severity of their functional failures has "no safety effect." (See paragraph 3.1.1 of this AC for the definition of "no safety effect.") Therefore, the qualification requirements for such equipment, systems, and installations can be reduced to the necessary tests for showing that their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations covered by § 25.1309(a)(1), or the safety of the airplane or its occupants. Examples of adverse effects include fire, explosion, exposing passengers to high voltages, and so forth. The FAA expects normal installation practices to result in sufficiently obvious isolation of the impacts of such equipment on safety that substantiation can be based on a relatively simple qualitative installation evaluation. If the possible failure effects and their evaluation are questionable, or isolation between systems is provided by complex means, then more formal structured evaluation methods or a design change may be necessary.

5.3 Compliance with § 25.1309(b).

Section 25.1309(b)(1) requires that the airplane's systems and associated components, as installed, and considered both separately and in relation to other systems, must be designed so that any catastrophic failure condition is extremely improbable and does not result from a single failure. Section 25.1309(b)(2) requires that any hazardous failure condition is extremely remote, and § 25.1309(b)(3) requires that any major failure condition is remote. An analysis should consider the application of the fail-safe design concept described in paragraph 2.2 of this AC. The analysis should give special attention to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions. Additionally, § 25.1309(b)(4) requires the applicant to eliminate significant latent failures (SLFs) (see definition in paragraph 1.5.26 of this AC) to the extent practical, and provides criteria for accepting those SLFs that cannot be practically eliminated. Section 25.1309(b)(5) applies to the catastrophic failure conditions that result from two failures, either of which could be latent for more than one flight. The failure conditions addressed by § 25.1309(b)(5) are a subset of the failure conditions addressed in § 25.1309(b)(4).

5.3.1 General.

Appendix C of this AC provides an overview of the typical safety assessment process. Compliance with the requirements of § 25.1309(b) should be shown by safety analyses. Where necessary, the failure effects should be substantiated by appropriate ground, flight, or simulator tests. Failure conditions should be identified, and their effects assessed. The maximum allowable probability of the occurrence of each failure condition is determined from the failure condition's effects. When assessing failure conditions, appropriate analysis considerations should be accounted for. Any analysis should consider the following:

5.3.1.1 Possible failure conditions and their causes, modes of failure, and damage from sources external to the system.

5.3.1.2 The possibility of multiple failures due to a common cause, multiple independent failures, and undetected failures.

5.3.1.3 The possibility of requirement, design, and implementation errors.

5.3.1.4 The effect of flightcrew errors reasonably expected in service after the occurrence of a failure or failure condition. (See AC 25.1302-1.)

5.3.1.5 The effect of reasonably anticipated errors when performing maintenance actions.

5.3.1.6 The flightcrew alerting cues, corrective action required, and the flightcrew capability of detecting faults.

5.3.1.7 The resulting effects on the airplane and its occupants, or other persons (such as ground crew or maintenance personnel), considering the stage of flight, the operational sequences (sequence of system responses or expected flightcrew actions following a failure(s)), and operating and environmental conditions.

5.3.2 Planning.

This AC provides guidance on methods of accomplishing the safety objective. The detailed methodology needed to achieve this safety objective depends on many factors, particularly, the degree of system complexity and integration. For proposed airplane designs that will contain many complex or integrated systems, it is likely that the applicant will need to propose and develop a plan to describe the intended process. In general, the extent and structure of the analyses to show compliance with § 25.1309 will be greater when the system is more complex, and the effects of the failure conditions are more severe. Industry standards such as those listed in paragraph 1.4.5 of this AC provide further information on the planning activity. This plan should include consideration of all of the following aspects:

5.3.2.1 Functional and physical interrelationships of systems.

5.3.2.2 Determination of detailed means of compliance, which may include the use of development assurance techniques.

5.3.2.3 Means for establishing the accomplishment of the plan, including how the plan is followed throughout the project to ensure completion.

5.3.3 Availability of Industry Standards and Guidance Materials.

There are a variety of acceptable techniques used currently in industry, some of which are reflected in SAE ARP 4754 and ARP 4761. This AC is not intended to constrain the applicant to the use of these documents in defining their particular methods for

satisfying the objectives of this AC. However, these documents contain material and methods that an applicant may choose to use for performing the safety assessment. The FAA recognizes these methods, when correctly applied, as valid for showing compliance with § 25.1309(b). In addition, SAE ARP 4761 contains tutorial information on applying specific engineering methods (for example, Markov analysis and fault tree analysis) that an applicant may wish to use in whole or in part.

5.3.4 Acceptable Application of Development Assurance Methods.

5.3.4.1 Paragraph 5.3.1.3 of this AC states that any analysis necessary to show compliance with § 25.1309(b) should consider the possibility of errors in requirement, design, and implementation. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterizing the performance of the system. These direct techniques may still be appropriate for simple systems, which perform a limited number of functions and are not highly integrated with other airplane systems.

5.3.4.2 For integrated systems, or systems that perform complex functions, exhaustive testing might be either impossible because all of the system states (within a particular system and within the interfacing systems) cannot be determined, or impractical because of the number of tests that must be accomplished. For these types of systems, the applicant may use development assurance techniques to minimize errors. The rigor of development assurance should be determined by the severity of potential effects on the airplane in case of system malfunctions or loss of functions. Acceptable guidelines for development assurance are described in—

- AC 20-174, which recognizes SAE ARP 4754 for aircraft and systems,
- AC 20-115D, which addresses the software aspects of certification, including the use of RTCA Document DO-178, supplements to DO-178, and tool qualification, and
- AC 20-152A, which addresses airborne electronic hardware aspects of certification, including the use of RTCA Document DO-254.

5.3.4.3 Development assurance activities should define and identify all requirements, including any derived safety requirements needed to manage the many interactions between the systems. The activities should also validate that these requirements are complete and correct and verify that the system design meets those requirements. The development assurance activities should verify that the design provides for fault containment, so that the integrated systems are shown to be fail-safe.

5.3.5 Crew and Maintenance Actions.

5.3.5.1 Where the applicant's analysis identifies recognition and response, and/or action by the flightcrew, cabin crew, or maintenance personnel that is necessary to show that the design complies with § 25.1309(b), the applicant should accomplish all of the activities in paragraphs 5.3.5.1.1 through 5.3.5.1.3. For these verification activities, it is acceptable to assume a fully available indication function (except for the system failures being indicated).

5.3.5.1.1 Verify that any identified indications are actually provided by the system. This includes verification that the sensor coverage and logic that detects the situations and triggers the indicator are sufficient to always detect the situations considering various causes, flight phases, operating conditions, operational sequences, and environments.

5.3.5.1.2 Verify that any identified indications will, in fact, be recognized.

5.3.5.1.3 Verify that any actions required have a reasonable expectation of being accomplished successfully and in a timely manner.

5.3.5.2 The applicant should accomplish the verification activities described in paragraph 5.3.5.1 by consulting with engineers, pilots, flight attendants, maintenance personnel, and human factors specialists, as appropriate, taking due consideration of any relevant service experience and the consequences if the assumed action is performed improperly or not performed. In the case where the flightcrew may not recognize and respond as expected within constraints on the time available, consider the impacts at the system and aircraft level, accounting for circumstances, the phase of flight, and the complexity of the situation, to determine the tasks and/or the systems that need to be modified.

5.3.5.3 In complex situations, the results of the review by specialists may need to be confirmed by inspection, simulator, ground tests, or flight tests. However, quantitative assessments of the probabilities of crew or maintenance errors are not currently considered feasible. If the failure indications are considered to be recognizable and the required actions do not cause an excessive workload, then for the purposes of the analysis, such corrective actions can be considered to be satisfactorily accomplished. If the necessary actions cannot be satisfactorily accomplished, the tasks and/or the systems need to be modified.

5.3.6 Failure Conditions involving Significant Latent Failures.

5.3.6.1 Eliminating all significant latent failures may be impractical in some designs, as it is not always possible to detect any and all failures that may occur during flight. Paragraphs (b)(4) and (b)(5) of § 25.1309 are intended to ensure the minimization of SLFs where it is not possible to completely eliminate them.

5.3.6.2 The elimination and minimization requirement of § 25.1309(b)(4) does not apply to SLFs where the system failure condition meets the safety objectives of § 25.1309(b)(1) or (b)(2) with the assumption that the latent failure has occurred.

5.3.6.3 Where § 25.1309(b)(4) does apply, a hierarchy of safety objectives for managing exposure to SLFs needs to be shown.

1. To meet § 25.1309(b)(4), limiting exposure to SLFs should be an integral part of the applicants' normal design practice. The applicant must first eliminate SLFs to the maximum practical extent. To do so, the applicant should utilize the current state-of-the-art technology, e.g., by implementing practical and reliable failure monitoring and flight crew indication systems to detect failures that would otherwise be latent.

2. For each significant latent failure that cannot reasonably be eliminated, the applicant must minimize the exposure time by design. To do so, the applicant should utilize current state-of-the-art technology rather than relying on scheduled maintenance tasks at lengthy intervals, i.e., implementing pilot-initiated checks, or self-initiated checks (e.g., first flight of the day check, power-up built-in tests, or other system automated checks).

5.3.6.4 An acceptable means of compliance to minimization is to limit the latency of the SLF by minimizing the time the failure is allowed to be present such that the product of this exposure time and the average failure rate of the SLF does not exceed 1/1000. Another acceptable means of compliance to minimization is to show that the failure would not be latent for more than one flight.

5.3.6.5 There can be situations where it is not practical to meet the 1/1000 criterion. For example, if meeting it would result in performing complex or invasive maintenance tasks on the flight line, thereby increasing the risk of incorrect maintenance and associated cost. In such situations, safety is better served when the latent failure is serviced at a suitable maintenance facility. In cases where the applicant can demonstrate that meeting the 1/1000 criterion is not practical, the applicant must minimize the time the failure is expected to be present.

5.3.6.6 In those situations where the significant latent failure is assumed to be latent for the life of the airplane, the applicant should include a qualitative assessment to determine whether a periodic maintenance task is necessary to avoid undue risk due to the exposure to catastrophic or hazardous failure conditions.

5.3.6.7 For a catastrophic failure condition that involves two failures, either of which could be latent for more than one flight, compliance with § 25.1309(b)(5) is required. These failure conditions are denoted as CSL+1. The applicant must first show that it is impractical to design the system with additional fault tolerance, such as adding failure monitors. The assessment should explain why avoidance is not practical and provide supporting rationale for the acceptability. The rationale should be based on the proposed design being state-of-the-art, experience, sound engineering judgment, or other arguments, which led to the decision not to implement additional fault tolerance (e.g., adding failure monitors to eliminate the significant latent failure or adding redundancy to avoid the CSL+1 condition).

5.3.6.8 Once an applicant has shown that CSL+1 conditions are eliminated to the extent practical, the applicant must then apply the criteria in § 25.1309(b)(5)(ii) and (iii) to limit the residual risk in the presence of a latent failure and limit the probability of occurrence of the latent failure itself. These requirements are applied in addition to the requirement of § 25.1309(b)(1) where catastrophic failure conditions must be shown to be extremely improbable and do not result from a single failure.

5.3.6.9 Compliance with § 25.1309(b)(1), (b)(4), and (b)(5) together achieves a balance between the residual risk and latency exposure. For example, in a simple CSL+1 condition, the residual risk would need to be on the order of 1×10^{-6} per flight hour (or better) when the latency is 1/1000 to satisfy the requirement is extremely improbable (1×10^{-9} per flight hour). Conversely, if the failure rate of the residual component is 1×10^{-5} per flight hour, then latency is limited to a probability of 1×10^{-4}. Appendix D of this AC gives a more comprehensive example of how an applicant may conduct limit latency and residual risk analysis to show compliance with § 25.1309(b)(5)(ii) and (iii).

5.3.6.10 Although exposure to latency time is normally expressed in terms of flight hours, if the relevant failures depend on flight cycles, then their exposure times should be evaluated in terms of flight cycles when showing compliance. (See paragraph 7.6.1.4.)

5.4 Compliance with § 25.1309(c).

5.4.1 Section 25.1309(c) requires that information concerning unsafe system operating conditions be provided to the flightcrew to enable them to take appropriate corrective action in a timely manner, thereby mitigating the effects of the condition to an acceptable level. Any system operating condition that, if not detected and properly accommodated by flightcrew action, would significantly contribute to, or result in, a hazardous or catastrophic condition, should be considered an unsafe system operating condition. Compliance with this requirement usually relies on the analysis identified in paragraph 5.3.1 of this AC, which also includes consideration of crew alerting cues, required corrective action, and the capability of detecting faults. Section 25.1309(c) further requires that the applicant design the systems and controls, including indication and annunciation, to minimize crew errors that could create additional hazards (in compliance with § 25.1302). The required information may be provided by an indication and/or annunciation whose forms and functions meet the requirements of § 25.1322 or may be provided by other dedicated means of information,[2] or may be made apparent by the inherent airplane responses. The required information also depends on the degree of urgency for recognition and corrective action by the crew.

5.4.2 When a system provides failure monitoring and indication, the system reliability should be compatible with the safety objectives associated with the system function for which it provides that indication. For example, if the effects of having a system failure and not annunciating that failure are catastrophic, the combination of the system failure with the failure of its annunciation must be extremely improbable. The loss of annunciation should be considered a failure condition in and of itself, due to its impact on the ability of the flightcrew to cope with the subject failure. The subject failure condition should be classified as major unless the applicant can show otherwise. In addition, the applicant should assess unwanted operation (for example, nuisance alerts). The failure monitoring and indication should be reliable, technologically feasible, and economically practicable. Reliable failure monitoring and indication should use current state-of-the-art technology to maximize the probability of detecting and indicating genuine failures, while minimizing the probability of falsely detecting and indicating non-existent failures. Any indication to the flightcrew should be timely, obvious, clear, and unambiguous.

5.4.3 In the case of airplane conditions requiring immediate flightcrew action, a suitable warning indication must be provided to the flightcrew in accordance with § 25.1322, if not provided by inherent airplane characteristics (for example, buffeting). In either case, any warning should be rousing and should occur at a point in a potentially catastrophic sequence where the airplane's capability and the flightcrew's ability still remain sufficient for effective crew action to prevent the catastrophic outcome. For

[2] The terms alert, annunciation and indication are used interchangeably throughout this AC. These terms have been defined and used in different ways, and their definitions may change in the future. Refer to AC 25.1322 and other relevant ACs for the definitions of these terms and their specific application.

other cases that require a flight crew alert, refer to § 25.1322 and other applicable system regulations.

5.4.4 Procedures for the flightcrew to follow after the occurrence of failures must be described in the FAA-approved AFM in accordance with §§ 25.1581 and 25.1585, or AFM revision or supplement.

5.4.5 To meet § 25.1309(c), even if operation or performance is unaffected or insignificantly affected at the time of failure, the applicant should ensure that the design provides any information necessary for the flightcrew to take any action or observe any precautions. Examples include reconfiguring a system, flightcrew awareness of a reduction in safety margins if flightcrew action is necessary, changing the flight plan or regime, making an unscheduled landing to reduce exposure to a more severe failure condition that would result from subsequent failures, or operational or environmental conditions. The applicant should also ensure that the design provides any information concerning unsafe system operating conditions if a failure must be corrected before a subsequent flight. Information and alerting indications may be inhibited during specific phases of flight where awareness or corrective action by the crew is considered more hazardous than no awareness or corrective action; for example, during critical flight phases like takeoff, or if operation or performance is unaffected or insignificantly affected.

5.4.6 The use of periodic maintenance or flightcrew checks to detect SLFs after they occur is undesirable and should not be used in place of practical and reliable failure monitoring and indications. Where such monitoring and indications cannot be accomplished, see paragraph 5.3.6 of this AC for guidance. Chapter 8 of this AC provides further guidance on the use of periodic maintenance or flightcrew checks. Comparison with similar, previously approved systems is sometimes helpful. However, if a new design solution allows practical and reliable failure monitoring and indications, this should be preferred in lieu of periodic maintenance or flightcrew checks.

5.4.7 Applicants should give particular attention to the placement of switches or other control devices, relative to one another, to minimize the potential for inadvertent incorrect flightcrew action, especially during emergencies or periods of high workload. Extra protection, such as the use of guarded switches, may sometimes be needed. See AC 25.1302-1 and other relevant ACs for additional guidance on these and other design attributes related to the avoidance and management of flightcrew error.

5.5 Compliance with § 25.1309(e).

Section 25.1309(e) requires that certification maintenance requirements be established, as necessary, to prevent development of failure conditions described in § 25.1309(b), and that these requirements be included in the Airworthiness Limitations section (ALS) of the ICA required by § 25.1529. See chapter 8 of this AC for detailed guidance on establishing the required scheduled maintenance tasks. Once these tasks are established, they must be included in the ALS in accordance with paragraph (a)(6) of section H25.4 to appendix H, part 25.

CHAPTER 6. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS

6.1 Identification of Failure Conditions.

In order to identify the failure conditions regulated by § 25.1309, applicants should consider the potential effects of failures on the airplane and occupants. The applicant may also need to consider failure conditions that could present threats to persons on the ground, such as ground crew, or adjacent to the airplane during ground operations. Threats include electric shock threats to mechanics, atmospheric events, unwanted door or thrust reverser movement, and other similar situations. These should be considered from the following perspectives:

6.1.1 By Considering Failures of Functions at the Airplane Level.

Failure conditions identified at this level are not dependent on the way the functions are implemented and the systems' architectures.

6.1.2 By Considering Failures of Functions at the System Level.

These failure conditions are identified through examination of the way the functions are implemented and the systems' architectures. Part of this examination is a systematic method, such as failure mode and effects analysis (FMEA), to look for failures within the systems' architectures that could result in their loss or partial loss, or malfunctions that are not limited by the failure condition evaluations (for example, to discover system behaviors that have unintended safety consequences when those systems fail).

Note: The analysis of complex, highly integrated systems, in particular, should be conducted in a methodical and structured manner to ensure all significant failure conditions that arise from multiple failures and combinations of failure conditions are properly identified and accounted for. The relevant combinations of failures and failure conditions should be determined by the whole safety assessment process that encompasses the airplane and system-level functional hazard assessments (FHAs), Particular Risk (PRA), Zonal Safety (ZSA), and Common Mode (CMA) analyses. The overall effect on the airplane due to a combination of individual system failure conditions occurring as a result of a common or cascade failure may be more severe than the effect of each individual system failure. For example, failure conditions classified individually as minor or major may have hazardous or catastrophic effects at the airplane level when considered in combination.

6.1.3 By Considering Failures at the Equipment Level.

These failures may not affect a system's functionality, but they could compromise safe operations or injure persons. These may include individual equipment with intrinsic hazards such as energy supply devices, chemical storage containers, or pressure storage bottles that are part of a system. The analysis should address the equipment's normal operating conditions and failure conditions that could endanger the airplane or its occupants. Examples of intrinsic hazards to be evaluated include, but are not limited to, fires; explosions; release of toxic gases or fluids corrosive to surrounding structures;

and thermal runaway or excessive temperatures that could damage adjacent structures or systems.

Note: Identify any necessary mitigation means including, but not limited to, containment of resultant effects; pressure and temperature relief including venting provisions, if present; and indication or fault annunciation, where applicable. The testing necessary to verify the mitigation effectiveness is equally significant and should also be determined.

6.2 Identification of Failure Conditions Using a Functional Hazard Assessment.

6.2.1 Before an applicant proceeds with a detailed safety assessment, an FHA of the airplane and system functions to determine the need for, and scope of, subsequent analysis should be prepared. This assessment may be conducted using service experience; engineering and operational judgment; and/or a top-down deductive qualitative examination of each function. An FHA is a systematic, comprehensive examination of airplane and system functions to identify potential no safety effect, minor, major, hazardous, and catastrophic failure conditions that may arise as a result of malfunctions or failures to function as intended. The assessment should take into consideration normal system responses to unusual and abnormal external factors. The assessment involves the operational vulnerabilities of systems rather than a detailed analysis of the actual implementation.

6.2.2 Each system function should be examined with respect to the other functions performed by the system, because the loss or malfunction of multiple functions performed by the system could result in a more severe failure condition than the failure of a single function. In addition, each system function should be examined with respect to functions performed by other airplane systems because the loss or malfunction of different but related functions, provided by separate systems, may affect the severity of failure conditions postulated for a particular system.

6.2.3 The FHA should be performed early in the design of the project and updated as necessary as the design develops. It is used to define the airplane-level or system-level safety objectives that must be considered in the proposed airplane or system architectures. Some systems may need only a simple review of the system design to determine the hazard classification. The FHA should also be used to determine the function development assurance levels. An FHA requires experienced engineering judgment to ensure completeness of failure condition identification, and early coordination between the applicant and certification authority.

6.2.4 Depending on the relationship between functions and the systems that perform them, different approaches to an FHA may be taken. Where there is a clear correlation between functions and systems, and where interactions are relatively simple, it may be feasible to conduct separate FHAs for each system, provided that any interface aspects are properly considered and are easily understood. However, where systems and functional relationships are complex or integrated, a top-down approach, from an airplane-level perspective, should be considered when planning and conducting FHAs.

With increasing integrated system architectures, this traditional top-down approach should be performed in conjunction with common-cause considerations (e.g., common resources) in order to adequately address the cases where one system contributes to multiple airplane-level functions.

6.3 Considerations when Assessing Failure Condition Effects.

6.3.1 The requirements of § 25.1309(b) are intended to ensure an orderly and thorough evaluation of the effects on safety of foreseeable failures or other external events, separately or in combination, involving one or more system functions. The interactions of these factors within a system and among relevant systems should be considered. In assessing the effects of a failure condition, factors that might alleviate or intensify the direct effects of the initial failure condition should be considered. Some of these factors include consequent or related conditions existing within the airplane that might affect the flightcrew's ability to deal with direct effects, such as the presence of smoke, acceleration effects, interruption of communication, interference with cabin pressurization, and so forth. When assessing the consequences of a given failure condition, the applicant should consider the failure information provided, the complexity of the flightcrew action, and the relevant crew training. The number of overall failure conditions may influence the expected flightcrew performance. Training recommendations may need to be identified in some cases.

6.3.2 The applicant should evaluate the severity of failure conditions according to the following:

6.3.2.1 Effects on the airplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity. When the effects of a failure condition are complex, the hazard classification may need to be validated by tests, simulation, or other appropriate analytical techniques.

6.3.2.2 Effects on the flightcrew, such as increases above their normal workload that would affect their ability to cope with adverse operational or environmental conditions or subsequent failures. Consider any other human factors assumptions made about the flightcrew's ability to detect, diagnose, and respond appropriately to the failure.

6.3.2.3 Effects on the occupants (passengers and cabin crew).

6.3.2.4 Risks to persons other than airplane occupants (such as ground crew or maintenance personnel) should be taken into account when assessing systems failure conditions in compliance with § 25.1309. See also the discussion in paragraph 1.2.2.13 of this AC.

6.3.3 The applicant should classify the severity of each effect as no safety effect, minor, major, hazardous, or catastrophic. These terms are defined in chapter 3 of this AC (and in § 25.4).

6.3.3.1 The classification of failure conditions does not depend on whether a system or function is the subject of a specific requirement or regulation. Some required systems, such as transponders, position lights, and public address systems, may have the potential for only minor failure conditions. Conversely, other systems that are not required, such as autoflight systems, may have the potential for major, hazardous, or catastrophic failure conditions.

6.3.3.2 Regardless of the types of assessment used, the classification of failure conditions should always be accomplished with consideration of all relevant factors, internal and external; for example, system, crew, performance, operational, and environmental. It is particularly important to consider factors that would alleviate or intensify the severity of a failure condition. Where flight duration, flight phase, or maximum length diversion time can adversely affect the FHA outcome, they must be considered as intensifying factors. Other intensifying factors include conditions (not related to the failure, such as weather or adverse operational or environmental conditions), which reduce the capability of the airplane, or the ability of the flightcrew to cope with a failure condition. An example of an alleviating factor is the continued performance of identical or operationally similar functions by other systems not affected by the failure condition. Another example of an alleviating factor is the flightcrew's ability to recognize the failure condition and take action to temper its effects. (Note that such flightcrew action can in some cases be used to alleviate a failure condition, but it should not be used in lieu of appropriate system design, integrity, and availability requirements.) Whenever this is taken into account, attention to the detection means should be given to ensure the flightcrew's ability (including physical and timeliness) to detect and take corrective action is sufficient. To correlate with the flightcrew's annunciation requirements in § 25.1309(c), consider the case of the flightcrew taking action and also the effects if they do not act or their response is delayed. If their inaction or delayed response results in a severe effect, it may be considered an unsafe system operating condition that carries certain considerations for flightcrew annunciations and evaluation of flightcrew responses. If flightcrew action is used to alleviate the effects of a failure condition, the associated information provided to the flightcrew should comply with § 25.1309(c). See paragraph 5.4 of this AC for more detailed guidance on those considerations. Combinations of intensifying or alleviating factors only need to be considered if they are anticipated to occur together.

6.3.3.3 For hazardous conditions that result in a large reduction in safety margins or functional capabilities, or excessive flightcrew workload, the applicant should show that the remaining capabilities of the airplane and flightcrew will be sufficient to ensure the condition does not become catastrophic.

CHAPTER 7. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS

7.1 General.

After the applicant has identified the failure conditions and assessed the severity of the effects of failure conditions, it is the applicant's responsibility to determine how to show compliance with § 25.1309(b) and obtain a finding of compliance from the FAA. An applicant may use appropriate combinations of one or more of the following methods to show compliance: design and installation reviews, analyses, flight tests, ground tests, simulator tests, or other approved means.

7.2 Assessment of Failure Condition Probabilities.

7.2.1 The probability that a failure condition would occur may be assessed as probable, remote, extremely remote, or extremely improbable. These terms are defined in chapter 3 of this AC (and in § 25.4). Each failure condition should have a probability that is inversely related to the severity of its effects as described in chapter 4 of this AC.

7.2.2 When a system provides protection from events (for example, cargo compartment fire, gusts), its reliability should be compatible with the safety objectives necessary for the failure condition and be associated with the failure of the protection system and the probability of the events. (See additional guidance in paragraph 7.8 and appendix E of this AC.)

7.2.3 An assessment to identify and classify failure conditions is necessarily qualitative. On the other hand, an assessment of the probability of a failure condition may be either qualitative or quantitative. An analysis may range from a report that interprets applicable service data or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the types of functions performed by the system, the severity of failure conditions, and whether the system is complex. Paragraph 7.5, *Depth of Analysis*, provides more guidance on using a combination of qualitative and quantitative probability assessments of failure conditions.

7.3 Single Failure Considerations.

7.3.1 According to the requirements of § 25.1309(b)(1)(ii), a catastrophic failure condition must not result from the failure of a single component, part, or element of a system. To preclude catastrophic failure conditions, the system design should provide failure containment that limits the propagation of the effects of any single failure. In addition, there must be no common cause failure that could affect both the single component, part, or element, and its failure containment provisions. A single failure includes any set of failures that cannot be shown to be independent from each other. Because errors may cause failures, the implications of errors in requirement specification, design, implementation, installation, flightcrew or ground crew operations, maintenance, and

manufacturing that could result in common mode failures should be assessed. Appendix B of this AC and SAE ARP 4761 describe types of analysis methods that may be conducted to identify and minimize common mode failures and document that adequate independence exists between multiple failures. Failure containment techniques available to establish independence may include partitioning, separation, and isolation. It should be noted that only the dominant modes of failure are typically identified and evaluated in a bottom-up component FMEA. For example, the dominant mode "loss of command signal" may be caused by one or more failures of components that produce, process, or transmit the command signal. However, identifying only the dominant failure modes may not be sufficient. To show that no failure mode is anticipated to cause a catastrophic event, consideration of less-obvious failure modes may be required. The information available from top-down analyses, such as the fault tree analysis, can help focus the single failure analysis onto areas of the design where an obscure failure mode might be able to violate an otherwise fail-safe design. (One example of an obscure failure mode is intermittent shorting in the monitored signal's path that allows it to defeat the monitor coverage.)

7.3.2 While single failures must normally be assumed to occur, there are cases where it is obvious that, from a realistic and practical viewpoint, any knowledgeable, experienced person would unequivocally conclude that a failure mode simply would not occur, unless it is associated with a wholly unrelated failure condition that would itself be catastrophic. These types of failures may be considered as not foreseeable. Once identified and accepted, such cases need not be considered failures in the context of § 25.1309. Probabilistic methods may not be used in making this assessment.

7.4 **Common Cause Failure Considerations.**

An analysis should consider the application of the fail-safe design concept described in paragraph 2.2 of this AC. The analysis should also give special attention to ensuring the effective use of design and installation techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel, more than one system performing operationally similar functions, or any system and an associated safeguard.

When considering such common cause failures or other events, consequential or cascading effects should be taken into account. Cascading effects are the set of effects resulting from the propagation of an initiating condition (e.g., a failure or initiating event).

Some examples of potential sources of common cause failures or other events would include the following:

- Rapid release of energy from concentrated sources, such as uncontained failures of rotating parts (other than engines and propellers) or pressure vessels,
- Pressure differentials,
- Non-catastrophic structural failures,
- Loss of environmental conditioning,

- Disconnection of more than one subsystem or component by overtemperature protection devices,
- Contamination by fluids,
- Damage from localized fires,
- Loss of power supply or return (for example, mechanical damage or deterioration of connections),
- Failure of sensors that provide data to multiple systems,
- Excessive voltage,
- Physical or environmental interactions among parts,
- Requirements, design, implementation, installation, flightcrew or ground crew operations, maintenance, and manufacturing errors, or
- Events external to the system or to the airplane.

7.5 **Depth of Analysis.**

The following identifies the depth of analysis expected based on the classification of a failure condition. In all cases discussed below, the applicant should consider the combinations of failure condition effects, as noted in chapter 6 of this AC.

7.5.1 No Safety Effect Failure Conditions.

An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. If it is apparent that an FHA is not necessary for a simple function (for example, the loss of an in-flight entertainment function) and the applicant chooses not to do an FHA, then the safety effects may be derived from the design and installation appraisal performed by the applicant.

7.5.2 Minor Failure Conditions.

An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. If the applicant chooses not to do an FHA, then the safety effects may be derived from the design and installation appraisal performed by the applicant. The applicant should document the result of the appraisal. If system complexity or integration is such that a design or installation appraisal alone cannot establish such isolation or functional independence, then more formal methods as described in SAE ARP 4754/4761 should be applied.

7.5.3 Major Failure Conditions.

Major failure conditions must be remote, per § 25.1309(b)(3).

7.5.3.1 If the system is similar in its relevant attributes to those used in other airplanes and the effects of failure would be the same, then design and installation appraisals (as described in Appendix B of this AC) and satisfactory service history of the equipment being analyzed, or of similar design, is usually acceptable for showing compliance. The applicant should substantiate similarity claims by identifying the differences between the system/equipment being certified and other system/equipment to which similarity is claimed. The applicant should also provide the rationale for why the service history of the other system/equipment is applicable.

7.5.3.2 For systems that are not complex, where similarity cannot be used as the basis for compliance, then compliance may be shown with a qualitative assessment showing that the system-level major failure conditions of the system, as installed, are consistent with the FHA and are remote (for example, redundant systems).

7.5.3.3 For complex systems without redundancy, compliance may be shown as in paragraph 7.5.3.2 above. To show that malfunctions are remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative functional FMEA supported by failure rate data and fault detection coverage analysis.

7.5.3.4 An analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems where functional redundancy is required, a qualitative FMEA and qualitative fault tree analysis may be necessary to determine whether redundancy actually exists (for example, no single failure affects all functional channels).

7.5.4 Hazardous and Catastrophic Failure Conditions.

Hazardous failure conditions must be extremely remote, per § 25.1309(b)(2), and catastrophic failure conditions must be extremely improbable, per § 25.1309(b)(1).

7.5.4.1 Except as specified in paragraph 7.5.4.2 below, a detailed safety analysis is necessary for each hazardous and catastrophic failure condition identified by the FHA. The analysis is usually a combination of qualitative and quantitative assessment of the design.

7.5.4.2 For very simple and conventional installations—that is, low complexity and similarity in relevant attributes—it may be possible to assess a hazardous or catastrophic failure condition as extremely remote or

extremely improbable, respectively, based on experienced engineering judgment using only qualitative analysis. The basis for the assessment is the degree of redundancy, the established independence, isolation of the channels, and the reliability record of the technology involved. Satisfactory service experience on similar systems commonly used in many airplanes may be sufficient when a close similarity is established in respect to both the system design and operating conditions.

7.5.4.3 For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may also be possible to assess a hazardous or catastrophic failure condition as extremely remote or extremely improbable, respectively, based on experienced engineering judgment using only qualitative analysis. A high degree of similarity in both design and application is required to be substantiated. Further, the applicant must be able to demonstrate that the baseline design complies. This typically requires that the applicant has access to all the type design data for the baseline against which the comparison is being made.

7.6 Calculation of Average Probability per Flight Hour (Quantitative Analysis).

7.6.1 The average probability per flight hour is the probability of occurrence, normalized by the flight time, of a failure condition during a flight representing the average “at risk” time of the overall possible flights of the airplane fleet to be certified. The calculation of the average probability per flight hour for a failure condition should consider all of the following:

7.6.1.1 The average flight duration and average flight profile for the airplane type to be certified. Note that this assumption may be affected when showing compliance with section K25.1 ETOPS requirements.

7.6.1.2 All combinations of failures and events that contribute to the failure condition.

7.6.1.3 The conditional probability if a sequence of events is necessary to produce the failure condition.

7.6.1.4 The relevant “at risk” time if a failure condition or event is only relevant during certain flight phases. If the failure condition occurs during specific flight operations or certain flight phases, it should meet the average risk criteria under those specific conditions rather than allowing the risk to be averaged out over a flight of mean duration. In these cases, the probability requirement is applied as a probability per flight or per flight cycle. To convert to per flight hour, divide the per flight probability by one hour.

7.6.1.5 The total exposure time if the failure can persist for multiple flights.

7.6.2 The details of how to calculate the average probability per flight hour for a failure condition are given in appendix F of this AC and in SAE ARP 4761.

7.6.3 If the probability of a subject failure condition occurring during a typical flight of mean duration for the airplane type divided by the flight's mean duration in hours is likely to be significantly different from the predicted average rate of occurrence of that failure condition during the entire operational life of all airplanes of that type, then a better model of the flight of average risk must be used. For example, the loss of consumable material (for example, fluid leakage) may become a critical failure condition for a flight that is longer than the flight of mean duration.

7.6.4 For various reasons, component failure rate data are not typically precise enough to enable accurate estimates of the probabilities of failure conditions. This results in some degree of uncertainty, as indicated by the wide line in figure 4-1 of this AC, and the expression "on the order of" in the descriptions of the quantitative probability terms that are provided above. (See paragraph 3.3 of this AC.) When calculating the estimated probability of each failure condition, this uncertainty should be accounted for in a conservative way that does not compromise safety.

7.7 **Integrated Systems.**

7.7.1 Both physical and functional interconnections between systems have been a feature of airplane design for many years. Section 25.1309(b) accounts for this in requiring systems to be considered in relation to other systems. Provided the interfaces between systems are relatively few and simple, and hence readily understandable, compliance may often be shown through a series of system safety assessments (SSA). Each SSA deals with a particular failure condition (or more likely a group of failure conditions) associated with a system and, where necessary, accounts for failures arising at the interface with other systems. However, where the systems and their interfaces become more complex and extensive, the task of showing compliance may become more complex. It is therefore essential that the means of compliance are considered early in the design phase to ensure that the design can be supported by a viable safety assessment strategy. Aspects of the guidance material that should be given particular consideration are as follows:

7.7.1.1 Planning the proposed means of compliance. This should include development assurance activities to mitigate the occurrence and effects of errors in the design.

7.7.1.2 Considering the importance of architectural design in limiting the impact and propagation of failures.

7.7.1.3 The potential for common cause failures and cascading failure effects and the possible need to assess combinations of multiple lower level failure conditions. (For example, multiple minor and/or major failure conditions can lead up to a hazardous or catastrophic failure condition).

7.7.1.4 The importance of multi-disciplinary teams in identifying and classifying failure conditions.

7.7.1.5 Effect of flightcrew and maintenance procedures in limiting the impact and propagation of failures. However, the effects of overreliance on flightcrew and maintenance actions are also a part of this consideration.

7.7.2 Rigorous and well-structured design and development procedures play an essential role in facilitating a methodical safety assessment process and providing visibility to the means of compliance. SAE ARP 4754 is recognized as the industry standard of practice for certification of highly integrated or complex airplane systems.

7.7.3 Experienced engineering and operational judgment should be applied when determining whether a system is complex. Comparison with similar, previously approved systems is sometimes helpful. All relevant systems attributes should be considered; however, the complexity of software and hardware do not need to be a dominant factor in determining complexity at the system level. The design of a system may be very complex, but predicting its potential malfunctions may be straightforward. For example, the software and interfaces of a predictive windshear system might be considered complex, but the potential failures of the system could be summarized as false alerts, misleading information, and the loss of ability to predict windshear.

7.8 Operational or Environmental Conditions.

7.8.1 A probability of 1 should usually be used for encountering a discrete condition for which the airplane is designed, such as instrument meteorological conditions or Category III weather operations, or landing distance field length provided in the AFM. However, appendix E of this AC contains allowable probabilities that may be assigned to various operational and environmental conditions for use in computing the average probability per flight hour of failure conditions without further justification. The FAA has provided appendix E for guidance and does not intend it to be exhaustive or prescriptive. Currently, a few items do not have accepted standard statistical data from which to derive a probability figure. However, these items are included either for future consideration, or as items for which the applicant may propose a probability figure supported by statistically valid data or supporting service experience. The applicant may propose additional conditions or different probabilities from those in appendix E of this AC, provided they are based on statistically valid data or supporting service experience. The applicant should provide justification for the data and obtain early agreement from the certification authority when such conditions will be included in an analysis. When combining the probability of such a random condition with that of a system failure(s), care should be taken to ensure that the condition and the system failure(s) are independent of one another, or that any dependencies are properly accounted for.

7.8.2 Single failures in combination with operational or environmental conditions leading to catastrophic failure conditions are in general not acceptable. However, single failures do not need to be assumed in combination with operational events or environmental conditions that are extremely remote or that occur outside the normal flight envelope defined in AC 25.671-1. Other cases that are properly justified may be accepted on a case-by-case basis by the certifying authority. In limited cases where a non-redundant system provides protection against an operational or environmental condition (for example, a fire protection system in the cargo compartment comprised of detection and suppression functions) any single failure that results in the loss of the protection function should meet the criteria associated with the major failure condition classification, to ensure adequate system reliability and development assurance.

7.9 Justification of Assumptions, Data Sources, and Analytical Techniques.

7.9.1 Any analysis is only as accurate as the assumptions, data, and analytical techniques it uses. Therefore, to show compliance with the requirements, the underlying assumptions, data, and analytic techniques should be identified and justified to assure that the conclusions of the analysis are valid. Variability may be inherent in elements such as failure modes, failure effects, failure rates, failure probability distribution functions, failure exposure times, failure detection methods, fault independence, limitation of analytical methods, processes, and assumptions. The justification of the assumptions made with respect to the above items should be an integral part of the analysis and summarized in the safety analysis. Assumptions can be validated by using experience with identical or similar systems or components with due allowance made for differences of design, duty cycle, and environment. Where it is not possible to validate a safety analysis in which data or assumptions are critical to the acceptability of the failure condition, extra conservatism should be built into either the analysis or the design. Alternatively, any uncertainty in the data and assumptions should be evaluated to the degree necessary to show that the analysis conclusions are insensitive to that uncertainty.

7.9.2 Where adequate validation data is not available (for example, new or novel systems) and extra conservatism is built into the analysis, then the normal post-certification in-service follow-up may be performed to obtain the data necessary to alleviate any consequence of the extra conservatism. This data may be used, for example, to extend system check intervals.

CHAPTER 8. OPERATIONAL AND MAINTENANCE CONSIDERATIONS

8.1 Overview.

This AC addresses operational and maintenance considerations that are directly related to compliance with § 25.1309. Flightcrew and maintenance tasks related to compliance with § 25.1309 should be appropriate and reasonable. However, the FAA does not currently consider quantitative assessments of flightcrew errors to be feasible. Reasonable tasks are those that can be realistically anticipated to be performed correctly when they are required or scheduled. Paragraph 5.3.5 addresses the expected validation and verification tasks related to flightcrew mitigating actions during a safety assessment. In addition, based on experienced engineering and operational judgment, the discovery of obvious failures during normal operation or maintenance of the airplane may be assumed, even though identification of such failures is not the primary purpose of the operational or maintenance actions. During the safety assessment process associated with § 25.1309 compliance, useful information or instructions associated with the continued airworthiness of the airplane might be identified. This information should be made available to those compiling the ICA covered by § 25.1529.

8.2 Flightcrew Action.

When assessing the ability of the flightcrew to cope with a failure condition, the information provided to the crew, the complexity of the required action, and pilot response time should be considered. When considering the information provided to the flightcrew, refer also to the guidance on § 25.1309(c) (paragraph 5.4 of this AC). Credit for flightcrew actions and consideration of flightcrew errors should be consistent with relevant service experience and acceptable human factors evaluations. If the evaluation indicates that a potential failure condition can be alleviated or overcome without jeopardizing other safety related flightcrew tasks and without requiring exceptional pilot skill or strength, credit may be taken for both qualitative and quantitative assessments. Similarly, credit may be taken for correct flightcrew performance of the periodic checks required to show compliance with § 25.1309(b), provided that performing such checks does not require exceptional pilot skill or strength and the overall flightcrew workload is not excessive. Flightcrew actions should be described in the AFM in compliance with § 25.1585. The applicant should provide a means to ensure the AFM contains all the required flightcrew actions used as mitigation in the hazard classification or to limit the exposure time of the failure condition.

8.3 Maintenance Action.

The applicant’s safety assessment may take credit for the correct accomplishment of reasonable maintenance tasks, for both qualitative and quantitative assessments while also taking into consideration the effects of reasonably anticipated maintenance errors. The maintenance tasks required to show compliance with § 25.1309(b) and (e) should be established. In doing this, the maintenance scenarios in the following paragraphs 8.3.1 and 8.3.2 can be used.

8.3.1 Certification Maintenance Requirements.

8.3.1.1 Periodic maintenance or flightcrew checks may be used to help show compliance with § 25.1309(b). These checks are used to (1) detect the presence of, and thereby limit the exposure time to, SLFs, or (2) detect an impending wear-out of an item whose failure is associated with a hazardous or catastrophic failure condition. Where such checks cannot be accepted as basic servicing or reasonably anticipated flightcrew actions, they should be identified as candidate certification maintenance requirements (CCMRs) or required flightcrew actions in the SSA. Advisory Circular 25-19A details the handling of CCMRs and the selection of CMRs. In compliance with § 25.1309(e), CMRs are included in the ALS of the ICA. Required flightcrew actions must be included in the approved section of the AFM.

8.3.1.2 Quantitative probability analysis of failure conditions, test data, relevant service experience, or other acceptable method should be used to determine check intervals. Because quantitative probability analysis contains inherent uncertainties as discussed in paragraph 7.6.4 of this AC, these uncertainties justify the controlled escalation (in other words, minor adjustments of the task intervals) or exceptional short-term extensions to individual CMRs.

Note: Some latent failures can only be verified by return-to-service tests on the equipment following its removal and repair. The mean time between failures of the equipment can be used to establish the time interval to detect the presence of latent failures if it can be ascertained that the equipment is removed and inspected at a rate more frequent than the safety analysis requires. This credit should be substantiated in the SSA. The means of detecting the latent failures should be clearly documented. For example, these means can be the acceptance tests performed before the equipment leaves the shop, or the system integrity and functional tests when the equipment is installed on the airplane.

8.3.2 Flight with Equipment or Functions Known to be Inoperative.

An applicant may elect to develop a list of equipment and functions that can be inoperative for flight, based on stated compensating precautions that should be taken (for example, operational or time limitations, flightcrew procedures, or ground crew checks). The documents used to show compliance with § 25.1309, together with any other relevant information, should be considered when developing this list. Also, experienced engineering and operational judgment should be applied when developing this list. If more than one flight is made with equipment known to be inoperative and that equipment affects the probabilities associated with hazardous and/or catastrophic failure conditions, then time limits might be needed for the number of flights or allowed operation time in that airplane configuration. The applicant should propose these time limits to the FAA Flight Standards Service for approval.

CHAPTER 9. ASSESSMENT OF MODIFICATIONS TO PREVIOUSLY CERTIFICATED AIRPLANES

9.1 Assessment of Modifications.

The means to ensure continuing compliance with § 25.1309 for modifications to previously certificated airplanes should be determined on a case-by-case basis and depend on the applicable airplane certification basis and the extent of the change, in accordance with § 21.101. The change could be a simple modification affecting only one system or a major redesign of many systems, possibly incorporating new technologies. For any modification, the minimal effort for showing compliance with § 25.1309 is an assessment of the impact on the SSA, and the associated development assurance data. The result of this assessment may range from a simple statement that the existing SSA (and any associated development assurance data) still applies to the modified system in accordance with the original means of compliance, to the need for new means of compliance encompassing the plan referred to in paragraph 5.3.2 of this AC. (If the type certificate holder is unwilling to release or transfer proprietary data in this regard, then a supplemental type certificate applicant might need to create the SSA and the development assurance data covering the relevant changed parts, and parts affected by those changes, of the type design. SAE ARP 4754 guidelines may be used when making a modification to an aircraft, equipment, or item or when reusing a system, equipment, or item.) The FAA recommends that the applicant contact the appropriate certification office early to obtain agreement on the means of compliance in accordance with the latest policies (see PS-AIR-21.15-01).

9.2 Reserved.

APPENDIX A. HISTORICAL PERSPECTIVE ON THE USE OF STATISTICAL PROBABILITIES IN SYSTEM SAFETY ASSESSMENT

A.1 Concorde Transport Supersonique Standard.

The British Civil Aviation Authority (BCAA) applied the concept of proportionally assigning statistical rate goals to categories of accident causes during the design and certification of the Concorde in the Concorde Transport Supersonique Standard in the 1960s. At that time, the BCAA considered the probability of a severe accident to be on the order of one per one million hours of flight (1×10^{-6} per flight hour). The BCAA roughly estimated that 10 percent of those accidents were the result of design systems-related hazards. Based on those assumptions for the Concorde, the BCAA reasoned that probability of a severe accident from design systems-related hazards should be less than 1 in 10 million flight hours, or 1×10^{-7} per flight hour. The BCAA standard defined hazard categories as minor, major, hazardous, and catastrophic, and it assigned qualitatively allowable probability for each category, e.g., probable, remote, and extremely remote. The BCAA also apportioned statistical probabilities to the categories (except the catastrophic category) for use in controlling "statistically controllable" hazards. The standard did not establish a numerical probability for catastrophic failure conditions because, per the overriding fail-safe philosophy, no single failure regardless of probability should foreseeably be allowed to result in a catastrophic failure condition. However, the cumulative probability of all catastrophic failure conditions should be no greater than 1×10^{-7}.

A.2 British Civil Airworthiness Requirements.

The British Civil Aviation Authority replicated the Concorde airworthiness requirements in the British Civil Airworthiness Requirements (BCAR). During certification of the Concorde, the BCAA recognized that analyzing every hazard for the purpose of assuring that the probabilities collectively were less than 1×10^{-7} was an onerous and somewhat impractical task. To address this problem, the BCAA assumed that there were no more than one hundred systems-related, catastrophic failure conditions and that a direct allotment would be sufficient for certification. Therefore, the BCCA apportioned the allowable average probability per flight hour of 1×10^{-7} equally among the theoretical, one hundred catastrophic failure conditions, resulting in 1×10^{-9} per flight hour as the upper limit average probability per flight hour of a statistically controllable catastrophic failure condition. The 1×10^{-9} per flight hour probability was not applicable for single failure conditions that could lead to a catastrophic outcome.

A.3 FAA AC 25.1309-1.

The intent of the BCAR systems guidance was first adopted by the FAA in AC 25.1309-1, *System Design Analysis*, dated September 7, 1982. The BCAR and previous Concorde standards defined four hazard categories in terms of specific airplane level hazards and the effect of those hazards on the airworthiness of the airplane. AC 25.1309-1 defined three functional hazard categories. The AC defined the

functional categories as non-essential, essential, and critical. However, for all practical purposes, the non-essential category was synonymous with the minor category in the BCAR; the essential category spanned the BCAR major and hazardous categories; and critical was the same as catastrophic in the BCAR. The qualitative and quantitative probabilities that were defined in AC 25.1309-1, and the described application of those probabilities, were, for the most part, the same as the BCAR.

A.4 **FAA AC 25.1309-1A.**

In the 1980s, the FAA and the Joint Aviation Authorities (JAA) of Europe harmonized SSA requirements in § 25.1309 and Joint Airworthiness Requirement 25.1309, and the guidance in AC 25.1309-1A and its counterpart JAA Advisory Material Joint (AMJ) 25.1309. The only substantive difference between the AC and AMJ was that the JAA retained the "hazardous" category and its associated probability definitions from the BCAR; whereas the FAA did not but implied an intermediate "severe major" hazard category similar to "hazardous." Otherwise, the definitions and probability values in the AC and AMJ were the same as those in the BCAR and Concorde standard. Both the AC and AMJ also contained a continuing strong emphasis on fail-safe design as the basic intent of the requirements.

A.5 **This AC.**

In revising § 25.1309 at amendment 25-152 (89 FR 68706, August 27, 2024), the FAA added the "hazardous" category. In this AC, the FAA addresses five failure condition classifications (no safety effect, minor, major, hazardous, and catastrophic) and their associated qualitative and quantitative probabilities. These terms are harmonized with European Union Aviation Safety Agency (EASA) Acceptable Means of Compliance (AMC) 25.1309.

A.6 **Quantitative Probability Terms.**

The quantitative probability values contained in this AC should not be applied independently of the qualitative guidance. For example, meeting the 1×10^{-9} per flight hour quantitative probability guidance alone is not sufficient to show compliance with the intent of the "extremely improbable" requirement of § 25.1309(b) if relevant experience indicates the failure condition can occur. The FAA's guidance for using quantitative probability values to meet airworthiness standards has been unchanged since the 1970s. The probability numbers contained in this AC are provided solely for use in evaluating "statistically controllable" hazard contributors within the context of the analysis methodology described. The quantitative values in this AC do not represent FAA accident-rate goals or expectations. The values are unchanged from those derived for the Concorde program because it has been shown in service that the actual system safety achieved using fail-safe design techniques and the combination of qualitative and quantitative guidance in this AC continues to be acceptable.

APPENDIX B. ASSESSMENT METHODS FOR FAILURE CONDITIONS

B.1 **Assessment Methods.**

Various methods for assessing the causes, severity, and probability of failure conditions are available to support experienced engineering and operational judgment. Some of these methods are structured. The various types of analysis are based on either inductive or deductive approaches. Probability assessments may be qualitative or quantitative. Descriptions of some types of analysis are provided below and in SAE ARP 4761.

B.1.1 Design Appraisal.

This is a qualitative appraisal of the integrity and safety of the system design.

B.1.2 Installation Appraisal.

This is a qualitative appraisal of the integrity and safety of the installation including the evaluation of any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, especially in the case of modifications made after entry into service.

B.1.3 Failure Modes and Effects Analysis.

This is a structured, inductive, bottom-up analysis that is used to evaluate the effects on the system and airplane of each foreseeable element or component failure. When properly formatted, the FMEA should aid in identifying latent failures and possible causes of each failure mode. SAE ARP 4761 provides methodology and detailed guidelines, which may be used to perform this type of analysis. In SAE ARP 4761, an FMEA could be a “piece-part” FMEA or a “functional” FMEA. For modern microcircuit-based line replaceable units and systems, an exhaustive piece-part FMEA is not practically feasible with the present state of the art. In that context, an FMEA may be more functional than piece-part oriented. A functional FMEA can lead to uncertainties in the qualitative and quantitative aspects, which can be compensated for by a more conservative assessment such as—

- Assuming all failure modes result in the failure conditions of interest,
- Careful choice of system architecture, or
- Taking into account the experience lessons learned on the use of similar technology.

B.1.4 Fault Tree or Dependence Diagram Analysis.

These are structured, deductive, top-down analyses used to identify the conditions, failures, and events that would cause each defined failure condition. They are graphical methods of identifying the logical relationship between each particular failure condition and the primary element or component failures, other events, or combinations thereof that can cause it. An FMEA may be used as the source document for those primary failures or other events.

B.1.5 Markov Analysis.

A Markov model represents various system states and the relationships among them. The states can be either operational or non-operational. The transitions from one state to another are a function of the failure and repair rates. Markov analysis can be used as a replacement for fault tree or dependence diagram analysis, but it often leads to more complex representation, especially when the system has many states. The FAA recommends using Markov analysis when fault tree or dependence diagrams are not easily usable, namely to account for complex transition states of systems that are difficult to represent and handle with classic fault tree or dependence diagram analysis.

B.1.6 Zonal Safety, Particular Risk, and Common Mode Analyses.

The acceptance of adequate probability of failure conditions is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognize that such independence may not exist in the practical sense, and specific studies are necessary to ensure that independence can either be assured or deemed acceptable. These analyses might also identify failure modes and effects that otherwise would not be foreseen. The evaluation of independence is sub-divided into three areas of study:

B.1.6.1 **Zonal Safety Analysis (ZSA).**

The objective of zonal safety analysis is to ensure that equipment installations within each zone of the airplane meet an adequate safety standard with respect to design and installation standards, interference between systems, and maintenance errors. The analysis also needs to consider the risk that various installers may make with decisions regarding routing, supporting a harness, clearances, etc. In those areas of the airplane where multiple systems and components are installed in close proximity, it should be ensured that the zonal safety analysis identifies any failure or malfunction, which by itself is considered sustainable, but could have more severe effects by adversely affecting other adjacent systems or components.

B.1.6.2 **Particular Risk Analysis (PRA).**

Particular risks are defined as those events or influences that are outside the systems concerned. Examples are fire, leaking fluids, bird strike, tire burst, high intensity radiated fields exposure, lightning, uncontained failure of high energy rotating machines, etc. Each risk should be studied to examine and document the simultaneous or cascading effects or influences that may violate independence.

B.1.6.3 **Common Mode Analysis (CMA).**

Common mode analysis is performed to confirm the assumed independence of the events that were considered in combination for a given failure condition. This analysis should consider the effects of specification, design, implementation, installation, maintenance, and manufacturing errors; environmental factors other than those already considered in the particular risk analysis; and failures of system components.

APPENDIX C. OVERVIEW OF THE SAFETY ASSESSMENT PROCESS

C.1 **Purpose.**

In showing compliance with § 25.1309(b), the applicant should address the considerations covered in this AC in a methodical and systematic manner, which ensures that the process and its findings are visible and readily assimilated into compliance-showing documents. The FAA has provided this appendix primarily for applicants who are unfamiliar with the various methods and procedures typically used in the industry to conduct safety assessments. This guide and figures C-1 and C-2 are not certification checklists, and they do not include all the information provided in this AC. There is no necessity for an applicant to use them or for the FAA to accept them, in whole or in part, to show compliance with any regulation. The sole purpose of this guidance is to assist applicants by illustrating a systematic approach to safety assessments, to enhance understanding and communication by summarizing some of the information provided in this AC, and to provide some suggestions on documentation. You can find more detailed guidance in SAE ARP 4761. SAE ARP 4754 includes additional guidance on how the safety assessment process relates to the system development process.

C.2 **Safety Assessment Process.**

C.2.1 Define the system and its interfaces and identify the functions that the system is to perform. The safety assessment process may identify additional safety requirements for the functions during the system development life cycle.

C.2.2 Determine whether the system is complex, similar to systems used on other airplanes, or conventional. Where multiple systems and functions should be evaluated, consider the relationships between multiple safety assessments.

C.2.3 Identify and classify failure conditions. All relevant applicant engineering organizations, such as systems, structures, propulsion, and flight test, should be involved in this process. This identification and classification may be done by conducting an FHA, which is usually based on one of the following methods, as appropriate:

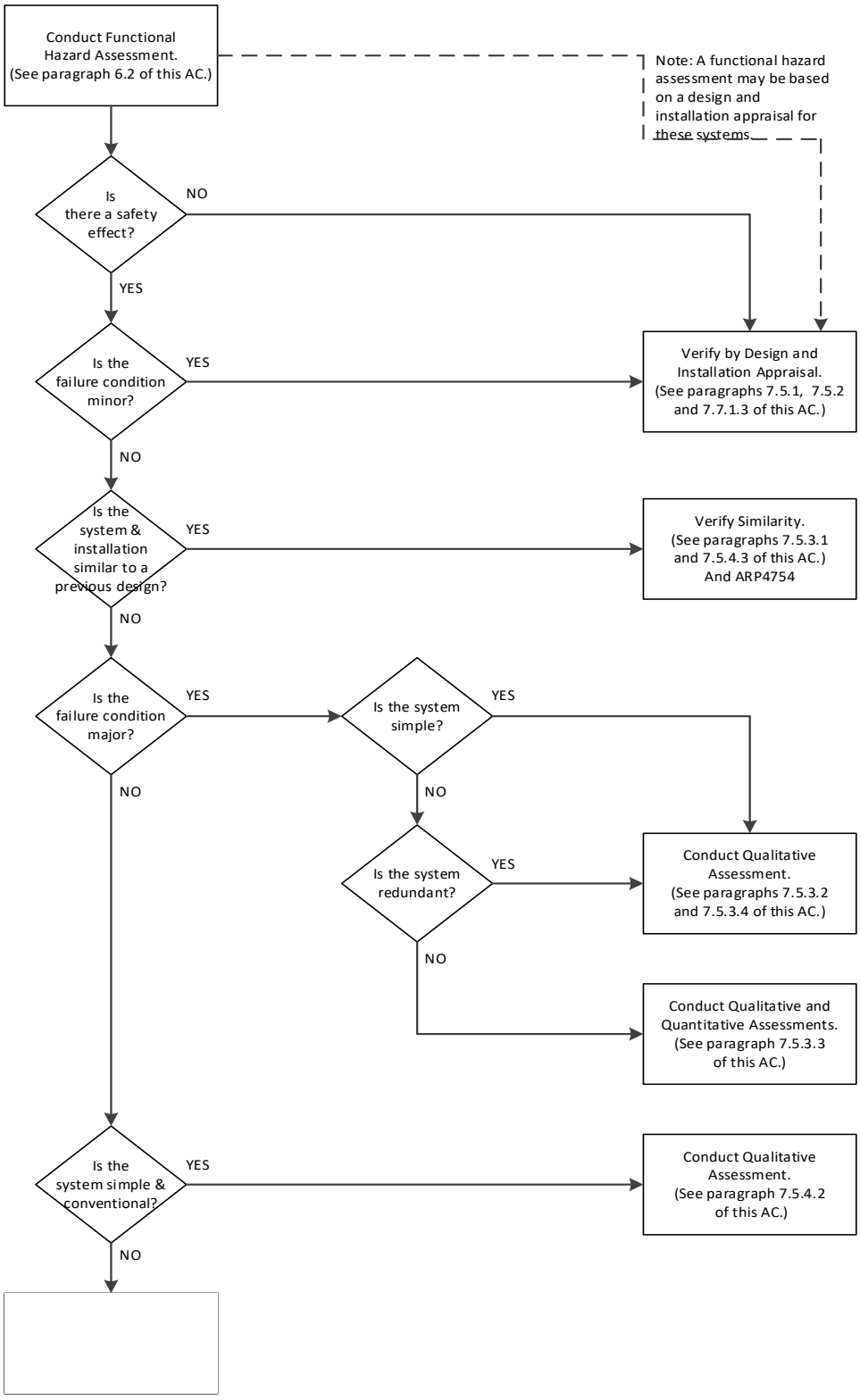
C.2.3.1 If the system is not complex and its relevant attributes are similar to those of systems used on other airplanes, the identification and classification may be derived from design and installation appraisals and the service experience of the comparable, previously approved systems.

C.2.3.2 If the system is complex, it is necessary to postulate systematically the effects on the safety of the airplane and its occupants resulting from any possible failures, considered both individually and in combination with other failures or events.

C.2.3.3 In order to identify the failures that could result in intermittent behaviors, erroneous behaviors, or otherwise unintended behavior, testing should be used where necessary to aid the analytical process.

C.2.4 Choose the means to be used to determine compliance with § 25.1309. The depth and scope of the analysis depends on the types of functions performed by the system, the severity of system failure conditions, and whether or not the system is simple and conventional (see figure C-1). For major failure conditions, experienced engineering and operational judgment, design and installation appraisals, and comparative service experience data on similar systems may be acceptable, either on their own or in conjunction with qualitative analyses or selectively used quantitative analyses. For hazardous or catastrophic failure conditions, the safety assessment should be very thorough. The applicant should obtain early concurrence from the FAA on the choice of an acceptable means of compliance.

Figure C-1. Depth of Analysis Flowchart



C.2.5 Conduct the analysis and produce the data, which have been agreed with by the FAA as being acceptable to show compliance. Refer to SAE ARP 4761 for analysis techniques such as FHA, PSSA, FMEA, CMA, PRA, and ZSA. A typical analysis should include the following information to the extent necessary to show compliance:

C.2.5.1 A statement of the functions, boundaries, and interfaces of the system.

C.2.5.2 A list of the parts and equipment that compose the system, including their performance specifications or design standards and development assurance levels if applicable. This list may reference other documents, for example, TSOs, manufacturer's or military specifications, and so forth.

C.2.5.3 The conclusions, including a statement of the failure conditions and their classifications and probabilities (expressed qualitatively or quantitatively, as appropriate) that show compliance with the requirements of § 25.1309.

C.2.5.4 A description that establishes correctness and completeness and traces the work leading to the conclusions. This description should include the basis for the classification of each failure condition (for example, analysis or ground, flight, or simulator tests). It should also include a description of precautions taken against common cause failures, provide any data such as component failure rates and their sources and applicability, support any assumptions made, and identify any required flightcrew or ground crew actions including any CCMRs.

C.2.6 Assess the analyses and conclusions of multiple safety assessments to ensure compliance with the requirements for all airplane level failure conditions.

C.2.7 Prepare compliance statements, maintenance requirements, flight manual requirements, and any other relevant ICA.

C.2.8 Figure C-2 depicts an overview of a typical safety assessment process starting from the requirements of § 25.1309(b) and (c). For the purpose of this appendix, this figure only shows the principal activities of a safety assessment process. Applicants may refer to SAE ARP 4761 for details of a complete process. Consistent with the system engineering practice in SAE ARP 4754 and ARP 4761, the process is presented in a "V" shape. On the left side of the "V" are the activities to evaluate the preliminary systems designs. On the right side are the activities to evaluate the final designs.

C.2.8.1 **Airplane-Level Functional Hazard Assessment (Airplane FHA).**
A systematic, comprehensive evaluation of aircraft functions to identify and classify failure conditions of those functions according to their severity.

C.2.8.2 **System Functional Hazard Assessment (FHA).**

A systematic, comprehensive evaluation of system functions to identify and classify failure conditions of those functions according to their severity. Because there are many systems on an airplane, the figure depicts multiple system FHAs.

C.2.8.3 **Analyses.**

Analyses of the preliminary or proposed system designs. These analyses include Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), Zonal Safety Analysis (ZSA), Particular Risk Analysis (PRA), Cascading Effects Analysis (CEA) and Common Mode Analysis (CMA).

C.2.8.4 **System Safety Assessments (SSAs).**

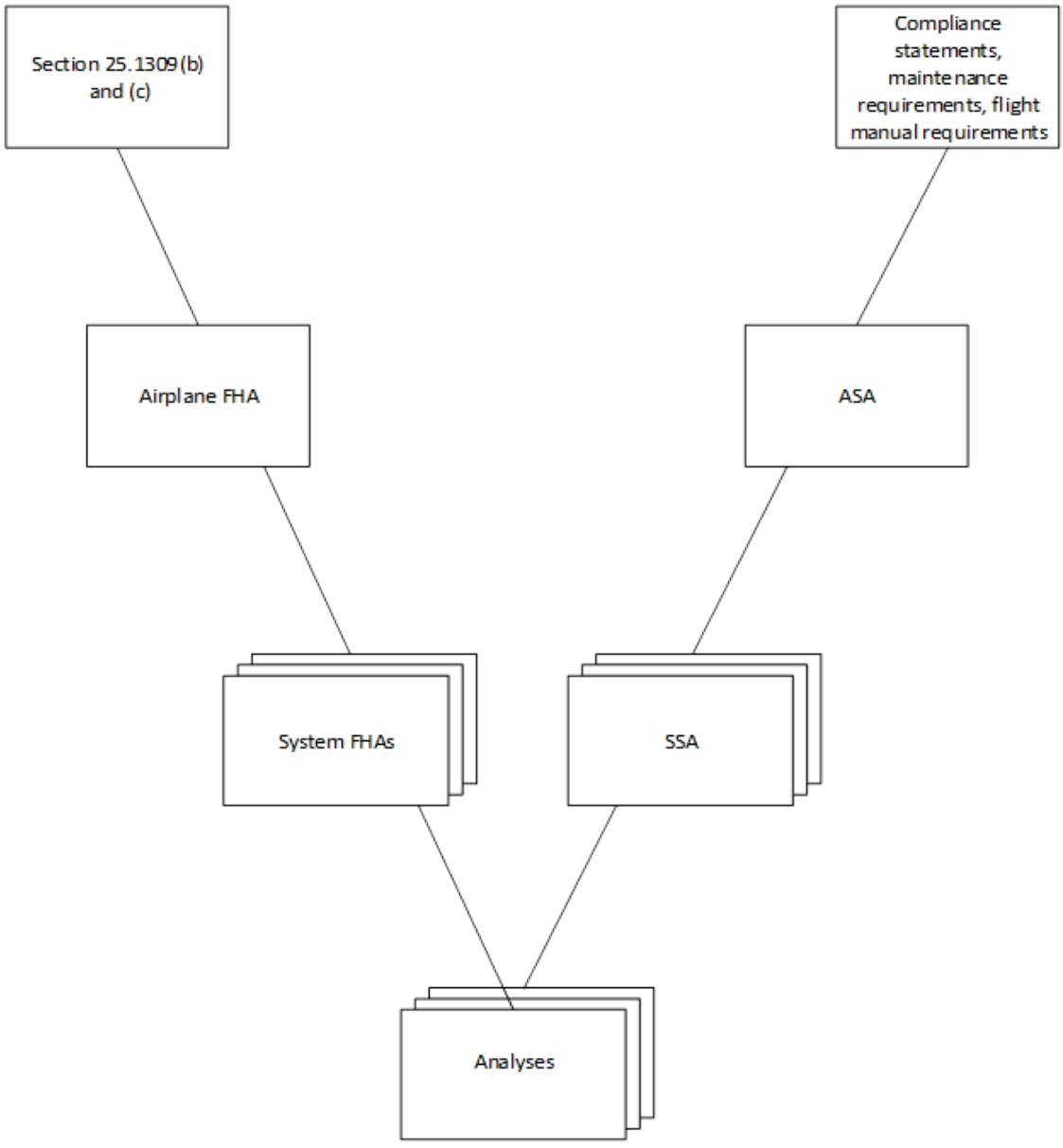
A systematic, comprehensive evaluation of the design implementation to verify it meets all applicable requirements. There are multiple SSAs, and typically one SSA for each system. The SSA may be preceded by a Preliminary System Safety Assessment (PSSA), which is used to evaluate the preliminary design and validate its safety requirements.

C.2.8.5 **Aircraft Safety Assessment (ASA).**

The Aircraft Safety Assessment (ASA) is a systematic, integrated evaluation of the SSAs taken together, to verify that the airplane as a whole meets all applicable requirements. This assessment corresponds to the requirement in § 25.1309(b) that specifies systems be evaluated in relation to other systems.

C.2.9 The applicant documents the results, together with any maintenance requirements (e.g., CMRs) and required flight crew procedures (e.g., flightcrew actions in response to flight deck alerts).

Figure C-2. Overview of Safety Assessment Process



APPENDIX D. EXAMPLE OF LIMIT LATENCY AND RESIDUAL RISK ANALYSIS FOR COMPLIANCE WITH § 25.1309(b)(5)(ii) and (iii)

D.1 Implementing Quantitative Criteria for a CSL+1 Failure Condition.

The following example illustrates how the criteria of § 25.1309(b)(5)(ii) and (iii) may be applied quantitatively. This example uses the fault tree analysis technique described in SAE ARP 4761. Assume a fault tree as shown in figure D-1.

D.1.1 CSL+1 Conditions.

Note: The term minimal cutset (MCS) refers to the smallest set of basic events in the fault tree whose occurrence is sufficient to cause the CSL+1 failure condition. Table D-1 lists all the cutsets in this example.

D.1.1.1 Identify the CSL+1 conditions. The CSL+1 condition is shown as a dual order MCS which contains a basic event that is considered as latent for more than one flight.

D.1.1.2 Group the dual order minimal cutsets.

(a) Group those CSL+1 conditions that contain the same latent failure. For each group, assume that latent failure has occurred, and sum the remaining active failures probabilities. For each group, the sum of the active failure probabilities should be on the order of 1×10^{-5} per flight hour or less. This is intended to show the residual risk safety objective of § 25.1309(b)(5)(ii).

(b) Group those CSL+1 that contain the same active basic event. For each group, sum the remaining latent failure probabilities. For each group, the sum of the latent basic events probability should not exceed 1/1000. This is intended to show the limit latency risk safety objective of § 25.1309(b)(5)(iii).

D.1.1.3 The sum of all the MCS should be on the order of 1×10^{-9} per flight hour or less in order to show § 25.1309(b)(1) compliance.

D.1.2 Alternative Method for Step D.1.1.2(a).

An alternative but more conservative method is to assume a latent failure has occurred and perform step D.1.1.2(a) for each combination and show that the top event average probability is on the order of 1×10^{-5} per flight hour or less. Run the calculations for each and every latent failure.

D.1.3 Results.

The results of the limit latency and residual risk analysis are provided in table D-1.

FIGURE D-1. Example Of Fault Tree For § 25.1309(b)(5) Compliance

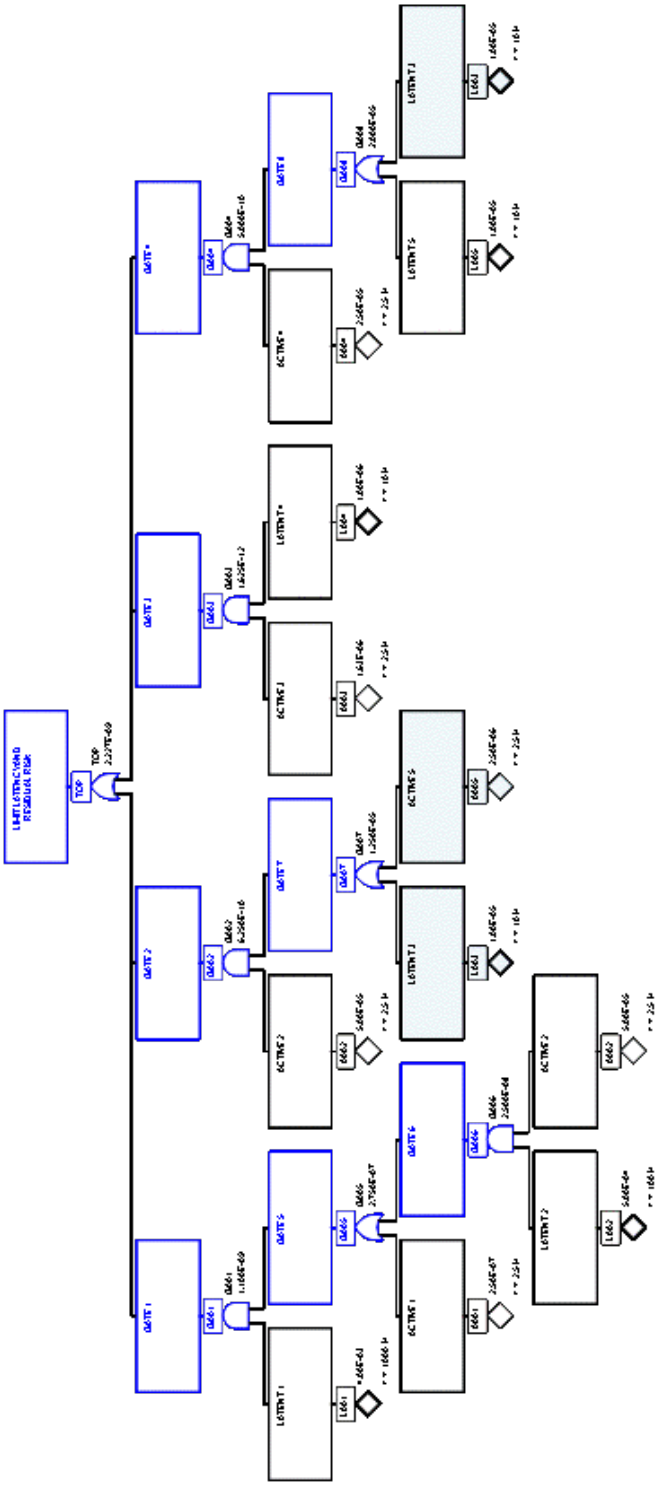


TABLE D-1. EXAMPLE OF CSL+1 IDENTIFICATION FOR § 25.1309(B)(5) COMPLIANCE

MCS No.	Combined Probability	Basic Event	CSL+1?	Failure Rate	Exposure time	Event Probability	Section 25.1309(b)(5)(ii) and (iii) Applicability and Compliance
1	1.0×10^{-9}	A001	Yes	1×10^{-7}	2.5 h	2.5×10^{-7}	Not compliant with limit latency criterion since L001 probability is more frequent than 1×10^{-3}.
		L001		4×10^{-6}	1000 h	4×10^{-3}	
2	5.000×10^{-10}	A002	Yes	2×10^{-5}	2.5 h	5×10^{-5}	Not compliant with residual risk criterion since A002 probability is more frequent than 1×10^{-5}/FH
		L003		1×10^{6}	10 h	1×10^{-5}	
3	2.500×10^{-10}	A004	Yes	1×10^{-5}	2.5 h	2.5×10^{-5}	**Note:** MCS no. #2 and #3 are grouped due to common L003. Although A004 probability is equal to 1 x 10-5/FH, the residual risk criterion is not met because the combined probability of A004 and A002 $(2.5 \times 10^{-5} + 5 \times 10^{-5})$/FH is more frequent than 1×10^{-5}/FH.
		L003		1×10^{-6}	10 h	1×10^{-5}	
4	2.500×10^{-10}	A004	Yes	1×10^{-5}	2.5 h	2.5×10^{-5}	Compliant with both limit latency and residual risk criteria. Note: MCS no. #3 and #4 are grouped due to common A004. Combined L003 and L005 $((1 \times 10^{-5} + 1 \times 10^{-5})$ is less than 1×10^{-3}
		L005		1×10^{6}	10 h	1×10^{-5}	
5	1.250×10^{-10}	A002	No	2×10^{-5}	2.5 h	5×10^{-5}	Section 25.1309(b)(5) does not apply since this dual failure combination does not contain any latent failure.
		A005		1×10^{-6}	2.5 h	2.5×10^{-6}	
6	1.625×10^{-12}	A003	Yes	6.5×10^{-7}	2.5 h	1.625×10^{-6}	Compliant with both limit latency and residual risk criteria. A003 = 1.625×10^{-6}/FH is less than 1.0×10^{-5}/FH L004=1×10^{-6} less than 1×10^{-3}
		L004		1×10^{-7}	10.0 h	1×10^{-6}	
7	1.000×10^{-10}	A002	No	2×10^{-5}	2.5 h	5×10^{-5}	Section 25.1309(b)(5) does not apply since this is a triple-failure combination.
		L001		4×10^{-6}	1000 h	4×10^{-3}	
		L002		5×10^{-6}	100 h	5×10^{-4}	

MCS: Minimal Cut Set: the smallest set of events whose occurrence is sufficient to cause the Top event or failure condition.
A: Active failure; L: Latent failure
Flight time = 2.5 hour of flight
P[LAT i] ~ FR * T

APPENDIX E. ACCEPTED PROBABILITIES

E.1 **Probabilities.**

The probabilities in tables E-1 through E-5 may be used for environmental conditions and operational factors in quantitative safety analyses to show compliance with § 25.1309. If "No accepted standard data" appears in the tables below, the applicant must provide a justified value if a probability of less than 1 is used in the analysis.

Note: The accepted probabilities may not always be appropriate for use in the context of showing compliance to other regulations.

TABLE E-1. ENVIRONMENTAL FACTORS

Condition	Model or Other Justification	Probability
14 CFR part 25, Appendix C, "Flight in Atmospheric Icing."	AC 25-28	1
14 CFR part 25, Appendix O, "Flight in Supercooled Large Drop Icing Conditions"	AC 25-28	10^{-2} per flight hour
Flight into icing conditions that exceed those the airplane has been certified to operate in.		No accepted standard data
Probability of specific icing conditions (largest water droplet, temperature, and so forth) within a given flight.		No accepted standard data
Head wind greater than 25 knots during takeoff and landing.	AC 120-28D / CS-AWO NLR-CR-2016-601	10^{-2} per flight 5×10^{-3} per flight
Tail wind greater than 10 knots during takeoff and landing.	AC 120-28D / CS-AWO NLR-CR-2016-601	10^{-2} per flight 3×10^{-3} per flight
Cross wind greater than 20 knots during takeoff and landing.	AC 120-28D / CS-AWO NLR-CR-2016-601	10^{-2} per flight 3×10^{-3} per flight
Limit design gust and turbulence.	§ 25.341	10^{-5} per flight hour
Air temperature less than -70 °C.		No accepted standard data

TABLE E-2. AIRPLANE CONFIGURATIONS

Condition	Model or Other Justification	Probability
Center of gravity	Standard industry practice	1 (uniform over approved range)
Landing and takeoff weights/masses	Standard industry practice	1 (uniform over approved range)

TABLE E-3. FLIGHT CONDITIONS

Condition	Model or Other Justification	Probability
Flight condition requiring stall warning	In-service observation NLR-CR-2016-601	10^{-2} per flight 4 x 10^{-6} per flight 2.5 x 10^{-6} per flight hour
Flight condition resulting in a stall	In-service observation NLR-CR-2016-601	10^{-5} per flight 5 x 10^{-8} per flight 3 x 10^{-8} per flight hour
Exceedance of V_{MO}/M_{MO} Note: Refer to other regulations with specific requirements that supersede the guidance for this condition.	In-service observation NLR-CR-2003-554	10^{-2} per flight 2 x 10^{-3} per flight 3 x 10^{-4} per flight hour
Flight condition greater than or equal to 1.5g due to gusts	NLR-CR-2003-554	7 x 10^{-3} per flight
Flight condition less than or equal to 0g	NLR-CR-2005-015	1 x 10^{-6} per flight 4 x 10^{-7} per flight hour

TABLE E-4. MISSION DEPENDENCIES

Condition	Model or Other Justification	Probability
Any rejected takeoff	NLR-CR-2016-601	1.5×10^{-4} per flight
High energy (near V_1) rejected takeoff	NLR-CR-2016-601	7×10^{-6} per flight
Need to jettison fuel	NLR-CR-2016-601	1.5×10^{-4} per flight 2.5×10^{-4} per flight hour
Go-around Note: Should be considered as within the normal operating envelope.	NLR-CR-2016-601	7×10^{-4} per flight

TABLE E-5. OTHER EVENTS

Condition	Model or Other Justification	Probability
Fire in a lavatory	NLR-CR-2016-601	2.5×10^{-7} per flight 1.5×10^{-7} per flight hour
Fire in a cargo compartment	NLR-CR-2016-601	4×10^{-8} per flight 3.5×10^{-8} per flight hour

APPENDIX F. CALCULATING THE "AVERAGE PROBABILITY PER FLIGHT HOUR"

F.1 Purpose.

This appendix provides applicants with guidance for calculating the "average probability per flight hour" for a failure condition, so it can be compared with the quantitative criteria in this AC. (As discussed in paragraph 7.6.1.4, for failure conditions and associated classifications that are only relevant during a specific flight phase, evaluate the average risk under those specific conditions rather than allowing the risk to be averaged out over a flight of mean duration. For these cases, the probability is calculated as an average probability per flight. To convert to "average probability per flight hour", divide the per flight probability by one hour.) The process of calculating the "average probability per flight hour" for a failure condition is described here as a four step process and is based on the assumption that the life of an airplane is a sequence of average flights:

- Step 1: Determine the average flight.
- Step 2: Calculate the probability of a failure condition for a certain average flight.
- Step 3: Calculate the average probability per flight of a failure condition.
- Step 4: Calculate the average probability per flight hour of a failure condition.

F.2 Determining the "Average Flight."

The "average probability per flight hour" is based on an average flight. The applicant should estimate the average flight duration and average flight profile for the airplane fleet to be certified. The average flight duration should be estimated based on the applicant's expectations and historical experience for similar types. The average flight duration should reflect the applicant's best and latest estimate of the cumulative flight hours divided by the cumulative airplane flights for the service life of the airplane. The average flight profile should be based on the operating weight and performance expectations for the average airplane when flying a flight of average duration in an International Civil Aviation Organization standard atmosphere. The duration of each flight phase (for example, takeoff, climb, cruise, descent, approach, and landing) in the average flight should be based on the average flight profile. Average taxi times for departure and arrival at an airport should be considered where appropriate and added to the average flight time. The average flight duration and profile should be used as the basis for determining the average probability per flight hour for a quantitative safety assessment. Note that to meet 14 CFR Appendix K to Part 25, K25.1 ETOPS design requirements, the consideration for maximum flight duration with the longest diversion time should be used when showing compliance with § 25.1309(b).

F.3 **Calculating the Probability of a Failure Condition for a Certain Average Flight.**

The probability of a failure condition occurring on an average flight P_{flight}(*failure condition in a flight*) should be determined by structured methods (see SAE ARP 4761 for example methods) and should consider all significant elements (e.g., combinations of failures and events) that contribute to the failure condition. The following should be considered:

F.3.1 The component failure rates used to calculate the "average probability per flight hour" should be estimates of the mature constant failure rates after infant mortality and prior to wear out. For components whose probability of failure may be associated with non-constant failure rates within the operational life of the airplane, reliability analysis may be used to determine component replacement times. In either case, the failure rate should be based on all causes of failure (operational, environmental, and so forth). The failure rate is for the type design hardware that is operated and maintained through servicing plans or ICA requirements. Where available, service history of same or similar components in the same or similar environment should be used.

F.3.1.1 Aging and wear of similarly constructed and similarly loaded redundant components that could directly, or when in combination with one other failure, lead to a catastrophic or hazardous failure condition should be assessed when determining scheduled maintenance tasks for such components.

F.3.1.2 Replacement times—necessary to mitigate the risk due to aging and wear of those components whose failures could directly, or in combination with one other failure, lead to a catastrophic or hazardous failure condition within the operational life of the airplane—should be assessed through the same methodology as other scheduled maintenance tasks required to satisfy § 25.1309 (for example, AC 25-19A) and documented in the ALS as appropriate.

F.3.2 If one failed element in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation should consider the relevant exposure times (for example, time intervals between maintenance and operational checks/inspections). In such cases, the total probability of the failure condition increases with the number of flights during the latency period.

F.3.3 If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the failure occurring on an average flight. It is assumed that the average flight can be divided into n phases (phase 1, ... , phase n). Let T_F be the average flight duration, T_j be the duration of phase j, and t_j be the transition point between T_j and T_{j+1}, $j = 1, \ldots, n$:

$$T_F = \sum_{j=1}^{n} T_j \quad \text{and} \quad t_j - t_{j-1} = T_j$$

Let $\lambda_j(t)$ be the failure rate function during phase j, i.e., for $t \in [t_{j-1}, t_j]$. $\lambda_j(t)$ may be equal to 0 for all $t \in [t_{j-1}, t_j]$ for a specific phase j.

Let $P_{phase\ j}(failure)$ be the probability that the element fails in phase j.

Two cases are possible:

F.3.3.1 The element is checked operative at the beginning of the certain flight. Let the $P_{flight}(failure)$ be the probability that the element fails during one certain flight (including non-flying time).

Then:

$$P_{flight}(failure) = \sum_{j=1}^{n} P_{phase\ j}(failure) = \sum_{j=1}^{n} P\left(element\ failure \middle| t \in [t_{j-1}, t_j]\right)$$
$$= 1 - \prod_{i=1}^{n} exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)dx\right)$$

F.3.3.2 The state of the element is unknown at the beginning of the certain flight. Let the $P_{flight}(failure)$ be the probability that the element is failed by the end of one certain flight (including non-flying time).

Then:

$$P_{flight}(failure\ by\ end\ of\ flight) = P_{prior}(failure\ prior\ to\ flight) + P_{flight}(failure\ in\ flight)$$
$$= P_{prior}(failure\ prior\ to\ flight) + \left(1 - P_{prior}(failure\ prior\ to\ flight)\right)$$
$$* \left(1 - \prod_{i=1}^{n} exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)dx\right)\right)$$

Where $P_{prior}(failure)$ is the probability that the failure of the element has occurred prior to the certain flight.

F.3.4 If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce the failure condition.

F.4 **Calculation of the "Probability per Flight" of a Failure Condition over a period of N flights.**

The next step is to calculate the probability per flight for the failure condition. In other words, the probability of the failure condition for each flight (which might be different although all flights are average flights) during the relevant time (for example, the least common multiple of the exposure times or the airplane life) should be calculated, summed up, and divided by the number of flights during that period. The principles of calculating are described below and in more detail in SAE ARP 4761.

F.4.1.1 The element is checked operative at the beginning of the certain flight, Then:

$$P_{flight}(failure\ condition\ in\ flight) = \frac{\sum_{k=1}^{N} P_{flight\ k}\ (failure\ condition\ in\ flight\ k)}{N}$$

F.4.1.2 The state of the single element is unknown at the beginning of the certain flight.

Then: $\sum_{k=1}^{N} P_{flight\ k}\ (failure\ condition\ in\ flight\ k)\ is\ equal\ to\ P_{flight}(failure\ by\ end\ of\ flight) = P_{prior}(failure\ prior\ to\ flight) + P_{flight}(failure\ in\ flight)$

$$= P_{prior}(failure\ prior\ to\ flight) + \left(1 - P_{prior}(failure\ prior\ to\ flight)\right) * \left(1 - \prod_{i=1}^{n} exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)dx\right)\right)$$

Thus: $P_{per\ flight}(failure\ condition\ in\ flight) =$

$$\frac{P_{prior}(failure\ prior\ to\ flight) + \left(1 - P_{prior}(failure\ prior\ to\ flight)\right) * \left(1 - \prod_{i=1}^{n} exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)dx\right)\right)}{N}$$

Where N is the quantity of all flights during the relevant time, and $P_{flight\ k}$ is the probability that the failure condition occurs in flight k.

F.5 **Calculation of the "Average Probability per Flight Hour" of a Failure Condition.**

Once the average probability per flight has been calculated, it should be normalized by dividing it by the average flight duration T_F in flight hours to obtain the average probability per flight hour. This quantitative value should be used in conjunction with the hazard category/effect established by the FHA to determine if it is compliant for the failure condition being analyzed.

$$P_{average\ per\ flight\ hour}(failure\ condition) = \frac{P_{per\ flight}(failure\ condition\ in\ flight)}{T_F}$$

APPENDIX G. ACRONYMS

14 CFR	Title 14, Code of Federal Regulations
AFM	Airplane Flight Manual
ALS	Airworthiness Limitations Section
AMC	Acceptable Means of Compliance
AMJ	Advisory Material Joint
ARAC	Aviation Rulemaking Advisory Committee
ARP	Aerospace Recommended Practice
ASAWG	Airplane-Level Safety Analysis Working Group
BCAR	British Civil Airworthiness Requirements
CMA	Common Mode Analysis
CCMR	Candidate Certification Maintenance Requirement
CEA	Cascading Events Analysis
CMR	Certification Maintenance Requirement
CSL+1	Catastrophic with Single Latent Plus One
EASA	European Union Aviation Safety Agency
ETOPS	Extended Range Twin-engine operations Performance Standards
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
ICA	Instructions for Continued Airworthiness
JAA	Joint Aviation Authorities
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RTCA	RTCA, Inc. (formerly “Radio Technical Commission for Aeronautics”)
SAE	SAE International (formerly “Society of Automotive Engineers”)
SLF	Significant Latent Failure
SSA	System Safety Assessment
STC	Supplemental Type Certificate
TC	Type Certificate
TSO	Technical Standard Order
ZSA	Zonal Safety Analysis

OMB Control Number: 2120-0746
Expiration Date: 11/30/2024

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to (_____) or (2) faxing it to the attention of the LOB/SO (_____).

Subject:_____ Date: _____

Please mark all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph_____on page_____.

☐ Recommend paragraph_____on page_____be changed as follows:

☐ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by:_____Date: _____