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:

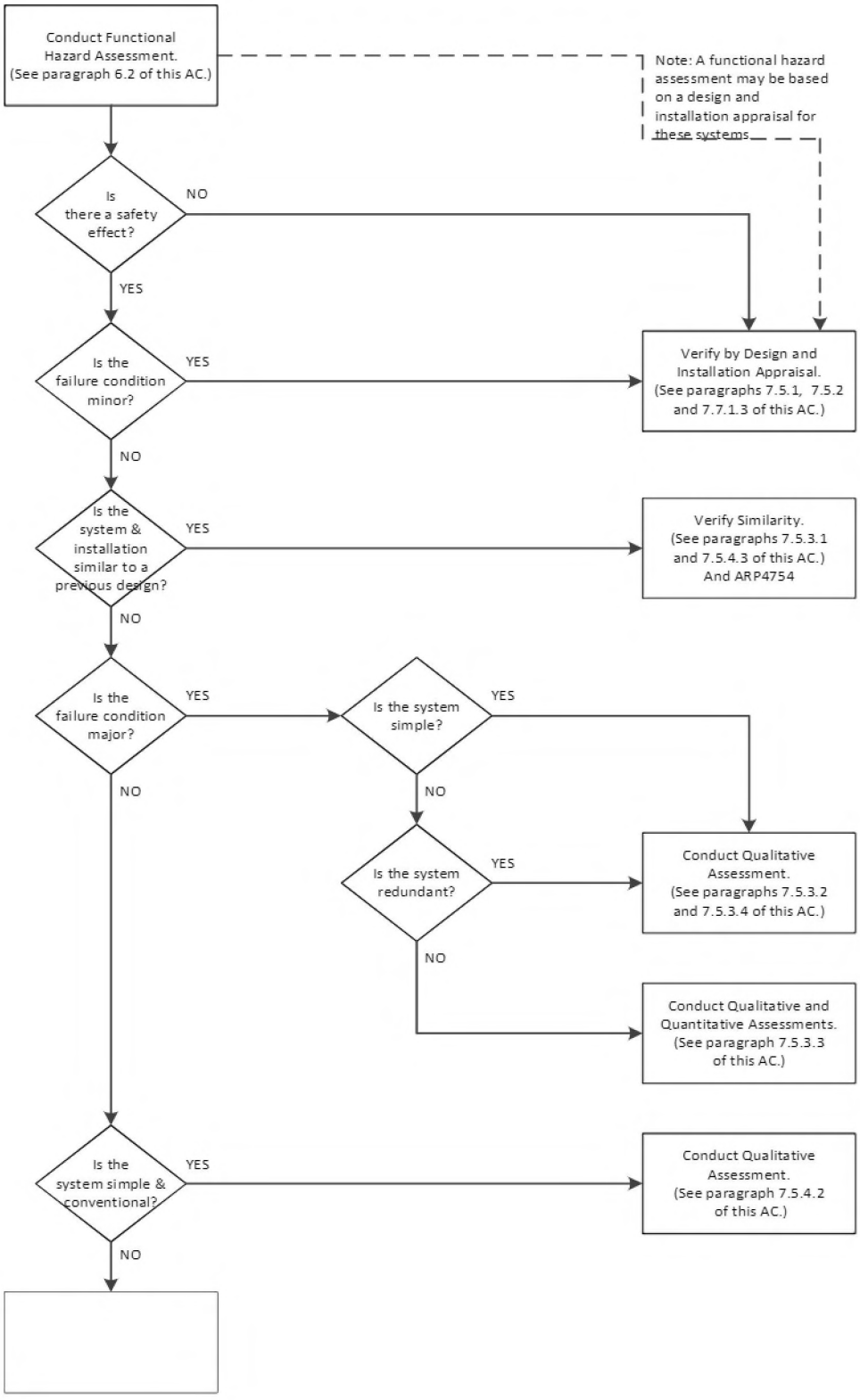
C.2.3.1 If the system is not complex and its relevant attributes are similar to those of systems used on other airplanes, the identification and classification may be derived from design and installation appraisals and the service experience of the comparable, previously approved systems.

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).**

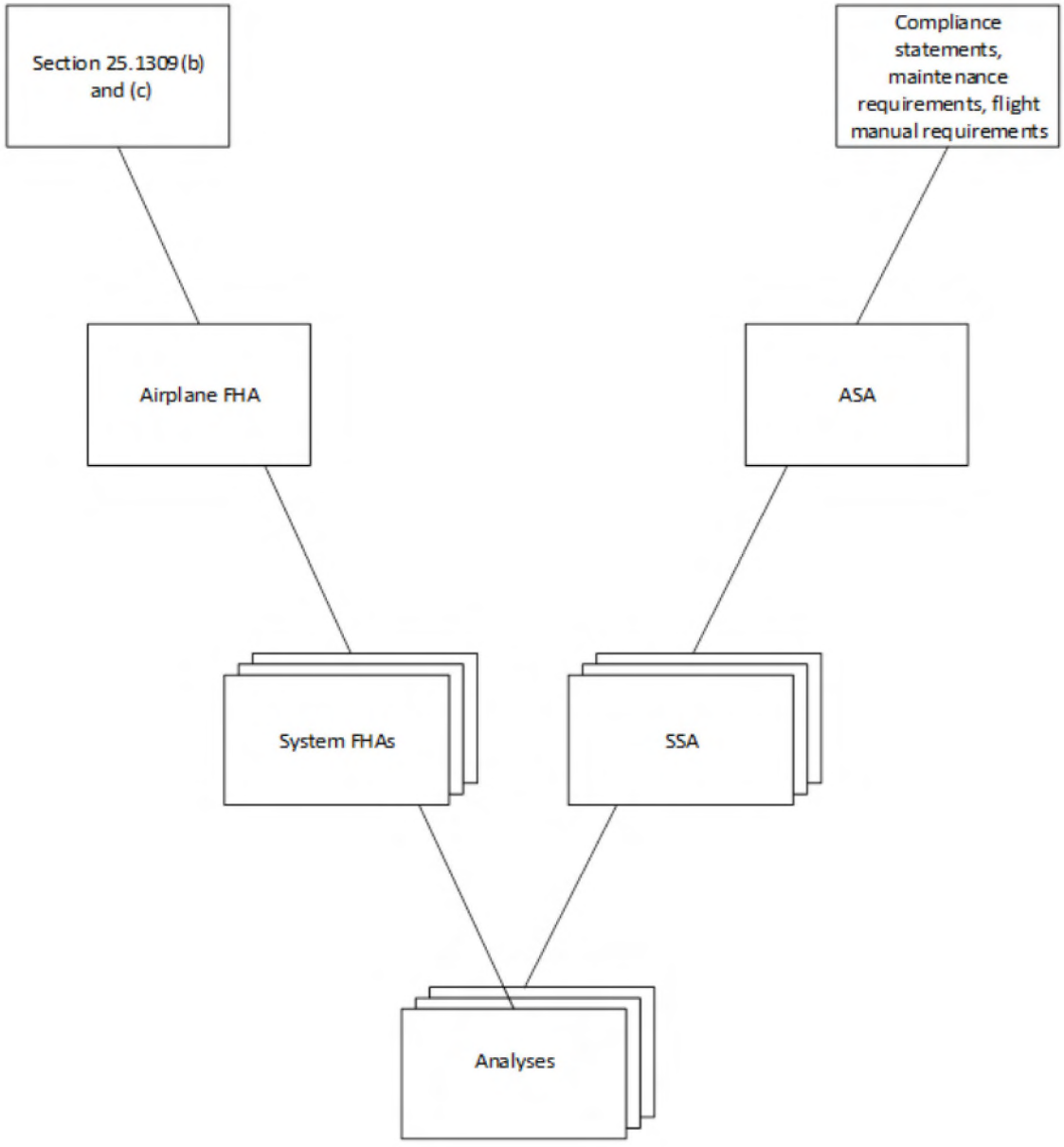
A systematic, comprehensive evaluation of the design implementation to verify it meets all applicable requirements. There are multiple SSAs, and typically one SSA for each system. The SSA may be preceded by a Preliminary System Safety Assessment (PSSA), which is used to evaluate the preliminary design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

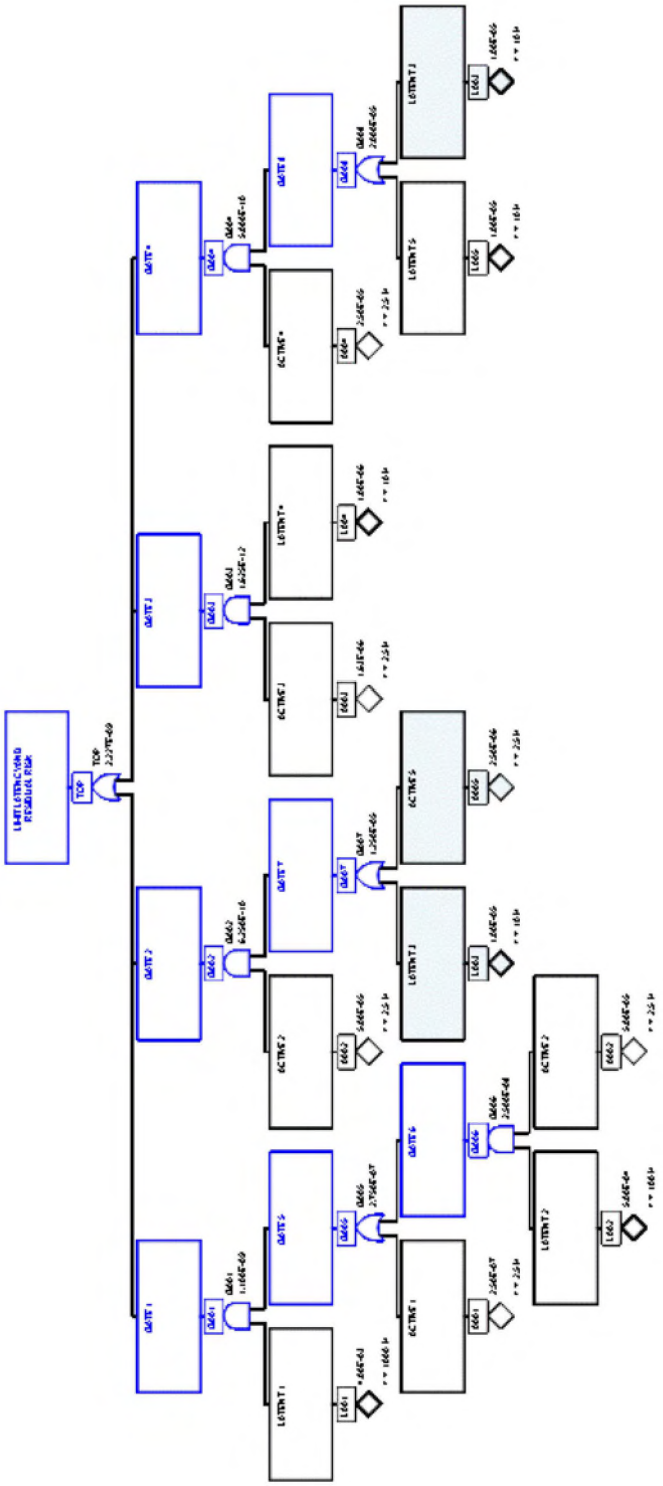


TABLE D-1. EXAMPLE OF CSL+1 IDENTIFICATION FOR § 25.1309(B)(5) COMPLIANCE

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 4×10^{-6} per flight 2.5×10^{-6} per flight hour
Flight condition resulting in a stall	In-service observation NLR-CR-2016-601	10^{-5} per flight 5×10^{-8} per flight 3×10^{-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 2×10^{-3} per flight 3×10^{-4} per flight hour
Flight condition greater than or equal to 1.5g due to gusts	NLR-CR-2003-554	7×10^{-3} per flight
Flight condition less than or equal to 0g	NLR-CR-2005-015	1×10^{-6} per flight 4×10^{-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: $\sum_{k=1}^{N} P_{flight\ k}\,(failure\ condition\ in\ flight\ k)\ is\ equal\ to\ P_{flight}(failure\ by\ end\ of\ flight) = P_{prior}(failure\ prior\ to\ flight) + P_{flight}(failure\ in\ flight)$

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

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

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

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: _____