U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: EQUIPMENT, SYSTEMS, AND INSTALLATIONS IN PART 23 AIRPLANES

Date: 7/28/95
Initiated by: ACE-100

AC No: 23.1309-1B
Change:

1. PURPOSE. This advisory circular (AC) provides guidance and information for an acceptable means, but not the only means for showing compliance with the requirements of § 23.1309(a) and (b) (amendment 23-41) of the Federal Aviation Regulations (FAR), for equipment, systems, and installations in part 23 airplanes. This material is neither mandatory nor regulatory in nature and does not constitute a regulation.

2. CANCELLATION. AC 23.1309-1A, Equipment, Systems, and Installations in Part 23 Airplanes, dated June 3, 1992, and Change 1 to AC 23.1309-1A, dated August 5, 1992, are canceled.

3. RELATED REGULATIONS AND DOCUMENTS.

a. Regulations. Sections 23.1301 and 23.1309 of part 23 of the Federal Aviation Regulations (FAR) (through amendment 23-41).

b. Advisory Circulars and Notices. The AC's listed below can be obtained from the U.S. Department of Transportation, General Services Section, M-443.2, Washington, D.C. 20590:

AC 21-16C	Radio Technical Commission for Aeronautics Document DO-160C
AC 20-115B	RTCA, Inc., Document RTCA/DO-178B
AC 20-136	Protection of Aircraft Electrical/ Electronic Systems Against the Indirect Effects of Lightning
AC 25.1309-1A	System Design and Analysis
N 8110.53	Transition to RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification"

c. Industry Documents.

(1) The RTCA documents listed below are available from the RTCA, Inc., 1140 Connecticut Avenue, N.W., Suite 1020, Washington, D.C. 20036-4001:

RTCA/DO-160C	Environmental Conditions and Test Procedures for Airborne Equipment
RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certification

(2) The SAE documents listed below are available from the Society of Automotive Engineers (SAE), Inc., 400 Commonwealth Drive, Warrendale, PA 15096-0001:

ARP 926A	Fault/Failure Analysis Procedure
ARP 1834	Fault/Failure Analysis for Digital Systems

d. Related Reading Material. A comprehensive discussion on lighting protection, with additional nonregulatory guidance information, is available in the current edition of FAA Report DOT/FAA/CT-89/22, "Aircraft Lightning Protection Handbook," dated September 1989. This document is available to the public by ordering it through the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, Virginia 22161.

4. APPLICABILITY.

a. This AC is generally applicable only to the original applicant seeking issuance of type certificate (TC), amended type certificate (ATC), and supplemental type certificate (STC) for the initial approval of the new type design or a change in the type design. This document addresses general applicability, and it should not be utilized to replace any specific guidance intended for individual types of equipment, systems, and installations. Because § 23.1309 is a regulation of general requirements, it should not be used to supersede any specific requirements of part 23.

b. Section 23.1309 does not apply to the performance, flight characteristics, and structural loads and strength requirements of subparts B and C; but it does apply to any system on which compliance with the requirements of subparts B and C is based. For example, it does not apply to an airplane's inherent stall characteristics or their evaluation of § 23.201, but it does apply to a stick pusher (stall barrier) system used to enable compliance with § 23.201.

c. Section 23.1309 is applicable to the installation of all airplane systems and equipment including pneumatic systems, fluid systems, electrical/electronic systems, mechanical systems, and powerplant systems included in the airplane design except for the following:

(1) Systems approved as part of a type-certificated engine or propeller and whose malfunction or failure could have no adverse effect on other airplane systems or equipment.

(2) The flight structure (such as wings, fuselage, empennage, control surfaces, mechanical flight control cables, pushrods, control horns, engine mounts, and structural elements of the landing gear) whose requirements are specified in subparts C and D of part 23.

5. BACKGROUND.

a. Prior to amendment 23-14 to part 23 of the FAR (effective December 20, 1973), neither part 3 of the Civil Air Regulations (CAR) nor part 23 of the FAR contained safety requirements for equipment, systems, and installations for small airplanes. In 1968, the Federal Aviation Administration (FAA) instituted an extensive review of the airworthiness standards of part 23. Because of the increased use in all weather operations and the increased reliance on systems and equipment in part 23 airplanes, the FAA promulgated § 23.1309 to provide for an acceptable level of reliability for such equipment, systems, and installations in the interest of safety. When § 23.1309 (amendment 23-14) was adopted, it was not envisioned that systems, which perform critical functions, would be installed in small airplanes; therefore, prior to amendment 23-14, this section did not contain adequate safety standards for evaluating critical functions. When such equipment, systems, and installations

were included in the airplane design, they were evaluated under special conditions in accordance with the procedures of part 21 of the FAR.

b. With the adoption of amendment 23-34 (effective February 17, 1987), § 23.1309 was expanded to include certification of commuter category airplanes. This expansion added a requirement to ensure that applicable systems and installations are designed to safeguard against hazards and also added requirements for equipment identified as essential loads and affected power sources.

c. With the adoption of amendment 23-41 (effective November 26, 1990), § 23.1309 retained the existing reliability requirements adopted by amendment 23-14 for airplane equipment, systems, and installations that are not complex and do not perform critical functions. For those cases where the applicant finds it necessary or desirable to include complex systems and/or systems that perform critical functions, amendment 23-41, § 23.1309, provided additional requirements for identifying such equipment, systems, and installations and provided additional requirements needed for their certification. This amendment permitted the approval of more advanced systems having the capability to perform critical functions.

d. Qualitative and quantitative analyses are often used in assessing the acceptability of complex designs that have a high degree of integration, that use new technology or new or different applications of conventional technology, or that perform critical functions. These assessments led to the selective use of quantitative analyses to support experienced engineering and operational judgment and to supplement qualitative analyses and tests. Numerical probability ranges, associated with the terms used in § 23.1309(b), are accepted for evaluating the quantitative analyses that have a logical and acceptable inverse relationship between the probability and severity of each failure condition.

6. DEFINITIONS.

a. Adverse Effects. A response of a system that results in an undesirable operation of an aircraft system or subsystem.

b. Adverse Operating Conditions. A set of circumstances in which a failure or other emergency situation results in a significant increase in flight crew workload.

c. Attribute. A feature, characteristic, or aspect of a system or a device, or a condition affecting its operation. Some examples would include design, construction, technology, installation, functions, applications, operational uses, environmental and operational stresses, and relationships with other systems, functions, and flight or structural characteristics.

d. Complex. A system is considered to be complex if it is characterized by a very complicated or involved arrangement of parts, units, etc., and a very methodical and organized method of analysis is needed for a valid safety assessment. Failure modes and effects and fault tree analyses are examples of such methods.

e. Continued Safe Flight and Landing. This phrase means that the airplane is capable of continued controlled flight and landing, possibly using emergency procedures but without requiring exceptional pilot skill or strength. Some airplane damage may occur as a result of the failure condition or upon landing.

f. Conventional. An attribute of a system is considered to be conventional if it is the same as, or closely similar to, that of previously-approved systems that are commonly used. The systems have established adequate service history and the means of compliance for approval are generally accepted.

g. Critical Function. A function whose failures would prevent the continued safe flight and landing of the airplane. See note under definition of failure condition.

h. Equipment Essential to Safe Operation. Equipment installed in order to comply with the applicable certification requirements of part 23 or operational requirements of parts 91 and 135.

i. Equipment Not Essential to Safe Operation. Equipment whose failure or malfunction would not have any appreciable impact on the safe operation of the airplane. The following are typical of this equipment:

(1) Galley and entertainment equipment.

(2) Non-required heating and cooling equipment.

(3) Non-required equipment installed for completion of a specific mission, such as photography, medical evacuation, etc.

(4) Any other equipment whose functions have not been approved for fulfilling any airplane certification or operational requirements.

j. Essential Function. Function whose failure would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions. See note under definition of failure condition.

k. Essential Load. Equipment essential to safe operation that requires a power source for normal operation.

l. Extremely Improbable. For qualitative assessments, this term describes failures or malfunctions that are so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type. For quantitative assessments, this term describes failures or malfunctions having a probability of occurrence on the order of 1×10^{-9} or less.

m. Failure. A loss of function or a malfunction of a system.

n. Failure Condition. The effects on the airplane and its occupants, both direct and consequential, caused or contributed to by one or more failures, considering relevant adverse operational or environmental conditions. Failure conditions may be classified according to their severities as follows:

(1) Minor. Failure conditions which would not significantly reduce airplane safety, and which involve flight crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in flight crew workload, such as routine flight plan changes, or some inconvenience to occupants.

(2) Major. Failure conditions which would reduce the capability of the airplane or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be, for example:

(i) Major. A significant reduction in safety margins or functional capabilities, a significant increase in flight crew workload or in conditions impairing flight crew efficiency, or some discomfort to occupants; or

(ii) Severe-Major. In more severe cases, a large reduction in safety margins or functional capabilities, higher workload or physical distress such that the flight crew could not be relied on to perform its tasks accurately or completely, or adverse effects on occupants.

(3) Catastrophic. Failure conditions which would prevent continued safe flight and landing.

NOTE: For information, these terms may have the following relationships to the terms used in other documents that classify failure conditions: failure conditions adversely affecting non-essential functions could be minor; failure conditions adversely affecting essential functions could be major; and failure conditions adversely affecting critical functions could be catastrophic.

o. Hazard. Any condition which compromises the overall safety of the airplane or which significantly reduces the ability of the flight crew to cope with adverse operating conditions.

p. Hazard Assessment. The logical systematic examination of a system to identify and classify potentially hazardous failure conditions and to describe them in functional and operational terms.

q. Improbable. For qualitative assessments, this term describes failures or malfunctions that are not anticipated to occur during the entire operational life of a single random airplane of one type. However, they may occur occasionally during the entire operational life of all airplanes. For quantitative assessments, this term is descriptive of a probability on the order of 1×10^{-5} or less, but greater than a probability on the order of 1×10^{-9}.

r. Malfunction. Failure of a system, subsystem, unit, or part to operate in the normal or usual manner.

s. Minimize. To reduce, lessen, or diminish a hazard to the least practical amount with current technology and materials. The least practical amount is that point at which the effort to further reduce a hazard significantly exceeds any benefit, in terms of safety, derived from that reduction. Additional efforts would not result in any significant improvements of reliability.

t. Power Source. A system that provides power to installed equipment. This system would normally include prime mover(s),

required power converter(s), energy storage device(s), and required control and interconnection means.

u. Probable. For qualitative assessments, a probable malfunction or failure is any single malfunction or failure which is expected to occur one or more times during the entire operational life of any single airplane of a specific type. This may be determined on the basis of past service experience with similar components in comparable airplane applications. For quantitative assessments, this term describes a probability on the order of greater than 1×10^{-5}.

v. Qualitative. Those analytical processes that assess system and airplane safety in a subjective, non-numerical manner.

w. Quantitative. Those analytical processes that apply mathematical methods to assess system and airplane safety.

x. Redundancy. The existence of more than one independent means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical.

y. Reliability. The determination that a system, subsystem, unit, or part will perform its intended function for a specified interval under stated operational and environmental conditions.

z. Similarity. The process of claiming that the equipment type, form, function, design, and installation are nearly identical to already approved equipment. The reliability and operational characteristics and other qualities should have no appreciable affects on the airworthiness of the installation.

7. APPLICATION OF § 23.1309 AS ADOPTED BY AMENDMENT 23-14.

a. The airworthiness standards in § 23.1309(a) as amended by amendment 23-41 were originally adopted by amendment 23-14, and they are based on single-fault or fail-safe concepts and experience based on service-proven designs and engineering judgment. Paragraphs (a), (a)(1), (a)(2), and (a)(3) of § 23.1309, as amended by amendment 23-41, are derived from paragraphs (a), (b), and (c) of § 23.1309, as amended by amendment 23-14. The requirements in § 23.1309(a) are generally used for equipment systems and installation that are not complex and/or whose failure conditions are not classified as catastrophic or severe-major. Section 23.1309(a) is appropriate for systems used for airplanes approved to fly VFR and/or IFR, and for

systems where analysis by single-fault or fail-safe concepts and experience based on service-proven designs and engineering judgments. A design safety assessment is not necessary, but it may be used.

b. In order to show compliance with the requirements of § 23.1309(a) (amendment 23-41), it will be necessary to verify that the installed systems and equipment will cause no unacceptable adverse effects and also verify that the airplane is adequately protected against any hazards that could result from probable malfunctions or failures. A probable malfunction or failure is any single malfunction or failure that is considered probable on the basis of past service experience and/or analysis with similar components in comparable airplane applications. Multiple malfunctions or failures should be considered probable when the first malfunction or failure would not be detected during normal operation of the system, including preflight checks, or if the first malfunction or failure would inevitably lead to other malfunctions or failures. Equipment, systems, and installations should be analyzed, inspected, and tested to ensure compliance with the requirements of § 23.1309. A step-by-step diagram to comply with § 23.1309(a) is shown in figure 1 and these steps are listed below:

(1) Evaluate all airplane systems and equipment in order to determine whether they are:

(i) Essential to safe operation; or

(ii) Not essential to safe operation.

(2) Determine that operation of installed equipment has no unacceptable adverse effects. This can be verified by applicable flight or ground checks as follows:

(i) If it can be determined that the operation of the installed equipment will not adversely affect equipment essential to safe operation, the requirements of § 23.1309(a)(1)(i) have been satisfied.

(ii) If it is determined that the operation of the installed equipment has an adverse effect on equipment not essential to safe operation and a means exists to inform the pilot of the effect, the requirements of § 23.1309(a)(1)(ii) have been met. An acceptable means to inform the pilot would include any visual or

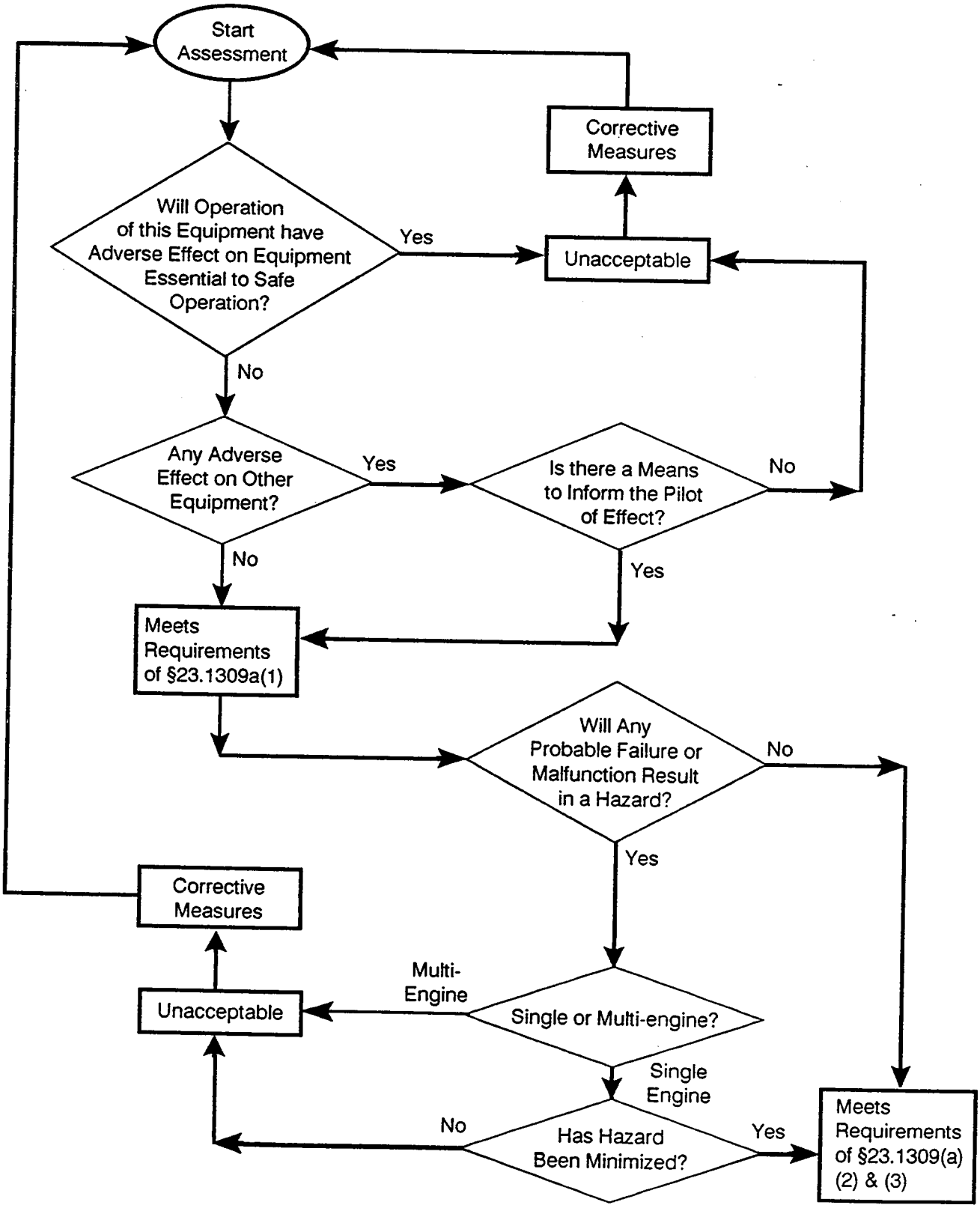

FIGURE 1 - METHOD TO COMPLIANCE DIAGRAM OF §23.1309(a)

aural method (flags, lights, horns, loss of display, etc.) that will indicate to the pilot that the affected system is not performing properly.

(3) Determine that failure or malfunction of the installed equipment could not result in unacceptable hazards.

(i) All equipment should be evaluated for general installation hazards. These types of hazards would normally include those hazards that would directly compromise the safety of the airplane or its occupants, such as fire, smoke, explosion, toxic gases, depressurization, etc. A hazard could also result from loss of essential equipment or systems when minimum required functions are lost. Individual failure of redundant equipment would not necessarily be considered a hazard. For example, the single failure of either communication transceiver or a navigation receiver (but not both) during IFR operation is not considered a hazard; however, a single failure of a common power supply to those systems would be considered a hazard.

(ii) Systems and equipment essential to safe operation should also be assessed for probability of malfunction or failure if loss of required functions could result in a hazard. Where the installation is conventional and where there is a high degree of similarity in installations and a significant amount of service history is available for review, this determination can be an engineering judgment. If the installation is not similar in its relevant attributes, it should be evaluated in more detail by a qualitative assessment as described in paragraph 9b(3).

(iii) Hazards that have been identified and found to result from probable failures are not acceptable in multiengine airplanes. In these situations, some design changes may be required to remove the hazard or reduce the probability of failure, such as increasing redundancy, substitution of more reliable equipment, annunciation, etc.

(iv) If it has been determined that a probable failure or malfunction could result in a hazard to a single engine airplane, that hazard should be minimized. To sufficiently minimize a hazard, all appropriate means to reduce the hazard should be exhausted with current technology and materials. The means to minimize the hazard should provide the level of safety intended by the applicable airworthiness requirements of the certification basis.

Safety, similarity, conventionality, technical feasibility, and benefits should be taken into account. These efforts may become impractical; that is, additional effort may not result in any significant improvement of reliability. This determination should be an experienced engineering judgment, based on the criticality of the hazard and the intended kinds of operation.

8. APPLICATION OF § 23.1309(d) AS ADOPTED BY AMENDMENT 23-34.

a. The commuter category requirements of § 23.1309(d) as adopted by amendment 23-34 for commuter airplanes were inadvertently not incorporated in § 23.1309 as adopted by amendment 23-41. However, these requirements are still applicable for those commuter airplanes that include the certification basis of amendment 23-34 (which requires all applicable systems and installations to be designed to safeguard against hazards to the airplane in the event of their failure).

b. Design features should be taken into account to safeguard against hazards by ensuring the failure condition will not occur or by having redundancy or annunciation with the associated flight crew corrective action. The reliability is such that independent failures of the redundant systems are not likely to occur during the same flight. If a redundant system is required, a probable failure in one system should not adversely affect the other system operation. No probable failure in a system should result in a safe indication of an unsafe condition of flight so the system would be used or inadvertently put into operation. When the unsafe condition is annunciated or detected, the Airplane Flight Manual (AFM) should have clear and precise corrective procedures for handling the failure without an excessive increase in workload.

c. Service history for similar installation may be utilized to meet part or all of this requirement if a system or installation has been previously approved and has significant and favorable service history in similar aircraft environments. The claim of similarity should be based on equipment type, function, design, and installation similarities and other relevant attributes.

9. APPLICATION OF § 23.1309(b) AS ADOPTED BY AMENDMENT 23-41.

a. Application of § 23.1309(b) is for equipment, systems, and installation that are complex and/or whose failure conditions are catastrophic for all types of airplanes and, generally, whose

failure conditions are severe-major for those airplanes not limited to VFR conditions. These systems should be evaluated by performing a design safety assessment.

b. Design Safety Assessments. The applicant is responsible for identifying and classifying each failure condition and choosing the methods of safety assessment. The applicant should then obtain early concurrence of the cognizant certificating office on the failure conditions, their classifications, and the choice of an acceptable means of compliance. Figure 2 provides an overview of the information flow to conduct a design safety assessment. This figure is a guide and it does not include all information provided in this AC.

(1) A functional hazard assessment (FHA) is a useful preliminary step to identify and classify potentially-hazardous failure conditions, and to describe them in functional and operational terms. An FHA is qualitative and is conducted using service experience, experienced engineering, and operational judgment. All applicable engineering disciplines, such as systems, structures, propulsion, and flight test, should be involved in the identification and classification of failure conditions. An FHA is often used by applicants as a preliminary engineering tool to help determine the acceptability of a design concept, to identify potential problem areas or desirable design changes, or to determine the need for and scope of any additional analyses.

(2) An assessment to identify and classify failure conditions is generally 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 simple report that interprets test results 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 system failure conditions, and whether or not the system is complex. Failure conditions should be classified according to their severities as minor, major, or catastrophic as defined in paragraph 6.

(i) The classification of failure conditions does not depend on whether or not a system or function is required by any specific regulation. Some systems required by specific regulations, such as transponders, position lights, and public address systems,

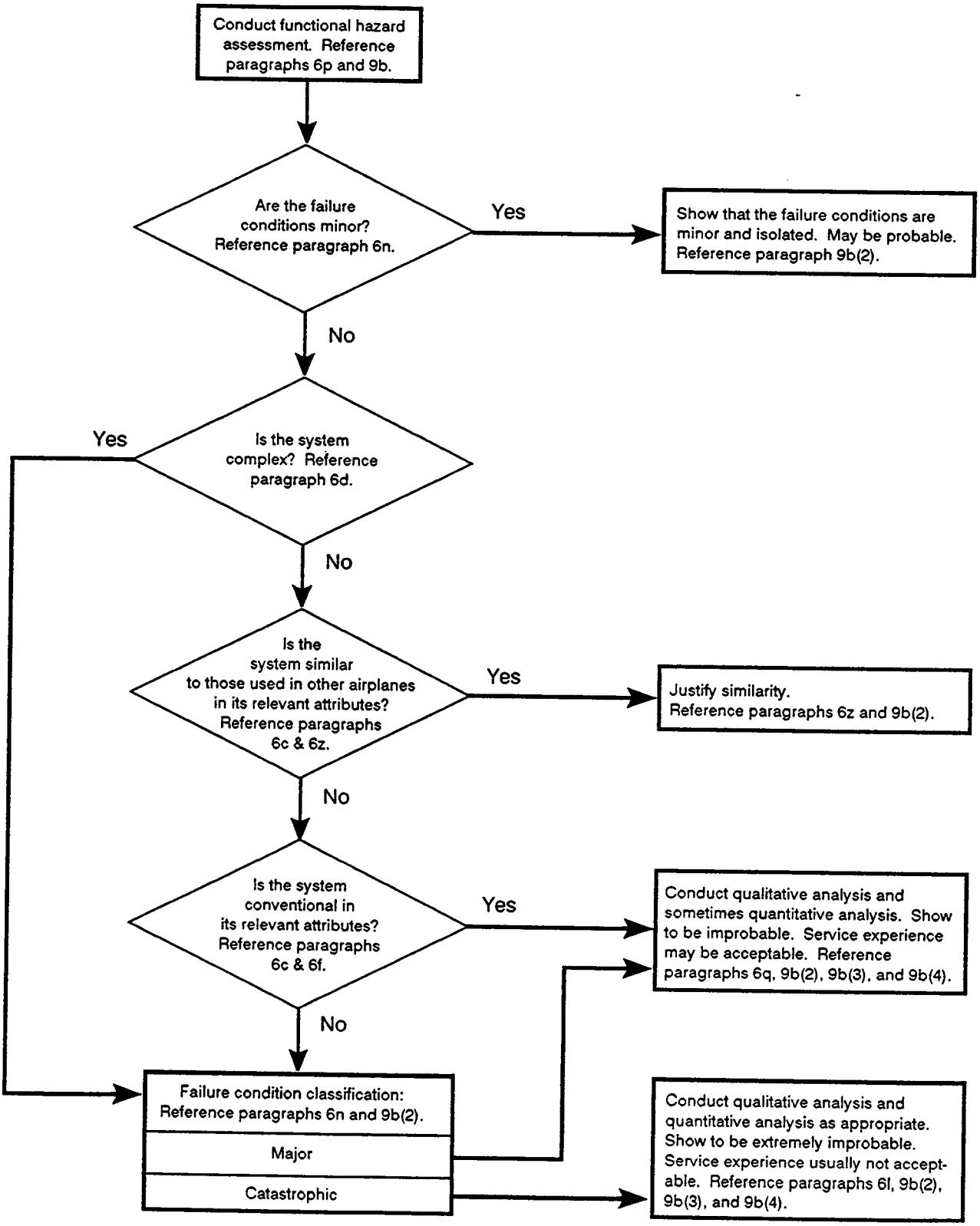

FIGURE 2 - DESIGN SAFETY ASSESSMENT FLOWCHART

may have the potential for only minor failure conditions. Conversely, other systems not required by any specific regulation, such as flight management systems and automatic landing systems, may have the potential for major or catastrophic failure conditions.

(ii) The classification of failure conditions should consider all relevant factors. Examples of factors would include the nature of the failure modes, system degradation, flight crew actions, flight crew workload, performance degradation, reduced operational capability, effects on airframe, etc. It is particularly important to consider factors that would alleviate or intensify the severity of a failure condition. An example of an alleviating factor would be the continued performance of identical or operationally-similar functions by other systems not affected by a failure condition. Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a failure condition, such as weather or other adverse operational or environmental conditions, or failures of other unrelated systems or functions.

(iii) Analysis of Minor Failure Conditions. Minor failure conditions may be probable. An analysis should consider the effects of system failures on other systems or their functions. The analysis is complete if it shows that system failures would cause only minor failure conditions. In general, the system does not perform airworthiness-related functions, and the common design practice provides physical and functional isolation from airworthiness-related components.

(iv) Analysis of Major Failure Conditions. Major failure conditions should be shown to be improbable.

(A) An assessment using experienced engineering and operational judgment is often sufficient. Compliance may also be shown by qualitative analysis. A quantitative analysis is sometimes used to support experienced judgment and to supplement qualitative analysis for the more severe-major failure conditions.

(B) If the installation is not complex but similar in its relevant attributes, a design and installation appraisal with satisfactory service experience will usually be acceptable for showing compliance. If the installation is not complex and similar, but the system is conventional in its relevant attributes, compliance may be shown by a qualitative assessment.

(C) 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, a failure modes and effects analysis or a fault tree analysis is often used to show that isolation actually exists (that is, any single failure would not cause the failure of a function in more than one redundant system channel) and to show that the failure modes of the system do not have any adverse effects on safety-related functions performed by other systems.

(v) Analysis of Catastrophic Failure Conditions. Catastrophic failure conditions should be shown to be extremely improbable. A very thorough safety assessment is necessary.

(A) The assessment usually consists of an appropriate combination of qualitative and quantitative analyses.

(B) In limited cases, using experienced engineering and operational judgment could be sufficient for conventional systems that have similar attributes and are not complex when service experience data shows no potentially catastrophic failure.

(C) In general, a failure condition resulting from a single failure mode of a device cannot be accepted as being extremely improbable. In very unusual cases, however, experienced engineering judgment may enable an assessment that such a failure mode is not a practical possibility. The assessment's logic and rationale should be so straightforward and obvious that the failure mode simply would not occur unless it is associated with an unrelated failure condition that would itself be catastrophic.

(3) Methods for qualitatively assessing the causes, severity, and likelihood of potential 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. Descriptions of typical types of analysis are provided below:

(i) Design Appraisal. A qualitative appraisal of the integrity and safety of the design, such as, the effective use of design techniques that would prevent single failures from adversely affecting redundant systems. An effective appraisal requires experienced judgment.

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

(iii) Failure Modes and Effects Analysis (FMEA). A structured, inductive, bottom-up analysis, which is used to evaluate the effects on the system and the airplane of each possible element or component failure. When properly formatted, it should aid in identifying latent failures, and the possible causes of each failure mode. For some equipment that has an enormous number of failure modes, a thorough, accurate, and dependable analysis by FMEA may not be feasible.

(iv) Fault Tree Analysis. Structured, deductive, top-down analyses, which are 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 is usually used as the source document for those primary failures or other events. A fault tree analysis is failure-oriented and is conducted from the perspective of which failures would occur to cause a defined failure condition.

(4) A quantitative analysis may be used to support experienced engineering and operational judgment and to supplement qualitative analyses. A quantitative analysis is often used for catastrophic or severe-major failure conditions of systems that are complex, that have insufficient service experience to help substantiate their safety, or that have attributes that differ significantly from those of conventional systems.

(i) Probability Analysis may be a failure modes and effects analysis or fault tree analysis, which also includes numerical probability information. The probabilities of primary failures can be determined from failure rate data and exposure times, using failure rates derived from service experience on identical or similar items, or acceptable industry standards. Conventional mathematics of probability can then be used to calculate the estimated probability of each failure condition as a function of the estimated probabilities of its identified contributory failures or other events.

(A) When calculating the estimated probability of each failure condition, a margin may be necessary to account for uncertainty. A margin is not normally required for an analysis that is based on proven data or from operational experience and tests. Where data has limited background for substantiation, a margin may be required depending on the available justification.

(B) Because the improbable range is broad, the applicant should obtain early concurrence of the cognizant certificating office of an acceptable probability for each major failure condition. Unless acceptable probability criteria are provided elsewhere, such as in other AC's, acceptable probabilities for failure conditions should be derived from complete event scenarios leading to an inability for continued safe flight and landing.

10. OPERATIONAL AND MAINTENANCE CONSIDERATIONS. Flight crew and ground crew tasks related to compliance should be appropriate and reasonable. Quantitative assessments of the probabilities of flight crew errors are not considered feasible. Reasonable tasks are those for which full credit can be taken because the flight crew or ground crew can realistically be anticipated to perform them correctly when they are required or scheduled. In addition, based on experienced engineering and operational judgment, the discovery of obvious failures during normal operation and maintenance of the airplane may be considered, even though such failures are not the primary purpose of focus of the operational or maintenance actions.

a. Flight Crew Action. When assessing the ability of the flight crew to cope with a failure condition, the warning information, the crew capability of determining the faults, and the complexity of the required action should be considered.

(1) Annunciation that requires flight crew actions should be evaluated to determine if the required actions can be accomplished in a timely manner without exceptional pilot skills. If the evaluation indicates that a potential failure condition can be alleviated or overcome during the time available without jeopardizing other safety related flight crew tasks, and without requiring exceptional pilot skill or strength, credit may be taken for correct and appropriate corrective action, for both qualitative and quantitative assessments. Similarly, credit may be taken for

correct flight crew performance if overall flight crew workload during the time available is not excessive, and if the tasks do not require exceptional pilot skill, or strength.

(2) Unless flight crew actions are accepted as normal airmanship, the appropriate procedures should be included in the FAA-approved AFM, or AFM revision, or supplement. The AFM should include procedures for operation of complex systems such as integrated flight guidance and control systems. These procedures should include proper pilot response to cockpit warnings, diagnosis of system failures, discussion of possible pilot-induced flight control system problems, and use of the system in a safe manner.

b. Ground Crew Action. Credit may be taken for correct ground crew accomplishments for both qualitative and quantitative assessments. Such requirements should be provided for use in FAA-approved maintenance programs.

11. ELECTROMAGNETIC PROTECTION FOR ELECTRICAL/ELECTRONIC SYSTEMS. Current trends indicate increasing reliance on electrical/electronic systems for safe operations. For systems that perform flight, propulsion, navigation, and instrumentation functions, electromagnetic effects should be considered.

a. High Intensity Radiated Fields (HIRF). The words "radio frequency energy" in § 23.1309(e) are not intended to include HIRF; therefore, special conditions must be issued until the HIRF requirements in a final rule are incorporated in part 23 of the FAR's. These special conditions are applicable for systems that perform functions whose failure to provide that function correctly could lead to a catastrophic failure condition.

b. Lightning Protection.

(1) Section 23.1309(e) contains the regulatory requirements for the protection of aircraft electrical/electronic systems against the indirect effects of lightning. These requirements are applicable for electrical/electronic functions whose failure conditions are classified as catastrophic, severe-major, or major effect. For guidance, AC 20-136, "Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning," dated March 5, 1990, and RTCA/DO-160C, section 22, "Lightning Induced Transient Susceptibility," Change No. 2, dated June 19, 1992, or subsequent revisions, provide acceptable methods

and procedures for determining compliance with the indirect effects of lightning requirements. AC 20-136 provides guidance to verify the protection of systems installed in an aircraft, while section 22 of RTCA/DO-160C provides methods to qualify equipment prior to installation in an aircraft.

(2) Functions performed by systems whose failure conditions are classified as severe-major or major would require protection to the extent that the function should recover in a timely manner after the airplane has been exposed to the lightning. Testing and analysis are directed toward a component damage, that is, a damage tolerance test. Multiple stroke and multiple burst testing should not be required; therefore, the laboratory test procedures in RTCA/DO-160C are acceptable. A specific category or level of testing as defined in RTCA/DO-160C is not being given, but a simple analysis method by experienced engineering judgment is normally sufficient to determine the appropriate testing level. Systems that have been previously approved may be approved by similarity provided there has been no unresolved in-service history of problems relating to lightning strikes to the aircraft. The need for lightning protection for systems on aircraft limited to VFR operations is determined on a case-by-case study.

(3) Functions whose failure conditions are classified as catastrophic would require protection to the extent that the function should not be adversely affected when the airplane is exposed to lightning. These functions should continue to be provided during and after exposure to lightning. If the function is provided by multiple systems, then loss of a system or systems, during exposure of the airplane to lightning, should not result in the loss of the function. After the airplane is exposed to lightning, each affected system that performs these functions should automatically recover normal operation, unless this conflicts with other operational or functional requirements of that system. Multiple stroke and multiple burst testing and/or analysis usually should not be required for damage assessment, but they can be the primary factor in a system functional upset.

(4) Appendix 3 of AC 20-136, "Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning," defines total lightning environment, including the multiple stroke and multiple burst lightning environment to be used for test and analysis purposes in qualifying systems and equipment for lightning protection. AC 20-136 is proposed as a basis to use in demonstrating compliance with the lightning protection

requirements except for the multiple burst lightning environment, which has been changed to agree with recommendations from the Society of Automotive Engineers (SAE) AE4L Committee dated July 6, 1992. The multiple burst lightning environment that is defined in AC 20-136 has been changed from 24 bursts to 3 bursts and it is mainly used for test and analysis of system functional upset.

12. SOFTWARE QUALIFICATION FOR AIRBORNE SYSTEM AND APPLICATIONS. AC 20-115B, "RTCA, Inc., Document RTCA/DO-178B," dated January 11, 1993, discusses how RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992, provides an acceptable means for showing that software complies with pertinent airworthiness requirements. N 8110.53, Transition to RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated September 29, 1994, provides guidelines in applying RTCA/DO-178B.

a. Software Assessment. The applicant should perform the safety assessment process to determine the software levels as defined in RTCA/DO-178B. RTCA/DO-178B defines five software levels which are based upon the contribution of software to potential failure conditions as determined by the system safety assessment process. The classification of failure conditions and the software levels are related as shown below:

Failure Conditions	Software Levels
Catastrophic	A
Severe-Major	B
Major	C
Minor	D
No Effect	E

Compliance to a software level provides assurance that software errors have been eliminated to a degree of confidence appropriate for the failure condition. It does not imply a numerical probability of errors remaining, nor numerical failure rate for the software.

b. Use of RTCA/DO-178.

(1) The applicant may continue to use RTCA/DO-178 or RTCA/DO-178A as a means of compliance for software modifications on the same aircraft installation. Applicants may continue to use

RTCA/DO-178 or RTCA/DO-178A for software modifications to an appliance that will be installed on a different aircraft if the guidelines of RTCA/DO-178B, section 12, are satisfied. For software developed prior to the availability of RTCA/DO-178B, section 12.1.4 of RTCA/DO-178B provides applicants with a method for upgrading a baseline for software development so that changes can be made in accordance with the criteria contained in RTCA/DO-178B.

(2) If software was developed using RTCA/DO-178A procedures, the applicant may need to further evaluate some features of the software. RTCA/DO-178A does not address some applications of digital technology commonly found in airborne systems and applications, for example, user-modifiable software; option-selectable software; software development and verification tools; or previously developed software. In these cases where RTCA/DO-178A does not provide adequate procedures, the applicant should include in the software aspects of a certification plan the means for showing that these features comply with pertinent airworthiness requirements. One acceptable means for demonstrating such features comply with the pertinent airworthiness requirements is to comply with pertinent portions of the criteria contained in RTCA/DO-178B, which would supplement the basic criteria contained in RTCA/DO-178A.

GERALD W. PIERCE
Acting Manager, Small Airplane Directorate
Aircraft Certification Service

U.S. Department
of Transportation

**Federal Aviation
Administration**

800 Independence Ave., S.W.
Washington, D.C. 20591

**FORWARDING AND RETURN
POSTAGE GUARANTEED**

Official Business
Penalty for Private Use $300

BULK MAIL
POSTAGE & FEES PAID
FEDERAL AVIATION
ADMINISTRATION
PERMIT NO. G-44