U.S. Department
of Transportation
Federal Aviation Administration

Advisory Circular

Subject: SYSTEM SAFETY ANALYSIS AND ASSESSMENT FOR PART 23 AIRPLANES

Date: 11/17/2011
Initiated by: ACE-100

AC No: 23.1309-1E

This advisory circular (AC) sets forth an acceptable means of showing compliance with Title 14 of the Code of Federal Regulations (14 CFR), § 23.1309, through Amendment 23-62 for equipment, systems, and installations in 14 CFR part 23 airplanes.

This AC is not mandatory and does not constitute a regulation. It is issued for guidance purposes and to outline a method of compliance with the rules. An applicant may elect to follow an alternate method, provided the FAA finds it to be an acceptable means of complying with the applicable requirements of 14 CFR. However, if the applicant uses the means described in the AC, they must follow it in all important respects.

John Colomy

FOR Earl Lawrence
Manager, Small Airplane Directorate
Aircraft Certification Service

CONTENTS

Paragraph **Page**

1. What is the purpose of this AC?

a. This AC provides guidance and information for an acceptable means, but not the only means, for showing compliance with the requirements of § 23.1309 (Amendment 23-62) for equipment, systems, and installations in 14 CFR part 23 airplanes.

b. This material is neither mandatory nor regulatory in nature and does not constitute a regulation. It describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations. We will consider other methods of demonstrating compliance that an applicant may elect to present. While these guidelines are not mandatory, they are derived from extensive FAA and industry experience in determining compliance with the relevant regulations. Whenever an applicant’s proposed method of compliance differs from this guidance, the proposal should be coordinated with the Small Airplane Directorate Standards Staff, ACE-110. In addition, if an office believes that an applicant’s proposal that meets this guidance should not be approved, that office should coordinate its response with the Small Airplane Directorate Standards Staff, ACE-110.

c. Terms such as “must” are used in this AC only in the sense of ensuring applicability of this particular method of compliance when the acceptable method of compliance described herein is used**.** The word “must” is also used in this AC when referring to a specific regulation or guidance that is essential when the applicant uses this AC for the means of compliance. In this case there is no deviation. The word “should” is used to express a recommendation. Deviation from the specified recommendation may require justification.

2. Who does this AC apply to?

The guidance provided in this document is directed to airplane manufacturers, modifiers, foreign regulatory authorities, and Federal Aviation Administration (FAA) personnel. This AC is applicable only to the original applicant seeking issuance of a Type Certificate (TC), an Amended Type Certificate (ATC), a Supplemental Type Certificate (STC), or a Parts Manufacturer Approval (PMA) for the initial approval of the new type design or a change in the approved type design.

3. Cancellation.

This AC cancels AC 23.1309-1D, System Safety Analysis and Assessment for Part 23 Airplanes, dated January 16, 2009.

This AC supersedes PS-ACE100-2005-50001, “Applying AC 20-152, ‘RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware,’ to Title 14 Code of Federal Regulations, Part 23 Aircraft”; dated January 26, 2007

4. Related regulations and documents.

a. Regulations. Sections 23.1301 and 23.1309 of part 23 (through Amendment 23-62).

b. ACs, orders, and policy. You may access the latest version of ACs, notices, orders, and policy on the FAA website: www.faa.gov.

AC 20-115B	RTCA, Inc., Document RTCA/DO-178B
AC 20-136A	Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning
AC 20-138B	Airworthiness Approval of Positioning and Navigation Systems
AC 20-152	RTCA, Inc., Document RTCA/DO-254, “Design Assurance Guidance for Airborne Electronic Hardware”
AC 20-158	The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF) Environment
AC 21-16F	RTCA, Document DO-160 version D, E, and F , “Environmental Conditions and Test Procedures for Airborne Equipment”
AC 21.101-1A	Establishing the Certification Basis of Changed Aeronautical Products
AC 23-17C	Systems and Equipment Guide for Certification of Part 23 Airplanes and Airships
AC 23.1311-1C	Installation of Electronic Displays in Part 23 Airplanes
AC 25.1309-1A	System Design and Analysis
AC 33.75-1A	Guidance Material for 14 CFR 33.75, Safety Analysis
Order 8110.4C	Type Certification
Order 8110.105	Simple and Complex Electronic Hardware Approval Guidance

c. Industry documents. You may obtain copies of current editions of the following publications as listed. These documents are excellent resource materials.

(1) RTCA documents. The following RTCA documents are available from RTCA, Inc., Suite 805, 1828 L Street NW, Washington, DC 20036-4001 or at their website at www.rtca.org.

RTCA/DO-160G	Environmental Conditions and Test Procedures for Airborne Equipment

RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certification
RTCA/DO-254	Design Assurance Guidance for Airborne Electronic Hardware

(2) Society of Automotive Engineers (SAE), Inc. The following SAE, Inc., Aerospace Recommended Practice (ARP) documents are available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001 or from their website at www.sae.org.

ARP 4754A	Guidelines for Development of Civil Aircraft and Systems
ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Note: ARPs 4754A and 4761 provide guidelines and methods of performing the safety assessment for certification of civil aircraft. The guidelines in ARP 4754A were developed in the context of 14 CFR part 25. It may be applicable to other 14 CFRs, such as parts 23, 27, 29, 33, and 35.

This AC is not intended to constrain the applicant to the use of these documents in the definition of their particular methods of satisfying the objectives of this AC. However, these documents contain material and methods of performing the System Safety Assessment (SSA) that an applicant may choose to use. The guidance in this AC takes precedence over the recommended practices in these ARPs if there is a conflict. (See paragraph 21 for more guidance) Contact the Small Airplane Directorate if there are conflicts with other guidance or ACs and this AC.

5. Applicability.

a. In addition to specific part 23 design requirements, § 23.1309 requirements, except as identified below, are applicable to any equipment or system installed in the airplane. This section addresses general requirements and does not supersede any specific requirements contained in other part 23 sections. New advance technology in electrical, electronic, and mechanical systems designs that include complex electronics with software, complex hardware, HIRF, and/or lightning requires a § 23.1309 analysis. An SSA is required to determine the level of certitude for the processes in standard and guidance documents such as RTCA/DO-178B, RTCA/DO-254, AC 20-136A, and AC 20-158 or equivalent. Section 23.1309 should be used to determine failure condition, probability of failure condition, software Development Assurance Level (DAL), and complex hardware DALs shown in Figure 2. The safety assessment process is used to determine the failure condition classification, which determines the HIRF and lightning protection levels (reduced DALs in Figure 2 are not used). For simple and conventional mechanical or analog electromechanical systems, or both, with well-established design and certification processes (where the installation is not complex), safety analysis may be satisfied by a qualitative assessment such as the single-failure concept and experience based on service-proven designs and engineering judgment. In this case, a FHA, a design appraisal, and an installation appraisal addressed in this AC may satisfy § 23.1309 as shown in Figure 3.

b. Section 23.1309 does not apply to the performance, flight characteristics requirements of subpart B, and structural loads and strength requirements of subparts C and D. However, except as noted below, § 23.1309 does apply to systems that comply with subparts B, C, D, and E requirements. The flight structure such as wing, empennage, control surfaces and their simple systems; the fuselage, engine mounting, and landing gear and their related primary attachments are excluded. For example, § 23.1309 does not apply to an airplane's inherent stall characteristics or their evaluation of § 23.201, but does apply to a stick pusher (stall barrier) system installed to attain compliance with § 23.201. We will determine additional exceptions in the future. Until then, contact the Small Airplane Directorate for determination and approval of proposed exceptions not included in this AC.

c. Experienced engineering and operational judgment should be applied when determining whether or not a system is complex. Comparison with similar, previously approved systems is sometimes helpful. All relevant systems attributes should be considered. For example, the design may be complex, such as a satellite communication system used only by the passenger, but its failure may cause only minor safety effects.

6. Regulations and AC background.

a. Regulation.

(1) Amendment 23-14 (effective December 20, l973) adopted the original airworthiness standards in § 23.1309(a). Before amendment 23-14, neither the Civil Air Regulations (CAR) part 3, nor 14 CFR part 23, contained safety requirements in § 23.1309 for equipment, systems, and installations in small airplanes. In 1968, the FAA instituted an extensive review of the airworthiness standards of part 23. Because of the increased use of part 23 airplanes in all weather operations and the pilot’s increased reliance on installed systems and equipment, the FAA issued § 23.1309 to provide an acceptable level of safety for such equipment, systems, and installations. When the FAA adopted § 23.1309 (Amendment 23-14), it did not envision installation of systems that perform critical functions in small airplanes; therefore, before Amendment 23-41, this section did not contain 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 14 CFR part 21.

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

(3) Amendment 23-41 (effective November 26, 1990) retained in § 23.1309 the existing safety requirements adopted by amendment 23-14 for airplane equipment, systems, and installations that are not complex and that do not perform critical functions. For those cases where the applicant includes complex systems, or systems that perform critical functions, Amendment 23-41, § 23.1309, provides additional requirements for certification and identifying such equipment, systems, and installations. This amendment permitted the approval of more advanced systems having the capability to perform critical functions.

(4) Amendment 23-49 (effective March 11, 1996), amended § 23.1309(a)(4) to correct Amendment 23-41, which inadvertently removed the commuter category requirement originally added by Amendment 23-34 as § 23.1309(d).

(5) Amendment 23-62 consolidated and revised the existing requirements to reduce the certification burden. The FAA removed § 23.1301(d) and clarified the requirement in § 23.1309(a) to improve standardization for systems and equipment certification, particularly for non-required equipment and non-essential functions embedded within complex avionic systems. Section 23.1309(b) requires minor, major, hazardous, or catastrophic failure condition(s) that occur during certification testing have a root cause analysis and corrective action. Section 23.1309(c) updates the safety assessment process terminology. Amendment 23-62 also made § 23.1309(d) compatible with § 23.1322 (Warning, caution, and advisory lights) for the design of systems and controls, including indications and annunciations. The power source capacity and distribution requirements, which are not directly related to the other safety and analysis requirements from § 23.1309, Amendment 23-49, were moved to a new section in § 23.1310 with clarification.

(6) Qualitative and quantitative analyses are often used in assessing the acceptability of complex designs that have a high degree of integration, use new technology, are new or different applications of conventional technology, or are designs that perform critical functions. These assessments lead 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 are accepted for evaluating quantitative analyses that have a logical and acceptable inverse relationship between the probability and severity of each failure condition.

b. AC.

(1) AC Revisions.

(a) The revision from AC 23.1309-1B to AC 23.1309-1C on March 12, 1999, provided the four-tier certification classes with different criteria for probability of failures and software levels for systems. The purpose of this certification approach is to increase safety by enhancing equipment on General Aviation (GA) airplanes that facilitate new technologies.

(b) Since the issuance of AC 23.1309-1C, there has been a large number of electronic displays and electronic systems installed on part 23 airplanes, especially Primary Flight Displays (PFD), Multifunction Flight Displays (MFD), Integrated Flight Systems, and Synthetic Vision Systems (SVS). A study of the FAA Alaska Capstone demonstration program for new avionics systems technology determined that four-tier certification classes demonstrated significant operational safety benefit and reduced accident rates. These installations, especially on Class I and II airplanes, would have been too costly without the establishment of the four-tier certification classes of airplanes as shown in paragraph 15.

(2) Broad causes of fatal accidents. Accident rate is a function of many factors. These factors include human performance, weather, design, operation, training, maintenance, and airspace system infrastructure. For all airplanes, but particularly GA airplanes, pilot decision-making causes most accidents. Pilot decision-making accidents are often the result of a lack of situational awareness relative to terrain or weather, or to a loss of control due to excess workload. Correct pilot interventions and actions have prevented some of these accidents. Increases in avionics equipage rates that improve pilot situational awareness or simplify the task have a significant positive impact on the GA accident rate. The Aircraft Owners and Pilots Association, Air Safety Foundation, conducted a study of safety effects of glass cockpits and concluded that technologically advanced aircraft provide added situational awareness tools that have dramatically improved aspects of GA safety. Technologically advanced aircraft deliver multiple safety benefits to GA pilots, but pilot training tied to experience has to evolve with it.

(3) Installing affordable systems.

(a) Enhancing the quantity, quality, and presentation of situational data in the cockpit can improve pilot situational awareness, efficiency, and safety. Many studies have shown that equipping these airplanes with safety devices such as Terrain Awareness Warning Systems (TAWS), Graphical Weather Displays, Map Displays, Integrated Flight Systems, SVS, and Enhanced Vision Systems may dramatically reduce a number of accident types. Pilots have reported that integrated flight displays help reduce workload, improve situational awareness, and increase safety.

(b) The aviation industry as a whole is on the threshold of a revolutionary change in communication, navigation, and surveillance of aircraft operations. The Next Generation Air Transportation System will overhaul the National Airspace System (NAS) to take advantage of new technology. It will also likely result in the long-term replacement of many avionics and instrument equipment in the existing fleet as well as in new production aircraft. Facilitating safety equipment installation should enhance the NAS efficiency and safety. If GA is to operate within a revised NAS, new technologies should be available and affordable for GA aircraft. With the four-tier certification class criteria, new technologies are affordable for GA. If GA had only one class for certification, due to the cost of equipment for the NAS architecture, implementation would be incomplete or exclude large portions of the GA fleet from the NAS system. Neither situation is desirable or acceptable.

7. Acronyms.

14 CFR	Title 14 Code of Federal Regulation
AC	Advisory Circular
ACO	Aircraft Certification Office
AFM	Airplane Flight Manual
AFMS	Airplane Flight Manual Supplement
ARP	Aerospace Recommended Practice
ATC	Amended Type Certificate
CAR	Civil Air Regulations
CFR	Code of Federal Regulations
CHT	Cylinder Head Temperature
DAL	Development Assurance Level

EEC	Electronic Engine Control
EGT	Engine Gas Temperature
EPR	Engine Pressure Ratio
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GA	General Aviation
GNSS	Global Navigation Satellite System
HW	Hardware
HIRF	High Intensity Radiated Fields
ICA	Instructions for Continued Airworthiness
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
MFD	Multifunction Flight Display
MRE	Multiple Reciprocating Engine
MTE	Multiple Turbine Engine
MTBF	Mean Time Between Failures
NAS	National Airspace System
P	Primary System
PFD	Primary Flight Display
PMA	Parts Manufacturer Approval
PSSA	Preliminary System Safety Assessment
R	Reserved
S	Secondary System
SAE	Society of Automotive Engineers
SRE	Single Reciprocating Engine
SSA	System Safety Assessment
STE	Single Turbine Engine
STC	Supplemental Type Certificate
SVS	Synthetic Vision Systems
SW	Software
TCAS	Traffic Collision Avoidance System
TIA	Type Inspection Authorization
TAWS	Terrain Awareness Warning System
TC	Type Certificate
TIT	Turbine Inlet Temperature
TSO	Technical Standard Order
VFR	Visual Flight Rules
WAAS	Wide Area Augmentation System

8. Definitions.

a. Adverse effect. A response of a system that results in an undesirable operation of an airplane system, or subsystem.

b. **Analysis.** An evaluation based on decomposition into simple elements.

c. Adverse operating condition. A set of environmental or operational circumstances applicable to the airplane, combined with a failure or other emergency situation that results in a significant increase in normal flight crew workload.

d. Assessment. An evaluation based upon engineering judgment.

e. 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, and environmental and operational stresses. It would also include relationships with other systems, functions, and flight or structural characteristics.

f. Average probability per flight hour. A representation of the number of times the subject failure condition is predicted to occur during the entire operating life of all airplanes of a type, divided by the anticipated total operating hours of all airplanes of that type.

Note: The average probability per flight hour is normally calculated as the probability of a failure condition occurring during a typical flight of mean duration divided by that mean duration. See Appendix 3.

g. Caution. A clear and unambiguous indication to the flight crew or pilot of a failure that requires subsequent crew action. An inherent characteristic of the airplane or a device that will give clearly distinguishable indications of malfunction or misleading information may provide this caution.

h. Complex hardware item. All items that are not simple are considered to be complex. See definition of simple hardware item. Source: RTCA/DO-254, Appendix C and Order 8110.105.

i. Complex system. A system is “complex” when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured assessment methods. FMEA and FTA are examples of such structured assessment methods. Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships. For example, for these types of systems, a portion of the compliance may be shown by the use of DALs such as by processes in RTCA/DO-178B or RTCA/DO-254 or equivalent. See the definitions for “conventional” and “simple” for more information.

j. Continued safe flight and landing. This phrase means that the airplane is capable of continued controlled flight and landing, possibly using emergency procedures, without requiring exceptional pilot skill or strength. Upon landing, some airplane damage may occur as a result of a failure condition.

k. **Conventional system.** A system is considered “conventional” if its function, the technological means to implement its function, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly used. The systems that have established an adequate service history and the means of compliance for approval are generally accepted as "conventional." Normally conventional and simple systems may be analyzed by qualitative assessments as shown in Figure 3. See the definitions for complex and simple systems for more information.

l. Critical function. A function whose loss would prevent the continued safe flight and landing of the airplane.

Note: The term “critical function” is associated with a catastrophic failure condition. Newer documents may not refer specifically to the term “critical function.”

m. Design appraisal. A qualitative appraisal of the integrity and safety of the system design. An effective appraisal requires experienced judgment.

n. Design assurance level. All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that design errors have been identified and corrected such that the items (hardware, software) satisfy the applicable certification basis. This term may be used in some SAE and RTCA documents, but in this AC it is intended that design assurance levels will correlate to the same levels as the DALs for the safety assessment process. See section 21 for more information.

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

Note: For this AC, DALs in figure 2 and throughout this AC are also intended to correlate to software levels in RTCA/DO-178B and complex hardware design assurance levels in RTCA/DO-254 for the system or item. See section 21 for more information.

p. 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, 121, and 135.

q. Error. An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.

r. Essential function. A function whose loss would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions.

Note: The term "essential function" is associated with failure conditions between major and hazardous. Newer documents may not refer specifically to the term "essential function."

s. Event. An internal or external occurrence that has its origin distinct from the airplane, such as atmospheric conditions (for example, gusts, temperature variations, icing, and, runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, fire, leaking fluids, tire burst, HIRF exposure, lightning, uncontained failure of high energy rotating machines, etc.). The term is not intended to cover sabotage.

t. Essential load. Equipment essential to safe operation that requires a power source for normal operation.

u. Extremely remote failure conditions. Those failure conditions not anticipated to occur to each airplane during its total life but which may occur a few times when considering the total operational life of all airplanes of this type. For quantitative assessments, refer to the probability values shown for hazardous failure conditions in figure 2.

v. Extremely improbable failure condition. For commuter category airplanes, those failure conditions so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type. For other classes of airplanes, the likelihood of occurrence may be greater. For quantitative assessments, refer to the probability values shown for catastrophic failure conditions in figure 2.

w. Failure. An occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction).

Note: Errors may cause failures but are not considered failures.

x. Failure conditions. A condition having an effect on either the airplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events. Failure conditions may be classified according to their severity as follows:

(1) No safety effect. Failure conditions that would have no effect on safety (that is, failure conditions that would not affect the operational capability of the airplane or increase crew workload).

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

(3) Major. Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins or functional capabilities. In addition, the failure condition has a significant increase in crew workload or in conditions impairing crew efficiency;

or a discomfort to the flight crew or physical distress to passengers or cabin crew, possibly including injuries.

(4) Hazardous. Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be the following:

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

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

(c) Serious or fatal injury to an occupant other than the flight crew.

(5) Catastrophic. Failure conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane.

Notes: (1) The phrase “are expected to result” is not intended to require 100 percent certainty that the effects will *always* be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic. (2) The term “catastrophic” was defined in previous versions of advisory materials as a failure condition that would prevent continued safe flight and landing.

y. Function. The lowest defined level of a specific action of a system, equipment, and flight crew performance aboard the airplane that, by itself, provides a completely recognizable operational capability (e.g., an airplane heading is a function). One or more systems may contain a specific function or one system may contain multiple functions.

z. Functional hazard assessment. A systematic, comprehensive examination of airplane and system functions to identify potential minor, major, hazardous, and catastrophic failure conditions that may arise as a result of a malfunction or a failure to function.

aa. Hazard. A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or combinations thereof. This term is intended for single malfunctions or failures that are considered probable based on either past service experience or analysis with similar components in comparable airplane applications, or both. There is no quantitative analysis intended in this application.

Note: There is a difference between “hazardous” as used in general policy or regulations and “hazardous failure condition” as used in an FHA. When the term "hazard" or "hazardous" is used in general policy or regulations, it is generally used as shown in this definition. A hazard could be a failure condition that relates to major, hazardous, or catastrophic.

bb. Improbable failure conditions. Those failure conditions unlikely to occur in each airplane during its total life, but that may occur several times when considering the total operational life of a number of airplanes of this type. Also, those failure conditions not anticipated to occur to each airplane during its total life but that may occur a few times when considering the total operational life of all airplanes of this type. For quantitative assessments, refer to the probability values shown for major and hazardous failure conditions in figure 2. For more specific guidance, see definitions of "remote failure conditions" and "extremely remote failure conditions"

cc. Item. One or more hardware and/or software elements treated as a unit.

dd. Installation appraisal. A qualitative appraisal of the integrity and safety of the installation. Any deviations from normal industry-accepted installation practices should be evaluated.

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

ff. Malfunction. Failure of a system, subsystem, unit, or part to operate in the normal or usual manner. The occurrence of a condition whereby the operation is outside specified limits.

gg. 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 to safety and would inappropriately add to the cost of the product without a commensurate benefit.

hh. 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.

ii. Primary function. A function installed to comply with applicable regulations for the required function and provides the most pertinent controls or information instantly and directly to the pilot. For example, the PFD is a single physical unit that always provides the primary display and complies with the requirements of all the following: altitude, airspeed, aircraft heading (direction) and attitude. The PFD is located directly in front of the pilot and used instantly and first by the pilot. A standby or another display intended to be used in the event of failure of the PFD or as a cross reference is an example of a secondary system. For example, a brake control system normally uses the electronic brake system most of the time because of its better performance, but it does not comply with all the requirements. In this case, the mechanical brakes are used as the backup systems; yet, it is consider the primary with regard to meeting the requirements and the electronic brake system is the secondary.

jj. Primary system. A system that provides the primary function.

kk. Probable. Probable as defined for § 23.1309(a) through Amendment 23-49, as a probable malfunction or failure, is any single malfunction or failure that is considered likely on the basis of either past service experience or analysis with similar components in comparable airplane applications, or both.

Note: Normally, there is no quantitative analysis intended in this application. This should not be confused with a probable failure condition when used for a safety assessment process.

ll. Probable failure conditions. Those failure conditions anticipated to occur one or more times during the entire operational life of each airplane. These failure conditions may be determined on the basis of past service experience with similar components in comparable airplane applications. For quantitative assessments, refer to the probability values shown for minor failure conditions in figure 2.

mm. Qualitative. Those analytical processes that assess system and airplane safety in an objective non-numerical manner.

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

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

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

qq. Remote failure conditions. Those failure conditions that are unlikely to occur to each airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type. For quantitative assessments, refer to the probability values shown for major failure conditions in figure 2.

rr. Secondary system. A redundancy system that provides the same function as the primary system.

ss. Similarity. The process of showing that the equipment type, form, function, design, and installation have only minor differences to previously approved equipment. The safety and operational characteristics and other qualities of the new proposed installation should have no appreciable effects on the airworthiness of the airplane.

tt. Simple hardware item. An item with a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level that ensures correct functional performance under all foreseeable operating conditions, with no anomalous behavior.--Source: RTCA/DO-254, paragraph 1.6 and Order 8110.105.

uu. Simple system. Usually a system that can be evaluated by only qualitative analysis and it is not complex. Functional performance is determined by combination of tests and analyses. See the definitions for “conventional” and “complex” systems for more information.

vv. Single failure concept. The objective of this design concept is to permit the airplane to continue safe flight and landing after any single failure. Protection from multiple malfunctions or failures should be provided when the first malfunction or failure would not be detected during normal operations of the airplane, which includes preflight checks, or if the first malfunction or failure would inevitably cause other malfunctions or failures.

ww. System. A combination of components, parts, and elements that are interconnected to perform one or more functions.

xx. Warning. A clear and unambiguous indication to the flight crew or pilot of a failure that requires immediate corrective action. An inherent characteristic of the airplane or a device that will give clearly distinguishable indications of malfunction or misleading information may provide this warning.

9. Application of § 23.1309(a), (a)(1), (a)(2), and (a)(3), as adopted by Amendments 23-41 and 23-49.

If the certification basis for the airplane is Amendment 23-14, § 23.1309(a) (See Note in paragraph 10.) is appropriate to use for systems in airplanes approved to fly either VFR or IFR, or both. With the certification basis at Amendment 23-14, systems that must meet the single-failure concept with the requirements of § 23.1309(a) should comply if the guidance in paragraph 10 of this AC is used. Under the certification basis at Amendment 23-14, compliance with § 23.1309(b) is not required and a safety assessment is not necessary, but it may be used. For complex systems, the requirements of Amendment 23-14 may not provide an adequate level of safety. Then, the certification basis should be Amendment 23-41 or 23-49 as appropriate. In accordance with AC 21.101-1, in cases where no regulatory standards are defined in the existing certification basis for the design change, but applicable regulatory standards exist in a subsequent amendment to the regulations, the subsequent amendment will be made part of the certification basis. Therefore, the change must comply with later appropriate regulations.

10. Showing compliance with the requirements of § 23.1309 (a) through Amendment 23-49.

> **Note:** The requirements of paragraphs (a), (a)(1), (a)(2), and (a)(3) of § 23.1309, as amended by Amendments 23-41 and 23-49, are the same requirements as paragraphs (a), (b), and (c) of § 23.1309, as amended by Amendment 23-14. These same requirements in paragraphs (a), (a)(1), (a)(2), and (a)(3) (above) were deleted in § 23.1309 by Amendment 23-62 because there was a significant revision of § 23.1309.

a. In order to show compliance with the requirements of § 23.1309(a), (a)(1), (a)(2), and (a)(3), it will be necessary to verify that the installed systems and each item of equipment will cause no unacceptable adverse effects and to verify that the airplane is adequately protected against any hazards that could result from probable malfunctions or failures. Analyze, inspect, and test equipment, systems, and installations to ensure compliance with the requirements of § 23.1309(a), (a)(1), (a)(2), and (a)(3).

b. A step-by-step diagram to comply with § 23.1309(a), (a)(1), (a)(2), and (a)(3) is shown in figure 1. These steps are described below.

(1) Evaluate all airplane systems and each item of equipment in order to determine whether they are the following:

(a) Essential to safe operation; or

(b) Not essential to safe operation.

(2) Determine that operation of installed equipment has no unacceptable adverse effects. Verify this by applicable flight or ground checks, as follows:

(a) 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; and

(b) 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 that the affected system is not performing properly would include any visual or aural method (flags, lights, horns, loss of display, etc.).

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

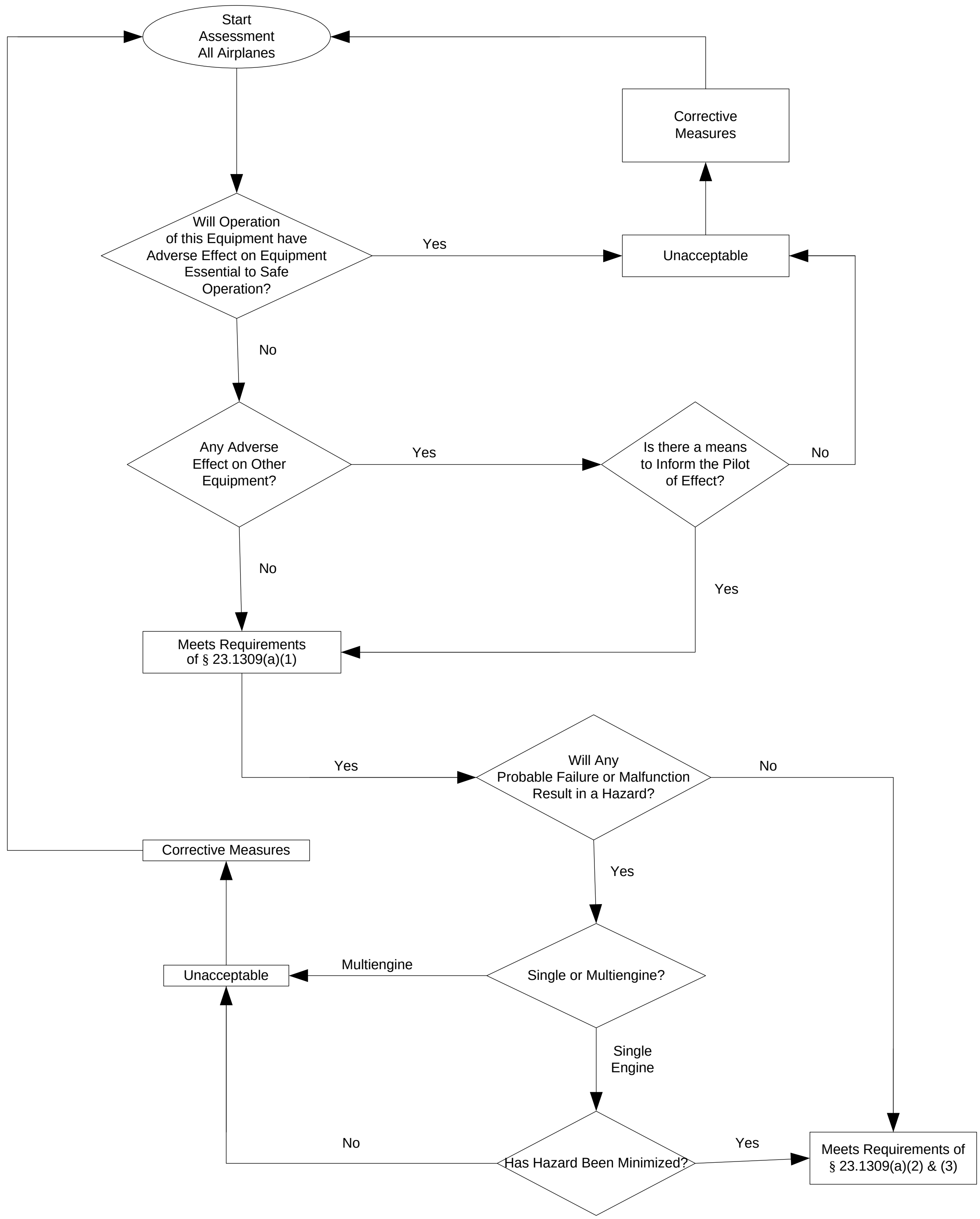
(a) Each item of equipment must be evaluated for general installation hazards. These types of hazards would normally include those hazards that would directly compromise the safety of the airplane or its occupants, such as fire, smoke, explosion, toxic gases, depressurization, etc. A hazard could also result from loss of equipment or systems essential to safe operations when the minimum required functions are lost. Individual failure of redundant equipment would not necessarily be considered a hazard. For example, the single failure of either a 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.

(b) Systems and equipment essential to safe operation must also be assessed for probability of malfunction or failure. 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. Service history should show that past malfunctions or failures have not resulted in hazards and there are no unresolved problems.

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

(d) If it has been determined that a probable failure or malfunction could result in a hazard to a single-engine airplane, that hazard must be minimized or prevent hazards in a multiengine airplane. To minimize is to reduce, lessen, or diminish a hazard to the least practical amount with current technology and materials. Design features should be taken into account to prevent hazards either by ensuring that the failure condition will not occur or by having redundancy or annunciation with the associated flight crew's corrective action. In either case, the hazards should be addressed to the least practical amount to the point at which the effort to further reduce a hazard significantly exceeds any benefit in terms of safety derived from that reduction that is practical for this type of airplane. Additional efforts would not result in any significant improvements of safety and would inappropriately add to the cost of the product without a commensurate benefit. This determination should come from an experienced engineering judgment based on the criticality of the hazard and the intended kinds of operation.

FIGURE 1. METHOD OF COMPLIANCE DIAGRAM OF § 23.1309(a) THROUGH AMENDMENT 23-49



11. Application of § 23.1309(a)(4), as adopted by Amendment 23-49.

a. For those commuter airplanes that include the certification basis of Amendments 23-34, 23-41, or 23-49, § 23.1309(a)(4) requires all applicable systems and installations to be designed to safeguard against hazards to the airplane in the event of their failure. This requirement in § 23.1309(a)(4) for commuter airplanes was introduced into part 23 airplanes by Amendment 23-34 before the safety assessment process was included by Amendment 23-41.

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

c. Service history for similar installations may be utilized to meet part or all of this requirement if a system or installation has a significant and favorable service history in environments similar to the airplane. The claim of similarity should be based on equipment type, function, design and installation similarities, and other relevant attributes. It is the applicant's responsibility to provide accepted/approved data that supports any similarity claims to a previous installation. More information is available in Order 8110.4C.

12. Application of § 23.1309(a)(1) and (a)(2), as adopted by Amendments 23-62.

a. Section 23.1309(a) requires the airplane equipment and systems be designed and installed so that:

(1) Those required for type certification or by operating rules perform as intended under the airplane operating and environmental conditions, including the indirect effects of lightning strikes.

(2) Any equipment and system does not adversely affect the safety of the airplane or its occupants, or the proper functioning of those covered by paragraph (a)(1) of this section.

b. Section 23.1309(a) has requirements for different classes of equipment and systems installed in the airplane, that is, those that are required and not required. Section 23.1309(a)(1) covers the equipment and systems installed to meet a regulatory requirement. Such systems and equipment are required to "perform as intended under the airplane's operating and environmental conditions."

c. Section 23.1309(a) gives the conditional qualifiers "under the airplane operating and environmental conditions." This section describes two actions for the applicant. First, the applicant must consider the full normal operating envelope of the airplane, as defined by the AFM, with any modification to that envelope associated with abnormal or emergency procedures and any anticipated crew action. Second, the applicant must consider the anticipated external and internal airplane environmental conditions, as well as any additional conditions where equipment and systems are assumed to "perform as intended." Although certain operating conditions are foreseeable, achieving normal performance when they exist is not always possible and may not need to be considered. For example, you may foresee ash clouds from volcanic eruptions; however, airplanes with current technology cannot safely fly in such clouds.

d. Other external environmental conditions such as atmospheric turbulence, HIRF, lightning, and precipitation, which the airplane is reasonably expected to encounter, must be considered. These severities of the external environmental conditions to be considered are limited to those established by certification standards and precedence. Also, the environmental effect within the airplane must be considered. These effects should include vibration and acceleration loads, variations in fluid pressure and electrical power, and fluid or vapor contamination due to either the normal environment or accidental leaks or spillage and handling by personnel.

e. We accept equipment susceptible to failures if these failures do not contribute significantly to the existing risks (e.g., some degradation in functionality and capability is routinely allowed during some environmental qualifications, such as HIRF and lightning testing). For example, system lightning protection allows momentary lost or upset of specific functions of electrical/electronic systems. These functions are for failure conditions that are hazardous or major. But, the function must recover in a timely manner after the airplane is exposed to lightning. See AC 20-158 and AC 20-136B for more specific guidance. The safety assessment process of § 23.1309 does not supersede either the HIRF or lightning specific requirements. Environmental effects such as HIRF and lightning should not be considered in combination with another single failure or pre-existing latent failure.

f. Using § 23.1309(a)(2), we must analyze any installed equipment or system that has potential failure condition(s) that are catastrophic, hazardous, major, or minor to determine their impact on the safe operation of the airplane. Usually, normal installation practices can be based on a relatively simple qualitative installation evaluation. If the possible safety impacts, including failure modes or effects, are questionable, or isolation between systems is provided by complex means, more formal structured evaluation methods or a design change may be necessary. Operational and environmental qualification requirements for those equipment, systems, and installations are reduced to the necessary tests that show their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations under § 23.1309 (a)(1) and does not otherwise adversely influence the safety of the aircraft or its occupants. Examples of adverse influences include fire, explosion, exposing passengers to high voltages, etc.

g. Section 23.1309(a)(2) requires the applicant to show that all required and non required equipment and systems (including approved "amenities," such as a coffee pot and entertainment systems) have no safety effect on the operation of the airplane. Section 23.1309(a)(2) does not require non-required equipment and systems to function properly during all airplane operations once in service if analysis shows that all potential failure condition(s) have no adverse safety effects on safe operation of the airplane. The equipment or system must function in accordance with the manufacturer's operating manual or specification. An applicant's statement of intended function must be sufficiently specific and detailed so the FAA can evaluate whether the system is appropriate for the intended function(s) and the associated flight crew tasks. However, we would require equipment or systems to function when they are tested to verify that they do not interfere with the operation of other airplane equipment and systems and do not pose a hazard themselves. The normal operation of non-required systems should not interfere with the proper operation of any required systems or present a hazard themselves. Non-required systems are not required to perform their intended function throughout the aircraft operating and environmental conditions. However, in situations where the non-required system has failed, there can be no adverse safety effect to the aircraft, its occupants, or any adverse effect on required equipment and systems. Malfunctioning and erroneous behavior of all systems, including non-required, should be addressed under § 23.1309(c).

13. Application of § 23.1309(b), as adopted by Amendment 23-62.

a. Section 23.1309 (b) requires for minor, major, hazardous, or catastrophic failure condition(s) which occur during TIA or FAA flight-certification testing must have root cause analysis and corrective action. Testing is an important aspect of the overall compliance processes with §§ 23.1301 and 23.1309. The applicant should conduct bench, ground, and/or flight testing when necessary to validate hazard classifications, acceptability of crew procedures, human factors, and other assumptions made during the root cause analysis processes and corrective actions. The applicant must also discuss with the project ACO what aspects of this testing will need to be included in the FAA certification testing. Those aspects required for formal certification testing must be included in the appropriate FAA approved test plans and conducted on an FAA conformed test article in the presence of the FAA or delegated FAA witness in accordance with Order 8110.4C. Before receiving TIA, the applicant should be able to show qualitatively that the proposed design change will meet the requirements of section 23.1309.

b. The FAA will typically conduct some level of function and qualitative reliability testing during certification to ensure required functions demonstrate an acceptable level. The FAA will also conduct other required certification tests and analyses. These tests are meant to verify availability, accuracy, and qualitative reliability of the system. The FAA expects the applicant to show that the system does not exhibit unintended or undesirable functionality failure conditions that are minor, major, hazardous, or catastrophic. The FAA also expects that failures, malfunctions, and design errors with potential safety hazards have a full assessment of the problem, root cause analysis processes, and corrective action.

c. It is not intended for the probability requirements based on random distribution across a fleet of aircraft be applied on the beginning phase and to be fully complaint with this requirements. It is not appropriate to apply probability values to the typical certification flight test because the sample is too small. Failures during TIA and FAA flight-certification testing must have root cause analysis and corrective action (include traceability to production within the change) with robust corrections and substantiation of the corrections. The regulations do not required FAA approval for the root cause analysis.

14. Application of § 23.1309(b), as adopted by Amendments 23-41 and 23-49 and § 23.1309(c), as adopted by Amendment 23-62.

a. The installed systems should be evaluated by performing a safety assessment as shown in this AC. The depth and scope of the safety assessment depends on the types of functions performed by the systems, the severity of the failure conditions, and whether the system is complex. For instance, the safety assessment for a slightly modified single-engine airplane with simple systems might consist only of an FHA with a design and installation appraisal. This FHA will be much less extensive than the FHA for a commuter category or a multiple turbine-engine airplane with more complex systems. The types of analyses selected by an applicant and approved by the certification authority should be based on factors such as the system architecture, complexity, particular design, etc.

b. The safety assessment objective is to ensure an acceptable safety level for equipment and systems installed on the airplane. A logical and acceptable inverse relationship should exist between the average probability per flight hour and the severity of failure conditions effects (as shown in figure 2). This figure defines the appropriate airplane systems probability standards for four certification classes of airplanes designed to part 23 standards. The relationship between probability and severity of failure condition effects are as follows:

(1) Failure conditions with no safety effect have no probability requirement.

(2) Minor failure conditions may be probable.

(3) Major failure conditions must be no more frequent than remote.

(4) Hazardous failure conditions must be no more frequent than extremely remote.

(5) Catastrophic failure conditions must be extremely improbable.

c. Compliance with § 23.1309(c) may be shown by analysis and, where necessary, by appropriate ground, flight, or simulator test. The analysis should consider—

(1) Possible modes of failure, including malfunctions and damage from external sources;

(2) The probability of multiple failures and the probability or undetected faults;

(3) The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions; and

(4) The crew warning cues, corrective action required, and the crew's capability of determining faults.

15. Four certification classes of airplanes.

a. The four-certification classes of airplanes for this AC are shown in figure 2 and the acronyms are defined in paragraph 7. They are Class I (Typically SRE 6,000 pounds (lbs.) or less (Maximum Certificated Gross Takeoff Weight)), Class II (Typically MRE, MTE and STE, 6,000 pounds or less), Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds), and Class IV (Typically Commuter Category).

b. Numerical values are assigned for use in cases where the impact of system failures is examined by quantitative methods of analysis. Also, the related software and complex hardware DALs for the various failure conditions are part of the matrix in figure 2 for most systems. These levels should be used unless there are some unique architecture considerations. For these unusual situations there should be specific policy, guidance, or approval by the Small Airplane Directorate. (See paragraph 21 for more information) The probability standards are based on historical accident data, systems analyses, and engineering judgment for each class of airplane.

c. In assessing the acceptability of a design, the FAA recognized the need to establish rational probability values. Historically, failures in GA airplanes that might result in catastrophic failure conditions are predominately associated with the primary flight instruments in IMC. Historical evidence indicates that the probability of a fatal accident in restricted visibility due to operational and airframe-related causes is approximately one per ten thousand flight hours or 1×10^{-4} per flight hour for single-engine airplanes under 6,000 pounds. Furthermore, from accident databases, it appears that about 10 percent of the total was attributed to failure conditions caused by the airplane's systems. It is reasonable to expect that the probability of a fatal accident from all such failure conditions would not be greater than one per one hundred thousand flight hours or 1×10^{-5} per flight hour for a newly designed airplane. From past service history, it is also assumed that there are about ten potential failure conditions in an airplane that could be catastrophic. The allowable target average probability per flight hour of 1×10^{-5} was thus apportioned equally among these failure conditions, which resulted in an allocation of not greater than 1×10^{-6} to each. The upper limit for the average probability per flight hour for catastrophic failure conditions would be 1×10^{-6}, which establishes an approximate probability value for the term "extremely improbable." Failure conditions having less severe effects could be relatively more likely to occur. Similarly, airplanes over 6,000 pounds have a lower fatal accident rate; therefore, they have a lower probability value for catastrophic failure conditions.

FIGURE 2. RELATIONSHIP AMONG AIRPLANE CLASSES, PROBABILITIES, SEVERITY OF FAILURE CONDITIONS, AND SOFTWARE AND COMPLEX HARDWARE DAL

Classification of Failure Conditions	**No Safety Effect**	**<----Minor----->**	**<----Major---->**	**<--Hazardous--->**	**< Catastrophic>**
Allowable Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Classes of Airplanes:	**Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development Assurance Levels (Note 2)**				
Class I (Typically SRE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 and 4 P=C, S=D	$<10^{-5}$ Note 4 P=C, S=D	$<10^{-6}$ Note 3 P=C, S=C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-6}$ Note 4 P=C, S=C	$<10^{-7}$ Note 3 P=C, S=C
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=C, S=C	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Note 1: Numerical values indicate an order of probability range and are provided here as a reference.
Note 2: The letters of the alphabet denote the typical SW and HW Development Assurance Levels for Primary System (P) and Secondary System (S). For example, HW or SW Development Assurance Level A on Primary System is noted by P=A.
Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.
Note 4. Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria.

d. The criteria shown in figure 2 directly reflect the historical accident and equipment probability of failure data in the CAR 3 and 14 CFR part 23 airplane fleet. Characteristics of the airplane, such as stall speed, handling characteristics, cruise altitude, ease of recognizing system failures, recognition of entry into stall, pilot workload, and other factors (which include pilot training and experience) affect the pilot's ability to safely handle various types of system failures in small airplanes. The criteria considered for all airplanes' failure conditions is based on service experience, operational exposure rates, and total airplane system reliability. The values for individual system probability of failure could be higher than probability values shown in figure 2 for specific failure conditions because it considers the installed airplane systems, events, and factors.

e. These classes were defined based on the way accident and safety statistics are currently collected. Generally, the classes deal with airplanes of historical equivalent levels of system complexity, type of use, system reliability, and historical divisions of airplanes according to these characteristics. However, these classes could change because of new technologies. The placement of a specific airplane in a class should be done in reference to all of the airplane's missions and performance characteristics. The applicant should have the concurrence of the certification authority that is knowledgeable about the applicable airplane class early in the program. When unusual situations develop, consult the Small Airplane Directorate to obtain specific policy guidance or approval.

f. For example, airplanes with considerably more than 10 catastrophic failure conditions, that have greater performance characteristics and incorporate many complex systems and advance technologies may have lower probability values and higher DALs. These airplanes' probability values and DALs may fall between the classes of the airplanes. For instance, the performance characteristics of a complex airplane including airplane handling qualities and stall speed may be similar to existing Class II airplanes. However, this airplane's mission and other performance characteristics including high speed, high altitude, and extended range operations may be similar to existing Class III airplanes. The major difference between the DALs for Class II and Class III airplanes is for primary systems whose failure would result in a catastrophic failure condition for the airplane. Since this complex airplane falls between these two classes, it is reasonable to choose the higher DAL and a lower probability level.

g. For example, in part 23, turbine-engine airplanes traditionally have been subject to more stringent requirements than a single-engine reciprocating airplane. A single-engine reciprocating airplane generally has a wider stall-cruise speed ratio than traditional turbine-engine airplanes. Such an airplane with a stall speed under 61 knots with simple systems, and with otherwise similar characteristics to a traditional single-engine reciprocating airplane (except for a higher cruise speed and a more reliable engine that is simpler to operate), can be treated as a Class I airplane under this analysis. Conversely, if a single-engine reciprocating airplane has the performance, mission capability, and system complexity of a higher class (such as cabin pressurization, high cruise altitude, and extended range), then that type of airplane design may align itself with the safety requirements of a higher class (for example, Class II airplane). These determinations should be made during the development of the certification basis.

h. This AC uses terminology similar to AC 25.1309-1A. However, the specific means of compliance for § 25.1309 are defined differently due to the higher safety level required for transport category airplanes. However, there are some similarities with part 23 commuter category airplanes.

16. Safety assessments.

a. The applicant is responsible for identifying and classifying each failure condition and choosing the methods for safety assessment. The applicant should then obtain early concurrence from the cognizant certificating authority on the identification of failure conditions, their classifications, and the choice of an acceptable means of compliance. Figure 3 provides an overview of the information flow to conduct a safety assessment. This figure is a guide and it does not include all information provided in this AC or the documents referenced in section 4 of this AC.

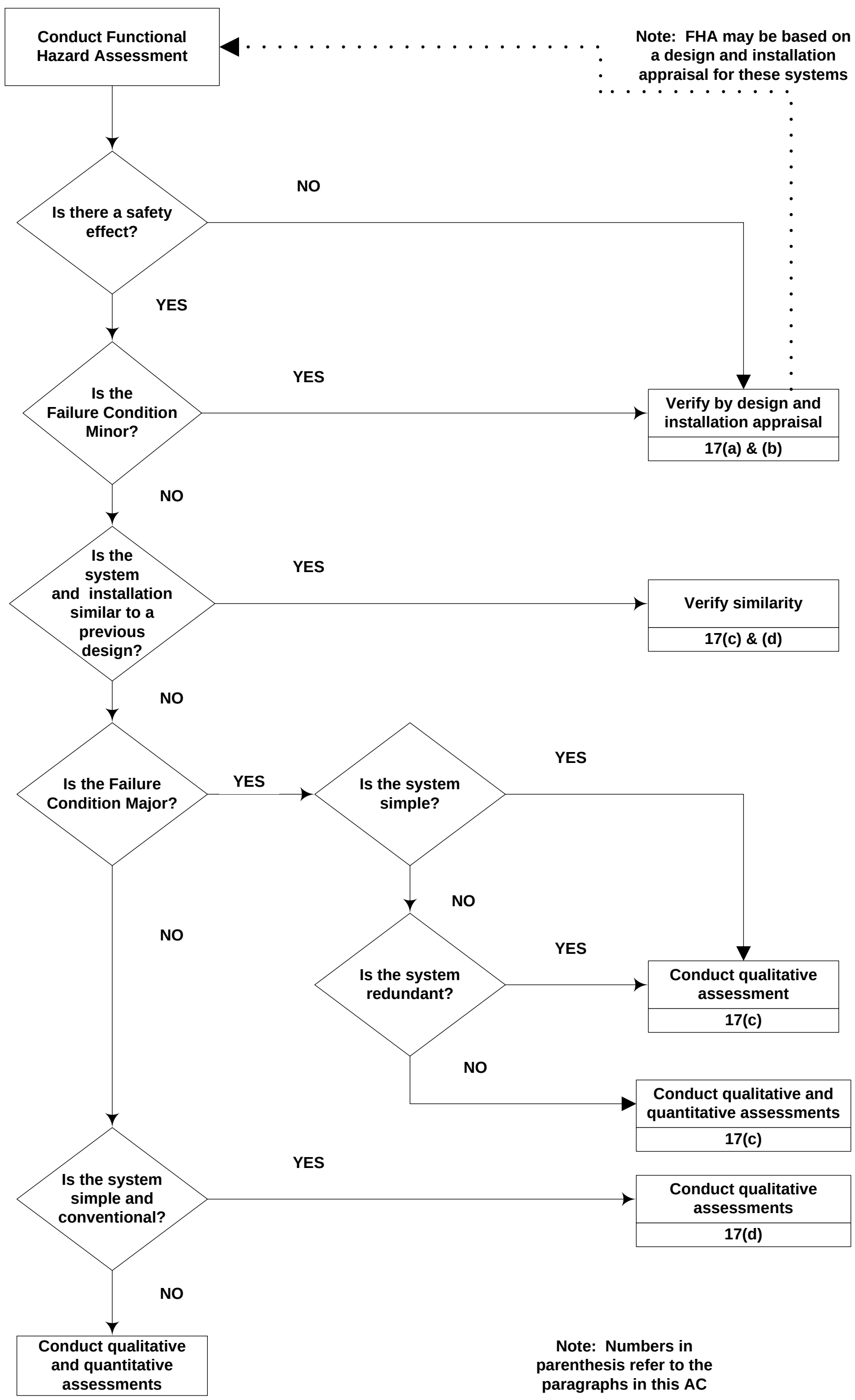
b. Functional hazard assessment (FHA).

(1) Before an applicant proceeds with a detailed safety assessment, an FHA of the airplane and system functions to determine the need for and the scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgment, or service experience and a top-down deductive qualitative examination of each function. An FHA is a systematic, comprehensive examination of airplane and system functions to identify potential no safety effect, minor, major, hazardous, and catastrophic failure conditions that may arise, not only as a result of malfunctions or failure to function but also as a result of normal responses to unusual or abnormal external factors. The FHA concerns the operational vulnerabilities of systems rather than a detailed analysis of the actual implementation.

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

(3) The FHA is an engineering tool that should be performed early in the design and updated as necessary. It is used to define the high-level airplane or system safety objectives that should be considered in the proposed system architectures. Also, it should be used to assist in determining the DALs for the systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. An FHA requires experienced engineering judgment and early coordination between the applicant and the certification authority.

FIGURE 3. DEPTH OF ANALYSIS FLOW CHART



(4) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to FHA may be taken. Where there is a clear correlation between functions and systems, and where system and function interrelationships are relatively simple, it may be feasible to conduct separate FHA's for each system. However, this is conditional providing any interface aspects are properly considered and easily understood. However, a top-down approach from an airplane level perspective should be taken in planning and conducting an FHA where system and function interrelationships are more complex.

(5) After each failure condition is classified, refer to figure 2 to identify the failure condition probability and software and complex hardware DALs. For example, the probability requirement for a hazardous failure condition for a Class I airplane should be less than 1×10^{-5}. In addition, the primary system for a Class I airplane should have software and complex hardware DALs of C and, if required, the secondary system for a Class I airplane should have software and complex hardware DALs of D.

(6) The classification of failure conditions does not depend on whether 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, 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, hazardous, or catastrophic failure conditions.

(7) The classification of failure conditions should consider all relevant factors. Examples of factors include the nature of the failure modes, which includes common mode faults, system degradation resulting from failures, 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. The ability of a system to inform the pilot of potential or real failure conditions so that timely corrective action can be taken to reduce the effects of the combination of events is desirable. This approach may reduce the severity of the failure condition.

(8) Because of the large number of combinations of failures, various mitigating factors, airplane characteristic effects, and similar factors, a specific FHA and the related safety assessments may be significantly different for each evaluated airplane type and configuration. These factors preclude providing a concrete example of a FHA that applies across the board to every installation. However, general examples may be provided that illustrate the concepts involved in an FHA. It is critical to understand that significant engineering judgment and common sense are necessary to provide a practical and acceptable evaluation of the airplane and its systems.

c. Appendix 1 provides a partial list of FHA for consideration for part 23 IFR Class I airplanes with typical functions and, in general, the related failure conditions are at the aircraft level. The criteria at the aircraft level are useful to derive the system FHA. The failure conditions for the examples in Appendix 1 cannot be applied indiscriminately to a particular airplane installation. This table is primarily for use to reduce the regulatory burden on applicants who are not familiar with the various methods and procedures generally used in industry to conduct safety assessments. It is only intended to be a guide, not a certification checklist, since it does not include all the information necessary for an FHA for a specific airplane with its various functions and its intended use. The functions listed in the partial FHA as a guide for the classification of failure conditions when the functions are installed. The list of functions is not intended to suggest that the functions are required for Class I airplanes. Even if there is guidance information in Appendix 1, the applicable regulations provide the requirements of the functions for installations.

(1) The applicant should use Appendix 1 and the appropriate certification authority as a point of departure for the specific system or airplane assessment. It can be used to arrive at the appropriate failure conditions for a specific system by similarity to or by interpolating between the example systems. It does not necessarily provide, by itself, an answer for an applicant's system unless that system is exactly as described. Its sole purpose is to assist applicants by illustrating typical functions and the related failure conditions. This appendix addresses general applicability, which is valuable for determining software and complex hardware DALs, and it should not be utilized to replace any specific guidance intended for individual types of equipment, systems, and installations. The FHA results are airplane characteristic and system architecture dependent. The examples in this appendix are based on traditional airplanes and traditional architectures. Section 23.1309 is a regulation of general requirements and should not be used to supersede any specific requirements of part 23.

(2) In addition to the general technical guidance provided in Appendix 1, a sample of one suggested format is provided in Appendix 2 for documenting the results of an FHA. This format illustrates how factors other than those directly illustrated in Appendix 1 are pertinent. It also illustrates that failure conditions are not limited to only the three general types shown in Appendix 1. The actual data shown in Appendix 2 is only used to illustrate the typical approach and should not be viewed as technically representative of any particular airplane. A complete FHA could be comprised of the layout shown in Appendix 2 by utilizing pertinent technical considerations identified in Appendix 1, which are modified and expanded to reflect the specific proposed airplane design under consideration.

d. Part 23 airplanes cover a wide range of airplane sizes and capabilities. These airplanes range from single-engine, single-seat, low-performance airplanes to complex multiengine, high-speed, high-performance airplanes. At the bottom end of these part 23 airplane types, there are several compensating characteristics that mitigate many of the effects of a failure. Docile handling characteristics, low stall speeds, spin resistant designs, lower probability of operation in extreme weather conditions, and the inherent design philosophies used to design single-engine airplanes are specific examples of characteristics to consider in an FHA for systems installed in this class of airplane. Usually, air traffic control support is not a mitigating factor.

17. Failure conditions.

a. Failure conditions with no safety effect. An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. In general, common design practice provides physical and functional isolation from related components, which are essential to safe operation. If the applicant chooses not to do a detailed FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

b. Analysis of minor failure conditions. An analysis should consider the effects of system failures on other systems or their functions. An FHA with a design and installation appraisal to establish independence from other functions is necessary for the safety assessment of these failure conditions. In general, common design practice provides physical and functional isolation from components that are essential to safe operation. If the applicant chooses not to do a detailed FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

c. Analysis of major failure conditions. An assessment based on engineering judgment is a qualitative assessment, as are several of the methods described below:

(1) Similarity allows validation of a requirement by comparison to the requirements of similar certified systems. The similarity argument gains strength as the period of experience with the system increases. If the system is similar in its relevant attributes to those used in other airplanes and if the functions and effects of failure would be the same, then a design and installation appraisal and satisfactory service history of either the equipment being analyzed or of a similar design is usually acceptable for showing compliance. It is the applicant's responsibility to provide data that is accepted, approved, or both, and that supports any claims of similarity to a previous installation.

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

(3) To show that malfunctions are indeed remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is necessary to conduct a qualitative functional FTA or FMEA supported by failure rate data and fault detection coverage analysis.

(4) An analysis of a redundant system in the airplane 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 or FTA may be necessary to determine that redundancy actually exists (for example, no single failure affects all functional channels).

d. Analysis of hazardous and catastrophic failure conditions. For these failure conditions, a thorough safety assessment is necessary. The assessment usually consists of an appropriate combination of qualitative and quantitative analyses. Except as specified in the next paragraphs below, a detailed safety analysis must be completed for each hazardous and catastrophic failure condition identified by an FHA. The analysis will usually be a combination of qualitative and quantitative assessments of the design.

(1) For 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 being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for the assessment will be the degree of redundancy, the established independence and 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 regarding both the system design and operating conditions.

(2) 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 being extremely remote or extremely improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. A high degree of similarity in both design and application is required.

(3) No catastrophic failure condition (Note 3 in figure 2) should result from the failure of a single component, part, or element of a system. Experienced engineering judgment and service history should show that a catastrophic failure condition by a single failure mode is not a practical possibility. The logic and rationale used in the assessment should be so straight-forward and obvious that the failure mode simply would not occur unless it is associated with an unrelated failure condition that would, in itself, be catastrophic.

18. Assessment methods.

a. Assessment methods. Methods for qualitatively and quantitatively 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 analyses are based on either inductive or deductive approaches. The applicant should select analyses to validate the safety of a particular design based on factors such as the system architecture, complexity, criticality of the function, etc. ARP 4761 has more details of the various methods. Descriptions of typical types of analyses that might be used are provided below.

(1) Design appraisal. A qualitative appraisal of the integrity and safety of the system design. An effective appraisal requires experienced judgment.

(2) Installation appraisal. This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices should be evaluated. An effective appraisal requires experienced judgment.

(3) Failure Modes and Effects Analysis (FMEA). A structured, inductive, and bottom-up analysis that 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. ARP 4761 provides methodology and detailed guidelines that may be used to perform this type of analysis. 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-oriented FMEA can lead to uncertainties in the qualitative and quantitative aspects, which can be compensated for by more conservative assessments, such as the following: Assuming all failure modes result in failure conditions of interest, carefully choosing system architecture, and using lessons learned from similar technology.

(4) Fault Tree Analysis (FTA). A structured, deductive, and top-down analysis that is used to identify the conditions, failures, and events that would cause each defined failure condition. FTAs 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. The fault tree should be developed to the lowest level for which failure rates can be substantiated. Rates derived from applicable service experience, acceptable industry wide sources, manufacturer's accelerating testing data, or from an FMEA may be used as inputs to the lowest level events.

(5) Common cause analysis. 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. The "common cause analysis" is divided into three areas of study:

(a) Zonal safety analysis. This analysis has the objective of ensuring that the equipment installations within each zone of the airplane are at an adequate safety standard regarding design and installation standards, interference between systems, and maintenance errors.

(b) Particular risk analysis. Particular risks are defined as those events or influences outside the systems concerned (e.g., fire, leaking fluids, bird strike, tire burst, HIRF exposure, lightning, uncontained failure of high energy rotating machines, etc.). Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects, or influences, which may violate independence.

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

19. Assessment of failure condition probabilities and analysis considerations.

a. 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 type of functions performed by the system, the severity of failure conditions, and whether the system is complex. A quantitative analysis is intended to supplement, but not replace, qualitative methods based on engineering and operational judgment. A quantitative analysis is often used for catastrophic or hazardous failure conditions of systems that are complex and major failure conditions that are complex without redundancy. For the cases were there is insufficient service experience to help substantiate their safety, or that have attributes that differ significantly from those of conventional systems.

b. A probability analysis may be either an FMEA or an FTA, which also includes numerical probability information. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative analysis methods.

c. The probabilities of primary failures can be determined from failure rate data and exposure times using failure rates derived from either service experience on identical or similar items, manufacturer's accelerating testing data, or from 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 the various identified contributory failures or other events. See Appendix D of ARP 4761 for more information.

d. 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.

e. The applicant should obtain early certification authority concurrence for an acceptable classification of the failure conditions and probability for each minor, major, hazardous, and catastrophic failure condition. Early concurrence on the classification of the failure conditions may reduce the applicant's efforts in determining the probabilities resulting from changes.

f. The details on how to calculate the "average probability per flight hour" for a failure condition are given in Appendix 3. The "average probability per flight hour" is the probability of occurrence, normalized by the flight time of a failure condition during a single flight. 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 risk model that better reflects the failure condition should be used. The single flight is analyzed to be representative of an average over all possible flights of the fleet of airplanes to be certified. The calculation of the "average probability per flight hour" for a failure condition should consider the following:

(1) The average flight duration and the average flight profile for the airplane type to be certified. A common assumption for part 23 airplanes is that the average flight duration is 1 hour;

(2) All combinations of failures and events that contribute to the failure condition;

(3) The conditional probability if a sequence of events is necessary to produce the failure condition;

(4) The relevant "at risk" time if an event is only relevant during certain flight phases; and

(5) The average exposure time if the failure can persist for multiple flights.

20. Operational and maintenance considerations.

a. Alerts

(1) Section 23.1309(d) requires information concerning unsafe system operating condition(s) must be provided in a timely manner to the crew to enable them to take appropriate corrective action. An appropriate alert must be provided if immediate pilot awareness and immediate or subsequent corrective action is required. The particular method of indication depends on the urgency and need for flight crew awareness or action necessary for the particular failure. Inherent airplane characteristics may be used in lieu of dedicated indications and annunciations if they can be shown to be timely and effective. However, the use of periodic maintenance or flight crew checks to detect significant latent failures when they occur should not be used in lieu of practical and reliable failure monitoring and indications.

(2) Section 23.1309(d) specifies that the design of systems and controls, including indications and annunciations, must be design to minimize crew errors, which could create additional hazards. The additional hazards to be minimized include those caused by inappropriate actions by a crewmember in response to the failure, or those that could occur after a failure.

b. Flight crew and maintenance task. These tasks, which relate to compliance, should be appropriate and reasonable. Quantitative assessments of the probabilities of flight crew and maintenance 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. For the purposes of quantitative analysis, a probability of one can be assumed for flight crew and maintenance tasks that have been evaluated and found to be reasonable. 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 or focus of the operational or maintenance actions.

c. Flight crew action. When assessing the ability of the flight crew to cope with a failure condition, the information provided to the crew and the complexity of the required action should be considered.

(1) If the evaluation indicates that a potential failure condition can be alleviated or overcome in a timely manner without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, correct crew action may be assumed in both qualitative and quantitative assessments.

(2) 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.

(3) Unless flight crew actions are accepted as normal airmanship, the appropriate procedures should be included in the FAA approved AFM or in the 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 indications, diagnosis of system failures, discussion of possible pilot-induced flight control system problems, and use of the system in a safe manner.

d. Maintenance actions. Credit may be taken for correct accomplishment of maintenance tasks in both qualitative and quantitative assessments if the tasks are evaluated and found to be reasonable. Required maintenance tasks, which mitigate hazards, should be provided for use in the FAA approved maintenance programs such as the ICA. Annunciated failures will be corrected before the next flight or a maximum duration will be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance action is required. A scheduled maintenance task may detect latent failures. If this approach is taken, and the failure condition is hazardous or catastrophic, then a maintenance task should be established. Some latent failures can be assumed to be identified based upon a return to service test on the equipment following its removal and repair (component MTBF should be the basis for the check interval time).

21. Software and complex hardware DALs for airborne system and applications.

a. Background. AC 20-115B discusses how RTCA/DO-178B provides an acceptable means for showing that software complies with pertinent airworthiness requirements. AC 20-152 and Order 8110.105 provide acceptable means for showing that complex hardware complies with the pertinent airworthiness requirements.

b. Acceptable application of software and complex hardware DALs. It is necessary to consider the possibility of requirement, design, and implementation errors in order to comply with the requirements of § 23.1309. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components. These tests used direct inspection and other direct verification methods capable of completely characterizing system the performance. These direct techniques may still be appropriate for simple systems, which perform a limited number of functions and which are not highly integrated with other airplane systems.

(1) For more complex or integrated systems, exhaustive testing may either be impossible because all of the systems states cannot be determined or it may be impractical due to the number of tests that must be accomplished. For these types of systems, compliance may be shown by the use of software and complex hardware DALs. The software and complex hardware DALs should be determined by the severity of potential effects on the airplane in case of system malfunctions or loss of functions.

c. Software and complex hardware DALs criteria for part 23 airplanes. The DALs in figure 2 and throughout this AC correlate to the software level in RTCA/DO-178B and the complex design assurance level in RTCA/DO-254 documents. The classification of the failure condition and airplane class must be determined before figure 2 is used to determine these levels. These levels in figure 2 are acceptable for part 23 airplanes instead of software levels in paragraph 2.2.2 in RTCA/DO-178B and of the complex hardware design assurance levels defined in paragraph 2.2 in RTCA/DO-254.

d. Complex hardware level D. AC 20-152 provides an exclusion from FAA review for complex hardware design assurance level "D" developed under DO-254. The exclusion from FAA review of life cycle data only applies for minor failure conditions and will not apply to level D for the reduced levels shown for major and hazardous failure conditions identified in figure 2.

e. System architecture for determination of the appropriate DALs.

(1) SAE S-18, Airplane Safety Assessment Committee, revised ARP 4754 to ARP 4754A and is revising ARP 4761. The committee developed new concepts for DAL and Design Assurance Levels in ARP 4754A. These SAE documents are guidelines for assigning the DALs that start from the aircraft/system level and end at the item/component level. ARP 4754A addresses the development phase in two phases: Function Development Phase and Item Development Phase, with two different types of development processes.

(2) These assignments depend on the failure condition classification, the number of independent failure paths, and their associated independence attributes. The independence attributes are the functional independence, design independence, and physical independence. In essence, functional independence ensures that the functional requirements that are implemented in the design are different, whereas design independence ensures that the hardware or software design, in which the functions are implemented, is different.

(3) There may be significant difference in the guidance provided on the use of system architecture for appropriate determination of the DALs between this AC and guidelines contained in ARP 4754A. Where apparent differences exist between this AC and ARP 4754A, this AC takes precedence. The FAA recognizes that consideration of system architecture for determining DALs is appropriate and may lead to lower levels in some specific cases. Figure 2 in this AC already allows reduction of software and complex hardware DALs for Class I, II, and III airplanes; therefore, no additional reductions from these levels are permitted without the Small Airplane Directorate approval or there is established specific policy or guidance. If the Small Airplane Directorate has established specific guidance or policy for these levels, then the approval can made by the ACO. For commuter category airplanes, the guidance in ARP 4754A is more likely to be appropriate since its DALs are higher. There may be acceptability only if additional credit for architecture is requested for hazardous or catastrophic failure conditions in Class IV, commuter category airplanes.

f. Equipment installed in part 23 airplanes that performs functions addressed by TSO standards. Equipment installed in part 23 airplanes that performs functions addressed by TSO standards should meet applicable TSO standards. FAA prefers the equipment meet design approval of the functional TSO. However, the equipment is not required to have TSO authorization, but it would need to meet other equivalent minimum performance standards acceptable to the Administrator. The TSO data should include the equipment complex hardware and software DALs. For both TSO and non-TSO equipment, the safety assessment and figure 2 should be used to check the complex hardware and software DALs against the installation requirements.

22. Electromagnetic protection for electrical/electronic systems.

Current trends indicate increasing reliance on electrical/electronic systems for safe operations. Electromagnetic effects, environmental effects, and environmental qualifications should be considered for systems that perform flight, propulsion, navigation, and instrumentation functions. The software and complex hardware DALs shown in figure 2 are not applicable for HIRF and lightning protection levels. For guidance for the protection against these effects, refer to the latest version of AC 21-16F, AC 23-17C, AC 20-136A, and AC 20-158.

APPENDIX 1.
PARTIAL LIST OF FUNCTIONAL HAZARD ASSESSMENT (FHA) FOR CONSIDERATION TO MEET 14 CFR PART 23 REQUIREMENTS FOR IFR CLASS I AIRPLANES

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of attitude information to control roll and pitch	Catastrophic	Major	Catastrophic	For electronic displays, dual independent attitude systems generally meet requirements for 14 CFR part 23, §§ 23.1301, 23.1309, & 23.1311 for airplanes with less than 10 passengers and for conventional mechanical or analog electromechanical systems. A single attitude display meets 14 CFR part 91 requirements to operate under IFR. If the certification basis includes Amendment 23-43 or later, two independent power sources are required by § 23.1331. The requirement for two power sources in § 23.1331 are not applicable for pitot-static pneumatic systems. Partial panel techniques may be used in some cases where it has been historically shown to be acceptable. Credit (mitigation) may be given for automatic flight control systems if the system can maintain stable attitude independent of the primary attitude display.
Display of directional heading information	Major	Minor	Major	A hazardously misleading heading is usually when the accuracy error is greater than 10 degrees on the primary heading instrument and it is an undetected error. Assumes installation of a single stabilized heading system and only a non-stabilized magnetic compass to operate under IFR for 14 CFR part 91. If the certification basis includes Amendment 23-43 or later, two independent power sources are required by § 23.1331. The requirement of two power sources of § 23.1331 are not applicable for pitot-static pneumatic systems. Navigation assumed to be operating. See AC 23-17C for additional information.

***Note:** This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of altitude information	Hazardous	Minor	Catastrophic	For electronic displays, dual independent altitude systems generally meet requirements for 14 CFR part 23, §§ 23.1301, 23.1309, & 23.1311 and for conventional mechanical or analog electromechanical systems. A single altitude display meets 14 CFR part 91 requirements to operate under IFR. If the certification basis includes Amendment 23-43 or later, two independent power sources are required by § 23.1331. The requirement of two power sources of § 23.1331 are not applicable for pitot-static pneumatic systems. Existing single static systems that are heated have been historically acceptable based on similarity and may be used for programs that have certification basis prior to Amendment 23-42. If a single or dual air data computer is used, it must meet the requirements of this AC with respect to safety and DAL.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of airspeed information	Major. May be Hazardous for higher performance airplanes.	Minor	Major. May be hazardous or catastrophic for higher performance airplanes.	For electronic displays, dual independent airspeed systems generally meet requirements for 14 CFR part 23, §§ 23.1301, 23.1309, & 23.1311 and for conventional mechanical or analog electromechanical systems. A single airspeed display meets 14 CFR part 91 requirements to operate under IFR. If the certification basis includes Amendment 23-43 or later, two independent power sources are required by § 23.1331. The two power sources in § 23.1331 are not applicable for pitot-static pneumatic systems. Classification is usually Major, if overspeed and underspeed airspeed alerting is acceptable (alerting may be provided by inherent aerodynamic qualities or independent alerting system); otherwise, loss of function, malfunction, or misleading of information is Hazardous. It may be catastrophic when combined with the loss of stall warning or overspeed warning functions. Assumes no vertical speed indicator. Existing single pitot static systems that are heated have been historically acceptable based on similarity and may be used for programs that have certification basis prior to Amendment 23-42. If a single or dual air data computer is used, it must meet the requirements of this AC with respect to safety and DAL.
Display of Flight Path Vector	Minor	R	Major	Providing the other normal cues remains for primary flight information, loss of the sensor should remove the flight path vector. The pilot should recognize it and use other displays. Misleading indication could cause the pilot to temporarily maneuver the aircraft using erroneous guidance information.
Display of rate-of-turn information	Minor	Minor	Minor	Rate-of-turn display is generally required to operate under 14 CFR part 91 IFR requirements unless a third attitude is installed. If the certification basis includes Amendment 23-43 or later, two independent power sources are required. In IMC, misleading rate-of-turn information is consider to be Minor if there is a functional attitude display.
Display of slip-skid information	Minor	Minor	Minor	R

***Note:** This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of time information	Minor	Minor	Minor	R
Display of primary navigation information	Major	Major. Minor, if two navigation systems are installed.	Major for CAT I ILS. Hazardous or major depending on type of WAAS operations.	Two navigation systems are generally installed to support navigation, but two are not required for 14 CFR part 91 operations. Dual ILS receivers below Category I limits are required with single antenna for part 91 operations. See AC 20-138B for more guidance on WAAS operations.
Display of navigation information on MFD	Minor	R	Minor	Pilot should cross check with the course deviation indicator and other navigation sources.
Weather displays for situation awareness	Minor	Minor	Minor	Pilot is responsible to use standard procedures. It is used for only strategic planning and operation and is not intended for tactical maneuvering.
Terrain Awareness and Warning System (TAWS)	Minor	R	Major	The loss of that system should be no greater than 10^{-3} per average flight hour, and the possibility of misleading information on the display due to undetected or latent failures should be no greater than 10^{-4} per average flight hour. For a Class A TAWS, the software development assurance level should be at least to Level C as defined in RTCA DO-178B or an acceptable alternative approved by the FAA. For Class B TAWS, the software development assurance level should be at least to Level D providing the required alerts and visual annunciations are independent of the terrain display(s). If the required alerts and visual annunciations are integrated on the displays, the DAL should be at least Level C. NOTE: A terrain display is not mandatory for Class B equipment. See AC 23-18 for more information.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Communication	Minor. Total loss of navigation and communication is Hazardous.	Minor	Major, if data link. Otherwise, Minor.	Future installations may use data link for primary functions and voice for secondary.
Traffic information for situation awareness	Minor	Minor	Minor to Major depending on the intended function of the alert warning or caution signal.	Pilot is responsible to use standard "see and avoid procedures". Traffic information is not an approved substitute for traffic avoidance. See the applicable AC and TSO for additional guidance.
Mode A or C Transponder	Minor	R	Minor to Major depending on the intended function of signals from the transponder.	Air traffic control may receive misleading or loss of airplane identification, or altitude, which increases their workload. An incorrect resolution advisory may increase pilot workload in another aircraft. See the applicable AC and TSO for additional guidance.
Display of radio altitude information	Minor	R	Minor	Not required for 14 CFR part 91 operations, Category I ILS. Loss of function may affect other equipment that depends upon radio altimeter.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of vertical speed information	Minor	R	Mino r or Major.	Not required for most 14 CFR part 91 operations. May be major classification when required by the operational requirements of parts 91 (Category II), 121, and 135 and it is considered required equipment essential to safe operation.
Display of flight guidance commands (Category I operation)	Minor	R	Major	Not required for 14 CFR part 91 operations, Category I ILS. For Category II ILS, an autopilot or flight director is required. Minor for loss of flight guidance commands for Category I operations providing the other normal cues remains for primary flight information. Loss of the sensor should remove the guidance command. The pilot should recognize it and use other displays. Misleading indication could cause the pilot to temporary maneuver the airplane if using erroneous guidance information.
Autopilot	Minor, with warning. Major, without warning.	R	Major, single axis and limited authority. Hazardous, multi-axis and limited authority. Catastrophic, if authority is unlimited.	Malfunction effects of autopilot hardovers are very dependent on the design and installation details. Maximum inputs (hardovers) or (slowovers) to aircraft primary control surfaces should not exceed aircraft structural limits. See AC 23.17C under section 23.1329 for additional information.
Autopilot guidance or flight director cue on display	Minor	Minor	Major for pitch. Minor for roll.	Pilot must monitor autopilot operation and disconnect autopilot to recover flight promptly. May cause go around and reductions in safety margins.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Autopilot, inability to disengage with A/P disconnect switch	Major	Major	Major	The pilot is assumed to overcome the servo slip clutches in both pitch and roll and able to maintain control of aircraft. Minor if the circuit breaker to disconnect the autopilot is readily available in flight.
Electrical-Electronic primary powered flight controls	Catastrophic	Minor	Hazardous to catastrophic	Assumes redundant electrical/electronic primary flight control systems with no manual reversion that provide independent control for each axis. Hazardous for loss of one channel on the lateral or longitudinal axis. Some fly-by-wire system designs may incorporate many solutions which mitigate the severity of the loss of a single channel. They may have three or four independent channels for pitch and roll, so the loss of one has little functional effect and control can be maintained with a single channel, although normally with the loss of some envelope protections. Additionally there may be mitigating factors such as inherent stability which can reduce hazards.
Stability augmentation	Variable	Minor	Variable	It needs to be evaluated on a case-by-case basis since it depends on aircraft stability and handling characteristics when installed and required to meet minimum performance and flight handling requirements.
Stick pusher	Hazardous, if loss is not annunciated. Major if the stall warning is functioning. Minor, if failure is annunciated and the stall warning is functioning.	Minor	Catastrophic to hazardous if the pilot is able to override or able for quick disconnect.	The system is installed to protect against a hazardous stall characteristic and/or unrecoverable catastrophic condition such as a deep stall. Assumes dual systems to prevent single-failure modes. Stick pusher malfunction with or without warning can be catastrophic depending on phase of flight and system attributes. Airplane response to stick pusher may be considered and pilot procedures may mitigate to a lower failure condition.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Stick shakers with Stall warning	Major without other means of stall warning and unannunciated loss of stall warning. Minor for annunciated loss of stall warning	Major without other means of stall warning and unannunciated loss of stall warning. Minor for annunciated loss of stall warning	Major without other means of stall warning.	Assumes that inherent airplane characteristics do not exist so the pilot is aware of being close to stall (for example, stick force changes, buffeting, etc.).
Trim control	Minor	Minor	Major, if manual trim. Catastrophic or hazardous for electrical.	Studies have shown trim runaways are not a significant problem if pilot takes quick corrective action. Major, for trim runaways if there is a trim-in-motion aural alert. Hazardous or catastrophic for trim runaways without a failure indication depending on trim authority and phase of flight.
Gear control	Major	Minor	Major	R
Brake control	Major, for airplanes ≥ 6,000 lbs. Minor, for airplanes < 6,000 lbs.	Major. Could be minor, if thrust reversers are installed.	Major	Electronic anti-skid and brake systems can cause significant ground handling problems if they malfunction under adverse conditions due to asymmetrical loading. Light airplanes braking loss is not as significant and can be reviewed on a case-by-case basis.
Display of trim indications	Minor	Minor	Variable	Each airplane has to be reviewed on a case-by-case basis. The most severe case is the phase of flight before takeoff. After takeoff, the trim position indication is not as critical because the pilot will adjust the trim position to relieve the control forces.
Display of gear indications	Minor	R	Minor	R

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of fuel level indication	Minor	Minor	Minor	Pilot is required to calculate fuel range and endurance during normal flight planning operations.
Display of powerplant indication tachometer	Minor	Minor	Minor	Assumes fixed pitch propeller and reciprocating engine; otherwise, a propeller governor will maintain the engine r.p.m. Turbofan and turbojet engines may need r.p.m. data for inflight restart capability. Refer to 14 CFR part 23, § 23.1311.
Display of powerplant Cylinder Head Temperature (CHT)	Minor	Minor	Minor	Assumes a CHT indicator is required. Refer to 14 CFR part 23, § 23.1305.
Display of powerplant indication coolant temperature	Minor	Minor	Minor	Refer to 14 CFR part 23, § 23.1305.
Display of powerplant indication oil pressure	Minor	Minor	Minor	Assumes oil temperature is used as a backup.
Display of powerplant indication oil temperature	Minor	Minor	Minor	Assumes oil pressure is used as a backup.

***Note:** This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of powerplant indication manifold pressure	Minor	Minor	Minor	Assumes backup use of CHT, Engine Gas Temperature (EGT), and possible fuel flow readings if installed.
Display of powerplant air inlet temperature	Minor	Minor	Minor	R
Display of powerplant indication fuel pressure	Minor	Minor	Minor	R
Display of powerplant indication fuel flow	Minor	Minor	Major	Manifold pressure and r.p.m. or torque indications can be used as an emergency backup to control power until a safe landing can be made.
Display of powerplant fire warning	Major	Major	Major	Required for commuter category and part 23 turbojet powered airplanes using special conditions. Part 23 airplanes usually have one fire warning system on board.
Display of powerplant indication thrust	Minor	Minor	Hazardous	System is not normally used in part 23 airplanes. Torque, Engine Pressure Ratio (EPR), EGT, or Turbine Inlet Temperature (TIT), fuel flow, and r.p.m. are normally displayed.

***Note:** This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Display of powerplant thrust reverser position	No effect	No effect	Major	No certification credit is given for enhanced performance when a thrust reverser is installed.
Thrust reversal	Minor	Minor	Variable (inadvertent deployment)	No certification credit is given for enhanced performance when a thrust reverser is installed. No credit can be given for a warning.
Display of powerplant torque	Minor	Minor	Major	Misleading torque could affect takeoff performance.
Display of powerplant propeller blade angle	No safety effect	No safety effect	No safety effect	System is not normally used in part 23 airplanes. Propeller governor would control r.p.m.
Electronic displays of significant powerplant parameters	Minor to Hazardous	R	Hazardous	Reversionary display is considered not available. If the risk of possible engine failure due to pilot mishandling can be mitigated by appropriate procedures or by EEC, the loss of function may be major or minor.
Visual warnings, cautions, and alerts	R	R	R	Failure conditions depend on the criticality of systems being monitored and pilot action required.
Display of air temperature	Minor	R	Minor	R

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	Classification of Failure Conditions			Analysis Consideration
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Overspeed warning	Minor	Minor	Minor	Airspeed may be used as a backup to the overspeed warning for continued safe flight and landing. Crew recognizes conditions by other equipment and procedures.
Primary weather radar	Minor to Major depended on the intended operations	R	Major	The loss could be major when the equipment is required by operational regulations. Also, Air Traffic guidance in some locations might not be available to provide hazardous weather information. It could be minor if there are appropriate AFM limitations.
Flight Information Service Weather	Minor	Minor	Minor	Normal operating procedures should states that the weather information should be used only as a strategic planning tool for pilot decision.
Electronic Chart on the MFD	Minor Major, if paperless cockpit.	Minor, if backup available	Major with own-ship position.	While we are not requiring any backup, we strongly recommend that AFMS normal procedure section recommend that the pilot carry a paper backup with at least all other necessary information to make a successful approach at their destination or alternate airport. In addition, the AFMS should contain emergency procedures for loss of approach charts on the MFD. A backup to the electronic charts on the MFD could be an Electronic Flight Bag with charts, paper approach charts of the destination and alternate airports, or a pilot simply make notes of minimums and all other necessary information to make a successful approach at their destination or alternate airport. When the own-ship position is shown, it is not considered the primary navigation display, so a primary navigation display is required.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 1 (CONTINUED)

Aircraft Function	**Classification of Failure Conditions**			**Analysis Consideration**
	Total Loss of Function	**Loss of Primary Means of Providing Function**	**Misleading and/or Malfunction Without Warning**	
Aural warnings	Major	R	Major	Aural alerts tend to be reserved for required flight crew's immediate corrective action. Failure conditions depend on the criticality of the system. Crew recognizes conditions by other equipment and procedures.
Electrical system indication	Minor	Minor	Major	Depends on crew reference and analysis.
Vacuum pressure indication	Minor	Minor	Major	Provides an indication that flight instruments are operating within power source limits.
Electrical power	Catastrophic, if primary flight instruments require electrical power.	Hazardous for IFR. Depends upon capability of secondary power system.	Installation dependent	Depends on electrical system loads and the criticality of the functions.

*****Note: This table is only intended to be a guide and is not a certification checklist since it may not include all the information necessary for an FHA on part 23 IFR Class I airplanes with its various functions and its intended use. This partial FHA does not reflect considerations needed to properly develop FHA. See paragraph 16 and its associated subparagraphs for more complete guidance. R = Reserved, intentionally left blank.

APPENDIX 2. SAMPLE FUNCTIONAL HAZARD ASSESSMENT (FHA) FORMAT

Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification
Display of attitude information to control roll and pitch	Loss of primary means of attitude information used for control in roll and pitch. Information from standby or other means still available.	All	Crew would not be able to use primary means of attitude information and would have to resort to standby or other means. As long as it is clear that the primary means cannot be relied upon, then using the standby or other means would create an increase in crew workload, but doubtful anything more severe. Hypothetical cases where it is not clear as to the integrity of the information may come under the "Misleading attitude information" case below.	Major	AC 23.1311-1C	Qualitative analysis. May require FTA May use PSSA or SSA
Display of attitude information to control roll and pitch	Loss of all means of attitude information.	All	If certified for IFR operation, the crew would not have sufficient information to maintain a proper attitude and would likely inadvertently exceed attitude limits, which could result in the loss of control of the aircraft.	Catastrophic	AC 23.1311-1C	Quantitative FTA and Qualitative analysis. May use PSSA or SSA

*Note: This sample FHA is intended to be a guide for format purposes only to illustrate what items should be considered when performing an FHA. Since other pertinent information regarding the type of airplane and its features is not provided, the technical content may not be appropriate for other airplanes.

APPENDIX 2. SAMPLE FUNCTIONAL HAZARD ASSESSMENT (FHA) FORMAT

Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition on Aircraft/Crew	Classification	Reference to Supporting Material	Verification
Display of attitude information to control roll and pitch	Incorrect attitude information on one display, but not on all displays (not misleading in nature).	All	Generally, this condition would be the incorrect attitude with warning on one means of attitude information. For this condition, the crew would realize that this information was incorrect. If there is any chance this would not be clear, the scenario would have to be considered "Misleading attitude information" as described below.	Major	AC 23.1311-1C	Qualitative analysis. May require FTA May use PSSA or SSA
Display of attitude information to control roll and pitch	Misleading attitude information. Note: Failure condition with misleading data provided to the autopilot that is handled with the autopilot failure conditions.	All	If certified for IFR operation, the crew would unknowingly follow incorrect attitude information, and inadvertently exceed attitude limits which could result in the loss of control of the aircraft.	Catastrophic	AC 23.1311-1C	Quantitative FTA and Qualitative analysis. May use PSSA or SSA
Display of powerplant indication oil pressure	Total Loss of oil pressure display	All	Assumes oil temperature is used as a backup	Minor	AC 23.1311-1C	Design and Installation Appraisal
(Next function)	(Next failure condition, and so on)					

*Note: This sample FHA is intended to be a guide for format purposes only to illustrate what items should be considered when performing an FHA. Since other pertinent information regarding the type of airplane and its features is not provided, the technical content may not be appropriate for other airplanes.

APPENDIX 3. CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR

1. The purpose of this material is to provide guidance for calculating the "average probability per flight hour" for a failure condition so that it can be compared with the quantitative requirements of § 23.1309. The process of calculating the "average probability per flight hour" for a failure condition is a four-step process and based on the assumption that the life of an aircraft is a sequence of "average flights."

Step 1: Determination of the "average flight;"
Step 2: Calculation of the probability of a failure condition for a certain "average flight;"
Step 3: Calculation of the "average probability per flight" of a failure condition; and
Step 4: Calculation of the "average probability per flight hour" of a failure condition.

a. Determination of the "average flight:" The "average probability per flight hour" is to be based on an "average flight." The applicant should estimate the average flight duration and average flight profile for the fleet of aircraft 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 estimate of the cumulative flight hours divided by the cumulative aircraft flights for the service life of the aircraft. The average flight profile should be based on the operating weight and performance expectations for the average aircraft when flying a flight of average duration in an ICAO standard atmosphere. The duration of each flight phase (e.g., 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 average airport should be considered where appropriate and added to the average flight time to obtain "average flight--block time." The average flight duration and profile should be used as the basis for determining the "average probability per flight hour" for quantitative safety assessment as means of compliance with this AC.

b. Calculation of the probability of a failure condition for a certain "average flight:" The probability of a failure condition occurring on an "average flight" should be determined by structured methods (see ARP 4761 for various methods) and should consider all elements (e.g., combinations of failures and events) that contribute to a failure condition. 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 a failure condition. The probabilities of the basic events (component or part level failures) that contribute to the probability of a failure condition should consider the following:

(1) The individual part, component, and assembly failure rates utilized in calculating the "average probability per flight hour" should be estimates of the mature constant failure rates after infant mortality and prior to wear-out. Alternatively, a non-constant failure rate can be used (i.e. Weibull or other accepted means). Inspection intervals or component life limits employed to protect against wear out are to be placed in chapter 4 or 5 of the maintenance manual. In either case, the failure rate should be based on all causes of failure (operational, environmental, etc.). Where available, service history of same or similar components in the same or similar environment should be used.

(2) If the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant "at risk" time for the "average flight."

(3) If one or more failed elements in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation has to consider the relevant exposure times (e.g., time intervals between maintenance checks/ inspections). In such cases, the probability of the failure condition increases with the number of flights during the latency period.

(4) 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 condition occurring on an "average flight." It is assumed that the "average flight" can be divided into n phases (e.g., phase 1, ... , phase n). Let T_F the "average flight" duration, T_j the duration of phase j and t_j the transition point between T_j and T_{j+1}, j = 1, ... , n . I.e.

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

Let $\lambda_j(t)$ the failure rate function during phase j, i.e. for $t \in [t_{j-1}, t_j]$.

Remark: $\lambda_j(t)$ may be equal 0 for all $t \in [t_{j-1}, t_j]$ for a specific phase j.

Let P_{Flight} (failure) the probability that the element fails during one certain flight (including non-flying time) and $P_{Phase\ j}$ (failure) the probability that the element fails in phase j.

Two cases are possible:

(i) The element is checked operative at the beginning of a certain flight. Then

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

(ii) The state of the item is unknown at the beginning of a certain flight. Then

$$P_{Flight}\ (\text{failure}) = P_{prior}\ (\text{failure}) + \left(1 - P_{prior}\ (\text{failure})\right) \cdot \left(1 - \prod_{i=1}^{n} \exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)\,dx\right)\right)$$

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

Note: For the two mathematical operators, $\prod$ is a product sign and $\in$ is element of.

(5) 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 a failure condition.

c. Calculation of the "average probability per flight" of a failure condition: The next step is to calculate the "average probability per flight" for a failure condition, that is, the probability of a 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 aircraft life) have to be calculated, summed up, and divided by the number of flights during that period. The principles of calculating are described below and are in more detail in ARP 4761.

$$P_{Average\ per\ Flight}(\text{failure condition}) = \frac{\sum_{k=1}^{N} P_{Flight\ k}(\text{failure condition})}{N}$$

Note**:** N is the number of all flights during the relevant time, and $P_{Flight\ k}$ is the probability that a failure condition occurs in flight k. In the special case of a duplex system (i.e., one component failure latent, the other detected), this method results in an "average probability per flight," which equals the product of both failure rates multiplied by the "average flight" duration T_F multiplied by one-half (50 percent) of the relevant exposure time.

d. Calculation of the "average probability per flight hour" of a failure condition: Once the "average probability per flight" is 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.

$$P_{Average\ per\ FH}(\text{failure condition}) = \frac{P_{Average\ per\ Flight}(\text{failure condition})}{T_F}$$