**NATIONAL TRANSPORTATION SAFETY BOARD**

Office of Aviation Safety
Washington, D.C. 20594

March 09, 2015

**Attachment 16**

**FAA Advisory Circular, 23.1309-1D, dated 1-16-2009**

# SYSTEM SAFETY

**DCA15MA019**

U.S. Department
of Transportation
**Federal Aviation**
**Administration**

# Advisory Circular

**Subject: SYSTEM SAFETY ANALYSIS AND ASSESSMENT FOR PART 23 AIRPLANES**

**Date:** 1/16/09
**Initiated by:** ACE-100

**AC No:** 23.1309-1D

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(a) and (b) (Amendment 23-49) 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 alternative 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.

s/ James E. Jackson
Acting Manager, Small Airplane Directorate
Aircraft Certification Service

# TABLE OF CONTENTS

**Section** **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(a) and (b) (Amendment 23-49) for equipment, systems, and installations in Title 14 Code of Federal Regulations (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 "shall" or "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 "shall" and "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, Federal Aviation Administration (FAA) part 23 airplane type certification engineers, and designees.

**3. Cancellation**. **This AC cancels** AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes, dated March 12, 1999.

It also cancels 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 23-49).

**b. ACs, orders, and policy.** You may access the ACs, notices, orders, and policy on the FAA website: www.faa.gov. You may obtain copies of current editions of the following publications free from the U.S. Department of Transportation, Subsequent Distribution Office, M-30, Ardmore East Business Center, 3341 Q 75th Avenue, Landover, MD 20785.

| | |
|---|---|
| AC 20-115B | RTCA, Inc., Document RTCA/DO-178B |
| AC 20-152 | RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware |
| AC 21-16E | RTCA, Inc. Document RTCA/DO-160E, Environmental Conditions and Test Procedures for Airborne Equipment |
| AC 23-17B | Systems and Equipment Guide for Certification of Part 23 Airplanes and Airships |
| AC 23.1311-1B | Installation of Electronic Displays in Part 23 Airplanes |
| AC 20-136A | Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning |
| AC 20-158 | The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF) Environment |
| AC 21.101.1 | Establishing the Certification Basis of Changed Aeronautical Products |
| AC 20-138A | Airworthiness Approval of Global Navigation Satellite System (GNSS) Equipment |
| AC 25.1309-1A | System Design and Analysis |
| AC 33.75-1 | Guidance material for 14 CFR section 33.75, Safety Analysis |
| Order 8110.4C | Type Certification |
| Policy Statement | ACE100-2004-10024; Installation of Electronic Engine Control for Reciprocating Engine |

**c. Industry documents.** You may obtain copies of current editions of the following publications as follows. 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-160E | Environmental Conditions and Test Procedures for Airborne Equipment |
| RTCA/DO-178A/B | 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 Society of Automotive Engineers (SAE), Inc., documents are available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001 or from their website at www.sae.org.

| | |
|---|---|
| ARP 4754 | Certification Considerations for Highly Integrated or Complex Aircraft Systems |
| ARP 4761 | Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment |

**Note**: ARP's 4754 and 4761 state that these documents describe guidelines and methods of performing the safety assessment for certification of civil aircraft. They further state that the guidance material in these ARP's were developed in the context of 14 CFR part 25 and the Joint Aviation Requirements 25 (JAR 25). They are primarily associated with showing compliance with part 25, § 25.1309/JAR 25.1309. A subset of this material may be applicable to non-25.1309 equipment, such as other requirements in parts 23, 25, 27, 29, and 33. However, some of the processes included are not necessary or appropriate for part 23 airplanes. ARP 4754 contains information on applying specific engineering methods that an applicant may wish to utilize in whole or in part.

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 ARP's if there is a conflict. Contact the Small Airplane Directorate if there are conflicts with other guidance or ACs and this AC.

## 5. Applicability.

**a.** This AC is generally applicable only to the original applicant seeking issuance of a type certificate (TC), amended type certificate (ATC), and supplemental type certificate (STC) for the initial approval of the new type design or a change in the type design. This document addresses general applicability, and it should not be utilized to replace any specific guidance intended for individual types of equipment, systems, and installations. For simple and conventional mechanical or analog electromechanical systems, or both, with well established design and

certification processes and where the installation is not complex, the single-fault concept and experience that are based on service-proven designs and engineering judgment are appropriate. In this case, a Functional Hazard Assessment (FHA), a design appraisal, and an installation appraisal addressed in this AC may satisfy § 23.1309(b).

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

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

**(1)** Systems and installations approved only as part of a type-certificated engine or propeller, and

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

> **Note:** The current Small Airplane Directorate Standards Office policy on electronic engine control (EEC) installation in small airplanes, under § 23.1309, has been to issue two special conditions. The first special condition applies § 23.1309(a) through (e) to the propulsion system installation since § 23.1309(f)(1) may exclude the requirements that should apply. The second special condition is protection of the EEC from exposure to High Intensity Radiated Fields (HIRF). The § 23.1309 certification evaluation should be limited to the interfaces of the engine/control system and verification that none of the assumptions made for part 33 certification of the engine are invalidated by the installation. The analysis should not extend into data submitted and approved as part of the engine certification program. See policy statement, Installation of Electronic Engine Control for Reciprocating Engine; PS-ACE100-2004-10024, for more information.

## 6. Regulations and AC background.

### a. Regulation.

**(1)** Amendment 23-14 adopted the original airworthiness standards in § 23.1309(a). Before Amendment 23-14 to part 23 (effective December 20, l973), neither Part 3 of the Civil Air Regulations (CAR) nor 14 CFR part 23 contained safety requirements in § 23.1309 for equipment, systems, and installations for 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 Federal Aviation Administration (FAA) issued § 23.1309 to provide for an acceptable level of safety for such equipment, systems, and installations. When the FAA adopted § 23.1309 (Amendment 23-14), it did not envision that systems that perform critical

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

**(3)** With the adoption of Amendment 23-41 (effective November 26, 1990), § 23.1309 retained 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 finds it necessary or desirable to include complex systems, or systems that perform critical functions, Amendment 23-41, § 23.1309, provides additional requirements for identifying such equipment, systems, and installations. It also provides additional requirements needed for certification. This amendment permitted the approval of more advanced systems having the capability to perform critical functions.

**(4)** With the adoption of Amendment 23-49 (effective March 11, 1996), § 23.1309(a)(4) was amended to correct the error in Amendment 23-41, which inadvertently removed the commuter category requirement. Amendment 23-34 originally added the commuter category requirements of § 23.1309(a)(4) to part 23 as § 23.1309(d), but the requirements were inadvertently not incorporated into § 23.1309 as adopted by Amendment 23-41. Amendment 23-49 corrected this error by again adding the requirements to part 23 as § 23.1309(a)(4).

**(5)** Qualitative and quantitative analyses are often used in assessing the acceptability of complex designs that have a high degree of integration, that use new technology, that 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 both to support experienced engineering and operational judgment and to supplement qualitative analyses and tests. Numerical probability ranges, associated with the terms used in § 23.1309(b), are accepted for evaluating quantitative analyses that have a logical and acceptable inverse relationship between the probability and severity of each failure condition.

**b. AC.**

**(1) Revision to AC.**

**(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 for GA airplanes.

**(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). These installations, especially on the Class I and II airplanes, would have been too costly for these airplanes without the establishment of the four-tier certification classes of airplanes as shown in paragraph 13. In a study of the Capstone program, it was determined that the four-tier certification classes has demonstrated significant operational safety benefit and reduced accident rates.

**(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, the largest single cause, often are 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. An increase in avionics equipage rates that improved pilot situational awareness or simplify the task had a significant positive impact on the GA accident rate. The Air Safety Foundation of the Aircraft Owners and Pilots Association conducted a study of safety effects of glass cockpits and they concluded that technologically advanced aircraft provide added situational awareness tools that have dramatically improved aspects of GA safety. Technologically advanced aircraft has delivered 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 available to the pilot 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, 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 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 and will likely result in the long-term replacement of nearly all avionics and instrument equipment in the existing fleet as well as in new production aircraft. Facilitating the installation of safety equipment should enhance NAS efficiency and safety. If GA is to operate within a revised NAS system, new technologies should be available and affordable for GA aircraft. With the four-class certification 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 | Code of Federal Regulations for the Federal Aviation Regulation |
| AC | Advisory Circular |
| 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 |
| JAR | Joint Aviation Requirements |
| 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 |
| 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 and assessment.** The terms "analysis" and "assessment" are used throughout. Each has a broad definition and the two terms are, to some extent, interchangeable. However, the term “analysis” generally implies a more specific and more detailed evaluation, while the term “assessment” may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application (for example, FTA, Markov analysis, PSSA, etc.).

**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. 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.

**e. 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.

**f. 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.

**g. Complex.** 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 these types of systems, 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.

**h. 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.

**i. Conventional.** 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 and usually do not contain software or complex hardware that require compliance by detailed processes. See the definitions for complex and simple for more information.

**j. 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.”

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

**l. 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 same levels as the DALs for the safety assessment process. See section 22 for more information.

**m. 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.

**n. 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.

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

**p. 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."

**q. 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 lightning strikes, 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.

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

**s. 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.

**t. 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.

**u. 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.

**v. Failure conditions.** A condition having an affect 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 affect 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 well 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.

**w. 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 complete recognizable operational capability (for example, an airplane heading is a function). One or more systems may contain a specific function or one system may contain multiple functions.

**x. 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.

**y. Hazard.** A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or combinations thereof. This term is normally used in regulations and policy that is intended for single malfunctions or failures that are considered probable on the basis of 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.

**z. 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.”

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

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

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

**dd. 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.

**ee. 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.

**ff. 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.

**gg. Probable.** Probable as defined for section 23.1309(a), as a probable malfunction or failure is any single malfunction or failure that is considered probable 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 probable failure condition when used for a safety assessment process.

**hh. 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.

**ii. Primary function.** A function that is installed to comply with the applicable regulations for the required function and that 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 of all the following: altitude, airspeed, aircraft heading (direction) and attitude located directly in front of the pilot in a fixed layout in accordance with § 23.1321. For controls such as brake or engine controls, the primary may be the backup systems. For example, a mechanical backup brake system could be considered to be the primary with regard to meeting the requirements and the electronic brake system would be the secondary.

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

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

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

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

**nn. 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.

**oo. 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.

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

**qq. Similarity.** The process of showing that the equipment type, form, function, design, and installation is nearly identical to already approved equipment. The safety and operational characteristics and other qualities of the new proposed installation should have no appreciable affects on the airworthiness of the airplane.

**rr. Simple.** Usually a conventional 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” for more information.

**ss. 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 failures 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.

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

**uu. 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.**

**a.** If the certification basis for the airplane is Amendment 23-14, § 23.1309(a) (See NOTE below) 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 meet the single-fault concept should comply with the requirements of § 23.1309(a) if the guidance in the next section 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.

**Note:** All references to regulatory sections in this AC refer to § 23.1309, as amended by Amendment 23-49. 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 in paragraphs (a), (b), and (c) of § 23.1309, as amended by Amendment 23-14.

**b.** 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. If the system contains software or complex hardware, a system safety assessment will be needed to determine the level of certitude for the processes in RTCA/DO-178B or RTCA/DO-254 or equivalent. 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.

**10. Showing compliance with the requirements 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 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, and these steps are listed below.

**(1)** Evaluate all airplane systems and 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:

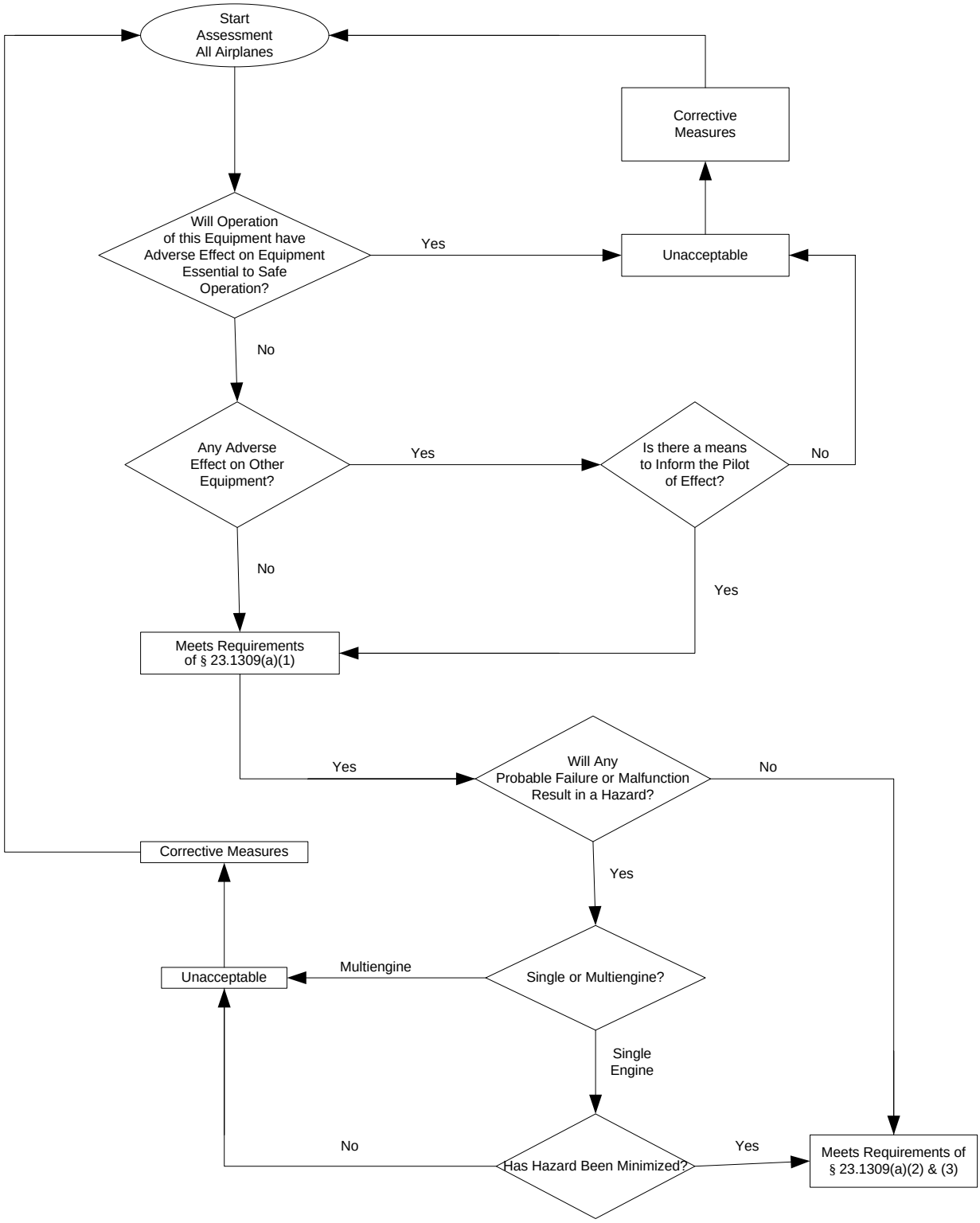
**(a)** If it can be determined that the operation of the installed equipment will not adversely affect equipment essential to safe operation, the requirements of § 23.1309(a)(1)(i) have been satisfied; and

**(b)** If it is determined that the operation of the installed equipment has an adverse affect 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)** All equipment should be evaluated for general installation hazards. These types of hazards would normally include those hazards that would directly compromise the safety of the airplane or its occupants, such as fire, smoke, explosion, toxic gases, depressurization, etc. A hazard could also result from loss of 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.

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



**(b)** Systems and equipment essential to safe operation should 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 the past malfunctions or failures have not resulted in hazards and there are no unresolved problems.

**(c)** Hazards that have been 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 should be minimized. To minimize is to reduce, lessen, or diminish a hazard to the least practical amount with current technology and materials. The least practical amount is that point at which the effort to further reduce a hazard significantly exceeds any benefit in terms of safety derived from that reduction. Additional efforts would not result in any significant improvements of 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.

**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 Title 14 Code of Federal Regulations (14 CFR) 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 airplane flight manual (AFM) should have clear and precise corrective procedures for handling the failure without an excessive increase in workload.

**c.** Service history for similar installations may be utilized to meet part or all of this requirement if a system or installation has 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 claims of similarity to a previous installation. More information is available in Order 8110.4C.

**12. Application of § 23.1309(b), as adopted by Amendments 23-41 and 23-49.**

**a.** If the certification basis is Amendment 23-41 or later, the requirements of § 23.1309(b) are applicable. 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 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 14 CFR part 23 standards. The relationship between probability and severity of failure condition effects is 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.

**13. Four certification classes of airplanes.**

**a.** The four-certification classes of airplanes for this AC are shown in figure 2. They are as follows: Class I (Typically SRE under 6,000 pounds (lbs.) (Maximum Certificated Gross Takeoff Weight)), Class II (Typically MRE, MTE and STE, under 6,000 pounds), Class III (Typically SRE, STE, MRE, and MTE equal or over 6,000 pounds), and Class IV (Typically Commuter Category). The acronyms for these airplanes in the four classes of part 23 airplanes are Single Reciprocating Engine (SRE), Multiple Reciprocating Engine (MRE), Single Turbine Engine (STE), and Multiple Turbine Engine (MTE).

**b.** Numerical values are assigned for use in those 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 new probability standards

are based on historical accident data, systems analyses, and engineering judgment for each class of airplane.

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

| **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) DALs (Note 2)** | | | | |
| **Class I** (Typically SRE under 6,000 lbs.) | No Probability or SW & HW DALs Requirement | $<10^{-3}$<br>Note 1 & 4<br>P=D, S=D | $<10^{-4}$<br>Notes 1 & 4<br>P=C, S=D<br>P=D, S=D(Note 5) | $<10^{-5}$<br>Notes 4<br>P=C, S=D<br>P=D, S=D(Note 5) | $<10^{-6}$<br>Note 3<br>P=C, S=C |
| **Class II** (Typically MRE, STE, or MTE under 6000 lbs.) | No Probability or SW & HW DALs Requirement | $<10^{-3}$<br>Note 1 & 4<br>P=D, S=D | $<10^{-5}$<br>Notes 1 & 4<br>P=C, S=D<br>P=D, S=D(Note 5) | $<10^{-6}$<br>Notes 4<br>P=C, S=C<br>P=D, S=D(Note 5) | $<10^{-7}$<br>Note 3<br>P=C, S=C |
| **Class III** (Typically SRE, STE, MRE, & MTE equal or over 6000 lbs.) | No Probability or SW & HW DALs Requirement | $<10^{-3}$<br>Note 1 & 4<br>P=D, S=D | $<10^{-5}$<br>Notes 1 & 4<br>P=C, S=D | $<10^{-7}$<br>Notes 4<br>P=C, S=C | $<10^{-8}$<br>Note 3<br>P=B, S=C |
| **Class IV** (Typically Commuter Category) | No Probability or SW & HW DALs Requirement | $<10^{-3}$<br>Note 1 & 4<br>P=D, S=D | $<10^{-5}$<br>Notes 1 & 4<br>P=C, S=D | $<10^{-7}$<br>Notes 4<br>P=B, S=C | $<10^{-9}$<br>Note 3<br>P=A, S=B |

Note 1: Numerical values indicate an order of probability range and are provided here as a reference. The applicant is usually not required to perform a quantitative analysis for minor and major failure conditions. See figure 3.
Note 2: The alphabets denote the typical SW and HW DALs for most primary system (P) and secondary system (S). For example, HW or SW DALs Level A on primary system is noted by P=A. See paragraphs 13 & 21 for more guidance.
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.
Note 5. A reduction of DALs applies only for navigation, communication, and surveillance systems if an altitude encoding altimeter transponder is installed and it provides the appropriate mitigations. See paragraphs 13 & 21 for more information.

**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 $1 \times 10^{-4}$ per flight hour for single-engine airplanes under 6,000 pounds. Furthermore, from accident data bases, 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 $1 \times 10^{-5}$ 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 $1 \times 10^{-5}$ was thus apportioned equally among these failure conditions, which resulted in an allocation of not greater than $1 \times 10^{-6}$ to each. The upper limit for the average probability per flight hour for catastrophic failure conditions would be $1 \times 10^{-6}$, 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.

**d.** Acceptable criteria for DALs levels of part 23 airplanes are shown in figure 2. Note 5 allows an additional reduction of DALs for navigation, communication, and surveillance systems if an altitude encoding altimeter transponder is installed and it provides the appropriate mitigations. This option does not apply to CAT II/III operations. DALs in figure 2, under Note 5, have been determined if an altitude encoding altimeter transponder is installed and provides the appropriate mitigations so that failure of navigation and communication systems used for IFR operations do not affect other airplanes. If the transponder is based on DAL, the DAL should be developed to at least Level C. If this option is used, the AFM must include a limitation such as, "A transponder with a valid altitude reporting mode must be operating for IFR operations unless otherwise instructed by ATC." Proper separation is provided by the Air Traffic Control (ATC) surveillance system and Traffic Collision Avoidance System (TCAS) equipped airplanes in IFR operations in the NAS or other equivalent airspace systems.

**e.** The criteria shown in figure 2 directly reflect the historical accident and equipment probability of failure data in the Civil Air Regulations (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 ability of the pilot to safely handle various types of system failures in small airplanes. The criteria considered over 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 since it considers the installed airplane systems, events, and factors.

**f.** These classes were defined based on the way accident and safety statistics are currently collected. Generally, the classes deal with airplanes of historically 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.

**g.** 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 example, 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.

**h.** 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.

**i.** This AC uses terminology similar to AC 25.1309-1A. However, the specific means of compliance for § 25.1309 of part 25 are defined differently due to the higher level of safety required for transport category airplanes.

**14. Safety assessments.**

**a**. The applicant is responsible for identifying and classifying each failure condition and for choosing the methods for safety assessment. The applicant should then obtain early concurrence of 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.

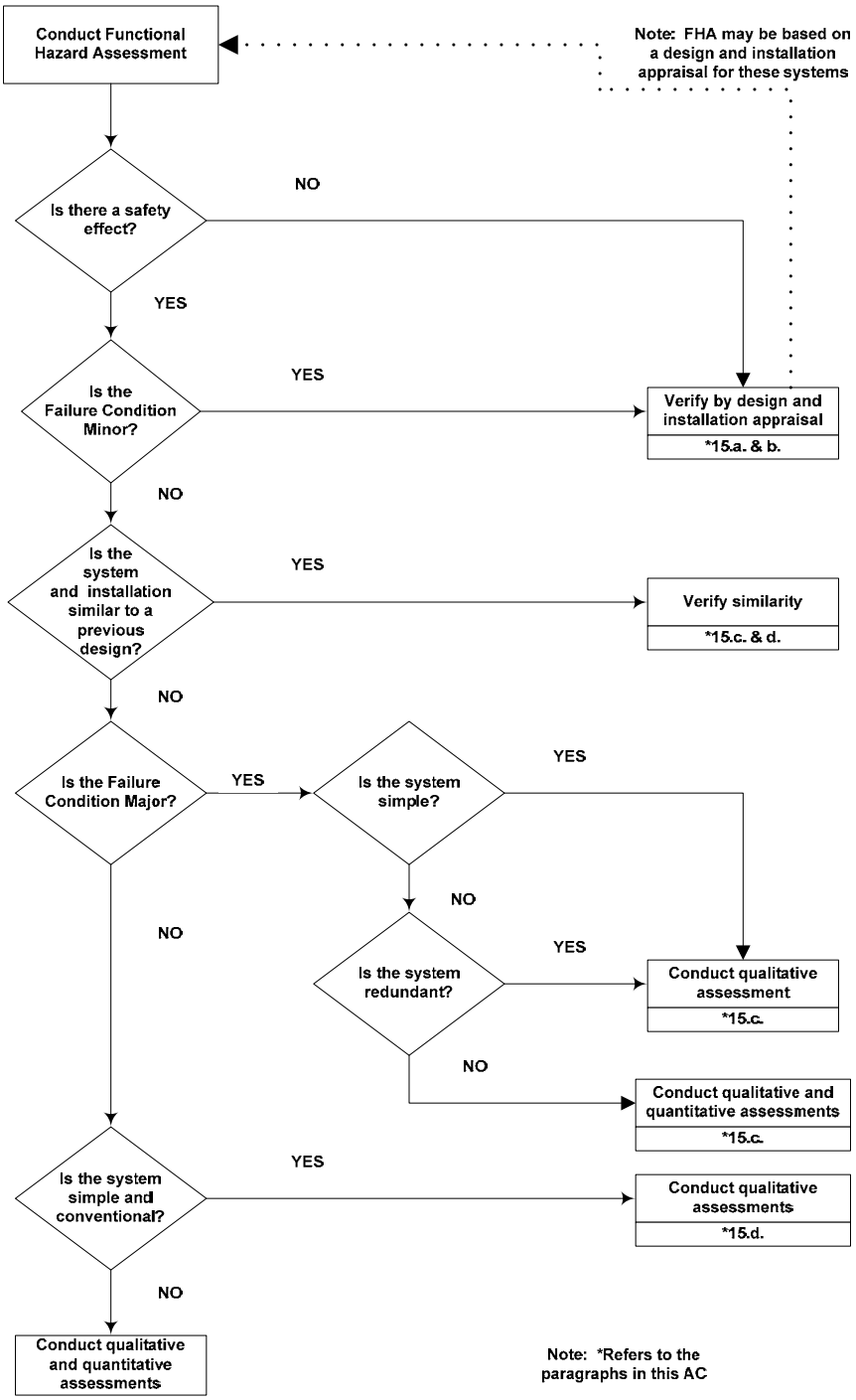
**b.** Functional hazard assessment (FHA).

**(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 hence function, interrelationships are relatively simple, it may be feasible to conduct separate FHA's for each system providing any interface aspects are properly considered and are easily understood. However, a top down approach, from an airplane level perspective, should be taken in planning and conducting 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 $1 \times 10^{-5}$. In addition, the primary system should have software and complex hardware DALs of C and, if required, the secondary system 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 airplane type and configuration evaluated. 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 provided 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, and is 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 are 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 the 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 assessment of the specific system or airplane in question. It can be used to arrive at the appropriate failure conditions for this specific system by similarity to or by interpolating between the example systems. It does not, by itself, necessarily provide 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 the traditional airplane and traditional architectures. Because § 23.1309 is a regulation of general requirements, it 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 that may be considered in an FHA for systems installed in this class of airplane. Usually, support from Air Traffic Control is not considered as a mitigating factor.

**15. 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 the 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 an 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, 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 sometimes necessary to conduct a qualitative functional 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 and 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 shall 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.

**16. 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) 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) 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. These 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 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 (for example, 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, that 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.

**17. 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, that have 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 methods of analyses.

**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 concurrence of the certification authority of an acceptable classification of the failure conditions and probability for each 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 in case there are changes.

**f.** The details on how to calculate the "average probability per flight hour" for a failure condition are given in Appendix 3 of this AC. 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 14 CFR 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.

**18. Testing and compliance with the requirements of §§ 23.1301 and 23.1309.**

**a.** Testing is an important aspect of the overall compliance processes with §§ 23.1301 and 23.1309. The applicant should conduct bench, ground and flight testing necessary to validate hazard classifications, acceptability of crew procedures, human factors, and other assumptions made during the safety analysis processes. 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 delegated FAA witness in accordance with Order 8110.4C, Type Certification. Prior to entry into TIA, the applicant should be able to show at least 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 reliability testing during certification to ensure required functions to demonstrate an acceptable level of functional reliability in addition to other required certification tests and analyses. These tests are meant to

verify availability, accuracy, and reliability of the system. The FAA expects the applicant to show that the system does not exhibit unintended or undesirable functionality for required flight critical functions that have failure conditions that are major, hazardous, or catastrophic. The FAA also expects that failures, malfunctions, and design errors that would have a potential safety hazard will only occur at a frequency appropriate for the associated failure condition and classification.

**19. Operational and maintenance considerations.**

**a. Flight crew and maintenance task.** These tasks, which are related 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.

**b. 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.

**c. 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 time period 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).

**20. Electromagnetic protection for electrical/electronic systems**. Current trends indicate increasing reliance on electrical/electronic systems for safe operations. For systems that perform flight, propulsion, navigation, and instrumentation functions, electromagnetic effects, environmental effects, and environmental qualifications should be considered. 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 23-17, AC 20-136, and AC 20-158.

**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 provides 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(b). Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components by direct inspection and by other direct verification methods capable of completely characterizing the performance of the system. These direct techniques may still be appropriate for simple systems, which perform a limited number of functions and 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. Criteria for software DALs of part 23 airplanes.** The DALs in figure 2 and throughout this AC are also intended to 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 considered 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, granted to complex hardware DALs D in AC 20-152, will only apply for minor failure conditions and it 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.** There may be significant difference in the guidance provided on the use of system architecture for determination of the appropriate DALs. The FAA recognizes that consideration of system architecture for this purpose is appropriate in some cases. This AC, in figure 2, 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. These levels should be used unless there are some unique architecture considerations and there is specific policy, guidance, or approval by the Small Airplane Directorate. If the Small Airplane Directorate has established specific guidance or policy for these levels, then the approval can made by the Aircraft Certification Office. Where apparent differences exist between these two documents on this subject, then the guidance contained in ARP 4754 should only be used if additional credit for architecture is requested for hazardous or catastrophic failure conditions in Class IV, commuter category airplanes. For commuter category airplanes, the guidance in ARP 4754 is more likely to be appropriate since its DALs are higher.

**f.** Equipment installed in part 23 airplanes that performs functions addressed by TSO standards should meet applicable TSO standards, but the equipment is not required to have TSO authorization. The TSO data should include the equipment complex hardware and software DALs. For both TSO and non-TSO equipment, the complex hardware and software DALs should be checked against the installation requirements by the safety assessment and figure 2.

**22. Information only note for future policy.**

**a.** At the time this AC was being developed for issuance, SAE S-18, Airplane Safety Assessment Committee, was revising ARP 4754 and ARP 4761. The committee is planning new concepts for (DAL)and Design Assurance Levels. These SAE documents are preliminary draft guidelines for assigning the DALs that start from the aircraft/system level and end at the item/component level. The DAL assignments for the aircraft and system function are determined during the airplane and system safety assessment processes, specifically the FHA.

**b.** The committee considerations for the DAL assignment 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. As previously stated, these documents are in preliminary draft stages; therefore, these concepts are not considered in this AC. When these documents are approved, we will consider them in the next revision of this AC.