Designation: F3309/F3309M – 21

Standard Practice for Simplified Safety Assessment of Systems and Equipment in Small Aircraft[1]

This standard is issued under the fixed designation F3309/F3309M; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This practice covers methods for conducting a simplified safety assessment of aircraft systems and equipment. The material was developed through open consensus of international experts in general aviation. This information was created by focusing on Level 1 and Level 2 Normal Category aeroplanes employing conventional systems. The content may be more broadly applicable. It is the responsibility of the Applicant to substantiate broader applicability as a specific means of compliance. If the criteria specified within this simplified practice is deemed not to be relevant to a particular application, the Applicant should use the safety assessment process defined in Practice F3230. The topics covered within this practice are: Procedural Flowchart, Failure Condition Identification and Classification, Safety Objectives, Design and Installation Appraisal, Qualitative Analysis of Failure Conditions, Common Mode Analysis, Use of Similarity, and Documentation.

1.2 An applicant intended to propose this information as Means of Compliance for a design approval must seek guidance from their respective oversight authority (for example, published guidance from applicable CAA) concerning the acceptable use and application thereof. For information on which oversight authorities have accepted this standard (in whole or in part) as an acceptable Means of Compliance to their regulatory requirements (hereinafter "the Rules"), refer to the ASTM Committee F44 web page (www.astm.org/COMMITTEE/F44.htm).

1.3 *Units*—This practice may present information in SI units, English Engineering units, or both; the values stated in each system may not be exact equivalents. Each system shall be used independently of the other; combining values from the two systems may result in nonconformance with the standard.

1.4 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.5 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 Following is a list of external standards referenced throughout this practice; the earliest revision acceptable for use is indicated. In all cases later document revisions are acceptable if shown to be equivalent to the listed revision, or if otherwise formally accepted by the governing civil aviation authority; earlier revisions are not acceptable.

2.2 *ASTM Standards:*[2]

F3060 Terminology for Aircraft

F3061/F3061M Specification for Systems and Equipment in Small Aircraft

F3230 Practice for Safety Assessment of Systems and Equipment in Small Aircraft

F3232/F3232M Specification for Flight Controls in Small Aircraft

2.3 *SAE Recommended Practices:*[3]

SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

2.4 *Federal Aviation Administration:*[4]

AC 23.1309-1E System Safety Analysis and Assessment for Part 23 Airplanes

AC 25.1309-1A System Design and Analysis

AC 43.13-1B Acceptable Methods, Techniques and Practices – Aircraft Inspection and Repair

[1] This practice is under the jurisdiction of ASTM Committee F44 on General Aviation Aircraft and is the direct responsibility of Subcommittee F44.50 on Systems and Equipment.

Current edition approved July 15, 2021. Published July 2021. Originally approved in 2018. Last previous edition approved in 2020 as F3309/F3309M–20. DOI: 10.1520/F3309_F3309M-21.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from SAE International (SAE), 400 Commonwealth Dr., Warrendale, PA 15096, http://www.sae.org.

[4] Available from Federal Aviation Administration (FAA), 800 Independence Ave., SW, Washington, DC 20591, http://www.faa.gov.

AC 43.13-2B Acceptable Methods, Techniques and Practices – Aircraft Alterations

3. Terminology

3.1 Terminology specific to the system safety assessment process is contained in Practice F3230. Terminology specific to this standard is provided below. For general terminology, refer to Terminology F3060.

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *active failure*—a failure is active if it is not latent.

3.2.2 *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.

3.2.3 *latent failure*—a failure is latent until it is made known to the flight crew or maintenance personnel.

3.2.4 *on the order of*—used to allow some tolerance on meeting the stated quantitative requirement. For purposes of this practice, a predicted failure rate or probability is considered "on the order of" when the result is calculated to be no more than half an order of magnitude higher than the stated quantitative objective. The more severe the failure condition being considered is, the more conservative the analysis is expected to be in order to use this allowance.

4. Procedure

4.1 The flowchart shown in Fig. 1 provides an overview of the simplified safety assessment process.

4.1.1 The following abbreviations are used in the flowchart shown in Fig. 1:

4.1.1.1 FC – failure condition

4.1.1.2 NSE – Negligible Safety Effect

4.1.1.3 MIN – Minor

4.1.1.4 MAJ – Major

4.1.1.5 HAZ – Hazardous

4.1.1.6 CAT – Catastrophic

4.2 *Failure Condition Identification and Classification*—An assessment of the aircraft and system functions must be performed to identify and classify the various failure conditions associated with each function; refer to Table 1. A Functional Hazard Assessment (FHA) in accordance with the methodology outlined in SAE ARP4761 is one means of performing this assessment; however, other simpler methodologies may be employed as appropriate to the complexity of the system(s) and the availability of published guidance.

4.3 *Safety Objectives*—The assessment described in the subsequent paragraphs of this practice must be completed to:

4.3.1 Show that each failure condition identified by the analysis specified in 4.2 meets the probability objectives shown in Table 2, and

4.3.2 To ensure that no other hazard has been introduced because of the system installation.

4.4 *Design and Installation Appraisal*—A design and installation appraisal must be performed for all system and equipment installations.

4.4.1 *Design Appraisal*—This is a qualitative appraisal of the integrity and safety of the system design. An effective appraisal requires experienced judgment. The design features that provide integrity and safety must be explained in a form that are easy to follow. The use of system architecture/block diagrams are effective ways to aid the understanding of the system. Other tools that can aid the design appraisal include an extended FHA table where the effects listed in the approved FHA can be shown along with the failure mitigations. Integrity and safety considerations like the use of aerospace components, component qualification, independence, separation, and redundancy should also be discussed as appropriate.

4.4.2 *Installation Appraisal*—This is a qualitative appraisal of the integrity and safety of the installation. An effective appraisal requires experienced judgment. The installation features must be presented in forms that are easy to follow such as installation drawings, equipment installation requirements, and any required analyses. Deviations from normal, industry-accepted installation practices, for example AC 43-13, need to be evaluated. The appraisal must consider any potential interference with other aircraft systems and issues introduced by maintenance. In general, common design practice provides physical and functional isolation from components contributing to the Negligible or Minor failure conditions from the components that are essential to safe operation. For systems with major, hazardous, or catastrophic failure conditions, the potential for events or influences outside of the systems concerned that might invalidate independence must also be considered.

4.5 *Qualitative Analysis of Failure Conditions*—The following subsections define the requirements that must be addressed for failure conditions identified in 4.2.

4.5.1 Except as provided in 4.5.2, for failure conditions classified as Negligible, Minor, or Major, no additional qualitative analysis beyond the design and installation appraisals is required.

4.5.2 For Level 2 aircraft, additional substantiation is required to show that major failure conditions are remote. This can be accomplished using one of the following methods:

4.5.2.1 A similarity argument to a previously approved design that was previuosly shown to meet this probability objective. Refer to 4.7; or

4.5.2.2 For systems where similarity argument cannot be used, then compliance to the remote safety objective may be shown by means of a qualitative assessment. For "loss of function" failure conditions, this can be accomplished by:

(1) Showing that there is redundancy in the equipment providing that function. 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; or

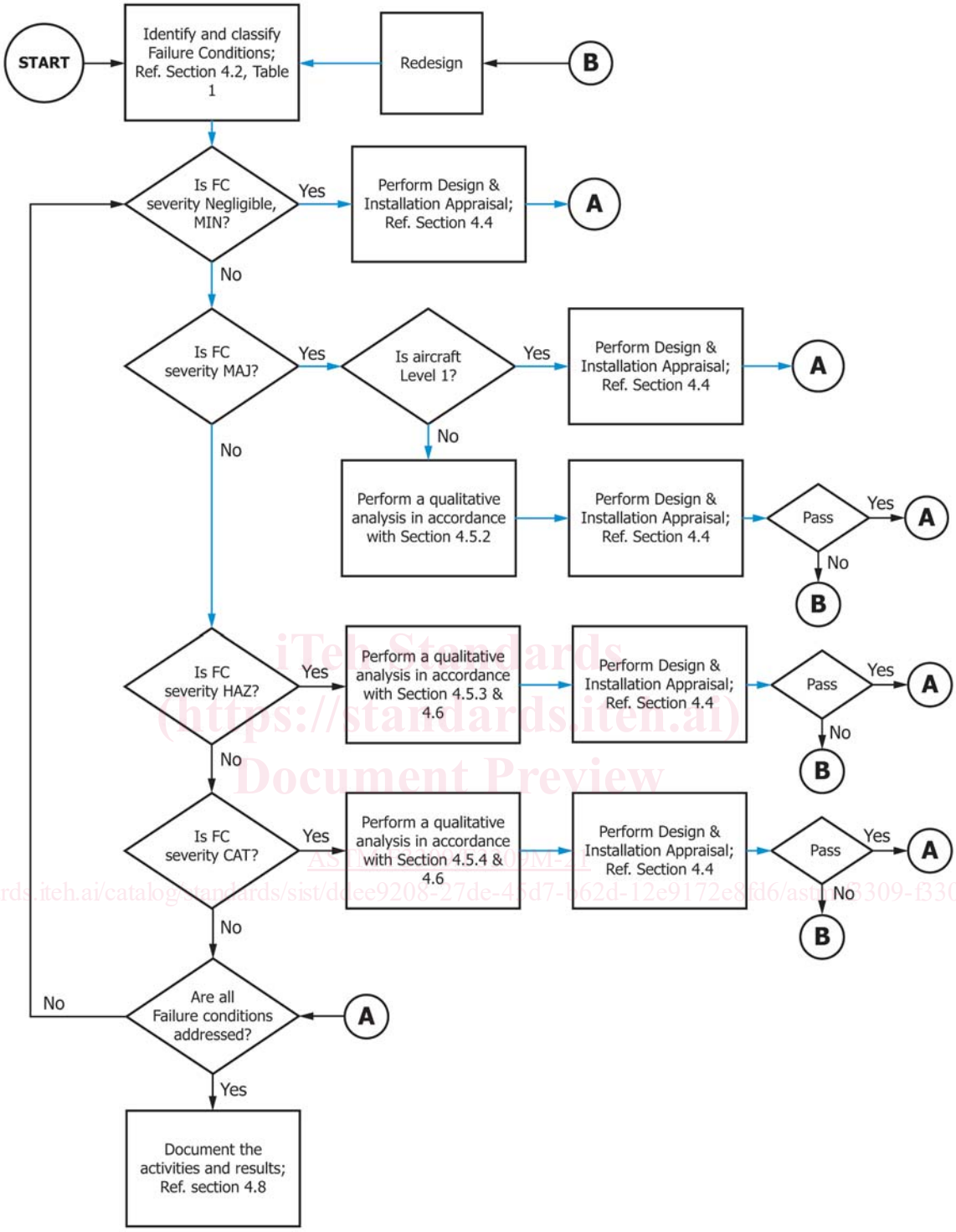

FIG. 1 Overview of the Simplified Safety Assessment Process

(2) In the case where single failures can cause the failure condition, by showing the system is simple, uses conventional architecture, is appropriately qualified for the installed environment and the individual failure rates of its components are below the objective of 1E-5.

4.5.2.3 For "malfunction" failure conditions, this can be accomplished by:

(1) Showing that the failure condition requires at least two independent failures; or

TABLE 1 Failure Condition Classifications

		Classification of Failure Conditions				
		Negligible	Minor	Major	Hazardous	Catastrophic
Classification Considerations[A]	Effect on Aircraft	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

[A] These phrases are descriptions of likely consequences for a given failure condition and not necessarily absolute criteria for classifying that failure condition. For example, the phrase "normally with hull loss" is a description of likely consequences for a catastrophic failure condition and not necessarily criteria for classifying a failure condition as catastrophic.

TABLE 2 Qualitative Probability Objectives

	Classification of Failure Conditions				
	Negligible	Minor	Major	Hazardous	Catastrophic
Qualitative Probability Objective	N/A	Probable	Remote	Extremely Remote	Extremely Improbable

(2) In the case where a single component can cause the event, showing that only specific component failure modes or a subset of a unit's internal components can result in the failure condition. Justification must be provided for the failure rate apportionment and how that would result in a failure rate on the order of 1E-5.

4.5.3 *Hazardous Failure Conditions*—These failure conditions must be shown to be extremely remote. This can be accomplished using one of the following methods:

4.5.3.1 A similarity argument to a previously approved design that was previously shown to meet this probability objective. Refer to 4.7; or

4.5.3.2 Qualitative analysis showing that each scenario that can cause the failure condition can only result from two or more independent failures. If the second failure in each combination is latent for more than one flight, the function of the component must be verified at an interval not to exceed the aircraft's annual inspection (or equivalent 100 h inspection as appropriate to the aircraft maintenance program). This can be accomplished by requiring an AFM/AFMS preflight check or by including an inspection/maintenance task in the Instructions for Continued Airworthiness. If a longer interval is desired, the methods outlined in Practice F3230 must be used. Common modes that could invalidate the independence between these failures must be addressed in accordance with 4.6.

4.5.3.3 Single point failures that contribute to hazardous failure conditions must be shown to be extremely remote. If the component is simple and can be shown to meet good design practice, it may be possible to qualitatively justify that its failure is extremely remote; see examples below. For all other single point failures that can result in a hazardous failure condition, refer to Practice F3230.

Example: 1—Failures of simple mechanical system components such as cables, pulleys, pushrods, bearings, bell cranks that have been designed to meet the component selection considerations used for manual flight control system requirements of Specification F3232/F3232M are typically accepted to be extremely remote.

Example 2—If the component failures have been previously shown to be extremely remote in the past and the design being evaluated is similar enough that the previous service history can reasonably be expected, then failures can be considered extremely remote.

4.5.4 *Catastrophic Failure Conditions*—These failure conditions must be shown to be extremely improbable and must not occur as the result of a single failure. This can be accomplished using one of the following methods:

4.5.4.1 A similarity argument to a previously approved design that was previously shown to meet this probability objective. Refer to 4.7; or

4.5.4.2 Qualitative analysis shown that each scenario that can cause the failure condition requires at least two independent failures. One of these failures could be latent provided it is not latent for more than one flight. The other failure must be an active failure. This qualitative analysis must identify how each failure would be detected. Common modes that could invalidate the independence between these failures must be addressed in accordance with 4.6.

4.6 *Common Mode Analysis:*

4.6.1 When credit is taken for the independence between failures, a common mode analysis must be performed to ensure that there are no common mode failures that would invalidate the assumed independence. The analysis must substantiate that the two failures are indeed independent when considering their design, installations, wiring, and potential common dependencies such as electrical power. Where this independence is not easily justifiable, additional analysis such as an FMEA may be required. Consideration must be given to the implications of common mode failures such as power sources or electrical