Designation: F3230 – 20a

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

This standard is issued under the fixed designation F3230; 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 internationally accepted methods for conducting safety assessments of systems and equipment for "small" aircraft.

1.2 The applicant for a design approval must seek the individual guidance of their respective civil aviation authority (CAA) body concerning the use of this practice as part of a certification plan. For information on which CAA regulatory bodies have accepted this practice (in whole or in part) as a means of compliance to their Small Aircraft Airworthiness regulations (hereinafter referred to as "the Rules"), refer to ASTM F44 webpage (www.ASTM.org/COMMITTEE/F44.htm) which includes CAA website links.

1.3 The values stated in inch-pound units are to be regarded as standard. No other units of measurement are included in this 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 CAA; earlier revisions are not acceptable.

2.2 *ASTM Standards:*[2]
F3060 Terminology for Aircraft
F3061/F3061M Specification for Systems and Equipment in Small Aircraft

2.3 *EASA Standard:*[3]
ETSO-C26d Aircraft Wheels And Wheel-Brake Assemblies (CS-23, -27 and -29 aircraft)

2.4 *FAA Standard:*[4]
TSO-C26d Aircraft Wheels, Brakes and Wheel/Brake Assemblies for Parts 23, 27, and 29 Aircraft

2.5 *Military Standard:*[5]
MIL-PRF-87257 Hydraulic Fluid, Fire Resistant, Low Temperature Synthetic Hydrocarbon Base, Aircraft and Missile

2.6 *RTCA Standard:*[6]
DO-160 Environmental Conditions and Test Procedures for Airborne Equipment

2.7 *SAE Standards:*[7]
SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
SAE AS5714 Minimum Performance Standard for Parts 23, 27, and 29 Aircraft Wheels, Brakes, and Wheel and Brake Assemblies

3. Terminology

3.1 Terminology specific to this practice is provided below. For general terminology, refer to Terminology F3060.

[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 Nov. 15, 2020. Published January 2021. Originally approved in 2017. Last previous edition approved in 2020 as F3230–20. DOI: 10.1520/F3230-20A.

[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 European Union Aviation Safety Agency (EASA), Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, https://www.easa.europa.eu/.

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

[5] Available from DLA Document Services, Building 4/D, 700 Robbins Ave., Philadelphia, PA 19111-5094, http://quicksearch.dla.mil.

[6] Available from RTCA, 1150 18th NW, Suite 910 Washington, D.C. 20036, https://www.rtca.org.

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

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *aircraft type code, n*—an aircraft type code (ATC) is defined by considering both the technical considerations regarding the design of the aircraft and the aeroplane certification level established based upon risk-based criteria; the method of defining an ATC applicable to this practice is defined in Specification F3061/F3061M.

3.2.2 *catastrophic failure condition, n*—a catastrophic failure condition is one that would result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crew member, normally with the loss of the aircraft.

3.2.3 *complex system, n*—a complex system is a system whose operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured assessment methods, such as failure modes and effects analysis (FMEA) or fault tree analysis (FTA); increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

3.2.4 *conventional system, n*—a conventional system is a system whose 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.

3.2.5 *design appraisal, n*—a design appraisal is a qualitative appraisal of the integrity and safety of the system design; an effective appraisal requires experienced judgment.

3.2.6 *extremely improbable, n*—extremely improbable means that an event is considered so unlikely that it is not anticipated to occur during the entire operational life of all aircraft of one type.

3.2.7 *extremely remote, n*—extremely remote means that an event is not anticipated to occur to each aircraft during its total life, but may occur a few times when considering the total operational life of all aircraft of the type.

3.2.8 *failure condition, n*—a failure condition is a condition having an effect on the aircraft or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors; the severity of a failure condition may be affected by flight phase, relevant adverse operational or environmental conditions, or other external events, or combinations thereof.

3.2.9 *hazardous failure condition*—a hazardous failure condition is one that would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: a large reduction in safety margins or functional capabilities; physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or, serious or fatal injuries to a relatively small number of persons other than the flight crew.

3.2.10 *installation appraisal, n*—an installation appraisal is a qualitative appraisal of the integrity and safety of the installation; any deviations from normal industry-accepted installation practices should be evaluated.

3.2.11 *major failure condition, n*—a major failure condition is one that would reduce the capability of the aircraft or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: a significant reduction in safety margins or functional capabilities; a significant increase in flight crew workload or in conditions impairing the efficiency of the flight crew; discomfort to the flight crew; or, physical distress to passengers or cabin crew, possibly including injuries.

3.2.12 *minor failure condition, n*—a minor failure condition is one that would not significantly reduce aircraft safety, and which involves 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.

3.2.13 *negligible failure condition, n*—a negligible failure condition is one that would have no procedural or operational effect on the flight crew so as to interfere with the reliable performance of published and trained duties, or on the operation or capabilities of the aircraft; however, the event may result in an inconvenience to aircraft occupants.

3.2.14 *probable, n*—probable means that the event is anticipated to occur one or more times during the entire operational life of each aircraft.

3.2.15 *qualitative analysis, n*—a qualitative analysis relies on analytical processes that assess system and aircraft safety in an objective, non-numerical manner.

3.2.16 *quantitative analysis, n*—a quantitative analysis relies on analytical processes that apply mathematical methods to assess the system and aircraft safety.

3.2.17 *redundancy, n*—the term redundancy refers to the presence of more than one independent means for accomplishing a given function; each means of accomplishing the function need not be identical.

3.2.18 *remote, n*—remote means that the event is not anticipated to occur at each aircraft during its total life, but may occur several times when considering the total operational life of all aircraft of the type.

3.2.19 *similarity, n*—the term similarity refers to a condition where the equipment type, form, function, design, and installation have only minor differences to previously approved equipment. The safety and operational characteristics and other qualities of the new installation should have no appreciable effects on the airworthiness of the aircraft.

3.2.20 *simple system, n*—a simple system is a system that can be evaluated by only qualitative analysis and that is not a complex system; functional performance is determined by combination of tests and analyses.

3.2.21 *single failure, n*—a single failure is considered to be any occurrence, or set of occurrences, that: cannot be shown to be independent from each other; affects the operation of components, parts, or elements of a system such that they can no longer function as intended; or, results in inadvertent system operation.

4. Basic Information

NOTE 1—Table 1 provides correlation between various ATCs and the individual requirements contained within this section; refer to 3.2.1. For

TABLE 1 ATC Compliance Matrix, Section 4

Section	Aeroplane Certification Level				Number of Engines		Type of Engine(s)		Stall Speed			Cruise Speed		Meteorological Conditions			Altitude		Maneuvers	
	1	2	3	4	S	M	R	T	L	M	H	L	H	D	N	I	L	H	N	A
4																				
4.1																				
4.2	○								○					○						
4.2.1	○								○					○						
4.2.2	○								○					○						
4.2.3	○								○					○						
4.2.3.1	○								○					○						
4.2.3.2	○								○					○						
4.2.3.3	○								○					○						
4.2.3.4	○								○					○						
4.2.4	○								○					○						
4.2.4.1	○								○					○						
4.2.4.2	○								○					○						
4.2.4.3	○								○					○						
4.2.5	○								○					○						

each subsection, an indicator can be found under each ATC character field; three indicators are used:

An empty cell ( ) in all applicable ATC character field columns indicates that an aircraft must meet the requirements of that subsection.

A white circle (○) in multiple columns indicates that the requirements of that subsection are not applicable to an aircraft *only* if all such ATC character fields are applicable.

A mark-out (×) in any of the applicable ATC character field columns indicates that the requirements of that subsection are not applicable to an aircraft if that ATC character field is applicable.

Example—An aircraft with an ATC of 1SRLLDLN is being considered. Since all applicable columns are empty for 4.1, that subsection is applicable to the aircraft. Since the "1" aeroplane certification level column, the "L" stall speed column, and the "D" meteorological column for 4.2.1 all contain white circles, then that subsection is not applicable; however, for an aircraft with an ATC of 1SRMLDLN, 4.2.1 would be applicable since the "M" stall speed column does not contain a white circle.

4.1 *Failure Condition 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 3.2.8 and Table 2. 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 (for example, a design and installation appraisal) may be employed as appropriate to the complexity and criticality of the system(s).

4.2 *Classification-Based Analyses*—Based on the results of the assessment in accordance with 4.1, the depth of analysis required to show compliance may be determined using Fig. 1 and the Assessment Levels defined in Table 3.

4.2.1 In showing compliance with the provisions of 4.2, for negligible failure conditions (refer to 3.2.13), a design and installation appraisal to establish independence from other functions is necessary for the safety assessment. In general, common design practice provides physical and functional isolation from related components which are essential to safe operation.

4.2.2 In showing compliance with the provisions of 4.2, for minor failure conditions (refer to 3.2.12), a design and installation appraisal to establish independence from other functions is necessary for the safety assessment. This appraisal should consider the effects of system failures on other systems and their functions. In general, common design practice provides

TABLE 2 Failure Condition Classifications

		Classification of Failure Conditions				
		Negligible[A]	Minor[A]	Major[A]	Hazardous[A]	Catastrophic[A]
Classification Considerations	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] Refer to Section 3.

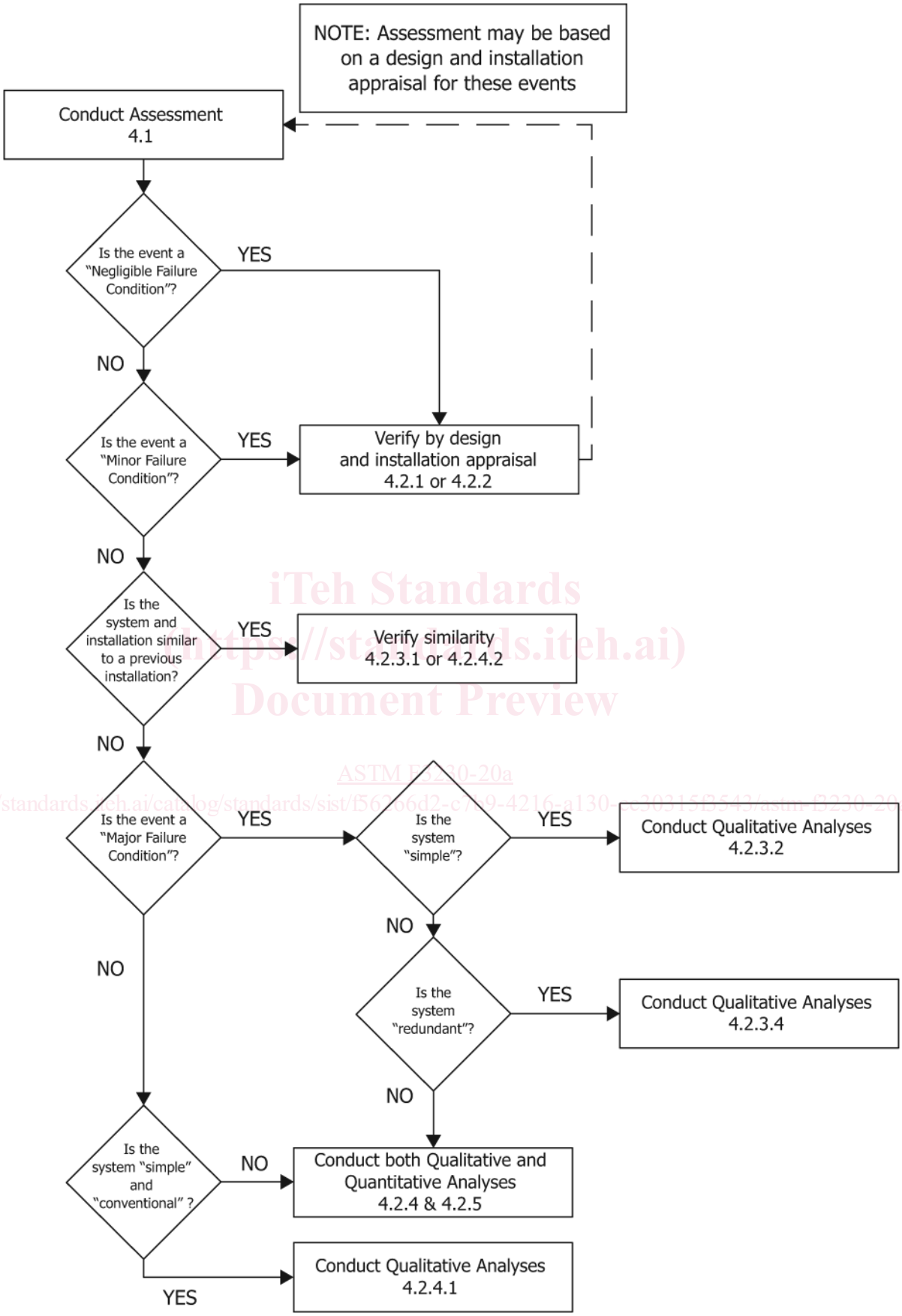

FIG. 1 Depth of Analysis Flowchart

TABLE 3 Assessment Level Selection Matrix

Aeroplane Certification Level	Engine Information			
	Reciprocating		Turbine	
	1	>1	1	>1
Level 1[A]	I	II	II	II
Level 2[A]	I	II	II	II
Level 3[A]	III	III	III	III
Level 4[A]	IV	IV	IV	IV

[A] Refer to Specification F3061/F3061M.

physical and functional isolation from related components which are essential to safe operation.

4.2.3 In showing compliance with the provisions of 4.2, for major failure conditions (refer to 3.2.11), a qualitative analysis (refer to 3.2.15) must be performed to determine compliance with the requirements of Table 4; in certain circumstances, a quantitative analysis (refer to 3.2.16) may also be required. There are several methods of performing a valid qualitative analysis.

4.2.3.1 A "similarity argument" allows validation of a requirement by comparison to the requirements of similar certified systems. A 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 aircraft 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, supports any claims of similarity to a previous installation.

4.2.3.2 For systems that are not complex, and where similarity arguments cannot be used, "qualitative occurrence arguments" may be presented to demonstrate that the major failure conditions of the system, as installed, are consistent with the requirements of Table 4; for example, redundant systems may qualify for this approach.

4.2.3.3 For systems that are complex and possess low redundancy (for example, a system with a self-monitoring microprocessor), a qualitative functional FTA or FMEA supported by failure rate data and fault detection coverage analysis must be presented to demonstrate that the major failure conditions of the system, as installed, are consistent with the requirements of Table 4.

4.2.3.4 A Qualitative Analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems where functional redundancy is required, a qualitative functional FTA or FMEA may be necessary to demonstrate that redundancy actually exists (for example, no single failure affects all functional channels).

4.2.4 In showing compliance with the provisions of 4.2, for Hazardous and Catastrophic Failure Conditions (refer to 3.2.9 and 3.2.2, respectively) a thorough safety assessment is necessary. Except as allowed in 4.2.4.1 – 4.2.4.3, a detailed safety analysis must be completed for each hazardous and catastrophic failure condition identified in accordance with 4.1. Such an assessment usually consists of an appropriate combination of qualitative and quantitative analyses; a system safety analysis (SSA) in accordance with the methodology outlined in SAE ARP4761 is one means of performing these analyses; however, other simpler methodologies may be employed as appropriate.

4.2.4.1 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 (refer to 3.2.7) or extremely improbable (refer to 3.2.6), respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for such an 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 aircraft may be sufficient when a close similarity is established regarding both the system design and operating conditions.

4.2.4.2 For complex systems where true similarity can be rigorously established in all relevant attributes, including installation 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 such an assessment will be a high degree of similarity in both design and application.

4.2.4.3 No catastrophic failure condition 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 due to a single failure mode is not a practical possibility. The logic and rationale used in the assessment should be straightforward and obviously substantiate that the failure mode simply would not occur

TABLE 4 Allowable Qualitative Probability

All Assessment Level[A]	Failure Condition Classification (from Table 2)				
	Negligible[B]	Minor[B]	Major[B]	Hazardous[B]	Catastrophic[B]
ALL	No Probability Requirement	Probable[B]	Remote[B]	Extremely Remote[B]	Extremely Improbable[B]

[A] Refer to Table 3.
[B] Refer to Section 3.

TABLE 5 Allowable Quantitative Probabilities[A]

Assessment Level[B]	Failure Condition Classification (from Table 2)				
	Negligible[C]	Minor[C]	Major[C]	Hazardous[C]	Catastrophic[C]
I	No Probability Requirement	$<10^{-3}$	$<10^{-4}$	$<10^{-5}$	$<10^{-6}$ (See[D])
II		$<10^{-3}$	$<10^{-5}$	$<10^{-6}$	$<10^{-7}$ (See[D])
III		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-8}$ (See[D])
IV		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$ (See[D])

[A] Numerical values indicate an order of probability range and are provided here as a reference; refer to 4.2.5.
[B] Refer to Table 3.
[C] Refer to Section 3.
[D] At the aircraft function level, no single failure resulting in a catastrophic failure condition is permitted.

unless it is associated with an unrelated failure condition that would, in itself, be Catastrophic.

4.2.5 In showing compliance with the provisions of 4.2.4, where Quantitative Analysis is required by Fig. 1, the analysis should demonstrate that the probability of the failure condition occurrence meets the probability range shown in Table 5. It is recognized that there is inherent variance in predictions used to demonstrate that these probabilities are met; it may therefore be acceptable, provided the analysis can be shown to be conservative and is acceptable to the governing CAA, to be slightly above the probabilities shown in Table 5.

5. Keywords

5.1 catastrophic; failure condition; FHA; FMEA; FTA; hazardous; major; minor; qualitative; quantitative; similarity; SSA; system safety

APPENDIXES

(Nonmandatory Information)

X1. SUPPORTING INFORMATION FOR REVISIONS

X1.1 Revisions to Table 3

X1.1.1 *Revision 16 to Previous Location (Specification F3061/F3061M, Table 2):*

X1.1.1.1 *Discussion*—Section 3.2.1.1 of Specification F3061/F3061M defines the risk-based criteria that establish the various Airworthiness Levels. Each of the row header cells in the "Airworthiness Level" column of Table 2 of Specification F3061/F3061M currently contains a condensed version of the corresponding definition, which is redundant to 3.2.1.1 of Specification F3061/F3061M.

X1.1.1.2 *Proposal*—Remove the redundant language from the row header cells identified as Affected Content, and instead add a reference to 3.2.1.1 of Specification F3061/F3061M.

X1.1.1.3 *Rationale for Change(s)*—The proposal is for the removal of redundant information only; no technical content is added, deleted, or modified.

X1.2 Revisions to Table 5

X1.2.1 *Revision 16 to Previous Location (Specification F3061/F3061M, Table 3):*

X1.2.1.1 *Discussion*—In the "Allowable Quantitative Probabilities" portion of Table 3 of Specification F3061/F3061M, under the "Catastrophic" column, the original intent as to apply Note D to all Assessment Levels (Note D currently reads "At the aircraft function level, no single failure resulting in a Catastrophic Failure Condition is permitted."); this is consistent with the pre-existing regulatory guidance material from which Table 3 of Specification F3061/F3061M was derived, and is reflected in the approved version of the document. However, during final editing the note-reference was inadvertently removed from Assessment Levels I through III.

X1.2.1.2 *Proposal*—Restore "(See Note D)" to Assessment Levels I through III under the "Catastrophic" column within the "Allowable Quantitative Probabilities" portion of Table 3 of Specification F3061/F3061M.

X1.2.1.3 *Rationale for Change(s)*—The proposal is for the reintroduction of the originally intended and approved material. This will serve to realign the technical content with the pre-existing regulatory guidance material from which Table 3 of Specification F3061/F3061M was derived.

X2. GUIDANCE FOR QUALITATIVE PROBABILITY ANALYSIS

X2.1 Introduction

X2.1.1 This appendix contains supplemental information on how to perform the qualitative analysis for hazardous and catastrophic failure conditions for systems that have been accepted as simple and conventional in accordance with 4.2.4.1.

X2.1.1.1 *Qualitative Probability Requirements*—Requirements for the qualitative analysis are based on failure condition classifications, which usually come from the FHA in accordance with 4.1. The definitions of *extremely improbable* and *extremely remote* from Section 3 are used for the qualitative analysis and not the quantitative values from Table 5.

(1) Catastrophic failure conditions must be so unlikely that they are not anticipated to occur during the entire operational life of all aircraft of one type.

(2) Hazardous failure conditions must be so unlikely that they are not anticipated to occur to each aircraft during its total life, but may occur a few times when considering the total operational life of all aircraft of the type.

X2.1.1.2 *Substantiation*—It is difficult to prove definitively how frequently a failure condition will occur in the future. However, there must be justification supporting the claim that the failure condition can reasonably be anticipated to be so unlikely that the requirement is met. The basis of this assessment is experienced engineering judgment, which can make it difficult for designers, analysts, and reviewers to know when the assessment is sufficient. The goal of this appendix is to provide information on acceptable substantiation and an example that shows sufficient detail in the substantiation.

X2.1.1.3 *Qualitative Analysis Steps*—There are three steps to performing qualitative analysis for 4.2.4.1. The first step of the analysis is to establish that the design is conventional. In other words, is the design consistent with existing system designs that have established an acceptable service history? The second step is to show that the design is simple. A design may be considered simple if its failure modes can be evaluated without the aid of structured analysis such as FMEA or a FTA. The third step is to establish that the likelihood of the failure condition is acceptable. This evaluation identifies failures or combinations of failures that must occur to result in the failure condition and considers redundancy, independence, isolation, and common causes. The evaluation considers component qualification data or other data that supports the conclusion that failures aren't expected during various operating conditions and environments. The evaluation considers latent failures that could contribute to the failure condition. Fig. X2.1 shows the high-level process described above.

X2.1.1.4 *Example Analysis*—Appendix X2.6 contains an example qualitative analysis for a simple and conventional brake system. The example is not intended to show a complete system safety assessment. The intent is to show how a qualitative assessment could be constructed using this guidance.

X2.2 Establish that System is Conventional

X2.2.1 The foundation of the qualitative analysis for 4.2.4.1 is that the system is 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 and that have established an acceptable service history. The use of service history in this context is not to show that the probability of the failure condition has been met but rather to show that similar systems have performed acceptably in service. Fig. X2.2 shows the decision path that should be used to determine that a system is

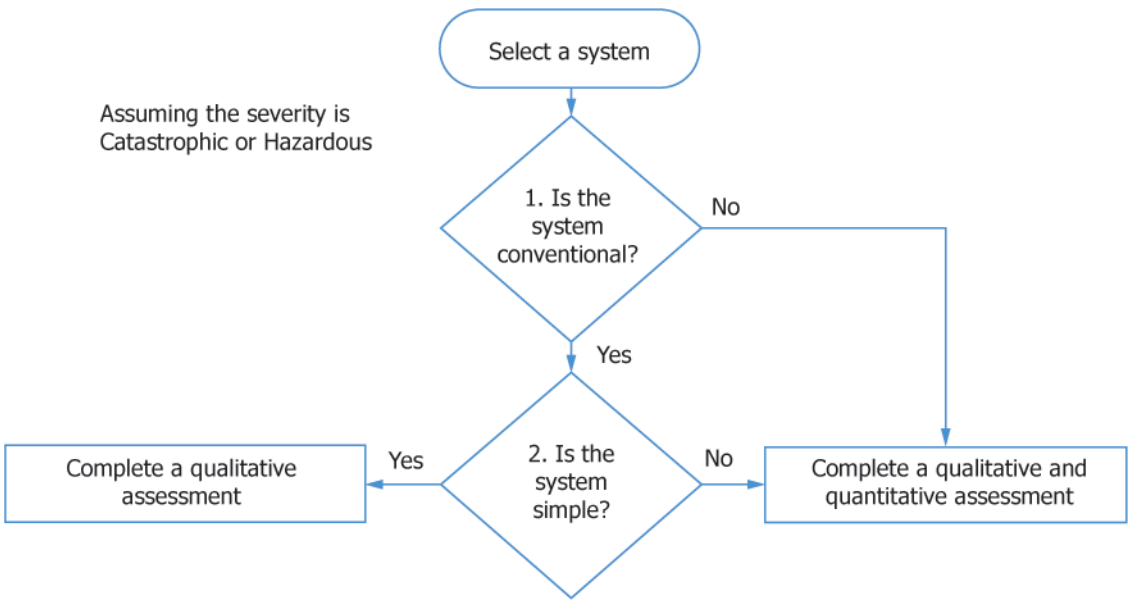

FIG. X2.1 Process Overview