



Designation: F3230 – 21a

Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft¹

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.

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. 1, 2021. Published December 2021. Originally approved in 2017. Last previous edition approved in 2021 as F3230–21. DOI: 10.1520/F3230-21A.

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.

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