Designation: F3479 – 20

Standard Specification for Failure Tolerance for Occupant Safety of Suborbital Vehicles[1]

This standard is issued under the fixed designation F3479; 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 specification provides system safety engineering and failure tolerance requirements applicable to occupant safety for suborbital vehicles.

1.2 This specification is not intended to provide failure tolerance requirements for conditions that do not impact occupant safety. For example, conditions resulting in facility damage, vehicle damage, loss of mission objectives, or adverse impact to public safety that do not also have an impact to occupant safety are not subject to the requirements identified in this specification. This specification does not address malfunctions caused by malicious attacks on software systems.

1.3 *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.*

1.4 *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 *NASA Handbooks:*[2]

NASA/SP-2010-580 NASA System Safety Handbook Volume 1: System Safety Framework and Concepts for Implementation

NASA/SP-2014-612 NASA System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples

2.2 *RTCA Standards:*[3]

RTCA DO-178 Software Considerations in Airborne Systems and Equipment Certification

RTCA DO-278 Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems

2.3 *SAE Standards:*[4]

SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems

SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

2.4 *Other Standards:*

IEEE/EIA 12207 International Standard - Systems and software engineering[5]

MIL-STD-882E Department of Defense Standard Practice System Safety[6]

3. Terminology

3.1 *Definitions:*

3.1.1 *catastrophic event*—loss of life or permanent disability for the purposes of this specification.

3.1.2 *failure condition*—a condition, or set of conditions, that affects the operation of a component, part, or element such that it can no longer function as intended. Types of failure conditions that should be considered include:

3.1.2.1 *incorrect function*—incorrect functional output(s), when required, and functional outputs produced at the wrong time (inadvertent function).

3.1.2.2 *loss of function*—the absence of functional output(s), when required.

3.1.2.3 *safety critical function or item*—a failure of the function or item causes one or more failure conditions that result in a catastrophic event.

[1] This specification is under the jurisdiction of ASTM Committee F47 on Commercial Spaceflight and is the direct responsibility of Subcommittee F47.01 on Occupant Safety of Suborbital Vehicles.

Current edition approved Oct. 1, 2020. Published November 2020. DOI: 10.1520/F3479-20

[2] Available from NASA Technical Reports Server (NTRS), NASA Headquarters, 300 E. Street, SW, Suite 5R30, Washington, DC 20546, https://ntrs.nasa.gov.

[3] Available from RTCA, Inc. (RTCA), 1150 18th NW, Suite 910, Washington, DC 20036, https://www.rtca.org.

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

[5] Available from Institute of Electrical and Electronics Engineers, Inc. (IEEE), 445 Hoes Ln., Piscataway, NJ 08854-4141, http://www.ieee.org.

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

3.1.3 *failure tolerance*—the ability to sustain a certain number of failures and still retain capability to satisfy safety objectives.

4. Requirements

4.1 *System Safety Engineering:*

4.1.1 A structured system safety engineering process shall be implemented to identify and characterize each hazard, assess the risk to occupant safety, reduce risks through the use of hazard elimination and mitigation measures, and verify that risks have been reduced to an acceptable level. The process shall:

4.1.1.1 Identify and describe hazards and the associated causes, including those that result from:

(1) Component, subsystem, or system failures;

(2) Software errors and operations;

(3) Human errors;

(4) Functional and physical interfaces;

(5) Incompatible materials;

(6) Environmental conditions;

(7) Biological sources; and

(8) Interactions of any of the above.

4.1.1.2 Identify and describe each safety-critical system and function.

4.1.1.3 Implement a hazard control strategy that will prevent the occurrence of the hazard, or mitigate the risk to an acceptable level. These hazard controls may include, but are not limited to, the following:

(1) Failure tolerance,

(2) Sufficient design margins,

(3) Operational constraints,

(4) Monitoring of safety-critical systems,

(5) An environmental qualification and acceptance testing program,

(6) Operating and emergency response procedures, and

(7) Training or certification.

4.1.1.4 Verify that the hazard controls and risk mitigation measures have been successfully implemented through objective verification evidence.

4.1.1.5 Assess the impact of design or operational changes, including review of all existing hazard analyses and updating as necessary to reflect any new causes, mitigations, and changes to overall risk.

4.1.1.6 Assess the impact or reported problems/anomalies against a fielded system configuration, including:

(1) Reviewing all existing hazard analyses and updating as necessary to reflect any new causes, mitigations, or changes to overall risk.

(2) Disposition the continued use of the fielded system configuration with which the reported problems/anomalies are associated.

4.1.1.7 See Appendix X2 for additional considerations.

4.1.2 *Software System Safety:*

4.1.2.1 Hazards from computing systems and software should be considered as an integral component of the system safety engineering process as outlined in 4.1.

4.1.2.2 A software development and verification process and maintenance approach should be documented and maintained. The process should, at a minimum, include:

(1) Software development methods and standards, including how intended software behaviors are defined.

(2) Software design (for example, architecture definition, components/modules definition, interface definition, data definitions).

(3) Validation and verification, including integration verification.

(4) Approach to analyze and approve off-the-shelf software.

(5) Activities that support identification and removal of latent design errors in any and all software lifecycle data, with independence. In this context, independence reduces the opportunity for latent design errors by relying on a second set of eyes. Examples of independence include review by peers in the same organization, by a separate organization within the company, or by a third party.

4.1.3 *Methods for Addressing Human Error*—A method for assessing human errors shall be defined to assess the contribution of human errors to catastrophic events. The method should facilitate characterization of human error risk as well as tolerance of the system to human errors that may result in a catastrophic event, regardless of likelihood.

4.1.4 *Industry System Safety Standards and Methods*—Note that the listing of the following standards shall not be construed to constrain compliance with system safety engineering requirements only by means of the listed standards. Other system safety engineering approaches may be employed provided that they are evaluated for compliance with this specification. The compliance matrix in Appendix X1 provides an example for capturing compliance. Compliance with the following system safety standards is expected to satisfy the system safety engineering requirements of this specification:

4.1.4.1 SAE ARP-4761,

4.1.4.2 SAE ARP-4754,

4.1.4.3 MIL-STD-882E,

4.1.4.4 NASA System Safety Handbook Volume 1 and Volume 2, and

4.1.4.5 Software safety standards:

(1) RTCA DO-178,

(2) RTCA DO-278,

(3) IEEE/EIA12207, and

4.1.4.6 Human error assessment methods:

(1) Technique for human error-rate prediction (THERP),

(2) Human error assessment and reduction technique (HEART), and

(3) Human/procedure hazard and operability study (Human-HAZOP).

4.2 *Hardware Failure Tolerance to Catastrophic Events*—The vehicle shall control hazards that can lead to catastrophic events with no less than single failure tolerance for hardware failures. A risk-informed approach may be employed to determine where greater than single failure tolerance is appropriate. For zero fault tolerant items, see Section 5 covering Single Points of Failure.

4.3 *Human Error Tolerance to Catastrophic Events*—No single inadvertent action, incorrect action, or failure to perform an action shall result in a catastrophic event. In specific cases where human error does not immediately or irreversibly result

in a catastrophic event—events for which corrective actions are possible, where cues that show the need for corrective action are available, and where sufficient time exists for crew to reliably recognize the condition and respond with corrective action—this requirement is satisfied.

5. Single Points of Failure

5.1 Where high confidence can be established in the reliability of a component for which a failure, on its own results in a catastrophic event, exemption may be claimed against the failure tolerance requirements in this specification. Such components represent single points of failure. Examples of single points of failure typically include, but are not limited to, structural failure of primary structure, pressure vessels, and pressurized lines and fittings. Other examples include components where it is either impractical or impossible to implement a design solution that would satisfy failure tolerance requirements.

5.2 Strategies shall be implemented to establish confidence in the expected reliability of single point of failure components for the specific failure conditions that result in a catastrophic event. Strategies should ensure the design adequately controls the likelihood of such component failures, ensure that the manufacturing process adequately controls manufacturing defects that would increase the likelihood of failure of such components, and ensure that the operations and maintenance processes adequately control the likelihood of such component failures over the life of the system. Examples of strategies include, but are not limited to, understanding and bounding the failure modes and environments, design margins, factors of safety, derating, manufacturing process control of key characteristics, component life tracking and limited life parts inspection and preemptive replacement.

6. Common Cause Assessment

6.1 A common cause assessment (CCA) shall be performed to identify any potential sources of failure that may compromise the failure tolerance of the system (that is, the hardware failure tolerance requirements defined in this specification). Common cause sources to be considered include, but are not limited to, common design, common environments, common location, and common procedures

7. Limitations on Failure Tolerance

7.1 If crew intervention is required to satisfy failure tolerance requirements (for example, by activating a backup system), the system shall provide cues indicating the need for crew intervention, and the time required for crew intervention shall include time for the crew to recognize intervention cues and the time to perform the intervention. If the cues are inadequate to provide sufficient crew recognition, and the time required for crew intervention exceeds the time to criticality of a failure condition that would result in a catastrophic event (with acceptable margin to account for variation in crew response), then the system shall be designed to satisfy its failure tolerance requirements without relying on crew intervention.

8. Keywords

8.1 failure tolerance; fault tolerance; occupant safety; suborbital

APPENDIXES

(Nonmandatory Information)

X1. EXAMPLE COMPANY A PROJECT X COMPLIANCE MATRIX

TABLE X1.1 Example Company A Project X Compliance Matrix

Section	Compliance Statement
4.1.1 A structured system safety engineering process shall be implemented to identify and characterize each hazard, assess the risk to occupant safety, reduce risks through the use of risk elimination and mitigation measures, and verify that risks have been reduced to an acceptable level.	Comply: Company A's system safety program plan (SSPP) implements a system safety engineering process that satisfies SAE ARP 4754A and SAE ARP 4761.
4.1.1.1 [the process shall] Identify and describe hazards and the associated causes, including those that result from: 1) Component, subsystem, or system failures; 2) Software errors and operations; 3) Human errors; 4) Design or procedural deficiencies; 5) Functional and physical interfaces; 6) Incompatible materials; 7) Environmental conditions; 8) Biological sources; and 9) Interactions of any of the above.	Comply: Company A's SSPP implements a system safety engineering process that satisfies SAE ARP 4754A and SAE ARP 4761. Identification of hazards and associated causes are accomplished by performing aircraft and system functional hazard assessments (FHAs), preliminary system safety assessments (PSSAs), fault tree analyses (FTAs), CCAs, and failure modes and effects analyses (FMEAs) in accordance with the SSPP.
4.1.1.2 [the process shall] Identify and describe each safety-critical system and its function.	Safety-critical systems and functions are described in safety assessment report in accordance with the SSPP.
[the process shall] Identify and describe all safety-critical events.	Safety-critical events are described in safety assessment report in accordance with the SSPP.
4.1.1.3 [the process shall] Implement a hazard control strategy that will prevent the occurrence of the hazard, or mitigate the risk to an acceptable level.	Hazard control strategies are described in the system safety assessment report in accordance with the SSPP.
4.1.1.4 [the process shall] Verify that the hazard controls and risk mitigation measures have been successfully implemented through objective verification evidence.	Hazard control verification is described in the system safety assessment report in accordance with the SSPP.
4.1.1.5 [the process shall] Assess the impact of design or operational changes, including review of all existing hazard analyses and updating as necessary to reflect any new causes, mitigations, and changes to overall risk.	Changes to engineering lifecycle data is controlled in accordance with Company A's configuration management plan (CMP). The SSPP defines requirements for performing a safety assessment of the impact of design and operational changes.
4.1.1.6 [the process shall] Assess the impact or reported problems/anomalies against a fielded system configuration, including: 1) Reviewing all existing hazard analyses and updating as necessary to reflect any new causes, mitigations, or changes to overall risk. 2) Disposition the continued use of the system configuration with which the reported problems/anomalies are associated.	Problem/anomalies are reported and managed in accordance with Company A's non-conformance reporting process (NRP), including requirements for disposition of continued use of the system. The SSPP defines requirements for assessing the impact to safety of reported problems/anomalies.
4.1.2.1 Hazards from computing systems and software should be integrated into the system safety engineering process as outlined in 4.1.	Section [x] of the SSPP specifies requirements to address hazards from computing systems and software.
Computing systems and functions implemented in software should be considered safety critical if they can cause or contribute to failure conditions that may result in a catastrophic hazard.	The SSPP definition of "safety critical" are applied to computing systems.
4.1.2.2 A software development process and maintenance approach should be documented and maintained.	The Company A Project X software development and verification plans comply with RTCA DO-178C and satisfy this requirement.
4.1.2.2 (1) [The process should, at a minimum, include] Software development methods and standards, including expectations for functional and performance requirements identification and decomposition.	The Company A Project X software development and verification plans comply with RTCA DO-178C and satisfy this requirement.
4.1.2.2 (2) [The process should, at a minimum, include] Software design (that is, architecture, components, modules, interfaces, and data).	The Company A Project X software development and verification plans comply with RTCA DO-178C and satisfy this requirement.
4.1.2.2 (3) [The process should, at a minimum, include] Validation and verification, including integration verification.	The Company A Project X software development and verification plans comply with RTCA DO-178C and satisfy this requirement.
4.1.2.2 (4) [The process should, at a minimum, include] Approach to analyze and approve off-the-shelf software.	The Company A Project X plan for software aspects of certification (PSAC) complies with RTCA DO-178C Section 2.5.3, 11.1.g, 12.1.4, and 12.3.4 satisfies this requirement.
4.1.2.2 (5) [The process should, at a minimum, include] Methods for identification and removal of errors in any and all software lifecycle data (requirements, design data, code, binaries, test cases and procedures, etc.), with independence, that may manifest in a failure that results in a catastrophic event.	The Company A Project X software development and verification plans comply with RTCA DO-178C and satisfy this requirement.
4.1.3 A method for assessing human errors shall be defined to assess the contribution of human errors to catastrophic events. The method should facilitate characterization of human error risk as well as tolerance of the system to human errors that may result in a catastrophic event, regardless of likelihood.	The SSPP defines THERP as the method used to assess the contribution of human errors to catastrophic events.