U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Flight Hazard Analysis

Date: 08/05/2021

AC No: 450.109-1

Initiated By: AST-1

This Advisory Circular (AC) provides guidance for conducting a flight hazard analysis to identify and control public safety hazards and risks associated with flight, and phases of flight, for a launch or reentry vehicle (hereafter referred to as system) in accordance with § 450.109 of Title 14 of the Code of Federal Regulations (14 CFR). Section 450.109 requires an operator using a flight hazard analysis as a hazard control strategy for one or more phases of flight to identify, describe, and analyze all reasonably foreseeable hazards to public safety resulting from the flight of a launch or reentry vehicle. In accordance with § 450.109(b)(3) through (5), operators must mitigate hazards, as appropriate, and validate and verify the hazard mitigations.

The FAA considers this AC an accepted means of compliance for satisfying the regulatory requirements of § 450.109 It presents one, but not the only, acceptable means of compliance with the associated regulatory requirements. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. The document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

If you have suggestions for improving this AC, you may use the Advisory Circular Feedback form at the end of this AC.

WAYNE R MONTEITH Digitally signed by WAYNE R MONTEITH
Date: 2021.08.05 12:08:44 -04'00'

Wayne R. Monteith
Associate Administrator
Commercial Space Transportation

Contents

Paragraph **Page**

1 Purpose....4
2 Applicability....4
3 Applicable Regulations and Related Documents....5
4 Definition of Terms....6
5 Acronyms....6
6 Overview....7
6.1 Objective of Flight Hazard Analysis....7
6.2 A Flight Hazard Analysis differs from Flight Safety Analysis....7
6.3 Flight Hazard Analysis Methodology....7
6.4 Aspects of a Flight Hazard Analysis....7
6.5 Formal Traceability of System Safety Hazards....8
6.6 System Safety Hazards and Software Safety....8
7 Performing a Flight Hazard Analysis....9
7.1 Identify Hazards....9
7.1.1 Hazard Traceability....9
7.1.2 Data from the Functional Hazard Analysis....9
7.1.3 Data beyond the Functional Hazard Analysis....9
7.2 Assessing Likelihood and Severity of Each Hazard....10
7.2.1 Resources for System Safety Risk Assessments....10
7.2.2 Utilizing a Systematic Assessment Process....10
7.2.3 Risk Assessment Traceability....10
7.3 Mitigate Risk to Acceptable Levels....11
7.3.1 Proper Risk Mitigation Process....11
7.3.2 Developing Risk Acceptance Criteria....11
7.3.3 Baseline of Risk Acceptability....11
7.4 Identifying and Describing Risk Mitigation Measures....12
7.4.1 Risk Mitigation Traceability....12
7.4.2 System Safety Design Order of Precedence....12
7.4.3 Potential Risk Mitigation Methods....12
7.5 Validation and Verification....14

Contents (continued)

Paragraph **Page**

7.5.1 Validation of Risk Mitigations and Verification Methods 14
7.5.2 Verifying Risk Mitigations 14
7.5.3 Iterative Approach of Validation and Verification 15
7.6 Identifying New Hazards and Updating the Flight Hazard Analysis 16
7.6.1 Updates from Lifecycle Data 16
7.6.2 Accuracy via the System Safety Program 16
7.6.3 Completeness Prior to Flight 16
7.7 Application Requirements 16
Appendix A. System Safety Template for § 450.109 Flight Hazard Analysis A-1

1 PURPOSE.

1.1 This advisory circular (AC) provides guidance for an operator to apply a systematic and logical hazard analysis to identify, analyze, and control public safety hazards and risks associated with flight, and phases of flight, for a launch or reentry vehicle (hereafter referred to as system) in accordance with § 450.109.

1.2 **Scope**.

Section 450.109(b) requires a flight hazard analysis to identify, describe, and analyze reasonably foreseeable hazards to public safety resulting from the flight of a launch or reentry vehicle. The flight hazard analysis must identify all reasonably foreseeable hazards associated with the launch or reentry system relevant to public safety, in accordance with § 450.109(b)(1); assess each hazard's likelihood and severity, in accordance with § 450.109(b)(2); and document the risk mitigation, with associated verifications, of each one, in accordance with § 450.109(b)(5). Section 450.107(c) states that an operator must conduct a flight hazard analysis, in accordance with § 450.109 for the flight, or phase of flight, of a launch or reentry vehicle if the public safety hazards cannot be mitigated adequately to meet the public risk criteria of § 450.101(a), (b), and (c) using physical containment, wind weighting, or flight abort.

1.3 **Level of Imperatives**.

This AC presents one, but not the only, acceptable means of compliance with the associated regulatory requirements. The FAA will consider other means of compliance that an applicant may elect to present. In addition, an operator may tailor the provisions of this AC to meet its unique needs, provided the changes are accepted as a means of compliance by FAA. Throughout this document, the word "must" characterizes statements that directly follow from regulatory text and therefore reflect regulatory mandates. The word "should" describes a requirement if electing to use this means of compliance; variation from these requirements is possible, but must be justified and accepted by the FAA as an alternative means of compliance. The word "may" describes variations or alternatives allowed within the accepted means of compliance set forth in this AC. In general, these alternative approaches can be used only under certain situations that do not compromise safety.

2 APPLICABILITY.

2.1 The guidance in this AC is for launch and reentry vehicle applicants and operators required to comply with 14 CFR part 450. The guidance in this AC is for those seeking a launch or reentry vehicle operator license, and a licensed operator seeking to renew or modify an existing vehicle operator license.

2.2 The material in this AC is advisory in nature and does not constitute a regulation. This guidance is not legally binding in its own right and will not be relied upon by the FAA as a separate basis for affirmative enforcement action or other administrative penalty. Conformity with this guidance document (as distinct from existing statutes and

regulations) is voluntary only, and nonconformity will not affect rights and obligations under existing statutes and regulations. It describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations. The FAA will consider other means of compliance that an applicant may elect to present.

2.3 The material in this AC does not change or create any additional regulatory requirements, nor does it authorize changes to, or deviations from, existing regulatory requirements.

3 APPLICABLE REGULATIONS AND RELATED DOCUMENTS.

3.1 Related U.S.C. Statute.

- 51 U.S.C. Subtitle V, Chapter 509.

3.2 Related FAA Commercial Space Transportation Regulations.

The following 14 CFR regulations must be accounted for when showing compliance with 14 CFR 450.109 Flight Hazard Analysis. The full text of these regulations can be downloaded from the U.S. Government Printing Office e-CFR. A paper copy can be ordered from the Government Printing Office, Superintendent of Documents, Attn: New Orders, PO Box 371954, Pittsburgh, PA, 15250-7954.

- Section 450.101, *Safety criteria.*
- Section 450.103, *System safety program.*
- Section 450.107, *Hazard control strategies.*
- Section 450.141, *Computing Systems*.

3.3 Related FAA Advisory Circulars.

FAA Advisory Circulars are available through the FAA website, http://www.faa.gov.

- AC 450.103-1, *System Safety Program, when published*.
- AC 450.107-1, *Hazard Control Strategy Determination, dated June 15, 2021*.
- AC 450.141-1, *Computing Systems Safety, dated October 15, 2020*.

3.4 Related Industry Documents.

- MIL-STD-882E, Department of Defense Standard Practice, *System Safety*, dated May 11, 2012, https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=36027.

Note: The industry documents referenced in this section refer to the current revisions or regulatory authorities' accepted revisions.

4 DEFINITION OF TERMS.

For this AC, the terms and definitions from § 401.7 apply.

5 ACRONYMS.

AC – Advisory Circular

CFR – Code of Federal Regulations

ESD – Electro-Static Discharge

FAA – Federal Aviation Administration

FOD – Foreign Object Debris

FHA – Flight Hazard Analysis

FMEA – Failure Modes and Effects Analysis

FSS – Flight Safety System

FTA – Fault Tree Analysis

NOTMARs – Notices to Mariners

OMB – Office of Management and Budget

TBD – To Be Determined

V&V – Validation and Verification

6 OVERVIEW.

6.1 Objective of Flight Hazard Analysis.

A flight hazard analysis identifies key system design and operation data, documents the overall system safety risk to the public, and determines the necessary hazard controls (mitigations) to ensure the residual risk meets acceptable criteria. System safety risk documented in the flight hazard analysis is typically expressed in qualitative terminology; however, there may be sufficient operational history and subsystem analysis to express risk in quantitative terms.

6.2 A Flight Hazard Analysis differs from Flight Safety Analysis.

6.2.1 Risk as stated in the flight hazard analysis is different than as stated in the flight safety analysis requirements of § 450.113. Flight hazard analysis and flight safety analysis are somewhat interrelated but intentionally independent analyses that are both integral to the overall hazard control strategy. It is important to note that compliance with § 450.101 risk criteria does not relieve the operator from completing the flight hazard analysis.

6.2.2 A flight hazard analysis will identify all reasonably foreseeable hazards to public safety from the operation. Most of those hazards can be eliminated or mitigated with validation and verification. But there will always be residual risk from the operation. A flight hazard analysis must ensure that the likelihood of any hazardous condition that may cause death or serious injury to the public is extremely remote in accordance with § 450.109(b)(3).

6.2.3 The objective of the flight safety analysis is to characterize the overall risk to the public caused by the operation as a whole in consistent quantitative terms. A flight safety analysis is used to derive necessary operational controls and demonstrate compliance with public safety criteria in accordance with § 450.101.

6.3 Flight Hazard Analysis Methodology.

The flight hazard analysis methodology must be defined per § 450.103(b)(1). Per the guidance of AC 450.103-1, *System Safety Program*, this should be accomplished by the documented system safety program. Application of mitigation measures identified by the flight hazard analysis are intended to help reduce the system safety risk to the public to the acceptable levels determined by the system safety program and in accordance with § 450.109(b)(3). Additionally, the data documented in the flight hazard analysis is utilized to ensure public safety as defined by the documented system safety program.

6.4 Aspects of a Flight Hazard Analysis.

Flight hazard analysis may be utilized as a hazard control strategy but is also mandated by § 450.107(c) for a flight, or phase of flight, if the public safety hazards cannot be mitigated adequately to meet the public risk criteria of § 450.101(a), (b), and (c) using physical containment, wind weighting, or flight abort. This use of a flight hazard analysis to derive hazard controls provides flexibility that does not currently exist under the prescriptive requirements of Part 417 but is broadly consistent with Part 431 and

Part 435. In accordance with § 450.109(b), a flight hazard analysis must identify, describe, and analyze all reasonably foreseeable hazards to public safety resulting from the flight of a launch or reentry vehicle. The flight hazard analysis should be performed early in system development and operation conceptualization to define the system safety risk to the public in order to positively influence design and operation decisions. Flight hazard analysis products must be submitted to the FAA as part of an application, per § 450.109(f)(1) and continued to be maintained throughout the lifecycle of the launch or reentry system, in accordance with § 450.109(c) through (e). A flight hazard analysis must:

1. Identify all reasonably foreseeable hazards, and the corresponding failure mode for each hazard, associated with the launch or reentry system relevant to public safety (§ 450.109(b)(1));
2. Assess the likelihood and severity of each system safety hazard to the public (§ 450.109(b)(3);
3. Ensure that the system safety risk associated with each system safety hazard to the public meets defined acceptance criteria (§ 450.109(b)(3));
4. Identify and describe the risk elimination and mitigation measures required to satisfy the acceptance criteria (§ 450.109(b)(4)); and
5. Document that the risk elimination and mitigation measures achieve the acceptable levels through validation and verification (§ 450.109(b)(5)).

6.5 **Formal Traceability of System Safety Hazards**.

Formal tracking methods should be established to show direct connections between all aspects of system safety hazards to the public. Hazard tracking systems may contain all the necessary data but do not typically show these direct connections. **Table A-1** shows the types of information that an applicant should provide to demonstrate traceability.

6.6 **System Safety Hazards and Software Safety**.

6.6.1 In accordance with § 450.141(a), if the flight hazard analysis identifies software or data utilized in a subsystem or the integrated system as potential hazard sources or hazard controls, then the applicant should perform a software hazard analysis to identify computing system safety items and assess their level of criticality.

6.6.2 Per the guidance of AC 450.141-1, software hazard analyses identify potential software faults and their effects on the computing system and the system as a whole, as well as mitigation measures that can be used to reduce the risk. The analytical method and level of detail in the analysis should correspond to the complexity of the software and computing system, intricacy of the operations, and scope of the program. Also, software hazard analyses should consider a range of potential error conditions.

7 PERFORMING A FLIGHT HAZARD ANALYSIS.

7.1 **Identify Hazards**.

The hazards referred to in a flight hazard analysis are the system safety hazards to the public that occur from a system failure. The starting point for identifying system safety hazards to the public is the functional hazard analysis as required by § 450.107(b) that decomposes the system functions and assesses the end effect of their possible failures on system operation. In accordance with § 450.109(b)(1), a flight hazard analysis must identify all reasonably foreseeable hazards associated with a launch or reentry system relevant to public safety.

7.1.1 Hazard Traceability.

Traceability ensures proper identification of system safety hazards to the public for § 450.109(b)(1) and should be demonstrated from:

1. Subsystem and component functional failures to their causes; and
2. Subsystem and component functional failures to respective system safety hazards to the public at the system and mission level.

7.1.2 Data from the Functional Hazard Analysis.

System failures leading to system safety hazards to the public should include all applicable failures identified in the functional hazard analysis. Other possible failures not in the functional hazard analysis should be included if new ones are uncovered when considering public safety. To ensure proper identification of system safety hazards to the public for § 450.109(b)(1), an operator should use decomposition of systems beyond what is in the functional hazard analysis to identify the causes of system failures. This identification is an essential precursor to applying mitigations that reduce or eliminate the system safety hazards to the public. There will likely be multiple potential causes for each system failure. To ensure proper identification and mitigation of system safety hazards to the public for § 450.109(b)(1) and (4), each potential cause of a failure should be specified to a level of detail (down to a subsystem or component level) in accordance with § 450.109(b)(1)(ii) where it is possible to apply a mitigation.

7.1.3 Data beyond the Functional Hazard Analysis.

Beyond the functional hazard analysis, supplemental data routinely utilized to identify system failures and their causes include:

- Fault Tree Analysis (FTA) – A reliability engineering analysis that uses a logic diagram to identify and map causes of top-level events. Additionally, a FTA allows for quantification of system failure probability, determination of fault tolerance, identification of common causes and single point failures, etc.
- Failure Modes and Effects Analysis (FMEA) – A reliability engineering analysis used to identify low-level component failures and their causes and assess their effects on higher-level systems.

7.2 **Assessing Likelihood and Severity of Each Hazard.**

The likelihood and severity of each system safety hazard to the public must be assessed, in accordance with § 450.109(b)(2), in order to determine the associated system safety risk. The characterization of each system safety risk allows for determining the necessity, and proper application, of any additional mitigation actions.

7.2.1 Resources for System Safety Risk Assessments.

To satisfy § 450.109(b)(2), suitable assessment severity categories and likelihood levels criteria should be determined for each specific program. The risk assessment with respect to system safety hazards to the public generally utilizes qualitative statements; however, there may be sufficient data to utilize quantitative terms. AC 450.103-1, *System Safety Program*, provides guidance on assessing and documenting system safety risk, including severity categories and likelihood levels.

7.2.2 Utilizing a Systematic Assessment Process.

7.2.2.1 The FAA encourages, but does not require, the utilization of a systematic development process that allows for a baseline assessment of pre-mitigation risk for each hazard. It is a common system safety practice to assess risk prior to implementing a mitigation in order to deliberately design a mitigation strategy for each hazard. The FAA recognizes that some applicants will not utilize a pre-mitigation risk assessment as is common in rapid development and experimental programs. The FAA recommends that applicants who choose not to utilize a pre-mitigation risk assessment strategy discuss the appropriateness of their development process and any risk assessment assumptions during pre-application consultation. This strategy may not be acceptable with all programs. Irrespective of the applicant's development process, post-mitigation risk assessment should be performed to determine the residual system safety risk to the public.

7.2.2.2 Additionally, to ensure proper mitigation of system safety hazards to the public for § 450.109(b)(4), risk assessment should be performed at the appropriate levels, primarily the: (1) subsystem and component level and (2) system and mission level. Risk assessment at these levels allows for greater insight into the effectiveness of mitigations and verifications specific to each cause of each functional failure resulting in a system safety hazard to the public and appropriate application of component, subsystem, system and mission mitigations and verifications.

7.2.3 Risk Assessment Traceability.

Traceability ensures proper assessment for § 450.109(b)(3) and should be demonstrated from subsystem and component level risk assessment to system and mission level risk assessment.

7.3 **Mitigate Risk to Acceptable Levels**.

Risk elimination or mitigation measures must be implemented to reduce risks to the acceptable level of § 450.109(b)(3).

7.3.1 Proper Risk Mitigation Process.

Mitigating risk does not change severity of the hazard, only the likelihood. If there is a change in severity, it should be documented as a new risk. For example, a main fuel valve mechanical failure may cause unterminated thrust and a departure of the vehicle from the operating area. The hazard risk was determined to have a consequence of "Catastrophic" and a likelihood of "Remote." That valve was replaced with a more reliable valve as a mitigation. The mitigation is determined to change the likelihood to "Extremely Remote," but the new valve cannot impact the consequence of the failure, which remains "Catastrophic."

7.3.2 Developing Risk Acceptance Criteria.

Risk acceptance is determined by comparison of final assessed system safety risk against established acceptance criteria. Suitable risk acceptance criteria must be determined for each specific program and documented in the system safety program compliant with § 450.103 and utilizing the guidance of AC 450.103-1, *System Safety Program*. To ensure proper acceptance of risks associated with system safety hazards to the public for § 450.109(b)(3), the associated residual risk should meet the established acceptance criteria and the rationale for acceptance should be documented.

7.3.3 Baseline of Risk Acceptability.

In accordance with § 450.109(b)(3), the baseline standard for risk acceptability of system safety hazards to the public is to ensure the likelihood of any hazardous condition that may cause death or serious injury to the public is extremely remote as defined in AC 450.103-1.

As documented in AC 450.103-1, *System Safety Program*, extremely remote should be considered "so unlikely, it can be assumed occurrence may not be experienced, with a likelihood of occurrence less than 10^{-6} in any one mission."

Note: The standards for risk acceptability are intentionally strict to ensure protection of the public. Sufficient mitigation to control the hazard should be demonstrated.

7.4 **Identifying and Describing Risk Mitigation Measures**.

Risk elimination and mitigation measures must be identified and described for system safety risks to the public that are initially deemed unacceptable in accordance with § 450.109(b)(4). In accordance with § 450.109(b)(5), the risk elimination and mitigation measures must document reduction to the acceptable qualitative level of § 450.109(b)(3). Consideration should be given as to whether proposed risk mitigation measures introduce new hazards. To allow flexibility, the FAA has not mandated any particular mitigation approach. Selection of a risk elimination or mitigation measure is usually based on a number of factors, such as the type of operation, feasibility of implementation, effectiveness, and impact on system performance. Where possible, the FAA expects the utilization of existing industry standards for mitigations.

7.4.1 Risk Mitigation Traceability.

Traceability ensures proper application of mitigations for § 450.109(b)(4) and should be demonstrated from:

1. Subsystem and component functional failures to their causes to respective mitigations;
2. Subsystem and component functional failures to respective system safety hazards to the public at the system and mission level;
3. Subsystem and component level risk assessment to system and mission level risk assessment; and
4. System safety hazards to the public at the system and mission level to their respective mitigations.

7.4.2 System Safety Design Order of Precedence.

MIL-STD-882E identifies the following mitigation approaches in order of decreasing effectiveness:

a. Eliminate hazards through design selection;
b. Reduce risk through design alteration;
c. Incorporate engineered features or devices;
d. Provide warning devices; and
e. Incorporate signage, procedures, training, and personal protective equipment (PPE).

7.4.3 Potential Risk Mitigation Methods.

7.4.3.1 Design or Operate for Minimum Risk.

The first priority should be to eliminate system safety hazards to the public through appropriate design selections or operational decisions. Unacceptable system safety risk to the public that cannot be eliminated must be reduced to acceptable levels. An example of designing out risk to the public would be eliminating the use of toxic substances.

7.4.3.2 Incorporate Safety Devices.

If system safety hazards to the public cannot be eliminated through design selection or operational decisions, then system safety risks to the public should be reduced using active or passive safety devices. An example of an active safety device would be utilization of a computing system for shutting down a rocket engine when sensors detect thrust chamber temperatures outside of operational parameters. Examples of passive safety devices include burst disks in pressure systems, spring-loaded pressure relief valves, and break wires between stages. Provisions should be made for periodic functional checks of safety devices, where appropriate.

7.4.3.3 Provide Warning Devices.

When neither design nor safety devices eliminate or adequately reduce the risk of identified system safety hazards to the public, devices should be used to detect a hazardous condition and produce adequate warning. Warning signals and their application should be designed into the system to minimize the likelihood of inappropriate human reaction and response. A warning indicator on a flight controller console is an example of a warning device.

7.4.3.4 Develop and Implement Procedures and Training.

Procedures and training are generally used to supplement other mitigation measures. When it is not feasible to eliminate or adequately reduce the risk of identified system safety hazards to the public through design selection or specific safety and warning devices, procedures and training should be developed and implemented. Specific procedural and training mitigation measures that may be utilized include:

- Conducting dress rehearsals to ensure crew readiness under nominal and non-nominal flight conditions.
- Creating and using current and consistent checklists that ensure safe conduct of flight operations during nominal and non-nominal flights.
- Consolidating flight rules, procedures, checklists, contingency plans, and emergency plans in a safety directive, notebook, or other compilation.
- Establishing communication protocols, including defined radio communications terminology and a common intercom channel for communications.
- Conducting flight readiness reviews.

7.5 **Validation and Verification**.

The reduction of system safety hazards to the public via risk mitigations applied at various levels (component, subsystem, system, or mission) must be validated and verified as required by § 450.109(b)(5).

7.5.1 Validation of Risk Mitigations and Verification Methods.

Per § 450.109(b)(5), validation evidence must be documented. It must demonstrate that the risk elimination and mitigation measures achieve the risk level specified by § 450.109(b)(3). This documented evidence (e.g., V&V Tracking Log) must be provided to the FAA in accordance with 450.109(f)(1). Validation determines whether the implemented mitigation measures and their respective verification methods are sound. Thus, the validation effort ensures that each mitigation and verification is unambiguous, correct, complete, and consistent. In addition, the validation process evaluates that each mitigation measure and respective verification is well understood and operationally and technically feasible.

7.5.2 Verifying Risk Mitigations.

Verification is the process of identifying and producing verifiable and measurable evidence for ensuring that the respective mitigation measures adequately support the documented reduction of system safety risk to the public. Where possible, the FAA expects verification of mitigation measures to utilize existing industry standards. Essential information for verification includes:

- Identification of specific method(s) used to verify the mitigation measure;
- Identification of specific evidence to be produced; and
- Indication of closure based on successful completion of specified method with production of adequate, verifiable, and measurable evidence.

7.5.2.1 Verification Artifacts.

Per § 450.109(b)(5), verification evidence must be documented and it must demonstrate that the risk elimination and mitigation measures achieve the risk level specified by § 450.109(b)(3). This documented evidence, which can include design analysis, test data, and inspection reports, must be provided to the FAA in accordance with 450.109(f)(1). Ideally, all mitigation measures should be validated and verified by the time of application submittal. The FAA recognizes that applicants may not have the ability to verify all mitigations prior to submission of an application. In those instances, an acceptable verification closure strategy should be documented with expected completion dates (which must be closed prior to licensed operation pursuant to any relevant terms and conditions of the license). This strategy should be provided to the FAA with adequate time to review the closure status of verification evidence prior to the initiation of the applicable licensed activity.

7.5.2.2 Verification Traceability.

Traceability ensures proper application of verifications for § 450.109(b)(5) and should be demonstrated from:

1. Subsystem and component functional failures to their causes to respective mitigations to adequate verifications;
2. Subsystem and component functional failures to respective system safety hazards to the public at the system and mission level;
3. Subsystem and component level risk assessment to system and mission level risk assessment; and
4. System safety hazards to the public at the system and mission level to their respective mitigations to adequate verifications.

7.5.2.3 Verification Methods.

The FAA encourages discussion on proposed verification methods early in the licensing process. Four acceptable methods of verifying mitigation measures, in accordance with § 450.109(b)(5), include:

- Analysis – Technical or mathematical evaluation, mathematical models, simulations, algorithms, and circuit diagrams.
- Component, subsystem, or system test – Actual operation to evaluate performance of system elements during ambient conditions or in operational environments at or above expected levels to measure safety margins. These tests include functional tests and environmental tests.
- Demonstration – Actual operation of the system or subsystem under specified scenarios, often used to verify reliability, transportability, maintainability, serviceability, and human engineering factors.
- Inspection – Physical examination of hardware, software code, or documentation to verify compliance of the feature with predetermined criteria.

7.5.3 Iterative Approach of Validation and Verification.

The validation and verification (V&V) process is a comprehensive, closed-looped, iterative process to be used in all phases of the lifecycle of a launch or reentry system. Any mitigation that fails V&V cannot be relied on for elimination or reduction of system safety risks to the public.

7.6 **Identifying New Hazards and Updating the Flight Hazard Analysis.**

In accordance with § 450.109(c), criteria and techniques must be established and documented for identifying new hazards and updating a flight hazard analysis throughout the lifecycle of the launch or reentry system. In accordance with § 450.109(e), a process must be defined and implemented for continually updating the flight hazard analysis and system safety risk assessment to reflect knowledge gained during the lifecycle of the launch or reentry system.

7.6.1 Updates from Lifecycle Data.

Foreseeably, data gained during design, manufacture, test and operation, including the discovery of anomalies and faults, usually impacts a flight hazard analysis. Necessary data should be identified, and approaches should be implemented, to detect anomalies and failures in order to improve the flight hazard analysis. Additionally, information gained during assembly and operation of components, subsystems, and next-level systems contributes to the further understanding of the overall system and mission and may lead to additional updates to the flight hazard analysis. A process should be implemented to update the flight hazard analysis and residual system safety risk assessment to reflect knowledge gained during the lifecycle of the integrated system and mission.

7.6.2 Accuracy via the System Safety Program.

In accordance with § 450.103(b) and (d) and explained more fully in AC 450.103-1, *System Safety Program*, methods to detect flight anomalies and system failures and processes for evaluating post-flight data must be defined in the documented system safety program. The flight hazard analysis should adequately reflect the data gained from these methods and processes to ensure accuracy throughout the lifecycle of a launch or reentry system.

7.6.3 Completeness Prior to Flight.

In accordance with § 450.109(d), the flight hazard analysis must be complete and all system safety hazards to the public must be mitigated to acceptable levels, specifically that of § 450.109(b)(3), for every launch or reentry.

7.7 **Application Requirements.**

In accordance with § 450.109(f), an application must include: (1) the flight hazard analysis data produced in accordance with § 450.109(b)(1) through (5), including the verification evidence for the risk elimination and mitigation measures; and (2) the criteria and techniques for identifying new hazards throughout the lifecycle of the launch or reentry system, as required by § 450.109(c).

Appendix A. System Safety Template for § 450.109 Flight Hazard Analysis.

Table A-1 conveys the types of data that should be provided by an acceptable system safety analysis, including a method for traceability between all aspects of system safety hazards to the public. It is intended as a guide to show what information should be provided within a flight hazard analysis. It also shows how logical tracking for each item can be used to show the relationships between the different pieces of information. A hazard analysis format conveying the information of **Table A-1**, such as similar tables or traditional worksheets, should be utilized.

TABLE A-1. System Safety Template for § 450.109 Flight Hazard Analysis

		Subsystem and Component Level												**System and Mission Level[1]**			
		Subsystem(s)	**Component(s) / Item(s)**	**Functional Failure ID(s)**	**Failure Description and End Effect**	**Possible Cause(s)**	**Risk Before Mitigation Measures**			**Risk Elimination / Mitigation Measures**	**Risk After Mitigation Measures**			**Verification Evidence**	**Hazard to Public[1]**	**Risk Elimination / Mitigation Measures[1]**	**Risk After Mitigation Measures[1]**	**Verification Evidence[1]**
							L	**S**	**R**		**L**	**S**	**R**				**L**	**S**	**R**	
Top-Level System [TBD]	**Next-Level System [TBD]**	Avionics	Main Computer	TBD	Main computer [Function TBD] during [Mission Phase TBD] fails [Failure TBD], possibly resulting in loss of vehicle control, break-up, or [End Effect TBD]	**C1** Board Failure **C2** Electro-Static Discharge (ESD) **C3** Foreign Object Debris (FOD) **C4**, and so on…	Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of board failure (design, test, manufacturing process, etc.) **C1.M2** – Specific to mitigation of C1 **C1.M3**, and so on…	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on… **C1.M3.V1,** and so on…	**H1** Off-nominal trajectory **H2** Abort Debris **H3** Reentry Debris **H4**, and so on…	**H1.M1** - Specific to mitigation of **H1** [Flight Safety System (FSS), operational restrictions, clear areas, etc…] **H1.M2**, and so on…	TBD	TBD	TBD	**H1.M1.V1** – Documented evidence specific to **H1.M1** mitigation **H1.M1.V2**, and so on… **H1.M2.V1**, and so on…
										C2.M1 – Specific to mitigation of ESD (design, test, manufacturing process, etc.) **C2.M2** - Specific to mitigation of C2 **C2.M3**, and so on…				**C2.M1.V1** – Documented evidence specific to performed **C2.M1** mitigation **C2.M1.V2**, and so on… **C2.M2.V1**, and so on… **C2.M3.V1**, and so on…		**H2.M1** - Specific to mitigation of **H2** [deorbit criteria, contingencies, established clear areas for NOTAM and NOTMAR, etc…] **H2.M2,** and so on…				**H2.M1.V1** – Documented evidence specific to **H2.M1** mitigation **H2.M1.V2**, and so on… **H2.M2.V1**, and so on…
										C3.M1 – Specific to mitigation of FOD (design, test, manufacturing process, etc.) **C3.M2** - Specific to mitigation of C3 **C3.M3**, and so on…				**C3.M1.V1** – Documented evidence specific to performed **C3.M1** mitigation **C3.M1.V2**, and so on… **C3.M2.V1**, and so on… **C3.M3.V1**, and so on…		**H3.M1** - Specific to mitigation of **H3** [abort criteria, mission rules, contingencies, established clear areas for NOTAM and NOTMAR, etc…] **H3.M2**, and so on…				**H3.M1.V1** – Documented evidence specific to **H3.M1** mitigation **H3.M1.V2**, and so on… **H3.M2.V1**, and so on…

Note:

1 - “System and Mission Level” may be captured as shown or in a separate table or spreadsheet with traceability to “Subsystem and Component Level”

2 - “C1.M1.V1” is only an example; the key is to demonstrate traceability by a suitable method.

3 - L = Likelihood; S = Severity; R = Risk

4 - Typically within system safety: Likelihood (L) = Probability (P); Severity (S) = Consequence (C); L x S = R

OMB Control Number: 2120-0746
(Expiration Date: 08/31/2023)

Advisory Circular Feedback

Paperwork Reduction Act Burden Statement: A federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a currently valid OMB Control Number. The OMB Control Number for this information collection is 2120-0746. Public reporting for this collection of information is estimated to be approximately 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. All responses to this collection of information are voluntary to obtain or retain benefits per 14 CFR 77. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: Information Collection Clearance Officer, Federal Aviation Administration, 10101 Hillwood Parkway, Fort Worth, TX 76177-1524.

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to ASTApplications@faa.gov, or (2) faxing it to (202) 267-5450.

Subject: (insert AC title/number here) Date: Click here to enter text.

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph Click here to enter text. on page Click here to enter text..

☐ Recommend paragraph Click here to enter text. on page Click here to enter text. be changed as follows:

Click here to enter text.

☐ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

Click here to enter text.

☐ Other comments:

Click here to enter text.

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____