FAA
Commercial Space Transportation
faa.gov/space

SYSTEM SAFETY WORKSHOP

Presented by
Rene Rey & Christopher Vance
System Safety Branch [ASA-220]

Tuesday, May 16, 2023,
9:00 am — 10:30 am EST

Questions can be sent in
through the Q&A Zoom Chat Box

Agenda

Overview of Part 450 System Safety

- ❑ § 450.103 “System Safety Program”
- ❑ § 450.107 “Hazard Control Strategies”
- ❑ § 450.109 “Flight Hazard Analysis”
- ❑ § 450.143* “Safety-Critical Systems Design, Test, & Documentation (DT&D)”
- ❑ Additional Safety-Critical Requirements
- ❑ § 450.141 “Computing System Safety”
- ❑ § 450.139* “Toxic Hazards for Flight”

* AC as not been published yet and this information is currently in draft form only. Information may change upon publication of AC.

Agenda

Overview of Part 450 System Safety

- ❑ § 450.103 “System Safety Program”
- ❑ § 450.107 “Hazard Control Strategies”
- ❑ § 450.109 “Flight Hazard Analysis”
- ❑ § 450.143* “Safety-Critical Systems Design, Test, & Documentation (DT&D)”
- ❑ Additional Safety-Critical Requirements
- ❑ § 450.141 “Computing System Safety”
- ❑ § 450.139* “Toxic Hazards for Flight”

* AC as not been published yet and this information is currently in draft form only. Information may change upon publication of AC.

§ 450.109 Flight Hazard Analysis

(a) ***Applicability.*** This section applies to the use of a flight hazard analysis as a hazard control strategy to derive hazard controls for the flight, or phase of flight, of a launch or reentry vehicle. Hazards associated with computing systems and software are further addressed in § 450.141.

(b) ***Analysis.*** 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.…

Ref. AC 450.109-1, Section 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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 6.2: "A Flight Hazard Analysis differs from Flight Safety Analysis (FSA)"

- ❑ Risk as stated in the flight hazard analysis (HA) is different than as stated in the FSA
- ❑ Flight HA and FSA are somewhat interrelated but intentionally independent analyses that are both integral to the overall hazard control strategy.
- ❑ A flight HA 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)]
- ❑ The objective of the FSA is to characterize the overall risk to the public caused by the operation as a whole in consistent quantitative terms.
- ❑ Compliance with § 450.101 safety criteria does not relieve the operator from completing the flight HA, when determined as a hazard control strategy

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 6.3 "Flight Hazard Analysis Methodology"

- ❑ The flight HA 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.
- ❑ The data documented in the flight HA is utilized to ensure public safety as defined by the documented system safety program.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 6.4 "Aspects of a Flight Hazard Analysis"

- Flight HA 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 HA 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.
- 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 continue to be maintained throughout the lifecycle of the launch or reentry system, in accordance with § 450.109(c) through (e).

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 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.

Subsystem and Component Level

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
					L	S	R		L	S	R	
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)	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

System and Mission Level[1]

Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1]			Verification Evidence[1]
		L	S	R	
H1 Off-nominal trajectory **H2** Abort Debris	**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…

[*The template of*] **Table A-1** shows the types of information that an applicant should provide to demonstrate traceability.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 6.6 "System Safety Hazards and Software Safety"

- 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.
- 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.

§ 450.109 Flight Hazard Analysis

(b) *Analysis*. 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. Each 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, including those resulting from: (i) through (x)
2) Assess each hazard's likelihood and severity.
3) Ensure that the likelihood of any hazardous condition that may cause death or serious injury to the public is extremely remote.
4) Identify and describe the risk elimination and mitigation measures required to satisfy paragraph (b)(3) of this section.
5) Document that the risk elimination and mitigation measures achieve the risk level of paragraph (b)(3) of this section through validation and verification. Verification includes: (i) Analysis; (ii) Test; (iii) Demonstration; (iv) Inspection.

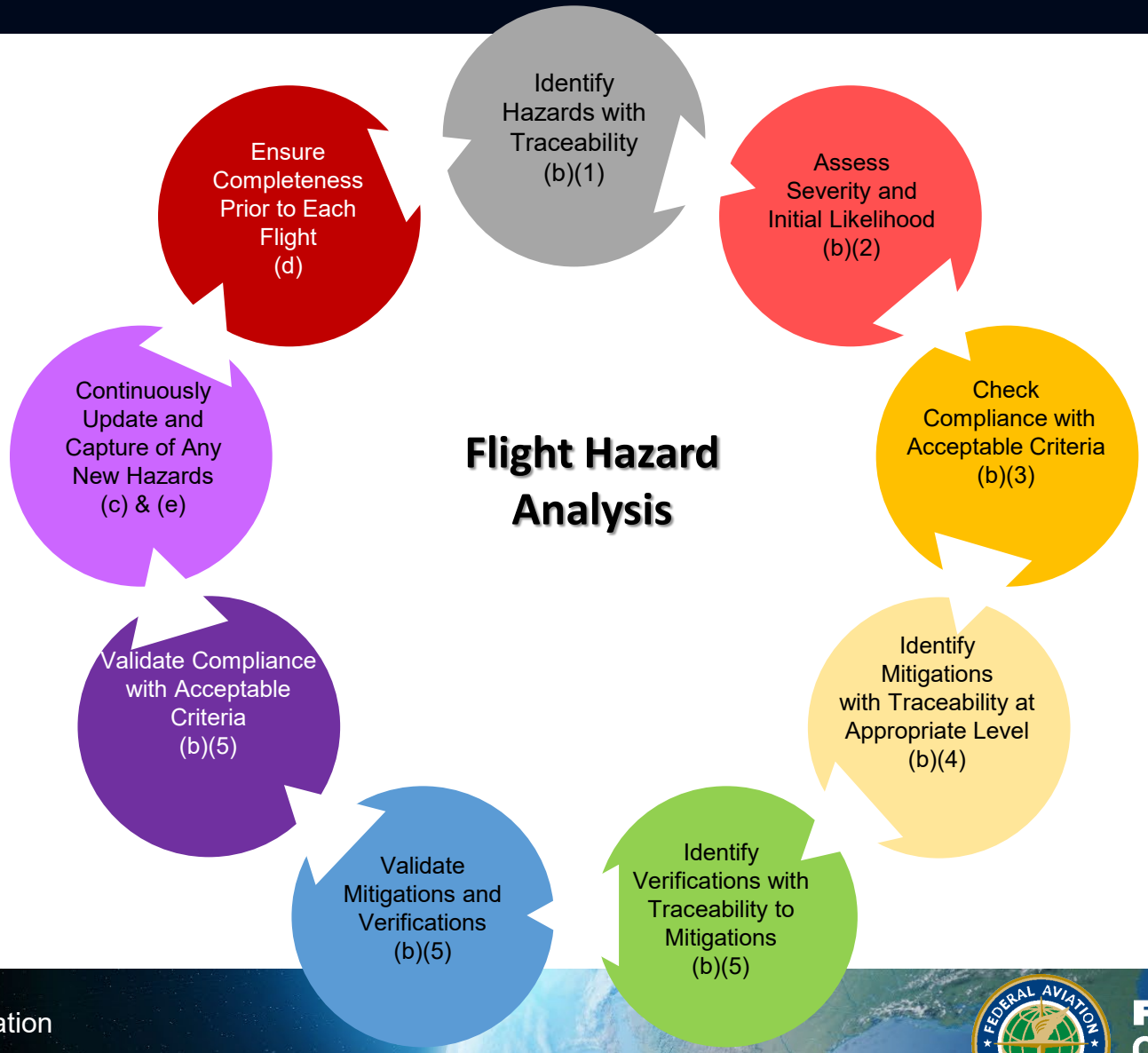
§ 450.109 Flight Hazard Analysis

(c) ***New Hazards****.* An operator must establish and document the criteria and techniques for identifying new hazards throughout the lifecycle of the launch or reentry system.

(d) ***Completeness Prior to Flight****.* For every launch or reentry, the flight hazard analysis must be complete and all hazards must be mitigated to an acceptable level in accordance with paragraph (b)(3) of this section.

(e) ***Updates****.* An operator must continually update the flight hazard analysis throughout the lifecycle of the launch or reentry system.

§ 450.109 Flight Hazard Analysis



§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.1: Identify Hazards.

Identify Hazards with Traceability (b)(1)

- ❑ 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 Assessment of the "end effect" resulting from each mechanism of each function during each phase, excluding mitigation and redundancy.

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.1: Identify Hazards. [CONTINUED]

Identify Hazards with Traceability (b)(1)

Data from/beyond 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.
- ❑ An operator should use decomposition of systems beyond what is in the functional hazard analysis to identify the causes of system failures. Beyond the functional hazard analysis, supplemental data routinely utilized to identify system failures and their causes include Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA)

  Note: Additional analysis tools include, at a minimum: Preliminary Hazard Analysis; Functional Hazard Analysis; System Requirements Hazard Analysis; Subsystem Hazard Analysis; Human Error Analysis; System Hazard Analysis; Operations Hazard Analysis; Health Hazard Analysis; and Integrated Systems Hazard Analysis
- ❑ There will likely be multiple potential causes for each system failure.
- ❑ 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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.2 "Assessing Likelihood and Severity of Each Hazard"

Assess Severity and Initial Likelihood (b)(2)

- ❑ 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.

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. Section A.1 of AC 450.103-1, *System Safety Program*, provides guidance on assessing and documenting system safety risk, including severity categories and likelihood levels.
- ❑ 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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.2 "Assessing Likelihood and Severity of Each Hazard" [CONTINUED]

Assess Severity and Initial Likelihood (b)(2)

Utilizing a Systematic Assessment Process

- 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.
- 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.
- 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.

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.3 "Mitigate Risk to Acceptable Levels"

Check Compliance with Acceptable Criteria (b)(3)

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

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.

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.3 "Mitigate Risk to Acceptable Levels" [CONTINUED]

Check Compliance with Acceptable Criteria (b)(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.

* At the System and Mission Level

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.4 "Identifying and Describing Risk Mitigation Measures"

Identify Mitigations with Traceability at Appropriate Level (b)(4)

- 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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.4 "Identifying and Describing Risk Mitigation Measures" [CONTINUED]

Identify Mitigations with Traceability at Appropriate Level (b)(4)

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.4 "Identifying and Describing Risk Mitigation Measures" [CONTINUED]

Identify Mitigations with Traceability at Appropriate Level (b)(4)

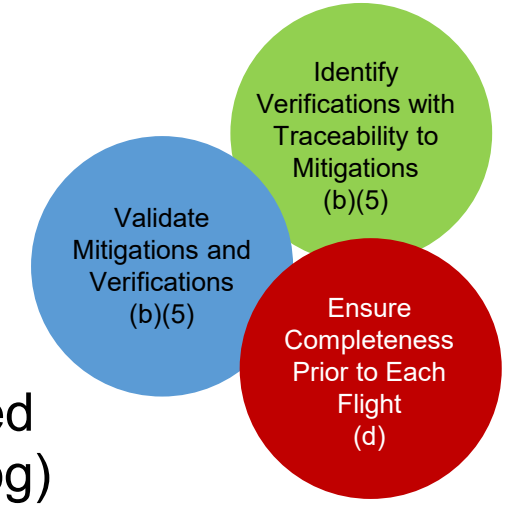
System Safety Design Order of Precedence

- 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).
- 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.
- Potential risk mitigation methods include: design or operate for minimum risk; incorporate safety devices; provide warning devices; develop and implement procedures and training.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 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).



<u>Validation of Risk Mitigations and Verification Methods</u>

- ❑ Per § 450.109(b)(5), validation evidence 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.
- ❑ The validation effort ensures that each mitigation and verification is unambiguous, correct, complete, and consistent.
- ❑ The validation process evaluates that each mitigation measure and respective verification is well understood and operationally and technically feasible.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.5 "Validation and Verification" [CONTINUED]

Identify Verifications with Traceability to Mitigations (b)(5)

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.5 "Validation and Verification" [CONTINUED]

Identify Verifications with Traceability to Mitigations (b)(5)

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.5 "Validation and Verification" [CONTINUED]

Identify Verifications with Traceability to Mitigations (b)(5)

Verification Artifacts

- ❑ Documented evidence can include design analysis, test data, and inspection reports
- ❑ 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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Section 7.5 "Validation and Verification" [CONTINUED]

Identify Verifications with Traceability to Mitigations (b)(5)

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.

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.

§ 450.109 Flight Hazard Analysis

Ref. AC 450.109-1, Appendix A

Top-Level System [TBD]	Next-Level System [TBD]	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 L	S	R	Risk Elimination / Mitigation Measures	Risk After Mitigation Measures L	S	R	Verification Evidence	Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1] L	S	R	Verification Evidence[1]
		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…

Data from Functional Hazard Analysis

Via Fault Tree Analyses; FMEA/FMECA; HEA Subsystem Hazard Analysis, etc.

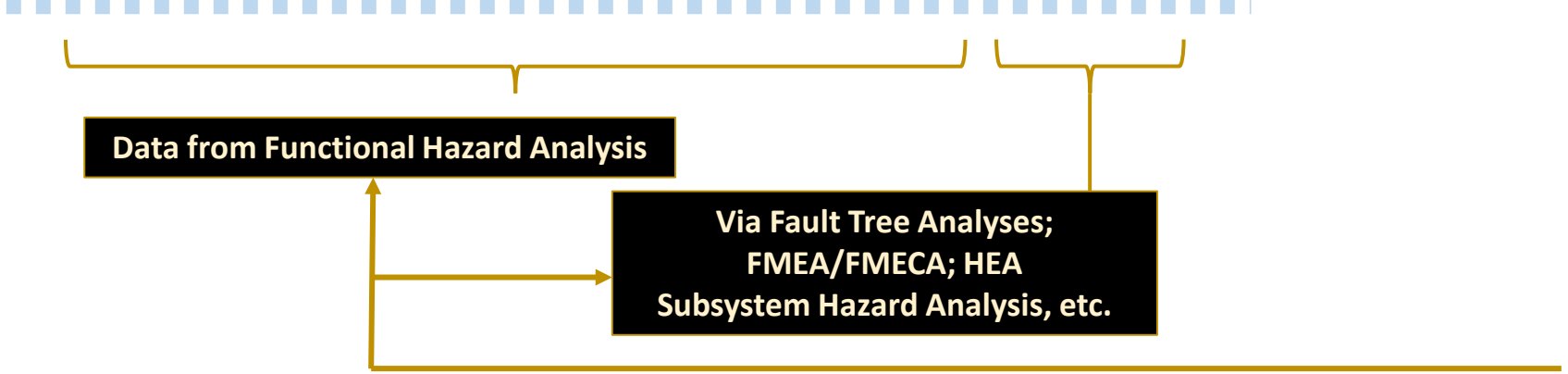
Identify/Verify mitigations to specific causes of functional failures at the subsystem/component level (e.g., design, manufacturing, etc.)

Identify/Verify specific system/mission mitigations for residual system safety risk of public safety hazards (e.g., FSS, ops restrictions, etc.)

↓ Traceability ↑

§ 450.109 Flight Hazard Analysis

Top-Level System [TBD]	Next-Level System [TBD]	Subsystem and Component Level					
		Subsystem(s)	Component(s) / Item(s)	Functional Failure ID(s)	Failure Description and End Effect	Possible Cause(s)	
		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	



§ 450.109 Flight Hazard Analysis

Risk Before Mitigation Measures			Risk Elimination / Mitigation Measures	Risk After Mitigation Measures			Verification Evidence
L	S	R		L	S	R	
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…
			C2.M1 – Specific to				C2.M1.V1 –

Identify/Verify mitigations to specific causes of functional failures at the subsystem/component level (e.g., design, manufacturing, etc.)

§ 450.109 Flight Hazard Analysis

System and Mission Level[1]					
Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1]			Verification Evidence[1]
		L	S	R	
H1 Off-nominal trajectory **H2** Abort Debris **H3** Reentry Debris	**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...
	H2.M1 - Specific to				**H2.M1.V1** – Documented

Identify/Verify specific system/mission mitigations for residual system safety risk of public safety hazards (e.g., FSS, ops restrictions, etc.)

Traceability

§ 450.109 Flight Hazard Analysis

(c) *New Hazards.* An operator must establish and document the criteria and techniques for identifying new hazards throughout the lifecycle of the launch or reentry system.

(e) *Updates.* An operator must continually update the flight hazard analysis throughout the lifecycle of the launch or reentry system.

Continuously Update and Capture of Any New Hazards (c) & (e)

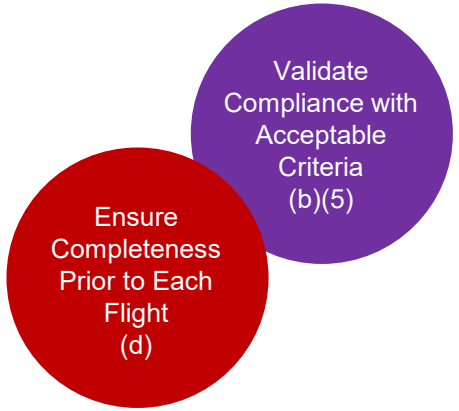
Ref. AC 450.109-1, Section 7.6 "Identifying New Hazards and Updating the Flight Hazard Analysis"

<u>Updates from Lifecycle Data</u>

- ❑ 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.

§ 450.109 Flight Hazard Analysis

(d) *Completeness Prior to Flight.* For every launch or reentry, the flight hazard analysis must be complete and all hazards must be mitigated to an acceptable level in accordance with paragraph (b)(3) of this section.



Ref. AC 450.109-1, Section 7.6 "Identifying New Hazards | and Updating the Flight Hazard Analysis" [CONTINUED]

<u>Accuracy via the System Safety Program</u>.

- ❑ 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.

§ 450.109 Flight Hazard Analysis

(f) *Application Requirements*. An applicant must submit in its application the following:

1) Flight hazard analysis products of paragraphs (b)(1) through (5) of this section, including data that verifies the risk elimination and mitigation measures resulting from the applicant's flight hazard analyses required by paragraph (b)(5) of this section; and
2) The criteria and techniques for identifying new hazards throughout the lifecycle of the launch or reentry system as required by paragraph (c) of this section.

AC 450.109-1, Appendix A "System Safety Template for § 450.109 Flight Hazard Analysis"

Adobe Acrobat Document

AC 450.109-1: Flight Hazard Analysis Appendix A

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

Top-Level System [TBD]	Next-Level System [TBD]	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 L	S	R	Risk Elimination / Mitigation Measures	Risk After Mitigation Measures L	S	R	Verification Evidence	Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1] L	S	R	Verification Evidence[1]
		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

Summary of § 450.109 Discussion

Summary of Key Topics

- ❑ Identifying all reasonably foreseeable hazards, and the corresponding failure mode (cause) for each hazard, associated with the launch or reentry system relevant to public safety
- ❑ Assess each hazard's likelihood and severity, at the "subsystem/component-level" and "system/mission-level"
- ❑ Identify and describe the risk elimination and mitigation measures, at the "subsystem/ component-level" and "system/mission-level"
- ❑ Document Verification and Validation, to ensure likelihood of any hazardous condition achieves the risk level of § 450.109(b)(3)
- ❑ Criteria and techniques for identifying new hazards throughout the lifecycle
- ❑ § 450.109 Flight Hazard Analysis is continually updated throughout the lifecycle and complete prior to each flight

§ 450.109 “Flight Hazard Analysis”

Agenda

Overview of Part 450 System Safety

- ❑ § 450.103 “System Safety Program”
- ❑ § 450.107 “Hazard Control Strategies”
- ❑ § 450.109 “Flight Hazard Analysis”
- ❑ § 450.143* “Safety-Critical Systems Design, Test, & Documentation (DT&D)”
- ❑ Additional Safety-Critical Requirements
- ❑ § 450.141 “Computing System Safety”
- ❑ § 450.139* “Toxic Hazards for Flight”

* AC as not been published yet and this information is currently in draft form only. Information may change upon publication of AC.

§ 450.143 "Safety-Critical Systems Design, Test & Documentation (DT&D)" [Non-FSS]

(a) ***Applicability.*** This section applies to all safety-critical systems, except for—

1) Highly reliable flight safety systems covered under § 450.145; or
2) Safety-critical systems* for which an operator demonstrates through its flight hazard analysis that the likelihood of any hazardous condition specifically associated with the system that may cause death or serious injury to the public is extremely remote, pursuant to § 450.109(b)(3).

AC 450.143-2 "Safety-Critical Systems DT&D (Non-FSS)" [Planned]

- ❑ Forthcoming to provide acceptable means of compliance
- ❑ AC 450.143-1** to cover non-"highly reliable" flight safety systems

Disclaimer: AC 450.143 is currently under development and is subject to change upon publication.

* Identified per § 450.107(b) and guidance of AC 450.107-1
** In development

§ 450.143 "Safety-Critical Systems Design, Test & Documentation (DT&D)" [Non-FSS]

(b) ***Design.*** An operator must design safety-critical systems such that no credible fault can lead to increased risk to the public beyond nominal safety-critical system operation.

(c) ***Qualification testing of design.*** An operator must functionally demonstrate the design of the vehicle's safety-critical systems at conditions beyond its predicted operating environments. The operator must select environmental test levels that ensure the design is sufficiently stressed to demonstrate that system performance is not degraded due to design tolerances, manufacturing variances, or uncertainties in the environment.

(d) Acceptance of hardware.

An operator must—

1) Functionally demonstrate any safety-critical system, while exposed to its predicted operating environments with margin, is free of defects, free of integration and workmanship errors, and ready for operational use; or
2) Combine in-process controls and a quality assurance process to ensure functional capability of any safety-critical system during its service life.

§ 450.143 “Safety-Critical Systems Design, Test & Documentation (DT&D)” [Non-FSS]

(e) Lifecycle of safety-critical systems.

1) The predicted operating environments must be based on conditions predicted to be encountered in all phases of flight, recovery, and transportation.

2) An operator must monitor the flight environments experienced by safety-critical system components to the extent necessary to—

   (i) Validate the predicted operating environments; and

   (ii) Assess the actual component life remaining or adjust any inspection period.

§ 450.143 "Safety-Critical Systems Design, Test & Documentation (DT&D)" [Non-FSS]

(f) ***Application requirements.***

	(1) A list and description of each safety-critical system;	> § 450.107 Functional Hazard Analysis > § 450.185 Ground Hazard Analysis > Systems Descriptions
	(2) Drawings and schematics for each safety-critical system;	Drawings and Schematics
	(3) A summary of the analysis to determine the predicted operating environments and duration to be applied to qualification and acceptance testing covering the service life of any safety-critical system;	> Environments Definition and Validation Method > Qualification Test Plan & Report/Results > Acceptance Test Plan & Report/Results
	(4) A description of any method used to validate the predicted operating environments;	Environments Definition and Validation Method
	(5) A description of any instrumentation or inspection processes to monitor aging of any safety-critical system;	> Acceptance and functional checkouts > Quality assurance process
		> Environments Monitoring Approach > Aging Assessment Process
	(6) The criteria and procedures for disposal or refurbishment for service life extension of safety-critical system components; and	Reuse Plan/Process
	(7) A description of the standards used in all phases of the lifecycle of each safety-critical system.	Identification and describe any utilization industry standards for the above

Summary of § 450.143 Discussion

Summary of Key Topics

- ❑ Determining applicability of § 450.143 design, test, and documentation requirements
- ❑ Design for credible faults of safety-critical systems
- ❑ Performing qualification testing and acceptance
- ❑ Accounting for environments encountered during the lifecycle

§ 450.143 “Safety-Critical Systems Design, Test & Documentation (DT&D)” [Non-FSS]

Agenda

Overview of Part 450 System Safety

- ❑ § 450.103 “System Safety Program”
- ❑ § 450.107 “Hazard Control Strategies”
- ❑ § 450.109 “Flight Hazard Analysis”
- ❑ § 450.143* “Safety-Critical Systems Design, Test, & Documentation (DT&D)”
- ❑ Additional Safety-Critical Requirements
- ❑ § 450.141 “Computing System Safety”
- ❑ § 450.139* “Toxic Hazards for Flight”

* AC as not been published yet and this information is currently in draft form only. Information may change upon publication of AC.

Additional Safety-Critical Requirements

Part 450 Preamble, Section 4, y, 6th Paragraph

The applicant's identification and proper management of safety-critical systems is fundamental to mitigating potential hazards and ensuring public safety, and the FAA will work with an applicant if it believes the applicant has failed to identify all safety-critical systems. The potential failure of safety-critical systems is integral to the FSA, and the vulnerabilities of safety-critical systems must be accounted for in the flight commit criteria, hazard analyses, lightning protection criteria, management of radio frequency to prevent interference, and communications plans.

System safety analysis to guide application and depth of "safety-critical" requirements

Additional Safety-Critical Requirements

REGULATION	PROVIDES FOR
§ 450.45	**Safety review and approval.** (e) *Vehicle description*. An applicant must submit the following: (3)(ii) A drawing of each vehicle that identifies: (C) Location of all safety-critical systems
§ 450.115	**Flight safety analysis methods.** (a) *Scope of the analysis*. An operator's flight safety analysis method must account for all reasonably foreseeable events and failures of safety-critical systems during nominal and non-nominal launch or reentry that could jeopardize public safety.
§ 450.149	**Safety-critical personnel qualifications.** (a) *General*. An operator must ensure safety-critical personnel are trained, qualified, and capable of performing their safety-critical tasks, and that their training is current. (b) Application requirements. An applicant must— (1) Identify safety-critical tasks that require qualified personnel;
§ 450.151	**Work shift and rest requirements.** (a) *General*. For any launch or reentry, an operator must document and implement rest requirements that ensure safety-critical personnel are physically and mentally capable of performing all assigned tasks.
§ 450.153	**Radio frequency management.** (a) *General*. For any radio frequency used, an operator must— (1) Ensure radio frequency interference does not adversely affect performance of any flight safety system or safety-critical system; and
§ 450.155	**Readiness.** (a) General. An operator must document and implement procedures to assess readiness to proceed with the flight of a launch or reentry vehicle. These procedures must address, at a minimum, the following: (2) Readiness of safety-critical personnel, systems, software, procedures, equipment, property, and services;

Additional Safety-Critical Requirements

REGULATION	PROVIDES FOR
§ 450.157	(a) An operator must implement communication procedures during the countdown and flight of a launch or reentry vehicle that— (2) Assign communication networks so that personnel identified in paragraph (a)(1) of this section have direct access to real-time, safety-critical information required to issue "hold/resume," "go/no go," and any abort commands; and …. (c) An operator must record all safety-critical communications network channels that are used for voice, video, or data transmissions that support safety-critical systems during each countdown.
§ 450.163	**Lightning hazard mitigation.** (a) *Lightning hazard mitigation*. An operator must— (2) Use a vehicle designed to protect safety-critical systems in the event of a direct lightning strike or nearby discharge.
§ 450.165	**Flight Commit Criteria.** (a) *General*. For each launch or reentry, an operator must establish and observe flight commit criteria that identify each condition necessary prior to flight to satisfy the requirements of § 450.101, and must include: (4) Confirmation that any safety-critical system is ready for flight;
§ 450.213	**Pre-flight reporting.** (f) *Launch or reentry schedule*. A licensee must file a launch or reentry schedule that identifies each review, rehearsal, and safety-critical operation. The schedule must be filed and updated in time to allow FAA personnel to participate in the reviews, rehearsals, and safety-critical operations.

Additional Safety-Critical Requirements

SYSTEM SAFETY WORKSHOP

Thank you for joining us.

FAA
Commercial Space Transportation
faa.gov/space