FAA
Commercial Space Transportation
faa.gov/space

SYSTEM SAFETY WORKSHOP

Presented by
Bhavyakumar Dave
System Safety Branch [ASA-220]

Thursday, May 11, 2023,
4:00 pm — 5:30 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”
  - Functional Hazard Analysis
- ❑ § 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.

§ 450.107 “Hazard Control Strategies”

(a) ***General.*** To meet the safety criteria of § 450.101(a), (b), or (c) for the flight, or any phase of flight, of a launch or reentry vehicle, an operator must use one or more of the hazard control strategies identified in § 450.108 through § 450.111.

(b) ***Hazard control strategy determination.*** For each phase of flight during a launch or reentry, an operator must use a functional hazard analysis to determine a hazard control strategy or strategies that account for—

(1) All functional failures associated with reasonably foreseeable hazardous events that have the capability to create a hazard to the public;
(2) Safety-critical systems; and
(3) A timeline of all safety-critical events.

Ref. AC 450.107-1, Section 6.1 “Hazard Control Strategies”

- ❑ The hazard control strategy is determined by conducting a functional hazard analysis.
- ❑ As appropriate, different hazard control strategies may be utilized during separate phases of flight, and multiple hazard control strategies may be necessary in the same phase.

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1, Section 6.1 “Hazard Control Strategies”

The hazard control strategies are:

- ❑ § 450.108 “Flight Abort” - The traditional safety approach for expendable launch vehicles. It is a process to limit or restrict the hazards to public safety and the safety of property presented by a launch vehicle or reentry vehicle, including any payload, while in flight by initiating and accomplishing a controlled ending to vehicle flight.
- ❑ § 450.109 “Flight Hazard Analysis” - The traditional safety approach for reusable launch vehicles, is the most flexible hazard control strategy because it allows for deriving specific hazard controls unique to the launch or reentry vehicle system and operations concept.
- ❑ § 450.110 “Physical Containment” - Used for low energy test flights when a launch vehicle does not have sufficient energy for any hazards associated with its flight to reach the public or critical assets.
- ❑ § 450.111 “Wind Weighting” - Traditionally used in the launch of unguided suborbital launch vehicles, otherwise known as sounding rockets, where launcher azimuth and elevation settings are adjusted to correct for the effects of wind conditions at the time of flight to provide a safe impact location for the launch vehicle or its components.

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1, Section 6.2.1 “Purposes of a Functional Hazard Analysis”

A functional hazard analysis is a critical element for ensuring public safety during flight.

- ❑ At a foundational level, the analysis provides a holistic, systematic approach to identifying potential hazards.
- ❑ Second, the analysis supports the validation of adequacy for determined hazard control strategies.
- ❑ Third, the analysis supports a justification for use of historical flight outcome data in the probability of failure analysis. Development of prior launch and reentry vehicles has included a structured system safety process, and thus this foundational system safety analysis is one necessary element in defining similar vehicles in accordance with § 450.131, *Probability of Failure Analysis*.
- ❑ Fourth, it provides a basis for developing quantitative models of debris, in accordance with § 450.121, and malfunction trajectories, in accordance with § 450.119.
- ❑ Fifth, the analysis is a basis for a flight hazard analysis if that hazard control strategy is used.

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1, Section 6.2.2

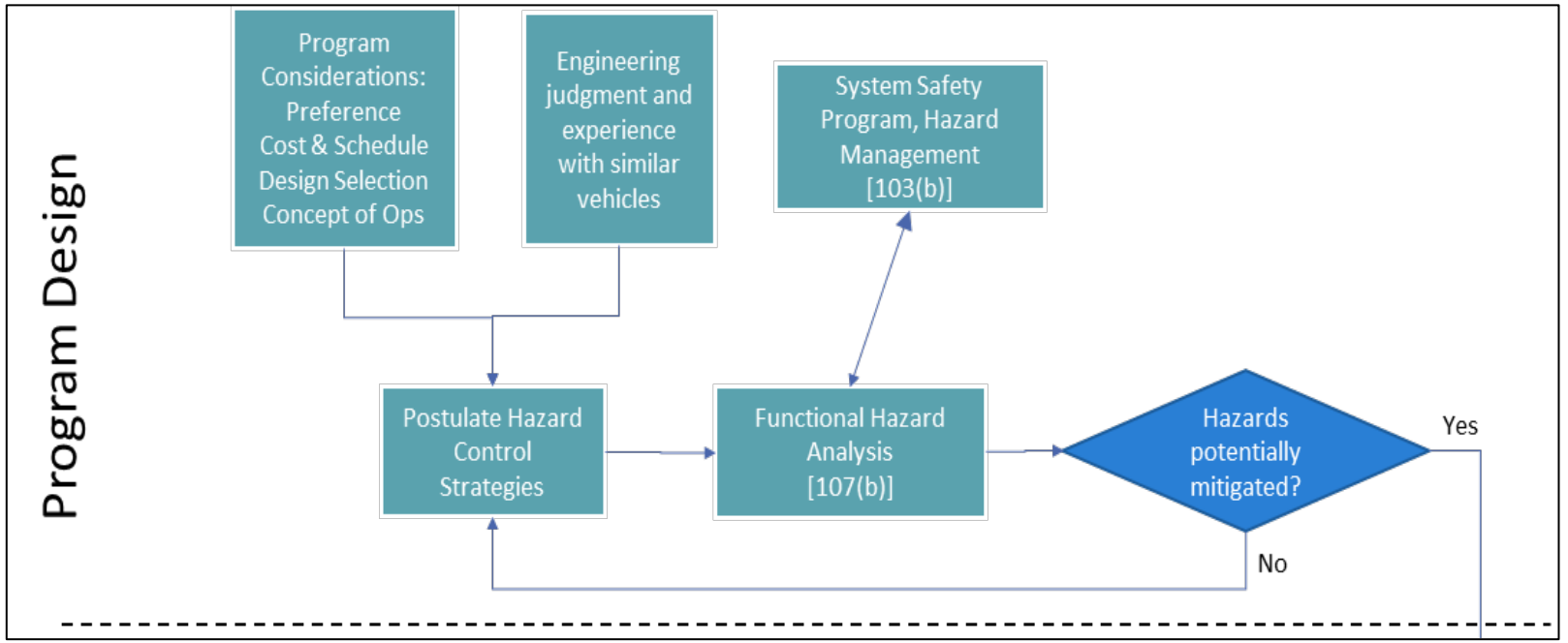
Two Constraints to HCS Determination

- **§ 450.107(c) *Flight hazard analysis*.** An operator must conduct a flight hazard analysis in accordance with § 450.109 of this part 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.
- In accordance with **§ 450.101(c) “High consequence event protection”**, if the consequence of any reasonably foreseeable failure mode, in any significant period of flight, is greater than 1×10^{-3} conditional expected casualties, then flight abort must be used as a hazard control strategy in accordance with the requirements of § 450.108, or the launch or reentry vehicle must have sufficient demonstrated reliability as agreed to by the FAA Administrator based on conditional expected casualties during that phase of flight. AC 450.101-1, *High Consequence Event Protection*, provides additional guidance on conditional expected casualty.

§ 450.107 “Hazard Control Strategies”

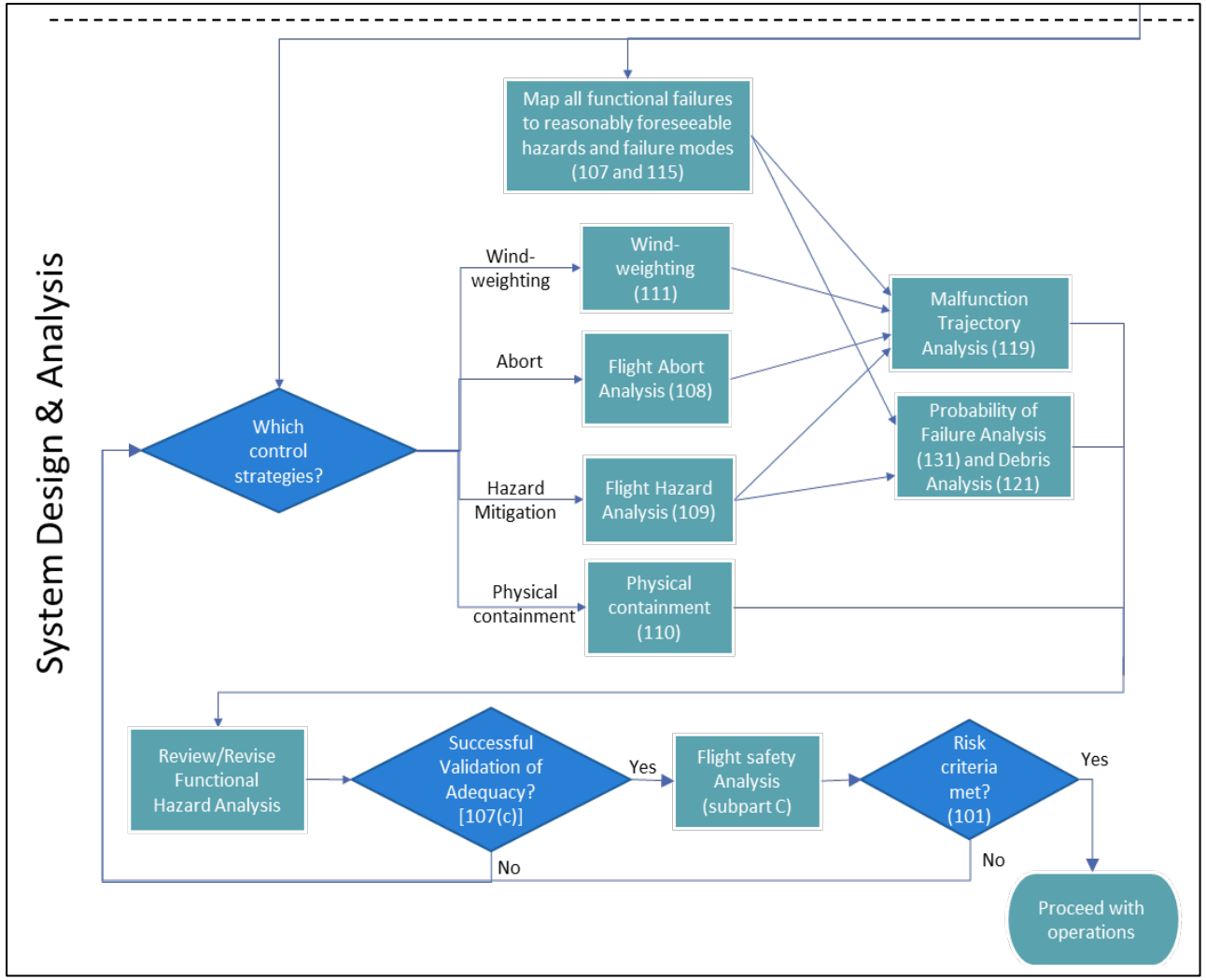
Ref. AC 450.107-1, Section 6.2.3: “Hazard Control Strategy Determination Logic”

- ❑ The approach to determining and validating hazard control strategies is a process, which is iterative.
- ❑ The functional hazard analysis is utilized to ensure that all potential hazards to the public have a determined hazard control strategy.
- ❑ Generally, the applicant will determine a hazard control strategy based on engineering and program considerations.



§ 450.107 “Hazard Control Strategies”

- If the hazards to the public are potentially mitigated, then the selected strategies are developed, and the supporting data is used as general input for the flight safety analysis.
- If adequate mitigation is not validated by supporting data, then the hazard control strategy should be revisited.
- If validation is successful, then the flight safety analysis is used to demonstrate whether the safety criteria are satisfied.
- If the safety criteria cannot be met, then additional hazard controls must be implemented, in accordance with 450.107(c).



§ 450.107 “Hazard Control Strategies”

(b) ***Hazard control strategy determination.*** For each phase of flight during a launch or reentry, an operator must use a functional hazard analysis to determine a hazard control strategy or strategies that account for—

(1) All functional failures associated with reasonably foreseeable hazardous events that have the capability to create a hazard to the public;

(2) Safety-critical systems; and

(3) A timeline of all safety-critical events.

Ref. AC 450.107-1, Section 7.1 “Functional Hazard Analysis”

- ❑ The functional hazard analysis should be completed as early as possible in the launch or reentry system’s lifecycle.
- ❑ A functional hazard analysis is used to analyze system functions associated with the operating concept.
- ❑ The term “reasonably foreseeable” is not associated with probability or likelihood, but is inherent to a methodical assessment of the entire system. “Reasonably foreseeable hazardous events” are those identifiable through the system safety process, beyond those that could be determined solely by “brainstorming.”

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1*, Section 7.1 “Functional Hazard Analysis”

- ❑ The functional hazard analysis is primarily used to identify and classify the overall system functions and consequences of functional failure or malfunction.
  - The objective is to identify all potential system, subsystem, and component functional failures that could impact public safety**.
  - Any foreseeable mitigations or predetermined hazard control strategies should not affect the identification of potential system safety hazards and respective functional sources (i.e. subsystem functional failures).
- ❑ Prior to performing a functional hazard analysis, an operator should have sufficient understanding of the mission.
- ❑ Subsequently, the functional hazard analysis, at a minimum, should provide***:

Will be available on the FAA.gov website:
PDF of AC 450.107-1A*,
Appendix A “System Safety Template for § 450.107 Functional Hazard Analysis:”

* Rev A updated this section - In release process
** At the System and Mission Level
*** Adapted from the guidance of MIL-STD-882E

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1*, Section 7.2 “Accuracy and Adequacy with Flight Safety Analysis”

- Section 450.113(a) requires that an FSA be performed and documented for all phases of flight, except as specified in § 450.113(b) regarding demonstrated reliability.
- The functional hazard analysis is essential for ensuring that all potential functional hazards are captured in the FSA, which in turn assists in assessment of the “end effect”.
- Thus, assistance from initial FSA data supports the accuracy of the functional hazard analysis by identifying which functional hazards are truly system and mission level hazards to the public.

* Rev A updated this section - In release process

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1*, Section 7.3: “Primary Outputs (Key Data) of the Functional Hazard Analysis”

- In accordance with § 450.107(b), the functional hazard analysis documents the determination of a hazard control strategy for each phase of flight during a launch or reentry [Ref. Section 7.1.3], accounting for:

  1) Identification of all functional failures associated with reasonably foreseeable hazardous events that have the capability to create a hazard to the public [Ref. Section 7.1.3]

  2) Identification of safety-critical systems (see Section 7.1.3 of this AC), by identifying each system carrying an assessed “end effect” resulting from each mechanism of each function during each phase, excluding mitigation, posing a potential system or mission hazard to the public [Ref. Section 7.1.3]

  3) Timeline of safety-critical events [Ref. Paragraph 7.1.3(e)]

* Rev A updated this section - In release process

Part 450 “Safety-Critical”

Traditional System Safety Approach to Part 450 “Safety-Critical”

Per § 401.7

> *“Safety critical* means essential to safe performance or operation. A safety-critical system, subsystem, component, condition, event, operation, process, or item, is one whose proper recognition, control, performance, or tolerance, is essential to ensuring public safety and the safety of property.”

Part 450 Preamble, Section 4, y, 5th Paragraph

> If the failure of a system can create a hazard to the public*, then the system is a safety-critical system.

MIL-STD-882E “Department Of Defense Standard Practice - System Safety”

> “*Safety-critical item (SCI).* A hardware or software item that has been determined through analysis to potentially contribute to a hazard with Catastrophic or Critical mishap potential, or that may be implemented to mitigate a hazard with Catastrophic or Critical mishap potential.”
>
> **[Traditional System Safety Approach]**

*Includes waterborne vessels and air traffic

Part 450 “Safety-Critical”

Traditional System Safety Approach to Part 450 “Safety-Critical”

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 identify “public safety-critical systems” and guide application and rigor of Part 450 “safety-critical” requirements ***

§ 450.107 "Hazard Control Strategies"

System Safety Template for § 450.107 Functional Hazard Analysis

Top-Level System [TBD]	Next-Level System	Subsystem	Component	Function	Implementation	Function ID	Phase of Flight[1]	Mechanism	Assessed End Effect	Functional Hazard ID[2] or NSI[3]	Severity[4]	FSA[5] Failure Mode[6]	Failure Response Mode[7]	Potential Hazard to Public[8]	Hazard Control Strategy[9]	Verification Evidence & Data[10]	CSSI Degree of Control[11]	CSSI Level of Criticality[11]
	Launch Vehicle Stage 1 [LVS1]	Avionics System (AVI)	Computer [COMP]	Function 1	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-AVI-COMP-001	Launch	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
							Ascent	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
							Abort	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
							Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
				Function 2; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-AVI-COMP-002; and so on…	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
			Battery [BATT]; and so on…	Function 1	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-AVI-BATT-001	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
				Function 2; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-AVI-BATT-002; and so on…	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
		Propulsion System [PROP];	Engine(s) [ENG]; and so on…	Function(s) TBD; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-PROP-ENG-001; and so on…	Launch; Flight; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
		Control System [CONT];	Reaction Control System [RCS]; and so on…	Function(s) TBD; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-CONT-RCS-001; and so on…	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
		Flight Safety System [FSS]; and so on…	Safe & Arm [S&A]; and so on…	Function(s) TBD; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS1-FSS-S&A-001; and so on…	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
	Launch Vehicle Stage 2 [LVS2]	Avionics System; Propulsion System; Control System; FSS; and so on…	Component(s) TBD; and so on…	Function(s) TBD; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	LVS2-TBD-TBD-001; and so on…	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
	Spacecraft/ Payload [S/P]; and so on…	Avionics System; Propulsion System; Control System; and so on…	Component(s) TBD; and so on…	Function(s) TBD; and so on…	Hardware (HW); Software (SW); Firmware (FW); Discrete Logic (DL)	S/P-TBD-TBD-001; and so on…	Launch; Ascent; Abort; Reentry; Landing	Functions properly	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Failure to function	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions early / late	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions out of sequence / time	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Functions inadvertently	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
								Degraded function or malfunction	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD

Determination and Validation of Hazard Control Strategies:

- ❑ Understand the system and operation
- ❑ Document a Functional HA
- ❑ Integrate with FSA data to ensure accuracy and adequacy
- ❑ Identify the hazard control strategy for each phase of flight
- ❑ Validate the adequacy of the determined hazard control strategy

NOTE: Continuous, iterative process

Disclaimer

The material in this document is advisory in nature and does not constitute a regulation. This template 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 template document (as distinct from existing statutes and regulations) is voluntary only, and nonconformity will not affect rights and obligations under existing statutes and regulations. Draft document pending clearance pursuant to 49 CFR part 5.

Adobe Acrobat Document

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1, Section 9.0 “Hazard Control Strategy Validation”

- In accordance with § 450.107(a), the safety criteria of 450.101(a), (b), and (c) must be met by using hazard control strategies. In accordance with § 450.107(c), if an operator cannot adequately mitigate the public safety hazards to meet the public risk criteria of § 450.101(a), (b), and (c) using physical containment, wind weighting, or flight abort, then the operator must conduct a flight hazard analysis in accordance with § 450.109.
  1) The hazard control strategy should mitigate system safety hazards to the public such that the likelihood of any hazardous condition that may cause death or serious injury to the public is extremely remote*;
  2) Hazards and hazard control strategies are characterized with fidelity commensurate with the flight safety analysis, per § 450.115(b), such that they are valid for use in debris data development (§ 450.121) and malfunction trajectory analysis (§ 450.119), and are consistent with the probability of failure analysis (§ 450.131); and
  3) The flight safety analysis incorporating the hazard control strategy satisfies the safety criteria of § 450.101(a), (b), and (c).
- If an operator using the means of compliance in this AC is unable to demonstrate the three criteria above as applied to physical containment, wind weighting, or flight abort, then the operator would need to perform a flight hazard analysis or utilize another means of compliance to demonstrate the hazard control strategy adequately mitigates the hazard.

* At the System and Mission Level

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1, Section 9.1 “Adequacy of Determined Hazard Control Strategy"

Compliance data from the following items will support the validation of adequacy:

- ❑ Flight Safety Analysis - Assistance from the initial FSA is important for identifying system and mission hazards to the public. Additionally, FSA data assists in understanding the effectiveness of mitigations. Thus, the final FSA should inform the validation of any hazard control strategy for a phase of flight.
- ❑ Flight Hazard Analysis - Documenting compliance to § 450.109 for a flight hazard analysis produces data that should inform the validation of a flight hazard analysis strategy for each phase of flight in which it is used. Reference AC 450.109-1 for further guidance on flight hazard analyses.
- ❑ Computing Systems - Documenting compliance to § 450.141 for computing systems produces data that should inform the validation of a flight abort and flight hazard analysis strategy for each phase of flight in which it is used. Reference AC 450.141-1 for further guidance on computing systems and software safety.
- ❑ Safety-Critical Systems Design, Test, and Documentation - Documenting compliance to § 450.143 for safety-critical systems produces data that should inform the validation of a flight abort and flight hazard analysis strategy for each phase of flight in which it is used. Reference AC 450.143-1 for further guidance on safety-critical systems DT&D.

§ 450.107 “Hazard Control Strategies”

Ref. AC 450.107-1, Section 9.1 [CONTINUED]

- Highly Reliable Flight Safety System - Documenting compliance to § 450.145 for a highly reliable FSS produces data that should inform the validation of a flight abort strategy for each phase of flight in which it is used.
- Wind Weighting Safety System DT&D - Documenting compliance to § 450.111 for a wind weighting safety system should produce data that validates the adequacy of a wind weighting strategy for each phase of flight in which it is used.

§ 450.107 “Hazard Control Strategies”

(d) ***Application requirements.*** An applicant must submit in its application—

(1) The results of the hazard control strategy determination, including—

(i) All functional failures identified under paragraph (b)(1) of this section;

(ii) The identification of all safety-critical systems; and

(iii) A timeline of all safety-critical events.

(2) A description of its hazard control strategy or strategies for each phase of flight.

Adobe Acrobat Document

AC 450.107-1*, Appendix A “System Safety Template for § 450.107 Functional Hazard Analysis”

* Revision A in release process

Summary of § 450.107 Discussion

Summary of Key Topics

- ❑ Determination of Hazard Control Strategies from § 450.108 through § 450.111
- ❑ Conducting a § 450.107 Functional Hazard Analysis accounting for
  1) All functional failures associated with reasonably foreseeable hazardous events that have the capability to create a hazard to the public;
  2) Safety-critical systems; and
  3) A timeline of all safety-critical events.
- ❑ Conducting a § 450.109 Flight Hazard Analysis, if required by § 450.107(c)
- ❑ Adequacy and Validation of determined hazard control strategy

SYSTEM SAFETY WORKSHOP

Thank you for joining us.

FAA
Commercial Space Transportation
faa.gov/space