FAA
Commercial Space Transportation
faa.gov/space

SYSTEM SAFETY WORKSHOP

Presented by
Christopher Vance & Joe Leal
System Safety Branch [ASA-220]

Tuesday, May 9, 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.

Evolution of FAA AST System Safety

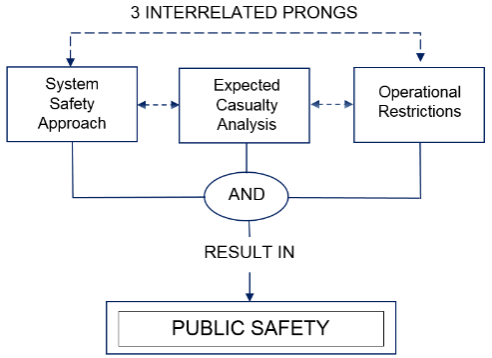
System Safety via Prescriptive Regulations

Part 415/417: Launch License/Safety
§ 415.33/417.103 – Safety Organization
§ 415.115/417.107 – Flight Safety
§ 415.117/417.109 – Ground Safety
§ 415.123/417.123 – Computing Systems and Software
§ 415.127 – Flight Safety System Design & Operation Data
§ 417.309 – Flight Safety System Analysis

Part 431: Launch and Reentry of a Reusable Launch Vehicle (RLV)
Part 435: Reentry of a Reentry Vehicle other than a RLV
§ 431.33 – Safety Organization
§ 431.35(c) & (d) – System Safety Process and Analysis
§ 435.33 – Safety Review Requirements and Procedures

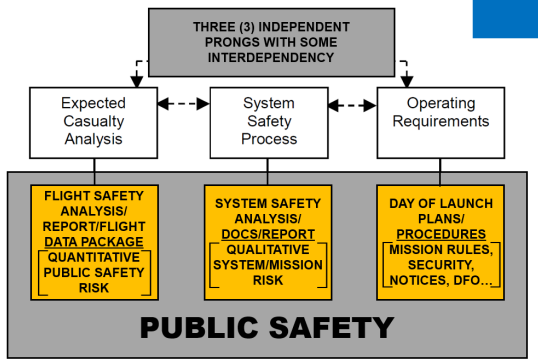
Part 437: Experimental Permits
§ 437.55 – Hazard Analysis

2019 System Safety Tiger Team
"Assessment of AST's Current Practices for System Safety-Related Evaluations"



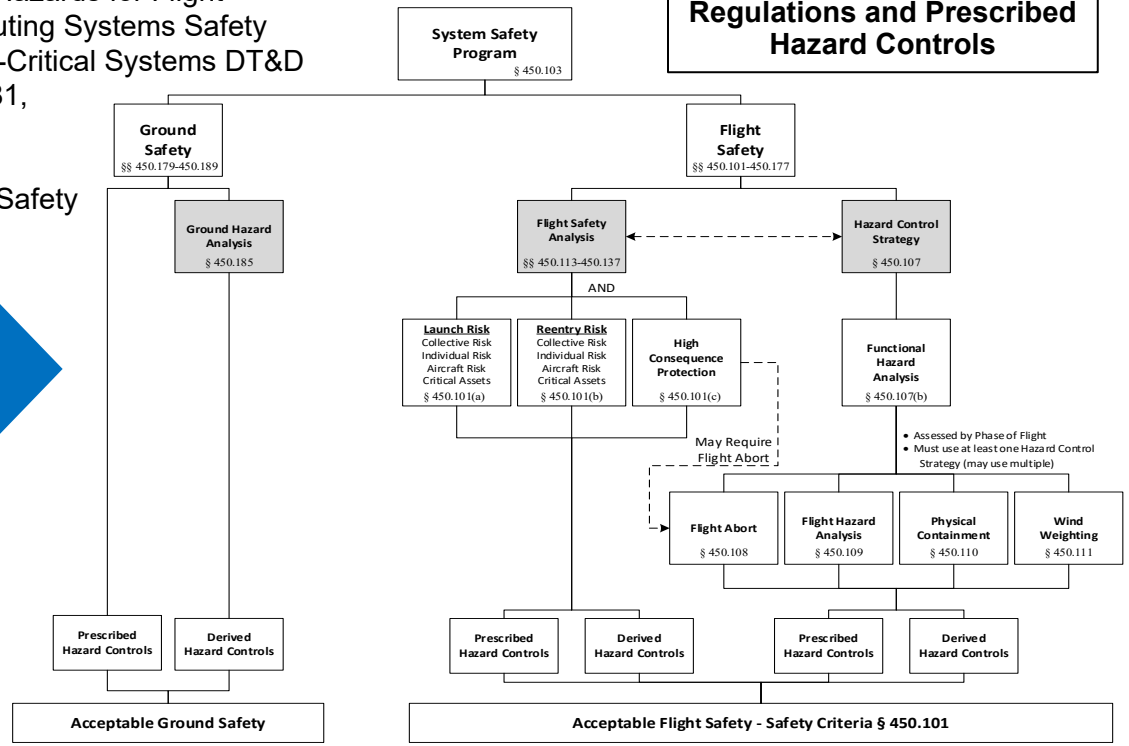
*Includes waterborne vessels and air traffic

System Safety via Process-Based Regulations



Part 450: Streamlined Launch and Reentry License Requirements
§ 450.103 – System Safety Program
§ 450.107 – Functional Hazard Analysis Hazard Control Strategy Determination and Validation of Adequacy
§ 450.109 – Flight Hazard Analysis
§ 450.139 – Toxic Hazards for Flight
§ 450.141 – Computing Systems Safety
§ 450.143 – Safety-Critical Systems DT&D
§§ 450.179, 450.181, 450.183, 450.185, 450.187, and 450.189 – Ground Safety

System Safety Centric with Performance-Based Regulations and Prescribed Hazard Controls



Public* Safety is central focus of AST System Safety

Advisory Circulars (ACs) and Workshops

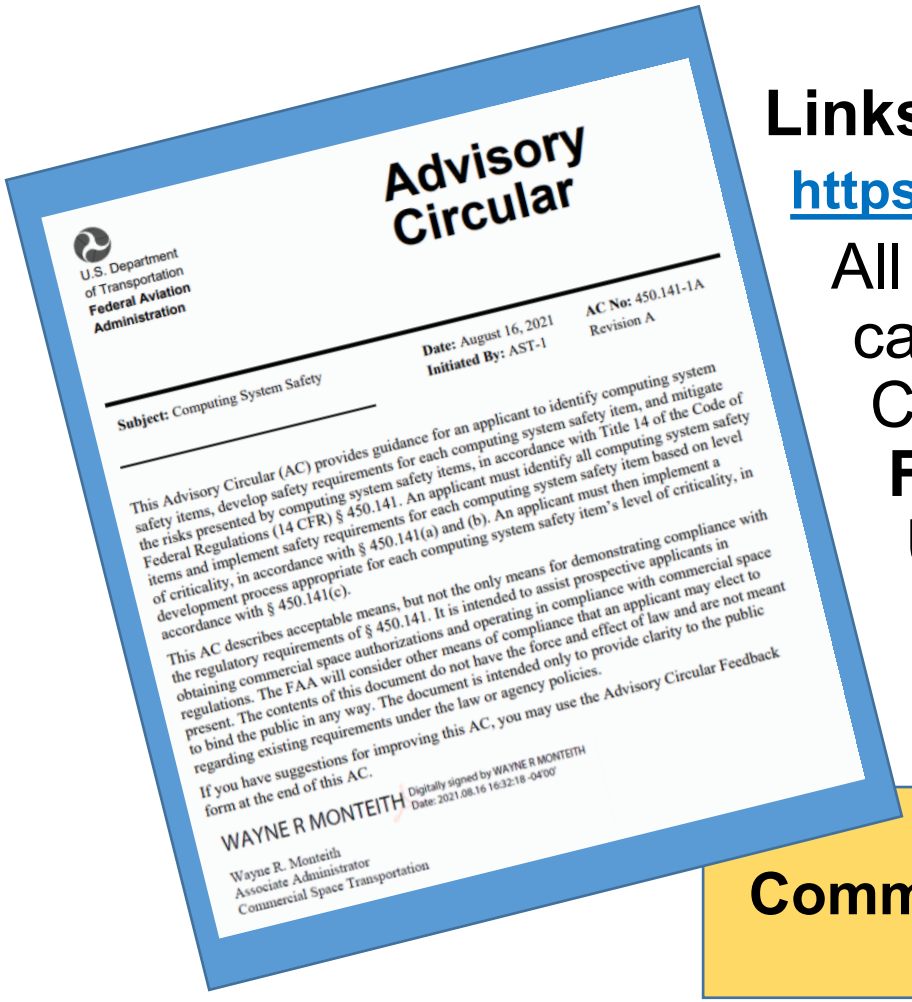
Primary Advisory Circulars & Workshops

All published Advisory Circulars & Workshop links
can be found on our website
FAA.gov/Space
Under **Legislation & Policies, Regulations & Guidance** on the
Commercial Space Advisory Circulars (AC) page

Background on Advisory Circulars

- Advisory Circulars (ACs) provide guidance on AST's streamlined commercial space regulations.
- The goals of the ACs are to:
  - Further explain the meaning of the regulatory text and its intent
  - Provide **a** means of compliance
- The ACs are guidance, not a regulation, and so compliance is voluntary.
- To demonstrate compliance using a means of compliance found in an AC, the entire AC must be implemented. This means that the FAA must approve any variance from a "should" statement in the AC.

Find ACs on the FAA Website



Advisory Circular

U.S. Department of Transportation
Federal Aviation Administration

Subject: Computing System Safety

Date: August 16, 2021 **AC No:** 450.141-1A
Initiated By: AST-1 Revision A

This Advisory Circular (AC) provides guidance for an applicant to identify computing system safety items, develop safety requirements for each computing system safety item, and mitigate the risks presented by computing system safety items, in accordance with Title 14 of the Code of Federal Regulations (14 CFR) § 450.141. An applicant must identify all computing system safety items and implement safety requirements for each computing system safety item based on level of criticality, in accordance with § 450.141(a) and (b). An applicant must then implement a development process appropriate for each computing system safety item's level of criticality, in accordance with § 450.141(c).

This AC describes acceptable means, but not the only means for demonstrating compliance with the regulatory requirements of § 450.141. It is intended to assist prospective applicants in obtaining commercial space authorizations and operating in compliance with commercial space regulations. The FAA will consider other means of compliance that an applicant may elect to present. 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: 2021.08.16 16:32:18 -04'00'

Wayne R. Monteith
Associate Administrator
Commercial Space Transportation

Links to ACs (search: 450)

https://www.faa.gov/regulations_policies/advisory_circulars/

All published Advisory Circulars & Workshop links can be found on the Commercial Space Transportation website **FAA.gov/Space**

Under **Legislation & Policies, Regulations & Guidance** on the **Commercial Space Advisory Circulars (AC)** page

Comments and questions are considered in future revisions

FAA AST System Safety

Discussion

Floor open for questions/comments

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”

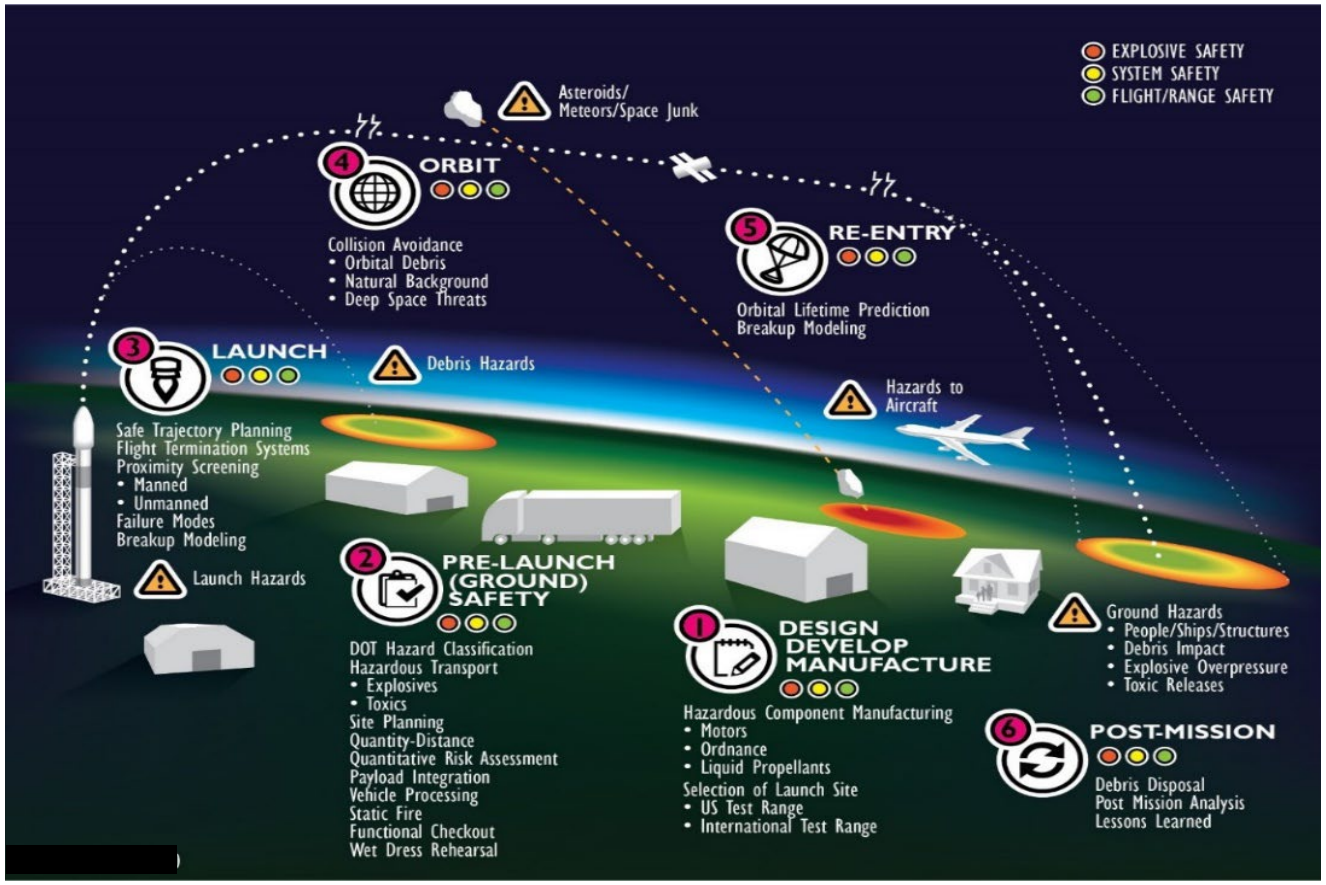
* AC as not been published yet and this information is currently in draft form only. Information may change upon publication of AC.

§ 450.103 "System Safety Program"

An operator must implement and document a system safety program throughout the lifecycle of a launch or reentry system that includes:

(a) Safety Organization;
(b) Hazard Management;
(c) Configuration Management and Control; and
(d) Post-Flight Data Review

An effective system safety process should be incorporated throughout the lifecycle of the program as public safety hazards associated with systems and operations of a launch or reentry vehicle are generally reliant on sound design, manufacturing, and operational processes and procedures that span the lifecycle.



Generic Lifecycle of a Launch or Reentry System

§ 450.103 “System Safety Program”

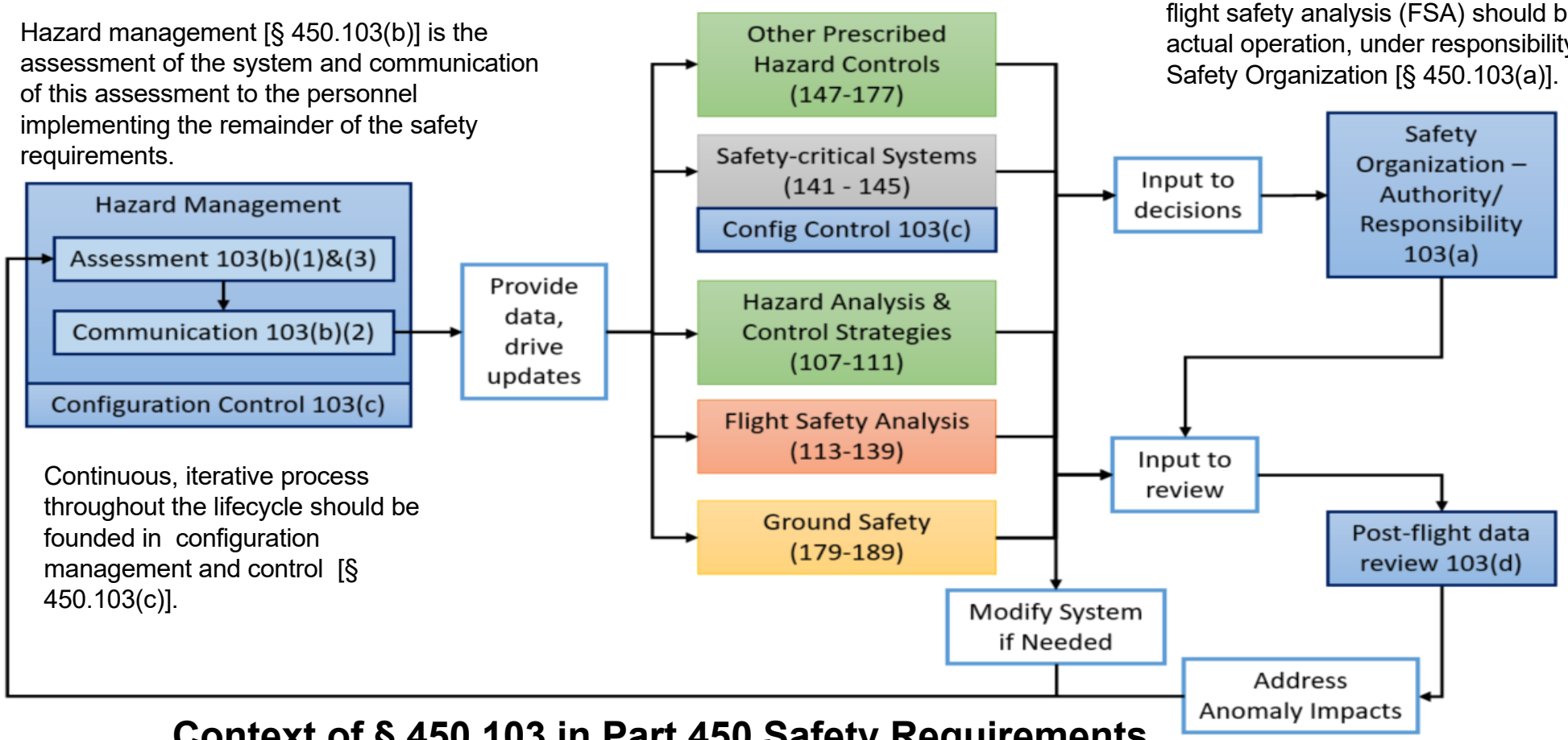
Ref. AC 450.103-1, Section 6.2 “Context for System Safety Program”

- The scope of system safety incorporates all elements of the program that contribute to achieving compliant operations.
- Section 450.103 specifically deals with the organizational structures and management processes and principles relied on for ensuring that hazard controls and analyses z correspond to the actual system operations.
- SSP documents the core processes that ensure that the fundamental risk requirements in § 450.101 and system safety risk criteria of §§ 450.109(b)(3) and 450.185(c) are met over the lifecycle of the system.

§ 450.103 "System Safety Program"

Ref. AC 450.103-1, Section 6.2

Hazard management [§ 450.103(b)] is the assessment of the system and communication of this assessment to the personnel implementing the remainder of the safety requirements.



Continuous, iterative process throughout the lifecycle should be founded in configuration management and control [§ 450.103(c)].

The outcomes of the functional hazard analysis, hazard control strategy determination, flight hazard analysis, and flight safety analysis (FSA) should be implemented in the actual operation, under responsibility and authority of the Safety Organization [§ 450.103(a)].

Post-flight data review [§ 450.103(d)] after each operation allows for determining and implementing necessary updates to the hazard management approach and processes before future operations.

Context of § 450.103 in Part 450 Safety Requirements

§ 450.103 “System Safety Program”

(a) *Safety organization.* An operator must maintain a safety organization that has clearly defined lines of communication and approval authority for all public safety decisions. At a minimum, the safety organization must have the following positions:

1) *Mission director*. For each launch or reentry, an operator must designate a position responsible for the safe conduct of all licensed activities and authorized to provide final approval to proceed with licensed activities. This position is referred to as the mission director in this part.

2) *Safety official*. For each launch or reentry, an operator must designate a position with direct access to the mission director who is—

   i. Responsible for communicating potential safety and noncompliance issues to the mission director; and

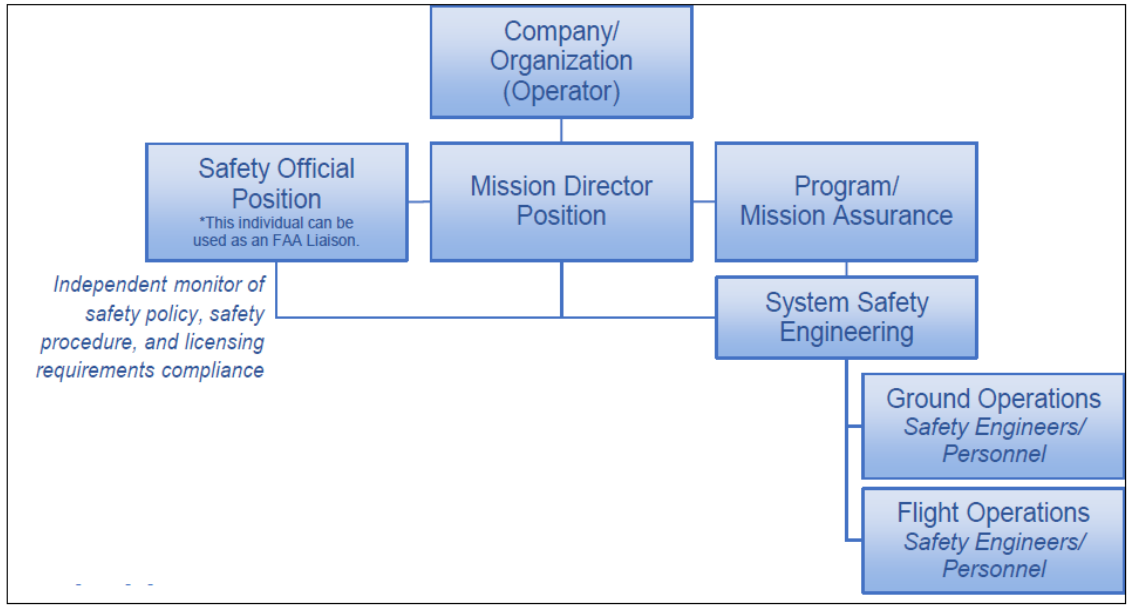
   ii. Authorized to examine all aspects of the operator’s ground and flight safety operations, and to independently monitor compliance with the operator’s safety policies, safety procedures, and licensing requirements.

3) *Addressing safety official concerns*. The mission director must ensure that all of the safety official’s concerns are addressed.

§ 450.103 "System Safety Program"

Ref. AC 450.103-1, Section 7.0 "Safety Organization."

- The establishment of a safety organization* is a critical component of launch and mission operations and public safety, whose primary responsibility is to carry out the processes needed to protect public safety, as identified in the documented SSP.
- As defined in § 401.7, mishap includes a failure of the safety organization.
- The safety organization must have clearly defined lines of communication and an approval authority for all public safety decisions associated with a licensed operation or mission, per § 450.103(a).
- The FAA encourages the development of an organizational chart that depicts the safety organization in the context of the larger organization.



Sample Safety Organization of § 450.103(a)

* Generally, distinct from the system safety organization

§ 450.103 “System Safety Program”

(b) *Hazard management.* For hazard management:

1) An operator must implement methods to assess the system to ensure the validity of the hazard control strategy determination and any flight hazard or flight safety analysis throughout the lifecycle of the launch or reentry system;

2) An operator must implement methods for communicating and implementing any updates throughout the organization; and

3) Additionally, an operator required to conduct a flight hazard analysis must implement a process for tracking hazards, risks, mitigation measures, and verification activities.

Ref AC 450.103, Section 8.1.1 “Functional Hazard Analysis”

- ❑ Must be performed for all Part 450 license applications, in accordance with 450.107(b)
- ❑ Provides a means for methodical determination and continual validation of the hazard control strategy, the flight safety analysis, and the flight hazard analysis, for each phase of flight during a launch or reentry operation.
- ❑ Should provide traceability between each functional source to the associated system and mission hazard during each phase of flight to the respective hazard control strategy to the verification evidence necessary for validation.

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 8.1.2 “Reasonably Foreseeable”

"Reasonably foreseeable" is not associated with a probability or likelihood, but is inherent to a methodical assessment of the entire system.

- Expected that "reasonably foreseeable hazardous events" are those identifiable through the system safety process, beyond those that could be determined solely by “brainstorming”.
- Functional hazard analysis is the system safety analysis tool primarily used to identify, classify, and analyze system functions and consequences of functional hazards associated with the conceptualized operation (mission).
- The objective is to identify all pertinent potential system, subsystem, and component functional hazards that could impact public safety.
- It is important to note that the identification of potential system safety hazards and respective functional sources should not consider any foreseeable mitigation, redundancy, or predetermined hazard control strategy.

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 8.1.3 “Flight Hazard Analysis”

- ❑ The system safety approach of an flight hazard analysis may be determined as a hazard control strategy per § 450.107(a), or required, per § 450.107(c).
- ❑ The documented SSP should:
  - Define the methodology and the process for ensuring continued validity, in accordance with §§ 450.103(b)(1) and 450.109, and
  - Define a process for tracking hazards, risks, mitigation measures, and verification activities, in accordance with § 450.103 (b)(3) and the guidance of AC 450.109-1, *Flight Hazard Analysis*.

Ref. AC 450.103-1, Section 8.1.4 “Flight Safety Analysis”

- ❑ A flight safety analysis must be performed and documented in accordance with §§ 450.113 through 450.139.
- ❑ The documented SSP should ensure the validity of this analysis, with appropriate methodology in place to achieve these requirements.

§ 450.103 “System Safety Program”

(b) ***Hazard management.*** For hazard management:

1) An operator must implement methods to assess the system to ensure the validity of the hazard control strategy determination and any flight hazard or flight safety analysis throughout the lifecycle of the launch or reentry system;

2) An operator must implement methods for communicating and implementing any updates throughout the organization; and

3) Additionally, an operator required to conduct a flight hazard analysis must implement a process for tracking hazards, risks, mitigation measures, and verification activities.

§ 450.103 “System Safety Program”

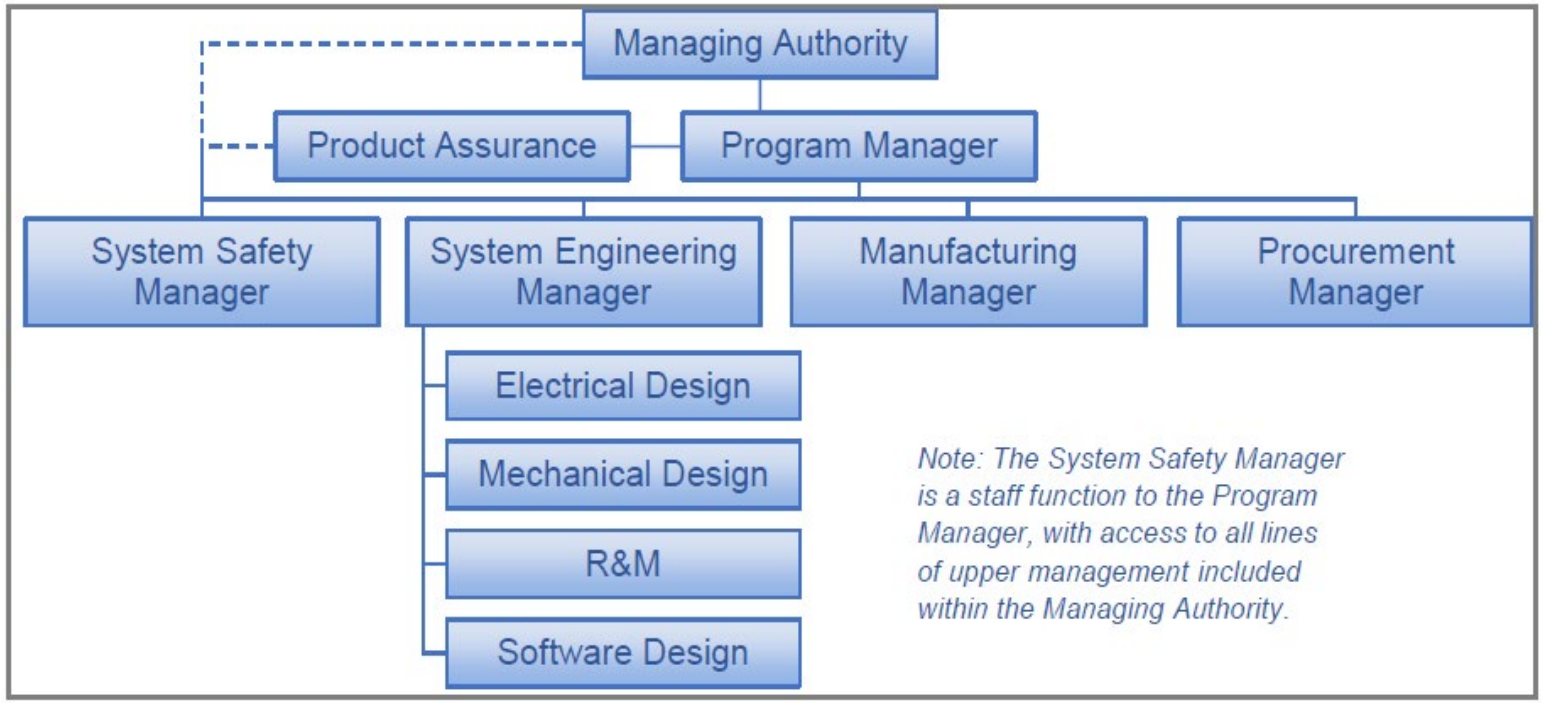
Ref. AC 450.103-1, Section 8.2 “Managing Updates”

- In accordance with § 450.103(b)(2), the system safety organization ensures communication and implementation of any updates throughout the organization.
- The documented SSP should define the tools and processes utilized by the system safety organization to ensure that safety analysis data is effectively communicated, required actions and necessary updates are efficiently implemented, and safety information is thoroughly organized and maintained.
- The system safety organization should be described in sufficient detail to clearly show how each of the divisions and roles within the larger organization will work to accomplish the goals of the SSP.
- For the system safety organization, the documented SSP should, at a minimum, detail established communication lines to management and engineering for informing of impacts to risks to the public and necessary implementation actions to address the impacts.

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 8.2.1 “Organizational Structure”

- Organizational charts or diagrams should be utilized to identify the system safety organization and illustrate functional relationships and lines of communication within the program.



Sample System Safety Organization

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 8.2.2 “Integration”

The documented SSP should provide clarity about how the different parts of the organization interface with the system safety organization and each other, and should:

- Define the interfaces with functional organizations and other involved disciplines, to include:
  - Program management, systems engineering, design engineering (system, subsystems, interfaces), test engineering, software engineering, system operations development, ground operations development, reliability engineering, human system integration, logistics and sustainment engineering, quality engineering, subcontractor management, and others, as applicable.
- Define interfaces with other applicable safety disciplines, such as software system safety, range safety, nuclear safety, explosive and ordnance safety, chemical and biological safety, occupational safety and health, laser safety, etc.
- Define the procedures for integrating and coordinating the system safety effort, including: definition of system safety requirements within design specifications and operations documents; dissemination of system safety requirements to relevant organizations and contractors; support to program and design reviews and trade studies; support to engineering and software change reviews; status reporting of system safety efforts; and institution of system safety groups.

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 8.2.2 “Integration” [Continued]

- Define expected criteria for interaction with CM processes, software development processes, data management processes, system and design engineering processes, etc. The interfaces and criteria should include requirements, data exchange, and communications.
- Describe tools used to convey system safety information, such as hazard tracking systems or internal workflow systems.

Ref. AC 450.103-1, Section 8.2.3 “Oversight”

An effective plan also includes oversight and tracking, so the documented SSP should:

- Define the management of contractor’s and subcontractor’s system safety efforts that have been procured, to include integration of contractor system safety analyses and data.
- Identify when formal approval action of safety documentation is required, by whom, and how that approval is documented.
- Define the process by which management decisions will be made, including timely notification of unacceptable risks, necessary action, mishaps, anomalies, waivers to system safety requirements, and program deviations.

§ 450.103 “System Safety Program”

(b) *Hazard management.* For hazard management:

1) An operator must implement methods to assess the system to ensure the validity of the hazard control strategy determination and any flight hazard or flight safety analysis throughout the lifecycle of the launch or reentry system;
2) An operator must implement methods for communicating and implementing any updates throughout the organization; and
3) Additionally, an operator required to conduct a flight hazard analysis must implement a process for tracking hazards, risks, mitigation measures, and verification activities.

Ref. AC 450.103-1, Section 8.3 “Tracking of Flight Hazard Analysis Data”

- ❑ Data tracking is essential for a sound and continually valid flight hazard analysis.
- ❑ The documented SSP should define the process and mechanism for identifying, detailing, tracking, collecting, analyzing, and retaining the flight hazard analysis data. Examples of mechanisms are: hazard reports, a hazard database, systems engineering management tools, etc.
- ❑ As discussed in AC 450.109-1, *Flight Hazard Analysis*, traceability methods should be established for all relevant system safety requirements and analysis data.
  [Further discussion to follow]

§ 450.103 “System Safety Program”

(c) ***Configuration management and control.*** An operator must—

1) Employ a process that tracks configurations of all safety-critical systems* and documentation related to the operation;
2) Ensure the use of correct and appropriate versions of systems and documentation tracked in paragraph (c)(1) of this section; and
3) Document the configurations and versions identified in paragraph (c)(2) of this section for each licensed activity.

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

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 9.0: “Configuration Management and Control”

- ❑ The documented SSP should define the configuration management and control (CM&C) process specific for all safety critical systems* and documentation
- ❑ Standards for CM&C can be found in MIL–HDBK–61.
- ❑ The CM&C processes defined in the documented SSP should include lifecycle change, modification, and redesign activity.
  - As the functional hazard analysis may evolve throughout the lifecycle, the CM&C processes should apply not just to known safety-critical systems*, but also track system changes for potential implications in regards to public safety.

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

§ 450.103 “System Safety Program”

(d) ***Post-flight data review.*** An operator must employ a process for evaluating post-flight data to:

1) Ensure consistency between the assumptions used for the hazard control strategy determination, any flight hazard or flight safety analyses, and associated mitigation and hazard control measures;
2) Resolve any inconsistencies identified in paragraph (d)(1) of this section prior to the next flight of the vehicle;
3) Identify any anomaly that may impact any flight hazard analysis, flight safety analysis, or safety-critical system, or is otherwise material to public safety; and
4) Address any anomaly identified in paragraph (d)(3) of this section prior to the next flight as necessary to ensure public safety, including updates to any flight hazard analysis, flight safety analysis, or safety-critical system.

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 10.0 “Post-Flight Data Review”

Review of post-flight data provides valuable safety information on future operations. The documented SSP should define the process for post-flight data review in sufficient detail to allow the FAA to evaluate and audit the process for compliance.

Data Collection

- ❑ Post-flight data should be formally collected, reviewed, and recorded. The data should be utilized to identify trends, in the context of previous flights, and gauge effectiveness of corrective actions.

Analysis Consistency

- ❑ If the flight data indicates an incorrect assumption, the hazard management approach should be reassessed for any necessary modifications, and the inconsistency must be resolved prior to the next flight of the vehicle, in accordance with § 450.103(d)(2).
- ❑ To ensure there is no increased likelihood of system safety hazards to the public, additional mitigation measures may be required. The updated analyses should be used for future flights of the system.

§ 450.103 “System Safety Program”

(d) *Post-flight data review.* An operator must employ a process for evaluating post-flight data to:

1) Ensure consistency between the assumptions used for the hazard control strategy determination, any flight hazard or flight safety analyses, and associated mitigation and hazard control measures;

2) Resolve any inconsistencies identified in paragraph (d)(1) of this section prior to the next flight of the vehicle;

3) Identify any anomaly that may impact any flight hazard analysis, flight safety analysis, or safety-critical system*, or is otherwise material to public safety; and

4) Address any anomaly identified in paragraph (d)(3) of this section prior to the next flight as necessary to ensure public safety, including updates to any flight hazard analysis, flight safety analysis, or safety-critical system*.

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

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 10.3 “Anomaly Reporting and Investigation”

- ❑ Anomaly reporting and investigation is essential for ensuring continually valid system assessment.
- ❑ The documented SSP should define system safety involvement in the anomaly reporting, investigation, and resolution process.
- ❑ The resolution process should be outlined for updating analyses and risks to address the anomaly, including any additional required mitigations, as well as for the periodic review of these analyses and risks (i.e., before flight, after flight).
- ❑ The FAA notes that, if an anomaly constitutes a mishap, as defined in § 401.7, additional requirements apply, per § 450.173 (see also AC 450.173-1, *Mishap Reporting, Response, and Investigation*).

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

§ 450.103 “System Safety Program”

Ref. AC 450.103-1, Section 10.3 “Reporting to FAA”

- In accordance with § 450.215, a licensee must submit, among other things, information on any anomaly that occurred during countdown or flight that is material to public health and safety and the safety of property, along with any corrective action implemented or to be implemented after the flight due to an anomaly or mishap.
- A summary of the flight anomaly, the closure strategy, and acceptance rationale should be documented and provided to the FAA for review.

§ 450.103 “System Safety Program”

(e) ***Application requirements.*** An applicant must submit in its application the following:

1) A description of the applicant’s safety organization as required by paragraph (a) of this section, identifying the applicant’s lines of communication and approval authority, both internally and externally, for all public safety decisions and the provision of public safety services; and

2) A summary of the processes and products identified in the system safety program requirements in paragraphs (b), (c), and (d) of this section.

Note: Submission could take the form of one comprehensive document or an identified set of documents that together demonstrate compliance with the application requirements of this chapter.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.1 "System Safety Risk Assessment"

- This risk assessment should be utilized for system safety for flight and ground safety, and is generally qualitative; however, there are instances when quantitative demonstration may be possible or necessary.
- For system safety for flight, it is meant to augment the quantitative risk calculated by the flight safety analysis and inform the development and refinement of applicable mitigations.
- An operator must assess each hazard's likelihood and severity, per §§ 450.109(b)(2) and 450.185(b). Therefore, an operator should define severity categories and likelihood levels to ensure that the system safety risk meets the criteria of §§ 450.109(b)(3) and 450.185(c).
- These severity categories and likelihood levels may be informed by industry practice and existing government standards.
- Utilizing a matrix allows for more effective characterization of each system safety risk against acceptance criteria.
- The applicant may consider MIL-STD-882E, *Department of Defense Standard Practice – System Safety*

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.1 "System Safety Risk Assessment"

Severity Categories

DESCRIPTION	CATEGORY	CONSEQUENCE DEFINITION
Catastrophic	I	Could result in one or more of: fatality or serious injury (as defined in 49 C.F.R. § 830.2) to the public or loss of safety-critical system.
Critical	II	Applicant should define consequences in regards to: injury to the public; property damage to the public; safety-critical system damage or reduced capability; reduction in safety margins; or increase in crew workload.
Marginal	III	
Negligible	IV	

Likelihood Levels

DESCRIPTION	LEVEL	LIKELIHOOD CRITERIA
Frequent	A	Likely to occur often in the life of an item, with a likelihood of occurrence greater than 10^{-2} in any one mission.
Probable	B	Will occur several times in the life of an item, with a likelihood of occurrence less than 10^{-2} but greater than 10^{-3} in any one mission.
Occasional	C	Likely to occur sometime in the life of an item, with a likelihood of occurrence less than 10^{-3} but greater than 10^{-5} in any one mission.
Remote	D	Unlikely but possible to occur in the life of an item, with a likelihood of occurrence less than 10^{-5} but greater than 10^{-6} in any one mission.
Extremely Remote	E	So unlikely, it can be assumed occurrence may not be experienced, with a likelihood of occurrence less than 10^{-6} in any one mission.
Eliminated	F	Incapable of occurrence. Potential hazard is identified and later eliminated.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.2 "System Safety Requirements"

- ❑ Identification and implementation of system safety requirements within the systems engineering process ensures the effectiveness and validity of system assessments.
- ❑ The systems engineering process should be outlined for:
  - Safety design requirements for which objectives are to mitigate system hazards through a systematic application of design guidance from standards, specifications, regulations, design handbooks, safety design checklists, and other sources.
  - Safety design requirements should be included in the system specification and expanded for inclusion in the associated lower level specifications.
  - Safety operational requirements should be included in procedures, test, and inspection documentation, applicable rules or commit criteria, operational clear areas, etc.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.3 "Integrated Schedule"

- ❑ The system safety schedule ensures effectiveness of the system assessment throughout the lifecycle of the program.
- ❑ The documented SSP should detail the system safety activities and milestones within the overall program schedule, including product or task start and completion dates, reports, reviews, and safety milestones.
- ❑ Typically, the milestones of the system safety program coincide with the license process, program reviews, and other contract milestones. Thus, the schedule should detail the system engineering activities for which system safety efforts are integrated (e.g., technical reviews, program reviews, design/analysis/test activities, etc.).
- ❑ Updates to the schedule and product deliveries in the plan should occur when license processing, contract, or system design changes are implemented.
- ❑ An operator should identify any interdependencies for the safety tasks and artifacts.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.3.1 "Integration within Program Activities"

- ❑ To be effective, the system safety activities of any program should be integrated into other program activities.
- ❑ To be efficient, each system safety task should be carefully scheduled to have the most positive effect.
  - A system safety analysis performed early in the design process can lead to the inexpensive elimination of a hazard through design changes.
  - The later the hazard is identified in the design cycle, the more expensive and difficult the change. Hazards identified late in the design phase and testing cycles may be impractical to design out.
  - In such cases, hazards may still be controlled through procedural and training steps but having to do so, when they could have been prevented, reflects unnecessary long-term costs and risk.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.4 “Management of Lifecycle Risk”

- ❑ Management of lifecycle risks is essential for ensuring the continued validity of safety analyses.
- ❑ Impacts to risk due to design or operational changes are typically managed by change impact analysis.
  - The impact should be determined for any changes to the design configuration or operation of a safety-critical system*.
  - The current hazard management approach and hazard control strategy should be reassessed with respect to the change, and updated appropriately.
- ❑ Impacts to risk due to reuse of systems, subsystems, or components are typically managed by a reusability approach.

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

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.5 "System Safety Data Handling"

- ❑ Data tracking is essential for sound and continually valid system assessment.
- ❑ The documented SSP should define the process for identifying, detailing, tracking, collecting, analyzing, and retaining system safety data.
- ❑ Examples of this data include test documentation and data, hazard reports, procedures, lessons learned, contractor deliverables, post-flight documentation, anomaly reports, and pertinent historical hazard or mishap data.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.6 "Consideration of Additional System Safety-Related Tasks"

A complete system safety effort should consider and integrate tasks and activities usually performed by other organizations or disciplines, including associate contractors, to ensure sound and continually valid safety analyses.

TASK	DESCRIPTION
Operations & Maintenance	Processes identified by system safety analyses that are required to ensure public safety during ground operations and each flight of the vehicle. These operations and maintenance processes should align with FAA requirements and guidance.
Training	Techniques and procedures to be used for ensuring that the objectives and requirements of the SSP are met in the training of responsible personnel.
Reliability	Reliability predictions and analysis, failure modes and effects analysis, and reliability testing and demonstration. Results of these activities are used to complement and ensure completeness of safety analyses, as well as identify and resolve reliability issues on safety-critical systems.

AC 450.103-1, Appendix A
Key Aspects of a Sound System Safety Plan

Ref. AC 450.103-1, Section A.6 "Consideration of Additional System Safety-Related Tasks"

TASK	DESCRIPTION
Quality Engineering and Assurance	• Calibration • Configuration assurance • Corrective action identification and reporting • Hardware acceptance • Material, nonconformance, and process reviews • Metrology • Production quality performance and evaluation • Quality assurance Program management and engineering • Quality data collection • Software testing and acceptance • Supplier selection, quality surveillance, and audits • System safety acceptance • Test assurance • Vehicle acceptance • Validation and Verification Results of these activities are used to complement and ensure completeness of safety analyses, as well as identify and resolve quality issues with safety-critical systems.

Summary of § 450.103 Discussion

Summary of Key Topics

- ❑ Implement and document System Safety Program throughout the life cycle
- ❑ § 450.103(a) Safety Organization, with Mission Director and Safety Official
- ❑ § 450.103(b) Hazard Management, employing methods for assessment and validation of the determined hazard control strategy and safety analyses, communication and implementation of updates throughout the organization, and process for tracking flight hazard analysis data
- ❑ § 450.103(c) Configuration Management, employing process for tracking, maintaining, and capturing configurations / versions of safety-critical systems and documentations
- ❑ § 450.103(d) Post-flight Data Review, employing process for evaluating post-flight data
- ❑ Key Aspects of a Sound System Safety Plan

§ 450.103 “System Safety Program”

SYSTEM SAFETY WORKSHOP

Thank you for joining us.

FAA
Commercial Space Transportation
faa.gov/space