AST Commercial Space Transportation

FAA AST Workshop: AC 450.103-1

Advisory Circular (AC) for System Safety Program

Christopher Vance
Dr. Erik Larson
13 October 2021

Federal Aviation Administration

Background on Advisory Circulars

Advisory Circulars (ACs) are being used to supplement streamlined regulations by the Federal Aviation Administration (FAA), Commercial Space Transportation (AST).

Their goal is to assist license applicants in two ways:

1. Further explain the meaning of the regulatory text and its intent/goal
2. Provide **a** means of compliance

The ACs are guidance, not a regulation, and compliance is voluntary

To demonstrate compliance using an AC, the entire AC must be implemented. This means all "should" statements must be accomplished if an AC is used.

DISCUSSION IS ENCOURAGED

We have up to two hours today, with incremental periods for Q&A as we step through the chapters of the AC.

NOTE:

Answers by presenters are preliminary; a future revision of the AC is the official response.

Regulation § 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 the following:

(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.

Regulation § 450.103 System Safety Program (Cont.)

(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.

(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.

Regulation § 450.103 System Safety Program (Cont.)

(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.

(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.

AC 450.103-1: System Safety Program

SECTION 1: PURPOSE.

This Advisory Circular (AC) provides guidance to define an acceptable system safety program (SSP) in accordance with Title 14 of the Code of Federal Regulations (14 CFR) § 450.103 System Safety Program.

This AC presents one, but not the only, acceptable means of compliance with the associated regulatory requirements. The FAA will consider other means of compliance that an applicant may elect to present.

SECTION 2: APPLICABILITY.

The guidance in this AC is for launch and reentry vehicle applicants and operators required to comply with 14 CFR part 450.

SECTION 3: APPLICABLE REGULATIONS AND RELATED DOCUMENTS.

SECTION 4: DEFINITIONS OF TERMS.

No new terms. Terms and definitions from § 401.7 apply.

SECTION 5: ACRONYMS.

AC 450.103-1: System Safety Program

SECTION 6.0: SYSTEM SAFETY PROGRAM

- Section 450.103 requires the implementation and documentation of a system safety program (SSP) applicable throughout the lifecycle of a launch or reentry system.
- Documented SSP establishes the methodologies and management principles for flight safety; as such, should define pertinent organizational structures, processes, and safety analysis methodologies.
- Demonstrate that an SSP has been established and documented such that compliance with FAA regulations can be determined and maintained.
- Advisory Circular 450.179-1, *Ground Safety*, provides guidance on ground safety for requirements in §§ 450.179, 450.181, 450.183, 450.185, 450.187, and 450.189.

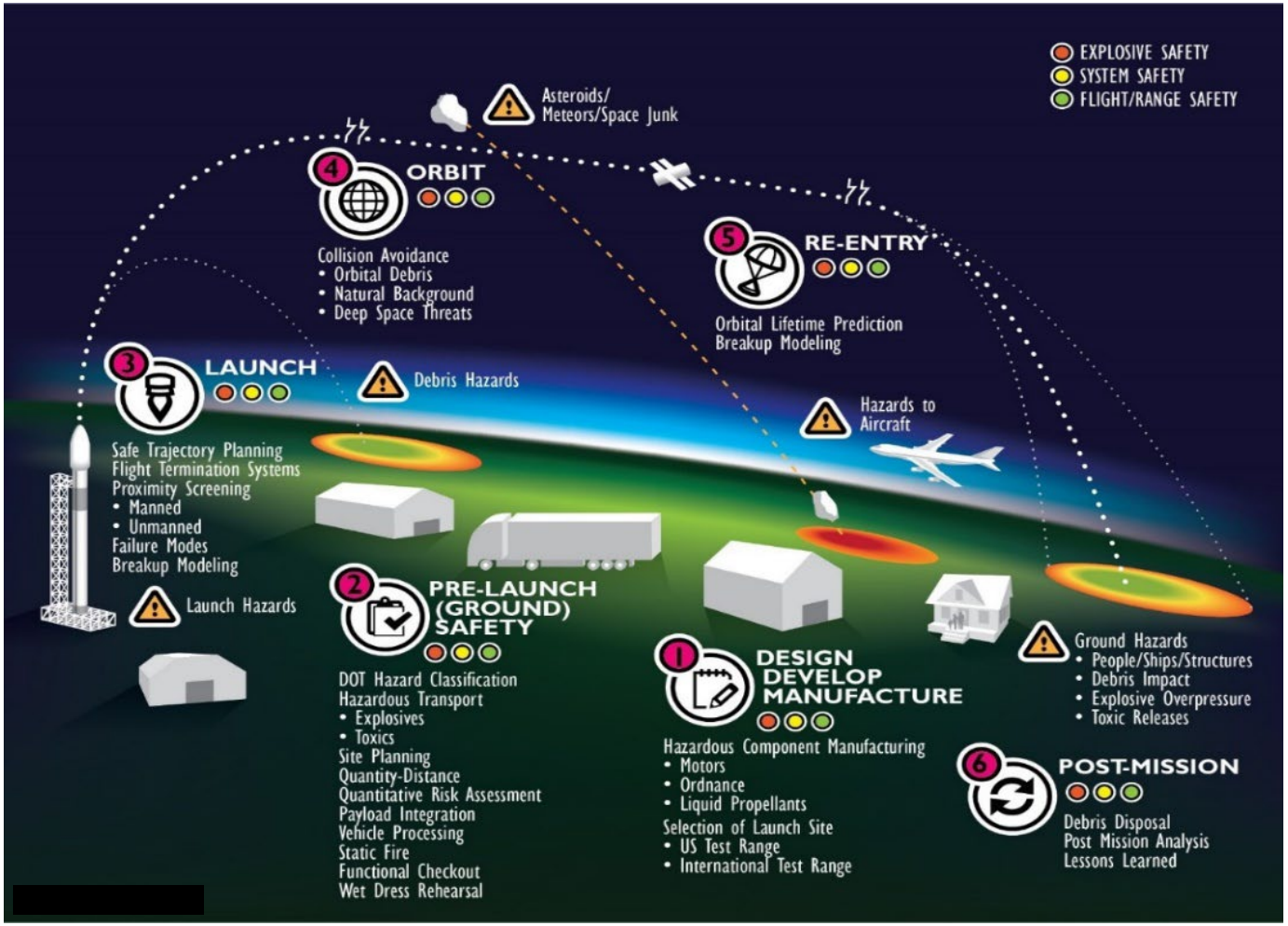
AC 450.103-1: System Safety Program

SECTION 6.0: SYSTEM SAFETY PROGRAM

Section 6.1: Lifecycle System Safety.

- An effective system safety process should be incorporated throughout the lifecycle of the program.
- 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.

AC 450.103-1: System Safety Program



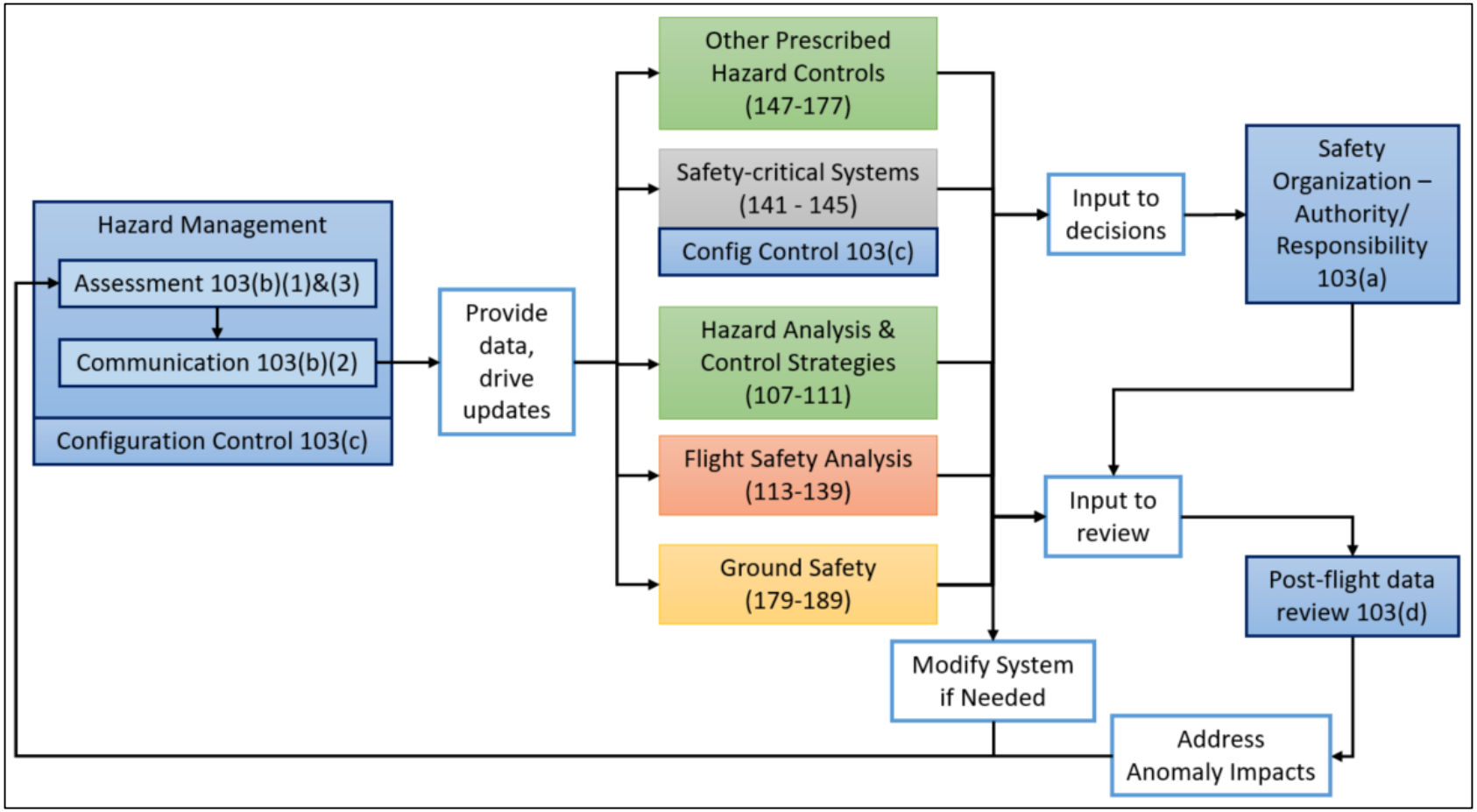
Generic Lifecycle of a Launch or Reentry System

AC 450.103-1: System Safety Program

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 correspond to the actual system operations.
- Thus, these are 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.

AC 450.103-1: System Safety Program



Context of § 450.103 in Part 450 Safety Requirements

AC 450.103-1: System Safety Program

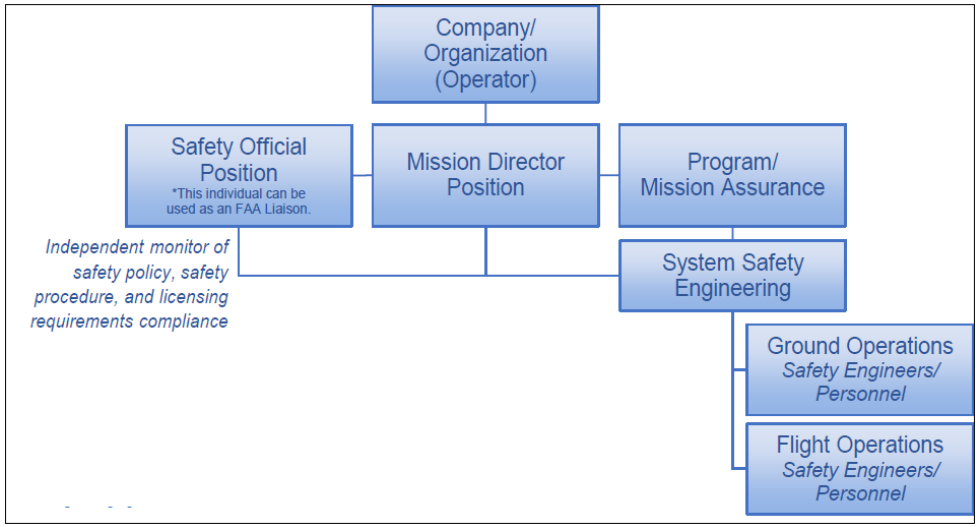
Section 6.2: Context for System Safety Program.

- Hazard management, in § 450.103(b), is the assessment of the system and communication of this assessment to the personnel implementing the remainder of the safety requirements.
- This is a continuous, iterative process throughout the lifecycle; thus, configuration management and control, in § 450.103(c), is a necessary foundation.
- 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, which necessitates clear responsibility and authority, as described in § 450.103(a).
- Finally, each operation provides critical information for improving safety and rectifying errors before future operations, thus post-flight data review is required, per § 450.103(d), from which necessary updates to the hazard management approach and processes should be determined and implemented.

AC 450.103-1: System Safety Program

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, separate of the system safety engineering organization

AC 450.103-1: System Safety Program

SECTION 7.0: SAFETY ORGANIZATION.

Section 7.1: Required Personnel

- At a minimum, two specific positions are required for each launch or reentry: a Mission Director and a Safety Official, in accordance with § 450.103(a)(1) and (2).
- The qualifications for these specific positions should also be documented.
- Lessons learned from previous mishaps have identified the importance of the independence of the Mission Director and Safety Official roles to ensure that the goal of safety is primary. To achieve this independence, these must be different persons, as indicated by § 450.103(a).

7.1.1 Personnel Assignment.

- A Mission Director and Safety Official should be named and in place prior to the initiation of any licensed activity.
- The same persons may be used for multiple launch or reentry sites. However, it may be difficult for a single individual to serve as a Safety Official for multiple sites if launch or reentry activities were to occur close in time to each other. In those instances, multiple persons may be chosen.

AC 450.103-1: System Safety Program

SECTION 7.0: SAFETY ORGANIZATION.

Section 7.1: Required Personnel

- Mission Director
  - Responsible for the safe conduct of all licensed activities and authorized to provide final approval to proceed with licensed activities, in accordance with § 450.103(a)(1).
  - Ensures that all of the Safety Official's concerns are addressed, per § 450.103(a)(3).
- Safety Official
  - Required to have direct access to the Mission Director.
  - Responsible for communicating potential safety and noncompliance issues to the Mission Director, in accordance with § 450.103(a)(2)(i).
  - Authorized to examine all aspects of the ground and flight safety operations, and independently monitor compliance with safety policies, safety procedures, and licensing requirements, in accordance with § 450.103(a)(2)(ii).
  - Responsible to ensure safety issues are identified across the organization and presented to the Mission Director. The Safety Official will be held responsible if a safety issue is not presented to the Mission Director. The Safety Official should ensure that these issues are presented in a timely manner so they can be addressed.

AC 450.103-1: System Safety Program

SECTION 7.0: SAFETY ORGANIZATION.

Section 7.2: Addressing Concerns of the Safety Official.

- In accordance with § 450.103(a)(3), the Mission Director must ensure that all of the Safety Official's concerns are addressed.
- The documented SSP should contain a defined process for communication of the concerns of the Safety Official to the Mission Director and verification that they have been addressed.
- A meeting prior to the commencement of preparations for a licensed activity, such as a Launch Readiness Review, should be held. Minutes of the meeting should be kept, to include, at a minimum, the attendees and any safety issues that are discussed.
- During the operation countdown, the Safety Official should have a designated step to declare "Go" or "No-Go" to the Mission Director, and this declaration should be recorded and/or have witnesses.
- Additional specific requirements for communications during the countdown and flight are listed in § 450.157.

AC 450.103-1: System Safety Program

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.1: System Assessment Methods.

- In accordance with § 450.103(b)(1), methods must be implemented to assess the system to ensure the validity of the hazard control strategy determination and any flight hazard or FSA throughout the lifecycle of the launch or reentry system.
- As such, the documented SSP should establish the process by which:
  - Public safety hazards are systematically identified, defined, and mitigated with verification; and
  - Hazard control strategies and safety analyses are validated and managed to ensure continual validity throughout the lifecycle of a launch or reentry system.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.1: System Assessment Methods.

8.1.1 Functional Hazard Analysis. (Per § 450.107)

- Must be performed for all Part 450 license applications
- Informs and ensures the validity of the hazard control strategy determination, the Flight Safety Analysis, and the Flight HA, by accounting for all functional failures associated with reasonably foreseeable hazardous events that have the capability to create a hazard to the public.
- Provides a means for methodical and continual validation of the hazard control strategy for each phase of flight during a launch or reentry.
- Should provide traceability between each functional failure and associated hazards during each phase of flight to respective hazard control strategies that should mitigate the hazard at the system and mission level to the associated verification evidence for the hazard control strategy for each phase of flight.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.1: System Assessment Methods.

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”.
- A system safety analysis tool primarily used to identify, classify, and analyze system functions and consequences of functional failure or malfunction associated with the proposed operation (mission).
- The objective is to identify all pertinent potential system, subsystem, and component functional failures that could impact public safety.
- It is important to note that the identification of potential system safety hazards and respective functional sources (i.e. subsystem functional failures) should not consider any foreseeable mitigation or predetermined hazard control strategy.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.1: System Assessment Methods.

8.1.3 Flight Hazard Analysis.

- The system safety approach of an Flight HA may be determined as a hazard control strategy per § 450.107(a), or required, per § 450.107(c). If used, 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). The operator may also elect to use the guidance of AC 450.109-1, *Flight Hazard Analysis*.

8.1.4 Flight Safety Analysis.

- An FSA 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.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.2: Managing Updates.

- The documented SSP should define the tools and processes used 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.
- In accordance with § 450.103(b)(2), the system safety organization (SSO) ensures communication and implementation of any updates throughout the organization.
- 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.

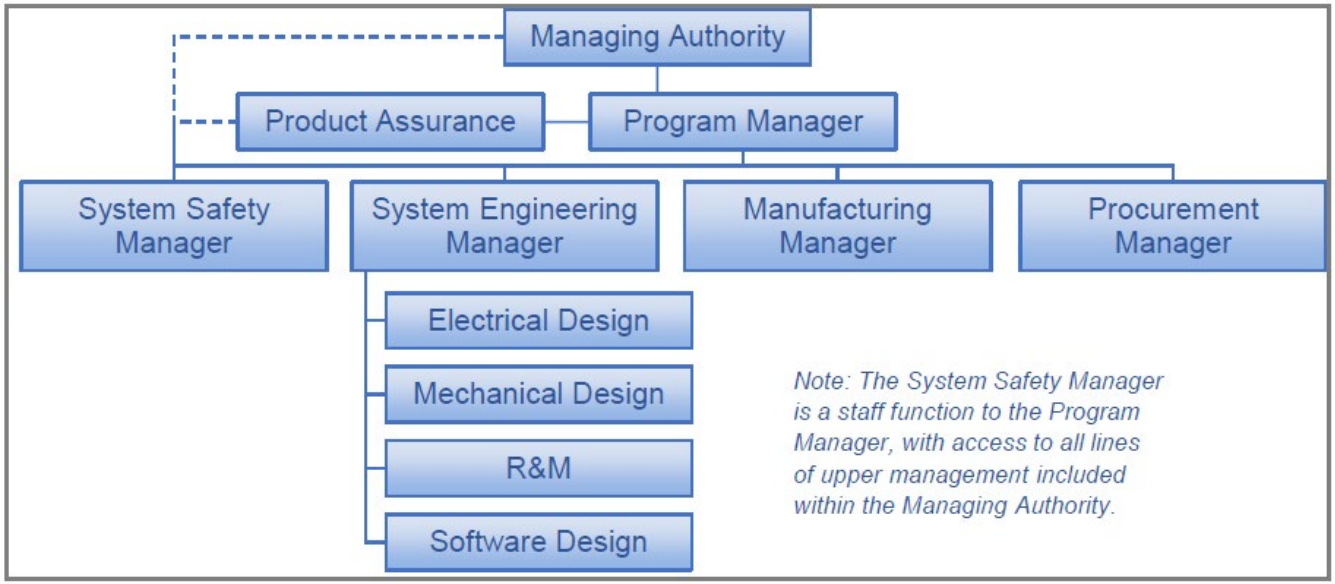
AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.2: Managing Updates.

8.2.1 Organizational Structure.

- Diagrams or organizational charts should be utilized to show the system safety organization with functional relationships and lines of communication within the program.



Sample System Safety Organization

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.2: Managing Updates.

8.2.2 Integration.

- The documented SSP should provide clarity about how the different parts of the organization interface with each other. Specifically, it 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.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.2: Managing Updates.

8.2.2 Integration. [Continued]

- 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.

- 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.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.2: Managing Updates.

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.

AC 450.103-1: System Safety Program

SECTION 8.0: HAZARD MANAGEMENT.

Section 8.3: Tracking of Flight HA Data.

- In accordance with § 450.103(b)(3), operators that are required to conduct a § 450.109 Flight HA must implement a process for tracking hazards, risks, mitigation measures, and verification activities.

- Data tracking is essential for a sound and continually valid Flight HA.

- The documented SSP should define the process and mechanism for identifying, detailing, tracking, collecting, analyzing, and retaining the Flight HA data. Examples of mechanisms are hazard reports, a hazard database, systems engineering management tools, etc.

8.3.1 Traceability.

- As discussed in AC 450.109-1, *Flight Hazard Analysis*, traceability methods should be established for all relevant system safety requirements and analysis data.

AC 450.103-1: System Safety Program

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.103-1: System Safety Program

SECTION 9.0: CONFIGURATION MANAGEMENT AND CONTROL.

- The documented SSP must track the configuration of all safety critical systems* and documentation, Standards for configuration management and control can be found in MIL–HDBK–61.

- The documented SSP should define a CM process for:
  - Documenting and tracking configurations of all safety-critical systems* and documentation, in accordance with § 450.103(c)(1);
  - Ensure the use of correct and appropriate versions of all systems and documentation, in accordance with § 450.103(c)(2); and
  - Document the configurations and versions identified via § 450.103(c)(2) for each licensed activity, in accordance with § 450.103(c)(3)

- The CM process defined in the documented SSP should include lifecycle change, modification, and redesign activity.
  - As the functional HA may evolve throughout the lifecycle, the CM process should apply not just to known safety-critical systems, but also track system changes for potential implications in regards to public safety.

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

AC 450.103-1: System Safety Program

SECTION 10.0: POST-FLIGHT DATA REVIEW.

- An operator is required to employ a process for evaluating post-flight data, in accordance with § 450.103(d).

- 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.

10.1 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.

10.2 Analysis Consistency.

- An operator must employ a process for evaluating post-flight data to 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, per § 450.103(d)(1).

AC 450.103-1: System Safety Program

SECTION 10.0: POST-FLIGHT DATA REVIEW.

10.2 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.

  Note: Flight abort events are typically rare, so verifying the success of a flight abort strategy will rarely be possible. However, post-flight data reviews of other aspects of flight abort may frequently be possible, such as verifying that vehicle data required to evaluate flight abort rules is available to the FSS under all reasonably foreseeable conditions during normal and malfunctioning flight, and that FSS environments did not exceed qualification levels.

AC 450.103-1: System Safety Program

SECTION 10.0: POST-FLIGHT DATA REVIEW.

10.3 Anomaly Reporting and Investigation.

- An operator must employ a process for identifying and addressing (prior to the next flight) any anomaly that may impact any Flight HA, FSA, or safety-critical system*, or is otherwise material to public safety, per §§ 450.103(d)(3) and 450.103(d)(4).
- 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*).

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

AC 450.103-1: System Safety Program

SECTION 10.0: POST-FLIGHT DATA REVIEW.

10.4 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.

AC 450.103-1: System Safety Program

SECTION 11.0: APPLICATION REQUIREMENTS.

- In accordance with § 450.103(e), the following must be submitted:

  1) a description of the applicant's safety organization, identification of 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 §§ 450.103(b), (c), and (d).

- 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: System Safety Program

§ 450.103	DOCUMENT	EVIDENCE
(a)(1) &(2)	Site Safety Doc TBD	TBD
(a)(3)	Site Safety Doc TBD	TBD
	Flight Review Process Doc TBD	TBD
(b)(1) & (2)	System Safety Program Doc TBD	TBD
	Software Development Doc TBD	TBD
	System Engineering Management Doc TBD	TBD
(b)(3)	System Safety Program Doc TBD	TBD
	Flight Hazard Analysis Doc TBD	TBD
(c)(1) - (3)	Configuration Management Doc TBD	TBD
	Flight Review Process Doc TBD	TBD
	Flight System Configuration Doc TBD	TBD
(d)(1) - (4)	System Safety Program Doc TBD	TBD
	System Engineering Management Doc TBD	TBD
	Flight Review Process Doc TBD	TBD
	Post-Flight Review Doc TBD	TBD

Example Compliance Table

AC 450.103-1: System Safety Program

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.103-1: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

Section A.1: System Safety Risk Assessment.

- The system safety risk assessment can be utilized for flight safety and ground safety, and is generally qualitative; however, there are instances when quantitative demonstration may be possible or necessary.
- For flight safety, it is meant to augment the quantitative risk calculated by the FSA 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.
- 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: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

Section A.1: System Safety Risk Assessment.

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	

Severity Categories

AC 450.103-1: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

Section A.1: System Safety Risk Assessment.

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.

Likelihood Levels

AC 450.103-1: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

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: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

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.).

AC 450.103-1: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

Section A.3: Integrated Schedule.

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: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

Section A.3: Integrated Schedule.

A.3.2 Specific Milestones.

- 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.

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.

AC 450.103-1: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

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: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

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: System Safety Program

APPENDIX A: KEY ASPECTS OF A SOUND SYSTEM SAFETY PLAN

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.

AC 450.103-1: System Safety Program

Discussion

Floor open for questions/comments
Either verbally or via comments

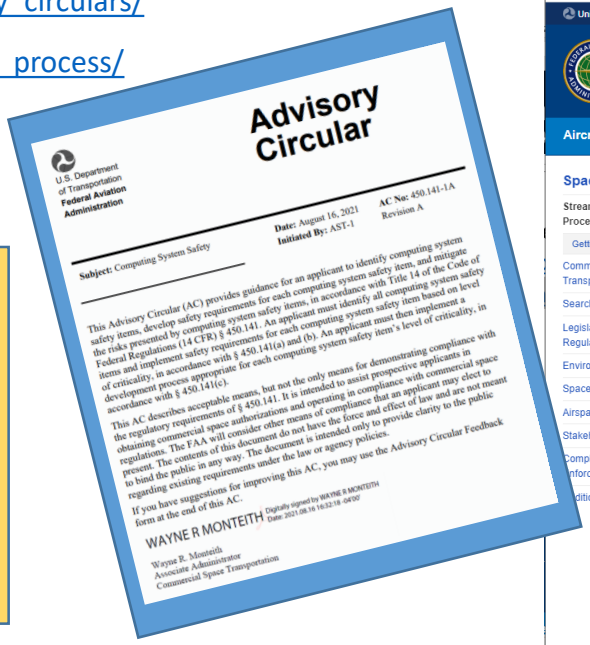
Where to Find Part 450 ACs

Links to ACs:

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

https://www.faa.gov/space/streamlined_licensing_process/

To ensure your comments and questions are considered in a future revision of the AC, please submit via the Feedback Form: https://www.faa.gov/documentLibrary/media/Form/FAA1320-73.pdf. Attachments to this form are welcome.



Advisory Circular

U.S. Department of Transportation
Federal Aviation Administration

Subject: Computing System Safety

Date: August 16, 2021
Initiated By: AST-1

AC No: 450.141-1A
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

Wayne R. Monteith
Associate Administrator
Commercial Space Transportation

Upcoming Workshops

- October 27, 1300
  AC 450.179-1 Ground Safety
- Date/Time TBD (October):
  AC 450.173-1 Mishap Plan-Response, Reporting, and Investigation Requirements