U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: System Safety Program

Date: September 7, 2021 **AC No:** 450.103-1
Initiated By: AST-1

This Advisory Circular (AC) provides guidance on developing a system safety program in accordance with Title 14 of the Code of Federal Regulations (14 CFR) § 450.103, System Safety Program. It is intended to assist prospective applicants in obtaining commercial space authorizations and operating in compliance with commercial space safety regulations. Section 450.103 requires an operator to implement and document a system safety program throughout the lifecycle of a launch or reentry system. The documented system safety program must maintain a safety organization pursuant to § 450.103(a), implement hazard management processes pursuant to § 450.103(b), perform configuration management and control pursuant to § 450.103(c), and employ processes for evaluating post-flight data pursuant to § 450.103(d).

The Federal Aviation Administration (FAA) considers this AC an accepted means of compliance for complying with the regulatory requirements of § 450.103. This guidance is not legally binding in its own right and will not be relied upon by the FAA as a separate basis for affirmative enforcement action or other administrative penalty. Conformity with the guidance is voluntary only and nonconformity will not affect rights and obligations under existing statues and regulations.

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: 2021.09.07 16:02:16 -04'00'

Wayne R. Monteith
Associate Administrator
Commercial Space Transportation

Contents

Paragraph **Page**

Contents (continued)

Paragraph **Page**

Tables

Figures

1 PURPOSE.

1.1 This advisory circular (AC) provides guidance and an acceptable method, but not the only method, that may be used 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.

1.2 **Level of Imperatives**.

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

2 APPLICABILITY.

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

2.2 The material in this AC is advisory in nature and does not constitute a regulation. This guidance is not legally binding in its own right and the FAA will not rely upon this guidance as a separate basis for affirmative enforcement action or other administrative penalty. Conformity with this guidance document (as distinct from existing statutes and regulations) is voluntary only, and nonconformity will not affect rights and obligations under existing statutes and regulations.

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

3 APPLICABLE REGULATIONS AND RELATED DOCUMENTS.

3.1 Related United States Code Statute.

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

3.2 Related FAA Commercial Space Transportation Regulations.

The following 14 CFR regulations must be accounted for when showing compliance with 14 CFR 450.103. The full text of these regulations can be downloaded from the U.S. Government Printing Office e-CFR. A paper copy can be ordered from the Government Printing Office, Superintendent of Documents, Attn: New Orders, PO Box 371954, Pittsburgh, PA, 15250-7954.

- Section 450.101, *Safety criteria.*
- Section 450.107, *Hazard control strategies*.
- Section 450.108, *Flight abort*.
- Section 450.109, *Flight hazard analysis*.
- Section 450.110, *Physical containment*.
- Section 450.111, *Wind weighting*.
- Section 450.113, *Flight safety analysis requirements—scope*.
- Section 450.115, *Flight safety analysis methods*.
- Section 450.139, *Toxic hazards for flight*.
- Section 450.141, *Computing Systems*
- Section 450.143, *Safety-critical system design, test, and documentation*.
- Section 450.157, *Communications*.
- Section 450.179, *Ground safety—general*.
- Section 450.181, *Coordination with a site operator*.
- Section 450.183, *Explosive site plan*.
- Section 450.185, *Ground hazard analysis*.
- Section 450.187, *Ground safety prescribed hazards*.
- Section 450.209, *Compliance monitoring*.
- Section 450.219, *Records*.

3.3 **Related FAA Advisory Circulars.**

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

- AC 450.107-1, *Hazard Control Strategy Determination,* dated July 27, 2021.
- AC 450.109-1*, Flight Hazard Analysis*, dated August 5, 2021.
- AC 450.141-1A, *Computing Systems Safety*, Revision A, dated August 16, 2021.
- AC 450.173-1, *Mishap Reporting, Response, and Investigation*, dated August 12, 2021.
- AC 450.179-1, *Ground Safety*, when published.

3.4 **Related Industry Documents**.

- American National Standards Institute, ANSI-EIA-649C, National Consensus Standard for Configuration Management, dated February 7, 2019.
- Department of Defense Standard, MIL-STD-882E, *System Safety*, dated May 11, 2012, https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=36027.
- Military and Government Specifications and Standards, MIL-HDBK-61B, Configuration Management Guidance, dated April 7, 2020.

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

4 **DEFINITION OF TERMS.**

For this AC, the definitions from § 401.7 apply.

5 ACRONYMS.

AC – Advisory Circular

CFR – Code of Federal Regulations

CM – Configuration Management

FAA – Federal Aviation Administration

FHA – Flight Hazard Analysis

FSA – Flight Safety Analysis

FSS – Flight Safety System

OMB – Office of Management and Budget

SSP – System Safety Program

U.S.C. – United States Code

U.S. – United States

6 SYSTEM SAFETY PROGRAM.

Section 450.103, *System Safety Program*, requires the implementation and documentation of a system safety program (SSP) applicable throughout the lifecycle of a launch or reentry system. A documented SSP establishes the methodologies and management principles for flight safety. It should be demonstrated that an SSP has been established and documented such that compliance with FAA regulations can be determined and maintained. To demonstrate compliance with § 450.103, the documented SSP should define pertinent organizational structures, processes, and safety analysis methodologies. 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.

6.1 Lifecycle System Safety.

Figure 1 of this AC depicts a generic launch or reentry system lifecycle. 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.

Figure 1. Generic Lifecycle of a Launch or Reentry System

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. This is illustrated in **Figure 2**. 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 (FHA), 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.

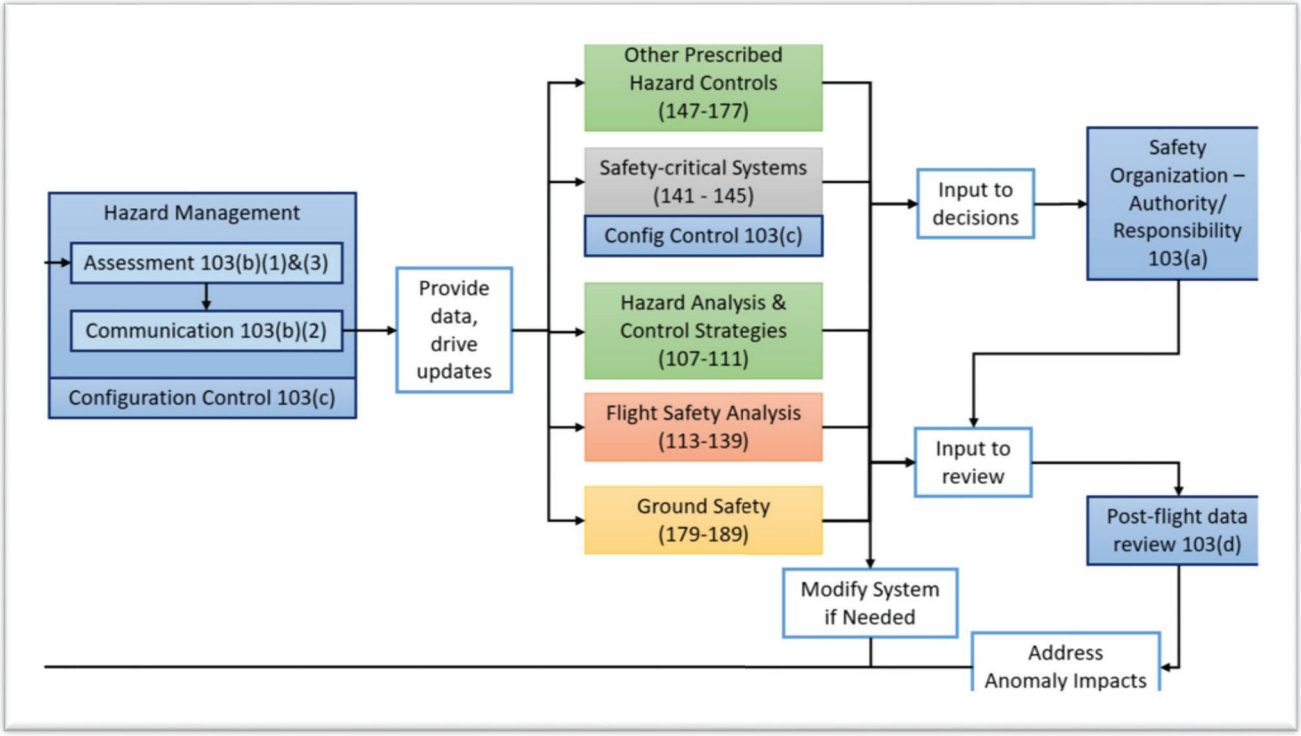

Figure 2. Context of § 450.103 in Part 450 Safety Requirements

7 SAFETY ORGANIZATION.

Section 450.103(a) requires an operator to maintain a safety organization. The establishment of a safety organization is a critical component of launch and mission operations and public safety. As defined in § 401.7, mishap includes a failure of the safety organization. The safety organization's primary responsibility is to carry out the processes needed to protect public safety, as identified in the documented SSP. In addition to the typical system safety engineering organizations, the documented SSP should include a safety organization that addresses and covers all aspects of the public safety of Part 450 Launch and Reentry License Requirements. 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. **Figure 3** of this AC is an example illustration of the foundational structure of a compliant safety organization.

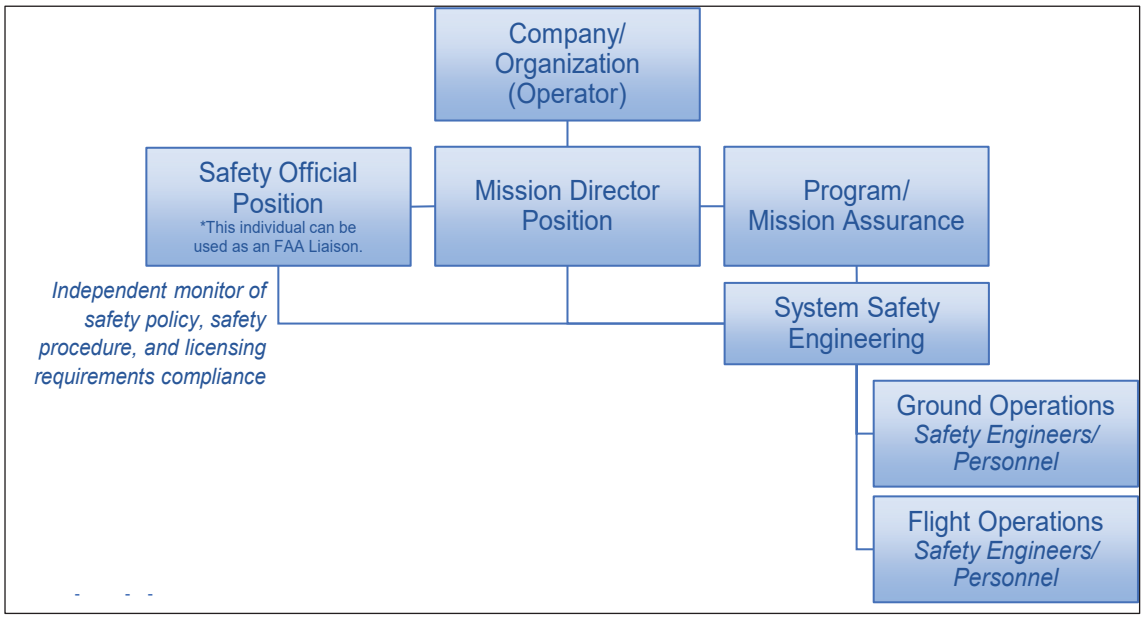

Figure 3. Sample Safety Organization of § 450.103(a)

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. **Table 1** of this AC provides an example format for identification of safety organization personnel.

Table 1 – Example Safety Organization Personnel Table for an Operation

POSITION	NAME	COMPANY & JOB TITLE	CONTACT INFORMATION
Mission Director	-	-	-
Safety Official	-	-	-

Note: This table should be expanded to include other directors, officials, and personnel, as necessary.

7.1.2 Mission Director.

The Mission Director is 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). This includes ensuring that all of the Safety Official's concerns are addressed, per § 450.103(a)(3). The organization should make this responsibility clear to the Mission Director.

7.1.3 Safety Official.

The Safety Official is required to have direct access to the Mission Director. The Safety Official is responsible for communicating potential safety and noncompliance issues to the Mission Director, in accordance with § 450.103(a)(2)(i). The Safety Official is 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). Thus, it is the responsibility of the Safety Official 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. The organization should make this responsibility clear to the Safety Official for each operation.

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.

8 HAZARD MANAGEMENT.

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.

8.1.1 Functional Hazard Analysis.

The system safety approach of a functional hazard analysis must be performed for all Part 450 license applications in accordance with § 450.107(b), *Hazard control strategies*. The functional hazard analysis should inform and ensure the validity of the hazard control strategy determination, the FSA, and the FHA, by accounting for all functional failures associated with reasonably foreseeable hazardous events that have the capability to create a hazard to the public. The functional hazard analysis should also provide a means for methodical and continual validation of the hazard control strategy for each phase of flight during a launch or reentry. Thus, the functional hazard analysis 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.

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. It is expected that "reasonably foreseeable hazardous events" are those identifiable through the system safety process, beyond those that could be determined solely by “brainstorming.” The functional hazard analysis is the system safety analysis tool used to analyze system functions associated with the proposed operation (mission). 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 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.

8.1.3 Flight Hazard Analysis.

The system safety approach of an FHA 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 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. This includes risks from debris, toxics, explosions, and far-field overpressure effects. The documented SSP should ensure the validity of this analysis, with appropriate methodology in place to achieve these requirements.

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 ensures communication and implementation of any updates throughout the organization. This section includes aspects of the system safety organization that can be used as a means of compliance for § 450.103(b)(2). 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. Effective communication is accomplished through clear organizational structure, well defined roles and responsibilities, defined interfaces through the organization, and active management oversight.

8.2.1 Organizational Structure.

Diagrams or organizational charts, such as **Figure 4** of this AC, should be utilized to show the system safety organization with functional relationships and lines of communication within the program.

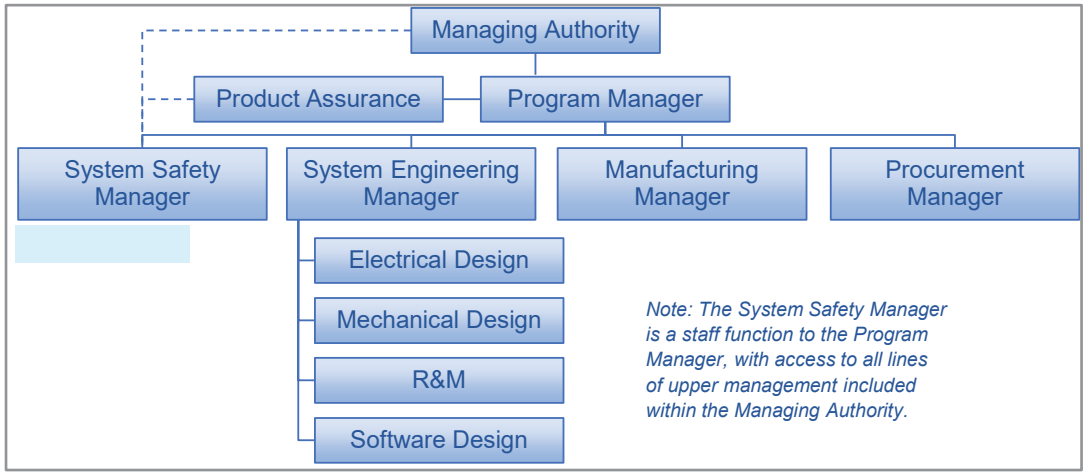

Figure 4. Sample System Safety Organization

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 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.
- 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.

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.

8.3 **Tracking of FHA Data**.

In accordance with § 450.103(b)(3), operators that are required to conduct an FHA must implement a process for tracking hazards, risks, mitigation measures, and verification activities. Section 450.109 contains detailed requirements for performing an FHA, and FAA provides additional guidance in AC 450.109-1, *Flight Hazard Analysis*. Data tracking is essential for a sound and continually valid FHA. The documented SSP should define the process and mechanism for identifying, detailing, tracking, collecting, analyzing, and retaining the FHA 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 analyses. For the FHA, traceability should be demonstrated from:

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

9 CONFIGURATION MANAGEMENT AND CONTROL.

9.1 Standards for configuration management and control can be found in MIL–HDBK–61. The documented SSP must track the configuration of all safety critical systems and documentation, per § 450.103(c)(1). The documented SSP should define a CM process for documenting and tracking configurations of all safety-critical systems. Of course, a key step is identification of those systems which are safety-critical. Safety-critical systems must be identified and documented via the functional hazard analysis in accordance with § 450.107(b)(2), and this may evolve through the lifecycle. Thus, the configuration management process should apply not just to known safety-critical systems, but also track system changes for potential implications in regards to public safety.

9.2 The CM process should: 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 FAA encourages the use of automated, internal workflow systems to accomplish this task. The process defined in the documented SSP should include lifecycle change, modification, and redesign activity. The documented SSP should clearly detail how the CM process meets the requirements sufficient for the FAA to assess compliance of the system.

10 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). 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.

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 FHA, 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. This 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*).

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.

11 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).

11.1 **Safety Organization**.

The documentation of the safety organization should address the specific requirements of chapter 7 of this document and identify lines of communication discussed in paragraph 8.2 of this document.

11.2 **Summary of Processes and Products**.

The 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. The overall SSP documentation will typically also include the processes and products required for the functional hazard analysis per § 450.107(b), FHA (if performed) per § 450.109, safety-critical software and systems per §§ 450.141 and 143, and ground safety per §§ 450.179, 181, 183, 185, and 189. **Table 2** of this AC is an example compliance table that may be provided, along with the identified documentation, to demonstrate compliance with the requirements of § 450.103.

Table 2 – Example of a Compliance Table

§ 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

Appendix A. **Key Aspects of a Sound System Safety Plan**

A.1 SYSTEM SAFETY RISK ASSESSMENT.

The system safety risk assessment can be utilized for flight safety and ground safety. The system safety risk assessment 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 §§ 450.185(b) and 450.109(b)(2). Therefore, an operator should define severity categories and likelihood levels to meet these regulations and to ensure that the system safety risk meets the criteria of §§ 450.185(c) and 450.109(b)(3). 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*. The following guidance on severity categories (**Table 3** of this AC) and likelihood levels (**Table 4**) may be utilized to assess system safety risk to the public.

Table 3 – 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	

Table 4 – 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.

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.

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.).

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.

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.

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.

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.

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. **Table 5** of this AC lists some of the tasks and activities most directly associated with system safety.

Table 5 – Additional System Safety-Related Tasks

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.
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.

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

Advisory Circular Feedback Form

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

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

Please check all appropriate line items:

- o An error (procedural or typographical) has been noted in paragraph Click here to enter text. on page Click here to enter text..
- o Recommend paragraph Click here to enter text. on page Click here to enter text. be changed as follows:

  Click here to enter text.
- o In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

  Click here to enter text.
- o Other comments:

  Click here to enter text.
- o I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____