FAA
Commercial Space Transportation
faa.gov/space

SYSTEM SAFETY WORKSHOP

Presented by
Sean Schindzielorz &
Dr. Kenyatta Washington
System Safety Branch [ASA-220]

Thursday, May 18, 2023,
4:00 pm — 5:30 pm EST

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

Agenda

Overview of Part 450 System Safety

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

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

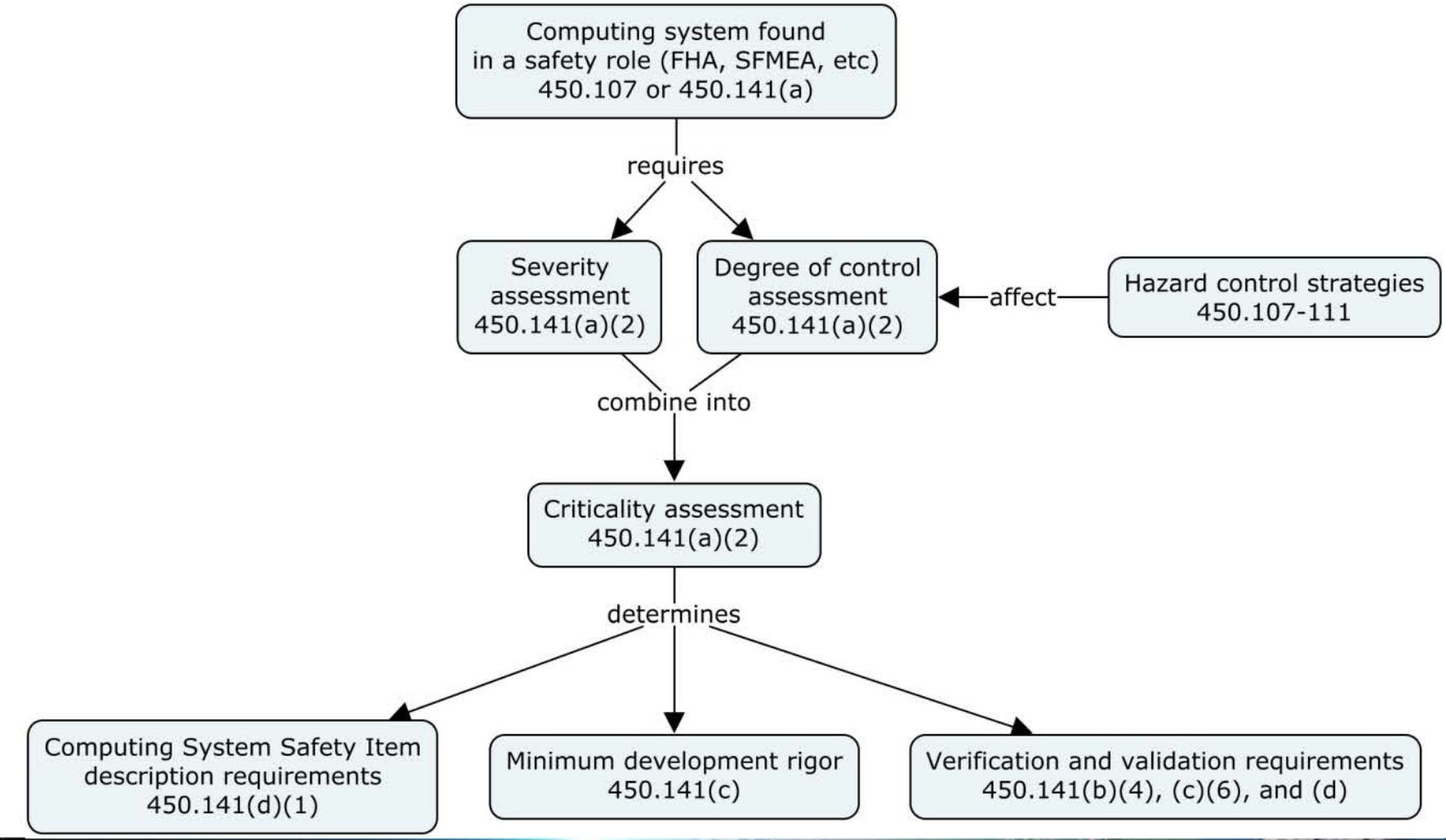
Agenda

Overview of Part 450 System Safety

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

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

Structure of § 450.141



Structure of AC 450.141-1A

Walks through the regulation

AC 450.141-1: 

Adobe Acrobat Document

- Each requirement has one or more means of compliance

Describes a method to document compliance

- Software safety is iterative

Appendices provide supplemental information

- Appendix A provides sample safety requirements
- Appendix B provides sample software safety analysis methods
- Appendix C provides lessons learned from spacecraft failures and aircraft accidents
- Appendix D provides lessons learned from commercial, military, and experimental aircraft accidents

Means of Compliance

AC 450.141-1A has two means of compliance:

1. Tailoring RCC 319-19
   - Recommended for FSS, AFSS, and other dedicated safety systems
   - Tailored version must be tailored during pre-application consultation and included in the application
2. The methods detailed in Chapters 6 through 9 of AC 450.141-1A

§ 450.141(a) Regulation

Replaces prescriptive requirements with performance-based standards and provides increased flexibility for operators to demonstrate compliance.

Scales level of rigor based on each computing system's system-level criticality by severity and degree of control, rather than by degree of autonomy.

Section 450.141 requires the identification and assessment of the public safety-related computing system requirements, functions, and data items in order to streamline the evaluation of computing system safety.

(a) *Identification of Computing System Safety Items*.

An operator must identify:

1) Any software or data that implements a capability that, by intended operation, unintended operation, or non-operation, can present a hazard to the public; and
2) The level of criticality of each computing system safety item identified in subparagraph (1), commensurate with its degree of control over hazards to the public and the severity of those hazards.

§ 450.141(a) In Practice

Ref AC 450.141-1A, Section 6 “Identification Of Computing System Safety Items”

- “Computing system safety item” means any software or data that implements a capability that, by intended operation, unintended operation, or non-operation, can present a hazard to the public, and the criticality of each computing system safety item, commensurate with its degree of control over hazards to the public and the severity of those hazards.
  - Includes software that could interfere with the operation of a computing system safety item, as well as each computing system safety item’s human and hardware interfaces
- Identified computing system safety items should be evident in a standalone document, Functional Hazard Analysis, or other system safety product
  - Applicant and FAA should agree on the list of computing system safety items prior to application submission

Identifying Computing System Safety Items

System Safety Analyses may identify Computing System Safety Items (CSSIs) [Ref AC 450.141-1A, Section 6.1]

- ❑ CSSI is a collection of software or data that can present a hazard to the public
- ❑ Evident as a cause or control to a hazard in functional hazard analysis
- ❑ Evident in software requirements derived from system safety analyses

Assessing Criticality

- Criticality Assessments
  - Define severity levels [Ref AC 450.141-1A, Section 6.2.3]
  - Define control levels using one of several methods [Ref AC 450.141-1A, Section 6.2.4]
- Criticality assessments drive minimum acceptable rigor in development and testing
- Highly-reliable flight safety systems can reduce degree of control, typically from "Autonomous" to "Redundant fault-tolerant"

§ 450.141(b) Regulation

Section 450.141(b) requires an operator to develop safety requirements for each computing system safety item.

"Safety requirements" means computing system requirements that specify attributes or functionality that have public safety significance. Identification of this subset of requirements related to public safety is essential to focus an operator's safety efforts on those parts of the computing system safety item that have public safety consequences.

(b) *Safety Requirements*.

- An operator must develop safety requirements for each computing system safety item. In doing so, the operator must:

1) Identify and evaluate safety requirements for each computing system safety item;
2) Ensure the safety requirements are complete and correct;
3) Implement each safety requirement; and
4) Verify and validate the implementation of each safety requirement by using a method appropriate for the level of criticality of the computing system safety item. For each computing system safety item that is safety critical under § 401.7, verification and validation must include testing by a test team independent of the development division or organization.

§ 450.141(b) In Practice

- **Computing system safety items implement safety requirements [Ref AC 450.141-1A, Section 7 “Safety Requirements”]**

❑ Identify safety requirements for each computing system safety item [Section 7.1]
  - Safety requirements are a subset of software or system requirements

❑ Validate the safety requirements [complete and correct, Section 7.2]
  - Should check that the safety requirements are consistent with the system’s safety requirements
  - Should check that the safety requirements fully specify all needed safety functionality

❑ Implement the safety requirements
  - As normal for computing system requirements

❑ Verify and validate the implementation of safety requirements [Section 7.3]
  - Includes IV&V for safety-critical computing system safety items

Safety Requirements

"Safety requirements" are design requirements that have public safety consequences

- ❑ Describe safety-related design attributes and functionality
- ❑ Examples in AC 450.141-1A, Appendix A

Complete safety requirements [Ref AC 450.141-1A, Section 7.2.1]

- ❑ Define set from design and system safety/software safety documentation
- ❑ Ensure completeness with a feedback loop through testing and operation

Correct safety requirements [Ref AC 450.141-1A, Section 7.2.2]

- ❑ Relies on identification of system requirements and design requirements
  - Checked by independent analysts, testers, and operators
- ❑ Expected to be a cyclical refinement process

Implementing and Verifying Safety Requirements

Implement safety requirements as with any other design requirements

Independent verification and validation required for safety-critical CSSI [Ref AC 450.141-1A, Section 7.3.1]

- ❑ Essential to ensuring public safety and the safety of property (§ 401.7)
- ❑ IV&V should:
  - Be managed independent of the development process
  - Use incentives that encourage thoroughness
  - Have latitude to check for undocumented requirements
  - Provide feedback and findings to development team in a timely manner

Verification and validation should be proportional to criticality [Ref AC 450.141-1A, Section 7.3.2)

- ❑ Testing is preferred whenever feasible
- ❑ Optimal methods are often specific to the system

§ 450.141(c) Regulation

Operators need not employ a separate development process for each computing system safety item. The development process for each computing system safety item must be appropriate to the level of criticality of the computing system safety item and must satisfy the criteria listed in § 450.141(c), at a minimum

(c) *Development Process*.

An operator must implement and document a development process for computing system safety items appropriate for the level of criticality of the computing system safety item. A development process must define:

1) Responsibilities for each task associated with a computing system safety item;
2) Processes for internal review and approval—including review that evaluates the implementation of all safety requirements—such that no person approves that person's own work;
3) Processes to ensure development personnel are trained, qualified, and capable of performing their role;
4) Processes that trace requirements to verification and validation evidence;
5) Processes for configuration management that specify the content of each released version of a computing system safety item;
6) Processes for testing that verify and validate all safety requirements to the extent required by paragraph (b)(4);
7) Reuse policies that verify and validate the safety requirements for reused computing system safety items; and
8) Third-party product use policies that verify and validate the safety requirements for any third-party product.

§ 450.141(c) In Practice

Ref AC 450.141-1A, Section 8 “Development Process”

Performance requirements for development processes scale with criticality

- ❑ Assignments of responsibility for development tasks, usually by position or title (8.2.1)
- ❑ Review processes, typically for requirements vetting, implementation, and testing (8.2.2)
- ❑ Training and qualification process for personnel in safety-related development roles (8.2.3)
- ❑ Process for tracing requirements to verification and validation evidence (8.2.4)
  - Should link each requirement to V&V thereof, enabling verification of a complete safety requirement set
- ❑ Configuration management to specify version content per computing system safety item (8.2.5)
  - See also § 450.103(c) “Configuration Management and Control”
- ❑ Testing process rigor proportional to criticality, with IV&V for safety-critical computing system safety items (8.2.6)
- ❑ Reuse policy (8.2.7)
  - Should define evaluation and testing processes
- ❑ Third-party policy (8.2.8)
  - Should define acceptance, evaluation, and testing processes

Development Process Requirements

Assign responsibilities for safety tasks

- ❑ Often by position and qualification
- ❑ Accomplished when the applicant documents who did each safety task for each CSSI

Review and approval processes

- ❑ Similar to code reviews, but can be a distributed, iterative process
- ❑ Accomplished when reviews are documented to have been independent

Training processes should put appropriately trained/experienced people in safety roles

- ❑ Methods are applicant-specific
- ❑ AST verifies that the applicant has a sound method and standards

More Development Process Requirements

Define processes that trace requirements to verification and validation evidence

- ❑ Connect computing system requirements to tests/analyses or other evidence of implementation
- ❑ Evaluation focuses on potential errors or gaps in traceability

Configuration management sufficient to specify the content of each released version

- ❑ CM is a broader discipline; this is the minimum
- ❑ Accomplished when the applicant has records of what has flown and will fly

Verification and validation in proportion to criticality

- ❑ Tests should check implementation of safety requirements at a minimum
- ❑ Often needs test plans, descriptions, and results in addition to analyses

Even More Development Process Requirements

Previously developed CSSI (reused or 3rd party)

- ❑ Verify and validate safety requirements for reused and 3rd party CSSI
- ❑ Includes COTS, GOTS, and legacy CSSI
- ❑ Should evaluate the differences between prior uses or design documents and its use in the system
- ❑ Need not replicate tests or analyses conducted by supplier, but should ingest data into the applicant's safety analyses

AC 450.141-1A, Section 8.3 "Development Process Considerations"

Considerations for development processes

- ❑ Is not a means of compliance in itself
- ❑ Discusses concepts that may aid applicants in accomplishing elements of safe development
  - Software implementation analysis (8.3.1)
  - Development standards (8.3.2)
  - Quality assurance (8.3.3)
  - Formal inspections (8.3.4)
  - Anomaly reports (8.3.5)
  - Maintenance and repair of computing system hardware (8.3.6)
  - Maintenance of computing system software (8.3.7)
  - Building maintainable software (8.3.8)

§ 450.141(d) Regulation

Section 450.141(d) contains the application requirements for this section. Each of the five requirements in paragraph (d) mirrors a key aspect of computing system safety, allowing the applicant and FAA to understand the rigor of development in terms of public safety. This structure is meant to reflect the typical formats of computing system safety data submissions received by the FAA to date.

These application requirements need not be met in separate documents.

(d) *Application Requirements*.

An applicant must:

1) Identify and describe all computing system safety items involved in the proposed operations;
2) Provide the safety requirements for each computing system safety item;
3) Provide documentation of the development processes that meets § 450.141(c);
4) Provide evidence of the execution of the appropriate development process for each computing system safety item; and
5) Provide evidence of the implementation of each safety requirement.

§ 450.141(d) In Practice

Requires documentation of (a-c)

- ❑ Identify and describe computing system safety items, including their criticality (9.1)
- ❑ Provide safety requirements for each computing system safety item (9.2)
- ❑ Document a process that meets (c)(1)-(8) (9.3)
- ❑ Provide evidence of execution of the appropriate development processes (9.4)
  - Note which development process applied to each computing system safety item and which process path options are used
  - Provide artifacts of the development process that verify that the computing system safety item followed the process
- ❑ Provide evidence of the implementation of each safety requirement (9.5)
  - Test record, analysis, or other verification evidence per process

Some Key Revisions in AC 450.141-1A

- Functional Hazard Analyses conducted to meet 450.107 or 109 can, when appropriately configured, meet 450.141(a)
- Reasonably foreseeable faults are those that an analyst can discover through methodical assessment of the system.
  - Could depend on:
    - Programming language
    - Hardware configuration
    - Other computing systems that interact with the vehicle
- Fault tolerance analysis should:
  - Identify the conditions under which each tolerance is acceptable
  - Identify each computing system safety item by fault tolerance
  - Describe the measures in place to limit risk for each CSSI

Summary of § 450.141 Discussion

Summary of Key Topics

- ❑ Identification of computing system safety items and level of criticality
- ❑ Developing safety requirements, including identification, implementation, and verification & validation
- ❑ Implementing and documenting a development process for computing system safety items

§ 450.141 “Computing System Safety”

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.

§§ 450.139 “Toxic Hazards for Flight”

(a) *Applicability.*

1) Except as specified in paragraph (a)(2), this section applies to any launch or reentry vehicle, including all vehicle components and payloads, that use toxic propellants or other toxic chemicals.
2) No toxic release hazard analysis is required for kerosene-based fuels, unless the Administrator determines that an analysis is required to protect public safety.

AC 450.139-1 “Toxics” [In Development*]

- ❑ Forthcoming to provide acceptable means of compliance

  Disclaimer: AC 450.139 is under development and is subject to change upon publication.

* Plus modifications to AC 450.179-1 to address specifics for toxic hazards during ground operations

§§ 450.139 “Toxic Hazards for Flight”

(b) *General.* An operator must—

1) Conduct a toxic release hazard analysis in accordance with paragraph (c) of this section;
2) Manage the risk of casualties that could arise from the exposure to toxic release through one of the following means:
    i. Contain hazards caused by toxic release in accordance with paragraph (d) of this section; or
    ii. Perform a toxic risk assessment, in accordance with paragraph (e) of this section,
        - § 450.139: that protects the public in compliance with the safety criteria of § 450.101, including toxic release hazards.
3) Establish [§ 450.139: flight commit criteria] based on the results of its toxic release hazard analysis and toxic containment or toxic risk assessment for any necessary evacuation of the public from any toxic hazard area.

§§ 450.139 “Toxic Hazards for Flight”

(c) ***Toxic release hazard analysis.*** A toxic release hazard analysis must—

1) Account for any toxic release that could occur during nominal or non-nominal [§ 450.139: flight : launch or reentry ground operations];
2) Include a worst-case release scenario analysis or a maximum-credible release scenario analysis for each process that involves a toxic propellant or other chemical;
3) Determine if toxic release can occur based on an evaluation of the chemical compositions and quantities of propellants, other chemicals, vehicle materials, and projected combustion products, and the possible toxic release scenarios;
4) Account for both normal combustion products and any unreacted propellants and phase change or chemical derivatives of released substances; and
5) Account for any operational constraints and emergency procedures that provide protection from toxic release.

§§ 450.139 “Toxic Hazards for Flight”

(d) ***Toxic containment.*** An operator using toxic containment must manage the risk of any casualty from the exposure to toxic release either by—

1) Evacuating, or being prepared to evacuate, the public from any toxic hazard area in the event of a worst-case release or maximum-credible release scenario; or

2) Employing meteorological constraints to limit an operation to times during which prevailing winds and other conditions ensure that any member of the public would not be exposed to toxic concentrations and durations greater than accepted toxic thresholds for acute casualty in the event of a worst-case release or maximum-credible release scenario.

§§ 450.139 “Toxic Hazards for Flight”

(e) ***Toxic risk assessment.*** An operator using toxic risk assessment must:

- § 450.139: establish flight commit criteria that demonstrate compliance with the safety criteria of § 450.101.

A toxic risk assessment must—

1) Account for airborne concentration and duration thresholds of toxic propellants or other chemicals. For any toxic propellant, other chemicals, or combustion product, an operator must use airborne toxic concentration and duration thresholds identified in a means of compliance accepted by the Administrator;
2) Account for physical phenomena expected to influence any toxic concentration and duration in the area surrounding the potential release site;
3) Determine a toxic hazard area for the launch or reentry, surrounding the potential release site for each toxic propellant or other chemical based on the amount and toxicity of the propellant or other chemical, the exposure duration, and the meteorological conditions involved;

§§ 450.139 “Toxic Hazards for Flight”

(e) ***Toxic risk assessment.*** A toxic risk assessment must—

4) Account for all members of the public who may be exposed to the toxic release [§ 450.139: including all members of the public on land and on any waterborne vessels, populated offshore structures, and aircraft that are not operated in direct support of the launch or reentry]; and

5) Account for any risk mitigation measures applied in the risk assessment.

§§ 450.139 “Toxic Hazards for Flight”

(f) *Application requirements.* An applicant must submit:

1) The identity of toxic propellant, chemical, or combustion products or derivatives in the possible toxic release;
2) The applicant’s selected airborne toxic concentration and duration thresholds;
3) The meteorological conditions for the atmospheric transport and buoyant cloud rise of any toxic release from its source to downwind receptor locations;
4) Characterization of the terrain, as input for modeling the atmospheric transport of a toxic release from its source to downwind receptor locations;
5) The identity of the toxic dispersion model used, and any other input data;
6) Representative results of an applicant’s toxic dispersion modeling to predict concentrations and durations at selected downwind receptor locations, to determine the toxic hazard area for a released quantity of the toxic substance;

§§ 450.139 "Toxic Hazards for Flight"

(f) *Application requirements.* An applicant must submit:

7) A toxic release hazard analysis in accordance with paragraph (c) of this section:
   i. A description of the failure modes and associated relative probabilities for potential toxic release scenarios used in the risk evaluation; and
   ii. The methodology and representative results of an applicant's determination of the worst-case or maximum-credible quantity of any toxic release that might occur during [§ 450.139: the flight of a vehicle]

8) [§ 450.139] In accordance with § 450.139(b)(2),
   i. A toxic containment in accordance with paragraph (d) of this section, identify the evacuation plans or meteorological constraints and associated launch commit criteria needed to ensure that the public will not be within a toxic hazard area in the event of a worst-case release or maximum-credible release scenario; or
   ii. A toxic risk assessment in accordance with paragraph (e) of this section:
      A. A demonstration that the safety criteria in § 450.101 will be met;
      B. The population characteristics in receptor locations that are identified by toxic dispersion modeling as toxic hazard areas;
      C. A description of any risk mitigations applied in the toxic risk assessment; and
      D. A description of the population exposure input data used in accordance with § 450.123.

Summary of "Toxics" Discussion

Summary of Key Topics

- ❑ Determining use of toxic propellants or other toxic chemicals
- ❑ Conducting a toxic release hazard analysis
- ❑ Managing the risk of casualties that could arise from the exposure to toxic release, via:
    i. Contain hazards caused by toxic release in accordance with paragraph (d) of this section; or
    ii. Perform a toxic risk assessment, in accordance with paragraph (e) of this section, that protects the public in compliance with the safety criteria of § 450.101, including toxic release hazards.
- ❑ Establishing [§ 450.139: flight commit criteria] based on the results of its toxic release hazard analysis and toxic containment - or - toxic risk assessment for any necessary evacuation of the public from any toxic hazard area.

§§ 450.139 “Toxic Hazards for Flight”

SYSTEM SAFETY WORKSHOP

Thank you for joining us.

FAA
Commercial Space Transportation
faa.gov/space