AST Commercial Space Transportation

FAA AST Workshop: AC 450.179-1

Advisory Circular (AC) for Ground Safety

Christopher Vance
Said Hamouch
27 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 §§ 450.179 through 450.189

§ 450.179 *Ground Safety - General*.

(a) At a U.S. launch or reentry site, an operator must protect the public and property from adverse effects of hazardous operations and systems associated with (1) through (3).

(b) An operator is not required to comply with §§ 450.181 through 450.189 of this part if: (1) through (3).

§ 450.181 *Coordination with a Site Operator.*

(a) *General*. For a launch or reentry conducted from or to a Federal launch or reentry site or a site licensed under part 420 or 433 of this chapter, an operator must coordinate with the site operator to (1) through (2).

§ 450.183 *Explosive Site Plan*.

(a) *Explosive siting requirements*. For a launch or reentry conducted from or to a site exclusive to its own use, an operator must comply with the explosive siting requirements of §§ 420.63, 420.65, 420.66, 420.67, 420.69, and 420.70 of this chapter.

Regulation §§ 450.179 through 450.189

§ 450.185 *Ground Hazard Analysis*.

An operator must perform and document a ground hazard analysis, and continue to maintain it throughout the lifecycle of the launch or reentry system.

§ 450.187 *Toxic Hazards Mitigation for Ground Operations.*

(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.

§ 450.189 *Ground Safety Prescribed Hazard Controls.*

(a) *General.* In addition to the hazard controls derived from an operator's ground hazard analysis and toxic hazard analysis, an operator must comply with paragraphs (b) through (e) of this section.

AC 450.179-1: Ground Safety

SECTION 1: PURPOSE.

- This Advisory Circular (AC) provides guidance for an operator to meet the Ground Safety requirements defined by Title 14 of the Code of Federal Regulations (14 CFR) §§ 450.179, 450.181, 450.183, 450.185, 450.187, and 450.189. This includes ground safety general requirements; coordination with a site operator; explosive site planning; ground hazard analysis; toxic hazards mitigation for ground operations; and ground safety prescribed hazard controls.

- 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.

AC 450.179-1: Ground Safety

SECTION 4: DEFINITIONS OF TERMS.

Terms and definitions from § 401.7 apply. For this AC, the following terms and definitions apply:

Countdown Abort. A method to abort a launch, including launch scrubs, recycle operations, hang-fires, or an instance in which the launch vehicle does not lift-off after a command to initiate flight has been sent. After a countdown abort, an operator must comply with § 450.189(c).

Explosives Site Plan (ESP). A document that lists the attributes of each potential explosion site and the exposed sites it can potentially affect (workers, unrelated buildings, power lines, etc.) that demonstrates safe separation quantity-distances (QDs) are met or provides justification for violating QD distances.

Ground System. The integrated set of subsystems, personnel, and processes utilized for performing pre-flight and post-flight operations at a launch or reentry site.

SECTION 5: ACRONYMS.

AC 450.179-1: Ground Safety

SECTION 6.0: OVERVIEW

Section 6.1: Objective of Ground Safety.

- In accordance with § 450.179(a), an operator must ensure ground safety at a U.S. launch or reentry site by protecting the public and property from adverse effects of hazardous operations and systems.
  - Demonstrating regulatory compliance to §§ 450.179, 450.181, 450.183, 450.185, 450.187, and 450.189; and
  - Ensuring protection of the public (including neighboring operations personnel) and property from hazards associated with licensed ground operations and activities involving ground systems and flight systems.

Section 6.2: Ground Safety Methodology.

- The documented system safety program (SSP) should define the ground safety methodology to show compliance with these regulations.

AC 450.179-1: Ground Safety

SECTION 6.0: OVERVIEW

Section 6.3: Aspects of Ground Hazard Analysis.

- A Ground Hazard Analysis (GHA) is required by § 450.185 and should provide an integrated assessment of the ground system, flight system, and operational hazards to the public and property associated with licensed pre-flight and post-flight ground operations.
- The GHA is utilized to derive ground hazard controls for implementation in addition to prescribed hazard controls defined in § 450.189.
- A GHA is a qualitative system safety analysis, similar to a flight hazard analysis outlined in AC 450.109-1, *Flight Hazard Analysis*.
- The GHA should be performed early in system development and operation conceptualization to define the ground safety risk to the public and property in order to positively influence design and operation decisions.
- A GHA must be maintained throughout the lifecycle of the launch or reentry system, in accordance with § 450.185.

AC 450.179-1: Ground Safety

SECTION 6.0: OVERVIEW

Section 6.3: Aspects of Ground Hazard Analysis.

- A ground hazard analysis should:

1) Identify system and operation hazards to the public and property associated with licensed pre-flight and post-flight ground operations involving the launch or reentry vehicle, ground hardware used by the launch site, and ground support equipment provided by the launch site or unique support equipment required by the system, along with associated software and firmware [§ 450.185 (a)];

2) Assess the likelihood and severity of each hazard to the public [§ 450.185(b)];

3) Ensure that the ground safety risk associated with each hazard to the public and property meets defined acceptance criteria [§ 450.185(c)];

4) Identify and describe the risk elimination and mitigation measures required to satisfy the acceptance criteria [§ 450.185(d)]; and

5) Demonstrate that the risk elimination and mitigation measures achieve the acceptable levels through validation and verification [§ 450.185(e)].

AC 450.179-1: Ground Safety

AC 450.179-1: Ground Safety

Section 6.4: Formal Traceability of Ground Safety Hazards.

- Formal tracking methods should be established to show direct connections between all aspects of aspects of ground safety hazards to the public and property, source, causes, mitigations, and verification evidence.

Subsystem and Operator Level

Subsystem	Failure Description and End Effect	Component(s) / Item(s)	IDs	Possible Cause(s)	Risk Before Mitigation Measures			Risk Elimination / Mitigation Measures	Risk After Mitigation Measures			Verification Evidence
					L	S	R		L	S	R	
Fuel Servicing Ground Support Equipment	Fuel Servicing Ground Support Equipment[Function TBD] during [Operations Phase(s) TBD] fails [Failure TBD], possibly resulting in fire/ explosion [End Effect TBD]	Local Processor	Functional Failure ID; Fault Tree ID	**C1** TBD **C2** TBD **C3**, and on…	Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of **C1** [design, test, manufacturing process, etc.] **C1.M2**, and so on…	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on…

Integrated System and Operation Level[1]

Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1]			Verification Evidence[1]
		L	S	R	
H1 Fire/Explosion **H2** Toxic Release	**H1.M1** - Specific to mitigation of **H1** [Clear areas, operational restrictions, etc…] **H1.M2**, and so on…	TBD	TBD	TBD	**H1.M1.V1** – Documented evidence specific to **H1.M1** mitigation **H1.M1.V2**, and so on… **H1.M2.V1**, and so on…

[*The template of*] **Table A-1** shows the types of information that an applicant should provide to demonstrate traceability.

AC 450.179-1: Ground Safety

Section 6.5: Ground Safety Hazards and Software Safety

- In accordance with § 450.141(a), if the GHA identifies software or data utilized in a subsystem or the integrated system as potential hazard sources or hazard controls, then the applicant should perform a software hazard analysis to identify computing system safety items and assess their level of criticality.

- Per the guidance of AC 450.141-1, software hazard analyses identify potential software faults and their effects on the computing system and the system as a whole, as well as mitigation measures that can be used to reduce the risk.

AC 450.179-1: Ground Safety

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.179-1: Ground Safety

SECTION 7.0: GENERAL GROUND SAFETY

Section 7.1: General Guidance.

- A licensed operator must document and ensure compliance to ground safety regulations in accordance with §§ 450.179, 450.181, 450.183, 450.185, 450.187, 450.189.
- In accordance with § 450.179(a), the following operations, at a minimum, must be assessed for hazards affecting the public:
  - Preparing launch vehicle for flight;
  - Returning launch or reentry vehicle to safe condition after landing;
  - Returning launch or reentry vehicle to safe condition after aborted launch attempt; and
  - Returning launch or reentry site to safe condition.

AC 450.179-1: Ground Safety

SECTION 7.0: GENERAL GROUND SAFETY

Section 7.2: Exemption Potential.

- In accordance with § 450 .179(b) and (c), operations from a federal launch range may be exempt from §§ 450.181, 450.183, 450.185, 450.187, and 450.189, if they meet the following:

  1) The launch or reentry is being conducted from a Federal launch or reentry site;

  2) The operator has a written agreement with the Federal launch or reentry site for the provision of ground safety services and oversight; and

  3) The Administrator has determined that the Federal launch or reentry site's ground safety processes, requirements, and oversight are not inconsistent with the Secretary's statutory authority over commercial space activities.

Note: If the site meets the conditions in § 450.179(b) and (c), the FAA will develop a Memorandum of Agreement (MOA) with the approved site and publish the MOA on FAA's website.

AC 450.179-1: Ground Safety

SECTION 7.0: GENERAL GROUND SAFETY

Section 7.3: Defining Ground Operations.

- To properly conduct ground safety, the pre-flight and post-flight operations should be defined and documented.
- This list of defined pre-flight and post-flight operations should include all systems and operations involving the vehicle or any payload.
- At minimum, the operations within the scope of a license must be defined. Determining scope of license is discussed further in AC 413.5 Pre-Application Consultation.

AC 450.179-1: Ground Safety

SECTION 8.0: SITE OPERATOR COORDINATION

- It is important that the launch or reentry operator define roles, responsibilities, and timelines with the site operator to ensure that timely responses to mishaps are established prior to licensed hazardous operations at the launch or reentry site.

- The launch or reentry operator must coordinate with the site operator to ensure public safety and comply with § 450.181(a). [When conducting a launch or reentry from a Federal site or site licensed under Part 420, License to operate a launch site, or Part 433, License to operate a reentry site.]

Section 8.1: Control of Public Access.

- For public access control, the operator should identify the day, time, and length of controlled access required for each applicable location.

AC 450.179-1: Ground Safety

SECTION 8.0: SITE OPERATOR COORDINATION

Section 8.2: Site Operator Agreements.

- In accordance with § 450.181(b), the operator must demonstrate they have coordinated with the site operator, and should demonstrate they have coordinated with other operators if applicable on their hazardous operations to establish roles and responsibilities for reporting, responding to, and investigating any mishap during ground activities at the site.
- In accordance with § 450.147, vehicle operators are required to have agreements with any sites or services that are necessary to meet the safety requirements for a license.
- The operator should identify the site operator agreements already in place to determine the applicability and intended execution. If the current site operator agreements already in place are not sufficient for the identified hazardous operations, then the operator must acquire the necessary modified or additional agreements.
- These agreements should be made available to the FAA and site operator for their awareness.

AC 450.179-1: Ground Safety

SECTION 8.0: SITE OPERATOR COORDINATION

Section 8.3: Ground Hazard Area Designation and Coordination.

- The impacts to other sites should be documented and evaluated as changes are made.
- The site coordination activity should include the identification of the ground operation hazardous processes, their potential exposure interval, and their mitigations.
- The operator and the site operators should define the mechanism by which they will communicate and acknowledge requests prior to and during the hazardous operations.
- Operators and site operators should ensure ground hazard areas remain controlled during a mishap according to documented emergency procedures defined in § 450.189(e).

AC 450.179-1: Ground Safety

SECTION 8.0: SITE OPERATOR COORDINATION

Section 8.4: Mishap Reporting, Response, Investigation.

- The operator must assess and adhere to the site mishap reporting, response, and investigation requirements defined by § 450.173. This will ensure that prompt and effective responses to any mishaps provide adequate protection to the general public.

- Ground operations requiring fire department, medical, and other emergency or facility services should be made aware of the operations and their potential hazards and expected mitigations.

- In addition to developing an adequate mishap response plan, the operator must, in accordance with § 450.181(b), coordinate with the site operator to establish roles, responsibilities, and timelines associated with:
  - Reporting mishaps during ground activities at the launch or reentry site;
  - Investigations of mishaps during g round activities at the launch or reentry site; and
  - Responding to mishap reports for ground activities at the launch or reentry site.

Note: For additional information see AC 450.173-1, *Mishap Reporting, Response, and Investigation*.

AC 450.179-1: Ground Safety

SECTION 9.0: EXPLOSIVES SITE PLAN (ESP)

Per § 450.183, an ESP for exclusive use sites must be documented and followed throughout the lifecycle of a licensed operation employing explosives and energetic liquids in accordance with §§ 420.63, 420.65, 420.66, 420.67, 420.69, and 420.70. Part 420 Appendix E contains tables that can be utilized to document the ESP.

Note: In accordance with § 420.63(b), an applicant operating at a launch site located on a federal launch range does not have to comply with these requirements if the applicant is in compliance with the federal launch range's explosive safety requirements.

Note: Licensed site operators, rather than licensed launch or reentry operators operating at an FAA-licensed site, are required to comply with the explosive siting requirements in Part 420.

AC 450.179-1: Ground Safety

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

- In accordance with § 450.185, a GHA must be performed, documented, and continually maintained throughout the life cycle of the launch or reentry system.
- A GHA should include an assessment of the launch or reentry vehicle, the launch or reentry integrated systems, ground support equipment, and other relevant site hardware and software.
- An applicant must identify hazards; assess the associated risk; and document mitigations, controls, and provisions for hazard control validation and verification, in accordance with § 450.185.

Note: All regulated operators, including hybrid launch or reentry systems operators, need to prepare a ground hazard analysis to ensure public safety is protected. Hybrid launch or reentry vehicles may pose a risk to the public; therefore, the FAA also imposes these ground hazard analysis requirements on hybrid launch vehicles in order to identify and mitigate those risks.

AC 450.179-1: Ground Safety

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Identify Hazards with Traceability (a)

Section 10.1: Identify Hazards.

The ground safety hazards referred to in a GHA generally result from:

- Ground and flight system hazards existing due to the current configuration or operationally induced [ref § 450.185(a)(1)]; and
- Operation hazards unique to ground processing at a launch and reentry site [ref § 450.185 (a)(2)].

Identification and Decomposition of All System and Operation Failures.

Analysis and supplemental data routinely utilized to identify system failures and their causes include:

- Functional Hazard Analysis for Flight System;
- Functional Hazard Analysis for Ground System;
- Fault Tree Analysis;
- Failure Modes and Effects Analysis; and
- Human Error Analysis (HEA); etc.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.1: Identify Hazards.

Identify Hazards with Traceability (a)

<u>Documenting a Ground Hazard Analysis</u>.

- In GHAs are typically documented similar to “Task 206, Operating and Support Hazard Analysis” of MIL-STD 882.
- An O&SHA analyzes the processes and procedures of the entire operation while considering the source data discussed in the section above.
- In accordance with § 450.185(a), the potential causes of all system and operation hazards should be identified as a precursor to apply mitigations to reduce or eliminate the ground safety hazards to the public and property.
- There will likely be multiple potential causes for each hazard. Each potential cause of a hazard should be specified to a level of detail where it is possible to apply a mitigation and the required level of verification.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Identify Hazards with Traceability (a)

Section 10.1: Identify Hazards.

Hazard Traceability.

Traceability ensures proper identification of ground safety hazards to the public for § 450.185 (a) and should be demonstrated from:

1) Subsystem functional failures and operator failures to their causes; and

2) Subsystem functional failures and operator failures to respective ground safety hazards to the public and property at the integrated system and operation level.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Assess Severity and Initial Likelihood (b)

Section 10.2: Hazard Assessment.

- The severity and likelihood of each ground safety hazard to the public and property must be assessed, in accordance with § 450.185(b), in order to determine the associated ground safety risk.

- The characterization of each ground safety risk allows for determining the necessity, and proper application, of any additional mitigation actions.

Resources for Qualitative Assessment.

- Suitable assessment severity categories and likelihood level criteria should be determined for each specific program to demonstrate compliance with § 450.185(b) and (c). AC 450.103-1, *System Safety Program*, provides guidance on severity categories and likelihood levels in Table A-1 of Appendix A.

- The risk assessment with respect to ground safety hazards to the public and property will utilize qualitative statements.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.2: Hazard Assessment.

Assess Severity and Initial Likelihood (b)

<u>Utilizing a Systematic Assessment Process</u>.

- The FAA encourages, but does not require, an operator to utilize a systematic development process that allows for a baseline assessment of pre-mitigation risk for each hazard.
- The FAA recommends that operators who choose not to utilize a pre-mitigation risk assessment strategy discuss the appropriateness of their development process and any risk assessment assumptions during pre-application consultation. This strategy may not be acceptable with all programs.
- Irrespective of the applicant's development process, post-mitigation risk assessment is required to determine the residual risk to the public and property.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.2: Hazard Assessment.

Assess Severity and Initial Likelihood (b)

Utilizing a Systematic Assessment Process.

- Risk assessment should be performed at the appropriate levels, primarily the: (1) subsystem and operator level; and (2) integrated system and operation level.
- Risk assessment at these levels allows for greater insight into the effectiveness of mitigations and verifications specific to each cause of each failure resulting in a ground safety hazard to the public and property and appropriate application of subsystem, integrated system and operation mitigations and verifications.

Risk Assessment Traceability.

Traceability ensures proper assessment for § 450.185(b) and should be demonstrated from the subsystem and operator level risk assessment to the integrated system and operation level risk assessment.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Check Compliance with Acceptable Criteria (c)

Section 10.3: Risk Acceptability Criteria.

<u>Developing Risk Acceptance Criteria</u>.

- Risk acceptance is determined by comparison of final assessed ground safety risk against established acceptance criteria.
- Suitable risk acceptance criteria must be determined for each specific program and documented in the SSP utilizing the guidance of AC 450.103-1, *System Safety Program*.
- To ensure proper acceptance of risks associated with ground safety hazards to the public for § 450.185(c), the associated residual risk should meet the established acceptance criteria an d the rationale for acceptance should be documented.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Check Compliance with Acceptable Criteria (c)

Section 10.3: Risk Acceptability Criteria.

Baseline of Risk Acceptability.

In accordance with § 450.185(c), the FAA considers the baseline standard for risk acceptability or ground safety hazards to the public and property to be the following:

- The likelihood of any hazardous condition that may cause death or serious injury to the public must be extremely remote.

  Note: As documented in AC 450.103-1, *System Safety Program*, extremely remote should be considered "so unlikely, it can be assumed occurrence may not be experienced, with a likelihood of occurrence less than 10^{-6} in any one mission."

- The likelihood of any hazardous condition that may cause major property damage to the public not associated with the launch or reentry, must be remote.

  Note: As documented in AC 450.103-1, *System Safety Pro*gram, remote is considered "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."

Note: The standards for risk acceptability are intentionally strict to ensure protection of the public. Sufficient mitigation to control the hazard should be demonstrated.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Identify Mitigations with Traceability at Appropriate Level (d)

Section 10.4: Risk Mitigation.

Risk elimination or mitigation measures must be identified and fully described to reduce the risk to an acceptable level as required by § 450.185(d).

Proper Risk Mitigation Process.

Mitigating risk does not change severity of the hazard, only the likelihood. If there is a change in severity, it should be documented as a new risk.

System Safety Design Order of Precedence.

In order to mitigate risk from ground safety hazards to the public, an operator should follow a process using a systematic order of precedence. An applicant may follow the "System Safety Design Order of Precedence" documented in MIL-STD-882.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Identify Mitigations with Traceability at Appropriate Level (d)

Section 10.5: Considerations for Risk Mitigation Measures.

- Consideration should be given as to whether proposed risk mitigation measures introduce new hazards. To allow flexibility, the FAA has not mandated any particular mitigation approach.
- Selection of a risk elimination or mitigation measure is usually based on a number of factors, such as the type of operation, feasibility of implementation, effectiveness, and impact on system performance.
- Where possible, the FAA expects the utilization of existing industry standards for mitigations.

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.5: Considerations for Risk Mitigation Measures.

Identify Mitigations with Traceability at Appropriate Level (d)

Risk Mitigation Traceability.

Traceability ensures proper application of mitigations for § 450.185(d) and should be demonstrated from:

1) Subsystem and operator failures to their causes to respective mitigations;
2) Subsystem and operator failures to respective ground safety hazards to the public and property at the integrated system and operation level;
3) Subsystem and operator level risk assessment to integrated system and operation level risk assessment; and
4) Ground safety hazards to the public and property at the integrated system and operation level to their respective mitigations.

AC 450.179-1: Ground Safety

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.6: Validation and Verification.

Risk mitigations of ground safety hazards to the public and property applied at various levels (subsystem, operator, integrated system, or operation) must be validated and verified as required by § 450.185(e).

<u>Validating Risk Mitigations</u>.

- Per § 450.185(e), validation evidence must demonstrate that the risk elimination and mitigation measures achieve the risk acceptability criteria specified by § 450.185(c). This documented evidence [e.g., V&V Tracking Log] must be provided to the FAA in accordance with § 450.185(f)(3).
- Validation determines whether the implemented mitigation measures and respective verifications are sound.
- The validation effort ensures that each mitigation and verification is unambiguous, correct, complete, and consistent.
- The validation process evaluates that each mitigation measure and respective verification is well understood and operationally and technically feasible.

Identify Verifications with Traceability to Mitigations (e)

Validate Mitigations and Verifications (e)

Validate Compliance with Acceptable Criteria (c)

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.6: Validation and Verification.

<u>Verifying Risk Mitigations</u>.

- Verification is the process of identifying and producing verifiable and measurable evidence for ensuring that the respective mitigation measures adequately support the documented reduction of ground safety risk to the public and property.
- Where possible, the FAA expects verification of mitigation measures utilizing existing industry standards.
- Essential information for verification includes:
  - Identification of specific method(s) used to verify the mitigation measure;
  - Identification of specific evidence to be produced; and
  - Indication of closure based on successful completion of specified method with production of adequate, verifiable, and measurable evidence.

Identify Verifications with Traceability to Mitigations (e)

Validate Mitigations and Verifications (e)

Validate Compliance with Acceptable Criteria (c)

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.6: Validation and Verification.

Verification Methods.

The FAA encourages discussion on proposed verification methods early in the licensing process. Four acceptable methods of verifying safety measures include:

- Analysis – Technical or mathematical evaluation, mathematical models, simulations, algorithms, and circuit diagrams.
- Component, subsystem, or system test – Actual operation to evaluate performance of system elements during ambient conditions or in operational environments at or above expected levels to measure safety margins. These tests include functional tests and environmental tests.
- Demonstration – Actual operation of the system or subsystem under specified scenarios, often used to verify reliability, transportability, maintainability, serviceability, and human engineering factors.
- Inspection – Physical examination of hardware, software, or documentation to verify compliance of the feature with predetermined criteria.

Identify Verifications with Traceability to Mitigations (e)

Validate Mitigations and Verifications (e)

Validate Compliance with Acceptable Criteria (c)

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.6: Validation and Verification.

<u>Verification Artifacts</u>.

- Per § 450.185(e), verification evidence must be documented and demonstrate that the risk elimination and mitigation measures achieve the risk level of paragraph § 450.185(c).
- Documented evidence can include design analyses, test data, inspection reports).
- Ideally, all mitigation measures should be validated and verified by the time of application submittal. The FAA recognizes that applicants may not have the ability to verify all mitigations prior to submission of an application.
- In those instances, an acceptable verification closure strategy should be documented with expected completion dates (which must be closed prior to licensed operation pursuant to any relevant terms and conditions of the license).
- This strategy should be provided to the FAA with adequate time to review the closure status of verification evidence prior to the initiation of the applicable licensed activity.

Identify Verifications with Traceability to Mitigations (e)

Validate Mitigations and Verifications (e)

Validate Compliance with Acceptable Criteria (c)

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.6: Validation and Verification.

Verification Traceability.

- Traceability ensures proper application of verifications for § 450.185(e) and should be demonstrated from:
  1) Subsystem and operator failures to their causes to respective mitigations to adequate verifications;
  2) Subsystem and operator failures to respective ground safety hazards to the public and property at the integrated system and operation level;
  3) Subsystem and operator level risk assessment to integrated system and operation level risk assessment; and
  4) Ground safety hazards to the public and property at the integrated system and operation level to their respective mitigations to adequate verifications.

Identify Verifications with Traceability to Mitigations (e)

Validate Mitigations and Verifications (e)

Validate Compliance with Acceptable Criteria (c)

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.6: Validation and Verification.

<u>Iterative Approach of Validation and Verification</u>.

- The V&V process is a comprehensive, closed-looped, iterative process to be used in all phases of the lifecycle of a launch or reentry system.
- Any mitigation that fails V&V cannot be relied on for elimination or reduction of ground safety risks to the public and property.

Identify Verifications with Traceability to Mitigations (e)

Validate Mitigations and Verifications (e)

Validate Compliance with Acceptable Criteria (c)

AC 450.179-1: Ground Safety

Top-Level Operation [Pad Servicing - TBD]

Next-Level Operation [Fuel Servicing - TBD]

Subsystem and Operator Level											Integrated System and Operation Level[1]						
Subsystem	Failure Description and End Effect	Component(s) / Item(s)	IDs	Possible Cause(s)	Risk Before Mitigation Measures			Risk Elimination / Mitigation Measures	Risk After Mitigation Measures			Verification Evidence	Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1]			Verification Evidence[1]
					L	S	R		L	S	R				L	S	R	
Fuel Servicing Ground Support Equipment	Fuel Servicing Ground Support Equipment[Function TBD] during [Operations Phase(s) TBD] fails [Failure TBD], possibly resulting in fire/ explosion [End Effect TBD]	Local Processor	Functional Failure ID; Fault Tree ID	**C1** TBD **C2** TBD **C3**, and so on…	Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of **C1** [design, test, manufacturing process, etc.] **C1.M2**, and so on… **C2.M1** – Specific to mitigation of **C2** [design, test, manufacturing process, etc.] **C2.M2**, and so on… **C3.M1** – and so on	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on… **C2.M1.V1** – Documented evidence specific to performed **C2.M1** mitigation **C2.M1.V2**, and so on… **C2.M2.V1**, and so on… **C3.M1.V1** – and so on…	**H1** Fire/Explosion **H2** Toxic Release **H3**, and so on…	**H1.M1** - Specific to mitigation of **H1** [Clear areas, operational restrictions, etc…] **H1.M2**, and so on… **H2.M1** - Specific to mitigation of **H2** [Clear areas, operational restrictions, etc…] **H2.M2**, and so on… **H3.M1** - and so on…	TBD	TBD	TBD	**H1.M1.V1** – Documented evidence specific to **H1.M1** mitigation **H1.M1.V2**, and so on… **H1.M2.V1**, and so on… **H2.M1.V1** – Documented evidence specific to **H2.M1** mitigation **H2.M1.V2**, and so on… **H2.M2.V1**, and so on… **H3.M1.V1** – and so on…
Human Systems Integration	[Basic Event TBD] during [Operations Phase(s) TBD] possibly results in fire/ explosion [Top-Level TBD]	N/A	Human Error Assessment ID; Fault Tree ID	**C1** TBD **C2** TBD **C3**, and so on…	Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of **C1** [design, procedures, training etc.] **C1.M2**, and so on **C2.M1** – Specific to mitigation of **C2** [design, procedures, training etc.] **C2.M2**, and so on… **C3.M1** – and so on	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on… **C2.M1.V1** – Documented evidence specific to performed **C2.M1** mitigation **C2.M1.V2**, and so on… **C2.M2.V1**, and so on… **C3.M1.V1** – and so on…							

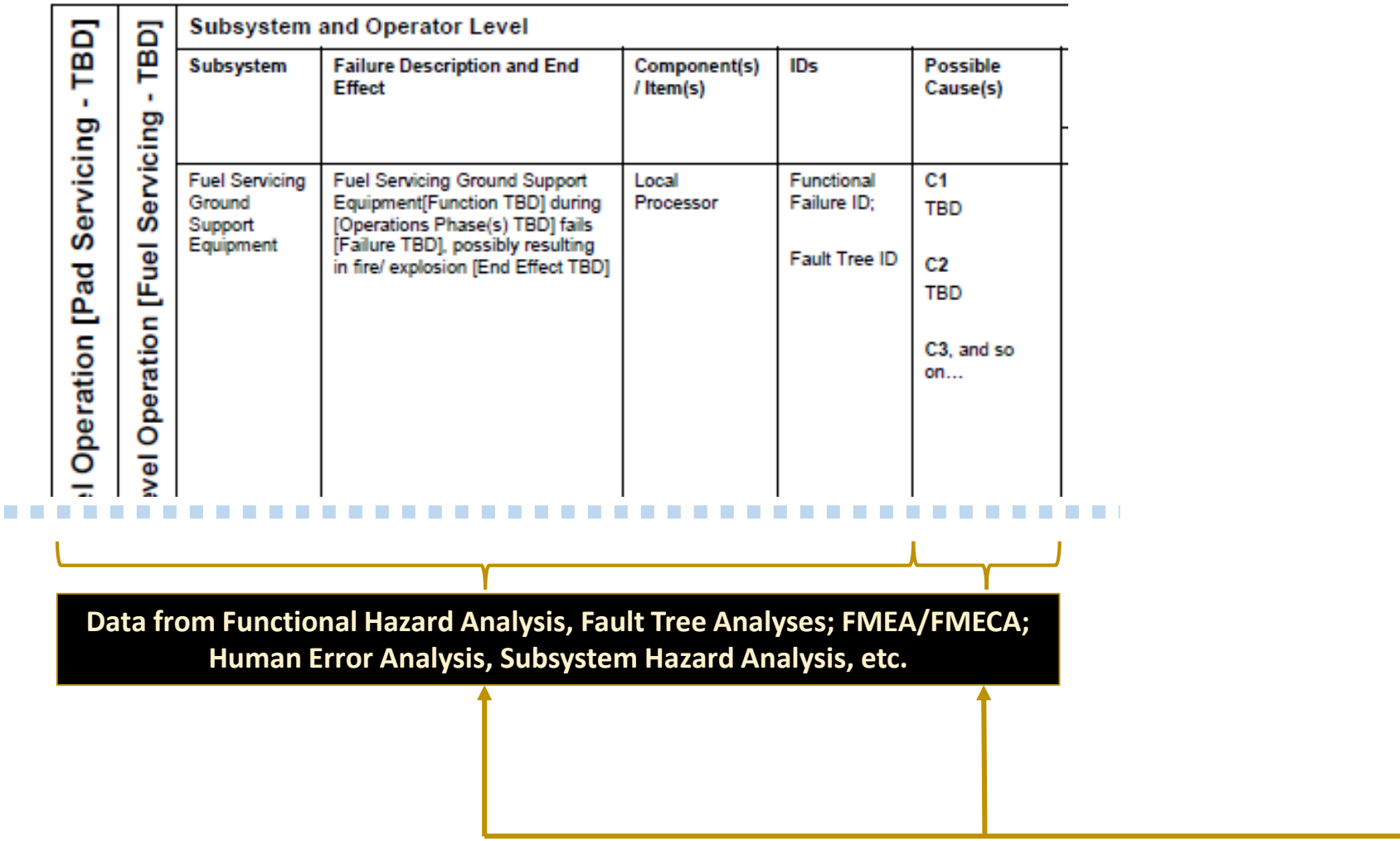
Data from Functional Hazard Analysis, Fault Tree Analyses; FMEA/FMECA; Human Error Analysis, Subsystem Hazard Analysis, etc.

Identify/Verify mitigations to specific causes of functional failures at the subsystem/operator level (e.g., design, manufacturing, etc.)

Identify/Verify specific system/operation mitigations for residual ground safety risk of public safety hazards (e.g., FSS, ops restrictions, etc.)

Traceability

AC 450.179-1: Ground Safety



AC 450.179-1: Ground Safety

Risk Before Mitigation Measures			Risk Elimination / Mitigation Measures	Risk After Mitigation Measures			Verification Evidence
L	S	R		L	S	R	
Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of **C1** [design, test, manufacturing process, etc.] **C1.M2**, and so on…	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on…
			C2.M1 – Specific to mitigation of **C2** [design, test, manufacturing process, etc.]				**C2.M1.V1** – Documented evidence specific to performed **C2.M1** mitigation

Identify/Verify mitigations to specific causes of functional failures at the subsystem/operator level (e.g., design, test, procedures, etc.)

AC 450.179-1: Ground Safety

Integrated System and Operation Level[1]					
Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1]			Verification Evidence[1]
		L	S	R	
H1 Fire/Explosion H2 Toxic Release H3, and so on…	H1.M1 - Specific to mitigation of H1 [Clear areas, operational restrictions, etc…] H1.M2, and so on…	TBD	TBD	TBD	H1.M1.V1 – Documented evidence specific to H1.M1 mitigation H1.M1.V2, and so on… H1.M2.V1, and so on…

Identify/Verify specific system/operation mitigations for residual ground safety risk of public safety hazards (e.g., clear areas, ops restrictions, etc.)

Traceability

AC 450.179-1: Ground Safety

SECTION 10.0: GROUND HAZARD ANALYSIS.

Section 10.7: Identifying New Hazards and Updating the Ground HA.

- Data gained during design, manufacture, test, and operation, including the discovery of anomalies and faults, usually impacts a GHA.
- Necessary data should be identified, and approaches should be implemented, to detect anomalies and failures in order to improve the GHA.
- Additionally, information gained during assembly and operation of components, subsystems, and next-level systems contributes to the further understanding of the overall integrated system and operation and may lead to additional updates to the GHA.
- A process should be implemented to update the GHA and final ground safety risk assessment to reflect knowledge gained during the life of the integrated system and operation.

AC 450.179-1: Ground Safety

Discussion

Floor open for questions/comments
Either verbally or via comments

AC 450.179-1: Ground Safety

SECTION 11.0: TOXIC HAZARDS MITIGATION FOR GROUND OPERATIONS.

- In accordance with § 450.187(a)(1), ground safety hazards to the public associated with the use of toxic propellants or other toxic chemical must be mitigated.
- In accordance with § 450.187, an operator must:
  - Conduct a TRHA per § 450.187(c);
  - Manage the risk of casualties that could arise from the exposure to a toxic release, either per toxic containment of § 450.187(d) or per toxic risk assessment of § 450.187(e); and
  - Establish ground hazard controls based on the results of its TRHA and toxic containment or toxic risk assessment, per § 450.187(b)(3).
- Section 11 of AC 450.139-1, *Toxic Release Hazard Analysis*, provides additional guidance specific to mitigating toxic hazards during licensed ground operations.

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.1: General.

- In addition to an operator's specific hazard controls derived by an operator's GHA and TRHA, an operator must comply with § 450.189(b) through (e).
- Implementation of the following prescribed hazard controls should be verified and validated to demonstrate compliance.

Section 12.2: Protection of Public on the Site.

- The operator should be cognizant of all members of the public who enter an area under the operator's control.

Limiting Access.

- In accordance with § 450.189(b), the operator must document, distribute, and adhere to an acceptable process to protect members of the public from ground safety hazards.

- The public access control (no entry, limited entry, etc.) should be coordinated with security, other site coordinators, management, and any other potential areas of concern.

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.2: Protection of Public on the Site.

Limiting Access.

The process to protect the public should include at a minimum:

1) Access requirements (including approvals required);

2) Sign-In / Sign-Out documentation (POC, location, duration, etc.);

3) Required escorting;

4) Definition of applicable clear zones;

5) Required personnel protection equipment (PPE) (ear plugs, mask, hard hat, steel toed shoes, etc.); and

6) Advise the public on site of the potential hazards.

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.2: Protection of Public on the Site.

Notification.

- The process should also document the public's notification of the applicable policies, procedures, and hazard controls required for entry into the operator's area.

  1) Safety Briefing (including hazard areas/clear zones):

  2) Emergency phone numbers and procedures;

  3) Departing or evacuating (e.g., during emergencies, launch aborts, mishaps, etc.); and

  4) Violation policy/reprimands.

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.3: Countdown Abort.

- In accordance with § 450.189(c), procedures to be performed must be established, maintained throughout the life cycle, and validated to ensure the control of ground safety hazards to the public and property and to return the integrated system and site facilities to a safe condition after a countdown abort or delay in launch.
- Thus, the known safe state for the integrated system and the launch site must be defined in the event of a countdown abort or recycle operation.
- The GHA should consider and assess a launch countdown abort or recycle operation.

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.3: Countdown Abort.

- Specifically, in accordance with § 450.189(a) through (c), the procedures must:

  1) Ensure the vehicle and payload are in a safe configuration;

  2) Prohibit entry of the public into any identified hazard areas until the site is returned to a safe condition; and

  3) Maintain and verify that any flight safety system remains operational until verification that the launch vehicle does not represent a risk of inadvertent flight. The timing of safing the flight safety system should be fed directly into the timeline for return to safe condition state and determining an “all clear.”

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.4: Fire Suppression.

- In accordance with § 450 .189(d), the operator must have in place reasonable precautions for reporting and controlling any fires.
- Reporting procedures for a fire should be defined, and documented, as well as coordinated with the site operator.
- Meeting industry standards and fire codes are expected. Reasonable precautions include: documentation of emergency fire phone number, fire suppression devices, evacuation procedures, notification to nearby facilities, and isolation measures if available.

Note: Fire suppression chemicals should be assessed in the TRHA.

AC 450.179-1: Ground Safety

SECTION 12.0: GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

Section 12.5: Emergency Procedures.

- In accordance with § 450.189(e), applicant must have general emergency procedures to protect the public and property that are not covered by a § 450.173 mishap plan.
- Emergency procedures should exist for a fire event, a toxic release event, and any other event that may create a hazard to the public, including weather conditions and any unique emergency procedures identified by the GHA and TRHA.
- Mishap reporting, response, and investigation requirements are documented in § 450.173. Additional information for mishap reporting can be found in AC 450.173-1, *Mishap Reporting, Response, and Investigation*.

SECTION 13.0: APPLICATION REQUIREMENTS.

If required by § 450.179, an applicant must provide documentation and data, as outlined in §§ 450.181(c), 450.183(b), 450.185(f), 450.187(f), and 450.189(f).

AC 450.179-1: Ground Safety Appendix A

Table A-1 conveys the types of data that should be provided by an acceptable system safety analysis, including a method for traceability between all aspects of ground safety hazards to the public and property. It is intended as a guide to show what information should be provided within a GHA. It also shows how logical tracking for each item can be used to show the relationships between the different pieces of information. A hazard analysis format conveying the information of **Table A-1**, such as similar tables or traditional worksheets, should be utilized.

Table A-1: System Safety Template for § 450.185 Ground Hazard Analysis

Top-Level Operation [Pad Servicing - TBD]	Next-Level Operation [Fuel Servicing - TBD]	Subsystem and Operator Level											Integrated System and Operation Level[1]				
		Subsystem	Failure Description and End Effect	Component(s) / Item(s)	IDs	Possible Cause(s)	Risk Before Mitigation Measures L	S	R	Risk Elimination / Mitigation Measures	Risk After Mitigation Measures L	S	R	Verification Evidence	Hazard to Public[1]	Risk Elimination / Mitigation Measures[1]	Risk After Mitigation Measures[1] L	S	R	Verification Evidence[1]
		Fuel Servicing Ground Support Equipment	Fuel Servicing Ground Support Equipment[Function TBD] during [Operations Phase(s) TBD] fails [Failure TBD], possibly resulting in fire/ explosion [End Effect TBD]	Local Processor	Functional Failure ID; Fault Tree ID	**C1** TBD **C2** TBD **C3**, and so on…	Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of **C1** [design, test, manufacturing process, etc.] **C1.M2**, and so on… **C2.M1** – Specific to mitigation of **C2** [design, test, manufacturing process, etc.] **C2.M2**, and so on… **C3.M1** – and so on	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on… **C2.M1.V1** – Documented evidence specific to performed **C2.M1** mitigation **C2.M1.V2**, and so on… **C2.M2.V1**, and so on… **C3.M1.V1** – and so on…	**H1** Fire/Explosion **H2** Toxic Release **H3**, and so on…	**H1.M1** - Specific to mitigation of **H1** [Clear areas, operational restrictions, etc…] **H1.M2**, and so on… **H2.M1** - Specific to mitigation of **H2** [Clear areas, operational restrictions, etc…] **H2.M2**, and so on… **H3.M1** - and so on…	TBD	TBD	TBD	**H1.M1.V1** – Documented evidence specific to **H1.M1** mitigation **H1.M1.V2**, and so on… **H1.M2.V1**, and so on… **H2.M1.V1** – Documented evidence specific to **H2.M1** mitigation **H2.M1.V2**, and so on… **H2.M2.V1**, and so on… **H3.M1.V1** – and so on…
		Human Systems Integration	[Basic Event TBD] during [Operations Phase(s) TBD] possibly results in fire/ explosion [Top-Level TBD]	N/A	Human Error Assessment ID; Fault Tree ID	**C1** TBD **C2** TBD **C3**, and so on…	Initial or no data	TBD	TBD	**C1.M1** – Specific to mitigation of **C1** [design, procedures, training etc.] **C1.M2**, and so on **C2.M1** – Specific to mitigation of **C2** [design, procedures, training etc.] **C2.M2**, and so on… **C3.M1** – and so on	TBD	TBD	TBD	**C1.M1.V1** – Documented evidence specific to performed **C1.M1** mitigation **C1.M1.V2**, and so on… **C1.M2.V1**, and so on… **C2.M1.V1** – Documented evidence specific to performed **C2.M1** mitigation **C2.M1.V2**, and so on… **C2.M2.V1**, and so on… **C3.M1.V1** – and so on…							

NOTES:
1 – "Integrated System and Operation Level" may be captured as shown or in a separate table or spreadsheet with traceability to "Subsystem and Operator Level"
2 – "C1.M1.V1" is only an example. Key is to demonstrate traceability by a suitable method
3 – L = Likelihood; S = Severity; R = Risk
4 – Typically within system safety and ground safety, Likelihood (L) = Probability (P); Severity (S) = Consequence (C); L & S = R

AC 450.179-1: Ground Safety

Discussion

Floor open for questions/comments
Either verbally or via comments

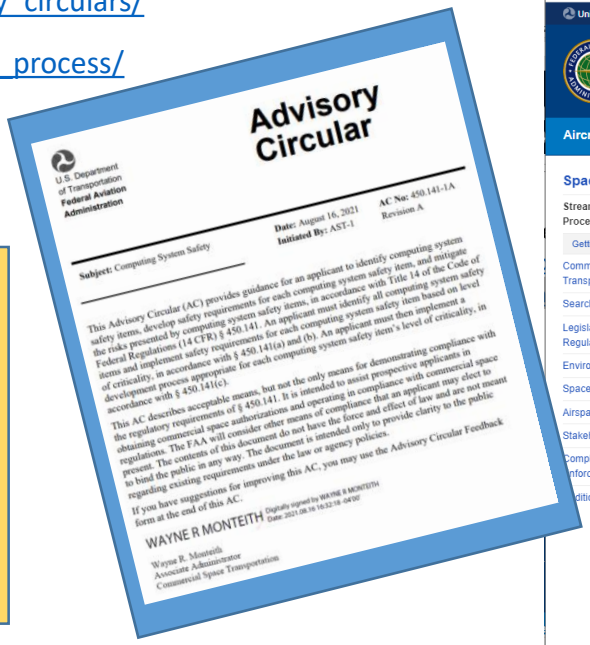
Where to Find Part 450 ACs

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

- Date/Time: November 18 @ 1300 Eastern time
  AC 450.173-1 Mishap Plan-Response, Reporting, and Investigation Requirements