U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Ground Safety

Date: 09/22/2021
Initiated By: AST-1

AC No: 450.179-1

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 acceptable means of compliance with §§ 450.179, 450.181, 450.183, 450.185, 450.187, and 450.189. Launch and reentry license applicants may use this AC to guide their internal processes or format their license applications, or both.

This AC describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations. It is intended to assist prospective applicants in obtaining commercial space authorizations and operating in compliance with commercial space regulations. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. The document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

If you have suggestions for improving this AC, you may use the Advisory Circular Feedback form at the end of this AC.

WAYNE R MONTEITH Digitally signed by WAYNE R MONTEITH
Date: 2021.09.22 10:08:32 -04'00'

Wayne R. Monteith
Associate Administrator
Commercial Space Transportation

Contents

Paragraph **Page**

1 PURPOSE.

This Advisory Circular (AC) provides guidance and a comprehensive method for performing a ground safety analysis in accordance with title 14, Code of Federal Regulations (14 CFR) §§ 450.179, 450.181, 450.183, 450.185, and 450.189. This AC does not constitute a regulation and does not contain requirements but is intended to assist prospective applicants in obtaining commercial space licenses and ensure they are operating in compliance with commercial space regulations.

1.1 Level of Imperatives.

This AC presents one, but not the only, acceptable means of compliance with the associated regulatory requirements. The Federal Aviation Administration (FAA) will consider other means of compliance that an applicant may elect to present. Throughout this document, the word "must" characterizes statements that directly flow 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 be justified and approved as an alternative means of compliance. The word "may" describes variations or alternatives allowed within the accepted means of compliance set forth in this AC. In general, these alternative approaches can be used only under certain situations that do not compromise safety.

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, *Launch and Reentry License Requirements*. 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 will not be relied upon by the FAA 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. This AC describes acceptable means, but not the only means, for demonstrating compliance with the applicable 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 Statute.

- 51 United States Code (U.S.C.) Subtitle V, Chapter 509.

3.2 Related Regulations.

The following regulations from titles 14 of the CFR must be accounted for when showing compliance with 14 CFR § 450.179. 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 401.7, *Definitions*.
- Section 420.63, *Explosive siting.*
- Section 420.65, *Separation distance requirements for handling division 1.1 and 1.3 explosives*.
- Section 420.66, *Separation distance requirements for storage of hydrogen peroxide, hydrazine, and liquid hydrogen and any incompatible energetic liquids stored within an intraline distance*.
- Section 420.67, *Separation distance requirements for handling incompatible energetic liquids that are co-located*.
- Section 420.69, *Separation distance requirements for co-location of division 1.1 and 1.3 explosives with liquid propellants*.
- Section 420.70, *Separation distance measurement requirements*.
- Section 450.35, *Means of compliance*.
- Section 450.103, *System safety program.*
- Section 450.107, *Hazard control strategies*.
- Section 450.139, *Toxic hazards for flight*.
- Section 450.141, *Computing systems*.
- Section 450.147, *Agreements*.
- Section 450.173, *Mishap plan–reporting, response, and investigation requirements*.
- 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, *Toxic hazards mitigation for ground operations*.
- Section 450.189, *Ground safety prescribed hazard controls*.

3.3 Related FAA Advisory Circulars.

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

- AC 413.5-1, *Pre-Application Consultation*, when published.
- AC 450.103-1, *System Safety Program*, dated September 2021.
- AC 450.107-1, *Hazard Control Strategies*, dated July 20, 2021.
- AC 450.109-1, *Flight Hazard Analysis*, dated August 5, 2021.
- AC 450.139-1, *Toxic Hazards for Flight*, when published.
- AC 450.141-1A, *Computing Systems Safety*, dated August 16, 2021.
- AC 450.173-1, *Mishap Reporting, Response, and Investigation*, dated August 12, 2021.

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

3.4 Government Guidance Documents.

- MIL-STD-882E, Department of Defense Standard Practice, *System Safety*, dated May 11, 2012, https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=36027.
- *Memorandum of Agreement between the Department of the Air Force and the Federal Aviation Administration for Launch and Reentry Activity on Department of the Air Force Ranges and Installations Agreement Number* FAA-DAF-SLR-2021, dated June 15, 2021, https://www.faa.gov/space/legislation_regulation_guidance/media/MOA_DAF_FAA_Launch_and_Reentry_Activity_FINAL_SIGNED_6_15_2021.pdf.

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

4 DEFINITION OF TERMS.

For this AC, the following terms and definitions apply:

4.1 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).

4.2 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.

4.3 **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.

5 **ACRONYMS.**

AC – Advisory Circular

ESP – Explosives Site Plan

FAA – Federal Aviation Administration

FMEA – Failure Modes and Effects Analysis

FTA – Fault Tree Analysis

GHA – Ground Hazard Analysis

HEA – Human Error Analysis

MOA – Memorandum of Agreement

O&SHA – Operating and Support Hazard Analysis

QD – Quantity-distance

SSP – System Safety Program

TBD – To be Determined

TRHA – Toxic Release Hazard Analysis

U.S.C. – United States Code

V&V – Validation and Verification

6 OVERVIEW.

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 associated with: preparing a launch or reentry vehicle for flight; returning a launch or reentry vehicle to a safe configuration after landing or countdown abort attempt; and performing launch or reentry site operations required to return the site to a safe, known, expected configuration. Thus, the operator's ground safety program is responsible for 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.

6.2 Ground Safety Methodology.

Ground Safety regulations, as outlined in §§ 450.179 through 450.189, cover many aspects, including: launch and reentry site coordination, explosive site planning, documenting a ground hazard analysis (GHA), conducting a toxic release hazard analysis (TRHA), and implementing prescribed hazard controls. The documented system safety program (SSP) should define the ground safety methodology to show compliance with these regulations, per guidance of AC 450.103-1, *System Safety Program*.

6.3 Aspects of Ground Hazard Analysis.

A 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 and should be performed similarly 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 performed and documented as part of an application per § 450.185(f)(3) and continue to be maintained throughout the lifecycle of the launch or reentry system, in accordance with § 450.185. 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)].

Chapter 10 of this AC further details aspects of a GHA.

6.4 Formal Traceability of Ground Safety Hazards.

Formal tracking methods should be established to show direct connections between all aspects of ground safety hazards to the public and property, source, causes, mitigations, and verification evidence. Hazard tracking systems may contain all the necessary data but do not typically show these direct connections. Table A-1 of Appendix A of this AC conveys the types of information that an applicant should provide to demonstrate traceability.

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(s) 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. The analytical method and level of detail in the analysis should correspond to the complexity of the software and computing system, intricacy of the operations, and scope of the program. Also, software hazard analyses should consider a range of potential error conditions.

7 GENERAL GROUND SAFETY.

7.1 General Guidance.

As part of the license application process, a licensed operator, hereafter referred to as "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. To protect public and property at a U.S. launch or reentry site, the identification of hazardous ground operations and the risks associated with them must be documented in accordance with § 450.185. 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.

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.

7.2.1 Memorandums of Agreement with Approved Launch and Reentry Sites.

When the FAA finds that a site meets the conditions in § 450.179(b), the FAA develops an MOA with the approved site and publishes the MOA on the FAA's website at https://www.faa.gov/space/legislation_regulation_guidance/. If these conditions are met, then the operator can seek FAA permission during pre-application consultation to comply only with the ground safety regulations imposed by the Federal site. The FAA will publish, maintain, and update the Federal launch and reentry site ground safety MOAs on its website.

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. Doing so facilitates a thorough identification and assessment of system and operational hazards to the public and property associated with licensed ground operations at the launch or reentry site. 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*.

8 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. 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*, the launch or reentry operator must coordinate with the site operator to ensure public safety and comply with § 450.181(a).

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. 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.

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.

8.3 Ground Hazard Area Designation and Coordination.

The site coordination activity should include the identification of the ground operation hazardous processes, their potential exposure interval, and their mitigations. The impacts to other sites should be documented and evaluated as changes are made. The ESP, as discussed in greater detail in Chapter 9 of this AC, provides clear zones necessary to provide public protection from potential hazards. If the zones extend into other sites, the operator should adequately convey this information to the site operator for their required action. 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.

8.3.1 In addition, coordination with other adjacent sites should include the examination of concurrent hazardous operations such that all mitigation procedures (from GHA, TRHA, and prescribed hazard mitigations) are evaluated for effectiveness. If the coordination efforts indicate a hazardous condition is not mitigated by the current controls, adequate mitigation(s) should be provided, or the launch or reentry event will be rescheduled.

8.3.2 Operators and site operators should ensure ground hazard areas remain controlled during a mishap according to documented emergency procedures defined in § 450.189(e).

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.

8.4.1 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 ground activities at the launch or reentry site; and
- Responding to mishap reports for ground activities at the launch or reentry site.

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

9 **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.

10 GROUND HAZARD ANALYSIS.

In accordance with § 450.185, the documented SSP must specify that, a GHA 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. In its analysis, 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.

10.1 Identifying 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)].

10.1.1 Identification and Decomposition of All System and Operation Failures.

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

10.1.1.1 Functional Hazard Analysis for Flight System – A starting point for identifying flight system hazards is a functional hazard analysis. A functional hazard analysis is required for a flight system per § 450.107(b) and AC 450.107-1, *Hazard Control Strategies Determination*, provides guidance on conducting the analysis for phases of flight, which can be modified to account for ground phases. A functional hazard analysis is used to analyze system functions associated with the proposed operation. 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 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 or predetermined mitigation.

10.1.1.2 Functional Hazard Analysis for Ground System – Similarly to a flight system, a starting point for identifying ground system hazards may utilize a functional hazard analysis. The guidance of AC 450.107-1, *Hazard Control Strategies Determination,* on conducting a functional hazard analysis for a flight system during phases of flight, can be modified to

account for identifying functional failures of a ground system during phases of ground operations.

10.1.1.3 Fault Tree Analysis (FTA) – A reliability engineering analysis that uses a logic diagram to identify and map causes of top-level events. Additionally, an FTA allows for: quantification of system failure probability, determination of fault tolerance, identification of common causes and single point failures, etc.

10.1.1.4 Failure Modes and Effects Analysis (FMEA) – A reliability engineering analysis used to identify low-level component failures and their causes and assess their effects on higher-level systems.

10.1.1.5 Human Error Analysis (HEA) – A systematic method of considering the possible errors and other human failures that may occur when performing a task.

10.1.2 Documenting a Ground Hazard Analysis.

GHAs are typically documented by identifying an assessing the hazards introduced by ground safety operational and support activities, systems, processes, and equipment similar to those outlined in Task 206, *Operating and Support Hazard Analysis* of MIL-STD 882. An example of how system requirement risks are mitigated and documented is found in Table A–1 System Safety Template of Appendix A. An O&SHA analyzes the processes and procedures of the entire operation while considering the source data discussed in the section above.

10.1.2.1 Thus, the O&SHA allows for detailing all ground safety hazards due to potential system functional failures and operation failures associated with ground operations involving ground and flight systems.

10.1.2.2 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.

10.1.3 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.

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.

10.2.1 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). The risk assessment with respect to ground safety hazards to the public and property will utilize qualitative statements. AC 450.103-1, *System Safety Program*, provides guidance on severity categories and likelihood levels in Table A-1 of Appendix A.

10.2.2 Utilizing a Systematic Assessment Process.

10.2.2.1 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. It is common system safety practice to assess risk prior to the implementation of a mitigation in order to deliberately design a mitigation strategy for each hazard. Pre-mitigation risk assessment also facilitates greater traceability from hazard cause through mitigation and verification. The FAA recognizes that some operators will not utilize a pre-mitigation risk assessment as is common in rapid development and experimental programs. 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 posed during licensed ground operations to demonstrate compliance with § 450.185(c).

10.2.2.2 Additionally to ensure proper mitigation of system safety hazards to the public for § 450.185(d), 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.

10.2.3 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.

10.3 **Risk Acceptability Criteria.**

10.3.1 Developing Risk Acceptance Criteria.

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 and the rationale for acceptance should be documented.

10.3.2 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 Program*, 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.

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).

10.4.1 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. For example, a fill/drain valve mechanical failure may have a high probability of significant leakage resulting in a toxic release. The hazard risk was determined to have a consequence of "Catastrophic" and a likelihood of "Occasional." That valve was replaced with a more reliable valve as a mitigation. The mitigation is determined to change the likelihood to "Extremely Remote," but the new valve cannot impact the consequence of the failure, which remains "Catastrophic."

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.

10.5.1 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.

10.5.2 System Safety Design Order of Precedence.

In order to mitigate risk from system 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.

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).

10.6.1 Validating Risk Mitigations.

The validation process evaluates that each mitigation measure and respective verification is well understood and operationally and technically feasible. In accordance with § 450.185(e), validation evidence must be documented and it must demonstrate that the risk elimination and mitigation measures achieve the risk acceptability criteria defined in paragraph § 450.185(c). This documented evidence [e.g., Validation and Verification (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. To do this, the validation effort ensures that each mitigation and verification is unambiguous, correct, complete, and consistent.

10.6.2 Verifying Risk Mitigations.

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.

10.6.2.1 Verification Artifacts.

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). This documented evidence (e.g., design analyses, test data, inspection reports) must be provided to the FAA in accordance with § 450.185(f)(3). 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.

10.6.2.2 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.

10.6.2.3 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.

10.6.3 Iterative Approach of Validation and Verification.

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.

10.7 **Identifying New Hazards and Updating the Ground Hazard Analysis.**

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.

11 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.

12 GROUND SAFETY PRESCRIBED HAZARD CONTROLS.

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 with § 450.189(b) through (e).

12.2 Protection of Public on the Site.

An operator is required to document how it protects members of the public who enter areas that are under their control, in accordance with § 450.189(b).

12.2.1 Limiting Access.

In order to protect the public, the operator should be cognizant of all members of the public who enter an area under the operator's control. 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. An applicant must submit the process for protecting members of the public who enter any area under the control of a launch or reentry operator in accordance with § 450.189(f). 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.

12.2.2 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. This includes the following:

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.

12.3 **Countdown Abort.**

The GHA should consider and assess a launch countdown abort or recycle operation. 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. There may be several procedures required depending on the phase of the integrated system operation at the time the event occurs. 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."

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. Reasonable precautions include: documentation of emergency fire phone number, fire suppression devices, evacuation procedures, notification to nearby facilities, and isolation measures if available. Meeting industry standards and fire codes are expected.

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

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.

12.5.1 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*.

13 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).

Appendix A

A.1 SYSTEM SAFETY TEMPLATE FOR § 450.185 GROUND HAZARD ANALYSIS.

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**			**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…	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…	**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…
										C2.M1 – Specific to mitigation of **C2** [design, test, manufacturing process, etc.] **C2.M2**, 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…		**H2.M1** - Specific to mitigation of **H2** [Clear areas, operational restrictions, etc…] **H2.M2,** 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…
										C3.M1 – and so on				**C3.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	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…		**H3.M1** - and so on…				**H3.M1.V1** – and so on…
										C2.M1 – Specific to mitigation of **C2** [design, procedures, training etc.] **C2.M2**, 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 – 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

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:

☐ An error (procedural or typographical) has been noted in paragraph Click here to enter text. on page Click here to enter text..

☐ Recommend paragraph Click here to enter text. on page Click here to enter text. be changed as follows:

Click here to enter text.

☐ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

Click here to enter text.

☐ Other comments:

Click here to enter text.

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____