U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: HAZARD ANALYSES FOR THE LAUNCH OR REENTRY OF A REUSABLE SUBORBITAL ROCKET UNDER AN EXPERIMENTAL PERMIT

Date: April 20, 2007
Initiated by: AST-1

AC No: 437.55-1
Change:

1.0 PURPOSE

a. This Advisory Circular (AC) provides guidance for applying a systematic and logical hazard analysis to the identification, analysis, and control of public safety hazards and risks associated with the launch and reentry of a reusable suborbital rocket under an experimental permit. The approach described here provides an acceptable approach to a hazard analysis methodology. Other approaches that fulfill regulatory objectives may be acceptable to the Federal Aviation Administration (FAA).

b. This AC is not, in itself, mandatory and does not constitute a regulation. It is issued to describe an acceptable means, but not the only means, for demonstrating compliance with certain requirements associated with the launch or reentry of a reusable suborbital rocket.

c. This AC affects any entity that intends to obtain an experimental permit to launch or reenter a reusable suborbital rocket.

2.0 APPLICABLE REGULATIONS AND RELATED DOCUMENTS

a. Regulations

14 CFR III

Part 401, Organization and Definitions

Part 437, Experimental Permits for Reusable Suborbital Rockets

b. FAA Advisory Circulars and Guidance Documents (available through the FAA web site, www.faa.gov)

AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes, March 12, 1999.

AC 431.35-2A, Reusable Launch and Reentry Vehicle System Safety Process, July 20, 2005.

FAA System Safety Handbook, December 30, 2000.

Guide to Reusable Launch Vehicle Safety Validation and Verification Planning, Version 1.0, September 2003.

Guide to Commercial Reusable Launch Vehicle Operations and Maintenance, Version 1.0, March 2005.

Guide to Reusable Launch and Reentry Vehicle Reliability Analysis, Version 1.0, April 2005.

Guide to Reusable Launch and Reentry Vehicle Software and Computing System Safety, Version 1.0, July 2006.

Shappell, Scott A. and Wiegmann, Douglas A., *The Human Factors Analysis and Classification System – HFACS*, Final Report. DOT/FAA/AM-00/7, Federal Aviation Administration, Office of Aviation Medicine, Washington, DC, February 2000.

c. Industry and U.S. Military Documents

American Institute of Aeronautics and Astronautics, *Guide to the Identification of Safety-Critical Hardware Items for Reusable Launch Vehicle (RLV) Developers*, May 1, 2005.

Department of Defense, *Standard Practice for System Safety,* MIL-STD-882D, February 10, 2000.

3.0 ACRONYMS AND DEFINITIONS

3.1 Acronyms

a.	AC	Advisory Circular
b.	AST	Office of Commercial Space Transportation
c.	FAA	Federal Aviation Administration
d.	FHA	Functional Hazard Analysis
e.	FMEA	Failure Modes and Effects Analysis
f.	FMECA	Failure Modes, Effects, and Criticality Analysis
g.	FSS	Flight Safety System
h.	IIP	Instantaneous Impact Point
i.	PHA	Preliminary Hazard Analysis
j.	MIL-STD	Military Standard
k.	NASA	National Aeronautics and Space Administration
l.	R&D	Research and Development
m.	V&V	Validation and Verification

3.2 Definitions

a. **Anomaly.** A problem that occurs during verification or operation of a system, subsystem, process, facility, or support equipment.

b. **Failure Modes and Effects Analysis (FMEA).** System analysis by which each potential failure in a system is analyzed to determine the effects on the system and to classify each potential failure according to its severity and likelihood.

c. **Failure Modes, Effects, and Criticality Analysis (FMECA).** Failure Modes and Effects Analysis that includes the relative mission significance or criticality of all potential failure modes.

d. **Fault.** An anomalous change in state of an item that may warrant some type of corrective action to decrease risk.

e. **Flight Safety System (FSS).** The system that provides a means of control during flight for preventing a hazard from a launch or reentry vehicle, including any payload hazard, from reaching any populated or other protected area in the event of a launch or reentry vehicle failure. A flight safety system includes:

(1) All hardware and software used to protect the public in the event of a launch or reentry vehicle failure; and
(2) The functions of any flight safety crew.

f. **Functional Hazard Analysis (FHA).** Systematic, comprehensive examination of vehicle and system functions to identify potentially hazardous conditions that may arise as a result of an anomaly.

g. **Hazard.** Equipment, system, operation, or condition with an existing or potential condition that may result in loss or harm.

h. **Launch accident.**

(1) An event that causes a fatality or serious injury (as defined in 49 CFR 830.2) to any person who is not associated with the flight;

(2) An event that causes damage estimated to exceed $25,000 to property not associated with the flight that is not located at the launch site or designated recovery area;
(3) An unplanned event occurring during the flight of a launch vehicle resulting in the impact of a launch vehicle, its payload, or any component thereof:
(i) For an expendable launch vehicle, outside designated impact limit lines; and
(ii) For a reusable launch vehicle, outside a designated landing site;
(4) For a launch that takes place with a person on board, a fatality or serious injury to a space flight participant or crew member.

i. **Launch incident.** An unplanned event occurring during the flight of a launch vehicle, other than a launch accident, involving a malfunction of a flight safety system or safety-critical system, or a failure of the licensee's or permittee's safety organization, design, or operations.

j. **Mishap.** A launch or reentry accident, launch or reentry incident, launch site accident, failure to complete a launch or reentry as planned, or an unplanned event or series of events resulting in a fatality, serious injury, or greater than $25,000 worth of damage to the payload, launch or reentry vehicle, launch or reentry support facility, or government property located on the launch or reentry site.

k. **Preliminary Hazard Analysis (PHA).** Examination of a system or subsystem to identify and classify each potential hazard according to its severity and likelihood of occurrence and to develop mitigation measures to those hazards.

l. **Risk.** Measure that takes into consideration the likelihood of occurrence and the consequence of a hazard to people or property.

m. **Risk mitigation.** Process of reducing the likelihood of occurrence, severity of consequences, or both the likelihood and severity of a hazard to people or property.

n. **Safety critical.** Essential to safe performance or operation. A safety-critical system, subsystem, condition, event, operation, process, or item is one whose proper recognition, control, performance, or tolerance is essential to system operation such that it does not jeopardize public safety.

o. **Validation.** An evaluation to determine whether each safety measure derived from a system safety process is correct, complete, consistent, unambiguous, verifiable, and technically feasible. Validation is the process that ensures that the implemented safety measure is right.

p. **Verification.** An evaluation to determine whether safety measures derived from a system safety process are effective and have been properly implemented. Verification provides measurable evidence that a safety measure reduces risk to acceptable levels.

4.0 BACKGROUND

The FAA is responsible for regulating commercial space transportation operations to the extent necessary to ensure public health and safety and the safety of property. To fulfill its responsibilities, the FAA issues licenses for the launch or reentry of a launch or reentry vehicle or the operation of a launch or reentry site. In addition, the Commercial Space Launch Amendments Act of 2004 authorized the FAA to issue experimental permits for the launch or reentry of a developmental reusable suborbital rocket.

As part of the requirements for obtaining an experimental permit, § 437.55 requires an operator to perform a hazard analysis and provide the results to the FAA. A hazard analysis is a systematic process used to identify, characterize, and eliminate the potential for loss or harm from a reusable suborbital rocket and to reduce the associated risk to the public. In addition to meeting the requirements of this section, the hazard analysis can assist in identifying safety measures that help meet other experimental permit requirements.

While extremely important in creating a strong foundation for ensuring the safety of a system, a hazard analysis itself does not ensure public safety. Application of the hazard analysis approach in combination with operating area containment, operating requirements identified by regulation, and safety measures identified by the hazard analyses are all intended to help decrease the risk to the public to the levels defined by §437.55.

5.0 HAZARD ANALYSIS

Figure 1 shows a hazard analysis. This process is used to identify and characterize hazards, assess risks, identify risk reduction measures, and provide evidence that the risks have been reduced. The hazard analysis is iterative; for ease of discussion, this process is presented here in a linear, one-pass fashion. As the launch vehicle development

life cycle progresses, continuing to apply the process may identify additional hazards, risks, and mitigation measures.

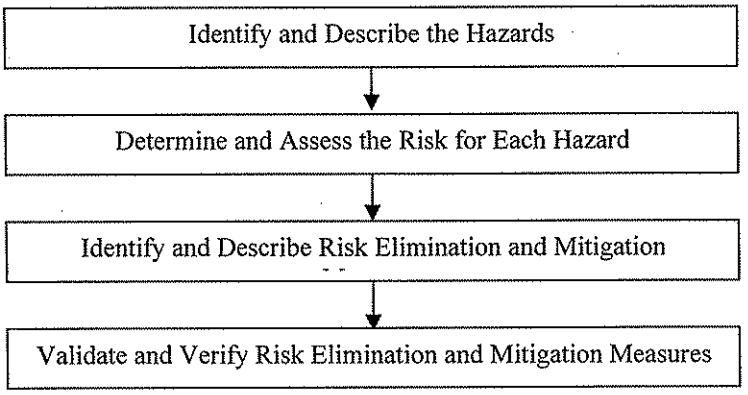


Figure 1. Hazard analysis.

a. Identify and Describe the Hazards

The first step in the hazard analysis is to identify and describe the hazards. An operator may identify hazards from a number of sources including the following:

- Examining similar systems,
- Reviewing system specifications,
- Reviewing industry standards and guidance documents,
- Reviewing system safety studies from other systems,
- Reviewing historical documents, and
- Brainstorming.

An operator should describe hazards in terms that identify each potential source of harm, the mechanism by which the harm may be caused, and the potential outcome if the harm were to remain unaddressed. For example, a potential source of harm could be a leak in a rocket engine fuel system line caused by a manufacturing defect, overpressure, or improper installation. The mechanism for harm could be fire resulting from that leak. The outcome could be loss of the vehicle. Examples of hazard descriptions are provided in the appendix.

A hazard analysis must address the following:

- Component, subsystem, or system failures and faults, including inherent process variability, such as a variation in the flow rate through a propellant feed system from flight to flight.
- Software and computing system errors, such as improper data, improper commands, or unexpected shutdown of the computing system.
- Environmental conditions, such as lightning, wind, or bird strikes.
- Human errors, including
    - decision errors, such as using flight controls at the wrong time;
    - skill-based errors, such as improperly following a procedure;
    - perceptual errors, such as spatial disorientation;
    - violations, such as a failure to adhere to abort procedures; and

- organizational and supervisory factors, such as poor scheduling, inadequate or non-existent training, inadequate communications, or inadequate resources.

- Design inadequacies, such as improper tolerances and clearances.
- Procedural deficiencies, including inadequate or non-existent procedures and documentation.

The AIAA *Guide to the Identification of Safety-Critical Hardware Items for Reusable Launch Vehicle (RLV) Developers* (2005) provides information on hardware hazards and mitigation approaches. Information on human error can be found in *The Human Factors Analysis and Classification System – HFACS* by Shappell and Wiegmann. Information on software and computing system safety can be found in FAA's *Guide to Reusable Launch and Reentry Vehicle Software and Computing System Safety (2006)*.

Note that hazards may exist in some phases of flight but not in others. For example, a hazard related to leaking fuel may not exist later in flight after all the fuel has been consumed, vented, or otherwise expended. For this reason, the launch vehicle operator should determine the phases of flight where the hazards exist and only analyze those hazards for that phase.

b. Determine and Assess the Risk for Each Hazard

After hazards have been identified and described, an operator characterizes the risk by assigning qualitative severities and likelihoods to the hazards to characterize the risk. This characterization of risk is used to establish priorities for corrective action.

Examples of suggested qualitative severity and likelihood categories are provided in Tables 1 and 2. The severity and likelihood are then combined and compared to criteria in a risk acceptability matrix. A risk acceptability matrix that incorporates the risk requirements of 14 CFR 437.55(a)(3) is shown in Table 3.

In this risk acceptability matrix, Category 2 risks (low risk, those in blocks 7 and 9-20) satisfy the criteria of §437.55(a)(3). Category 1 risks (high risk, those in blocks 1-6 and 8) do not satisfy the criteria in the regulations and therefore are unacceptable risks. These criteria are as follows:

- The likelihood of any hazardous condition that may cause death or serious injury to the public must be extremely remote.
- The likelihood of any hazardous condition that may cause major property damage to the public, major safety-critical system damage or reduced capability, a significant reduction in safety margins, or a significant increase in crew workload must be remote.

An operator must implement risk elimination or mitigation measures to reduce the risk to acceptable levels for the risks that do not meet these criteria.

In developing qualitative criteria to assess risk, the FAA was informed by industry practice and existing government standards. The FAA based its criteria on MIL-STD-882D, Department of Defense Standard Practice for System Safety; FAA AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes; and FAA System Safety Handbook. Examples of risk assessments using the severity and likelihood categories in Tables 1 and 2 and the risk acceptability criteria in Table 3 are provided in the appendix.

Table 1. Hazard Severity

DESCRIPTION	CATEGORY	CONSEQUENCE DEFINITION
Catastrophic	I	Death or serious injury to the public.
Critical	II	Major property damage to the public, major safety-critical system damage or reduced capability, significant reduction in safety margins, or significant increase in crew workload.
Marginal	III	Minor injury to the public or minor safety-critical damage.
Negligible	IV	Not serious enough to cause injury to the public or safety-critical system damage.

Table 2. Hazard Likelihood

DESCRIPTION	LEVEL	INDIVIDUAL ITEM
Frequent	A	Likely to occur often in the life of an item, with a likelihood of occurrence greater than 10^{-2} in any one mission.
Probable	B	Will occur several times in the life of an item, with a likelihood of occurrence less than 10^{-2} but greater than 10^{-3} in any one mission.
Occasional	C	Likely to occur sometime in the life of an item, with a likelihood of occurrence less than 10^{-3} but greater than 10^{-5} in any one mission.
Remote	D	Unlikely but possible to occur in the life of an item, with a likelihood of occurrence less than 10^{-5} but greater than 10^{-6} in any one mission.
Extremely Remote	E	So unlikely, it can be assumed occurrence may not be experienced, with a likelihood of occurrence less than 10^{-6} in any one mission.

Table 3. Risk acceptability matrix

Severity / Likelihood	Catastrophic I	Critical II	Marginal III	Negligible IV
Frequent (A)	1	3	7	13
Probable (B)	2	5	9	16
Occasional (C)	4	6	11	18
Remote (D)	8	10	14	19
Extremely Remote (E)	12	15	17	20

Category 1 – High (1-6, 8). Elimination or mitigation actions must be taken to reduce the risk.
Category 2 – Low (7, 9-20). Risk is acceptable

c. Identify and Describe Risk Elimination and Mitigation Measures

The next step in the hazard analysis is to identify and describe risk elimination and mitigation measures for those risks that are unacceptable and must be reduced. In developing these analyses, the operator should consider whether the risk mitigation measures introduce new hazards. The recommended order of precedence for eliminating or mitigating risk is as follows:

- *Design or operate for minimum risk.* The first priority should be to eliminate hazards through appropriate design or operational choices. An example of designing out risk to the public would be to operate in an unpopulated area. Those risks that cannot be eliminated should be minimized through appropriate design or operational choices.
- *Incorporate safety devices.* If hazards cannot be eliminated through design or operation selection, then the permit operator should reduce risks through the use of active or passive safety devices. The

operator should make provisions for periodic functional checks of safety devices where appropriate. An example of an active safety device would be a computing system that automatically shuts down the rocket engine when a sensor detects high thrust chamber temperatures. A passive safety device might be a firewall to prevent a fire from reaching the pilot.

- *Provide warning devices.* When neither design nor safety devices can eliminate or adequately reduce identified risks, the operator should use devices to detect the hazardous condition and produce an adequate warning signal. Operators should design warning signals and their application into their systems to minimize the likelihood of inappropriate human reaction and response. An abort indicator, such as a flashing light or a message on a cockpit instrument panel, would be an example of a warning device.
- *Develop and implement procedures and training.* When it is impractical to eliminate risks through design selection or specific safety and warning devices, the operator should develop and implement procedures and training that mitigate the risks. Abort procedures and rehearsals of those procedures would be examples of procedures and training. Training and procedures can also be used to supplement other mitigation measures. For example, an operator may create procedures for training and using warning devices.

Specific procedural and training mitigation measures that the hazard analysis may identify include:

- Conducting dress rehearsals to ensure crew readiness under nominal and non-nominal flight conditions.
- Creating and using current and consistent checklists that ensure safe conduct of flight operations during nominal and non-nominal flights.
- Consolidating flight rules, procedures, checklists, contingency abort plans, and emergency plans in a safety directive, notebook, or other compilation.
- Establishing communication protocols, including defined radio communications terminology and a common intercom channel for communications.
- Conducting flight readiness reviews.

Two other risk mitigation measures often used for launch vehicles and derived from a hazard analysis include the use of flight safety systems (FSS) and flight hazard area analyses. An FSS consists of all components that limit or restrict the hazards by ending vehicle flight and preventing the vehicle from reaching a populated area in the event of a failure. For example, a reusable suborbital rocket may use a system that terminates engine thrust in combination with other measures, such as propellant dumping or parachutes, to reduce potential consequences to the public. For a piloted vehicle, the pilot or other crew members may be part of the FSS.

A flight hazard area analysis identifies any regions of land, sea, or air that must be monitored, publicized, controlled, or evacuated to control the risk to the public from debris impact hazards. As part of the hazard analysis, an operator should identify when the public is potentially at risk and whether a flight hazard area analysis is necessary.

To allow flexibility in reducing risk and to encourage innovation in improving safety, the FAA has not mandated any one particular mitigation approach. Selection of a risk elimination or mitigation approach is usually based on a number of factors, such as the type of operation, feasibility of implementing the approach, effectiveness of the approach, and impact on system performance. Example mitigation approaches for sample hazards are provided in the appendix.

d. Validate and Verify Risk Elimination and Mitigation Measures

It is important that the operator ensure that the appropriate risk elimination and mitigation measures (safety measures) derived from the hazard analysis are being used and that the safety measures selected are effective. This evaluation is done through a validation and verification (V&V) process.

Validation determines whether the implemented safety measures are right. To do this, the validation effort ensures that each safety measure is unambiguous, correct, complete, and consistent. In addition, this process demonstrates that each safety measure is well understood by the operator and that each safety measure is operationally and technically feasible.

Verification provides measurable evidence that a safety measure reduces risk to acceptable levels. The four acceptable methods of verifying safety measures are as follows:

- 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. These tests include functional tests and environmental tests.
- Demonstration test – 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.

These methods are often used in combination. The acceptability of one method over another depends on the feasibility of the method and the maturity of the vehicle and operations.

Validation and verification is a comprehensive, closed-looped, iterative process to be used in all phases of a system's life cycle. The FAA *Guide to Reusable Launch Vehicle Safety Validation & Verification Planning* (2003) discusses the essential components of an acceptable V&V process. This guide includes a set of sample implementation documents.

6.0 UPDATING THE HAZARD ANALYSIS

A hazard analysis is performed early in launch vehicle development to identify system hazards and risks in order to influence system design and operation to prevent mishaps. However, "real world" experience gained during design, manufacture, and test, including discovery of anomalies and faults, usually translates into changes in the analysis. Knowledge gained during assembly and operation of components, subsystems, and systems as the program matures contributes to further understanding of the system and should lead to additional changes to the hazard analysis. As part of the hazard analysis, a launch vehicle operator should identify the approaches and data needed to detect anomalies and failures in order to improve the analysis. As required by §437.55(c), a permit holder must ensure the continued accuracy and validity of its hazard analysis throughout the term of its permit. Therefore, the launch vehicle operator should also implement a process to update the hazard analysis and risk assessment to reflect the knowledge gained during the life of the system.

7.0 ACCEPTABLE METHODS

Common analytical approaches to identifying and characterizing hazards and risks include the following:

- Preliminary Hazard Analyses (PHA)
- Failure Modes and Effects Analyses (FMEA)
- Failure Modes, Effects, and Criticality Analyses (FMECA)
- Functional Hazard Analyses (FHA)

Any of these approaches may satisfy regulatory requirements as long as the approach includes the information described in paragraph 5.0, Hazard analysis.

ADDITIONAL CONSIDERATIONS

Although not mandated by regulation, several additional factors should be accounted for by a hazard analysis. These factors include, but are not limited to, the following:

- System Safety Data
- Configuration Management
- Reliability
- Operations and Maintenance
- Training
- Quality Assurance

a. System Safety Data

Safety data may include anomaly reports, procedures, test data, hazard reports, and lessons learned, regardless of whether they came from the operator or an operator's subcontractor. Means for describing, collecting, and processing this safety data should be part of the hazard analysis.

b. Configuration Management

Development of any system requires that changes be made throughout the life cycle. Changes to the vehicle, especially to safety-critical systems, can have significant impacts on public safety and will result in changes to the hazard analysis. The launch vehicle operator should implement a configuration control process to, at a minimum, identify components, subsystems, and systems; establish baselines and traceability; and track changes to the configuration and system safety documentation.

c. Reliability

Reliability plays an important role in protecting public safety because the risk to the public can depend on the failures of system elements and the consequences of those failures. Reliability analyses may aid in determining system safety design tradeoffs. Reliability testing and analyses may provide input into the validation and verification of the system and subsystems and assist in validating qualitative likelihood estimates in the hazard analysis. The launch vehicle operator should, where appropriate, perform reliability activities, including conducting reliability analyses, performing reliability testing and demonstration, developing approaches to improving reliability, and resolving reliability issues of safety-critical systems.

d. Operations and Maintenance

Operations of reusable suborbital rockets provide an opportunity to collect vital safety data and to ensure that all safety-critical systems perform as expected. Also, the operator may obtain trend data during operations that may be used to warn of operational safety problems or lead to corrective or preventative actions to prevent future safety problems from occurring. Therefore, an operator should collect and analyze operations safety data.

Maintenance engineering ensures that systems and subsystems will remain at the design safety level by minimizing wear-out failures through replacement of failed items and identification of possible degraded environments. Maintenance engineering personnel also participate in analyzing the safety implications of proposed maintenance procedures on the ground and in flight. Therefore, the launch vehicle operator should perform maintenance activities to aid maintenance and repair in the expected operating environments. The Federal Aviation Administration's *Guide to Commercial Reusable Launch Vehicle Operations and Maintenance*, Version 1.0, May 2005, describes important considerations for the operations and maintenance of reusable suborbital rockets.

e. Training

Designing safety into the system requires that personnel involved in system development, production, and operation understand and practice operations and procedures that protect public safety. Training can help ensure that personnel produce a safe system or operation. In addition, training may be included as a risk mitigation measure. The launch vehicle operator should incorporate training into its hazard analysis.

f. Quality Assurance

Quality assurance is implemented to verify that objectives and requirements of the system safety process, including those developed from analysis, are being satisfied and that deficiencies are detected, evaluated, tracked, and resolved. Quality assurance is usually performed through audits and inspections of elements and processes, such as plans, standards, and problem tracking and configuration management systems. In addition, quality assurance evaluates the validity of system safety data. The launch vehicle operator should perform quality assurance suitable to the objectives of the program.

8.0 RELATIONSHIP TO OTHER EXPERIMENTAL PERMIT REQUIREMENTS

As part of the requirements for obtaining an experimental permit, an operator must perform a hazard analysis. Additionally, a hazard analysis may also assist in meeting other experimental permit requirements. For example, in granting an experimental permit for a reusable suborbital rocket, the FAA requires that a permit holder stay within an operating area and outside any exclusion areas. An operating area is a three-dimensional region where permitted flights may take place. The operating area is similar to that used in granting special airworthiness certificates to experimental aircraft in that the FAA allows an operator to propose an area that best suited its needs. An operator could propose different operating areas for different flight tests in its application. Acceptable methods and systems for keeping the vehicle within the operating area may include, but are not limited to:

- Proof of physical limitations on a vehicle's ability to leave the operating area, or
- Abort criteria and safety measures derived from a system safety process. Specific safety measures resulting from a system safety process could include a dedicated flight safety system, a real-time instantaneous impact point (IIP) display with abort lines, or both.

An operator may use a hazard analysis to determine safety measures that keep a reusable suborbital rocket's IIP within its operating area. For example, an operator may use a hazard analysis to identify the safety measures necessary to avoid the hazards of a propulsion shutdown system not operating properly. A hazard analysis used to demonstrate containment may use the approach and qualitative risk criteria described in this document.

Specific safety measures obtained from a hazard analysis may include a dedicated flight safety system or other safety measures derived from the hazard analysis that are not exclusively dedicated only to flight safety. A dedicated flight safety system could protect the public and property from harm by terminating powered flight of a vehicle that does not stay on its intended course. Other safety measures may also include an operator's use of a ground or cockpit display that includes both the real-time IIP and abort criteria to assist in containment of the IIP.

9.0 OBTAINING A REUSABLE LAUNCH VEHICLE MISSION LICENSE

Some operators may ultimately wish to obtain a reusable launch vehicle license after they have obtained a permit. One purpose of conducting operations under an experimental permit is for an operator to show compliance with the requirements for obtaining a license. Therefore, the FAA recommends that permit operators be well versed in the system safety process requirements for obtaining a reusable launch vehicle mission license, as described in AC 431.35-2A, Reusable Launch Vehicle System Safety Process (2005).

As part of the requirements for obtaining an experimental permit, the FAA requires that an operator conduct a hazard analysis. To obtain a reusable launch vehicle license, an operator must employ a comprehensive system safety program consisting of both system safety management and system safety engineering. A hazard analysis is typically only part of a detailed system safety engineering process. However, a system safety process normally includes additional elements, such as the following:

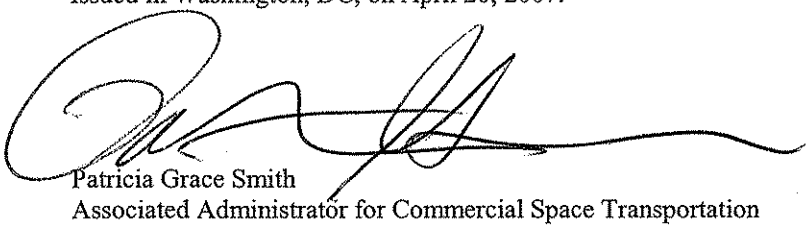
- Inclusion of a safety organization
- Designation of a safety official
- Development of a system safety program plan
- Identification of safety-critical systems and events
- Documentation of system and subsystem hazard analyses and risk assessments

Therefore, an operator who intends to seek a license may wish to conduct its permitted operations with these other requirements in mind.

10.0 FOR FURTHER INFORMATION

For more information on the guidance contained in this AC contact the Office of Commercial Space Transportation, Federal Aviation Administration, 800 Independence Ave. S.W., Washington, DC 20591. Telephone: 202-267-7793.

Issued in Washington, DC, on April 20, 2007.



Patricia Grace Smith
Associated Administrator for Commercial Space Transportation

APPENDIX

Example Hazard Analyses and Risk Assessments

The following tables provide examples of hazard analyses and risk assessments for hypothetical hazards for a reusable suborbital rocket. The severity (Sev), Likelihood (Like), and Risk values shown in the examples were obtained from Tables 1, 2, and 3. The format and content of these tables is for illustration purposes only. The operator should develop approaches to hazard analyses and risk assessments that are appropriate to its operation.

Table A-1. Hazard example: leak in rocket engine fuel system line

Hazard description	Risk before mitigation measures			Risk elimination or mitigation measures	Risk after mitigation measures		
	Sev	Like	Risk		Sev	Like	Risk
Leak in the rocket engine fuel system line caused by a manufacturing defect, overpressure, or improper installation could lead to a fire, resulting in possible loss of the vehicle.	I Catastrophic	C Occasional	High	Implementing all of the following reduces the risk to required levels: – Conducting envelope expansion flights over unpopulated areas. – Incorporating fire detection and suppression systems. – Implementing firewall to prevent spread of fire to cockpit. – Providing audible, visual, or both, warning displays to pilot of fire. –Developing procedures to inspect fuel system and fire suppression system before flight.	II Critical	D Remote	Low

Table A-2. Hazard example: pilot incapacitation

Hazard description	Risk before mitigation measures			Risk elimination or mitigation measures	Risk after mitigation measures		
	Sev	Like	Risk		Sev	Like	Risk
Vehicle motion could exceed the pilot's tolerance level and lead to pilot disorientation or loss of consciousness, resulting in temporary or permanent loss of control of the vehicle.	I Catastrophic	D Remote	High	Implementing all of the following reduces the risk to required levels: – Training the pilot in an aerobatic airplane to prepare for similar high rates of roll and g-tolerance. – Establishing operating limitations to assure that the pilot is not subjected to excessive stresses. – Using cockpit displays to warn the pilot of excess rates of motion. – Using cockpit displays to issue abort signal when roll exceeds operating limits of XX.	I Catastrophic	E Extremely Remote	Low

Table A-3. Hazard example: flight control display

Hazard description	Risk before mitigation measures			Risk elimination or mitigation measures	Risk after mitigation measures		
	Sev	Like	Risk		Sev	Like	Risk
Flight control display is lost or provides erroneous data during rocket-powered portion of flight because of hardware failure or software fault, leading to flight outside of operating area or possible vehicle loss.	I Catastrophic	D Remote	High	Implementing all of the following reduces the risk to required levels: – Aborting the mission if the display is lost. – Using independent ground support systems to monitor vehicle conditions. – Having both the pilot and computer systems perform manual and automated checks to ensure that hardware and software are in a safe state and functioning properly before initiating engine start, including checking safety-critical circuits, components, inhibits, interlocks, exception limits, safing logic, memory integrity, and program loads. – Confirming that flight control display software will meet requirements for operating properly with invalid inputs, out of range inputs, boundary value inputs, invalid outputs, timing errors, out of sequence commands, divide by zero errors, or greater-than-allowed data rates. – Developing procedures for mission abort and conduct training on abort procedures.	I Catastrophic	E Extremely Remote	Low

Table A-4. Hazard example: lightning strike

Hazard description	Risk before mitigation measures			Risk elimination or mitigation measures	Risk after mitigation measures		
	Sev	Like	Risk		Sev	Like	Risk
Natural or triggered lightning could strike the vehicle in flight leading to flight safety system malfunction; guidance, navigation, and control failure; or general electrical system failure. Any of these events could result in vehicle loss.	I Catastrophic	D Remote	High	Implementing all of the following reduces the risk to required levels: – Developing procedures to monitor and report meteorological conditions to the mission conductor. – Developing procedures to meet the natural and triggered lightning commit criteria specified in 14 CFR Part 417, appendix G. – Conducting training on those procedures.	I Catastrophic	E Extremely Remote	Low

Table A-5. Hazard example: turbopump component wear

Hazard description	Risk before mitigation measures			Risk elimination or mitigation measures	Risk after mitigation measures		
	Sev	Like	Risk		Sev	Like	Risk
Tolerance stack up, contamination, or component aging could lead to wear in turbopump bearings and other components, leading to loss of the engine or fire caused by increased heat in an oxygen environment and resulting in possible vehicle loss.	I Catastrophic	D Remote	High	Implementing all of the following reduces the risk to required levels: – Using long-life bearings to minimize wear. – Developing procedures to perform routine teardown and inspection of the bearings and components during the qualification tests of the engine to ensure continued reliable operation. – Developing contamination control procedures. – Conducting training on those procedures.	I Catastrophic	E Extremely Remote	Low