U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: REUSABLE LAUNCH AND REENTRY VEHICLE SYSTEM SAFETY PROCESS

Date: July 20, 2005
Initiated by: AST-1

AC No: 431.35-2A
Change:

1.0 PURPOSE

a. This Advisory Circular (AC) provides guidance concerning applying a systematic and logical system safety process for identification, analysis, and control of public safety hazards and risks associated with the operation of reusable launch vehicle (RLV) and reentry vehicle (RV) systems. The approach described here provides an acceptable approach to system safety methodology. Other approaches that fulfill regulatory objectives may be acceptable to the Federal Aviation Administration (FAA), Office of Commercial Space Transportation (AST).

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 RLV and RV systems requirements. While not mandatory, these guidelines are derived from extensive FAA/AST and industry experience.

2.0 CANCELLATION

AC 431.35-2, Reusable Launch and Reentry Vehicle System Safety Process, dated September 2000, is canceled.

3.0 RELATED REGULATIONS AND DOCUMENTS

a. Regulations

14 CFR Parts 401; 431, Subpart C; and 435: Commercial Space Transportation Reusable Launch Vehicle and Reentry Licensing

401, Organization and Definitions

431, Subpart C, Safety Review and Approval for Launch and Reentry of a Reusable Launch Vehicle

435, Reentry of a Reentry Vehicle Other Than a Reusable Launch Vehicle

b. FAA Advisory Circulars and Guidance Documents

AC 431.35-1, Expected Casualty Calculations for Commercial Space Launch and Reentry Missions, August 2000

AC 431.35-3, Licensing Test Flight Reusable Launch Vehicle Missions, August 2002

AC 25.1309-1A, System Design and Analysis, June 1988

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

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

c. Industry and U.S. Military Documents

ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, December 1996

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

MIL-STD-882D, Standard Practice for System Safety, February 10, 2000

System Safety Society, Inc., *System Safety Analysis Handbook*, 2nd Edition, Unionville, Virginia, 1997.

4.0 DEFINITIONS

4.1 Acronyms

a.	AC	Advisory Circular
b.	AST	Office of Commercial Space Transportation
c.	CDR	Critical Design Review
d.	CDRL	Contract Data Requirements List
e.	E_c	Expected number of casualties
f.	ESD	Event Sequence Diagram
g.	ETA	Event Tree Analysis
h.	FAA	Federal Aviation Administration
i.	FMEA	Failure Modes and Effects Analysis
j.	FMECA	Failure Modes, Effects, and Criticality Analysis
k.	FSS	Flight Safety System
l.	FTA	Fault Tree Analysis
m.	FTS	Flight Termination System
n.	HRI	Hazard Risk Index
o.	O&M	Operations and Maintenance
p.	PDR	Preliminary Design Review
q.	PHA	Preliminary Hazard Analysis
r.	PHL	Preliminary Hazard List
s.	MIL-STD	Military Standard
t.	R&D	Research and Development
u.	RLV	Reusable Launch Vehicle
v.	RV	Reentry Vehicle
w.	SHA	System Hazard Analysis
x.	SOW	Statement of Work
y.	SSHA	Subsystem Hazard Analysis
z.	SSP	Safety System Process
aa.	SSPP	System Safety Program Plan
bb.	TIM	Technical Interchange Meeting
cc.	TTS	Thrust Termination System
dd.	V&V	Validation and Verification
ee.	VDD	Vehicle Design Document

4.2 Definitions

a. **Criticality.** Relative measure of the consequences of a failure or hazard and its frequency of occurrence.

b. **Event Sequence Diagram (ESD).** Qualitative graphical technique that analyzes the order of events that is likely to occur given that an initiating event has occurred.

c. **Event Tree Analysis (ETA).** System analysis technique that explores responses to an initiating event and enables assessment of the probabilities of unfavorable or favorable outcomes.

d. **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.

e. **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.

f. **Fault Tree Analysis (FTA).** Deductive system reliability analysis that provides qualitative and quantitative measures of the likelihood of failure of a system, subsystem, or event. This analysis estimates the likelihood that a top-level or causal event will occur, identifies possible causes leading to that event, and documents the results of the analytic process to provide a baseline for future studies of alternate designs.

g. **Flight Safety System (FSS).** Destructive or nondestructive system designed to limit or restrict the hazards to public health and safety and the safety of property presented by a launch vehicle or reentry vehicle while in flight by initiating and accomplishing a controlled ending to vehicle flight.

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

i. **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.

j. **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 to protect the public.

k. **Preliminary Hazard List (PHL).** Initial list of potential system hazards, compiled without regard to risk or possible mitigation measures.

l. **Risk.** Measure that takes into consideration the likelihood of occurrence and the consequence of a hazard to a population or property. Types of risk include the following:

(1) **Unacceptable.** Risk to a population or property that is identified and cannot be tolerated under existing law. Unacceptable risk is the part of the identified risk that must be either eliminated or controlled.

(2) **Acceptable.** Risk to a population or property that is identified and allowed to persist without further engineering or management action.

(3) **Residual.** Risk to a population or property remaining after the system safety efforts have been employed. Residual risk is the sum of the known acceptable risk and the unidentified (unknown) risk. This is the total risk to the public. Although unidentified risk cannot be directly measured, it is accounted for through risk mitigation measures.

(4) **Individual.** The likelihood of a casualty to an individual member of the uninvolved public.

(5) **Collective.** Expected average number of casualties to members of the uninvolved public.

m. **Risk acceptance.** The act by a decision maker of tolerating a risk.

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

o. **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.

p. **System safety program**. The combined tasks and activities of system safety management and engineering that enhance operational effectiveness by satisfying safety requirements throughout all phases of the system life cycle.

q. **Validation.** Process that determines that the safety requirements created in the system safety process are correct and complete.

r. **Verification.** Evaluation (test, demonstration, analysis, inspection) to determine that applicable safety requirements created in the system safety process have been met.

5.0 BACKGROUND

The FAA requires an RLV or RV operator to use a three-pronged approach to ensure that public health and safety and the safety of property would not be jeopardized by the conduct of an RLV mission, defined to include ascent and descent flight of an RLV that has been authorized under an FAA license. Figure 1 shows the three-pronged approach. The three safety-related elements reflected in the FAA's safety strategy for RLV and RV missions and licensing are as follows:

- Acceptable public risk as determined through a calculation of the individual and collective risk, measured by expected number of casualties (E_c).
- Logical, disciplined system safety process to identify hazards and to mitigate and control risks.
- Operational requirements.

Together these interrelated elements ensure risks are sufficiently contained at an acceptable level. Just as system redundancy compensates for failure, flawed design, or imperfect performance, interrelated safety elements ensure that hazards from vehicle operation, whether expected in analytical assessments or unforeseen, will not increase risk to the public beyond an acceptable level. The FAA requires the combination of the three elements, working together, to reduce public risk to an acceptable level.

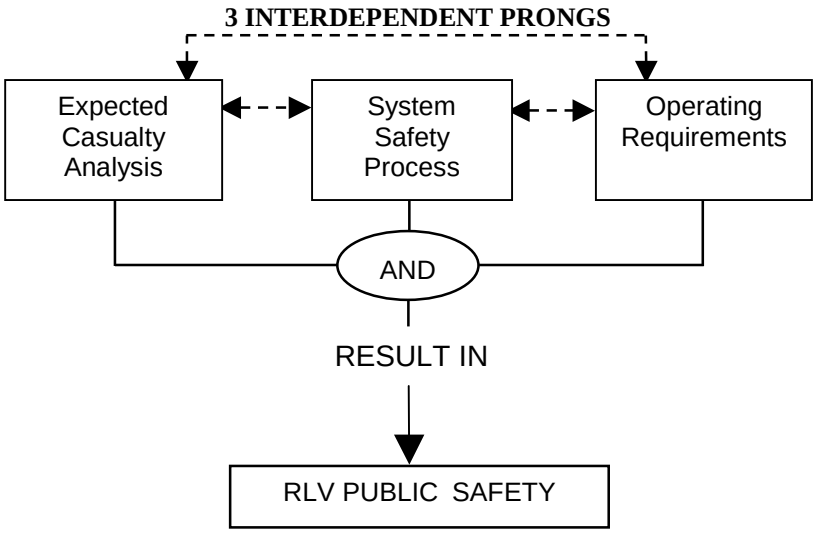


Figure 1. Three-Pronged Approach to RLV Public Safety

Understanding the relationship of the system safety process to the licensing process and the safety of the proposed operation is important. Using a systematic process for the identification and control of safety-critical systems and operations provides the foundation supporting the expected casualty analysis (see AC 431.35-1). Without a process that helps ensure a disciplined approach to the design, manufacture, integration, test, and operation of a system, establishing confidence in the probabilities of failure provided for the expected casualty analysis may prove very difficult. An analytical or statistical approach is normally used to obtain a probability of failure. In addition, the results of the analysis are supported by historical data resulting from a system safety process.

While extremely important in creating a strong foundation for ensuring the safety of a system, a system safety process does not ensure public safety. Application of the system safety engineering approach in combination with the expected casualty analysis, mandatory operational restrictions defined in regulations, and operational requirements derived from the collective and individual risk analyses, and system safety processes are all intended to help maintain the risk to the public at an acceptable level.

Paragraph 6 describes each element of the three-pronged approach to public safety, with an emphasis on the system safety process. This discussion also provides an acceptable system safety engineering process. The System Safety Program Plan (SSPP) is part of an RLV license application. Therefore, the operator is bound by the terms of the SSPP it submits to the FAA. Appendix A provides an example of an SSPP, and a format for reporting risk, including sample forms, is in appendix B.

6.0 SYSTEM SAFETY PROCESS

The requirements for the RLV system safety process are addressed in 14 CFR 431.35 (c) and (d). The RV system safety process is addressed in 14 CFR 435.33.

Reusable launch vehicles typically include ascent and descent phases of flight, while RVs include only a descent phase. Although RLVs and RVs could technically be different types of vehicles, the system safety process described here is the same for both types of vehicles. For the purposes of this document, the term "RLV" is used for both RLVs and RVs.

The system safety process consists of the structured application of system safety engineering and management principles, criteria, and techniques to address safety within the constraints of operational effectiveness, time, and resources throughout all phases of the life cycle of a system. This process identifies and analyzes hazards and risks, then reduces or controls such risks to acceptable levels. The launch vehicle operator implements this process. An acceptable system safety analysis identifies and assesses the likelihood and consequences of any reasonably foreseeable hazardous event and safety-critical system failures during flight or reentry that could result in a casualty to the public. At a minimum, a system safety analysis should meet the following criteria:

- Identify and describe safety-critical systems
- Identify and describe safety-critical failure modes and their consequences
- Provide a timeline identifying safety-critical events
- Identify mitigation and control measures to reduce or minimize risk
- Provide evidence that validates and verifies the system safety analysis

Because of the complexity and variety of vehicle concepts and operations, a system safety process can help ensure that all risks to public safety are considered and addressed. Without a system safety process, very detailed requirements would have to be imposed on all systems and operations to ensure that all potential hazards have been addressed. Imposing detailed requirements could have the undesired effect of restricting design alternatives and innovation or could effectively dictate design and operations concepts.

As described in Military Standard (MIL-STD) 882D, Standard Practice for System Safety, a system safety process consists of two elements: system safety management and system safety engineering. The system safety process is documented in the SSPP. Each of these elements is discussed below.

a. System Safety Management

System safety management defines the system safety program requirements and ensures the planning, implementation, and accomplishment of the identified tasks within the scope of the overall system design, engineering, and integration program. At a minimum, system safety management is responsible for the following items:

- Ensuring that safety is consistent with mission objectives.
- Planning, organizing, and implementing the system safety program, including generating and maintaining the SSPP.
- Establishing overall requirements.
- Establishing the decision-making process for managing risks.
- Defining functions, authority, and interrelationships.
- Reviewing contractor efforts and data.
- Identifying and creating policies and procedures.

- Resolving conflicts between safety and other mission requirements.

Some of these system safety management elements are required under sections in 14 CFR 431. However, system safety management takes a broader view in that it defines the tasks and rules for conducting system safety engineering.

The development of a safety organization is a critical component in the management of the system safety program. The following are requirements in 14 CFR 431.33 for the safety organization. An operator must:

- Maintain a safety organization and document it by identifying lines of communication and approval authority for all mission decisions that may affect public safety. Such documentation typically includes descriptions of the roles and graphical representations showing the interactions of those roles.
- Designate a person, often called the mission conductor, responsible for the conduct of licensed RLV mission activities.
- Designate a person, often called the safety official, responsible for safety operations and procedures. This official examines all aspects of the operator's operations with respect to safety of RLV mission activities and monitors independently compliance by vehicle safety operations personnel with the safety policies and procedures of the operator.

Lessons learned from mishaps have identified the importance of the independence of the mission conductor and safety official roles to ensure that safety is a primary goal of the operator. To help achieve this independence, FAA/AST requires that one individual will be assigned to each of these roles.

The safety official reports to the mission conductor. In turn, the mission conductor ensures that all the safety official's concerns are addressed both before a mission is started and before reentry or descent flight of an RLV is started. Safety officials monitor and evaluate dress rehearsals to ensure such trial runs are conducted in keeping with procedures identified in the regulations. These evaluations also examine the readiness of the safety operations personnel to conduct missions under nominal and off-nominal conditions. The safety official reports any non-compliance with procedures or representations in the license application to the mission conductor.

b. System Safety Engineering

System safety engineering consists of scientific and engineering principles, criteria, and techniques necessary to identify and eliminate hazards and reduce the associated risk to acceptable levels. In addition, system safety engineering performs those tasks and activities identified by system safety management; consists of tasks and activities that define safety-critical systems, identify hazards and risks, develop top- and design-level safety requirements; and provides evidence for validation and verification (V&V) of safety-critical systems and requirements.

Figure 2 shows a traditional system safety engineering process modified by the FAA to focus only on risks to the public. The U.S. Department of Defense, National Aeronautics and Space Administration, and aerospace industry have successfully used this process for decades. This process represents one acceptable methodology. Other approaches that fulfill regulatory requirements may be acceptable. Note that the FAA recommends operators use a process comparable to that reflected in MIL-STD-882D, *System Safety Analysis Handbook* (a System Safety Society Standard), or FAA AC 25-1309.

The system safety process is iterative; for ease of discussion, this process is presented here in a linear, one-pass fashion. As the development life cycle progresses, continuing to apply the system safety engineering process may identify additional safety-critical systems, hazards, failure modes, mitigation measures, and safety requirements. Detailed discussion of each element is provided.

(1) System Safety Engineering Planning

The operator must include the system safety engineering plans as part of an overall SSPP. At a minimum, such plans must include approaches to be used in the following elements:

- Identifying safety-critical systems
- Conducting hazard analyses and risk assessments

- Performing V&V
- Tracking hazards through the development life cycle of the program

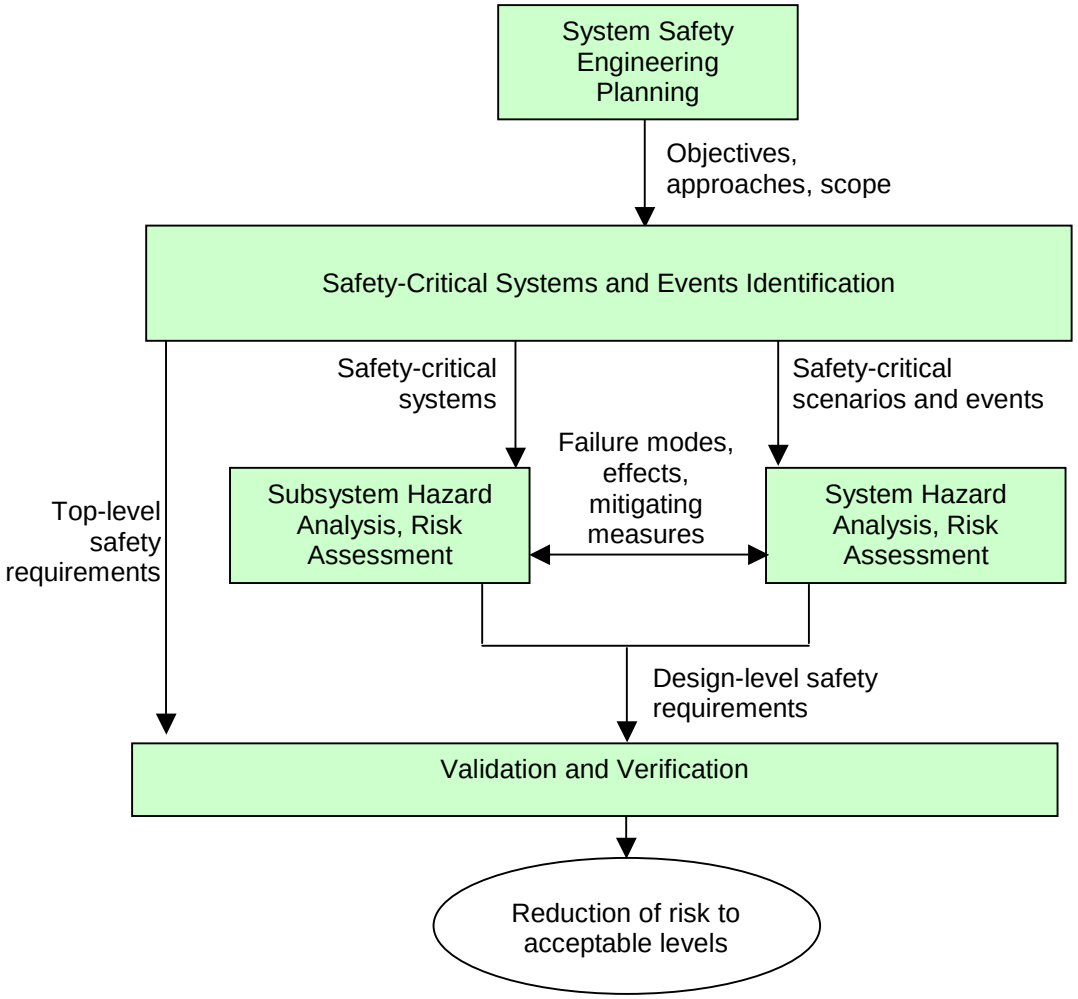


Figure 2. System Safety Engineering Process Flow

These elements provide the ground rules for conducting the analyses (see appendix A). Planning also covers the collection of data to provide descriptions of systems and subsystems (including the vehicle weight, structure, and physical dimensions) and interactions among people, procedures, tools, materials, equipment, facilities, software, and environment for use in later analyses. This phase includes defining hazardous materials and flight trajectory, including launch or ascent, orbital insertion, reentry or descent, and landing. Outputs of this phase of the process include system safety engineering objectives, approaches, and scope.

(2) Safety-Critical Systems and Events Identification

The next step of the system safety engineering process is to identify the safety-critical systems and events using the approaches outlined in the planning phase (see figure 3). Whether they directly or indirectly affect the operation of the vehicle, safety-critical systems may or may not be critical at all times. For example, the vehicle's flight path, ability to reach populated areas, or both, may vary

greatly, thereby influencing the periods when a specific system is safety-critical. For this reason, the launch vehicle operator should determine the phases where these systems are safety-critical and only analyze those systems for that phase. Identifying safety-critical systems as early as practicable is important. The life cycle of such systems may be divided into the following six phases:

- Conception
- Research and Development (R&D)
- Design
- Deployment
- Operation
- Decommissioning and Disposition

Common analytical approaches used for identifying safety-critical systems and events include Preliminary Hazard Lists (PHL), Preliminary Hazard Analyses (PHA), Event Tree Analyses (ETA), and Fault Tree Analyses (FTA). Any of these approaches would be acceptable to the FAA. Other tools that may be acceptable for determining safety-critical systems include industry guidelines that may list safety-critical systems, mishap data, and experience with similar systems. Outputs from the identification of safety-critical systems, scenarios, and events include top-level safety requirements. (For example, all composite structures shall be proof tested to 110 percent of the maximum expected flight load per company standard XYZ-001.)

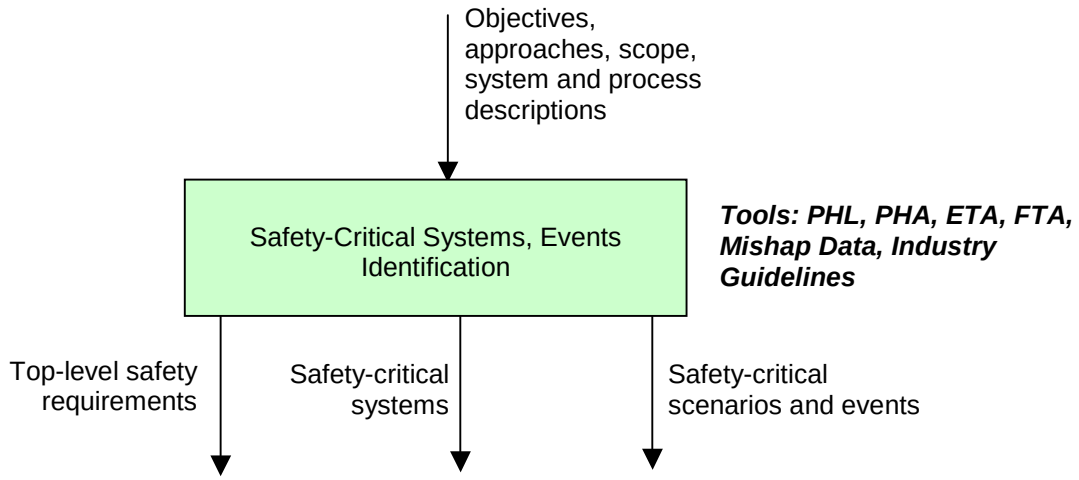


Figure 3. Identification of Safety-Critical Systems and Events

(3) Hazard Analysis and Risk Assessment

Once the safety-critical subsystems, components, and events have been identified, analyses are normally performed to identify hazards associated with those items. Then risks associated with those hazards are assessed (see figure 4). Such assessments focus on identifying, characterizing, quantifying, and evaluating risks in terms of likelihood and severity. Generally, performing a risk assessment requires answering three questions:

- What can go wrong?
- How likely is it?
- What are the consequences?

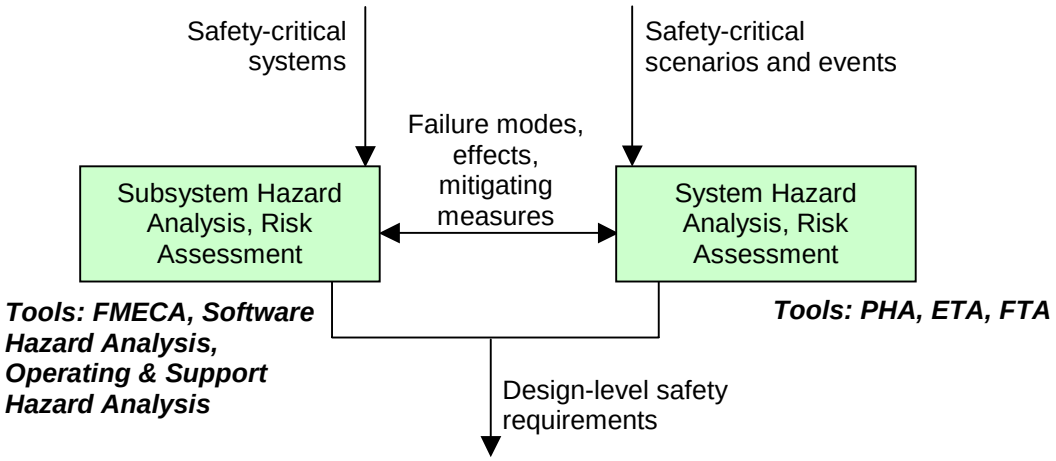


Figure 4. Hazard Analysis and Risk Assessment

To answer these questions, the FAA requires the use of systematic methods for characterizing the hazards and quantifying the risks in terms of likelihood and severity. These methods include both inductive or "bottom-up" subsystem analyses and deductive or "top-down" system analyses.

i. Subsystem Hazard Analysis

Failure Modes, Effects, and Criticality Analysis is one acceptable subsystem hazard analysis (SSHA) and risk assessment method. In this bottom-up (inductive) system analysis technique, each potential failure mode in a system is analyzed to identify its consequences and determine the qualitative severity and likelihood of occurrence. MIL-STD-882D provides definitions that the launch vehicle operator can use in the qualitative evaluation of severity and likelihood in these bottom-up risk assessments. Tables 3.1 and 3.2 in appendix A provide examples of qualitative severity and likelihood categories.

Through the System Safety Engineering Process, risks are identified and reduced. Typically, the severity and likelihood are combined and used to define risk acceptability criteria. These risk acceptability criteria determine when risk control measures are required. MIL-STD-882D provides a recommended risk acceptability matrix. Figure 3.3 in appendix A provides an example of a risk acceptability matrix.

Based on the qualitative risk acceptability matrix, a launch vehicle operator makes a decision on whether to eliminate or mitigate the hazard. The recommended order of precedence for eliminating or mitigating risk is as follows:

- *Design for minimum risk.* The first priority should be to design to eliminate risk. If the identified risk cannot be eliminated, reduce the risk to an acceptable level through design selection.
- *Incorporate safety devices.* If risks cannot be eliminated through design selection, then launch vehicle operators should reduce risks through the use of active and passive safety devices. The launch vehicle operator must make provisions for periodic functional checks of safety devices.
- *Provide warning devices.* When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, the launch vehicle operator should use devices to detect the condition and produce an adequate warning signal. The launch vehicle operator must design warning signals and their

application to minimize the likelihood of inappropriate human reaction and response.

- *Develop procedures and training.* When it is impractical to eliminate risks through design selection or specific safety and warning devices, the launch vehicle operator should use procedures and training.

Selection of a mitigation approach is usually based on a number of factors, such as the feasibility of implementing the approach, effectiveness of the approach, and impact on system performance. The analysis should also consider whether the mitigation measure introduces new hazards.

Outputs of the SSHA include design-level safety requirements derived from the mitigation measures chosen. See paragraph 6.0 b (4), Validation and Verification, for further discussion of safety requirements.

ii. System Hazard Analysis

The majority of mishaps result from a combination of such factors as the environment, mechanical failure, software, human error, procedures, and system design. System hazard analyses (SHA) and risk assessments are necessary because these factors may not be represented in the subsystem analyses. Therefore, the FAA recommends that the launch vehicle operator use system risk assessment methods in addition to the bottom-up, subsystem risk assessment.

System risk assessment usually consists of inductive scenario modeling supplemented by deductive (top-down) failure modeling. The failure models and scenarios are often developed based on safety-critical events, failure modes, effects, and mitigation measures from the earlier tasks of identifying safety-critical systems and performing SSHA and risk assessment. Acceptable methods for performing scenario modeling include, but are not limited to, ETA and ESD. Other methods, such as PHA, can also aid in developing mishap scenarios. Failure modeling is performed to supplement the scenario models, and an FTA is one acceptable method for performing the failure modeling. The output from the SHA and risk assessment includes additional design-level requirements. In addition, the SHA may be used to identify additional failure modes, effects, and mitigation measures that can then be analyzed further on a subsystem level.

iii. Updating and Combining Analyses

Experience gained during design, manufacture, and test usually translates into changes in the analyses. In addition, knowledge gained during assembly and operation of components, subsystems, and systems as the program matures contributes to such changes. The launch vehicle operator must implement a process to update the hazard analysis and risk assessment to reflect the knowledge gained during the life cycle of the system.

In the interest of preserving resources, it may make sense to combine analyses. To identify safety-critical systems and investigate system interactions, for example, an SHA may examine mechanical failure as well as the environment, software, human error, and procedures. The decision to combine analyses should be made based on the complexity of the system, operations, and program scope.

iv. Specific Risk Mitigation Measures

Two specific risk mitigation measures often used for launch vehicles and derived from the system safety process include the use of flight safety systems (FSS) and flight hazard area analyses. An FSS limits or restricts the hazards to the uninvolved public by initiating and accomplishing a controlled ending to vehicle flight, thereby, preventing the vehicle from reaching a populated area in the event of a failure. Expendable launch vehicles launching from the United States typically use a flight termination system (FTS) as the FSS to end the flight whenever the launch vehicle strays outside of a predefined envelope. This FTS normally includes a flight destruct system or a

thrust termination system (TTS). Reusable launch vehicles may also use an FTS, depending on the design and application, although other systems may be appropriate. For example, an RLV may use a TTS in combination with other measures, such as propellant dumping or parachutes, to reduce potential consequences to the public. By identifying the specific safety-critical failure modes, timelines of safety-critical events, consequences, and risks to the public, the system safety process helps determine the criteria for activating an FSS. Note that this FSS may also serve to reduce the quantitative risk as part of an expected casualty analysis.

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. This analysis establishes the ship and aircraft hazard areas for Notices to Mariners and Notices to Airmen. The system safety process will identify when the public is potentially at risk based on safety-critical failure modes and events and if a flight hazard area analysis is necessary. This analysis often accounts for the following items:

- Regions of land, sea, and air potentially exposed to debris resulting from normal flight events and potential malfunctions.
- Waterborne vessels or aircraft exposed to debris from events resulting from normal, abnormal, or both, flight events.
- Operational controls implemented to control risks to the public from debris hazards.
- Debris identified from debris analysis.
- Vehicle trajectory dispersion effects in the surface impact domain.

(4) Validation and Verification

Safety analyses generate top- and design-level safety requirements. These requirements typically result from implementation of mitigation measures or operational controls to reduce residual risk to an acceptable level. Other sources may include operating practices, standard industry practices, and regulations. Regardless of the source, effective management of the complete set of safety requirements is an essential component of system safety engineering. The V&V process is used to manage the set of safety requirements (see figure 5).

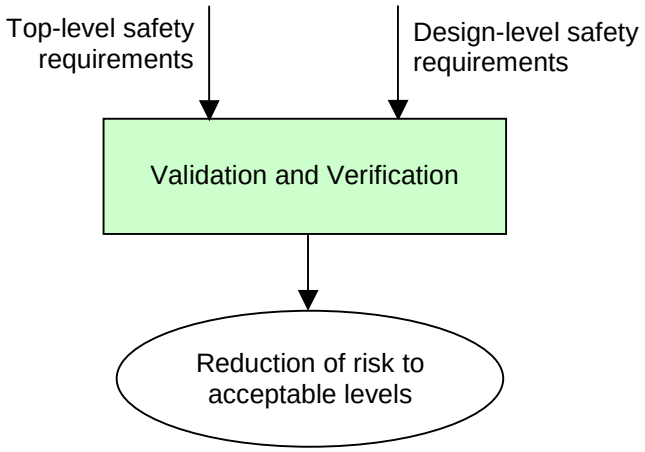


Figure 5. Validation and Verification

The V&V process determines that the correct safety-critical system is being built (validation), as represented by a correct and complete set of safety requirements, and that the design solution meets all of the safety requirements (verification). This comprehensive, closed-looped, iterative process is to be used in all phases of the system's life cycle. Although validation of the safety requirements is performed before verification efforts, it is the closed-looped final validation that ultimately ensures the safety system will perform as intended.

The FAA/AST *Guide to Reusable Launch Vehicle Safety Validation & Verification Planning*, Version 1.0, September 2003, discusses the essential components of an acceptable V&V process. This Guide includes a set of sample implementation documents.

(5) Additional Considerations

Several additional factors should be considered in the management of the system safety process. These factors include:

- System Safety Data
- Configuration Management
- Quality Assurance
- Reliability
- Operations and Maintenance (O&M)
- Anomaly Reporting and Corrective Action
- Training

i. System Safety Data

Safety data can include such items as anomaly reports, procedures, test data, hazard reports, lessons learned, and subcontractor safety effort deliverables. Means for describing, collecting, and processing this safety data are part of the system safety process.

ii. Configuration Management

Development of any system requires that changes be made throughout the life cycle. Changes to the vehicle, especially on safety-critical systems, can have significant impacts on public safety. 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.

iii. Quality Assurance

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

iv. 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

analysis can be used to aid in system safety design tradeoffs. Reliability testing and analyses can provide input into the V&V of the system and subsystems. In addition, reliability estimates and system failures identified during the system safety process can be used in the expected number of casualties (E_c) calculation. The launch vehicle operator should 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.

v. Operations and Maintenance

Operations of RLVs provide critical safety data to ensure that all safety-critical systems are performing as expected. Also, the operator may obtain trend data during operations that can 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 develop a function to 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 surveillance over 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 FAA/AST *Guide to Commercial Reusable Launch Vehicle Operations and Maintenance*, Version 1.0, May 2005, describes important considerations for the O&M of RLVs.

vi. Anomaly Reporting and Corrective Action

Analyses of mishaps often show that clues existed before the mishap in the form of anomalies during the project life cycle. Examination and understanding of launch vehicle system and subsystem anomalies throughout the life cycle can warn of an impending mishap and provide important information leading to safety measures to mitigate public risk. The launch vehicle operator should develop standardized processes to document anomalies, analyze the root cause, and determine corrective actions to help prevent recurrence of safety-related anomalies and form a proactive means to protect public safety.

vii. 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 can produce a safe system or operation. In addition, training can be included as a risk mitigation measure; therefore, training can be a critical element in helping ensure the safety of the public. The launch vehicle operator should develop plans that describe essential training.

c. System Safety Program Plan

The methodology by which the system safety process is employed for a specific program is documented in the SSPP (see appendix A). The plan also defines the products that result from the system safety program. The objectives of a system safety program are to ensure the following items:

- Safety, consistent with overall system objectives and requirements, is designed into the system.
- Hazards associated with the form, fit, function, operation, and support of the system are identified, evaluated, and eliminated, or the associated risk is reduced to acceptable levels throughout its entire life cycle.
- System safety data, including lessons learned from similar systems, are identified and applied.

- Safety evaluation and analytical techniques are selected and applied to new designs, materials, processes, and procedures to minimize the associated risk.
- Methods employed to eliminate hazards and reduce risks are properly applied and documented. Effectiveness of such methods should be included in the documentation.
- Design changes required to meet specified levels of risk are minimized through the efficient and effective application of safety features during the R&D or acquisition phase of the system.
- Changes in system design, configuration, or application are evaluated and analyzed for impacts to overall system safety.
- Data banks are established to ensure that significant safety data are retained and readily available for trend analysis.

The SSPP describes the planned methods by which recognized and accepted safety standards and requirements are to be integrated with other system engineering functions to ensure hazards are identified and eliminated. This plan also includes methods by which the likelihood of occurrence or severity of consequences is reduced to acceptable levels of risk. Organizational responsibilities, resources, methods of accomplishment, milestones, and levels of effort should be addressed. An SSPP also describes how hazards and residual risk are communicated to the program manager and how the program manager will formally accept and track the hazards and residual risk. At a minimum, this plan should exhibit the following essential attributes of a system safety program:

- Planned approaches for task accomplishment
- Qualified staff to accomplish tasks
- Authority to carry out tasks through all levels of management
- Appropriate staffing to ensure completion of tasks

To demonstrate these essential attributes, the plan must include the following system safety management and engineering elements:

(1) System Safety Management

- Purpose, scope, and objectives of the overall system safety program and its tasks. This description includes a breakdown of the project by organization and responsibilities of each organization, including reliability, quality assurance, operations, maintenance, design, flight test, and associate contractors.
- System safety organization to meet the requirements of 14 CFR 431.33, including tracing the lines of communication and approval authority for all mission decisions that may affect public safety and identifying a person responsible for conduct of all licensed RLV mission activities.
- System safety reviews and milestones.
- General system safety requirements.
- Preferable approaches to minimizing risk to the public.

(2) System Safety Engineering

- Methods for identifying safety-critical systems and events.
- Methods and procedures for hazard analysis and risk assessment, including hazard severity categories, hazard likelihood levels, acceptable risk levels, order of precedence for eliminating and mitigating risk, and procedures used for taking action to resolve identified hazards.

- Approaches to V&V of safety-critical systems and requirements.
- Descriptions of what system safety data is maintained and approaches to maintaining that data.
- Approaches to configuration management, quality assurance, reliability engineering, and O&M engineering.
- Approaches to mishap and anomaly reporting and corrective action.
- Approaches to safety training.

d. Determination of Risk to the Public

The FAA/AST uses collective and individual risk measures to quantify the public risk. A successful application of a system safety process should yield acceptable risks, which are risks that have been identified and allowed to persist. If it does not, the vehicle, by design or operation, is too risky for the FAA to authorize. However, system and operational uncertainties lead to unidentified (unknown) risk. The combination of known acceptable risk and unknown risk is residual risk. Expected number of casualties (E_c) is a statistical calculation used in the space transportation industry as a collective measure of residual risk to public safety. A collective risk calculation yields the consequences, measured in terms of human casualties, of the probability of occurrence of all events multiplied by the severity of impacts on public safety. Human casualty is defined as a fatality or serious injury. Collective risk measures the sum total risk or the probability of injury or death to the public exposed to the risk of an event.

However, FAA/AST also requires determination of individual risk, which measures the risk to a single person in the exposed population. An individual risk measure is used to address circumstances under which certain people may be exposed to risk, such as where a single dwelling exists along a vehicle trajectory. Application of an individual risk measure for persons residing within the dwelling would dictate whether or not the dwelling must be evacuated for launch or reentry activity along that trajectory to occur safely.

Requirements for collective and individual risk are addressed in 14 CFR 431.35 (b). The FAA AC 431.35-1, Expected Casualty Calculations for Commercial Space Launch and Reentry Missions, August 2000, describes an acceptable means of calculating the expected number of casualties (E_c) to determine public risk.

e. Operating Requirements

In combination with the expected casualty analysis, the system safety process yields methods of operation that demonstrate the operator's ability to operate within the limits of acceptable risk to public safety. Note, however, these analytical processes may not reflect real-world performance even under the best of circumstances. Because of the uncertainty in RLV performance and operation, the FAA specifies operating requirements. However, the hazard analysis and risk assessment, V&V, O&M experience, and expected casualty analysis assumptions can yield additional operational requirements or restrictions.

An interrelationship exists between the system design capabilities and system operational limitations. Design changes are not the only way to control risk. Operational limitations are used to restrict risk. While FAA regulatory operational limitations and requirements (14 CFR 431.43 and 435.33 for RLVs and RVs, respectively) must be met, the launch vehicle operator may employ additional operational requirements to limit risk to an acceptable level. Typically, the operator's decisions reflect a balance between design considerations and operational limitations and are based on such factors as the need to satisfy regulatory risk safety standards, technological capabilities, and cost-benefit tradeoffs.

Figure 6 depicts the relationship between the safety-critical systems and the scope of operations within which the vehicle is operated. Intended operational requirements affecting the proposed vehicle design requirements, capabilities, and limitations also establish the operational system constraints necessary to protect public health and safety. For example, landing sites may have to be within a specific cross-range distance from the orbital ground trace because of cross-range limitations of the vehicle. A vehicle operator may choose or be required to mitigate certain vehicle limitations through the use of operational controls rather than relieving vehicle limitations through design changes.

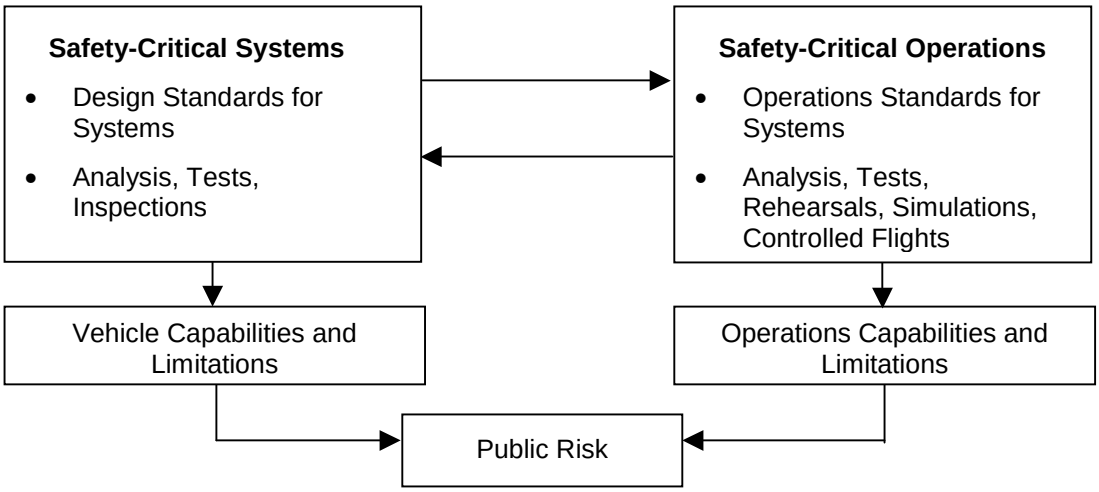


Figure 6. Interrelationship Between Safety-Critical Systems and Operations

Test parameters and analytic assumptions further define the limits of flight operations. The scope of the analyses and environmental tests, for example, will make up the dimensions of the operator's demonstration process and, therefore, define the limits of approved operations if a license is issued. Testing limits, identified system and subsystem limits, and analyses identified through application of a system safety process also are expected to be reflected in mission monitoring and mission rules addressing such aspects as commit to launch, flight abort, and commit to reentry.

Vehicle capabilities, limitations, and operational factors, such as launch location and flight path, affect public risk. Completion of system operation demonstrations, such as flight simulations and controlled flight tests, increases confidence in the systems and performance capabilities of the vehicle. As confidence in overall operational safety performance of the system increases, operational restrictions, such as limitations on the operating area, identified through the system safety process may be relaxed.

The following types of operations-related considerations, discussed in 14 CFR 431, may need to be addressed by the launch vehicle operator when establishing operations scenarios:

- Launch commit criteria and rules.
- Human activation or initiation of an FSS to initiate safe abort during launch and reentry.
- System monitoring, inspection, and checkout procedures.
- Inspection and maintenance for reflight.
- Selection of primary and alternate landing sites for the vehicle or stages.
- Surveillance and control of landing areas.
- Standard limits on weather.
- Coordination with appropriate airspace authorities.
- Limits on flight regime (ties in with analysis, testing and demonstrating confidence in system performance and reliability).
- Regulatory limits on flights over populated areas.
- Other considerations identified through hazard analysis.

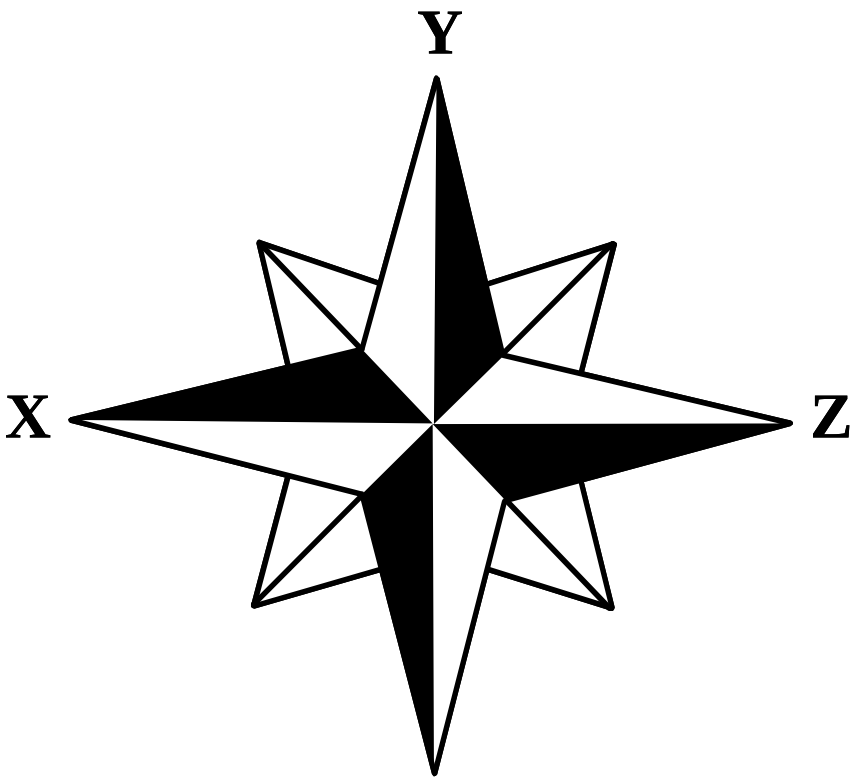
APPENDIX A

Sample Reusable Launch Vehicle System Safety Program Plan

The System Safety Program Plan (SSPP) is part of an RLV license application. Therefore, the launch vehicle operator is bound by the terms of the SSPP it submits to the FAA. This appendix provides guidance on developing an acceptable SSPP that addresses public safety considerations. Based on a hypothetical scenario, an RLV operator creates its system safety program as described in this sample SSPP. The intention is to demonstrate a systematic, logical, and disciplined approach for identifying hazards and assessing risks to the public during the design, development, and operation of an RLV system.

Methods and procedures described here illustrate an acceptable SSPP, but they are not the only ones acceptable to the Federal Aviation Administration (FAA), Office of Commercial Space Transportation (AST). Addressing all RLV safety-related systems activities in an SSPP even if they do not relate to public safety is acceptable; however, FAA/AST will only assess those matters that may impact public safety.

Leading The Way



COMPANY ABC, INC.

XYZ VEHICLE
SYSTEM SAFETY PROGRAM PLAN

CONTENTS

1.0 Introduction
2.0 System Safety Management
2.1 Purpose
2.2 Scope and Objectives
2.3 Tasks and Activities
2.4 System Safety Organization
2.4.1 Integration and Management of Associate Contractors
2.5 System Safety Program Milestones
2.6 Safety Requirements
2.7 Approaches to Reducing Risk
3.0 System Safety Engineering
3.1 Safety-Critical Systems and Events Identification
3.2 Hazard Analyses and Risk Assessment
3.2.1 Subsystem Hazard Analysis
3.2.2 System Hazard Analysis
3.2.3 Software Safety
3.2.4 Risk Assessment
3.2.5 Risk Acceptability Criteria
3.2.6 Risk Mitigation Measures
3.3 Validation and Verification
3.4 Operations and Maintenance
3.5 Anomaly Reporting and Corrective Action
3.6 Safety Risk Tracking
3.7 Additional Considerations

1.0 INTRODUCTION

This Company ABC, Inc., System Safety Program Plan (SSPP) for the XYZ Vehicle Program covers aspects of the design and development of the XYZ vehicle affecting public safety. Ground operations, launch facilities, support equipment, flight tests, and subsequent operations of the vehicle system are addressed.

System safety management and engineering tasks required during the life cycle of the XYZ vehicle to identify, evaluate, and eliminate hazards or to reduce the associated risk to a level acceptable to program management and the FAA are discussed. In addition, this plan provides direction and guidance between Company ABC and its associate contractors as to how the system safety program will be accomplished. In this SSPP, the term "associate contractors" refers to all contractors, subcontractors, suppliers, and vendors. Company ABC will ensure that all associate contractors supporting the XYZ Vehicle Program adhere to this SSPP.

The XYZ vehicle system safety program described in this plan will be conducted jointly by the system safety organizations of Company ABC and its associate contractors. In addition to providing the necessary resources, the system safety organizations of each company will coordinate and accomplish the tasks, activities, and data preparation required by Company ABC in accordance with this plan. Company ABC will give direction to the associate contractors to integrate the system safety program and provide a single point of contact for program management on system safety issues.

2.0 SYSTEM SAFETY MANAGEMENT

2.1 PURPOSE

The XYZ system safety program ensures that safety, consistent with Company ABC and FAA requirements, is designed into the XYZ vehicle, including its subsystems, supporting equipment, operations, and interfaces. During development of the XYZ vehicle, the emphasis will be on ensuring the safety of the uninvolved public and public property.

2.2 SCOPE AND OBJECTIVES

The XYZ vehicle is scheduled to start flight tests on Month/ Day /Year. Objectives of these flight tests are to obtain flight data. Specific goals include the following:

- Validation of the design
- Verification of vehicle performance
- Identification of system deficiencies
- Demonstration of safe operations

Following successful completion of the flight test program, the vehicle will become operational.

The principal system safety objective is to protect public health and safety and to ensure safe and successful flight operations can be conducted within acceptable risk limits. Other objectives of the system safety program are as follows:

- Identify hazards and implement safety features and requirements during the design phase that provide the optimum degree of system safety consistent with mission requirements.
- Ensure that system safety issues are properly considered with respect to conducting ground tests, ground servicing, initial flight tests, and flight and reentry operations of the XYZ vehicle.
- Contain risks to uninvolved public and property to acceptable levels during all phases of the XYZ Vehicle Program.

- Provide lessons learned for application to the design and operation of the XYZ vehicle.

2.3 TASKS AND ACTIVITIES

The tasks and activities will be accomplished by the system safety organization of Company ABC. Each associate contractor will perform a hazard analysis on the subsystems for which they have design responsibility. They will also prepare the corresponding portions of the System and Subsystem Hazard Analysis Reports in support of Company ABC's system safety effort (see appendix B). Unless otherwise stated, the approaches to the tasks and activities listed below apply to all phases of the program, including design, manufacture, and operations (which includes ground and flight test, launch, recovery, and maintenance).

2.4 SYSTEM SAFETY ORGANIZATION

The XYZ System Safety Program will be conducted jointly by the system safety organizations of the Company ABC and its associate contractors. Company ABC will act as the focal point of contact and primary integrator of all safety-related activities between Company ABC and other safety organizations. Company ABC will assign tasks to appropriate team members and ensure the safety requirements addressed by the XYZ System Safety Program are accomplished. The system safety tasks assigned to each associate team member will support the work agreed to by their respective organizations and take advantage of their safety expertise in specific areas.

Company ABC's safety official is the XYZ Vehicle Program System Safety Manager, John Doe. All safety personnel will report directly to the System Safety Manager. Mr. Doe reports directly to Company ABC Program Manager Jane Smith, who serves as the mission conductor. The safety official monitors and evaluates dress rehearsals to ensure that they are conducted in accordance with procedures identified in the regulations and to ensure the readiness of the safety operations personnel to conduct the mission under nominal and off-nominal conditions. The safety official monitors and reports to the mission conductor any non-compliance with procedures or representations in the license application. The mission conductor ensures that all the safety official's concerns are addressed both before a mission is started and before reentry or descent flight of the XYZ vehicle. Table 2.1 lists sample contact information for Company ABC's safety official and mission conductor.

Table 2.1. Company ABC Contact Information

COMPANY	NAME	TITLE	CONTACT
Company ABC	John Doe	Program System Safety Manager/Safety Official	(800) 123 - 4567
Company ABC	Jane Smith	Program Manager/Mission Conductor	(800) 123-7654

2.4.1 INTEGRATION AND MANAGEMENT OF ASSOCIATE CONTRACTORS

At the discretion of Company ABC, associate contractors will perform significant portions of the XYZ Vehicle Program. These organizations provide subsystems and components that are critical to the safety of the XYZ vehicle. System safety requirements for associate contractors will generally be imposed through statements of work (SOW), equipment specifications, and contract data requirements lists (CDRL). Because of the widely varied nature of the products and services provided, safety requirements for each product or service will be tailored on a case-by-case basis. Specific equipment safety requirements will be identified and included in equipment specifications. System safety program and task requirements will be specified in the SOW to ensure that safety is addressed in the equipment design and that associate

contractor efforts are integrated into the system safety program described in this plan. The CDRL requirements will specify data needed to document compliance with specification requirements, track hazards, and provide inputs to the hazard analysis process.

2.5 SYSTEM SAFETY PROGRAM MILESTONES

The XYZ vehicle is a new vehicle development program. As a result, the system safety program milestones are scheduled to coincide with the traditional design review milestones. System safety data will be prepared and available for the scheduled safety reviews. Updates will be provided as necessary by each company and coordinated by Company ABC. All analyses generated during the program will be available to all participants. Table 2.2 lists examples of major events and dates.

Table 2.2. XYZ Vehicle System Safety Program Milestones

REVIEW/TASK	PROJECTED SCHEDULE	STATUS
Preliminary Design Review (PDR)/Preliminary Hazard Analysis (PHA)	Month/ Day /Year	
Preliminary Hazard Review	Month/ Day /Year	
Critical Design Review (CDR)/Subsystem Hazard Analysis (SSHA)	Month/ Day /Year	
Subsystem Hazard Review	Month/ Day /Year	
First Flight Test Readiness Review/ System Hazard Analysis (SHA)	Month/ Day /Year	Complete Month/ Day /Year (Approximately 90 days before 1st flight)
System Hazard Review	Month/ Day /Year	
First Flight Test (Test does not meet definition of a launch vehicle.)	Month/ Day /Year	
Second Flight Test (Test does not meet definition of a launch vehicle.)	Month/ Day /Year	
First Operational Flight (FAA – Licensed)	Month/ Day /Year	
Second Operational Flight (FAA – Licensed)	Month/ Day /Year	

2.6 SAFETY REQUIREMENTS

Safety requirements will be established as a result of hazard analyses performed, validation and verification (V&V) efforts, use of lessons learned from similar programs, results of anomaly reporting and corrective action processes, and company design safety standards. Additionally, safety requirements for the XYZ Vehicle Program are identified through FAA regulations and Company ABC's use of guidance material. In general, safety requirements will be established to control the safety risk associated with individual hazards to levels acceptable to the Company ABC Program Management and FAA.

2.7 APPROACHES TO REDUCING RISK

For the XYZ Vehicle Program, the order of precedence for eliminating and mitigating risk is as follows:

a. *Design for minimum risk*. Company ABC's priority will be to design to eliminate risk. If the identified risk cannot be eliminated, then the risk will be reduced to an acceptable level through design selection.

b. *Incorporate safety devices.* If risks cannot be eliminated through design selection, then the risks will be reduced through the use of active and passive safety devices. Provisions for periodic functional checks of safety devices will be incorporated in the safety review process.

c. *Provide warning devices.* If neither design selection nor safety devices can effectively eliminate identified risks or adequately reduce risk, then warning devices will be used to detect the condition and to produce an adequate warning signal.

d. *Develop procedures and training.* If it is impractical to eliminate or reduce risks through design selection or specific safety and warning devices, then training and procedures will be incorporated to mitigate the risk.

In addition to the risk reduction order of precedence, XYZ vehicle safety-critical systems and functions will incorporate the following fault tolerance and risk mitigation approaches:

a. *Failure Tolerance.* The XYZ vehicle must be able to perform its function in the presence of faults within its hardware or software. This criterion applies to the XYZ operations when loss of a function or inadvertent occurrence of a function results in a hazardous event (risk to public safety).

b. *Fault Tolerant*. The XYZ vehicle safety-critical command and control functions will be designed to be at least two fault tolerant where applicable. No combination of two failures or operator errors shall result in the potential for loss of control of the vehicle or death or injury to the public.

c. *Risk Inhibitors*. A function that could lead to death or injury to the public shall be controlled by a minimum of three independent inhibits where possible, whenever the hazard potential exists. Monitoring of these inhibits shall be available to verify that at least two of the three inhibits are in place.

3.0 SYSTEM SAFETY ENGINEERING

Figure 3.0 depicts the Company ABC public safety strategy. Each step of Company ABC's system safety process is described in the following subparagraphs.

3.1 SAFETY-CRITICAL SYSTEMS AND EVENTS IDENTIFICATION

The identification of safety-critical systems will be undertaken as early as practicable in the life cycle of the XYZ Vehicle Program. Figure 3.1 shows a process for identifying safety-critical systems. The life cycle will be divided into the following six phases:

- Conception
- Research and Development (R&D)
- Design
- Deployment
- Operation
- Decommissioning and Disposition

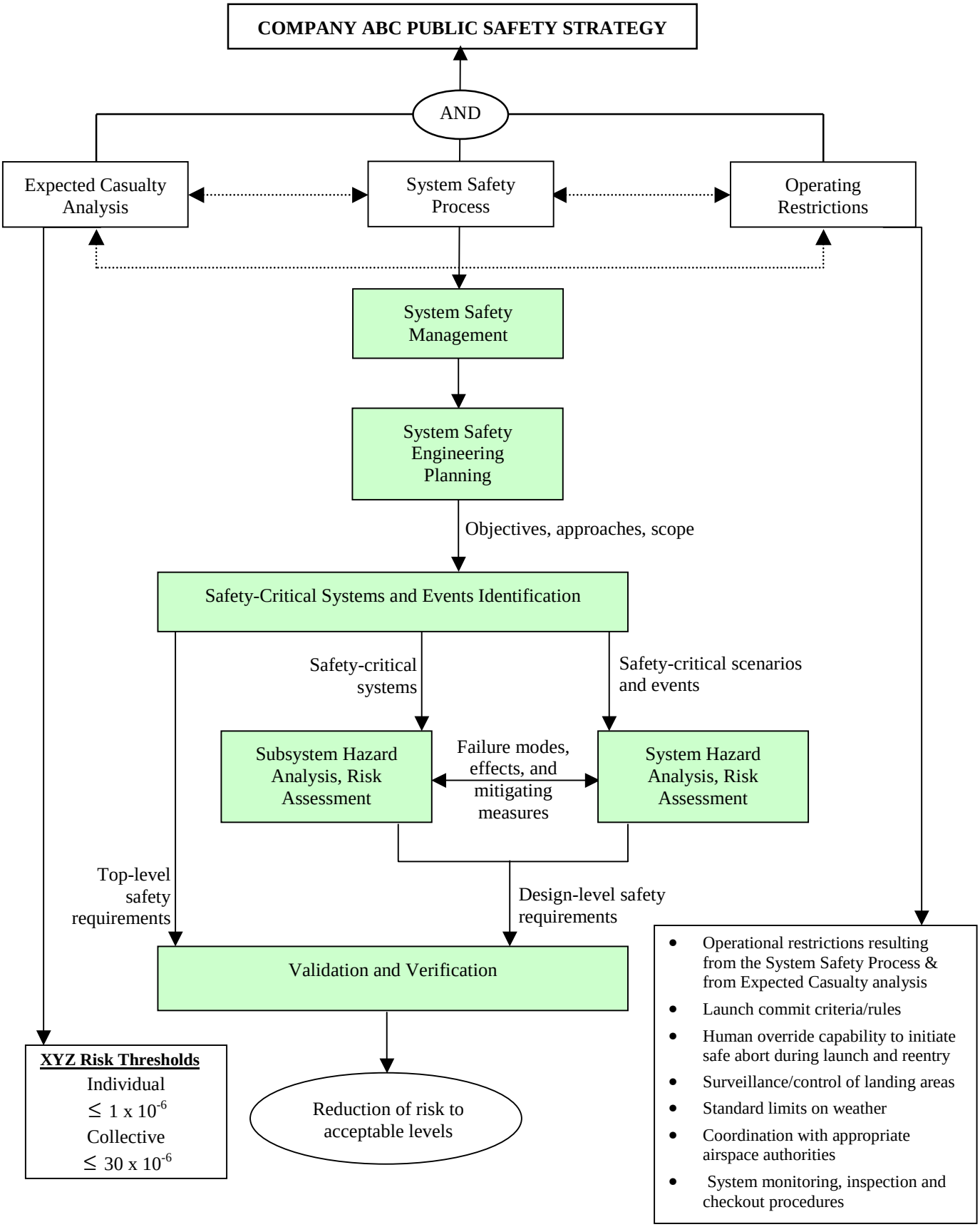


Figure 3.0. Company ABC Public Safety Strategy

Company ABC will employ a PHA and an Event Tree Analysis (ETA) for identifying the safety-critical systems and events. Additional safety-critical systems will also be derived from company operating practices, standard industry practices, and regulations. Outputs from the identification of safety-critical systems include, but are not limited to, top-level safety requirements as well as safety-critical systems, scenarios, and events (see figure 3.1).

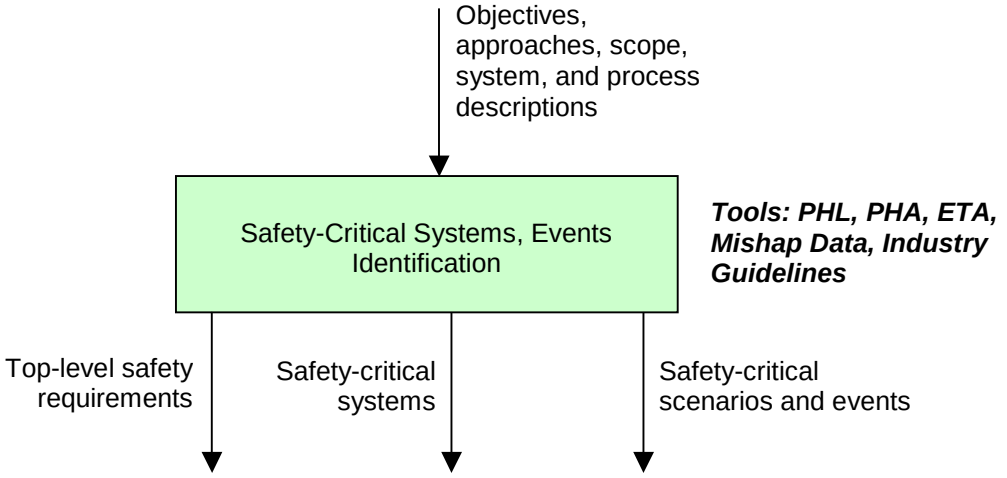


Figure 3.1. Identification of Safety-Critical Systems

Preliminary Hazard Analysis will be started as soon as design work has begun so that safety considerations are used to evaluate design alternatives and trade studies. The PHA is used to identify hazards and aid in establishing safety requirements as early in the program as possible. A common format for the PHA will be used to aid in tracking and transfer of risk reports between Company ABC and associate contractors where necessary. The PHA will serve as the baseline for performing future analyses. See appendix B for details and examples of the risk report format.

The PHA and resulting descriptions of the safety-critical systems and events will be presented at the Company ABC Preliminary Design Review (PDR). Associate contractors are responsible for performing the analyses and submitting these analyses to Company ABC for that portion of the XYZ vehicle design or operation for which they have accepted responsibility. Company ABC will consolidate results and keep them available for program management and FAA review.

3.2 HAZARD ANALYSES AND RISK ASSESSMENT

Analyses will be performed to identify hazards, their causes and effects, controls to eliminate or mitigate the hazards, risk assessment, and status of hazard resolution (see figure 3.2). For the XYZ Vehicle Program, the intent is to have a database containing all of the hazards involved with the total system throughout its life cycle. Within this database, individual hazards will be identified as relating to the areas normally covered in the traditional hazard analyses.

Hazard analyses are performed to identify hazards during ground and flight tests. They include the hazards in the equipment, procedures, hardware, and software necessary to complete safe and successful tests in all areas of testing (development, qualification, and acceptance). These types of hazards are included in the database.

3.2.1 SUBSYSTEM HAZARD ANALYSIS

Immediately after the PDR, Company ABC will perform a FMECA. Company ABC, associate contractors, or both, will perform the analysis on the portion of the system for which they are responsible, in the format outlined in appendix B. This analysis will be based on detailed subsystem design data, PHA results, and safety design requirements for the subsystem. The FMECA must be complete by the Critical Design Review (CDR) to the point that all subsystem failure modes and hazards have been identified, mitigating actions have been planned, and verification requirements for these hazards have been identified. The FMECA and resulting failure modes and effects will be briefed at the CDR and made available to XYZ program management and FAA.

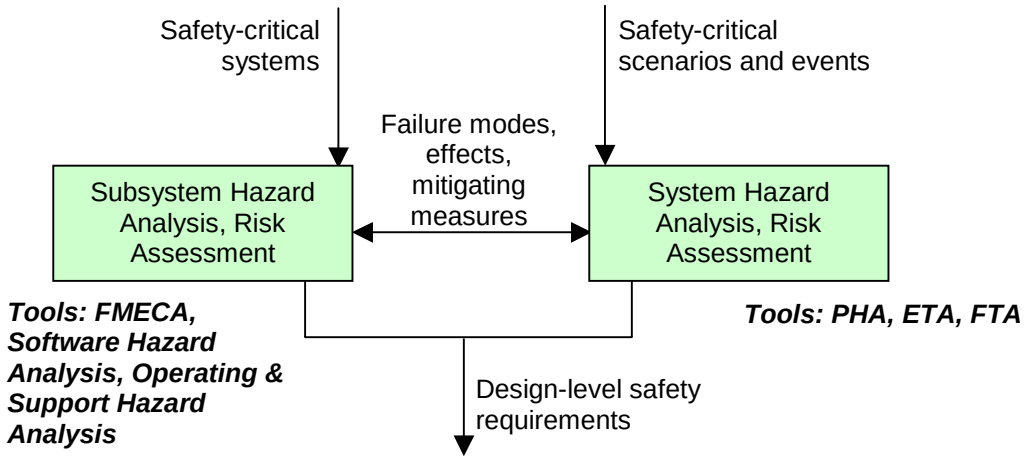


Figure 3.2. Hazard Analysis and Risk Assessment

3.2.2 SYSTEM HAZARD ANALYSIS

Company ABC will perform a Fault Tree Analysis (FTA). It will incorporate each company's FMECA into a system level analysis, with emphasis on system interfaces and interactions. Company ABC and associate contractors will ensure that all hazards discovered since the CDR have been added to their respective FMECA. The FTA will be presented at the First Flight Test Readiness Review. Work on the analysis will continue past this time, however, until all actions required on identified hazards have been completed.

3.2.3 SOFTWARE SAFETY

Software and firmware hazard analysis is imbedded in the XYZ vehicle hazard analysis process through the system PHA, FMECA, and FTA. Potential software causes for all hazards are to be addressed on each risk report (see appendix B). Additional or detailed software hazard analysis requirements may be identified through the FMECA and a software-specific PHA or FTA.

3.2.4 RISK ASSESSMENT

Risk is a function of the combination of the severity (consequences) and the likelihood (frequency of occurrence) levels illustrated in tables 3.1 and 3.2. The risk assessment will generally be qualitative and will be performed with respect to risk to public health and safety. Qualitative measures of hazard severity categories are defined in table 3.1, and table 3.2 lists hazard likelihood categories.

3.2.5 RISK ACCEPTABILITY CRITERIA

The acceptability of risk will be determined for individual hazards by comparing the Hazard Risk Index (HRI) with the HRI acceptability criteria. The HRI is a number from 1 to 20, which ranks the risk, with 1 representing the maximum risk. Hazards with the lowest HRIs will receive priority for corrective action. The matrix in figure 3.3 shows HRI values and acceptability criteria corresponding to the qualitative severity and likelihood categories.

Table 3.1. Hazard Severity

DESCRIPTION	CATEGORY	MISHAP DEFINITION
Catastrophic	I	Death to uninvolved public or safety-critical system loss.
Critical	II	Severe injury or illness to the uninvolved public, or major safety-critical system damage.
Marginal	III	Minor injury, illness, or safety-critical system damage.
Negligible	IV	Less than minor injury, illness, or safety-critical system damage.

Table 3.2. Hazard Likelihood

DESCRIPTION	LEVEL	INDIVIDUAL ITEM
Frequent $(X > 10^{-1})$	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in any one mission.
Probable $(10^{-1} > X > 10^{-2})$	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in any one mission.
Occasional $(10^{-2} > X > 10^{-3})$	C	Likely to occur sometime in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in any one mission.
Remote $(10^{-3} > X > 10^{-6})$	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in any one mission.
Improbable $(10^{-6} > X)$	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in any one mission.

Severity / Frequency	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
Improbable (E)	12	15	17	20

Level	Index	Hazard Risk Acceptability Criteria
High	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below "II" or reduce the likelihood of occurrence below "C".
Medium	7 - 10	If not controlled, the risk must be accepted by Program Management and FAA.
Low	11 - 20	Project Management decides on actions, if any.

Figure 3.3. Hazard Risk Index Matrix

3.2.6 RISK MITIGATION MEASURES

To reduce the risk to the uninvolved public during conduct of operations, Company ABC will implement additional risk mitigation measures, including performing a flight hazard area analysis and using a flight safety system (FSS). This system will be designed to limit or restrict hazards by initiating and accomplishing a controlled ending to flight, thereby preventing the vehicle from reaching a populated area in the event of a failure. The XYZ vehicle will use a thrust termination system as the FSS to end the flight whenever the vehicle strays outside of a predefined envelope. By identifying specific safety-critical failure modes, timelines of safety-critical events, consequences, and risks to the public, the system safety process will determine the circumstances when an FSS is necessary as a mitigation measure.

The XYZ vehicle flight hazard area analysis will identify any regions of land, sea, or air that must be monitored, publicized, controlled, or evacuated to control risks from debris impact hazards. This analysis will establish the ship and aircraft hazard areas for Notices to Mariners and Notices to Airmen. In addition, the system safety process will identify when the public is potentially at risk based on safety-critical failure modes and events and if a flight hazard area analysis is necessary. This analysis will account for the following items:

- Regions of land, sea, and air potentially exposed to debris resulting from normal flight events and from potential malfunctions.
- Waterborne vessels or aircraft exposed to debris from events resulting from potential normal or abnormal flight events, including vehicle malfunction.
- Operational controls implemented to control risk to the public from debris hazards.

- Debris identified from debris analysis.
- Vehicle trajectory dispersion effects in the surface impact domain.

3.3 VALIDATION AND VERIFICATION

The V&V process shall apply to all levels of safety requirements captured throughout the life cycle of the system. The process will determine that the correct safety-critical system is being built (validation), as represented by a correct set of safety-critical requirements, and that XYZ vehicle design solutions meet all the safety-requirements (verification). The V&V process used by Company ABC to manage and document the set of safety requirements is in alignment with the FAA/AST *Guide to Reusable Launch Vehicle Safety Validation and Verification Planning,* Version 1.0, September 2003.

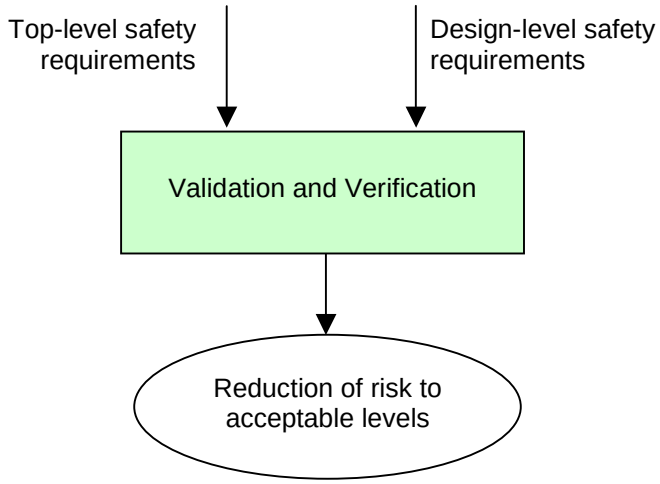


Figure 3.4. Validation and Verification

3.4 OPERATIONS AND MAINTENANCE

The Operations and Maintenance (O&M) process applies to all levels of safety requirements captured throughout the life cycle of the system. This process will determine the O&M programs and safety data necessary to ensure that safety is maintained before and during each flight of the XYZ vehicle. Company ABC will provide a maintenance program that addresses safety-critical system and subsystem maintenance and refurbishment considerations. This process will identify and track limited life items throughout the life cycle of the XYZ Vehicle Program.

The operations program will address operating procedures and processes for conducting safe operations over the lifetime of the XYZ Vehicle Program. The O&M process implemented by Company ABC is in alignment with the FAA/AST *Guide to Commercial Reusable Launch Vehicle Operations and Maintenance,* Version 1.0, May 2005.

3.5 ANOMALY REPORTING AND CORRECTIVE ACTION

Company ABC will establish an anomaly reporting and corrective action system to support anomaly identification, tracking, reporting, and disposition. This system will allow Company ABC to implement design improvements and corrections as part of the design process. Data collected will support tracking the root cause of problems. The corrective action system will continue to be used to support upgrading system O&M performance. Anomalies with potential safety implications occurring in a system or subsystem of a

launch vehicle during verification activities, prelaunch processing, launch, flight, or post-launch processing will be reported to the FAA/AST for review. Company ABC will notify the FAA/AST of all anomaly reviews, meetings, or both. In addition, Company ABC will provide the FAA/AST copies of the briefings, reports, meeting minutes, and actions identified and taken to address these anomalies.

3.6 SAFETY RISK TRACKING

All hazards discovered, including those resolved informally, shall be recorded on a risk report (see appendix B). To ensure that the actions taken to control the risks are acceptable to system safety and program management, the risk reports will be used to track identified hazards. The signatures of the originator, Company ABC System Safety Manager, and Company ABC Program Manager will be required to dispose of all risk reports.

3.7 ADDITIONAL CONSIDERATIONS

Company ABC has listed additional scheduled safety-related tasks and activities that have system safety imbedded within them. Table 3.3 lists the tasks and activities usually performed by other organizations or disciplines, including associate contractors, which apply most directly to the system safety tasks.

Table 3.3. Additional Safety-Related Tasks

ORGANIZATION/ DISCIPLINE/ ACTIVITIES	SAFETY RELATED TASK
System Safety Data	*Documentation of safety data*. Company ABC will document safety data. Examples of this data include anomaly reports, procedures, test data, hazard reports, lessons learned, and associate contractor safety effort deliverables. The system safety process will include the means for describing, collecting, and processing this safety data.
Configuration Management	*Tracking of changes.* Development of any system requires that changes be made throughout the life cycle. Changes to the vehicle, especially on safety-critical systems, can have significant impacts on public safety. At a minimum, Company ABC will implement a configuration control process to identify components, subsystems, and systems; establish baselines and traceability; and track changes to the configuration and system safety documentation.
Quality Assurance (QA)	*Establishment of a quality assurance program*. Company ABC will establish a QA program. This program will be suitable to Company ABC system safety objectives; QA program management; vehicle and hardware acceptance; QA engineering; supplier selection, quality surveillance, and audits; production quality performance and evaluation; verification; configuration assurance; calibration; metrology; test assurance; material, nonconformance, and process reviews; and corrective action identification, quality data collection, and reporting.
Reliability	*Performance of reliability analyses.* Company ABC will perform reliability analysis, predictions, critical item

ORGANIZATION/ DISCIPLINE/ ACTIVITIES	SAFETY RELATED TASK
	identification, testing and demonstration, and FMECA. Results of these analyzes will be used to develop parts selection and derating criteria and to identify and resolve reliability issues on safety-critical systems.
Training	*Development of training plans.* Designing safety into the system requires that personnel involved in system development, production, and operation understand and practice operations and procedures that protect the public safety. Training can help ensure that personnel can produce a safe system or operation. Training used as a risk mitigation measure will be identified as such. Training is a critical element in helping ensure the safety of the public.

APPENDIX B
RISK REPORT FORMAT

This appendix provides a format for reporting all hazards associated with the operation of reusable launch, reentry, or both vehicles. The format is designed to allow for ease of hazard tracking, flexibility in analysis presentation, and reduction of time and effort in report preparation. Such reports should include the following information:

- Report number
- Company name
- Hazard title
- Analysis phase
- Initial date of the report
- Closeout date of the report
- Originator
- Hazard status (initial and closeout frequency, severity, and Hazard Risk Index)
- Mission phase
- Risk level (frequency and severity)
- Hazard Risk Index acceptability criteria
- System
- Subsystem
- Controlling documents
- System function
- Hazard description
- Failure modes and causes
- Effects
- Mitigation of hazard and controls
- Verification methods and documentation
- Closure signatures (originator, safety system manager, and program manager)

The FAA does not generate or require use of specific forms for submission of risk reports. Elements from this format have been used to show a simple form that a company might create for its risk reporting functions. Although this appendix demonstrates use of the format as a form, other approaches to presenting this information are acceptable. Regardless of the approach used in presenting the needed information, closure of a risk report should have the signature of the report originator, system safety manager, and program manager.

Examples of risk reports Company ABC might submit as part of an RLV license application presented in this appendix include two examples from a Failure Modes, Effects, and Criticality Analysis and one example from a Preliminary Hazard Analysis. In addition, a blank copy of a sample risk report form is provided.

RISK REPORT NO.: 1.0

Company:	Company ABC, Inc.
Hazard Title:	Primary Load Structural Failure: Vehicle Airframe Failure
Analysis Phase:	Failure Modes, Effects, and Criticality Analysis (FMECA)

	Initial	**Closeout**
Date	12/ 5/ 00	4/15/02
Originator	John Doe, XYZ	

Hazard Status:

	Frequency*	**Severity***	**HRI***
Initial	D	I	8
Closeout	D	I	8

*See FAA Advisory Circular 431.35-2A

Mission Phase:					
		Prelaunch to Launch		X	Descent
	X	Ascent			Landing/Recovery
	X	On-Orbit to Reenty			Post-launch

Risk Level: (See FAA Advisory Circular 431.35-2A for explanation of risk level.)

Severity / Frequency	**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**
Improbable (E)	**12**	**15**	**17**	**20**

Level	**Index**	**Hazard Risk Index Acceptability Criteria**
High (Red)	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below “II” or reduce the likelihood of occurrence below “C”.
Medium (Yellow)	7 - 10	If not controlled, must be presented to Program Management and FAA as accepted risk.
Low (Green)	11 - 20	Project Management decides on actions, if any.

RISK REPORT NO.: 1.0

System: Main Structure: Vehicle Airframe	**Subsystem:** Wings, booms, stabilizers, fuselage	**Controlling Doc. (Name, #, etc.):** Systems Requirements Database XXX
Function: Primary load-carrying structure		
Hazard Description: Overload failure of primary structural load path—most critical at or near maximum dynamic pressure or maximum acceleration—consider wings, booms, stabilizers.		
Failure Mode(s)/Cause(s): Structural failure caused by aerodynamic loading, inadequate maintenance, or improper flight test procedures		
Effect: Loss of control, loss of vehicle—show by simulation likely worst-case trajectories of intact vehicle		
Mitigation of Hazard/Controls: Structural analysis showing minimum 1.5 factor of safety on design limit loads on critical structures; see Vehicle Design Document (VDD) for specific results. Pre- and post-flight vehicle inspections in accordance with approved maintenance plan and specific checklists. Static proof tests of specific structural elements.		
Verification Method(s) & Documentation: (1) Loads are defined in VDD, sec. 1.0, Jan 2004 Structural Analysis PowerPoint package (ref 39). (2) Crew chief Pre- & Post Checklist & Systems Requirements Database Inspection Plan. (3). VDD, sec. 1.0; proof test plans for critical structures (most); flight load comparison plots between maximum test loads experienced to date and the maximum expected flight loads. (4) Process described and representative plots at the Jan 2002 Technical Interchange Meeting (TIM). See TIM minutes (ref. 14).		
Additional Remarks:		

Closure Signatures

Originator: _____

System Safety Manager: _____

Program Manager: _____

RISK REPORT NO.: 2.1

Company:	Company ABC, Inc.
Hazard Title:	Uncontrolled Crash: Propulsion Shutdown System
Analysis Phase:	Safety-Critical System Identification: Preliminary Hazard Analysis (PHA)

	Initial	**Closeout**
Date	12/ 5/ 01	4/15/02
Originator	John Doe, XYZ	

Hazard Status:

	Frequency*	**Severity***	**HRI***
Initial	B	II	5
Closeout	D	II	10

*See FAA Advisory Circular 431.35-2A

Mission Phase:					
		Prelaunch to Launch			Descent
	X	Ascent			Landing/Recovery
		On-Orbit to Reenty			Post-launch

Risk Level: (See FAA Advisory Circular 431.35-2A for explanation of risk level.)

Severity / Frequency	**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**
Improbable (E)	**12**	**15**	**17**	**20**

Level	**Index**	**Hazard Risk Index Acceptability Criteria**
High (Red)	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below “II” or reduce the likelihood of occurrence below “C”.
Medium (Yellow)	7 - 10	If not controlled, must be presented to Program Management and FAA as accepted risk.
Low (Green)	11 - 20	Project Management decides on actions, if any.

RISK REPORT NO.: 2.1

System: Vehicle propulsion system	**Subsystem:** Propulsion shutdown system	**Controlling Doc. (Name, #, etc.):** Vehicle Operations Handbook

Function:

The propulsion shutdown system terminates thrust during nominal and off-nominal operations.

Hazard Description:

Component failure, software faults, human error, environmental impacts, or any combination thereof, could lead to the inability to shut down the engine with the potential for an uncontrolled crash in populated areas.

Failure Mode(s)/Cause(s):

Not applicable to this analysis phase. Preliminary Hazard Analysis does not normally include failure modes and causes.

Effect:

Not applicable to this analysis phase. Preliminary Hazard Analysis includes the effect in the hazard description.

Mitigation of Hazard/Controls:

(1) Use redundant engine shutdown systems with different methods of operation, such as an automated system (valve with software-driven controller) and a manual system (manually operated valve). (2) Incorporate operating and training procedures to operate manual shutdown system.

Verification Method(s) & Documentation:

Not applicable to this analysis phase.

Additional Remarks:

See risk report No. 3.2 for description of one safety-critical system failure mode for this hazard.

Closure Signatures

Originator: _____

System Safety Manager: _____

Program Manager: _____

RISK REPORT NO.: 3.2

Company:	Company ABC, Inc.
Hazard Title:	Main Propellant Feed Valve Failure
Analysis Phase:	Subsystem Hazard Analysis (FMECA)

	Initial	**Closeout**
Date	3/ 5/ 02	6/15/02
Originator	John Doe, XYZ	

Hazard Status:

	Frequency*	**Severity***	**HRI***
Initial	C	II	6
Closeout	D	II	10

*See FAA Advisory Circular 431.35-2A

Mission Phase:					
		Prelaunch to Launch			Descent
	X	Ascent			Landing/Recovery
		On-Orbit to Reenty			Post-launch

Risk Level: (See FAA Advisory Circular 431.35-2A for explanation of risk level.)

Severity / **Frequency**	**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**
Improbable (E)	**12**	**15**	**17**	**20**

Level	**Index**	**Hazard Risk Index Acceptability Criteria**
High (Red)	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below “II” or reduce the likelihood of occurrence below “C”.
Medium (Yellow)	7 - 10	If not controlled, must be presented to Program Management and FAA as accepted risk.
Low (Green)	11 - 20	Project Management decides on actions, if any.

RISK REPORT NO.: 3.2

System: Vehicle propulsion system	**Subsystem:** Main propellant valve	**Controlling Doc. (Name, #, etc.):** Vehicle Operations Handbook

Function:

The main propellant valve is a manually controlled valve used to shut off the propulsion system during nominal and off-nominal operations

Hazard Description:

See Effect below.

Failure Mode(s)/Cause(s):

Manufacturing process error or contamination causes the main propulsion valve to remain open or partially open when commanded to shut down.

Effect:

Failure to shut down the propulsion system could result in the potential to provide thrust after shutdown command, leading to possible crash in a populated area.

Mitigation of Hazard/Controls:

(1) Use high-reliability valve designed to XYZ Standard 126-P. (2) Use redundant valve in series that uses an automated programmable logic controller to shut down propulsion system in the event of failure of the manual valve.

Verification Method(s) & Documentation:

(1) Inspect and operate the valve before flight per Mission Procedure Checklist 26. (2) Acceptance tests of valve per XYZ Standard 126-P – test results provided at 2/15/02 TIM. (3) System tests of valve operation during envelope expansion tests per Vehicle Flight Plan item 35.

Additional Remarks:

See risk report 2.1 for description of hazard of this failure mode.

Closure Signatures

Originator: _____

System Safety Manager: _____

Program Manager: _____

RISK REPORT NO.: _____

Company:	
Hazard Title:	
Analysis Phase:	

	Initial	Closeout
Date		
Originator		

Hazard Status:

	Frequency*	Severity*	HRI*
Initial			
Closeout			

*See FAA Advisory Circular 431.35-2A

Mission Phase:					
		Prelaunch to Launch			Descent
		Ascent			Landing/Recovery
		On-Orbit to Reenty			Post-launch

Risk Level: (See FAA Advisory Circular 431.35-2A for explanation of risk level.)

Severity / Frequency	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
Improbable (E)	12	15	17	20

Level	Index	Hazard Risk Index Acceptability Criteria
High (Red)	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below "II" or reduce the likelihood of occurrence below "C".
Medium (Yellow)	7 - 10	If not controlled, must be presented to Program Management and FAA as accepted risk.
Low (Green)	11 - 20	Project Management decides on actions, if any.

RISK REPORT NO.: _____

System:	**Subsystem:**	**Controlling Doc. (Name, #, etc.):**
Function:		
Hazard Description:		
Failure Mode(s)/Cause(s):		
Effect:		
Mitigation of Hazard/Controls:		
Verification Method(s) & Documentation:		
Additional Remarks:		

Closure Signatures

Originator: _____

System Safety Manager: _____

Program Manager: _____



Patricia Grace Smith July 20, 2005
Associate Administrator for
Commercial Space Transportation