Integrating Launch Vehicle Safety and Reliability Analyses

Terry L. Hardy; Federal Aviation Administration, Office of Commercial Space Transportation; Washington, DC, USA

Keywords: Safety analysis, Reliability analysis, Launch vehicle

Abstract

A number of safety and reliability analysis tools are available to identify potential safety and reliability problems and to meet specified requirements. Traditionally, safety and reliability analyses are performed independently, often by different organizations. However, separate safety and reliability analyses can require significant resources, especially in new launch vehicles using innovative designs, and can lead to inaccuracies and inconsistent results. By integrating safety and reliability analyses, a launch vehicle developer can use these tools more efficiently and effectively to improve both safety and reliability. This paper describes a process for integrating a traditional system safety process with reliability analyses and provides a simplified example of how those analysis tools might be used for a sample reusable launch vehicle.

Introduction

The Federal Aviation Administration (FAA) Office of Commercial Space Transportation (AST) is responsible for regulating and licensing commercial space transportation to, among other things, ensure public health and safety and the safety of property. In fulfilling its responsibilities, AST issues licenses for the operation of launch and reentry vehicles and launch and reentry sites. AST also issues experimental permits for suborbital reusable launch vehicles (RLV). The components of the AST licensing process include a pre-licensing consultation and an application evaluation consisting of a policy review, payload review, safety evaluation, financial responsibility determination, and an environmental review.

A launch vehicle license applicant uses system safety analyses to systematically identify and control hazards throughout the life cycle of a vehicle program, program or activity to prevent accidents and mishaps. Accidents and mishaps are prevented by proactively identifying, assessing and eliminating or controlling safety-related hazards to reduce the risk to the uninvolved public to acceptable levels as determined by existing regulations. Reliability also plays a role in ensuring safety because the risk to the public can depend on the probability of failure of safety-critical system elements and the consequences of those failures. Reliability analyses are qualitative or quantitative tools used to determine whether an item will perform as intended for a specified interval under foreseeable operating conditions. Reliability analysis tools are used to provide risk assessment data to support launch vehicle system safety analyses, including inputs to quantitative risk assessments.

System safety analyses and reliability analyses are often performed independently in a traditional approach to analyzing the risk to the uninvolved public. However, separate analyses can lead to inconsistent and possibly inaccurate results, often because different assumptions and data are used for each analysis. An integrated approach to safety and reliability is especially important in the context of AST's mission because its highest concern is for those failures that result in increased risk to the uninvolved public. Integrating safety and reliability analyses can also help provide additional clarity and structure to the analyses used to develop the vehicle design. This paper presents an approach to integrating safety and reliability analyses for launch vehicle applications. AST does not require an integrated approach to obtain a license or permit, but the launch vehicle developer can use this methodology to improve both reliability and safety. This paper also presents a simplified example of how this integrated approach to analyzing safety and reliability can be used for a sample RLV.

System Safety Engineering Process

FAA regulations (14 CFR part 431, subpart C, Safety Review and Approval for Launch and Reentry of a Reusable Launch Vehicle) require that a launch vehicle developer seeking an RLV license employ a system safety process to identify hazards and assess the risks to public health and safety and the safety of property associated with the

mission. As described in Advisory Circular (AC) 431.35-2 (ref. 1), the system safety process is the structured application of system engineering and management principles, criteria, and techniques to address safety within the constraints of operational effectiveness throughout all phases of a system's life cycle. The intent of the system safety process is to identify, eliminate, or control hazards to acceptable levels of risk throughout a system's life cycle. According to AC 431.35-2, the general methodology of a system safety engineering process is shown in Figure 1.

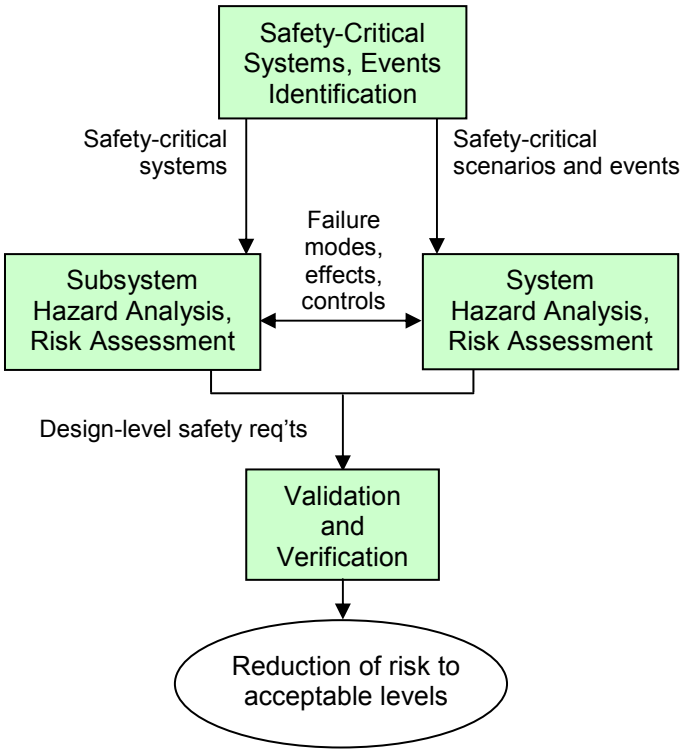

Figure 1 – Reusable Launch Vehicle System Safety Engineering Process

Safety-Critical Systems and Events Identification:

The first step in the system safety engineering process is to identify safety-critical systems and events. As defined in FAA regulations, 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 so it does not jeopardize public safety. Analytical approaches are often used to identify the safety-critical systems and events. Some of the most common analytical approaches for identifying safety-critical systems and events include Preliminary Hazard Analyses (PHA) and Event Tree Analyses (ETA). A PHA produces a line item tabular inventory of nontrivial system hazards, and an assessment of their remaining risk after countermeasures have been imposed. An ETA is a system analysis technique that explores responses to an initiating event and enables assessment of success and failure probabilities (ref. 2). Safety-critical systems can also be determined using industry guidelines, mishap data, and experience with similar systems. The outputs from this step include top-level safety requirements (e.g., "All composite structures shall be proof tested to 110 percent of the maximum expected flight load per Company Standard XYZ"), identification of safety-critical systems, and identification of safety-critical scenarios and events.

Subsystem Hazard Analysis and Risk Assessment:

Once the safety-critical subsystems, components, and events have been identified, a launch vehicle developer would perform an analysis to identify hazards associated with those subsystems, components, and events, and then to assess the risks associated with those hazards. Risk assessment is the process of identifying, characterizing,

quantifying and evaluating risks in terms of likelihood and severity. Generally, performing a risk assessment requires answering three questions (ref. 3):

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

The answers to these questions require the use of systematic methods for identifying and characterizing the risks. These methods usually include both "bottom-up" subsystem analyses and "top-down" system analyses. One acceptable subsystem hazard analysis and risk assessment method is a Failure Modes, Effects, and Criticality Analysis (FMECA), which is a bottom-up (inductive) system analysis technique by which each potential failure mode in a system is analyzed to identify the consequences and determine the severity and likelihood of occurrence (ref. 4). Based on the assessment of risk and whether that risk is acceptable, a developer would take steps to mitigate or eliminate the risk by designing for minimum risk, incorporating safety devices, providing warning devices, or developing procedures and training. Outputs of the subsystem hazard analysis include design-level safety requirements (for example, "The wing attach bolts must be designed to withstand a maximum wing load of 'X' with a safety factor of 'Y'"), generated based on the mitigation measures chosen.

System Hazard Analysis and Risk Assessment:

Many mishaps are the result of a confluence of factors, including mechanical failure, software, human error, procedures, the environment, and system design, and these factors may not be represented in the subsystem analyses. Therefore, system hazard analysis and risk assessments may be required to supplement the bottom-up, subsystem risk assessment to capture these factors and to analyze combinations of faults, failures, and conditions. System risk assessment usually consists of scenario modeling and top-down (deductive) failure modeling. The scenario and failure models are often developed based on safety-critical events, failure modes, effects, and mitigation measures developed from the earlier tasks of identifying safety-critical systems and performing subsystem hazard analysis and risk assessment. Acceptable methods for performing scenario modeling include Event Tree Analysis and Preliminary Hazard Analysis. Fault Tree Analysis (FTA) is one acceptable method for performing failure modeling. An FTA is a top-down graphical logic model that systematically identifies all possible causes leading to the top event (ref. 5). The output from the system hazard analysis and risk assessment includes design-level requirements. The system hazard analysis may also be used to identify additional failure modes, effects, and mitigation measures that can then be analyzed further on a subsystem level.

Validation and Verification:

The next step in the system safety engineering process is validation and verification of the safety requirements developed in the previous steps of the process. Validation is the process of determining that the safety-critical requirements for a launch vehicle and its operations are correct, clear, complete, consistent, and feasible. In other words, validation assures that the correct system is being built. Verification is the evaluation to determine that applicable safety-critical requirements and operations have been met. A verified system shows measurable evidence that it complies with the overall system safety needs. Four acceptable methods of verifying safety requirements include analysis, test, demonstration, and inspection. A launch vehicle developer will often use these methods in combination. The acceptability of one method over another depends on feasibility as well as maturity of a launch vehicle and its operations (ref. 6).

Note that although the system safety engineering process is presented here in a linear, one-pass fashion, the process is in fact iterative. As the life cycle progresses, additional safety-critical systems, hazards, failure modes, mitigation measures, and safety requirements may be identified, modified or eliminated.

Reliability Analyses

As described in reference 7, reliability analyses can provide input to the system safety engineering process in the following areas:

- Identifying potential reliability or safety problems and the risks associated with those problems. For example, a reliability analysis might be used to determine failure modes and effects.
- Comparing alternate designs to improve reliability and eliminate or mitigate safety problems. For example, an analysis can help in identifying mitigation measures or in analyzing the effects of component failures on reliability of safety-critical systems.
- Assisting in defining operational, test and safety requirements. For example, the analysis could result in requirements for hardware, software, procedures, and training to reduce the risks identified.
- Providing results that can be used to evaluate whether safety criteria and requirements have been met. For example, reliability data could be included as part of the validation and verification effort to determine whether an item will perform its intended function under specified conditions.

Figure 2 shows how reliability analyses are integrated into the system safety process.

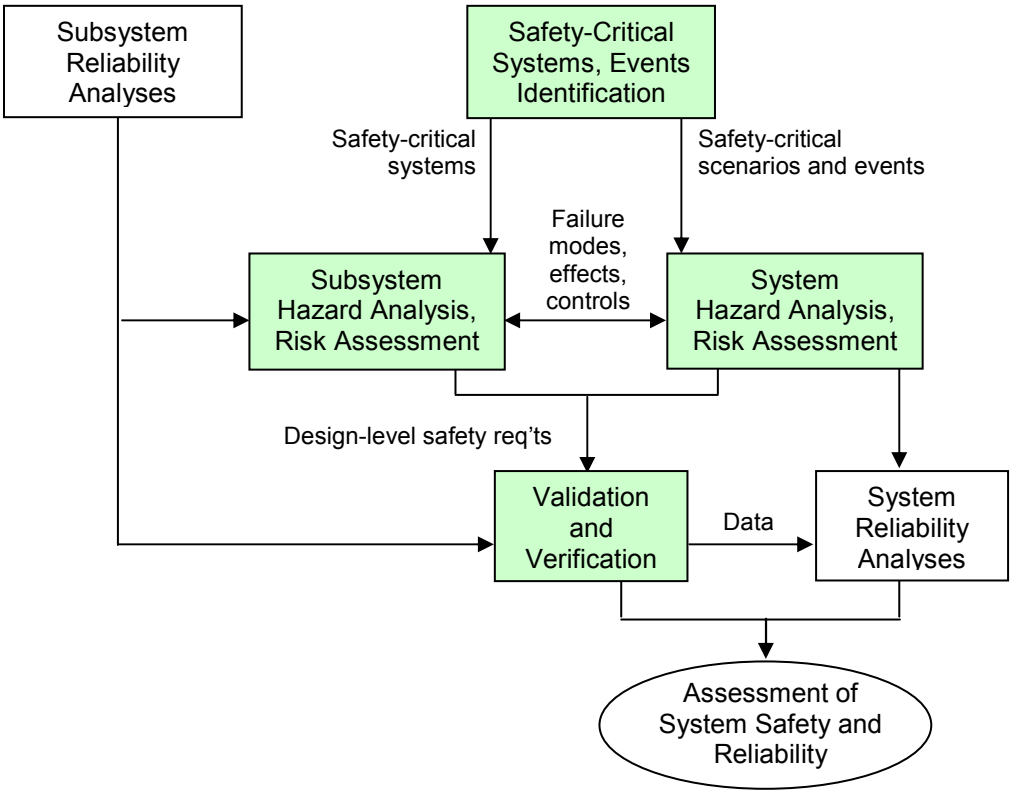

Figure 2 – Integrating Reliability Analyses into the System Safety Engineering Process.

After identifying safety-critical systems and events, the launch vehicle developer may perform subsystem hazard analyses. A subsystem reliability analysis can be used to provide input to this subsystem hazard analysis by providing probability of failure estimates that are used in the assessment. Alternatively, the subsystem reliability analysis may be used to help identify effects of failures that could ultimately result in hazards. A subsystem hazard analysis may also provide input to the validation and verification process by providing probability of failure estimates used to meet safety requirements. A system hazard analysis is often used as an input to a system reliability analysis to help estimate the vehicle probability of failure. This system reliability analysis uses data obtained during the validation and verification process to assist in estimating vehicle reliability.

A launch vehicle developer can apply some of the same techniques used for system safety to reliability analyses. In analyzing system safety, a developer will often use FMECA, ETA, and FTA qualitatively to identify hazards and risks. When analyzing reliability, defined as the probability that an item will perform its intended function for a

specified interval under stated conditions, these same methods can be used quantitatively by applying appropriate mathematical relationships. For example, MIL-STD-1629A (ref. 4) describes a method for obtaining reliability estimates using an FMECA. Therefore a developer can perform the subsystem safety analysis and subsystem reliability analysis using the same analytical tool. A Fault Tree Analysis or Event Tree Analyses can also yield reliability estimates using Boolean logic and input probabilities (ref. 5). A launch vehicle developer could therefore produce a system event tree to help identify safety-critical scenarios, and then use a fault tree to quantify pivotal events, thereby combining the system safety and reliability analyses. This developer could also use an FMECA to assist in determine component failure rates based on the verification effort and resulting problem reports and corrective action analyses, and use this data as input to quantify the fault tree. In performing these quantitative reliability analyses, it is important to explicitly analyze the parameter and model uncertainty. A developer can use Monte Carlo simulation to assist in analyzing this uncertainty. Monte Carlo simulation is an approach where a logical model of a system is repeatedly evaluated using random values for the input parameters (ref. 8). Ultimately, the resulting analysis will provide estimates of vehicle or system reliability based on the system safety engineering process, leading to a conditional probability of failure based on system safety.

It is important to note that reliability and safety are not the same, as discussed in reference 9. Safety is a system property, not a component property. This means that safety can only be determined by considering the reliability of a component in relation to other components in the system as well as the external environment, with consideration to the intended use of that component. For example, a relay contact could be used to signal an elevator to return to the bottom floor of a building and open the doors in the event of a fire. The relay itself might be extremely reliable, but it would not be safe if the fire were on the ground level. A component or components could be safe in one environment while unsafe in another. In addition, accidents usually arise not only because of component failure but also because of interactions between machines, software, humans and the environment. Therefore, system safety should be analyzed in terms of what can go wrong, not just in terms of what can fail. By integrating system safety and reliability analysis methods a launch vehicle developer can better identify the potential component and system failures that could lead to increased risk to the public.

Example

Consider a simplified example using a sample RLV. Assume that this RLV uses a flight profile similar to the X-15 (ref. 10) with the following normal functional operations:

- Drop from carrier vehicle
- Start engines
- Increase thrust to a specified level
- Shut engines down at a specified time

The first step of the system safety process is to define safety-critical systems and events. To define safety-critical systems a developer may decide to use a Preliminary Hazard Analysis (PHA), using the severity (Sev.), likelihood (Like.), and risk criteria provided in MIL-STD-882D. For a generic RLV, the hazard shown in Table 1 might be identified.

In this case countermeasures have been identified to prevent the uncontrolled crash from failure to shut down the rocket engines. Based on this analysis, the launch vehicle developer would identify the rocket engine shut down system, consisting of the automated and manual valves and associated hardware and software, to be considered safety-critical.

In identifying safety-critical events and scenarios, it is important to identify those initiating events that could result in both desirable end states (completion of mission and protection of the public) and undesirable end states (mission failure and increased risk to the public). One approach in developing initiating events is to consider nominal functional operations and the off-nominal states of those same operations. Nominal functional operations of an RLV might include starting and stopping the engines. Off-nominal states for these operations might be failure to start the engines, failure to control thrust, or failure to shut engines down at specified time. The launch vehicle developer can then identify event scenarios based on the nominal and off-nominal initiating events. A common approach is to use an Event Tree Analysis. The event tree for this simplified example is shown in Figure 3.

Table 1 – Example Preliminary Hazard Analysis Worksheet

ID	Hazard Description	Target	Risk before counter-measures			Countermeasures	Risk after counter-measures		
			Sev.	Like.	Risk		Sev.	Like.	Risk
2.0	Component failure, software faults, human error and/or environmental conditions could lead to the inability to shut down the engine with the potential for an uncontrolled crash in populated areas.	Public	II	B	High	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).	II	D	Low

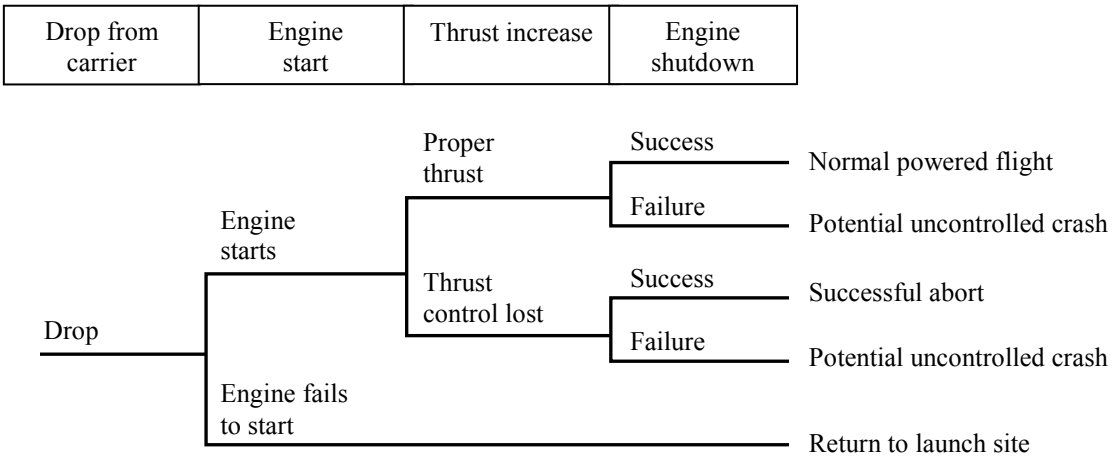

Figure 3 – Example Event Tree Analysis

The next step is to develop system and subsystem hazard analyses and risk assessments. A developer could use a Fault Tree Analysis to formulate the system hazard analyses based on the pivotal events in the Event Tree Analysis. For example, Figure 4 shows a fault tree for the pivotal event "Unable to shut down engine after cutoff," which could potentially lead to an uncontrolled crash as shown in the event tree in Figure 3.

An FMECA can assist in developing failure modes and failure rates for subsystems and components. Table 2 shows one element of an FMECA, for the mechanical failure of a valve, using the severity, likelihood, and risk criteria from MIL-STD-1629A (ref. 4).

Conditional probabilities are then developed using these failure modes. The analyst can obtain component, subsystem, and event failure probabilities from (in order of preference):

- Direct operational experience
- Test data obtained from similar equipment
- Manufacturer data
- Physical models
- Databases and compilations (such as the Non-Electronic and Electronic Parts Reliability Data available from the Reliability Analysis Center)

However, for the following reasons, the developer must exercise care when using failure probabilities:

- Data may have been obtained under environments different from those expected in flight.
- Components used may not be of the same configuration as those used to obtain the data.
- Circumstances of operation, such as operating time, may differ.
- Data may be valid only in special circumstances.
- The failure rate may not be constant with respect to time or cycles, as is assumed in most analyses.
- Data may not take into account manufacturing or operational variability.
- Failure probabilities may have been based on a very small sample size.

Therefore, it is important in any reliability analysis to identify the source of the data and assumptions made.

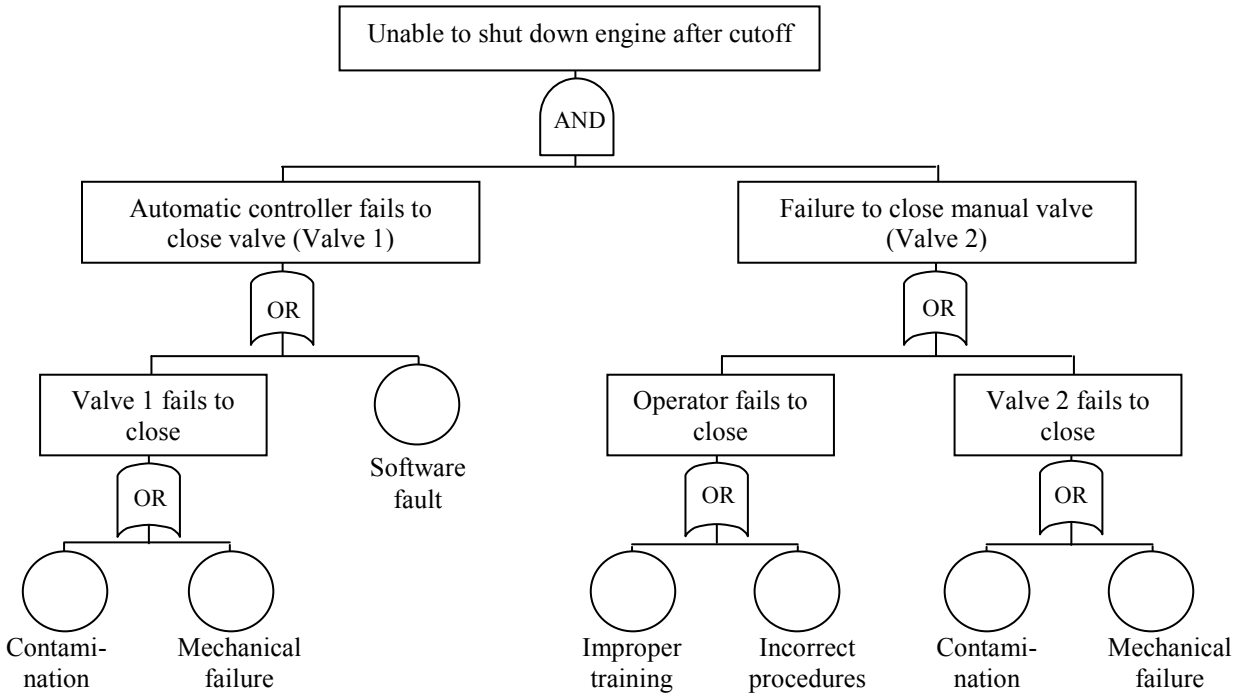

Figure 4 – Example Fault Tree Analysis

Table 2 – Example Failure Modes, Effects, and Criticality Analysis for Mechanical Valve Failure

ID	Item	Failure Mode(s)	Failure Cause(s)	Failure Effect(s)	Risk Assessment			Detection Methods and Controls
					Sev.	Like.	Risk	
2.1	Valve 1 mechanical failure	a. Stuck open b. Stuck partially open c. Stuck closed	a., b., c. Manufact. process problem	a., b. Potential to provide thrust after shutdown c. Failure to provide thrust	a.II b.II c.III	a.C b.C c.C	a.6 High b.6 High c.11 Low	a., b., c. Inspection, manual shutdown valve as backup, cycle valve before launch

In developing reliability estimates with respect to system safety, conditional probabilities are developed. In these cases only those failures that could lead to increased safety risk to the public are considered. MIL-STD-1629A and reference 7 provide a method for calculating conditional probabilities. This method of calculating conditional probabilities takes into account:

- α, the probability that the part or item will fail as a result of the mode identified (the sum of all α for a part equals 1), and,
- β, the conditional probability of the identified severity given that the failure mode has occurred.

The conditional failure probability for each mode is determined by multiplying the α and β for each failure mode by the component failure probability, and the total conditional failure probability for the component is obtained by summing all conditional failure probabilities for each mode. Table 3 provides an example of hypothetical failure rates developed based on the FMECA in Table 2 and the approach described above.

Because of a general lack of data on launch vehicle components and events, a developer may have to derive or estimate reliability data based on engineering judgment, expert opinion, and similarity to historical systems. Factors defining similar systems include vehicle design characteristics, the vehicle's development and integration processes, flight history, and other factors as defined in reference 11. In these cases, placing bounds on the data to explicitly recognize this uncertainty is appropriate. Randomness in the data resulting from natural variability in the physical processes should also be considered. Techniques such as Monte Carlo simulation may be employed to examine the effects of uncertainty and variability on the system reliability estimate. For example, from an FMECA, assuming data was obtained from tests on similar equipment, the hypothetical probability values for the basic events of the fault tree could be developed as shown in Table 3.

Table 3 – Hypothetical Input Failure Probability Values Based on an FMECA

ID	Item	Failure Mode(s)	Component failure probability p	Prob. of failure from mode, α	Conditional probability β	Failure mode probability $p_m = \alpha\beta p$	Conditional failure probability, p_r
2.1	Valve 1 mechanical failure	a. Stuck open b. Stuck partially open c. Stuck closed	0.01 per mission (source: operator experience based on verification testing)	a. 0.25 b. 0.25 c. 0.50 (source: operator exper-ience)	a. 1.0 b. 1.0 c. 0.0 (conservative assumption for a and b; c could not lead to vehicle failure)	a. 0.0025 b. 0.0025 c. 0	0.0050 (only failure modes a and b could cause catastrophic failure)

Using the mathematical relationships for an FTA as provided in references 5 and 7 and the mean failure probability values from Table 4, the probability of the top event, "Unable to shut down engine after cutoff," is then calculated to be 8.4E-05.

A developer can then use Monte Carlo simulation to determine the confidence levels on the top event failure probability. Based on a Monte Carlo simulation (5000 trials), the lower 5% confidence limit on the failure probability would be 2.8E-05 and the upper 95% confidence limit would be 1.4E-04. Figure 5 shows the distribution obtained for the top event failure probability.

Table 4 – Hypothetical Input Failure Probability Values with Uncertainty

Basic Event	Failure Probability	Lower 5%	Upper 95%	Distribution Type
Mechanical Failure	5.0E-03	1.0E-03	9.0E-03	Normal
Contamination	6.0E-04	2.0E-04	1.0E-03	Normal
Improper Training	1.0E-03	5.0E-04	1.5E-03	Normal
Incorrect Procedures	1.0E-03	5.0E-04	1.5E-03	Normal
Software Fault	5.5E-03	2.5E-03	7.5E-03	Normal

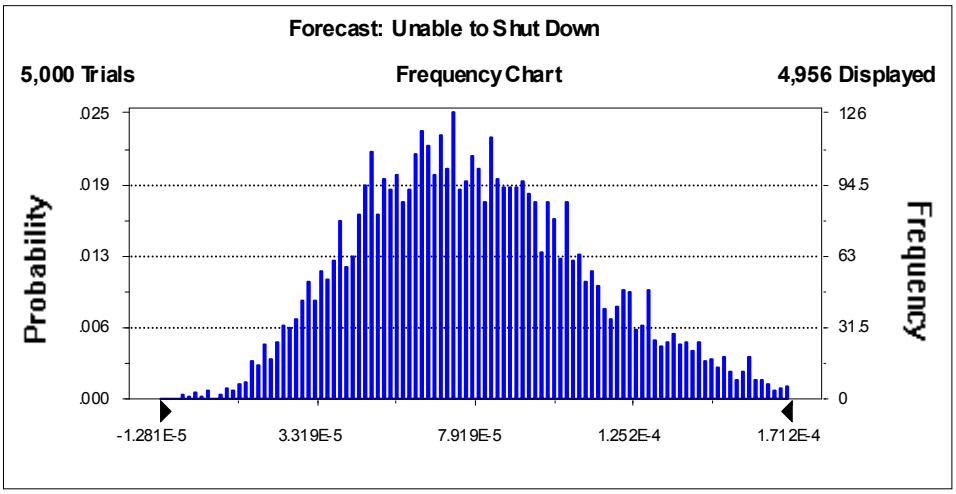

Figure 5 – Monte Carlo Simulation Output Distribution

Using estimates from the fault tree failure models, the event tree shown in Figure 3 can also be quantified to provide an estimate of vehicle failure for all phases of flight, with respect to system safety, as described in reference 7.

The reliability analyses shown in this example have been used to identify potential safety and reliability problems (for example, the failure of the mechanical valve to close when commanded). In addition, by quantifying the fault trees and event trees, alternate designs can be compared for safety and reliability improvements and to see if safety requirements have been met. For example, a safety requirement may be that the vehicle must use a flight safety system to limit or restrict the hazards to public by initiating and accomplishing a controlled ending to vehicle flight. An additional safety requirement might be that each major component of the flight safety system must show by analysis a failure probability of 0.001 or less with 95% confidence. For this vehicle one component of the flight safety system could be the engine shutdown system. Therefore, based on the analysis above including uncertainty, the requirement appears to have been met for this component. If the requirement had not been met, the launch vehicle operator may have decided to make design changes, such as to use a different valve proven by test to be of higher reliability. The operational reliability data for the new valve would be used as input to the fault tree to determine the degree of improvement in the estimated reliability of the engine shutdown system. Alternatively, the operator may choose to conduct operations in a remote location to protect the public until sufficient data demonstrating a level of reliability could be obtained. Additional operational requirements to assure flight safety system reliability may also be imposed based on the integrated safety and reliability analysis. For example, inspections may be required of the valve prior to each flight, as specified in the FMECA in Table 2.

Summary

Analysis techniques such as FMECA, FTA, and ETA have often been used as tools for analyzing both safety and reliability. However, these analyses can be labor-intensive, requiring efforts to define the model as well as to define the input parameter data. Integrating the safety and reliability efforts can help to streamline the analysis process, thereby improving the efficiency of the analyses. In addition, without efforts to integrate the safety and reliability efforts, separate safety and reliability analysis results can be inaccurate or misleading because of differences in assumptions and input data. This paper described an approach to integrating launch vehicle safety and reliability analyses to improve the efficiency and accuracy of both analyses. In addition, this paper provided an example of how the integrated approach might be used for a hypothetical reusable launch vehicle. The FAA Office of Commercial Space Transportation encourages the use of integrated analysis techniques such as those presented here in order to improve launch vehicle safety and reliability.

References

1. AC 431.35-2A, *Reusable Launch and Reentry Vehicle System Safety Process*, Federal Aviation Administration, Office of Commercial Space Transportation, July 2005.
2. Goldberg, et al., *System Engineering "Toolbox" for Design-Oriented Engineers*, National Aeronautics and Space Administration Reference Publication 1358, Dec. 1994.
3. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,* version 1.1, National Aeronautics and Space Administration Office of Safety and Mission Assurance, Aug. 2002.
4. MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, Nov. 1980.
5. Vesely, et al., *Fault Tree Handbook*, NUREG-0492, Nuclear Regulatory Commission, Nov. 1981.
6. *Guide to Reusable Launch Vehicle Safety Validation and Verification Planning,* Version 1.0, Federal Aviation Administration, Office of Commercial Space Transportation, Sept. 2003.
7. *A Guide to Reusable Launch Vehicle and Reentry Vehicle Reliability Analysis,* Federal Aviation Administration, Office of Commercial Space Transportation, April 2005.
8. *Guiding Principles for Monte Carlo Analysis*, EPA/630/R-97/001, U.S. Environmental Protection Agency, March 1997.
9. Leveson, N.G., *Safeware: System Safety and Computers*, Addison-Wesley, 1995.
10. *X-15: The NASA Mission Reports*, Robert Godwin, editor, Apogee Books, 2000.
11. *Draft FAA Guidelines on Probability of Failure Analysis for New Expendable Launch Vehicles*, Federal Aviation Administration, Office of Commercial Space Transportation, Sept. 2004.

Biography

Terry L. Hardy, Aerospace Engineer, Federal Aviation Administration, Office of Commercial Space Transportation, Systems Engineering and Training Division, FAA Headquarters, AST-300, 800 Independence Ave., SW, Room 331, Washington, DC 20591, telephone – (202) 267-8437, facsimile – (202) 267-5463, e-mail – terry.hardy@faa.gov.

Terry Hardy is the Principle Engineer for Reliability in FAA's Office of Commercial Space Transportation, leading efforts to develop safety, reliability, and risk management regulations, guidance documents, and training. Mr. Hardy has over 20 years of experience in the areas of launch vehicles, space propulsion, cryogenics, software, and risk management. Prior to joining FAA he held positions of Director of Desktop Development at Decisioneering, Inc., leading development and testing of statistical software risk management products, and Resident Assurance Manager at NASA Glenn Research Center, overseeing quality, reliability, and safety for launch vehicles integrated and tested at the Lockheed Martin Denver plant. Mr. Hardy holds a BS degree in chemical engineering from Michigan State University, an MS degree in chemical engineering from the University of Toledo, and an MS degree in civil engineering from Cleveland State University. He is also certified as a Reliability Engineer, Quality Engineer, and Software Quality Engineer through the American Society for Quality.