Guide to Reusable Launch and Reentry Vehicle Reliability Analysis

Federal Aviation Administration
Associate Administrator for Commercial Space Transportation
800 Independence Avenue, Room 331
Washington, DC 20591

Version 1.0 **April 2005**

Guide to Reusable Launch and Reentry Vehicle Reliability Analysis

Version 1.0

April 2005

Federal Aviation Administration
Associate Administrator for Commercial Space Transportation
800 Independence Avenue, Room 331
Washington, DC 20591

NOTICE

Use of trade names or names of manufacturers in this document does not constitute an official endorsement of such products or manufacturers, either expressed or implied, by the Federal Aviation Administration.

TABLE OF CONTENTS

FIGURES

TABLES

1.0 INTRODUCTION

1.1 Purpose

This guide is designed to help reusable launch vehicle (RLV) and reentry vehicle (RV) operators conduct reliability analyses. Other approaches that fulfill regulatory objectives may be acceptable to the Federal Aviation Administration (FAA). Such approaches should provide a clear and convincing demonstration of a level of fidelity equivalent to that provided in this document.

The FAA Office of Commercial Space Transportation (AST) is responsible for regulating commercial space transportation only to the extent necessary to ensure public health and safety and the safety of property. In fulfilling its responsibilities, AST issues licenses for expendable launch vehicle (ELV), RLV, and RV launch and reentry activities. Reliability plays an important role in protecting public safety because the risk to the public depends on the likelihood of failure of 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 provide risk assessment data to support launch vehicle system safety analyses.

The licensing process for RLV and RV launch and reentry activities includes a pre-application consultation and an application evaluation. Reliability analyses may be useful during any phase of the licensing process to

- support assessments of risks identified in the system safety process,
- provide vehicle failure probability estimates needed for the expected casualty calculations,
- assist in specifying operating requirements, and
- provide reliability estimates of any flight safety system.

1.2 Scope

This reliability analysis guide provides acceptable methods and approaches for analyses to assist applicants in developing valid reliability estimates that demonstrate compliance with RLV and RV regulatory requirements. Examples of the methods are provided where practicable. The guide is not intended to cover all reliability methods or all aspects of the methods identified here. For example, testing to demonstrate reliability or analysis of historical reliability data is not addressed. To demonstrate compliance with the FAA RLV and RV regulations, an applicant may use either the methods described here or other methods with approval from AST.

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 reliability approaches described here are the same for both types of vehicles. For the purposes of this document, the term “RLV” is assumed to encompass both RLVs and RVs. Many of the methods discussed in this guide could apply to ELVs. However, the intent of this guide is to show the application of reliability analysis approaches for RLVs. For these reasons, probability of failure approaches for ELVs are not explicitly covered in this guide.

1.3 Authority

49 USC Title IX chapter 701, Commercial Space Launch Activities, section 70105

14 CFR part 431, subpart C, Safety Review and Approval for Launch and Reentry of a Reusable Launch Vehicle

14 CFR part 435, Reentry of a Reentry Vehicle Other Than a Reusable Launch Vehicle (RLV)

2.0 DEFINITIONS AND ACRONYMS

2.1 Definitions

Block diagram

Graphical representation of the system or subsystem that illustrates the operation, interrelationships, and interdependencies of functional entities.

Common cause failures

Failure of two or more similar components resulting from a single cause. Common cause failures result from an interdependence between items, systems, or functions.

Confidence interval

Region within the limits of a parameter with an associated confidence level that bounds the true parameter value. Confidence intervals provide an estimate of the amount of uncertainty or error in a parameter.

Critical Items List

List of items that require special attention because of complexity, application of state-of-the-art techniques, consequences of potential failure, or anticipated reliability problems that might increase the risk to the uninvolved public or to property.

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

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

Event Sequence Diagram
Qualitative graphical technique that analyzes the order of events likely to occur given that an initiating event has occurred.

Failure
Any anomalous condition that exhibits the potential for the vehicle, its stages, or its debris to impact the Earth, reenter the atmosphere, or leave a specified operating area during a flight or any future flight**.**

Failure cause
Physical or chemical processes, design deficiencies, quality defects, part misapplication, or other processes that are the reason for a failure.

Failure mode
The way a failure occurs or the category of failure.

Failure Modes and Effects Analysis
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.

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

Fault
Change in state of an item that is considered anomalous and may warrant some type of corrective action to decrease risk.

Fault tolerance
Ability of a system or subsystem to perform a function or maintain control of a hazard in the presence of one or more faults within its hardware, firmware, or software.

Fault Tree Analysis
Deductive system reliability analysis that provides qualitative and quantitative measures of the probability of failure of a system, subsystem, or event. A Fault Tree Analysis estimates the probability that a top-level or

causal event will occur, identifies systematically possible causes leading to that event, and documents the results of the analytic process to provide a baseline for future studies of alternate designs.

Flight Safety System
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.

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

Interface
Boundary (often conceptual) between two or more functions, systems, or items or between a system and a facility.

Model
Representation of a real system. The model includes inputs, outputs, and mathematical relationships.

Monte Carlo simulation
Analytical method where a logical model is repeatedly evaluated, each individual evaluation using different values of the independent parameters that have uncertainty or variability. Selection of parameter values is made randomly but with probabilities of those input values governed by assigned probability distribution functions.

Parts Count analysis
Reliability analysis that determines system reliability by summing part failure rates or probabilities of failure, adjusted for environmental, stress, quality, and other conditions.

Preliminary Hazard Analysis
System analysis conducted to classify each potential hazard in a system according to its severity and likelihood of occurrence and to develop mitigation measures to those hazards.

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

Probability
Mathematical basis for prediction of the ratio of outcomes that would produce a given event

to the total number of outcomes.

Probability distribution
Pattern or function that describes the possible random variable values and the probability associated with each.

Redundancy
Design feature that provides a system with more than one function for accomplishing a given task so that more than one function must fail before the system fails to perform the task.

Reentry vehicle
Vehicle designed to return from Earth orbit or outer space to Earth substantially intact. An RLV that is designed to return from Earth orbit or outer space to Earth substantially intact is a reentry vehicle.

Reliability
Probability that an item will perform its intended function for a specified interval under specified conditions.

Reliability allocation
Assignment of reliability requirements to subsystems and elements within a system that results in meeting the overall reliability requirements for the system. This approach is also known as reliability apportionment.

Reliability block diagram
Reliability analysis that uses logical connections between components and mathematical models based on those relationships to develop system reliability estimates.

Reliability prediction
A forecast of the reliability of a system or system element, postulated on analysis, experience, and tests.

Reusable launch vehicle
Launch vehicle that is designed to return to Earth substantially intact and therefore may be launched more than one time or that contains vehicle stages that may be recovered by a launch operator for future use in the operation of a substantially similar launch vehicle.

Risk
Measure that takes into consideration the probability of occurrence and the consequence of a hazard to a population or installation.

Risk acceptance The act by a decision maker of accepting a risk.

Risk management Organized means of controlling the risk on a program or project.

Risk mitigation Process of reducing either the likelihood or the severity of a risk.

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.

Severity Consequences of a failure mode. Severity accounts for the worst credible potential consequence of a failure, determined by the degree of injury, property damage, or system damage that could occur.

Single-point failure Failure of an item that would result in failure of a system and is not compensated for by redundancy or alternative operational procedures.

Statistics Branch of mathematics dealing with the collection, analysis, interpretation, and presentation of numerical data.

Subsystem Grouping of items satisfying a logical group of functions within a system.

System Integrated composite of people, products, and processes that provide an ability to satisfy a specified need or objective.

Validation Process that determines that the safety requirements are correct and complete.

Verification Evaluation (test, demonstration, analysis, inspection) to determine that applicable safety requirements have been met.

2.2 Acronyms

AC	Advisory Circular
AST	Office of Commercial Space Transportation

CIL	Critical Items List
E_c	Expected Average Number of Casualties
ELV	Expendable Launch Vehicle
ESD	Event Sequence Diagram
ETA	Event Tree Analysis
FAA	Federal Aviation Administration
FDS	Flight Destruct System
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FSS	Flight Safety System
FTA	Fault Tree Analysis
FTS	Flight Termination System
IEEE	Institute of Electrical and Electronics Engineers
NASA	National Aeronautics and Space Administration
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PRA	Probabilistic Risk Assessment
RBD	Reliability Block Diagram
RLV	Reusable Launch Vehicle
RV	Reentry Vehicle
TTS	Thrust Termination System

3.0 RELIABILITY ANALYSES AND SYSTEM SAFETY

The AST requires a launch 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. Figure 3.0-1 shows such a three-pronged approach.

The three safety-related elements reflected in AST's safety strategy for RLV mission and vehicle operations licensing are as follows:

- Using a logical, disciplined system safety process to identify hazards and to mitigate or eliminate risk,
- Establishing limitations of acceptable public risk as determined through a calculation of the individual and collective risk, including the expected number of casualties (E_c), and
- Imposing mandatory and derived operating requirements.

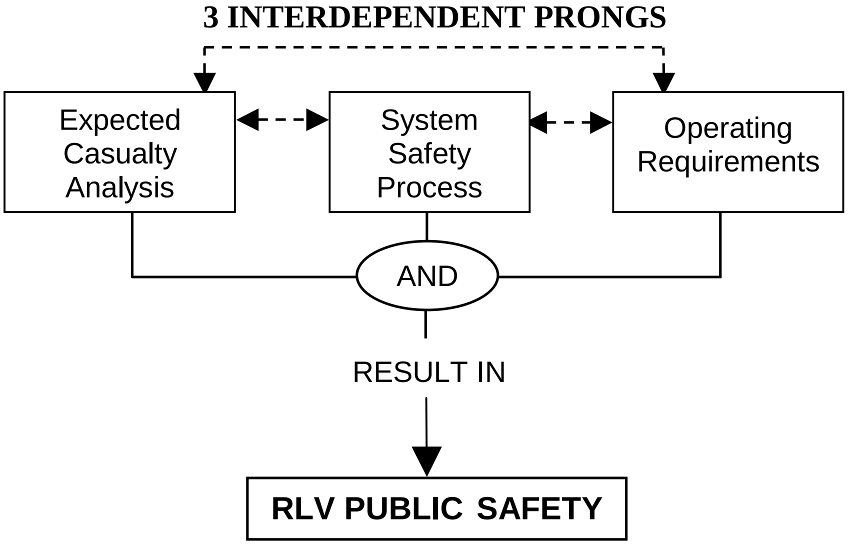


Figure 3.0-1: Three-pronged approach to RLV public safety

The three-pronged approach to RLV public safety is used not only during license evaluation but also after a license has been issued. The FAA intends its safety inspection activities to evaluate whether the operation is performed in a manner consistent with the representations made in the launch operator's application and with terms and conditions set forth in the permit or license.

Reliability analyses are part of each element of the three-pronged approach to public safety. In addition, reliability analyses are often conducted on flight safety systems. Paragraphs 3.1 through 3.5 describe these applications of reliability analyses. Appendix A provides detailed discussions of these methods.

Appendix B provides examples of approaches used to support an expected casualty analysis. This appendix also shows how different analyses can work together to produce a valid assessment of system reliability.

3.1 System Safety Process

Reliability analyses are part of the RLV system safety process addressed in §431.35 (c) and (d). As described in Advisory Circular (AC) 431.35-2, 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, time, and cost 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, a system safety process includes the following items:

- Identification of safety-critical systems, operations, and events.
- Subsystem and system hazard analyses and risk assessments to identify safety-critical failure modes, define resulting hazards and risks to the public, and determine means of eliminating or controlling those risks.
- Validation and verification, using analysis, inspection, test, and demonstration, to determine the effectiveness of mitigation measures and confirm that safety requirements have been met.

Reliability analyses provide input to the system safety 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 identify mitigation measures or evaluate 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, as part of the validation and verification effort to determine whether an item will perform its intended function under specified conditions).

Figure 3.1-1 shows how the reliability and system safety analyses are integrated. Integration of reliability and system safety is based on the system safety process described in AC 431.35-2. The process shown in the diagram does not indicate iterations that naturally occur as part of the process. For example, in the process of obtaining verification data, new failure modes may be identified which then must be analyzed for risk.

In this process, after identifying safety-critical systems and events, the analyst 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. On the other hand, 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 identifies combinations of hazards and includes such factors as the environment, software, and human error. 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.

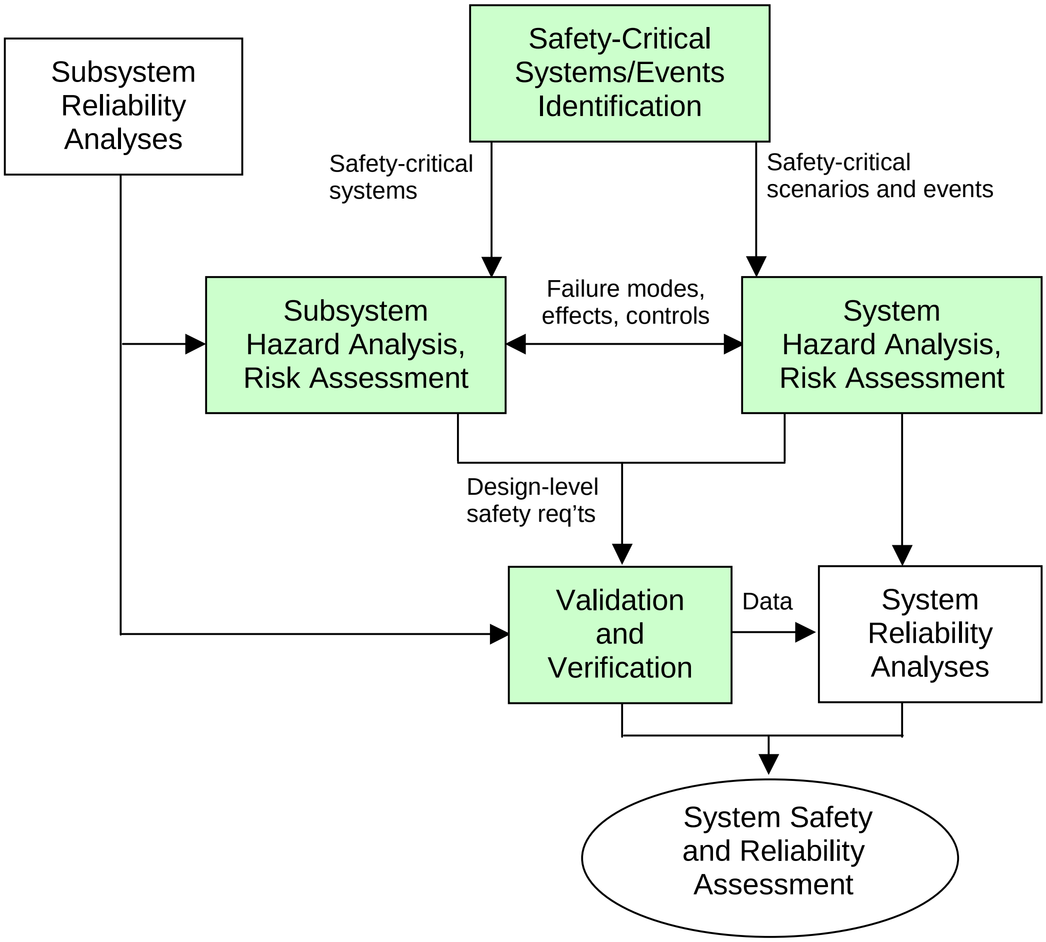

Subsystem Reliability Analyses
Safety-Critical Systems/Events Identification
Safety-critical systems
Safety-critical scenarios and events
Subsystem Hazard Analysis, Risk Assessment
Failure modes, effects, controls
System Hazard Analysis, Risk Assessment
Design-level safety req'ts
Validation and Verification
Data
System Reliability Analyses
System Safety and Reliability Assessment

Figure 3.1-1: Integrated reliability and system safety assessment (system safety process indicated by shaded boxes)

Acceptable subsystem reliability analyses to assist in identifying failure modes and consequences include, but are not limited to, Failure Modes, Effects and Criticality Analysis (FMECA) and Fault Tree Analysis (FTA) (see appendix A). These analyses identify potential subsystem reliability issues that could ultimately result in safety issues, leading to specific design requirements. For example, an RLV operator may use an FMECA to identify a failure mode in the cockpit instrumentation panel that leads to loss of the display. This display supplies the pilot with vehicle attitude and guidance information necessary to prevent the overflight of populated areas. Based on a quantitative analysis of the reliability of that panel using that FMECA, an RLV operator may determine that the cockpit instrumentation display has an unacceptably high probability of failure in the anticipated flight environments. Therefore, the operator may require an independent means to measure attitude and other flight parameters.

Some techniques used for subsystem reliability analyses also prove effective for analyzing hazards and risks; therefore, combining subsystem reliability and safety analyses is acceptable in some cases. For example, a license applicant may use an FMECA to determine the failure modes and consequences and to provide a preliminary estimate of subsystem reliability. The results of the integrated subsystem reliability, risk, and hazard analyses normally include failure modes, consequences, risk mitigation measures, and preliminary component failure probabilities.

Mishaps are rarely caused by a single component failure. The majority of mishaps result from a confluence of factors (Leveson 1995). Such factors include the environment, mechanical failure, software, human error, procedures, and system design. Therefore, system hazard analyses and risk assessments are used to develop possible system mishap scenarios. The system analyses are usually based on critical scenarios and events, combined with the outputs from the subsystem analyses, to determine the risk to public health and safety. Acceptable methods for performing these system hazard analyses, risk assessments, or both, include Event Tree Analysis (ETA) and FTA. Often, these methods are used qualitatively to analyze system risk during development. However, these methods can also be used to produce quantitative system reliability estimates. These system reliability analyses may use preliminary component failure probabilities identified in a preliminary subsystem reliability analyses. As information becomes available through validation and verification and as development progresses, the fidelity of the reliability inputs should be improved. Increasingly detailed quantitative system reliability estimates can then be developed which include not only component failure but also system factors, such as software and human factors.

Use of both subsystem and system reliability analyses can assist in identifying design trade-offs to improve reliability and reduce the risk to public safety, especially in determining the reliability of safety-critical systems and the overall effects on system safety. For example, a redundant valve may be a potential mitigation measure for failure of a safety-critical valve. By using both qualitative and quantitative reliability analyses, a vehicle designer can determine whether implementing the mitigation measure has detrimental effects on system reliability, such as introducing new failure modes (for example, the failure to switch to a redundant valve when the first valve fails), or whether the improvement in subsystem reliability is enough to compensate for the complexity added by redundancy.

Validation and verification of the safety-critical systems, requirements, and mitigation measures can be performed in part through subsystem and component reliability analyses. Acceptable reliability analysis approaches for design verification include reliability block diagrams, parts count analysis, FMECA, FTA, and ETA supplemented by reliability test data, performance data, performance analysis, and subsystem and system inspection.

A reliability analysis is iterative in nature and is a continuing activity throughout a project. Reliability estimates should be updated to account for increases in design, test, and evaluation data as it becomes available during development.

3.2 Expected Casualty (E_c) Analysis

Existing FAA RLV and ELV regulations require a launch operator to perform collective and individual risk analyses to quantify public risk. Expected number of casualties (E_c) is a statistical calculation used to quantify and access the risk to the public from exposure to inert and explosive debris, toxic substances, and blast hazards from a proposed launch. Vehicle failure probability is one input in the calculation of E_c; therefore, determination of launch vehicle failure probability is essential to public safety risk determination.

Vehicle failure probability estimates should use accurate data, scientific principles, and statistically or probabilistically valid methods. In this context, accurate data means completeness, exactness, and fidelity to the maximum extent possible. Scientific principles refer to knowledge, based on the scientific method, such as that established in the fields of physics, chemistry, and engineering. A probability of failure estimate that is statistically and probabilistically valid should at least be the result of a sound application of mathematics. A sound application of mathematics uses correct premises and makes only conclusions that are properly derived from the premises. A valid statistical analysis should account for the uncertainty in a statistical inference caused by sample size limits, degree of applicability of data to a particular system, and degree of homogeneity of the data.

Approaches to analyzing the probability of failure are generally classified as deductive or inductive. Deductive analyses are top-down, postulating system failure and analyzing behaviors contributing to the failure. Inductive analyses are bottom-up, analyzing the failure of individual components to determine the likelihood of system failure. However, each analytic approach contains inherent limitations, and the results of any analytical construct are by their very nature uncertain. The National Aeronautics and Space Administration (NASA), U.S. military, nuclear industry, and commercial airline industry have recognized that a single analytical approach is usually insufficient for estimating system reliability and risks to the public. Therefore, the FAA recommends the use of both top-down and bottom-up analysis approaches, including measures of uncertainty, to estimate the probability of vehicle failure. In addition, reliability assessments should be integrated with system safety analyses to assure that the focus of the effort is on risk reduction by elimination or mitigation and public health and safety.

Two acceptable approaches that combine top-down and bottom-up reliability analyses to estimate vehicle failure probability are reliability allocation and probabilistic risk assessment (see figures 3.2-1 and 3.2-2). Both use elements of the system safety process to inform the reliability estimate. The level of detail required for each depends on the complexity of the vehicle and the scope of the operations. Other approaches that fulfill regulatory objectives and meet the performance criteria may be acceptable.

3.2.1 Reliability Allocation

NASA and the military use reliability allocation as a tool in determining whether reliability requirements can be met (Larson and Wertz, 1995). This approach can also be applied to RLV programs to estimate system reliability. Reliability allocation employs reliability data from launches of vehicles developed and launched under similar circumstances, apportions that figure among different mission phases and systems, and verifies those apportioned reliability values.

The steps in the reliability allocation approach are as follows (see figure 3.2-1):

1. Set a vehicle reliability estimate based on a comparison to historical data from previous launches of vehicles developed and launched in similar circumstances.
2. Account for the differences in the mission and system parameters used for this vehicle compared to the previous launches, where possible. (For example, comparing the aerodynamic stresses on the vehicle or whether components with little test experience are being used.)
3. Allocate the vehicle reliability estimate among mission phases based on allocation models using historical data from launches of similar vehicles.
4. Allocate the vehicle reliability estimate among subsystems for each mission phase based on allocation models and historical data.
5. Employ bottom-up subsystem assessments to assess individual contributors to failure, to calculate probabilities when allocations are no longer reasonable (because the subsystems become interdependent or data are simply not available) or when it becomes impossible to propagate failures to a lower level, or to verify that the allocated reliability requirement has been met. FMECA, RBD, and Parts Count analyses are often used. Verification data can also be used to provide additional data support or to disprove the analysis or the allocation.
6. Use system reliability analyses, such as ETA and FTA, to assist in verifying overall reliability estimates. The system reliability analyses are important. Reliability allocation approaches and bottom-up reliability analysis methods typically assume no interaction between components. In addition, they tend to ignore other systems factors, such as the environment, human interactions, and software, resulting in optimistic estimates of reliability. Therefore, system reliability analyses help ensure that the system safety goals have been achieved. Verification data can also be used to provide additional data supporting or disproving the analysis.

The FAA recommends that system and subsystem reliability analyses account for uncertainty through the use of Monte Carlo simulation and sensitivity analyses.

Appendix A describes reliability analysis methods used in reliability allocation. Appendix B provides a simplified example of reliability allocation for system reliability analysis.

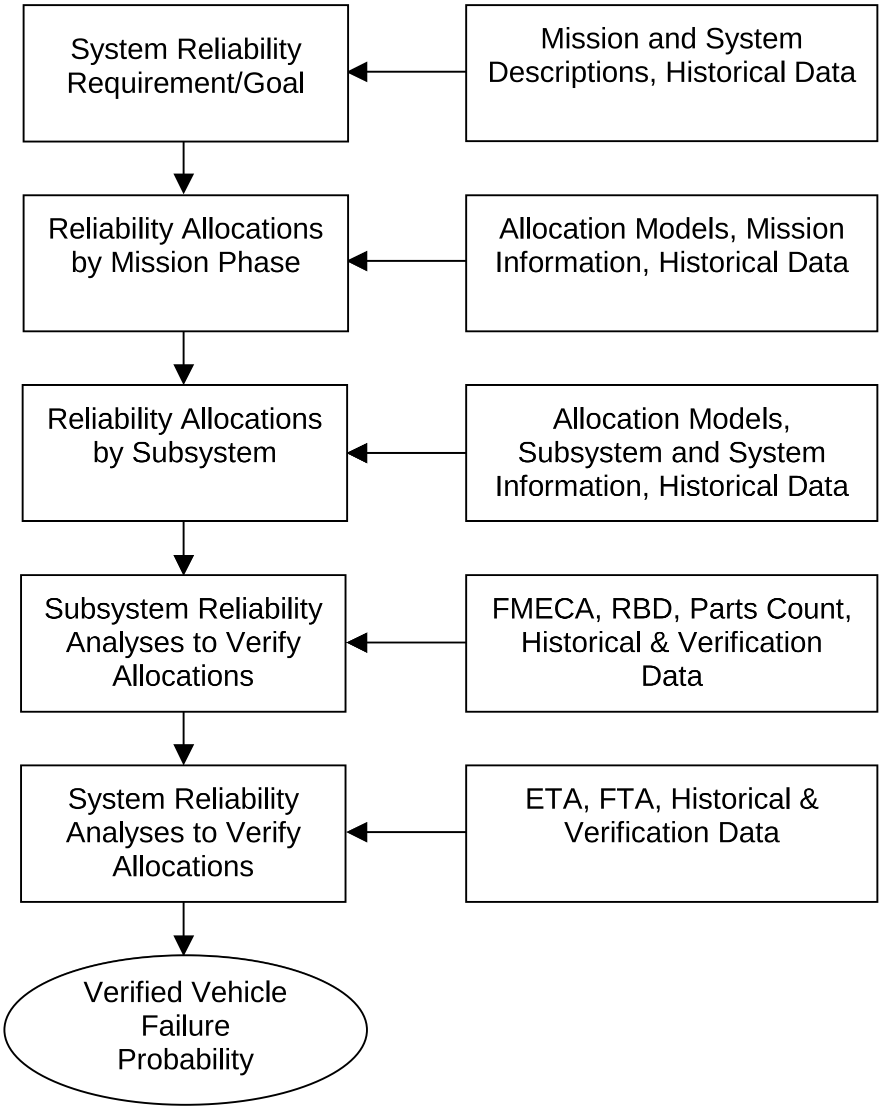

System Reliability Requirement/Goal
Mission and System Descriptions, Historical Data
Reliability Allocations by Mission Phase
Allocation Models, Mission Information, Historical Data
Reliability Allocations by Subsystem
Allocation Models, Subsystem and System Information, Historical Data
Subsystem Reliability Analyses to Verify Allocations
FMECA, RBD, Parts Count, Historical & Verification Data
System Reliability Analyses to Verify Allocations
ETA, FTA, Historical & Verification Data
Verified Vehicle Failure Probability

Figure 3.2-1. Reliability allocation

3.2.2 Probabilistic Risk Assessment

Probabilistic risk assessment (PRA) contains key elements from NASA, the nuclear industry, commercial aircraft, and military aerospace approaches to analyzing risk and reliability for complex systems. In a PRA, an analyst determines the sequence of events (scenarios) that can lead to failure, develops failure models to analyze those scenarios, and then analyzes the effects of uncertainty of the models and input parameters on the failure probability estimates.

Figure 3.2-2 shows the steps in the PRA approach as defined in the *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners* (NASA 2002).

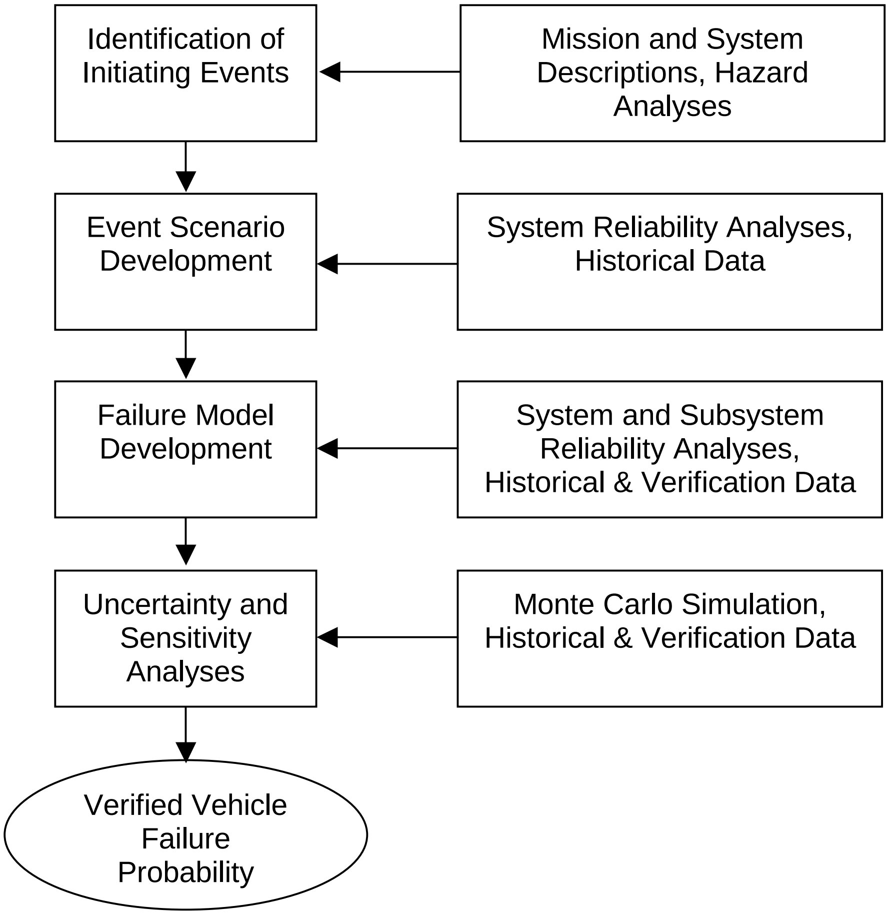

Identification of Initiating Events
Mission and System Descriptions, Hazard Analyses
Event Scenario Development
System Reliability Analyses, Historical Data
Failure Model Development
System and Subsystem Reliability Analyses, Historical & Verification Data
Uncertainty and Sensitivity Analyses
Monte Carlo Simulation, Historical & Verification Data
Verified Vehicle Failure Probability

Figure 3.2-2. Probabilistic risk assessment

1. Identify specific system and mission parameters, such as vehicle configuration, phases of flight, and methods of operation.
2. Identify initiating events. Initiating events are the triggering events in sequences of events (scenarios) that ultimately lead to either successful or unsuccessful states, such as “mission success with no impact on public safety” or “abort to landing site.” An initiating event can be normal operation, such as “launch,” or an anomalous event, such as “valve sticks.” Preliminary Hazard

Analyses, Preliminary Hazard Lists, and FMECA can be used in identifying the initiating events. Initiating events can also arise from nominal and non-nominal system functions, such as "engine shutdown" or "failure of software to close valve when commanded."

3. Develop scenarios that can lead to the defined end states once the initiating events have been identified. Acceptable methods for developing event scenarios include ETA and Event Sequence Diagrams (ESD). The event scenarios start with the initiating event and progress through what are known as pivotal events until an end state is reached. Pivotal events are those successes and failures that can ultimately lead to the success of a mission or a mishap. In other words, a pivotal event is the first in a sequence of events that lead to the mishap or success scenario. An example of a pivotal event might be "failure of thrust termination system."
4. Develop failure models for pivotal events from these event scenarios. A failure model describes how a pivotal event occurs. The FTA is the top-down system reliability analysis normally used to develop system failure models of pivotal events in the ETA or ESD. Bottom-up techniques, such as FMECA and RBD, are often used as well to assist in the development of the failure models. Data is collected and analyzed for use in quantifying the failure models. This data includes probabilities for component failures, structural failures, human errors, process failures, and common causes.
5. Apply uncertainty bounds to input data to account for the uncertainty in the input parameter data. Quantify this uncertainty for the entire system. Uncertainty analyses, such as Monte Carlo simulation, are used for analyzing this input parameter uncertainty. Model uncertainty can also be analyzed using sensitivity analyses.

Appendix A describes reliability analysis methods used in the PRA approach. Appendix B provides a simplified example of this system reliability analysis approach. Refer to Bedford and Cook (2001) and Henley and Kumamoto (1992) for additional information on PRA approaches.

3.3 Operating Requirements

In combination with the expected casualty analysis, the system safety process yields methods of operation that demonstrate the applicant's ability to operate without excessive risk to public safety. Note, however, that even under the best of circumstances, these analytical processes may not reflect real-world performance. Because of the uncertainty in operational performance, especially in new launch vehicles, the launch operator and the FAA specify operating requirements. Regulatory operational restrictions and requirements are specified for RLVs (for example, in 14 CFR 431.43), but the launch operator and the FAA may specify additional operating requirements based on the reliability analyses conducted as part of the system safety process or the expected casualty analysis. For example, an FMECA may show that the loss of a carbon dioxide scrubbing system in an RLV crew cabin would lead to pilot incapacitation, resulting in a mishap. Based on the FMECA, the risk may not be acceptable without mitigation measures, such as a robust design approach that includes an analysis showing that the scrubbing system could handle the carbon dioxide output generated by a given number of crewmembers during flight. Verification measures to assure proper operation of the carbon dioxide scrubbing system could include load testing, preflight inspection of the system, and preflight component integrity testing. Based on the design and verified carbon dioxide scrubbing capacity, operating requirements limiting the number of crew for each RLV flight might then be imposed.

3.4 Flight Safety Systems

A flight safety system (FSS) serves to protect the public and property from harm in the event of non-nominal vehicle flight. The ELVs launching from the United States typically use a Flight Termination System (FTS) as the FSS to end the flight whenever the vehicle strays outside a predefined performance envelope. This FTS normally includes either a Flight Destruct System (FDS) or a Thrust Termination System (TTS). Depending on the design and application, RLVs may also use a conventional FTS or an alternative FSS that does not destroy the vehicle. Such systems require high reliability. The U.S. Air Force has identified reliability goals for the FTS used in ELVs. For example, the reliability goal for the airborne portion of flight is 0.999 with 95-percent confidence. Testing is an acceptable method for demonstrating reliability. However, testing FTS components several thousand times to prove the reliability at the specified confidence level is impractical because of the costs and difficulties involved in testing the complete system. Therefore, a launch vehicle operator would normally prepare system reliability analyses using multiple methods in addition to implementing procedures and approaches that lead to high reliability, such as robust design, to meet the reliability goals.

Acceptable reliability analyses for meeting the reliability goals for an FTS include FMECA and FTA, combining bottom-up and top-down reliability analyses. The operator would normally first do an FTA to identify FTS paths and command control system paths that could cause the FSS to fail to function. This FTA would include the probability of occurrence of any undesired event as part of each system's reliability design determination. An FMECA would then be performed based on failures identified by an FTA to determine and document all possible failure modes and their effects on FTS and command control system performance. The output from the FMECA would include failure modes and their probability of occurrence, single-point failures, areas requiring redundancy, functions that can and cannot be tested, and input to reliability predictions. As part of this analysis, a launch operator should perform a single failure point analysis to verify that no single failure can cause inadvertent FTS activation or disable the FTS or command control system.

Note that this FTS reliability estimate is obtained in the context of implementing procedures that improve reliability, such as single fault tolerance, system independence to reduce the risk of common cause failure, use of highly reliability parts, use of flight-proven components, system testability, configuration control, and specified component lifetimes. In addition to the quantitative reliability analyses, FTS evaluation normally includes sneak circuit, bent pin, fratricide, software, and radio frequency link analyses.

Flight safety systems other than a conventional FTS may be appropriate for an RLV. For example, an RLV may use a thrust termination system in combination with other measures, such as propellant dumping or parachutes, to reduce potential consequences to the public. In these cases, the reliability should be analyzed using a similar methodology to that described in paragraph 3.1, System Safety Process, to assure that reliability is analyzed in the context of system and subsystem interactions and system safety.

3.5 Reliability Data Usage

Fidelity of a reliability analysis in support of system safety will usually be limited by the lack of appropriate data and a lack of understanding of the interactions of the environment, humans, software, and components in complex systems. Therefore, it is expected that engineering judgment and expert opinion be used on the final system reliability estimate. For example, a reliability goal for an RLV might be based on experimental supersonic vehicle (X-Plane) experience. However, it is known that the failure probabilities for new ELV launch vehicles are higher for the first few flights. In addition, the failure probability can depend on the experience of the launch vehicle operator. Therefore, in this example an initial reliability goal for use in reliability allocations might be based on X-Plane experience with appropriate adjustments made for the launch vehicle operator experience and flight test history based on engineering judgment. Expert opinion, including opinions from a peer review process, may also assist in quantifying reliability models when data is unavailable, refining data, and estimating model and parameter uncertainty. Methods for obtaining and using expert opinion are provided in Bedford and Cooke (2001). The U.S. Office of Management and Budget has created guidelines for peer review (OMB 2004). The rationale, methods, and assumptions behind any engineering judgments and expert opinions should be explicitly stated.

Component, subsystem, and event failure probabilities can be obtained from the following sources (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 and MIL-STD-217)

However, for the following reasons, care must be exercised 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.
- 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.

Because of a general lack of data on launch vehicle components and events, reliability data may have to be derived or estimated based on engineering judgment, expert opinion, and similarity to historical systems. Factors defining similar systems include vehicle design characteristics, development and integration processes, and other factors as defined in the Draft FAA Guidelines on Probability of Failure Analysis for New Expendable Launch Vehicles (2004). 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, should be employed to examine the effects of uncertainty and variability on the system reliability estimate.

The FAA may instruct the operator to adjust failure probability estimates to account for the level of experience demonstrated by the launch operator, evidence from previous flights, or both. Other factors that affect the likelihood of failure may contribute such adjustments.

Qualitative reliability products (failure modes, effects, etc.) and quantitative reliability estimates should be updated as new information is obtained. New failure modes will be identified as ground and flight testing proceed. In addition, residual risk (the combination of acceptable risk and unidentified risk) can be “retired” in some cases as more is known about the vehicle operation. Application of Bayesian statistics (Guikema and Pate'-Cornell, 2004) is one approach that may be appropriate for updating quantitative reliability estimates. Other approaches may be considered.

4.0 ELEMENTS OF RELIABILITY ANALYSIS DOCUMENTATION

The validity and usefulness of a reliability analysis rest on how well that analysis was prepared, interpreted, and applied. Users of the reliability analysis results will only be able to trust those results if they understand the basis for the analysis, including inputs, assumptions, and uncertainties. The AST has selected the following elements from standards used by the NASA, U.S. military, and Institute of Electrical and Electronics Engineers (IEEE) for documenting reliability analyses. These elements should be included in documentation of launch vehicle reliability analysis.

4.1 Item Identification and Description

When a reliability analysis is performed on an item, that item should be identified and described. Such descriptions could include the following information:

- Product, system, subsystem, component, assembly, or part
- Product function, architecture, and materials
- Performance requirements
- Redundancy, if applicable
- Hardware and software relationships
- Human factors
- Interfaces
- Operating conditions and constraints

Documents that apply to this description should be identified in the item description, including system schematics, drawings, and specifications.

4.2 Intended Use of the Reliability Analysis Results

The reliability analysis should include a statement of the intended use of the analysis results. For example, the reliability analysis could be used to assist in the management or mitigation of launch vehicle risks, to assist in identification of vehicle failure modes and effects, to provide input to the expected casualty analysis, or to predict the reliability of an FSS. The statement of intended use should include the following information:

- Why the reliability analyses were performed.
- Specific uses of the results.
- How the results should not be used, with specific precautions for using the results.

4.3 Analysis Methods

The reliability analysis should include a description of the methods used and the rationale for using the method. The analysis should include a general description of the approach along with a reference to documentation for the analysis technique. The description should include the following information:

- Assumptions
- Limitations

- Methods
- Models
- Software used to perform the analysis
- Sources of data

4.4 Analysis Inputs

The analysis should describe inputs used, along with the limitations and assumptions for those inputs. Where fault or failure probability data are used, the sources of the data should be provided with known limitations on the use of the data. Differences between the vehicle operating conditions and the conditions used to obtain the data, such as differences in number of cycles or operating time should also be provided.

4.5 Analysis Results

Results of a reliability analysis should include outputs, conclusions, and recommendations, usually in the form of a report. Quantitative prediction outputs should be in the form of figures of merit, such as reliability and mean time between failures. Figures of merit should be defined, and confidence intervals should be provided where applicable. Qualitative results include failure modes and effects, criticality of failure modes, single-point failure modes, areas requiring redundancy, functions that cannot be tested, mitigations to minimize or eliminate risk, and combinations of events that could lead to system failure. The outputs should also include all assumptions. If prior analyses of similar systems are available, those analyses should be documented. Differences between the new analysis and the prior analysis must be stated. Recommendations should be stated in terms of specific actions. Note that in some cases a separate report documenting the findings is not required. Depending on the complexity of the analysis, the documentation elements may be included within the analysis. For example, assumptions and data sources are typically documented within an FMECA.

4.6 Confidence in Analysis

Numerous factors can affect the level of confidence that can be placed in the results of any analysis methodology. Three of the most common factors are discussed next. Note, however, the factors described here are intended to be illustrative rather than an exhaustive list.

4.6.1 Uncertainty

Sources of uncertainty should be explicitly stated in the reliability analysis. Numerous factors can affect the accuracy of the reliability analysis, including, but not limited to, operating environment, manufacturing operations, assembly operations, support operations, software and human interactions. In many cases, a lack of information or knowledge about these factors exists; therefore, the inputs to the reliability analysis or the model contain uncertainty. In addition, inputs could be described by a natural variability, or the models may not accurately represent the system.

4.6.2 Assumptions

Assumptions made for the model inputs should be accounted for and included in the documentation of the analysis. If probability distributions are used to describe the uncertainty, then assumptions used to develop those distributions should be stated, if known.

4.6.3 Limitations

The documentation should state the known limitations of the modeling method and the data inputs.

5.0 SOFTWARE TOOLS

Software tools are available which can assist in conducting reliability analyses. Descriptions and manufacturer information for such tools can be found through organizations, such as IEEE Reliability Society, Reliability Analysis Center, American Society for Quality Reliability Division, and the Society of Automotive Engineers Reliability, Maintainability, Supportability, and Logistics Division. The following links provide access to some of this information:

http://www.asq-rd.org/links.htm

http://www.ieee.org/portal/site/relsoc/

http://www.sae.org/standardsdev/

http://rac.alionscience.com/

http://www.enre.umd.edu/tool.htm

http://www.foodriskclearinghouse.umd.edu/modeling_simulation_tool.cfm

6.0 ADDITIONAL CONSIDERATIONS

Reliability analyses are intended to support decisions related to public safety. Through analyses, launch vehicle developers can select courses of action that may improve the reliability and safety of the vehicle. Reliability estimates may allow a launch vehicle developer to compare design solutions that improve safety and reliability, eliminate potential safety problems, or identify whether a reliability goal will be met. However, reliability analysis itself does not ensure safety or reliability. 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. Components could be safe in one environment while unsafe in another. For example, a relay contact could be used to signal elevator doors 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. In addition, accidents usually arise not only because of component failure but also because of interactions between the environment, machines, software, and humans. Therefore, system safety should be analyzed in terms of what can go wrong, not just in terms of what can fail.

Many control and mitigation measures are used to reduce risk, improve reliability, and increase safety. These methods and others should be considered when designing highly reliable systems. Typical methods include the following measures:

- Design integrity and quality to ensure intended function and prevent failures.
- Use of proven components of known reliability.
- Ability to check the condition of a component.
- Warning or indication to provide failure detection.
- Isolation of systems, components, and elements so that the failure of one does not cause failure of another.
- Redundant or backup systems to enable continued function after any failure.
- Design failure effect limits, including the ability to sustain damage and to limit the safety impact or effects of failure.
- Design failure paths to control and direct the effects of failure in a way that limits its safety impact.
- Margins or factors of safety to allow for any undefined or unforeseeable adverse conditions.
- Error tolerance that accounts for adverse effects of foreseeable errors during design, test, manufacture, operation, and maintenance of the vehicle.
- Computer software verification, validation, documentation, configuration management, and quality assurance.
- Personnel qualification and training.
- Contingency planning, including operator procedures after failure detection to enable continued safe flight, evacuating personnel from high-risk areas, and modifying vehicle trajectory to avoid high-risk areas.
- Established processes, including:
    - Risk management approaches
    - Anomaly reporting, analysis, and corrective action systems
    - Parts, materials, and process programs
    - Configuration management
    - Maintainability
    - Quality assurance and compliance monitoring
    - Validation and verification

The validity of the results of a reliability analyses depend on the validity of the model and the input parameters used. Care must be taken in understanding whether the reliability model and data are appropriate for the launch vehicle being analyzed. The analyst should understand the underlying assumptions of the models, identify the uncertainty in inputs, and anchor the models to real-world data in any engineering analysis, whether it is an analysis of thermal loads, a determination of a stress-strain relationship, or an FTA identifying potential failure modes in a vehicle design. As in any engineering analysis, reliability analyses should be used to support, not replace, good engineering practice and judgment.

APPENDIX A: RELIABILITY ANALYSIS METHODS

This appendix describes selected methods for the analysis of system reliability. Acceptable methods for prediction and modeling are discussed. Examples of the use of each method are provided. Additionally, the advantages and disadvantages of each method are presented. The following nomenclature is used in the equations contained in this appendix:

α Probability that the part or item will fail due to the mode identified (sum of all α for a part = 1).

β Conditional probability of mission loss (or of the identified severity) given that the failure mode has occurred.

λ Failure rate

λ_{Gi} Average failure rate for i^{th} generic part

λ_i Failure rate for component or subsystem i or for event i (λ_1 = failure rate for component 1, etc.)

λ_p Failure rate for a part

λ_s System failure rate

λ_{sg} System failure rate determined from reliability goal

π_{Qi} Quality adjustment factor for the i^{th} generic part

π_{Si} Stress adjustment factor for the i^{th} generic part for Telcordia/Bellcore approach

π_{Ti} Temperature adjustment factor for the i^{th} generic part for Telcordia/Bellcore approach

π_{Ei} Environmental adjustment factor for the i^{th} generic part for MIL-STD-217 approach

π_{Li} Learning adjustment factor for the i^{th} generic part based on years in production for MIL-STD-217 approach

ω_i Weighting factor for component or subsystem i

C_1,C_2 Complexity factors for MIL-STD-217 approach

C_m Criticality number for a failure mode

C_r Criticality number for an item

C_s Criticality number for a system

j Number of failure modes for a part

k Number of parts

n	Number of system elements, subsystems, or components
N_i	Quantity of i^{th} generic part
p	Failure probability
p_i	Failure probability of component or subsystem i or event i (p_1 = failure probability for component 1, etc.)
p_m	Failure probability for a failure mode
p_p	Failure probability for a part
p_r	Failure probability for an item
p_s	System failure probability
p_t	Total failure probability
r	Minimum number of components which must survive
R	Reliability, $R = \exp(-\lambda t) = 1 - p$
R_c	Component reliability
R_i	Reliability for component or subsystem i (R_1 = reliability of component 1, etc.)
R_s	System reliability
R_{sg}	Reliability goal for the system
R_{switch}	Switching reliability
t	Operating time
z	Number of different generic part categories

A.1 Reliability Block Diagrams

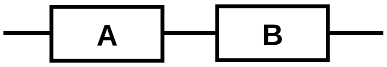
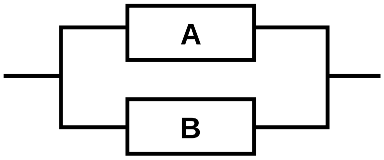
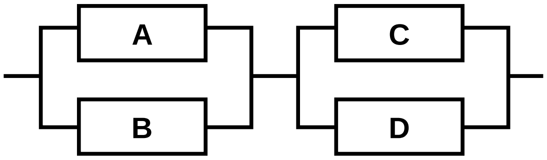
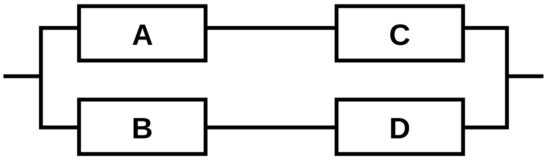
The reliability block diagram (RBD) technique shows the logical connections between components of the system. Using this logic, a mathematical model can be developed to determine the subsystem or system failure probability. The RBD is useful for evaluating the reliability of various potential configurations, thereby allowing for trade-offs related to system safety. In addition, the technique is useful in the subsystem verification process as part of the system safety process and can assist in verifying reliability allocations.

The generalized approach for developing reliability block diagrams is as follows:

1. Divide the system into its elements using schematics, functional diagrams, etc.
2. Construct the block diagram using the RBD conventions described.
3. Assign reliabilities to each component.
4. Calculate a system reliability value using the appropriate equations provided.

Simple RBDs are constructed of series, parallel, or combinations of series and parallel elements. Table A.1-1 shows an example of RDB construction adapted from Goldberg (1994) and assumes all components function independently of each other. Each block represents a system element or event. Series blocks are used when all components are required to operate for successful system operation. Parallel blocks are used when only one element needs to operate successfully for successful system operation. The entire system will operate successfully if an uninterrupted path exists between the input and the output.

Table A.1-1: Simple reliability block diagram construction

Type	**Block Diagram Representation**	**System Reliability (R_S)**
Series		$R_S = R_A R_B$ R_A = reliability, component A R_B = reliability, component B
Parallel		$R_S = 1-(1-R_A)(1-R_B)$
Series-Parallel		$R_S = [1-(1-R_A)(1-R_B)]*$ $[1-(1-R_C)(1-R_D)]$ R_C = reliability, component C R_D = reliability, component D
Parallel-Series		$R_S = 1-(1-R_A R_C)*$ $(1-R_B R_D)$

More generally, the following describe the calculations of reliability for series and parallel systems.

Series Systems:

$$R_s = \prod_{i}^{n} R_i$$

$$R_s = R_1 R_2 R_3 ... R_n$$

$$p_s = 1 - R_s$$

Active Parallel Systems:

$$R_s = 1 - \prod_{i}^{n} (1 - R_i)$$

$$R_s = 1 - (1 - R_1)(1 - R_2)(1 - R_3)...(1 - R_n)$$

where

R = Reliability, $R = \exp(-\lambda t) = 1 - p$
R_s = System reliability
R_i = Reliability for component or subsystem i (R_1 = reliability of component 1, etc.)
λ_i = Failure rate for component or subsystem i (λ_1 = failure rate for component 1, etc.)
t = Operating time
n = Number of system elements or subsystems (which function independently)
p_s = System failure probability
p_i = Failure probability of component or subsystem i (p_1 = failure probability for component 1, etc.)

In an active parallel system, primary and redundant subsystems normally operate at all times. This calculation for active parallel systems assumes that all subsystems are activated when the system is activated. In addition, failures do not influence the reliability of the surviving subsystems. However, many systems use standby redundancy instead of active redundancy. In such cases, the standby component is not activated unless the online component fails. An example of such a standby redundant system is a spare tire on a car. In this configuration, there must be some method of detecting the failure and switching to the standby elements. Because the “switch” can fail, this configuration introduces additional reliability considerations. Table A.1-2 lists mathematical equations for standby redundant systems for two parallel components.

Another type of parallel system is the shared load parallel system. In the shared load parallel system, the components are active. However, if one component fails the failure rate for the surviving component increases upon the failure of the first component. This case makes intuitive sense in some real world applications. For example, if one lug nut comes loose on an automobile wheel assembly, the remaining lug nuts must support the increased load.

Table A.1-2: Standby redundancy, two components in parallel (Dovich, 1990)

Standby Parallel Model	**System Reliability**
Equal failure rates, perfect switching	$R_s = e^{-\lambda t}(1+\lambda \mathrm{t})$
Unequal failure rates, perfect switching	$R_s = e^{-\lambda_1 t} + \lambda_1 (e^{-\lambda_1 t} - e^{-\lambda_2 t}) / (\lambda_2 - \lambda_1)$
Equal failure rates, imperfect switching	$R_s = e^{-\lambda t}(1+ \mathrm{R}_{\mathrm{switch}} \lambda \mathrm{t})$
Unequal failure rates, imperfect switching	$R_s = e^{-\lambda_1 t} + \mathrm{R}_{\mathrm{switch}} \lambda_1 (e^{-\lambda_1 t} - e^{-\lambda_2 t}) / (\lambda_2 - \lambda_1)$
where R_s = System reliability λ = Failure rate t = Operating time R_{switch} = Switching reliability	

For a two-component shared load parallel system, the reliability is described as follows (Dovich, 1990):

$$R_s = e^{-2\lambda_1 t} + 2\lambda_1 (e^{-\lambda_2 t} - e^{-2\lambda_1 t}) / (2\lambda_1 - \lambda_2)$$

where

R_s = System reliability
λ_1 = Failure rate for component 1
λ_2 = Failure rate for component 2
t = Operating time

Another type of parallel system is the "r out of n system." This system has n parallel components, but r components must survive for the system to continue operating. Unlike the shared load parallel system, the failure rate of the surviving component does not increase upon failure of the first component. An example of this form of redundancy is a suspension bridge where a certain number of cables are required to support the structure. The reliability of an r out of n system is given as follows, assuming the component reliability is the same for each component (Kapur and Lamberson, 1977; Dhillon, 1999):

$$R_s = \sum_{x=r}^{n} R_c^{\;x}(1-R_c)^{n-x}\, n!/[x!(n-x)!]$$

where

R_s	= System reliability
R_c	= Component reliability
n	= Number of components
r	= Minimum number of components which must survive

Some systems cannot be modeled with simple series or parallel RBDs. In these cases, more complex diagrams are required. Figure A.1-1 shows an example of a complex RBD.

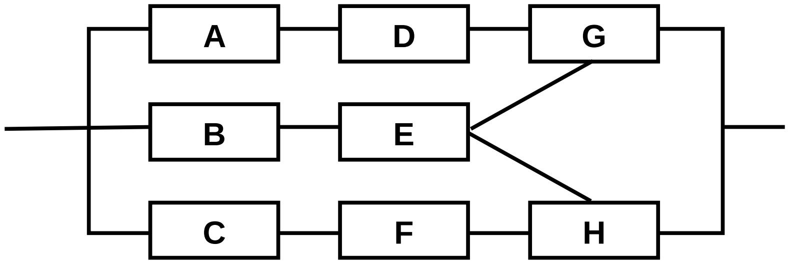


Figure A.1-1: Complex reliability block diagram

In this system, if part E fails, then paths BEG and BEH are unsuccessful. Kapur and Lamberson (1977), Dhillon (1999), and MIL-STD-756B provide approaches to calculating these complex RBDs. In such cases, the approach and assumptions behind that approach must be clearly stated.

Consider the example, illustrated in figure A.1-2, which could represent several components in an engine propellant feed system. Two valves in series (parts A and B) are followed by two sets of active redundant valves. The first set of active redundant valves is represented by parts C and D. Parts E and F represent the second set.

Assume the following component reliabilities:

$R_A = 0.95$
$R_B = 0.97$
$R_C = 0.99$
$R_D = 0.99$
$R_E = 0.92$
$R_F = 0.92$

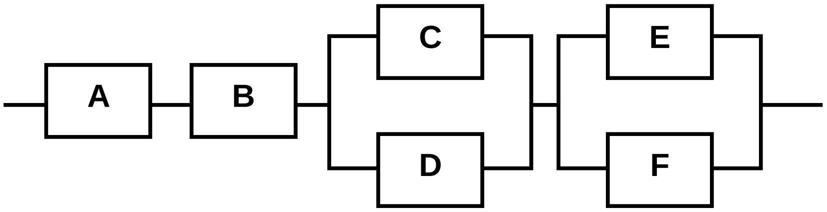


Figure A.1-2: Example reliability block diagram

Using the equations provided in table A.1-1, the following expression for total reliability R_T could be developed.

$R_T = R_A\ R_B\ [1-(1-R_C)(1-R_D)]\ [1-(1-R_E)(1-R_F)]$

$R_T = (0.95)(0.97)[1-(1-0.99)(1-0.99)]\ [1-(1-0.92)(1-0.92)]$

$R_T = 0.916$

The data used to quantify RBD can be uncertain, in part, because the estimates may have been obtained from limited sampling. Also, data may have been obtained under different conditions than those assumed for the RBD.

Uncertainties are usually evaluated using either sensitivity or formal uncertainty analyses. In sensitivity analysis, an input parameter, such as a component failure probability, is changed while holding all other parameters constant. Then the affect on the total system reliability is determined. In uncertainty analysis, a probability distribution is used to represent the range of values possible because of uncertainty or variability for each failure probability in the RBD. The range is usually determined from statistical data obtained on a particular subcomponent. Monte Carlo simulation is then used to obtain the range of possible values for the system reliability (see paragraph A.7).

Advantages

- A reliability block diagram allows early assessment of design concepts and allows an analyst to easily visualize the system logic.

Disadvantages

- Obtaining reliability elements requires breaking down the systems to identify multiple levels of components.
- Breaking down large systems can require considerable effort.
- Analyzing complex reliability diagrams can be difficult. Not all systems can be easily modeled using series or parallel configurations.

- Modeling non-hardware failure mitigation measures, such as training and procedures, is difficult using this technique. Complementary techniques, such as ETA or FTA, can be used to identify and model non-hardware failures.

Dhillon (1999), Kapur and Lamberson (1977), MIL-STD-756B, Goldberg (1994), and O'Connor (1991) provide additional information on reliability block diagrams.

A.2 Parts Count Analysis

Parts Count analysis models predict reliability of a system by summing the part failure rates or probabilities, while accounting for conditions, such as the environment, stress, and quality of workmanship. This analysis is used to evaluate configurations in the preliminary design phase when the number of parts is reasonably fixed. In addition, the overall complexity is not expected to change appreciably during later development and production. This analysis can also be used to provide verification data. Parts Count analyses have generally been used to predict the reliability of electronic components. However, the models can be extended to mechanical subsystems when appropriate data is available. A Parts Count analysis assumes the time to failure of the parts is exponentially distributed (that is, a constant failure rate). This analysis also assumes that all elements of the item reliability model are in series or can assumed to be in series for purposes of approximation. The failure rates used in the analysis are based on historical data. Adjustment factors are usually applied to the failure rates to account for items, such as differences in application, temperature, and stress.

Multiple Parts Count analysis models exist. Telcordia/Bellcore and MIL-STD-217 are the most commonly used models. Regardless of the model selected, a Parts Count analysis is conducted in the following steps:

1. List the parts types and quantities.
2. Identify non-series elements in the system and document assumptions related to these elements. For such non-series elements as redundancies and alternate modes of operation, system reliability can be determined either by considering only the series elements of the model as an approximation or by summing part failure rates for the individual elements and calculating an equivalent series failure rate for non-series elements of the model. Refer to paragraph A.1 for the reliability block diagram methods.
3. Assign part failure rates for each part type, using failure rates derived from service experience on identical or similar items or acceptable industry standards. Identify the source of the data.
4. Identify adjustment factors, such as quality, stress, environment as defined in MIL-HDBK-217, Telcordia/Bellcore SR-322, or other acceptable industry sources. Multiple adjustment factors may exist, and sources for the methods and adjustment factors must be clearly stated.

5. Multiply the failure rates, quantity of parts, and adjustment factors for a given part type.
6. Sum the resulting part type failure probabilities for each part type.

Generally, Parts Count analysis methods take the following form:

$$\lambda_s = \sum_{i=1}^{z} N_i (\lambda_G \pi_Q)_i$$

where

λ_s = System failure rate
λ_{Gi} = Average failure rate for ith generic part
π_{Qi} = Quality adjustment factor for the ith generic part
N_i = Quantity of ith generic part
z = Number of different generic part categories

Because part failure rates vary significantly with applied stresses, system failure probability models that include stress factors have been developed. The Telcordia/Bellcore model uses the following approach:

$$\lambda_s = \sum_{i=1}^{n} N_i (\lambda_G \pi_Q \pi_S \pi_T)_i$$

where

π_{Si} = Stress adjustment factor for the ith generic part
π_{Ti} = Temperature adjustment factor for the ith generic part

MIL-STD-217F also provides a model that includes stress factors, given as follows:

$$\lambda_s = \sum_{i=1}^{n} N_i ([C_1 \pi_T + C_2 \pi_E] \pi_Q \pi_L)_i$$

where

C_1, C_2 = Complexity factors
π_{Ei} = Environmental adjustment factor for the ith generic part
π_{Li} = Learning adjustment factor for the ith generic part based on years in production

Detailed examples are provided in MIL-HDBK-338B and MIL-HDBK-217F.

Advantages

- Parts Count analyses are straightforward methods of calculating reliability.
- These methods assist in identifying areas where special attention is required, especially when considering safety critical systems.

Disadvantages

- Adjustment factors may not be readily available for all components.
- The technique can provide a pessimistic estimate of reliability because not all part failures lead to system failure. Complementary techniques, such as FTA or FMECA, can be used to balance the reliability predictions.

Additional information on Parts Count analysis methods can be found in MIL-HDBK-217, MIL-HDBK-338B, MIL-STD-756B, and O’Connor (1991).

A.3 Failure Modes, Effects, and Criticality Analysis

A Failure Modes, Effects, and Criticality Analysis (FMECA) is a bottom-up, inductive, reliability analysis. Here potential failure modes are analyzed to determine results or effects on the system. Then, each potential failure mode is classified according to its severity, probability of occurrence, or both. An FMECA can be useful for qualitatively identifying areas of the system vulnerable to system failure. In addition, the tool helps identify single-point failures, which are failures and faults that result in failure of the system. An FMECA can also provide quantitative data used to help verify safety requirements or reliability allocations. For either the quantitative or qualitative approach, the procedure for performing an FMECA is as follows:

1. Define the system to be analyzed. The system definition includes identification of components and interfaces and uses system schematics, specifications, drawings, component lists, and so forth. Mission phases are established in this step.
2. Categorize the system into elements to be analyzed. These elements include subsystems, assemblies, drawings, components, and piece parts. Usually block diagrams or a system breakdown diagram is used. A system breakdown diagram is a graphical description of the logical connections between systems, subsystems, assemblies, subassemblies, and components. Figure A.3-1 shows the format of a system breakdown diagram.
3. Define a coding system for each of the elements, using a block diagram or system breakdown diagram.
4. Describe the qualitative severity and likelihood classifications to be used. Tables A.3-1 and A.3-2 show typical definitions. These categories should be for consequences to the uninvolved public and property, not mission assurance.

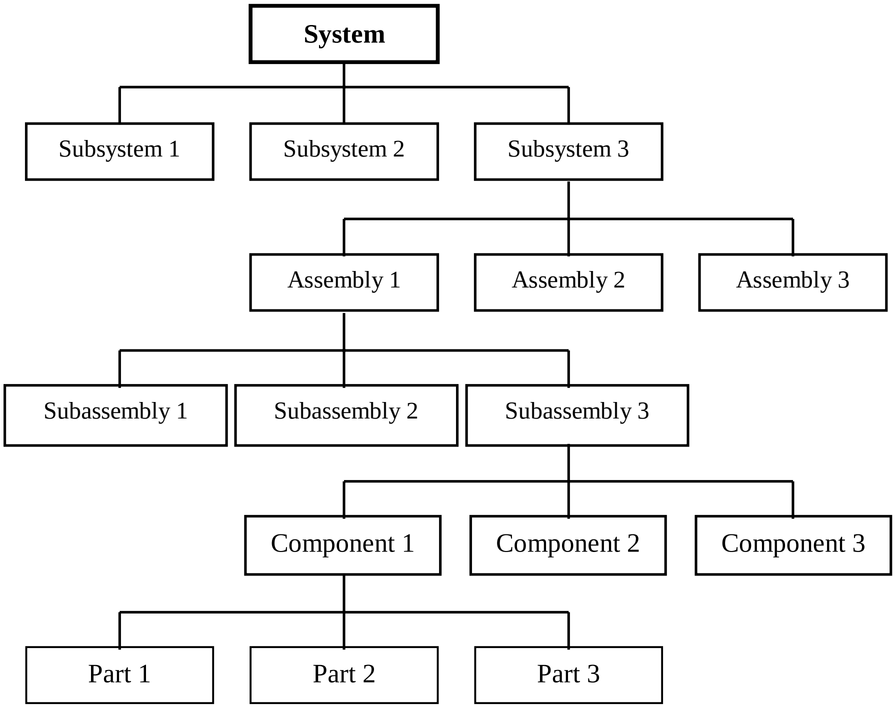


Figure A.3-1. System breakdown chart (adapted from Goldberg, 1994)

Table A.3-1: Qualitative severity classification (AC 431.35-2)

Description	**Category**	**Environmental, Safety, and Health Result Criteria**
Catastrophic	I	Failure that may cause death to the uninvolved public or safety-critical system loss.
Critical	II	Failure that may cause severe injury to the uninvolved public, major property damage, or major safety-critical system damage.
Marginal	III	Failure that may cause minor injury to the uninvolved public or minor safety-critical damage.
Negligible	IV	Failure not serious enough to cause injury to the uninvolved public or safety-critical system damage.

Table A.3-2: Qualitative likelihood classification (AC 431.35-2)

Description	Level	Likelihood Criteria
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} per mission.
Probable	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} per mission.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} per mission.
Remote	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} per mission.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} per mission.

5. Document levels of acceptable risk. Table A.3-3 shows a typical risk acceptability matrix. Again, this risk acceptability matrix must be documented in terms of risk to the uninvolved public.
6. For each element to be analyzed:

   a. Identify the ways to fail, which are referred to as failure modes. Identifying causes of failure is useful because each cause may have its own mitigation approach. For example, if a fuel valve assembly has a failure mode of leakage, the leakage could be caused by contamination. Therefore, contamination control procedures may be required. If the leakage were caused by fatigue, operation limits might be used.

   b. Identify all the effects or consequences of each failure mode. Multiple areas of concern, such as personnel, equipment, or product, may exist. Identify all the effects for each area of concern. Note that the effects should be explicitly stated in terms of risk to the public. For example, "loss of oxygen generation system" could lead to pilot unconsciousness, resulting in vehicle impact in populated areas.

   c. Identify the worst credible severity and probability for each failure mode as designated in the severity and likelihood definitions from step 4.

   d. Assess the risk, using the risk acceptability matrix defined in step 5. If the risk is category 3 as shown in table A.3-3, then continue to the next step. If the risk is category 1, then identify measures (controls) to mitigate risk. Measures to mitigate risk should be defined for category 2 risks, or FAA can choose to accept category 2 risks. Failure detection mechanisms can also be specified.

e. Reevaluate the risk with the new countermeasures.

7. Document the analysis using an FMECA worksheet. In addition, a Critical Items List (CIL) is often developed as part of the documentation. The CIL is a list of those items that require mitigation or control measures because of complexity, application of state-of-the-art techniques, impact of potential failure, or anticipated reliability problems. For the purposes of this guide, the CIL should include those items that result in substantial increase to the risk to the public. For example, the CIL may include those items that are identified as having a severity of catastrophic or critical as defined in AC 431.35-2.

Table A.3-3: Risk acceptance matrix (AC 431.35-2)

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

Category 1 (1-6). Controlling, mitigating , or both, actions must be taken to reduce the risk.
Category 2 (7-10). If no mitigating actions taken, FAA can accept risk.
Category 3 (11-20). Project management decides on action, if any.

Figure A.3-2 shows a worksheet for one component of a hypothetical upper stage propulsion system. The risk was evaluated and documented using the criteria from AC 431.35-2.

FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS WORKSHEET

System: Upper Stage Propulsion System

Mission: Satellite Delivery to GEO

Phase: Orbital Insertion

Ref. Drawing: GTYD-1002B008

Sheet 1 of 20

Prepared by: John Smith

Reviewed by: Janet Jones

Approved by: Sharon Jackson

Date: January 2, 2004

ID	Item	Failure Modes	Failure Causes	Failure Effects	Risk Assessment			Detection Methods and Controls
					Sev.	Prob.	Risk	
2.0	Combustion Chamber	a. Coolant loss b. Seal failure	a. Manufact. process problem b. Cyclic fatigue	a. Reduced performance, burn-through, possible crash and injury to involved public b. Reduced performance	a.II b.III	a.C b.D	a.6 b.14	a. Inspect welds b. Seal redundancy

Figure A.3-2: Failure modes, effects, and criticality analysis worksheet

Military Standard 1629A provides a method of performing a quantitative FMECA. This method combines the failure rate or probability with assessments of criticality to obtain a failure mode criticality number. The resulting number provides a quantitative measure of system reliability, as follows:

$$C_m = \alpha \beta \lambda_p t$$

$$C_r = \sum_{n=1}^{j} (C_m)_n$$

$$C_s = \sum_{i=1}^{k} (C_r)_i$$

where

C_m = Criticality number for a failure mode

C_r = Criticality number for an item
C_s = Criticality number for a system
α = Probability that the part or item will fail because of the mode identified (sum of all α for a part = 1)
β = Conditional probability of mission loss (or of the identified severity) given that the failure mode has occurred
λ = Part failure rate
t = Operating time
j = Number of failure modes for a part
k = Number of parts

The resulting system criticality number applies to the entire system. This system criticality number is the number of failures of a specific severity classification expected due to the item's failure modes.

This approach can be generalized using the following part failure probabilities:

$$p_m = \alpha \beta \mathrm{p}_\mathrm{p}$$

$$p_r = \sum_{n=1}^{j} (p_m)_n$$

$$p_s = \sum_{i=1}^{k} (p_r)_i$$

where

p_p = Failure probability for a part
p_m = Failure probability for a failure mode
p_r = Failure probability for an item (component or subsystem)
p_s = Failure probability for a system

The factor α is used because usually when a part fails, different failure modes contribute to different degrees to the historical failure rate data. For example, a valve may have two failure modes, failed open and failed closed. The historical data may show that 60 percent of the time it failed open, and 40 percent of the time it failed closed. Therefore, α_1 for the first mode would be 0.60, and α_2 for the second mode would be 0.40. Note that all α must sum to 1.

The factor β is used because not all part failures lead to mission failures. Therefore, historical data or judgments are required to determine the level to which any failure mode in question could lead to mission failure. The β values are classified as follows:

Actual loss: $\beta = 1$
Probable loss: $0.10 < \beta < 1.0$
Possible loss: $0.00 < \beta < 0.1$
No effect: $\beta = 0$

If the valve failing to open leads to mission failure 50 percent of the time, then $\beta_1 = 0.5$. If the valve failing to close has no effect, then $\beta_2 = 0$. For this example, if the failure probability for the valve is 0.10, then $p_r = \alpha_1 \beta_1 p + \alpha_2 \beta_2 p = (0.60)(0.50)(0.10) + (0.40)(0.00)(0.10) = 0.003$.

Advantages

- An FMECA allows for systematic evaluation of item failures and helps identify single-point failures.
- An FMECA may identify hazards overlooked in other system analysis techniques.

Disadvantages

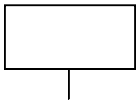
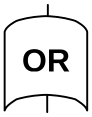
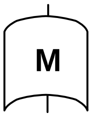
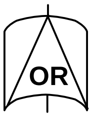
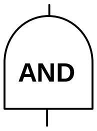
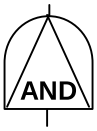
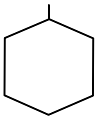
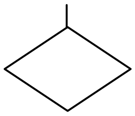
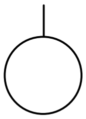
- An FMECA does not account for the consequences of coexisting, multi-element faults and failures. Complementary techniques, such as FTA or ETA, can be used to identify multiple faults and failures.
- The majority of FMECA do not account for human error or hostile environments.
- An FMECA can give an optimistic estimate of system reliability if a quantitative approach is used. Therefore, this analysis should be used with other analyses, such as FTA, in developing reliability estimates.

Additional information on Failure Modes, Effects, and Criticality Analysis can be found in ARP 4761, Dhillon (1999), MIL-STD-1629A, NASA RP 1358 (Goldberg, 1994), and O'Connor (1991).

A.4 Fault Tree Analysis

Fault Tree Analysis is a top-down, deductive reliability analysis that graphically depicts the sequence of events that can lead to an undesirable event and provides a quantitative estimate of system reliability. An FTA generates a fault tree, which is a symbolic logic model of the failures and faults. Failure probabilities can be applied to each fault or failure, and the failure probabilities can be combined to determine the failure probability of a top-level event. An FTA is often used to model failures in complex processes and can be used as an aid for system safety improvement. An FTA also assists in verifying the allocation of reliability values. Standard symbols are used in constructing an FTA to describe events and logical connections. Table A.4-1 shows the most common logic symbols.

Table A.4-1: Common fault tree logic and event symbols

Symbol	**Description**
	Top Event – Foreseeable, undesirable event (also intermediate event)
	"OR" Gate – Any of the events below gate will lead to an event above the gate
	Mutually Exclusive "OR" Gate - "OR" Gate – Any of the events below the gate will lead to an event above gate. However, all other inputs are precluded.
	Exclusive "OR" Gate – An event above gate occurs if one, but only one, event occurs.
	"AND" Gate – All events below gate must occur for event above gate to occur.
	Priority "AND" Gate – An event occurs if all inputs exist and occur in a predetermined order.
	"INHIBIT" Gate – An event occurs if a single input event occurs in the presence of enabling conditions.
	Undeveloped Event – An event not further developed because of a lack of need, resources, or information.
	Initiator (Basic Event) – Initiating fault or failure, not developed further (marks limit of analysis).

Usually an FTA can be conducted with just a few logic symbols. The most commonly used logic symbols are the “AND” gate and the “OR” gate. Logic symbols should not be directly connected together in the fault tree. Inputs and outputs to logic symbols should be events.

The process for performing an FTA is as follows:

1. Identify the undesirable events that require analysis. Usually these are called pivotal events – events that could ultimately lead to failure of the vehicle or system. Each pivotal event is a top event for the fault tree, and a new tree is required for each top event. The top event is often determined from other analyses, such as a hazard analysis or FMECA, or from a known undesirable event, such as a mishap.
2. Define the scope of the analysis to determine whether the analysis will be quantitative and to determine the level of depth of the analysis for each undesirable event. The level of depth may be determined based on the application of the analysis. Examples include design improvement, mishap analysis, safety verification, and reliability allocation. Often in quantitative analyses, the analysis is done to a level where failure probability data are available.
3. Identify causes leading to the undesirable event, known as first-level contributors to the top event. Contributors must be independent of each other. For example, for a top event of “car broken down on highway,” the events “unable to start car” and “broken timing belt” are not independent events. The timing belt could cause the car not to start. Data gathering may be required to determine events and contributors. Sources of this information include specifications, drawings, block diagrams, and so forth.
4. Link the first-level contributors to the top event by a logic gate.
5. Identify the second-level contributors to the first-level events.
6. Link the second-level contributors to the first-level contributors.
7. Repeat until the analysis reaches a desired level. The bottom-most contributors are known as initiators or basic events.
8. Evaluate the tree to determine the validity of the input and failure paths.
9. Document the results.

The evaluation step usually includes determination of the cut sets and calculation of the failure probability. A cut set is any group of initiators that will, if all occur, cause the top event to occur. A minimal cut set is a minimal number of initiators that will, if they all occur, cause the top event to occur. These cut sets are the combinations of events that can lead to the undesirable event. In addition, importance ranking is often used to assess the impact of various cut sets on the undesired top event. Vesely (1981), ARP 4761, Dhillon (1999), and Goldberg (1994) describe methods for determining the cut sets and importance of the contributors.

If a fault tree is evaluated quantitatively, then the probability of failure for each initiator must be determined. Sources of data usually include manufacturer data, industry-consensus data, military standards, historical evidence, testing or simulation. Often, confidence bands, ranges or distributions are used for the probability data to explicitly identify the uncertainty in the data.

Once probabilities are estimated for all basic events or initiators, they are propagated through logic gates to the intermediate events and finally to the top event. The probability of failure for "AND" and "OR" gates is calculated as shown in table A.4-2.

Table A.4-2. Failure probability expressions for selected fault tree gates

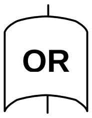
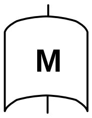
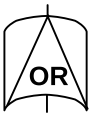
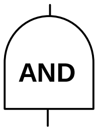
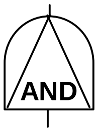
Symbol	**Gate Name**	**Failure Probability, Two Inputs**
	Inclusive "OR"	$p_t = p_1 + p_2 – (p_1p_2)$ p_t = Total failure probability p_1 = Failure probability, event 1 p_2 = Failure probability, event 2
	Mutually Exclusive "OR"	$p_t = p_1 + p_2$
	Exclusive "OR"	$p_t = p_1 + p_2 – 2(p_1p_2)$
	"AND"	$p_t = p_1p_2$
	Priority "AND"	$p_t = p_1p_2$

Figure A.4-1 shows a fault tree developed for the failure event, "thruster supplied with propellant after cutoff."

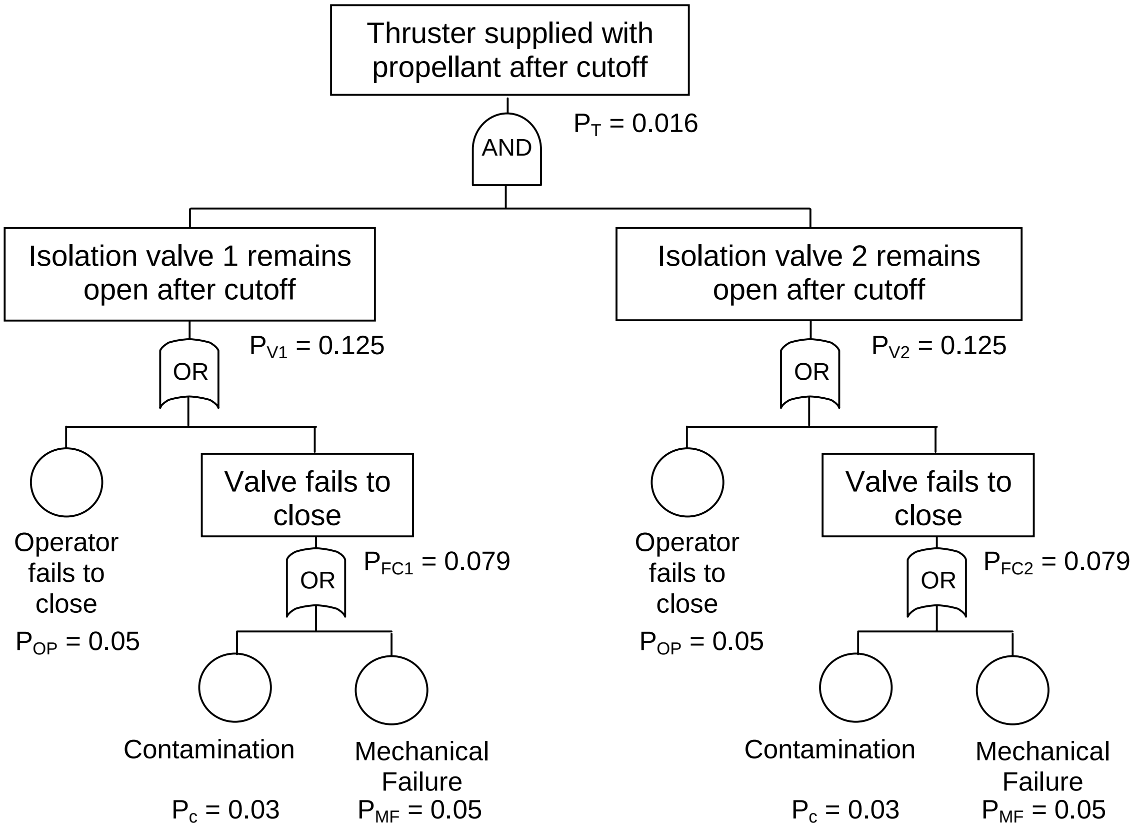


Figure A.4-1: Fault tree analysis example

Because data used to quantify fault trees can be uncertain or variable, uncertainties are usually evaluated using formal uncertainty analysis techniques, such as Monte Carlo simulation. In addition, sensitivity analyses are often performed to identify the effect of individual events on the top event. More details about uncertainty analyses are provided in Vesely (1981) and Philipson and Wilde (2000).

Advantages

- An FTA enables risk assessment of complex systems.
- An FTA allows calculation of probabilities of combined faults and failures in the system.
- An FTA aids in identifying and assessing common cause failures and single-point failures.

Disadvantages

- Fault trees account for only one undesirable condition or event, and the analyst must foresee that event.
- Fault trees can be flawed if all significant contributors have not been identified or if common causes have not been identified. Complementary analyses, including ETA and FMECA, can assist in identifying contributors and common causes.
- Failure rates or probabilities must be available for each basic event, and obtaining those failure rates may prove difficult.

Additional information on FTA can be found in ARP 4761, Dhillon (1999), NASA's *Fault Tree Handbook with Aerospace Applications* (2002), and Vesely (1981).

A.5 Event Tree Analysis

An ETA is a bottom-up, inductive reliability analysis that graphically explores system responses to an initiating event and enables the assessment of the probability of an unfavorable or favorable outcome. The initiating event in an ETA may be a failure or fault, an undesirable event, or a normal system operating command. An event tree portrays all plausible operating paths from the initiating event and incorporates binary branching to illustrate that the system either succeeds or fails at each branching node.

An ETA is often used to model operating procedures, management decision options, and other non-hardware causes. An event tree can be used to analyze the reliability of systems in which all the components are continuously operating or for systems in which some of the components are in standby mode. The analysis is also used to model accidents and to analyze the effectiveness of engineered safety features and emergency response systems. The analysis is especially useful in operations of vehicles, such as RLVs, where failure of one system does not necessarily lead to public safety impacts because of contingency operations, such as an abort. An ETA is often used with deductive analyses, such as FTA.

Figure A.5-1 shows an example generic event tree. The process for performing an ETA is as follows:

1. Identify the initiating event for the system being examined. Initiating events are the triggering events in sequences of events (scenarios) that ultimately lead to either successful or unsuccessful states. Often in performing risk assessments, this initiating event has been determined from a hazard analysis, FMECA, or knowledge of system functions. Initiating events range from failures, such as a burst pipe, to normal operating events, such as lift off.
2. Determine the paths (alternate logic sequences). Start by determining what happens after the initiating event occurs, especially in regard to engineered

safety systems, such as alarms, interlocks, or valves, and processes, such as abort procedures, emergency response, human detection, and instrument detection. If, for example, the initiating event is a car accident, then the engineered safety systems may include air bags and seat belts.

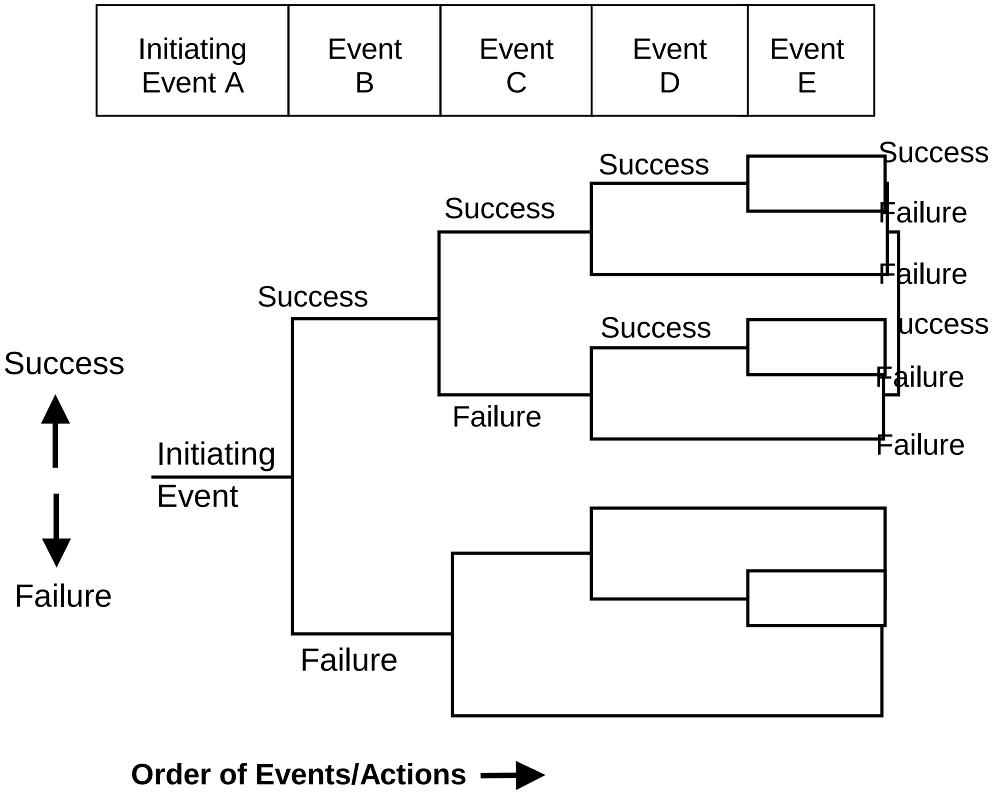
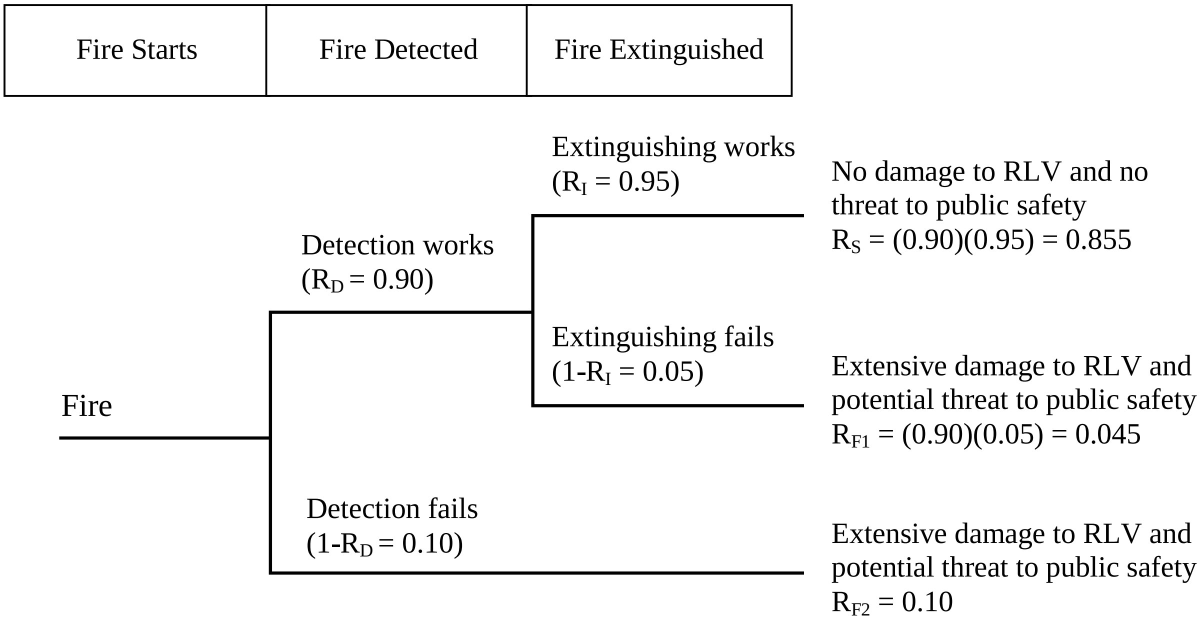


Figure A.5-1: Generic event tree

3. Use binary branching to show the system pathways. Note that some branch points will have two outcomes, success and failure; others will only have one outcome, success or failure. In the car accident example, the first branch might be the air bags will deploy (success), or the air bags will fail to deploy (failure).
4. Trace all possible permutations of a success or a failure. For example after “air bag fails to deploy,” the analyst might consider “seat belts hold” and “seat belts fail to hold” as the branches.
5. Prune the tree to eliminate unnecessary branches. Branches are unnecessary if they represent undefeatable successes or non-recoverable failures.
6. Assign probabilities to each branch.
7. Determine the probability for each potential path by multiplying the individual probabilities of events making up the path.

8. Determine the probability of system success by adding the probabilities for all paths ending in success.
9. Determine the probability of system failure by adding the probabilities for all paths ending in failure. Uncertainty analyses may also be incorporated by applying probability distributions to each path and then using Monte Carlo simulation to determine the uncertainty on the system failure probability. (See Philipson and Wilde for approaches to ETA with non-binary branches.)
10. Document the results.

Figure A.5-2 shows an event tree for a fire in a propellant feed system of an RLV.



Fire Starts
Fire Detected
Fire Extinguished
Extinguishing works
(R_I = 0.95)
No damage to RLV and no threat to public safety
R_S = (0.90)(0.95) = 0.855
Detection works
(R_D = 0.90)
Extinguishing fails
(1-R_I = 0.05)
Extensive damage to RLV and potential threat to public safety
R_{F1} = (0.90)(0.05) = 0.045
Fire
Detection fails
(1-R_D = 0.10)
Extensive damage to RLV and potential threat to public safety
R_{F2} = 0.10

Figure A.5-2: Example ETA for a fire in an RLV propellant feed system

In this example, one success scenario was identified, namely, where the fire was detected and extinguished. Therefore, the system success probability is R_S or 0.855. The system failure probability is calculated by summing R_{F1} and R_{F2}, which equals 0.145. Note that an FTA might be used to analyze the failures related to the fire detection system and provide input for the probability of failure for that subsystem.

<u>Advantages</u>

- An ETA enables assessment of multiple, coexisting faults and failures.
- An ETA identifies areas of system vulnerability, and failure propagation paths can be identified and traced.

Disadvantages

- An ETA accounts for only one initiating event; therefore, multiple analyses may be needed for a system.
- The analyst must foresee all the pathways in the analysis. Complementary analyses, such as FTA and FMECA, can assist in identifying additional pathways.
- The comparable failure and success probability estimates can be difficult to obtain. Failure modeling using FTA can assist in the development of these estimates.

Henley and Kumamoto (1992), NASA's *Probabilistic Risk Assessment Procedures Guide* (2002), NASA RP 1358 (Goldberg, 1994), and Philipson and Wilde (2000) provide additional information about ETA.

A.6 Reliability Allocation

In large complex systems, obtaining empirical data regarding the reliability of the whole system is sometimes possible. Verifying this estimate, determining the reliability drivers and the expected improvement to meet the reliability estimate, or identifying the needed amount of reliability testing may require assigning reliabilities to individual components or phases of flight. The process of assigning reliabilities is called reliability apportionment or reliability allocation. By allocating the reliability to subsystems, the importance of the subsystem function for the entire system can be realized. Additionally, basic reliability problems inherent in the design can be understood.

Reliability allocation models typically use the following assumptions:

- Component failures are independent.
- Failure of any component results in system failure (i.e., the system is comprised of components in series).
- Failure rates of the components are constant.

The process for performing a reliability allocation analysis is as follows:

1. Determine the reliability estimate for the system based on historical data for previous launches of vehicles developed and launched in similar circumstances.
2. Break the system down into subsystems.
3. Use a reliability allocation model to determine the minimum subsystem reliability necessary to meet the goal.

The simplest reliability allocation model assigns equal reliabilities to all subsystems to verify the specified level of reliability for the entire system. This model is called the “equal apportionment technique.” The reliability for each subsystem is calculated as follows:

$R_i = R_{sg}{}^{1/n}$

where

R_i	= Reliability for component or subsystem i
R_{sg}	= Reliability goal for the system
n	= Number of system elements or subsystems

Assume that a communications system consists of three components (transmitter, receiver, and coder). If the entire communications system must operate at a reliability of 0.99, then the component reliability assigned to each of these subsystems can be calculated as $R_i = R_s{}^{1/n} = (0.99)^{1/3} = 0.997$.

In the majority of circumstances, assuming that the subsystem reliability is allocated equally may not be reasonable. Using historical failure probabilities based on similar systems provides a more reasonable approach to allocating reliability. First, the percentage of failures for each subsystem is based on the historical data. Then, those percentages are used to allocate the reliability. For each component or subsystem, the reliability is calculated as follows:

$R_i = 1 - \omega_i\ (1- R_{sg})$

where

ω_i	= Weighting factor for component or subsystem i (based on historical data)
R_{sg}	= Reliability goal for the system
R_i	= Reliability for component or subsystem i

Consider a new launch vehicle with a reliability goal of 0.99. If for similar launch vehicles, historical data show 75 percent of the failures were caused by the propulsion system, 15 percent were caused by avionics, and 10 percent were caused by electrical systems, then the following apportionment could be developed:

$\omega_{propulsion} = 0.75$
$\omega_{avionics} = 0.15$
$\omega_{electrical} = 0.10$

$R_{propulsion} = 1- (0.75)(1 - 0.99) = .9925$

$R_{avionics} = 1 - (0.15)(1 - 0.99) = 0.9985$

$R_{electrical} = 1 - (0.10)(1 - 0.99) = 0.9990$

Kapur and Lamberson (1997) described a related method for allocating reliability when the subsystem reliabilities are unequal. This method uses subsystem failure rates based on historical data to determine weighting factors. The resulting weighting factors are then used to determine the subsystem reliability as follows:

$$\lambda_T = \sum_{i=1}^{n} \lambda_i$$

$$\omega_i = \lambda_i / \lambda_T$$

$$\lambda_s = -\ln(R_{sg})/t$$

$$R_i = \exp(-\omega_i \lambda_s t)$$

where

ω_i = Weighting factor for component or subsystem i
λ_I = Failure rate for component or subsystem i
R_{sg} = Reliability estimate for the system
λ_{sg} = System failure rate determined from reliability estimate
R_i = Reliability for component or subsystem i
t = Operating time

For example, consider a system composed of three subsystems with estimated failure rates of $\lambda_1 = 0.005$, $\lambda_2 = 0.003$, $\lambda_3 = 0.001$, based on historical data. The system has a mission time of 10 hours. Assuming a system reliability of 0.90 is required, component reliabilities are calculated as follows:

$$\omega_1 = 0.005/(0.005 + 0.003 + 0.001) = 0.555$$

$$\omega_2 = 0.003/(0.005 + 0.003 + 0.001) = 0.333$$

$$\omega_3 = 0.001/(0.005 + 0.003 + 0.001) = 0.111$$

$$\lambda_s = -\ln(0.90)/10 = 0.0105$$

$$R_1 = \exp -[(0.555)(0.0105)(10)] = 0.943$$

$$R_2 = \exp -[(0.333)(0.0105)(10)] = 0.966$$

$$R_3 = \exp -[(0.111)(0.0105)(10)] = 0.988$$

Other methods, such as the AGREE (Advisory Group on Reliability of Electronic Equipment) method and Effort Minimization, are described in Kapur and Lamberson (1977) and Lloyd and Lipow (1984).

Advantages

- Reliability allocation can be a powerful tool for performing design trade-offs, identifying reliability drivers and determining level of effort required for subsystems in regard to reliability testing and demonstration.

Disadvantages

- Based on the assumption that the subsystems must be independent, reliability allocation has its greatest value at the breakdown of a system into its major subsystems. However at lower levels of the system, the components can become interdependent. For example, the propellant feed system and the igniter on a rocket engine may interact. In these cases alternate methods, such as FTA, should be used.
- Simple allocation models may not be useful for highly complex systems, but other reliability allocation models are available (Mettas 2000).

Kapur and Lamberson (1977), Larson and Wertz (1995), Lloyd and Lipow (1984), MIL-STD-338B, and O'Connor (1991) provide additional information on reliability allocation.

A.7 Monte Carlo Simulation

In Monte Carlo simulation, a logical model of the system is repeatedly evaluated. Each individual evaluation of the logical model uses different values of the input parameters. Selection of input values is made randomly from probability distributions identified for each input parameter. The output is a set of values that may be characterized as a probability distribution, which can be used to identify the likelihood of an outcome or a range of outcomes. Monte Carlo simulation is often used for analyzing risk under conditions of uncertainty resulting from natural variability in processes, a lack of knowledge of the processes, or both.

The process for performing a Monte Carlo simulation is as follows:

1. Define the model of the system (inputs, outputs, mathematical relationships).
2. Define the possible values using a probability distribution for each uncertain input parameter. These distributions generally come from historical data or from operator experience.
3. Select the value for each input parameter randomly, based on the probability distribution.
4. Use the randomly generated input values and the mathematical relationships to determine the output values.

5. Repeat steps 3 and 4 for a sufficient number of trials.
6. Use all outputs generated to develop an output probability distribution.

Because the method requires hundreds or even thousands of trials, Monte Carlo simulations are normally performed using computer programs. Convergence criteria based on a desired confidence level and an allowable error can be used to determine whether the number of trials is sufficient (Murphy 2001). Alternately, a user may perform multiple simulations with the same number of trials and different random number generator seeds and compare the results to determine whether the differences in the output distribution parameters are acceptable or whether additional trials are needed.

As an example, consider again the propellant feed system reliability block diagram shown in figure A.1-2. The mathematical reliability relationship for the subsystem was developed using the reliability block diagram as follows:

$R_T = R_A\ R_B\ [1-(1-R_C)(1-R_D)]\ [1-(1-R_E)(1-R_F)]$

Instead of using point estimates to evaluate reliability, consider uncertainty in the inputs, and assign the probability distributions listed in table A.7-1.

Table A.7-1: Reliability data for Monte Carlo simulation

Item	Distribution Type	Mean	Standard Deviation
A	Normal	0.95	0.005
B	Normal	0.97	0.004
C	Lognormal	0.99	0.001
D	Lognormal	0.99	0.001
E	Lognormal	0.92	0.003
F	Lognormal	0.92	0.003

A Monte Carlo simulation could be run for 5000 trials producing the following results for the pressurization system reliability (see figure A.7-1).

Mean: 0.915
5% Lower Confidence Limit: 0.905
5% Lower Confidence Limit: 0.925

Advantages

- Monte Carlo simulation allows complex models to be simulated hundreds and thousands of times, and provides more information about risk than do single-point estimates (range and likelihood of outcomes).

- Monte Carlo simulation allows explicit analysis of uncertainty and provides analysis of the most important variables.

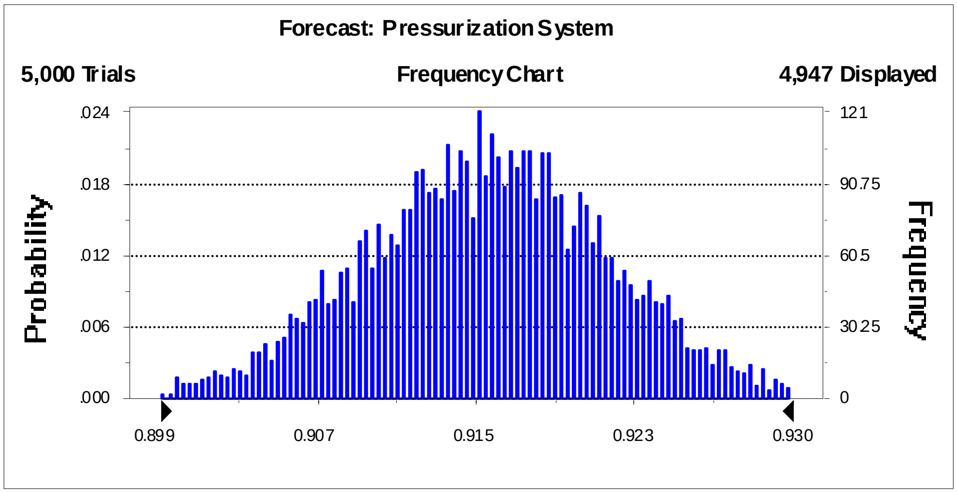


Figure A.7-1: Monte Carlo simulation output probability distribution for the pressurization system example

- Monte Carlo simulation can assist in the identification of the most sensitive parameters in an analysis.
- Monte Carlo simulation provides estimates of the confidence in the outputs.

<u>Disadvantages</u>

- Results of a Monte Carlo simulation depend on the quality of the random number generator.
- More information is needed about the inputs in a Monte Carlo simulation.
- A greater degree of analysis sophistication is required compared to conventional approaches.

Hammonds (1994), Henley and Kumamoto (1992), and EPA's *Guiding Principles for Monte Carlo Analysis* (1997) provide additional information on reliability allocation Monte Carlo simulations.

APPENDIX B: SYSTEM RELIABILITY ANALYSES

In this appendix, simplified examples illustrate how reliability allocation and probabilistic risk assessment estimate system reliability. Levels of detail required in developing a vehicle reliability estimate vary greatly, depending on the system complexity and scope of operations. These examples also illustrate how different reliability analyses can work together to produce a valid analysis and how reliability can be integrated with system safety.

Note that these examples are meant for illustration purposes only. The reliability values used and developed here do not represent an actual vehicle, so these values should not be used in preparing an RLV reliability estimate.

B.1 Reliability Allocation

Allocating reliability by mission phase and subsystem permits a developer to verify vehicle reliability, determine how much testing is required, and identify reliability drivers. Consider a new launch vehicle developer manufacturing an RLV to fly a mission similar to that of the X-15 airplane, which includes the following mission phases:

1. Drop from carrier vehicle
2. Powered flight
3. Reentry
4. Glide to landing

A developer should first identify past vehicle reliability of similar vehicles using historical mission and system descriptions and available data. Based on historical X-plane experience, the developer may estimate a vehicle failure probability of 0.05 for all phases of flight. However, vehicles built by inexperienced launch vehicle developers fail at rates 3 to 4 times higher than those built by experienced manufacturers. Therefore, an initial vehicle failure rate of 0.20 may be a more appropriate choice.

Expert opinion and X-plane experience also may show the following for conditional probability of failure by flight phase:

1.	Drop from carrier vehicle	1%
2.	Powered flight	48%
3.	Reentry	40%
4.	Glide to landing	11%

Therefore, by allocating the reliability based on historical data, the following conditional probabilities of failure can be obtained for each flight phase:

1.	Drop from carrier vehicle	(0.01)(0.20) = 0.002
2.	Powered flight	(0.48)(0.20) = 0.096

3. Reentry	(0.40)(0.20) = 0.080
4. Glide to landing	(0.11)(0.20) = 0.022

The next step is to break down the system into subsystems. The developer should consider the following subsystems based on the vehicle design:

- Structures
- Thermal Protection System
- Pneumatics and Hydraulics
- Propulsion and Propellant Feed
- Mechanical Flight Controls
- Electrical
- Life Support
- Guidance and Navigation

Information from U.S. launches may show the following subsystem contributions to failure during powered flight:

Structures	7%
Thermal Protection System	3%
Pneumatics and Hydraulics	11%
Propulsion and Propellant Feed	42%
Mechanical Flight Controls	17%
Electrical	11%
Life Support	5%
Guidance and Navigation	4%

The developer should decide whether these allocations apply to this X-plane-type vehicle. For the powered flight portion, using the powered flight probability of failure of 0.096, the following values can then be calculated for each subsystem based on equations shown in appendix A:

Structures	(0.07)(0.096) = 0.00672
Thermal Protection System	(0.03)(0.096) = 0.00288
Pneumatics and Hydraulics	(0.11)(0.096) = 0.01056
Propulsion and Propellant Feed	(0.42)(0.096) = 0.04032
Mechanical Flight Controls	(0.17)(0.096) = 0.01632
Electrical	(0.11)(0.096) = 0.01056
Life Support	(0.05)(0.096) = 0.00480

Guidance and Navigation	(0.04)(0.096) = 0.00384

The next step is to verify that the reliability estimates match the historical data for each subsystem. Often, this step is done using an FMECA approach. For each subsystem, a set of failure modes is identified and a failure probability is obtained (see appendix A). For the mechanical flight controls, the developer may postulate the failure modes (see figure B.1-1). The resulting probability of failure estimates would then be applied (see figure B.1-2).

ID	Item	Failure Modes	Failure Causes	Failure Effects	Risk Assessment			Detection Methods and Controls
					Sev.	Prob.	Risk	
2.0	Mechanical Flight Controls	a. Inability of elevators, ailerons, rudders to move. b. Breakage of elevators, ailerons, rudders.	a., b. Wear, fatigue, extreme operations, defective materials, poor workmanship	a., b. Loss of control, vehicle impact, debris	a.I b.I	a.B b.B	a.2 b.2	a., b. Design safety factor of 2, inspections, flight envelop expansion

Figure B.1-1: Sample FMECA for mechanical flight controls

ID	Item	Failure Modes	Component Failure Probability, p	Probability of failure from mode, α	Conditional probability, β	Failure mode probability, $p_m = \alpha\beta p$	Conditional failure probability, p_r
2.0	Mechanical Flight Controls	a. Inability of elevators, ailerons, rudders to move. a. Breakage of elevators, ailerons, rudders.	0.014 (Source: NASA CR-2001-210647)	a. 0.60 b. 0.40 (Source: Operator experience)	a. 1.0 b. 1.0 (conservative assumption)	a. 0.0084 b. 0.0056	0.014

Figure B.1-2: Failure probability estimates for mechanical flight controls

Assuming no additional failure modes have been identified, the failure probability of 0.014 is less than the allocated failure probability of 0.01632 for the mechanical flight controls. Therefore, the estimate appears to have been verified. This step would be repeated for each subsystem and for each flight phase.

Note that the developer should also account for uncertainty bounds on the data. For example, the data may show that the upper bound on the 90-percent confidence limit is 0.0155 for mechanical flight controls. Given the simplicity of the subsystem described in this example, this upper bound could be used to determine whether the subsystem met the allocated reliability goal. In this case, the subsystem still would meet the goal. For complex subsystems with multiple failure modes, Monte Carlo simulation could be used to identify the uncertainty associated with the probability of failure of the subsystem.

Because of limitations on reliability allocation as well as those of FMECA, additional verification methods are often employed. These analyses are especially useful when the difference between the historical reliability and the calculated system reliability is large. Such differences usually occur because the majority of analyses based on inductive methods fail to include system factors, such as the environment, software faults, and human error. For example, an analyst may construct a qualitative fault tree to examine the effects of multiple failures as well as the effects of non-hardware anomalies. A qualitative FTA can aid in examining the effects of mitigation measures used to improve reliability, such as adding redundancy. The following fault tree may be developed for the RLV system of this example (see figure B.1-3). Then the qualitative fault tree could be quantified, using existing data and the mathematical relationships in appendix A, in order to determine whether the top-level reliability estimate had been met.

B.2 Probabilistic Risk Assessment

Again, consider a new launch vehicle developer who is building an RLV to fly a mission similar to that of the X-15 airplane. The first step in PRA is to identify those initiating events that could result in desirable end states, such as completion of mission and protection of the public, and undesirable end states, such as mission failure and increased risk to the public. One approach in developing initiating events is to consider satisfactory and unsatisfactory states of the same operations. For example, an RLV using a flight profile similar to the X-15 airplane might have the following normal functional operations:

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

As determined from a functional analysis or hazard analysis, abnormal conditions after drop might be as follows:

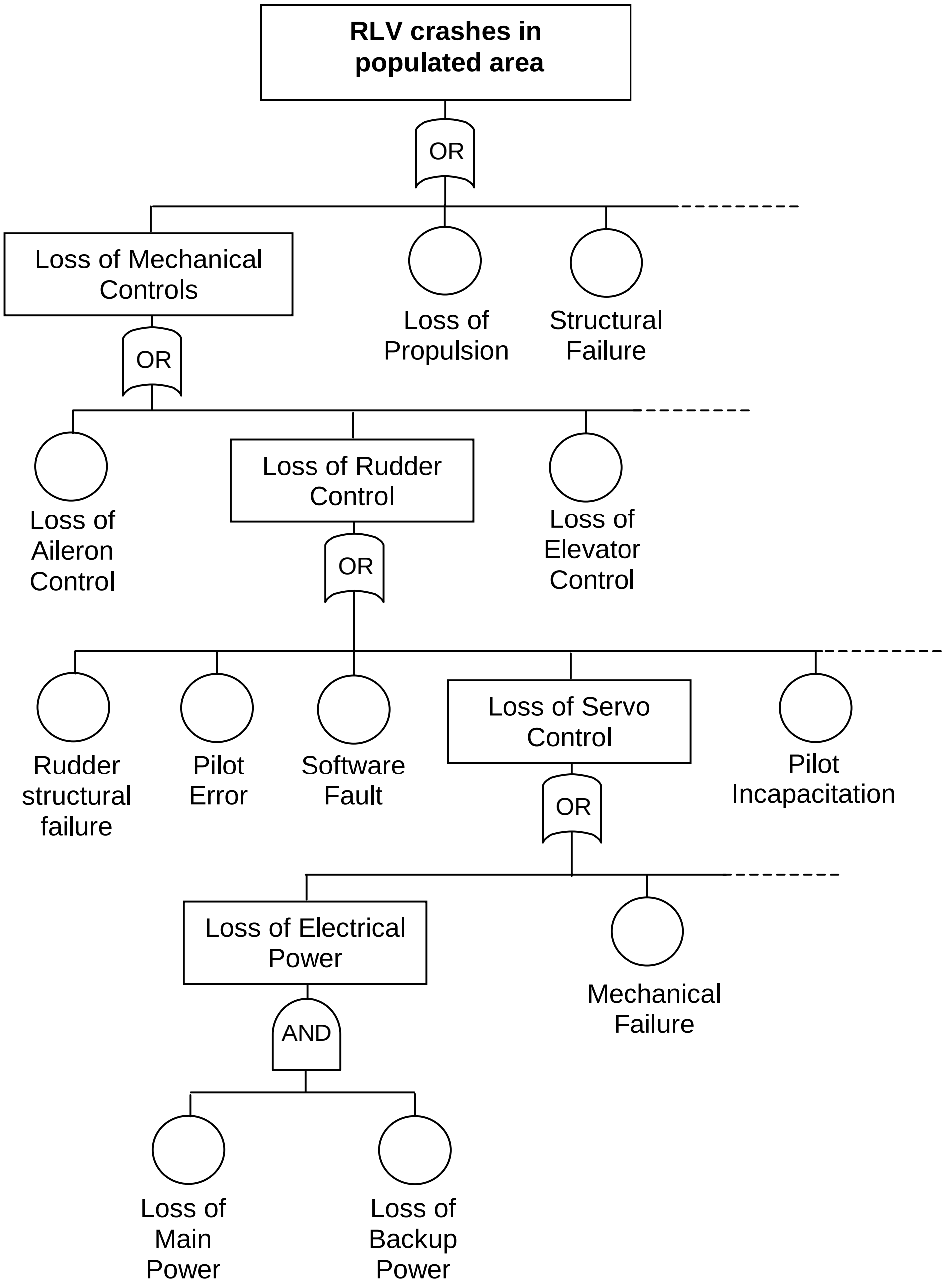


Figure B.1-3: Partial FTA for loss of mechanical controls

- Failure to start engines
- Failure to control thrust
- Failure to shut engines down at specified time

Event scenarios can then be developed based on the satisfactory and unsatisfactory initiating events. A common approach is to use an ETA. Figure B.2-1 shows the event tree for this simplified example.

The next step in the process involves developing failure models for the pivotal events, those successes and failures that can ultimately lead to the success of a mission or a mishap. Figure B.2-1 shows the failure of the engine to shut down properly as a pivotal event, leading to the potential for an uncontrolled crash. Fault Tree Analysis is often used to develop these failure models. Figure B.2-2 shows an example of a fault tree for engine shutdown failure.

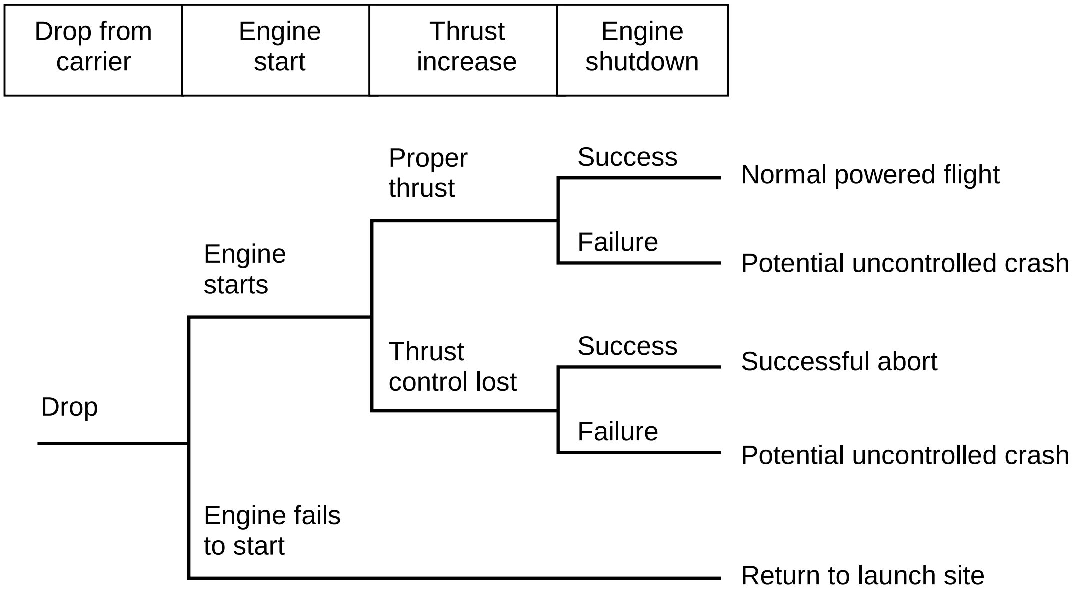


Figure B.2-1: Sample event tree for an RLV

The next step is to quantify the fault tree. Consider the data in table B.2-1 for use in the example. Using the mathematical relationships in appendix A, the probability of the top event (unable to shut down engine after cutoff) is then calculated to be 8.4E-05.

Monte Carlo simulation can then be run to determine the confidence levels on the top event failure probability by evaluating the logical model using random values of the input parameters from probability distributions identified for each input parameter. Based on a Monte Carlo simulation (5000 trials), the lower 5-percent confidence limit on the failure probability would be 2.8E-05. The upper 95-percent confidence limit would be 1.4E-04. Figure B.2-3 shows the distribution obtained for the top event failure probability.

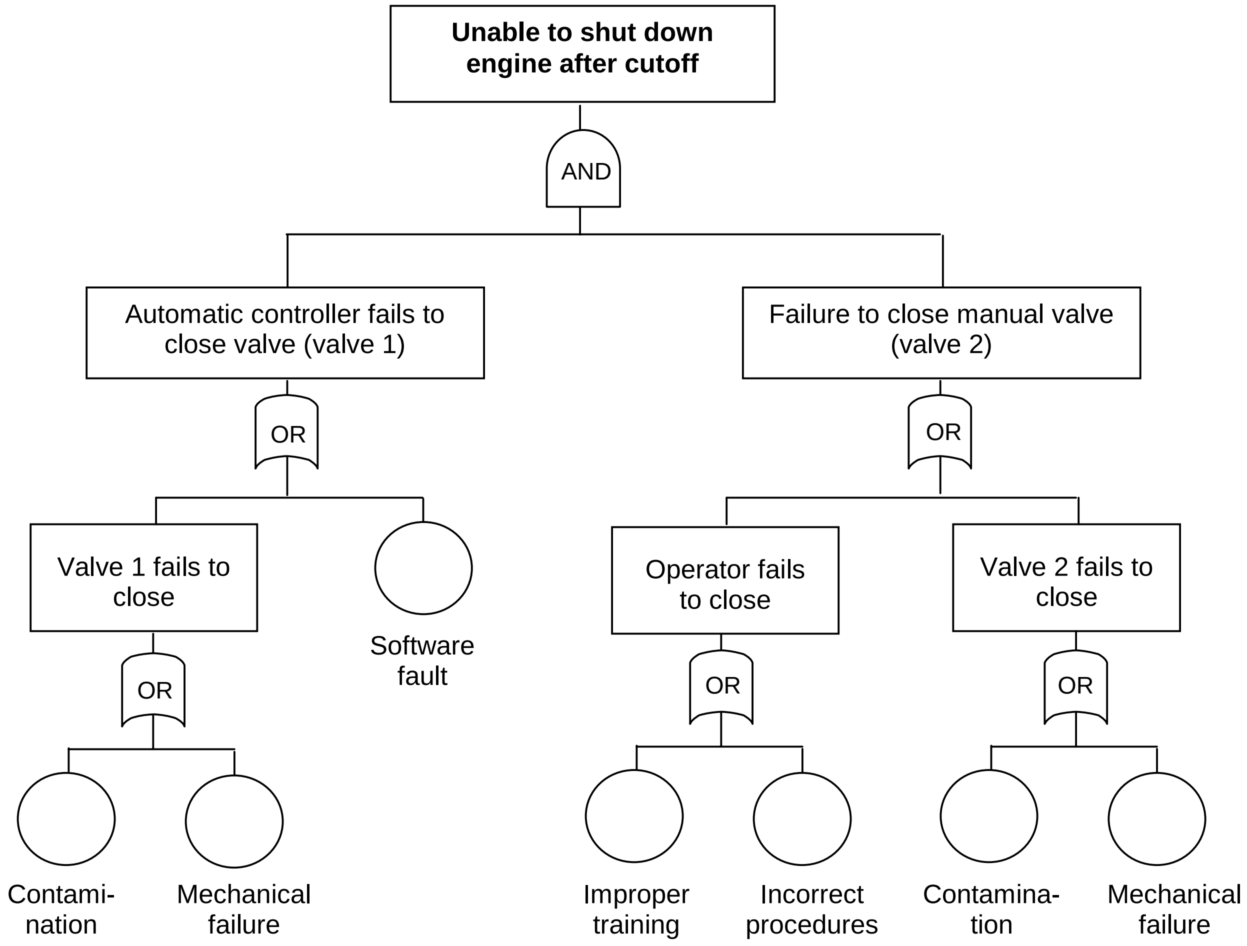


Figure B.2-2: Fault tree for engine shutdown failure

Table B.2-1: Hypothetical input failure probability values

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

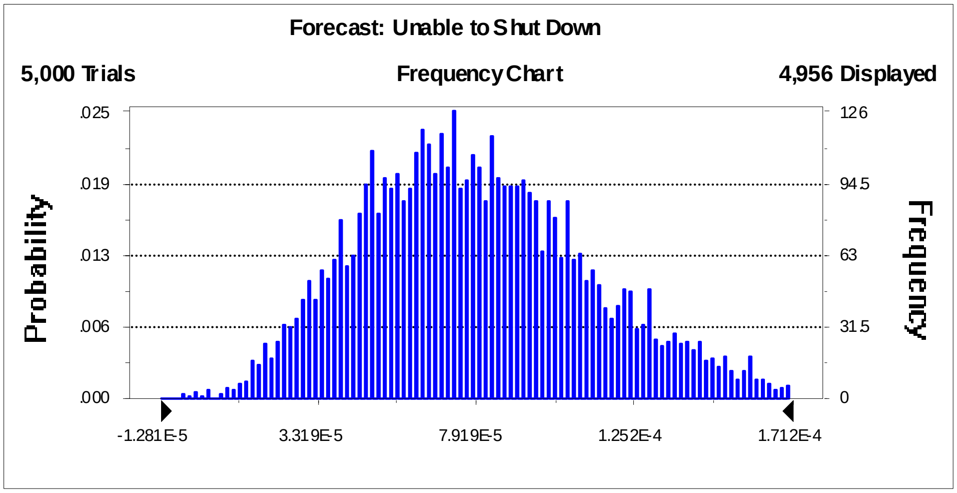


Figure B.2-3: Monte Carlo simulation output distribution, engine shutdown failure probability

REFERENCES

Bedford, Tim and Roger Cooke, *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge: Cambridge University Press, 2001.

Christenson, R. L., M. R. Whitley, and K. C. Knight, *Comprehensive Design Reliability Activities for Aerospace Propulsion Systems,* NASA Technical Publication 2000-209902, January 2000.

Dhillon, B. S., *Design Reliability*, Boca Raton: CRC Press, 1999.

Dovich, Robert A., *Reliability Statistics*, Milwaukee, WI: ASQC Quality Press, 1990.

Department of Defense, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, MIL-STD-1629A, Washington, D.C., November 24, 1980.

--------. *Reliability Modeling and Prediction*, MIL-STD-756B, Washington, D.C., November 18, 1981.

--------. *Reliability Program Requirements for Space and Launch Vehicles*, MIL-STD-1543B (USAF), Washington, D.C., October 25, 1988.

--------. *Reliability Prediction of Electronic Equipment*, MIL-HDBK-217F, Washington, D.C., December 2, 1991.

--------. *Electronic Reliability Design Handbook*, MIL-HDBK-338B, Washington, D.C., October 1, 1998.

Environmental Protection Agency, *Guiding Principles for Monte Carlo Analysis*, EPA/630/R-97/001, March 1997.

Federal Aviation Administration, *System Design and Analysis*, Advisory Circular 25.1309-1A, Washington, D.C., June 21, 1988.

--------. Associate Administrator for Commercial Space Transportation, *Reusable Launch and Reentry Vehicle System Safety Process*, Advisory Circular 431.35-2, Washington, D.C., September 2000.

--------. Associate Administrator for Commercial Space Transportation, *Guide to Reusable Launch Vehicle Safety Validation and Verification Planning*, version 1.0, Washington, D.C., September 2003.

--------. Associate Administrator for Commercial Space Transportation, *Draft FAA Guidelines on Probability of Failure Analysis for New Expendable Launch Vehicles*, Washington, D.C., September 2004.

Goldberg, et al., *System Engineering "Toolbox" for Design-Oriented Engineers*, NASA Reference Publication 1358, December 1994.

Guikema, Seth D. and M. Elizabeth Pate'-Cornell, "Bayesian Analysis of Launch Vehicle Success Rates," *Journal of Spacecraft and Rockets*, vol. 41, no. 1, January-February 2004, pp. 93-102.

Hammonds, J. S., F. O. Hoffman, and S. M. Bartell, *An Introductory Guide to Uncertainty Analysis in Environmental and Health Risk Assessment*, ES/ER/TM-35/R1, Oak Ridge National Laboratory, December 1994.

Henley, Ernest J. and Hiromitsu Kumamoto, *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*, New York: IEEE Press, 1992.

Institute of Electrical and Electronics Engineers, Inc., *IEEE Standard Methodology for Reliability Prediction and Assessment for Electronic Systems Equipment*, IEEE 1413-1998, New York, 1998.

Kapur, Kailash C. and L. R. Lamberson, *Reliability in Engineering Design*, New York, NY: Wiley & Sons, 1977.

Hecht, Herbert, "Reliability During Space Mission Concept Exploration," *Space Mission Analysis and Design*, 2nd edition, edited by Wiley J. Larson and James R. Wertz, Torrance, CA: Microcosm, Inc., and Dordrecht: Kluwer Academic Publishers, 1995, pp. 700-714.

Leveson, Nancy G., *Safeware: System Safety and Computers*, Reading: Addison-Wesley, 1995.

Lloyd, David K. and Myron Lipow, *Reliability: Management, Methods, and Mathematics*, 2nd ed., Milwaukee, WI: ASQC Press, 1984.

Mettas, Adamantios, "Reliability Allocation and Optimization for Complex Systems," *Proceedings, 2000 Reliability and Maintainability Symposium*, Los Angeles: January 24-27, 2000.

Murphy, Kenneth E., Charles E. Carter, and Larry H. Wolf, "How Long Should I Simulate, and for How Many Trials? A Practical Guide to Reliability Simulations," *Proceedings, 2001 Reliability and Maintainability Symposium*, Philadelphia: January 22-25, 2001.

National Aeronautics and Space Administration, *Planning, Developing, and Managing an Effective Reliability and Maintainability (R&M) Program*, NASA Technical Standard 8729.1, Washington, D.C., December 1998.

--------. *Fault Tree Handbook with Aerospace Applications*, version 1.1. Prepared for Office of Safety and Mission Assurance, Washington, D.C., August 2002.

--------. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, version 1.1. Prepared for Office of Safety and Mission Assurance, Washington, D.C., August 2002.

O'Connor, Patrick D. T., *Practical Reliability Engineering*, 3rd ed., Chichester: Wiley & Sons, 1991.

Philipson, L. L. and P. D. Wilde, "Sampling of Uncertain Probabilities at Event Tree Nodes with Multiple Branches," *Reliability Engineering and System Safety*, 70 (2000), pp. 197-203.

Society of Automotive Engineers, Inc., *Reliability and Safety Process Integration*, Aerospace Information Report (AIR) 5022, Warrendale, PA, 1996.

--------. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, Aerospace Recommended Practice (ARP) 4761, Warrendale, PA, 1996.

U.S. Air Force, Air Force Space Command, *Range Safety User Requirements Manual – Air Force Space Command Range Safety Policies and Procedures,* AFSC manual 91-710, vol. 1, July 1, 2004.

U.S. Office of Management and Budget, *Revised Information Quality Bulletin for Peer Review*, Washington, D.C., April 15, 2004.

Vesely, W. E., et al., *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D.C., November 1981.

Vesely, W. E. and D. M., Rasmuson, "Uncertainties in Nuclear Probabilistic Risk Analyses," *Journal of Risk Analysis*, vol. 4, no. 4, 1984.