RELIABILITY ENGINEERING
MISSION SUCCESS STARTS WITH RELIABILITY
Introduction

- This tutorial is a brief summary of a three-day reliability engineering course offered by A-P-T Research, Inc.
- The course is intended to provide a better understanding of reliability engineering as a discipline with focus on the reliability analysis tools and techniques and their application in technical assessments and special studies.
- The material in the course is based on over 30 years of extensive industry and Government experience in reliability engineering and risk assessment.
- For offerings, contact: Megan Stroud, 256-327-3373, training@apt-research.com.
- **Note:** Attendees of the full course will be credited with 2.0 Continuing Education Units (CEU).
Table of Contents

- Introduction
- Probability Basics
- Reliability Engineering Overview
- Reliability Allocation
- Reliability Prediction
- Reliability Demonstration
- Failure Modes and Effects Analysis (FMEA)
- Reliability Growth
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)

- Probabilistic Risk Assessment (PRA)
- Human Reliability – Understanding Operator Error
- Availability Analysis
- Accelerated Testing
- Parts Derating
- Sneak Circuit Analysis
- Concluding Remarks
- Summary Tables

This tutorial covers only sections shown in blue.
SEAC Courses

- System Safety
- Software System Safety
- Explosives Safety
- Launch Safety (inactive)
- Risk Management
- Reliability Engineering
- Probabilistic Risk Assessment (PRA)
Definitions

- **Reliability Engineering** is the engineering discipline that deals with how to design, produce, ensure, and assure reliable products to meet pre-defined product functional requirements.

- **Reliability Metric** is the probability that a system or component performs its intended functions under specified operating conditions for a specified period of time. Other measures used: Mean Time Between Failures (MTBF), Mean Time to Failure (MTTF), Safety Factors, and Fault Tolerances, etc.

- **Operational Reliability Prediction** is the process of quantitatively estimating the mission reliability for a system, subsystem, or component using both objective and subjective data.

- **Design Reliability Prediction** is the process of predicting the reliability of a given design based on failure physics using statistical techniques and probabilistic engineering models.

- **Process Reliability** is the process of mapping the design drivers in the manufacturing process to identify the process parameters critical to generate the material properties that meet the specs. A high process reliability is achieved by maintaining a uniform, capable, and controlled processes.

- **Reliability Demonstration** is the process of quantitatively demonstrating certain reliability level (i.e., comfort level) using objective data at the level intended for demonstration.
Why Reliability Engineering

- Reliability engineering is a design-support discipline.
- Reliability engineering is critical for understanding component failure mechanisms and identifying critical design and process drivers.
- Reliability engineering has important interfaces with, and input to, design engineering, maintainability and supportability engineering, test and evaluation, risk assessment, risk management, system safety, sustainment cost, and quality engineering.
A comprehensive reliability program is essential to address the entire spectrum of engineering and programmatic concerns, from loss of function and loss of life to sustainment and system life cycle costs.
Design Reliability

- Element Design
- Critical Design Parameters (CDP)
- Materials Properties & Geometry

Process Reliability

- Processing
  - Map the CDP To Processing
  - Identify Critical Process Variables (CPV)

- Process Characterization
  - Explore Relationship between CDP and CPV

- Process Control
  - Select Control Strategy
  - Assess Process Capability
Design Reliability
The Challenger Accident

Causes and Contributing Factors

- The zinc chromate putty frequently failed and permitted the gas to erode the primary O-rings.
- The particular material used in the manufacture of the shuttle O-rings was the wrong material to use at low temperatures.
- Elastomers become brittle at low temperatures.
Process Reliability
The Columbia Accident

**Causes and Contributing Factors**

- Breach in the Thermal Protection System caused by the left bipod ramp insulation foam striking the left wing leading edge.
- There were large gaps in NASA’s knowledge about the foam.
- Dissections of foam revealed subsurface flaws and defects as contributing to the loss of foam.
Reliability Check List

The following is a partial reliability check list:

- **Design Reliability**
  - Do we understand the design drivers?
  - Do we understand the design uncertainties?
  - Do we understand the physics of failure?
  - Do we understand the failure causes?
  - Do we have the right design margins?

- **Process Reliability**
  - Is the process capable of building the tolerances?
  - Do we have process uniformity?
  - Do we have process control?

- **Reliability Analysis and Testing**
  - Have we done a timely FMEA consistent with design timeline?
  - Do reliability predictions support the goals and requirements of the program?
  - Have we done enough reliability testing and demonstration to support the design?

- **Systems Engineering**
  - Do we understand the requirements?
  - Are we part of system integrated analysis environment?
There are many ways to measure and evaluate reliability. The following are the most commonly used across government and industry:

- **Mean Time Between Failures (MTBF)/Mean Time to Failure (MTTF)**
  - MTBF is a basic measure of reliability for repairable items. MTBF is the expected value of time between two consecutive failures, for repairable systems.
  - MTTF is a basic measure of reliability for non-repairable systems. It is the mean time expected until the first failure.

- **Predicted Reliability Numbers**
  - Reliability prediction is the process of quantitatively estimating the reliability using both objective and subjective data (e.g. 0.99999).
Reliability Metrics (Continued)

- **Demonstrated reliability numbers**
  - Unlike reliability prediction, reliability demonstration is the process of quantitatively estimating the reliability of a system using objective data at the level intended for demonstration. In general, demonstrated reliability requirement is set at a lower level than predicted reliability. It is intended to demonstrate a comfort level with a lower reliability than the predicted reliability because of the cost involved *(e.g., 0.99 with 90% confidence)*.

- **Safety factors**
  - Safety factor (SF) is a term describing the capability of a system beyond the expected loads or actual loads *(e.g., safety factor of 2)*.

- **Fault tolerances**
  - Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some of its components *(e.g., one fault tolerance means you can tolerate one failure and still operate successfully)*.
“How Reliable is Reliable Enough?”

- In reliability engineering, no one likes things to fail. We don’t like bridges to collapse and we don’t like nuclear plants to leak radioactive material.

- Engineers still have to address the question “How reliable is reliable enough?” Is it one in a thousand? One in ten thousands? One in a million?

- The answer is: It depends. For example, “reliable enough” for a critical situation might mean a high safety factor (e.g., 2.0 or better), or high reliability (e.g., 0.999999 or better). For degraded performance, a lower safety factor or lower reliability might be acceptable.

- For these reasons, engineers must design things to certain reliability specifications depending on the safety and economics of the situation, technology availability, and design constraints.
A comprehensive reliability program is essential to address the entire spectrum of engineering and programmatic concerns, from loss of function and loss of life to sustainment and system life cycle costs.
Reliability Relationship to Life Cycle Cost

TOTAL COST OF OWNERSHIP

- Unscheduled Maintenance
- Purchase Price
- Scheduled Maintenance

Cost vs. Level of Reliability
### Reliability Relationship to Safety

<table>
<thead>
<tr>
<th></th>
<th>Reliability</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Roles</strong></td>
<td>To ensure the product functions successfully.</td>
<td>To ensure the product and environment are safe and hazard free.</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td>Design function specific within the function boundary. Internally imposed.</td>
<td>Non-function specific such as “no fire,” “no harm to human beings.” Externally imposed.</td>
</tr>
<tr>
<td><strong>Approaches</strong></td>
<td>Bottom-up and start from the component or system designs at hand.</td>
<td>Top-down and trace the top-level hazards to basic events, then link to the designs.</td>
</tr>
<tr>
<td><strong>Analysis Boundaries</strong></td>
<td>Focus on the component or sub-system being analyzed (assumes others are at as-designed and as-built conditions). Component interactions and external vulnerability and uncertainty are usually not addressed.</td>
<td>System view of hazards with multiple and interacting causes. External vulnerability and uncertainty may be required to be addressed.</td>
</tr>
</tbody>
</table>

*Safety and Reliability are unique but closely related — they complement each other and need to be integrated.*
RELIABILITY ALLOCATION

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com
Reliability Allocation Definitions

- **Reliability allocation** is the process of allocating the system reliability requirement or goal down to the subsystems level through apportionment.

- In general, reliability allocation is intended to drive a process to improve the product reliability during the design development process through prediction down to the subsystem or component levels.

- **Note:** Quantitative reliability requirements can be predicted, demonstrated, or both, depending on the objectives and the economics of the project or the program.
  
  - Predicted reliability requirement calls for estimating the reliability using both objective and subjective data, where reliability prediction is performed to the lowest identified level of design for which data is available.
  
  - Demonstrated reliability requirement calls for estimating the reliability of a system using objective data at the level intended for demonstration. **Demonstrated reliability requirement is intended to provide empirical evidence of design reliability and can’t be allocated.**
Reliability Allocation Process

- Reliability allocation involves solving the following inequality:

\[ f(R_1, R_2, \ldots, R_n) \geq R_s \]

where:
\( R_i \) is the reliability allocated to the \( i^{th} \) subsystem/component.
\( f \) is the functional relationship between the subsystem/component and the system.
\( R_s \) is the required system reliability.
Several techniques have been used over the years for reliability allocation. Commonly used techniques are:

- The simplest technique is **Equal Apportionment**, which distributes system reliability equally among all the subsystems.
- The **ARINC** apportionment method designed by ARINC Research Corporation, a subsidiary of Aeronautical Radio, Inc (ARINC).
- The **AGREE** apportionment method, designed by the Advisory Group on Reliability of Electronic Equipment (AGREE).

Both the AGREE and ARINC techniques take additional weighting factors into consideration during allocation.

To obtain good results, it is important to choose an appropriate apportionment method based on the system reliability requirement and the system properties.

_The following charts cover the Equal Apportionment and the ARINC Methods. The AGREE method is included in the backup section._
Reliability Allocation Methods/Techniques

- **Equal Apportionment**
  - The simplest apportionment technique is to distribute the reliability uniformly among all components. This method is called equal apportionment.
  - Equal apportionment assumes a series of n subsystems, all in series and having an exponential failure distribution. Each subsystem is assigned the same reliability. The mathematical model can be expressed as:

\[
R^* = \prod_{i=1}^{n} R_i^* \quad \text{for } i = 1, 2, ..., n
\]

Where:
- \( R^* \) is the required system reliability
- \( R_i^* \) is the reliability requirement apportioned to subsystem i
- n is the total number of subsystems.

\[
R_i^* = \left( R^* \right)^{\frac{1}{n}}
\]
Consider a proposed communication system which consists of three subsystems (transmitter, receiver, and coder), each of which must function if the system is to function. Each of these subsystems is to be developed independently. Historical data from previous programs showed that the three subsystems have very similar failure rates. What reliability requirement should be assigned to each subsystem in order to meet a system requirement R of 0.729?

The apportioned subsystem requirements are found as:

\[ R_T = R_R = R_C = (R)^{1/n} = (0.729)^{1/3} = 0.90 \]

Where \( R_T \), \( R_R \), and \( R_C \) are the transmitter, receiver, and coder reliabilities, respectively.

A reliability requirement of 0.90 should be assigned to each subsystem in order to meet a system reliability requirement of 0.729.
The ARINC Apportionment Method assumes that all subsystems are in series and have an exponential failure rate. Allocations are derived based on weighting factors. The mathematical expression is:

\[ w_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} \]

Where, n is the total number of subsystems, \( \lambda_i \) is the present failure rate of the \( i^{th} \) subsystem, \( \lambda_S \) is the required system failure rate, and \( \lambda_i' \) is the failure rate allocated to the \( i^{th} \) subsystem.

ARINC Apportionment Example


<table>
<thead>
<tr>
<th>Name</th>
<th>Part Number</th>
<th>Include</th>
<th>Present Failure Rate (FITS)</th>
<th>Allocated Failure Rate (FITS)</th>
<th>Allocated MTBF (hrs)</th>
<th>Current Failure Rate (FITS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>1.1</td>
<td>✓</td>
<td>30.9971</td>
<td>6.3508</td>
<td>1.5746E+05</td>
<td>30.9971</td>
</tr>
<tr>
<td>Transformer</td>
<td>1.2</td>
<td>✓</td>
<td>19.5772</td>
<td>4.0110</td>
<td>2.4931E+05</td>
<td>19.5772</td>
</tr>
<tr>
<td>Switch</td>
<td>1.3</td>
<td>✓</td>
<td>3.8967</td>
<td>0.7984</td>
<td>1.2526E+06</td>
<td>3.8967</td>
</tr>
<tr>
<td>Load</td>
<td>1.4</td>
<td>✓</td>
<td>4.2330</td>
<td>0.8673</td>
<td>1.1530E+06</td>
<td>4.2330</td>
</tr>
</tbody>
</table>

\[
W_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i}
\]

\[
\lambda_i = w_i \lambda_S
\]
Main Advantages

► Reliability allocation helps optimize the best combination of component reliability improvements that meet the intended reliability goals and at sufficient allocated costs.

► It provides a realistic view of subsystem performance required to meet system objectives.

► It shows the most cost-effective areas for design improvements; and avoids putting design efforts into subsystems that may not gain any additional reliability by improvements.
Main Limitations

- Most allocation methods apply only to series configurations.
- The apportionment process of reliability values between the various subsystems in many cases has high level of subjectivity. It is usually made on the basis of achievable reliability, or any other factors considered appropriate by the analyst making the allocation.
- Most allocation methods require the availability of equipment historical data in order to reduce subjectivity and produce credible and reasonable allocation estimates.
RELIABILITY PREDICTION

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com
Reliability Prediction - Definition

- Reliability prediction is the process of quantitatively estimating the reliability using both objective and subjective data. It is one of the most common forms of reliability analysis.
- Reliability prediction is performed to the lowest identified level of design for which data is available.
- Reliability prediction techniques are dependent on the degree of the design definition and the availability of the relevant data.
The Bathtub Curve - Hardware Reliability

- **Infant Mortality Region**: (Decreasing Failure Rate) (e.g., Process-Related Failures)
- **Random Failures**: (Design Life)
- **Wearout Region**: (Increasing Failure Rate) (e.g., Physics-Related Failures)

**TIME**

**INSTANTANEOUS FAILURE RATE**
RELIABILITY PREDICTION USING RELIABILITY BLOCK DIAGRAMS (RBDS)
A Reliability Block Diagram (RBD) is a **static form** of reliability analysis using inter-connected boxes (blocks) to show and analyze the effects of failure of any component on the system reliability.

The diagram represents the functioning state (i.e., success or failure) of the system in terms of the functioning states of its components. For example, a simple series configuration indicates that all of the components must operate for the system to operate, a simple parallel configuration indicates that at least one of the components must operate, and so on.
Reliability Block Diagrams

- RBDs provide a success-oriented view of the system.
- RBDs provide a framework for understanding redundancy.
- RBDs facilitate the computation of system reliability from component reliabilities.
- RBDs and fault trees provide essentially the same information. However, RBDs are easier to use and communicate.
Reliability Block Diagrams
Classifications

- The most commonly used types of RBDs are:
  - Simple series (all items have to function successfully)
  - Simple active parallel (all items operating simultaneously in parallel and only one is needed)
  - Standby parallel redundancy (alternate items are activated upon failure of the first item; only one item is operating at a time to accomplish the function)
  - Shared parallel (failure rate of remaining items change after failure of a companion item)
  - **r-out-of-n Systems** – Redundant system consisting of n items in which r of the n items must function for the system to function (voting decision).
- Combination of series and parallel systems

**Note:** We will not cover shared and r-out-of-n Systems redundancy
2-Components Case

The general expression for a series system with two components is:

\[ R_{\text{System}} = R_1 \times R_2 \]

Example

\[ R_{\text{System}} = 0.99 \times 0.95 \]

General n Series Components Case

\[ R_{\text{System}} = R_1 \times R_2 \times R_3 \times \ldots \times R_n \] where \( R_s \) = probability that system will work.
**2-Components Case**

The general expression for a parallel system with two components is:

\[ R_{\text{System}} = 1 - (1-R_1)(1-R_2) \]

If \( Q_1=1-R_1 \) and \( Q_2=1-R_2 \)

Then, \( R_{\text{System}} = 1-Q_1 \times Q_2 \)

**Example**

The reliability of the redundant system

\[ R = 1-Q_1 Q_2 = 1 - (0.01)(0.01) = 0.9999 \]

**General n redundant components Case**

\[ R_{\text{system}} = 1-(Q_1 Q_2 Q_3...Q_n) \]
The general reliability formula for \( n \) exponentially, identically distributed, and independent units in a standby redundant configuration (with perfect switching, \( R_s = 1 \)) is:

\[
R = \sum_{i=0}^{n-1} \left\{ \frac{(\lambda t)^i}{i!} \right\} e^{-\lambda t}
\]

**Two Component Case**

Assume, one shot switching reliability = 1, \( \lambda_{\text{switch}} = 0 \), failure rates are constant \( \lambda_1 = \lambda_2 = 0.0001 \) and

Mission duration \( t_1 = t_2 = 1000 \) hrs.

Substituting \( \lambda = 0.0001 \) and \( t = 1000 \) into the above equation we have:

\[
R = \left( \frac{(0.0001)^0}{0!} \right) e^{-0.0001 \times 1000} + \left( \frac{(0.0001)^1}{1!} \right) e^{-0.0001 \times 1000}
\]

\[
R = e^{-0.0001 \times 1000} + (0.0001 \times 1000) \times e^{-0.0001 \times 1000}
\]

\[
R = 0.90484 + (0.1) \times 0.90484 = 0.9953
\]
Assume

\[ R_1 = 0.99, \quad R_2 = 0.999, \quad R_3 = 0.95 \]
\[ R_4 = 0.85, \quad R_5 = 0.89, \quad R_6 = 0.78 \]

Solving first for the parallel portion of the system we have:

\[ R_X = 1 - Q_4 Q_5 Q_6 = 1 - (1-0.85)(1-0.89)(1-0.78) \]
\[ R_X = 1 - (0.15)(0.11)(0.22) = 1 - 0.00363 = 0.996 \]

Now solving the series and then combine with parallel portion of the diagram, we have:

\[ R_s = R_1 R_2 R_3 R_X \]
\[ R_s = (0.99)(0.999)(0.95)(0.996) = 0.936 \]
PHYSICS BASED RELIABILITY PREDICTION
Physics-Based Reliability Prediction

- Physics-based reliability prediction is a methodology to assess component reliability for given failure modes.

- The component is characterized by a pair of transfer functions that represent the load (stress, or burden) that the component is placed under by a given failure mode, and capability (strength) the component has to withstand failure in that mode.

- The variables of these transfer functions are represented by probability density functions.

- The interference area of these two probability distributions is indicative of failure.
Assuming both the stress and strength are normally distributed, the following expression defines the reliability for a structural component. If

\[ R = \Phi \left[ \frac{\mu_s - \mu_s}{\sqrt{\sigma_s^2 + \sigma_s^2}} \right] \]

Where
- \( \mu_s \) = mean value of the stress
- \( \sigma_s \) = standard deviation of the stress
- \( \mu_S \) = mean value of the strength
- \( \sigma_S \) = standard deviation of the strength

**Note 1:** In general, reliability is defined as the probability that the strength exceeds the stress for all values of the stress.

**Note 2:** Normality assumption does not apply to all engineering phenomena; and, under these special circumstances when the Normal does not apply, different methodology is used to determine reliability. As long as the engineering phenomena can be modeled, by whatever distribution, reliability could be obtained by methods such as the Monte Carlo method. Since the overwhelming majority of engineering phenomena do follow the normal distribution, the normality assumption is certainly the place to start.
During rig testing, the High Pressure Fuel Turbo-pump (HPFTP) Bearing of the Space Shuttle Main Engine (SSME) experienced several cracked races. Three out of four tests failed (440C bearing races fractured). As a result, a study was formulated to:

- Determine the probability of failure due to the hoop stress exceeding the material’s capability strength causing a fracture.
- Study the effect of manufacturing stresses on the fracture probability for two different materials, the 440C (current material) and the 9310 (alternative material).

The **hoop stress** is the force exerted circumferentially (perpendicular both to the axis and to the radius of the object) in both directions on every particle in the cylinder wall. Along with axial **stress** and radial **stress**, circumferential **stress** is a component of the **stress** tensor in cylindrical coordinates.
Physics-Based Reliability Prediction
A Rocket Engine Roller Bearing Example

- The Simulation Model

Randomly select values for inner race mat'l properties

Randomly select values for shaft/sleeve mat'l properties

Tolerance fits of rig test bearing

Inner race hoop stress at given conditions

Shaft/sleeve hoop stress at given conditions

Total hoop stress

Stress due to manufacturing

Stress > allowable load

Iterate and compute failure probability

Variation in:
- Fracture toughness
- Yield strength
- No. of cracks
- Crack depth
- Crack length

Compute allowable load for each crack

Compute allowable load (worst crack)
The Simulation Model

- Since this failure model is a simple overstress model, only two distributions need to be simulated: the hoop stress distribution and the materials capability distribution.
- In order to calculate the hoop stress distribution it was necessary to determine the materials properties variability.
- Of those materials, properties that affected the total inner race hoop stress, a series of equations was derived which mapped these life drivers (such as modulus of elasticity, coefficient of thermal expansion, etc.) into the total inner race hoop stress.
- In order to derive these equations, several sources of information were used which included design programs, equations from engineering theory, manufacturing stress data, and engineering judgment. This resulted in a distribution of the total hoop stress.
The Simulation Model

- In a similar fashion, a distribution on the materials capability strength was derived.
- In this case, life drivers such as fracture toughness, crack depth/length, yield strength, etc., were important. The resulting materials capability strength distribution was then obtained through a similar series of equations.
- The Monte Carlo simulation in this case would calculate a random hoop stress and a random materials capability strength. If the former is greater than the latter, a failure due to overstress occurs in the simulation. Otherwise, a success is recorded.
- The simulation was run for two different materials: 440C (current material) and 9310.
- After several thousand simulations are conducted, the percent which failed are recorded.
Analysis Results

<table>
<thead>
<tr>
<th>Test Failures</th>
<th>Race Configuration</th>
<th>Failures in 100,000 firings**</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 of 4</td>
<td>440C w/ actual* mfg. stresses</td>
<td>68,000</td>
</tr>
<tr>
<td>N/A</td>
<td>440C w/ no mfg. stresses</td>
<td>1,500</td>
</tr>
<tr>
<td>N/A</td>
<td>440C w/ ideal mfg. stresses</td>
<td>27,000</td>
</tr>
<tr>
<td>0 of 15</td>
<td>9310 w/ ideal mfg. stresses</td>
<td>10</td>
</tr>
</tbody>
</table>

* ideal + abusive grinding  
** Probabilistic Structural Analysis

- The results of this analysis clearly showed that the 9310 material was preferred over the 440C in terms of the inner race fracture failure mode.
- Manufacturing stresses effect for the 440C material was very significant.
- Material selection has a major impact on reliability.
- Probabilistic engineering analysis is critical to perform sensitivity analysis and trade studies for material selection and testing.
RELIABILITY PREDICTION
BASED ON OPERATIONAL DATA

Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com
During the inspection of the High Pressure Fuel Turbo-pump (HPFTP) Turbine blades of the Space Shuttle Main Engine (SSME) cracks were found in the blade firtree area. As a result, a study was formulated to determine the Space Shuttle flight risk due to a HPFTP first stage turbine blade failure.
**Background**

- A crack was found in a first stage turbine blade in HPFTP development unit 2423 during dye penetrant inspection 1/19/96.
- The subject blade had accumulated 20 starts and 9,826 seconds of operation.
- A total of 34 blade sets of the current configuration have been dye penetrant inspected, with no other crack being found.
- Metallurgical evaluation of the blade showed:
  - Fracture is hydrogen-assisted cracking.
  - Fracture origin approximately in middle of bottom firtree lobe – starting on pressure side.
  - No clear evidence of crack progression.
Assumptions

- A crack in a blade is a failure.
- Only last dye penetrant inspection times are used (34 sets).
- One failure (crack) at 20 starts and 9,826 seconds.

Assumptions and Database

<table>
<thead>
<tr>
<th>Starts</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>22,241</td>
</tr>
<tr>
<td>21</td>
<td>10,394</td>
</tr>
<tr>
<td>28</td>
<td>11,314</td>
</tr>
<tr>
<td>17</td>
<td>13,997</td>
</tr>
<tr>
<td>38</td>
<td>13,269</td>
</tr>
<tr>
<td>32</td>
<td>13,028</td>
</tr>
<tr>
<td>20</td>
<td>9,826</td>
</tr>
<tr>
<td>25</td>
<td>12,362</td>
</tr>
<tr>
<td>21</td>
<td>10,219</td>
</tr>
<tr>
<td>30</td>
<td>10,139</td>
</tr>
<tr>
<td>22</td>
<td>9,822</td>
</tr>
<tr>
<td>19</td>
<td>9,314</td>
</tr>
<tr>
<td>17</td>
<td>9,011</td>
</tr>
<tr>
<td>28</td>
<td>8,577</td>
</tr>
<tr>
<td>21</td>
<td>8,285</td>
</tr>
<tr>
<td>19</td>
<td>8,250</td>
</tr>
<tr>
<td>36</td>
<td>7,839</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Starts</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>7,604</td>
</tr>
<tr>
<td>27</td>
<td>7,344</td>
</tr>
<tr>
<td>5</td>
<td>2,337</td>
</tr>
<tr>
<td>15</td>
<td>7,302</td>
</tr>
<tr>
<td>8</td>
<td>3,759</td>
</tr>
<tr>
<td>10</td>
<td>6,308</td>
</tr>
<tr>
<td>11</td>
<td>4,792</td>
</tr>
<tr>
<td>8</td>
<td>4,178</td>
</tr>
<tr>
<td>11</td>
<td>4,076</td>
</tr>
<tr>
<td>5</td>
<td>2,402</td>
</tr>
<tr>
<td>5</td>
<td>2,337</td>
</tr>
<tr>
<td>4</td>
<td>2,110</td>
</tr>
<tr>
<td>5</td>
<td>1,871</td>
</tr>
<tr>
<td>4</td>
<td>1,851</td>
</tr>
<tr>
<td>5</td>
<td>1,612</td>
</tr>
<tr>
<td>4</td>
<td>1,598</td>
</tr>
<tr>
<td>2</td>
<td>600</td>
</tr>
</tbody>
</table>
The starts and run time for the three pumps:
2 STARTS / 817 SEC
2 STARTS / 780 SEC
4 STARTS / 1856 SEC
Weibull model was used for reliability predictions.

Analysis Results

<table>
<thead>
<tr>
<th>STS-75</th>
<th>HPFTP</th>
<th>Based on Starts</th>
<th>Based on Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine</td>
<td>Unit</td>
<td>Reliability</td>
<td>Risk</td>
</tr>
<tr>
<td>ME-1</td>
<td>4112R1</td>
<td>0.999486</td>
<td>1 / 1,944</td>
</tr>
<tr>
<td>ME-2</td>
<td>2128</td>
<td>0.999882</td>
<td>1 / 8,475</td>
</tr>
<tr>
<td>ME-3</td>
<td>4016R1</td>
<td>0.999221</td>
<td>1 / 1,283</td>
</tr>
<tr>
<td>3 Engine Cluster</td>
<td>0.998589</td>
<td>1 / 708</td>
<td>0.998896</td>
</tr>
</tbody>
</table>

Concluding Remarks

- Manufacturing records review for the flight set showed no discrepancies.
- Fleet leader blade set with 22,241 seconds and 46 tests.
- 53 blade sets were tested greater than the flight units.
- Flight reliability was assessed and risk was accepted by Shuttle program.
Main Advantages

- Allows the analyst to quantitatively and statistically analyze the relative reliability during the design or operational phase.
- Can aid in determining the resource allocation during the test and evaluation phase.
- Provides a means to quantify the uncertainty of design variables and their impact on reliability and risk.
- Identifies regions of high risk in a design.
- Provides a means to compare competing designs.
- Can reduce unnecessary conservatism.
- Estimates of the failure rates of components generated by reliability predictions are critical input to safety, maintainability, supportability, and cost.
- Reliability predictions are also the main source of data for Probabilistic Risk Assessments (PRAs).
Main Limitations

- Reliability prediction can be resource intensive.
- The analyst must have knowledge of engineering disciplines and experience in probability and statistics.
- For reliability predictions using historical population, data used must be very close to the as-planned design population to be viable. Extrapolation between populations can render the technique nonviable.
- For physics-based reliability predictions, it may be difficult to get an accurate and detailed description of failure modes, failure mechanisms, and acting loads and environments (i.e., determining the density functions of the random variables in the load and capability transfer functions).
Reliability

It takes about 13 tests with zero failures to get the reliability comfort level of 0.95 at 50% confidence.

Number of Tests
Reliability Demonstration Definition

- Reliability Demonstration is the process of quantitatively estimating the reliability of a system using objective data at the level intended for demonstration.
- It is used to provide empirical evidence of design reliability.
- It is the process of demonstrating the reliability of a design through testing and operation.
- It applies from test and evaluation through operation.
- Models and techniques used in reliability demonstration include Binomial, Exponential, Weibull models, etc.
There are a variety of probability distribution functions used for calculating reliability demonstration.

They cover both discrete and continuous data cases.

The most commonly used distributions are: The Exponential distribution for continuous data and the Binomial distribution for discrete data.

In the following charts we will cover the Binomial distribution for discrete data. The Exponential distribution for continuous data is included in the backup section.

http://reliabilityanalyticstoolkit.appspot.com/
Two-sided confidence, exact method

- For a sample size of \((N)\), a number of defects/failures of \((N_d)\), and a confidence level of \((1 - \alpha)\times 100\):
  
  - The equation to calculate the Binomial lower limit of the two-sided confidence interval, \(p_L\)
    
    \[
    \sum_{k=0}^{N_d-1} \binom{N}{k} p_L^k (1 - p_L)^{(N-k)} = 1 - \frac{\alpha}{2}
    \]

  - The equation to calculate binomial upper limit of the two-sided confidence interval, \(p_U\)
    
    \[
    \sum_{k=0}^{N_d} \binom{N}{k} p_U^k (1 - p_U)^{(N-k)} = \frac{\alpha}{2}
    \]

The following equations are solved iteratively to determine the two-sided upper confidence limit \((p_U)\) or two-sided lower confidence limit \((p_L)\):

https://reliabilityanalyticstoolkit.appspot.com/binomial_confidence_details
One-sided confidence, exact method

The calculation method for single sided limits are nearly identical to the two-sided case, except all the $\alpha$ is in either the upper or lower tail of the distribution.

- The equation to calculate binominal lower single-sided confidence limit:

\[
\sum_{k=0}^{N_d-1} \binom{N}{k} p_L^k (1 - p_L)^{(N-k)} = 1 - \alpha
\]

- The equation to calculate binominal upper single-sided confidence limit:

\[
\sum_{k=0}^{N_d} \binom{N}{k} p_U^k (1 - p_U)^{(N-k)} = \alpha
\]

Note 1: For the zero failure case, the Binomial upper limit on the probability of failure is: $P_U = 1 - \alpha^{1/n}$, and the reliability Lower confidence Limit:

$R_L = 1 - P_U = \alpha^{1/n}$  Where $\alpha = 1 - \text{Confidence Level}$

https://reliabilityanalyticstoolkit.appspot.com/binomial_confidence_details
Demonstrated Reliability* at 50% confidence
Using the Binomial Model With Zero Failure Case

<table>
<thead>
<tr>
<th>Number of tests</th>
<th>Reliability*</th>
<th>1-Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.500 (50.0%)</td>
<td>0.500</td>
</tr>
<tr>
<td>2</td>
<td>0.707 (70.7%)**</td>
<td>0.293</td>
</tr>
<tr>
<td>3</td>
<td>0.794 (79.4%)</td>
<td>0.206</td>
</tr>
<tr>
<td>4</td>
<td>0.841 (84.1%)</td>
<td>0.159</td>
</tr>
<tr>
<td>5</td>
<td>0.871 (87.1%)</td>
<td>0.129</td>
</tr>
<tr>
<td>6</td>
<td>0.891 (89.1%)</td>
<td>0.109</td>
</tr>
<tr>
<td>7</td>
<td>0.906 (90.6%)</td>
<td>0.094</td>
</tr>
<tr>
<td>8</td>
<td>0.917 (91.7%)</td>
<td>0.083</td>
</tr>
<tr>
<td>9</td>
<td>0.926 (92.6%)</td>
<td>0.074</td>
</tr>
<tr>
<td>10</td>
<td>0.933 (93.3%)</td>
<td>0.067</td>
</tr>
<tr>
<td>11</td>
<td>0.939 (93.9%)</td>
<td>0.061</td>
</tr>
<tr>
<td>12</td>
<td>0.944 (94.4%)</td>
<td>0.056</td>
</tr>
<tr>
<td>13</td>
<td>0.948 (94.8%)</td>
<td>0.052</td>
</tr>
</tbody>
</table>

*Reliability as a metric is the probability that an item will perform its intended function for a specified mission profile.

**A reliability, R, at 50% confidence level of 0.707, for example, means, 50% of the time the probability of success will be as good as or exceeds 0.707. Mathematically: \( P(R \geq 0.707) = 0.5 \)

It takes about 13 tests with zero failures to get the reliability comfort level of 0.95 at 50% confidence.
Reliability Demonstration

- Advantages
  - Provides empirical information on reliability.
  - Reduces the uncertainty of analytically based reliability estimates.
  - Supports the determining of the resource allocation during the test and evaluation phase.
  - Used to support the reliability prediction of a design through testing and operation.
Reliability Demonstration

- Limitations
  - Dedicated pre-operational demonstration testing cannot be performed for high levels of design indenture (e.g., launch vehicle) due to cost and schedule constraints.
  - Reliability testing at lower-levels of design indenture is highly limited due to the same constraints (i.e., cost and schedule).
  - Data from piggyback demonstration through other engineering testing can lack the resolution desired for good reliability modeling.
BACKUP

RELIABILITY ALLOCATION
THE AGREE METHOD
The AGREE Apportionment Method

- The AGREE apportionment method determines a minimum acceptable mean life for each subsystem in order to fulfill a minimum acceptable system mean life.
- The AGREE method assumes that all subsystems are in series and have an exponential failure distribution. This method takes into account both the complexity and the importance of each subsystem.
The mathematical model:

Let:

\( i \) = a counter representing each module, \( i = 1, 2, 3 \ldots, n \)

\( t \) = system operating time

\( R(t) \) = system reliability requirement at time \( t \)

For \( n \) total modules in the system, the contribution of each module containing \( m \) components to the overall system reliability is:

\[
R(t_i) = \left[R^*(t)\right]^{\frac{m_i}{n}}
\]

Where,

\[
n = \sum_{i=1}^{m} m_i = \text{total number of components in the system}
\]

\( m_i \) is the number of components in module \( i \).

\( t_i \) = operating time of module \( i \)
# The AGREE Apportionment Method
## Example 1

### Allocating the System Reliability

<table>
<thead>
<tr>
<th>Module (i)</th>
<th>Number of components (mi)</th>
<th>$\left[R^*(t)\right] \frac{m_i}{n}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td>0.98</td>
</tr>
<tr>
<td>2</td>
<td>40</td>
<td>0.96</td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td>0.98</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>0.98</td>
</tr>
<tr>
<td>n = 100</td>
<td></td>
<td>Rsystem = 0.90</td>
</tr>
</tbody>
</table>
Determining the module failure rate

Each module’s unreliability is: \(1 - [R(t)]^{\frac{m_i}{n}}\)

If an exponential failure is assumed, then the unreliability of a module is also given by: \(1 - e^{-\lambda_i t_i}\)

The probability that the module is critical and fails is:

\[w_i(1 - e^{-\lambda_i t_i})\]

Where,

\(\lambda_i = \) failure rate of module \(i\)

\(w_i = \) probability that the system fails given that module \(i\) is critical and fails

Equating the above two quantities and solving for \(\lambda_i:\)

\[w_i(1 - e^{-\lambda_i t_i}) = 1 - [R(t)]^{\frac{m_i}{n}}\]

\(\lambda_i^* = -\frac{1}{t_i} \ln\left[1 - \frac{1 - [R^*(t)]^{\frac{m_i}{n}}}{w_i}\right]\)

	\(*R(t) is the required system reliability*

A system has four subsystems, each with 20 modules. The required system reliability is 0.9 for a four hour mission. Assume all subsystems are critical (i.e. the probability that the system fails when a subsystem fails is 1.0). What should the allocated module reliability and failure rate be if:

► All subsystem are equally important?
► Module 3 becomes twice as complex as the other modules?
► Module 3 is only 10% as important as the other modules?
**Answer 1:** For the stated inputs, each subsystem must have an MTBF of 152 hours. The reliability of each subsystem must be 0.974, which when multiplied together results in an overall system reliability of 0.90.

**Question 2**

**Answer 2:** If module 3 has 40 components instead of 20, this module now has an allocated MTBF of 95 hours and the remaining three modules must have an MTBF of 190 hours to achieve the overall system reliability goal of 0.9 for a 4 hour mission.

**Reliability Allocation AGREE Example**

**Question 3**

**Answer – 3:** If the quantity of components is put back to 20, but module 3 now has an importance of only 0.1, meaning that 90% of the failures will not cause the system to fail, the allocated MTBF for this module is only 13 hours instead of 152 hours. Note, the product of the module reliability values, 0.684, does not equal the requirement of 0.9 because not all failures of module 3 will cause a system failure.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Required System Reliability, $R^*(t)$</td>
<td>0.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Mission Time (ti, Hours)</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>AGREE Allocation Input Data</td>
<td>Output Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Module $(i)$</td>
<td>Number of components $(m_i)$</td>
<td>Importance Factor (w_i) probability that the system fails given that subsystem i is critical and fails</td>
<td>Allocated module failure rate, failures/hours</td>
<td>Allocated module MTBF, hours</td>
<td>Allocated module reliability</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>20</td>
<td>1</td>
<td>0.00659</td>
<td>152</td>
<td>0.974</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>20</td>
<td>1</td>
<td>0.00659</td>
<td>152</td>
<td>0.974</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>20</td>
<td>0.1</td>
<td>0.07526</td>
<td>13</td>
<td>0.740</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>20</td>
<td>1</td>
<td>0.00659</td>
<td>152</td>
<td>0.974</td>
</tr>
<tr>
<td>12</td>
<td>$n = 80$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: [http://www.reliabilityanalytics.com/blog/2011/10/09/reliability-allocation/]
For estimating confidence intervals for the MTBF, two cases have to be considered:

- **Failure terminated case:** A test that is run until a pre-assigned number of failures have occurred.
- **Time terminated case:** A test that is stopped after a pre-assigned number of test hours have accumulated.

The formula for the confidence interval employs the $\chi^2$ (chi-square) distribution.

For tests with no failures occurring, only the one-sided lower confidence limit can be calculated.
Continuous Data Case
Exponential Example - Confidence Intervals

- **One-sided Confidence interval**
  - Lower limit, Failure Terminated.
    \[
    \left( \frac{2T}{\chi^2 (\alpha, 2r)}, \infty \right)
    \]
  - Lower limit, Time Terminated.
    \[
    \left( \frac{2T}{\chi^2 (\alpha, 2r + 2)}, \infty \right)
    \]

- **Two-sided Confidence interval**
  - Lower and Upper Limits, Failure Terminated
    \[
    \left( \frac{2T}{\chi^2 \left( \frac{\alpha}{2}, 2r \right)}, \frac{2T}{\chi^2 \left( 1 - \frac{\alpha}{2}, 2r \right)} \right)
    \]
  - Lower and Upper Limits, Time Terminated
    \[
    \left( \frac{2T}{\chi^2 \left( \frac{\alpha}{2}, 2r + 2 \right)}, \frac{2T}{\chi^2 \left( 1 - \frac{\alpha}{2}, 2r + 2 \right)} \right)
    \]

Where:
- \( T \) = total accumulated unit-hours
- \( r \) = total number of failures
- \((1 - \alpha)\times100 = \text{confidence level (\%)}\)

Transport vehicle example: One failure in 100 hours of operation

<table>
<thead>
<tr>
<th>Confidence bounds – Time Terminated</th>
<th>MTBF at 50%</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-sided lower 50% limit</td>
<td>60</td>
</tr>
<tr>
<td>Two-sided 50% limits</td>
<td>37 – 348</td>
</tr>
</tbody>
</table>

For the operating time = \( t \), the Reliability is:

\[
R(t) = e^{-\frac{t}{MTBF}}
\]

For the \( t = MTBF \), the Reliability is:

\[
R(MTBF) = e^{-\frac{MTBF}{MTBF}} = e^{-1} = 0.368 = 36.8\%
\]
Reliability Engineering Overview

Bibliography

- Designing for Reliability and Safety Control, Ernest J. Henley and Hiromitsu Kumamoto, Prentice Hall; 1985
- Introduction to System Safety Engineering, W. P. Rogers, John Wiley and Sons, 1980
- Reliability in Engineering design, Kailash Kapur, Published by John Wiley & Sons, 1977
- Reliability Engineering and Risk Assessment, Ernest J. Henley and Hiromitsu Kumamoto, Prentice Hall; 1991

- Reliability in Engineering design, Kailash Kapur, Published by John Wiley & Sons,, 1977


- Systems Engineering “Toolbox” for Design-Oriented Engineers, NASA Reference Publications 1358


NASA/SP-2009-569, “Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis”

Reliability in Engineering design, Kailash Kapur, Published by John Wiley & Sons,, 1977


Systems Engineering “Toolbox” for Design-Oriented Engineers, NASA Reference Publications 1358


http://reliabilityanalyticstoolkit.appspot.com/
Reliability Demonstration Bibliography

- Reliability in Engineering design, Kailash Kapur, Published by John Wiley & Sons, 1977
- Systems Engineering “Toolbox” for Design-Oriented Engineers, NASA Reference Publications 1358
- http://reliabilityanalyticstoolkit.appspot.com/ (All Distributions)
- http://reliabilityanalyticstoolkit.appspot.com/binomial_confidence (Binomial)
- http://reliabilityanalyticstoolkit.appspot.com/confidence_limits_exponential_distribution (Exponential)