Module Purpose: Reliability

♦ To understand the importance of reliability as an engineering discipline within systems engineering, particularly in the aerospace industry.

♦ To understand key reliability concepts, such as constant failure rate, mean-time-between failure, and “bathtub” curve.

♦ To introduce different forms of system redundancy, including fault tolerance, functional redundancy, and fault avoidance.

♦ Review ways to calculate reliability and the use of block diagrams.
“It appears incontrovertible that understanding failure plays a key role in error-free design of all kinds, and that indeed all successful design is the proper and complete anticipation of what can go wrong.”

Henry Petroski
Design Paradigms
Case Histories of Error and Judgment in Engineering
Risk Philosophy – A Key Design Driver

• Some expressions you will hear in the aerospace community:
  • Reliability of 0.9997
  • No single point failure mode design
  • Single thread design
  • Must not fail
  • Graceful degradation is OK
  • Fully redundant system
  • Critical function redundancy only
  • Faster, better, cheaper

• What do they mean?
Reliability Definitions

♦ **Reliability** is the probability that the system-of-interest will not fail for a given period of time under specified operating conditions.
  - Reliability is an inherent system design characteristic.
  - Reliability plays a key role in determining the system’s cost-effectiveness.

♦ **Reliability** engineering is a specialty discipline within the systems engineering process. Reflected in key activities:
  - *Design* - including design features that ensure the system can perform in the predicted physical environment throughout the mission.
  - *Trade studies* - reliability as a figure of merit. Often traded with cost.
  - *Modeling* - reliability prediction models, reflecting environmental considerations and applicable experience from previous projects.
  - *Test* - making independent predictions of system reliability for test planning/program; sets environmental test requirements and specifications for hardware qualification.
- **Constant Failure Rate:**
  - Probability Distribution of reliability is an exponential function.
  - Although an individual component may not have an exp reliability distribution, in a complex system with many components the overall reliability may appear as a series of random events and the system will follow an exponential reliability distribution.
The “Bathtub” Failure Rate Curve

Because of burn-in failures and/or inadequate quality assurance practices, the failure rate is initially high, but gradually decreases during the infant period. During the useful life period, the failure rate remains constant, reflecting randomly occurring failures. Later, the failure rate begins to increase because of wear-out failures.
Redundancy

Fault Tolerance
♦ Fault tolerance is a system design characteristic associated with the ability of a system to continue operating after a component failure has occurred.
♦ It is implemented by having design redundancy and a fault detection response capability.
♦ Design redundancy can take several forms: parallel, stand-by, and cross-strapped (see upcoming block diagram slide).

Functional Redundancy
♦ Functional redundancy is a system design and operations characteristic that allows the system to respond to component failures in a way sufficient to meet mission requirements.
♦ This usually involves operational work-arounds and the use of components in ways that were not originally intended.
  • Galileo high-gain antenna example
  • Apollo 13 example
Ways to Achieve Reliability in Space System

Also known as “Fault Avoidance”

♦ Provide ample environmental and design margins, or use appropriate de-rating guidelines.

♦ Use high-quality, carefully selected, screened parts where needed.

  • Reliability for Class S (space qualified) parts are typically 10 times that of good commercial parts. Class S parts tend to be expensive and with long delivery times.
  • Warning on Commercial-Off-The-Shelf (COTS) parts.

♦ Use rigorously controlled assembly procedures conducted in very clean environments.

♦ Conduct formal inspections of manufacturing facilities, processes and documentation.

  • Why is documentation of all steps in the process important?

♦ Perform acceptance testing or inspections on all parts when possible.
Reliability Calculations Section
Block Diagrams

Two units in series
\[ R = R_a \times R_b \]

You may combine series and parallel operations into arbitrarily complex block diagrams.
Suppose historical data demonstrates the number of failures per 100 launches of a particular launch vehicle.

What is the probability of launching 20 times without failure?

Recall from before that \( R(t) = \exp(-\lambda t) \)

- 1 failure / 100 launches: \( P_{\text{success}} = \exp(-20 \times (1/100)) = 0.819 \)
- 5 failure / 100 launches: \( P_{\text{success}} = \exp(-20 \times (5/100)) = 0.368 \)
- 10 failure / 100 launches: \( P_{\text{success}} = \exp(-20 \times (10/100)) = 0.135 \)
**Example Reliability Problem**

- A human-rated space launch system has a reliability, or probability of success, of 0.98. An abort system for the crew module is provided and has a reliability of 0.95.
  - What is the overall probability of crew survival?

Let $A = \text{event of crew death}$
Let $B_1 = \text{event of launch vehicle success}$
Let $B_2 = \text{event of launch vehicle failure}$

$P(B_1) = 0.98 \quad P(A/ B_1) = 0$ (abort system not needed)
$P(B_2) = 0.02 \quad P(A/ B_2) = 0.05$ (abort system fails)

Then from the Law of Conditional Probabilities,
$P(A) = P(B_1)P(A/ B_1) + P(B_2)P(A/ B_2) = (0.98)(0) + (0.02)(0.05) = 0.001$

The reliability of crew survival is then
$R_s = 1 - P(A) = 0.999$

The crew has a 99.9% chance of survival, even though neither the launch vehicle nor the abort system is anywhere close to being 99.9% reliable.
Example Reliability Problem

A human-rated space launch system has a reliability, or probability of success, of 0.98. An abort system for the crew module is provided and has a reliability of 0.95.

- What is the overall probability of crew survival?

\[ R = R_a + R_b - R_a R_b \]

\[ R = 0.98 + 0.95 - 0.98 \times 0.95 = 0.999 \]

Same as before!
Example: Apollo LM Ascent Engine

Consider the Apollo Lunar Module ascent engine. This system included three valves in the oxidizer lines and three valves in the fuel lines. For the system to function properly, at least one of the valves in each set must work. The reliability of each valve is $R_v = 0.9$.

This system may be expressed using the following block diagram.

What is the probability of the entire system working?
Additional Pause and Learn Opportunity

The Event Tree methodology (introduced in the Risk Module) can also be used to calculate reliability. You can redo the example problems in this lecture for the launch system or the Apollo ascent engine using event trees, and show the students that you get the same result.

You can also show additional example problems using the file Example_Reliability_Problems.pdf.
Module Summary: Reliability

♦ Reliability is a key attribute of space systems, influencing systems engineering activities such as design, trade studies, modeling, and test.

♦ The reliability function, $R(t)$, is determined from the probability that a system will be successful for at least some specified time.

♦ The Bathtub curve expresses the failure rate as it depends on the age of the system. Early and late in life of the system (similar to the human body) significantly higher failure rates occur called “infant mortality” and “old age” regions. Between these regions normally lies an extended period of approximately constant failure rate. The reliability of systems operating in this region can be simply characterized by an exponential function.

♦ Ways to achieve reliability include fault tolerance, functional redundancy and fault avoidance.

♦ Block diagrams and event trees are useful tools in calculating reliability. An understanding of probability basics is required.
Backup Slides for Reliability Module

Fault Tree Analysis is included in the Risk Module, however, it could also be addressed in the Reliability Module. Here are some additional slides related to fault tree analysis.
Fault Tree Analysis

♦ An analytical technique, whereby
  • An undesired state of the system is specified
  • System is analyzed to find all credible ways that this state can occur
♦ Modeled in a top-down fashion using symbolic logic.
♦ Looks at failure domain only.
♦ Provides a qualitative model that can be evaluated quantitatively using probabilistic assessment.
♦ Used in system design to understand what elements might cause loss of mission (or loss of crew).
♦ Used in the analysis of nuclear reactor safety.
♦ Also used in accident investigations.
  • e.g., Mars Climate Orbiter and Mars Polar Lander, lost in 1999.
Fault tree analysis is a graphical representation of the combination of faults that will result in the occurrence of some (undesired) *top event*. In the construction of a fault tree, successive subordinate failure events are identified and logically linked to the top event. The linked events form a tree structure connected by symbols called *gates*.
Refer to NASA Reference Publication 1358: System Engineering “Toolbox” for Design-Oriented Engineers

Section 3.6: Fault Tree Analysis
(Handout)
Particular points:
And/Or Gates explanation
Example Fault Tree (Fig 3-20)
## Reliability Relationships

<table>
<thead>
<tr>
<th>Name</th>
<th>Symbol</th>
<th>Mathematical</th>
<th>Relationships</th>
<th>Failures as random</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard Rate Or Failure Rate</td>
<td>$\lambda(t)$</td>
<td>$= -(1/R) \frac{dR}{dt}$</td>
<td>$= \frac{f(t)}{(1 - F(t))}$</td>
<td>$= \lambda$</td>
</tr>
<tr>
<td>Reliability</td>
<td>$R(t)$</td>
<td>$= \int_{t}^{\infty} f(\lambda) d\lambda$</td>
<td>$= 1 - F(t)$</td>
<td>$= e^{-\lambda t} = e^{-t/MTBF}$</td>
</tr>
<tr>
<td>Cumulative Failure Probability</td>
<td>$F(t)$</td>
<td>$= \int_{0}^{t} f(\lambda) d\lambda$</td>
<td>$= 1 - R(t)$</td>
<td></td>
</tr>
<tr>
<td>Failure Probability Density</td>
<td>$f(t)$</td>
<td>$= - \frac{dR(t)}{dt}$</td>
<td>$= \lambda(t)R(t)$</td>
<td></td>
</tr>
</tbody>
</table>

For systems that must operate continuously, it is common to express their reliability in terms of the Mean Time Between Failure (MTBF), where $MTBF = 1/\lambda$. 