Fayssal M. Safie, Ph. D.,
A-P-T Research, Inc.

RAM X Workshop Tutorial
Huntsville, Alabama
November 8-9, 2017

RELIABILITY ENGINEERING

MISSION SUCCESS STARTS WITH RELIABILITY

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

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

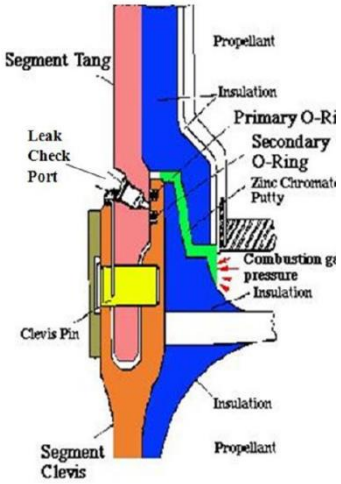
Introduction

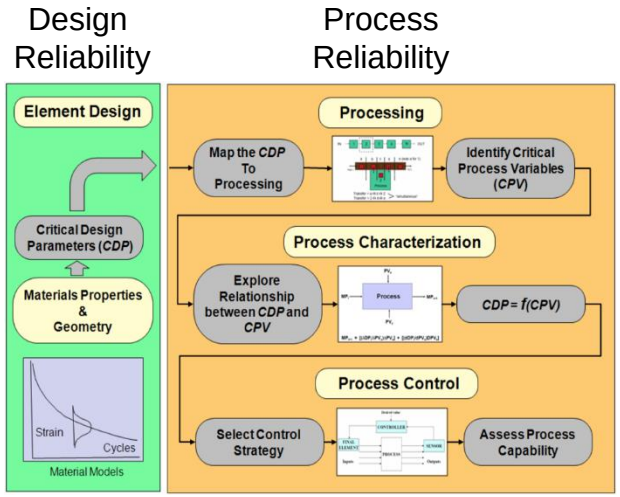
- This tutorial is a brief summary of a three-day reliability engineering course offered by A-P-T Research, Inc.
- The course is intended to provide a better understanding of reliability engineering as a discipline with focus on the reliability analysis tools and techniques and their application in technical 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 schedule and cost, visit www.apt-research.com/training or 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).

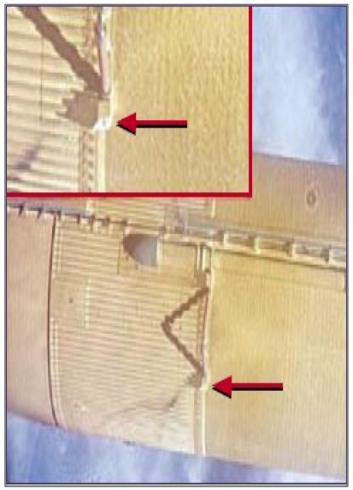
Table of Contents

- Introduction
- Probability Basics
- Reliability Engineering Overview
- Failure Modes and Effects Analysis (FMEA)
- Reliability Allocation
- Reliability Prediction
- Reliability Demonstration
- 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 three modules (shown in blue) out of 16 modules contained in the three-day course.







Reliability Engineering Overview

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

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

Topics

- Definitions
- Why Reliability Engineering
- The Reliability Engineering Case
- Design It Right And Build It Right
- Reliability Check List
- Reliability Metrics
- How Reliable is Reliable Enough
- The Bathtub Curve
- Reliability Relationship to Safety, Risk Assessment, Risk Management, Maintainability, Supportability, Affordability, and Life Cycle Cost
- Bibliography

Reliability Engineering Definition

- **Reliability as an engineering discipline** is the application of engineering principles to the design and processing of products, both hardware and software, for the purpose of meeting product reliability requirements or goals.
- **Reliability as a figure of merit** is the probability that an item will perform its intended function for a specified mission profile.
- For repairable item, reliability is defined as the probability that the component or system experiences no failures during a specified time interval given that the component or system was repaired to a like-new condition or was functioning at time zero.

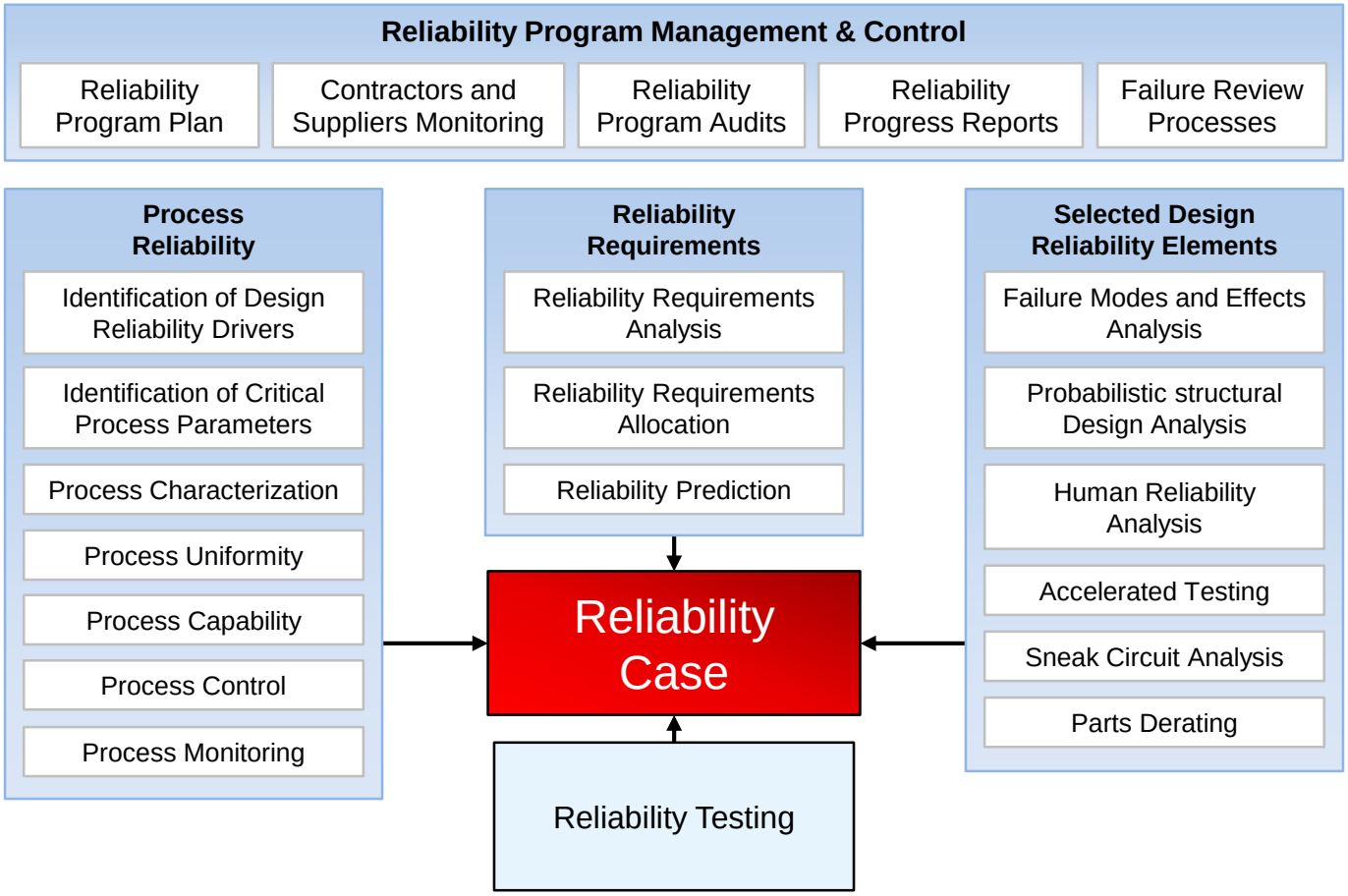
System Safety Definition

- **Safety:** The freedom from those conditions that can cause death, injury, occupational illness, or damage to the environment.
- **System Safety:** The application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.
- **Risk Assessment:** The process of determining the magnitude and consequences of risk.
- **Risk Management:** The systematic and iterative optimization of the project resources according to a risk management policy.

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.

Selected Elements of The Reliability Engineering Case



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 it Right and Build it Right

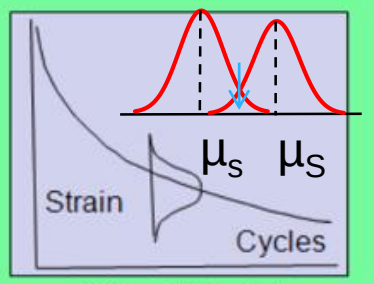
SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Design Reliability

Element Design

Critical Design Parameters (*CDP*)

Materials Properties & Geometry

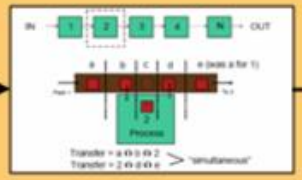


Material Models

Process Reliability

Processing

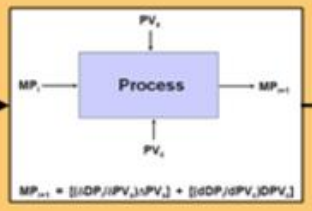
Map the *CDP* To Processing



Identify Critical Process Variables (*CPV*)

Process Characterization

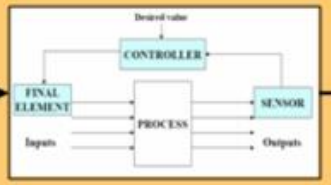
Explore Relationship between *CDP* and *CPV*



***CDP* = *f*(*CPV*)**

Process Control

Select Control Strategy

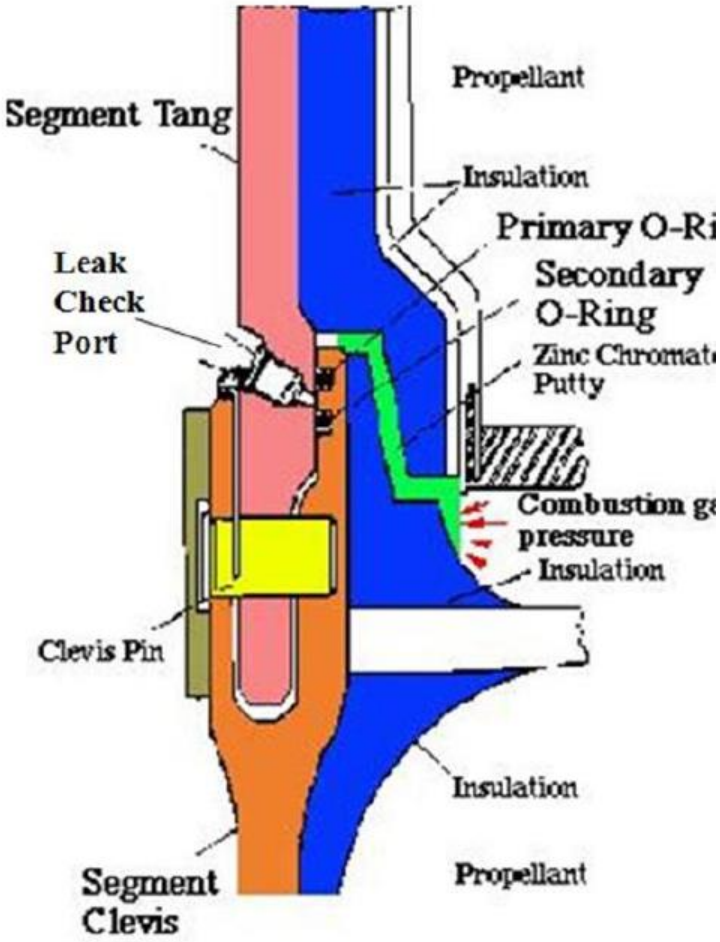


Assess Process Capability

Design Reliability
The Challenger Accident

Causes and Contributing Factors

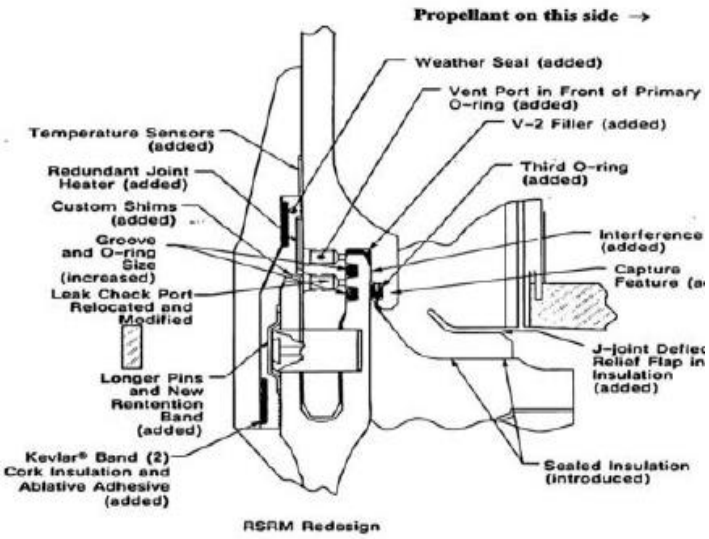
- The zinc chromate putty frequently failed and permitted the gas to erode the primary O-rings.
- The particular material used in the manufacture of the shuttle O-rings was the wrong material to use at low temperatures.
- Elastomers become brittle at low temperatures.



Design Reliability
The Challenger Accident

Redesigned Field Joint

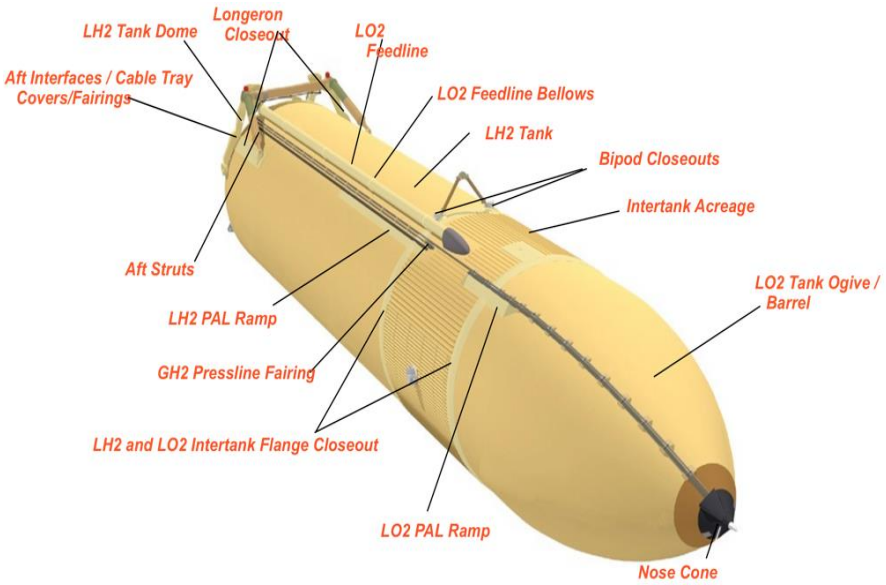
- The redesign of the joint/seal shown here added a third O-ring and eliminated the troublesome putty that served as a partial seal.
- Bonded insulation replaced the putty [Lewis, 1986].
- A capture device was added to prevent or reduce the opening of the joint as the booster inflated under motor gas pressure during ignition.
- The third O-ring would be added to seal the joint at the capture device.



- The former O-rings would be replaced by rings of the same size but made of a better performing material called fluorosilicone or nitrile rubber.
- Heating strips were added around the joints to ensure the O-rings did not experience temperatures lower than 75 degrees Fahrenheit regardless of the surrounding temperature.
- The gap openings that the O-rings were designed to seal were reduced to 6 thousandths of an inch from the former gap of 30 thousandths of an inch.

Process Reliability
The Columbia Accident

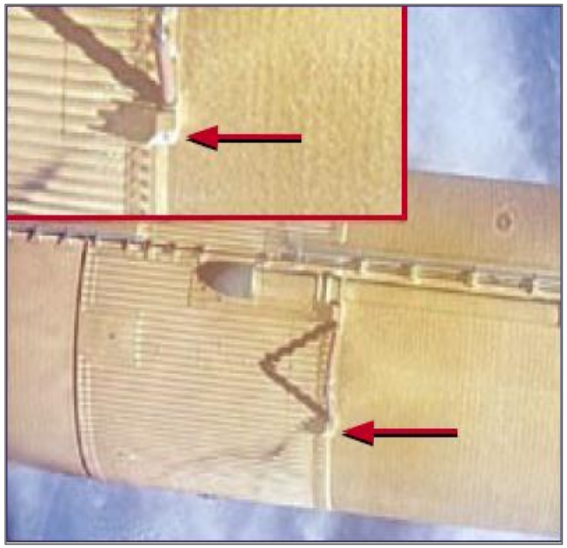
- The ET thermal protection system is a foam-type material applied to the external tank to maintain cryogenic propellant quality, minimize ice and frost formation, and protect the structure from ascent, plume, and re-entry heating.
- The TPS during re-entry is needed because after ET/Orbiter separation, premature structural overheating due to loss of TPS could result in a premature ET breakup with debris landing outside the predicted footprint.

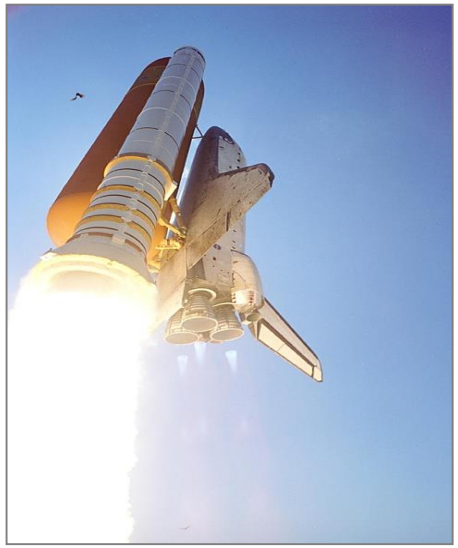


SAFETY ENGINEERING SEAC & ANALYSIS CENTER

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.
- Cryopumping and cryoingestion were experienced during tanking, launch, and ascent.
- Dissections of foam revealed subsurface flaws and defects as contributing to the loss of foam.





Enhanced Foam Process

- Conducted testing sufficient enough to understand and characterize the process variability and process capability
- Evaluated process capability for meeting the specification
- Evaluated process control for process uniformity
- Statistical evaluation of the data showed that significant improvements were made in process uniformity and process capability, including significant reduction in the coefficient of variation (COV) of the process critical output parameters (e.g., void frequency and void sizes)

Reliability Check List

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

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 time line?
  - 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?

Reliability Metrics

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. MTBF can be calculated as the inverse of the failure rate, λ, for constant failure rate systems.
  - MTTF is a basic measure of reliability for non-repairable systems. It is the mean time expected until the first failure. For constant failure rate systems, MTTF is the inverse of the failure rate, λ.
- ***Predicted Reliability Numbers***
  - Reliability prediction is the process of quantitatively estimating the reliability using both objective and subjective data.

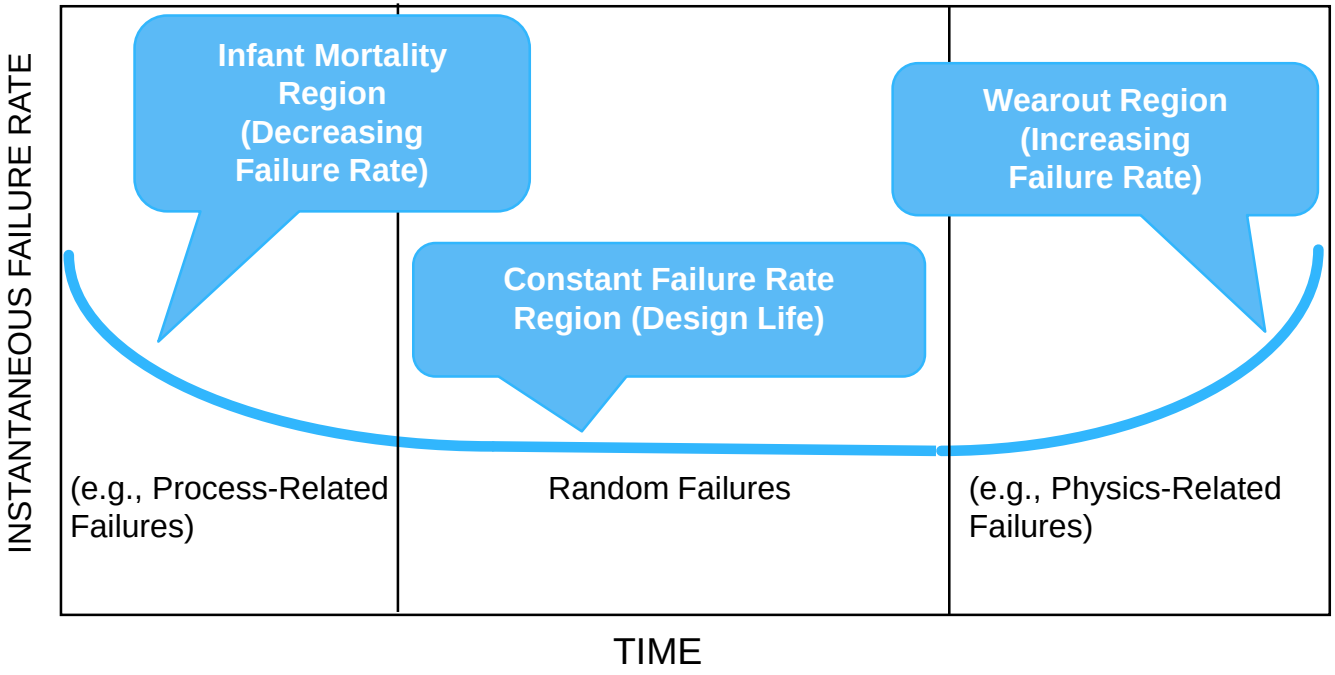
Reliability Metrics (Continued)

- ***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.

The Bathtub Curve - Hardware Reliability



Reliability Relationship to Safety

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

	Reliability	Safety
Roles	To ensure the product functions successfully.	To ensure the product and environment are safe and hazard free.
Requirements	Design function specific within the function boundary. Internally imposed.	Non-function specific such as “no fire,” “no harm to human beings.” Externally imposed.
Approaches	Bottom-up and start from the component or system designs at hand.	Top-down and trace the top-level hazards to basic events, then link to the designs.
Analysis Boundaries	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.	System view of hazards with multiple and interacting causes. External vulnerability and uncertainty may be required to be addressed.

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

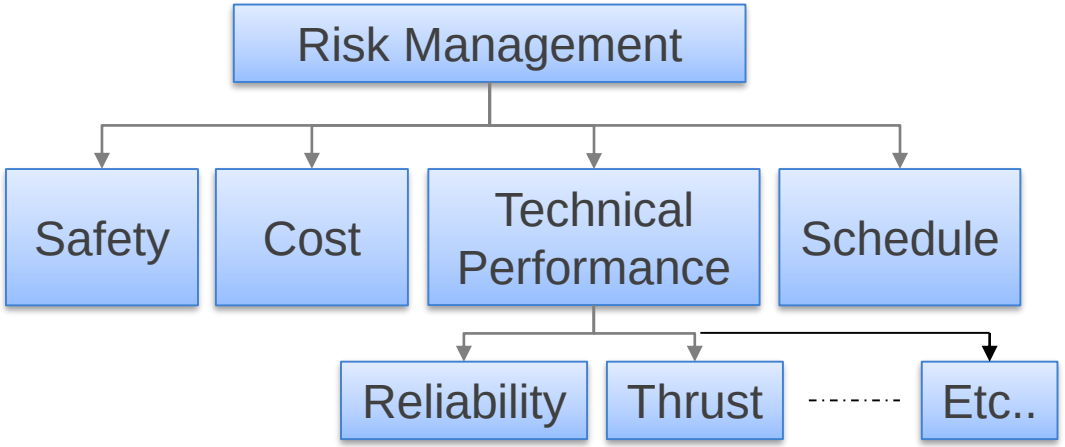
Reliability Relationship to Risk Assessment

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- Reliability engineering deals with failure analysis focusing on understanding failure mechanisms that could lead to loss of function.
- Risk assessment is a process that deals with system risk focusing on understanding the system risk scenarios that could lead to loss of mission or loss of life.
- Reliability prediction and reliability information are critical data sources to risk assessment.

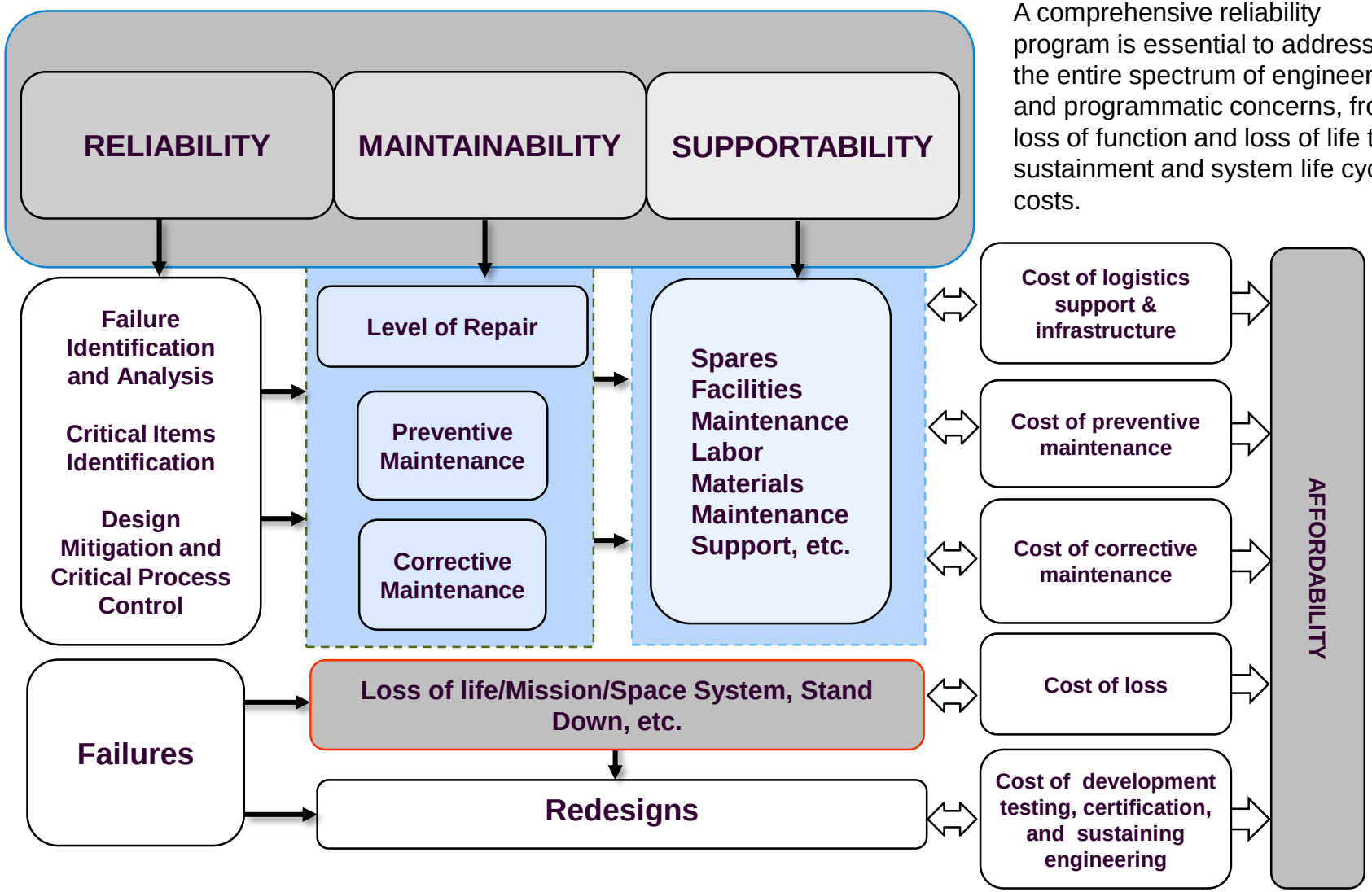
Reliability Relationship To Risk Management

- **Risk management** is the systematic and iterative optimization of the project resources according to a risk management policy.
- **Reliability** is a technical performance measure (TPM) and could be a major contributor to the overall program/project risk.

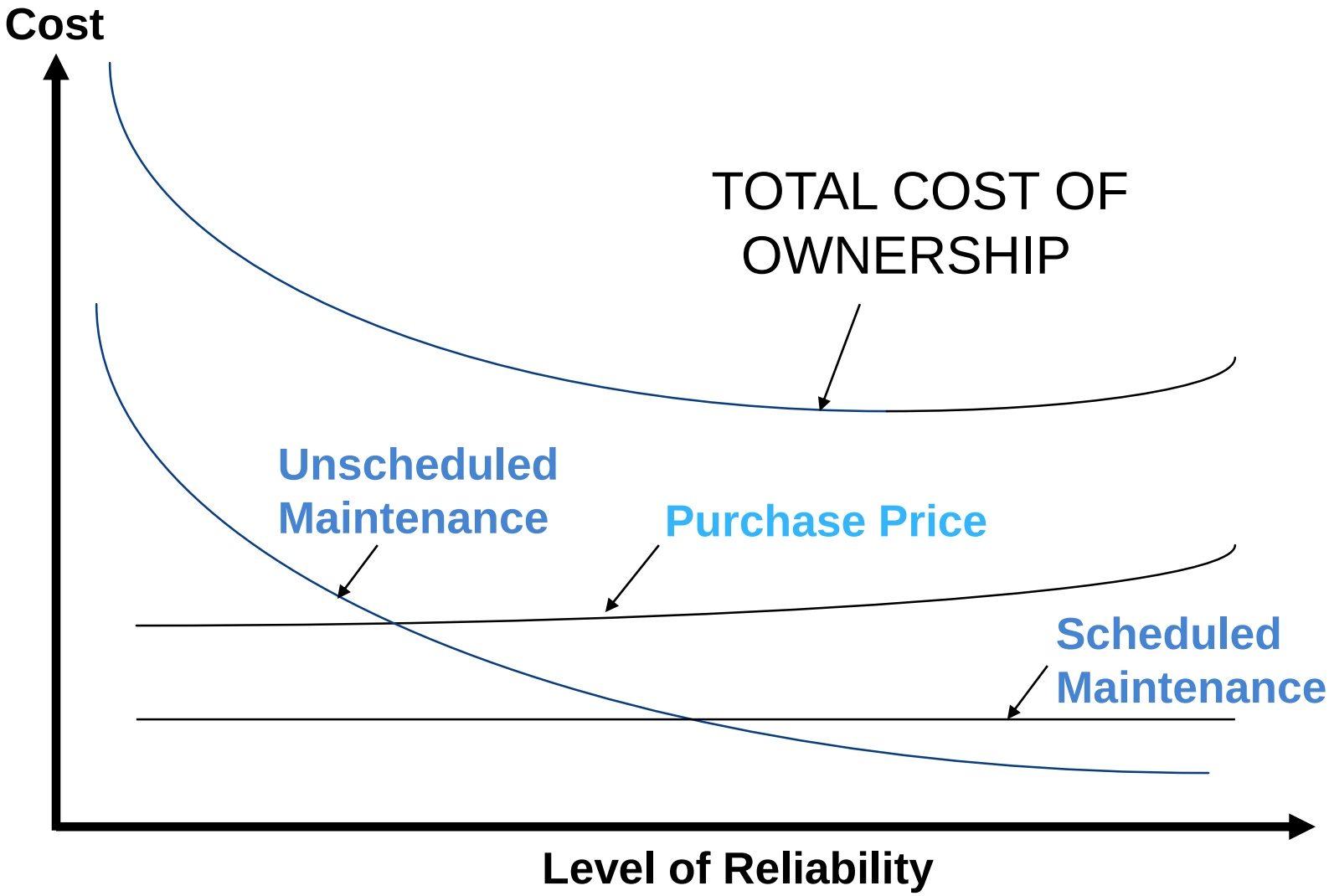


Reliability Relationship To Maintainability, Supportability, and Affordability

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.

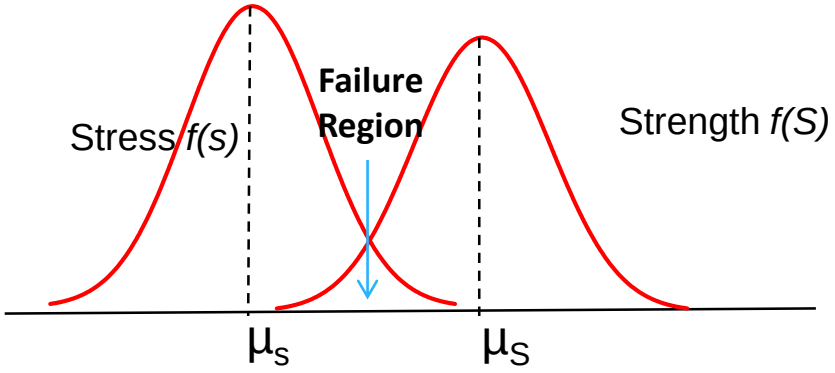


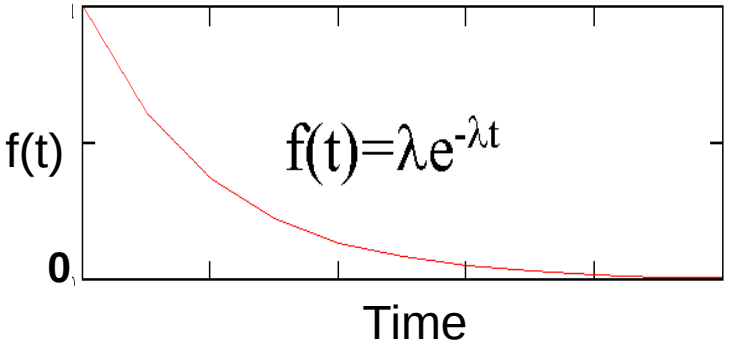
Reliability Relationship to Life Cycle Cost

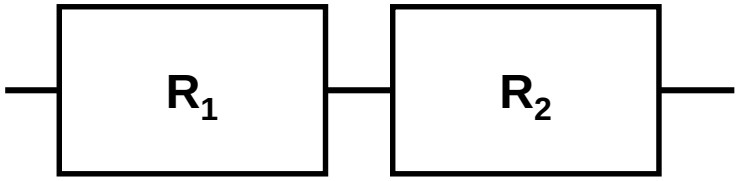


Reliability Engineering Overview Bibliography

- Challenger The Final Voyage, Lewis, S. R., New York: Columbia University Press, 1988
- Designing for Reliability and Safety Control, Ernest J. Henley and Hiromitsu Kumamoto, Prentice Hall; 1985
- Engineering Reliability — New Techniques and Applications, B. S. Dhillon and C. Singh, John Wiley & Sons; 1981
- Handbook of System and Product Safety, Willie Hammer, 1972, Prentice-Hall; 1972
- Introduction to System Safety Engineering, W. P. Rogers, John Wiley and Sons,1980
- NASA Systems Engineering Handbook, NASA/SP-2007-6105
- 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 Engineering Handbook: Vol 1 and 2 Hardcover, Dimitri B. Kececioglu, Prentice Hall, 2002







Reliability Prediction

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

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

Topics

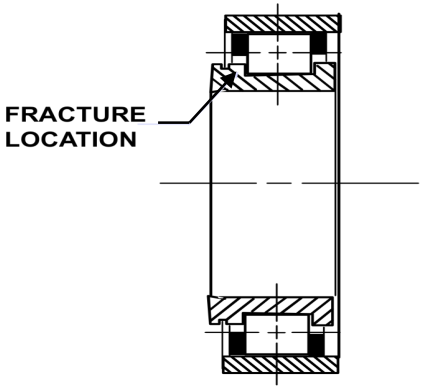
- Definitions
- Why Reliability Predictions
- Physics-Based Reliability Predictions
- Reliability Prediction Using Reliability Block Diagrams (Covered in the full course)
- Reliability Prediction Based on Operational Data (Covered in the Full course)
- Advantages and Limitations
- Bibliography

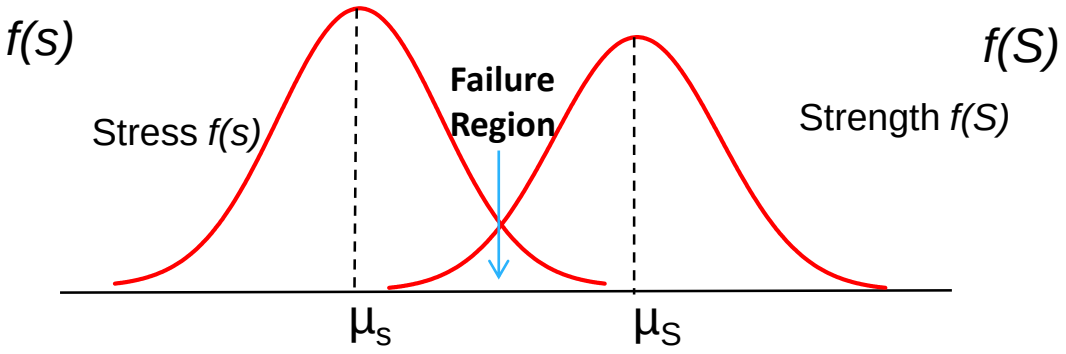
Reliability Prediction - Definition

- 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.

Why Reliability Prediction

- Reliability predictions are essential to evaluate design feasibility, compare design alternatives, identify potential failure areas, trade-off system design factors, and track reliability improvement.
- 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).





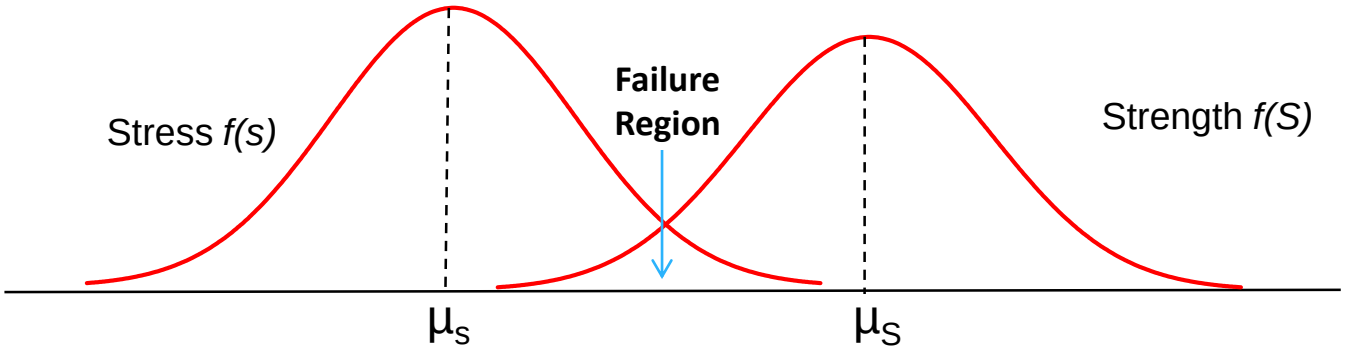
Physics-Based Reliability Prediction

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

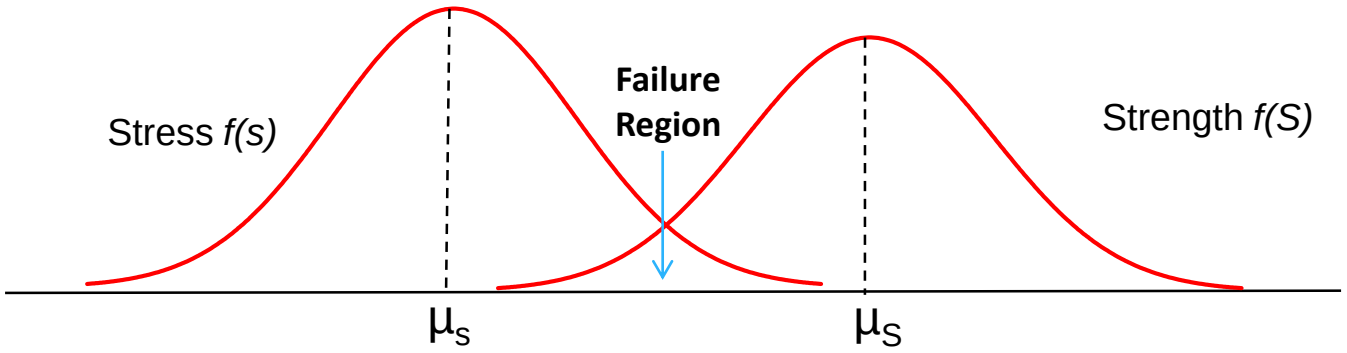
Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

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.



Physics Based Reliability Prediction
The Normal Case



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

μ_s = mean value of the stress

σ_s = standard deviation of the stress

μ_s = mean value of the strength

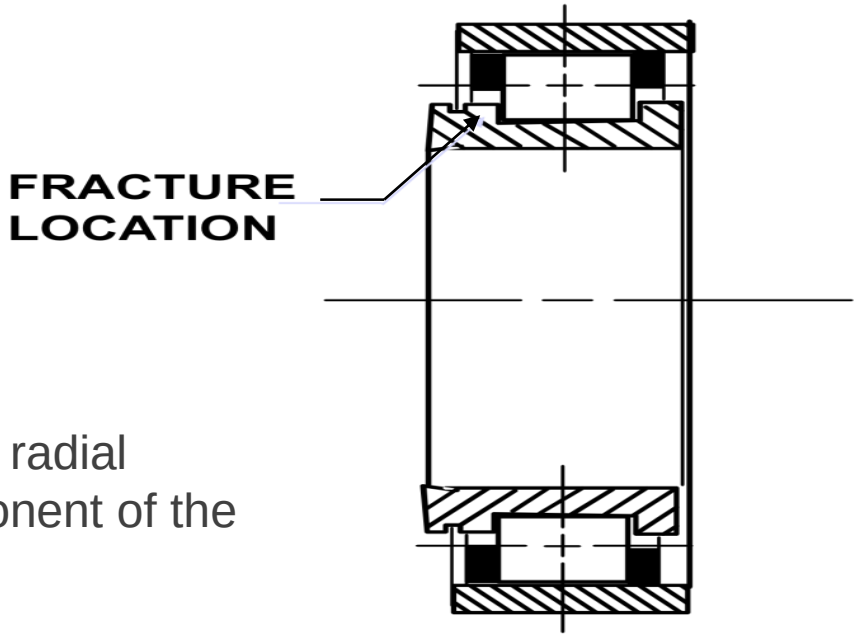
σ_S = standard deviation of the strength

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.

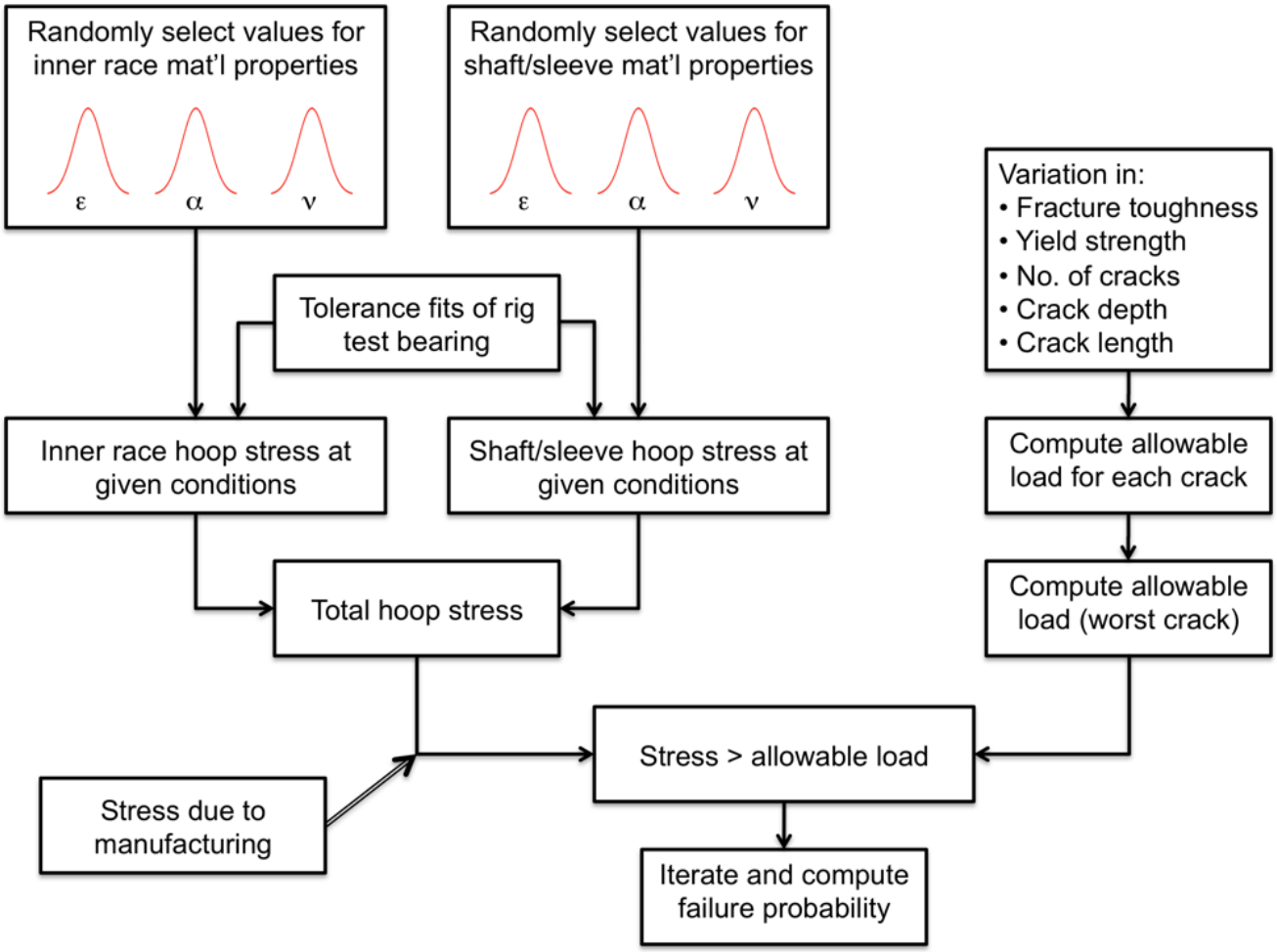
Physics-Based Reliability Prediction
A Rocket Engine Roller Bearing Example

- 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 Analytical Approach - The Simulation Model



SAFETY ENGINEERING SEAC & ANALYSIS CENTER

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

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

* 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 Advantages

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.

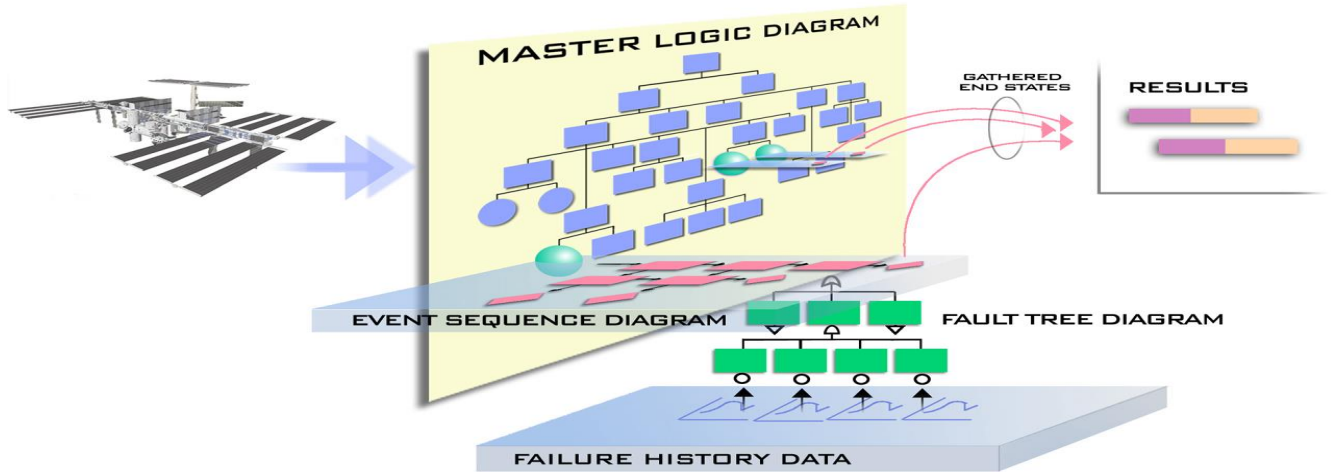
Reliability Prediction Limitations

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 Predictions Bibliography

- Modarres, M., Kaminskiy, M., & Krivtsov, V. (2010). *Reliability Engineering and Risk Analysis*, 2nd Ed. Boca Raton: CRC Press.
- 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
- ReliaSoft Corporation, *Lambda Predict Users Guide*, Tucson, AZ: ReliaSoft Publishing, 2007.
- Systems Engineering “Toolbox” for Design-Oriented Engineers, NASA Reference Publications 1358
- Safie, F . and Fox, E. P. , AIAA/SAE/ASME 27th Joint Propulsion Conference, June 1991. "A Probabilistic Design Analysis Approach For Launch Systems”
- http://reliabilityanalyticstoolkit.appspot.com/



Probabilistic Risk Assessment (PRA)

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

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

Topics

- Probabilistic Risk Assessment (PRA) - Definition
- Why PRA
- PRA Process
- PRA Elements
- Examples
- PRA Advantages and Limitations
- Bibliography

Probabilistic Risk Assessment (PRA) Definition

- PRA is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes. It attempts to quantify rare event probabilities of failures. It is inherently and philosophically a Bayesian methodology. In general, PRA is a process that seeks answers to three basic questions:
  - What can go wrong that would lead to loss or degraded performance (i.e., scenarios involving undesired consequences of interest)?
  - How likely is it (probabilities)?
  - What is the severity of the degradation (consequences)?
- PRA is the task of generating the triplet set:

$$R \equiv RISK \equiv \{S_i, P_i, C_i\}$$

- PRA is a formal method to derive and quantify this set in an integrated manner.
- This provides a framework to prioritize risks, identify risk contributors, and quantify cumulative (aggregate) risk and associated uncertainties.

Scenario	Likelihood (Probability)	Consequence
S_1	p_1	C_1
S_2	p_2	C_2
S_3	p_3	C_3
⋮	⋮	⋮
S_N	p_N	C_N

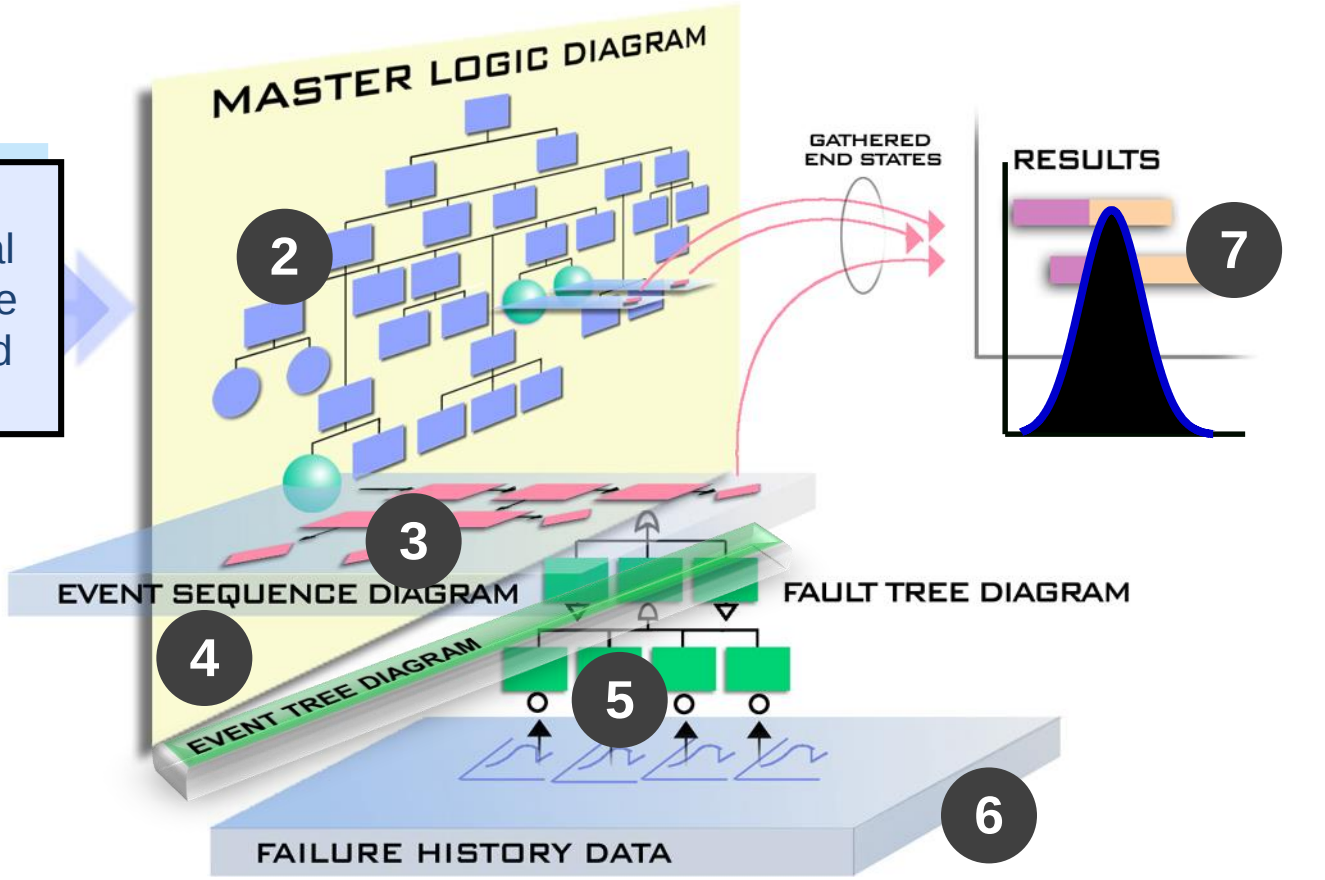
Why PRA

- PRAs are used to model and quantify rare events
  - They take into account external events (e.g., fire, micro-meteoroid, orbital debris, etc.)
  - They take into account human error and common cause
  - They perform uncertainty analysis
  - They take into account the physics of failures and physical interactions between the failure, affected systems, and its surrounding
  - PRA is recognized as a tool that has enhanced the understanding between operations people and engineers as to how the equipment really works, is used, and fails. It also gives a framework for resolving problems and failures.

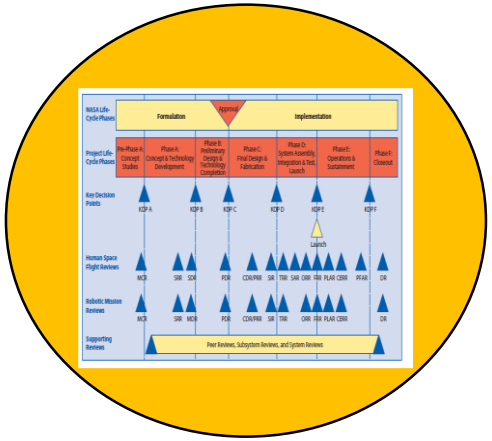
PRA Process

1

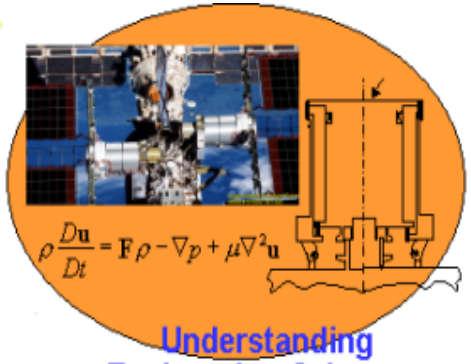
Detailed technical information on the systems modeled



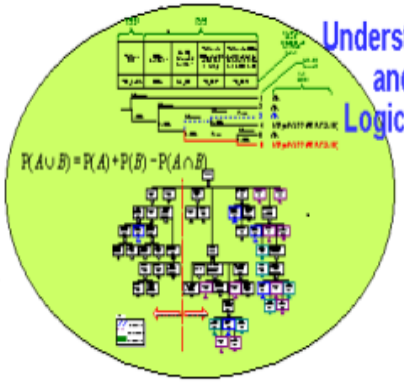
PRA Skills Needed



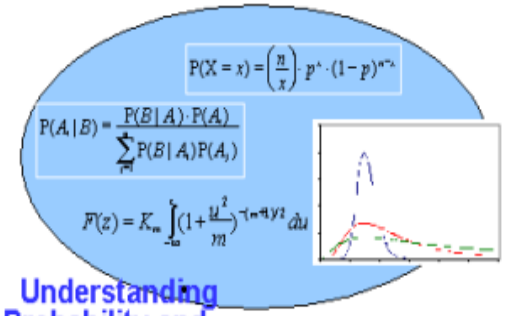
Understanding
Systems
Engineering



Understanding
Engineering Science



Understanding the Art
and Science of
Logical Structures



Understanding
Probability and
Statistics

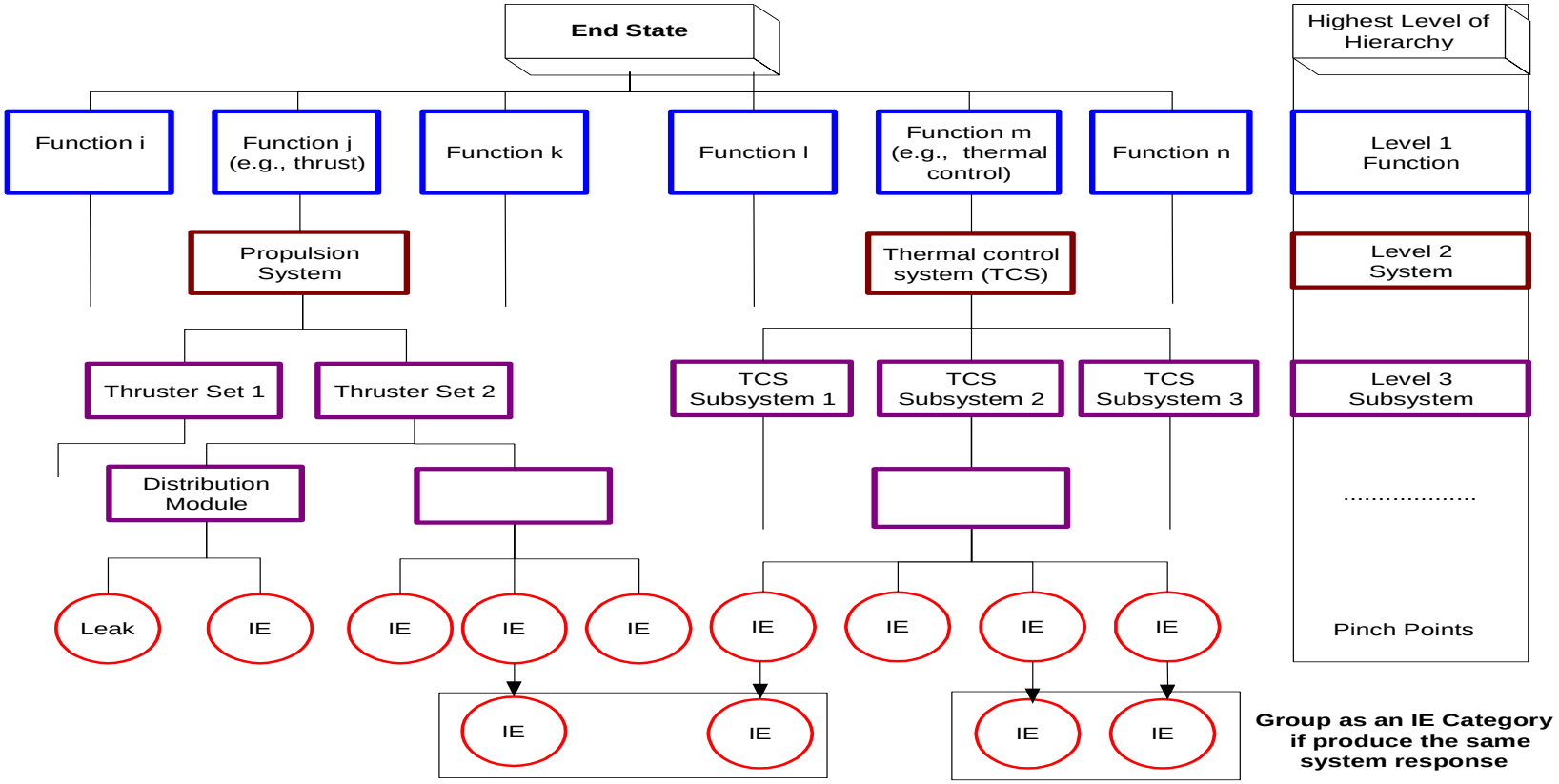
PRA Major Elements

- Major Elements are:
  - Master Logic Diagram (MLD)
  - Event Sequence Diagram (ESD)
  - Event Tree (ET)
  - Fault Tree (FT)
  - PRA Quantification – The Bayesian Approach

PRA Master Logic Diagram

- Master Logic Diagram (MLD) is a logic for identifying events initiating accidents for a given top event (e.g., loss of containment, loss of mission, etc.).
- It is a logic diagram that resembles a fault tree but without the formal mathematical properties of the latter.

PRA Master Logic Diagram

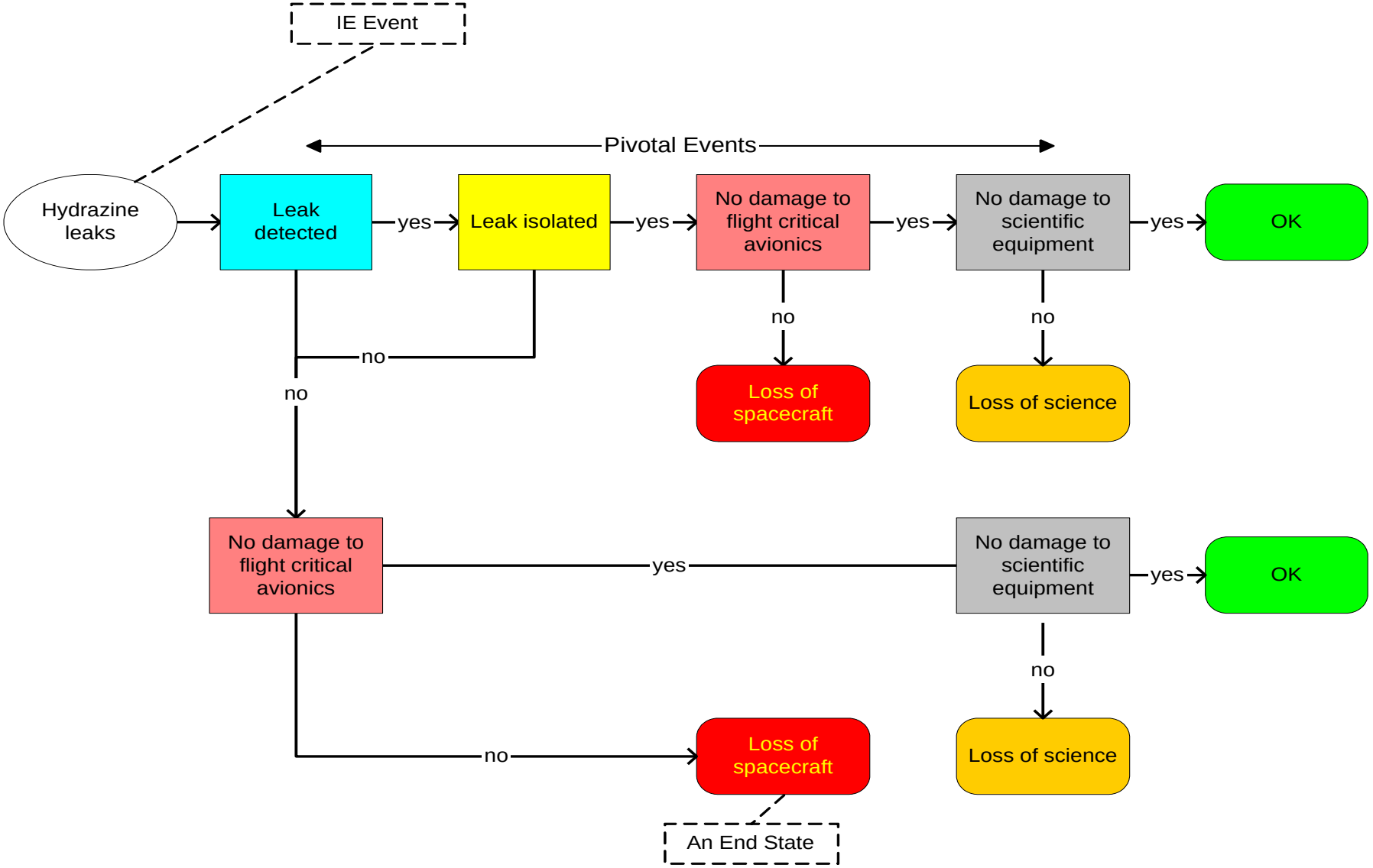


Hierarchical (top-down) method for obtaining initiating events

Event Sequence Diagram (ESD)

- ESD is essentially a forward logic with paths leading to different end states. Each path through the chart is a scenario.
- Its primary use is in supporting probabilistic risk assessments.
- An ESD is developed for each initiating event category in the PRA Master Logic Diagram.
- Input to an ESD is a defined initial state or “initiating event,” the “pivotal events,” and the end states of the scenarios of concern.
- Developing ESDs requires strong engineering knowledge and background in logic flows.
- ESDs are useful for identifying accident scenarios.
- Most engineers find ESDs intuitive and easy to understand.
- It is used for communication between PRA analysts and the engineering community.

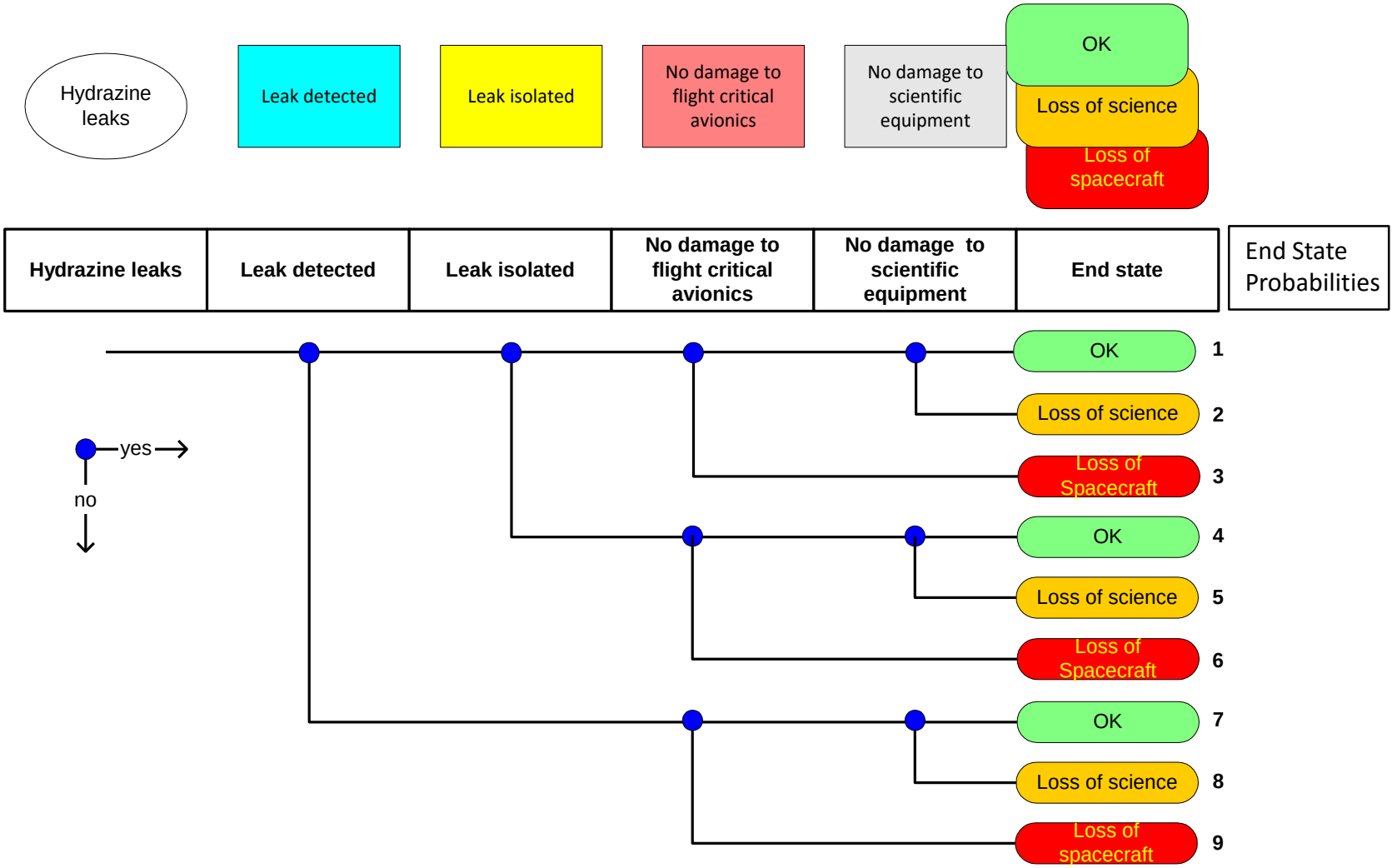
ESD - Propellant Leak



Event Tree Analysis

- Event tree analysis (ETA) is a forward binary logic modeling technique used to determine the propagation paths (sequence of events) to a set of final states resulting from a given initial state or condition.
- Input to the ETA includes a defined initial state or “initiating event” of concern from a master logic diagram, FMEA, Hazard Analysis, or other source.
- Event tree analysis is generally applicable for almost any type of risk assessment application, but used most effectively to model accidents where multiple safeguards are in place as protective features.
- Probabilities can be applied to the initial state and each node of the event sequences to determine the probabilities of end states.
- ETA is a primary tool of Probabilistic Risk Assessment.

ETA – Propellant Leak



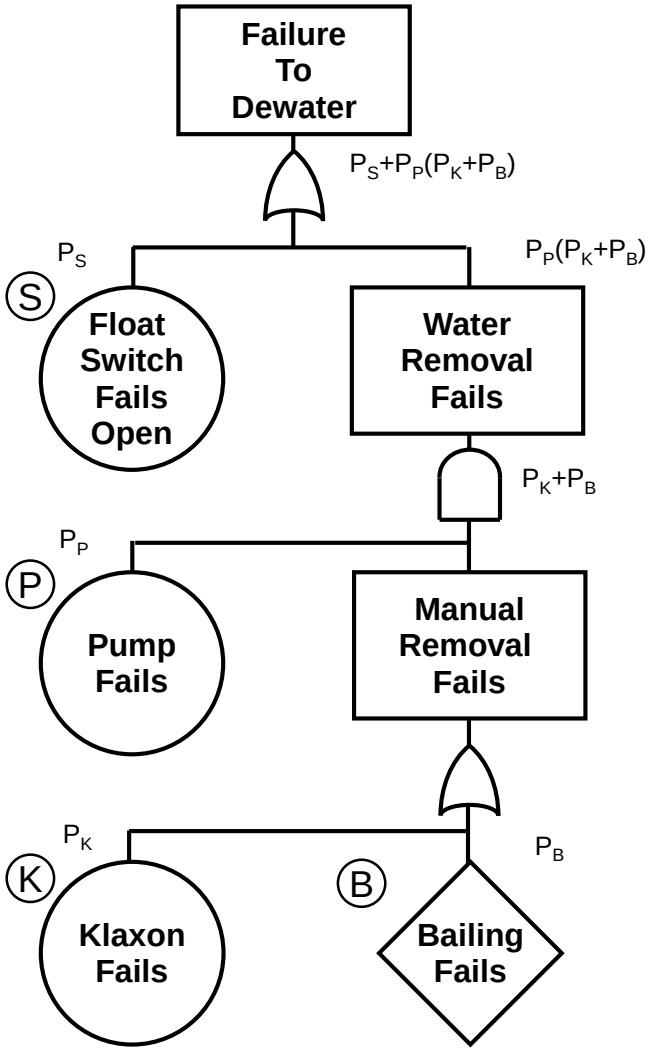
Fault Tree Analysis Definition

- FTA is “an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur.” *Fault Tree Handbook, NUREG-0492, 1981.”*
- FTA is a graphic “model” of pathways within a system that can lead to a foreseeable, undesirable loss event. The pathways interconnect contributory events and conditions, using standard logic symbols.
- Numerical probabilities of occurrence can be entered and propagated through the model to evaluate probability of the foreseeable, undesirable event.
- FTA is one of many reliability and system safety analytical tools and techniques.

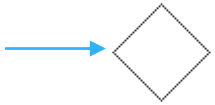
FTA - Water Pump Example

Rare event approximation

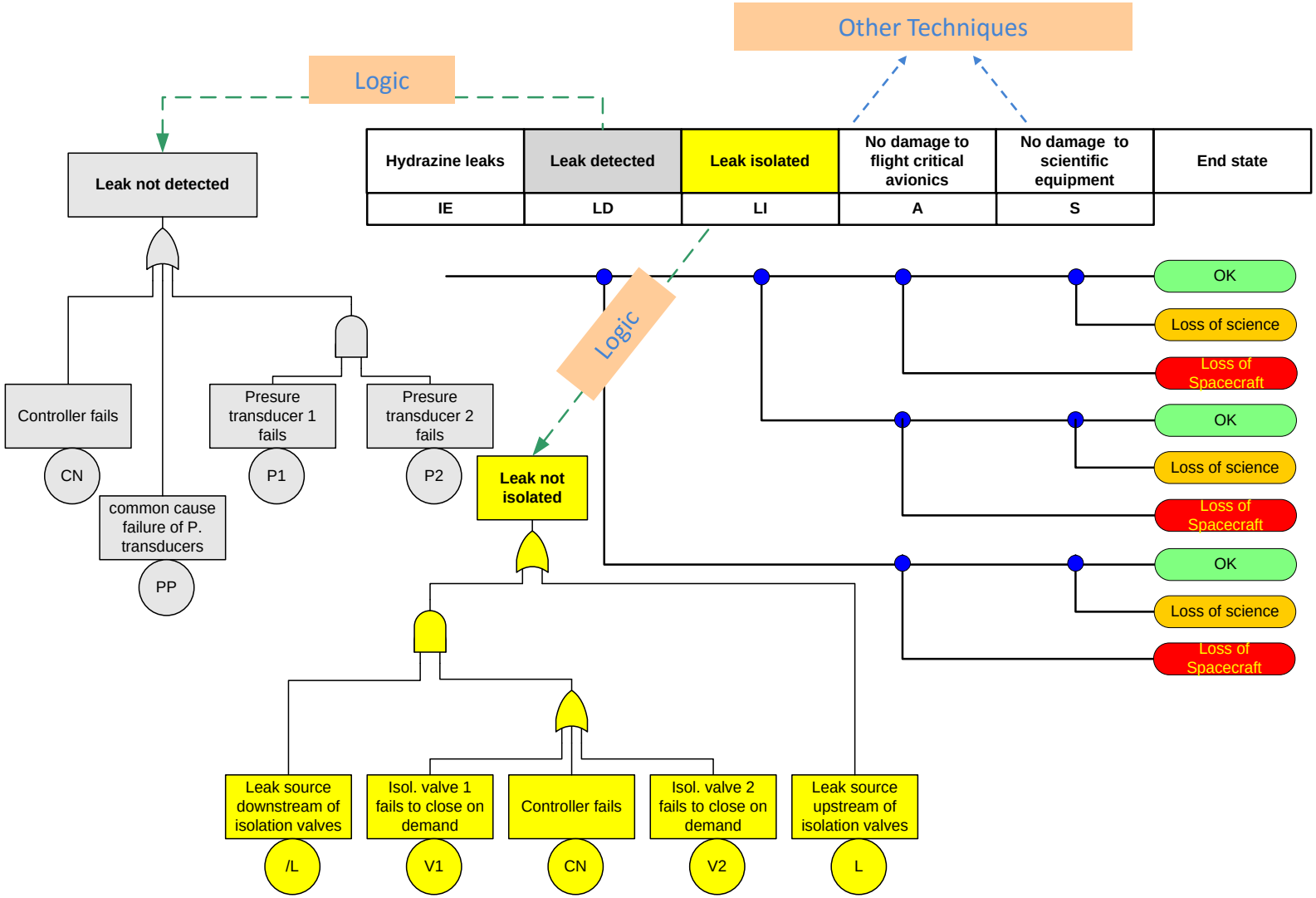
$$P_{TOP} = P_S + P_P P_K + P_P P_B$$



Undeveloped event: An event which is no further developed. It is a basic event that does not need further resolution.



Integration of Fault Trees and Event Trees



PRA Quantification – The Bayesian Approach

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Bayesian Inference

- In probability and statistics, Bayes' theorem (alternatively Bayes' law or Bayes' rule) relates current to prior belief. It also relates current to prior evidence.
- With the Bayesian interpretation of probability, the theorem expresses how a subjective degree of belief should rationally change to account for evidence. This is Bayesian inference, which is fundamental to Bayesian statistics.
- Bayesian inference is a method of statistical inference in which Bayes' Rule is used to update the probability for a hypothesis as evidence is acquired.

Bayesian vs. Classical Statistics

- Classical statistics tries to make inference on the unknown parameters via sampling failure times and establishing confidence intervals for parameters and eventually life length distribution percentiles (A and B allowable).
- In the Bayesian approach, probability is a quantification of degree of belief.
- Bayesian statistics uses the notion that uncertainty about the parameters can be expressed via probability distributions called prior distributions.
- The prior distribution is key to a successful Bayesian analysis.
- Construction of the prior distribution depends on careful quantification of sound expert judgment for the problem at hand.
- This process requires the use of domain experts for defensible implementation.

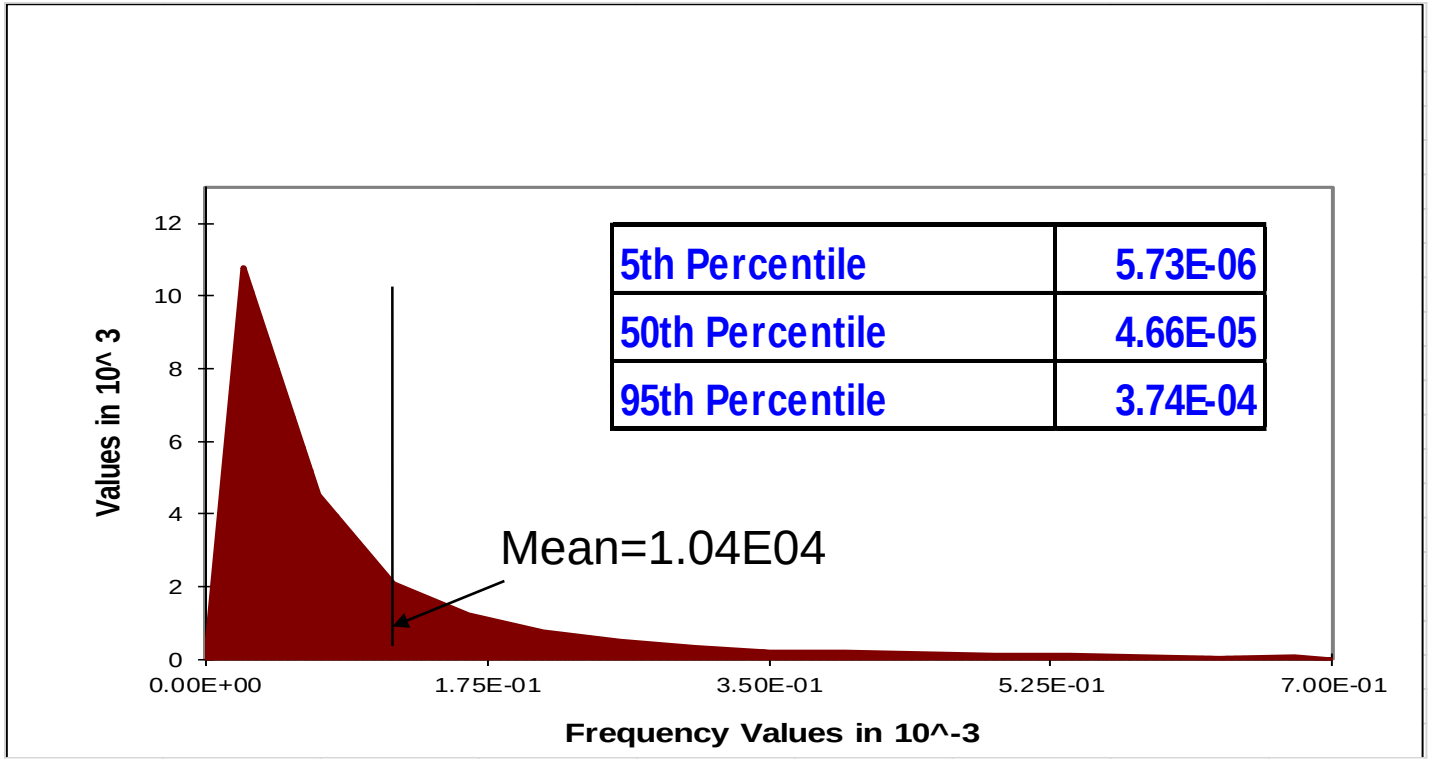
Bayesian Inference
Epistemic Uncertainty

- In Bayesian analysis, failure models such as exponential, binomial, etc., are called aleatory models. Most parameters of those models are themselves uncertain.
  - We describe this second layer of imprecision as epistemic uncertainty.
  - Epistemic uncertainty represents how accurate our state of knowledge is about the model, regardless of model type.
  - If we use an aleatory model (e.g., binomial), and if any parameter of these models is uncertain, then the model has epistemic uncertainty.
  - To determine the nature of the epistemic uncertainty, we rely on Bayesian quantification methods.

The Bayesian Process

- The general Bayesian procedure is:
  - Begin with a probability model for the process of interest.
  - Specify a prior distribution for parameter(s) in this model, quantifying uncertainty, i.e., quantifying degree of belief about the possible parameter values.
  - Obtain observe data.
  - Determine the posterior (i.e., updated) distribution for the parameter(s) of interest.
  - Check validity of model.

Posterior Distribution



The PRA Integrated Process Information Flow

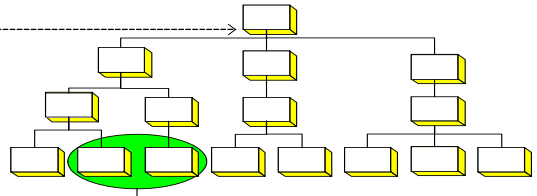
SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Defining the PRA Study Scope and Objectives

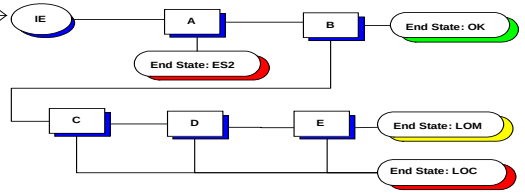
End State: LOC

End State: LOM

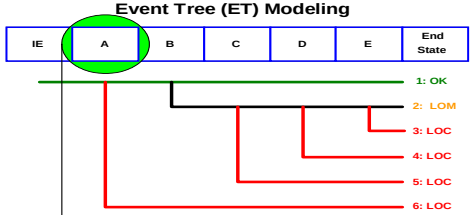
Initiating Events Identification



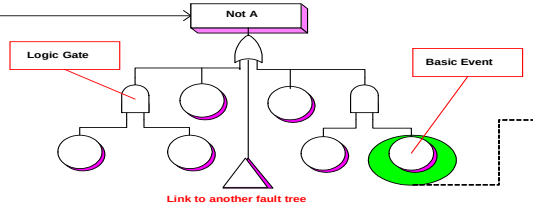
Event Sequence Diagram (Inductive Logic)



Event Tree (ET) Modeling



Fault Tree (FT) System Modeling



Mapping of ET-defined Scenarios to Causal Events

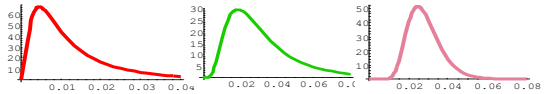
- Internal initiating events
- External initiating events
- Hardware failure
- Human error
- Software error
- Common cause failure
- Environmental conditions
- Other

One of these events

AND

one or more of these elementary events

Probabilistic Treatment of Basic Events



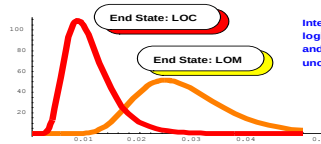
Examples (from left to right):
Probability that the hardware x fails when needed
Probability that the crew fail to perform a task
Probability that there would be a windy condition at the time of landing

The uncertainty in occurrence frequency of an event is characterized by a probability distribution

Model Logic and Data Analysis Review

Domain Experts ensure that system failure logic is correctly captured in model and appropriate data is used in data analysis

Model Integration and Quantification of Risk Scenarios



Integration and quantification of logic structures (ETs and FTs) and propagation of epistemic uncertainties to obtain

- minimal cutsets (risk scenarios in terms of basic events)
- likelihood of risk scenarios uncertainty in the likelihood estimates

Technical Review of Results and Interpretation

Communicating & Documenting Risk Results and Insights to Decision-maker

- Displaying the results in tabular and graphical forms
- Ranking of risk scenarios
- Ranking of individual events (e.g., hardware failure, human errors, etc.)
- Insights into how various systems interact
- Tabulation of all the assumptions
- Identification of key parameters that greatly influence the results
- Presenting results of sensitivity studies
- Proposing candidate mitigation strategies

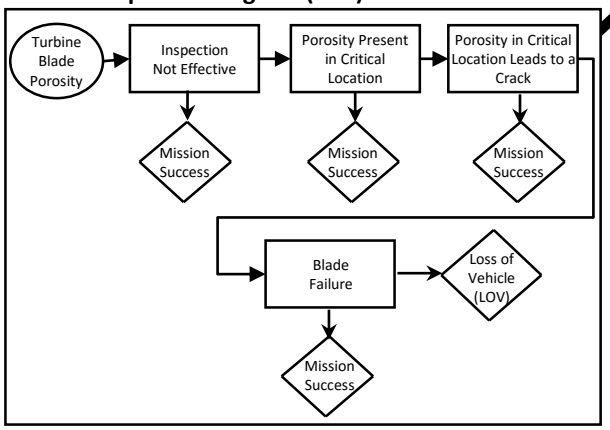
Probabilistic Risk Assessment (PRA) Process Example

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Master Logic Diagram (MLD)

MLD identifies all significant basic/ initiating events that could lead to loss of vehicle.

Event Sequence Diagram (ESD)



EVENT PROBABILITY DISTRIBUTION

APPLICABLE DATA
PROBABILISTIC STRUCTURAL MODELS
SIMILARITY ANALYSIS
ENGINEERING JUDGMENT

QUANTIFICATION OF ESD INITIATING & PIVOTAL EVENTS

Event Tree

Turbine Blade Porosity	Inspection Not Effective	Porosity Present in Critical Location	Porosity Present in Critical Location Leads to Crack in <4300 sec	Blade Failure	Scenario Number	End State
						LOV
						MS
						MS
						MS
						MS

UNCERTAINTY DISTRIBUTION FOR LOV DUE TO TURBINE BLADE POROSITY

UNCERTAINTY DISTRIBUTION FOR EVENT PROBABILITY

RISK AGGREGATION OF BASIC EVENTS

Products

1. System Risk
2. Element Risk
3. Subsystem Risk
4. Risk Ranking
5. Sensitivity Analysis, etc.

PRA Example
Space Shuttle Main Engine (SSME) Upgrades

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Three Engine Cluster
SSME Risk Summary for the Different Upgrades

Engine Configuration	5th Percentile	50th Percentile	Mean	95th Percentile
Phase II	1 in 848	1 in 404	1 in 365	1 in 192
Block I	1 in 1088	1 in 608	1 in 506	1 in 257
Block IIA	1 in 1865	1 in 999	1 in 881	1 in 471
Block II	1 in 2597	1 in 1283	1 in 1067	1 in 509

Reliability Prediction vs. PRA

Category	Reliability Prediction	PRA
What It Is	Methodology to Predict Reliability	Methodology to Predict System/Mission Accident Risk
Discipline	Reliability Engineering	System Safety
Domain	System Design	Mission
Objective	Successful System Function	Accident Avoidance
Measure	Probability of Success (e.g., 0.999)	LOC/LOM (e.g., 1/500)
Focus	How the space flight system can fail, i.e., loss of system function, causes, and effects	How and to what extent accident risk propagates from hazards/failure events, i.e., hazardous/failure events and their consequences
How It's Done	FMEA (Failure Modes, Mechanisms, Loads/Environments) → RBDs/Failure Logic Diagrams → Probability & Statistics	Hazards/Failure Mode Effects →Event Sequence Diagrams → Event Trees → FTA → Probability & Statistics
Input	System Design and Process (e.g., manufacturing) Data, FMEA	Space mission data, Hazard Analysis/FTA, Failure Modes/Effects, Reliability Predictions (i.e., uses output from reliability prediction)
Users	Engineering Design, Program Management, Maintenance Planning/Logistics Support, System Safety/PRA (i.e., Input to PRA)	Engineering Design, Mission Design, Program Management

Probabilistic Risk Assessment (PRA) Advantages and Limitations

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Advantages

- Imposes logic structure on risk assessment.
- Evaluates risk at various system levels including system interactions.
- Handles multiple failures and common causes.
- Provides more insight into the various system failure modes and the effects of human/process interaction.
- Supports sensitivity analysis.
- Provides a tool to combine both qualitative and quantitative risk analysis.
- Can be useful in evaluating risk reduction, risk ranking, identifying areas that requires further attention, and identifying system scenarios that have major impact on system risk.
- PRA is a good source of data for sanity check of the likelihood input data of the risk matrix.

Probabilistic Risk Assessment (PRA)

Limitations

- Could be very expensive.
- PRA faces a level of skepticism with respect to basic sources of quantification, basic failures/events modeled, basic quantification methods, completeness in covering all significant scenarios, quantification of uncertainty, etc.
- It is very difficult to account for design margins, maturity, manufacturing capabilities and uncertainties, unexpected failure modes, unexpected common-cause failures, dependency, etc.

Probabilistic Risk Assessment Bibliography

- Guidelines for Chemical Process Quantitative Risk Analysis (2nd Edition), 2000, Hard cover; 750 pp. (ISBN 0-8169-0402-2)
- Low-Probability High-Consequence Risk Analysis — Ray A. Waller and Vincent T. Covello (Editors), 1984 — Plenum Press; Hard cover; 571 pp.
- Nuclear Systems Reliability Engineering and Risk Assessment — J. B. Fussell and G. R. Burdick, 1977 — Society for Industrial and Applied Mathematics; Hard cover; 849 pp.
- NASA/SPSuccess-2011-3421 “PRA Procedures Guide for NASA Managers and Practitioners”
- PRA Procedure Guide — NUREG/CR-2300,1983 — Government Printing Office; Soft cover; large format; two volumes; 698 pp.
- Probabilistic Risk Assessment and Management for Engineers and Scientists (2nd Edition) — Hiromitsu Kumamoto and Ernest J. Henley, 2000 — IEEE Press; Hard cover, 620 pp. (ISBN 0-7803-1004-7)
- Risk Assessment and Management — Lester B. Lave (Editor), 1987 — Plenum Press; Hard cover; 740 pp.
- Technological Risk — H. W. Lewis. 1992 — W. W. Norton and Company; Soft cover; 368 pp. (ISBN 0-393-02883-6)