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

RAM XV Tutorial
Huntsville, Alabama
November 1-2, 2023

RELIABILITY ENGINEERING

THE LINK TO SAFETY AND RISK ASSESSMENT

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
- Reliability Engineering Overview
- Reliability Requirement Allocation
- Reliability Prediction
- Reliability Demonstration
- The FMEA/CIL
- Safety Discussion – The Link to Reliability
- Probabilistic Risk Assessment (PRA) Discussion – The Link to Reliability
- The Reliability, Safety, and PRA integration
- Concluding Remarks

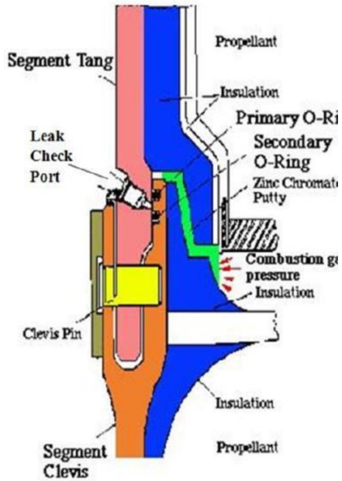
Introduction

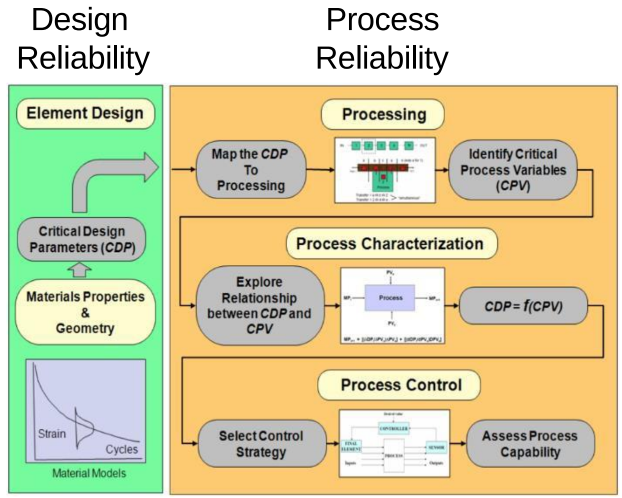
SAFETY ENGINEERING SEAC & ANALYSIS CENTER

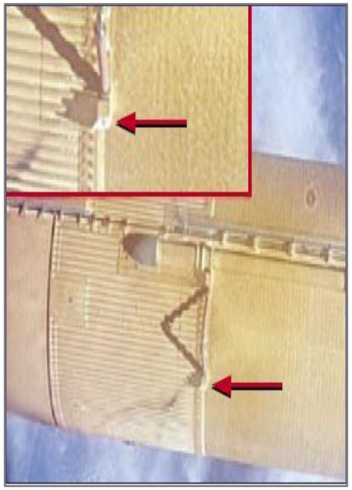
- This tutorial is intended to discuss the links between reliability, safety, and Probabilistic Risk Assessment (PRA).
- Some of the material for this tutorial is taken from a three-day reliability engineering course offered by A-P-T Research, Inc. The Reliability course is intended to provide a better 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: Heather Daniels, 256-327-3373, training@apt-research.com.
- **Note:** Attendees of the full course will be credited with 2.0 Continuing Education Units (CEU).

SEAC Courses

- System Safety
- Software System Safety
- Explosives Safety
- Range Safety
- Risk Management
- Reliability Engineering
- Probabilistic Risk Assessment (PRA)
- Radiation Safety







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

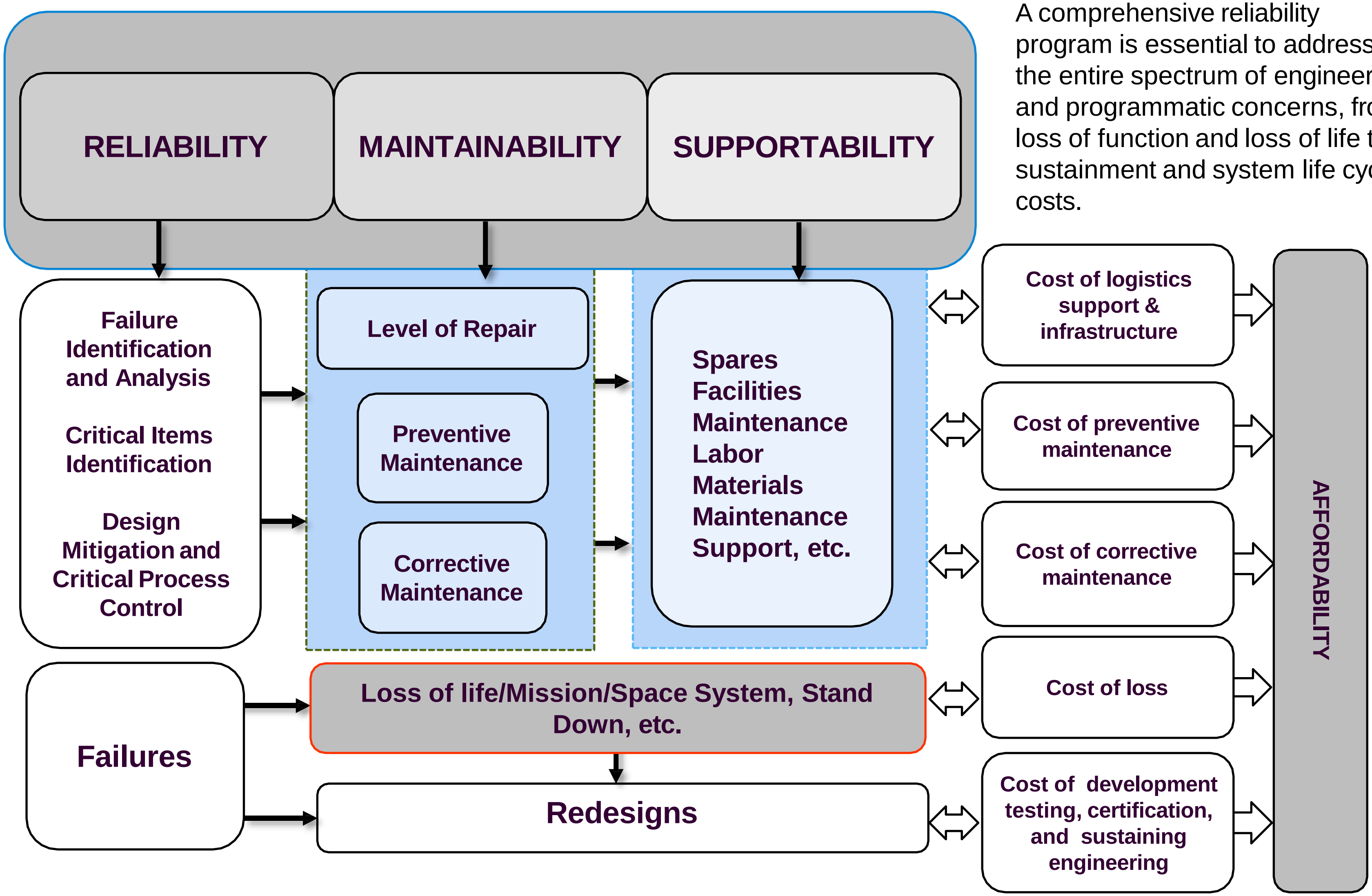
Definitions

- **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

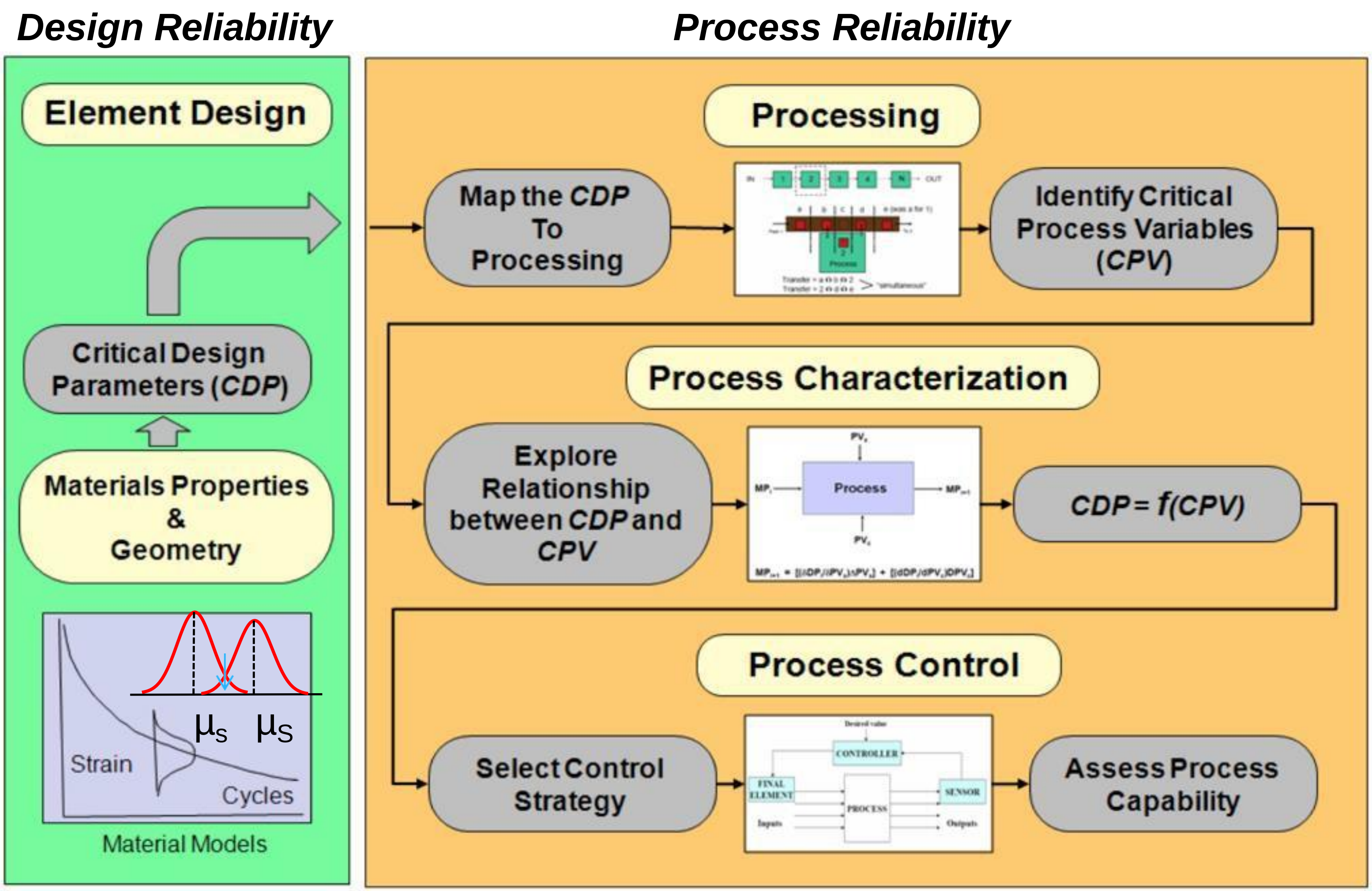
- Reliability engineering is a design-support discipline.
- Reliability engineering is critical for understanding component failure mechanisms and identifying critical design and process drivers.
- Reliability engineering has important interfaces with, and input to, design engineering, maintainability and supportability engineering, test and evaluation, risk assessment, risk management, system safety, sustainment cost, and quality engineering.

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.

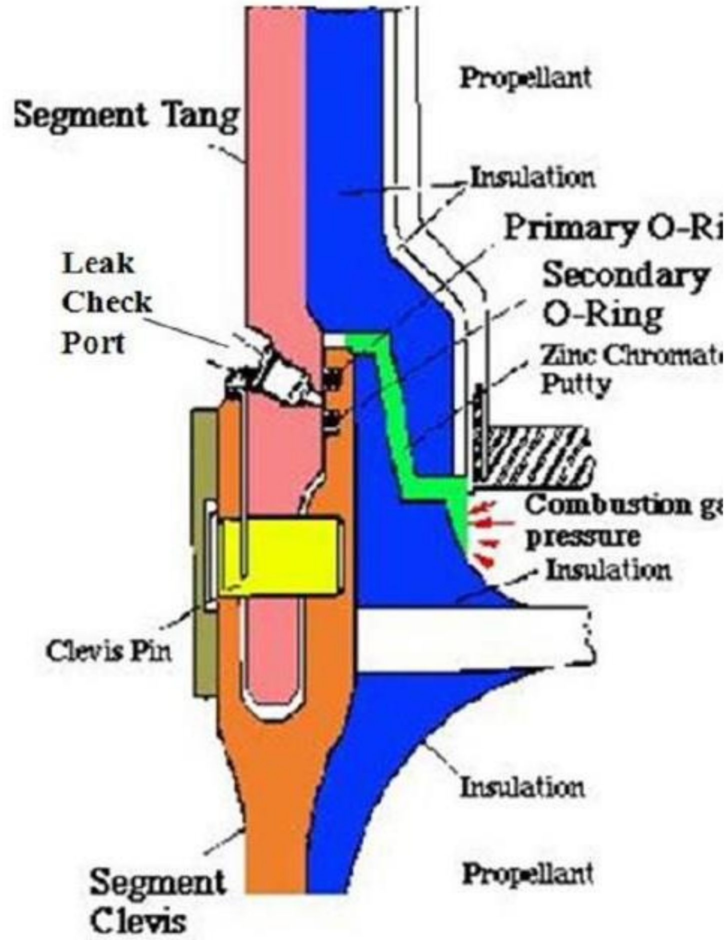
Design it Right and Build it Right



SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Causes and Contributing Factors

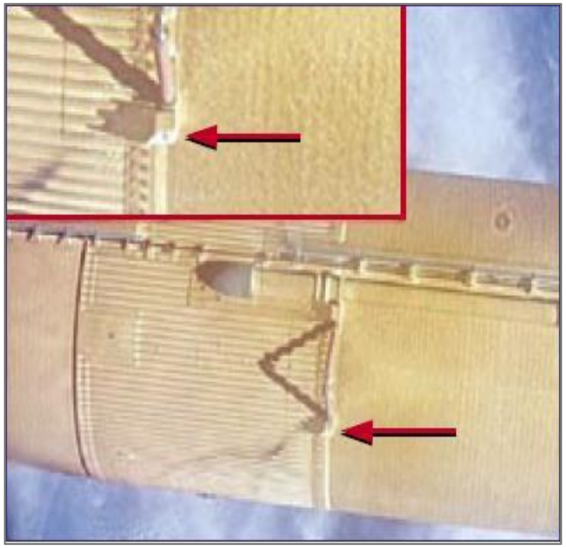
- The zinc chromate putty frequently failed and permitted the gas to erode the primary O-rings.
- The particular material used in the manufacture of the shuttle O-rings was the wrong material to use at low temperatures.
- Elastomers become brittle at low temperatures.

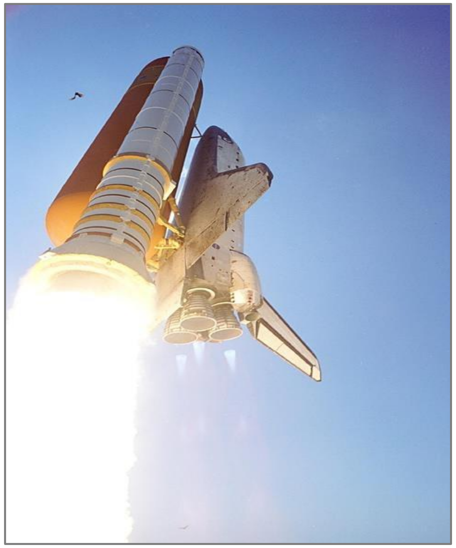


Process Reliability
The Columbia Accident

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?

Reliability Metrics

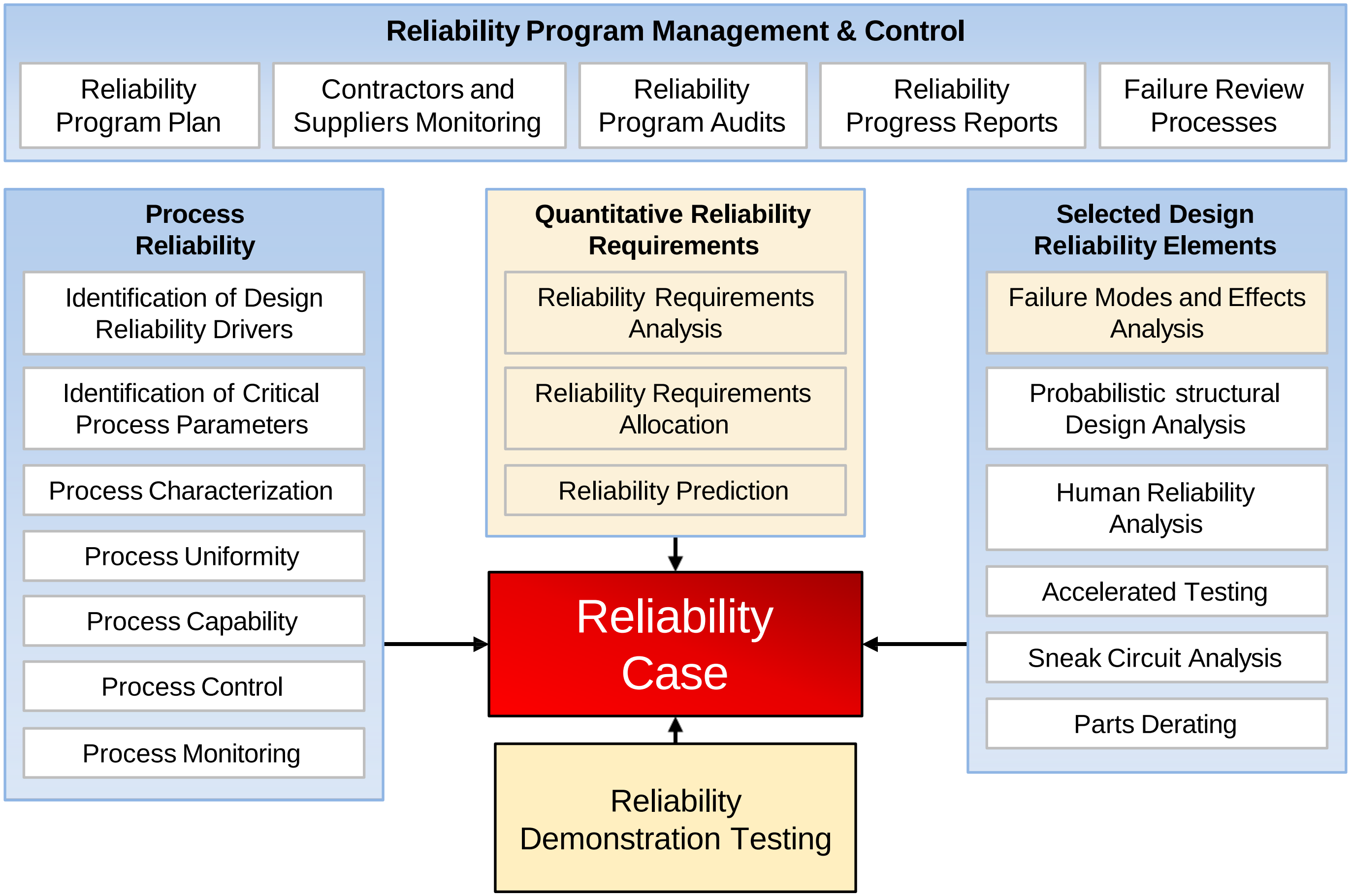
There are many ways to measure and evaluate reliability. The following are the most commonly used across government and industry:

- ***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.
  - 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).

Selected Elements of A 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.

RELIABILITY ALLOCATION

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

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:

$$f(R1, R2, \ldots, Rn) \geq Rs$$

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.

Equal Apportionment Example

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- 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:
  - $R_T = R_R = R_C = (R)^{l/n} = (0.729)^{1/3} = 0.90$
- 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

- 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:

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

$$\lambda_i' = w_i \lambda_S$$

Where,
n is the total number of subsystems,
λ_i is the present failure rate of the i^{th} subsystem,
λ_S is the required system failure rate, and
λ_i' is the failure rate allocated to the i^{th} subsystem.

ReliaSoft Corporation, Lambda Predict, Tucson, AZ: ReliaSoft Publishing, 2007.

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.

RELIABILITY PREDICTION

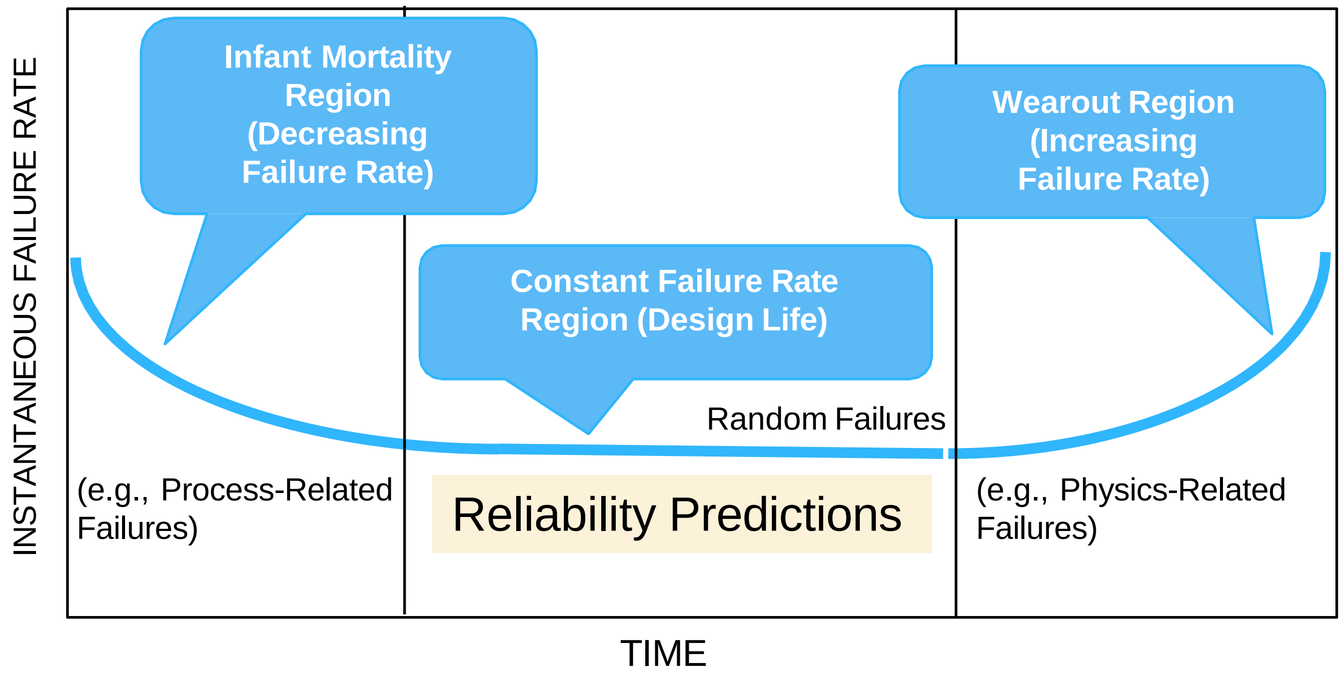
SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

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

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 (e.g. similarity analysis, physics-based reliability, failure models using actual operation data,, MIL-HDBK's, etc.
- Commonly used reliability prediction tools include Reliability Block Diagrams (RBD), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), FMECA etc.

The Bathtub Curve - Hardware Reliability



Reliability Prediction Using Reliability Block Diagrams

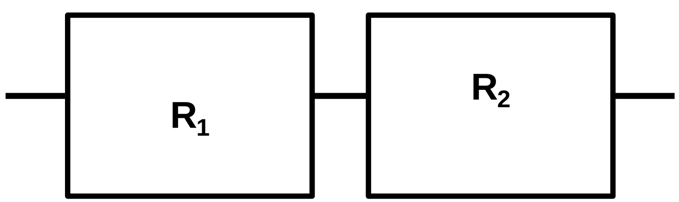
SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

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

Reliability Block Diagrams

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- 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

Reliability Prediction Using Fault Tree Analysis (FTA)

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

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.

Why FTA

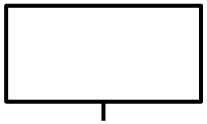
- FTA is important in:
  - Quantifying system failure probability
  - Assessing system Common Cause vulnerability
  - Optimizing resource deployment to control vulnerability
  - Identifying potential single point failures
  - Identification of those potential contributors to failure that are "critical"
  - Identification of resources committed to preventing failure
  - Supporting trade studies
  - Supporting problem investigation
  - Supporting hazard analysis

Origins

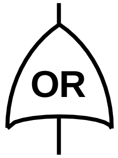
- Fault tree analysis was developed in 1962 for the U.S. Air Force by Bell Telephone Laboratories for use with the Minuteman system.
- It was later adopted and extensively applied by the Boeing Company.
- It has been used by NASA extensively as problem investigating tool.

Fault Tree Logic Symbols

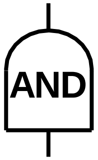
Many Fault Tree Analyses can be carried out using only these four symbols:



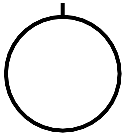
TOP Event – foreseeable, undesirable event, toward which all fault tree logic paths flow



"Or" Gate – produces output if any input exists.



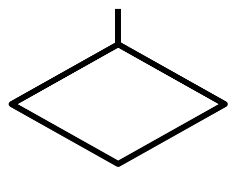
"And" Gate – produces output if all inputs co-exist.



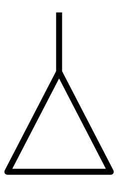
Basic Event – Initiating fault / failure, not developed further. (Often called "Leaf," "Initiator," or "Basic.") The Basic Event marks the limit of resolution of the analysis.

More Gates & Symbols

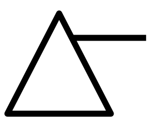
Intermediate Event
describing a system state produced by antecedent events



Undeveloped Event
An event not further developed.



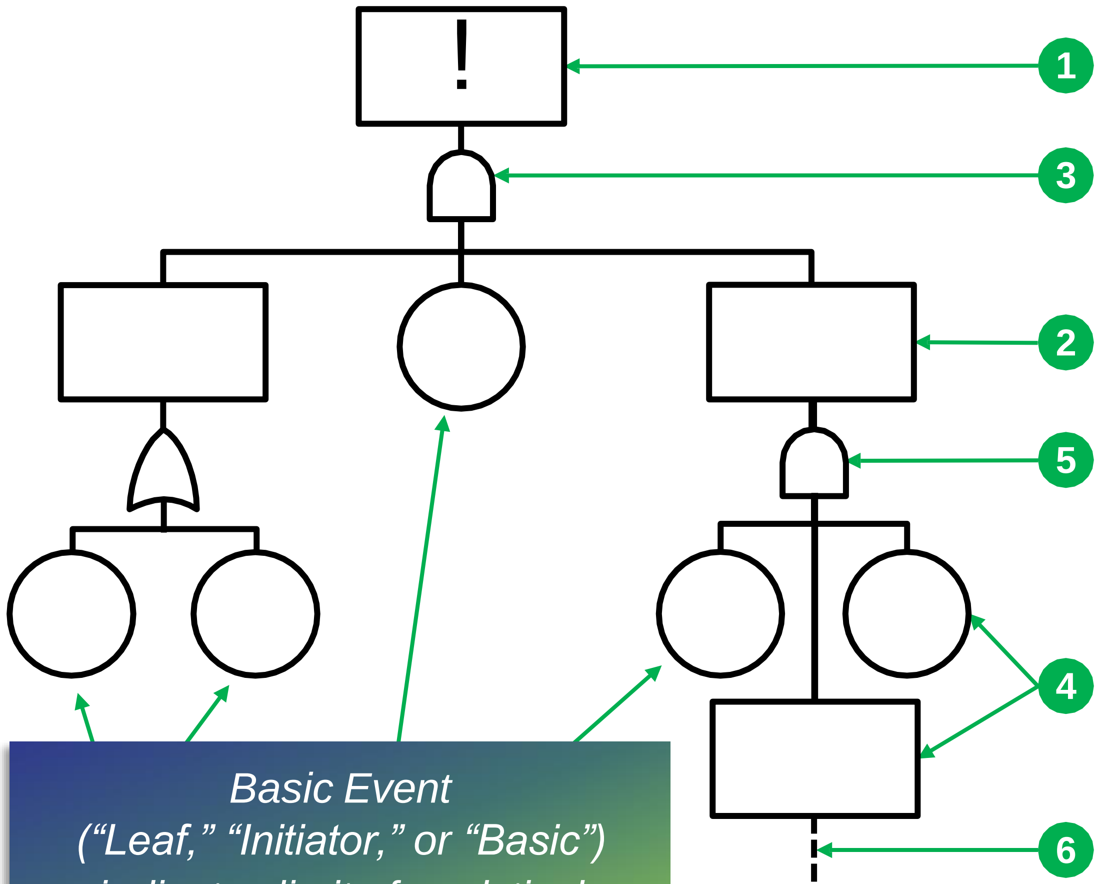
Transfer In



Transfer Out

Steps in Fault Tree Logic

S³86-8



Basic Event
(“Leaf,” “Initiator,” or “Basic”)
indicates limit of analytical resolution.

1. Identify undesirable TOP event.
3. Link contributors to TOP by logic gates.
2. Identify first-level contributors.
5. Link second-level contributors to TOP by logic gates.
4. Identify second-level contributors.
6. Repeat / continue.

Developing The Fault Tree

- A successful FTA requires the following steps:
  - Define the top event of the FT
  - Define the scope of the FTA
  - Define the resolution of the FTA
  - Construct the FT
  - Evaluate the FT
  - Interpret and present the results

Example TOP Events

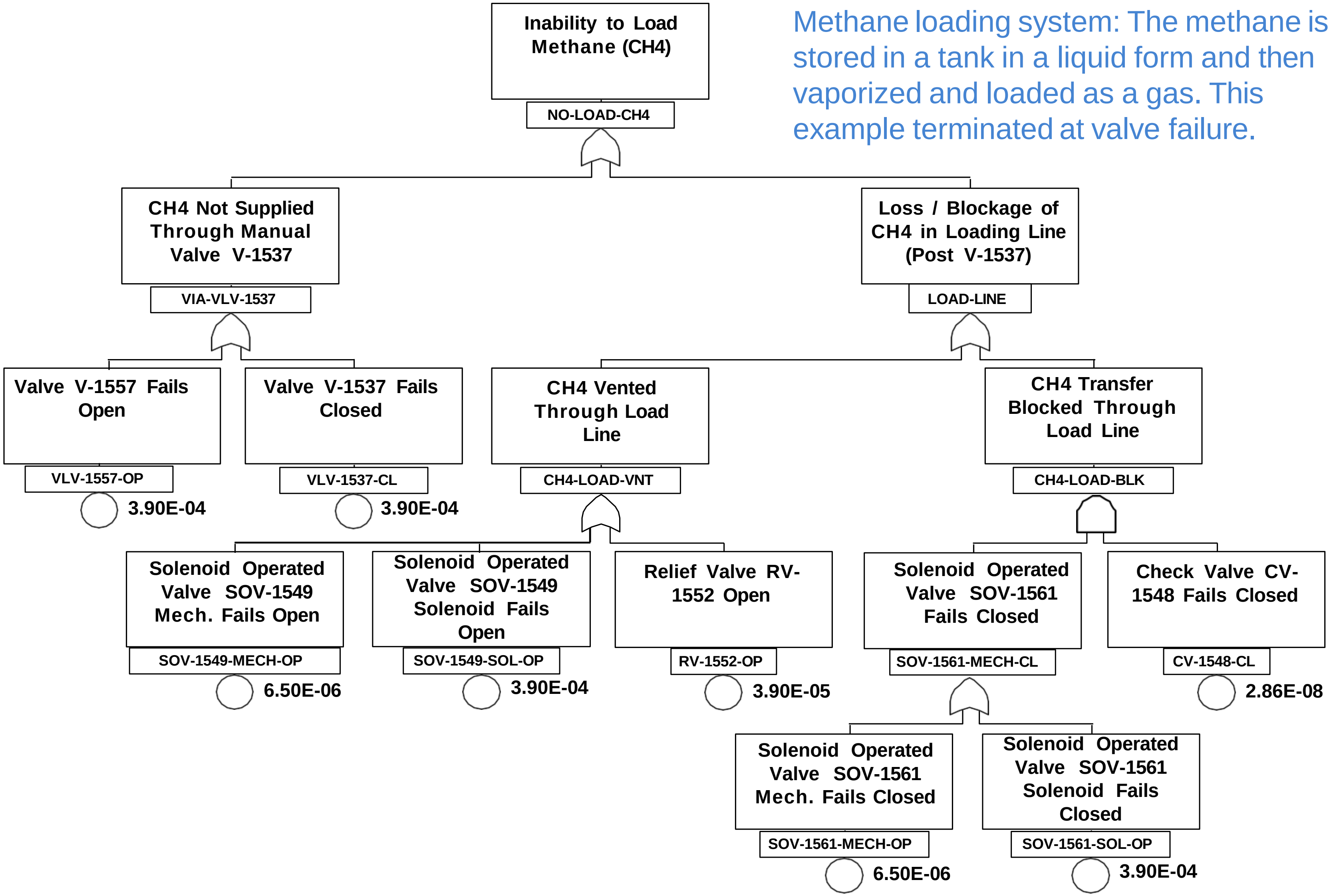
- Loss of Thermal Protection during vehicle reentry
- Hot gas leak in a solid rocket motor
- Mid-air collision
- Subway derailment
- Turbine engine FOD
- Irretrievable loss of primary test data
- Rocket failure to ignite
- Inadvertent nuke launch

TOP events represent potential high-penalty losses (i.e., high risk). Either severity of the outcome or probability of occurrence can produce high risk.

Quantitative FTA

X-33 Methane Ground Storage and Loading Example

Methane loading system: The methane is stored in a tank in a liquid form and then vaporized and loaded as a gas. This example terminated at valve failure.



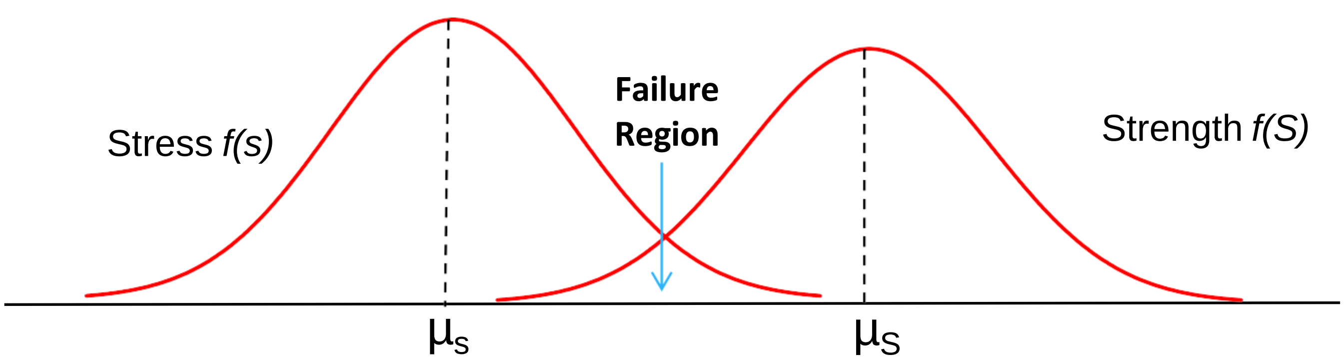
Physics Based Reliability Prediction

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

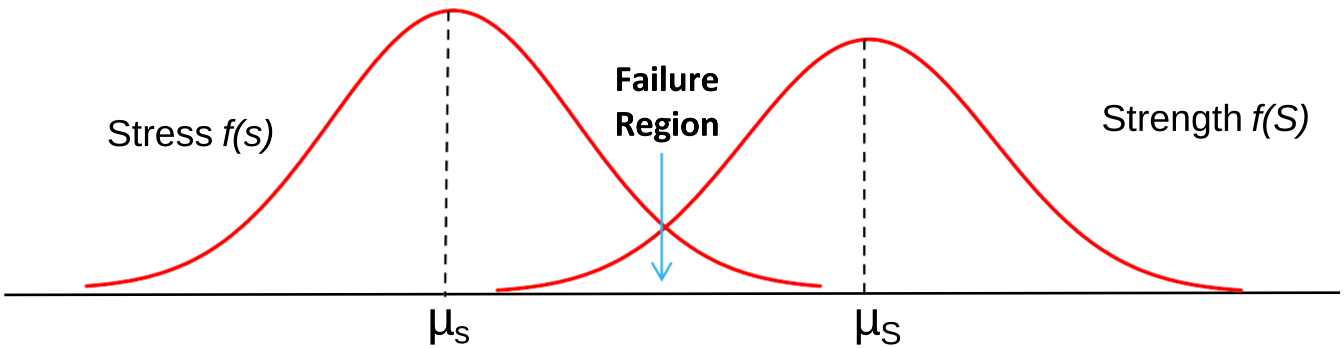
Physics Based Reliability Prediction

- 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

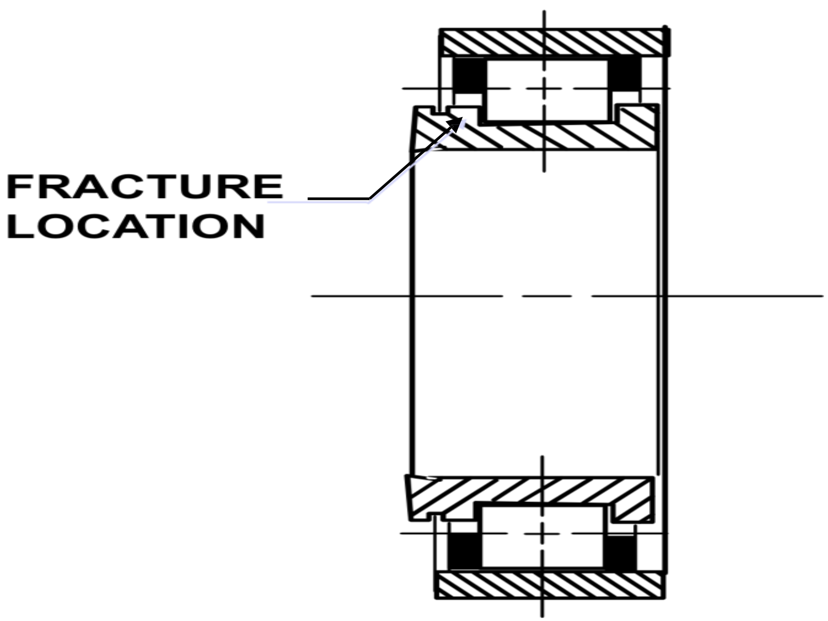
σ_S = standard deviation of the strength

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.

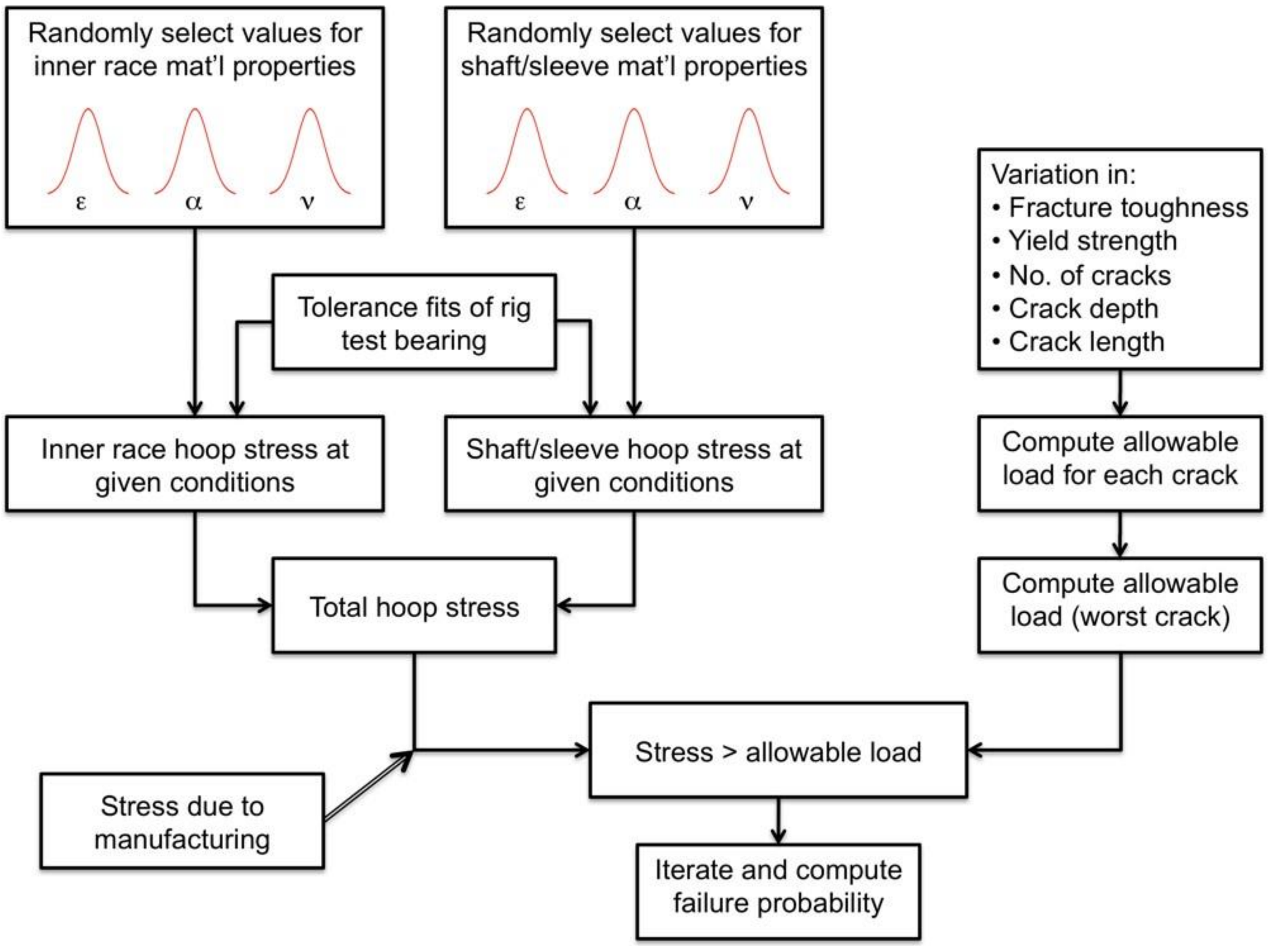
A Rocket Engine Roller Bearing Example

- 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.

The Analytical Approach - The Simulation Model



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.

A Rocket Engine Roller Bearing Example

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

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.

The Analysis Results

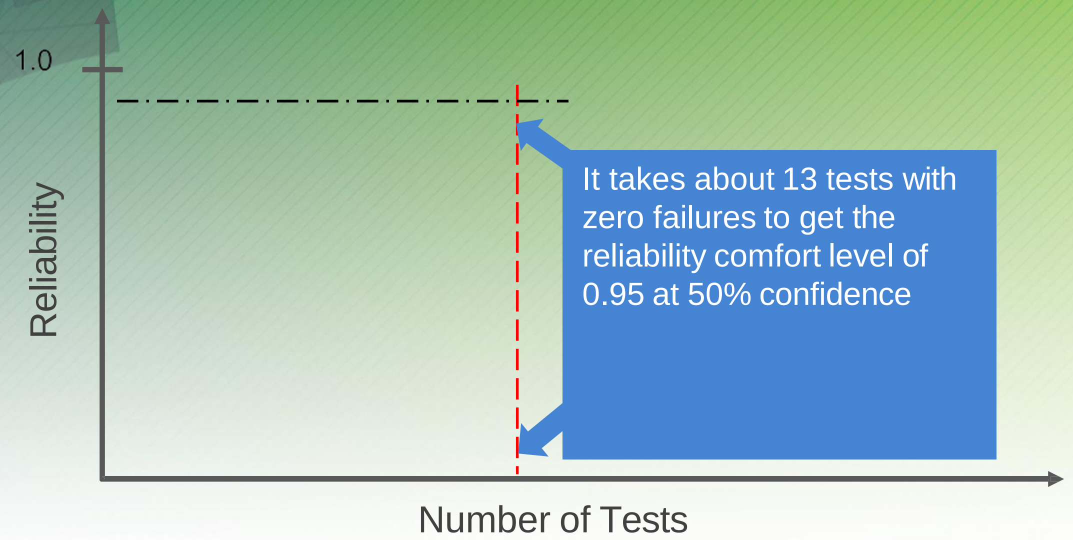
SAFETY ENGINEERING SEAC & ANALYSIS CENTER

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 DEMONSTRATION

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

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.

Commonly Used Distributions

- 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.

http://reliabilityanalyticstoolkit.appspot.com/

The Binomial Distribution Case - Exact Method

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

One-sided confidence, exact method

- The calculation method for single sided limits are nearly identical to the two-sided case, except all the α 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

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

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

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 α = 1- Confidence Level

https://reliabilityanalyticstoolkit.appspot.com/binomial_confidence_details

The Binomial Distribution Case
One-sided Exact Method Example

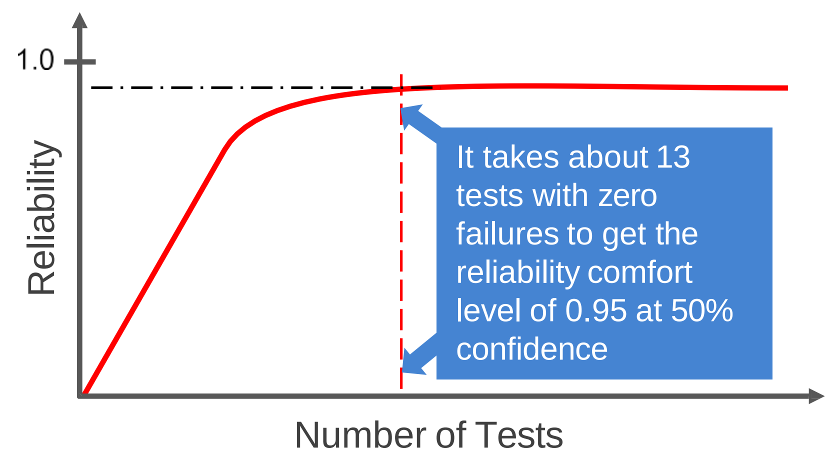
SAFETY ENGINEERING SEAC & ANALYSIS CENTER

Demonstrated Reliability* at 50% confidence
Using the Binomial Model With Zero Failure Case

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

***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: $P(R \geq 0.0.707)=0.5$



FAILURE MODES & EFFECTS ANALYSIS AND CRITICAL ITEM LIST (FMEA/CIL)

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

FMEA Definition

- **An FMEA** is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations.
- It is a **bottom-up**, tabular technique that explores the modes in which each system element can fail and the corresponding failure causes. It assesses the consequences of each of these failure causes on the system element in which it occurs, on other system elements, and on the success of the system mission.
- Also referred to as FMECA – Failure Modes, Effects and Criticality Analysis.
- **A FMECA** addresses the criticality or risk of individual failure causes.

NASA DESCRIPTION/USE: Failure Modes and Effects Analysis (FMEA) – to identify and document the possible failures modes and causes of each hardware item of a subsystem/system, the worst case effect of such failures for each mission phase and assigns criticality per the applicable FMEA/CIL guidelines document. This information is vital for design improvements, reliability and maintainability analysis

FMEA Definitions

- **Failure Mode**
  - The **manner** in which a fault occurs.
- **Failure causes**
  - Are defects in design, process, quality, or part application.
- **Failure Effect**
  - The consequence(s) of a failure mode on an operation/function/status of a system/process/activity/environment.
  - The undesirable outcome of a fault of a system element in a particular mode.
  - The effect may range from relatively harmless impairment of performance to multiple fatalities, major equipment loss and environmental damage.

Element	Failure Mode Examples
Switch	open, partially open, closed, partially closed
Valve	open, partially open, closed, partially closed
Spring	stretch, compress/collapse, fracture
Cable	stretch, break, kink, fray
Relay	contacts closed, contacts open, coil burnout, coil short
Operator	wrong action to proper item, wrong operation to wrong item, proper action to wrong item, perform too early or too late, failure to perform

Critical Items List (CIL) Definition

- What is a Critical Items List (CIL)?
  - It is the report documenting the failure modes for a system of interest that require added retention rationale.
  - It is based on results of Failure Modes and Effects Analysis (FMEA)
- What is a CIL Critical Item?
  - AN ITEM that has a failure mode classified as critical by Program definition

NASA Description/Use: Critical Items List (CIL) – to identify and document the list of critical failure modes of item(s) in each subsystem/system with potential worst case effect(s), such as Loss of Crew (LOC), Loss of Vehicle (LOV) and/or Loss of Mission (LOM) or detrimental failure effects as applicable to system under study per the applicable FMEA/CIL guideline document. The CIL provides details of relevant design features, testing and inspections processes and controls, as applicable to the failure mode, to mitigate/minimize the risk. CIL retention rationale bridges the gap in the design, test/verification requirements, inspection and process controls. CIL also facilitates in the identification of Government Mandatory Inspection Points.

Why do FMEA/CIL?

- Evaluate design approach to ensure compliance with reliability requirements
- Identify and eliminate critical single point failures
- Identify failure detection and isolation designs
- Identify methods to “deal with” failure modes
- Identify tests to “check for” failure modes
- Identify operational workarounds to “deal with” failures
- Identify critical items for program/project visibility
- Identify where fault-tolerant, fault-sensing, and performance monitoring
- features should be developed.
- Provide visibility into potential system interface problems.
- Use as a basis for assessing/quantifying the risks associated with engineering design or manufacturing process changes.
- Provide input to risk assessment, hazard analysis, quality inspections, etc.

What Are the Different FMEA Types?

- All FMEAs can basically be classified into one of three possible types: functional, Hardware (component), or process.
- Functional FMEAs:
  - A functional FMEA examines the intended functions that a product, process, or service is to perform rather than the characteristics of the specific implementation.
  - When a functional FMEA is developed, a functional block diagram is typically used to identify the top-level failures for each block in the diagram.
  - For example, a functional FMEA would consider that a capacitor is intended to regulate voltage and then analyze the effects of the capacitor failing to regulate voltage. It would not analyze what would occur if the capacitor fails open or fails shorted.

What Are the Different FMEA Types?

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- Hardware (component) FMEAs:
  - A Hardware or a component FMEA examines the characteristics of a specific implementation to ensure that the design complies with requirements for failures that can cause loss of end-item function, single-point failures, and fault detection and isolation.
  - Once individual items of a system are identified in the later design and development phases, component FMEAs can assess the causes and effects of failure modes on the lowest-level system items.
  - Component FMEAs for hardware, commonly referred to as piece-part FMEAs, are the most common type.

What Are the Different FMEA Types?

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- Process FMEAs:
  - A process FMEA examines the ways that failures in a manufacturing or assembly process can affect the operation and quality of a product or service.
  - A process FMEA can be performed at any level to evaluate possible failure modes in the process and limitations in equipment, tooling, gauges, or operator training.
  - The information collected can help to determine what can be done to prevent potential failures prior to the first production run. You can then take actions to reduce your exposure to risks deemed unacceptable.

The FMEA/CIL Process

- The main steps in a FMEA process can be summarized as follows:
  - Define the system to be analyzed, and obtain necessary drawings, charts, descriptions, diagrams, component lists. Break the system down into convenient and logical elements and establish a coding system to identify system elements.
  - Define the scope
  - Identify Assets to be considered/protected
  - Determine Failure Modes, Failure Causes, and failure Effects of
  - Components, including mitigation options.
  - Perform criticality Analysis.
  - ID Critical Items, develop retention rationale, and generate FMEA & CIL Reports

FMEA Worksheet (Space Shuttle)

SAFETY ENGINEERING SEAC

FAILURE MODE EFFECTS ANALYSIS

REVISION:
DATE:
PAGE: SUPERCEDES: ________
SEPARATION ANALYST:
APPROVED:

THRUST VECTOR CONTROL SUBSYSTEM

A FINAL COUNTDOWN
B BOOST
C
D DESCENT
E RETRIEVAL

NOMENCLATURE AND FUNCTION	FAILURE MODE AND CAUSE	FAILURE EFFECT ON SUBSYSTEM	FAILURE EFFECT ON SRB	FAILURE EFFECT ON MISSION/ CREW AND REACTION TIME	a. FAILURE DETECTION b. REDUNDANCY SCREENS	CORRECTING ACTION/ TIMEFRAME/REMARKS	CRIT CAT
20-01-44 Turbine Exhaust Duct Assembly P/N: 10206-0002-102 Ref. Des.: None 2 Required Vents HPU turbine exhaust gas to atmosphere out-side of the aft skirt. Exhaust Duct Assembly includes: Upper Exhaust Assembly (three bellows) 10206-0003-101 Middle Exhaust Assembly 10206-0007-101 Alt. 10206-0031-851 Alt. 10206-0044-851 Alt. 10206-0045-851 Lower Exhaust Assembly 10206-0010-101	FM Code A01 External leakage of hot exhaust gas (System A and/or B) caused by: • Bellows fracture/ fatigue • Flange/duct fracture • Seal failure • Seal surface defect • Improper torque • Contamination during assembly • Improperly lockwired.	A,B. Actual loss Loss of containment of hot exhaust gases. C,D,E. No Effect Failure mode not applicable to these phases.	A,B. Probable Loss Fire and explosion. C,D,E. No Effect Failure mode not applicable to these phases.	A,B. Probable Loss Fire and explosion will lead to loss of the mission, vehicle, and crew. Reaction Time: Seconds C,D,E. No Effect Failure mode not applicable to these phases.	a) None b) N/A a) N/A b) N/A	Correcting Action: None Timeframe: N/A	1 3

Criticality	Definition
1	Single failure that could result in loss of life or vehicle.
2	Single failure that could result in loss of mission.
1R	Redundant hardware item which, if all failed, could cause loss of life or vehicle
1S	Failure in a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous condition, potentially resulting in loss of life or vehicle.
2R	Redundant hardware item which, if all failed, could cause loss of mission.
3	All other failures.

A FMECA Form

MIL-STD-1629A

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

CRITICALITY ANALYSIS

System ______________________

Indenture Level ______________________

Reference Drawing ______________________

Mission ______________________

Date: ______________________

Sheet _____ **of** ______________________

Compiled By ______________________

Approved By ______________________

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS	FAILURE PROBABILITY FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	FAILURE RATE (λ_p)	OPERATING TIME (t)	FAILURE MODE CRIT # $C_m=\beta\alpha\lambda_p t$	Item Crit # $C_r=\Sigma(C_m)$	REMARKS

Worksheet from MIL-STD-1629A

SAFETY DISCUSSION

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

Safety Related Definitions

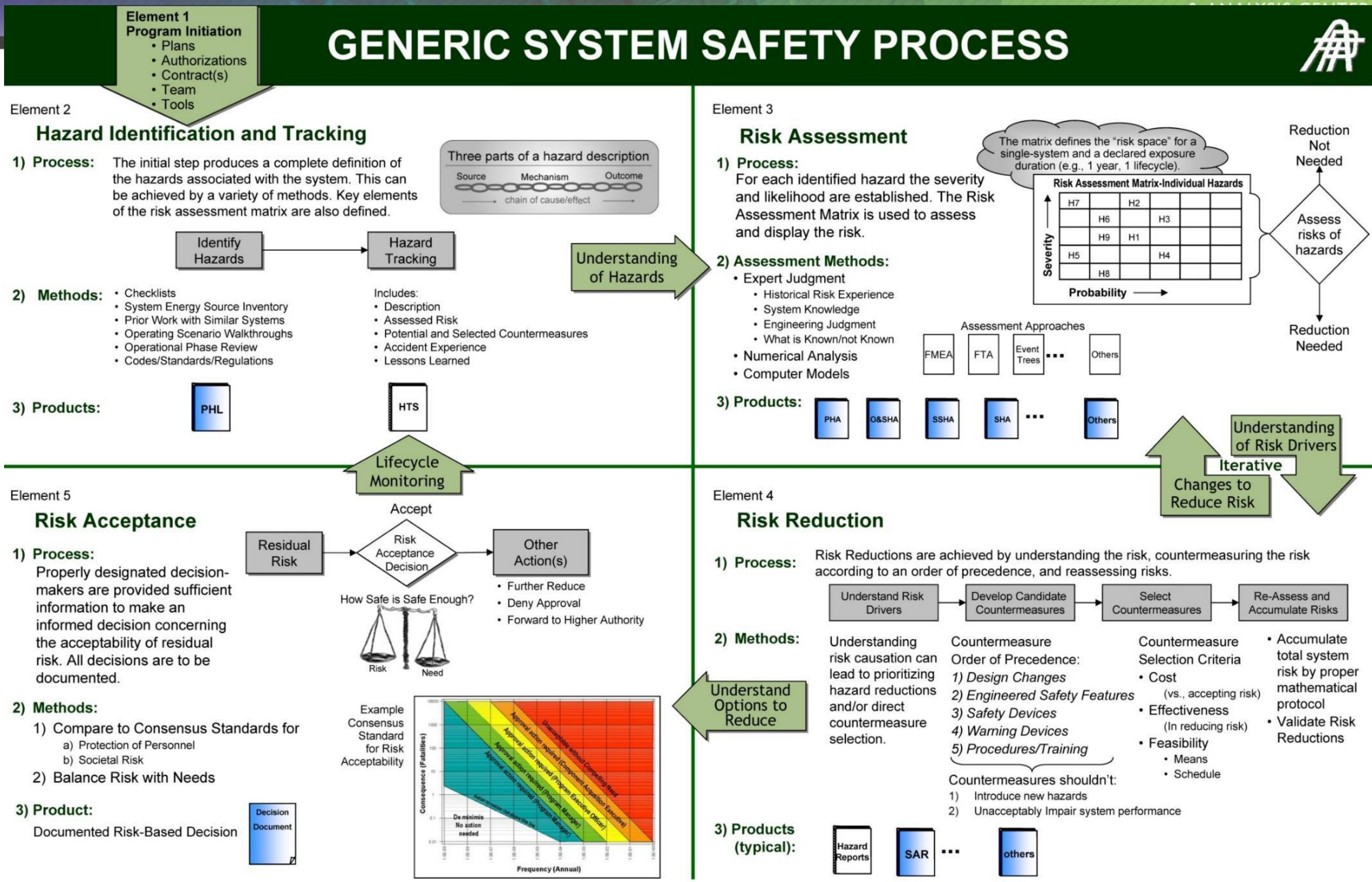
- **Safety** is the freedom from those hazards that can cause death, injury, or illness in humans, adversely affect the environment, or cause damage to or loss of equipment or property.
- **System Safety** is the application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.
- **Hazard Analysis** is the identification and evaluation of existing and potential hazards and the recommended mitigation of the hazard sources found (ref NPR 8715.3D)

Safety Overview

- Safety, by its definition, is primarily addressing hazardous conditions that may cause personal injury, illness or death, damage to the environment, the product, or facilities.
- Safety analyses are top-down, staring from a top level hazard event such as fire, explosion, personal injury, toxicity, environment pollution, and trace down and link the top level hazard to product design details.
- Typical System Safety tasks include hazard analysis and Fault Tree Analysis.
- In general, probabilistic Risk Assessment (PRA), under the context of addressing an undesirable system hazard event, is also part of a safety analysis.

(I-A-R-A*)

SAFETY ENGINEERING SEAC



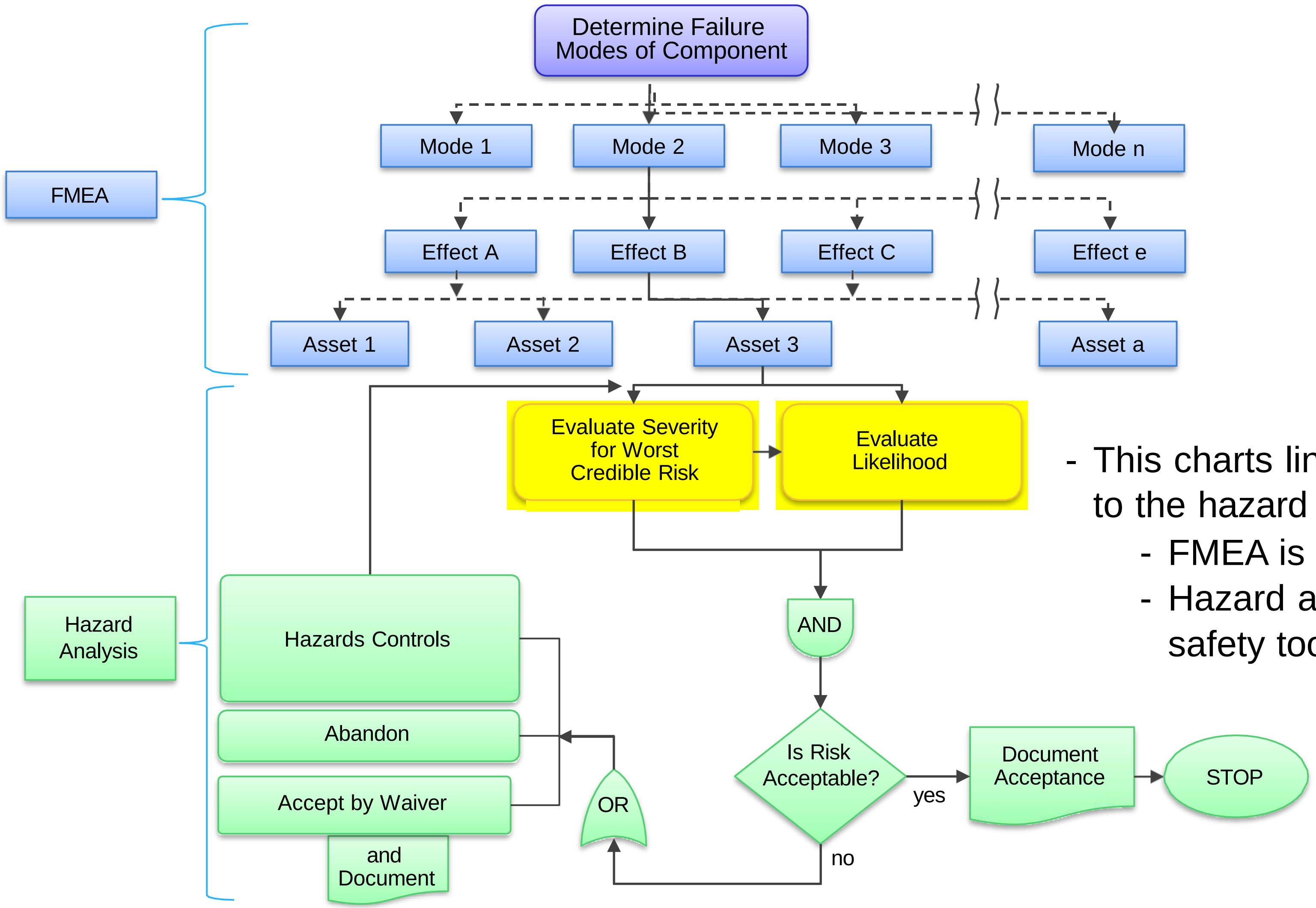
Reference: APT Safety Training Course

* I-A-R-A Identify, Assess, Reduce, Accept

Major Safety Techniques

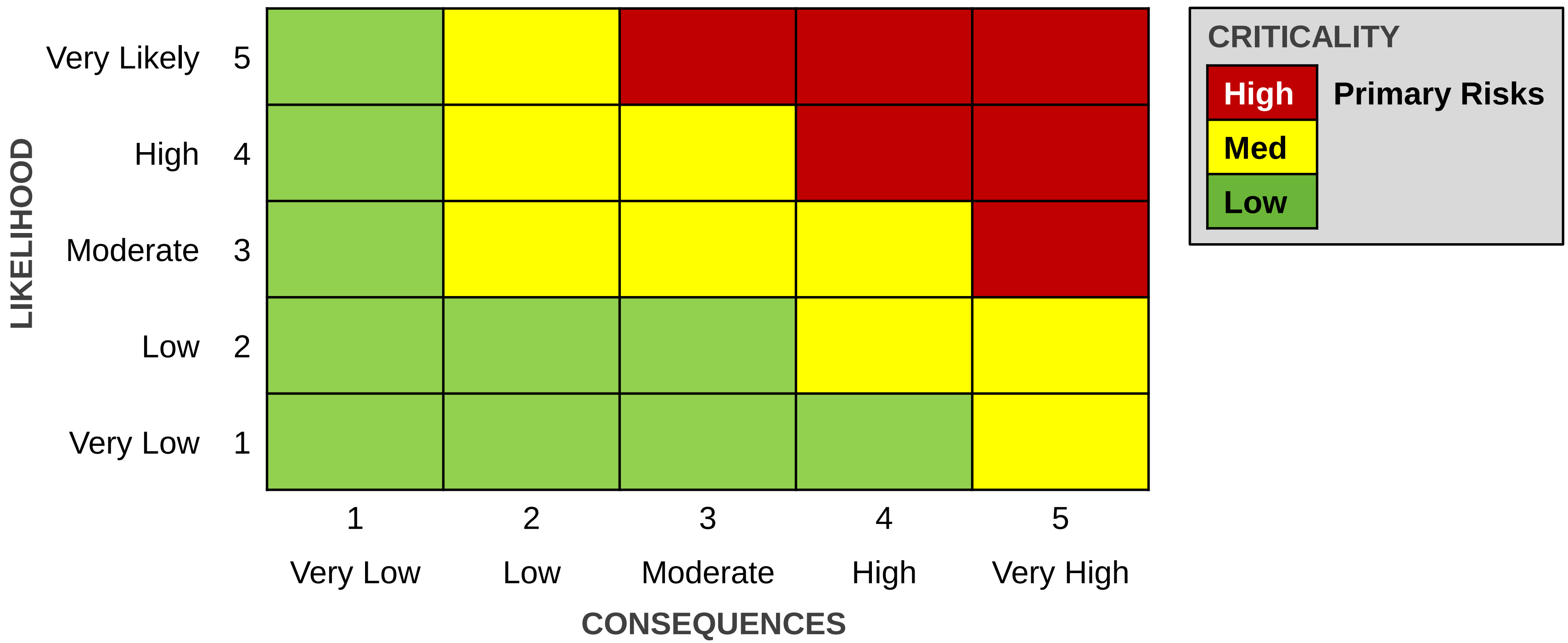
- Preliminary Hazard Analysis (PHA)
- Cause-Consequence Analysis
- Subsystem Hazard Analysis
- Operating and Support Hazard Analysis
- Occupational Health Hazard Analysis
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Probabilistic Risk Assessment (PRA)
- Human Reliability Analysis – Operator Error
- Sneak Circuit Analysis
- Others…

The Reliability and Safety Link



- This charts links the FMEA to the hazard analysis.
  - FMEA is a reliability tool
  - Hazard analysis is a safety tools

5×5 Risk Matrix



NOTE: Specific criteria for each of the likelihood and consequence categories are to be defined by each enterprise or program. Criteria may be different for manned missions, expendable launch vehicle missions, robotic missions, etc.

Safety Interface with Other Disciplines

System safety requires the support of and interaction with the other assurance functions

SYSTEM SAFETY
Hazard detection & mitigation

RELIABILITY
Hazard Causes
Probability Analyses

QUALITY
Process Controls
Verification Activities

Reliability and Safety Uniqueness

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

	Reliability	Safety
Roles	To ensure and assure product function achievability	To ensure and assure the product and environment are safe and hazards free by eliminating or controlling the hazards.
Requirements	Closed ended, design function specific within the function boundary. Internally imposed	Non-function specific such as “no fire”, “no harm to human being”.
Approaches	Bottom-up and start from the component or system designs at hand	Traces 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 address

PROBABILISTIC RISK ASSESSMENT (PRA)

SAFETY ENGINEERING
SEAC
& ANALYSIS CENTER

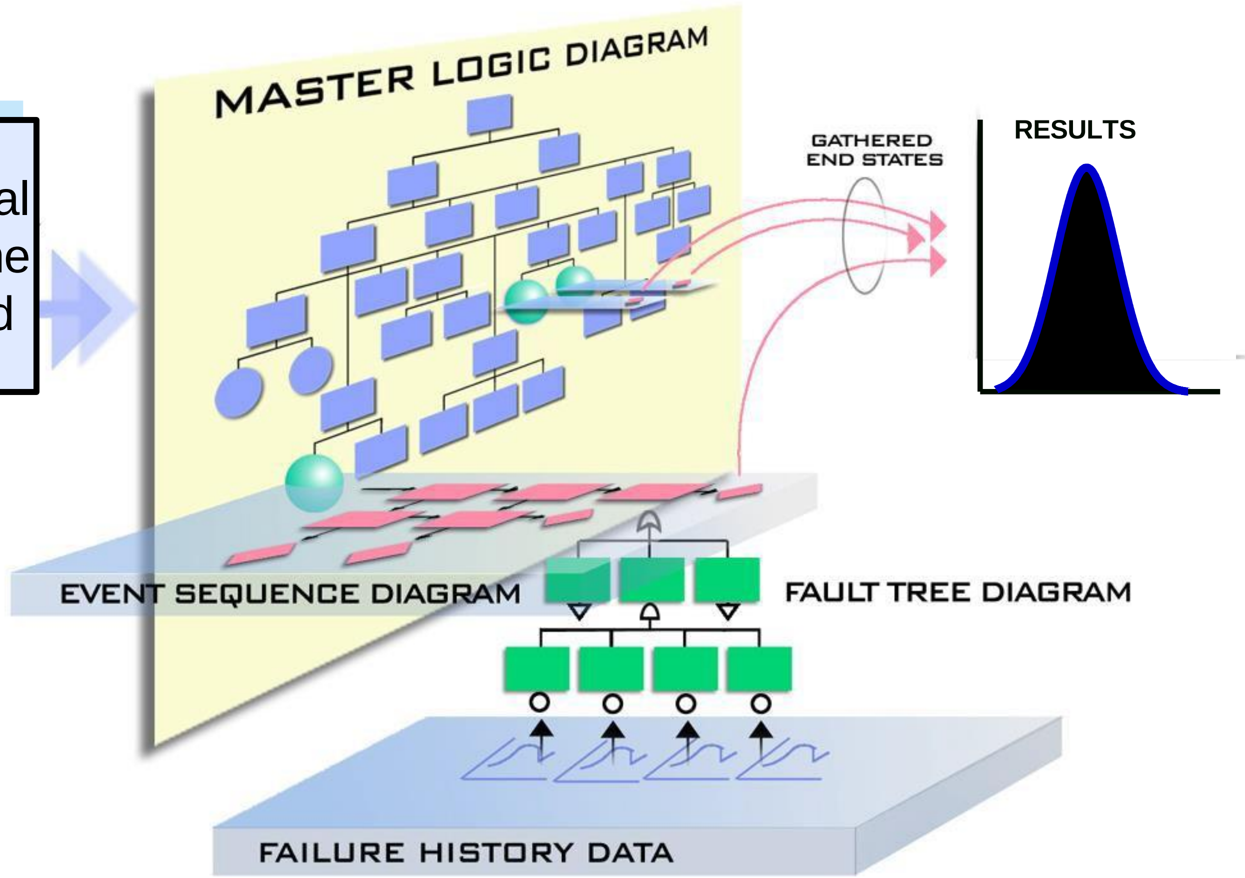
Safety Engineering and Analysis Center
A Division of A-P-T Research, Inc.
4950 Research Drive, Huntsville, AL 35805
256.327.3373 | www.apt-research.com

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 (Risk uncertainty distribution – Probabilities)?
  - What is the severity of the degradation (consequences)?

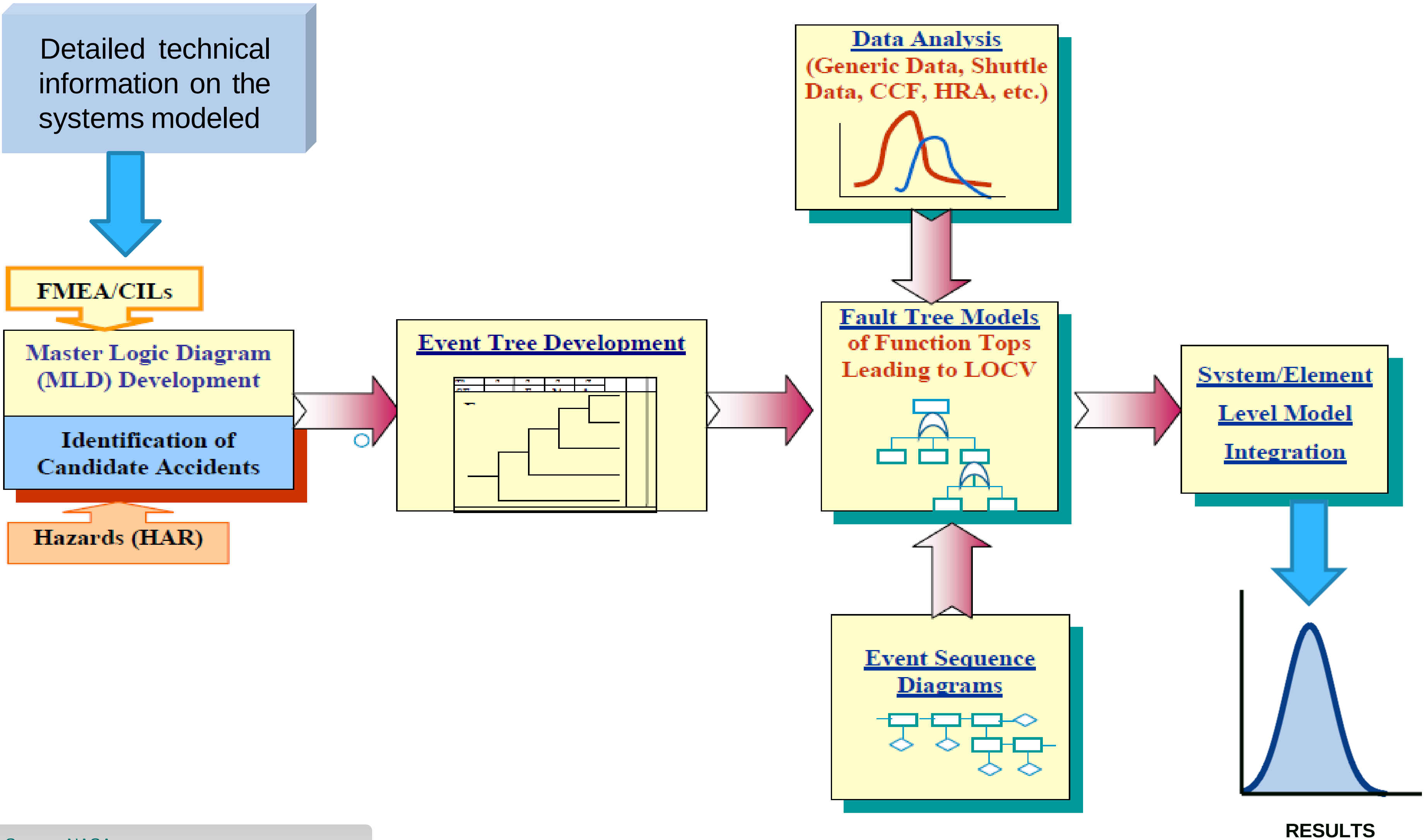
Notional PRA Process

Detailed technical information on the systems modeled



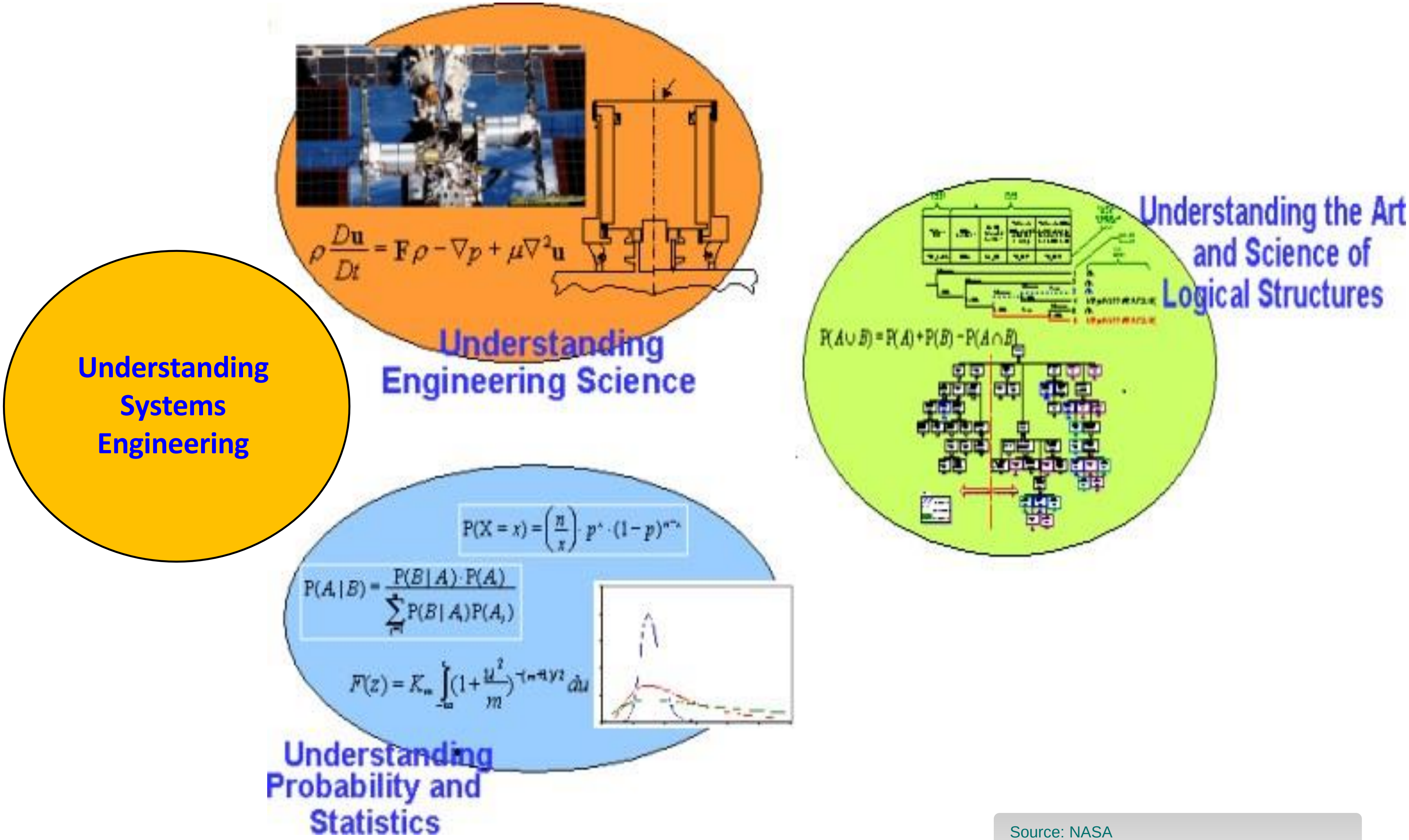
Source: NASA

A PRA Process Example



Source: NASA

The PRA Skills Needed



Source: NASA

The Knowledge Needed

- Specific areas you need to have knowledge of (as a minimum) are:
  - Probability and statistics
  - Master Logic Diagram (MLD)
  - Event Trees (ETs)
  - Fault Trees (FTs)
  - Event Sequence Diagrams (ESDs)
  - Bayesian Analysis
  - Common cause Failure Analysis
  - Human Reliability Analysis (HRA)

History of PRA
Early PRA Development

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- In late fifties / early sixties Boeing and Bell Labs developed Fault Trees to evaluate launch systems for nuclear weapons.
- Nuclear Power industry picked up the technology in early seventies and created WASH-1400 (Reactor Safety Study) in mid seventies.
- This is considered the first modern PRA. It was shelved until Three Mile Island (TMI) incident happened in 1979.
- It was determined that the WASH-1400 study gave insights into the incident that could not be easily gained by any other means.
- PRA is now practiced by all commercial nuclear plants in the United States and a large amount of data, methodology, and documentation for PRA technology has been developed by the industry and the Nuclear Regulatory Commission (NRC).
- All new nuclear plants must license their plants based on PRA.
- NASA experimented with Fault Trees and some early attempts to do PRAs in the sixties but then abandoned quantitative risk assessment
- Throughout the Apollo Program and until the Challenger Accident, NASA relied heavily on worst-case Failure Modes and Effects Analysis (FMEA) and Hazard Analysis for reliability and safety assessments
- In 1986, right after Changer accident, NASA started using PRA heavily to assess the risk of Loss of Mission (LOM) and Loss of Crew (LOC)

PRA History
Selected Major Accidents

1970 | 1980 | 1990 | 2000 | 2020

1967 Apollo Fire

"We can solve those problems we think of."
- Apollo Accident Review Board (?)

1979 Three Mile Island

"The most fundamental lesson learned is one that must be continually emphasized, accidents can happen."
- Congressional Subcommittee on Three Mile island

1986 Challenger Disaster

"There are enormous differences of opinion as to the probability of failure…estimates range from 1/100 to 1/100,000"
- Presidential Commission on Challenger Disaster

2003 Columbia Disaster

The problem of "debris shedding" was well known but considered "acceptable" by management. – Rogers Commission Report

1984 Union Carbide toxic gas leak, Bhopal, India

1996 Long March Rocket Explosion, China

1986 Chernobyl Nuclear Power Plant, USSR

- The concept of applying quantitative risk-based concepts dates from 1662. However, it often takes centuries for a mathematical concept to become widely accepted.
- Major failures in the last several decades brought more attention to QRA/PRA, which provides an opportunity to improve the discipline but also dictate caution and use of lessons learned.

NASA PRA Studies and Documents (partial list)

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- Space Shuttle PRA for Galileo mission (PRC)
- Galileo PRA update (SAIC)
- Space Shuttle PRA (SAIC)
- Space Shuttle PRA – QRAS
- PRA for the International Space Station
- PRA studies in support of nuclear missions
- Completion of QRAS and its commercialization
- NASA Procedural Requirements for PRA
- PRA Procedures Guide for aerospace applications
- Fault tree handbook for aerospace applications
- Dynamic fault tree methodology and software
- PRA for conceptual design (Exploration Systems Architecture Studies (ESAS))
- Constellation Systems PRA
- NASA-SP-2009-569: Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis
- Space Launch System (SLS) PRA

Failure Types

- **Functional** – A functional failure event is generally defined as failure of a component type, such as a valve or pump, to perform its intended function. Functional failures are specified by a component type (e.g., motor pump) and by a failure mode for the component type (e.g., fails to start)
- **Phenomenological** – Phenomenological events include non-functional events that are not solely based on equipment performance but on complex interactions between systems and their environment or other external factors or events. Phenomenological events can cover a broad range of failure scenarios, including leaks of flammable/explosive fluids, engine burn through, over pressurization, ascent debris, structural failure, and other similar situations.
- **Human Error** – Human error is simply some human output that is outside the tolerances established by the system requirements in which the person operates. Example: Crew fails to isolate the leak after automatic isolation fails
- **Common Cause** – Common Cause Failures (CCFs) are multiple failures of similar components within a system that occur within a specified period of time due to a shared cause. Example : common cause failure of both pressure transducers
- **Software failure** – Example: controller program fails to generate isolation signal due to a software error

PRA Quantification

- PRA addresses:
  - what can go wrong;
  - How likely it is to occur (the probability);
  - What are the consequences; and
  - what is the uncertainty associated with the risk numbers.
- PRAs deal with low-probabilities requiring interpretation
  - Admissible evidence might be vague
  - How do we evaluate probabilities when there may be little empirical evidence?
  - Are expert opinions admissible?
  - How do we deal with new or one-of-a-kind systems?
- PRA uses the Bayesian interpretation of probabilities to deal with uncertainty.

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.
- The 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.

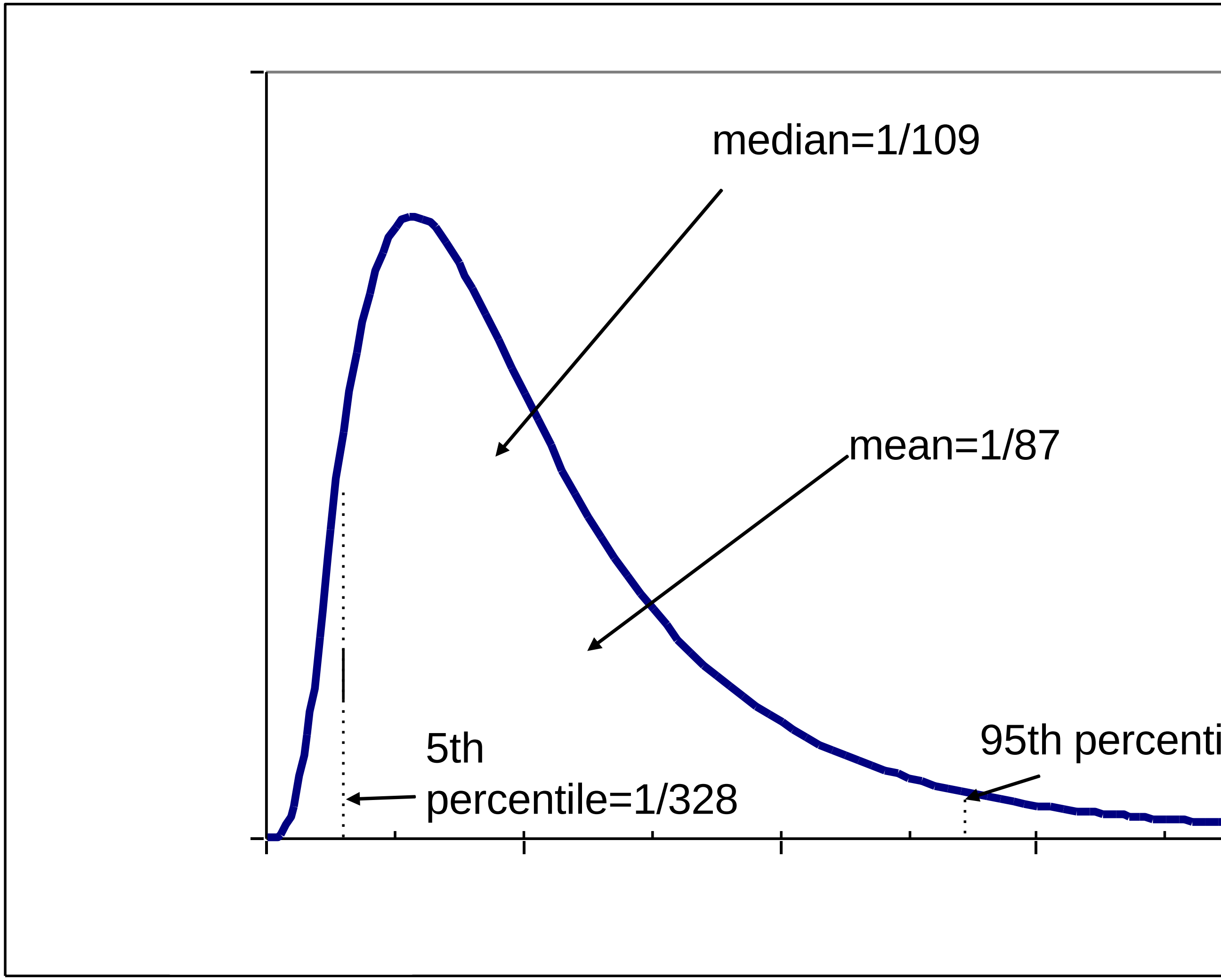
The Epistemic Uncertainty

- In Bayesian analysis, failure models such as exponential, binomial, etc., are called aleatory models.
- Most parameters of those models are themselves uncertain. We described 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., Poisson), 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

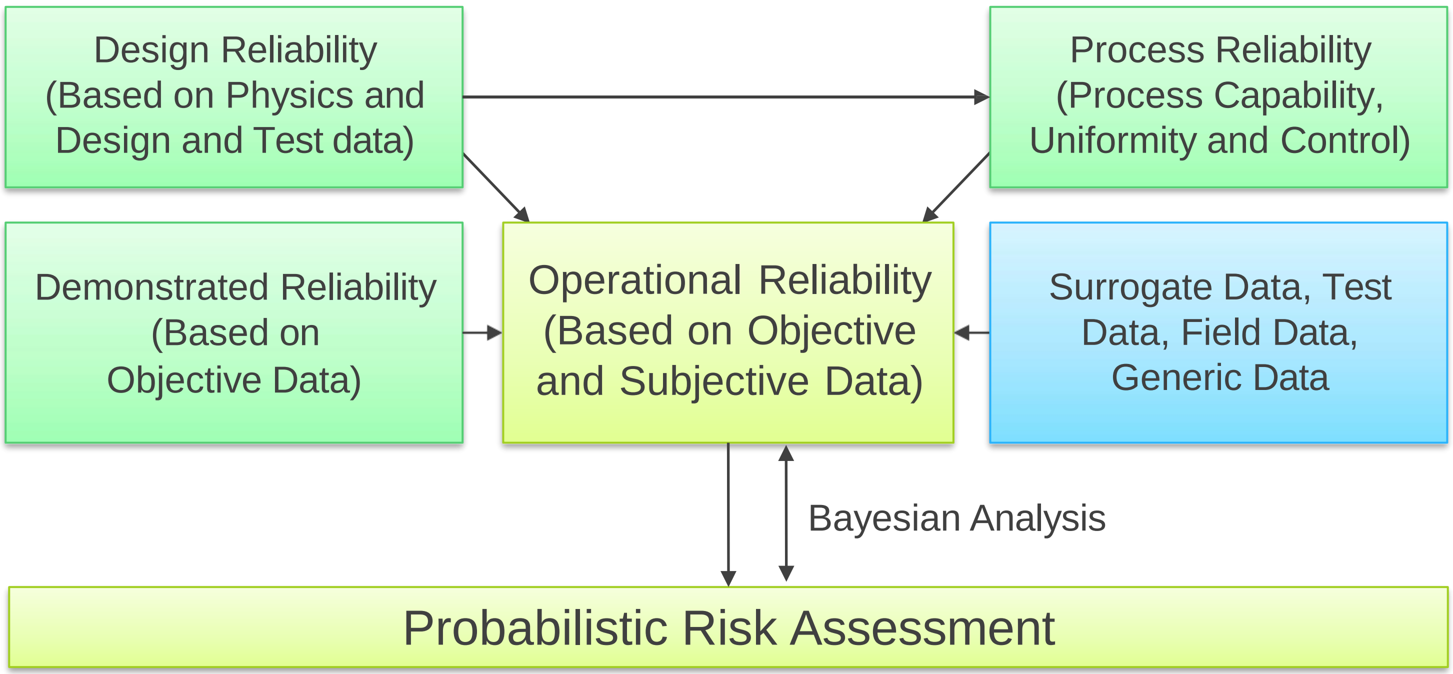
- The general Bayesian procedure is:
  - Begin with a probability model for the process of interest.
  - Specify a prior distribution for parameter(s) in this model, quantifying uncertainty, i.e., quantifying degree of belief about the possible parameter values.
  - Obtain observed data.
  - Determine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

A Typical Uncertainty Distribution



Modeling the uncertainty of complex systems requires the aggregation of uncertainties using stochastic methods. The most common way to address uncertainty is by using probability density functions

The Reliability - PRA Link



Reliability Prediction vs. PRA

Category	Reliability Prediction	PRA
Use	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	Loss of System Function, the Causes, and the 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) ➔ RBD's/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

Reliability Engineering VS PRA

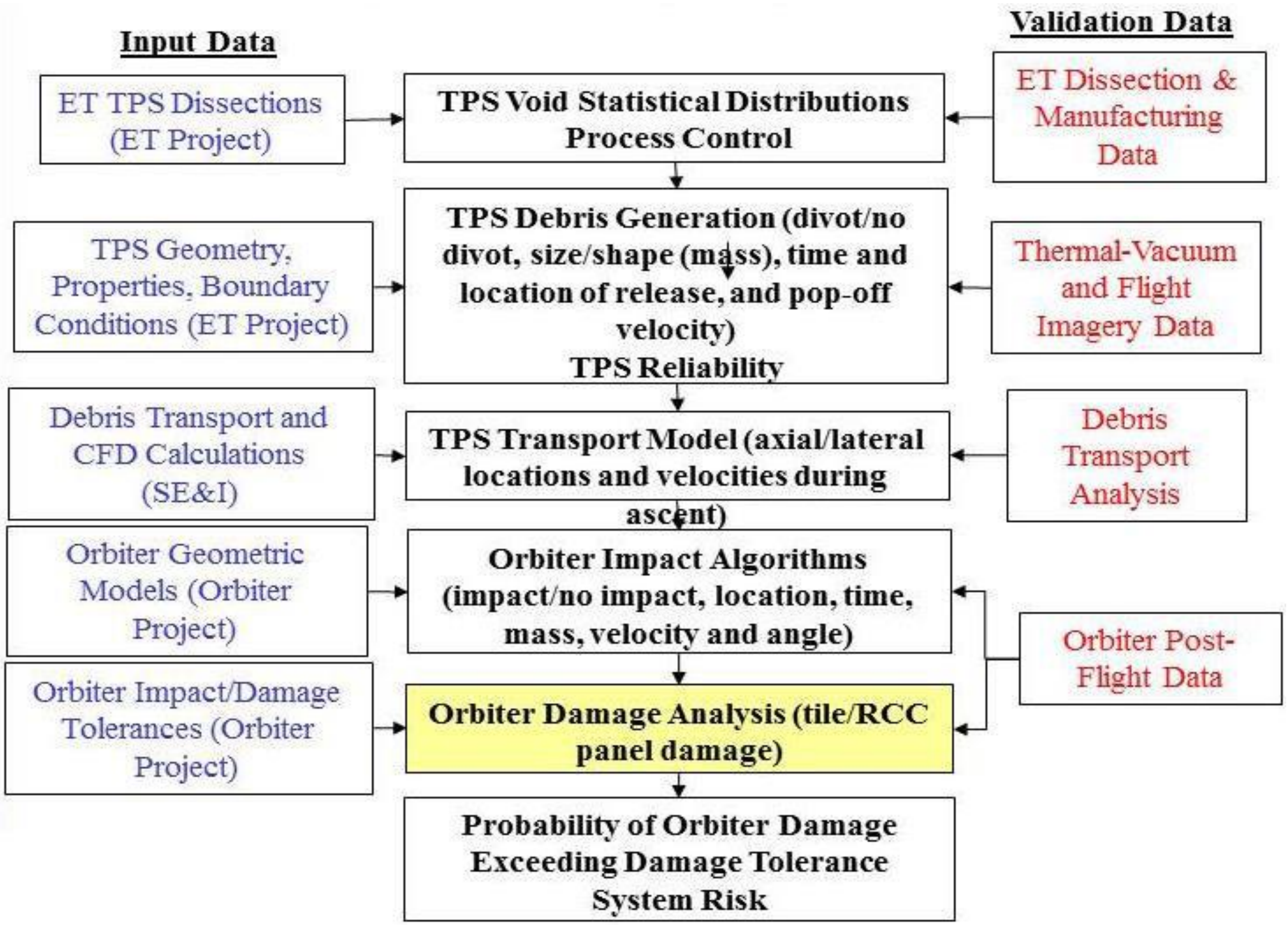
- Reliability engineering is a design function that deal with loss of function
- PRA is a process that deals with system risk scenarios that could lead to loss of mission or loss of crew
- PRA and reliability engineering are two different areas serving different functions in supporting the design and operation of launch vehicles; however, PRA as a risk assessment, and reliability as a metric could play together in a complimentary manner in assessing the risk and reliability of launch vehicles
- In general, reliability data is used as a critical data source for PRA

The Link Between Reliability, Safety and PRA

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

A good example of the linkage between reliability, safety, and PRA is the Space Shuttle External Tank (ET) Thermal Protection System (TPS) safety assessment shown in the next chart using a probabilistic risk assessment process to assess the risk of foam debris (reliability) hitting the Orbiter and leading to a loss of crew (Safety).

The Link Between Reliability, Safety and PRA



The Link Between Reliability, Safety and PRA

SAFETY ENGINEERING SEAC & ANALYSIS CENTER

- In summary, Reliability, Safety and PRA are three different areas serving different functions in supporting system design and system operational process. However, the tools and techniques in these different areas, in many cases, play together in a complementary manner.
- Reliability prediction is a critical input to PRA.
- PRA is part of and a critical input to safety.