Reliability and Probabilistic Risk Assessment - How They Play Together

Annual Reliability and Maintainability Symposium 2014

Palm Harbor, FL

January 26-29, 2015

Fayssal M. Safie, Ph. D.

NASA R&M Tech Fellow/Marshall Space Flight Center

Richard Stutts

NASA R&M Tech Discipline Lead/NASA Safety Center

Zhaofeng Huang, Ph.D.

Aerojet Rocketdyne, Technical Fellow

Agenda

- **Objective**
- **Probabilistic Risk Assessment (PRA)**
  - What Is It?
  - How Does it Works?
  - What Have We Done?
- **Reliability Engineering**
  - – The Reliability Engineering Case
  - – The Reliability Metric
- **The Link between PRA and Reliability**
- **Concluding Remarks**

Objective

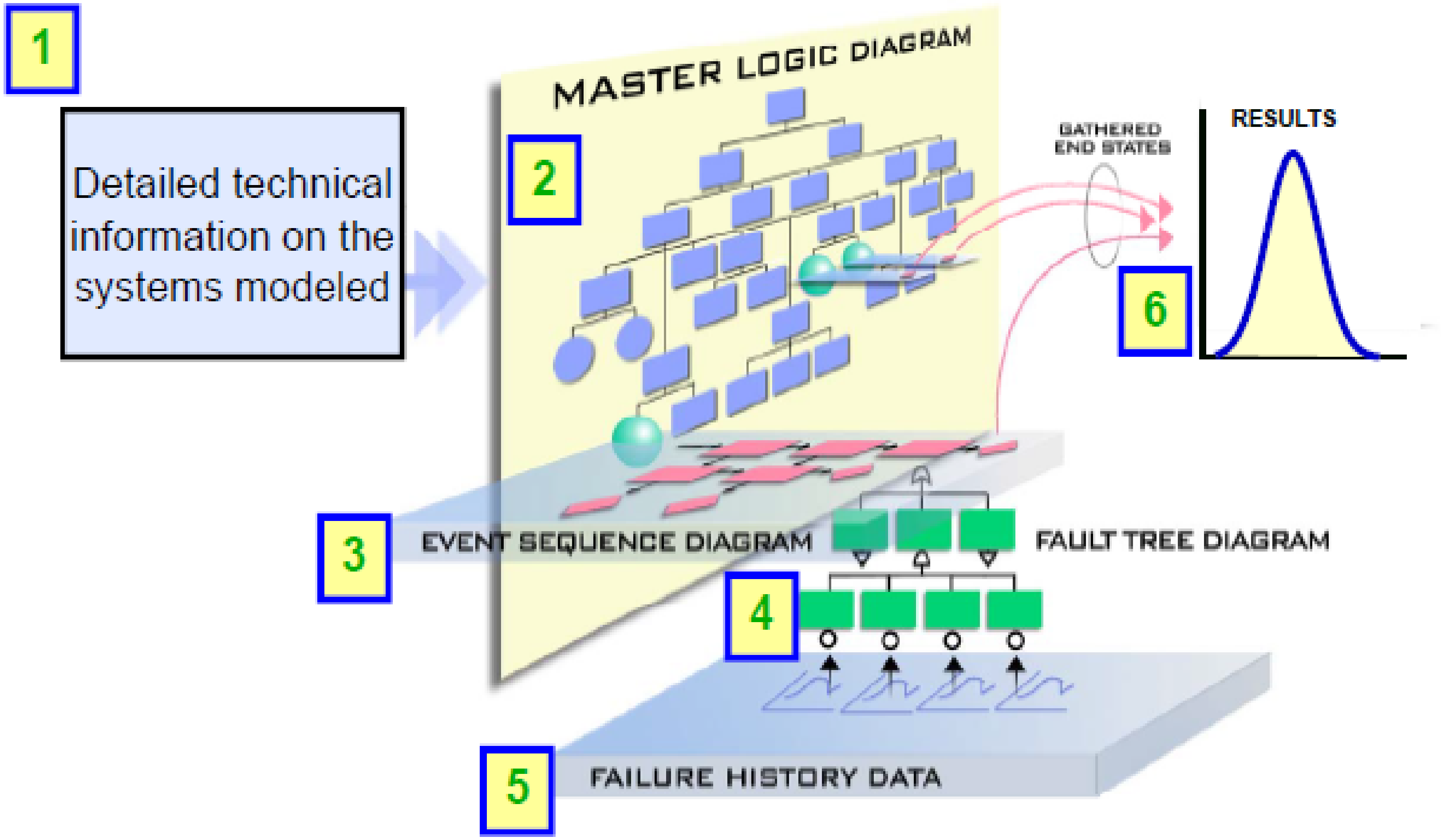
The objective of this presentation is to discuss the PRA process and the reliability engineering discipline, their differences and similarities, and how they are used as complimentary analyses to support design and flight decisions.

Probabilistic Risk Assessment (PRA) *What Is It?*

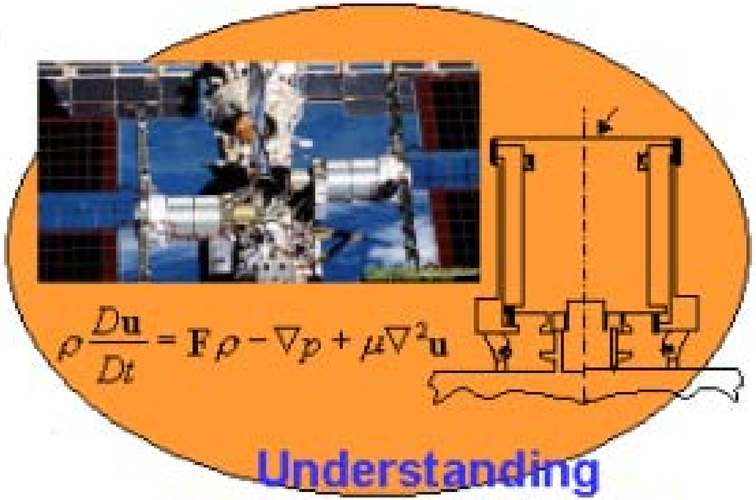
- ***PRA* is a systematic process designed to answer three basic questions:**
  - **What can go wrong that would lead to loss or degraded performance?**
  - **How likely is it?**
  - **What is the severity?**
- **In a PRA process, risk assessment is the task of generating the triplet set: $R \equiv RISK \equiv \{\langle S_i, P_i, C_i \rangle\}$ Where, S is the scenario, P is the likelihood of the scenario, and C is the consequence of the scenario respectively**

Probabilistic Risk Assessment (PRA)
How Does It Works?

The following are the major steps in a PRA process

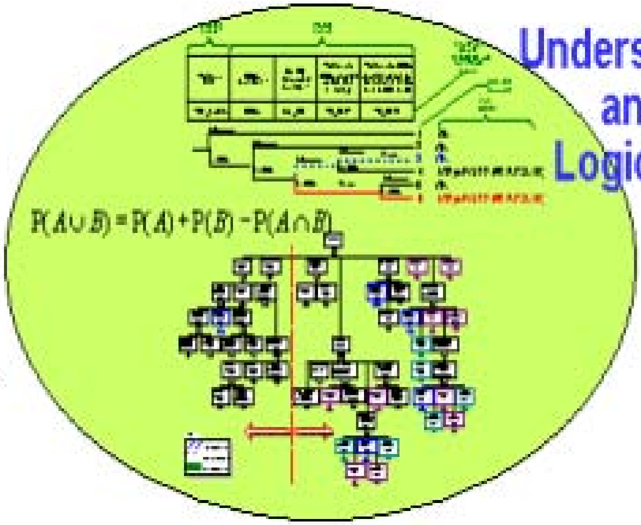


Probabilistic Risk Assessment (PRA) The Skills Needed



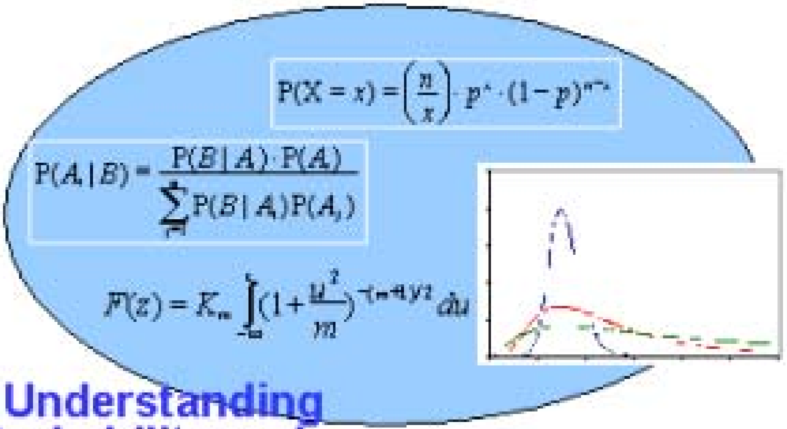
$$\rho \frac{D\mathbf{u}}{Dt} = \mathbf{F}\rho - \nabla p + \mu \nabla^2 \mathbf{u}$$

Understanding Engineering Science



$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Understanding the Art and Science of Logical Structures



$$P(X = x) = \binom{n}{x} \cdot p^{x} \cdot (1-p)^{n-x}$$

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{\sum_{i=1}^{n} P(B|A_i)P(A_i)}$$

$$F(z) = K_m \int_{-\infty}^{z} (1+\frac{u^2}{m})^{-(m+1)/2} du$$

Understanding Probability and Statistics

What Have We Done?

- **Since 1986, NASA Headquarters has conducted several PRA studies:**
  - **Planning Research Corporation conducted the first of these studies in 1988**
  - **In 1995, Science Applications International Corporation (SAIC) conducted a comprehensive PRA study**
  - **In July 1996, NASA conducted a study to develop a model that provided the overall Space Shuttle risk and estimates of risk changes due to proposed Space Shuttle upgrades**
  - **After the Columbia accident, NASA conducted a PRA on the Shuttle External Tank (ET) foam. This study was used to understand the risk due to ET foam loss in flight**
  - **Most recently, a PRA for Ares I launch vehicle was performed in support of the Constellation program**

fms1

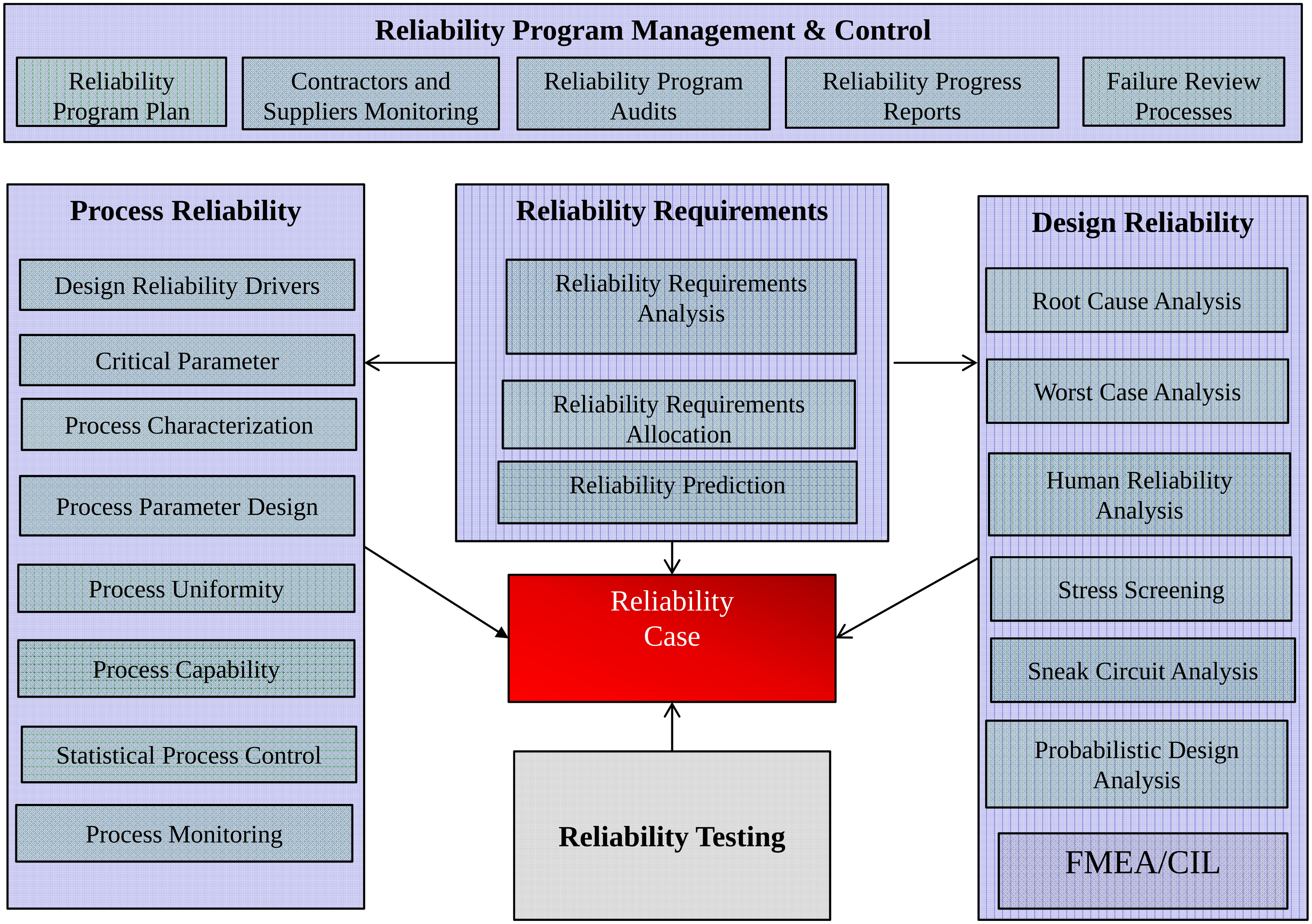
Reliability Engineering

- Reliability is a very broad design-support discipline. It has important interfaces with most engineering disciplines
- Reliability Engineering as a 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

Slide 8

fms1 fsafie, 11/12/2013

The Reliability Engineering Case



Reliability Program Management & Control

- Reliability Program Plan
- Contractors and Suppliers Monitoring
- Reliability Program Audits
- Reliability Progress Reports
- Failure Review Processes

Process Reliability

- Design Reliability Drivers
- Critical Parameter
- Process Characterization
- Process Parameter Design
- Process Uniformity
- Process Capability
- Statistical Process Control
- Process Monitoring

Reliability Requirements

- Reliability Requirements Analysis
- Reliability Requirements Allocation
- Reliability Prediction

Reliability Case

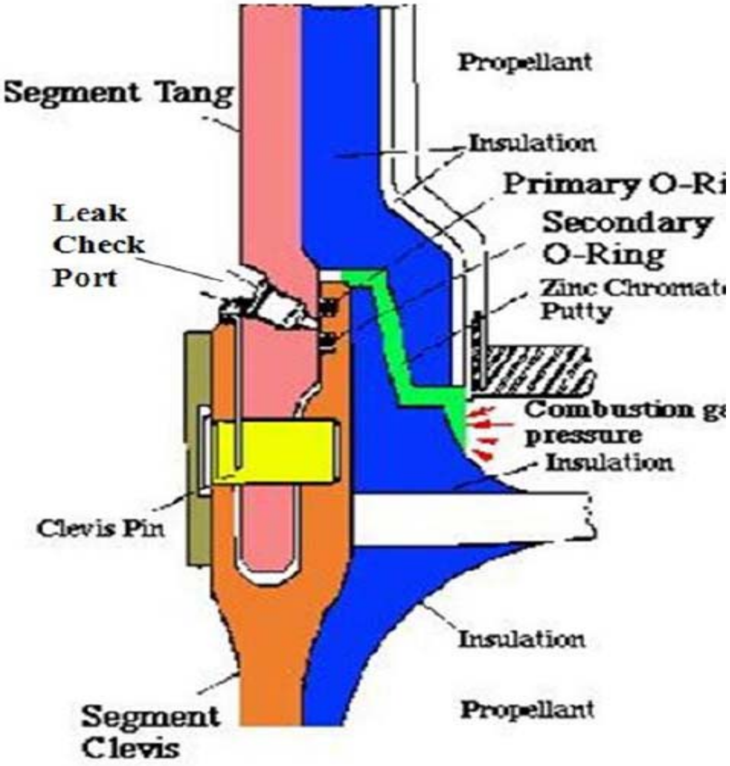
Reliability Testing

Design Reliability

- Root Cause Analysis
- Worst Case Analysis
- Human Reliability Analysis
- Stress Screening
- Sneak Circuit Analysis
- Probabilistic Design Analysis
- FMEA/CIL

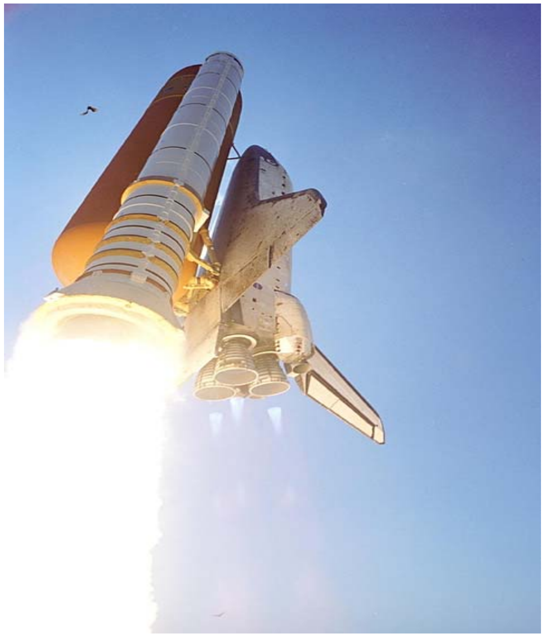
Design Reliability
The Challenger Case

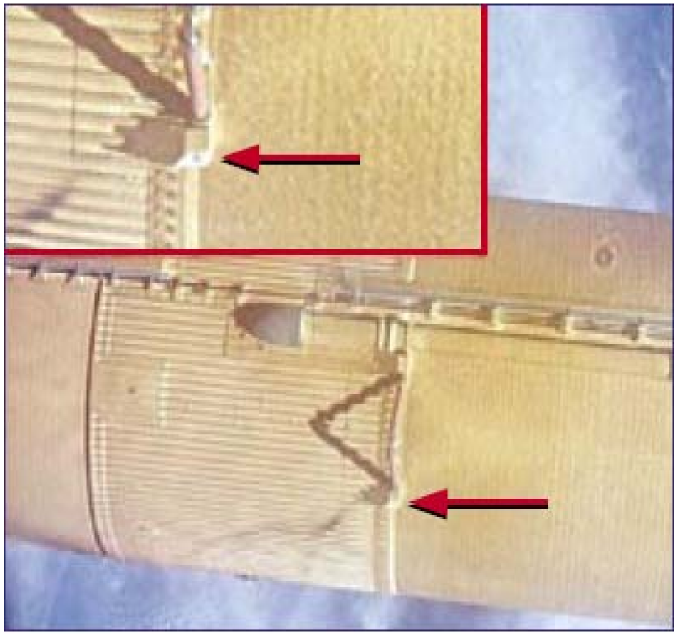
- **Causes and Contributing Factors**
  - The zinc chromate putty frequently failed and permitted the gas to erode the primary O-rings.
  - The particular material used in the manufacture of the shuttle O-rings was the wrong material to use at low temperatures.
  - Elastomers become brittle at low temperatures.



Process Reliability
The Columbia Case

- **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





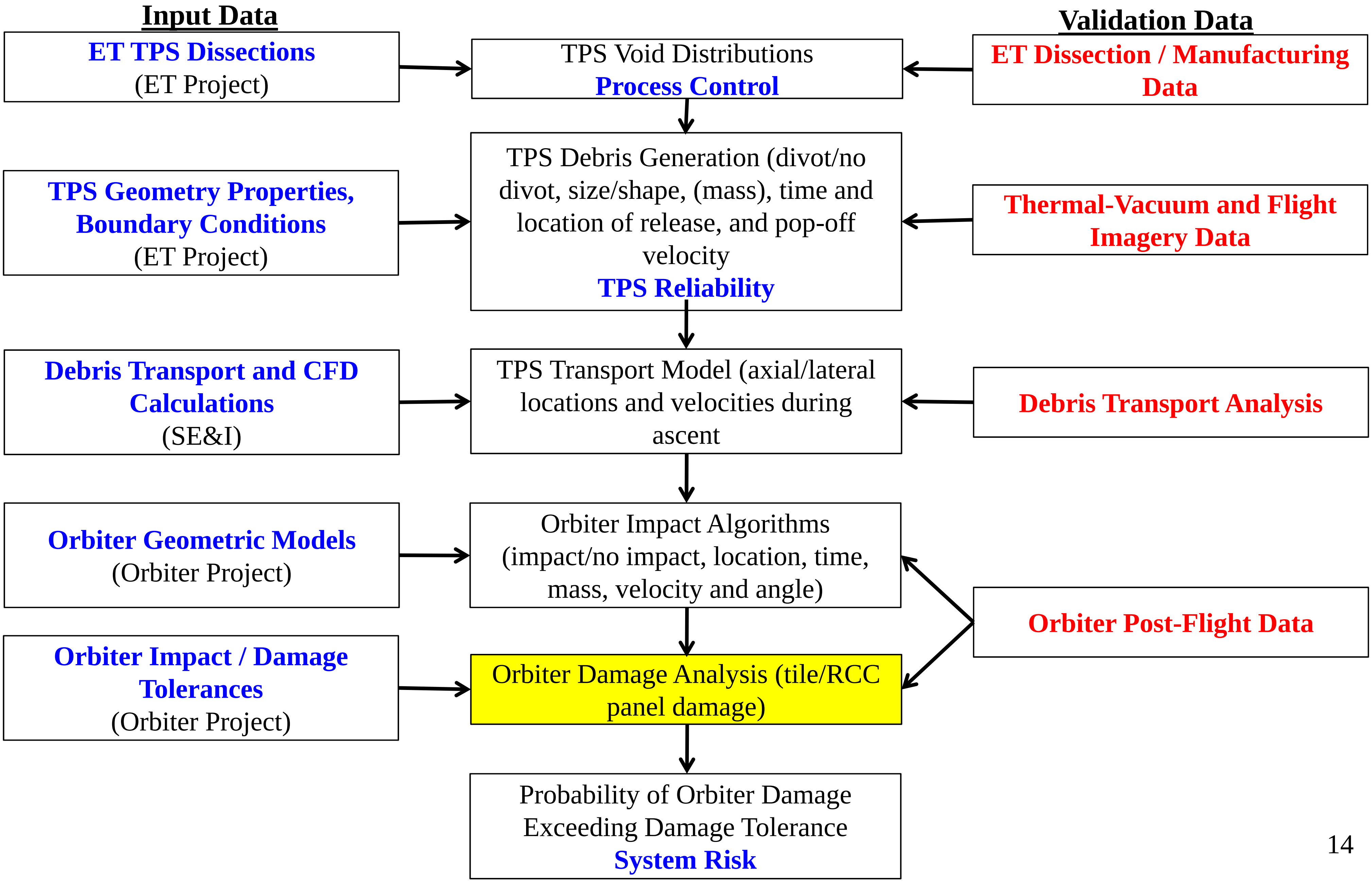
Reliability Predictions

- **The process of quantitatively estimating the reliability of a system using both objective and subjective data**
- **Performed to the lowest level for which data is available. The sub-level reliabilities are then combined to derive the system level prediction**
- **The techniques are dependent on the degree of the design definition and the availability of historical data. Examples are Techniques are:**
  - Similarity analysis
  - Physics-based
  - Techniques that utilize generic failure rates such as MIL-HDBK 217, Reliability Prediction of Electronic Equipment

Reliability Demonstration

- The process of quantitatively estimating the reliability of a system using objective data at the level intended for demonstration
- Statistical formulas are used to calculate the demonstrated reliability at some confidence level
- Models and techniques used in reliability demonstration include Binomial, Exponential, Weibull models, etc.
- Due to high cost and schedule impact of reliability demonstration, programs employed this method only to demonstrate a certain reliability comfort level. For example, a reliability goal of .99 at 95% confidence level is demonstrated by conducting 298 successful tests

The Link between PRA and Reliability
The ET Foam Probabilistic Risk Assessment



Input Data

ET TPS Dissections
(ET Project)

TPS Geometry Properties, Boundary Conditions
(ET Project)

Debris Transport and CFD Calculations
(SE&I)

Orbiter Geometric Models
(Orbiter Project)

Orbiter Impact / Damage Tolerances
(Orbiter Project)

TPS Void Distributions
Process Control

TPS Debris Generation (divot/no divot, size/shape, (mass), time and location of release, and pop-off velocity
TPS Reliability

TPS Transport Model (axial/lateral locations and velocities during ascent

Orbiter Impact Algorithms (impact/no impact, location, time, mass, velocity and angle)

Orbiter Damage Analysis (tile/RCC panel damage)

Probability of Orbiter Damage Exceeding Damage Tolerance
System Risk

Validation Data

ET Dissection / Manufacturing Data

Thermal-Vacuum and Flight Imagery Data

Debris Transport Analysis

Orbiter Post-Flight Data

Concluding Remarks

- **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**