A-P-T RESEARCH, INC.
AN EMPLOYEE-OWNED COMPANY

ADDRESSING UNIQUENESS AND UNISON OF RELIABILITY AND SAFETY FOR BETTER INTEGRATION

Fayssal M. Safie, PhD, A-P-T Research, Inc., Huntsville, Alabama

ISSS/SRE Monthly Meeting, September 11, 2018

AGENDA

- Definitions
- Reliability Engineering
- Safety Engineering
- Safety and Reliability Integration – Case Studies
- Safety and Reliability – Uniqueness
- Safety and Reliability – Unison
- Concluding Remarks

A-P-T RESEARCH, INC.

AN EMPLOYEE-OWNED COMPANY

RELIABILITY ENGINEERING

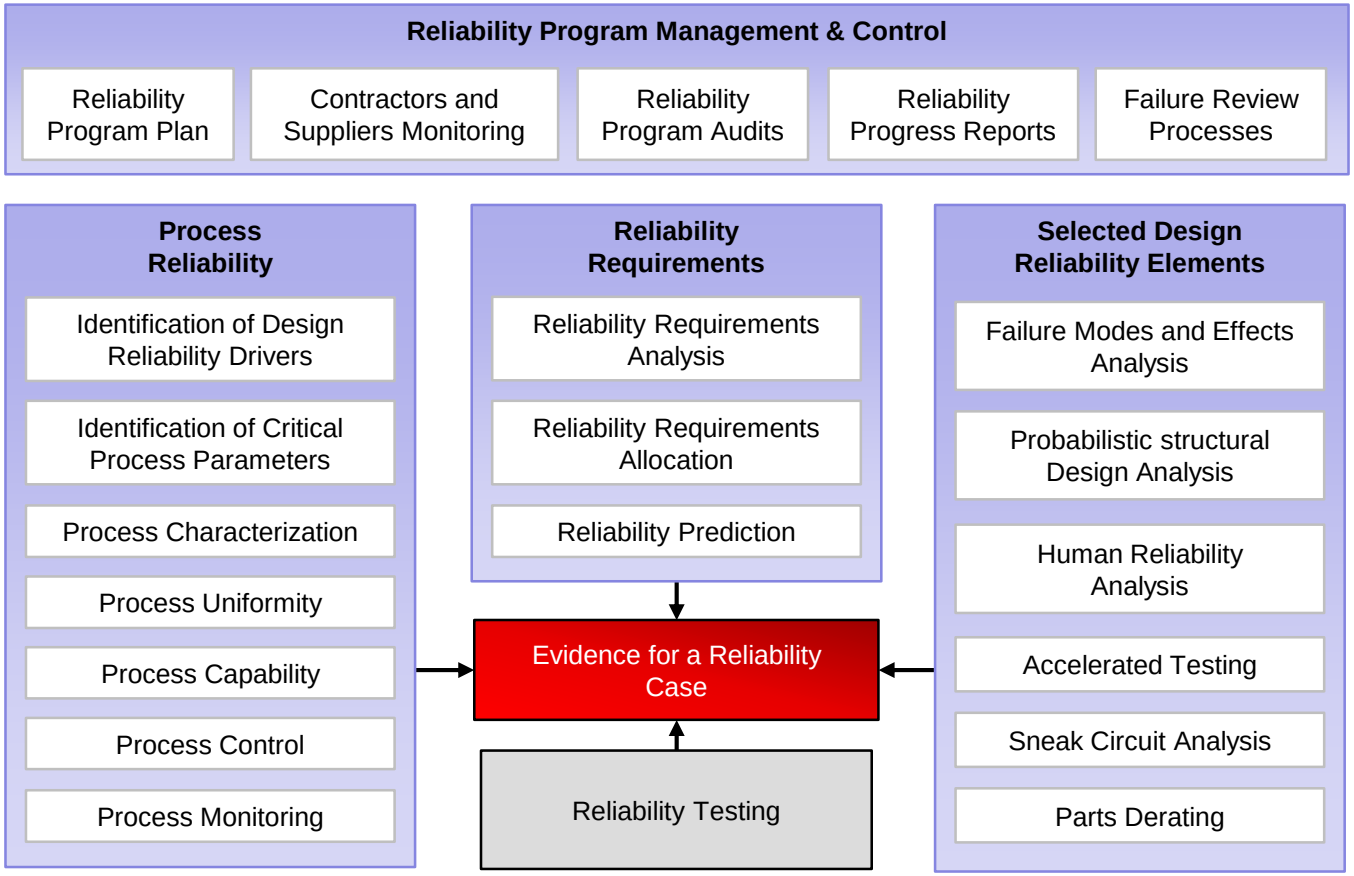
RELIABILITY RELATED DEFINITIONS

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

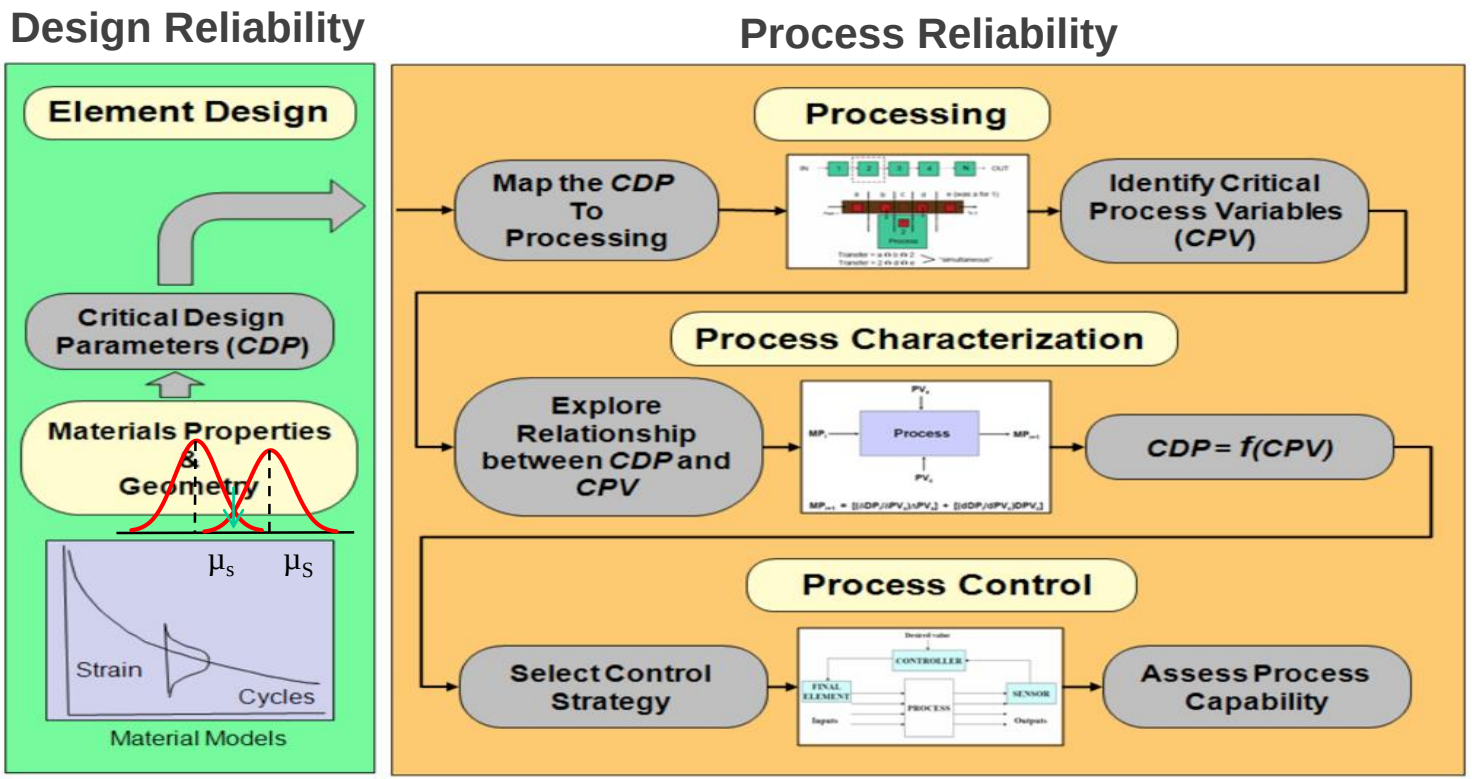
Reliability Engineering

MAJOR PROGRAM ELEMENTS

- The reliability community is exploring objective driven requirements and an evidence-based approach – a reliability case approach.
- A reliability case approach is a structured way of showing the work done on a reliability program by building arguments and showing the evidence.



DESIGN IT RIGHT AND BUILD IT RIGHT



- The chart shows that critical design parameters (on the left) are mapped in the process (on the right). The result is a set of critical process variables which are assessed for process capability, process uniformity, and process control.
- The design part is mainly driven by the loads and environment vs. capability.
- The process part is driven by process capability, process uniformity, and process control.

MAJOR RELIABILITY TECHNIQUES

- Reliability Allocation
- Reliability Prediction
- Reliability Demonstration
- Reliability Growth
- Accelerated Testing
- Parts Derating
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Probabilistic Risk Assessment (PRA)
- Human Reliability Analysis
- Sneak Circuit Analysis
- Others

RELIABILITY INTERFACE WITH OTHER DISCIPLINES

- Reliability engineering has important interfaces with and input to:
  - Design engineering
  - Risk assessment
  - Risk management
  - System safety
  - Quality engineering
  - Maintainability
  - Supportability engineering, and sustainment cost.

A-P-T RESEARCH, INC.

AN EMPLOYEE-OWNED COMPANY

SAFETY ENGINEERING

SAFETY RELATED DEFINITIONS

- **Safety** is the freedom from those conditions that can cause death, injury, occupational illness, damage to the environment, or 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 determination of potential sources of danger and recommended resolutions in a timely manner for those conditions found in either the hardware/software systems, the person-machine relationship, or both, which cause loss of personnel capability, loss of system, or loss of life.
- **Probabilistic Risk Assessment (PRA)** is the systematic process of analyzing a system, a process, or an activity to answer three basic questions: What can go wrong that would lead to loss or degraded performance; how likely is it (probabilities); and what is the severity of the degradation (consequences).

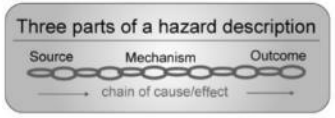
GENERIC SYSTEM SAFETY PROCESS (I-A-R-A)

Element 1
Program Initiation
- Plans
- Authorizations
- Contract(s)
- Team
- Tools

Element 2

Hazard Identification and Tracking

1) Process: The initial step produces a complete definition of the hazards associated with the system. This can be achieved by a variety of methods. Key elements of the risk assessment matrix are also defined.



Identify Hazards → Hazard Tracking

2) Methods:
- Checklists
- System Energy Source Inventory
- Prior Work with Similar Systems
- Operating Scenario Walkthroughs
- Operational Phase Review
- Codes/Standards/Regulations

Includes:
- Description
- Assessed Risk
- Potential and Selected Countermeasures
- Accident Experience
- Lessons Learned

3) Products: PHL, HTS

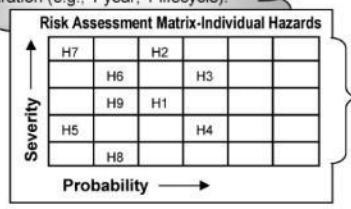
Understanding of Hazards

Element 3

Risk Assessment

1) Process: For each identified hazard the severity and likelihood are established. The Risk Assessment Matrix is used to assess and display the risk.

The matrix defines the "risk space" for a single-system and a declared exposure duration (e.g., 1 year, 1 lifecycle).



Assess risks of hazards → Reduction Not Needed / Reduction Needed

2) Assessment Methods:
- Expert Judgment
  - Historical Risk Experience
  - System Knowledge
  - Engineering Judgment
  - What is Known/not Known
- Numerical Analysis
- Computer Models

Assessment Approaches: FMEA, FTA, Event Trees ..., Others

3) Products: PHA, O&SHA, SSHA, SHA ..., Others

Understanding of Risk Drivers

Iterative

Changes to Reduce Risk

Lifecycle Monitoring

Element 5

Risk Acceptance

1) Process: Properly designated decision-makers are provided sufficient information to make an informed decision concerning the acceptability of residual risk. All decisions are to be documented.

Residual Risk → Risk Acceptance Decision → Other Action(s)

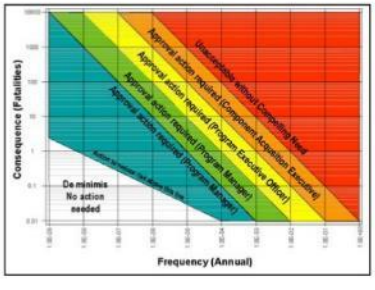
Accept

- Further Reduce
- Deny Approval
- Forward to Higher Authority

How Safe is Safe Enough?

2) Methods:
1) Compare to Consensus Standards for
   a) Protection of Personnel
   b) Societal Risk
2) Balance Risk with Needs

Example Consensus Standard for Risk Acceptability



3) Product: Documented Risk-Based Decision — Decision Document

Understand Options to Reduce

Element 4

Risk Reduction

1) Process: Risk Reductions are achieved by understanding the risk, countermeasuring the risk according to an order of precedence, and reassessing risks.

Understand Risk Drivers → Develop Candidate Countermeasures → Select Countermeasures → Re-Assess and Accumulate Risks

2) Methods:

Understanding risk causation can lead to prioritizing hazard reductions and/or direct countermeasure selection.

Countermeasure Order of Precedence:
1) *Design Changes*
2) *Engineered Safety Features*
3) *Safety Devices*
4) *Warning Devices*
5) *Procedures/Training*

Countermeasures shouldn't:
1) Introduce new hazards
2) Unacceptably Impair system performance

Countermeasure Selection Criteria
- Cost (vs., accepting risk)
- Effectiveness (In reducing risk)
- Feasibility
  - Means
  - Schedule

- Accumulate total system risk by proper mathematical protocol
- Validate Risk Reductions

3) Products (typical): Hazard Reports, SAR ..., others

Protected under U.S. Copyright Laws; Copyright © 2005 A-P-T Research, Inc.

T-04-01100 Strawman 032305

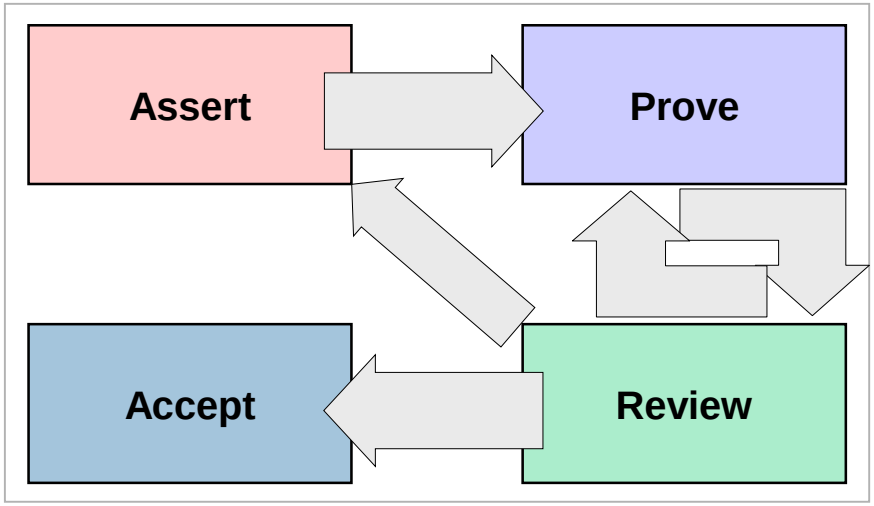
Reference: APT Safety Training Course

THE SAFETY CASE

- A safety case is a documented body of evidence that provides a convincing and valid argument that the system is safe. It Involves:
  - Making an explicit set of claims about the system(s)
    - E.g., probability of accident is low
  - Producing supporting evidence
    - E.g., operating history, redundancy in design
  - Providing a set of safety arguments that link claims to evidence

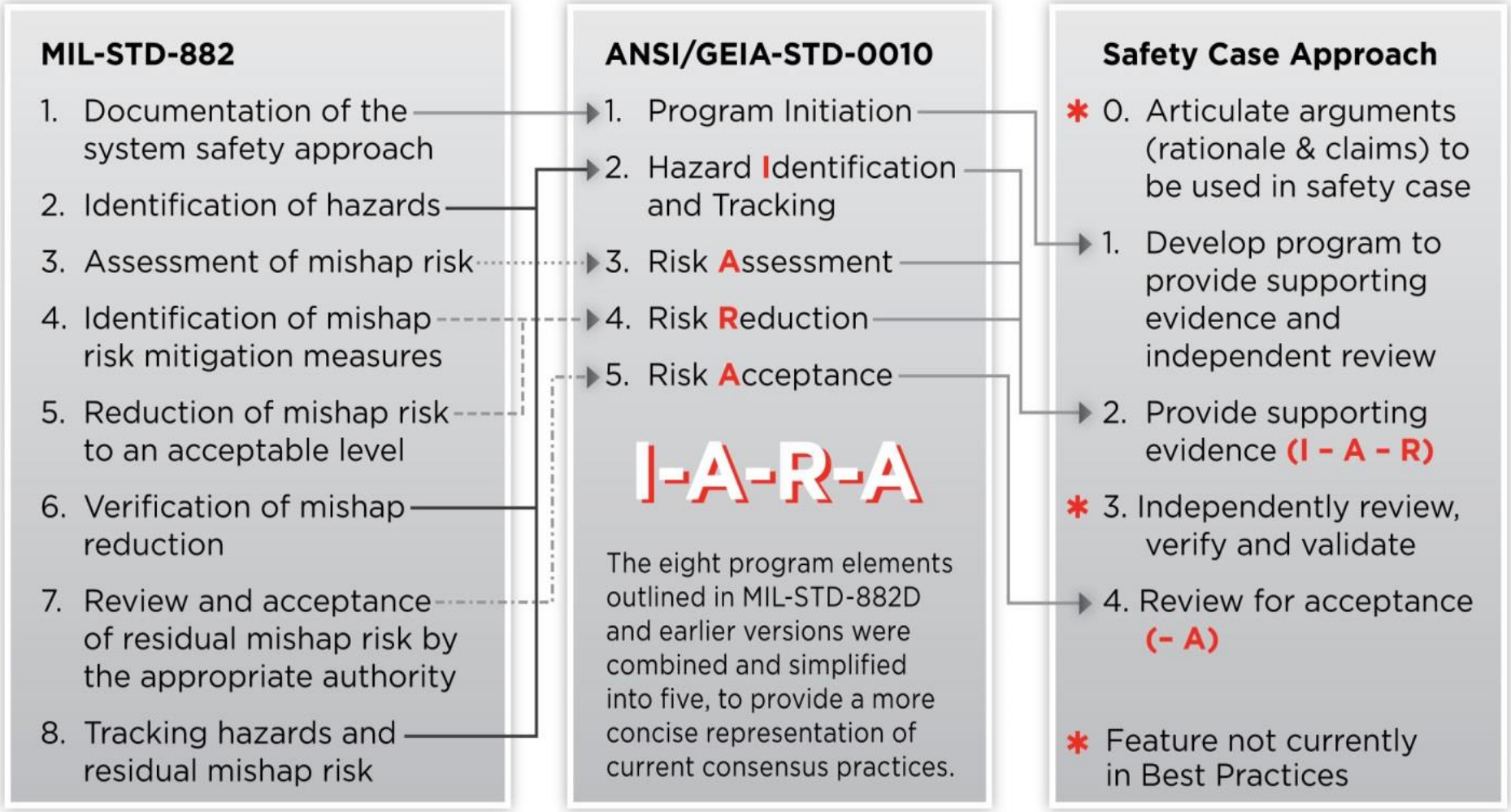
THE SAFETY CASE PROCESS

- Assert the case: This system is safe because it meets the following: (List requirements or claims which, if met, demonstrate the case that the system is adequately safe)
- Prove: Validate by demonstrations, tests, or analysis that each claim is met.
- Review: Independent reviewers examine the logical, legal, and scientific basis on which the validation is based. They then develop findings as to the adequacy of the validation.
- Accept: A properly designated decision authority then reviews the case, proofs, and finding of the reviewers, and makes an informed decision for acceptance of the risk or rejection.



Reference: APT safety course

COMPARISON OF EXISTING ANSI/GEIA-STD-0010, MIL-STD-882 TECHNIQUES AND THE SAFETY CASE



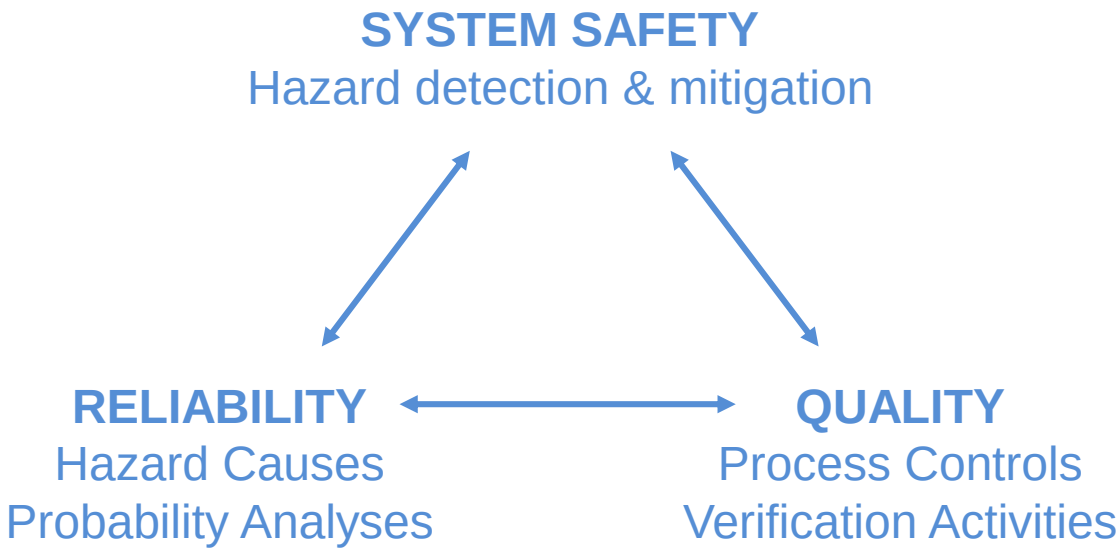
Reference: APT Safety Case

MAJOR SAFETY TECHNIQUES

- Hazard Analysis (PHA, SHA, etc.)
- 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…

SAFETY INTERFACE WITH OTHER DISCIPLINES

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



NOTE: In system safety engineering, the emphasis is on hazard identification and safety risk reduction activities. Other program elements have primary responsibility for determining schedule and cost factors. The project management has the ultimate responsibility for balancing the different factors that drive program development.

A-P-T RESEARCH, INC.

AN EMPLOYEE-OWNED COMPANY

SAFETY AND RELIABILITY INTEGRATION CASES TOOLS, TECHNIQUES, AND ANALYSIS

FMEA - Hazard Analysis

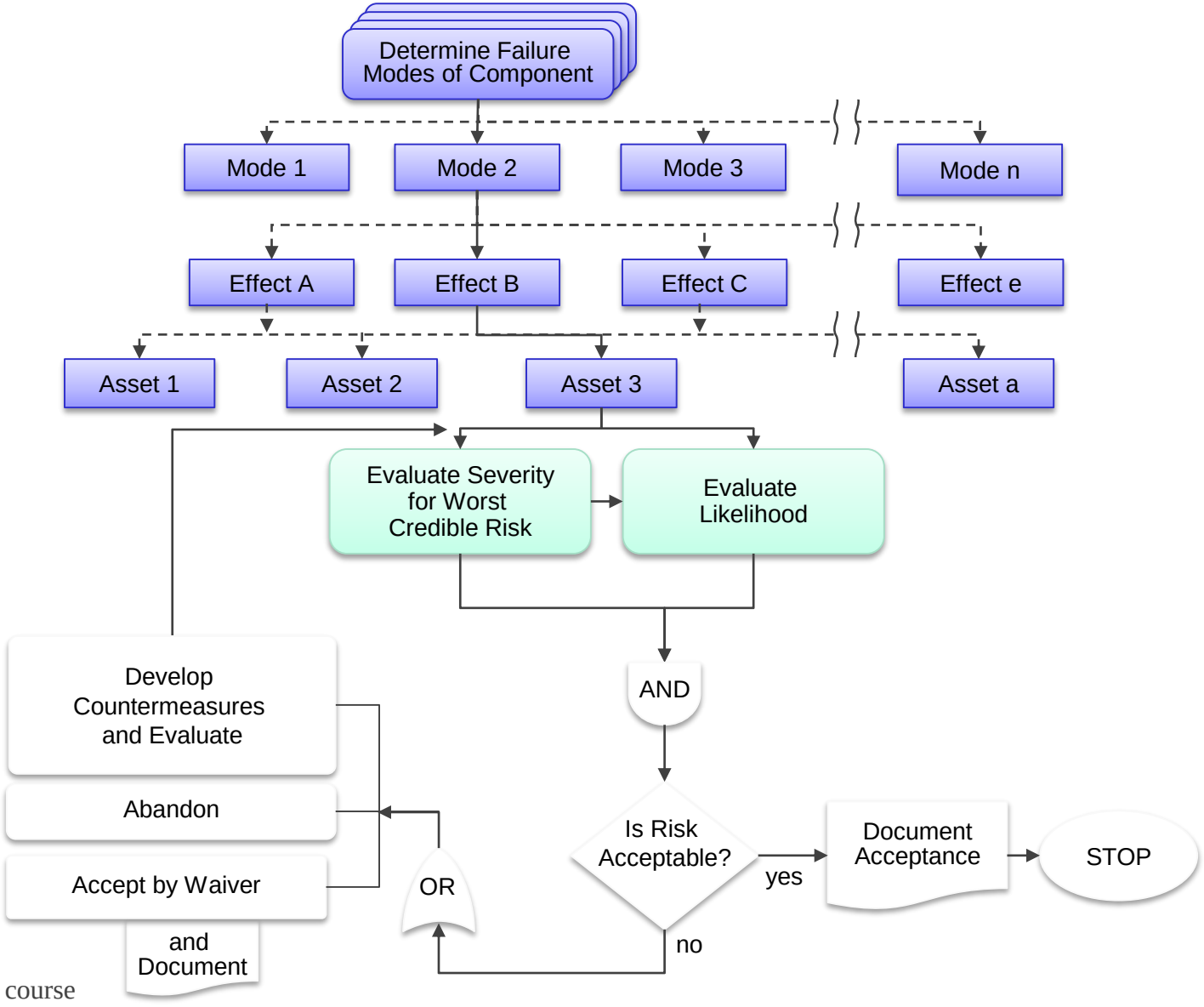
Reliability – Probabilistic Risk Assessment (PRA)

Design Reliability – The Challenger Accident

Process Reliability – The Columbia Accident

FMEA - Hazard Analysis

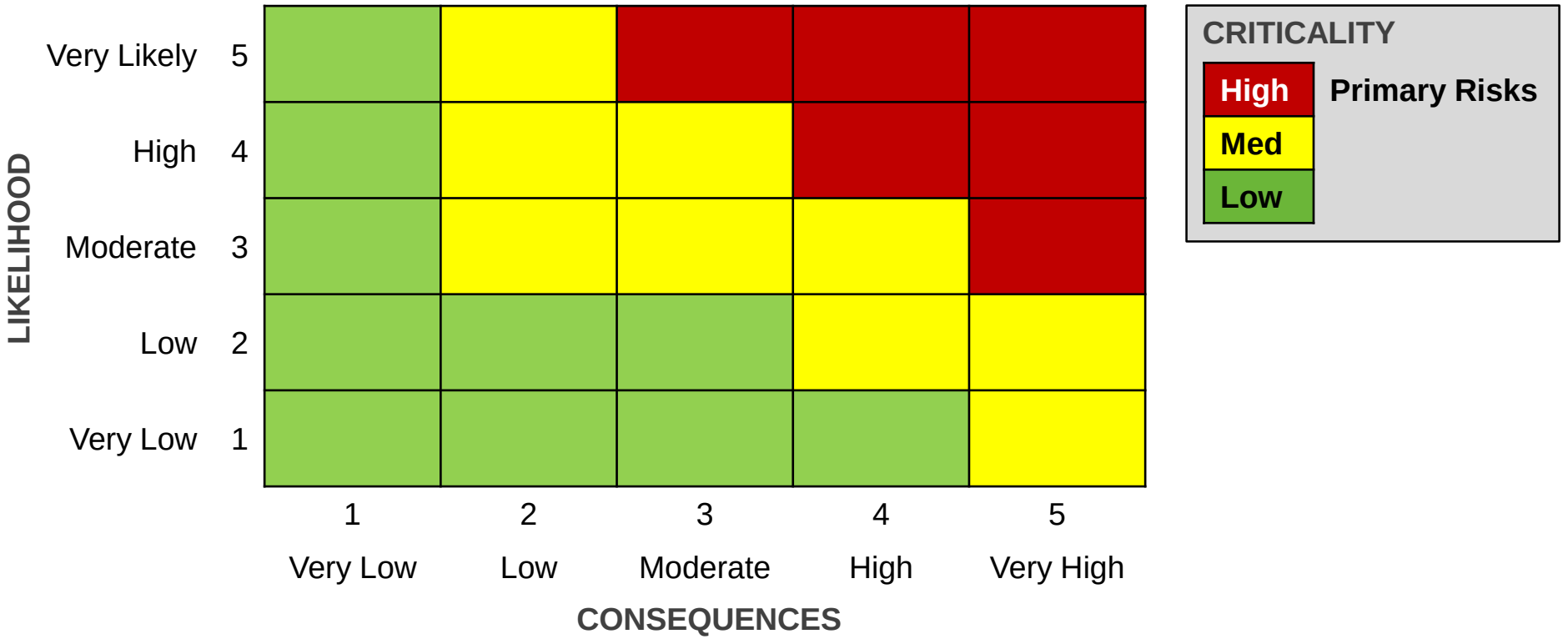
FMEA PROCESS LINKING TO HAZARD ANALYSIS



Reference: APT safety course

FMEA - Hazard Analysis

5×5 RISK MATRIX



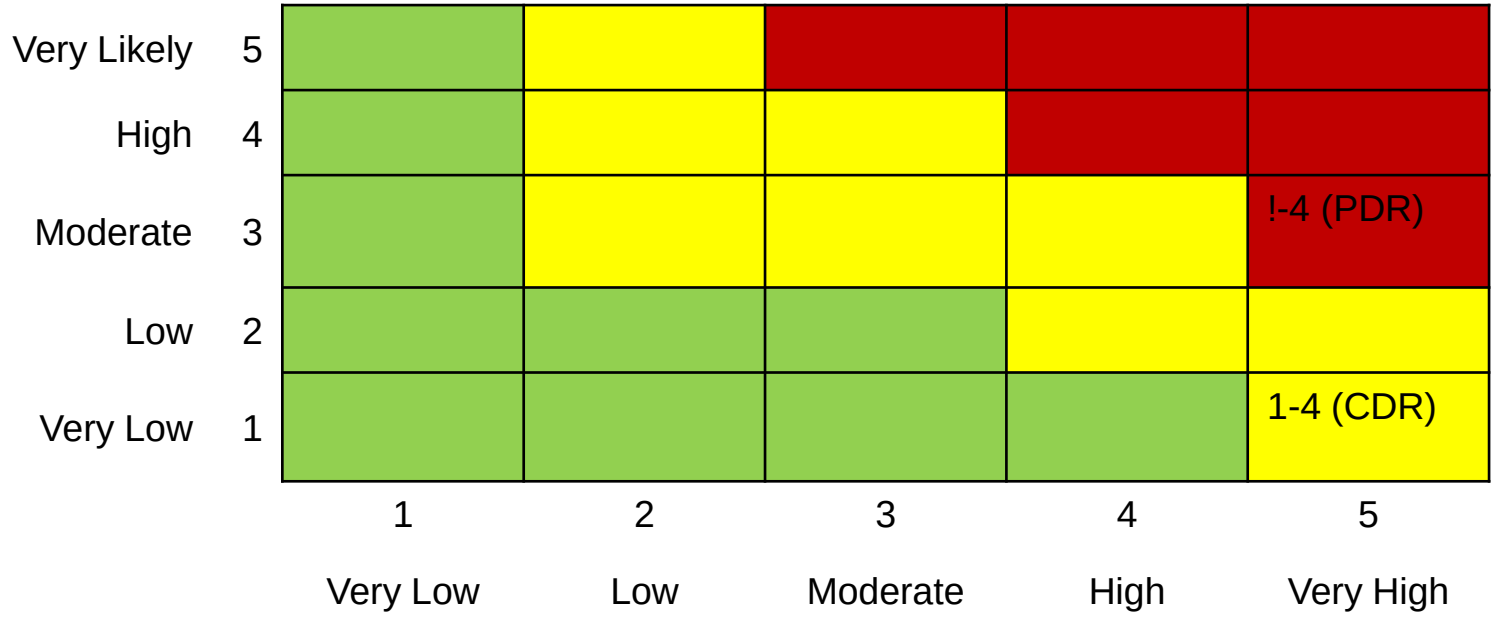
NOTE: Specific criteria for each of the likelihood and consequence categories are to be defined by each enterprise or program. Criteria may be different for manned missions, expendable launch vehicle missions, robotic missions, etc.

FMEA - Hazard Analysis

RISK MATRIX - A SOLID ROCKET EXAMPLE

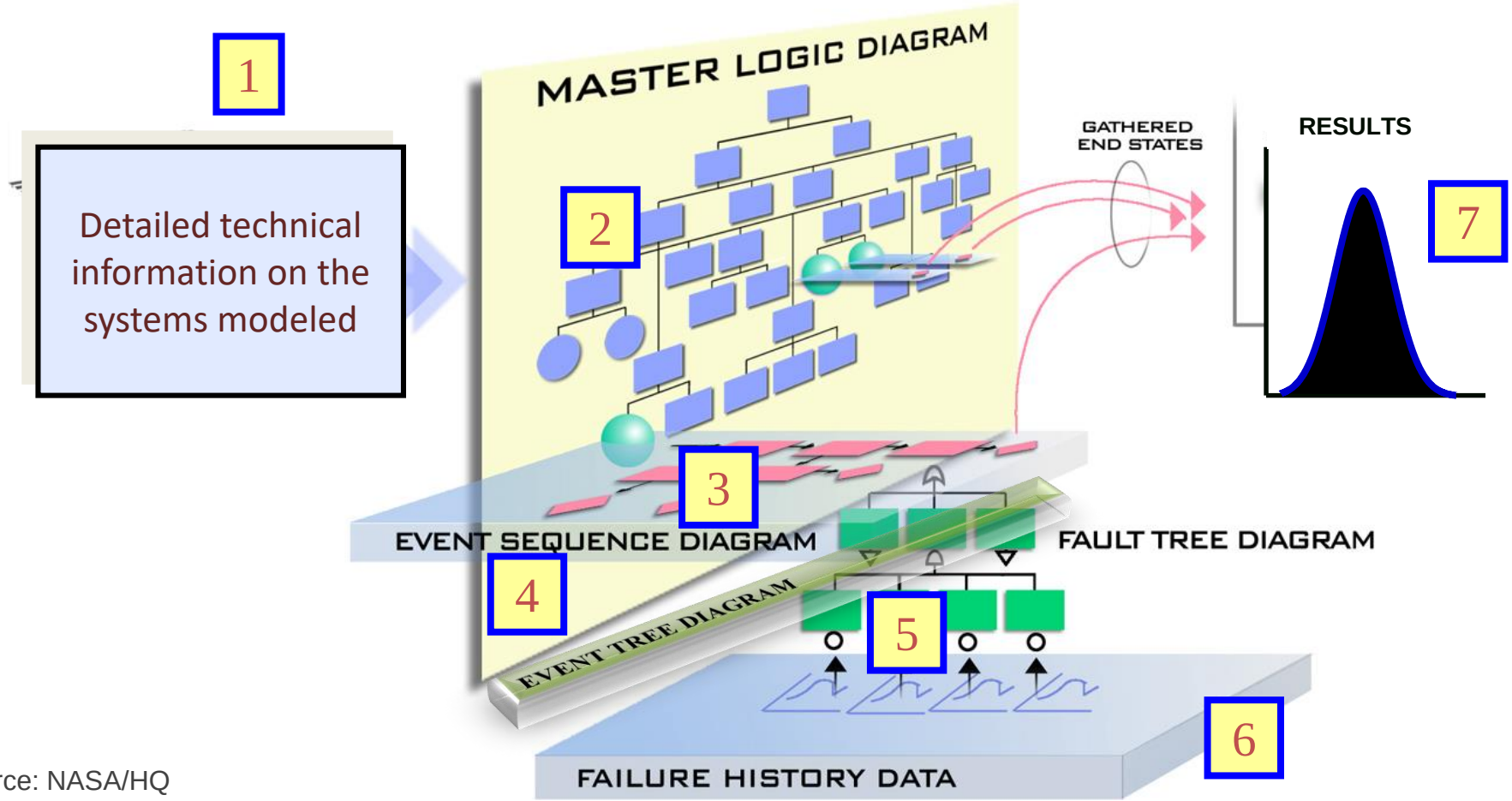
Structural Failure of the Integration and Assembly Structures

Hazard Causes	PDR Ranking (LxC)	CDR Ranking (LxC)	PRA (2 Boosters)		Downgrading Risk Justification
1-4. Structural Failures of Forward Assemblies	3 x 5	1 x 5			• Loads and analyses have matured since PDR which allows reduced risk



Reliability – Probabilistic Risk Assessment

THE PRA PROCESS



Source: NASA/HQ

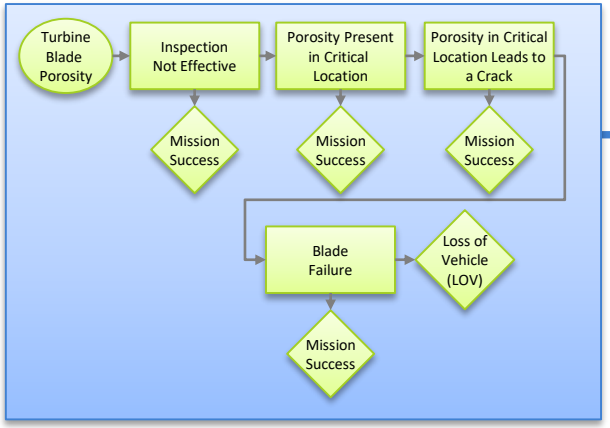
Reliability – Probabilistic Risk Assessment

EXAMPLE

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

Flight/Test Data
Probabilistic Structural Models
Similarity Analysis
Engineering Judgment

Quantification of ESD Initiating & Pivotal Events

Uncertainty Distribution for Event Probability

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

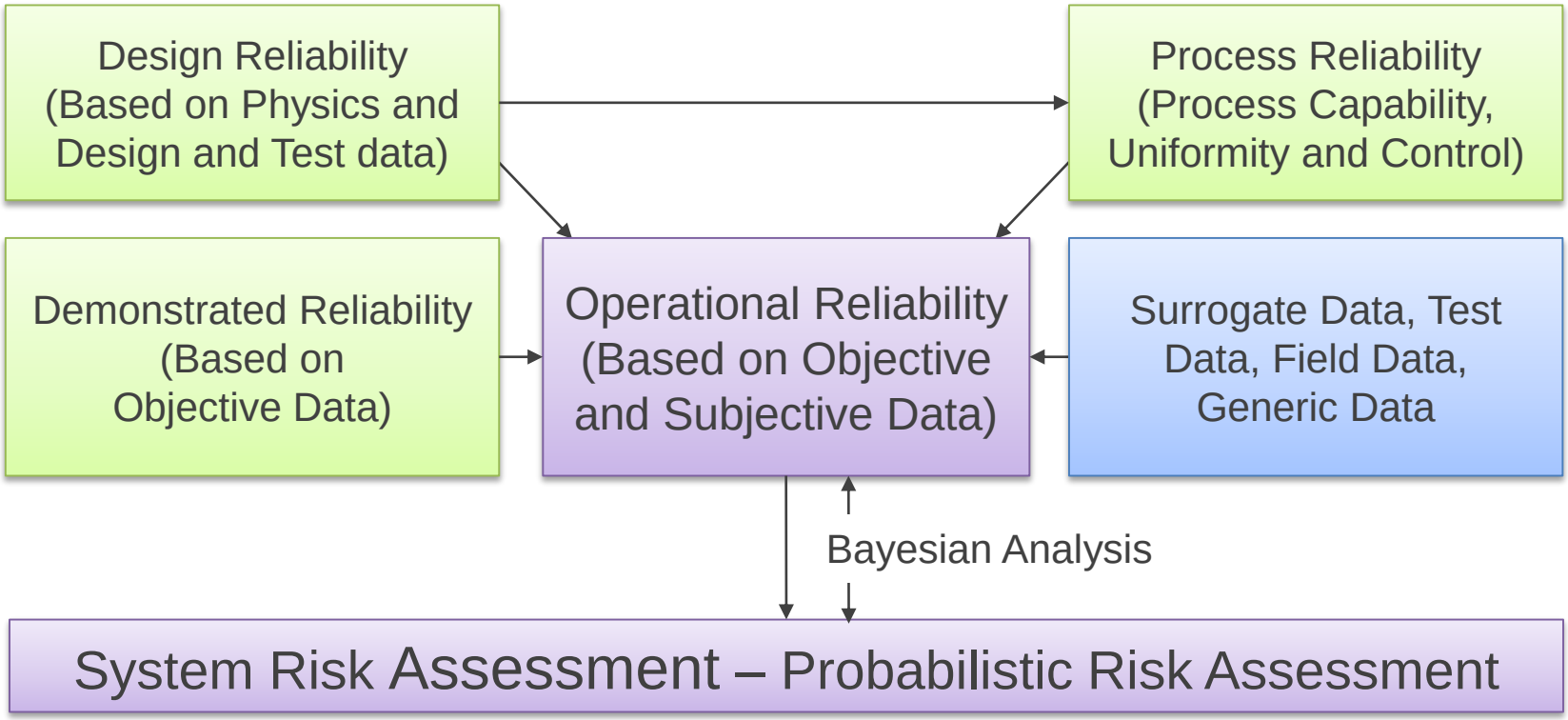
Risk Aggregation of Basic Events

Products

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

Reliability – Probabilistic Risk Assessment

THE LINK



Design Reliability - The Challenger

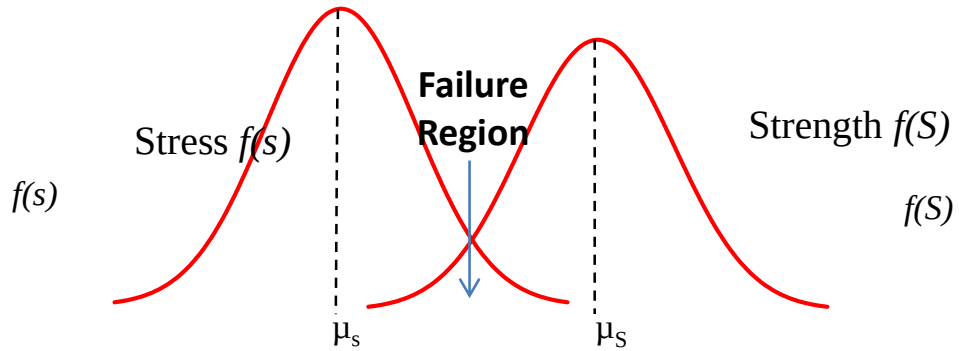
ACCIDENT

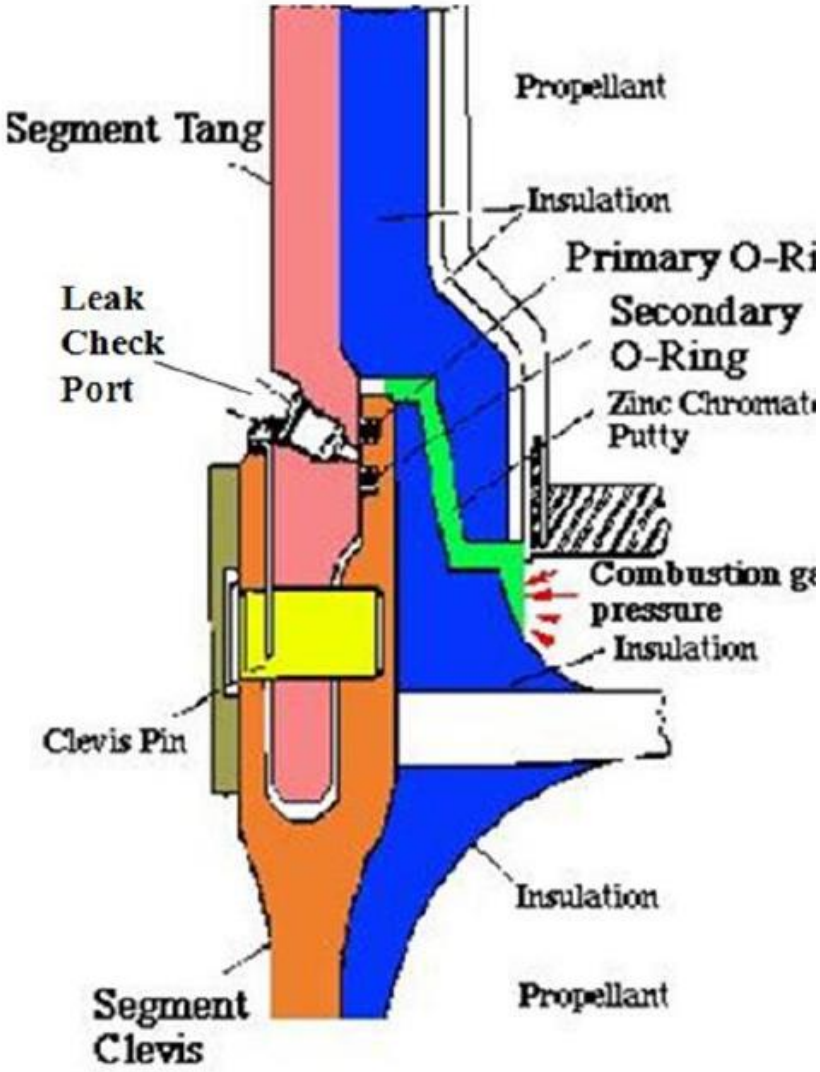
On January 28, 1986, the NASA shuttle orbiter mission STS-51-L and the tenth flight of Space Shuttle Challenger (OV-99) broke apart 73 seconds into its flight, killing all seven crew members, which consisted of five NASA Astronauts and two Payload Specialists. Failure of a field joint of the solid rocket booster was deemed to be the cause of the accident.

Design Reliability - The Challenger

ACCIDENT

- The solid rocket booster field joint was evaluated to determine the potential causes for the gas leak caused by the failure of the joint to seal.
- Evaluation identified the Zinc Chromate putty and the O-ring material were the weak links in the joint design.





Design Reliability

THE CHALLENGER ACCIDENT

- The Field joint design was modified to improve the reliability of the joint and reduce the risk of a catastrophic failure
  - The redesign of the joint/seal added a third O-ring and eliminated the troublesome putty which served as a partial seal.
  - Bonded insulation replaced the putty.
  - 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°F 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

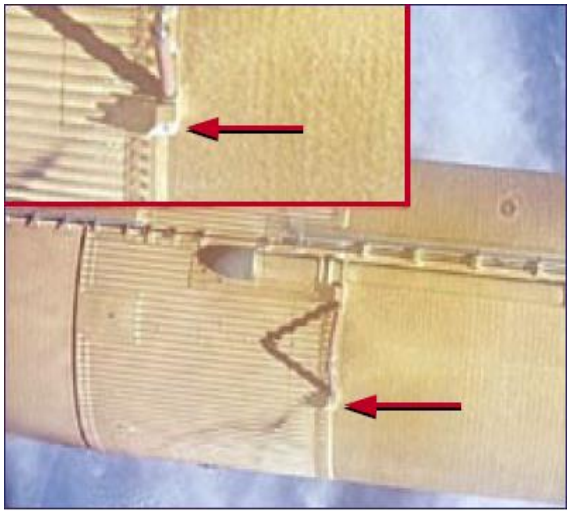
THE COLUMBIA ACCIDENT

- On February 1, 2003, the Space Shuttle Columbia disintegrated upon reentering earth atmosphere, killing all seven crew members.
- During the launch of STS 107, Columbia's 28th mission, a piece of foam insulation broke off from the Space Shuttle External Tank and struck the left wing of the orbiter.

Process Reliability

THE COLUMBIA ACCIDENT

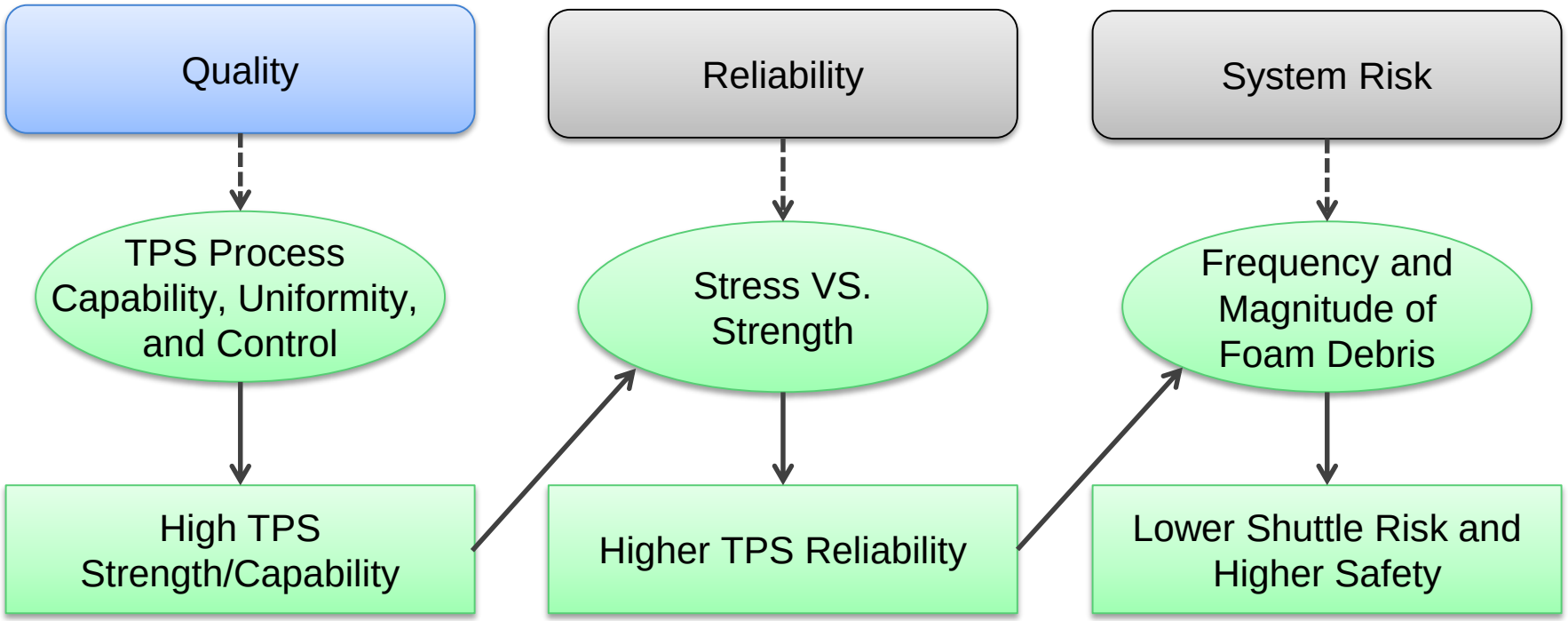
- Breach in the Thermal Protection System caused by the left bipod ramp insulation foam striking the left wing leading edge.
- The Thermal Protection System (TPS) design and manufacturing processes were evaluated for potential failure causes.
  - Process control for the TPS manual spray process was identified as a major process design weak link (process reliability case).
  - Cryopumping and cryoingestion were experienced during tanking, launch, and ascent.



Process Reliability

THE COLUMBIA ACCIDENT

The Relationship

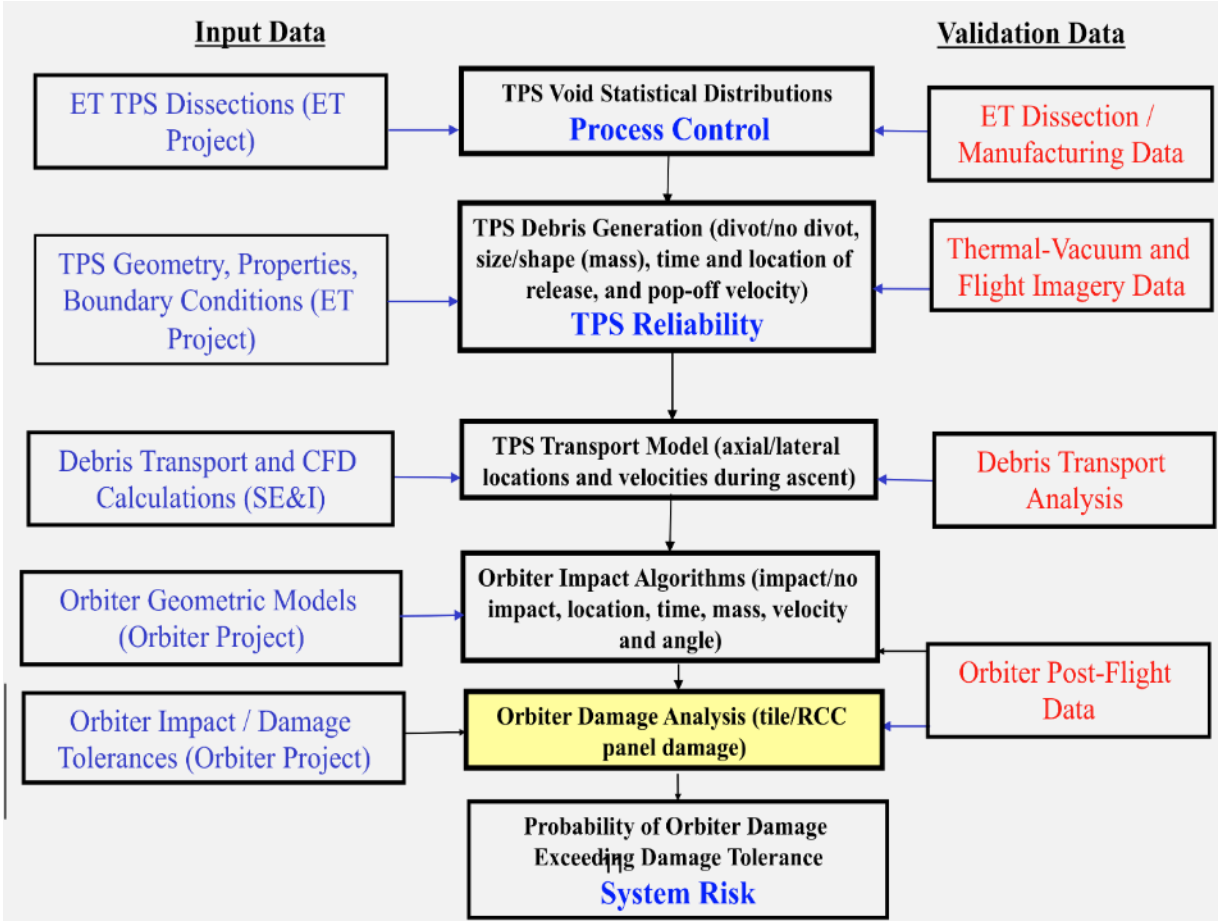


Process Reliability

THE COLUMBIA ACCIDENT

The Columbia Accident Case
The Impact of Reliability on System Risk/Safety

- The difficulties and sensitivities of the Space Shuttle External Tank (ET) Thermal Protection System (TPS) manual spray process is a good demonstration of the link between reliability and system risk.
- Fracture mechanics was used to derive the reliability of the foam (i.e. divot generation given a void).
- The divots generated were then transported to evaluate the damage impact on the orbiter and determine the system risk (i.e. Loss of Crew).



Reliability and Safety

UNIQUENESS

	Reliability	Safety
Roles	To ensure and assure product function achievability	To ensure and assure the product and environment safe and hazards free
Requirements	Closed ended, design function specific within the function boundary. Internally imposed	Open-ended, non-function specific such as “no fire”, “no harm to human being”. 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 maybe required to address

Reliability and Safety
UNISON

	Reliability and Safety
Roles	Both address some anomalous and undesirable conditions, develop methods to prevent or mitigate failures
Requirements	Lot of overlap between reliability and safety requirements (e.g. Loss of Mission (LOM), Loss of Vehicle (LOV), Loss of Crew (LOC))
Approaches	Safety and reliability share several techniques to address “what can go wrong?” (e.g. Fault tree analysis, event tree analysis)
Linkage	Strong linkage between reliability and safety in terms of input-output (e.g. FMEA –Hazard Analysis, Reliability Predictions – Risk Assessments)

CONCLUDING REMARKS

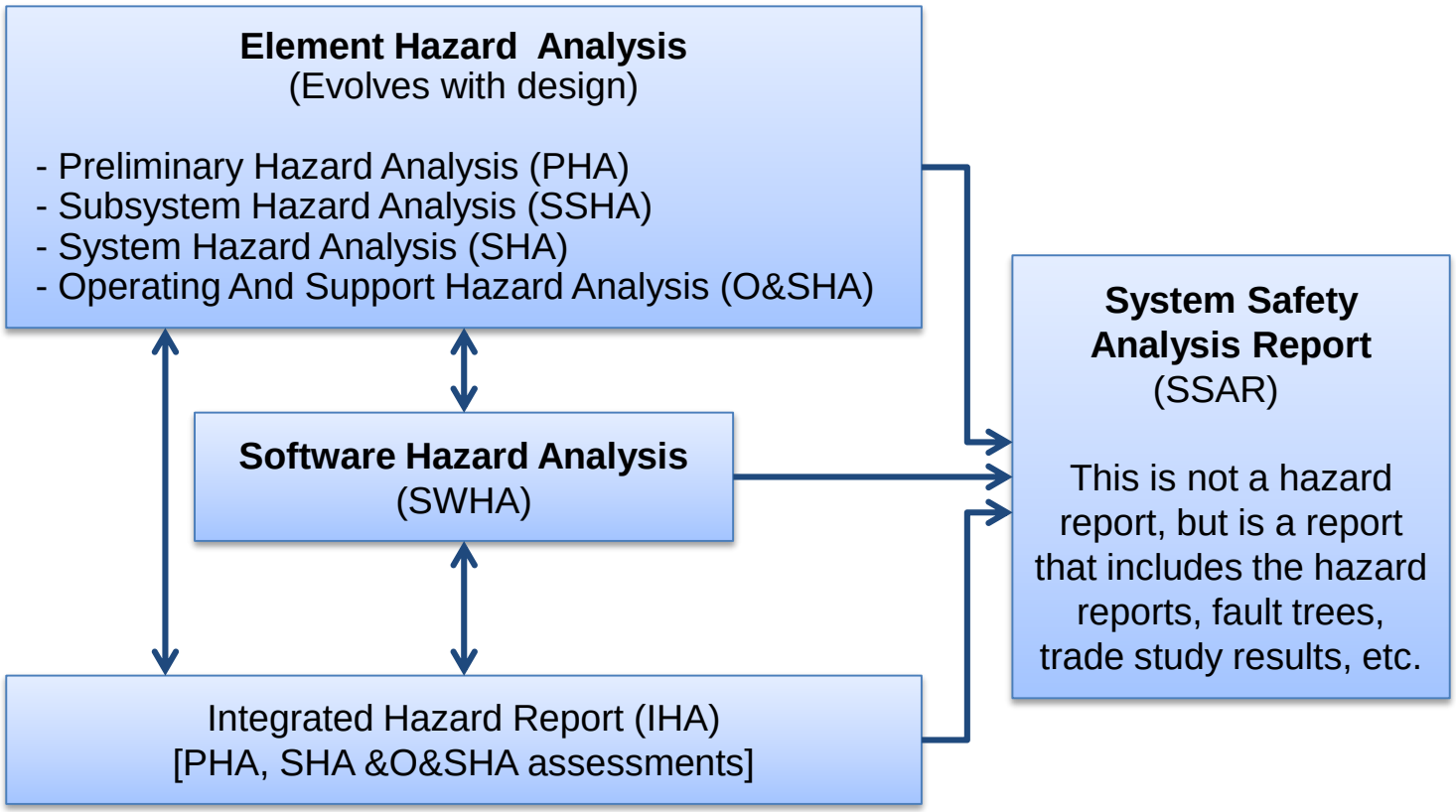
- Reliability and safety are unique but closely related, and compensating each other and need to be integrated.
- With better defined distinct roles and responsibilities, enhanced integration, shared resources, and improved tools and techniques, both disciplines will be better positioned to support product design and development.

A-P-T RESEARCH, INC.

AN EMPLOYEE-OWNED COMPANY

BACK-UP

HAZARD ANALYSES



Reference: John Livingston

THE COLUMBIA ACCIDENT

Cryopumping and Cryoingestion

- Cryopumping occurs when a void in a material or structure is at a low enough temperature to densify a contained volume of gases. As the gases are condensed, a vacuum is created. If there is a pathway to the surface or other voids, additional gases are pulled or pumped into the void. When the material or structure is heated, the densified gases expand and are expelled or pumped from the void. During this expansion phase of Cryopumping, the most damage in the material can be incurred. Cryopumping can be problematic for cryogenic materials and structures if the gases are densified into a void, then the void is rapidly heated, but the flow of gases from the void is restricted, causing a rapid pressure buildup. Cryopumping in the proof testing of the liquid hydrogen tank for the X-33 contributed to the failure of the honeycomb tank wall
- Cryoingestion, occurs when gases are pulled or ingested through leak paths into regions under the foam at cryogenic temperatures. These gases condense into liquid during tanking on the launch pad, and later expand back into gases during ascent as the tank structure warms. This rapid expansion can cause increases in pressure under the foam, potentially causing divots to be liberated. For the bipod, the leak path for this gas could have been through the heater or temperature sensor wiring harness. Another potential contributor to the cryoingestion scenario is the voids found in the material used to bond the wire harnesses to the substrate. These voids can act as reservoirs for the liquid nitrogen ingested through the harness.

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…