Lessons Learned in Design and Process Reliability

Fayssal M. Safie, Ph. D.,
NASA R&M Tech Fellow
Marshall Space Flight Center

RAM VI Workshop
Huntsville, Alabama
October 15-16, 2013

Agenda

- **Background**
  - Reliability Engineering
  - Why Reliability Engineering
- **The Reliability Engineering Case**
- **The Relationship to Safety and Affordability**
- **The Space Shuttle Lessons Learned**
  - The Challenger Accident
  - The Columbia Accident
- **Concluding Remarks**

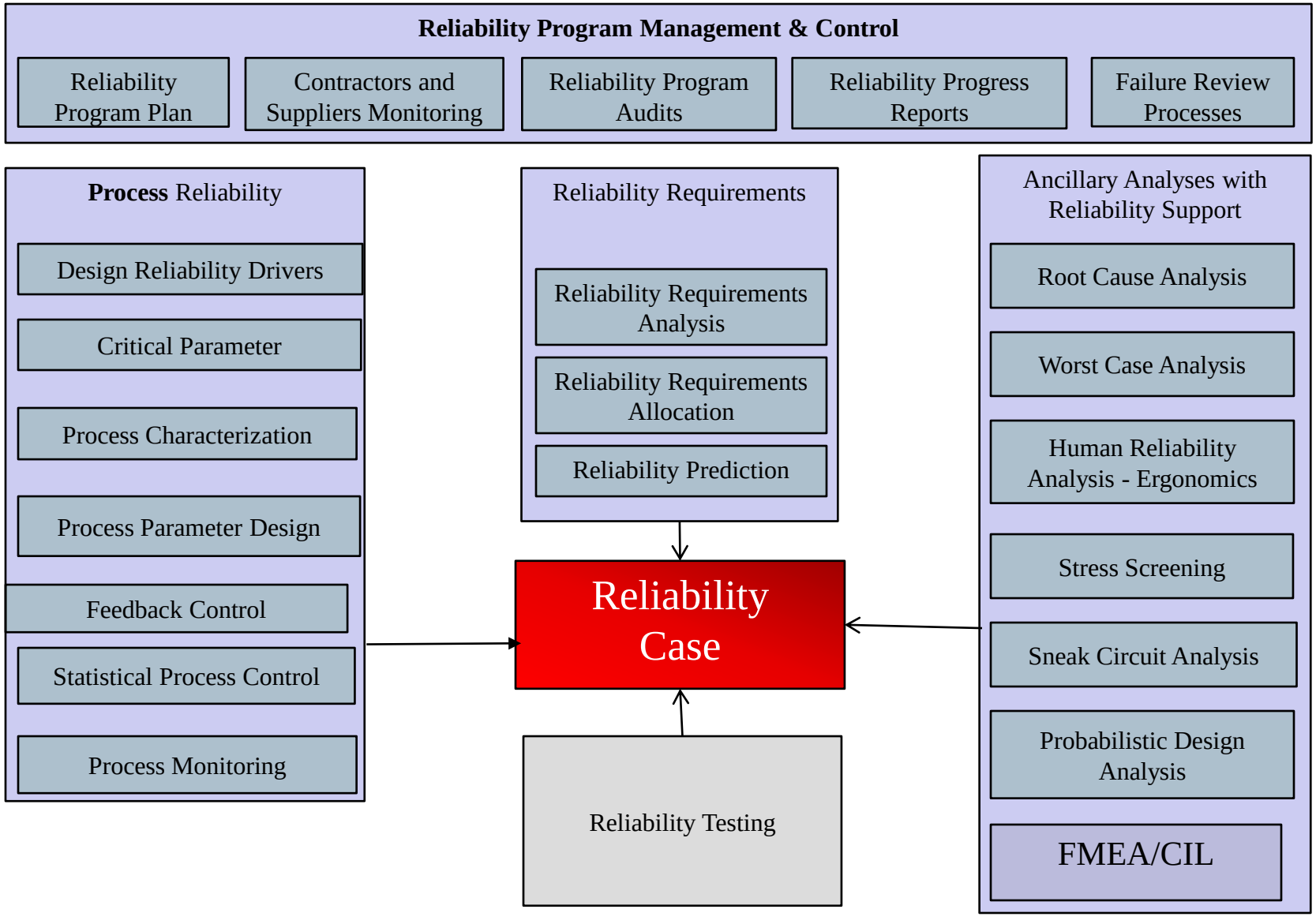
Reliability Engineering

- **Reliability Engineering is:**
  - The application of engineering and scientific principles to the design and processing of products, both hardware and software, for the purpose of meeting product reliability requirements or goals.
  - The ability or capability of the product to perform the specified function in the designated environment for a specified length of time or specified number of cycles
- **Reliability as a Figure of Merit is:**
  - Reliability: The probability that an item will perform its intended function for a specified mission profile.
- **Reliability is a very broad design-support discipline**
- **Reliability engineering has important interfaces with most engineering disciplines**

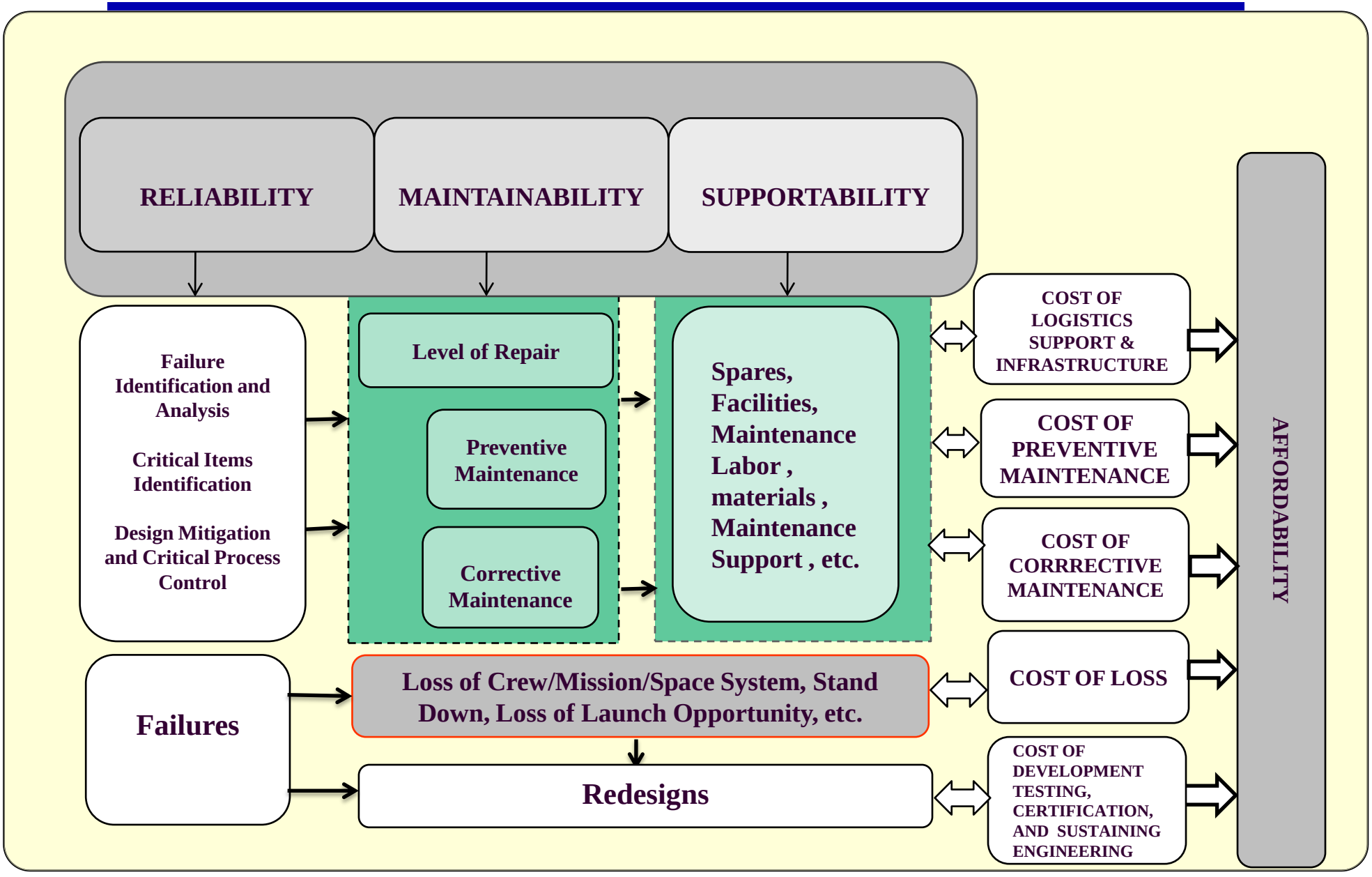
Why Reliability Engineering?

- Reliability engineering has important interfaces with safety, quality, maintainability, supportability, cost, test, and design engineering.
- Reliability analysis is critical for understanding component failure mechanisms and integrated system failures, and identifying reliability critical design and process drivers.
- A comprehensive reliability program is critical for addressing the entire spectrum of engineering and programmatic concerns, from Loss of Mission (LOM) risk and the Loss of Crew (LOC) risk to sustainment and system life cycle costs.

The Reliability Engineering Case



The Relationship to Safety and Affordability



The Space Shuttle Lessons Learned

- The Space Shuttle was a very successful program. Unfortunately, two major costly accidents occurred in the life of the program. They were the Challenger and the Columbia Accidents.

The Space Shuttle Lessons Learned

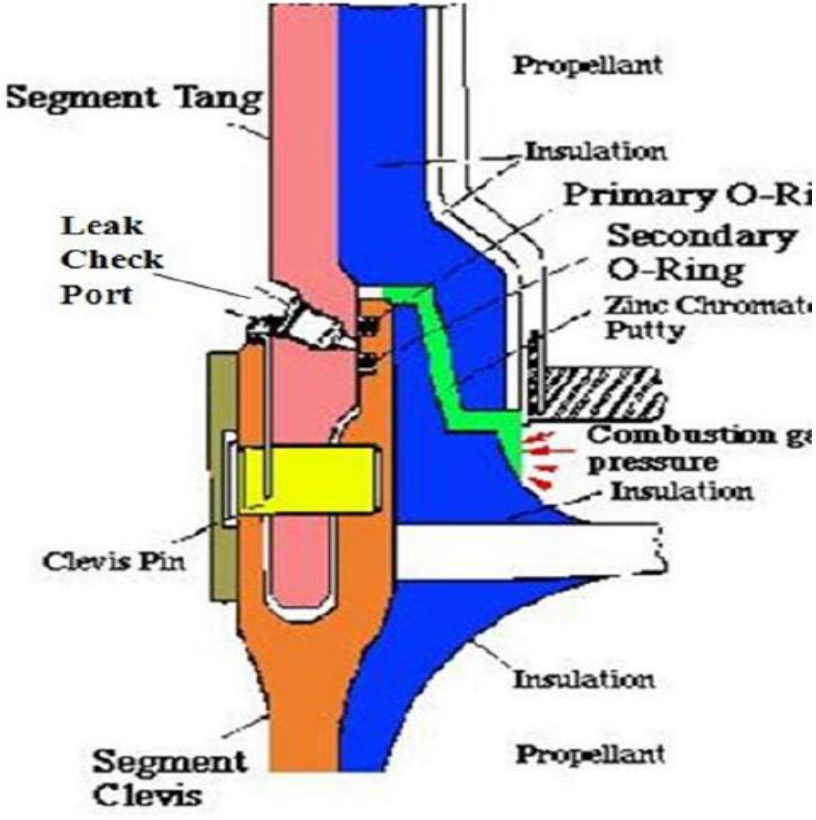
The Challenger Accidents

Photograph of the 51-L launch at approximately 58.82 seconds after launch shows an unusual plume in the lower part of the right hand SRB.

The Challenger Accident

The Problem

- **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.



The Challenger Accident

The Precursors

In 1977 a test of the SRB case showed an unexpected rotation of the joints which decompressed the O-rings making it more difficult for them to seal the joints.

In 1980 a review committee concluded that safety was not jeopardized and the joints were classified as Criticality 1R, denoting that joint failure could cause loss of life or shuttle, the 1 in the rating; and that secondary O-rings provided redundancy, the R in the rating.

In 1983 the SRBs were modified to use thinner walls, narrower nozzles, which worsened the joint rotation. Tests showed that the rotation could be so large that a secondary O-ring could not seal a joint and provide redundancy. The R rating was consequently removed from the joints' Criticality classification.

Criticality 1 was incorrectly listed as 1R for 3 years - Many NASA and Thiokol documents produced over the next 3 years continued to list the Criticality as 1R, and seemed to suggest that neither management thought that a secondary O-ring could really fail to seal a joint OR perhaps it was just sloppy configuration control.

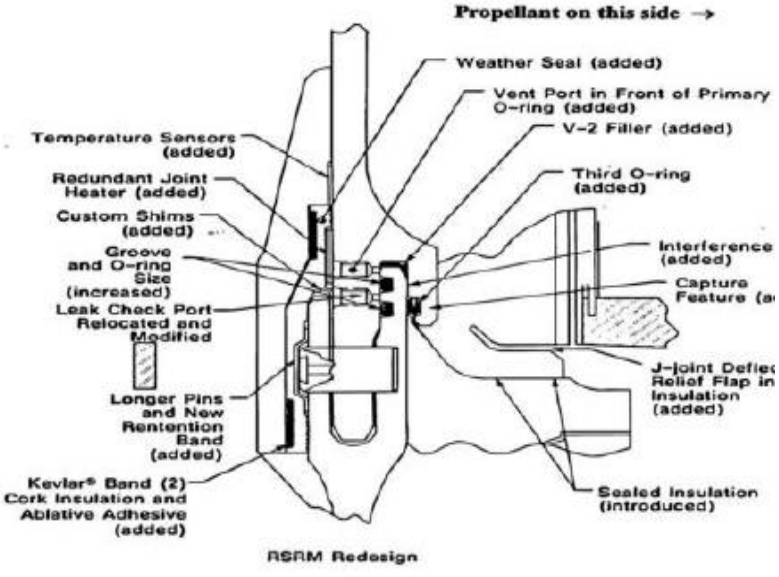
The Challenger Accident

Redesigned Field Joint

The redesign of the joint/seal shown here added a third O-ring and eliminated the troublesome putty which 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 assure the O-rings did not experience temperatures lower than 75 degrees Fahrenheit regardless of the surrounding temperature.

The gap openings which 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.

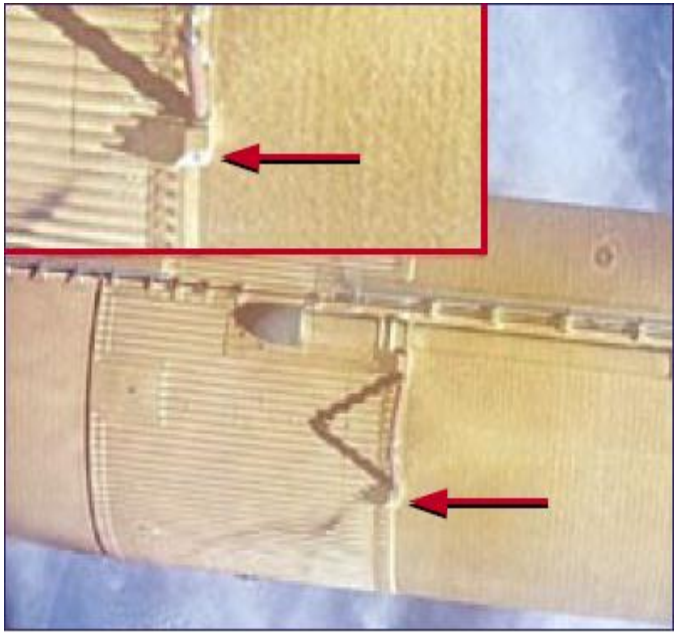
Challenger accident
The Lesson Learned

- **In Summary, the major causes that led to the Challenger accident are:**
  - Design flaw
  - Wrong material to use at low temperatures
  - Operating beyond the design environment
  - Precursors (e.g. O-ring erosion) were down-played
  - Problems in interpreting and communicating technical data
  - Schedule pressure
- **Design reliability was the major cause of the Challenger accident**

The Space Shuttle Lessons Learned

The Columbia Accident

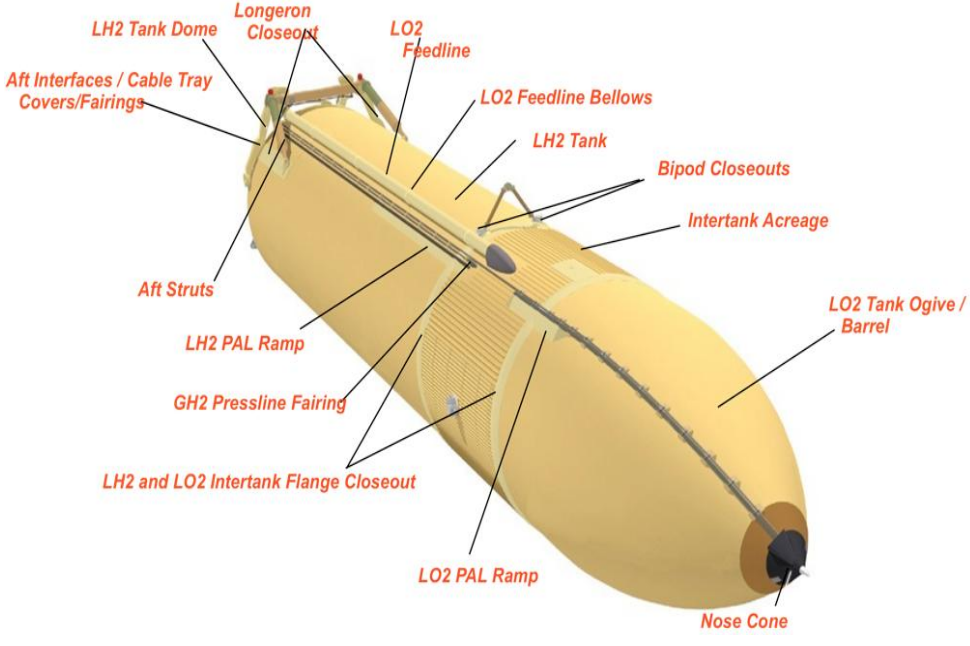
- **Causes and Contributing Factors**
  - Breach in the Thermal Protection System caused by the left bipod ramp insulation foam striking the left wing leading edge.
  - There were large gaps in NASA's knowledge about the foam.
  - cryopumping and cryoingestion, were experienced during tanking, launch, and ascent.
  - Dissections of foam revealed subsurface flaws and defects as contributing to the loss of foam.

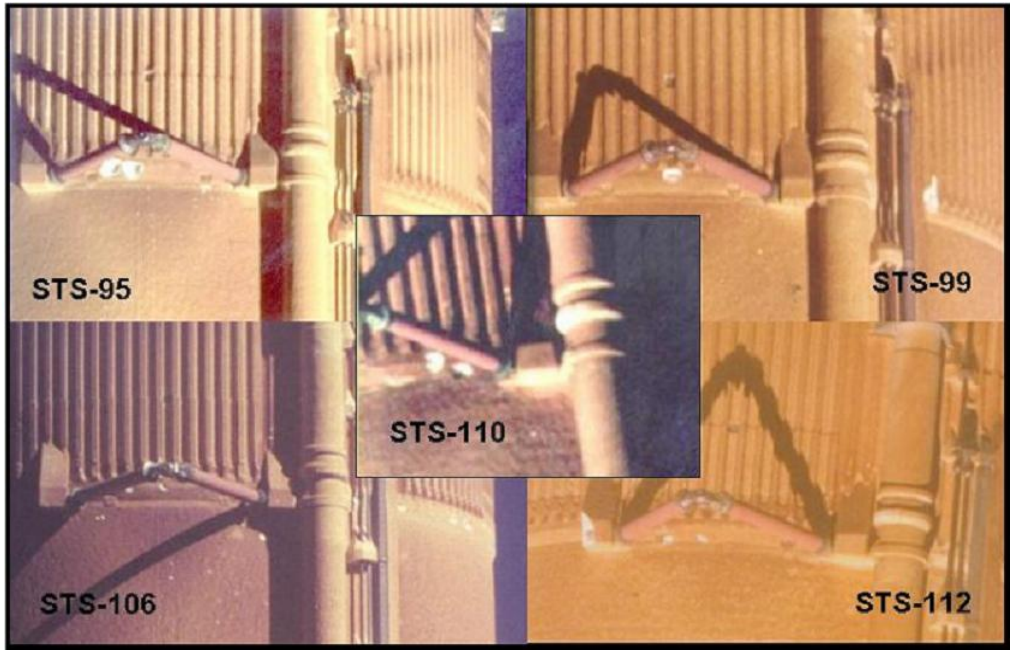


The Columbia Accident

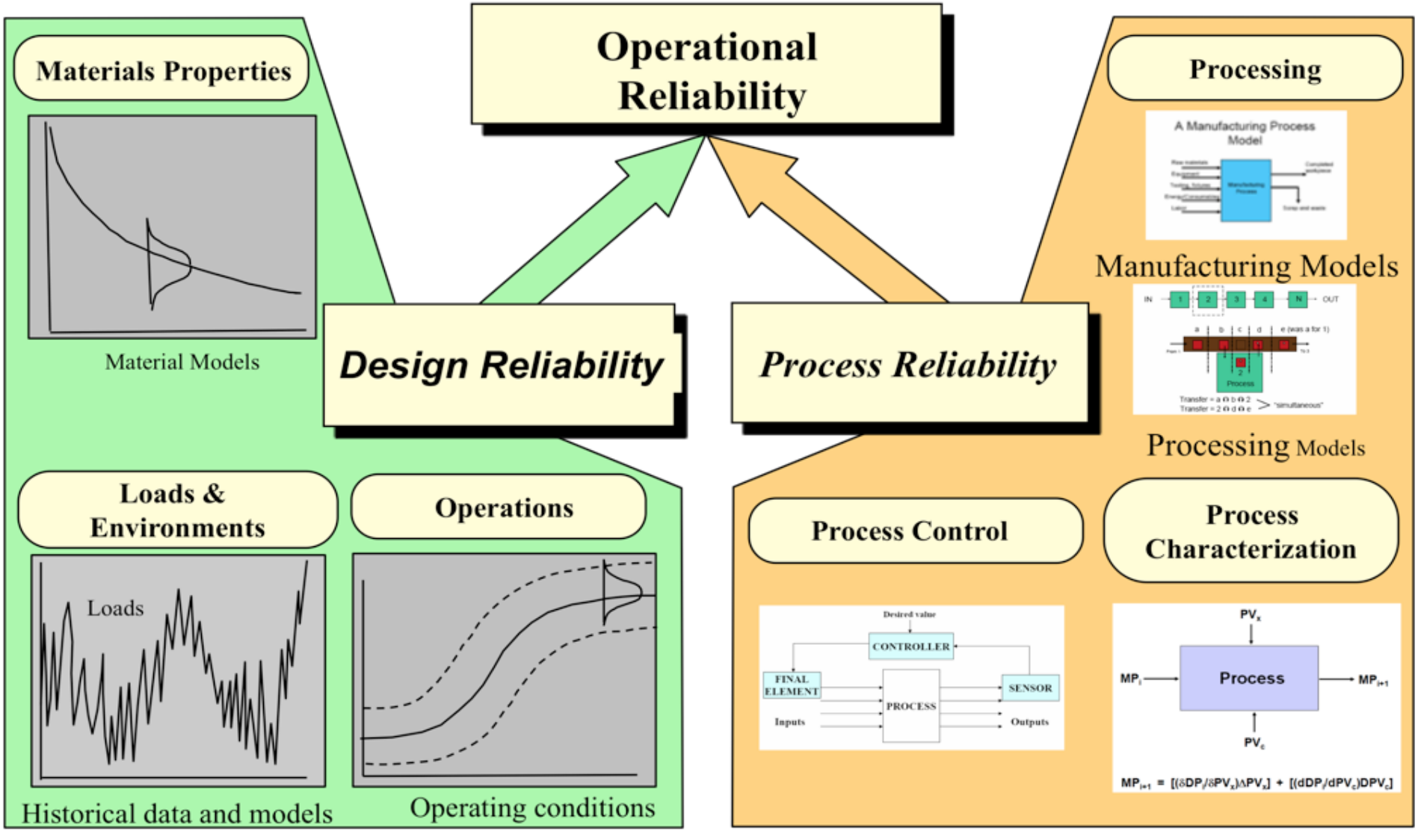
The Precursors

- 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.





The Foam Reliability



Foam Spray Process Evaluation

- Process variability was evaluated after the fact
- Dissection data collected after the Columbia accident showed excessive variability (Coefficient of variation is greater than 100%)
- Within tank variability was high, and tank to tank variability could not be fully characterized
- Defect/void characterization was difficult and statistics derived had high level of uncertainty
- The natural variation of the process was not well understood
- The relationship between process control variables and defects was not known

Evaluation of Redesigned Components and Process Enhanced Foam

- Conducted verification and validation 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)

The Columbia accident

The lesson Learned

- **In summary, the major causes that led to the Columbia accident are:**
  - Design Flaw
  - Wrong Requirement
  - Lack of integrated failure analysis
  - Insufficient process control
  - Lack of understanding of failure physics of the foam
  - Lack of certified NDE for the foam
  - Precursors (e.g. foam release) were down-played
  - Problems in interpreting and communicating technical data
- **Design and process reliability were the major causes of the Columbia accident**

Concluding Remarks

- Both the Challenger and Columbia accidents are examples of the severe impact of unreliability system safety, mission success, and affordability.
- These accidents demonstrated the criticality of reliability engineering in understanding reliability design drivers, component failure mechanisms, process reliability, and integrated system failures across the system elements' interfaces.
- Reliability is extremely critical to build safe, reliable, and cost effective systems.