Understanding the Elements of Operational Reliability
A Key for Achieving High Reliability

Fayssal M. Safie, Ph. D.
Marshall Space Flight Center
Huntsville, Alabama, USA

Trilateral Safety and Mission Assurance Conference (TRISMAC)
Cleveland, Ohio, October 26-28, 2010
Agenda

• Introduction
• Reliability Engineering Major Areas
  - Reliability Engineering Interfaces
• Design Reliability
• Process Reliability
• Reliability Applications
  - A Probabilistic Engineering Analysis Case Study
  - A Process Reliability Case Study
• Concluding Remarks
Reliability Engineering Major Areas

- Reliability, Allocation, Modeling, and Prediction
- Reliability Testing and Verification
- Reliability Program Planning and Control
- Reliability Growth
- Reliability Databases
- Reliability Analysis
- FMEA/CIL

Mission Success Starts with Safety
Reliability Engineering Major Interfaces

- Risk Management
- Maintainability Engineering
- Quality Engineering
- Supportability Engineering
- System Safety Engineering
- Test and Evaluation
- Engineering Design
Inherent Reliability versus Operational Reliability

- **Inherent Reliability** is the level of reliability inherent in the system as designed and manufactured (See design and process reliability).
- **Operational Reliability** is the reliability actually observed during operation.
- Failure occur due to weaknesses in the design, flaws in the materials, defects from the manufacturing processes, maintenance errors, improper operation, changes in operating concept, etc.
- The level of inherent reliability is determined through analysis and test (the "actual" system or prototypes). Although the design and development team attempts to simulate the actual operating environment, it is difficult if not impossible to account for some aspects of operation.
- If the operating environment is substantively different from that defined during design, more failures or failure modes may occur than were addressed during design and manufacturing.
Introduction - The Metric

**Reliability**: The probability that an item will perform its intended function for a specified mission profile.

**HIGH RELIABILITY MEANS:**

- **DESIGN IT RIGHT**
  - ESTABLISH DESIGN RELIABILITY REQUIREMENTS AND DEVELOP A PLAN WHICH SHOWS HOW REQUIREMENTS WILL BE MET
  - USE QUALITATIVE AND QUANTITATIVE ANALYSIS METHODS AND TOOLS TO VERIFY THAT REQUIREMENTS ARE MET

- **BUILD IT RIGHT**
  - ANALYZE THE MANUFACTURING, ASSEMBLY, AND TEST PROCEDURE CONCURRENT WITH THE DESIGN PROCESS
  - USE CONCURRENT ENGINEERING TO GET EVERYONE INVOLVED UP-FRONT
Design and Process Reliability

Design Reliability
- Materials Properties
- Material Models
- Loads & Environments
- Loads
- Historical data and models
- Operating conditions
- Operations

Process Reliability
- Process Control
- Process Characterization
- Manufacturing Models
- Processing & Models
- Processing

Reliability

Manufacturing Models

Process Control

Process Characterization
Design Reliability

- Design Process:
  - Loads
  - Environments
  - Usage
  - Sizing
  - Materials
  - Geometry

- Materials Production:
  - Acceptance Testing
  - Qualification Testing
  - Baseline Mat’l Strength

- Operating Stress

- Material Strength

- Failure Region
Process Reliability

Element Design

- Critical Design Parameters (CDP)
- Materials Properties & Geometry

Processing

- Map the CDP To Processing
- Identify Critical Process Variables (CPV)

Process Characterization

- Explore Relationship between CDP and CPV
- CDP = f(CPV)

Process Control

- Select Control Strategy
- Assess Process Capability
A Probabilistic Engineering Analysis Case Study
Probabilistic engineering analysis was used in the study to predict the probability of inner race over-stress, under the conditions experienced in the test rig, and estimate the effect of manufacturing stresses on the fracture probability.

Probabilistic engineering analysis is used when failure data is not available and the design is characterized by complex geometry or is sensitive to loads, material properties, and environments.

During rig testing the AT/HPFTP Bearing experienced several cracked races.

Summary of 440C race fractures/tests: 3 of 4 fractured
Turbo-pump Bearing Simulation Model

1. Randomly select values for inner race mat’l properties
   - ε
   - α
   - ν

2. Randomly select values for shaft/sleeve mat’l properties
   - ε
   - α
   - ν

3. Tolerance fits of rig test bearing

4. Inner race hoop stress at given conditions

5. Shaft/sleeve hoop stress at given conditions

6. Total hoop stress

7. Stress due to manufacturing

8. Stress > allowable load

9. Iterate and compute failure probability

10. Variation in:
    - Fracture toughness
    - Yield strength
    - No. of cracks
    - Crack depth
    - Crack length

11. Compute allowable load for each crack

12. Compute allowable load (worst crack)
### Turbo-pump Bearing Simulation Results

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

*ideal + abusive grinding  
**Probabilistic Structural Analysis

It is estimated that 50% of the through ring fractures would result in an engine shutdown. The shutdown 9310 HPFTP Roller Bearing Inner Race Failure Rate is then: 0.50 X 10/100k = 5 fail/100k firings.
The Message

• Probabilistic engineering analysis is critical:

  • To understand the uncertainty of the design and identify high risk areas

  • To perform sensitivity analysis and trade studies for reliability optimization.

  • To identify areas for further testing.
A Process Reliability Case Study
The ET TPS is a foam-type material applied to the ET 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.
Reliability of TPS

• The reliability of the TPS is broadly defined as its strength versus the stress put on it in flight.
• High TPS reliability means less debris released and fewer hits to the orbiter, reducing system risk.
• Process control, process uniformity, high process capability are critical factors in achieving high TPS reliability.
• Good process uniformity and high process capability yield fewer process defects, smaller defect sizes, and good material properties that meets the engineering specification—the critical ingredients of high reliability.
Impact of Process Reliability

**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)

**Validation Data**
- ET Dissection / Manufacturing Data
- Thermal-Vacuum and Flight Imagery Data
- Debris Transport Analysis
- Orbiter Post-Flight Data

**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
Mission Success Starts with Safety

Impact of Process Reliability

Process Control

Component Reliability

System Risk

TPS Process Uniformity and Capability

TPS Capability vs. Performance

TPS Failure Impact on Orbiter

High TPS Capability

Higher TPS Capability

Lower Shuttle Risk and Higher Safety

High TPS Capability

Higher TPS Capability

Lower Shuttle Risk and Higher Safety
The Message

• The clear message from the Columbia accident and the ET TPS foam experience is that inadequate manufacturing and quality control can have a severe negative impact on component reliability and system safety

• It is critical to understand the relationship between process control, component reliability, and system safety upfront in the design process.
Concluding Remarks

• Quantitative Reliability Engineering analysis involves more than just reliability predictions and reliability demonstration that are performed against a given program or project requirements.

• Quantitative Reliability Engineering analysis can play a key role in supporting a broad range of applications. It is critical in addressing design and manufacturing deficiencies.

• High Reliability means design it right and build it right