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
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.
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.

### MAJOR PROGRAM ELEMENTS

<table>
<thead>
<tr>
<th>Process Reliability</th>
<th>Reliability Requirements</th>
<th>Selected Design Reliability Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification of Design Reliability Drivers</td>
<td>Reliability Requirements Analysis</td>
<td>Failure Modes and Effects Analysis</td>
</tr>
<tr>
<td>Identification of Critical Process Parameters</td>
<td>Reliability Requirements Allocation</td>
<td>Probabilistic structural Design Analysis</td>
</tr>
<tr>
<td>Process Characterization</td>
<td>Reliability Prediction</td>
<td>Human Reliability Analysis</td>
</tr>
<tr>
<td>Process Uniformity</td>
<td></td>
<td>Accelerated Testing</td>
</tr>
<tr>
<td>Process Capability</td>
<td></td>
<td>Sneak Circuit Analysis</td>
</tr>
<tr>
<td>Process Control</td>
<td></td>
<td>Parts Derating</td>
</tr>
<tr>
<td>Process Monitoring</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Reliability Program Management & Control

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

### Evidence for a Reliability Case

- Reliability Testing
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 engineering has important interfaces with and input to:

- Design engineering
- Risk assessment
- Risk management
- System safety
- Quality engineering
- Maintainability
- Supportability engineering, and sustainment cost.
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).
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

MIL-STD-882
1. Documentation of the system safety approach
2. Identification of hazards
3. Assessment of mishap risk
4. Identification of mishap risk mitigation measures
5. Reduction of mishap risk to an acceptable level
6. Verification of mishap reduction
7. Review and acceptance of residual mishap risk by the appropriate authority
8. Tracking hazards and residual mishap risk

ANSI/GEIA-STD-0010
1. Program Initiation
2. Hazard Identification and Tracking
3. Risk Assessment
4. Risk Reduction
5. Risk Acceptance

Safety Case Approach
* 0. Articulate arguments (rationale & claims) to be used in safety case
1. Develop program to provide supporting evidence and independent review
2. Provide supporting evidence (I - A - R)
* 3. Independently review, verify and validate
4. Review for acceptance (- A)
* Feature not currently in Best Practices

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

**SYSTEM SAFETY**
Hazard detection & mitigation

- **RELIABILITY**
  - Hazard Causes
  - Probability Analyses

- **QUALITY**
  - Process Controls
  - Verification Activities

**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.
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

Determine Failure Modes of Component

- Mode 1
- Mode 2
- Mode 3
- Mode n

Effect A
- Asset 1

Effect B
- Asset 2

Effect C
- Asset 3

Evaluating Severity for Worst Credible Risk

Evaluate Likelihood

- Effect e
- Asset a

Develop Countermeasures and Evaluate

Abandon

Accept by Waiver

AND

Is Risk Acceptable?

OR

yes
- Document Acceptance
- STOP

no

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.
### Structural Failure of the Integration and Assembly Structures

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

![Risk Matrix Diagram](image)

- **Very Likely** (5)
- **High** (4)
- **Moderate** (3)
- **Low** (2)
- **Very Low** (1)

- **Very Low** (1)
- **Low** (2)
- **Moderate** (3)
- **High** (4)
- **Very High** (5)
Reliability – Probabilistic Risk Assessment

THE PRA PROCESS

1. Detailed technical information on the systems modeled

2.

3.

4.

5.

6.

7.

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)**
- **Turbine Blade Porosity**
  - **Inspection Not Effective**
    - **Porosity Present in Critical Location**
      - **Porosity in Critical Location Leads to a Crack**
        - **Mission Success**
          - **Blade Failure**
            - **Loss of Vehicle (LOV)**
            - **Mission Success**

**Event Probability Distribution**

**Quantification of ESD Initiating & Pivotal Events**

**Uncertainty Distribution for Event Probability**

**Flight/Test Data**
- Probabilistic Structural Models
- Similarity Analysis
- Engineering Judgment

**Uncertainty Distribution**
- For LOV Due to Turbine Blade Porosity

**Event Tree**

**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 (Based on Physics and Design and Test data)

Demonstrated Reliability (Based on Objective Data)

Operational Reliability (Based on Objective and Subjective Data)

Process Reliability (Process Capability, Uniformity and Control)

Surrogate Data, Test Data, Field Data, Generic Data

Bayesian Analysis

System Risk Assessment – Probabilistic Risk Assessment
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.
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.
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.
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.
The Relationship

Quality

TPS Process Capability, Uniformity, and Control

High TPS Strength/Capability

Reliability

Stress VS. Strength

Higher TPS Reliability

System Risk

Frequency and Magnitude of Foam Debris

Lower Shuttle Risk and Higher Safety

The Columbia Accident

Quality, Reliability, and System Risk

TPS Process Capability, Uniformity, and Control

Stress VS. Strength

Frequency and Magnitude of Foam Debris

High TPS Strength/Capability

Higher TPS Reliability

Lower Shuttle Risk and Higher 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

<table>
<thead>
<tr>
<th>Reliability</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Roles</strong></td>
<td>To ensure and assure product function achievability</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td>Closed ended, design function specific within the function boundary. Internally imposed</td>
</tr>
<tr>
<td><strong>Approaches</strong></td>
<td>Bottom-up and start from the component or system designs at hand</td>
</tr>
<tr>
<td><strong>Analysis Boundaries</strong></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>To ensure and assure the product and environment safe and hazards free</td>
</tr>
<tr>
<td></td>
<td>Open-ended, non-function specific such as “no fire”, “no harm to human being”. Externally imposed</td>
</tr>
<tr>
<td></td>
<td>Top-down and trace the top level hazards to basic events then link to the designs</td>
</tr>
<tr>
<td></td>
<td>System view of hazards with multiple and interacting causes. External vulnerability and uncertainty maybe required to address</td>
</tr>
</tbody>
</table>
## 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.
HAZARD ANALYSES

**Element Hazard Analysis**
(Evolves with design)

- Preliminary Hazard Analysis (PHA)
- Subsystem Hazard Analysis (SSHA)
- System Hazard Analysis (SHA)
- Operating And Support Hazard Analysis (O&SHA)

**Software Hazard Analysis**
(SWHA)

**Integrated Hazard Report (IHA)**
[PHA, SHA & O&SHA assessments]

**System Safety Analysis Report (SSAR)**

This is not a hazard report, but is a report that includes the hazard reports, fault trees, trade study results, etc.

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…