Reliability Tools and Analysis Methods for Nuclear Power Plants

Sharon Honecker, PhD
Research Scientist
ReliaSoft Corporation
Tucson, Arizona
Overview

What is reliability?

What methods can help me ensure reliability?

- Failure Mode and Effects Analysis
- System Modeling
- Life Data Analysis
- Failure Reporting and Corrective Action System

Conclusions
What Is Reliability?
A Textbook Definition

Reliability is the probability that a component, subsystem, or system will perform its desired function

- without failure
- for a specified duration
- in a specific operating environment
- with a desired confidence
A Management Definition

- What’s the expected life of the product?
- How many returns/failures are we expecting next year?
- How much is it going to cost us to develop and to support this product?
- Can we make it more cost-effective?
What Methods Can Help Me Ensure Reliability?
Design for Reliability Process

- **CONCEPT PHASE**
  - **DEFINE** Reliability Objectives

- **DESIGN PHASE**
  - **IDENTIFY** Key Reliability Risks
  - **ASSESS** Proposed Design Reliability

- **DEVELOPMENT PHASE**
  - **QUANTIFY** Analyze & Improve Reliability

- **MANUFACTURING PHASE**
  - **ASSURE** Reliability

- **SUPPORT PHASE**
  - **SUSTAIN** Monitor & Control Reliability
Failure Mode and Effects Analysis (FMEA) - Application

- Design or redesign of a product
- Use an existing product in a new way
- Assess or improve product reliability
- Provides inputs for other system analyses (PRA, Fault Tree, Reliability Block Diagram, Markov Model, etc.)
- Central repository for reliability-related information
- Learning tool for new employees
Failure Mode and Effects Analysis - Process

Identify potential failure modes for a product (DFMEA) or process (PFMEA)

Assess the risk associated with those failure modes and prioritize issues for corrective action based on

- Severity
- Probability of Occurrence
- Detectability

Carry out corrective actions to address the most serious concerns
Failure Mode and Effects Analysis – Process Details

Form a cross-functional team of experts
Define the scope and deliverables
Gather supporting documents

For every item in the FMEA scope:

- Functions
- Failures
- Effects – local and system level
- Causes
  - Current Controls
  - Recommended Actions
Failure Mode and Effects Analysis - Example

- Function: Convert pressure to analog signal
- Failure: Fail Low
- Effects: Makes “A” and “B” train 2/2
- Causes: Corrosion; Wear; Mechanical damage; Heat effects
- Controls: Monthly test; Comparison with redundant channel indicators; Possible immediate detection
## Functional Level:

- **System:** Typical Reactor Trip Function
- **Subsystem:** Sensor Circuit 1

## Equipment:

- **Pressure transmitter PT-1**
  - **Failure Mode:** Fail low
  - **Cause:** Corrosion, Wear, Mechanical damage, Heat effects
  - **Symptoms and Local Effects Including Dependent Failures:** Low output to alarm unit; ac relays will remain energized for channel 1
  - **Method of Detection:** Periodic test
  - **Inherent Compensating Provision:** Redundant channels, 2 and 3
  - **Effect Upon Reactor Protection System:** Both trip paths 2/2 logic
  - **Remarks and Other Effects:** Possible immediate detection

  - **Failure Mode:** Fail high
  - **Cause:** Misadjustment
  - **Symptoms and Local Effects Including Dependent Failures:** High signal level to alarm unit; ac relays will deenergize for channel 1 with no trip
  - **Method of Detection:** Periodic test
  - **Inherent Compensating Provision:** Redundant channels, 2 and 3
  - **Effect Upon Reactor Protection System:** Both trip paths 1/2 logic
  - **Remarks and Other Effects:** Partial trip alarm

- **DC power supply PQ-1**
  - **Failure Mode:** Fail low or off
  - **Cause:** Transformer failure, Diode failure
  - **Symptoms and Local Effects Including Dependent Failures:** Removes operating power for transducer; alarm unit will sense low pressure; ac relay will open with no trip on channel 1
  - **Method of Detection:** Periodic test
  - **Inherent Compensating Provision:** Redundant channels, 2 and 3
  - **Effect Upon Reactor Protection System:** Both trip paths 1/2 logic
  - **Remarks and Other Effects:** Spurious trip if other channel failed 1/2

  - **Failure Mode:** Fail high
  - **Cause:** Heat effects, Misadjustment
  - **Symptoms and Local Effects Including Dependent Failures:** Transducer setpoint exceeds trip level; relays will remain energized for channel 1
  - **Method of Detection:** Periodic test
  - **Inherent Compensating Provision:** Redundant channels, 2 and 3
  - **Effect Upon Reactor Protection System:** Both trip paths 2/2 logic
  - **Remarks and Other Effects:** —

- **Alarm unit, PC-1**
  - **Failure Mode:** Fail off
  - **Cause:** Transformer failure
  - **Symptoms and Local Effects Including Dependent Failures:** AC power to ac relays removed for channel 1; ac relay open when no trip on channel 1
  - **Method of Detection:** Periodic test
  - **Inherent Compensating Provision:** Redundant channels, 2 and 3
  - **Effect Upon Reactor Protection System:** Both trip paths 1/2 logic
  - **Remarks and Other Effects:** Spurious trip if other channel failed 1/2

  - **Failure Mode:** Fail on
  - **Cause:** Open circuit in output section
  - **Symptoms and Local Effects Including Dependent Failures:** Does not remove ac power to ac relay for channel 1 trip; ac relay remains energized; both paths become 2/2 logic
  - **Method of Detection:** Periodic test
  - **Inherent Compensating Provision:** Redundant channels, 2 and 3
  - **Effect Upon Reactor Protection System:** Both trip paths 2/2 logic
  - **Remarks and Other Effects:** —
Failure Mode and Effects Analysis – Actions

Risk Priority Number (RPN) is assigned to each failure mode.

- RPN = Severity × Occurrence × Detectability

The team ranks the following using a scale of (1 to 5) or (1 to 10):

- Severity of Effect
- Probability of Occurrence of Cause
- Detectability of Cause

Recommended actions are assigned for the highest RPN failure modes.
System Modeling - Application

- Assess product reliability (non-repairable) or availability (repairable)
- Optimize preventive maintenance strategy and test intervals
- Provide probabilistic inputs for Life Cycle Cost Analysis
- Assign reliability goals to subsystems and components
System Modeling - Process

Create a reliability-wise representation of the system

- Fault tree – What components must fail to make the system fail?
- Reliability block diagram – What components must operate to make the system operational?
- Markov model – What are the possible system states?

Use laws of probability to determine system reliability
System Modeling Example
System Modeling Example
System Modeling - Inputs

- At a minimum, provide a reliability model for each component
  - Output will be system reliability
- In addition, can provide a model for repair duration for some or all components
  - Output will be system availability
- Optional inputs include information about preventive maintenance and inspection, costs of components and maintenance crews, spare parts holdings, etc.
Life Data Analysis (LDA) - Application

- Determine a reliability model for a component or a specific failure mode of a component
- Demonstrate that a component meets a reliability specification
  - Reliability at a given time at a given confidence level
- Determine a repair model for a component
Life Data Analysis - Process

Gather laboratory or field data about a component

Fit a probability density function, \(pdf\), to the data

- Common models in LDA are exponential, Weibull, lognormal

Use the model to predict reliability or probability of failure at a given time, mean life, etc.
Life Data Analysis – Model Selection

Models are chosen based on the expected failure rate behavior of the component:

- Exponential: constant failure rate; useful life
- Weibull: decreasing, increasing, or constant failure rate; infant mortality, useful life, or wearout
- Lognormal: increasing followed by decreasing failure rate; fatigue or corrosion
Life Data Analysis – Model Selection

Idealized Bathtub Curve

- Infant Mortality
- Useful Life
- Wearout

Failure Rate, $\lambda(t)$

Time, $t$
Life Data Analysis – Model Selection

Select Failure Mechanisms

- Overstress Mechanisms
  - Mechanical
    - Yield, Fracture, Interfacial de-adhesion
  - Thermal
    - Thermal overstress
  - Electrical
    - Dielectric breakdown, Electrical overstress, Electrostatic discharge, Second breakdown
  - Radiation
    - Single event upset
  - Chemical
    - Ionic contamination

- Wearout Mechanisms
  - Mechanical
    - Fatigue, SDDV, Creep, Wear
  - Radiation
    - Radiation hardening
  - Electrical
    - Electromigration, TDDDB, Surface charge spreading, Hot electrons, Slow trapping
  - Chemical
    - Corrosion, Dendrite growth, Depolymerization, Intermetallic, Growth, Kirkendahl Voiding, Hydrogen Embrittlement, Hillock Formation

Life Data Analysis – Model Selection

Select Failure Mechanisms

- Overstress Mechanisms
  - Mechanical
    - Yield, Fracture, Interfacial de-adhesion
  - Thermal
    - Thermal overstress
  - Electrical
    - Dielectric breakdown, Electrical overstress, Electrostatic discharge, Second breakdown
  - Radiation
    - Single event upset
  - Chemical
    - Ionic contamination

- Wearout Mechanisms
  - Mechanical
    - Fatigue, SDDV, Creep, Wear
  - Radiation
    - Radiation hardening
  - Electrical
    - Electromigration, TDDDB, Surface charge spreading, Hot electrons, Slow trapping
  - Chemical
    - Corrosion, Dendrite growth, Depolymerization, Intermetallic, Growth, Kirkendahl Voiding, Hydrogen Embrittlement, Hillock Formation
Life Data Analysis - Example

Twenty lamps were tested in the laboratory with the following times to failure in hours:

- 7407
- 7807
- 4237
- 9677
- 11320
- 6742
- 5653
- 8916
- 7918
- 10397
- 6216
- 9336
- 9078
- 8848
- 5101
- 8549
- 11203
- 9891
- 10043
- 12238
Life Data Analysis - Example

Number of Failures vs Time (10^3 hours)

Weibull pdf
Life Data Analysis - Example

Some possible results assuming a population of 1000 lamps are put into operation:

- How many will survive 5000 hours? 932 lamps
- What is the average life of the lamps? 8526 hours
- When will only 10 lamps remain? 13474 hours
Life Data Analysis - Example

Exponential pdf

Number of Failures

Time (10^3 hours)

Probability
Life Data Analysis - Example

Some possible results assuming a population of 1000 lamps are put into operation:

- How many will survive 5000 hours?
  Weibull: 932 lamps
- What is the average life of the lamps?
  Weibull: 8526 hours
- When will only 10 lamps remain?
  Weibull: 13474 hours
Life Data Analysis - Example

Some possible results assuming a population of 1000 lamps are put into operation:

- How many will survive 5000 hours? Weibull: 932 lamps; Exponential: 427 lamps
- What is the average life of the lamps? Weibull: 8526 hours
- When will only 10 lamps remain? Weibull: 13474 hours
Life Data Analysis - Example

Some possible results assuming a population of 1000 lamps are put into operation:

- How many will survive 5000 hours?  
  Weibull: 932 lamps; Exponential: 427 lamps

- What is the average life of the lamps?  
  Weibull: 8526 hours; Exponential: 5881 hours

- When will only 10 lamps remain?  
  Weibull: 13474 hours
Some possible results assuming a population of 1000 lamps are put into operation:

- How many will survive 5000 hours?
  Weibull: 932 lamps; Exponential: 427 lamps

- What is the average life of the lamps?
  Weibull: 8526 hours; Exponential: 5881 hours

- When will only 10 lamps remain?
  Weibull: 13474 hours; Exponential: 27083 hours
Failure Reporting and Corrective Action System (FRACAS) - Application

- Repository for information regarding failures and other issues
- Data is used to
  - Improve product reliability
  - Streamline maintenance activities
- Used both during design / development and after item is fielded
Failure Reporting and Corrective Action System (FRACAS) - Process

Incidents
- Issues / failures reported by customers, maintenance personnel, etc.
- Resolved immediately by technicians to restore system operation

Problems
- Groups of incidents with a single cause
- Addressed by engineers through a documented process, e.g., 8D, DMIAC
Failure Reporting and Corrective Action System (FRACAS) - Process
Failure Reporting and Corrective Action System (FRACAS) - Outputs

- Times to failure data for LDA
  - Inputs for System Reliability Modeling
  - Quantitative Probabilities of Occurrence for FMEA
- Times to repair data for LDA
  - Inputs for System Reliability Modeling
- Field failure modes for FMEA
Reliability Analysis – Common Pitfalls

- FRACAS collects only cumulative number of failures and cumulative operating time
  - Only exponential model can be used
- FMEA is not a “living” document
  - Redevelopment for every design wastes resources
  - Valuable information is lost and mistakes are repeated
Conclusions

Design for Reliability is a long-term process that employs a variety of tools.

Proper implementation requires:

- Strategic vision
- Proper planning
- Sufficient organizational resource allocation
- Proper implementation
- Integration and institutionalization of reliability into the organization