Probabilistic Assessment: Principles and Methods

3rd International Seminar on Probabilistic Methodologies for Nuclear Applications (ISPMNA 2019)
Rockville, MD, U.S.A.
October 22-24, 2019

Professor M. Pandey
Industrial Research Chair
University of Waterloo
Waterloo, Canada

Dr. B. Wasiluk
Canadian Nuclear Safety Commission
Ottawa, Canada

The views expressed herein are those of the authors and do not represent official positions of the Canadian Nuclear Safety Commission

Presentation Outline

1. Introduction
2. Probabilistic Assessment
3. Reliability Problems
4. Remaining Considerations
5. Closing Remarks
6. Acknowledgements

1. Introduction
2. Probabilistic Assessment
3. Reliability Problems
4. Remaining Considerations
5. Closing Remarks
6. Acknowledgements

Introduction (1 of 2)

- Fitness-for-service assessments are integral parts of assuring operability of nuclear plant systems and components
  - Deterministic methods have been traditionally used
- Elements of a **deterministic method**
  - A mechanistic method defining the performance requirement
    - Example: Fracture protection, Leak-Before-Break (LBB)
  - A bounding scenario (near "*worst case*") representing a limiting condition
    - Example: postulated accident, bounding crack
  - Outcome is binary
    - Whether "*pass*" or "*fail*", or "*safe*" or "*not safe*"
    - Accordingly, mitigating actions may be required

Introduction (2 of 2)

- **Limitations** of a deterministic evaluation
  - The "*worst case*" scenario is postulated certain to occur
  - The nearly most unfavorable combination of the variables is postulated certain
- The degree of embedded **conservatism** is unquantified
  - Risk in beyond design basis condition is unknown
- Emergence of probabilistic assessments methods to address these limitations
  - Inspired by a long and successful history of Probabilistic Risk Assessment (PRA)
  - Many standards are being developed to guide the assessment process
- Presentation **objective** is to discuss general principles, methods and elements of a Probabilistic Assessment (PA)

1. Introduction
2. Probabilistic Assessment
3. Reliability Problems
4. Remaining Considerations
5. Closing Remarks
6. Acknowledgements

Probabilistic Assessment

- Typically a starting point is already existing deterministic evaluation method
  - A mechanistic method is the “*backbone*”
  - Adding randomization of the problem variables
    - Involve Monte Carlo simulations
  - Outcome: probability of occurrence of the limiting condition
- **Examples:**
  - Probabilistic Fracture Mechanics (PFM):
    - Leak-Before-Break (LBB) of primary piping system – xLPR
    - Pressurized Thermal Shock (PTS) – FAVOR
  - CANDU reactor or Pressurized Heavy Water Reactor (PHWR) components
    - PFM of pressure tubes, feeder piping
    - Probabilistic Core Assessment (PCA) of pressure tube reactor core

Probabilistic Assessment Scope

- PA is **NOT** merely an enhancement of a deterministic method with Monte Carlo simulations
- PA is a **conceptual shift** in the paradigm of demonstrating operability
- **The scope of PA can be considerably expanded as compared to a deterministic method**
- Several additional factors to be considered
  - Initiation and propagation of a degradation mechanism
  - Occurrence of a "*limiting condition*" (or accident condition)
  - Operator response under accident condition
  - Role of inspection quality, detection probability and maintenance actions
- **PA is information and resource intensive undertaking**
  - Scope of the PA could be tailored as per the need

Guiding Principles

- A consensus view about key guiding principles of probabilistic assessment is needed
  - A rapid emergence of probabilistic approaches could have led to the development of rather piecemeal approaches to satisfy urgent needs
  - Different systems have different procedures with wide differences in the reported outcomes and the reporting requirements
  - Diversity of methods and results may create confusion among the stakeholders

Fundamental Features

- **Meaningful**: The assessment must be representative of the actual problem and the results must be relevant to the purpose of the assessment
  - The reliability metric must have a meaning to the problem
- **Consistent**: The risk and reliability must be consistently evaluated across Structure Systems and Components (SSC)
  - The principles of risk estimation should be the same for all systems
  - Otherwise, comparison and acceptance standards for risk will be problematic
- **Transparent**: All key assumptions, procedural steps and sources of data must clearly stated and justified
  - To allow scrutiny by independent review and Verification and Validation (V&V) work
  - To inspire confidence by the public and the regulator

Major Considerations

- The goal of most probabilistic assessments presumably is to demonstrate that
  - With reference to the limiting condition, the risk in the specified operating interval is less than some acceptable limit
- PA scope is much wider than that of the deterministic assessment
  - Consideration of time
  - Metric of assessment (conditional probability, frequency)
  - Consideration of the uncertainties
  - Overall realism in the assessment
  - Developing probabilistic acceptance criterion
- Foundation of PA: Theory of **Time-Dependent Reliability** Analysis

Consideration of Time

- The most important aspect of PA is the modeling of various time dependent processes
- Various assumptions are implicitly or explicitly introduced in the modeling, which has a great deal of bearing on the final interpretation of the results
- Degradation process
  - The defect is no longer assumed to exist on the component but rather crack initiation and growth processes modelled
- Loading conditions
  - Occurrence of overloading
- Operator response and intervention
- Effect of inspection and maintenance actions

Modeling and Assumptions of Degradation Process

- The nature of degradation process
  - Flaw initiation as a “*Stationary*” or “*Non-Stationary*” process
  - Homogeneous Poisson Process (HPP) is a stationary process
  - Defects initiate cracking at random without any particular time trend
  - HPP implies that time to initiation is an exponential distribution
- Crack initiation and growth process is independent across component population
  - Crack growth variability can be constant over time, or it can embody temporal variability (i.e., stochastic process)
  - Degradation process can restart after a maintenance followed by a leak detection event
- **Several such assumptions are embedded in PA**
  - They should be carefully examined and technically justified

1. Introduction
2. Probabilistic Assessment
3. Reliability Problems
4. Remaining Considerations
5. Closing Remarks
6. Acknowledgements

Involved Definitions

- **Reliability**

> *The probability of a system functioning within* ***specified limits*** *for a specified* ***time*** *under postulated conditions.*

- **Hazard Rate** (mortality rate)

> *Instantaneous probability of “first” failure conditional on survival up to a given age of the system.*

- **Failure Frequency**

> *Expected number of failures in a unit time interval.*

Reliability Metric

- The next important point is to choose a **reliability metric** that is relevant to the problem
- Reliability theory tells that the metric depends on the type of the problem
  - "*First failure*" (or **Non-repairable**) problem or
  - "**Repairable**" system reliability problem
- In the "first-failure" problem, the **mission reliability** or mission probability of failure is a relevant metric of reliability
  - The probability of failure in the operating interval given that equipment is functioning at the start of the interval
- In the repairable system problem, the **failure frequency** or **unavailability** is a relevant metric
  - The system is repaired or component replaced after each failure

Classification of Reliability Problems

- The probabilistic assessment should begin with classifying the type of the problem, repairable or non-repairable
  - How do we decide about this?
- Classification depends on
  - Type of performance limit state (serviceability or ultimate)
  - Nature of the failure mode (self-announced or latent)
  - Rate of progression from serviceability to ultimate state
  - Maintainability of the system
- **Performance limit state** means the state (or condition) of the system which divides the system performance into acceptable and non-acceptable domains
  - Introduced in "*structural reliability theory*"

Types of Limit States

- The **serviceability limit state** indicates a significant deterioration from the original design state
  - Not compromise system safety and functionality in any major way
  - Alarm which prompts to initiate mitigating actions
  - Presence of minor service-induced flaws is an example
- The **ultimate limit state** means a failure that would severely impair the system safety and functionality with potentially severe consequences
  - Rupture in Primary Heat Transport System (PHTS)

Progression of Limit States

- In some reactor components, serviceability and ultimate limit states might be closely connected events
  - The **progression** of a serviceability into an ultimate limit state over a period of time
  - Example: flow accelerated corrosion of a feeder pipe bend
    - The wall thickness loss up to a certain limit can be considered as a serviceability limit state
    - Excessive wall thinning can ultimately cause a feeder failure (leak or rupture)
- Hence, the **rate of progression** from a serviceability to an ultimate limit state is an important consideration

Nature of Failure Mode

- Two classes of **failure modes** are in the reliability theory:
  - A **self-announced failure** means that the occurrence of a failure is (almost) immediately detected by the operator/user of the equipment
    - A loss of power event is an example
  - A **latent failure**, as the name implies, means the occurrence of a system failure that is not detectable until an inspection is carried out
    - The failure of a **standby** system is a latent failure mode

Maintainability (1 of 2)

- Maintainability refers to the degree to which a system is **amenable to repair** (or replacement) after a failure, such that its operation can be restored to a safe and functional state
- It should be stressed that maintainability by itself does not determine the type of reliability analysis
  - Repairable vs. non-repairable
- A problem is repairable only if there is an opportunity to repair right after a failure
  - It means that the consequences of failure can be mitigated
- If operating conditions are such that a repair is not possible, then the problem belongs to the non-repairable category

Maintainability (2 of 2)

- Examples
  - An aircraft engine is designed to have high maintainability
  - A failure to start the engine on the ground is repairable
  - An in-flight engine failure is non-repairable
- In general, the issue of repairable vs. non-repairable problems is not a cut-and-dry situation, rather it depends on several factors that have been discussed

Repairable vs. Non-Repairable

- Some general **guiding principles** are given here
  - It is most appropriate to model an ultimate limit state as a non-repairable reliability problem
  - A latent failure mode is typically in the realm of a non-repairable reliability problem
    - Especially when the mode can progress into an ultimate limit state
    - The probability of failure over the inspection interval is a meaningful reliability measure
  - A self-announced, serviceability limit state can be modelled as a repairable problem provided that the system is maintainable
  - A latent, serviceability limit state of static nature can be modelled as a repairable problem
    - As long as this does not evolve rapidly into an ultimate limit state
- Summarizing, the classification of a reliability problem is very much dependent on **operational considerations**

Probabilistic Assessment Summary

Conceptual Elements	**Procedural Elements**
Purpose of assessment	Mechanistic model of performance
Reliability metric	Random variables in the problem
Type of reliability problem	Data and distribution fitting
Type of Limit States of performance	Reliability calculation method
Failure Mode (Self-Announced vs. Latent)	Uncertainty analysis
Progression of failure modes	Final results, reporting and discussion
Maintainability	
Acceptance criteria	

Conceptual and Procedural Elements

- The conceptual elements are important to
  - Interpretation of numerical results
  - Evaluation of the robustness of the assessment
- The procedural elements are important to an analyst
  - Data collection, statistical analysis, computational methods

1. Introduction
2. Probabilistic Assessment
3. Reliability Problems
4. Remaining Considerations
5. Closing Remarks
6. Acknowledgements

Realistic Assumptions

- Simulations are commonly used in PA
- Simulation could involve combination of variables which are physically unlikely to take place
  - Random sampling can choose values of the loads and the strength that are physically impossible
- Limitations of a mechanistic model used in the simulation
  - Probabilistic assessment is as good as the underlying mechanistic modelling
  - The model should cover a wide spectrum of all plausible events

Uncertainty Analysis

- Separation of epistemic and aleatory uncertainties
  - Include conceptual difficulties
- Computational burden could be challenging
  - Double-loop Monte Carlo simulations are quite intensive
  - Outcome is probability distribution of the reliability metric
  - Selection of adequate measure is debatable
  - Mean value versus some probability bound (50/95 percentiles)
- Prediction interval on the chosen reliability metric must be evaluated
  - Prediction interval is not the same as the confidence interval on the mean value
- Predictive models typically involve epistemic uncertainties

Acceptance Criteria

- Fully probabilistic criteria
  - The (conditional) probability of failure or failure frequency less than the allowable
- The formulation of acceptance criteria is a raucous process
  - Evaluation of acceptable reliability of SSCs is complex
  - Inter-dependencies and final effect on core damage is difficult to quantify
  - Tradeoff between increasing safety and resource utilization creates conflict

1. Introduction
2. Probabilistic Assessment
3. Reliability Problems
4. Remaining Considerations
5. Closing Remarks
6. Acknowledgements

Closing Remarks

- Probabilistic assessment is not merely a conversion of a deterministic method with Monte Carlo simulation
- Probabilistic assessment is a conceptual shift in the paradigm of demonstrating component or system operability
  - The scope and complexity can be more involved
- Presented broad principles, methods and approaches to improve probabilistic assessments of nuclear plant systems and components

Acknowledgements

- This work was funded by the Canadian Nuclear Safety Commission under R&S project R706.1