Open Issues Associated with Passive Safety Systems Reliability Assessment

Luciano Burgazzi
ENEA, Bologna, Italy
luciano.burgazzi@enea.it
Outline

• Introduction
  – Passive Systems
  – Passive Systems Reliability and Safety
  – Applications to advanced reactors
  – Thermal-hydraulic (t-h) Passive Systems

• Reliability Assessment Approaches

• Open Issues and Implementation
  – Uncertainties
  – Dependencies
  – Integration into accident sequences within a psa framework
  – Passive vs active systems

• Summary

• Outlook
Generics

• Innovative reactors largely implement passive safety systems

• Reactivity control, decay heat removal, fission product containment

• Applications of passive systems for innovative reactors demand high availability and reliability

• PSA analysis

• Accident sequence definition and assessment
  – Event Tree and Fault Tree model

• Introduction of a passive system within an accident scenario in the fashion of a front-line system and in combination with active systems and human actions
Recalls

• **IAEA (IAEA-TECDOC-626) definitions:**
  – *Passive Component*: a component which does not need any external input to operate
  – *Passive System*: either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation

• **Passive System Categorization:**
  – **A**: physical barriers and static structures,
  – **B**: moving working fluids,
  – **C**: moving mechanical parts,
  – **D**: external signals and stored energy (passive execution/active initiation)
# Classification of Passive Systems

<table>
<thead>
<tr>
<th></th>
<th>Category-A</th>
<th>Category-B</th>
<th>Category-C</th>
<th>Category-D</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input Signal,</strong></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>External Power Sources,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forces</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Moving Mechanical</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Parts</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Moving Working</strong></td>
<td>No</td>
<td>Yes</td>
<td>Yes/No</td>
<td>Yes/No</td>
</tr>
<tr>
<td><strong>Fluid</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Some examples</strong></td>
<td>Core cooling system relying only on radiation/conduction</td>
<td>Reactor cooling based on natural circulation</td>
<td>Systems consisting of accumulators or storage tanks and discharge lines equipped with check valves.</td>
<td>Emergency core cooling systems based on gravity/compress-ed Nitrogen driven flow of water activated by battery-powered valves.</td>
</tr>
<tr>
<td></td>
<td>Physical barriers against release of fission products</td>
<td></td>
<td>Mechanical actuators such as check valves and spring loaded relief valves</td>
<td>Mechanical Shut-Off rods</td>
</tr>
</tbody>
</table>
Examples
Passive Systems Reliability

- Probabilistic reliability methods for passive A safety functions have been extensively developed and applied in fracture mechanics.
- For several passive C and D systems reliability figures may be derived from operating experience.
- For passive B type systems basing on physical principle (natural circulation) denoted as t-h (thermal-hydraulic) passive systems, there is no agreed approach towards their reliability assessment yet:
  - Deviations of natural forces or physical principles from the expected conditions, rather than classical component mechanical and electrical faults.
  - System/component reliability (piping, valves, etc.):
    - mechanical component reliability
  - Physical phenomena “stability” (natural circulation):
    - factors impairing the performance/stability of the physical principle (buoyancy and density difference) upon which passive system operation is relying.

Thermal-hydraulic Passive Systems

- **Natural circulation:** small engaged driving forces and thermal-hydraulic factors affecting the passive system performance (e.g. non-condensable fraction, heat losses)

- System from the **predictable** nominal performance to the state of degradation of the physical principle in varying degrees up to the failure

- Occurrence of **physical phenomena** leading to pertinent failure modes

- Physical principle deterioration dependency on the **boundary conditions** and **mechanisms** needed for start-up and maintain the **intrinsic** principle

- Passive Systems for **decay heat removal** implementing in-pool heat exchangers and foreseeing the free convection (e.g. **PRHR** for AP 600 and AP 1000, **Isolation Condenser** for SBWR and ESBWR)
T-h Passive Systems in Advanced reactors

AP600/AP1000 Passive Residual Heat Removal (PRHR) System
Core Decay Heat removal from the reactor, by natural circulation following an isolation transient, including a heat source and a heat sink where condensation occurs via a heat exchanger.

Limit the overpressure in the reactor system at a value below the set-point of the safety relief valves, preventing unnecessary reactor depressurization.

Isolation Condenser actuation on MSIV position, high reactor pressure and low reactor level.

T-h Passive Systems in Advanced reactors

Isolation Condenser (SBWR, ESBWR)
Reliability Assessment Approaches (basics)

• To provide essentials for passive system reliability assessment (ENEA)

• Approach based on independent failure modes

• Approach based on failure modes of passive system hardware components

• Functional reliability or load-capacity approach
Reliability Assessment Approaches (integrated methods)

• To achieve a more consistent methodology,
  – to include t-h code simulations
  – to capture all the phenomena involved and their interactions
  – to merge probabilistic and physical, i.e. t-h, aspects

• REPAS (REliability of PAssive Systems)
  – ENEA, University of Pisa, Polytechnic of Milano, University of Rome

• RMPS (Reliability Methods for Passive Safety Functions)

• APSRA (Assessment of Passive System ReliAbility)
  – Bhabha Atomic Research Centre (India)
REPAS Method

Simplified diagram of the REPAS methodology

System & related design goals → Selection of system parameters → Ranges of variation for system parameters

Analysis

Transient acceptability target for the system performance
Calculation of system performance when varying system parameter values

Result

System reliability
RMPS Methodology: roadmap

1. Identification of the system
   - Mission of the system
   - Failure mode (FMEA)
   - Success/failure criteria

2. Modeling of the System
   - B-E Code selection
   - Model development
   - Model testing on reference scenarios
   - Definition of model limitations
   - Validation of the model
   - Refinement of success/failure

3. Identification of the relevant parameters (EJ, AHP)

4. Quantification of the uncertainties of the relevant parameters (EJ)

5. Sensitivity analysis (B-E code runs)
   - Linear
   - Non-linear

6. Screening of the uncertain parameters

7. Choice of the response surface and experimental design

8. Calculation with the B-E code for each point of the experimental design

9. Determination of the coefficients of the response surface

10. Propagation of the uncertainties
    - Direct propagation through the B-E code
    - Propagation through a response surface

11. Quantitative Reliability Evaluation
    - Monte-Carlo simulation (direct or accelerate)
    - FORM/SORM
RMPS Methodology: Objectives

• To propose a specific methodology to evaluate the reliability of passive systems

• Identification and quantification of the sources of uncertainties and determination of the important variables

• Propagation of the uncertainties through a T-H model and reliability evaluation of the T-H passive system

• Integration of the T-H passive system in an accident sequence, as a basic event

• www.rmps.info
APSRA Methodology

Step I. Passive system for which reliability assessment is considered

Step II. Identification of parameters affecting the operation

Step III. Operational characteristics and failure criteria

Step IV. Key parameters which may cause the failure

Step V. Generation of failure surface and validation with test data

Step VI. Root diagnosis to find deviation of key parameters for causing ultimate failure of system

Can be an active component such as valve  
Can be a passive component such as rupture disc

Step VII. Evaluation of failure probability of components to cause failure

Step VIII. Incorporation of reliability number into the CDF
Assessment of Passive Systems Reliability (APSRA)

- **Failure surface**

- **Deviations** of all critical parameters influencing the system performance

- **Causes of deviation through root diagnosis**

- **Mechanical components** (as valves, control systems, etc.)

- **Failure probability** through classical PSA (fault tree)

- **Comparison** of test data with t-h code prediction to reduce uncertainties
Open issues related to t-h passive systems reliability

- **Analysis** of the different methodologies proposed so far

- **Uncertainties**
  - Passive system performance
  - T-h code

- **Dependencies**
  - Relevant variables

- **Integration** of passive systems into an accident sequence within a psa framework

- Passive vs **active** systems
Sources of uncertainties related to passive system performance

- **Uncertainties** related to natural circulation system behaviour prediction
  - Deviations of the natural forces or physical principles from the expected conditions
  - Phenomenological uncertainties, due to scarcity of operational and experimental data
  - Epistemic Uncertainties, i.e. related to the state of knowledge

- **Difficulties** in performing meaningful reliability analysis and deriving credible reliability figures
  - Expert judgment elicitation and engineering/subjective judgment


Categories of uncertainties associated with T-H passive systems reliability assessment

- **Zio, E., Pedroni, N.**, *Building confidence in the reliability assessment of thermal hydraulic passive systems*. Reliability Engineering and System Safety, 94 (2009), 268-281

<table>
<thead>
<tr>
<th>Aleatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geometrical properties</td>
</tr>
<tr>
<td>Material properties</td>
</tr>
<tr>
<td>Initial/boundary conditions (design parameters)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Epistemic</th>
</tr>
</thead>
<tbody>
<tr>
<td>T-H analysis</td>
</tr>
<tr>
<td>Model (correlations)</td>
</tr>
<tr>
<td>Parameters</td>
</tr>
<tr>
<td>System failure analysis</td>
</tr>
<tr>
<td>Failure criteria</td>
</tr>
<tr>
<td>Failure modes (critical parameters)</td>
</tr>
</tbody>
</table>
Sources of uncertainties related to t-h code

• Uncertainties in the best estimate codes can arise due to e.g.,
  – Inadequate physical models built in the codes to represent a specific phenomena;
  – Absence of models to represent a particular phenomena;
  – Approximation in simulating system geometry;
  – Deviations of the input parameters in respect of initial and boundary conditions;
  – Uncertainties in thermophysical properties and thermohydraulic relationships.

• The uncertainty analysis (of a code prediction) implies a procedure to evaluate the precision (or the error) that characterizes the application of a best-estimate code

• The reliability analysis (of a system) aims at characterizing the ability of a system ‘to operate satisfactorily’, following assigned specifications, over a period of time

• Therefore the uncertainty of the code can affect the prediction of the system
Uncertainty and sensitivity qualitative analysis

Grade Rank for Uncertainty and Sensitivity

<table>
<thead>
<tr>
<th>Grade</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>The phenomenon is not represented in the computer modelling or the model is too complex or inappropriate which indicates that the calculation results will have a high degree of uncertainty.</td>
</tr>
<tr>
<td>M</td>
<td>The phenomenon is represented by simple modelling based on experimental observations or results.</td>
</tr>
<tr>
<td>L</td>
<td>The phenomenon is modelled in a detailed way with adequate validation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grade</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>The phenomenon is expected to have a significant impact on the system failure</td>
</tr>
<tr>
<td>M</td>
<td>The phenomenon is expected to have a moderate impact on the system failure</td>
</tr>
<tr>
<td>L</td>
<td>The phenomenon is expected to have only a small impact on the system failure</td>
</tr>
</tbody>
</table>

Failure Modes related Uncertainty and Sensitivity

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>UNCERTAINTY</th>
<th>SENSITIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Envelope failure</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Cracking</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Non-condensible gas</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Thermal stratification</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Surface modification</td>
<td>M</td>
<td>L</td>
</tr>
</tbody>
</table>


Expert judgment elicitation process
Open Issues: Dependencies

- Assumption of independence among relevant parameters adopted in the analysis (zero covariance)
  - safety variables
    - e.g. flow rate, exchanged heat
  - critical parameters driving the modes of failure
    - e.g. non-condensable gas

- In case of dependence (e.g. degradation measures), parameters can not be combined freely and independently

- Joint pdfs, e.g. multivariate distributions
- Conditional subjective probability distributions
- Covariance matrix
- Functional relationships between the parameters

Open Issues: Integration of passive systems within an accident sequence

• Limitations of PSA (event tree development)
  – Binary representation (success or failure, intermediate states are usually not treated)
  – Time treatment (chronology of events instead of actual timing)

• Need for the development of dynamic event tree in order to evaluate the interaction between the parameter evolution during the accident and the system state

• Evaluation for 72 hours grace period, compared to 24 hrs in classical PSA

• Time-variant stochastic process
  – the evolution of physical parameters over time, in terms of probability distributions

Open Issues: Active vs Passive

- **Functional** and **economic** comparison of active vs passive safety systems, required to accomplish the same **mission**

- **Passive**
  
  - **Advantages** e.g.,
    - No **external power supply**: no loss of power accident
    - No **human factor**
    - Better **impact** on public acceptance, due to the presence of “natural forces”
    - Less complex system than active and therefore economic competitiveness
  
  - **Drawbacks** e.g.,
    - Reliance on “**low driving forces**”, as a source of uncertainty
    - **Licensing** requirement (open issue)
    - Reliability assessment in any case (lack of data)
Conclusions and Path forward (1/3)

• As the future reactor concept makes use of pass**ive safety features** in combination with active safety systems, the question of Natural Circulation Decay Heat Removal (NCDHR) reliability and performance assessment into the ongoing PSA constitutes a challenge

• Development of a consistent methodology for the evaluation of the reliability of the passive systems

• **Future needs**
  
  - **Clear rules for identification and quantification of uncertainties.**
  - **Formal expert judgment (EJ) protocol to estimate distributions for parameters whose values are either sparse or not available.**
  - **Sensitivity analysis techniques to estimate the impact of changes in the input parameter distributions on the reliability estimates.**

  - **Clear distinction** between the prediction of the thermal hydraulic code and the true behaviour of the passive system under consideration.
    - **Problem of model uncertainties**

  - **The time dependence** of the passive system reliability
    - **Dynamic event trees**
Conclusions and Path forward (2/3)

Future needs (following):

- Evaluation of the dependencies among relevant system parameters
- Comparison of different methodologies
- Merge elements of different methodologies: RMPS, APSRA/BARC, REPAS and ENEA methodologies, since high dependency of results upon the assumptions underlying the models
- Establish guidelines and criteria for the comparison of active and passive systems
Conclusions and Path forward (3/3)

International efforts in progress

- **IAEA Coordinated research project (CRP) on** “Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors” (2008-2011)
  - the objective is to determine a common analysis-and-test method for reliability assessment of passive safety system performance

  - TECDOC-XXXX, “Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants”, ready for publication