EASI SMR

D4.1: Identify and Review the Methodologies Currently Used for Passive System Reliability Evaluation

Y. Louet (EDF), F. Mascari, E. Cilia (ENEA), B. Grosjean (CEA), O. Sevbo (ENERGORISK), J. C. De La Rosa BluL (JRC), O. Zhabin (SSTC NRS), D. Grishchenko (KTH), P. Bízek (UJV)

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Atomic Energy Community ('EC-Euratom'). Neither the European

Table of Contents

List of Figures

List of Tables

Document information

Grant Agreement Number	n°101164810
Project Title	Ensuring Assessment of Safety Innovations for SMR
Project Acronym	EASI-SMR
Project Coordinator	Nicolas Sobecki
Project Duration	1 September 2024 – 31 August 2028 (48 months)
Related Work Package	WP4
Lead Organisation	ENEA
Contributing Partner(s)	Y. Louet (EDF), F. Mascari, E. Cilia (ENEA) B. Grosjean (CEA), O. Sevbo (ENERGORISK), J. C. De La Rosa BluL (JRC), O. Zhabin (SSTC NRS), D. Grishchenko (KTH), P. Bízek (UJV)
Submission Date	30/09/2025
Dissemination Level	Public

History

Date	Submitted by	Reviewed by	Version (Notes)
August 18, 2025	Petr Bizek	Fulvio Mascari	V1
August 27, 2025		Nicolas Sobecki	V2
September 29, 2025		Fulvio Mascari	VF

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Executive Summary

Deliverable D4.1 represents the first outcome of Work Package 4 (Reliability of Passive Systems) within the EASI-SMR project. It provides a comprehensive review and comparison of methodologies currently applied to the reliability assessment of Passive Safety Systems (PSSs) in nuclear reactors, with particular focus on their applicability to Light Water Small Modular Reactors (LW-SMRs).

The analysis combines an extensive bibliographical survey with a structured evaluation of approaches such as REPAS, RMPS, APSRA, ROAAM+, and PSA-based frameworks. Each method was assessed in terms of its ability to address functional failures, quantify uncertainties, and integrate deterministic and probabilistic elements. The strengths, limitations, and specific conditions of applicability were identified, highlighting their potential role in Probabilistic Safety Assessment (PSA) and Deterministic Safety Assessment (DSA).

Key findings confirm that while PSSs offer significant safety advantages by relying on inherent physical principles such as natural circulation, their reliability cannot be assumed a priori and must be rigorously demonstrated. Challenges remain in modelling functional failures, addressing scaling effects, and managing uncertainties. Recent progress in the last decades, including advances in dynamic reliability methodologies and the integration of Artificial Intelligence (AI) techniques, offers promising pathways to improve realism and computational efficiency, but these approaches are still at varying levels of maturity.

The deliverable also reviews current international requirements and recommendations (IAEA, WENRA, national regulations), emphasizing the need for harmonized methodologies, validated computational tools, and robust experimental support. In line with these recommendations, WP4 will focus on establishing a consistent framework for quantifying PSS reliability that is technically sound, risk-informed, and defensible for regulatory purposes.

The findings of D4.1 provide essential input to subsequent tasks of WP4 and contribute to the broader objectives of EASI-SMR: ensuring that passive safety innovations are effectively integrated into LW-SMR designs, thereby supporting licensing readiness, public acceptance, and the safe deployment of advanced nuclear systems in Europe

Keywords

Passive, safety, reliability, natural circulation, nuclear, SMR, PSA, DSA, T-H, NPP.

Abbreviations and acronyms

Acronym	Description
AI	Artificial Intelligence
AOO	Anticipated Operational Occurrence
APSRA	Assessment of Passive System ReliAbility
BDBA	Beyond Design Basis Accident
BE	Best-Estimate
BP	Basic Principle
CBC	Closed Boundary Conditions
CCF	Common Cause Failures
CDF	Core Damage Frequency
CR	Causal Relationships
DBA	Design Basis Accident
DDM	Data Driven Methodology
DiD	Defence-in-Depth
DSA	Deterministic Safety Assessment
ECCS	Emergency Core Cooling System
EOT	End Of the Transient
EPZ	Emergency Planning Zone
ET	Event Tree
FC	Failure Criteria
FM	Full Model
FMEA	Failure Mode and Effects Analysis
FOAK	First Of a Kind
FOM	Figure Of Merit
FSAR	Final Safety Analyses Report
FT	Fault Tree
IAEA	International Atomic Energy Agency
IC	Isolation Condenser
IE	Initiating Event
IETF	Integral Effect Test Facility
INS	Innovative Nuclear Energy System
I-PoF	Integrated physics-of-failure methodology
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-Site Power
LRF	Large Release Frequency
LWR	Light Water Reactor
LW-SMR	Light Water SMR
NC	Natural Circulation
NCG	Non-Condensable Gas
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant

Acronym	Description
OECD	Organisation for Economic Co-operation and Development
OPEX	Operational experience
PCT	Peak Cladding Temperature
PDF	Probability Density Functions
PDS	Plant Damage States
PFM	Probabilistic Fracture Mechanics
PHRS	Passive Heat Removal System
PI	Performance Indicator
PRA	Probabilistic Risk Assessment
PRZ	Pressurizer
PSA	Probabilistic Safety Assessment
PSS	Passive Safety System
PWR	Pressurized Water Reactor
RD&D	Research, Development and Demonstration (RD&D)
REPAS	Reliability Evaluation of Passive Safety Systems
RMPS	Reliability Methods for Passive Safety Functions
ROAAM+	Risk Oriented Accident Analysis Methodology
RPV	Reactor Pressure Vessel
SA	Severe Accident
SAM	Severe Accident Management
SBC	Scenario Boundary Conditions
SET	Separate effect Test facility
SM	Surrogate Model
SMR	Small Modular Reactor
SSC	Structure, System or Component
T-H	Thermal-Hydraulic
TM	Target Mission
TPI	Transient Performance Indicator
TS	Test Section
WP	Work Package

1. Introduction

In the field of nuclear reactor safety, PSSs have gained increasing attention due to their capability to perform safety functions without relying on external power sources (mainly for their long-term operation), active components, or operator intervention. By leveraging inherent physical principles, mainly gravity-driven mechanisms like natural circulation, PSSs offer certain conceptual advantages, particularly in scenarios involving the loss of off-site power or system failures (generally for transients with loosing or reducing the heat removal). PSSs can be used to perform key safety functions such as safety injection and residual heat removal (both from the core and containment).

While PSSs are often regarded as potentially more robust due to their inherent simplicity and reduced reliance on components requiring external power for the operation, their reliability — along with their performance across the wide range of possible operational and accidental conditions — must be demonstrated through rigorous analysis, not simply assumed because based on natural forces with low driven forces (as gravity). This includes a comprehensive evaluation of system behaviour under variable boundary conditions and transient scenarios, supported by qualified modelling tools and experimental validation.

Reliability analysis of PSSs is complicated mainly due to the systems' dependence on inherent physical principles, unlike the reliability of active systems, which can be more easily evaluated by conventional reliability approaches, based moreover on existing operational data. Uncertainties account for a major reason for the difficulty in evaluating PSS reliability.

A consistent and systematic reliability assessment methodology is therefore essential. This includes accurate modelling of system behaviour, robust reliability evaluation, and the consideration of other influencing factors such as materials degradation or coupling with other systems. Such an approach helps to minimize uncertainties and allows for more realistic and defensible reliability estimates.

The performance of PSSs is strongly dependent on system design and operational parameters. Deviations from nominal conditions can lead to functional failures (performance losses due to phenomenological deviations rather than mechanical breakdown). Complicating matters further, the same passive phenomena can be involved across multiple levels of Defence-in-Depth (DiD), raising concerns about Common Cause Failures (CCF) and making it more difficult to define and detect failure boundaries. Despite these challenges, reactor designers have been successful in addressing them, and several countries have supported the use of PSSs in advanced NPPs.

In practice, the behaviour of PSSs is often assessed using scaled-down experimental facilities, which inevitably introduce scaling-related uncertainties. These facilities typically support the evaluation of system performance under a limited number of operational scenarios, each involving transient conditions lasting several hours. Under such conditions, PSSs are generally found to satisfactorily fulfil their Target Mission (TM). However, when a broad spectrum of scenarios — on the order of thousands — is analysed, failures related to the TM may emerge due to variability in system response.

Given the impracticality of conducting such a high number of experimental tests, numerical simulations can integrate experiments for PSS reliability assessment. This mix approach, however, requires the use of fully qualified computational models, rigorously validated against experimental data, and capable of appropriately addressing scaling effects and boundary

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

condition variations. Moreover, the application of "extreme case" analysis — involving low-probability but high-impact combinations of input parameters — is a key strategy for identifying scenarios susceptible to functional deviation or failure and for defining the performance envelope of the system under investigation. This ensures that the assessment captures the full range of plausible system behaviours across the spectrum of possible conditions [2].

This report aims to critically review the methodologies currently adopted in the research community for evaluating the reliability of PSSs. The objective is to identify both the strengths/advantages and limitations/gaps in the existing approaches, with a focus on their applicability to realistic reactor conditions, the treatment of uncertainties, and the qualification of simulation tools. By doing so, the report seeks to support the development of more consistent and technically sound frameworks, enhancing the robustness of reliability assessments for PSSs in nuclear reactor applications.

1.1. Main Pillars of EASI-SMR and Context of WP2/WP3/WP4

Nuclear energy is increasingly viewed as a key solution to achieve Europe's Net Zero Goal by 2050, driving interest in advanced reactor technologies such as LW-SMRs. LW-SMRs offer inherent safety, simplified modular designs, shorter construction times, lower capital and operational costs, and are based on mature Light Water Reactor (LWR) technology. They can be effectively deployed in diverse applications, including electricity generation, district heating, and industrial processes. However, despite their many advantages, LW-SMRs are characterized by some safety challenges that must be addressed before their deployment.

The EASI-SMR project is structured to meet the challenges identified in the Work Stream 5 (WS5) roadmap of the EU SMR Pre-Partnership [3], and it has built in the frame of the NUGENIA Technical Area 6 [4] in a way to ensure that its research activities directly address the key challenges identified for a safe deployment of LW-SMR in Europe. Specifically, the project aims to ensure the highest level of safety of LW-SMRs based on PSSs integrating them into the EU regulatory framework. It also assesses the safety impact of LW-SMR designs features, considering their specific operational characteristics and technological innovations to guarantee compliance with European safety standards. Furthermore, it addresses regulatory and societal challenges towards the deployment of SMRs in Europe by fostering collaboration with the main stakeholders as regulatory bodies, policymakers, industry, research centers to contribute to develop harmonized licensing approaches and increase public trust in SMR technology. By integrating these objectives into a coordinated research effort, the EASI-SMR project contributes to creating a sound technical framework in Europe to support the safe deployment of LW-SMRs.

It specifically targets two leading European SMR designs—France's NUWARD [5] and Finland's LDR-50 [6] — incorporating innovations such as PSSs, hybrid co-generation, multi-module operation, etc. Coordinated by EDF, the EASI-SMR consortium comprises 38 partners from 16 countries and runs from September 2024 to August 2028, supported by €14.9 million in EU funding (total budget €23.6 million).

As said before, the EASI-SMR project is structured to address the key R&D challenges outlined in the EU SMR Pre-Partnership roadmap, ensuring that LW-SMR technology advances in alignment with European strategic priorities. EASI-SMR project is organized into 7 technical Work Packages (WPs) that systematically address these research topics:

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- **WP1**: Transverse topics for LW-SMR acceptability and licensing;
- **WP2**: Experimental tests program;
- **WP3**: Code validation, scaling;
- **WP4**: Reliability of passive systems;
- **WP5**: Human & Organizational Factors;
- **WP6**: SG Mock-up by additive manufacturing techniques;
- **WP7**: Advanced Core Physics Studies of Boron-Free SMR-cores;
- **WP8**: Communication, Education & Training;
- **WP9**: Project Management and Coordination),

as shown in the **Figure 1** listed below.

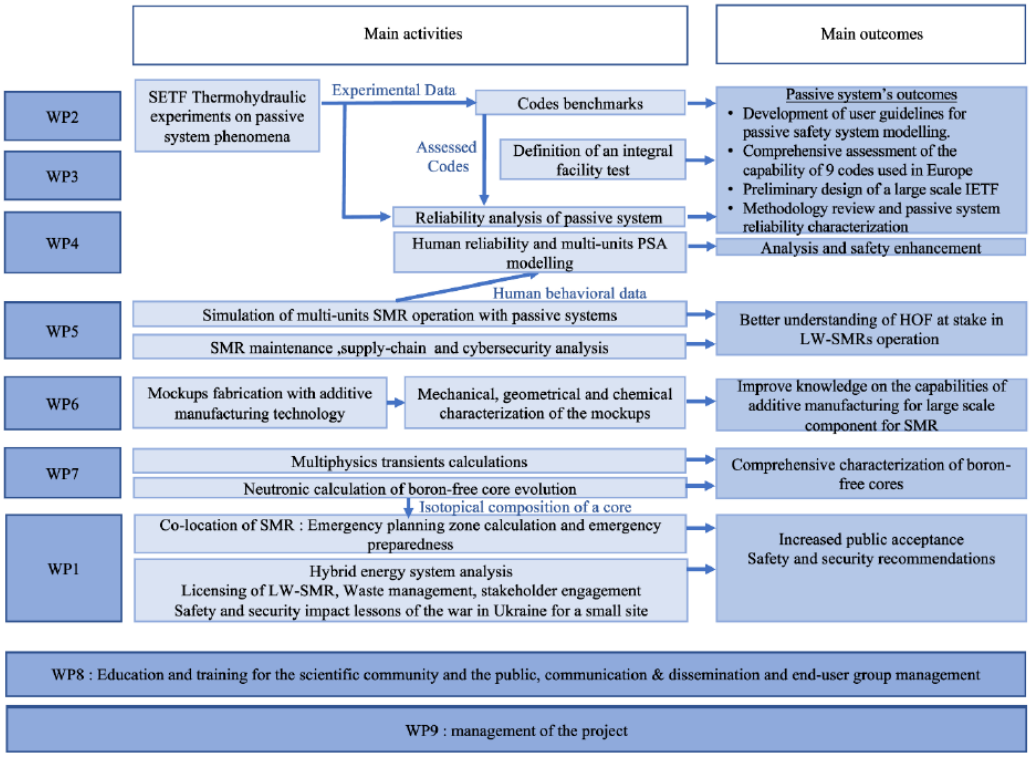

Figure 1 Overall organization of the EASI-SMR activities

Within this regard, the core of the project consists of three interconnected technical WPs, WP2/WP3/WP4, aiming at trying to address the key R&D needs related to PSSs performance assessment. In particular, benefiting of the activity in progress or already finalized in other EU projects (e.g. ELSMOR [7], McSAFER [8], PASTELS [9], SASPAM-SA [10], TANDEM [11]), the target of these WPs is to be synergic with them and address the still remaining lack of experimental data, the lack of validation of safety analysis codes, and the lack of safety assessment methodologies for PSS reliability analyses. In particular:

- **WP2 – Experimental Testing Program, coordinated by CEA (France):** Develops a new experimental campaign to investigate the key phenomena/processes that take place along the operation of PSSs under Design Basis Accident (DBA) and Beyond Design Basis

Accident (BDBA) conditions in LW-SMR. The experimental data generated in this WP provides the base for code validation in WP3.

- **WP3 – Code Validation and Scaling, coordinated by ENEA (Italy):** Assesses the capability of European-developed computational codes to simulate DBA and BDBA scenarios in LW-SMR. This WP also identifies best practices for PSSs modeling and highlights areas for further code development to improve simulation accuracy. The assessed codes will be used in WP4 for testing PSS reliability assessment methodologies. Given that the experimental facilities used in WP2 are primarily Separate Effect Test Facilities (SETFs) and no large-scale Integral Effect Test Facility (IETF) currently exists with open-access data, WP3 will also focus on developing a feasibility study for a large-scale IETF.
- **WP4 – Reliability of Passive Systems, coordinated by UJV (Czech Republic):** Applies the assessed codes from WP3 to perform reliability assessments for selected PSSs (ELSMOR II facility). The next evaluated facility here will then be the HWAT from KTH (using earlier validated codes). This WP, mainly oriented on PSA (and on DSA as well), focuses on quantifying uncertainties and system failure probabilities, risk analysis, and licensing readiness, ensuring that passive safety innovations will have a direct impact on lower risk values and a better overall safety of the new LW-SMRs, while simultaneously meeting regulatory requirements.

This structured process — from experimentation in WP2, to computational tool validation in WP3, and reliability assessment in WP4 — creates a comprehensive and interconnected safety demonstration framework that addresses the most R&D needs in LW-SMR development.

1.2. Importance of Reliability Analysis for PSSs

PSSs are an integral part of all new build (especially for SMRs) and it is broadly expected that their incorporation into the modern NPPs design will lead to the overall increase of their inherent safety (in comparison with current units). This topic is also crucial for their future development, licensing and also for their long-term safe operation and has also a direct impact to many other areas related to safety (PSA and DSA application, Emergency Planning Zone -EPZ- etc).

IAEA SSR-2.1 [12] requires considering reliability of active and PSSs (§ 5 General plant design requirement 23) as follow:

The reliability of items important to safety shall be commensurate with their safety significance.

5.37. The design of items important to safety shall be such as to ensure that the equipment can be qualified, procured, installed, commissioned, operated and maintained to be capable of withstanding, with sufficient reliability and effectiveness, all conditions specified in the design basis for the items.

5.38. In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes. Preference shall be given in the selection process to equipment that exhibits a predictable and revealed mode of failure and for which the design facilitates repair or replacement.

The reliability is the probability that a system or component will meet its minimum performance requirements when called upon to do so, for a specified period of time and under stated operating conditions. The reliability assessment is than a key factor for determining and ensuring that the PSS has the required reliability to fulfil its proposed safety function in the global plant design.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Contrary to active systems, the reliability of PSSs does not only depend on the failure rate of active components (e.g.: I&C, valves, pumps) but also (rather mainly) on the failure due to the deviation of process parameters, configuration of the system and unknown phenomena during a given scenario. This failure is named **functional failure**, and its (numerical) value depends on the initiating event and transient involving the PSS (generally on "specific boundary conditions" for analysed scenario). The numerical value is then incorporated into the PSA model structures to evaluate if and how the PSS functional failure contributes to risk – typical both to the Level 1 and Level 2 risk metrics, such as Core Damage Frequency (CDF) and Large Early Release Frequency (LERF).

From the PSA perspective, all SMRs vendors declare a very low values of their overall key risk indicators/metrics, specifically by a several orders of magnitude lower comparing to current operational units (CDF, LERF/LRF) mainly due to the inclusion of PSSs. But the basic question is whether is this realistic and will these SMRs really be that much more reliable in comparison with the current units? And are their vendors also able to prove it and convince the regulator and also the public about it? Moreover, the behaviour and function of PSSs (unlike the active ones) can be affected by uncertainties. **Therefore, it is essential to develop and use a consistent reliability method which when implemented can produce realistic results.**

Note: Importance of this topic also comes e. g. from the lates revision of the key IAEA safety guide for Level 1 PSA named SSG-3 (2024 [13]) where the new related recommendations for reliability analysis were added. This guide does not specify which current approach is the "best". Instead of, there is just a link to the more than ten years old IAEA TECDOC-1752 [1] (because there is nothing newer). The structure and content of individual tasks in WP4 is then proposed considering the recommendations in Chapter 5 of the SSG-3 latest (2024) revision [13].

1.3. Functional Failure

In active safety systems, reliability is typically ensured through redundancy, robust engineering practices, high-quality components, and rigorous programs of qualification, maintenance, and testing. Failures in these systems are generally due to identifiable mechanical or electrical faults, commonly referred to as **active failures**. Furthermore, failures in an active system can be often easily identified and also prevented through periodical testing and during regular maintenance.

In contrast, PSSs — which operate based on inherent physical principles and have no moving parts after activation — are inherently less susceptible to conventional hardware failures. However, they remain vulnerable to what is known as **functional failure** (also referred to as "phenomenological" failure), which can occur even in the absence of mechanical degradation. This type of failure arises when, due to low driving forces and high sensitivity to environmental or boundary conditions, the system deviates from expected behaviour or fails to deliver its intended safety function. In many cases, such conditions may depart from design assumptions while leaving the hardware intact.

A key challenge is the uncertainty surrounding the full range of operational scenarios that a PSS may experience. Under certain combinations of external and internal conditions, the T-H load may exceed the system's capacity or narrow the available safety margins, ultimately resulting in functional failure.
Critical parameters that may contribute to functional failure typically include:

- Presence of non-condensable gases;
- Undetected leaks;

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- Excessive heat losses;
- Suboptimal piping layout;
- Limited valve opening area in discharge lines;
- Fouling or plugging in heat exchangers.

These aspects require further clarification from a deterministic perspective, particularly to identify and assess the conditions under which they can occur. The development and application of appropriate methodologies to investigate such effects are therefore essential [2]. The methodology adopted in this report to address functional failure will be discussed in the following sections.

1.4. Link between PSA and DSA Approaches

Link between PSA and DSA is typically provided by the following steps:

- Selection of important initiating events and sequences in the accident/scenario progression using the input from PSA.
- Phenomenological analysis of the selected scenarios using a deterministic model coupled with a risk assessment approach.
- Identification of the key/dominant parameters (typically phenomenological) that are of the highest importance for the development of the accident progression.
- Improvement / re-definition of PSA sequences to adequately reflect phenomenological aspects of accident progression, PSS failure mechanisms, etc.:
    - Phenomenological findings can suggest the need to refine PSA event trees when specific parameters of a scenario have important impact on the outcome. E.g. the Plant Damage States (PDS) corresponding to the core damage due to inadequate core coolant inventory makeup at high pressure and low pressure, may require modification to include the:
        - Effect of water pool depth in the lower drywell:
            - Deep water pool;
            - Shallow water pool;
            - No water pool.
        - Lower head breach size:
            - Dripping flow;
            - Medium flow;
            - Large flow.
- Estimation of conditional failure probabilities and/or their distributions depending on sequences and varied parameters taking into account available knowledge on epistemic uncertainty.

For instance, ROAAM+ framework provides an assessment of the effect of epistemic (knowledge) uncertainty on the results employing “knowledge-based treatment” of epistemic uncertain parameters, i.e., no probability distributions of epistemic uncertain parameters are assumed if there is no available knowledge about them (see section 2.2.4. for more details)

ROAAM+ based examples of PSA/DSA integration can be found e.g. in [14], [15].

For instance, the REPAS/RMPS methodology provides a structured and systematic framework for integrating DSA with PSA, tailored to PSSs. This integration is realized through a multi-step process in which thermal-hydraulic system behavior is first analyzed deterministically using best-estimate (BE) codes (e.g., CATHARE, RELAP5, TRACE) to characterize a reference system configuration and mission success criteria. This deterministic baseline serves as the anchor point for the probabilistic component. Probabilistic elements are introduced by assigning PDFs to key design and operational parameters, which reflect the epistemic and aleatory uncertainties of the system. These uncertainties are propagated through stochastic sampling (e.g.. Monte Carlo techniques), enabling the generation of multiple system configurations. Each configuration is evaluated deterministically to assess whether the system satisfies the predefined Failure Criteria (FCs). The outcome is a reliability metric expressed as the conditional probability of system failure, given parameter variability and scenario conditions. This two-tier approach allows REPAS to quantify the likelihood of functional failure due to the degradation or deviation of passive phenomena (e.g., natural circulation) under realistic and uncertain conditions. The integration of DSA and PSA in REPAS not only enhances the robustness of the safety case but also enables risk-informed design optimization and decision-making in the development and deployment of passive safety features in SMRs.

1.5. Current progress on reliability assessment of passive systems (last 10 years) and compare results with IAEA TECDOC-1752

PSSs, which operate using natural forces such as gravity or natural convection rather than external power sources or operator action, are central to advanced reactor designs (including SMRs). Over the last decades, significant progress has been made in improving the assessment of PSSs reliability. In particular, key achievements include advanced approaches, benchmarks and regulatory guidance.

The IAEA TECDOC-1752 [1], issued in 2014, deals with early attempts to determine a common method for reliability assessment of PSSs in new nuclear reactor designs. For such systems, there is no operational data that would allow classical statistical reliability analysis (see Section 2.2.5 for more details regarding the statistical reliability analysis). Therefore, several approaches dealing with combination of deterministic and probabilistic aspects have been compared and benchmarked in the framework of IAEA TECDOC-1752, including:

- Reliability Evaluation of Passive Safety System (REPAS) methodology integrating DSA with probability aspects (see Section 2.2.1)
- The Risk-Informed Methodology for Passive Systems (RMPS), and its enhanced variant RMPS+ (see Section 2.2.2);
- The Advanced Passive System Reliability Assessment (APSRA) method (see Section 2.2.3);
- An approach, based on independent failure modes, which uses traditional techniques, such as Failure Mode and Effect Analysis (FMEA), to identify contributors to the PSS failure (see Section 2.2.5).

The insights from the study have shown that there is a clear need to obtain more data, especially related to thermal hydraulics. This conclusion highlighted the need for further development, testing, and research to address the unique technical challenges, posed by advanced reactor

technologies, including the need to consider diverse systems and phenomena, limited availability of critical reliability and experimental data, gaps in knowledge about new key phenomena, and also the lack of established accident analysis models. Moreover, it is essential to thoroughly assess the reliability of passive and evolutionary components, as well as CCFs in highly redundant systems and intersystem CCFs.

Simplified modelling approaches that were previously accepted may no longer be suitable for assessing the reliability of advanced reactors (including SMRs). For instance, to simplify analysis, the overall reliability of T-H PSSs was commonly assessed by evaluating the reliability of key individual components comprising the system. However, in most studies, the failure or performance assessment of these PSS components does not consider environmental influences or interactions. As a result, the effects of system or component dependencies on reliability are often not accounted for. To overcome these limitations, several advanced methods have been proposed – e.g., methods related to multivariate analysis/dependency consideration of critical parameters. Such methods include application of correlation analysis ([16], [17]), covariance matrix techniques [18], conditional subjective probability density function methods and other.

Past decade, the functional failure concept (see Section 1.3) was also applied for assessment of PSSs for SMR and Gen-IV reactors. For instance, [19] uses functional failure concept for analysis of the decay heat removal system in Gen-IV Sodium-cooled Fast Reactor. The functional reliability was calculated by uncertainty propagation of the system parameters that can affect system failure.

An emerging methodology related to deterministic aspect of PSS reliability assessment involves application of AI analysis to speed up computation by substituting the computationally demanding T-H code simulations with a simpler and faster surrogate metamodels. Several approaches that utilize artificial intelligence techniques have been recently developed/promoted. Examples include application of artificial neural networks [20], radial basis functions and support vector machines[1], and adaptive metamodel-based subset importance sampling [21].

In [22] a framework to identify the combinations of input configurations such as sequences of events, component states and values of design variables that can lead to functional failure or critical conditions of PSSs was developed. A time-demanding best-estimate T-H model of the system is used to train a fast-running metamodel embedded within an adaptive sampling technique (adaptive kriging Monte Carlo Sampling) to provide improved accuracy in proximity of the failure threshold and identify the input values that lead to PSS failure. Accounting for the time-variancy of the reliability of PSSs becomes essential to make the reliability methods more realistic and accurate.

Despite the clear benefits of AI, there are several concerns. As stated in [2], since the limited-size set of input/output data examples is used to construct the surrogate model, an important issue is the suitable choice of training data. Once the model is built, it is used to perform, in a negligible computational time, the functional failure analysis of PSS: in particular, the functional failure probability of the system is estimated together with global sensitivity indices of the naturally circulating coolant temperature. The use of regression models in safety-critical applications, such as NPPs, raises concerns about the model accuracy, which must be not only verified but also

[1] Support Vector Machines are supervised machine learning algorithms primarily used for classification tasks. They work by finding the optimal hyperplane that best separates data points into different classes, maximizing the margin between these classes. SVMs can handle both linear and non-linear data separation by using kernel functions.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

quantified. One of the approaches to obtain effective training data is presented in [23], where two-stage strategy is proposed: an initial sampling to gather information on the decision boundary, followed by an additional sampling stage to amplify the failure cases or to reduce data imbalance. The proposed method can construct the classifier with higher accuracy and precision even with a smaller dataset.

Another evolving area in the reliability assessment of PSS is consideration of dynamic aspects. The methods implemented to date generally do not consider dynamic failure of components or processes. Thus, in REPAS/RMPS, variation of process parameters is considered through a PDF treatment, with PDFs assumed to be invariant in time. However, in reality, the parameter variations from their nominal values could be time dependent. Similarly, APSRA relies on calculating failure probabilities of components for treatment of variation of process parameters through classical fault tree and event tree approach. These methods represent component failures using binary states, i.e. treating the components as either fully functional or completely failed. However, such components as control or relief valves may fail at intermediate states. Furthermore, some components do not fail instantaneously but instead experience gradual degradation over time, with functional performance deteriorating as the accident progresses. This partial degradation can significantly influence the PSS effectiveness, particularly in extended mission scenarios.

To obtain a more accurate estimate of PSS failure probability, dynamic reliability methodologies need to be incorporated into the analysis. These methodologies rely on integration of probabilistic and deterministic models to evaluate PSS in consistent manner (e.g., for proper consideration of long mission time in the models). Dynamic reliability methodologies are currently developed as dynamic PSA methods, such as state transitions or Markov models; dynamic event trees (both continuous and discrete); continuous event trees.

The objective of dynamic PSA is to capture the interplay between system process dynamics and its stochastic behaviour across different stages. The approach combines the parameter/state assessment capabilities of T-H analysis with the scenario development strengths of dynamic event tree methodologies in order to evaluate both the physical evolution of technical parameters and the frequency of accident sequences under dynamic conditions. When component failure probabilities (e.g., valve per-demand failure rates) are known, they can be integrated with the probability distributions of estimated parameters to forecast the probabilistic progression of each scenario outcome.

However, there are several challenges related to dynamic PSA:

- Availability of data

  Similar to a conventional (static) PSA model, the dynamic PSA model will likely include some parameters for which data are sparse (e.g., failures of analogous components under accident-like conditions), observable but not yet observed, or not even directly observable. Depending on the sensitivity of the PSA to the parameters, these data limitations may have an even greater impact on the overall outcomes and associated uncertainties than in conventional PSA. Consequently, it is particularly important to critically examine the evidence used to estimate key sub-model parameters and how this evidence was used.

- Parameter dependence

  Sub-model parameters might be dependent due to underlying phenomenological relationships. For example, if a thermal-hydraulic model requires that heat transfer

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

coefficients and friction factors be input rather than calculated, it should be recognized that these parameters are correlated through their dependence on the same fluid properties. In principle, therefore, a dynamic PSA might need to consider joint probability distributions for sets of parameters, rather than treating each parameter separately.

- Significantly higher number of scenarios that need to be analysed compared to traditional fault/event tree methods, that makes post-analysis information retrieval more demanding and complex.
- Substantial computational effort required to model dynamic reliability.

  This is especially critical for T-H natural circulation PSSs, whose performance is more heavily influenced by time-dependent factors and evolving system states during accident progression, compared to other safety systems.

Possible ways to account dynamic aspects under REPAS, RMPS and APSRA are discussed in [24]. Examples of application of dynamic methods for reliability assessment of PSS are presented in several studies, e.g., [25], [26], [27].

Experimental and high-fidelity simulation works have significantly expanded the data underpinning PSS reliability. The PERSEO integral test facility mentioned in OECD/NEA 2024 [28] is a notable example. In particular, the PERSEO benchmark has been conducted to evaluate the capability of system T-H codes in simulating natural circulation heat removal in PSS configurations, OECD/NEA 2024.

Thus, the decade following IAEA TECDOC-1752 has been marked not only by the enhancement and broader test application of the PSS reliability assessment methods presented in the document, but also by the development and application of novel approaches aimed at improving the realism and accuracy of such assessments. These advancements include incorporation of dynamic reliability methodologies and application of modern technologies such as machine learning and AI. However, despite their potential, these approaches remain largely at the research stage with different level of maturity and have not been adopted in the nuclear industry and regulatory process.

1.6. Current requirements and recommendations

1.6.1. IAEA and related TECDOCs

1.6.1.1. General IAEA requirements to the design and safety assessment

Most of the IAEA requirements to the design and safety assessment of NPPs as defined in **IAEA SSR-2/1 (Rev. 1) [12] and GSR Part 4 (Rev. 1) [31] do not differentiate between the passive and active safety systems**. The only requirement, that explicitly considers the passive features is para.5.40 of SSR-2/1 that specifically emphasizes the need to account the single failure of a passive component, unless it is demonstrated with a high level of confidence that its failure is very unlikely and that its function would remain unaffected by the initiating event.

Therefore it can be concluded that general system requirements of SSR-2/1 (Rev. 1) [12], including the ones to redundancy, diversity, physical separation and independence, reliability, resilience to the effect of internal and external hazards, and number of others are equally applicable to active and passive safety systems. This conclusion is consistent with recommendation no.1 of SMR Regulators' Forum [32], Working Group on Design and Safety

Assessment, to develop requirements to PSSs based on categorization proposed in IAEA-TECDOC-626 [33].

In addition to application of single failure criterion, two other requirements of SSR-2/1 (Rev. 1) [12] are directly related to the reliability assessment of the safety-important systems and components:

- **Requirement 23:** Reliability of items important to safety

  The reliability of safety-related components shall be commensurate with their safety significance (in section 1.2 reported),

- **Requirement 24**: Common cause failures

  The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

In conjunction with **requirement 23, para.5.38 of SSR-2/1 (Rev. 1**) [12] states that both spurious operation and unsafe failure modes need to be accounted in reliability assessment.

It should be noted that, in general, when innovative safety features are considered, the requirement 9 of SSR-2/1 (Rev. 1) [12] and the related paragraphs 4.14, 4.15, and 4.16 need to be taken into account. In particular as required by the 4.16, **where an unproven design or feature is introduced or where there is a departure from an established engineering practice**, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.

In relation to the target function of the PSSs, it is also important to recall Requirements 52 and 53 of SSR-2/1 (Rev. 1) [12] and the related paragraphs:

- **Requirement 52:** Emergency cooling of the reactor core

  Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant, even if the integrity of the pressure boundary of the primary coolant system is not maintained.

- **Requirement 53:** Heat transfer to an ultimate heat sink

  The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.

In particular, it should be noted that:

- **as required in #6.19:** Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfil the requirements of para. 6.18 with adequate reliability for each postulated initiating event.
- **As required in 6.19A:** Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

1.6.1.2. International Project on Innovative Nuclear Reactors and Fuel Cycles

Some specifics related to the inherent and PSSs can be found in the IAEA-TECDOC-1575 [34] that provides a guidance on application of the INPRO methodology for evaluation of innovative nuclear energy systems, proposed in the IAEA-TECDOC-1362 [35]. Relevant provisions of this methodology have been previously studied in ELSMOR project [36] and are briefly discussed below.

In particular, two of four INPRO Basic Principles (BP) for safety are specifically related to the inherent and PSSs [34], ch.3.3, 3.5:

- **BP2 (inherent safety)**

  Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and PSSs as a part of their fundamental safety approach.

- **BP4 (research, development and demonstration)**
  The development of INS shall include associated Research, Development and Demonstration (RD&D) work to bring the knowledge of plant characteristics, and the capability of analytical methods used for design and safety assessment to at least the same confidence level as for existing plants.

Though the incorporation of PSSs into the plant design is intended to enhance reliability of performing the required safety functions and, therefore, improve the overall safety of the plant, it is noted that failures in PSSs due to human error in design or maintenance, the presence of unexpected phenomena, and potential adverse system interactions, should be analyzed and may need to be compensated by other design measures. The deterministic and probabilistic analyses must cover all plant operating states including shutdowns, maintenance and repair intervals, be based on validated methods and reliable data, utilizing the adequate mathematical models, experimental investigations, supported by engineering judgement, operating experience and information from other industries ([34], ch.3.3).
Special considerations are necessary for the shutdown states as the specific working conditions, for example, the temperature difference, which are required for operation of some PSSs, may be non-existent in these states.

For the innovative system designs, lack of operating experience should be compensated by extensive RD&D effort specifically focusing on identification and studying of relevant (potentially new) phenomena; development, improvement and validation of analytical and computer models; addressing the scaling considerations in experimental and analytical tasks; investigation of coupled effects and interactions between the systems and components; and assessment of the system reliability.
As specified in user requirement UR4.2: RD&D on the reliability of components and systems, including PSSs and inherent safety characteristics, should be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment [34], ch.3.5.2. In the result:

- All significant phenomena, affecting safety, associated with design and operation of INS have to be understood, modeled and simulated (this includes the knowledge of uncertainties, and the effect of scaling and environment);

- Safety-related system or component behavior must be modeled with acceptable accuracy, including knowledge of all safety-relevant parameters and phenomena, and validated with a reliable database.

Typically, the RD&D is organized as an iterative process, starting with reduces scope of available experimental data, limited scope of understanding of physical processes and simplistic analytical models. As the design evolves, more experimental data are acquired, supporting the enhancement of the codes and models, extending the respective validation database, providing better understanding (and reducing, if necessary) of associated uncertainties. Ultimately, the whole range of code application is to be covered by the validation matrix, including quantification of uncertainties, and addressing the scaling considerations [34], ch.3.5.2.

1.6.1.3. Recommendations from SMR Regulators' Forum

A detailed evaluation of issues related to the applicability of existing IAEA requirements to SMRs has been conducted within IAEA SMR Regulators' Forum. Design and safety analysis topics, including the use of passive and inherent safety features in SMR designs, are addressed in [32]. As a result, common positions and recommendations were formulated, some of them align with the provisions of INPRO methodology, while others confirm the applicability of existing SSR-2/1 (Rev.1) [12] requirements to SMRs. The common positions of participating regulatory bodies on passive and inherent safety features are summarized below:

1. The safety case should systematically identify and address uncertainties in performance claims for passive and inherent features through a strategy that considers:
    - Results from substantiation activities (e.g. use of validated computer models, experimental prototypical systems, integral test facilities);
    - Compensatory design enhancements (if required),
    - Control provisions expected to be implemented by the operator; and,
    - Any additional activities to support performance claims and collect experience data.

2. Clear criteria for characterizing the strength of driving forces should be defined and conditions that may weaken those forces should be identified. This information should be used to identify the system failure modes and ensure that all parameters potentially affecting a safety function are taken into account.

3. Any combination of active and passive safety systems can be accepted, provided DiD and safety design principles are met. The priority should be given to inherent characteristics, passive features or continuously operating systems over those that need to be brought into service. The approach to optimization of use of passive and active features should be documented considering availability of information to substantiate safety claims and support safety classification.

4. The single failure criterion should be applied in safety evaluations of PSSs unless adequate reliability is demonstrated. Analyses should account for all potential failure modes, including their time-dependent evolution, to capture the worst-case scenario.

5. Designs should incorporate redundancy, diversity, and physical separation, where practicable to mitigate common cause failures. Functional diversity is especially important

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

for SMRs that rely exclusively on PSSs. Combining passive and active features may enhance resilience by providing additional diversity for critical safety functions.

1.6.1.4. IAEA recommendations on reliability assessment of passive systems

In line with characteristic features of PSSs, highlighted in other IAEA documents reviewed in this section, including reliance on low driving forces and sensitivity to environmental and boundary conditions, the Level 1 PSA guidance provided in the IAEA SSG-3 (Rev.1) [13] emphasizes the importance of thoroughly identifying and accounting for all relevant failure mechanisms and events, affecting those conditions, in the reliability assessment. These mechanisms should encompass the failure modes which are typical for active systems, such as valve failures, incorrect valve positioning, or flow blockages, and those that are unique or more characteristic to PSSs. The latter may include phenomena such as the ingress of non-condensable gases, corrosion, or other degradation processes that may significantly impair system performance under accident conditions. The potential for such mechanisms to simultaneously affect multiple system trains must be evaluated and appropriately accounted.

While the general approach to reliability assessment remains applicable to PSSs, estimating failure probabilities for phenomena- or ageing-related failure modes may require development and application of model-based methods and/or other techniques such as testing and expert judgment. According to para. 5.128 of SSG-3 ([13] Rev. 1), the reliability assessment of PSSs should follow a structured process consisting of the following main stages:

- System characterization to define the mission of the system, associated accident scenarios, failure modes and success or failure criteria;
- Identification of system failure mechanisms;
- Modelling of system performance in various conditions;
- Identification of relevant parameters and sources of uncertainties in system model and input data;
- Quantification of uncertainties (employing appropriate methods to account for both aleatory and epistemic uncertainties) to yield a reliability estimation for the system.

Note: The above sequence of individual steps from SSG-3 for performing reliability analysis for PSS will be also fulfilled in WP4, where individual tasks cover these areas.

1.6.2. WENRA report on Regulatory Aspects of Passive Systems

The regulatory implications of integrating PSSs into NPP designs are examined in the report [30], with emphasis on key safety-related attributes of PSSs that require special attention from the regulatory assessment perspective.

Although the PSSs involve fewer or no components with moving parts and do not require support functions from other systems, with the exception of signal inputs of ‘intelligence’ to initiate the passive process for Category D systems [37], it is recognized that demonstration of their reliability for all relevant hazards and accidents is more complex and challenging, than for active systems. This complexity primarily arises from the need to identify and account multiple interrelated phenomena and conditions that can influence system performance, beyond the

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

conventional failure modes of active components required for system start-up or components with mechanical moving parts (if applicable).

One of the key concerns identified in [30] is the relatively narrow range of conditions required for reliable operation of PSSs. These conditions can be affected by variations in environmental parameter, internal or external hazards, and ageing-related degradation. Accordingly, it should be demonstrated that appropriate margins are taken into account so that small parameters' variations do not lead to cliff-edge effects.

Additionally, the potential for adverse system interactions should be evaluated. Moreover, as the system operation itself may alter the boundary conditions (for example, in natural circulation heat removal systems the heat sink temperature may gradually increase due to system operation), the dynamic changes in system performance over the entire mission time must be considered in the assessment.

While PSSs are generally designed to operate without reliance on operation actions, human factors remain relevant. Therefore, human errors during maintenance, testing, or operation can impact system performance and must be addressed in the safety case.

The report also highlights the importance of ensuring that computer T-H codes used for modelling PSSs are capable of accurately representing the relevant phenomena within the range of system operating conditions. In some cases, this may require dedicated experimental tests for computer codes validation.

In summary, consistent with the IAEA documents discussed in Section 1.6.1, the report [30] identifies the same key features of PSSs and emphasizes similar concerns to be addressed in the safety assessment.

1.6.3.National legislation

In general, the legislation of IAEA member countries adopts the requirements and recommendations from relevant IAEA documents and guidelines.

The OECD/NEA survey on regulatory practices to assess PSSs in NPP designs [38], which included the regulatory bodies from five European and four non-EU countries, and was focused on AOO and DBA systems, indicated no significant differences in the requirements or assessment approaches for PSSs compared to those applied to active ones. However, certain variations in regulatory expectations and approaches in different countries were identified in the following areas:

- Application of single failure criterion to passive components;
- More stringent evaluation of system reliability and consideration of uncertainties;
- Greater emphasis on experimental justification of system performance, and analysis of potential adverse interactions arising from concurrent operation of multiple PSSs or trains.

Since the survey, additional provisions specific to passive components have been introduced into Finnish regulations. In particular, the (N+1) failure criterion, rather than (N+2), may be applied to passive components of decay heat removal systems or their auxiliary systems, provided the probability of failure of these components is low [39].

1.6.4. Summary

Although the general safety requirements established by the IAEA are equally applicable to both active and PSSs, the unique characteristics of PSSs, such as reliance on low driving forces, and limited operating experience, necessitate consideration of additional aspects in the safety assessment process.

A robust assessment must be underpinned by a comprehensive understanding of all physical phenomena governing the operation of the PSS. Particular emphasis should be placed on identifying and analysing conditions that may degrade or weaken the driving forces, thereby compromising system functionality under various plant states, including normal operation, and accident conditions.

Given the limited operational experience, the safety demonstration must be supported by extensive research, development, and demonstration activities. These efforts should focus on the identification and characterization of relevant physical phenomena, improvement and validation of analytical tools and computational models, resolution of scaling issues [40], and quantification of associated uncertainties.

The safety analyses must be conducted using validated computer codes, with explicit consideration of uncertainties related to environmental conditions, system interactions, and long-term degradation mechanisms. Due to the potentially narrow operational range of PSSs, the adequate design margins must be incorporated to prevent cliff-edge effects resulting from minor parameter deviations.

The compilation of recommendations related to reliability assessment of PSSs is provided in the table below.

Table 1 – Compilation of recommendations for reliability assessment of PSSs

No.	Requirements / Recommendations	Reference
1	Analyses must cover all plant operating states including shutdowns, maintenance and repair	TECDOC-1575 [34]
2	Periodic testing and maintenance practices or planned procedures should be considered	SSG-3 [13]
3	The reliability assessment of PSS should follow a structured process consisting of the following main stages: – system characterization to define the mission of the system, associated accident scenarios, failure modes and success or failure criteria; – identification of system failure mechanisms; – modelling of system performance in various conditions; – identification of relevant parameters and sources of uncertainties in system model and input data; – quantification of uncertainties (employing appropriate methods to account for both aleatory and epistemic uncertainties) to yield a reliability estimation for the system	SSG-3 [13]
4	Analyses must be based on validated analytical methods, analytical and computational models, and reliable data, supported by associated research, development and demonstration, operating experience, and, where applicable, engineering judgement and insights from other industries	TECDOC-1575 [34]

No.	Requirements / Recommendations	Reference
5	All significant phenomena, affecting safety, associated with design and operation of the system have to be understood, modelled and simulated with acceptable accuracy	TECDOC-1575 [34] WENRA [30]
6	The uncertainties in the system performance should be identified and addressed	TECDOC-1575 [34], SMR Regulator Forum [32]
7	Sufficient design margins must be provided {and demonstrated in deterministic analysis} to avoid cliff-edge effects due to small variations in key parameters	WENRA [30]
8	The analysis should identify and account for all potential failure modes including spurious operation, human errors in operation and maintenance, potential common-cause failures. The following factors should be considered: – phenomena affecting system performance; – initial plant state; – environmental conditions; – availability of I&C and support systems needed for the system actuation; – potential imperfections of the PSS components, such as improper inclination of pipes; – potential adverse interactions between the plant systems and components; – dynamic performance and potential long-term degradation of the system; – adverse conditions associated with internal and external hazards (e.g., changes in environmental conditions, temperature distribution due to fires, pipe deformation due to seismic or load drop events), and ageing effects.	SSR-2/1 [35], SSG-3 [13], TECDOC-1575 [34], SMR Regulator Forum [32], WENRA [30]
9	Criteria for characterizing the strength of driving forces should be defined, and conditions that may weaken those forces should be identified to ensure that all parameters potentially affecting the safety function are considered	SMR Regulator Forum [32]
10	The single failure criterion should be applied in {deterministic} safety assessment of passive safety systems unless adequate reliability is demonstrated	SSR-2/1 [12], SMR Regulator Forum [32], WENRA [30]

1.7. Methodologies Selected

The methodologies selected for this work include REPAS, RMPS, APSRA, ROAAM+, and a PSA-based framework. These approaches were chosen based on their relevance to the assessment of PSS reliability in advanced reactor designs. They offer complementary perspectives by combining deterministic and probabilistic techniques, enabling a structured treatment of uncertainties, scenario sensitivity, and system-level performance evaluation. Their integration provides a robust methodological basis for capturing both phenomenological and hardware-related failure modes. There is also real experience for the above approaches, as they have been applied in the past to the reliability analysis of real reactors/facilities.

Their integration is particularly important for WP4 of the EASI-SMR project, as it aims to establish a comprehensive framework for the quantification of PSS reliability, supporting the development of robust and defensible safety cases for SMR designs.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

2. Methodology Review and Comparison

In this chapter, a general guidance for analysing PSS reliability (Section 2.1) is being presented, followed by an overview of risk-oriented methods suitable for phenomenological analysis of PSS (Section 2.2).

2.1. General Overview of the methodology (general steps and challenges)

The purpose of this section is to discuss a coherent approach to PSS reliability analysis with the focus on high-risk systems characterized by potentially significant interactions between scenario and phenomenological complexities. The methodology is general in nature and applicable to any specific PSS, reactor design or reactor type.

The review presented in this section is inspired in some elements by the methodological framework for the PSS reliability analysis outlined in EPRI report [41] and thus could represent a suitable complement to the approaches used in Europe (like RMPS/REPAS). The approach to the reliability analysis of a PSS can be divided onto the following steps:

1) Establishing the need for comprehensive PSS analysis;
2) Collecting information on the PSS design including experimental and test data;
3) Identifying relevant accident scenarios;
4) Conducting phenomenological analysis of the PSS, to identify potential failure modes;
5) Quantifying PSS reliability.

The above steps are generally method-agnostic. However, the results in steps 4 and 5 strongly depend on a specific method for risk assessment and approach to phenomenological analysis employed. Furthermore, **the PSS analysis approach described here does not guarantee independence of the results from a particular method used (see Section 2.2).**

2.1.1. Entry conditions for comprehensive approach to PSS analysis

This initial step determines if a comprehensive analysis is required for a PSS. The decision criteria consider a combination of the PSS's risk significance, its functional margin to achieve safety functions, and the level of uncertainty regarding its performance. The need for a comprehensive analysis of a PSS is contingent upon meeting the following conditions with regards to risk significance and uncertainty in evaluation of the functional margin:

- Failure of the PSS is of high-risk importance. Otherwise, i.e. for the systems that have a low risk-significance, the basic reliability analysis process can be applied;
- Uncertainty in the evaluation of the functional margin is large, or the functional margin is small. Typically, this can be attributed to:
  - Large variability and complexity of scenarios that may present considerable challenges to reliability of a PSS;
  - Significant interactions with other active or PSSs;

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- Lack of operational experience or a comprehensive testing and demonstration program.
- Lack of well validated mechanistic models for describing relevant complex phenomena (e.g., coupled phenomena of different scales);
- Large (or unknown) uncertainties that may degrade the margin and require comprehensive uncertainty quantification.

The EPRI report [41] provides a list of questions, if at least one question gets a "yes" answer, evaluation of the PSS will not benefit from a comprehensive analysis:

- Does the system have a low risk-significance?
- Is the system dominated by hardware failure, e.g., active components responsible for PSS activation?
- Does system-level reliability data exist, e.g., is there extensive experimental data on system performance?
- Does the system have high (compared to modelling uncertainty) functional margin?

2.1.2. Collection of important information on the PSS design

Comprehensive analysis requires **careful collection of information on the PSS system design** and, importantly, on the coupled systems. Note that some of the data may have to be generated (e.g. with the phenomenological calculations). The following types of information have to be collected:

System level performance data, preferably including:

- Operational data from similar systems supported by the assessment of applicability for the system under the analysis;

Hardware component data, covering failure rates of individual components comprising the PSS, provided that

- Data collected are relevant to the operational conditions specific to the PSS;

Maintenance data, as:

- PSS sensitivity to variability in the initial and boundary conditions may manifest from insufficient or poorly carried out maintenance program of the system and associated systems/components;

Support system data, such as:

- Electric power, compressed gas, instrumentation;

Phenomenological calculations, including:

- **Design basis calculations**, commonly based on conservative assumptions and methods that provide confidence in the PSS operation in a wide range of conditions;
- BE calculations and sensitivity analysis for more realistic performance evaluation;
- Calculations of PSS performance **in extreme and rare conditions**;

Experimental data, including results:

- from design and licensing activities, as well as
- Experimental and testing data from similar or relevant scaled down systems;

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Expert elucidation, preferably involving:

- specialists from different scientific and engineering disciplines, that can help to identify potentially missed modes of system failure;

Unique plant-specific conditions, such as plant location, climate, seismic activity, flooding or tsunami risks, which may have effect on PSS performance and be accounted in reliability analysis.

2.1.3. Identification and characterization of relevant accident scenarios

In order to identify potential PSS failure modes, a broad search of all possible scenarios should be carried out. **The ultimate objective is to identify scenarios which can challenge the operation of the PSS.** Once identified, scenarios frequency and the likelihood of the PSS failure under the specific scenario conditions should be examined.

PSSs are expected to be designed with very high reliability during nominal operation. Therefore, identification of the failure scenarios should be focused on finding **potentially remote cases where the likelihood of PSS functional failure may be high.**

In the process of identification of relevant accident scenarios for PSS reliability analysis examples of the cases that should be considered are:

- **External events**, e.g., seismic activity, loss of off-site power, etc.;
- **Internal events**, e.g., inadvertent opening of a pressure relief valve, turbine trip, actuation signal failure, etc.;
- **Complex phenomenological aspects**, e.g., physical degradation of components, partial blocking of flow paths, reduced heat transfer capability, structural failures, etc.;
- **PSS interaction with and operational dependence on other systems**, e.g., isolation condenser water level, accumulation of non-condensable gases, mutual feedback between coupled PSSs, etc.

As example, EPRI report [41] outlines the following steps for identification of the accident scenarios:

1. Define the scope of the analysis:
   - Objectives of the analysis;
   - Physical and analytical boundaries of the analysis:

     Depending on the specific objectives, the scope of the analysis may vary from a narrowly focused evaluation of a particular PSS component under a limited set of conditions to a comprehensive assessment of the entire system across the full range of relevant accident scenarios. Furthermore, in addition to the limitations imposed by the analysis objectives, the definition of analysis boundaries may also be constrained by other practical considerations, such as the scope of available information, operational experience, and resources allocated to the project;
   - Potential interactions with other systems, including:

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- Systems needed for PSS operation, e.g. primary side depressurization system might be needed to allow operation of heat removal PSS that functions at low pressure;
- Dynamically interacting systems. The typical example is the operation of the containment cooling PSS that may have interactive effect on other systems. These systems may influence containment parameters, thus, in turn, affecting the effectiveness of containment cooling PSS;
- Systems needed for PSS activation or support systems, e.g. DC power to open or maintain opened PSS valves.

o Important safety functions for the analysis

The specific safety functions provided by the PSS should be defined in phenomenological terms (e.g., heat transfer function) and specified in measurable phenomenological factors (specified amount of transferred heat, specified amount of coolant injection, specified flow rate, etc.) reflecting specific requirements for successful operation of the PSS.

o Define nominal operation of the PSS and, as a result, map potential failures:

- Types of initiating events during which PSS must operate;
- Sequence of events from each initiating event until system initiation occurs;
- Sequence of events to initiate, continue operation, and complete operation;
- Expected plant phenomenological conditions prior to and during PSS operation;
- Expected environmental conditions prior to and during PSS operation;
- Expected plant conditions as a result of successful system operation;
- Expected indicators of system failure;
- Operator actions associated with operation or monitoring of the system.

2. Identify preliminary list of potential PSS failure mechanisms and modes[2]:

o **Hardware-based failures** include malfunctions of PSS components such as failure of a check valve to open, or human error to enable system actuation, which are typically addressed in conventional PRA;

o **Phenomenological failures** may be caused by

- abnormal operational conditions such as extreme environmental conditions, unexpected thermal-hydraulic conditions, or violation of design assumptions for the PSS;
- traditional (hardware-based) failures in connected systems, e.g., unexpected I&C signals. It should be noted that even if a single failure assumption in related systems is considered in PSS design, the potential for multiple failures in these systems that may produce unexpected phenomenological conditions still needs to be evaluated.

The commonly mentioned conditions that may result in phenomenological failures are:

o Blockage of tubes by corrosion / erosion products or other debris;

o Parameters falling outside the nominal operating limits of PSS: temperature, pressure, coolant level, flow rate, heat transfer, radiation and reactivity, deposits on

[2] Failure mode is defined as a functional failure of a PPS, e.g. to provide heat removal; failure mechanism is a physical cause of a failure mode, e.g. a blocked tube that inhibits coolant flow or accumulation of non-condensable gases that reduces heat transfer.

heat exchange surfaces, depletion or diversion of the coolant, flow instabilities, flow stratification, excessive level of non-condensable gases, external events (including environmental).

3. Identify key scenarios with potentially unexpected conditions that can affect the likelihood of PSS failure:

   Supported by information on potential PSS failure mechanisms and modes, this step includes:

   - Identification of PRA scenarios that deviate from normal operating conditions, which requires the plant-specific PRA model available;
   - Identification of additional scenarios that are not represented in PRA. Such scenarios may include unusual maintenance or testing configurations, latent human errors (e.g., from maintenance activities);
   - Ranking of the found scenarios by risk importance.

     This involves preliminary identification of important scenarios using both quantitative and qualitative indicators. Scenarios of high importance are typically characterized by:
     - Fast accident progression giving little time to core damage;
     - High frequency of events comprising the scenario;
     - Common cause failures;
     - Operation outside the traditional design-basis accident definitions.

     Conversely, scenarios of low importance are typically characterized by:
     - Multiple, independent failures that results in negligible likelihood of occurrence;
     - High likelihood of successful system restoration;
   - Identification of the most important scenarios (screening out scenarios with low-risk importance):
     - Mapping scenarios and corresponding failure modes for quantification of all scenarios contributing to a specific failure mode;
     - Grouping similar scenarios to facilitate subsequent PSS reliability analysis;
     - Distinguishing between scenarios that fall within the scope of PRA-type analysis, which can be addressed using standard PRA analysis techniques, and those that are phenomenologically driven, which require risk-oriented phenomenological simulations.

It should be noted that identification of scenarios, failure mechanisms and failure modes at this stage is based mainly on expert judgement. Reliability of such analysis can be quite limited due to the complexity of interactions between scenarios (different combinations of initiating events and failure mechanisms) and respective failure modes. To ensure completeness and consistency of further phenomenological analysis, it is therefore essential to:

- Explicitly and clearly state the assumptions for limiting the space of possible scenarios / failure mechanisms;
- Use sensitivity analysis, whenever possible, to justify the limitations imposed on the space of scenarios for which failure of the PSS will be evaluated.

The body of information collected at this point should be sufficient to classify the scenarios between two categories A and B:

- No further analysis is needed:

- Category #A1
  - Scenario lies within the design basis or is addressed via other available information and
  - Data indicates a very high likelihood of successful PSS function.
- Category #A2
  - Scenario lies within the design basis or is addressed via other available information and
  - Likelihood of the scenario is negligible.
- Category #A3
  - Scenario lies beyond the design basis or is not addressed via other available information and
  - Likelihood of the scenario is negligible.
- Category #A4
  - Scenario lies beyond the design basis or is not addressed via other available information and
  - Scenario characteristics indicate the PSS is unlikely to succeed.

- Further analysis is needed:
  - Category #B1
    - Scenario lies within the design basis or is addressed via other available information and
    - Data indicate the PSS function may not succeed and
    - Likelihood of the scenario is not negligible
  - Category #B2
    - Scenario lies beyond the design basis or is not addressed via other available information and
    - Likelihood of the scenario is not negligible
  - Category #B3
    - Scenario contains special phenomenological concerns or inter-system interactions that the design basis or other information does not adequately address

Scenarios belonging to categories A1-A4 usually do not require further analysis and are not expected to affect the estimate of PSS reliability. On contrary, for scenarios in the Categories B1-B3, one has to estimate the probability of PSS function to fail, for example, using one of the methods described in Section 2.2.

2.1.4. Statistical Selection of approaches to reduction of uncertainty in the PSS reliability

Scenarios in categories where the further analysis is needed B1-B3 are mainly associated with a gap in knowledge, which can be reduced. An approach should be suggested to close each gap using one of the following:

Expert opinion

- Expert elicitation can be a valuable source of and efficient way to provide information on PSS reliability. It is to note that if experimental knowledge is missing on safety relevant/dominant phenomena, expert opinion cannot be used to substitute the need of developing new experiments.

Conservative analysis

- Conservative analysis may provide a short cut to understand the importance of a specific failure mechanism and its potential contribution to the failure mode.

Design change to eliminate or modify the potential failure scenario.

- Modification of the PSS or related systems designs (if possible) can be an ultimate solution to reduce the number of possible failure scenarios or significantly reduce their frequency.

Experimentation and testing:

- While typically being the most expensive method, additional phenomenological experiments can provide direct information on PSS performance under scenario specific conditions.

Phenomenological calculations:

- This may involve exploratory calculations to identify relevant phenomena, as well as risk-oriented analysis with the objective to calculate the probability of the PSS function failure associated with each scenario.

2.1.5. Phenomenological analyses to identify failure modes of the PSS

It is important to note that EPRI report ([41], written almost 20 years ago) recommends limiting the number of phenomenological calculations to arrive to an acceptable estimate of PSS reliability sufficient for decision making within PRA. Specifically, EPRI report states: "The process recommended here is a successive parsing of the potential failure scenarios. That is, given a potential failure scenario for a given PSS, the ability of the system to successfully perform its intended function is uncertain. If the analyst identifies portions of that scenario as highly likely to succeed or fail, these portions can be "broken off" so that the uncertain areas are assessed separately. Therefore, the goal of the phenomenological calculations is to identify these success/failure bifurcations to successively narrow the degree of uncertainty in PSS behaviour and effectively use limited resources… The effort devoted to the reduction of uncertainty related to the PSS should be commensurate with its importance in the overall PRA application and proportionate to uncertainties in other aspects of the PRA such as initiating event analysis, component reliability, success criteria definition, and human reliability analysis."

Since publication of EPRI report, the computational resources, that would have been considered extensive by 2008 standards, can be readily available for an individual analyst. Therefore, it would be much more prudent to reduce the "user effect" in the described above approach through the means of automated search for the failure modes in the space of selected accident scenarios.

At this stage a good understanding of parameters importance, impact of the modelling uncertainty on risk figures and effect of code uncertainties should be established. A comprehensive methodology relying on sensitivity analysis and uncertainty quantification has to be applied (e.g., refer to Section 2.2).

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

2.2. Detailed Descriptions of Each Methodology

2.2.1. REPAS

2.2.1.1. Description

Introduction:

The Reliability Evaluation of Passive Safety Systems (REPAS) methodology was developed for the evaluation of the reliability of PSSs, whose function is strictly connected to the driving T-H phenomena. The methodology, developed by a cooperation between ENEA, University of Pisa and Polytechnic of Milan, is a core methodology integrating deterministic and probabilistic analyses to assess failure probabilities of PSSs under various scenarios.

Domain of applicability:

The REPAS methodology lends itself primarily to application on PSSs and the phenomenology (such as natural circulation) behind them. However, as was first carried out by [46], it is also possible to apply this methodology to active safety systems.

Purpose: It constitutes a procedure to assess the reliability of a PSS, that is, the reliability associated with the occurrence of T-H phenomena. Thus, its overall objective is to analytically characterize the performance of the analysed system in order to increase the confidence in its operation. Moreover, through such methodology, it is possible to compare the performance of active and PSSs or compare the performance of different PSSs [43].

Theoretical Foundation: In some steps of the procedure (see **Figure 2**) it is necessary to adopt the Event-Tree (ET) or Fault-Tree (FT) methods (step iii) to ensure that all possible causes of failure are properly addressed and also apply, e.g., the Wilks' formula [49], [50], (step xi) to determine the minimum number of code run that guarantee sufficient information for the evaluation of the overall system performance [43]. For cases where only one Figure Of Merit (FOM) is being examined, the required number of code runs N (for a one-sided tolerance interval), is determined by the desired probability α and confidence level β:

$$1 - \alpha^N \geq \beta$$

If more than one FOM is investigated, for the one-sided tolerance interval, the required number of code runs can be found by solving the following equation with respect to N [46], [51]:

$$\beta \leq \sum_{j=0}^{N-p} \frac{N!}{(N-j)!\,j!} \alpha^j (1-\alpha)^{N-j}$$

where p represents the number of FOMs.

Analytical Approach

The initial stage of the procedure is to select the PSS, then proceed as follows [43], [46], [47]:

i. Define the TM of the PSS and identify the relevant phenomenology involved. The parameters defining the operation and transient behavior of the PSS must be selected.

ii. Definition of FC. FC can be defined as specific single-value targets or as functions of time, potentially varying with environmental conditions where the PSS operates. Additionally, these criteria may change during a transient, so both threshold and continuous or integral criteria might be needed.

iii. Identification of all possible causes of failure. A systematic process is needed to ensure that all root and related causes of failure are addressed appropriately. This can be achieved through a hierarchical structure or the more common FT and ET methods.

iv. Decomposition of the phenomena occurring (or assumed to occur) in the system into the relevant fundamental parameters of the system.

v. Classification of the most important parameters. A generic PSS may function under steady-state conditions or during transients so considering all parameters may be impractical for computational purposes. Thus, a classification process is necessary, which may include grouping similar parameters.

vi. Selection of less important parameters. The goal, as in the previous case, is to reduce the number of design and critical parameters.

vii. Identification of parameter relationship and dependencies. Within this step, physical constraints and stochastic dependencies between the selected parameters should be highlighted.

viii. Detailed T-H code modeling.

ix. Deterministic Assessment of the Nominal/Reference case. It is necessary to determine a reference transient and complete a best-estimate prediction for it. The results of the reference transient constitute the system mission and are used in step (xii) to compare sensitivity study results and to derive the reliability value for the system under review. Therefore, there is a dotted line connecting steps (ix) and (xii).

x. Assignment of probability distributions. Each operational state and critical parameter value should be assigned a probability. This involves assigning (or updating) probability distributions, including ranges of variations and Probability Density Functions (PDFs), for all parameters identified in step (vii).

xi. Probability propagation and analysis. Once the PDFs (or discrete probability values) along with the variation ranges for the selected parameters have been established, the issue is how these results help determine the reliability of the system in question. Calculation of uncertainty for system code predictions can be obtained using Wilks' formula, which, under appropriate assumptions, relates the number of calculations required to the probability (and confidence level) of estimating the upper and lower bounds of system performance, given a set of (uncertain) input parameters that include ranges of variation and PDF. Using this formula, the minimum number of calculations required to characterize system performance is determined, which can be applied in the final step (xii) of reliability assessment.

xii. Quantitative reliability evaluation. At this point an 'analytical' comparison is made between the results of the N transient scenarios and the reference/target system performance, considering the FC defined in step (ii). This procedure produces FOMs for the system, where the probability of system failure is reported as a function of the probability of an assigned scenario occurring.

Main outcome FOMs: The main outcomes from this methodology are:

1) The probability of occurrence of FCs when the selected uncertainty parameters vary (failure probability of PSS).
2) Incidence of the uncertainty parameters on the physical quantities (i.e. cladding temperature, passive decay heat removal power removed, etc...) involved in the definitions of the FCs.

Subsequently these two points lead to the identification of the areas of successful operation of the PSS, in terms of acceptable range of variability of the physical quantities involved in the stability of the system, i.e. pressure in the primary circuit, cladding temperature, etc.

Workflow of the methodology needed

Figure 3 shows the REPAS workflow.

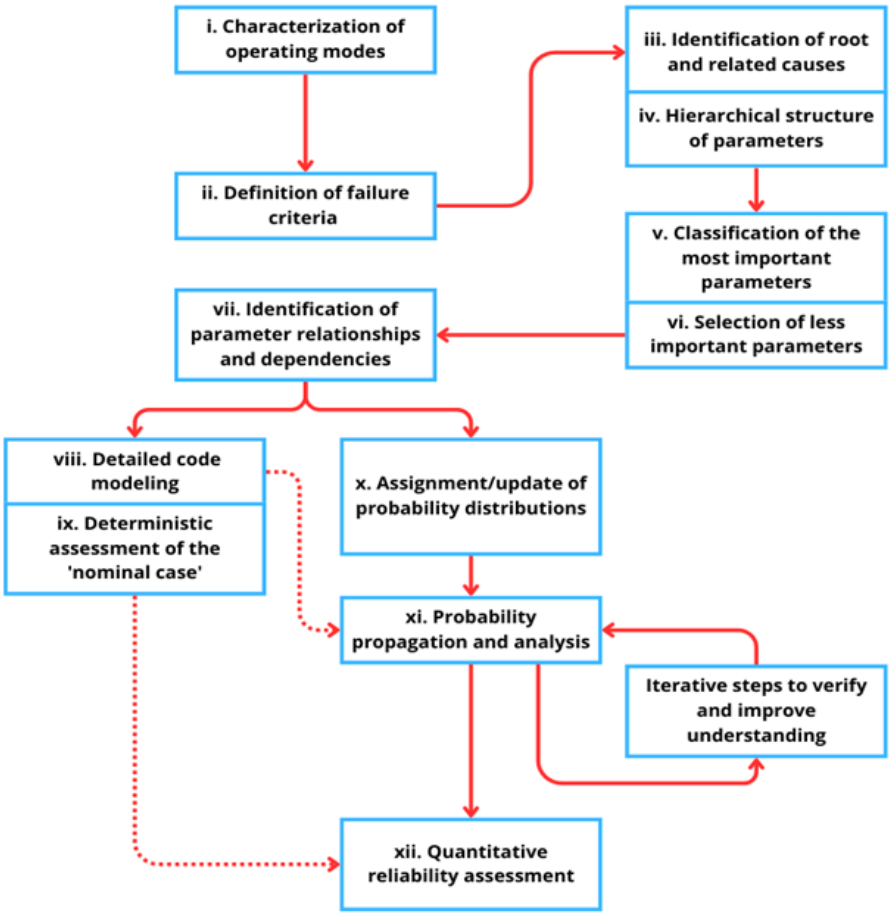

Figure 2 - REPAS workflow [43], [46], [47]

2.2.1.2. Advantages and Limitations

The main advantage of the REPAS methodology is its ability to provide a quantitative evaluation of the performance of PSS (and also active ones) through a structured and integrated approach combining both deterministic and probabilistic analyses. This allows the systematic assessment

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

of the probability that a safety function is successfully achieved, even in the presence of uncertainties affecting system behaviour.

The main challenges of the REPAS methodology lie in:

- **The identification of relevant uncertainty parameters,** which requires expert knowledge of the system configuration and governing physical phenomena;
- **The characterization of the uncertainty parameters,** including the assignment of appropriate PDFs and variability ranges, often in the absence of supporting experimental data;
- **The treatment of uncertainties associated with the T-H codes** used for system simulation, including model assumptions, numerical approximations, user effect, etc;
- **The dependence of the reliability evaluation on the specific accident scenario**, which limits the generalizability of the results and necessitates the analysis of a wide range of conditions to ensure completeness;
- **The high computational and time cost** associated with the methodology, particularly when performing uncertainty propagation through Monte Carlo samplings which may require thousands of code runs and substantial computational resources.

2.2.1.3. Applications already available

1) Application on a Isolation Condenser

The first attempt to apply the REPAS methodology was made in [42], where the authors chose a typical natural circulation, two-phase flow loop as a PSS test case. It consists of a heat exchanger immersed in a pool and connected to the pressure vessel by piping. The chosen configuration and operating conditions are those typical of a generic isolation condenser, and a conceptual diagram is shown in the next **Figure 3**.

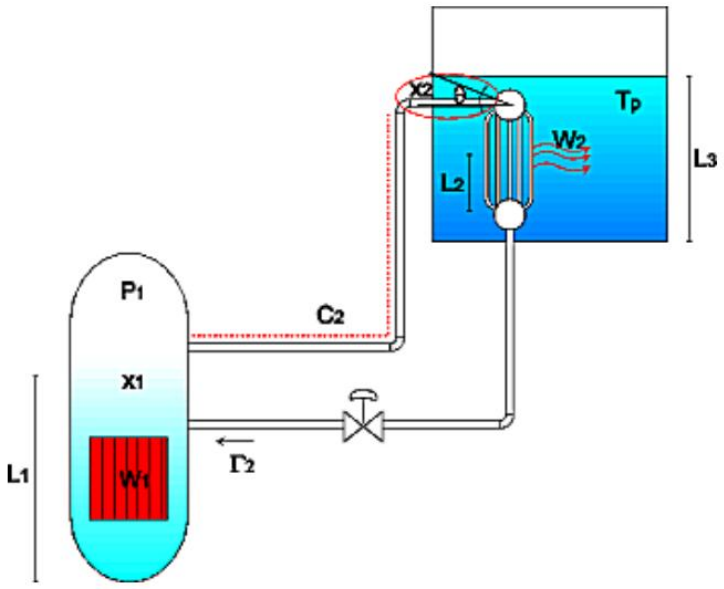

Figure 3 - PSS selected for the investigation in [42].

The nodalization of the system was developed with the RELAP5 best-estimate TH code [48], and the sketch is shown in **Figure 4**.

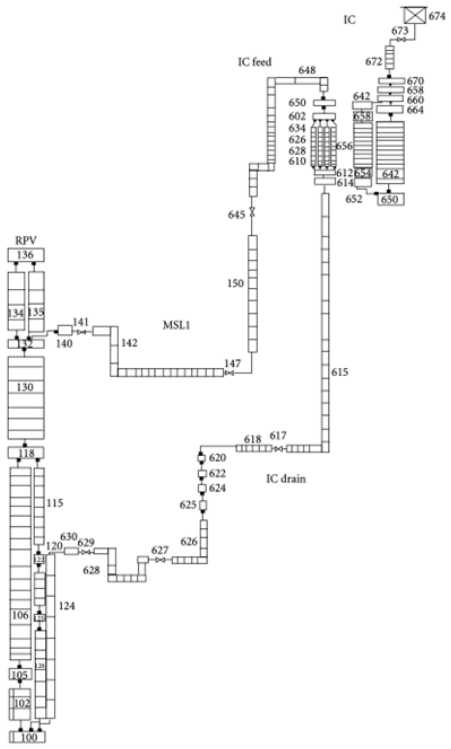

Figure 4 - RELAP5 nodalization of IC on an SBWR [44]

The TM of the system is to remove the core decay heat through the heat sink by condensing primary fluid into the heat exchanger tube bundle. The main parameters identified as design refer all to initial conditions for the system, namely the pressure in the Reactor Pressure Vessel (RPV) P_1, the liquid level in the vessel L_1 and in the pool L_3 and the initial water temperature in the pool T_P. They are reported in the Table 2 listed below. The nominal values, the ranges of variation and the selected initial values for the analysis are listed. The probability values for each initial status are reported in italics.

Table 2 - Design Parameters of the PSS [42]

Design Parameter		Unit	Nominal Value	Range	Discrete Initial Values & Probabilities
P_1	RPV pressure	MPa	7	0,2 – 9	0,2 1 3 7 9 *0,05 0,1 0,15 0,5 0,2*
L_1	RPV collapsed level	m	8,7	5 – 12	5 7 8,7 10 12 *0,05 0,1 0,5 0,2 0,15*
L_3	Pool level	m	4,3	2 – 5	2 4.3 5 *0,1 0,8 0,1*
$T_P(0)$	Pool initial temperature	K	303	280 – 368	280 303 368 *0,1 0,8 0,1*

The critical parameters which complete the identification of the system configuration during its mission are reported in the following **Table 3** together with the discrete ranges of variation. They refer to both initial and boundary conditions for the system, and to those items that could lead to a performance degradation, namely affecting the heat transfer capability (presence of non-

condensable gases in the RPV, x_1, or in the piping, x_2, heat losses in the draining pipe, C_2) and the natural circulation flow rate (inclination of the piping in the suction side of the heat exchanger, θ, liquid level in the tube bundle, L_2, undetected leakage in the piping, *UL*, uncomplete opening of the gate valve, *POV*). As in the previous table, a probability is arbitrarily assigned to each discrete value.

Since the combination of all the discrete values in **Table 2** and **Table 3** leads to several million possible configurations of the system, it is necessary to make a limited but still statistically significant selection of system configurations so that deterministic evaluation by best-estimate codes is feasible. For this purpose, through the Wilks equation, a sample of 64 configurations of the system was selected, thus obtaining with a confidence coefficient of 99%. In order to ensure that system configurations judged to be of particular interest are considered, a set of 6 deterministic calculations was added to the probabilistic calculation sets, whose data configurations can be seen in **Table 4**. Note to **Table 4**: Non-nominal values are marked in red.
The following criterion was used for FCs:

$$FC = \frac{Z - Z_{ref}}{Z_{ref}} \leq (-0.2)$$

where Z is (i) Thermal power exchanged through the IC (W_2);
(ii) Mass flow rate at the IC inlet (Γ_2).
and 'ref' refers to the code calculation for the reference or nominal system configuration.
In practice, the observed parameter has to follow the reference or nominal trend and it has not to fall below a 20% difference for more than a fixed time period of 100 [s].

Table 3 - Critical Parameters of the PSS [42]

Critical Parameter		Discrete Values & Probabilities
x_1	RPV non-condensable fraction	**0** *0,719* **0,01** *0,12* **0,1** *0,07* **0,2** *0,05* **0,5** *0,03* **0,8** *0,01* **1** *0,001*
x_2	Non-condensable fraction at the Inlet of IC piping	**0** *0,71* **0,01** *0,12* **0,1** *0,07* **0,2** *0,05* **0,5** *0,03* **0,8** *0,01* **1** *0,01*
θ	Inclination of the IC piping on the suction [deg]	**0** *0,5* **1** *0,4* **5** *0,08* **10** *0,02*
C_2	Heat Losses piping-IC Suction [kW]	**0** *0,1* **5** *0,7999* **20** *0,1* **100** *0,0001*
$L_2(0)$	Initial condition liquid level-IC tubes, inner side [%]	**0** *0,1* **50** *0,1* **100** *0,8*
UL	Undetected leakage [m^2]	**0** *0,8899* **1E-5** *0,1* **5E-5** *0,01* **10E-5** *0,0001*
POV	Partially opened valve in the IC discharge line [%]	**1** *0,001* **10** *0,01* **50** *0,1* **100** *0,889*

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Table 4 - Deterministic configuration and their probability of occurrence [42]

	Design Parameters				Critical Parameters							Probability
Main parameter considered	P_1 MPa	L_1 m	L_3 m	$T_{P(0)}$ K	x_1 -	x_2 -	θ deg	C_2 kW	$L_2(0)$ %	UL m^2	POV %	
Nominal Conditions	7	8,7	4,3	303	0	0	0	5	100	0	100	2,06E-2
Pressure & Level	0,2	12	4,3	303	0	0	0	5	100	0	100	6,2E-4
Gas	7	8,7	4,3	303	0,01	0,5	0	5	50	0	100	1,82E-5
Leakage	7	8,7	4,3	303	0	0	0	5	100	5E-5	100	2,32E-4
Valve	7	8,7	4,3	303	0	0	0	5	100	0	10	2,32E-4
'Extreme'	0,2	5	2	368	0,01	0,5	0	20	0	1E-5	50	4,5E-12

For the analysis the RELAP5 mod3.2 was adopted as best-estimate code for the deterministic characterisation of the PSS. As accident transient it was selected a turbine trip followed by a reactor SCRAM, with the safety system required to intervene in order to remove the core decay power via an external pool. A total of 134 code-runs were performed for an equal number of different system configurations selected based on deterministic and stochastic selection (two stochastic selections of 64 configurations each, the first based on the discrete PDF, the second based on the continuous PDF).

Typical outputs are reported in **Figure 5** and **Figure 6**. The time evolution of the thermal power rejected to the pool is shown. **Figure 5** refers to the core decay power and heat transfer capability of the system in nominal conditions, while **Figure 6** shows results of code runs in the Probabilistic Sets.

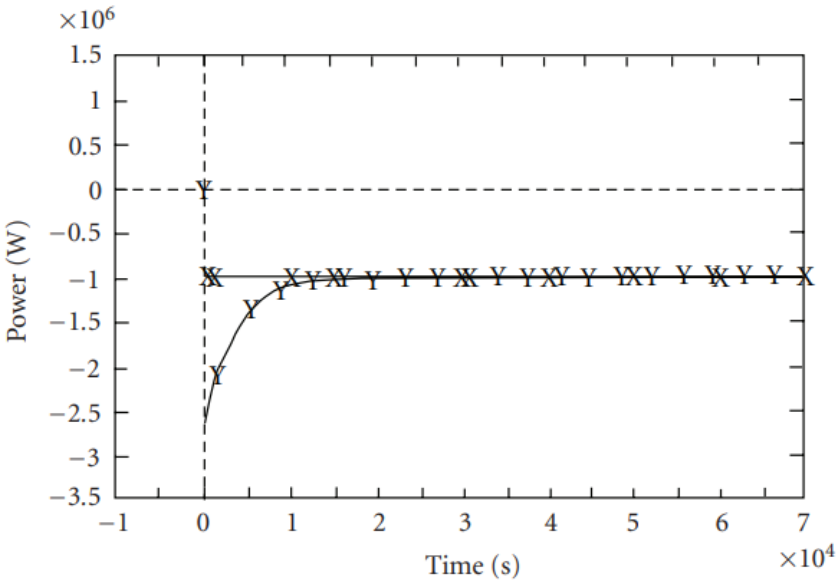

Figure 5 – Time evolution for the Core (X) and Reject (Y) Thermal Powers for the reference configuration (i.e. all Design and Critical Parameters with nominal values) [42]

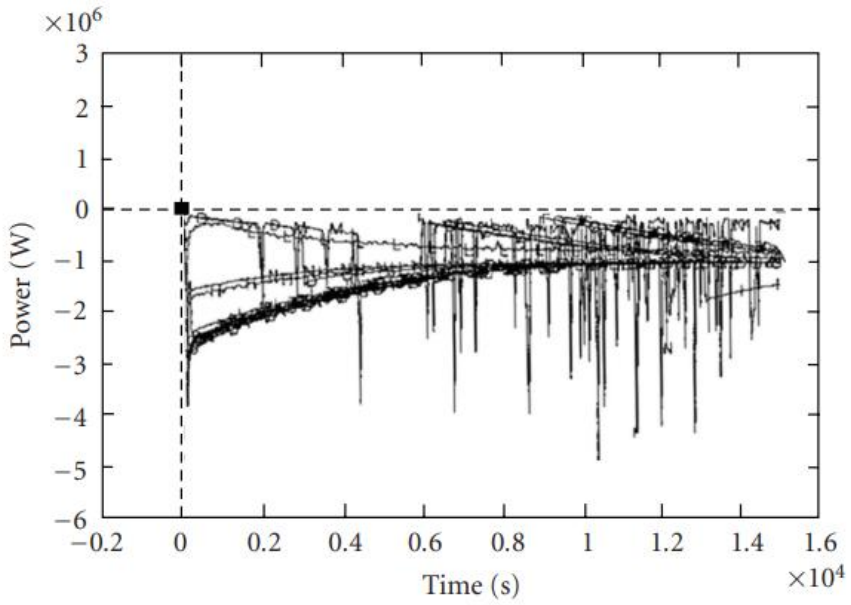

Figure 6 - Typical results for the Rejected Thermal Power for different system configurations belonging to the Probabilistic Set [42]

Finally, an additional indicator was defined for evaluating system performance and reliability. This parameter corresponds to the ratio Y/Y_{ref}, where Y is the integral of W_2 or Γ_2 between time 0 (start of system operation) and mission time (or observation time), calculated for each configuration in the probabilistic and deterministic sets; e.g. for the rejected thermal power:

$$\frac{Y}{Y_{ref}} = \frac{\int_0^{Tmission} W_2(t)dt}{\int_0^{Tmission} W_{2,ref}(t)dt}$$

Hence the result in **Figure 7**. In this case the curves of merit were used to judge the system acceptability and to compare the selected system with different system. They show the Performance Indicator (PI) values (Y/Y_{ref}) as a function of the probability of occurrence of the run.

2) Application on a passive Thermo-Hydraulic single-phase natural circulation separate effect test facility TTL-1.

Another example of the application of REPAS approach was carried out in [43] where the authors applied the methodology for deriving the reliability and for achieving design optimization information for a single-phase NC loop named TTL-1. A sketch of the test-facility is shown in **Figure 8**.

The sketch of the loop includes the main circulation pump (Pump), a filter (Filt.), the pre-heater (Preh.), a diesel engine for electric power generation (Mot. and Gen.), the electrically heated test section, the cooler, the pressurizer including heater and relief valves, a drain system, a N2 gas pressure source to control the pressure in the pressurizer and in the tank for liquid injection in the loop (Tank For Loc. Exps.). Instrumentation, including pressure (P), temperature (T) and flow rate (Flm.) transducers, valves and piping complete the loop.

The 29 design and critical parameters of the TTL-1 are reported in the second column of **Table 5**.

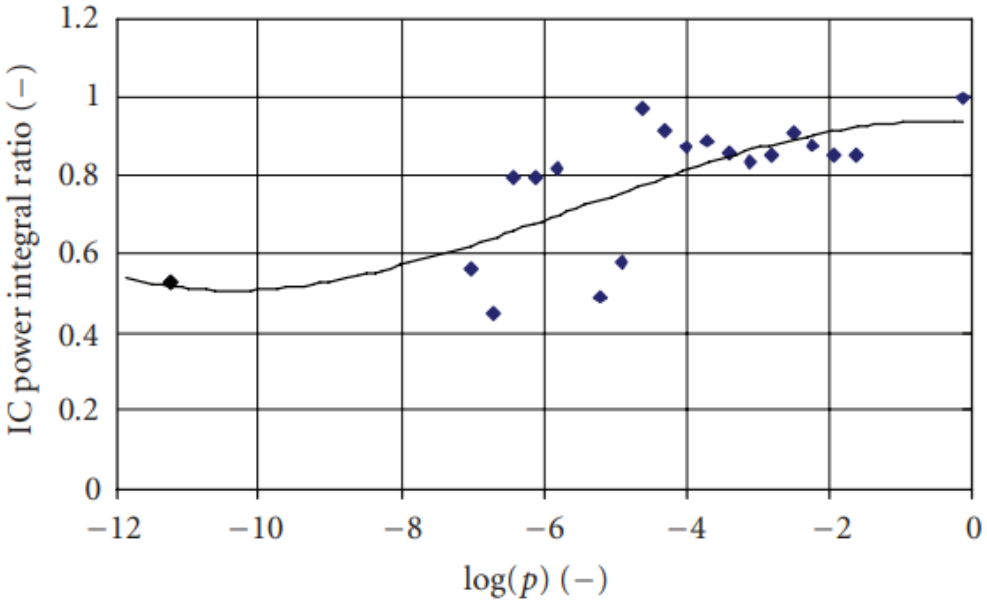

Figure 7 – Curves of merit: probability for the PI "IC power integral ratio" (discrete probability distribution) [42]

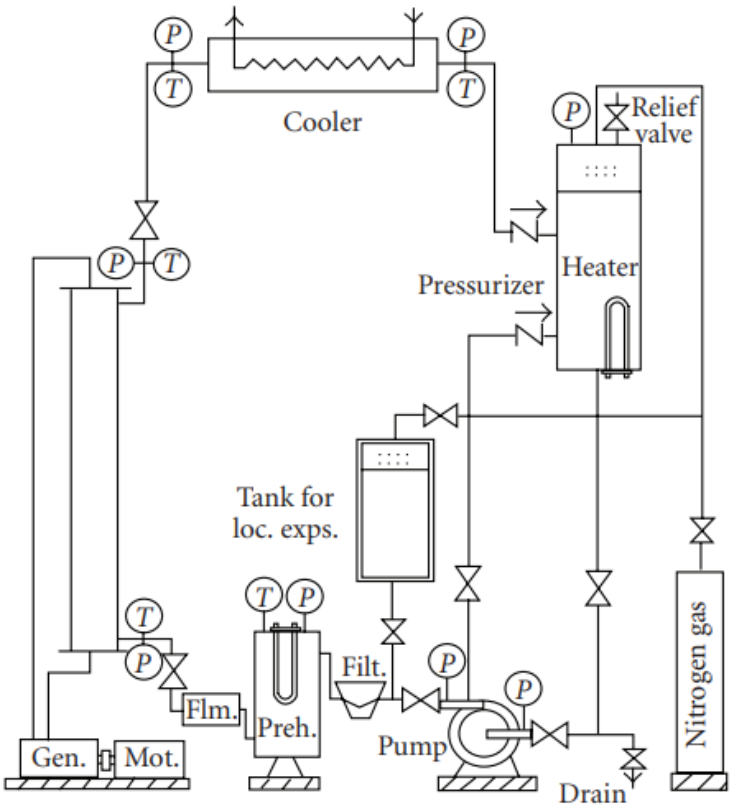

Figure 8 - Sketch of TTL-1 loop [43]

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Table 5 - Design and Critical parameters of the test facility [43]

Design & Critical Parameter		Unit	Nominal Value	Range	Discrete Initial Values & Probabilities
LP	Linear power of electrically heated rod	**W/m**	**30E+6**	**0 – 30E+6**	- *1*
P1	Initial pressure of the loop	**Bar**	**5**	**1 – 10**	**1 3 5 8 10** *0,02 0,13 0,7 0,1 0,05*
T2	Temperature of the SS fluid at the cooler inlet	**K**	**303**	**295 – 350**	**295 303 325 350** *0,18 0,65 0,15 0,02*
HL1	Heat losses from the test section (TS), %of TS power	**%**	**0,2**	**0 – 4,5**	**0 0,2 1 4,5** *0,1 0,69 0,15 0,06*
HL2	Heat losses from the loop w/o (TS), %of TS power	**%**	**3**	**0 – 20**	**0 3 10 20** *0,1 0,69 0,15 0,06*
L1	Total length of the loop	**m**	**21**	**12 – 34**	**12 21 28 34** *0,05 0,69 0,14 0,12*
LV	Loop volume (change of the pre-heater tank)	m^3	**0,09**	**0,07 – 0,2**	**0,07 0,09 0,12 0,2** *0,05 0,65 0,18 0,12*
PV	Volume of PRZ	m^3	**0,06**	**0,03 – 0,12**	**0,03 0,06 0,09 0,12** *0,05 0,65 0,18 0,12*
PN	Noding of the PRZ	-	**N**	**N1 – N2**	**N1 N N2** *0,1 0,8 0,1*
PP	Position of the PRZ	-	**U**	**U – D**[3]	**U D** *0,85 0,15*
K1	Local pressure drop coefficient (K) at the inlet of the TS	-	**0,2**	**0 – 1,2**	**0 0,2 0,4 1,2** *0,05 0,53 0,3 0,12*
K2	K factor at the outlet of the TS	-	**0,6**	**0 – 1**	**0 0,6 0,8 1,2** *0,05 0,53 0,22 0,2*

[3] Upstream the cooler (U), Downstream the cooler (D).

Design & Critical Parameter		Unit	Nominal Value	Range	Discrete Initial Values & Probabilities
TK	Sum of the K factors, w/o TS inlet and outlet	-	**7,5**	**3 – 25**	**3** *0,05* **7,5** *0,55* **15** *0,22* **25** *0,18*
EI	Electrical Insulation in the heater	-	**A**	**A – B**[4]	**A** *0,85* **B** *0,15*
CTT	Thickness of cooler tubes	**mm**	**2**	**1 – 3**	**1** *0,05* **2** *0,65* **3** *0,3*
CT	Cooler tubes	-	**Cu**	**Cu – SS**	**Cu** *0,85* **SS** *0,15*
E2	Equivalent diameter of secondary side of the cooler	**mm**	**10**	**7 – 20**	**7** *0,25* **10** *0,7* **20** *0,05*
E1	TS Equivalent diameter (coolant passage)	**mm**	**8**	**5 – 12**	**5** *0,05* **7** *0,3* **8** *0,55* **12** *0,1*
AR	Ratio of Heater heat transfer area to cooler heat transfer area	-	**0,18**	**0,05 – 0,37**	**0,05** *0,05* **0,12** *0,3* **0,18** *0,6* **0,37** *0,05*
PD	Axial power distribution	-	**U**	**C – S**[5]	**C** *0,1* **U** *0,65* **S** *0,25*
CO	Orientation of the cooler	-	**H**	**I – V**[6]	**I** *0,08* **H** *0,65* **V** *0,27*
MF2	Secondary side mass flow rate	**kg/s**	**1,2**	**0,4 – 1,8**	**0,4** *0,05* **1,2** *0,55* **0,8** *0,23* **1,8** *0,17*
P2	Secondary side pressure	**bar**	**1**	**1 – 10**	**1** *0,6* **5** *0,3* **10** *0,2*
LS	Presence of U-pipe or loop seal in the cold part of the loop	-	**No**	**Yes – No**	**Y** *0,2* **N** *0,8*

[4] AL_2O_3 **(A), Boron nitride (B).**
[5] Uniform(U), Cosine(C), Semi cosine(S).
[6] Vertical(V), Horizontal(H), Inclined(I).

Design & Critical Parameter		Unit	Nominal Value	Range	Discrete Initial Values & Probabilities
D1	Riser diameter	**mm**	**25**	**25 – 100**	**25** **50** **75** **100** *0,55* *0,25* *0,15* *0,05*
D2	Downcomer diameter	**mm**	**25**	**25 – 75**	**25** **50** **75** *0,55* *0,25* *0,2*
PC	PRZ Connection	**-**	**S**	**D – S**[7]	**S** **D** *0,8* *0,2*
G1	NCG mass fraction at the inlet of cooler piping	**-**	**0**	**0 – 1**	**0** **0,05** **0,3** **0,5** **0,8** *0,58* *0,3* *0,1* *0,01* *0,01*
G2	NCG mass fraction inside the TS	**-**	**0**	**0 – 1**	**0** **0,05** **0,3** **0,5** **0,8** *0,58* *0,3* *0,1* *0,01* *0,01*
UL	Undetected leakage	**kg/s**	**0**	**0 – 1E-2**	**0** **1E-5** **1E-3** **1E-2** *0,65* *0,25* *0,09* *0,01*

Different nodalizations of the TTL-1 loop have been set-up in order to fulfil the requirements coming from the selected parameters, e.g. different pressurizer layout (parameter PN), different loop length (parameter L1), presence of a 'U-pipe' or loop seal in the cold part of the loop (parameter LS). The nodalizations of the system were developed with the RELAP5 best-estimate TH code, and the sketch of one of these (that one related to the nominal configuration of the TTL-1) is shown in **Figure 9**.

[7] Direct(D), Surge Line(S).

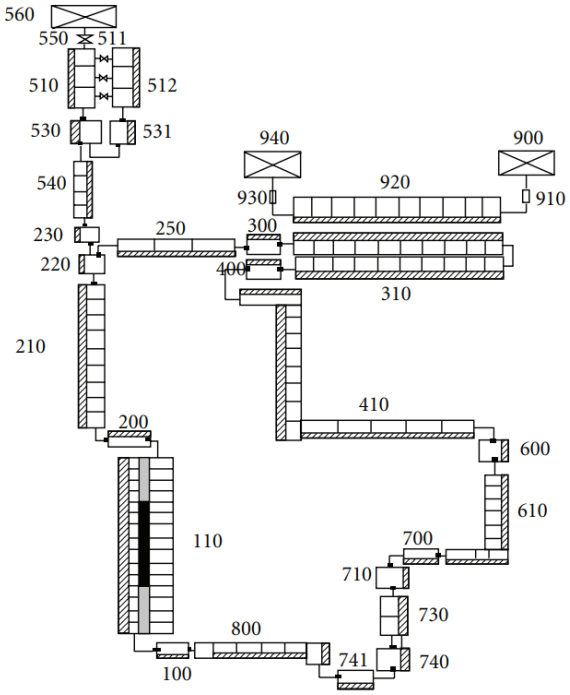

Figure 9 – RELAP5 nodalization [43]

Regarding the TM of the TTL-1 NC loop system, it has been established having in mind the procedure for the start-up of the NC process. It is assumed that at time 0s the loop is full of liquid water at 0,5 MPa and that a proper flow rate (constant value and constant inlet temperature) is flowing into the cooler. Starting from 0 s, electrical power is supplied to the heater rod, according to the following law:

- 0-3000 s, 10 kW;
- 3000-6000 s, 15 kW;
- 6000-9000 s, 20 kW;
- 9000-12000 s, 25 kW;
- 12000-18000 s, 30 kW.

The selected TM is that the above power must be transferred to the cooler via NC with an acceptable time delay as defined by the reference system performance.

For the present application, the FC adopted is of the “integral value over a mission time” type; specifically, the system must reject at least a specified average thermal power value during the observation time:

$$FC = \frac{W_{ref} - W}{W_{ref}} \leq 0.2 \qquad (2.1)$$

where

$$W = \frac{\int_0^{\tau_{obs}} \omega(t)dt}{\tau_{obs}} \qquad (2.2)$$

and

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

"ref" is related to the code calculation for the reference/nominal system configuration, ω is the power exchanged in the cooler and τ_{obs} is the "observation time".
Namely, the system performance is accepted if FC $\leq$ 0.2.

Using Wilks' formula, 100 sets of probabilistic inputs were selected to ensure a high level of confidence (greater than 95%). An additional 36 input sets were also identified deterministically through expert judgment. So, a total of 137 system configurations (namely, 36 deterministic, 100 stochastic configurations plus the reference configuration) have been considered that led to a corresponding number of code runs.

An idea of the results obtained can be derived from **Figure 10** , where the time evolution of the power exchanged (ω) through the TTL-1 cooler is plotted as a function of time in relation to the execution of the reference code and executions of code No. 37-56.

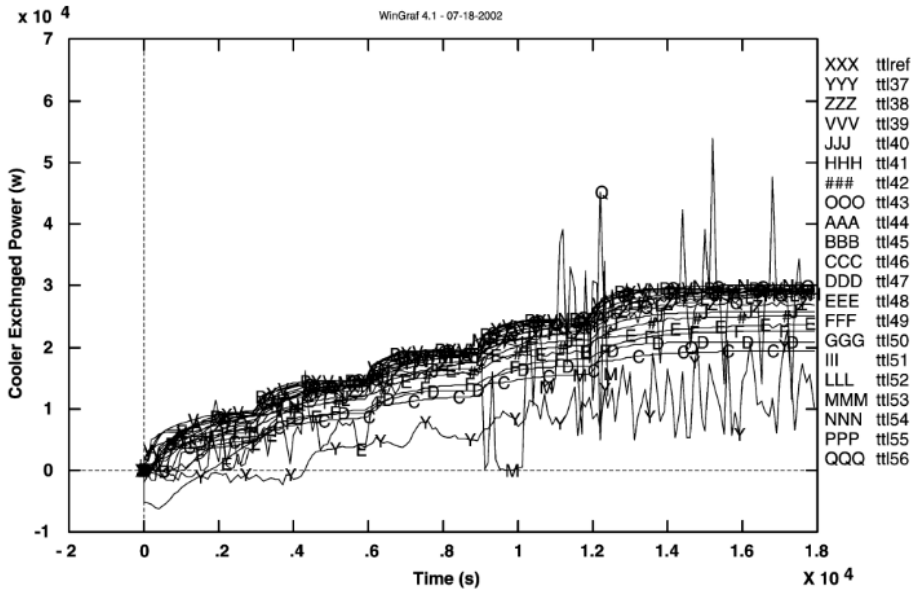

Figure 10 - Time trends related to the ensemble of 137 code runs (Ref. 37-56 probabilistic sets) "power exchanged in the cooler" [43]

Four definitions have been identified for the T-H reliability of the TTL-1 loop:

1. The "figure of merit" approach where the final result is given in **Figure 11**.

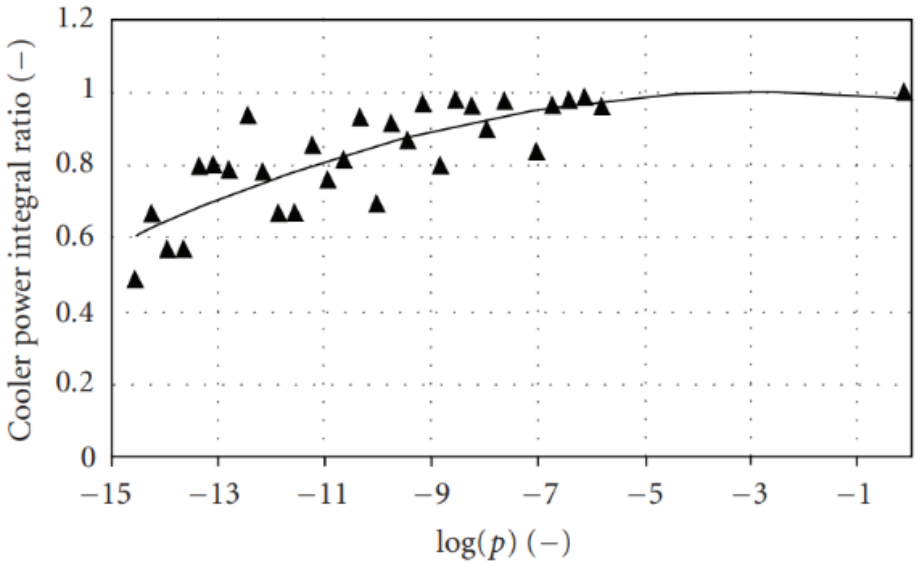

Figure 11 - Probability distribution for performance indicator W (Eq. 2.2) [43]

The proposed figure of merit shows the W/W_{ref} performance indicator values as a function of the probability interval range. The thick line is obtained by an automatic data interpolation technique.

2. The 'cumulative probability' approach (suggested by Marques et al. 2002 [52]) makes use of the classic Cumulative Distribution Function concept and the final result is given in **Figure 12**. In this plot a comparison was made with the result from a previous REPAS application (Bianchi et al., 2002 [42]).

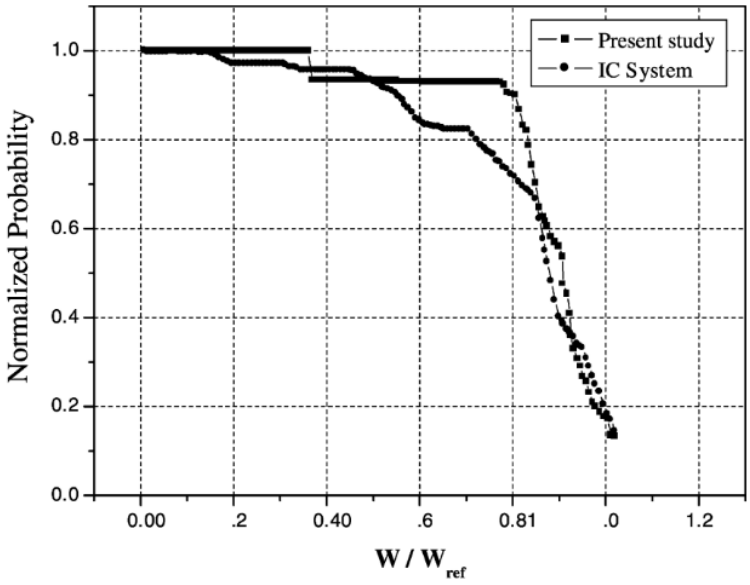

Figure 12 - Comparison between thermal hydraulic reliability for two different systems: IC-SBWR (two-phase NC system) and TTL 1 [43]

Here the PSS reliability is estimated by ordering the cooler power integral ratios (W/W_{ref}) with respect to the probability of occurrence of each configuration from the probabilistic and deterministic sets. The total sum of the occurrence probabilities is normalized to 1.

3. The R1 single-valued reliability definition:

$$R1 = 1 - \frac{NF}{N} = 0.7$$

where NF is the number of failed runs and N is the total number of runs.

4. The R2 single-valued reliability definition:

$$R2 = \frac{\sum_1^N (W/W_{ref})}{N} = 0.85$$

3) Application on a passive pool heat removal system for a prototypical integrated system [44]

In this example, the REPAS methodology is applied to a typical 'pool heat removal system' in which the heat source, the steam generator and the primary recirculation loop, are contained within the RPV, as illustrated in **Figure 13**.

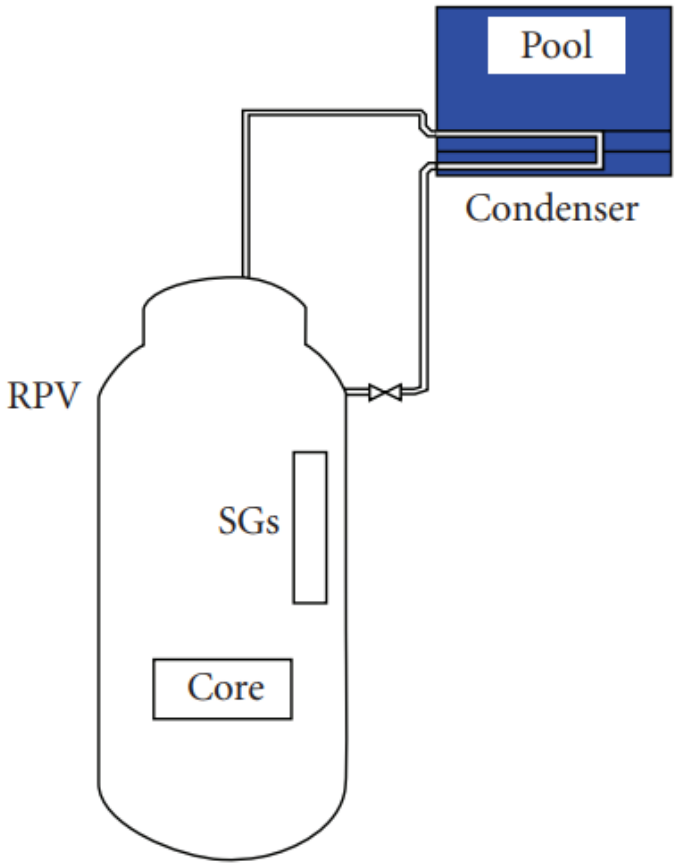

Figure 13 – Passive pool heat removal system for prototypical integrated system [44]

The TM of the system is to remove the decay heat reducing the pressure in the primary system.

In **Table 6** and **Table 7** are reported the design and critical parameters; for each of them are defined nominal values, range of variation, and an assigned probability distribution. The full characterization of a T-H system may need a very large number of such parameters. Therefore, a bounded number of parameters should be selected deterministically (based on engineering judgment) and statistically (e.g., through a Monte Carlo procedure).

Table 6 - Design parameters of the PHRS integrated system [44]

Design Parameter ID	Description
OP	Nominal Power
SD	SCRAM delay
DF	Decay power factor
$P1$	Reactor nominal pressure
SP	SCRAM: pressure set point
$P2$	PHRS: pressure set point
$L1$	RPV: dome water level
M	PCS: mass flow rate
$T1$	PHRS: valves opening time
PT	PHRS: pool temperature
TT	PHRS: tube thickness

Table 7 - Critical parameters of the PHRS integrated system [44]

Critical Parameter ID	Description
$C2$	Heat Losses piping
$W1$	PHRS tube thickness
HL	RPV dome heat losses
F	PHRS friction
Psp	Safety valves: pressure set point

The simulations concern the accidental scenario of loss of the ultimate heat sink with the assumption of loss of all safety systems involved (no feeding and bleeding strategy is considered).

The nodalization was developed with RELAP5 best-estimate code and it is shown in **Figure 14**.

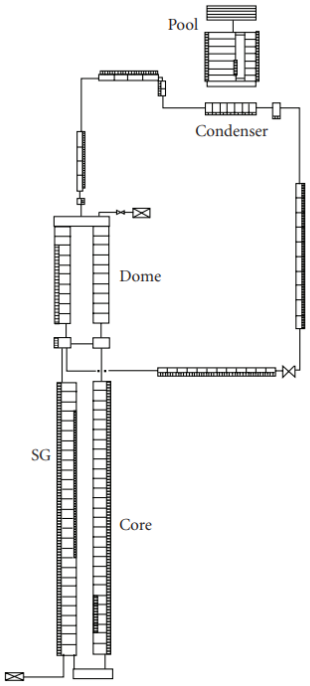

Figure 14 - Simplified RELAP5 nodalization of the PHRS [44]

The design FC defined for the transient sequence is the "opening of the safety valves during any stage of the transient". The failure of the system is reached when passive safety valves are open. As in the previous presented applications, applying the Wilks' formula, the minimum number of code runs needed for the purpose of the analysis had been addressed. The selected sample size is one hundred. Additionally, ten deterministic cases where added (based on engineering judgment) to add completeness to the analysis; in particular, five "a priori" to evaluate parameters combinations not achieved by the stochastic selection and five "a posteriori" considering as feedback the results obtained from sensitivity analysis.

To characterize the PSS performance three Transient Performance Indicators (TPI) were defined. In particular they indicate how far the system is from the opening condition of the passive safety valve of the condenser system. In terms of the system mission two design targets have been defined: long-term (e.g., hot shutdown condition) and short-term (e.g., primary overpressure) design target.

TPIs defined are:

I.
$$\chi_{CASEi}\big|_{65000} \geq 0.9 \cdot \chi_{NOMINAL\ CASE}\big|_{65000} \qquad \text{where} \quad \chi(t) = \frac{P_{HX}(t)}{P_{CORE}(t)}$$

II.
$$\frac{1}{(eot - T_i)}\int_{T_i}^{eot} \chi_{CASEi}(t)dt \geq 0.9 \cdot \frac{1}{(eot - T_{NOM})}\int_{T_i}^{eot} \chi_{NOMINAL\ CASE}(t)dt$$

III.
$$p_{CASEi}\big|_{65000} < 1.1 \cdot p_{NOMINAL\ CASE}\big|_{65000}$$

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

where P_{HX} is the Power exchanged across the condenser tubes, P_{CORE} is the Core power, T_{PHRS} is the activation time, p is the primary circuit pressure, *eot* is the end of transient (65000 seconds).

Below are reported the main outcomes of the three TPIs defined above (**Figure 15**, **Figure 16**, **Figure 17**).

In particular, only three probabilistically selected cases over 100 do not meet the first proposed TPI, the second proposed TPI is verified by all the 100 probabilistically selected cases and the third proposed TPI is verified by 78 over 100 probabilistically selected cases.

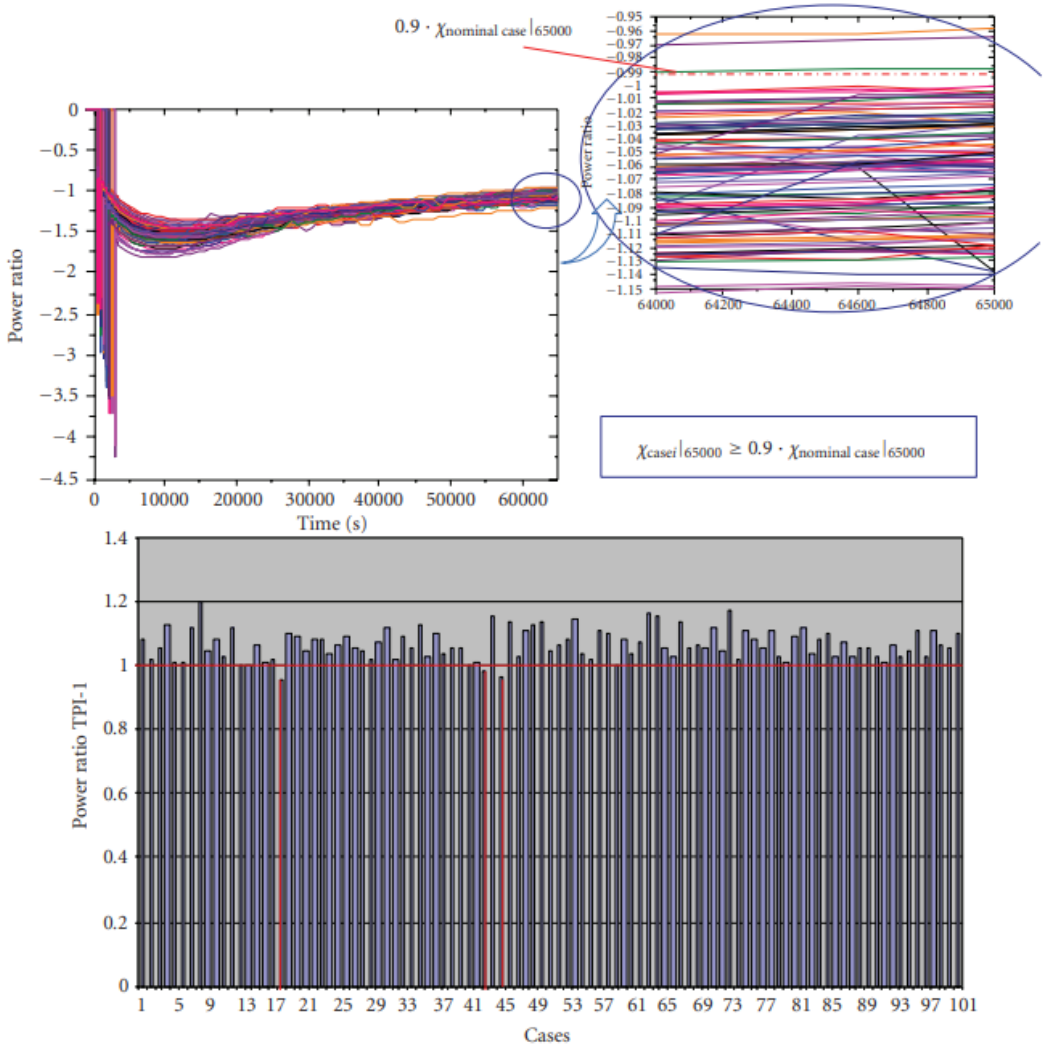

Figure 15 - TPI-1 results [44]

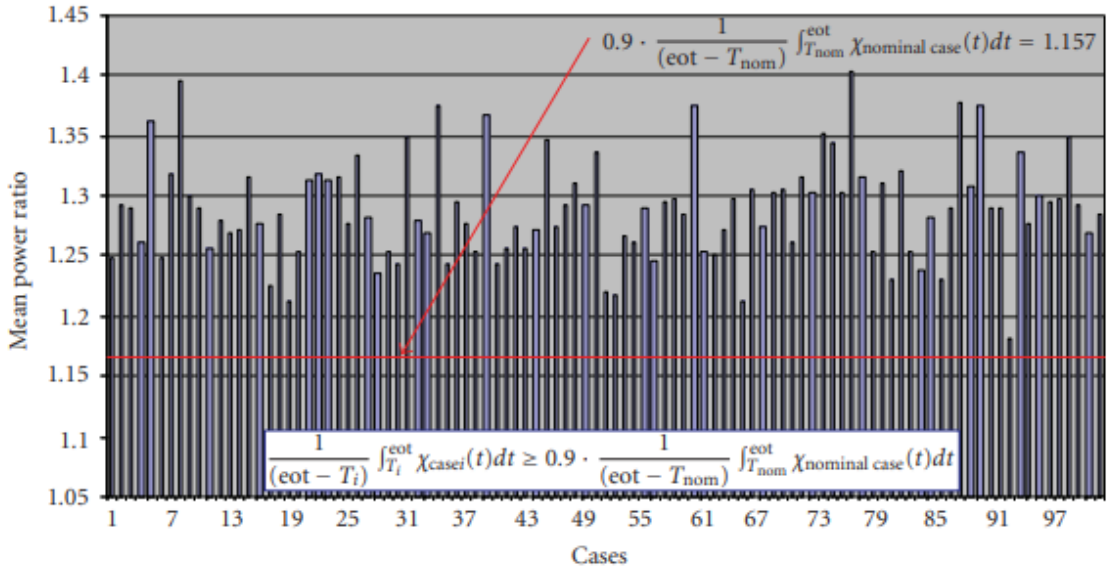

Figure 16 - TPI-2 results [44]

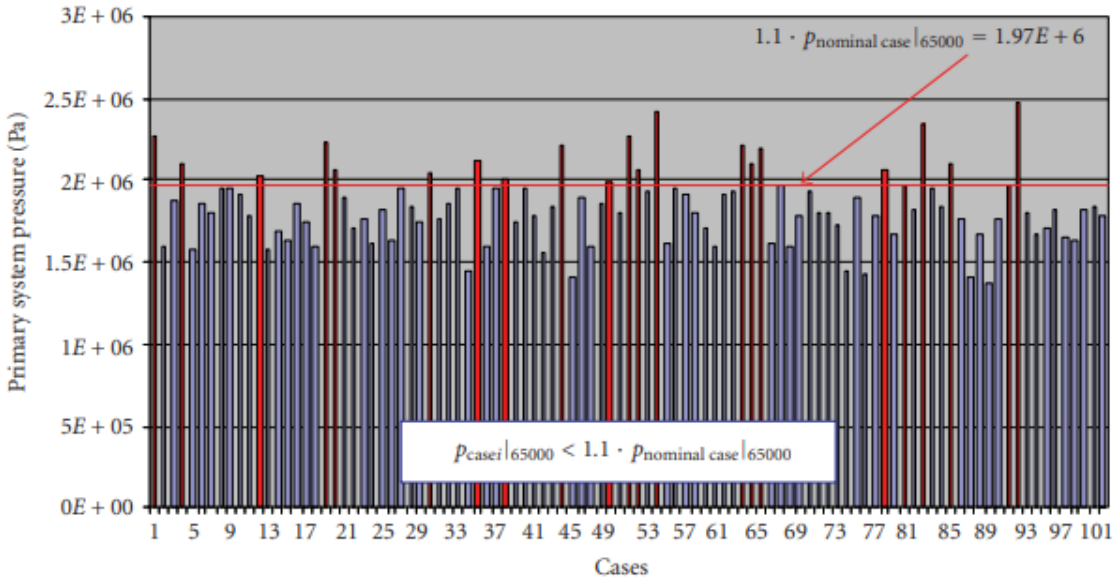

Figure 17 - TPI-3 results [44]

4) Application on an active system. The system in question is the sump of a generic three-loop PWR-900 [46]

The present study represents the first (and only) application of the REPAS methodology to an active system. In 1992, following a Loss Of Coolant Accident (LOCA) at the Barsebäck-2 NPP in Sweden, clogging of the sump strainers occurred, due to the accumulation of fibrous material stripped by the primary coolant jet from the pipe insulation. Following this event "Sump clogging" has been identified as a relevant issue. So, the aim of this work was to apply REPAS to analyze the sump clogging issue following a LOCA and its impact on the reliability of the ECCS long-term core cooling function. Therefore, the TM is to ensure long-term cooling of the core and the most important parameters (with their reference values, range of variation and associated PDFs) chosen for the scope of the analysis are shown in **Table 8**.

Table 8 – Selected parameters for the current REPAS probabilistic code calculations [46]

Parameter	Reference value	PDF
Sump opening ratio	1	Histogram 1%, 0≤x<0,05 2%, 0,05≤x<0,1 17%, 0,1≤x<0,5 80%, x≥0,5
Containment outer side heat transfer coefficient	10 W/m^2K	Histogram 15%, 0 W/m^2K ≤x<5 W/m^2K 70%, 5 W/m^2K ≤x<15 W/m^2K 15%, 15 W/m^2K ≤x≤20 W/m^2K
Core power scaling factor	1	Normal (mean 1, standard deviation 0,02)
Sump heat exchanger outer wall temperature	293,15 K	Histogram 17,5%, 283,15 K ≤x<285,15 K 65%, 285,15 K ≤x<301,15 K 17,5%, 301,15 K ≤x≤303,15 K
Sump strainers minor loss coefficient	100	Histogram 55%, 100 ≤x<150 25%, 150≤x<175 20%, 175≤x≤200
RWST mass offset	0 m^3	Histogram 17,5%, -1,692E5 kg ≤x< -8,4601E4 kg 65%, -8,4601E4 kg ≤x< 8,4601E4 kg 17,5%, 8,4601E4 kg ≤x≤ 1,692E5 kg
Pump sump volumetric flow rate	0,2 m^3/s	Uniform (min 0,18 m^3/s , max 0,22 m^3/s)

The application has been carried out for a generic three-loops PWR-900 modeled with TRACE (TRAC/RELAP Advanced Computational Engine) best-estimate thermal-hydraulic system code developed by USNRC [45]. In **Figure 18** we can observe the nodalization of the system.

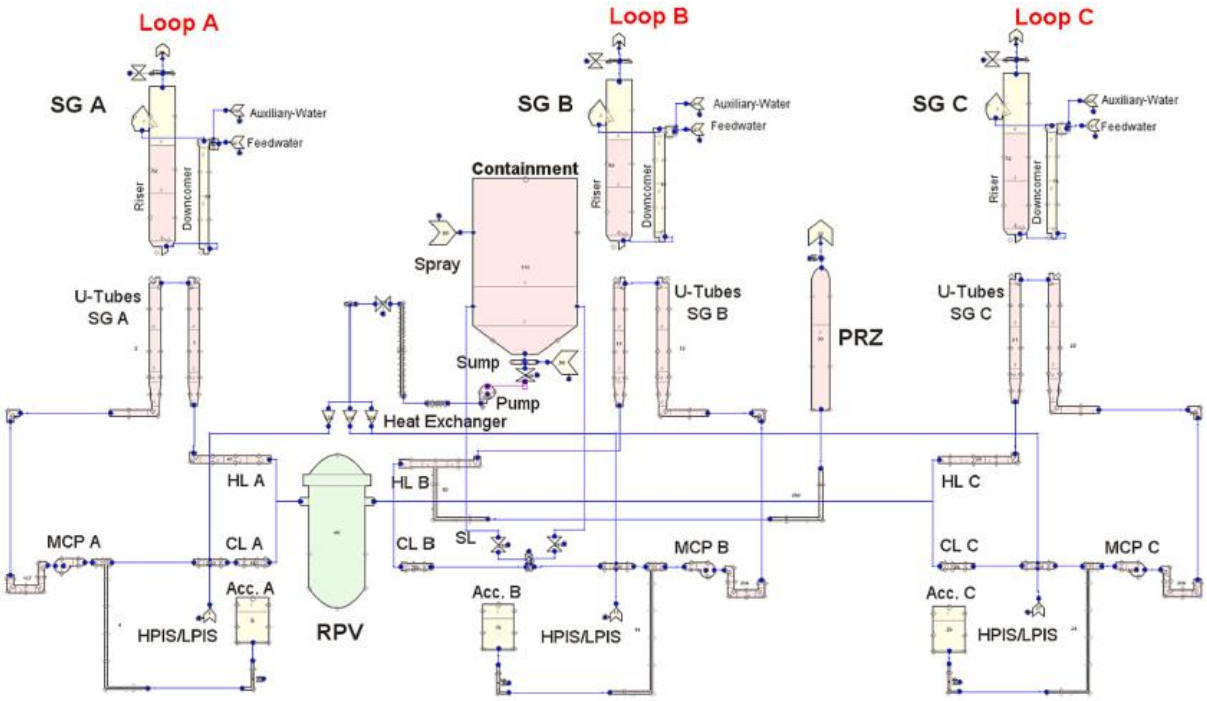

Figure 18 – TRACE nodalization of the PWR-900 [46]

For the present REPAS application, three FC have been identified based on the reference calculation results:

1) **Maximum cladding temperature**. In the reference calculation, the final cladding temperature is around 400 K, therefore:
   FC1: cladding temperature >600 K after the start of sump circulation;

2) **RPV collapsed level**. In the reference calculation, the core is always covered by the coolant after the end of the reflood phase, therefore:
   FC2: RPV collapsed coolant level <3/4 of the active core after the start of sump circulation;

3) **Containment pressure**. In the reference calculation, the final containment pressure is around 1.5 bar, therefore:
   FC3: Containment pressure >2.0 bar after the start of sump circulation.

It is important to underline that the above FC definitions are not related to engineering or safety limits, rather they are defined based on the reference calculation.

For probabilistic calculations, 200 runs were performed, while the deterministic calculations performed are 6 and were added to account for low values of sump opening area and high values of decay power.

In **Figure 19**, **Figure 20**, **Figure 21** are shown the results for both deterministic and probabilistic calculations, with the reference of the three FC identified.

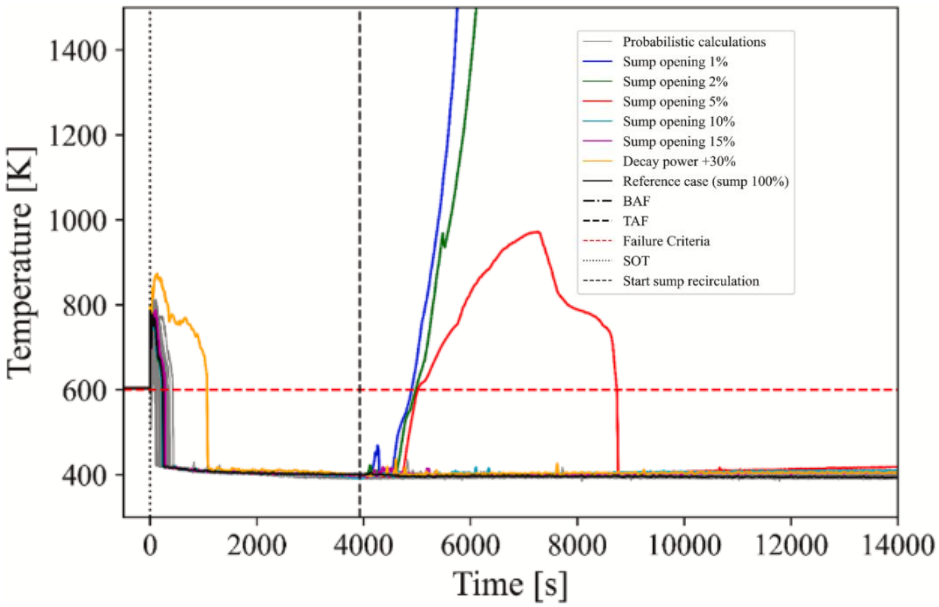

Figure 19 - Maximum cladding temperature [46]

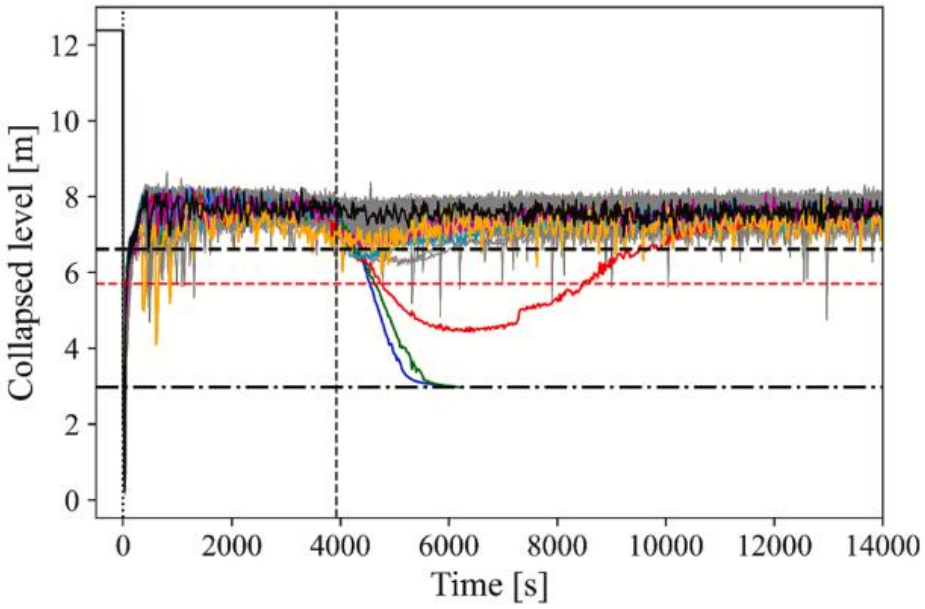

Figure 20- RPV collapsed coolant level [46]

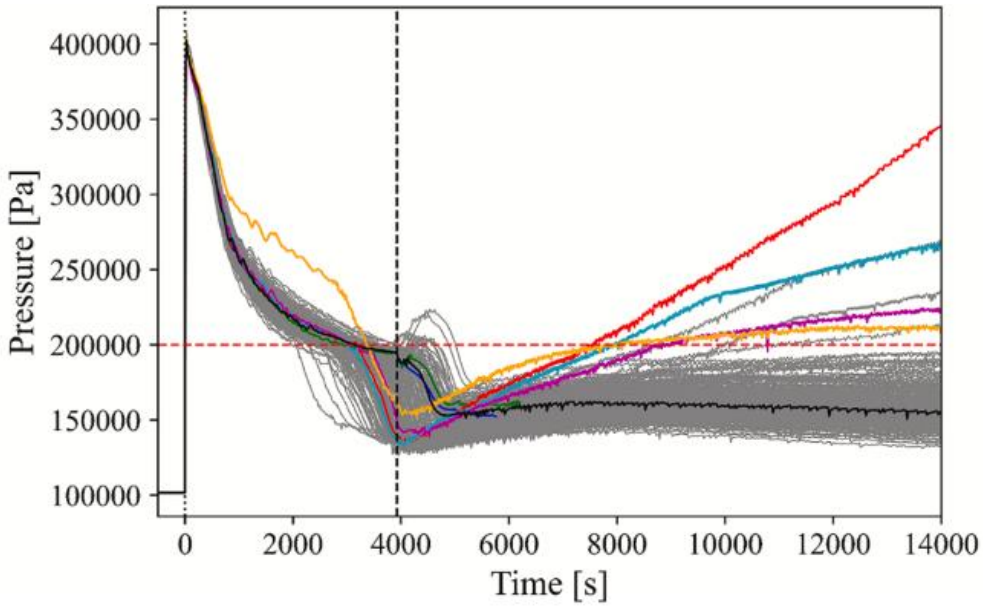

Figure 21 - Containment pressure [46]

No probabilistic calculation meets FC1 (**Figure 19**), as the maximum cladding temperature consistently stays below 600 K after sump circulation begins. FC2 is satisfied in 7 out of 200 probabilistic calculations (**Figure 20**). However, in these instances, the RPV level drops below the FC2 threshold only briefly due to local oscillations. As a result, core dry-out does not occur, and the maximum cladding temperature remains well below 600 K, meaning FC1 is still not met, as previously noted. When considering the third FC (containment pressure), it is fulfilled in 16 out of 200 probabilistic calculations (**Figure 21**). In 13 of these calculations, the pressure exceeds the threshold immediately after sump circulation starts, due to a local pressure peak. However, only 3 calculations remain above FC3 over the long term.

Based on deterministic calculations, FC1 is met in three cases: sump opening ratios of 1 %, 2 %, and 5 %. At 5 %, the maximum cladding temperature exceeds the FC threshold for about 4000 s before the core is quenched and the temperature drops back to around 400 K (for 1 % and 2 %, the core uncovers completely, and the temperature continues to rise until the calculation stops). For FC2, which is linked to FC1, it is met at 1 %, 2 %, and 5 % sump opening ratios. At 5 %, the collapsed level drops below half of the active core but then rises above the top of active fuel.

Regarding FC3 (containment pressure), it is exceeded with sump opening ratios of 5 %, 10 %, and 15 %. FC3 is not met with 1 % and 2 %, but the simulation stops due to the TRACE cladding temperature limit being reached, suggesting that FC3 would likely be met if the calculations continued. Additionally, FC3 is met when decay power is increased by 30 %, as the higher energy input exceeds the sump heat exchanger's capacity, causing the pressure to rise above the threshold.

The final step of the REPAS application is to estimate the probability of (functional) failure of the system, therefore **Figure 22**, **Figure 23**, **Figure 24** show respectively the maximum cladding temperature, the minimum RPV collapsed level and the maximum containment pressure after the start of sump circulation, as a function of their probability p of occurrence.

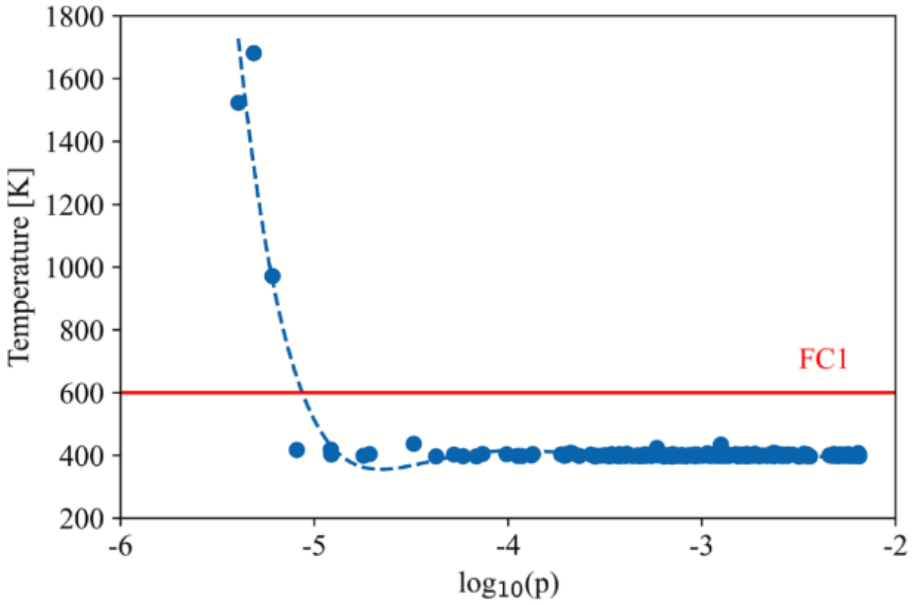

Figure 22 – Maximum cladding temperature as a function of the occurrence probability [46]

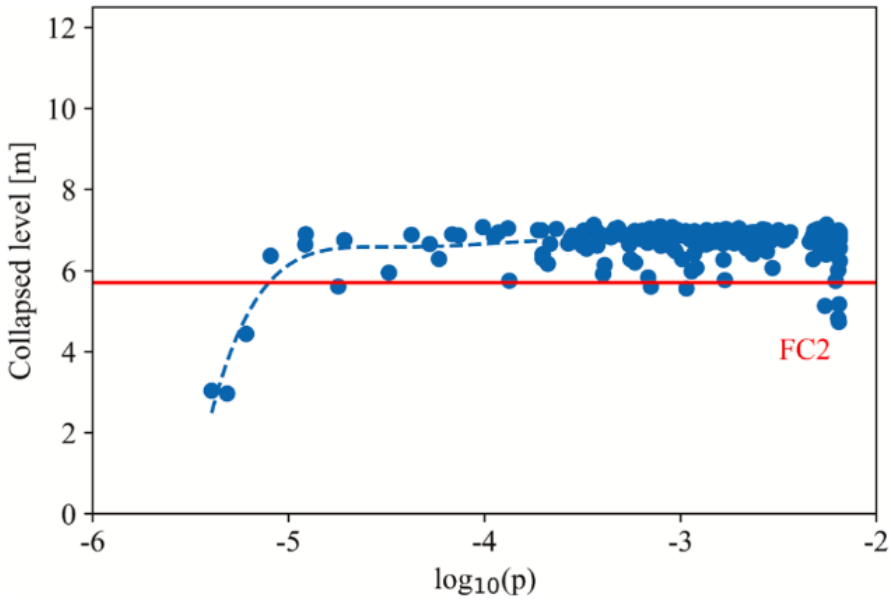

Figure 23 - Minimum RPV collapsed level as a function of the occurrence probability [46]

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

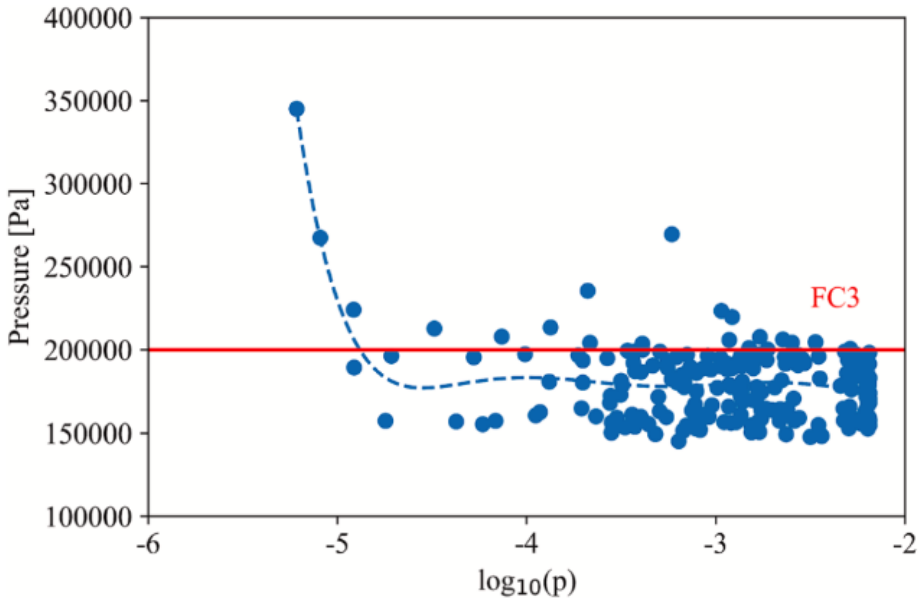

Figure 24 - Maximum containment pressure as a function of the occurrence probability [46]

2.2.1.4. Relevance for WP4

The REPAS methodology is crucial for a WP4 focused on the reliability of PSSs in nuclear reactors (including SMRs). Traditional PSAs often emphasize active components, potentially overlooking the functional failure modes of PSSs due to environmental or boundary condition variations. REPAS addresses this gap by providing a structured approach to evaluate the reliability of PSSs.

Key features of the REPAS methodology include:

- **Uncertainty Analysis:** Identifying and quantifying uncertainties in physical and geometric parameters that can affect system performance.
- **Thermal-Hydraulic Modeling:** Using best-estimate thermal-hydraulic codes (e.g., RELAP5, TRACE) to simulate system behavior under various conditions.
- **Monte Carlo Sampling:** Propagating uncertainties through simulations to assess the probability of system failure.
- **Integration into PSA:** Incorporating PSS reliability into broader safety assessments to provide a comprehensive risk profile.

By adopting REPAS, the project can achieve a deeper understanding of PSS reliability, leading to improved design, optimization, and safety assurance. This methodology supports the development of robust passive safety features, aligning with the project's objectives to enhance the reliability of nuclear reactor systems.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

2.2.2. RMPS

2.2.2.1. Description

The RMPS method (Reliability Methods for Passive Safety Functions) is an approach developed within the framework of the 5th European Framework Program to assess the reliability of passive safety functions in industrial systems [53]. While primarily applied to PSSs in the nuclear industry (as in WP4), it is also relevant to other high-risk sectors; such as chemical, oil, and gas facilities. The RMPS method is used to improve the understanding, analysis, and optimization of the reliability of PSSs in industrial environments, with a focus on applications where safety and failure prevention are critical.

The application of RMPS methodology is based on the following steps:

1) Characterization of the system (intended missions, possible failure modes, success and failure criteria) and definition of the scenario (for example, an accidental transient) in which the system will operate and the success/failure criteria,
2) Modelling of the system with a best-estimate (BE) code (for instance, a thermal-hydraulic system code as CATHARE or RELAP5),
3) Identification of the relevant parameters that significantly impact the system (based on sensitivity calculations, or on expert judgment),
4) Quantification of the uncertainties (a probability distribution function) for the relevant parameters (based on existing data, or on expert judgment),
5) Propagation of the uncertainties (for example, by applying the best-estimate code with a stochastic approach, potentially supplemented by surrogate methods to mitigate computational constraints),
6) Evaluation of the reliability (based on the uncertainties propagation and the success/failure criteria).

This RMPS methodology roadmap is summarized in **Figure 25** listed below. The main output is the system's failure probability for the considered scenario; through the uncertainties propagation, it also provides a better understanding of the system and its sensitivity regarding the input parameters.

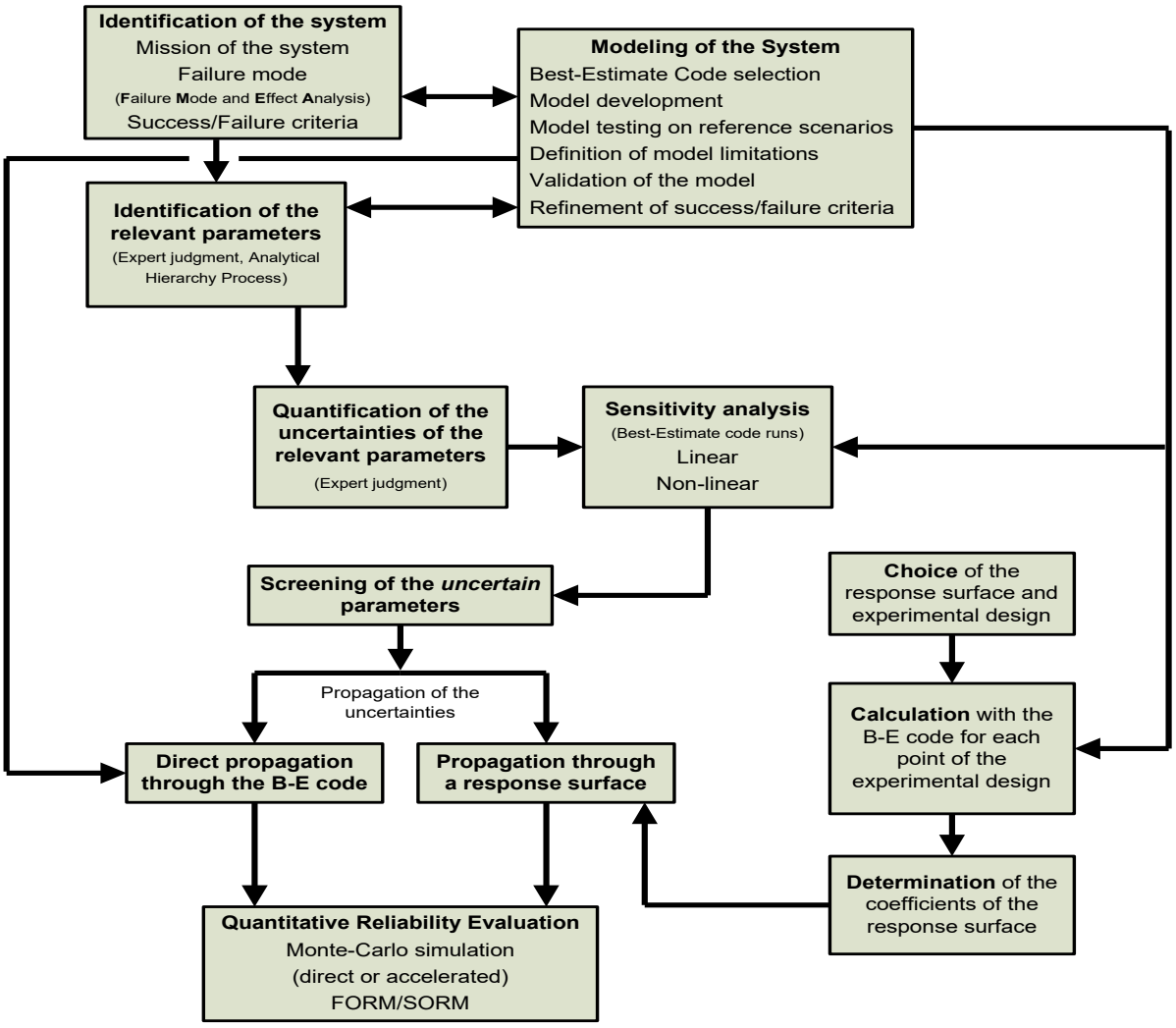

Figure 25 - RMPS methodology roadmap

2.2.2.2. Advantages and Limitations

The RMPS methodology provides a realistic and quantitative assessment of the PSS reliability, thanks to the flexibility of the Monte-Carlo simulation, which leverages the T-H model complexity without resort to simplifying approximation.

It has successfully been applied to various PSSs in different types of reactors (see chapter 2.2.2.3 for more details).

Thanks to the uncertainty propagation, this methodology enhances understanding of the analysed system and its sensitivity to the input parameters while also identifying critical reliability factors.

The first limitation of the RMPS methodology is linked to the use of the BE code, which should be validated for the specific application. However, validation is not always available, for example for T-H safety PSSs operating at low pressure (then the needed R&D should be developed). The reliability resulting from the methodology application can also be strongly affected by the system modelling (user effect), so it should follow the state-of-the-art (if existing). Moreover, the results may depend on the nodalization used to model the system, and so suffer from the influence of the user-effect.

A second difficulty in the application of the RMPS methodology is in the quantification of the uncertainties of the relevant parameters. In a T-H safety PSS, two categories of parameters can be encountered: T-H correlations of the BE code (for example nucleate boiling or interfacial friction) and system parameters (for example the non-condensable gas mass, or the fouling of a heat exchanger). For T-H correlations, the quantification of the uncertainties can be based on experiments (see for example the BEMUSE program [55]); for system parameters, the quantification can be based on operation data of existing similar systems. However, in most cases, the quantification of the uncertainties relies on expert judgment.

The third and main limitation of the methodology is the computational cost [56]. The first method for the propagation of the uncertainties is the direct Monte-Carlo simulation technique. Depending on the failure probability aimed for the system, this propagation requires a very large number of simulations (the smaller the failure probability and its variance, the greater the number of simulations). Very small failure probability may require millions of calculations, as the number N of calculation should be greater than $\frac{f^2}{P_f}$, with P_f the failure probability and f the fractional error [1]. However, If the system is complex (several circuits with two-phase flow phenomena for example), each simulation can involve a long calculation time (several hours), leading to non-affordable total computational cost. To reduce the number of T-H code runs and the computational time as much as possible, alternatives to be considered are fast running surrogate regression models (also called response surfaces or metamodels) and advanced Monte Carlo simulation methods. Fast-running surrogate regression models mimic the response of the original T-H model code, circumventing the long computing time. The main surrogate methods are polynomial response surfaces, polynomial chaos expansions, stochastic collocations, artificial neural networks, support vector machines and kriging.

A final limitation is that the reliability obtained from the application of the methodology is directly related to the studied scenario and must therefore be reassessed for any other scenario. This scenario-dependency can severely increase the workload and the complexity.

2.2.2.3. Applications already available

The initial application was performed for the development of the methodology [53], with the study of a residual passive heat removal system (called RP2) implemented on a PWR, as shown in **Figure 26.** The RP2 system has two main missions, first to depressurize the primary circuit, and second, to prevent core meltdown. For the exercise, the accidental transient considered was a loss of electrical supply; the duration of accidental sequence was arbitrarily set at 12 h, where no human intervention is simulated. The failure of the system is obtained if the maximum clad temperature or the fluid temperature at the core output exceed, respectively, the values of 500 °C and 450 °C, in less than 12 h. The PWR and the PR2 system are modelled with the CATHARE 2 code. On expert judgment, 14 uncertain parameters were identified, and uncertainties were associated. For example, in one scenario, 76 calculations were performed with CATHARE with values for the input variables randomly generated based on the probabilistic model. Among these 76 calculations, 18 cases of failure were observed, leading to a rough estimation of the failure probability of 0.24. The results of failure probabilities for different scenarios (availability of one or several RP2 loops) were integrated in a PSA for the loss of electrical supply accidental transient (see **Table 9**). The corresponding core damage frequency is then estimated at $7{,}5\times10^{-8}$ per year.

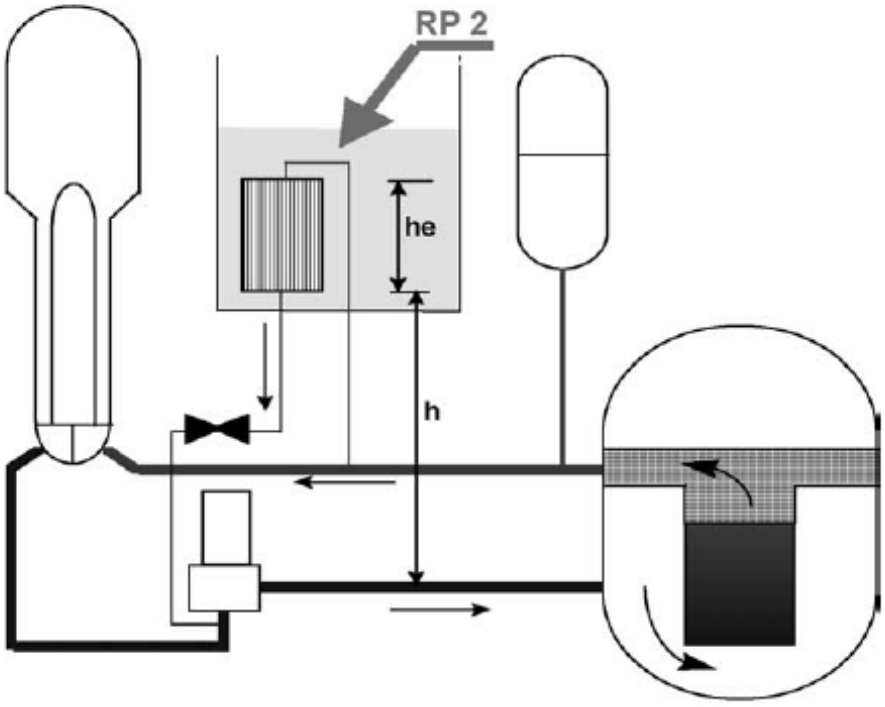

Figure 26 -Sketch of the residual passive heat removal system on the Primary circuit (RP2) [53]

Table 9 - Simplified event tree of Total Loss of Power Supply on a PWR equipped with the RP2 system [53]

Loss of electrical supply 10^{-5}/year	Number of RP2 available Failure on solicitation 10^{-2}/demand/RP2 loop	Broken tubes in, at least, one of 3 RP2 loops 3.10^{-3}/ 3 RP2	Failure of the thermal-hydraulic process (probability)	Safety injection 10^{-3}/demand	Number of the sequence	Final situation of the reactor	Yearly occurrence
	3 RP2 loops $P = 1 - 3.10^{-2} - \varepsilon$				1	Safe situation	
					2	Safe situation	
					3	Core damage	Less than 10^{-10}/y
	2 RP2 loops $P = 3.10^{-2}$				4	Safe situation	
			P_1		5	Core damage	$P_1 * 3.10^{-7}$/year
					6	Safe situation	
			P_2		7	Core damage	Less than 10^{-10}/y
					8	Core damage	$P_2 * 9.10^{-10}$/year
	1 RP2 loop $P = 3.10^{-4}$				9	Core damage	3.10^{-9}/year
					10	Core damage (envelop effect)	Less than 10^{-10}/y
	0 RP2 loop $P = 10^{-6}$				11	Core damage	Less than 10^{-10}/y
					12	Core damage	Less than 10^{-10}/y

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

A second application of the RMPS methodology has been performed on the "CAREM-like" reactor with the study of the Isolation Condenser (IC) [1], [57], see **Figure 27.** The term "CAREM-like" implies that the model used approximates the design characteristics of the CAREM-25 reactor (geometric values, systems layout, etc.) without being actual design values, and further simplifications have been taken into account. The accidental scenario considered is a station blackout: the IC's mission is to remove the decay heat from the primary system, to avoid an increase of the pressure and the opening of the safety valves. The system (primary circuit and IC) is modelled with the RELAP5 mod3.3 code; three different modelling are done, differing in the dome discretization (see **Figure 28**). Following expert judgment, 17 uncertain parameters were identified, and uncertainties were associated. 100 calculations were performed with RELAP5 by propagating the uncertainties in the model: none of them led to the failure of the PSS. A response surface (surrogate model) was then constructed, to estimate the failure probability. Depending on the modelling of the system (dome nodalization), the failure probability was estimated between $1{,}5x10^{-3}$ and $1{,}0x10^{-5}$, highlighting the influence of the user-effect on the methodology result.

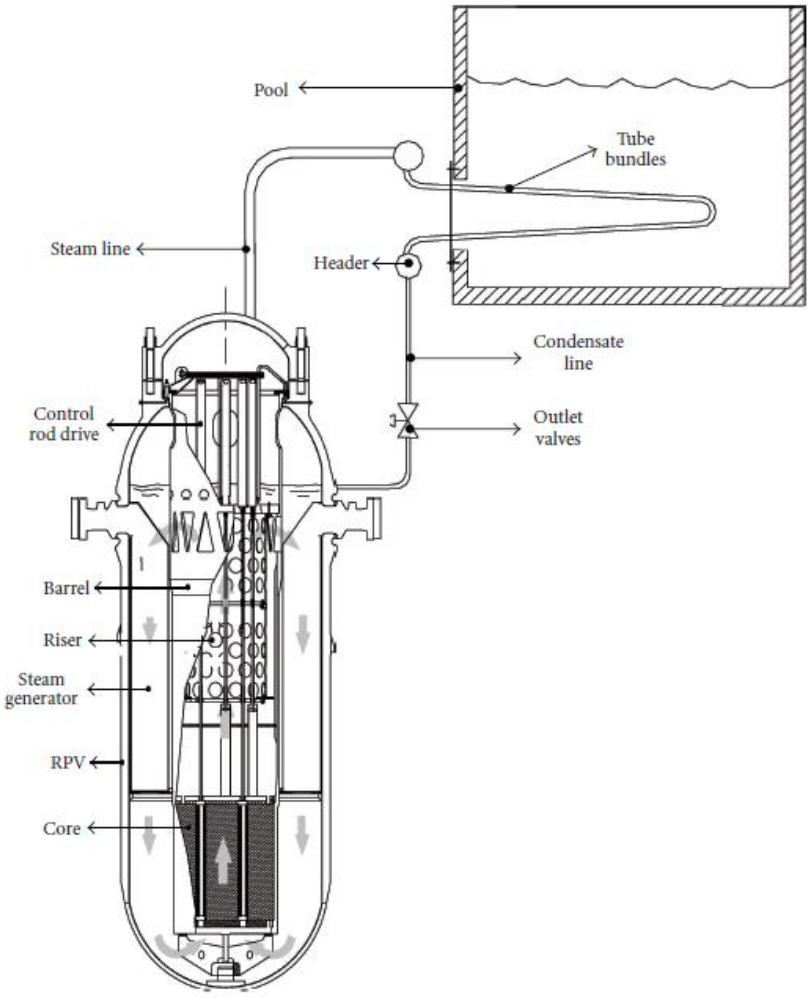

Figure 27 - CAREM-like primary system and isolation condenser [57]

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

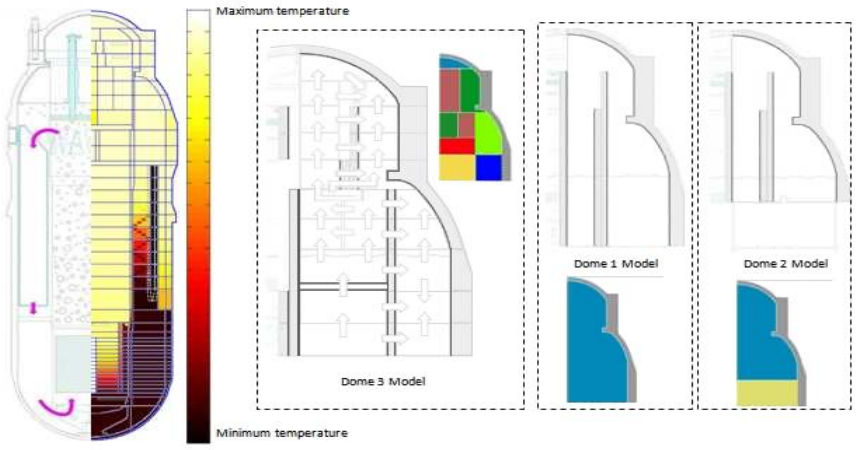

Figure 28 - Different nodalizations for the dome in the primary circuit [1]

Several other applications of the RMPS methodology can be mentioned (non-exhaustive list):

- In a demonstration sodium fast reactor using a reactor cooling system during a station black-out;
- In a 2400 MWth Gas-Cooled Fast Reactor with a decay heat removal system during a loss of coolant accident and a loss of offsite power;
- In the BWRX-300 SMR for the Isolation Condenser System during a reactor trip transient.

2.2.2.4. Relevance for WP4

First, the RMPS methodology has been specifically developed to assess the reliability of PSS, which the SIET test loop experimentally represents.

Second, many partners involved in the WP4 have already used the RMPS (FRAMATOME, ENEA, EDF, GRS, CEA ...) on the overall process, especially on PSS based on two-phase natural convection, like the SIET experimental loop.

Third, the RMPS methodology involves a TH BE code: CATHARE (available for many partners) has already been used to simulate the SIET facility, in the frame of the ELSMOR project [7].

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

2.2.3. APSRA

2.2.3.1. Description

Methodology APSRA (Assessment of Passive System ReliAbility) was proposed by Bhabha Atomic Research Centre, Nayak et al. 2007 [61].

According to the APSRA methodology, the PSS reliability is evaluated from the evaluation of the failure probability of the system to carry out the desired function. It is assumed that deviations of input parameters related to performance of PSSs can be associated solely with malfunctions or failures of mechanical components. Depending on type of PSS, mechanical components can be valves (check, control, pressure relief), rupture discs, control systems, etc. Impact of these deviations on PSS performance is simulated using T-H codes (e.g., RELAP, ATHLET, MELCOR, etc.). As a result of calculations, a failure surface (or failure curve, depending on the scope of analysis) is generated by considering the deviations of all those critical parameters, which influence the system performance. Then root-cause analysis is performed to find the cause of these deviations. Once the causes of these deviations are determined, the failure probabilities of these causes are evaluated. The failure probability of the PSS is then can be calculated by PSA technique used by the NPP PSA (e.g., fault tree method, success trees method, etc.).

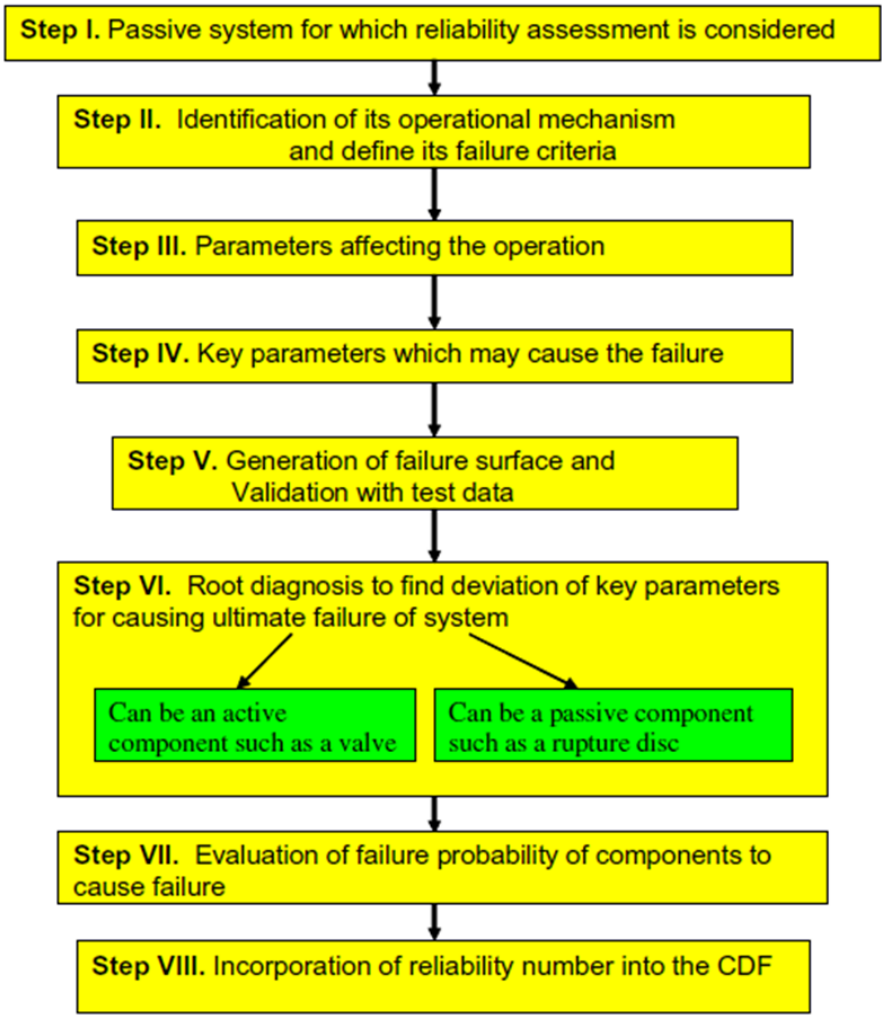

Figure 29 - APSRA workflow, Nayak et al. 2008 [63]

Overall steps of the method are shown at **Figure 29**. The process includes the following steps [1]:

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- **Step I**. Identification of PSS. This step deals with selection of PSS, and definition of the analysis objectives.
- **Step II.** Identification of the parameters affecting the operation. Some operating parameters may have vital impact on a PSS performance. For example, some of the critical operating parameters which influence the natural circulation flow rate in a boiling two-phase natural circulation system are: system pressure; heat addition rate to the coolant; water level in the steam drum; feed water temperature or core inlet sub-cooling; presence of non-condensable gases.
- **Step III.** Operational characteristics and FCs. The analyst must have a clear understanding of how the PSS operates, as well as how it can fail—in other words, a solid grasp of its key characteristics. To assess potential failure, the analyst needs to establish appropriate FCs. These system characteristics can often be simulated (either by T-H codes, or even by engineering calculations to understand the PSS behavior). At this stage, the objective is not to predict behavior with high accuracy, but rather to gain insight into the system's operation. To do this, the analyst (T-H engineer, designer) should utilize the parameters identified in the Step II. Among these, some parameters are critical, meaning that any disturbance in them could significantly impact system performance, while others are less important for successful operation of the PSS according to design objectives.
- **Step IV.** Key parameters which may cause the failure. Taking into account the results from previous step, the analyst should define the critical parameters/values that can meet /exceed the FCs.
- **Step V.** Generation of failure surface and validation with test data. The APSRA envisages that set of T-H calculations should be done prepare the failure surface, see example on **Figure 30**. This allows to demonstrate interrelations and mutual impact of different parameters on the system FCs. BE code such as RELAP5 is required for this step in order to reduce the uncertainty in the prediction of the failure conditions (in contrary with step III, at which simple codes or engineering calculations can be sufficient). To reduce the uncertainty in the predictions, experiments for failure data for different PSSs are essential.
- **Step VI**. Root diagnosis to find deviation of key parameters for causing ultimate failure of the system. After establishing the domain of failure, the next task is to find out the cause of deviation of key parameters which eventually result in the failure of the system. This is done through a root diagnosis method, like failure mode and effect analysis. For example, a reduction in core inlet sub-cooling in natural circulation reactor can be due to reduction of feed water flow rate. This can happen due to: partial availability of the feed pumps; failure of feed control valves or controller; failure of feed water heaters.
- **Step VII.** Evaluation of failure probability of component to cause failure. Failure probabilities for failure modes defined at step VI can be evaluated using the classical PSA approaches on component reliability data treatment (see Section 2.2.5).
- **Step VIII.** Evaluation of system reliability. The component failure probabilities are integrated to evaluate the reliability of the PSS. The PSS failure is modelled by fault tree method. The top event in the fault tree is considered as PSS functional failure (for example, PSS unable to maintain the temperature below certain threshold) and the basic events are malfunctioning or failed component states.

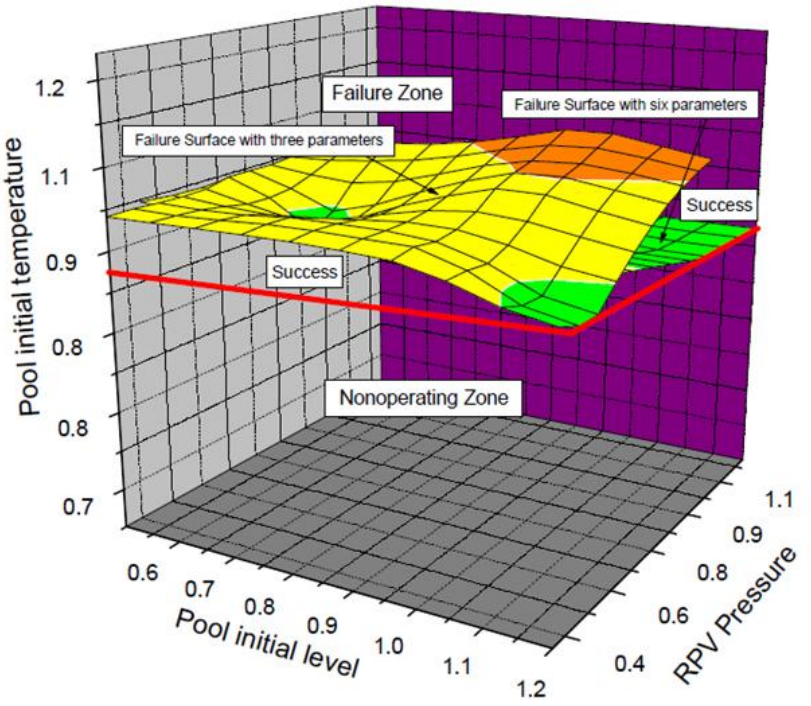

Figure 30 - Failure surface with different critical parameters, from APSRA benchmark in [1]

In the essence, modelling of the PSS is simplified by linking to the modelling of the unreliabilities of the hardware components of the system: this is achieved by identifying the hardware failures that degrade the natural mechanisms upon which the PSS relies and associating the relative unreliabilities of the components designed to assure the best conditions for passive function performance.

2.2.3.2. Advantages and Limitations

In general, APSRA methodology deals with similar domain as REPAS/RMPS methodology. There are, however, several differences between REPAS/RMPS and APSRA, outlined in [1], [24]:

- APSRA includes in the PSA model the failure of those components, which cause a deviation of the key parameters resulting in a system failure, but does not take into account the fact that the probability of failure of a physical process could be different from unity.
- Different treatment of variations of the process parameters from its nominal values. APSRA addresses such variations by focusing on the underlying root diagnosis. For instance, a deviation in pressure from its nominal value might stem from a malfunction in the pressure control system—ultimately a failure of a hardware component. By identifying the true source of the deviations, APSRA offers a more targeted approach to the PSS assessment.
- Different ways for accounting of uncertainties. While REPAS/RMPS treats model uncertainties using probability distribution function (similarly to process parameter variations) and it does not distinguish between the process parameter variations and model uncertainties. On the other hand, APSRA relies on uncertainty estimates of computer codes/models on the basis of experimental validation. As far as the uncertainty associated with the key parameters is concerned, APSRA attributes the variability of key parameters to the functional failure of associated active/PSSs riding on the PSS under consideration. In the absence of experimental data, APSRA treats the model uncertainties

using a PDF and they are propagated separately after evaluating the failure probability of the system through failure of process parameters.

- Different ways for assessment of reliability parameters. APSRA predicts failure surface and evaluates reliability using fault tree analysis, whereas REPAS/RMPS uses Monte Carlo evaluation.

APSRA includes in the PSA model the failure of those components, which cause a deviation of the key parameters resulting in a system failure, but does not take into account the fact that the probability of failure of a physical process could be different from unity.

Although step on evaluation of failure probability of components causing the failure is the most critical step in the safety system reliability evaluation, APSRA does not prescribe any specific methods for that step. It was mentioned that either generic or plant-specific data on component reliability can be used. Bayesian analysis for combination of generic and plant-specific data was not mentioned in APSRA.

2.2.3.3. Applications already available

There are several studies published by the APSRA developers dealing with evaluation of reliability of different PSSs:

- Passive containment isolation system of advanced heavy water reactor [63]. Reliability of the system was assessed taking into account frequencies of initiating event affecting the system functioning. The failure frequencies of the passive containment isolation system are found to be 3,142E-5 1/year and 7,017E-7 1/year for small break LOCA and large break LOCA, respectively. Since frequencies of IEs were already accounted in the system fault trees, double counting of the frequencies during quantification of PSA results (core damage frequency, large release frequency) must be avoided;
- Passive isolation condenser system of advanced heavy water reactor [64]. The failure probability of ICS to maintain the hot shutdown has been calculated and found to be 3,703E-07 1/year. It should be noted, that common cause failures for redundant components are not accounted in the analysis. So, the more precise value of the system failure probability by considering additional types of component failures would be higher, than described in [64];
- Passive decay heat removal system of advanced light water reactor [1]. The analysis shows that the unavailability of decay heat removal system to perform successfully is found to be 3,8E-03 per demand.

2.2.3.4. Relevance for WP4

It can be concluded that APSRA is relevant for WP4, since the method includes parts of traditional PSA techniques widely applied in PSA studies and PSA software. This allows to easily incorporate the results of the PSS analysis into the probabilistic models to calculate PSA risk metrics (CDF, LERF).

2.2.4. ROAAM+

2.2.4.1. Description

- **Domain of applicability:**
  - Integrated deterministic-probabilistic approach in problems where both aleatory and epistemic uncertainties are important for risk assessment including
    - Rare high-consequence hazards (e.g. SAs or failures of PSSs), which may require multi-million model sampling;
    - Problems with limited knowledge about epistemic uncertainty
      - e.g. lack of knowledge on possible distribution of model input parameters.

- **Purpose:**
  - Risk assessment for decision making support
    - Risk acceptability or system modification;
    - Integration with PSA;
    - Identification of main sources of uncertainty, need and means for uncertainty reduction.
  - Integration of risk assessment with PSA;
  - Conservative (necessity of failure) and BE plus uncertainty (probability of failure) analyses;
  - Sensitivity analysis and uncertainty quantification.

- **Theoretical Foundation**
  - Separation of aleatory and epistemic uncertainties
    - Treatment of risk as a triplet $\{s_i, pdf(f_i, P_i(c_i))\}$, i.e. a joint PDF of frequency and probability of consequences associated with a scenario.
  - Data sampling depends on the target application:
    - Qualification of uncertainty in failure probability: second order Montecarlo sampling.
    - Failure domain identification and visualization:
      - Adaptive sampling based on global optimum search for identification;
      - Grid-based sampling with adaptive mesh refinement for visualization.
  - Treatment of intangible parameters:
    - Splintering;
    - Second order uncertainty quantification.

- **Analytical Approach:**
  - Problem statement:
    - Development of the deterministic-probabilistic framework of Causal Relationships (CR) that describes the risk relevant phenomena;
    - Definition of risk relevant FOM, e.g. system “loads” and “capacities”.
  - Collection of data and development of full and SM;
  - Validation of Full Models (FM) and SM;
  - Quantification of FM and SM error distributions (to incorporate in risk analysis);
  - Application of SMs for sensitivity analysis and uncertainty quantification;
  - Forward and reverse analysis for, respectively:

        - Calculation of conditional failure probabilities with user-defined confidence level;
        - Construction of Failure Domains;
    - Framework refinement if needed (iterative approach).

- **Main outcome FOM:**
    - Failure and success domains which in terms of scenario parameters map conditional probability of system failure given a user-desired confidence level.

- **The workflow of the methodology** is illustrated in Figure 30, it includes:
    - Development of the risk-oriented decision framework for system acceptance criteria, i.e. definition of the
        - System modes of failure (system acceptance criteria);
        - Decision making approach to system acceptance or rejection.
    - Grouping and classification of failure scenarios:
        - Separation of aleatory and epistemic input parameters;
        - Identification of the most important model input parameters and their ranges;
        - Scenario classification according to available knowledge on:
            - Initiating events;
            - Equipment failure, operator actions;
            - Phenomenology;
            - PSA fault trees;
            - Etc.
    - Collection of relevant experimental data for model development and validation;
    - Development and validation of an FM using state-of-the-art codes (System code, CFD), physics models, etc.
    - Full model sampling for generation of a database of transient solutions;
    - Definition and quantification of target parameters including timing (analysis of relevant FOM);
    - Development and validation of fast running SM using machine learning methods and the database of FM transient solutions;
    - Sampling of the SM using the top level of ROAAM+ to quantify system failure probability and map failure domains;
    - Based on the results of the analysis, iterative refinement of
        - Input parameters and their ranges;
        - FM and SM;
        - System acceptance criteria,

      until farther refinement
        - does not affect the system acceptance criteria (no new phenomenological failure modes are identified) and the
        - decision on system acceptance/rejection is independent of the remaining modelling uncertainty.
    - Expert review of the modelling approaches and modelling results (not illustrated in the diagram).

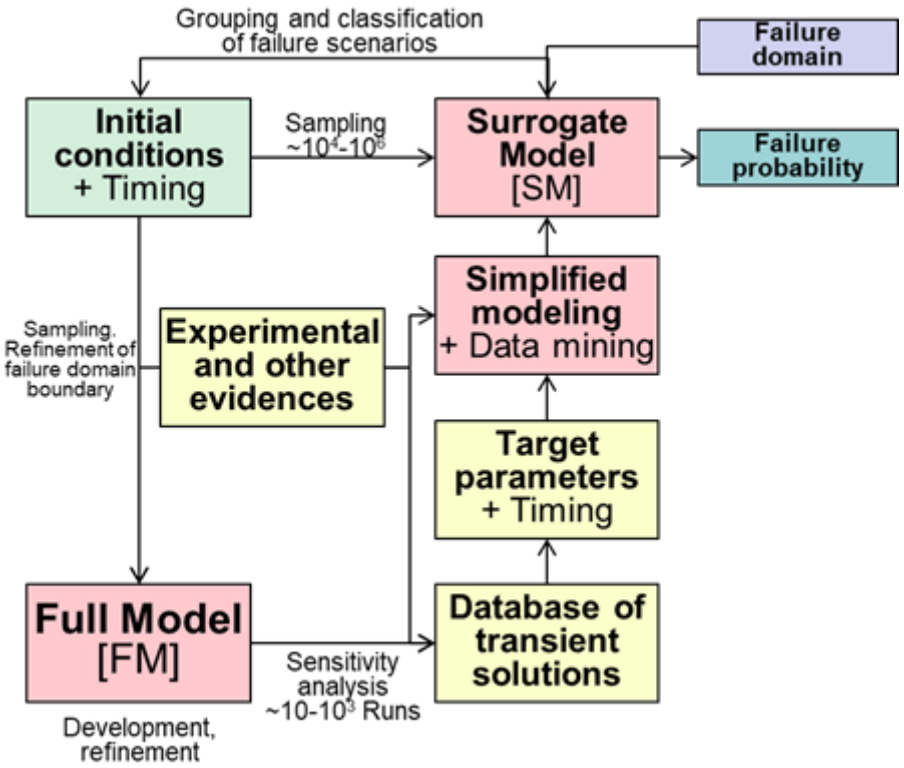

Figure 31 ROAAM+ workflow chart

2.2.4.2. Advantages and Limitations

The ROOAM+ framework is designed to support decision management with the focus on the:

- Detailed quantification of the modelling uncertainty,
- Uncertainty impact on the results of the analysis and system acceptance criteria,
- Transparency of the applied methodology to facilitate expert review of the adopted approaches and the results.

The framework is designed to be user independent. All user assumptions and simplifications are made traceable, and their impact is quantified.

If expert review identifies a potentially missed or omitted phenomena of importance, it is possible using conservative approaches to apply the ROAAM+ framework for the immediate quantification of the expected effect of such phenomena on the modelling uncertainty and final decision. If the decision remains unaffected by the new phenomena no further actions are needed. In the opposite case, FMs have to be revised to incorporate the phenomenon of interest and a new iteration(s) of the ROAAM+ framework has to be carried out.

Depending on the complexity of the FMs and selected FOMs, input space dimensionality, size of the failure domains, the development of representative SMs can range from straightforward and fast to complex and time consuming. Additional challenges may arise if the ROAAM+ top framework incorporates causal relationships (SMs) with multiple mutual feedback loops.

2.2.4.3. Applications already available

The ROAAM+ framework has been successfully applied for the analysis of SA progression in Nordic BWR (see the references [65] - [76] in Section 5). Results of the work have been reported in APRI research framework, published in peer reviewed papers and communicated to Swedish Radiation Safety Authority (SSM).

The framework incorporated coupled models of in-vessel accident progression, vessel wall failure, ablation and melt release into the drywell, ex-vessel steam explosion, ex-vessel debris bed formation including agglomeration, ex-vessel debris bed coolability and self-levelling. The analysis included FOM such as failure of the containment wall, base and hatch-door due to ex-vessel steam explosion, failure and ejection of instrument guide tubes and control rod guide tubes, failure of the cable protective cups on the containment floor. The objective of the analysis was to identify if the adopted SA mitigation strategy is adequate.

Current developments of ROAAM+ aim to incorporate an explicit treatment of time and analysis of radioactive release to the environment under site specific weather conditions.

2.2.4.4. Relevance for WP4

ROAAM+ is a versatile tool, that can be used for PSS reliability analysis. The analysis can be tested against experimental data from HWAT thermal-hydraulic loop following the methodology described in Section 2.

ROAAM+ relevance for PSS:

- ROAAM+ is highly relevant for problems with non-linear, time-dependent behavior, which are sensitive to initial and boundary conditions such as PSSs. Sensitivity analysis and uncertainty quantification are well-suited to capture how deviation from nominal conditions impacts system transient functionality.
- ROAAM+ combination of deterministic and probabilistic analysis is expected to provide a better understanding of the system performance and reliability.
- ROAAM+ application of SMs allows identification of rare failure modes that otherwise can be missed.
- ROAAM+ separate treatment of aleatory and epistemic uncertainties is highly important for PSS reliability analysis. For instance, buoyancy driven flows in most common PSS is highly sensitive to the uncertainty in scenario, code input and model parameters.
- ROAAM+ provides assessment of the safety margins, maps success and failure domains in terms of scenario parameters, relies on the principle of acceptable magnitude of the remaining uncertainty. This supports both system design and licensing.

2.2.5. Generic PSA Approach

2.2.5.1. Description

Conventional PSA methods are based on the principle of associating each physical failure mode with a failure mode of a hardware component designed for establishing and maintaining the conditions necessary for the PSS to perform its function. With these methods, the probabilities of physical failures which degrade the mechanisms upon which the PSS relies are represented in terms of unreliabilities of specific components whose failures challenge the normal functioning of the system.

A general objective of risk assessment is to determine the susceptibility of a system or of groups of systems to conditions of design, operation, test, and maintenance that could lead to failure. This objective can be achieved through system modelling, for which a variety of analytical techniques can be used. To be of greatest value to the overall PSA process, the techniques used in system modelling should have the following characteristics:

- The technique should be capable of predicting the unavailability of complex systems in a manner that can be employed by a variety of practitioners.
- The technique should be proceduralized to the extent that it can be used for a wide variety of systems in a manner that is traceable, repeatable, and verifiable.
- The technique should provide reasonable assurance of completeness.
- The technique should enhance understanding, communication, and the use of results.
- The technique should produce a model that promotes understanding of the principal ways in which the system can fail and the ways in which failures can be prevented, or their impact reduced.

Although no single technique completely satisfies all of these generalized criteria, the fault tree is one of the best available analytical tools for understanding how a system works and might fail, see NUREG-2300 [77].

The actual development of the fault tree (either detailed or simplified) commences after the analyst has gained a thorough understanding of the system, especially how it integrates into the overall accident sequence definition process. More than one fault tree may be required for a system should the system respond to different initiating events with different success criteria. Starting with the top event, the fault tree is developed by deductively determining the cause of the previous fault continually approaching finer resolution until the limit of resolution is reached. In this fashion the fault tree is developed from the system end point backwards to the system failure source. The limit of resolution is reached when the fault tree development below a gate consists only of primary events (i.e., faults which consist of component failures, faults which are not to be further developed, external events, or support system faults which are developed in separate fault trees). For simplified fault trees, the limit of resolution is the dominant failure modes.

A fault tree is a complex of entities known as gates which serve to permit or inhibit the passage of fault logic up the tree. The gates show the logical relationships of events needed for the occurrence of the top event of the fault tree. There are two basic types of fault tree gates: the OR-gate and the AND-gate. All other gates are really special cases of these two basic types [78].

In general, there are five types of basic events to include in the fault tree development are: component (or set of components) failure, test and maintenance unavailability, human error, dependent and subtle failure (including common cause events), and house event. A component failure occurs when the component does not perform its intended function. Component failures can be classified as demand failures or operational failures. Demand failures are failures of a component to respond as needed (e.g., to change state for valve). An operational failure occurs when the component fails to continue to operate for a specified period given it was either normally operating or was successfully started (e.g., to retain the required state for valve).

There are two basic categories of data sources relevant to PSA: plant-specific data; and generic data.

Generic data. Data developed from the following sources are considered under the classification, generic data:

1) the operating experience with similar components at different plants;
2) plant-specific data combined with data for similar components at other plants; and
3) subjective estimates.

Plant-specific data. Component reliability parameters are estimated for each identified failure mode. Calculating classical point estimates and confidence bounds is the first step in developing plant-specific reliability data.

For failure frequencies, the mean point estimate, $\overline{\lambda} = f_T/T$ where f_T is the number of time-related failures and T is the exposure time over which the ft failures occurred.

The lower and upper confidence bounds for the failure rate, λ_{05} and λ^{95} respectively, are:

$$\lambda_{05} = \frac{\chi^2(2f_T,\ 0.05)}{2T}$$

and:

$$\lambda_{95} = \frac{\chi^2(2f_T + 2,\ 0.95)}{2T}$$

The function $\chi^2(v, p)$, is the pth percentile of a χ^2 distribution with v degrees of freedom.

The mean point estimate, $\bar{p}$, for failure on demand probability is:

$$\bar{p} = \frac{f_D}{D}$$

Here:

f_D is the number of demand-related failures (including component random mechanical failures and human errors which cause component failure during test and maintenance without challenges in system configuration); and D is the total number of demands over which the f_D failures occurred.

The lower and upper confidence bounds for the failure probability, p_{05} and p^{95}, respectively, are:

$$p_{05} = \frac{f_D F(2f_D, 2D - 2f_D + 2, 0.05)}{D - f_D + 1 + f_D F(2f_D, 2D - 2f_D + 2, 0.05)}$$

and:

$$p^{95} = \frac{(f_D + 1(F(2f_D + 2, 2D - 2f_D, 0.95)}{D - f_D + (f_D + 1)F(2f_D + 2, 2D - 2f_D, 0,95)}$$

If there were no failures during plant observation time a conservative value of 0.5 typically used for point estimation.

Plant specific parameter estimates are calculated using Bayesian updates where feasible, (see [79]). Bayesian analysis is performed to combine plant-specific data with generic data. The prior failure rate/probability is calculated by the maximum likelihood estimation method. For this the generic failure data should be used. Bayes Theorem in discrete form:

$$P(x_i/E) = \frac{L\left(\frac{E}{x_i}\right)P_0(x_i)}{\sum_{j=1}^{N} L\left(\frac{E}{x_j}\right)P_0(x_j)}$$

Where: P_0 - Prior distribution; P- Posterior distribution; L - Likelihood function; E - Evidence; x_j - Discrete values for x, j = 1, 2, ... N; x - is an arbitrary variable equal to λ when frequencies are being evaluated and equal to p when probabilities are being analysed.

Prior distribution is assumed to be lognormal:

$$P(x) = \frac{1}{\sigma x \sqrt{2\pi}} \exp\left\{-\frac{(\ln(x) - \mu)^2}{2\sigma^2}\right\}$$

The Likelihood Function (i.e., the probability of evidence) given λ for failure rate per unit time is modelled by a Poisson distribution:

$$L(E < K, T > / x) = \frac{(x\,T)^K}{K!} e^{-xT}$$

The Likelihood Function (i.e., the probability of evidence) given p for failure probability per demand is modelled by a Binomial distribution:

$$L(E < K, N > / x) = \left(\frac{N}{K}\right) x^N (1 - x)^{N-K}$$

Thus, reliability of PSS components (both active components like valves and passive components like pipes) can be calculated taking into account operational experience (OPEX).

Reliability analysis of passive components (like pipelines, tanks) based solely on the analysis of actual failure data (e.g., pipe breaks or ruptures) has inherent limitations. Methodologies for reliability analysis for such components as piping should be broadened by incorporating consideration of root cause analysis, probabilistic fracture mechanics, aging considerations and deeper analysis of the available operating experience. Several methods can be applied for pipelines:

- Data driven methodology (DDM). DDM implies that a model of piping reliability as much as possible builds on technical insights obtained from detailed evaluations of operational experience data on piping material degradation and failure. Equations are similar to those

stated above. In the DDM approach the treatment of uncertainties is accomplished by using Bayesian techniques and Monte Carlo simulation;

- Probabilistic fracture mechanics methodology (PFM). It quantifies the conditions under which a load-bearing structure can fail due to the enlargement of a pre-existing dominant crack. The crack can be embedded within the pressure boundary component or be surface connected, for example, to an inside pipe wall. The key ingredients in deterministic fracture mechanics analysis are the initial crack size, crack driving force solution (i.e. stress intensity factors for linear elastic fracture mechanics analysis problems), applied stresses, and material properties describing the subcritical crack growth characteristics and conditions for final crack instability. PFM is fracture mechanics that considers some or all of the inputs to be random variables (e.g. the initial crack size). The principal application of PFM in the nuclear industry continues to be in the area of primary system piping integrity and reactor pressure vessel integrity analysis;
- Integrated physics-of-failure methodology (I-PoF). In the methodology, an integrated model of piping reliability is built with an explicit consideration of the physics-of-failure of material degradation from initiation to propagation, and reliability and integrity management processes to detect and repair a pipe flaw and leak before developing into a significant structural mode of failure.

Irrespective of the chosen method (DDM, PFM, I-PoF), a piping reliability analysis includes the following common elements:

- Statistical analysis of experimental data and/or OPEX data on crack initiation and propagation.
- Propagation of uncertainty distributions through a model of piping reliability.
- Evaluation of the effect of different reliability and integrity management strategies on the structural integrity of a piping pressure boundary.
- Specialization of piping reliability analysis results to account for plant specific application requirements. For example, determining the frequency of failure as a function of a certain through-wall flow rates or ranges of flow rates.

Document [80] deals with the aspects and methodologies above. Specifically, it provides state of the art information regarding piping reliability methodologies and their implementation; technical insights into piping reliability analysis tools and techniques for advanced water cooled reactors; approaches on how to modify an existing set of piping reliability parameters originally developed for operating water cooled reactors has to be made applicable to advanced water cooled reactors; methodology for ageing factor assessment that utilizes the existing data from operational experience.

3. Critical analyses and comparison of the methodology

This section, dedicated to the critical analysis and comparison of the methodologies, has been primarily prepared by authors who were not directly involved in their application and description. This approach allows the identification of strengths and weaknesses from the perspective of an external observer, providing an unbiased assessment of the methodologies under review.

3.1. Introduction

The events that challenge system performance can be basically classified into two categories:

- **Anticipated events:**
  - Internal events dealing with equipment malfunctioning (e.g. valve fails to open, seal leakage, etc.);
  - External events that lead to exceeding the limiting conditions foreseen in the design—namely, design conditions (e.g. peak ground acceleration exceeding the design value leading to structural failure, very high ambient temperature, etc.).

    Both types of events are random in nature and thereby linked to aleatory uncertainty.
- **Unanticipated events:** events not considered in the design.
  - Either because they are deemed preposterous, hence willingly screened out—e.g. meteorite fall;
  - Because their occurrence is beyond the state-of-the-art, hence the system behaviour departs from the expected one.

    Willingly screened-out scenarios are not of interest here (as they are dependent on the type of approach to safety analysis) while the second type of unanticipated events relate to a lack of knowledge, namely the wrong belief that the system will perform according to the expectations while it deviates from the expected performance. This second type of unanticipated events is related to epistemic uncertainty.

As for the first category, internal type of events, the PSSs resilience is expected and claimed to be higher compared to active systems due to a lower dependence on support systems (linked to the category of the PSS), consistent with a lower degree of equipment dependence (both in number of equipment and complexity). On the contrary, PSSs show a higher dependency on external type of anticipated events due to their higher sensitivity to the scenario boundary conditions. For instance, a higher non-condensable gas fraction in the containment might lead to a significant degradation of PSS performance while not being the case for containment systems provided with active cooling and air pumps.

The high sensitivity to the scenario boundary conditions, imposed by the challenging scenario, has its counterpart in an equal high sensitivity of the system performance to the system-specific

boundary conditions[8], namely the set of constraints that limit the solution space to a finite number of solutions, e.g. heat transfer coefficient, head loss coefficient, relative elevation, etc, but also geometry and layout. Performance deviations related to system-specific boundary conditions departing from the expectations refer to the second category of challenging events. PSSs are more sensitive to this type of challenging scenarios as their performance is more sensitive to system-specific boundary conditions compared to active systems. Such high sensitivity requires accurate account of all the highly sensitive sources affecting PSS performance:

- If reliability demonstration that the system fulfils its intended performance is carried out analytically, then validated analytical models are needed;
- If reliability demonstration that the system fulfils its intended performance is carried out experimentally, fine tuning of the experimental test conditions representing a faithful characterization of the system is required.

The higher sensitivity of PSSs to the scenario boundary conditions and system-specific boundary conditions related to anticipated external events and unanticipated events respectively requires careful addressing of aleatory uncertainty and epistemic uncertainty respectively and constitutes the main challenges in PSSs reliability assessment.

As it will be further elaborated in this section, there are two possible (both applicable for the same PSS) ways to tackle this challenge:

- Reliability is demonstrated via experiments
  - As for the scenario boundary conditions, the essential point is to ensure that the test campaign covers the challenging events specific to the PSS behaviour;
  - As for the system-specific boundary conditions, the essential point is to ensure that the PSS is a perfect twin of that installed in the actual facility, so that the system-specific boundary conditions, e.g. head losses, elevations, etc., are the same.
- Reliability is demonstrated via analytical simulations
  - As for the scenario boundary conditions, the essential point is to ensure that the challenging scenarios are covered by the set of simulations, which should not be cumbersome in view of the current computational capabilities able to run a large number of simulations in a relative short time. Given the dependency on the scenario boundary conditions, reasonable variation of the scenario parameters should be imposed as uncertainty;
  - As for the system-specific boundary conditions, the essential point is to ensure that the actual values of all the sources of uncertainty—corresponding to the system-specific boundary conditions—are captured within the postulated numerical ranges

[8] In the present context, *system-specific boundary conditions* refer to a set of fixed, plant-specific physical parameters and constraints that define the intrinsic configuration of the system and close the governing equations to a finite set of physically consistent solutions. They differ from conventional scenario-dependent boundary conditions, as they are inherent to the system's geometry, layout, and closure laws, and remain constant during normal operation.
Typical examples include:

- Heat transfer coefficients and head loss coefficients, as determined by closure correlations;
- Geometric constraints such as relative elevations and piping arrangements;
- Fixed component characteristics such as valve discharge areas or heat exchanger configurations.

While these parameters are not subject to active degradation, deviations from their expected values — due to manufacturing tolerances, installation differences, fouling, scaling effects, or unaccounted-for physical phenomena — can significantly alter system performance.
For PSSs, such deviations can narrow safety margins and lead to *functional (phenomenological) failure* even when all hardware remains intact, making their accurate characterization and uncertainty quantification essential.

integrated into the analytical models and the corresponding uncertainty adequately propagated in the simulations[9,10].

It should be noted that, considering the current state of practice, the key tools used to develop simulations need validation against experimental data. Therefore, a mixed approach is necessary, combining both experimental evidence and analytical modelling to ensure reliability.

3.2. Key Findings from the Methodology Comparison

Before making a critical review and comparison of the four methodologies at stake, it is important to clear up key terminology and to frame the context applicable to reliability engineering.

3.2.1. Definition and Approaches to Reliability Engineering

Reliability is the ability of systems, components, and processes to perform their intended function as defined in the Technical Specifications over their expected life without failure. Within the current report, by 'reliability' it is also meant the evidence provided for safety demonstration of the reliability of a Structure, System or Component (SSC), namely that the SSC performs according to the expectations (in terms of the safety function, performance criteria during a specific time window).

Reliability can be approached primarily in two ways:

Deterministic Approach:

In this § the deterministic approach is not a part of the deterministic safety demonstration but an approach usable in probabilistic domain when the most penalizing combination of parameters and the worst scenario can be identified. Usually, this approach can be used for a simple PSS.

- The goal is to make sure that the analysed SSC performs according to the expectations before a set of postulated challenging scenarios;
- The result is qualitative and binary: pass / not-pass for evaluation of probability of functional failure;
- Uses worst-case accident scenarios (bounding cases);
- Applies safety margins, e.g., doubling stress loads in Category I—i.e. more frequent—events;

Probabilistic (Risk-Informed) Approach:

In the Probabilistic (Risk-Informed) Approach:

- The goal is to quantify the contribution to risk brought by the analysed SSC;
- The result is quantitative and continuous, e.g. failure probability;

[9] Furthermore, if reliability assessment is done via probabilistic approach, uncertainty quantification—aside from identification—is required.

[10] Note that epistemic uncertainty is not limited to the modelling parameters as the system itself is a source of uncertainty. Depending on the path followed for the uncertainty analysis, the uncertainty related to the model might be addressed fully via the uncertainty assigned to the model parameters.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- Reliability is validated against risk-driven scenarios, e.g. resulting mainly from PSA but it can be also FMEA application;
- Safety margins do not apply (in conventional equipment, not FOAK; recommended for PSSs due to significant model uncertainties, as developed later on in the current section);
- Scenarios taken for the reliability quantification must be assigned with their frequency of occurrence.

Some methodologies claim the combination of the two approaches, but such combination is limited to summing up the independent variation of boundary and initial conditions for the accident sequence identification via random application, with an extra list of accidents postulated via expert judgement. But deterministic and probabilistic approaches differ in additional key aspects of system reliability, such as different success criteria, uncertainty treatment and system decomposition.

3.2.2. Reliability Demonstration

Reliability can be demonstrated by analytical and experimental methods.

3.2.2.1. Reliability Demonstration by Analytical Methods

Analytical Methods: e.g., stress-strain analysis, T-H modelling, finite element simulations. Analytical methods rely on phenomenological models featuring epistemic uncertainties. Uncertainty may come from the model parameters but also from the model itself. If analytical methods for reliability demonstration apply, the validation of the computational tools is a key element also to assess the uncertainty in the parameter values predicted by the code. Outputs of the code should be compared with relevant experimental data and, if possible, with data from operational transients (if available) representing the important phenomena expected to occur **[IAEA SSG-2 (Rev. 1)[87]].**

On one hand, if safety assessment is deterministic and reliability demonstration is carried out via analytical methods, there is no need of quantifying uncertainty, but just to ensure that the entire spectrum of possible results stemming from the variation of uncertainty sources has been computed. On the other hand, if it includes the probabilistic related to the range of values that can be taken by the parameters affecting the operation of the PSSs, then PDFs must be properly assigned.

If reliability is carried out via deterministic approach and demonstrated via analytical methods, there is no need for an extensive and highly accurate identification process on the key parameters leading to system functional deviation or failure: it suffices to run the entire list of accident scenarios as previously identified, e.g. within Final Safety Analysis Report (FSAR) Chapter XV, ensuring that the worst-case scenarios at overall reactor system level comprise the most challenging scenarios specific of the PSS. On the contrary, the significant degree of uncertainty featured by the current models representing PSSs performance needs conservative assignment of uncertainty ranges on the system-specific boundary condition parameters or on the model results.

If the reliability calculation is carried out via probabilistic approach and demonstrated via analytical methods, uncertainty needs to be also quantified as accurate as possible.

3.2.2.2. Reliability Demonstration by Experimental Methods

Experimental Methods: testing under representative (bounding or risk-informed) environments to characterize the operation/performance of the system and validate the T-H model representative of the physical phenomena used for PSS simulation. The tests must replicate the challenging accident conditions previously identified in the applied approach (i.e. bounding for deterministic; risk-significant for probabilistic). The main caveat here is to ensure that the whole spectrum of challenging scenarios is captured by the experimental campaign.

Experimental demonstration of reliability avoids the need for accurate uncertainty identification and assignment, although it requires extensive tests to ensure that the entire spectrum of challenging conditions has been considered. For that, previous detailed identification of key parameters is necessary. Furthermore, the experimental system shall accurately reflect the highly-sensitive system-specific boundary conditions of the real system installed in the actual facility.

3.2.2.3. Benefit and shortcomings

Each approach for reliability demonstration has its benefits and shortcomings:

- **Analytical methods** can easily cope with a huge number of simulations, which makes the scenario boundary conditions issue well addressed. Additional safety margins on the applied load conditions, i.e. scenario boundary conditions, by each accident scenario, e.g. increased rejected power, increased heat losses, etc., should apply as aleatory uncertainty sources. However, analytical methods may struggle with a correct and comprehensive uncertainty identification and assignment, hence the system-specific boundary conditions issue being more difficult to tackle.
- **Experimental methods** can have practical limitations in case the list of challenging scenarios is large, i.e. hence difficult to cope with scenario boundary conditions, while the system-specific boundary conditions should not be difficult to cope provided the tested system is a twin of the real system.

As said in previous section, **in practice, a mixed approach is generally adopted**. Given that a large number of experiments is unfeasible, a limited set of representative tests is performed to characterise the system and gain an initial insight into its performance. The resulting data are then used to validate the computational tools, which in turn enable a more exhaustive evaluation by covering the full spectrum of possible operating and accident conditions. Therefore, analytical methods make it possible to address the exhaustiveness of the scenarios to be considered, while experimental tests increase knowledge of system behaviour for a selected set of scenarios.

3.2.3. Reliability Assignment: Generic Versus Dedicated

Generic Reliability Assignment:

- **Basis:** uses historical data and statistical analysis of a broader family of similar components or systems;
- **Treatment:** random type of failure;
- **Advantage:** useful when large databases exist, and the behavior is well understood statistically;

- **Limitation:** may not capture the specific behavior of the analyzed SSC, e.g. higher maintenance frequency, higher quality of a component, more extreme environmental conditions, etc.

Dedicated/Specific Reliability Assignment

- **Basis:** focuses on the unique characteristics of the system under investigation;
- **Treatment:** mechanistic type of failure for the system function performance; if the system is broken down, random for real components of the system;
- **Advantage:** higher fidelity to the actual SSC reliability;
- **Limitation:** requires robust experimental data and validated models.

The lack of an extensive operational experience and the limited experimental database for PSSs makes **dedicated reliability** the only current viable option.

3.2.4. Systemic Analysis for PSS Reliability

As for any engineering system, PSSs are made up of several components so that its performance can be broken down at component level, unveiling the logical structure of the system performance.

Failures of physical components that can hardly be further broken down, e.g. relays, switches, etc., should be treated as random in nature and a general reliability assignment, i.e. statistical, applied. Component failures belong to *practical randomness*, namely phenomena that appear random due to limitations in our measurement capabilities, computational power, or understanding, but are theoretically deterministic if we could observe and model all variables. On the other hand, *fundamental randomness* stands for truly unpredictable phenomena due to inherent non-linear behaviours and chaotic dynamics. In this case, even with perfect knowledge of initial conditions and governing equations, these systems remain fundamentally unpredictable beyond certain time horizons.

For probabilistic approaches to system reliability, breaking down PSS into components is appropriate whenever the applicable scenario has to consider additional failures related to specific—real—equipment performance, e.g. rupture disk.

For deterministic approaches to system reliability, the performance of the components belonging to the PSS is postulated following deterministic design safety principles, without the need of assigning failure frequencies to each system component.

3.2.5. Fundamental Differences between Active and PSS Reliability Analysis

There are two key differences between **reliability of active systems against PSSs**, due to the fact that PSS operation relies primarily on gravity-driven phenomena (driven by weak forces):

- **System Survivability Dependency:**

  This is the ability of a system to perform as expected for a spectrum of different boundary conditions specific to a challenging scenario. Active systems feature low survivability dependency, while PSSs dependency is very high. For active systems, survivability dependency is only high in case of extreme environmental conditions, such as those typical of SAs.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- **Demonstration Robustness**:

  Reliability demonstration can either be conducted via analytical or experimental methods. Active systems feature extensive experimental databases and solid T-H models, while PSSs have currently a limited experimental database to characterise the full spectrum of conditions that may occur during scenarios and, therefore, to assess functional failure. This limitation makes it necessary to complement the available experiments with analytical methods to overcome existing knowledge gaps.

These two differences must be specifically addressed when performing reliability analysis of PSSs, e.g. among others, by means of the following approaches:

- Ensuring that the list of accident scenarios testing the PSS performance is comprehensive. Such comprehensiveness makes reliability demonstration hardly compatible with experimental methods. Furthermore, with today's advanced computational capabilities, addressing a large number of scenarios is much easier than it was a decade ago. It should be noted that computational tools can only be used if they are validated against representative experimental data. Therefore, a minimum number of representative experiments is necessary and cannot be avoided, both to assess PSS operation/performance and to validate the computational tools to be used[11].
- Applying conservative safety margins to the applicable load conditions characterizing each accident scenario, together with credible variation ranges for the uncertainty parameters, in order to account for the limitations of the model as an artificial representation of the physical phenomena.

3.2.6. RMPS and REPAS Methodologies

REPAS and RMPS methodologies share a nearly identical methodological structure and set of assumptions. Further, both aim to evaluate the functional reliability of T-H PSSs through BE system codes, supported by uncertainty quantification and similar probabilistic treatment of input parameters (both so-called design and critical parameters, equivalent to system boundary conditions and system-specific boundary conditions, putting them together under a similar treatment). However, the existing applications for RMPS [88] have more focused on probabilistic

[11] This is consistent with **#4.16** of IAEA SSR-2/1 (Rev. 1) [12] underlined in section 1.6.1.1 and **Section 5 of IAEA SSG-2 (Rev. 1) [87].** In particular, attention is drawn to:

- **5.26: Validation against test data is the primary means of validation**. However, in cases where no means to achieve appropriate data for validation are available for test cases of the types in para. 5.25(b)–(d), it is possible to enhance confidence in the results by means of code to code comparisons or using bounding engineering judgement to compensate for limitations in the full validation. The approach taken to validation and the use of the code should be justified.
- **5.27. The validation should ideally cover the full range of values** of parameters, conditions and physical processes that the computer code is intended to model, in the specific applications for which it is to be used.
- **5.30. The validation matrix should include test data from different experimental facilities and from different sets of conditions in the same facility**, and should ideally include basic tests, separate effect tests, integral effect tests and nuclear power plant level tests. The models and associated assumptions chosen at each level of validation should be consistent with one another and should not be different for different types of tests. If sufficient data from full scale experiments are not available, data from reduced scale experiments should be used, with appropriate consideration of scaling effects. The number and the selection of tests in the validation matrix should be justified as being sufficient for the intended application(s) of the computer code.
- **5.31. To ensure that the computer code is validated for conditions that are as close as possible to those in a nuclear power plant, it should be ensured that the boundary conditions and initial conditions for each test are appropriate**. If data relating to other conditions are used, consideration should be given to scaling effects. A scaled experimental facility cannot be used to represent all of the phenomena that are relevant for a full-size facility. Thus, for each scaled facility that is used in the validation process, the phenomena that are correctly represented and those that are not correctly represented should be identified. The effects of phenomena that are not properly represented should be addressed in other ways, taking into account the applicable level of conservatism.

approaches to system reliability, while that is not the case for REPAS that however represent the backbone of these two methodologies[12].

Given their common analytical workflow, including the use of Monte Carlo techniques, the probabilistic treatment of both design and model parameters, and similar approaches to defining FCs, RMPS and REPAS are treated together in this subsection. Notwithstanding with the above, key differences found within their different applications will also be underlined when applicable. Their conceptual foundation, strengths, and limitations largely overlap, and any subtle differences are more related to the Institutions that apply the methodology, or to the specific application context, than to the methodological substance. Therefore, a single analysis for the two methodologies allows for a clearer and more concise discussion of their role in PSS reliability assessment.

The main similarities and weak points featured by both methodologies follow:

Failure criteria:

- In some of the applications found in the literature, there maybe a not clear distinction between reliability analyses through deterministic and probabilistic (risk-related) approaches and are clarified hereafter:
    - If deterministic, FC are not quantitative but rather qualitative and binary: either the SSC meets or does not meet with the expected mission during a certain time (unless specifying a certain acceptance confidence when incorporating the model uncertainty). However, deterministic reliability might also accept a certain confidence threshold of, e.g. 95%, meaning that 95% of the scenarios demonstrate the pursued reliability according to the expectations.
    - If probabilistic, FC have to be computed as the probability of failure conditional to a specific accident scenario (in turn associated to a certain frequency of occurrence).
    - If probabilistic, a deterministic logical structure at subsystem level must first be developed, e.g. FTA. However, it is not strictly necessary to develop a highly detailed, fully broken down structure as long as the set of challenging sequences is comprehensive and the real components belonging to the PSS are identified.
    - Deterministic approaches only need to test the system (either via analytical methods or experiments) against bounding scenarios, i.e. worst-case scenarios, selected and defined via application of deterministic safety principles.
    - Given that deterministic approaches do not need to quantify the risk but to provide demonstration that the SSC behaves according to the expectation.

Aleatory and Epistemic Elements:

Both methods, in their application cases, sometimes lack a clear distinction between aleatory causes of failure and epistemic factors (e.g. REPAS samples the parameters that affect the operation/performance of the PSSs):

[12] A pioneering activity aimed at the evaluation of the reliability of PSSs was proposed in the mid-1990s within the framework of bilateral contacts between CEA and ENEA. Later, a work carried out by ENEA, University of Pisa and Polytechnic of Milan, led to the development of a procedure called REPAS, which help evaluate the reliability of natural circulation system under specific conditions. To assess the impact of uncertainties on the predicted performance of the PSSs, a large number of calculations with BE T-H codes are needed. If all the sequences where the PSS studied is involved are considered, the number of calculations can be prohibitive. For all these reasons, it appeared necessary to create a specific methodology to assess the reliability of PSS B or C (i.e. implementing moving working fluid, following the IAEA (1991) classification, and in particular to the PSSs that utilize natural circulation). The methodology has been developed within the framework of a project called Reliability Methods for Passive Safety Functions (RMPS), performed under the auspices of the European 5th Framework Programme [1] **[43] [44]**.

- On one hand, the scenario boundary conditions do not have to have an assigned probability for each specific condition, e.g. reactor water level, but an assigned probability to the scenario as such, since they represent a set of interrelated variables specific of one particular challenging scenario. This scenario is made up of a set of conditions stemming from a set of physical events, where each of them can be traced back to a specific, "material" failure, e.g. valve failed to fully open, pipe break, heat exchanger partly blocked, etc. This aleatory occurrence of the set of events constituting the challenging scenario, namely scenario boundary conditions, has therefore mechanistic / deterministic causes and its treatment cannot therefore be equal to the one assigned to system-specific boundary conditions.
- On the other hand, in fact, system-specific boundary conditions fall under the domain of epistemic uncertainties and hence are subject to probabilistic treatment, each of the conditions separately.

A detailed analysis of scenario boundary conditions and system-specific boundary conditions is necessary to be performed to select what parameters must be considered in REPAS/RMPS for uncertainty propagation. This ensures a physical credibility of the assessment.

Selection of Relevant Scenarios / Assignment of Dominant Parameters (i.e. scenario boundary conditions):

Some of the existing applications[13] found in the literature deal with design parameters (i.e. scenario boundary conditions) representing accident conditions (such as water level, pressure, or temperature) statistically (by assigning them independent, probability distribution functions, one by one individually) without preserving their physical interdependencies, so that each parameter or condition is treated independently.

To avoid this situation the following recommendation is given:

- Accident scenarios should be scenario-based "blocks", i.e. set of coupled initial and boundary conditions, and not a list of decoupled parameters, each of which with an assigned probability treated as a source of uncertainty;
- If probabilistic approach for reliability engineering is taken, then each of these blocks should be assigned the same frequency of occurrence (no need for such assignment in deterministic approaches);
- Worst-case scenarios should directly be drawn from deterministic safety principles, whereas the same applied for probabilistic, risk-related approaches to system reliability, developing the accident progression drawn from PRA principles with further scenario decomposition via application to the PSS components;
- A detailed analysis of scenario boundary conditions and system-specific boundary conditions must be performed to select what parameters must be considered in REPAS/RMPS for uncertainty propagation.

[13] Here we can mention the presentation done by Framatome: Evaluation of the functional reliability of PSSs using RMPS, Pierre Gaillard, Yolanda Rugama, Laurent Lefebvre, Mathieu Segond, Etienne Courtin. This presentation describes the work done to gather different scenarios, to select the relevant scenario for functional reliability evaluation and to implement in PSA the same value for all the scenarios of the group. It is to note that in case of a too large number of scenarios and configuration involving the PSS leading to a too cumbersome or unrealistic workload, it is necessary to gather them based on preliminary PSA analysis and T-H calculation and to select the relevant scenarios for functional reliability evaluation by RMPS/REPAS.

Epistemic Uncertainty Handling / Assignment of Critical Parameters (i.e. system-specific boundary conditions):

In relation to Epistemic Uncertainty Handling and Assignment of Critical Parameters:

- RMPS and REPAS can also quantify the uncertainty (epistemic) in the models by assigning PDFs to the model parameters. However, without a comprehensive validation against experimental data or full consideration of the model uncertainty itself, uncertainty quantification remains a challenge. Therefore, in the step of identifying relevant parameters and quantifying uncertainties, it is necessary to assess whether the current level of knowledge is sufficient, and, if not, to perform the necessary studies and experimental tests to reach this level;
- Model uncertainty is usually missing (not only in RMPS and REPAS, but to any uncertainty quantification method applied to PSS);
- Accident scenario boundary conditions are treated as uncertainty sources, with a PDF and range assigned independently to each parameter.

3.2.7.APSRA Methodology

The main comments about the APSRA methodology follow:

- APSRA is a methodology developed to quantify the reliability of T-H PSSs, particularly within a PSA context. The method is intended to address the epistemic uncertainty in system modelling while preserving a separation from aleatory variability;
- APSRA fits well with probabilistic approaches to system reliability;
- APSRA correctly distinguishes between uncertainties stemming from lack of knowledge (epistemic) and variability in accident scenarios (aleatory), in other words, it maintains clear separation between accident scenario variability and model uncertainty;
- APSRA is complex in some steps, e.g. the development of the failure surface is complex, especially when accident scenarios should be derived from deterministic or PRA principles—depending on the applicable approach;
- Furthermore, the failure surface might lead to scenarios characterised by questionable combinations of variables falling into the failure region;
- APSRA incorporates a metamodel-based representation of the system's response. Due to the current computational capabilities, such metamodel might not be necessary anymore (emphasizing the fact that any metamodel introduces new sources of uncertainty);
- Lack of extensive literature, and the available literature usually misses key steps such as uncertainty quantification and implementation dealing with model analysis vs experiments; good at least in not mixing up accident variability with model uncertainty;
- The original methodology includes the following key steps:
    - Identification of key system performance indicators and failure criteria;
    - Quantification of input parameter uncertainties;
    - Construction of metamodels to approximate system behaviour;
    - Development of a failure surface that separates success and failure regions in parameter space;
    - Monte Carlo simulations to estimate the probability of crossing the failure surface.

3.2.8.ROAAM+ Methodology

The main comments about the ROAAM+ methodology follow:

- ROAAM+ is a structured framework previously applied for the assessment of SA phenomena, including core degradation, lower vessel failure and melt release, steam explosion, debris bed formation and coolability, containment failure;
- The framework is phenomena agnostic and can be applied to any problem, including PSS reliability analysis;
- ROAAM+ provides a hierarchical and probabilistic structure for separate treatment of
  - Epistemic uncertainty in phenomenological modelling;
  - Aleatory uncertainty in scenario frequency.
- ROOAM+ is based on second order probability assessment vis so called intangible parameters. The methodology allows assessment of the effect of the uncertainty in the input parameters distribution on the safety evaluation.
- The framework emphasizes:
  - Transparency of the analysis via expert review of the results, made assumptions and modelling approaches;
  - Scenario-based integration.
- ROAAM+ supports integration into other probabilistic frameworks and was successfully applied for Level-2 PSA; current work is extending ROOAM+ application to Level-3 PSA.
- ROAAM+ is built on the premise of organizing and quantifying uncertainties through structured expert elicitation, scenario development, and probabilistic integration. Its application is grounded in phenomenological analysis and risk-informed decision making.
- The methodology includes the following key steps:
  - Identification of critical phenomena and scenario structure;
  - Sensitivity analysis for screening of unimportant model input parameters;
  - Causal modelling of system behaviour using full models and fast running surrogate models;
  - Expert elicitation of uncertain parameters and boundary conditions;
  - Quantification of failure probability distribution, evaluation of the necessity and possibility of system failure, confidence levels;
  - Integration through probabilistic logic and scenario weighting.
- No published applications to PSS reliability.

3.3. Selected Methodologies and Justifications

In line with the findings in Section 3.1, the reliability of PSSs in nuclear installations can be assessed following two logically distinct approaches: a **deterministic approach** and a **probabilistic (risk-informed) approach**. These approaches serve different purposes and are grounded in different regulatory frameworks.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

3.4. Elements to be considered for reliability assessment

Reliability stands for the evidence provided for safety demonstration of the component performing according to the expectations (in terms of the safety function, performance criteria during a specific time window). Reliability can be assessed either via deterministic or probabilistic approaches. Deterministic and probabilistic approaches for reliability demonstration lie on a common ground (system and function definitions, relevant parameters identification, validated modelling, and sensitivity analysis Choosing one method or the other depends on multiple reasons, the most important being the sort of regulatory framework and PSSs considered.

Some of the challenges of assessing functional reliability of the PSSs are the uncertainty surrounding the full range of operational scenarios that a PSS may experience, and the physical conditions that can affect the operation of the system. Combination of a large number of relevant parameters can lead to difficulties in identifying rare failure cases. Furthermore, the validation of the theoretical model if reliability is demonstrated via analytical methods is also essential and should include comparison against experimental tests and feedback available from plant in operation. Before evaluating functional reliability, it is necessary to define reliability target of the system for the relevant scenarios by a preliminary PSA taking into account all the component involved in the scenario: initiating event frequency, expected reliability of active systems preceding and succeeding PSS in the PSA sequence, and the reliability of PSS active components if any, in order to limit the CDF below an acceptable value.

The key elements to be considered for reliability assessment are considered in the following subsection.

3.4.1. Scenarios selection

The selection of scenarios for reliability demonstration is a key element, and the deterministic and probabilistic approaches are discussed here:

- For **deterministic approaches,** the identification of a comprehensive list of sequences for reliability demonstration might be cumbersome, as worst-case scenarios at overall reactor system level might be different compared to worst-case scenarios at PSSs level. This is why an additional step applies consisting of identifying the key environmental variables—i.e. initial and boundary conditions imposed on the PSS under analysis—affecting the PSS performance, and a subsequent step drawing a **relationship between credible, worst-case sequences and the list of key variables.**
- For **probabilistic approaches,** accident sequences come from PRA application coupled with further decomposition at PSS level. Therefore, system decomposition and corresponding expansion of the accident sequences is an additional step for probabilistic approaches to system reliability.

3.4.2. Operational parameters that affect the operation of the PSS

The identification of the parameters driving the PSS performance is critical of **deterministic approaches to system reliability**. Such identification is necessary to ensure that the list of sequences is comprehensive, i.e. that the **worst-case scenarios for the overall reactor system**

include the most challenging scenarios for the PSS. This identification should be carried out supported by experimental testing, model validation and expert judgement. The identification of critical parameters is not relevant for probabilistic approaches, as PRA already considers all the possible, credible sequences independently on whether it is challenging for a specific system or not. Nevertheless, as already mentioned above, further extension and coupling of the accident sequences by considering additional failures coming from the PSSs components is necessary here.

3.4.3. FCs selection

System reliability does not look at the reactor system as a whole—where safety function applies—but only at the system as designed. Therefore, **FCs should be directly linked to the system performance and not only related to a higher level of performance**, e.g. reactor level and overall safety function.

3.4.4. Application of safety margins

Safety margins are applied for deterministic approaches based on the scenario category, inversely to the scenario frequency of occurrence.

3.4.5. Uncertainties

3.4.5.1. Uncertainties in PSSs failure

The uncertainties[14] affecting the operation of the PSSs impacts the process towards their reliability evaluation. These uncertainties stem mainly from the deviations of the natural forces or physical principles, upon which they rely (e.g., gravity and density difference), from the expected conditions due to the inception of T-H factors impairing the system performance or to changes of the initial and boundary conditions.

The uncertainties concerned with the reliability of PSSs are both stochastic, because of the randomness of phenomena occurrence, and of epistemic nature, i.e. related to the state of knowledge about the phenomena, because of the scarcity of operational and experimental data. The broad categories of uncertainties to be addressed are the following:

[14] There are two general types of uncertainty that must be separately accounted [86]:

- **Aleatory uncertainty** – also called irreducible uncertainty or stochastic variability. We typically refer to this type of uncertainty as simply variability. Aleatory uncertainty (or variability) is naturally characterized, quantified, and communicated in terms of probability. Common examples are:
  - Variability in manufacturing processes;
  - Material composition;
  - Test conditions;
  - Environmental factors.

  This lead to variability in component or system performance.

- **Epistemic uncertainty** – also called reducible uncertainty. This type of uncertainty is due to lack of knowledge or incomplete knowledge. Common examples of epistemic uncertainty are:
  - So-called model form uncertainty (that is, uncertainty in how well the equations in the model capture the physical phenomena of interest);
  - Both known and unknown unknowns in scenarios;
  - Poor-quality physical test data.

  In some circumstances, epistemic uncertainty may be quantified by using probabilistic and statistical concepts or by using other methods.

- **Geometrical properties:** it concerns with the variations between the as built system layout and the design utilized in the analysis. Examples are:
    - Piping layout (e.g. suction pipe inclination at the inlet of the heat exchanger, in the isolation condenser reference configuration);
    - Heat loss modes of failure.
- **Material properties:** material properties are very important in estimating the failure modes concerning, e.g., undetected leakages and the heat loss.
- **Phenomenological analysis:** the natural circulation failure assessment is very sensitive to uncertainties in parameters and models used in the T-H analysis of the system. Some of the sources of uncertainties include, e.g., the
    - Definition of failure of the system used in the analysis;
    - Simplified model used in the analysis;
    - Analysis method and the analysis focus of failure locations and modes;
    - Selection of the parameters affecting the system performance.

The first and second groups fall within the category of aleatory uncertainties because they represent the stochastic variability of the analysis inputs and they are not reducible [81].

3.4.5.2. Uncertainties in BE T-H codes

Using T-H system code we need to consider also the following uncertainties that can be grouped as [89][82]:

- **Code or model uncertainties:** Examples are simplification in the field equations, uncertainties in material properties, assumption that fully developed flow exists in the system, etc.
- **Representation uncertainties:** The discretization of the system to obtain the control volumes that are represented by the field equations.
- **Scaling uncertainty:** use of data developed in scaled-down experiments and, e.g., reliance on scaling laws to apply the data results to full scale systems.
- **Plant uncertainty:** boundary and initial conditions for the nuclear power plant condition under consideration (e.g. core power).
- **User effect:** there are several reasons by which the users has influence in the predicted code results: system nodalization; code option physical model parameters; input parameters related to specific system characteristics, input parameters needed for specific components, specification of initial and boundary conditions, specification of state and transport property data, selection of parameters determining time step sizes, code input errors [83].

The uncertainty of the code can affect the prediction of the system operation/performance and therefore its reliability.

3.4.6. Computation of system reliability via numerical calculations

For each accident sequence, the needed propagation of uncertainty is performed via numerical calculations using validated state-of-the-art codes (hence one accident sequence leads to *n* simulations).

For deterministic approaches, the final conclusion is whether reliability is demonstrated or whether it failed.

For probabilistic approaches, the failure probability conditional to each scenario frequency of occurrence is computed. The number of calculations mainly depends on the number of accident sequences, FOMs, and confidence level whereas cannot depend on the number of input uncertainty parameters if non-parametric methods are used. For probabilistic approaches, it also depends on the reliability target defined in the analysis. Provided the current powerful computational capabilities, this number is not critical to the PSSs reliability method application.

It should be noted that the number of calculations with T-H codes can remain critical. The use of mathematical surrogate models may offer a solution to reduce calculation time to a realistic duration. However, the application of surrogate models in the nuclear field is still under development, and a solid validation methodology must be applied. At present, some industrial applications can be observed[84][85], but they are not yet considered in the regulatory process.

3.4.7. Confidence of the results

The confidence in the results obtained from the application of the different methodologies depends mainly on the robustness of the model (if reliability is demonstrated via analytical methods), on the comprehensive identification of driving parameters impacting the system performance and on the correct evaluation of their uncertainties.

Three main challenges for PSS reliability have been identified:

- **Identification, quantification and implementation of model uncertainty**

  PSS reliability highly depends on environmental conditions. This is why the experiments taken for the demonstration that the analytical models capture the system performance well should comprise the previously identified list of scenarios.

  Uncertainties relate to both the system parameters, e.g. natural condensation heat transfer coefficient on vertical surfaces, and the model itself, e.g. heat transferred in condensation conditions on vertical surfaces, must be identified and quantified via comparison of analytical results vs experimental results.

- **Lack of sufficient experimental database**

  Due to the high dependency of driving forces from the environmental conditions, i.e. initial and boundary conditions characterising challenging scenarios, development of an extensive experimental database is not easy to tackle. In other words, PSS reliability evaluation is “hardware-dependent” and “software-dependent”: as for the former, it means that reliability demonstration is not linked to the passive phenomena driving the system performance—e.g. buoyancy flowrate in a two-phase loop—, but that it depends on the actual system configuration. As for the latter, it means that the PSS reliability is very sensitive to the boundary conditions imposed by the accident sequence.

- **Lack of sufficiently validated analytical models**

  Issues related to the previous one, formula (correlation) of passive physical phenomena used by the PSS must be implemented or added in the code. [86] [81][82]

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

4. Conclusions

4.1. Summary of the Deliverable Findings

PSSs, based on inherent physical principles and without moving parts after activation, are less susceptible to conventional hardware failures but can still suffer from functional (or "phenomenological") failure. This occurs when, due to low driving forces and high sensitivity to conditions, the system cannot perform its safety function as expected despite intact hardware. Uncertainty over possible operational scenarios means that, under certain external or internal conditions, loads may exceed PSS capacity or narrow safety margins. Specific conditions, such as the presence of non-condensable gases, leaks, heat losses, suboptimal piping layout, or fouling can contribute, requiring targeted deterministic analysis and suitable investigative methods to assess their reliability.

A detailed and independent review of the advantages and disadvantages of existing methods (PSA and DSA) and specific approaches to PSS reliability assessment (RMPS, REPAS, APSRA, ROAAM+) was carried out and elements to be considered here as "challenging" were highlighted. In addition, specific examples of the application of individual approaches and results in the reliability analysis of selected technology were presented. The key findings from the review carried out are described in previous chapters and are also summarized in Table 11 in section 3.

Generally speaking, reliability stands for the evidence provided for safety demonstration of the component performing according to the expectations (in terms of the safety function, performance criteria during a specific time window). Reliability assessment can be performed either via deterministic or probabilistic approaches and is based on a common ground (system and function definitions, relevant parameters identification, validated modelling, and sensitivity analysis). Choosing one method or the other depends on multiple reasons, the most important being the type of regulatory framework and the safety approach implemented.

Some of the challenges of assessing functional reliability of the PSSs are the uncertainty surrounding the full range of operational scenarios that a PSS may experience, and the physical conditions that can affect the operation of the system. The combination of a large number of relevant parameters can lead to difficulties in identifying rare failure cases. Furthermore the validation of the theoretical model, when reliability is demonstrated via analytical methods, is also essential and should include comparison against experimental tests and feedback available from plant in operation. Before evaluating functional reliability, it is necessary to define the reliability target of the system for the relevant scenarios by a preliminary PSA taking into account all the components involved in the scenario, e.g., initiating event frequency, the expected reliability of active systems preceding and succeeding PSS in the PSA sequence, etc.

All future NPPs (including SMRs) are characterized by the extensive inclusion of PSSs in their design, so it can be expected that findings and conclusions of this deliverable will be beneficial for the whole nuclear community because the last similar and strongly coordinated effort was done more than 10 years ago (see IAEA TECDOC-1752 [1]).

4.2. Impact on WP4 and Project Activities

In accordance with the EASI-SMR project proposal, it is assumed that a reliability analysis for two (real) technologies will be performed within the framework of WP4 tasks. The first of these

is the ELSMOR II facility from SIET (Italy), whose ability to remove the heat from the primary circuit using a passive loop will be tested using the proven RMPS/REPAS approach. The second one will be the HWAT facility from KTH (Sweden), where the ROAAM+ approach is assumed to be used.

The impact of the D4.1 Deliverable on ongoing or future activities in WP4 is therefore obvious, as all of the above-mentioned approaches (along with their advantages and disadvantages) have been discussed in detail in the previous text, and the presented conclusions therefore form a strong basis and source of knowledge for their future application in WP4.

4.3. Recommendations for WP4 tasks

The review shows that both methodologies (i.e. RMPS/REPAS and ROAAM+) planned for application in WP4 represent currently well established approaches to PSS reliability assessment. All participants in subsequent tasks in WP4 are then recommended to take into account the identified facts to avoid possible problems in their application, especially in tasks T4.2 to T4.5. In addition, the use of both mentioned approaches in WP4 will serve to verify the identified facts and to further improve their related steps.

5. Bibliography

[1] IAEA: Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors. IAEA-TECDOC-1752. Vienna 2014.
[2] NEA, Status Report on Reliability of Thermal-Hydraulic Passive Systems with an Addendum of PERSEO Benchmark Report, vol. 2, NEA/CSNI/R(2021), Paris, 2021.
[3] European SMR pre-Partnership Reports, Workstream 5- Research, Development, and Innovation Roadmap: https://snetp.eu/wp-content/uploads/2023/07/European-SMR-pre-Partnership-WS5-report-and-roadmap-30-June-2023.pdf.
[4] Technical area 6 - Innovative Light Water Reactor Designs & Technologies - SNETP
[5] https://www.nuward.com/en
[6] https://www.steadyenergy.com/solution
[7] https://cordis.europa.eu/project/id/847553
[8] https://cordis.europa.eu/project/id/945063
[9] https://cordis.europa.eu/project/id/945275
[10] https://cordis.europa.eu/project/id/101059853
[11] https://cordis.europa.eu/project/id/101059479
[12] IAEA: Safety of Nuclear Power Plants: Design. Specific Safety Requirements. No. SSR-2/1 (Rev. 1). Vienna 2016.
[13] IAEA: Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants. No. SSG-3 (Rev. 1). Vienna 2024.
[14] Sergey Galushin, Lisa Ranlöf, Ola Bäckström, Yvonne Adolfsson, Dmitry Grishchenko, Pavel Kudinov, Anders Riber Marklund, Joint Application of Risk Oriented Accident Analysis Methodology and PSA Level 2 to Severe Accident Issues in Nordic BWR, PSAM-14, 2018.
[15] Sergey Galushin, Anders Riber Marklund, Anders Olsson, Ola Bäckström, Dmitry Grishchenko, Pavel Kudinov, Treatment of Phenomenological Uncertainties in Level 2 PSA for Nordic BWR Using Risk Oriented Accident Analysis Methodology, PSAM-16, 2022.
[16] Burgazzi, L. (2011, March). Reliability prediction of passive systems based on multiple failure measures modelling. In ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Wilmington, NC.
[17] Yu Yu, Guohang Ma, Zulong Hao, Shengfei Wang, Fenglei Niu, Enrico Zio, Correlation analysis for screening key parameters for passive system reliability analysis, Annals of Nuclear Energy, Volume 77, 2015, Pages 23-29, ISSN 0306-4549.
[18] Samuel Abiodun Olatubosun, Zhijian Zhang, Multivariate analysis of critical parameters influencing the reliability of thermal-hydraulic passive safety system, Nuclear Engineering and Technology, Volume 51, Issue 1, 2019, Pages 45-53, ISSN 1738-5733.
[19] Jintae Kim, Moosung Jae, A study on reliability assessment of a decay heat removal system for a sodium-cooled fast reactor, Annals of Nuclear Energy, Volume 120, 2018, Pages 534-539, ISSN 0306-4549.
[20] Solanki, Riddhi & Kulkarni, Harshavardhan & Singh, Suneet & Varde, Pv & Verma, A.. (2020). Reliability assessment of passive systems using artificial neural network based response surface methodology. Annals of Nuclear Energy. 144. 107487. 10.1016/j.anucene.2020.107487.
[21] Pedroni, N. and E. Zio (2017), An Adaptive metamodel-Based Subset Importance Sampling approach for the assessment of the functional failure probability of a thermalhydraulic passive system, Applied Mathematical Modelling, Vol. 48, pp 269-288.
[22] L. Puppo, N. Pedroni, A. Bersano, F. Di Maio, C. Bertani, E. Zio, Failure identification in a nuclear passive safety system by Monte Carlo simulation with adaptive Kriging, Nuclear Engineering and Design, Volume 380, 2021, 111308, ISSN 0029-5493.
[23] Kyungho Jin, Hyeonmin Kim, Seunghyoung Ryu, Seunggeun Kim, Jinkyun Park, An approach to constructing effective training data for a classification model to evaluate the

reliability of a passive safety system, Reliability Engineering & System Safety, Volume 222, 2022, 108446, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2022.108446.
[24] Arun Kumar Nayak, Amit Chandrakar and Gopika Vinod. A review: passive system reliability analysis – accomplishments and unresolved issues. Frontiers in Energy Research. October 2014.
[25] Acacia Brunett, David Grabaskas, Matthew Bucknor. Dynamic Methods for the Assessment of Passive System Reliability. Probabilistic Safety Assessment and Management PSAM 12, June 2014, Honolulu, Hawaii.
[26] A. Manish Tripathi, B. Lalit Kumar Singh, C. Suneet Singh, Dynamic reliability analysis framework for passive safety systems of Nuclear Power Plant, Annals of Nuclear Energy, Volume 140, 2020, ISSN 0306-4549.
[27] A. Masood and P. Robert, "A Predictive Dynamic Approach to Evaluating the Reliability of Passive Systems," in IEEE Access, vol. 11, pp. 93784-93792, 2023.
[28] F. Mascari, A. Bersano F. Alcaro M. Stempniewicz, L. Albright, T. Jevremovic, N. Andrews, R Gauntt, H. Austregesilo, S. Buchholz, A. Bellomo, F. D'Auria, G. Di Palma, M. Lanfredini, G. Spina, C. Bertani, M. De Salve, N. Falcone, G. Caruso, F. Giannetti, V. Narcisi, C. Choi, K. Ha, B.G. Jeon, K.H. Kang, K. Kim, H.S. Park, I. Karppinen, L.F. Lahovský, R. Meca, Z. Parduba, P.H. Lien, D.Y. Tomashchik, L. Burgazzi, C. Lombardo, P. Meloni, R. Ferri, OECD/NEA/CSNI/WGAMA PERSEO benchmark: Main outcomes and conclusions. February 2023.
[29] Nicola Pedroni, Enrico Zio, An Adaptive Metamodel-Based Subset Importance Sampling approach for the assessment of the functional failure probability of a thermal-hydraulic passive system, Applied Mathematical Modelling, Volume 48, 2017, p. 269-288.
[30] WENRA RHWG, Report Regulatory Aspects of Passive Systems, June 2018.
[31] IAEA: Safety Assessment for Facilities and Activities. General Safety Requirements. No. GSR Part 4 (Rev. 1). Vienna, 2016.
[32] Small Modular Reactors Regulators´ Forum. Working Group on Design and Safety analysis. Phase 2. Retrieved from https://www.iaea.org/sites/default/files/21/06/working_group_on_design_and_safety_analysis_phase_2_report.pdf
[33] IAEA-TECDOC-626, Safety Related Terms for Advanced Nuclear Plants. Vienna. 1991.
[34] IAEA-TECDOC-1575, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems INPRO Manual — Proliferation Resistance. Volume 5 of the Final Report of Phase 1 of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO). Rev. 1. November 2008.
[35] IAEA-TECDOC-1362, Guidance for the evaluation of innovative nuclear reactors and fuel cycles Report of Phase 1A of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO). June 2003.
[36] Ammirabile, L., Buchholz, S., & Nguyen, T. (2020). Overview of safety methodologies for innovative reactor designs, and proposal of a general methodology for LW-SMR, ELSMOR project D2.2.
[37] IAEA-TECDOC-1624, Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants. November 2009.
[38] OECD/NEA, Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants. Nuclear Regulation NEA/CNRA/R(2017)3 February 2019.
[39] STUK, Safety Design of a Nuclear Power Plant, Guide YVL B.1. Retrieved from https://www.stuklex.fi/en/ohje/YVLB-1
[40] NEA/CSNI/R(2016)14: A state-of-the-art report on scaling in system thermal hydraulics applications to nuclear reactor safety and design. March 2017.
[41] Program on Technology Innovation: Comprehensive Risk Assessment Requirements for Passive Safety Systems. EPRI, Palo Alto, CA; 2008. 1016747.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

[42] Bianchi, F., Burgazzi, L., D'Auria, F., & Ricotti, M. E. (2002). The REPAS approach to the evaluation of passive safety systems reliability. Unclassified NEA/CSNI/R (2002) 10, 133.
[43] Jafari, J., D'Auria, F., Kazeminejad, H., & Davilu, H. (2003). Reliability evaluation of a natural circulation system. Nuclear Engineering and Design, 224(1), 79-104.
[44] Pierro, F., Araneo, D., Galassi, G., & D′ Auria, F. (2009). Application of REPAS methodology to assess the reliability of passive safety systems. Science and Technology of Nuclear Installations, 2009(1), 768947.
[45] U.S. Nuclear Regulatory Commission, 2020, "TRACE v5.0 patch 6 Theory Manual".
[46] Bersano, A., Grippo, G., Agnello, G., Zio, E., & Mascari, F. (2024). Application of REPAS to analyze the sump clogging issue following a LOCA and its impact on the reliability of the ECCS long-term core cooling function. Nuclear Engineering and Design, 417, 112877.
[47] Tempesta, L. (2024). Application of the REPAS methodology to analyze the reliability of the EHRS in the decay heat removal strategy for an SMR. Master's Thesis, University of Bologna, 2024, https://amslaurea.unibo.it/32887.
[48] Ransom, V.H. et al., "RELAP5/mod3 code manuals", NUREG/CR-5535, INEL, Idaho Falls, 1995.
[49] S.S. Wilks, Determination of sample sizes for setting tolerance limits, Annals of Mathematical Statistics 12(1), pp. 91-96, 1941.
[50] S.S. Wilks, Statistical prediction with special reference to the problem of tolerance limits, Annals of Mathematical Statistics 13(4), pp. 400-409, 1942.
[51] Bajorek, S. M., & Gingrich, C. (2013). Uncertainty Methods Framework Development for the TRACE Thermal-Hydraulics Code by the US NRC (No. NEA-CSNI-R--2013-8).
[52] Marques, M., Pignatel, J. F., D'Auria, F., Burgazzi, L., Mu¨ ller, C., Cojazzi, G., & La Lumia, V. (2002, January). Reliability methods for passive safety functions. In International Conference on Nuclear Engineering (Vol. 35960, pp. 173-180).
[53] Marques, M., Pignatel, J. F., Saignes, P., D'auria, L., Muller, C., Bolado-Lavin, C., Kirchsteiger, C., La Lumina, V., Ivanov, L., Methodology for the reliability evaluation of a passive system and its integration into a probabilistic safety assessments, Nuclear Engineering and Design 235 (2005) 2612–2631.
[54] https://cathare.cea.fr/
[55] A. de Crécy, P. Bazin, H. Glaeser, T. Skorek, J. Joucla, P. Probst, K. Fujioka, B.D. Chung, D.Y. Oh, M. Kyncl, R. Pernica, J. Macek, R. Meca, R. Macian, F. D'Auria, A. Petruzzi, L. Batet, M. Perez, F. Reventos, Uncertainty and sensitivity analysis of the LOFT L2-5 test: Results of the BEMUSE programme, Nuclear Engineering and Design, Volume 238, Issue 12, 2008, Pages 3561-3578.
[56] Di Maio, F.; Pedroni, N.; Tóth, B.; Burgazzi, L.; Zio, E. Reliability Assessment of Passive Safety Systems for Nuclear Energy Applications: State-of-the-Art and Open Issues. Energies 2021, 14, 4688.
[57] G. Lorenzo, P. Zanocco, M. Gimenez, M.Marques, B. Iooss, R. Bolado Lavın, F. Pierro, G. Galassi, F. D'Auria, L. Burgazzi, Assessment of an Isolation Condenser of an Integral Reactor in View of Uncertainties in Engineering Parameters, Science and Technology of Nuclear Installations, Volume 2011, Article ID 827354.
[58] Matthew Bucknor, David Grabaskas, Acacia Brunett, Austin Grelle, Advanced Reactor Passive System Reliability Demonstration Analysis for an External Event, Nuclear Engineering and Technology Volume 49, Issue 2, March 2017, Pages 360-372.
[59] C. Bassi, M. Marques, Reliability Assessment of 2400MWth Gas-Cooled Fast Reactor Natural Circulation Decay Heat Removal in Pressurized Situations, Science and Technology of Nuclear Installations, 2008.
[60] Graeme Trundle, Reliability Assessment of Passive ICS in an SMR as part of the PSA Analysis, SH204X Master Thesis Report, TRITA-SCI-GRU 2023:208.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

[61] A.K. Nayak, M.R. Gartia, A. Antony, G. Vinod and R.K. Sinha, Reliability Analysis of a Boiling Two-phase Natural Circulation System Using the APSRA Methodology, Proceedings of ICAPP 2007, Nice, France, May 13-18, 2007.
[62] Nayak, A.K., Gartia, M.R., Antony, A., Vinod, G., Sinha, R.K., 2008. Passive system reliability analysis using APSRA methodology. Nuclear Engineering and Design.
[63] A.K. Nayak, Vikas Jain, M.R. Gartia, A. Srivastava, Hari Prasad, A. Anthony, A.J. Gaikwad, S. Bhatia, R.K. Sinha, Reliability assessment of passive containment isolation system using APSRA methodology. Annals of Nuclear Energy 35 (2008) 2270–2279.
[64] Nayak, A. K., Jain, V., Garita, M. R., Prasad, H., Antony, A., Bhatiya, S. K., et al. (2009). Reliability assessment of passive isolation condenser system of AHWR using APSRA methodology. Reliabil. Eng. Syst. Safety 94, 1064–1075. doi:10.1016/j.ress.2008.12.002.
[65] Galushin S., Ranlöf L., Bäckström O., Adolfsson Y., Grishchenko D., Kudinov P., Marklund A., Joint Application of Risk Oriented Accident Analysis Methodology and PSA Level 2 to Severe Accident Issues in Nordic BWR Probabilistic Safety Assessment and Management, PSAM-14, 2018.
[66] Galushin S., Grishchenko D., Kudinov P., Risk Analysis Framework for Severe Accident Mitigation Strategy in Nordic BWR: An Approach to Communication and Decision Making, PSA 2017, Pittsburgh, PA, 2017.
[67] Grishchenko D., Galushin S., Basso S., Kudinov P., Application of TEXAS-V surrogate model to assessment of the containment failure risk due to steam explosion in a Nordic type BWR NUTHOS-11: The 11th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, Operation and Safety, Sep-13, 2016.
[68] Galushin S., Grishchenko D., Kudinov P., The Effect Of Vessel failure And Melt Release On Risk Of Containment Failure Due To Ex-Vessel Steam Explosion In Nordic BWR, The Proceedings of the International Conference on Nuclear Engineering (ICONE), 2019.
[69] Galushin S., Grishchenko D., Kudinov P., Implementation of Probabilistic Framework of Risk Analysis Framework for Assessment of Severe Accident Management Effectiveness in Nordic BWR, Reliability Engineering & System Safety, Vol. 203, 2019.
[70] Kudinov P., Galushin S., Grishchenko D., Yakush S., Adolfsson Y., Ranlöf. L, Bäckström O., Enerholm A., Scenarios and phenomena affecting risk of containment failure and release characteristics Nordic nuclear safety research, Roskilde, 2017.
[71] Galushin S., Grishchenko D., Kudinov P., Quantification of the uncertainty due to state-of-knowledge using ROAAM+ framework for Nordic BWRs, PSAM-16, Charleston, United States, 834-840, 2019.
[72] Galushin S., Grishchenko D., Kudinov P., Risk Analysis Framework for Decision Support for Severe Accident Mitigation Strategy in Nordic BWR Probabilistic Safety Assessment and Management PSAM-14, 2018.
[73] Kudinov P., Galushin S., Grishchenko D., Yakush, S., Development of risk-oriented accident analysis methodology (ROAAM+) for assessment of ex-vessel severe accident management effectiveness, NURETH-18, 2519-2535, 2019.
[74] Grishchenko D., Galushin S., Kudinov P., Risk of containment failure due to ex-vessel steam explosion for Nordic BWRs, NURETH-18, 2019.
[75] Galushin S., Grishchenko D., Kudinov P., Analysis of the Effect of Vessel Failure and Melt Release on Risk of Containment Failure Due to Ex-Vessel Steam Explosion in Nordic Boiling Water Reactor Using ROAAM+ Framework, Journal of Nuclear Engineering and Radiation Science, 6, 2020.
[76] Galushin S., Marklund, Anders Riber, Olsson, Anders, Bäckström, Ola, Grishchenko D., Kudinov P., Treatment of Phenomenological Uncertainties in Level 2 PSA for Nordic BWR Using Risk Oriented Accident Analysis Methodology, PSAM-16, 2022.
[77] NUREG-2300, "PRA (Probabilistic Risk Assessments) Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants".

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

[78] [NUREG-0492, "Fault Tree Handbook", U.S. Nuclear Regulatory Commission, 1981.
[79] IAEA (2016). IAEA-TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants. Vienna: IAEA.
[80] IAEA (2023). IAEA Nuclear Energy Series NR-T-2.16, Methodologies for Assessing Pipe Failure Rates in Advanced Water Cooled Reactors. Vienna: IAEA.
[81] Burgazzi, L., Addressing the uncertainties related to passive system reliability, Progress in Nuclear Energy 49 (2007).
[82] Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, IAEA, safety report 52.
[83] https://www.oecd-nea.org/upload/docs/application/pdf/2020-01/csni-r1994-35.pdf.
[84] Presentation of Etienne Mullin Passive Safety System Reliability for the NuScale SMR Consultancy meeting IAEA 03/2025.
[85] Presentation of EDF Framatome Addressing Industrial Challenges in Passive System Reliability Assessment for PSA Model Consulatncuy meeting meeting IAEA 03/2025.
[86] Kathleen Diegert, Scott Klenke, George Novotny, Robert Paulsen, Martin Pilch, and Timothy Trucano, Toward a More Rigorous Application of Margins and Uncertainties within the Nuclear Weapons Life Cycle – A Sandia Perspective, SAND2007-6219 December 2007.
[87] IAEA (2019). Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide, SSG-2 (Rev. 1), IAEA, Vienna
[88] https://cordis.europa.eu/project/id/FIKS-CT-2000-00073
[89] INTERNATIONAL ATOMIC ENERGY AGENCY, Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, IAEA, Vienna (2008)
[90] NEA/CSNI/R(94)35, User Effects on the transient system code calculations, OECD/NEA, 1995, https://www.oecd-nea.org/upload/docs/application/pdf/2020-01/csni-r1994-35.pdf
[91] IAEA Nuclear Safety and Security Glossary, 2022 (Interim) Edition IAEA-NSS-GLO

6.Appendices

6.1. Glossary of Terms

Table 10: Glossary of Terms

Term	Definition
Actual components	A physical component of the system having material existence such as pipes, valves, heat exchangers, etc.
Adjoint algorithm	A numerical algorithm to evaluate derivatives in the reverse direction.
Adjoint operator	An operator B such that the inner product (Ax,y) and (x,By) are equal for a given operator A and for all elements x and y of a Hilbert space (mathematical space endowed with a property of inner product).
Aleatory uncertainty	Aleatory uncertainty is uncertainty inherent in a phenomenon and is of relevance for events or phenomena that occur in a random manner such as random failures of items of equipment.
Availability	The probability that a component, system, or structure is performing intended function at given time and under given conditions.
Available	The state of a system, structure or component being able to perform its intended function, under given conditions and at a given time.
Benchmark(ing)	Comparative exercise in which predictions of different computer codes and users for a given physical problem are compared with each other or with the results of a carefully controlled experimental study.
Code uncertainty	Uncertainties in the results of code prediction due to the approximations of physical models, correlations, numerical solution schemes, etc.
Conditional probability	The probability of an event, given that another event is known to have occurred.
Continuous probability density function	Probability density function of a continuous random variable.
Continuous random variable	A random variable takes values from an uncountable set, and the probability of any one value is zero, but a set of values can have positive probability.
Cumulative distribution function	Function giving, for all value x, the probability that the random variable X will be less than or equal to x.
Discrete probability density function	A list of probabilities associated with each possible values of the discrete random variable.
Discrete random variable	A random variable which takes values from a countable set of specific values, each with some probability greater than zero.
Dynamic PSA	PSA that utilises dynamic methods, such as dynamic fault trees, Markov models, and the dynamic flowgraph methodology, that can account for the coupling between systems through explicit consideration of time in system evolution and interaction.
Elicitation process	A heuristic process for gathering evidence and data or answering questions on issues/problems of concern.
Epistemic uncertainty	Epistemic uncertainty is uncertainty attributable to incomplete knowledge about a phenomenon, which affects the ability to model it.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Term	Definition
Expert judgement	An approach for soliciting informed opinions from individuals with particular expertise.
Failure	The loss of ability of a system, structure or component to perform a required function during required time.
Failure analysis	The logical, systematic examination of a system to identify the probability, causes, and consequences of potential failures.
Failure cause	The circumstances during design, manufacturing or use which have induced or activated a failure mechanism.
Failure criteria	Logical and/or numerical relationships which define the system failure or physical conditions that define the component or structure failure.
Failure effect	The consequences a failure has on the operation, function, or status of a system.
Failure mechanism	The physical, chemical, electrical, thermal or other process that causes a failure.
Failure mode	Distinguishing physical or behavioural characteristic that can be associated with a failure.
Failure mode and effect analysis (FMEA)	Procedure by which each potential failure mode in a system is analysed to determine its effect on the system and classify them according to its severity
Failure point	The most probable point of the failure surface which is at the minimal distance of the origin in a Gaussian space.
Failure rate	A function that describes the number of failures to a system, device or component that can be expected to take place over a given unit of time.
Failure surface	The surface defined by limit state function in multi-dimensional space that demarcates the state of failure from the state of success of the system, where the limit state function is zero.
Fault Tree	A graphical representation of an undesired event caused by a combination of factors arising from equipment failure, human error, or environmental events.
Fault Tree Analysis	A deductive technique in which an undesired state of a system is analysed using boolean logic to combine a series of lower-level events.
First-order reliability method (FORM)	Method of evaluation of the failure probability where the failure surface is approximated by a tangent hyper-plane passing through the design point.
Functional failure (in a passive safety system)	Failure of the passive system to perform it's intended function due to deviations of process parameters or unknown phenomena's.
Fuzzy logic	An extension of the concept of a set in which the characteristic function which determines membership of an object in the set is not limited to 1 (a member) or 0 (not a member), but can take on any value between 0 and 1 as well.
Fuzzy set	The logic of approximate reasoning bearing the same relation to approximate reasoning that two valued logic to precise reasoning.
Global sensitivity	Sensitivity analysis which apportions the output variability to the variability of the input parameters when they vary in their whole uncertainty domains. This uncertainty is generally described using probability densities for factors.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Term	Definition
Hardware failure (in a passive safety system)	Failure of a component or structure that can impact operation of the passive system.
HAZOP – Hazard and operability study	Structured and systematic examination of all credible deviations from normal conditions in a process or operation in order to identify and evaluate potential hazards and operability problems.
Human error	An inappropriate or undesirable human decision or behaviour that reduces, or has the potential for reducing, effectiveness, safety, or system performance.
Limit state	The condition beyond which a safety system or structure is deemed to have failed.
Limit state function	A mathematical expression that divides an n-dimensional probability space into failure domain and safe domain.
Local sensitivity	Sensitivity analysis performed by estimating the partial derivatives of the output with respect to each input parameter around given nominal values. It gives a local measure of the output sensitivity which may vary with the nominal value.
Mission time	Time interval during which a system has to carry out its safety function after it is demanded.
Passive component	A component whose operation does not depend on operation of other systems or components, e.g. control system, energy source etc.
Passive system	Either a system which is composed of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation.
Performance indicator	A numerical value representing the performance of a safety system.
Perturbation theory	The study of solution to differential equations based on the assumption that perturbations in the given conditions of a problem cause only small changes in the solution.
Probabilistic safety assessment	A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.
Probability density function	Derivative, if exists, of the cumulative distribution function of a random variable.
Propagation of uncertainty	Evaluation of the effects of the input parameters uncertainty on the output uncertainty.
Reliability	The probability that a system will perform its intended function in a satisfactory manner for a given period of time [0, t], when used under specified operating conditions.
Reliability Analysis	A quantification of the sources of failures in a system, with emphasis on the most significant contributors towards the overall system unreliability, in order to correct them and therefore improve the reliability of the fielded system.
Reliability index	A measure of the distance that the mean is away from the zero of the limit state function.
Response surface	Simplified mathematical expression as a function of input variables designed to approximate outcomes of complex mathematical model or possible experimental outcomes.

Term	Definition
Risk	A multi-attribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with actual or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences. In mathematical terms, this can be expressed generally as a set of triplets, R = {Si ; Pi; Xi}, where Si is an identification or description of a scenario i, Pi is the probability of that scenario and Xi is a measure of the consequence of the scenario.
Risk-informed approach	A safety focused approach aimed at consideration of risk insights together with other factors effecting safety with the main goal to ensure that any decision that affecting safety is sound.
Second order reliability method (SORM)	Method of evaluation of the failure probability where the failure surface is approximated by a tangent hyper-parabolic surface passing through the design point.
Unavailability	The complement of availability.
Uncertainty	**General**: 1. A state of having limited knowledge where it is impossible to exactly describe existing state or future outcome 2. The extent of our knowledge or ignorance **Statistics**: The estimated amount by which an observed or calculated value may depart from true value.
Uncertainty analysis	An analysis to estimate the uncertainties and error bounds of the quantities involved in, and the results from, the solution of a problem.
Unreliability	The complement of reliability.
Virtual components	A phenomenological component of the system having no material existence which functions based on natural laws such as gravity, buoyancy, etc.

Note to Table 10:

1. Terms were taken from [1] and some adjusted as needed.
2. Some of the terms are not used in the text, but are directly related to performing PSS reliability analyses and may therefore appear in subsequent stages of the project.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

6.2. Questionnaire on current approaches for PSS reliability assessment

Table 11: Questionnaire on current methods for PSS reliability assessment

Category	Question	REPAS	RMPS	APSRA	ROAAM+
General	**Objective**	Evaluation of functional reliability of PSSs. Similar to RMPS.	Evaluation of functional reliability of PSSs. Similar to REPAS.	Assessment of PSS reliability with functional failures directly linked with malfunctions/failures in mechanical components of PSS and related systems.	Analysis of SA phenomenology and quantification of associated risks
	Approach	BE codes with uncertainty analysis focused on functional failures.	Probabilistic approach for T-H PSSs.	Metamodeling techniques with separate treatment of model and parameter uncertainties.	Structured approach using hierarchical probabilistic framework with expert judgment
Accessibility	**Availability of publications to describe the method**	Well document both in theory and applications.	Well document both in theory and applications.	Very limited	No papers or reports on applications to PSSs, just regular application to SA phenomena
	Right of uses	Open	Open	Open	Open
Feedback of application	**Already applied to nuclear area as exercise**	Yes - Applied to several Gen III+ and Gen IV PSSs designs	Yes - Applied in 5th EU FP and natural circulation studies	Yes - Primarily applied to AHWR and other advanced reactor designs	Yes - Applied to SA scenarios in various reactor designs
	Already applied to nuclear area in safety demonstration and	Limited - Primarily research applications	Moderate - Some regulatory consideration in European context	Yes - Particularly in Indian regulatory context	Yes in Nordic plants for SA phenomena, unclear for PSSs.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

	regulatory feedback				
	Already applied to other industrial domains than Nuclear	No	No	No	No
	Developed but not applied	No	No	No	No
Integration in safety demonstration or passive systems design	**Output Type**	Functional reliability failure probability.	Similar to REPAS though also applied in PRA	Failure frequency	Probabilistic evaluation of phenomenological scenarios
	Integration with PSA	It depends on the specifics of the application: sometimes a direct implementation in PRA is feasible, but sometimes a compromise is necessary between functional reliability requirement (PSA) and architecture and sizing of the system	Explicitly addressed in literature though same shortcomings as REPAS.	Explicitly addressed in literature.	Specialized - Focuses on Level 2 PSA phenomena
	Integration with DSA	Yes	RMPS is dedicated to probabilistic approach, some steps are common with deterministic approach	Yes, deterministic approach is used to define key parameters that can cause the system failure	
	Additional data required in the application process	Uncertainty quantification	Same as REPAS	Same as REPAS plus accident frequencies and FTA development for	Event tree frequencies from PSA and formal documentation of expert opinions on

				specific challenging scenarios	phenomenological uncertainties
	Possibility to integrate in design phase	Yes, though first it is needed to correctly distinguish between accident conditions (so-called design parameters) and epistemic parameters.	Same as REPAS	Yes.	
	Possibility to be used for licensing	Same as for design phase	Same as for design phase	Same as for design phase	Same as for design phase
Execution	**Team needed**	T-H analysts. Probabilistic engineers for probabilistic, risk-related approaches to system reliability	Same as REPAS	Same than REPAS	Same than REPAS
	Steps needed	System modelling; Nominal performance; Parameters affecting PSSs operation identification; FCs definition (performance indicators); Uncertainty quantification, identification and propagation; Reliability evaluation.	Very similar to REPAS	Identification of operational mechanism and FC Parameters affecting the operation Key parameters causing failure Failure surface generation and validation Root diagnosis Evaluation of failure probability Incorporation into CDF	Problem identification Causal relation development Scenario quantification Expert elicitation Probabilistic integration Peer review
	Workload needed	Moderate	Same as REPAS	High – involves number complex steps	High - Requires detailed phenomenological

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

					analysis and expert elicitation
	Computational Burden	Moderate	Same as REPAS	High	High - Depends on phenomenological complexity
	Tools needed	T-H system codes, experimental database, statistical analysis	Same as REPAS	Same as REPAS	Same as REPAS
	Application complexity	Moderate – Easy-to-apply steps	Same as REPAS	High – complex steps such as failure surface and root diagnosis	High - Requires multidisciplinary expertise
	Methodology complexity	Moderate – Easy-to-apply steps	Same as REPAS	High	High - Complex phenomenological and probabilistic integration
	Limitation of the methodology	Results are affected by code capability and uncertainty parameters characterization.	Same as REPAS	APSRA does not consider that the probability of failure of a physical process might be less than one. APSRA does not specify any particular methods for evaluation of failure probability.	Focuses on SA phenomena, less applicable to normal operation
	Complexity of the Execution and methodology VS output	Medium REPAS applications mainly oriented towards deterministic approaches, which do not need	High RMPS applications oriented towards probabilistic	High Probabilistic approach, hence it requires thorough	Medium Does not need such an accurate

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

		to quantify reliability, they just need to demonstrate that the SSC behaves according to the expectations.	approaches, which need to quantify reliability, so that a failure region must first be accurately identified and all the uncertainty sources quantified.	uncertainty quantification.	application like RMPS do.
Performance	**Confidence in the results**	Depends on the code capability and PDF characterization of the parameters that affect the PSS operation	Same as REPAS	High for probabilistic approaches to system reliability	
	Possibility of Sensitivity	Yes	Same as REPAS	Yes	
	Reproducibility	Yes	Yes	Yes	Moderate - Expert judgment component reduces reproducibility
	Sources of uncertainties	Parameters affecting the operation of the PSSs.	Same as REPAS	Epistemic	Phenomenological uncertainties with both aleatory and epistemic components
	Validation	Extensively applied.	Same as REPAS	Benchmarking is envisaged to confirm failure surface prediction	Extensively applied in SAs, unclear for PSSs

EASI SMR